#StopRansomware: Vice Society | CISA

Published: 2022-09-08 · Archived: 2026-04-05 19:14:31 UTC

Summary

Actions to take today to mitigate cyber threats from ransomware:

• Prioritize and remediate known exploited vulnerabilities.
• Train users to recognize and report phishing attempts.
• Enable and enforce multifactor authentication.

Note: *This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate IOCs and TTPs associated with Vice Society actors identified through FBI investigations as recently as September 2022. The FBI, CISA, and the MS-ISAC have recently observed Vice Society actors disproportionately targeting the education sector with ransomware attacks.

Over the past several years, the education sector, especially kindergarten through twelfth grade (K-12) institutions, have been a frequent target of ransomware attacks. Impacts from these attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff. The FBI, CISA, and the MS-ISAC anticipate attacks may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks. School districts with limited cybersecurity capabilities and constrained resources are often the most vulnerable; however, the opportunistic targeting often seen with cyber criminals can still put school districts with robust cybersecurity programs at risk. K-12 institutions may be seen as particularly lucrative targets due to the amount of sensitive student data accessible through school systems or their managed service providers.

The FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

Download the PDF version of this report: pdf, 521 KB

Download the IOCs: .stix 31 kb

Technical Details

Note: *This advisory uses the MITRE ATT&CK® for Enterprise framework, version 11. See MITRE ATT&CK for Enterprise for all referenced tactics and techniques.*

Vice Society is an intrusion, exfiltration, and extortion hacking group that first appeared in summer 2021. Vice Society actors do not use a ransomware variant of unique origin. Instead, the actors have deployed versions of Hello Kitty/Five Hands and Zeppelin ransomware, but may deploy other variants in the future.

Vice Society actors likely obtain initial network access through compromised credentials by exploiting internet-facing applications [T1190]. Prior to deploying ransomware, the actors spend time exploring the network, identifying opportunities to increase accesses, and exfiltrating data [TA0010] for double extortion--a tactic whereby actors threaten to publicly release sensitive data unless a victim pays a ransom. Vice Society actors have been observed using a variety of tools, including SystemBC, PowerShell Empire, and Cobalt Strike to move laterally. They have also used "living off the land" techniques targeting the legitimate Windows Management Instrumentation (WMI) service [T1047] and tainting shared content [T1080].

Vice Society actors have been observed exploiting the PrintNightmare vulnerability (CVE-2021-1675 and CVE-2021-34527) to escalate privileges [T1068]. To maintain persistence, the criminal actors have been observed leveraging scheduled tasks [T1053], creating undocumented autostart Registry keys [T1547.001], and pointing legitimate services to their custom malicious dynamic link libraries (DLLs) through a tactic known as DLL side-loading [T1574.002]. Vice Society actors attempt to evade detection through masquerading their malware and tools as legitimate files [T1036], using process injection [T1055], and likely use evasion techniques to defeat automated dynamic analysis [T1497]. Vice Society actors have been observed escalating privileges, then gaining access to domain administrator accounts, and running scripts to change the passwords of victims' network accounts to prevent the victim from remediating.

Indicators of Compromise (IOCs)

Email Addresses
v-society.official@onionmail[.]org
ViceSociety@onionmail[.]org
OnionMail email accounts in the format of [First Name][Last Name]@onionmail[.]org
TOR Address
http://vsociethok6sbprvevl4dlwbqrzyhxcxaqpvcqt5belwvsuxaxsutyad[.]onion

IP Addresses for C2	Confidence Level
5.255.99[.]59	High Confidence
5.161.136[.]176	Medium Confidence
198.252.98[.]184	Medium Confidence
194.34.246[.]90	Low Confidence

See Table 1 for file hashes obtained from FBI incident response investigations in September 2022.

Table 1: File Hashes as of September 2022

MD5	SHA1
fb91e471cfa246beb9618e1689f1ae1d	a0ee0761602470e24bcea5f403e8d1e8bfa29832
	3122ea585623531df2e860e7d0df0f25cce39b21
	41dc0ba220f30c70aea019de214eccd650bc6f37
	c9c2b6a5b930392b98f132f5395d54947391cb79

MITRE ATT&CK TECHNIQUES

Vice Society actors have used ATT&CK techniques, similar to Zeppelin techniques, listed in Table 2.

Table 2: Vice Society Actors ATT&CK Techniques for Enterprise

Initial Access		
Technique Title	**ID**	**Use**
Exploit Public-Facing Application	T1190	Vice Society actors exploit vulnerabilities in an internet-facing systems to gain access to victims' networks.
Valid Accounts	T1078	Vice Society actors obtain initial network access through compromised valid accounts.
Execution		
Technique Title	**ID**	**Use**
Windows Management Instrumentation (WMI)	T1047	Vice Society actors leverage WMI as a means of "living off the land" to execute malicious commands. WMI is a native Windows administration feature.

Scheduled Task/Job	T1053	Vice Society have used malicious files that create component task schedule objects, which are often mean to register a specific task to autostart on system boot. This facilitates recurring execution of their code.
Persistence		
Technique Title	**ID**	**Use**
Modify System Process	T1543.003	Vice Society actors encrypt Windows Operating functions to preserve compromised system functions.
Registry Run Keys/Startup Folder	T1547.001	Vice Society actors have employed malicious files that create an undocumented autostart Registry key to maintain persistence after boot/reboot.
DLL Side-Loading	T1574.002	Vice Society actors may directly side-load their payloads by planting their own DLL then invoking a legitimate application that executes the payload within that DLL. This serves as both a persistence mechanism and a means to masquerade actions under legitimate programs.
Privilege Escalation		
Technique Title	**ID**	**Use**
Exploitation for Privilege Escalation	T1068	Vice Society actors have been observed exploiting PrintNightmare vulnerability (CVE-2021-1675 and CVE-2021-34527) to escalate privileges.
Defense Evasion		
Technique Title	**ID**	**Use**
Masquerading	T1036	Vice Society actors may attempt to manipulate features of the files they drop in a victim's environment to mask the files or make the files appear legitimate.
Process Injection	T1055	Vice Society artifacts have been analyzed to reveal the ability to inject code into legitimate processes for evading process-based defenses. This tactic has other potential impacts, including the ability to escalate privileges or gain additional accesses.
Sandbox Evasion	T1497	Vice Society actors may have included sleep techniques in their files to hinder common reverse engineering or dynamic analysis.
Lateral Movement		

Technique Title	ID	Use
Taint Shared Content	T1080	Vice Society actors may deliver payloads to remote systems by adding content to shared storage locations such as network drives.
Exfiltration		
Technique Title	**ID**	**Use**
Exfiltration	TA0010	Vice Society actors are known for double extortion, which is a second attempt to force a victim to pay by threatening to expose sensitive information if the victim does not pay a ransom.
Impact		
Technique Title	**ID**	**Use**
Data Encrypted for Impact	T1486	Vice Society actors have encrypted data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.
Account Access Removal	T1531	Vice Society actors run a script to change passwords of victims' email accounts.

Mitigations

The FBI and CISA recommend organizations, particularly the education sector, establish and maintain strong liaison relationships with the FBI Field Office in their region and their regional CISA Cybersecurity Advisor. The location and contact information for FBI Field Offices and CISA Regional Offices can be located at www.fbi.gov/contact-us/field-offices and www.cisa.gov/cisa-regions, respectively. Through these partnerships, the FBI and CISA can assist with identifying vulnerabilities to academia and mitigating potential threat activity. The FBI and CISA further recommend that academic entities review and, if needed, update incident response and communication plans that list actions an organization will take if impacted by a cyber incident.

The FBI, CISA, and the MS-ISAC recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise by Vice Society actors:

Preparing for Cyber Incidents

- **Maintain offline backups of data,** and regularly maintain backup and restoration. By instituting this practice, the organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure. Ensure your backup data is not already infected.
- **Review the security posture of third-party vendors and those interconnected with your organization.** Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.

- **Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs** under an established security policy.
- **Document and monitor external remote connections.** Organizations should document approved solutions for remote management and maintenance, and immediately investigate if an unapproved solution is installed on a workstation.
- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).

Identity and Access Management

- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) **to comply** with National Institute of Standards and Technology (NIST) standards for developing and managing password policies.
    - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length;
    - Store passwords in hashed format using industry-recognized password managers;
    - Add password user "salts" to shared login credentials;
    - Avoid reusing passwords;
    - Implement multiple failed login attempt account lockouts;
    - Disable password "hints";
    - Refrain from requiring password changes more frequently than once per year unless a password is known or suspected to be compromised.
      Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
    - Require administrator credentials to install software.
- **Require phishing-resistant multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege.
- **Implement 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 admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.

Protective Controls and Architecture

- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.

- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Secure and closely monitor** remote desktop protocol (RDP) use.
    - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. If RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a VPN, virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.

Vulnerability and Configuration Management

- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Organizations should prioritize patching of vulnerabilities on CISA's Known Exploited Vulnerabilities catalog.
- **Disable unused ports.**
- **Consider adding an email banner to emails** received from outside your organization.
- **Disable hyperlinks** in received emails.
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Ensure devices are properly configured and that security features are enabled.**
- **Disable ports and protocols that are not being used** for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).
- **Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary, and remove or disable outdated versions of SMB** (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.

REFERENCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment .

REPORTING

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with Vice Society actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

The FBI, CISA, and the MS-ISAC strongly discourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to a local FBI Field Office, or to CISA at report@cisa.gov✉ or by calling 1-844-Say-CISA (1-844-729-2472). SLTT government entities can also report to the MS-ISAC (SOC@cisecurity.org✉ or 866-787-4722).

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. The FBI, CISA, and the MS-ISAC 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 endorsement, recommendation, or favoring by the FBI, CISA, or the MS-ISAC.

Revisions

September 6, 2022: Initial Version
