CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

SITUATION REPORT

TLP:CLEAR
12 January 2023

Hackers Actively Exploiting Critical Control Web Panel RCE Vulnerability

Handling Caveat: *This product Recipients can share* TLP:CLEAR *information with the world; there is no limit on disclosure.*

CWP | RCE | CVE-2022-44877 | OS

Executive Summary

On 12 January 2023, the Cal-CSIC was made aware of threat actors attempting to exploit a recently patched critical vulnerability in Control Web Panel (CWP) that enables elevated privileges and remote code execution (RCE) via OS commands. Known as CVE-2022-44877, this vulnerability affects all versions of CWP software prior to the 0.9.8.1147 released. It was patched on 25 October 2022.[1]

Background

CWP is a popular for enterprise-based Linux systems and server administration tool. According to NIST, this vulnerability allows remote attackers to execute arbitrary OS commands via shell metacharacters in the login parameter. Numan Turle, a Gais Security researcher was credited with discovering and reporting the flaw to CWP developers. On 6 January 2023, exploitation of the flaw commenced following the release of a proof-of-concept (PoC).[2]

Indicators of Compromise (IOC)

- 206[.]189[.]170[.]136
- 185[.]117[.]73[.]208
- 157[.]230[.]62[.]113
- 180[.]183[.]132[.]35

Mitigation Recommendations

The Cal-CSIC recommends organizations patch their systems according to CWP.

Organization, Source, Reference, and Dissemination Information

About the Cal-CSIC	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT-1. To help us identify ways to better assist you, please submit feedback here.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients can share TLP:CLEAR information with the world; there is no limit on disclosure.
Information Needs	*HSEC 1.2; HSEC 1.3; HSEC 1.5; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.5*

[1] TheHackerNews; Ravie Lakshmanan; "Alert: Hackers Actively Exploiting Critical "Control Web Panel" RCE Vulnerability;" Accessed 12 January 2023; https://thehackernews.com/2023/01/alert-hackers-actively-exploiting.html; 12 January 2023;

[2] Github; "Centos Web Panel 7 Unauthenticated Remote Code Execution - CVE-2022-44877;" Accessed 12 January 2023; https://gist.github.com/numanturle/c1e82c47f4cba24cff214e904c227386;

Alert (AA22-047A)

More Alerts

Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

Original release date: February 16, 2022

Summary

Actions to Help Protect Against Russian State-Sponsored Malicious Cyber Activity:

- Enforce multifactor authentication.
- Enforce strong, unique passwords.
- Enable M365 Unified Audit Logs.
- Implement endpoint detection and response tools.

From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) have observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resources. These CDCs support contracts for the U.S. Department of Defense (DoD) and Intelligence Community in the following areas:

- Command, control, communications, and combat systems;
- Intelligence, surveillance, reconnaissance, and targeting;
- Weapons and missile development;
- Vehicle and aircraft design; and
- Software development, data analytics, computers, and logistics.

Historically, Russian state-sponsored cyber actors have used common but effective tactics to gain access to target networks, including spearphishing, credential harvesting, brute force/password spray techniques, and known vulnerability exploitation against accounts and networks with weak security. These actors take advantage of simple passwords, unpatched systems, and unsuspecting employees to gain initial access before moving laterally through the network to establish persistence and exfiltrate data.

In many attempted compromises, these actors have employed similar tactics to gain access to enterprise and cloud networks, prioritizing their efforts against the widely used Microsoft 365 (M365) environment. The actors often maintain persistence by using legitimate credentials and a variety of malware when exfiltrating emails and data.

These continued intrusions have enabled the actors to acquire sensitive, unclassified information, as well as CDC-proprietary and export-controlled technology. The acquired information provides significant insight into U.S. weapons platforms development and deployment timelines, vehicle specifications, and plans for communications infrastructure and information technology. By acquiring proprietary internal documents and email communications, adversaries may be able to adjust their own military plans and priorities, hasten technological development efforts, inform foreign policymakers of U.S. intentions, and target potential sources for recruitment. Given the sensitivity of information widely available on unclassified CDC networks, the FBI, NSA, and CISA anticipate that Russian state-sponsored cyber actors will continue to target CDCs for U.S. defense information in the near future. These agencies encourage all CDCs to apply the recommended mitigations in this advisory, regardless of evidence of compromise.

For additional information on Russian state-sponsored cyber activity, see CISA's webpage, Russia Cyber Threat Overview and Advisories.

Click here for a PDF version of this report.

Threat Details

Targeted Industries and Assessed Motive

Russian state-sponsored cyber actors have targeted U.S. CDCs from at least January 2020, through February 2022. The actors leverage access to CDC networks to obtain sensitive data about U.S. defense and intelligence programs and capabilities. Compromised entities have included CDCs supporting the U.S. Army, U.S. Air Force, U.S. Navy, U.S. Space Force, and DoD and Intelligence programs.

During this two-year period, these actors have maintained persistent access to multiple CDC networks, in some cases for at least six months. In instances when the actors have successfully obtained access, the FBI, NSA, and CISA have noted regular and recurring exfiltration of emails and data. For example, during a compromise in 2021, threat actors exfiltrated hundreds of documents related to the company's products, relationships with other countries, and internal personnel and legal matters.

Through these intrusions, the threat actors have acquired unclassified CDC-proprietary and export-controlled information. This theft has granted the actors significant insight into U.S. weapons platforms development and deployment timelines, plans for communications infrastructure, and specific technologies employed by the U.S. government and military. Although many contract awards and descriptions are publicly

accessible, program developments and internal company communications remain sensitive. Unclassified emails among employees or with government customers often contain proprietary details about technological and scientific research, in addition to program updates and funding statuses. See figures 1 and 2 for information on targeted customers, industries, and information.

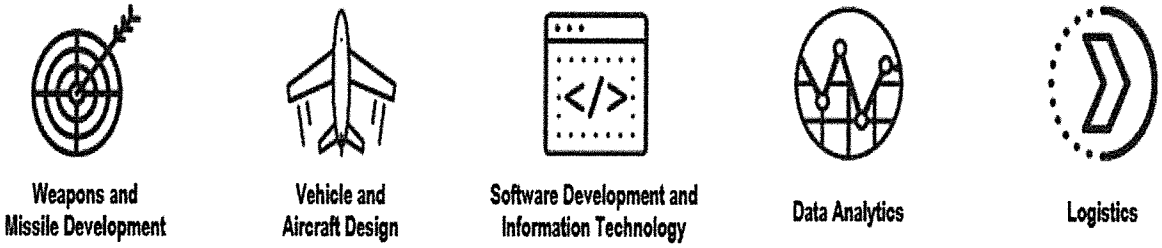


Figure 1. Targeted Industries

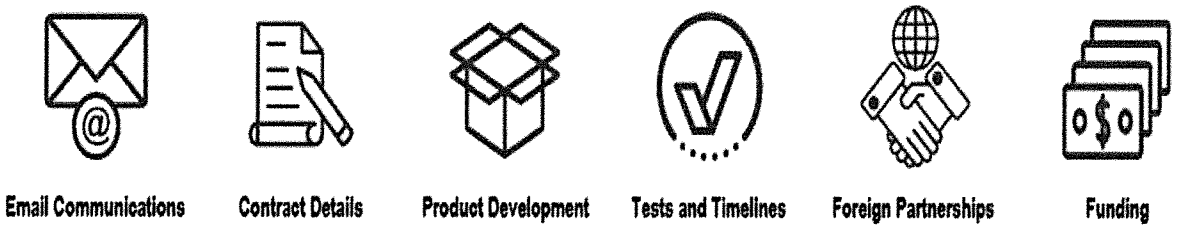


Figure 2. Exfiltrated Information

Threat Actor Activity

Note: *This advisory uses the MITRE ATT&CK® for Enterprise framework, version 10. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques. See the Tactics, Techniques, and Procedures (TTPs) section for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.*

Initial Access

Russian state-sponsored cyber actors use brute force methods, spearphishing, harvested credentials, and known vulnerabilities to gain initial access to CDC networks.

- Threat actors use brute force techniques [T1110] to identify valid account credentials [T1589.001] for domain and M365 accounts. After obtaining domain credentials, the actors use them to gain initial access to the networks. ***Note:*** *For more information, see joint NSA-FBI-CISA Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments.*
- Threat actors send spearphishing emails with links to malicious domains [T1566.002] and use publicly available URL shortening services to mask the link [T1027].

Embedding shortened URLs instead of actor-controlled malicious domains is an obfuscation technique meant to bypass virus and spam scanning tools. The technique often promotes a false legitimacy to the email recipient, increasing the probability of a victim's clicking on the link.

- The threat actors use harvested credentials in conjunction with known vulnerabilities—for example, CVE-2020-0688 and CVE-2020-17144—on public-facing applications [T1078, T1190], such as virtual private networks (VPNs), to escalate privileges and gain remote code execution (RCE) on the exposed applications.[1] In addition, threat actors have exploited CVE-2018-13379 on FortiClient to obtain credentials to access networks.
- As CDCs find and patch known vulnerabilities on their networks, the actors alter their tradecraft to seek new means of access. This activity necessitates CDCs maintain constant vigilance for software vulnerabilities and out-of-date security configurations, especially in internet-facing systems.

Credential Access

After gaining access to networks, the threat actors map the Active Directory (AD) and connect to domain controllers, from which they exfiltrate credentials and export copies of the AD database `ntds.dit` [T1003.003]. In multiple instances, the threat actors have used Mimikatz to dump admin credentials from the domain controllers.

Collection

Using compromised M365 credentials, including global admin accounts, the threat actors can gain access to M365 resources, including SharePoint pages [T1213.002], user profiles, and user emails [T1114.002].

Command and Control

The threat actors routinely use virtual private servers (VPSs) as an encrypted proxy. The actors use VPSs, as well as small office and home office (SOHO) devices, as operational nodes to evade detection [T1090.003].

Persistence

In multiple instances, the threat actors maintained persistent access for at least six months. Although the actors have used a variety of malware to maintain persistence, the FBI, NSA, and CISA have also observed intrusions that did not rely on malware or other persistence mechanisms. In these cases, it is likely the threat actors relied on possession of legitimate credentials for persistence [T1078], enabling them to pivot to other accounts, as needed, to maintain access to the compromised environments.

Tactics, Techniques, and Procedures

The following table maps observed Russian state-sponsored cyber activity to the MITRE ATT&CK for Enterprise framework. Several of the techniques listed in the table are based on observed procedures in contextual order. Therefore, some of the tactics and techniques

listed in their respective columns appear more than once. See Appendix A for a functional breakdown of TTPs. ***Note:*** *for specific countermeasures related to each ATT&CK technique, see the Enterprise Mitigations section and MITRE D3FEND™.*

Table 1: Observed Tactics, Techniques, and Procedures (TTPs)

Tactic	Technique	Procedure
Reconnaissance [TA0043] **Credential Access [TA0006]**	Gather Victim Identity Information: Credentials [T1589.001] Brute Force [T1110]	Threat actors used brute force to identify valid account credentials for domain and M365 accounts. After obtaining domain credentials, the actors used them to gain initial access.
Initial Access [TA0001]	External Remote Services [T1133]	Threat actors continue to research vulnerabilities in Fortinet's FortiGate VPN devices, conducting brute force attacks and leveraging CVE-2018-13379 to gain credentials to access victim networks. [2]
Initial Access [TA0001] **Privilege Escalation [TA0004]**	Valid Accounts [T1078] Exploit Public-Facing Application [T1190]	Threat actors used credentials in conjunction with known vulnerabilities on public-facing applications, such as virtual private networks (VPNs)—CVE-2020-0688 and CVE-2020-17144—to escalate privileges and gain remote code execution (RCE) on the exposed applications. [3]
Initial Access [TA0001] **Defense Evasion [TA0005]**	Phishing: Spearphishing Link [T1566.002] Obfuscated Files or Information [T1027]	Threat actors sent spearphishing emails using publicly available URL shortening services. Embedding shortened URLs instead of the actor-controlled malicious domain is an obfuscation technique meant to bypass virus and spam scanning tools. The technique often promotes a false legitimacy to the email recipient and thereby increases the possibility that a victim clicks on the link.

Tactic	Technique	Procedure
Initial Access [TA0001] **Credential Access [TA0006]**	OS Credential Dumping: NTDS [T1003.003] Valid Accounts: Domain Accounts [T1078.002]	Threat actors logged into a victim's VPN server and connected to the domain controllers, from which they exfiltrated credentials and exported copies of the AD database `ntds.dit`.
Initial Access [TA0001] **Privilege Escalation [TA0004]** **Collection [TA0009]**	Valid Accounts: Cloud Accounts [T1078.004] Data from Information Repositories: SharePoint [T1213.002]	In one case, the actors used valid credentials of a global admin account within the M365 tenant to log into the administrative portal and change permissions of an existing enterprise application to give read access to all SharePoint pages in the environment, as well as tenant user profiles and email inboxes.
Initial Access [TA0001] **Collection [TA0009]**	Valid Accounts: Domain Accounts [T1078.002] Email Collection [T1114]	In one case, the threat actors used legitimate credentials to exfiltrate emails from the victim's enterprise email system.
Persistence [TA0003] **Lateral Movement [TA0008]**	Valid Accounts [T1078]	Threat actors used valid accounts for persistence. After some victims reset passwords for individually compromised accounts, the actors pivoted to other accounts, as needed, to maintain access.
Discovery [TA0007]	File and Network Discovery [T1083]	After gaining access to networks, the threat actors used BloodHound to map the Active Directory.
Discovery [TA0007]	Domain Trust Discovery [T1482]	Threat actors gathered information on domain trust relationships that were used to identify lateral movement opportunities.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Threat actors used multiple disparate nodes, such as VPSs, to route traffic to the target.

Detection

The FBI, NSA, and CISA urge all CDCs to investigate suspicious activity in their enterprise and cloud environments. ***Note:*** *for additional approaches on uncovering malicious cyber activity, see joint advisory Technical Approaches to Uncovering and Remediating Malicious Activity, authored by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.*

Detect Unusual Activity

Implement robust log collection and retention. Robust logging is critical for detecting unusual activity. Without a centralized log collection and monitoring capability, organizations have limited ability to investigate incidents or detect the threat actor behavior described in this advisory. Depending on the environment, tools and solutions include:

- Cloud native solutions, such as cloud-native security incident and event management (SIEM) tools.
- Third-party tools, such as Sparrow, to review Microsoft cloud environments and to detect unusual activity, service principals, and application activity. ***Note:*** *for guidance on using these and other detection tools, refer to CISA Cybersecurity Advisory Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments.*

Look for Evidence of Known TTPs

- **Look for behavioral evidence or network and host-based artifacts** from known TTPs associated with this activity. To detect password spray activity, review authentication logs for system and application login failures of valid accounts. Look for frequent, failed authentication attempts across multiple accounts.
- To detect use of compromised credentials in combination with a VPS, follow the steps below:
  - **Review logs for suspicious "impossible logins,"** such as logins with changing usernames, user agent strings, and IP address combinations or logins where IP addresses do not align to the expected user's geographic location.
  - **Look for one IP used for multiple accounts,** excluding expected logins.
  - **Search for "impossible travel,"** which occurs when a user logs in from multiple IP addresses that are a significant geographic distance apart (i.e., a person could not realistically travel between the geographic locations of the two IP addresses in the time between logins). ***Note:*** *this detection opportunity can result in false positives if legitimate users apply VPN solutions before connecting to networks.*
  - **Evaluate processes and program execution command-line arguments** that may indicate credential dumping, especially attempts to access or copy the `ntds.dit` file from a domain controller.

- Identify suspicious privileged account use after resetting passwords or applying user account mitigations.
- **Review logs for unusual activity** in typically dormant accounts.
- **Look for unusual user agent strings,** such as strings not typically associated with normal user activity, which may indicate bot activity.

Incident Response and Remediation

Organizations with evidence of compromise should assume full identity compromise and initiate a full identity reset.

- **Reset passwords for all local accounts.** These accounts should include Guest, HelpAssistant, DefaultAccount, System, Administrator, and krbtgt. It is essential to reset the password for the krbtgt account, as this account is responsible for handling Kerberos ticket requests as well as encrypting and signing them. ***Note:*** *reset the krbtgt account twice and consecutively with a 10-hour waiting period between resets (i.e., perform the first krbtgt password reset, wait 10 hours, and then follow with a second krbtgt password reset). The krbtgt password resets may take a long time to propagate fully on large AD environments. Refer to Microsoft's AD Forest Recovery - Resetting the krbtgt password guidance and automation script for additional information. [4][5]*
- **Reset all domain user, admin, and service account passwords.**

Note: *for guidance on evicting advanced persistent threat (APT) actors from cloud and enterprise environments, refer to CISA Analysis Report Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/Microsoft 365 (M365) Compromise. Although this guidance was drafted for federal agencies compromised by the Russian Foreign Intelligence Service (SVR) via the SolarWinds Orion supply chain compromise, the steps provided in the Eviction Phase are applicable for all organizations crafting eviction plans for suspected APT actors.*

Mitigations

The FBI, NSA, and CISA encourage all CDCs, with or without evidence of compromise, to apply the following mitigations to reduce the risk of compromise by this threat actor. While these mitigations are not intended to be all-encompassing, they address common TTPs observed in these intrusions and will help to mitigate against common malicious activity.

Implement Credential Hardening

Enable Multifactor Authentication

- **Enable multifactor authentication (MFA)** for all users, without exception. Subsequent authentication may not require MFA, enabling the possibility to bypass MFA by reusing single factor authentication assertions (e.g., Kerberos authentication). Reducing the lifetime of assertions will cause account re-validation of their MFA requirements.[6] Service accounts should not use MFA. Automation and platform features (e.g., Group

Managed Service Accounts, gMSA) can provide automatic and periodic complex password management for service accounts, reducing the threat surface against single factor authentication assertions.[7]

Enforce Strong, Unique Passwords

- **Require accounts to have strong, unique passwords.** Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access.
- **Enable password management functions**, such as Local Administrator Password Solution (LAPS), for local administrative accounts. This will reduce the burden of users managing passwords and encourage them to have strong passwords.

Introduce Account Lockout and Time-Based Access Features

- **Implement time-out and lock-out features** in response to repeated failed login attempts.
- **Configure time-based access for accounts set at the admin level and higher.** For example, the Just-In-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable administrator accounts at the AD level when the account is not in direct need. When the account is needed, individual users submit their requests through an automated process that enables access to a system but only for a set timeframe to support task completion.

Reduce Credential Exposure

- **Use virtualization solutions on modern hardware and software** to ensure credentials are securely stored, and protect credentials via capabilities, such as Windows Defender Credential Guard (CredGuard) and Trusted Platform Module (TPM).[8] Protecting domain credentials with CredGuard requires configuration and has limitations in protecting other types of credentials (e.g., WDigest and local accounts).[9][10] CredGuard uses TPMs to protect stored credentials. TPMs function as a system integrity observer and trust anchor ensuring the integrity of the boot sequence and mechanisms (e.g., UEFI Secure Boot). Installation of Windows 11 requires TPM v2.0.[11] Disabling WDigest and rolling expiring NTLM secrets in smartcards will further protect other credentials not protected by CredGuard.[12][13]

Establish Centralized Log Management

- **Create a centralized log management system.** Centralized logging applications allow network defenders to look for anomalous activity, such as out-of-place communications between devices or unaccountable login failures, in the network environment.
  - Forward all logs to a SIEM tool.
  - Ensure logs are searchable.
  - Retain critical and historic network activity logs for a minimum of 180 days.

- **If using M365, enable Unified Audit Log (UAL)**—M365's logging capability—which contains events from Exchange Online, SharePoint online, OneDrive, Azure AD, Microsoft Teams, PowerBI, and other M365 services.
- **Correlate logs, including M365 logs, from network and host security devices.** This correlation will help with detecting anomalous activity in the network environment and connecting it with potential anomalous activity in M365.

In addition to setting up centralized logging, organizations should:

- **Ensure PowerShell logging is turned on.** Threat actors often use PowerShell to hide their malicious activities.[14]
- **Update PowerShell instances to version 5.0 or later** and uninstall all earlier versions of PowerShell. Logs from prior versions are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
- **Confirm PowerShell 5.0 instances have module, script block, and transcription logging** enabled.
- **Monitor remote access/Remote Desktop Protocol (RDP) logs** and disable unused remote access/RDP ports.

Initiate a Software and Patch Management Program

- **Consider using a centralized patch management system.** Failure to deploy software patches in a timely manner makes an organization a target of opportunity, increasing its risk of compromise. Organizations can ensure timely patching of software vulnerabilities by implementing an enterprise-wide software and patch management program.[15]
  - If an organization is unable to update all software shortly after a patch is released, **prioritize patches for CVEs that are already known** to be exploited or that would be accessible to the largest number of potential adversaries (such as internet-facing systems).
  - **Subscribe to CISA cybersecurity notifications and advisories** to keep up with known exploited vulnerabilities, security updates, and threats. This will assist organizations in maintaining situational awareness of critical software vulnerabilities and, if applicable, associated exploitation.
- **Sign up for CISA's cyber hygiene services**, including vulnerability scanning, to help reduce exposure to threats. CISA's vulnerability scanning service evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities.

Employ Antivirus Programs

- **Ensure that antivirus applications are installed on all organizations' computers** and are configured to prevent spyware, adware, and malware as part of the operating system security baseline.
- **Keep virus definitions up to date.**
- **Regularly monitor antivirus scans.**

Use Endpoint Detection and Response Tools

- **Utilize endpoint detection and response (EDR) tools.** These tools allow a high degree of visibility into the security status of endpoints and can be an effective defense against threat actors. EDR tools are particularly useful for detecting lateral movement, as they have insight into common and uncommon network connections for each host.

Maintain Rigorous Configuration Management Programs

- **Audit configuration management programs** to ensure they can track and mitigate emerging threats. Review system configurations for misconfigurations and security weaknesses. Having a robust configuration program hinders sophisticated threat operations by limiting the effectiveness of opportunistic attacks.[16]

Enforce the Principle of Least Privilege

- **Apply the principle of least privilege.** Administrator accounts should have the minimum permissions they need to do their tasks. This can reduce the impact if an administrator account is compromised.
- **For M365, assign administrator roles to role-based access control (RBAC)** to implement the principle of least privilege. Given its high level of default privilege, you should only use the Global Administrator account when absolutely necessary. Using Azure AD's numerous other built-in administrator roles instead of the Global Administrator account can limit assigning unnecessary privileges. ***Note:*** *refer to the Microsoft documentation, Azure AD built-in roles, for more information about Azure AD.*
- **Remove privileges not expressly required by an account's function or role.**
- **Ensure there are unique and distinct administrative accounts** for each set of administrative tasks.
- **Create non-privileged accounts for privileged users,** and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).
- **Reduce the number of domain and enterprise administrator accounts,** and remove all accounts that are unnecessary.
- **Regularly audit administrative user accounts.**
- **Regularly audit logs to ensure new accounts are legitimate users.**
- **Institute a group policy that disables remote interactive logins,** and use Domain Protected Users Group.

To assist with identifying suspicious behavior with administrative accounts:

- **Create privileged role tracking.**
- **Create a change control process** for all privilege escalations and role changes on user accounts.
- **Enable alerts on privilege escalations and role changes.**
- **Log privileged user changes** in the network environment, and create an alert for unusual events.

Review Trust Relationships

- **Review existing trust relationships with IT service providers,** such as managed service providers (MSPs) and cloud service providers (CSPs). Threat actors are known to exploit trust relationships between providers and their customers to gain access to customer networks and data.
- **Remove unnecessary trust relationships.**
- **Review contractual relationships** with all service providers, and ensure contracts include:
  - Security controls the customer deems appropriate.
  - Appropriate monitoring and logging of provider-managed customer systems.
  - Appropriate monitoring of the service provider's presence, activities, and connections to the customer network.
  - Notification of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks.

Note: *review CISA's page on APTs Targeting IT Service Provider Customers and CISA Insights: Mitigations and Hardening Guidance for MSPs and Small and Mid-sized Businesses for additional recommendations for MSP and CSP customers.*

Encourage Remote Work Environment Best Practices

With the increase in remote work and use of VPN services due to COVID-19, the FBI, NSA, and CISA encourage regularly monitoring remote network traffic, along with employing the following best practices. ***Note:*** *for additional information, see joint NSA-CISA Cybersecurity Information Sheet: Selecting and Hardening Remote Access VPN Solutions.*

- **Regularly update VPNs, network infrastructure devices, and devices used for remote work environments** with the latest software patches and security configurations.
- **When possible, require MFA on all VPN connections.** Physical security tokens are the most secure form of MFA, followed by authenticator applications. When MFA is unavailable, mandate that employees engaging in remote work use strong passwords.
- **Monitor network traffic for unapproved and unexpected protocols.**
- **Reduce potential attack surfaces by discontinuing unused VPN servers** that may be used as a point of entry by adversaries.

Establish User Awareness Best Practices

Cyber actors frequently use unsophisticated methods to gain initial access, which can often be mitigated by stronger employee awareness of indicators of malicious activity. The FBI, NSA, and CISA recommend the following best practices to improve employee operational security when conducting business:

- **Provide end user awareness and training.** To help prevent targeted social engineering and spearphishing scams, ensure that employees and stakeholders are aware of potential cyber threats and how they are delivered. Also, provide users with training on information security principles and techniques.

- **Inform employees of the risks of social engineering attacks,** e.g., risks associated with posting detailed career information to social or professional networking sites.
- **Ensure that employees are aware of what to do and whom to contact when they see suspicious activity or suspect a cyber intrusion** to help quickly and efficiently identify threats and employ mitigation strategies.

Apply Additional Best Practice Mitigations

- **Deny atypical inbound activity from known anonymization services,** including commercial VPN services and The Onion Router (TOR).
- **Impose listing policies for applications and remote access** that only allow systems to execute known and permitted programs under an established security policy.
- **Identify and create offline backups for critical assets.**
- **Implement network segmentation.**
- **Review CISA Alert** AA20-120A: Microsoft Office 365 Security Recommendations for additional recommendations on hardening M365 cloud environments.

Rewards for Justice Program

If you have information on state-sponsored Russian cyber operations targeting U.S. critical infrastructure, contact the Department of State's Rewards for Justice Program. You may be eligible for a reward of up to $10 million, which the Department is offering for information leading to the identification or location of any person who, while acting under the direction or control of a foreign government, participates in malicious cyber activity against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA). Contact (202) 702-7843 on WhatsApp, Signal, or Telegram, or send information via the Rewards for Justice secure Tor-based tips line located on the Dark Web. For more details, refer to rewardsforjustice.net.

Caveats

The information you have accessed or received is being provided "as is" for informational purposes only. The FBI, NSA, and CISA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the FBI, NSA, or CISA.

Contact Information

To report suspicious activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and

location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov. For NSA client requirements or general cybersecurity inquiries, contact the NSA Cybersecurity Requirements Center at (410) 854-4200 or Cybersecurity_Requests@nsa.gov. Defense Industrial Base companies may additionally sign up for NSA's free cybersecurity services, including Protective DNS, vulnerability scanning, and threat intelligence collaboration at dib_defense@cyber.nsa.gov.

Appendix: Detailed Tactics, Techniques, and Procedures

Reconnaissance [TA0043]

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. The adversary is known for harvesting login credentials [T1589.001].[17]

ID	Name	Description
T1589.001	Gather Victim Identity Information: Credentials	Adversaries may gather credentials that can be used during targeting.

Initial Access [TA0001]

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. For example, the adversary may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion [T1078].[18] These specific actors obtained and abused credentials of domain [T1078.002] and cloud accounts [T1078.004].[19] The actors also used external remote services to gain access to systems [T1133].[20] The adversary took advantage of weaknesses in internet-facing servers and conducted SQL injection attacks against

organizations' external websites [T1190].[21] Finally, they sent spearphishing emails with a malicious link in an attempt to gain access [T1566.002].[22]

ID	Name	Description
T1078	Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access.
T1078.002	Valid Accounts: Domain Accounts	Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
T1078.004	Valid Accounts: Cloud Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
T1133	External Remote Services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network.
T1190	Exploit Public-Facing Application	Adversaries may attempt to take advantage of a weakness in an internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior.
T1566.002	Phishing: Spearphishing Link	Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems.

Persistence [TA0003]

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. The adversary obtains and abuses credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion [T1078].[23]

ID	Name	Description
T1078	Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

Privilege Escalation [TA0004]

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. The adversary obtains and abuses credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion [T1078].[24] Specifically in this case, credentials of cloud accounts [T1078.004] were obtained and abused.[25]

ID	Name	Description
T1078	Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access.
T1078.004	Valid Accounts: Cloud Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

Defense Evasion [TA0005]

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. The adversary made its executables and files difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit [T1027].[26]

ID	Name	Description
T1027	Obfuscated Files or Information	Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.

Credential Access [TA0006]

Credential Access consists of techniques for stealing credentials like account names and passwords. The adversary attempted to access or create a copy of the Active Directory (AD) domain database to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights [T1003.003].[27] The adversary also used a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials [T1110.003].[28]

ID	Name	Description
T1003.003	OS Credential Dumping: NTDS	Adversaries may attempt to access or create a copy of the Active Directory domain database to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights.
T1110.003	Brute Force: Password Spraying	Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials.

Discovery [TA0007]

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. The adversary enumerated files and directories or searched in specific locations of a host or network share for certain information within a file system [T1083].[29] In addition, the adversary attempted to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain or forest environments [T1482].[30]

ID	Name	Description
T1083	File and Directory Discovery	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.

ID	Name	Description
T1482	Domain Trust Discovery	Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments.

Collection [TA0009]

Collection consists of both the techniques adversaries may use to gather information and the sources that information is collected from that are relevant to the adversary's objectives. The adversary leverages information repositories, such as SharePoint, to mine valuable information [T1213.002].[31]

ID	Name	Description
T1213.002	Data from Information Repositories: SharePoint	Adversaries may leverage the SharePoint repository as a source to mine valuable information.

Command and Control [TA0011]

Command and Control (C2) consists of techniques that adversaries may use to communicate with systems under their control within a victim network. The adversary chained together multiple proxies to disguise the source of malicious traffic. In this case, TOR and VPN servers are used as multi-hop proxies to route C2 traffic and obfuscate their activities [T1090.003].[32]

ID	Name	Description
T1090.003	Proxy: Multi-hop Proxy	To disguise the source of malicious traffic, adversaries may chain together multiple proxies.

Additional Resources

[1] NSA, CISA, FBI, NCSC Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments, 1 July 2021.
[2] NSA Cybersecurity Advisory: Mitigating Recent VPN Vulnerabilities, 7 October 2019.
[3] NSA, CISA, FBI, NCSC Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments, 1 July 2021.
[4] Microsoft Article: AD Forest Recovery – Resetting the krbtgt password, 29 July 2021.
[5] Microsoft GitHub: New-KrbtgtKeys.ps1, 14 May 2020.
[6] NSA Cybersecurity Information: Defend Privileges and Accounts, August 2019.
[7] Microsoft Article: Group Managed Service Accounts Overview, 29 July 2021.
[8] NSA Cybersecurity Information: Leverage Modern Hardware Security Features, August 2019.
[9] Microsoft Article: Protect derived domain credentials with Windows Defender Credential Guard, 3 December 2021.
[10] Microsoft Article: Windows Defender Credential Guard protection limits, 3 December 2021.
[11] Microsoft Article: Windows 11 requirements, 30 November 2021.
[12] Microsoft Blog Post: The Importance of KB2871997 and KB2928120 for Credential Protection, 20 September 2021.
[13] Microsoft Article: What's New in Credential Protection, 7 January 2022.
[14] NSA Cybersecurity Factsheet: PowerShell: Security Risks and Defenses, 1 December 2016.
[15] NSA Cybersecurity Information: Update and Upgrade Software Immediately, August 2019.
[16] NSA Cybersecurity Information: Actively Manage Systems and Configurations, August

2019.
[17] MITRE Groups: APT28, 18 October 2021.
[18] MITRE Groups: APT28, 18 October 2021.
[19] MITRE Software: Cobalt Strike, 18 October 2021.
[20] Based on technical information shared by Mandiant.
[21] MITRE Groups: APT28, 18 October 2021.
[22] Based on technical information shared by Mandiant.
[23] MITRE Groups: APT28, 18 October 2021.
[24] MITRE Groups: APT28, 18 October 2021.
[25] MITRE Software: Cobalt Strike, 18 October 2021.
[26] MITRE Software: Fysbis, 6 November 2020.
[27] MITRE Software: Koadic, 30 March 2020.
[28] MITRE Groups: APT28, 18 October 2021.
[29] Based on technical information shared by Mandiant.
[30] Based on technical information shared by Mandiant.
[31] MITRE Groups: APT28, 18 October 2021.
[32] MITRE Groups: APT28, 18 October 2021.

Revisions

February 16, 2022: Initial Version

News

UPDATE: Cybersecurity Experts Warn Ukraine, Russia Crisis Could Result in U.S. Cyberattacks

National security experts believe Russia could conduct a cyberattack against the U.S. if it feels it's threatened by the U.S. response to a possible Russian invasion of the Ukraine.

Photo via Adobe by beebright

March 23, 2022 Robin Hattersley-Gray Jump to Comments

"The magnitude of Russia's cyber capacity is fairly consequential, and it's coming. The federal government is doing its part to get ready," he said, imploring companies to invest "as much as you can" in beefing up technology capacity.

Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, echoed the president, urging "all organizations, large and small, to act now to protect themselves against malicious cyber activity."

UPDATE FEB. 16, 2022: European and U.S. regulators are warning banks they should be prepared for a possible Russian-sponsored cyber attack as tensions with Russia increase over its massive build up of troops at the Ukrainian border. The warning comes more than two weeks after the U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned all organizations in the U.S. to be on guard against possible cyber attacks coming from Russia.

While military action has yet to unfold, Ukraine has already suffered cyberattacks in recent weeks, including a malware campaign masquerading as ransomware and DDoS attacks that temporarily knocked some government and banking websites offline.

In a blog post, Sandra Joyce, executive vice president and head of global intelligence at Mandiant, says Russia's history of aggressive cyberattacks warrants concern. She cites Russia's cyberattacks against Ukraine's critical infrastructures and other attacks against Europe and the U.S.

compromise.

"Many of the same steps defenders might take to harden their networks against ransomware crime will serve to prepare them from a determined state actor, if they take them now," Joyce writes.

Despite those potential threats, Joyce cautions against panic, saying that the real target of cyberattacks is our perceptions.

"The purpose of these cyberattacks is not simply to wipe hard drives or turn out the lights, but to frighten those who cannot help but notice," Joyce writes. "The audience of these attacks is broad, but it is also empowered to determine how effective they are. While these incidents can be quite serious for many, we must remain mindful of their limitations. We only do the adversary a service by overestimating their reach."

Meanwhile, cybersecurity giant CrowdStrike says in a blog that while cyberattacks against Russia's adversaries during this crisis can't be discounted, they are unlikely due to the potential for global escalation.

"However, the incidental targeting of international businesses operating within Ukraine may be used by Russian-nexus adversaries to dissuade business operations and investment and destabilize the local economy," the company said.

In addition to Mandiant, CrowdStrike and several other high-profile cybersecurity providers advising customers to harden networks, CISA issued an advisory this week urging U.S. organizations to take steps now to harden its networks. The advisory includes several recommendations for preparing for a cyberattack and responding to one, as well as other CISA resources, including its catalog of known exploited vulnerabilities.

ORIGINAL JANUARY 25, 2022 ARTICLE:

Last week the DHS' Cybersecurity and Infrastructure Security Agency (CISA) warned that every organization in the U.S. is at risk from cyber threats that can disrupt essential services and potentially result in impacts to public safety.

The warning comes as more than 100,000 Russian troops are gathering at the Ukrainian border, and the Biden administration is weighing its military options if Russia invades. Russia could conduct a cyberattack against the U.S. if it believes it's threatened by the U.S. response to a Russian invasion.

and privileged or administrative access requires multi-factor authentication.
- Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.
- Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

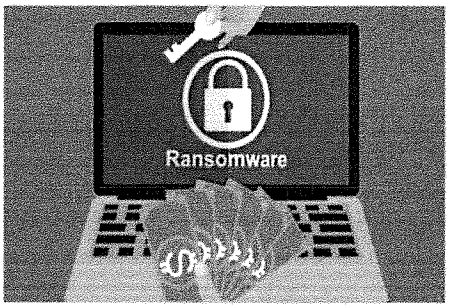
Related: Take Action Now: Russia Conducting Massive Cyber Attack Using Popular IT Management Software

The agency also urges organizations to take the following steps to quickly detect potential intrusions:

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

Recommended response steps include:

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/ responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.



Related: Pandemic Pushes Rise of School Cyber Attacks, Projected to Keep Climbing

The following steps are recommended to maximize an organization's resilience to a cyber attack:

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by

to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

CISA's warning comes on the heels of new research from WatchGuard Technologies, which found that despite a drop in third-quarter malware and ransomware activity, 2021 was an exceptional year for these kinds of attacks, reports MyTechDecisions.com.

The researchers also found that nearly half of zero-day malware is now delivered via encrypted connections, with Transport Layer Security (TLS)-delivered malware jumping from 31.6% to 47%. This suggests that many organizations aren't decrypting these connections and have poor visibility into the amount of malware hitting their networks.

The report also sheds light on new attack vectors as users upgrade to new versions of Microsoft Windows and Office, with attackers focusing on new vulnerabilities while still leveraging older, unpatched bugs. Additionally, the report confirms the increasing proliferation of ransomware, finding that 2021 ransomware attacks are on pace to reach 150% of 2020 volume when full-year data becomes available.

Russian-linked cyber gangs have a long history of launching cyber attacks against the U.S., including last year's damaging SolarWinds attack.

Tagged with: Cybersecurity • Data Breaches • Malware • Ransomware

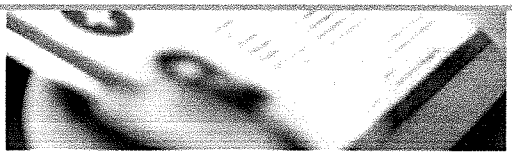
About the Author

ROBIN HATTERSLEY-GRAY, Editor-in-Chief

Contact:

Robin has been covering the security and campus law enforcement industries since 1998 and is a specialist in school, university and hospital security, public safety and emergency management, as well as emerging technologies and systems integration. She joined CS in 2005 and has authored award-winning editorial on campus law enforcement and security funding, officer recruitment and retention, access control, IP video, network integration, event management, crime trends, the Clery Act, Title IX compliance, sexual assault, dating abuse, emergency communications, incident management software and more. Robin has been featured on national and local media outlets and was formerly associate editor for the trade publication Security Sales & Integration. She obtained her undergraduate degree in history from California State University, Long Beach.

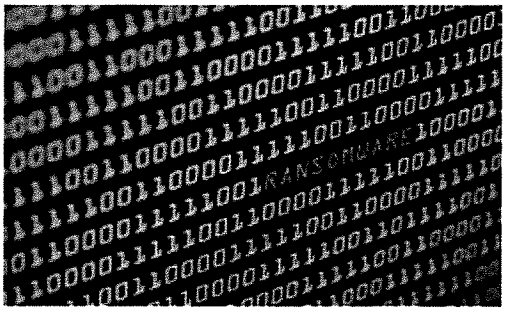
Related Content



New Law Enables FDA to Regulate Medical Device Cybersecurity

Registration Now Open for the 2023 Campus Safety Conferences!

Ransomware Gang Apologizes to Canadian Hospital That Treats Children



Cybersecurity Incident Shuts Down Des Moines School District

Leading in Turbulent Times: Effective Campus Public Safety Leadership for the 21st Century

This new webcast will discuss how campus public safety leaders can effectively incorporate Clery Act, Title IX, customer service, "helicopter" parents, emergency notification, town-gown relationships, brand management, Greek Life, student recruitment, faculty, and more into their roles and develop the necessary skills to successfully lead their departments. Register today to attend this free webcast!

Leave a Reply

Your email address will not be published. Required fields are marked *

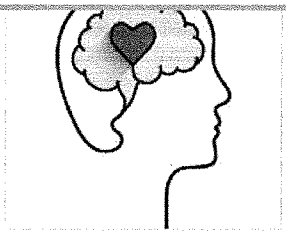
Name *

Email *

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment



Needs and Violence

In this webinar, attendees will learn the observable behaviors people exhibit as they head down a path of violence so we can help prevent the preventable.

Beyond Threat Assessment: Managing Threats with Appropriate Follow-up, Monitoring & Training

This discussion will help participants analyze, understand, and assess their own program effectiveness.

Latest Quizzes

Mental Health in America: Test Your Awareness with This Quiz

Test Your Hospital Safety and Security Knowledge with These 9 Questions

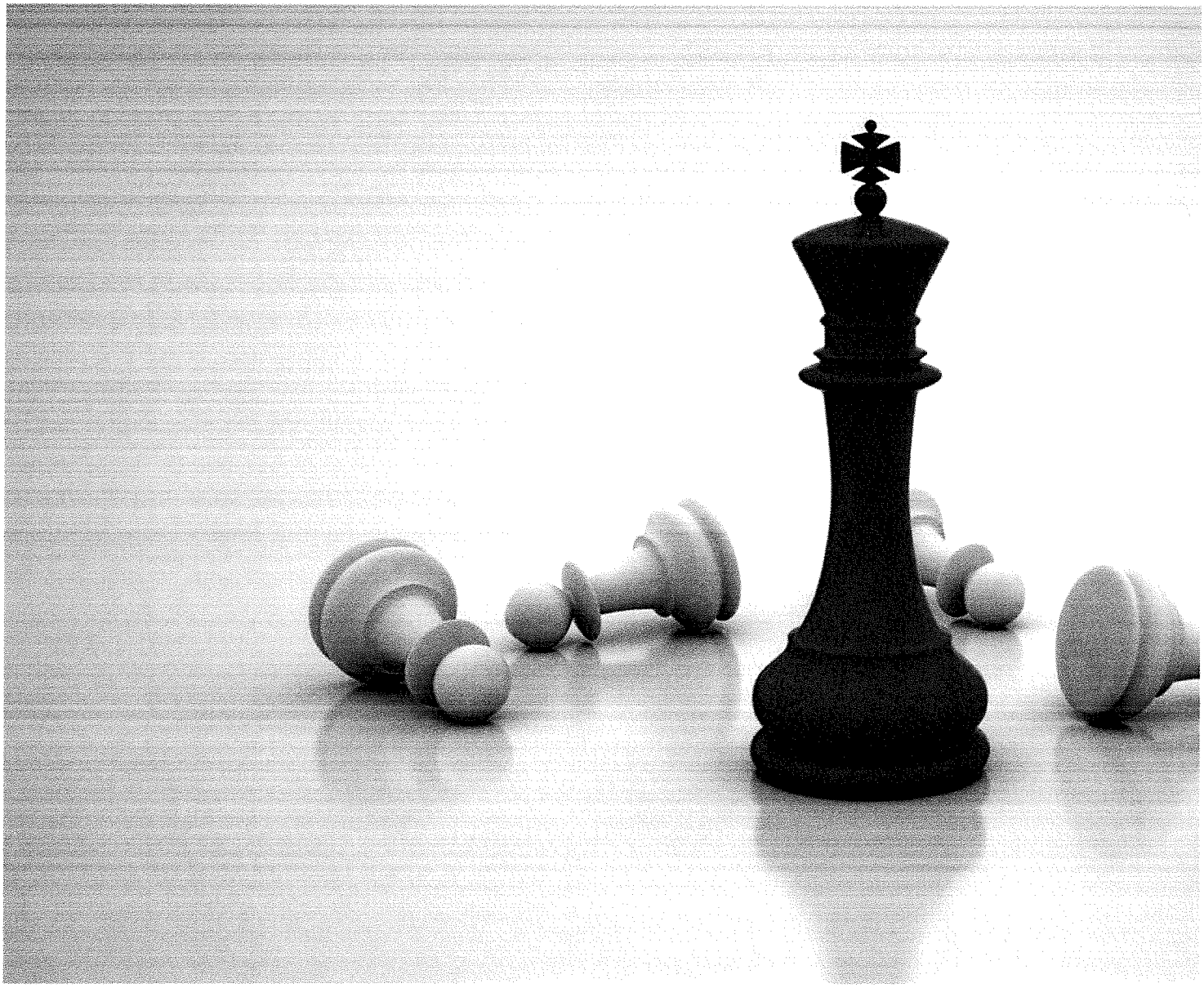
IS-800 D National Response Framework Exam Questions

New Royal Ransomware emerges in multi-million dollar attacks

By

Lawrence Abrams

- September 29, 2022
- 10:32 AM
- 0

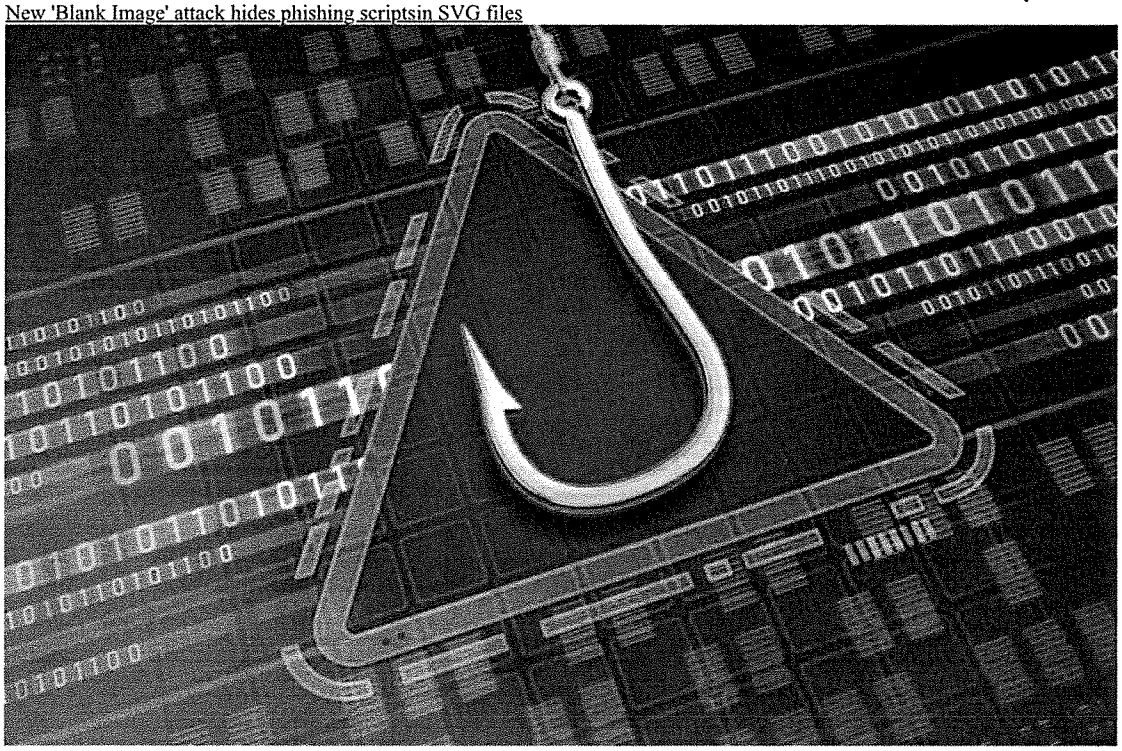


A ransomware operation named Royal is quickly ramping up, targeting corporations with ransom demands ranging from $250,000 to over $2 million.

Royal is an operation that launched in January 2022 and consists of a group of vetted and experienced ransomware actors from previous operations.

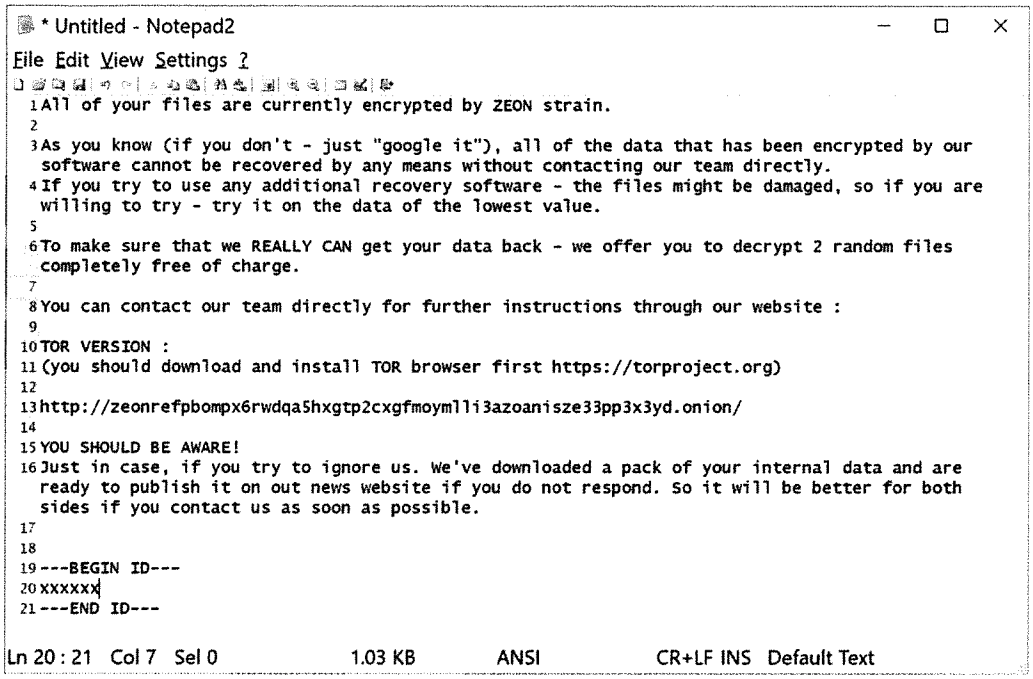
Unlike most active ransomware operations, Royal does not operate as a Ransomware-as-a-Service but is instead a private group without affiliates.

New 'Blank Image' attack hides phishing scriptsin SVG files



Vitali Kremez, CEO of AdvIntel, told BleepingComputer that they utilized other ransomware operation's encryptors when first starting, such as BlackCat.

Soon after, the cybercrime enterprise began using its own encryptors, the first being Zeon [Sample], which generated ransom notes very similar to Conti's.



Zeon ransom note
Source: BleepingComputer

However, since the middle of September 2022, the ransomware gang has rebranded again to 'Royal' and is using that name in ransom notes generated by a new encryptor.

How Royal breaches their victims

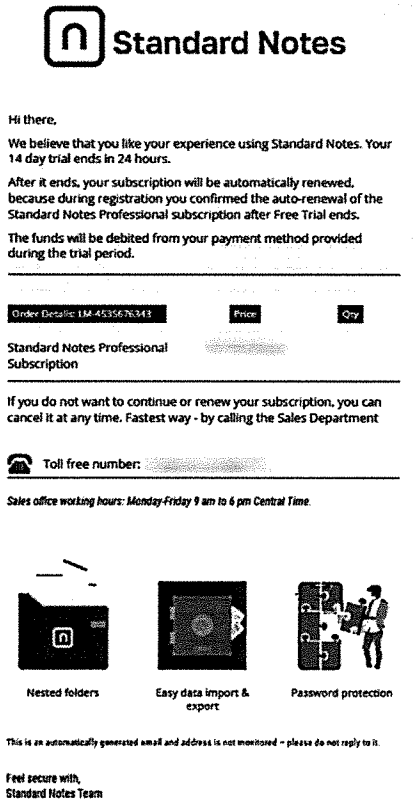
The Royal operation has been operating in the shadows, not using a data leak site and keeping news of their attacks quiet.

However, as the gang became more active this month, victims have appeared at BleepingComputer, and a sample was uploaded to VirusTotal.

In conversations with Kremez and a victim, BleepingComputer has created a better picture of how the gang operates.

According to Kremez, the Royal group utilizes targeted callback phishing attacks where they impersonate food delivery and software providers in emails pretending to be subscription renewals.

These phishing emails contain phone numbers that the victim can contact to cancel the alleged subscription, but, in reality, it is a number to a service hired by the threat actors.



Example of a Royal callback phishing email
Source: AdvIntel

When a victim calls the number, the threat actors use social engineering to convince the victim to install remote access software, which is used to gain initial access to the corporate network.

A Royal victim who spoke to BleepingComputer shared that the threat actors breached their network using a vulnerability in their custom web application, showing the threat actors are also being creative in how they gain access to a network.

Once they gain access to a network, they perform the same activities commonly used by other human-operated ransomware operations. They deploy Cobalt Strike for persistence, harvest credentials, spread laterally through the Windows domain, steal data, and ultimately encrypt devices.

When encrypting files, the Royal encryptor will append the **.royal** extension to the file names of encrypted files. For example, test.jpg would be encrypted and renamed to test.jpg.royal, as shown below.

Files encrypted by the Royal Ransomware
Source: BleepingComputer

A Royal victim also told BleepingComputer that they target virtual machines by directly encrypting their virtual disk files (VMDK). The threat actors then print out the ransom notes on network printers or create them on encrypted Windows devices.

These ransom notes are named **README.TXT** and contain a link to the victim's private Tor negotiation page at royal2xthig3ou5hd7zsliqagy6yygk2cdclaxtni2fyad6dpmpxcdid.onion. XXX in the ransom note below has been redacted but is unique to the victim.

Royal ransom note
Source: BleepingComputer

The Tor negotiation site is nothing special, simply containing a chat screen where a victim can communicate with the Royal ransomware operators.

As part of these negotiations, the ransomware gang will provide the ransom demand, with ransom demands between $250,000 and over $2 million.

The ransomware gang will also commonly decrypt a few files for the victims to prove their decryptor works and share file lists of the stolen data.

Royal Ransomware Tor negotiation site
Source: BleepingComputer

BleepingComputer is unaware of successful payments and has not seen a decryptor for this ransomware family.

While the group claims to steal data for double-extortion attacks, it does not appear that a data leak site has been launched under the Royal brand as of yet.

However, it is strongly advised that network, windows, and security admins keep an eye out for this group, as they are quickly ramping up operations and will likely become one of the more significant enterprise-targeting ransomware operations.

Update 8/29/22: Article updated with some corrections, including launch date and callback phishing example.

Related Articles:

Microsoft: Cuba ransomware hacking Exchange servers via OWASSRF flaw

Ransomware gang uses new Microsoft Exchange exploit to breach servers

The Week in Ransomware - December 9th 2022 - Wide Impact

Exploit released for critical ManageEngine RCE bug, patch now

Ransomware profits drop 40% in 2022 as victims refuse to pay

Russia Cyber Threat Overview and Advisories

This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the Russian government's malicious cyber activities. The overview leverages publicly available, open-source intelligence and information regarding this threat. This page also includes a complete list of related CISA publications, many of which are jointly authored with other U.S. government agencies (Note: unless specifically stated, neither CISA nor the U.S. Government attributed specific activity described in the referenced sources to Russian government actors). Additionally, this page provides instructions on how to report related threat activity.

The Russian government engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries.[1] Recent Advisories published by CISA and other unclassified sources reveal that Russian state-sponsored threat actors are targeting the following industries and organizations in the United States and other Western nations: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing. The same reporting associated Russian actors with a range of high-profile malicious cyber activity, including the 2020 compromise of the SolarWinds software supply chain, the 2020 targeting of U.S. companies developing COVID-19 vaccines, the 2018 targeting of U.S industrial control system infrastructure, the 2017 NotPetya ransomware attack on organizations worldwide, and the 2016 leaks of documents stolen from the U.S. Democratic National Committee.

According to the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis." The Assessment states that "Russia almost certainly considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts."[2]

Latest U.S. Government Report on Russian Malicious Cyber Activity

On April 20, 2022, the cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom released a joint Cybersecurity Advisory to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners. The advisory provides an overview of Russian state-sponsored advanced persistent threat groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

The Russian Malicious Cyber Activity section below lists all CISA Advisories, Alerts, and Malware Analysis Reports (MARs) on Russian malicious cyber activities. See CISA.gov/supply-chain-compromise for additional partner products.

Expand All Sections

Russian Malicious Cyber Activity

Report Activity Related to This Threat

Mitigate and Detect This Threat

Respond to an Incident

References

Kaufman, Linda

From: ODonnell, Patrick
Sent: Thursday, September 8, 2022 9:25 AM
To: Maruzzo, Marc
Subject: FW: Password Spraying Operation Targeting Colleges

Marc,
Please add these to the block list.

Patrick

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Thursday, September 8, 2022 9:07 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Password Spraying Operation Targeting Colleges

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

Hello,

We have been notified of a large scale password spraying operation originating from the following IP addresses, affecting multiple colleges:

107.175.238.250, 38.15.148.212, 107.172.238.14, 107.175.237.86, 192.210.195.29, 23.95.62.157, 107.175.237.75, 104.144.89.192, 104.144.91.101, 23.250.95.119, 45.57.193.1, 209.127.39.120, 104.144.215.175, 45.57.235.88, 209.127.17.123, 192.3.233.201, 104.144.191.188, 209.127.17.39, 209.127.76.40, 104.144.243.74, 104.144.6.186, 45.39.72.62, 104.165.169.113, 104.165.127.52, 104.165.127.215, 104.165.127.44, 23.27.240.100, 23.230.167.168, 23.230.167.72, 156.239.61.191, 156.239.61.89, 104.252.131.87, 104.227.51.20, 154.202.116.59, 104.252.131.215

It is recommended to block all traffic from these IPs addresses.

Thank you,
Omer Usmani
Security Analyst
California Community Colleges Technology Center

To unsubscribe from the ISAC list, click the following link:
https://LISTSERV.CCCNEXT.NET/scripts/wa-CCCNEXT.exe?SUBED1=ISAC&A=1

Kaufman, Linda

From: ODonnell, Patrick
Sent: Wednesday, November 9, 2022 3:53 PM
To: Maruzzo, Marc
Subject: FW: Royal Ransomware IP's

Please add these.

Patrick

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Wednesday, November 9, 2022 3:47 PM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Royal Ransomware IP's

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

Hello,

Traffic from the following IP addresses have been associated with Royal ransomware attacks on education institutions. These should be blocked at the firewall:

143.244.52.6
104.238.205.53
45.147.228.231

It is likely these IP addresses will change as their attack strategy continues to develop.

More information on the threat actor can be found here: https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/

--
Thank you,
Omer Usmani
Security Analyst
California Community Colleges Technology Center

HC3: Analyst Note
December 07, 2022 TLP:CLEAR Report: 202212071400

The Royal ransomware is a 64-bit executable that is written in C++ and targets window systems. The ransomware works to delete all Volume Shadow Copies, which provides a point-in-time copy of a file. With these, you can quickly recover deleted or changed files stored on a network. It will encrypt the network shares that are found on the local network and the local drives. The files are encrypted with the AES algorithm, with the key and IV being encrypted in the RSA public key, which is hard coded into the executable. The malware can either fully or partially encrypt a file based on its size and the '-ep' parameter. Once the files are encrypted, it will change the extension of the files to '.royal'.

Multiple actors have been spreading Royal ransomware, but in a report from Microsoft, it is also being distributed from DEV-0569. The group has been delivering the malware with human-operated attacks and has displayed innovation in their methods by using new techniques, evasion tactics, and post-compromise payloads. The group has been observed embedding malicious links in malvertising, phishing emails, fake forums, and blog comments. In addition, Microsoft researchers have identified changes in their delivery method to start using malvertising in Google ads, utilizing an organization's contact forum that can bypass email protections, and placing malicious installer files on legitimate looking software sites and repositories.

Analyst Comment

Royal is a newer ransomware, and less is known about the malware and operators than others. Additionally, on previous Royal compromises that have impacted the HPH sector, they have primarily appeared to be focused on organizations in the United States. In each of these events, the threat actor has claimed to have published 100% of the data that was allegedly extracted from the victim.

Outside of the techniques addressed in this report, HC3 continues to see the following attack vectors frequently associated with ransomware:

- Phishing
- Remote Desktop Protocol (RDP) compromises and credential abuse
- Compromises of exploilted vulnerabilities, such as VPN servers
- Compromises in other known vulnerabilities

The following sources contain indicators of compromise:

- https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware
- https://securityscorecard.pathfactory.com/research/the-royal-ransomware
- https://blog.polyswarm.io/royal-ransomware

References

Abrams, Lawrence. "New Royal Ransomware emerges in multi-million dollar attacks". Bleepingcomputer. Sep 29, 2022. https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/

Polyswarm Tech Team. "Royal Ransomware". Polyswarm. Dec 1, 2022. https://blog.polyswarm.io/royal-ransomware

Greig, Jonathan. "Microsoft: Royal ransomware group using Google Ads in campaign". Therecord. Nov 18,

2022. https://therecord.media/microsoft-royal-ransomware-group-using-google-ads-in-campaign/

Pasca, Vlad. "A Technical Analysis of Royal Ransomware". Securityscorecard. https://securityscorecard.pathfactory.com/research/the-royal-ransomware

Microsoft Security Threat Intelligence. "DEV-0569 finds new ways to deliver Royal ransomware, various payloads". Microsoft. Nov 17, 2022. https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

Imano, Shunichi. Slaughter, James. "Ransomware Roundup: Royal Ransomware". Fortinet. Oct 12, 2022. https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, September 12, 2022 12:54 PM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 9/05/22 - 9/11/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, Sep 12, 2022 at 11:16 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 9/05/22 - 9/11/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 9/05/22 - 9/11/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to OperationsSupport@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

In addition to the above lists, the MS-ISAC has begun making available IOCs which come directly from our Threat Intelligence Platform. Currently, the IOCs provided are IPv4; over time, we'll add hashes and other IOCs to help protect SLTT environments.

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_IPs.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Domains.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Hashes.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Emails.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us OperationsSupport@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at OperationsSupport@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Tuesday, September 6, 2022 12:14 PM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 8/29/22 - 9/04/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Tue, Sep 6, 2022 at 11:26 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 8/29/22 - 9/04/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 8/29/22 - 9/04/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to OperationsSupport@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

In addition to the above lists, the MS-ISAC has begun making available IOCs which come directly from our Threat Intelligence Platform. Currently, the IOCs provided are IPv4; over time, we'll add hashes and other IOCs to help protect SLTT environments.

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_IPs.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Domains.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Hashes.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us OperationsSupport@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at OperationsSupport@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, August 22, 2022 11:39 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 8/15/22 - 8/21/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, Aug 22, 2022 at 11:24 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 8/15/22 - 8/21/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 8/15/22 - 8/21/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to OperationsSupport@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

In addition to the above lists, the MS-ISAC has begun making available IOCs which come directly from our Threat Intelligence Platform. Currently, the IOCs provided are IPv4; over time, we'll add hashes and other IOCs to help protect SLTT environments.

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_IPs.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Domains.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Hashes.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Emails.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us OperationsSupport@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at OperationsSupport@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, August 15, 2022 11:40 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 8/08/22 - 8/14/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, Aug 15, 2022 at 11:08 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 8/08/22 - 8/14/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 8/08/22 - 8/14/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to OperationsSupport@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

In addition to the above lists, the MS-ISAC has begun making available IOCs which come directly from our Threat Intelligence Platform. Currently, the IOCs provided are IPv4; over time, we'll add hashes and other IOCs to help protect SLTT environments.

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_IPs.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Domains.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Hashes.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us OperationsSupport@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at OperationsSupport@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, August 8, 2022 11:54 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 8/01/22 - 8/07/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, Aug 8, 2022 at 11:21 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 8/01/22 - 8/07/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 8/01/22 - 8/07/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to OperationsSupport@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

In addition to the above lists, the MS-ISAC has begun making available IOCs which come directly from our Threat Intelligence Platform. Currently, the IOCs provided are IPv4; over time, we'll add hashes and other IOCs to help protect SLTT environments.

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_IPs.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Domains.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us OperationsSupport@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at OperationsSupport@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, July 25, 2022 11:49 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 7/18/22 - 7/24/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, Jul 25, 2022 at 11:47 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 7/18/22 - 7/24/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 7/18/22 - 7/24/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to OperationsSupport@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

In addition to the above lists, the MS-ISAC has begun making available IOCs which come directly from our Threat Intelligence Platform. Currently, the IOCs provided are IPv4; over time, we'll add hashes and other IOCs to help protect SLTT environments.

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_IPs.txt

https://cti-lists.cisecurity.org/lists/MS_ISAC_Collection_Domains.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us OperationsSupport@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at OperationsSupport@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Members that would like to use the API to access the MS-ISAC Malware IPs and Domains in order to auto populate their security perimeter devices may download the scripts from our GitHub repository at https://github.com/MSISAC/STIX-TAXII-Integration. The API requires IP whitelist access, which can be obtained by sending your IP address or range to OperationsSupport@cisecurity.org. If you were previously whitelisted for our Palo Alto external block lists, the IP address or range already provided is whitelisted for the above.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, May 23, 2022 11:20 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 5/16/22 - 5/22/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, May 23, 2022 at 11:16 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 5/16/22 - 5/22/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>, Indicator Sharing <Indicator.Sharing@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 5/16/22 - 5/22/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to Indicator.Sharing@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us indicator.sharing@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at Indicator.Sharing@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Members that would like to use the API to access the MS-ISAC Malware IPs and Domains in order to auto populate their security perimeter devices may download the scripts from our GitHub repository at https://github.com/MSISAC/STIX-TAXII-Integration. The API requires IP whitelist access, which can be obtained by sending your IP address or range to Indicator.Sharing@cisecurity.org. If you were previously whitelisted for our Palo Alto external block lists, the IP address or range already provided is whitelisted for the above.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, May 2, 2022 9:54 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 4/25/22 - 5/1/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, May 2, 2022 at 9:18 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 4/25/22 - 5/1/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>, Indicator Sharing <Indicator.Sharing@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

This week, there have been no IP addresses and domains associated with malware observed by MS-ISAC from 4/25/22 - 5/1/22 using our monitoring services; However, there is a submission from the SLTT community. Please check the "Member Submitted Domains" tab of the attached spreadsheet for further details.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to Indicator.Sharing@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning for and exploiting vulnerabilities in Log4j, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been added to the attached spreadsheet and made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/log4j_scanning_IPs.txt (IPs observed scanning for the vulnerability)

https://cti-lists.cisecurity.org/lists/log4j_callback_IPs.txt (IPs observed being used in second stage communications)

https://cti-lists.cisecurity.org/lists/log4j_domains.txt (Domains observed in exploit attempts against Log4 vulnerabilities)

https://cti-lists.cisecurity.org/lists/log4j_hashes.txt (Fingerprints of suspicious/malicious files associated with attack attempts against Log4j)

Also, in response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us indicator.sharing@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at Indicator.Sharing@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Members that would like to use the API to access the MS-ISAC Malware IPs and Domains in order to auto populate their security perimeter devices may download the scripts from our GitHub repository at https://github.com/MSISAC/STIX-TAXII-Integration. The API requires IP whitelist access, which can be obtained by sending your IP address or range to Indicator.Sharing@cisecurity.org. If you were previously whitelisted for our Palo Alto external block lists, the IP address or range already provided is whitelisted for the above.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, May 9, 2022 11:34 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 5/02/22 - 5/08/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, May 9, 2022 at 11:32 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 5/02/22 - 5/08/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>, Indicator Sharing <Indicator.Sharing@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 5/02/22 - 5/08/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to Indicator.Sharing@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us indicator.sharing@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at Indicator.Sharing@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Members that would like to use the API to access the MS-ISAC Malware IPs and Domains in order to auto populate their security perimeter devices may download the scripts from our GitHub repository at https://github.com/MSISAC/STIX-TAXII-Integration. The API requires IP whitelist access, which can be obtained by sending your IP address or range to Indicator.Sharing@cisecurity.org. If you were previously whitelisted for our Palo Alto external block lists, the IP address or range already provided is whitelisted for the above.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, May 2, 2022 9:54 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 4/25/22 - 5/1/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, May 2, 2022 at 9:18 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 4/25/22 - 5/1/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>, Indicator Sharing <Indicator.Sharing@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

This week, there have been no IP addresses and domains associated with malware observed by MS-ISAC from 4/25/22 - 5/1/22 using our monitoring services; However, there is a submission from the SLTT community. Please check the "Member Submitted Domains" tab of the attached spreadsheet for further details.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to Indicator.Sharing@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning for and exploiting vulnerabilities in Log4j, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been added to the attached spreadsheet and made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/log4j_scanning_IPs.txt (IPs observed scanning for the vulnerability)

https://cti-lists.cisecurity.org/lists/log4j_callback_IPs.txt (IPs observed being used in second stage communications)

https://cti-lists.cisecurity.org/lists/log4j_domains.txt (Domains observed in exploit attempts against Log4 vulnerabilities)

https://cti-lists.cisecurity.org/lists/log4j_hashes.txt (Fingerprints of suspicious/malicious files associated with attack attempts against Log4j)

Also, in response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us indicator.sharing@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at Indicator.Sharing@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Members that would like to use the API to access the MS-ISAC Malware IPs and Domains in order to auto populate their security perimeter devices may download the scripts from our GitHub repository at https://github.com/MSISAC/STIX-TAXII-Integration. The API requires IP whitelist access, which can be obtained by sending your IP address or range to Indicator.Sharing@cisecurity.org. If you were previously whitelisted for our Palo Alto external block lists, the IP address or range already provided is whitelisted for the above.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, April 18, 2022 11:48 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 4/11/22 - 4/17/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, Apr 18, 2022 at 11:39 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 4/11/22 - 4/17/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 4/11/22 - 4/17/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to Indicator.Sharing@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning for and exploiting vulnerabilities in Log4j, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been added to the attached spreadsheet and made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/log4j_scanning_IPs.txt (IPs observed scanning for the vulnerability)

https://cti-lists.cisecurity.org/lists/log4j_callback_IPs.txt (IPs observed being used in second stage communications)

https://cti-lists.cisecurity.org/lists/log4j_domains.txt (Domains observed in exploit attempts against Log4 vulnerabilities)

https://cti-lists.cisecurity.org/lists/log4j_hashes.txt (Fingerprints of suspicious/malicious files associated with attack attempts against Log4j)

Also, in response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us indicator.sharing@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at Indicator.Sharing@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Members that would like to use the API to access the MS-ISAC Malware IPs and Domains in order to auto populate their security perimeter devices may download the scripts from our GitHub repository at https://github.com/MSISAC/STIX-TAXII-Integration. The API requires IP whitelist access, which can be obtained by sending your IP address or range to Indicator.Sharing@cisecurity.org. If you were previously whitelisted for our Palo Alto external block lists, the IP address or range already provided is whitelisted for the above.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, April 11, 2022 11:44 AM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Malware IPs and Domains observed by MS-ISAC - 4/4/22 - 4/10/22 - TLP: GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, Apr 11, 2022 at 11:31 AM
Subject: Malware IPs and Domains observed by MS-ISAC - 4/4/22 - 4/10/22 - TLP: GREEN
To: MS-ISAC CTI <Intel@cisecurity.org>, Indicator Sharing <Indicator.Sharing@cisecurity.org>
Cc: MS-ISAC SOC <SOC@msisac.org>

TLP: GREEN

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 4/4/22 - 4/10/22 using our monitoring services and submissions from the SLTT community.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This is a weekly list based on data collected from public organizations and government entities within the United States. It contains indicators of compromise related to malware observed from our monitoring services and files uploaded by our members to our online sandbox. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains five tabs with the following information:

1. Malware IP

IP ADDRESS - This is either the IP address that is attacking a system, or is the IP address the malware on an infected system is communicating with.

LOG COUNT - This is the number of logged alerts generated for malicious traffic to or from the IP address.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic to or from the IP address.

COUNTRY, REGION, CITY - Location of the potentially malicious IP address.

ISP - ISP or hosting provider for the IP address.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

2. Malware Domains

DOMAIN - This is the domain that is hosting malware.

LOG COUNT - This is the number of logged alerts generated for malicious traffic involving the domain.

EVENT COUNT - This is the number of unique infections notified on by the MS-ISAC associated with malicious traffic involving the domain.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

ASSOCIATED THREAT - Malware type or activity associated with the infection.

THREAT DESCRIPTION - Threat category associated with the malware.

3. Member Submitted Domains

DOMAIN - This is the domain that is hosting malware.

COUNTRY, REGION, CITY - Location of the domain.

ISP - ISP or hosting provider for the domain.

4. Clean – Unblock List - **This section provides a list of previously reported IP addresses/domains, which were found to be clean within the last 4 weeks and no longer need to be blocked.**

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses and domains as reports have shown this to greatly reduce security incidents across our member networks. **Note that some of the IP addresses may belong to legitimate organizations.**
- If any traffic is found on any of the tabs, then check the source host for signs of infection. Report any traffic seen to the MS-ISAC.
- Note that an IP address can be associated with multiple legitimate domain names, especially for those belonging to a hosting provider.
- Note that a domain can be associated with multiple IP addresses, especially for those utilizing fast flux DNS or cloud hosting.

Getting these lists in an automated format:

The MS-ISAC has actively transitioned from our old indicator sharing infrastructure to new infrastructure with enhanced capabilities. Known and confirmed member IPs/ranges have already been ported over to the new infrastructure and whitelisted. If you would like to automate ingestion of these into your environment, please reach out to Indicator.Sharing@cisecurity.org with your external IP/CIDR information.

Landing Page: http://cti-lists.cisecurity.org/

Directory Listing: https://cti-lists.cisecurity.org/lists/

Malicious Domains - Direct Link: https://cti-lists.cisecurity.org/lists/domains.txt

Malicious IPs - Direct Link: https://cti-lists.cisecurity.org/lists/IPs.txt

In response to requests from members to compile and share potentially malicious IPs and domains scanning for and exploiting vulnerabilities in Log4j, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been added to the attached spreadsheet and made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/log4j_scanning_IPs.txt (IPs observed scanning for the vulnerability)

https://cti-lists.cisecurity.org/lists/log4j_callback_IPs.txt (IPs observed being used in second stage communications)

https://cti-lists.cisecurity.org/lists/log4j_domains.txt (Domains observed in exploit attempts against Log4 vulnerabilities)

https://cti-lists.cisecurity.org/lists/log4j_hashes.txt (Fingerprints of suspicious/malicious files associated with attack attempts against Log4j)

Also, in response to requests from members to compile and share potentially malicious IPs and domains scanning due to the recent conflict in Ukraine, the MS-ISAC has compiled information from our own collection and merged them with indicators from trusted third parties. The indicators have been made them available via our CTI Lists service here:

https://cti-lists.cisecurity.org/lists/Russian_Scanning_IPs.txt

The MS-ISAC intends to keep the lists updated daily as new indicators are observed.

Note: If you have already signed up and are receiving a 403 error when accessing the above links, check your with your internet-facing IP/CIDR info and email it to us indicator.sharing@cisecurity.org.

Connecting to the MS-ISAC STIX/TAXII Feed:

These same indicators are included in our STIX/TAXII feed (along with other curated indicators). If you're able to ingest a STIX/TAXII fee, contact the MS-ISAC at Indicator.Sharing@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Members that would like to use the API to access the MS-ISAC Malware IPs and Domains in order to auto populate their security perimeter devices may download the scripts from our GitHub repository at https://github.com/MSISAC/STIX-TAXII-Integration. The API requires IP whitelist access, which can be obtained by sending your IP address or range to Indicator.Sharing@cisecurity.org. If you were previously whitelisted for our Palo Alto external block lists, the IP address or range already provided is whitelisted for the above.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

College. If you are unsure of the authenticity of the sender, **DO NOT** click any links or download any attachments. If you suspect this message is a phishing attempt, please FORWARD the Email to HelpDesk@cerritos.edu

From: Omer Usmani <ousmani@CCCTECHCENTER.ORG>
Sent: Monday, March 7, 2022 3:03 PM
To: ISAC@LISTSERV.CCCNEXT.NET
Subject: Fwd: Scanning and Exploiting IPs observed by MS-ISAC - 2/1/22 - 2/28/22 - TLP:GREEN

---------- Forwarded message ---------
From: **MS-ISAC Advisory** <MS-ISAC.Advisory@msisac.org>
Date: Mon, Mar 7, 2022 at 12:23 PM
Subject: Scanning and Exploiting IPs observed by MS-ISAC - 2/1/22 - 2/28/22 - TLP:GREEN
To: MS-ISAC SOC <SOC@msisac.org>, MS-ISAC CTI <Intel@cisecurity.org>

TLP: GREEN

Nothing attached to this email as there is no significantly reoccuring activity observed by MS-ISAC from 2/1/22 - 2/28/22 using our monitoring services.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

This data is collected from public organizations and government entities within the United States. This list is produced on a monthly basis and contains the IP addresses that were repeat offenders of this activity over the entire duration of the date range specified above. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

The spreadsheet contains the following information:

1. **IP ADDRESS** - This is the IP address that is performing the scan or exploit.
2. **COUNTRY, REGION, CITY** - Location of the potentially malicious IP address.
3. **ISP** - ISP or Hosting provider for the IP address.
4. **ASSOCIATED THREAT** – Logged activity associated with the IP address.
5. **TARGETED ENTITY TYPES** – The types of entities that were being targeted.

MS-ISAC is sharing this information to provide better situational awareness to all partners. We recommend that the following actions be taken:

- Consider blocking and alerting on these IP addresses as they have been logged attempting to exploit vulnerabilities or otherwise gain access or information about SLTT network resources.
- Investigate any logged activity from the noted IP addresses for signs of successful exploitation.
- Note that an IP address can be associated with multiple legitimate domain names. Blocking outbound traffic may prevent legitimate traffic from reaching these domains. This is especially true for those belonging to a hosting company.

Connecting to the MS-ISAC STIX/TAXII Feed:

If you would like to connect to the MS-ISAC STIX/TAXII feed to receive these indicators, contact the MS-ISAC at Indicator.Sharing@cisecurity.org. A member of this team will walk you through the steps in setting up access to the MS-ISAC feed to begin receiving data.

Members that would like to use the API to access the MS-ISAC Malware IPs and Domains in order to auto populate their security perimeter devices may download the scripts from our GitHub repository at https://github.com/MSISAC/STIX-TAXII-Integration. The API requires IP whitelist access, which can be obtained by sending your IP address or range to Indicator.Sharing@cisecurity.org. If you were previously whitelisted for our Palo Alto external block lists, the IP address or range already provided is whitelisted for the above.

Please feel free to contact MS-ISAC if you have any questions or need any additional assistance. We can assist by performing a variety of incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.

If you have any questions, comments or need additional information, please contact us at 1-866-787-4722 or email us at soc@cisecurity.org.

24x7 Security Operations Center

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24×7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722

TLP: GREEN

https://www.cisa.gov/tlp

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. Do not release TLP:GREEN information outside of the community.

Please send all opt out requests to info@msisac.org.