LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Web Shell Malware: Threats and Mitigations

05/21/2020

Report #: 202005211030

Agenda

- What is a Web Shell?
- How are Web Shells Used by Adversaries?
- Web Shell Delivery Tactics
- Threat Actors Leveraging Web Shell Technique
- Malware Profile: China Chopper Web Shell
- What is the Risk to Healthcare Organizations?
- How Prolific are Web Shells?
- Summary of NSA/ASD Mitigations
- Technical Resources for Detection and Prevention
- References and Additional Resources
- Questions

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What is a Web Shell?

A web shell is a web security threat which is a web-based implementation of the shell concept. A web shell can be uploaded to a web server to allow remote access of the web server.

Web shells have both a legitimate and malicious use reference.

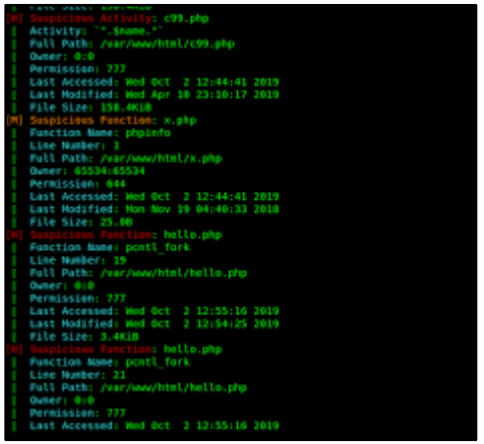
Legitimate use reference:

- Web-based system management tools used legitimately by administrators
- A script that can be uploaded to a web server to enable remote administration of the machine
- *Example*: Microsoft Azure Cloud Shell; IT admin

VS.

Malicious use reference:

- Malicious code used to gain foothold onto web servers and for proliferating compromise;
- Often considered a form of Remote Access Trojan (RAT)
- *Example*: China Chopper Web Shell



Note: Web shells may be either web-facing or on internal networks.

How are Web Shells Used by Adversaries?

Malicious web shells are commonly utilized for the following purposes:

1. To harvest and exfiltrate sensitive data and credentials;

2. To upload additional malware for the potential of creating, for example, a watering hole for infection and scanning of further victims;

3. To use as a relay point to issue commands to hosts inside the network without direct Internet access;

4. To use as command-and-control infrastructure, potentially in the form of a bot in a botnet or in support of compromises to additional external networks;

5. Website defacement by modifying files with malicious intent.

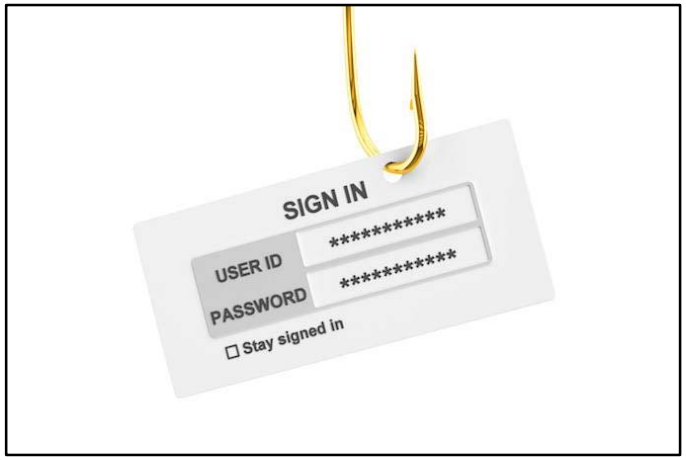


Image source: ThreatPost

Note: While a web shell itself would not normally be used for denial of service (DoS) attacks, it can act as a platform for uploading further tools, including DoS capability.

Source: https://www.us-cert.gov/

How Prolific are Web Shells?

In a February 2020 blog post, Microsoft said that on a daily basis the company's security team detects and tracks on average around 77,000 active web shells, spread across 46,000 infected servers.

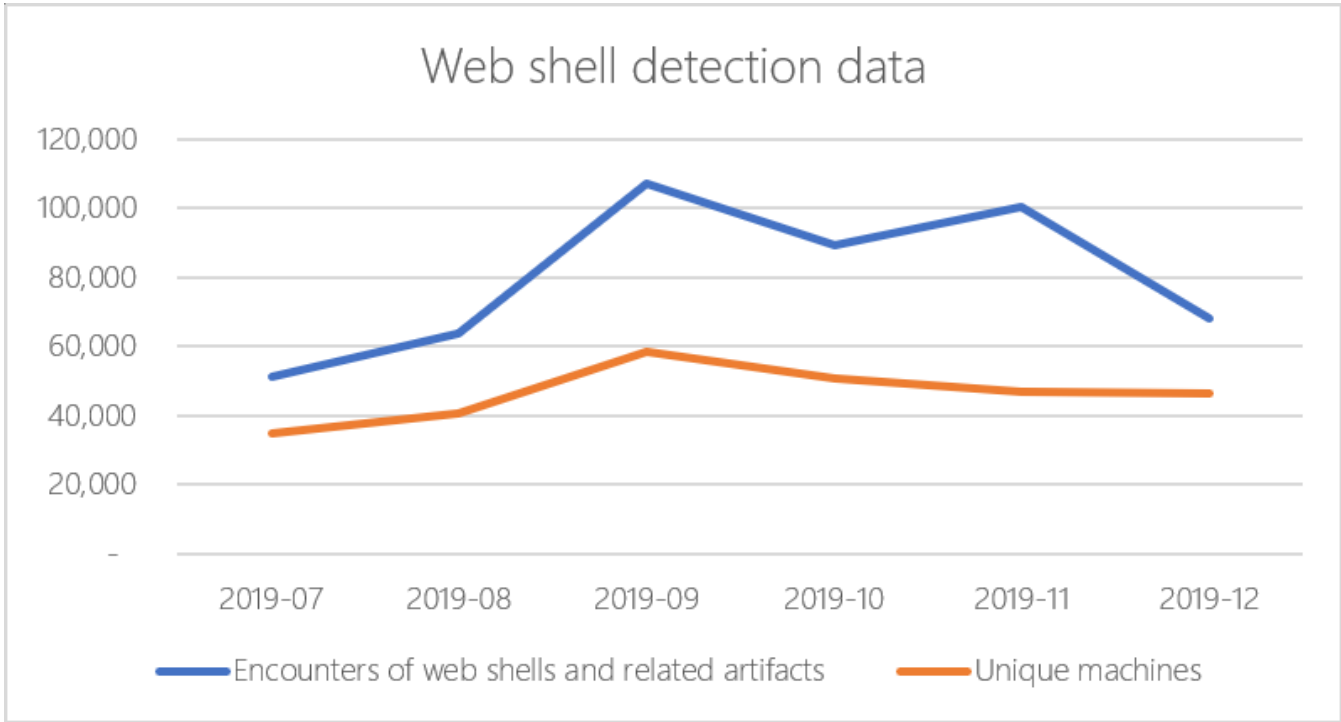


Image source: Microsoft

Web Shell Delivery Tactics

Web shells can be delivered through a number of web application exploits or configuration weaknesses including:

- Cross-Site Scripting (XSS);
- SQL Injection (SQLi);
- Vulnerabilities in applications/services;
- File processing vulnerabilities;
- Remote File Inclusion (RFI) and Local File Inclusion (LFI) vulnerabilities;
- Exposed Admin Interfaces;

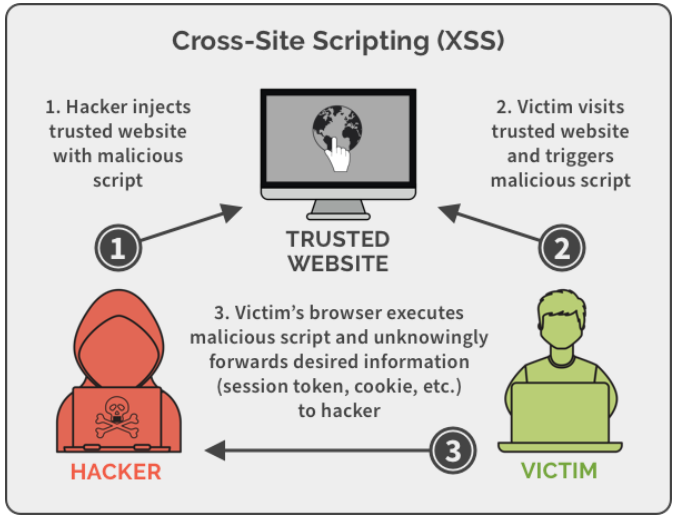


Image Source: Spanning Backup

The above tactics can be and are combined regularly. For example, an exposed admin interface also requires a file upload option, or another exploit method mentioned above, to deliver successfully.

Source: https://www.us-cert.gov/

Threat Actors Leveraging Web Shell Techniques

Some major threat actors commonly known to leverage web shell techniques in their attacks include APT39, Deep Panda, Leviathan, and APT34 (or OilRig).

Name	Description
APT39	APT39 has installed ANTAK and ASPXSPY web shells. APT39 is an Iranian cyber espionage group that has been active since at least 2014. They have targeted the telecommunication and travel industries to collect personal information that aligns with Iran's national priorities.
Deep Panda	Deep Panda uses Web shells on publicly accessible Web servers to access victim networks. Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. The intrusion into U.S. healthcare company Anthem has been attributed to Deep Panda. This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. Some analysts track Deep Panda and APT19 as the same group, but it is unclear from open source information if the groups are the same.
Leviathan	Leviathan relies on web shells for an initial foothold as well as persistence into the victim's systems. Leviathan is a cyber espionage group that has been active since at least 2013. The group generally targets defense and government organizations, but has also targeted a range of industries including engineering firms, shipping and transportation, manufacturing, defense, government offices, and research universities in the United States, Western Europe, and along the South China Sea.
OilRig (APT34)	OilRig has used Web shells, often to maintain access to a victim network. OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East.

Source: Mitre ATT&CK

Malware Profile: China Chopper Web Shell

China Chopper

- Among web shells used by threat actors, the China Chopper web shell is one of the most widely used, typically for **cyber espionage**.
- China Chopper is a web shell hosted on Web servers to provide access back into an enterprise network that does not rely on an infected system calling back to a remote command and control (C&C) server.
- Two key components: web shell C&C client binary and text-based web shell payload (server component)
- Cybersecurity agencies have previously reported seeing attackers take over SharePoint servers and plant a version of the China Chopper web shell.
- It has been used by several threat groups, mainly Chinese actors, and is widely available for use.

Image Source: Malware Expert

Malware Profile: China Chopper Web Shell

China Chopper Recent Campaigns

1) Cyber espionage campaign targeting an Asian government to steal documents

2) Organization in Lebanon targeted by several actors with China Chopper which was used as an infection vector to deploy ransomware and cryptominer.

3) Asian web-hosting provider was targeted by threat actors over a 10 month period who used China Chopper to compromise several Windows servers and then carry out additional operations

Image Source: Cisco Talos

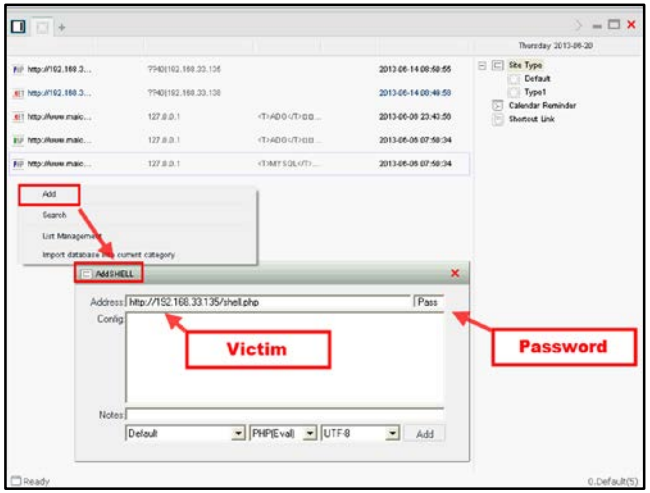


Image Source: FireEye

SharePoint Vulnerability Among Top 10 Exploited

On 12 May 2020, the Cybersecurity and Infrastructure Security Agency (CISA) along with other agencies released an alert on the Top 10 Routinely Exploited Vulnerabilities by threat actors from 2016 to 2019. One of these is a SharePoint vulnerability exploited by China Chopper.

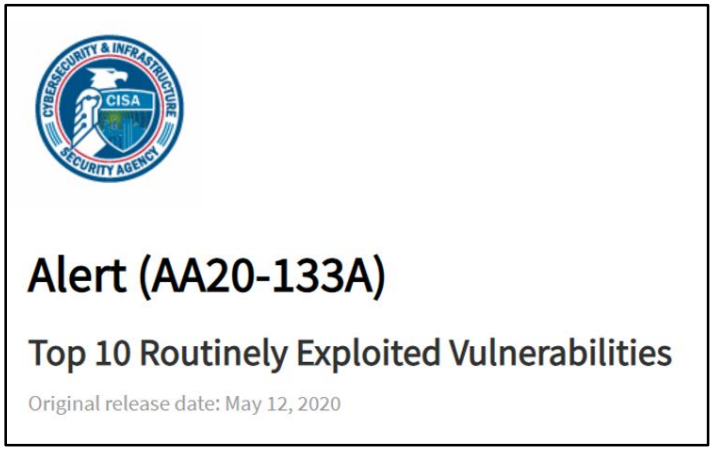


Image Source: DHS CISA

CVE-2019-0604

- **Vulnerable Products:** Microsoft SharePoint
- **Associated Malware:** China Chopper
- **Mitigation:** Update affected Microsoft products with the latest security patches

***More Detail*:** https://nvd.nist.gov/vuln/detail/CVE-2019-0604

What is the Risk to Healthcare Organizations?

Impact: A successfully uploaded shell script may allow a remote attacker to bypass security restrictions and gain unauthorized system access.

Image source: Security Info Watch

Question: Where might healthcare organizations be susceptible to Web Shell attacks?

- SharePoint servers or Content Management Systems
- Patient portals
- Hospital systems remote admin

Question: What do healthcare organizations have at risk due to successful exploitation?

- Unauthorized access to medical research
- Breach of protected health information (PHI) and electronic health records (EHR)
- Persistence mechanism to hospital network for further exploitation such as ransomware deployment

21 April 2020 Joint NSA / ASD Guidance

On 21 April 2020, the National Security Agency (NSA) and Australian Signals Directorate (ASD) published Cybersecurity Information (CSI) on how to Detect and Prevent Web Shell Malware. The report contains numerous mitigating actions including:

1) Mitigating Actions (DETECTION)

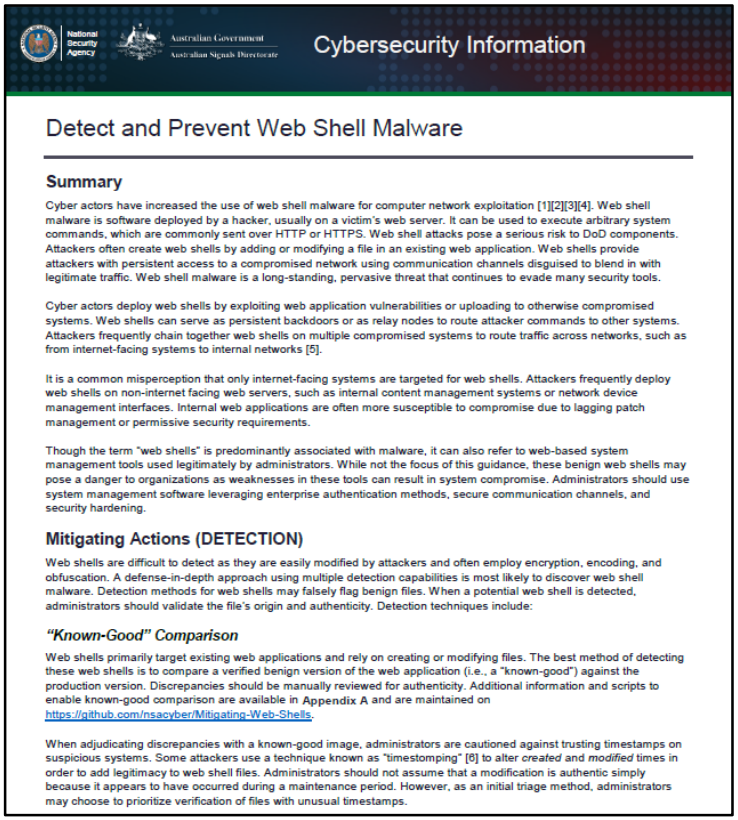
- **"Known-good" Comparison**
- **Web Traffic Anomaly Detection**
- **Signature-based Detection**
- **Other Anomalous Network Traffic Indicators**

2) Mitigating Actions (PREVENTION)

- **Web Application Updates & Permissions**
- **File Integrity Monitoring**
- **Intrusion Prevention (IPS and WAF)**
- **Network Segregation & Harden Web Servers**

3) Mitigating Actions (RESPONSE and RECOVERY)

- **How far did the attacker penetrate the network?**
- **Assess pivoting within network**



National Security Agency | Australian Government, Australian Signals Directorate

Cybersecurity Information

Detect and Prevent Web Shell Malware

Summary

Cyber actors have increased the use of web shell malware for computer network exploitation [1][2][3][4]. Web shell malware is software deployed by a hacker, usually on a victim's web server. It can be used to execute arbitrary system commands, which are commonly sent over HTTP or HTTPS. Web shell attacks pose a serious risk to DoD components. Attackers often create web shells by adding or modifying a file in an existing web application. Web shells provide attackers with persistent access to a compromised network using communication channels disguised to blend in with legitimate traffic. Web shell malware is a long-standing, pervasive threat that continues to evade many security tools.

Cyber actors deploy web shells by exploiting web application vulnerabilities or uploading to otherwise compromised systems. Web shells can serve as persistent backdoors or as relay nodes to route attacker commands to other systems. Attackers frequently chain together web shells on multiple compromised systems to route traffic across networks, such as from internet-facing systems to internal networks [5].

It is a common misperception that only internet-facing systems are targeted for web shells. Attackers frequently deploy web shells on non-internet facing web servers, such as internal content management systems or network device management interfaces. Internal web applications are often more susceptible to compromise due to lagging patch management or permissive security requirements.

Though the term "web shells" is predominantly associated with malware, it can also refer to web-based system management tools used legitimately by administrators. While not the focus of this guidance, these benign web shells may pose a danger to organizations as weaknesses in these tools can result in system compromise. Administrators should use system management software leveraging enterprise authentication methods, secure communication channels, and security hardening.

Mitigating Actions (DETECTION)

Web shells are difficult to detect as they are easily modified by attackers and often employ encryption, encoding, and obfuscation. A defense-in-depth approach using multiple detection capabilities is most likely to discover web shell malware. Detection methods for web shells may falsely flag benign files. When a potential web shell is detected, administrators should validate the file's origin and authenticity. Detection techniques include:

"Known-Good" Comparison

Web shells primarily target existing web applications and rely on creating or modifying files. The best method of detecting these web shells is to compare a verified benign version of the web application (i.e., a "known-good") against the production version. Discrepancies should be manually reviewed for authenticity. Additional information and scripts to enable known-good comparison are available in Appendix A and are maintained on https://github.com/nsacyber/Mitigating-Web-Shells.

When adjudicating discrepancies with a known-good image, administrators are cautioned against trusting timestamps on suspicious systems. Some attackers use a technique known as "timestomping" [6] to alter *created* and *modified* times in order to add legitimacy to web shell files. Administrators should not assume that a modification is authentic simply because it appears to have occurred during a maintenance period. However, as an initial triage method, administrators may choose to prioritize verification of files with unusual timestamps.

Source: https://www.nsa.gov/News-Features/News-Stories/

Technical Resources for Detection and Prevention

Below is a list of some of the technical resources for detecting and preventing web shell malware as provided in the NSA/ASD report from 21 April 2020:

1) Scripts to Compare a Production Website to a Known-Good Image
2) Splunk® Queries for Detecting Anomalous URIs in Web Traffic
3) Internet Information Services™ (IIS) Log Analysis Tool
4) Network Signatures of Traffic for Common Web Shells
5) Snort Rules for Identifying Unexpected Network Flows
6) Queries for Identifying Abnormal Process Invocations in Sysmon Data
7) Queries for Identifying Abnormal Process Invocations with Auditd

Image source: Splunk

Source: https://github.com/nsacyber/Mitigating-Web-Shells

Basic Mitigation Techniques

- The most powerful defense against a web shell is to avoid the web server being compromised in the first place.
- Ensure that all the software running on public facing web servers is up to date, with security patches applied.
- Audit custom applications for common web vulnerabilities
- Privileged Account Management

Image source: techzone360

Reference Materials

References

- National Security Agency & Australian Signals Directorate Cybersecurity Information
  - https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2159419/detect-prevent-cyber-attackers-from-exploiting-web-servers-via-web-shell-malware/
- NSA Cyber GitHub, Guidance for Mitigating Web Shells
  - https://github.com/nsacyber/Mitigating-Web-Shells
- Mitre, Enterprise ATT&CK Techniques, Web Shell (ID T1100)
  - https://attack.mitre.org/techniques/T1100/
- Acunetix, An Introduction to Web Shells (Web Shells Part 1)
  - https://www.acunetix.com/blog/articles/introduction-web-shells-part-1/
- InfoSec Institute, Web Shell Detection Using NeoPI
  - https://resources.infosecinstitute.com/web-shell-detection/
- Microsoft, Ghost in the shell: Investigating web shell attacks
  - https://www.microsoft.com/security/blog/2020/02/04/ghost-in-the-shell-investigating-web-shell-attacks/
- Cisco Talos Blog, China Chopper still active 9 years later
  - https://blog.talosintelligence.com/2019/08/china-chopper-still-active-9-years-later.html
- HealthITSecurity, NSA Shares Guide to Web Shell, Malware Vulnerabilities, Mitigation
  - https://healthitsecurity.com/news/nsa-shares-guide-to-web-shell-malware-vulnerabilities-mitigation

References

- Offensive Security, File Inclusion Vulnerabilities
  - https://www.offensive-security.com/metasploit-unleashed/file-inclusion-vulnerabilities/
- OWASP, SQL Injection
  - https://owasp.org/www-community/attacks/SQL_Injection
- FireEye, Threat Research: Breaking Down the China Chopper Web Shell - Part I
  - https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
- FireEye, The Little Malware That Could: Detecting and Defeating the China Chopper Web Shell
  - https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-china-chopper.pdf
- ZDNet, Microsoft says it detects 77,000 active web shells on a daily basis
  - https://www.zdnet.com/article/microsoft-says-it-detects-77000-active-web-shells-on-a-daily-average/
- ThreatPost, Elderly China Chopper Tool Still Going Strong in Multiple Campaigns
  - https://threatpost.com/china-chopper-tool-multiple-campaigns/147813/
- Cybereason, Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers
  - https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
- Rapid7, Web Shells 101: Detection and Prevention
  - https://blog.rapid7.com/2016/12/14/webshells-101/

Questions

Questions

Upcoming Briefs

- Healthcare Information Security Assessment and Auditing (5/28)
- Maze Ransomware (6/4)

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV