LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HEALTH SECTOR CYBERSECURITY COORDINATION CENTER

HC3

Distributed Denial of Service (DDoS) Attacks

07/16/2020

Report #: 202007161030

Agenda

- Attack Overview
- Example
- Motives
- Technical Information
- Mitigation Strategies

Slides Key:

👤	Non-Technical: managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

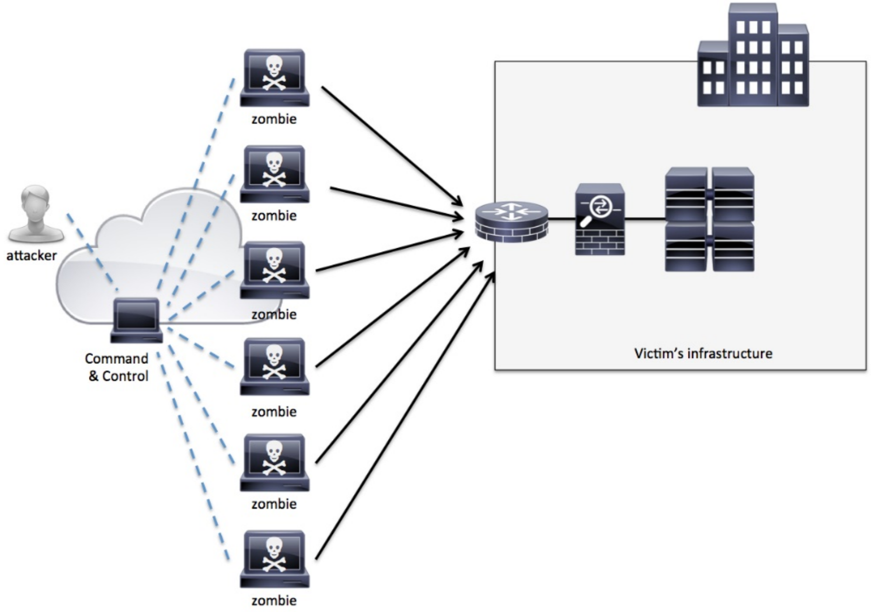
Attack Overview

Defining the Term:

Distributed:
The attack traffic originates from many sources, not from a single one that could easily be blocked. Frequently leverages botnets.

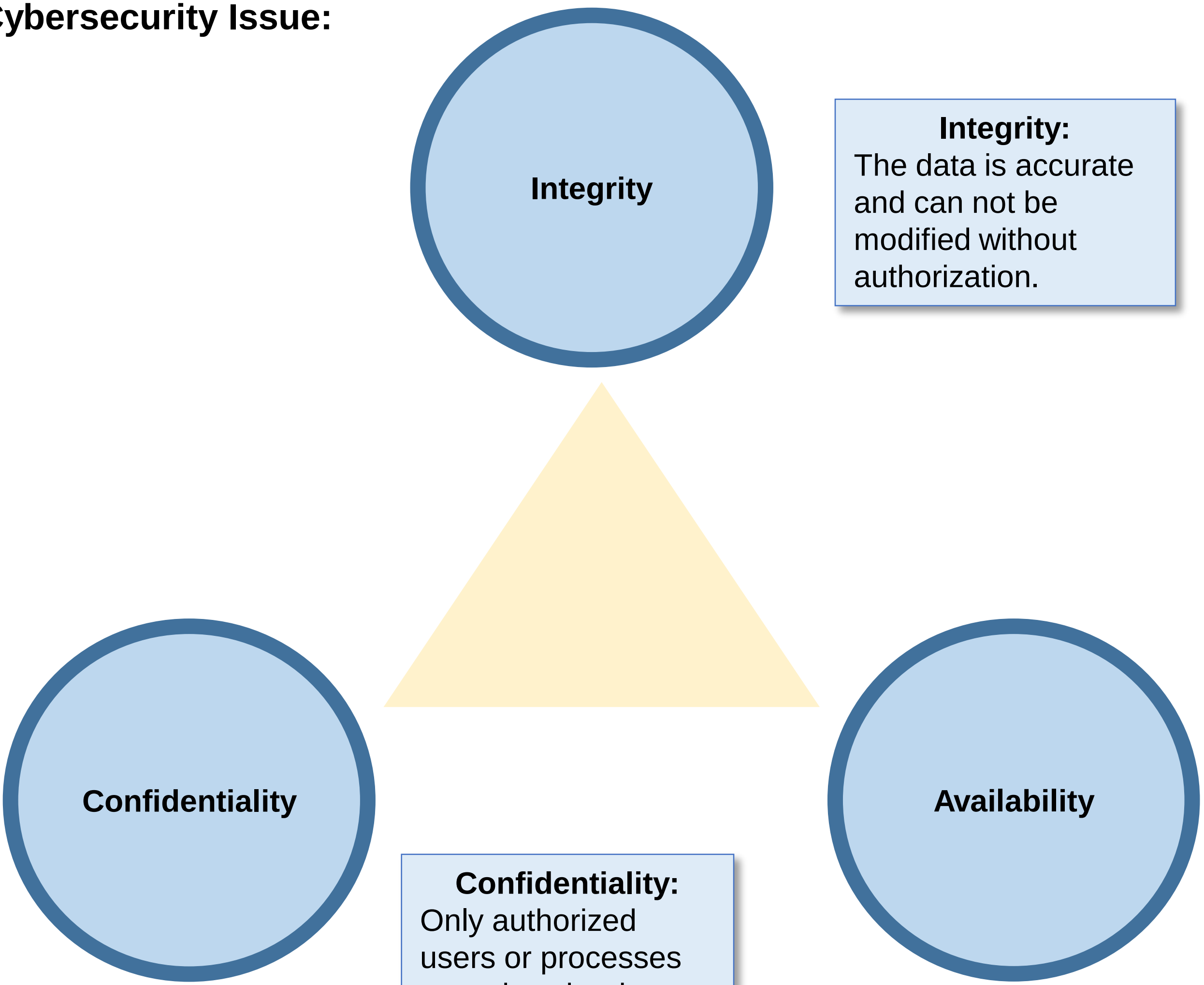
Denial:
The attack prevents the user access or degrades the access beyond acceptable limits.

Service:
The attack could be against any layer, or combination of layers, of the system, ranging from initial access to the system to the functionality of the application.



Attack Overview

Inherent Cybersecurity Issue:



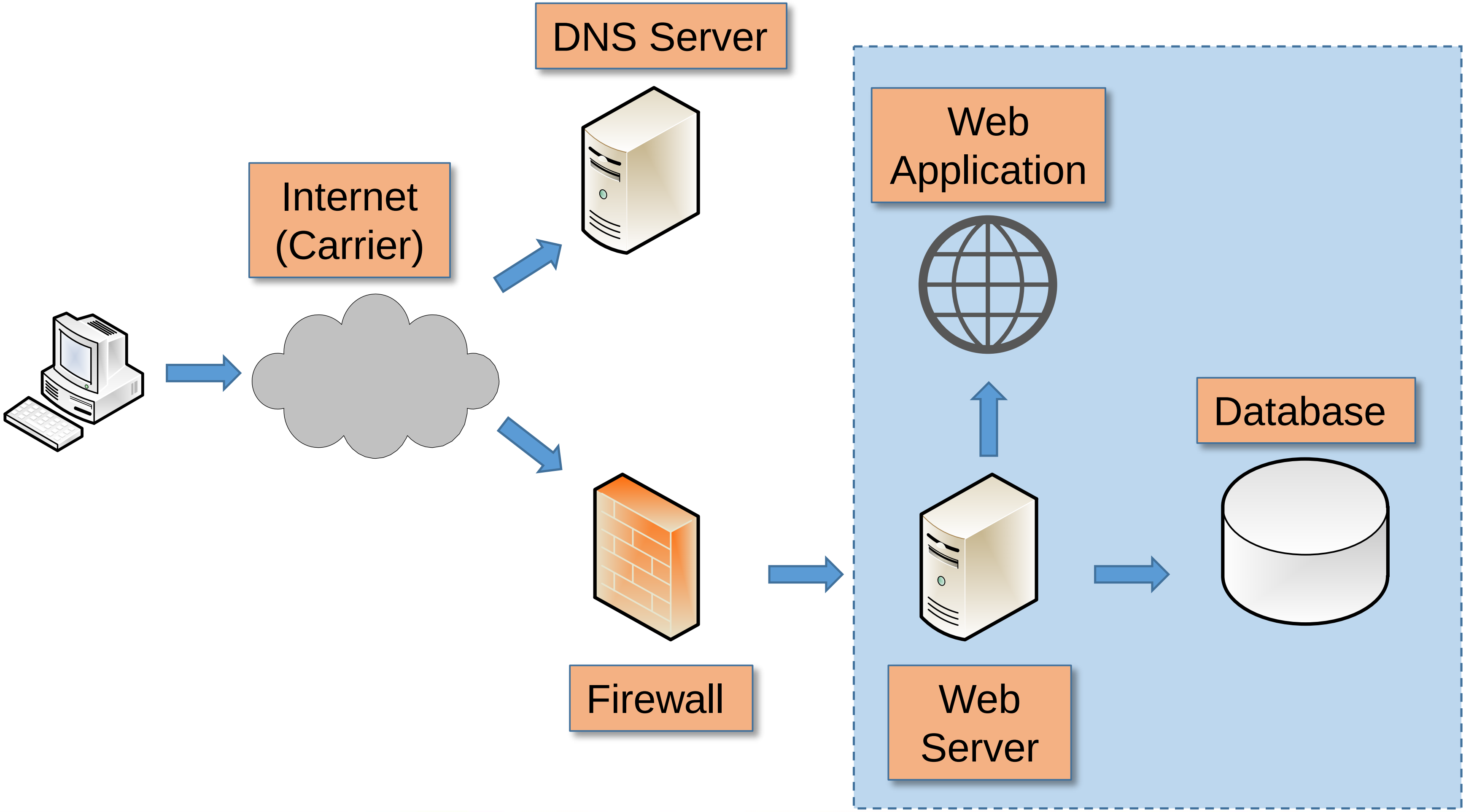
Integrity:
The data is accurate and can not be modified without authorization.

Confidentiality:
Only authorized users or processes may view the data.

Availability:
The data is available to authorized users in a timely manner when needed.

Attack Overview

Website Attack Points:



Example

2014 Hospital Attack

- “Anonymous” hacktivist group
- Attack against a children’s hospital
- In response to disagreement concerning a custody decision
- Not financially motivated

We are Anonymous, We are the Legion, We do not Forgive, We do not Forget
Expect Us

Motives

- Hacktivism
- Extortion
- Commercial
- Technical Challenge

Motives - Hacktivism

- Political or ideological agenda
- Usually not financially motivated
- Groups claim responsibility for attacks

Motives - Extortion

- “Pay or be knocked offline”
- Recent telework surge may increase impact
- Cryptocurrency frequently used
- Different from ransomware
- Extortion message may be from direct contact or from the traffic itself

Motives - Commercial

- DDoS attacks against competitors
- Attacks carried out for hire
- Could be used to knock competitors offline on busy shopping days, such as “Cyber Monday”

Motives - Technical Challenge

- The challenge of taking down a particular target
- DDoS due to boredom
- No financial gain or message to convey
- Could be used for bragging rights
- Could be used to “educate” entities about their flaws

Technical Information

- DNS Reflection
- Infrastructure Overload
- Application Layer Attacks

Technical Information – DNS Reflection

- Attack queries a 3rd party DNS server
- Attackers spoof the source IP address
- The attack uses DNS queries that generate large responses

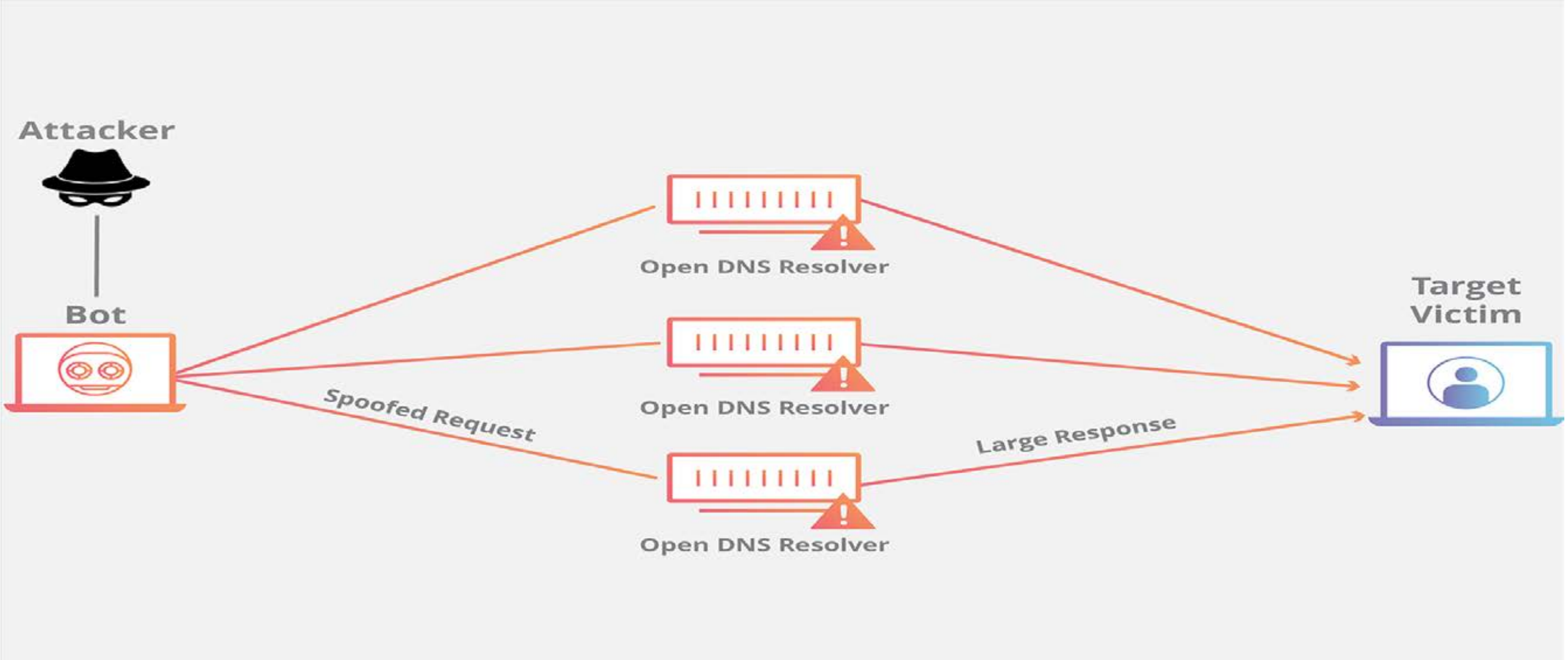
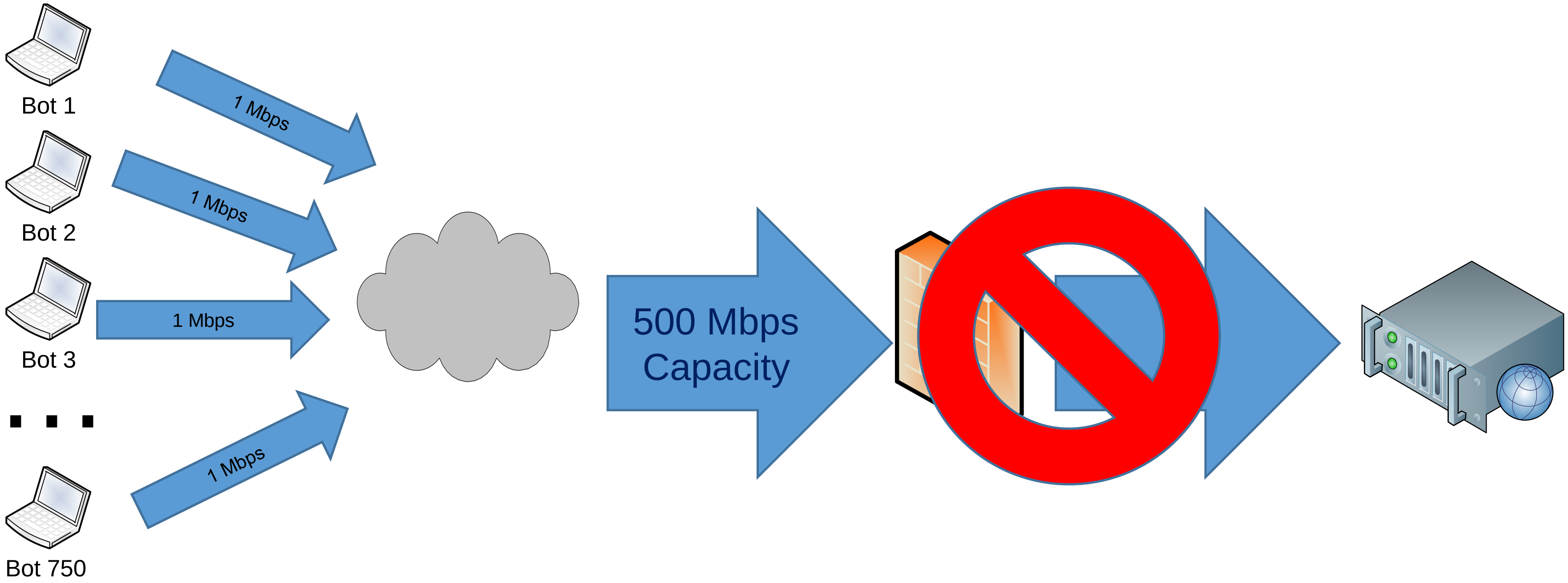


Image courtesy of CloudFlare

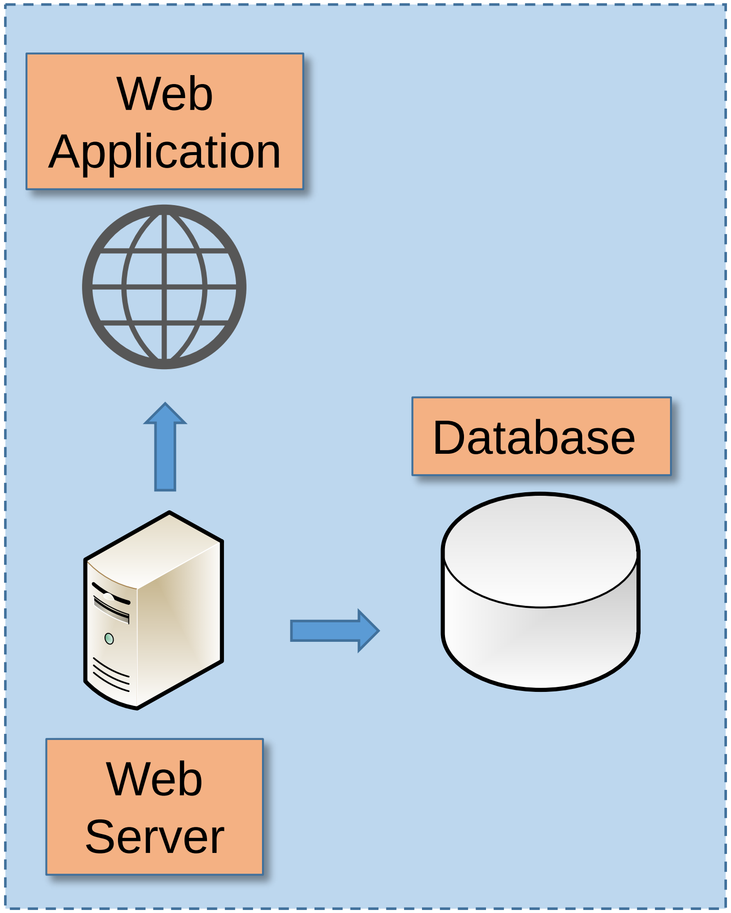
Technical Information – Infrastructure Overload

- Victims have a limit to bandwidth
- Attackers send traffic at a greater rate



Technical Information – Application Layer Attacks

- Processing web page requests takes up computing and memory resources
- Layer 7 Component Stack:
  - Web Server Software
  - Web Application
  - Database
- Rate of requests could overload the web software
- Number of requests could overload the web software
- Large database searches could overload the database connection



Mitigation Strategies

- Strategies, **NOT RECOMMENDATIONS**:

- Small amount of sources: block IPs or IP ranges
  - For DNS reflection, this may block legitimate IPs!
  - For cloud services, this may block legitimate IPs!
  - Attackers may change source IPs

- Some carriers (ISPs) offer DDoS mitigation services

- Increase computing power or bandwidth
  - Attackers could then increase rate of attack

- Change messaging
  - No guarantee this will prevent attack!

- Pay extortion fee
  - No guarantee this will prevent attack!

Reference Materials

References

- https://www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/
- https://sucuri.net/guides/what-is-a-ddos-attack/
- https://www.zdnet.com/article/ransomware-and-ddos-attacks-cybercrooks-are-stepping-up-their-activities-in-the-midst-of-coronavirus/
- https://krebsonsecurity.com/2018/03/powerful-new-ddos-method-adds-extortion/

Questions

Questions

Upcoming Briefs

- Dark Web and Cybercrime Deep Dive

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