



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

# HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY



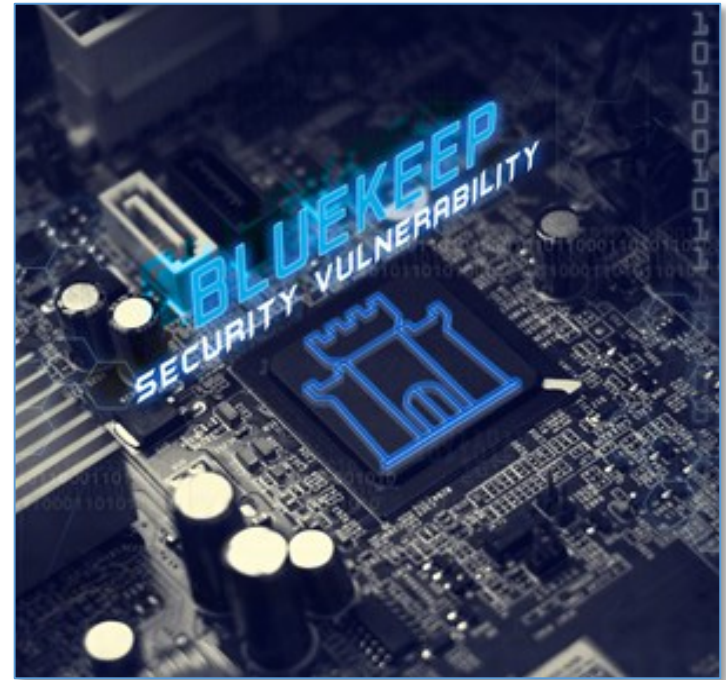
## BlueKeep Update

12/05/2019

# Agenda



- What is BlueKeep
- Timeline of BlueKeep
- BlueKeep Today
- Initial Attempts to Exploit BlueKeep
- Why Initial Attempts Failed
- BlueKeep Tomorrow
- Mitigations
- Indicators of Compromise (IOCs)
- HC3 Contact Information
- References



## Slides Key:



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



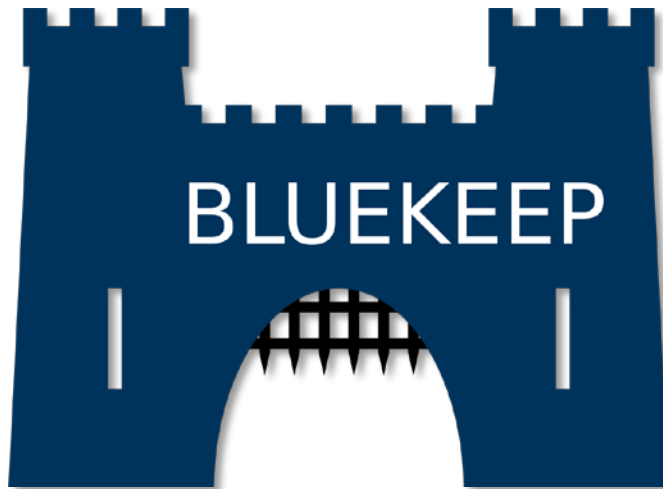
Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



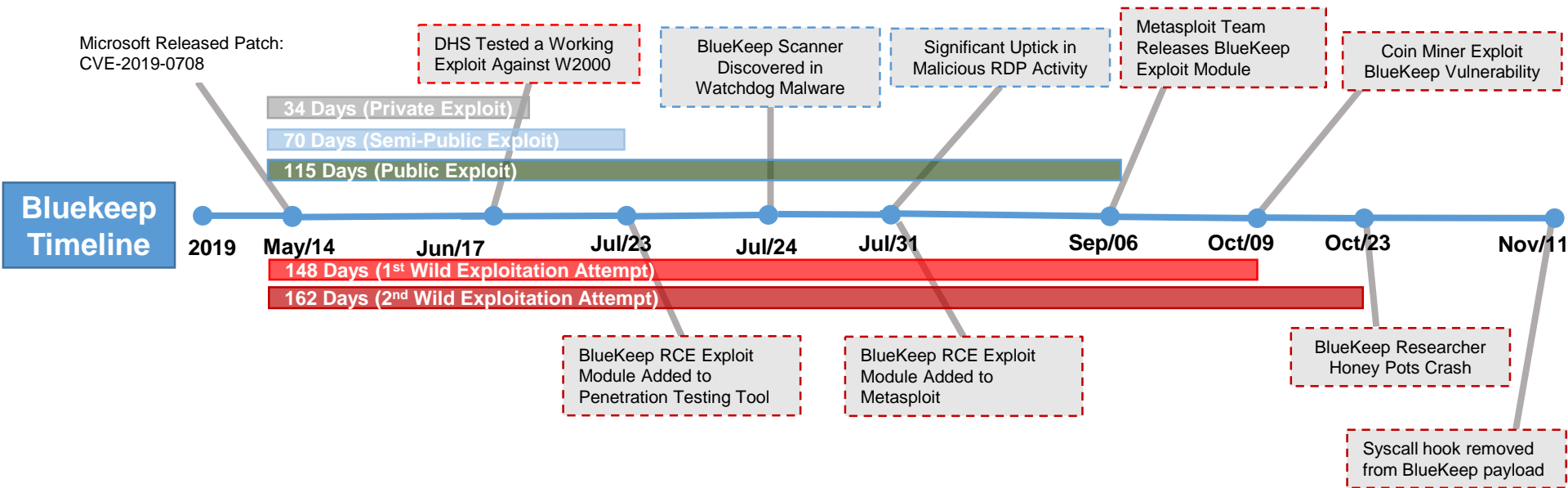
# What is BlueKeep



- BlueKeep ([CVE-2019-0708](#))
  - Vulnerability in Microsoft's (MS) Remote Desktop Protocol
    - Grants hackers full remote access and code execution on unpatched machines
      - No user interaction required
      - Essential owns the machine, malicious actor can do as they please
    - Affects: Windows XP, 7, Server 2003, Server 2008, and Server 2008 R2
      - [Deja Blue](#) (Related BlueKeep Vulnerabilities) affects: Windows 8, 10, and all older windows versions
      - [EternalBlue](#) affects: Server Message Block version 1 (SMBv1)
    - "Wormable" meaning it has the ability to self propagate (think WannaCry level of damage)
    - [MS](#), [NSA](#), [DHS](#), many other security vendors released advisories and warning on this exploit



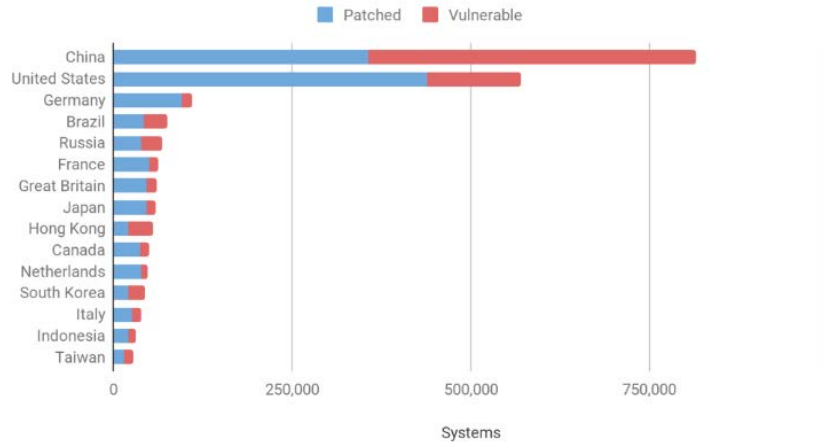
# BlueKeep Timeline



[Tencent](#) [RiskSense](#) [Microsoft](#) [Rapid7](#)



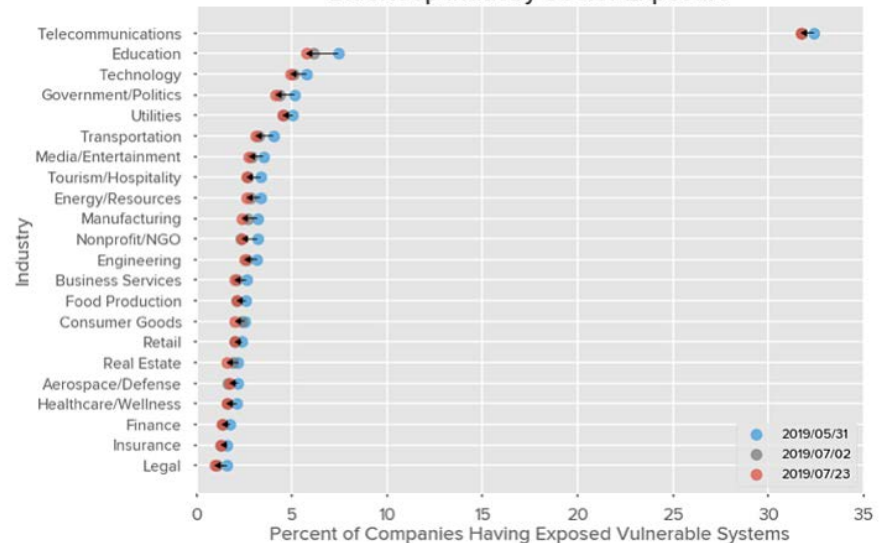
Top Countries Bluekeep Exposure



- Data Covers May 31 to July 2, 2019
- “As of July 2, 2019, approximately **805,665 systems** remain online that are vulnerable to BlueKeep, representing a decrease of 17.18% (167,164 systems) compared to May 31.”

*“There has been progress made across the board as all industries have demonstrated a reduction in the number of organizations with exposed vulnerable systems since data collected on May 31, 2019, with variable amount of progress made within each industry.” ~BitSight*

BlueKeep Industry Sector Exposure





- Out in the Wild!
  - Don't panic just yet
  - Spotted by security researchers [Kevin Beaumont](#) and [Marcus Hutchins](#) in early Nov
    - Beaumont's honeypots, set up to detect and monitor BlueKeep, kept crashing with "Blue Screen Of Deaths".
    - Sent Logs to Hutchins for deep dive analysis
  - Conclusion
    - No worm function
    - No self propagation
    - Used in low level attacks
      - Done by same group of malicious actors
      - Wild BlueKeep Shellcode matches Metasploits Shellcode
      - Attacks in Sept and Oct shared the same Command and Control infrastructure
        - Attackers most likely using manual port scans to find vulnerable machines
      - Cryptomining attacks ~type of coin is unknown

*"They're not seeking targets. They're scanning the internet and spraying exploits."*  
[Marcus Hutchins](#) – Kryptos Logic

<pre>fffffa80`08807058 488d0df9ffffff lea    rcx, [fffffa80`08807058] fffffa80`0880705f 49b86920e4ef0fac0db0 mov    r8, 0B00DAC0FEFE42069h  fffffa80`08807069 4881e900040000 sub    rcx, 400h fffffa80`08807070 482d00040000 sub    rax, 400h fffffa80`08807076 488b51f8 mov    rdx, qword ptr [rcx-8] fffffa80`0880707a 4c39c2 cmp    rdx, r8 fffffa80`0880707d 75ea ine    fffffa80`08807069 fffffa80`0880707f ffe1 jmp    rcx</pre>	<pre>359  _start: 360  lea rcx, [rel_start] 361  mov r8, 0x{KERNELMODE_EGG.to_s(16)} 362  _egg_loop: 363  sub rcx, 0x{CHUNK_SIZE.to_s(16)} 364  sub rax, 0x{CHUNK_SIZE.to_s(16)} 365  mov rdx, [rdx - 8] 366  cmp rdx, r8 367  jnz _egg_loop 368  jmp rcx</pre>
--	---

Side by side of the in-memory shellcode and the metasploit shellcode

[Kryptoslogic](#)



# Initial Attempts to Exploit BlueKeep



## MITRE ATT&CK

T1190 | Network Service Scanning



1. Scans for vulnerable RDP services

 Security update for CVE-2019-0708

T1190 | Exploit Public-Facing Application



2. BlueKeep RDP exploit

 Windows Defender Antivirus

 Security update for CVE-2019-0708

 Network level authentication

T1086 | PowerShell

T1064 | Scripting

T1027 | Obfuscated File or Information

T1140 | Deobfuscate/Decode Files or Information



3. Download and execution of multiple obfuscated PowerShell scripts

 EDR

T1053 | Scheduled Task



5. Scheduled task for payload persistence

 EDR

T1043 | Commonly Used Port  
T1065 | Uncommonly Used Port



6. C&C communication

 EDR

Microsoft



# Why Initial Attempts Failed



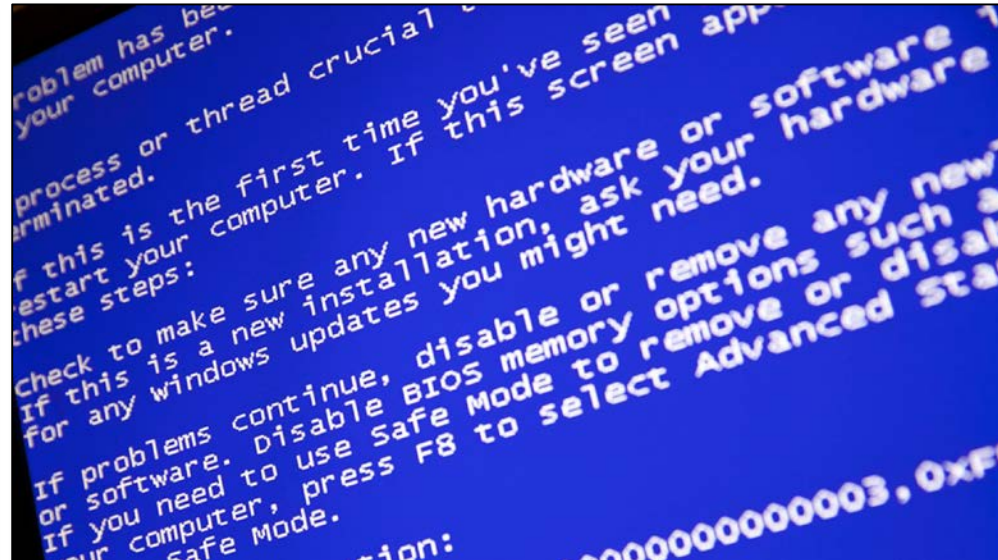
- BlueKeep is a [Fussy Exploit](#)
  - Reason why the attack [failed](#) was because of an incompatibility between the exploit code and a patch Microsoft had previously issued for the Intel CPU vulnerability known as [Meltdown](#)
  - Caused many machines to crash, causing many people to discount the [potential severity](#) of the Bluekeep vulnerability.
  - Already adapted
    - This incompatibility has already been [fixed](#) and patched into the Metasploit BlueKeep Module

**MalwareTech** [@MalwareTechBlog](#) · Nov 2, 2019  
Blog post on how I discovered mass exploitation of BlueKeep from a kernel dump of a crashed system. [twitter.com/kryptoslogic/s...](#)

**Kryptos Logic** [@kryptoslogic](#)  
BlueKeep (CVE 2019-0708) exploitation spotted in the wild [kryptoslogic.com/blog/2019/11/b...](#)

**Worawit Wang** [@sleepya\\_](#)  
From call stack, seems target has kva shadow patch. Original eternalblue kernel shellcode cannot be used on kva shadow patch target. So the exploit failed while running kernel shellcode

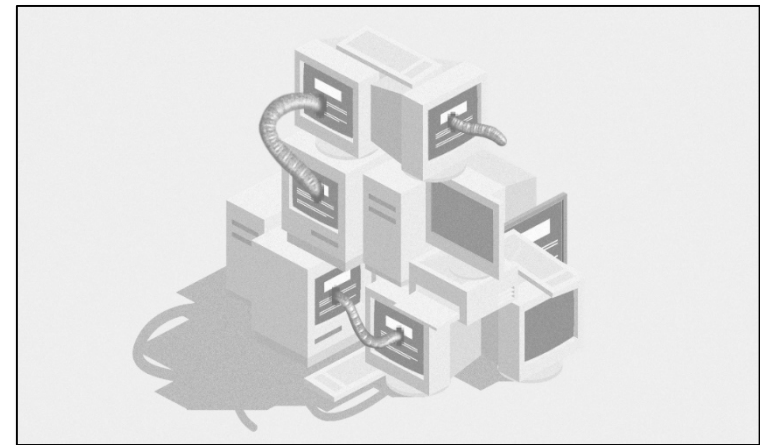
12 1:22 AM - Nov 4, 2019







- Where can BlueKeep go?
  - Will continue to [evolve](#), the risk of this vulnerability can [change](#) over time
  - Malicious Actors will focus on efforts that offer the greatest return (money) for effort
    - Wormable feature may be used in future attacks
      - Can spread without human interaction
      - [Loaded](#) with [ransomware](#) or other malicious programs
      - Can cause significant damage (ex. WannaCry)
  - Future attacks may focus [supply chain partners](#)
    - Unpatched Servers
    - Managed Service Providers
  - Unpatched systems will remain key in BlueKeep future success
    - Don't fall into the "[Avoidance](#)" (letting an acknowledged risk linger because there is no perceived penalty in procrastinating) trap





405(d) cybersecurity practice references denoted in red

- [Patch](#) and keep the system and its applications updated (or employ [virtual patching](#) to legacy or end-of-life systems) [7.S.A], [7.M.D]
- Restrict or [secure](#) the use of [remote desktop](#) services. For example, blocking port 3389 (or disabling it when not in use), can help thwart threats from initiating connections to systems behind the [firewall](#) [3.S.A], [3.M.A], [3.L.C]
- Enable [network level authentication](#) (NLA) to prevent unauthenticated attackers from exploiting BlueKeep. This can be [configured](#) in Windows 7 and Windows Server 2008 (including the R2 version) [3.S.A], [3.M.A], [3.L.C]
- Enforce the principle of least privilege. Employing security mechanisms like encryption, lockout policies, and other permission- or role-based access controls provide additional layers of security against attacks or threats that involve compromising remote desktops. [3.S.A], [3.M.A], [3.L.C]



**HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches

<https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx>



# BlueKeep Indicators of Compromise



- IOCs
  - IP Addresses
    - 109.176.117.11 port 8000
    - 5.100.251.106 port 52057
    - 217.114.18.50 port 52107
    - 193.27.73.223
    - 217.23.5.20
    - 157.245.82.38
    - 193.104.205.59
    - 217.23.5.70
    - 167.172.224.148
    - 160.20.146.133
    - 138.201.209.190
    - 167.71.240.219
    - 193.104.205.59
  - URLs
    - `hxxp://178.175.141.12:7023/9bccfaf8cd92/temp`
    - `hxxp://178.175.141.12:11008/6b53002fb437/temp`
    - `hxxp://138.201.209.190:10708/cc1ad438c54a/temp`

DoublePulsar





# Reference Materials



- Microsoft works with researchers to detect and protect against new RDP exploits  
<https://www.microsoft.com/security/blog/2019/11/07/the-new-cve-2019-0708-rdp-exploit-attacks-explained/>
- BlueKeep (CVE-2019-0708): From Rumor to Reality  
<https://risksense.com/blog/bluekeep-cve-2019-0708-from-rumor-to-reality/>
- DejaBlue vs BlueKeep vs Eternal Blue  
[https://www.linkedin.com/posts/jpcastro\\_exploit-dejablue-vulnerability-activity-6568053655193346048-KY6S/](https://www.linkedin.com/posts/jpcastro_exploit-dejablue-vulnerability-activity-6568053655193346048-KY6S/)
- Alert (AA19-168A) Microsoft Operating Systems BlueKeep Vulnerability  
<https://www.us-cert.gov/ncas/alerts/AA19-168A>
- Patch Remote Desktop Services on Legacy Versions of Windows  
[https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-bluekeep\\_20190604.pdf?ver=2019-06-04-123329-617](https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-bluekeep_20190604.pdf?ver=2019-06-04-123329-617)
- CVE-2019-1182 | Remote Desktop Services Remote Code Execution Vulnerability  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182>
- CVE-2019-1181 | Remote Desktop Services Remote Code Execution Vulnerability  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181>
- CVE-2019-0708  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708>



- Solved: Why in-the-wild Bluekeep exploits are causing patched machines to crash  
<https://arstechnica.com/information-technology/2019/11/solved-why-in-the-wild-bluekeep-exploits-are-causing-patched-machines-to-crash/>
- Spectre and Meltdown: What you need to know  
<https://www.tripwire.com/state-of-security/vert/spectre-meltdown-what-you-know/>
- BlueKeep: What you Need to Know  
<https://www.tripwire.com/state-of-security/featured/bluekeep-what-you-need-to-know/>
- Fixing Remote Windows Kernel Payloads to Bypass Meltdown KVA Shadow  
<https://zerosum0x0.blogspot.com/2019/11/fixing-remote-windows-kernel-payloads-meltdown.html>
- The First BlueKeep Mass Hacking Is Finally Here—but Don't Panic  
<https://www.wired.com/story/bluekeep-hacking-cryptocurrency-mining/>
- BlueKeep (CVE 2019-0708) exploitation spotted in the wild  
[https://www.kryptoslogic.com/blog/2019/11/bluekeep-cve-2019-0708-exploitation-spotted-in-the-wild/?source=post\\_page----bd6ee6e599a6-----](https://www.kryptoslogic.com/blog/2019/11/bluekeep-cve-2019-0708-exploitation-spotted-in-the-wild/?source=post_page----bd6ee6e599a6-----)
- BlueKeep exploitation activity seen in the wild  
<https://doublepulsar.com/bluekeep-exploitation-activity-seen-in-the-wild-bd6ee6e599a6>
- Data Insights on the BlueKeep Vulnerability  
[https://www.bitsight.com/blog/data-insights-on-bluekeep-vulnerability?utm\\_campaign=public-relations&utm\\_source=public-relations&utm\\_medium=referral](https://www.bitsight.com/blog/data-insights-on-bluekeep-vulnerability?utm_campaign=public-relations&utm_source=public-relations&utm_medium=referral)



- Avast Business report may help explain why users are resisting Microsoft's BlueKeep patch  
<https://blog.avast.com/avast-report-bluekeep-patch>
- Will BlueKeep Become WannaCry 2.0?  
<https://www.bitsight.com/blog/will-bluekeep-become-wannacry-2.0>
- The much-publicized BlueKeep threat has finally emerged – why should you care?  
<https://blog.avast.com/what-is-bluekeep>
- Debunking The BlueKeep Exploit Hype – What You Should Know  
<https://businessinsights.bitdefender.com/debunking-the-bluekeep-exploit-hype-what-you-should-know>
- Remove syscall hook from BlueKeep payload  
<https://github.com/rapid7/metasploit-framework/pull/12553>





**Questions**





## Upcoming Briefs

- Incident Response
- Emotet Update



## 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](mailto:HC3@HHS.GOV).

## Requests for Information

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



*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](mailto: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**