Data Exfiltration Trends in Healthcare

March 9, 2023

TLP: CLEAR, ID# *202303091300*

Agenda

- Background on Data Exfiltration
- Recent Trends in Healthcare
- Deep Dive into Data Exfiltration
  - Information Stealers
  - Ransomware & Custom Data Exfiltration Tools
  - Data Exfiltration and Extortion
  - Cyber Espionage
  - Cloud and Insider Threats
- Mitigations

Slides Key:

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

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

Background

What is Data Exfiltration?

- Relates to when malware and/or a malicious actor carries out an *unauthorized* data transfer from a device.
- Data exfiltration is one of the final stages of the cyber kill-chain and the most important objective of advanced persistent threats (APTs).
- Ransomware is most often associated with data exfiltration, file encryption and extortion.
- Data exfiltration = security breach!

What Type of Data is Targeted?

- Credentials
- Email conversations
- Sensitive corporate data
- Financial information
- Social security numbers
- Medical research
- **Protected Health Information (PHI)** including medical histories, laboratory results, physical records, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care.

How is Data Exfiltrated?

- There are numerous techniques threat actors may leverage to perform data exfiltration.
- These may be divided into multiple high-level categories:
  1) A threat actor **already has physical access** to the target system.
  2) A threat actor **gains physical access** to a target server.
  3) A threat actor **already has remote admin access** to the target.
  4) A threat actor **gains remote admin access** to the target system.

Why Data Exfiltration?

1. Cyber Espionage
   - Intelligence Collection
2. Financial Gain
   - Monetization of Stolen Data
   - Extortion
3. Insider Threat
   - Competitive Intelligence
   - Blackmail
   - Unintentional Data Leak

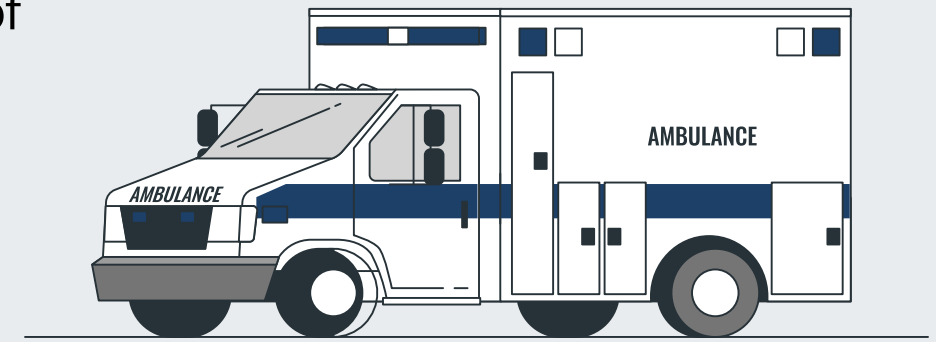
The Rise of Data Exfiltration

- Data exfiltration is rapidly becoming more prevalent. In 2022, incidents at Nvidia, Microsoft, and several other companies highlighted how big of a problem it has become – and how, for some organizations, it may be a threat that's even bigger than ransomware.
- While the number of total third-party breaches slightly dipped in 2022, the attacks impacted nearly twice as many victims, wreaking havoc on the healthcare industry more than any other sector.
- Important to also highlight the frequent news headlines of unauthorized data collection and sharing of private user data by legitimate organizations.

Data Exfiltration in Healthcare

Increase in Patient Records Breached

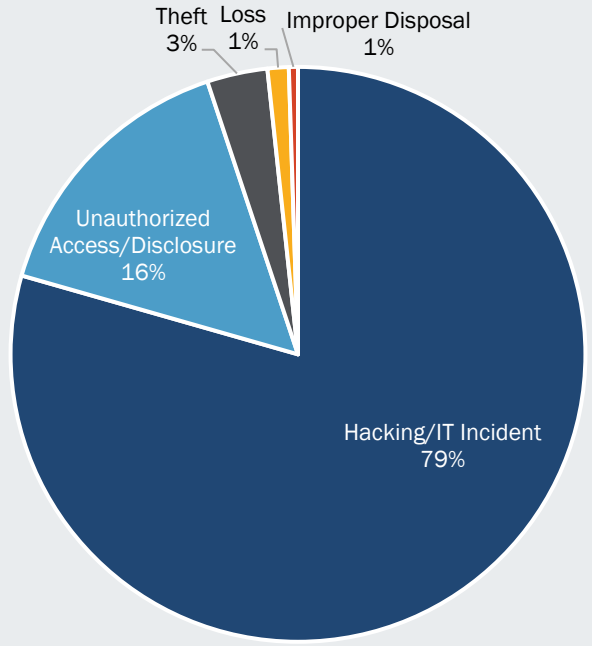
- Based on an analysis of breach data reported by healthcare organizations to the HHS in the second half of 2022, victims of healthcare data breaches had 28.5 million records exposed, which was an increase from 21.1 million in 2019.
- Healthcare data breaches had the greatest impact in the second quarter of 2022 compared to previous years.
- In 2022, 588 breaches were reported to the HHS Office of Civil Rights (OCR), affecting 44,665,819 patients in total.



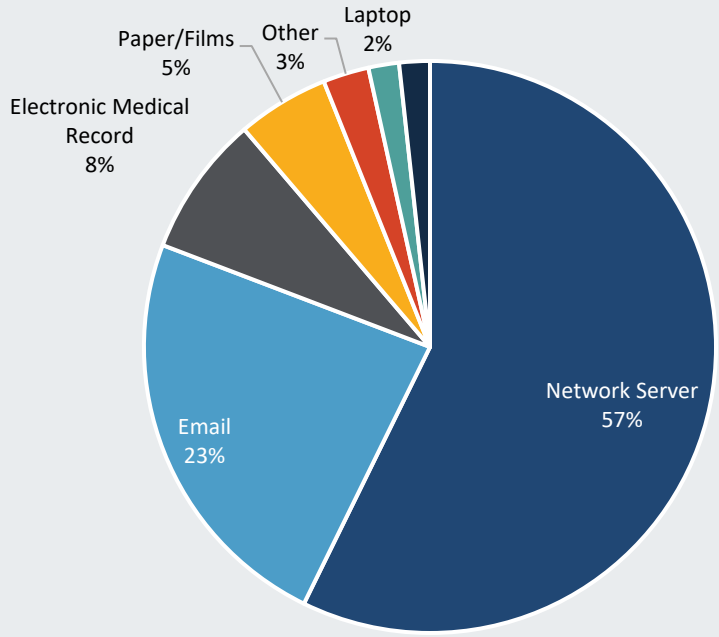
OCR Breach Report Statistics for 2022

The charts below show the types of breaches and the locations of breached information for incidents reported to the HHS Office of Civil Rights (OCR) in 2022:

Type of Breach Reported to OCR (2022)



Location of Breached Info Reported to OCR (2022)



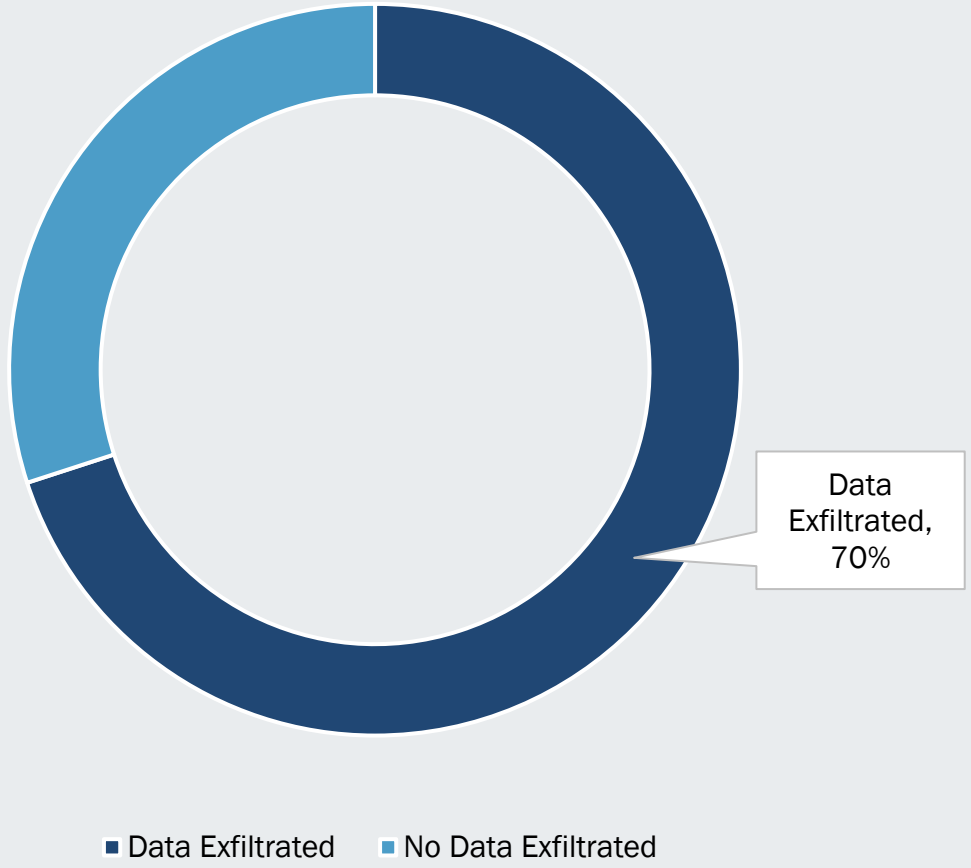
Ransomware in Healthcare (2022)

- Healthcare and Public Health (HPH) organizations bore the brunt of ransomware attacks on critical infrastructure sectors launched last year, according to the FBI's Internet Complaint Center (IC3).
- A recent report by Emsisoft found that ransomware attacks in 2022 impacted more than 200 large organizations in the U.S. in the government, educational, and healthcare verticals, including 24 healthcare providers operating 289 hospitals.
- Data collected from publicly available reports, disclosure statements, leaks on the dark web, and third-party intelligence show that hackers stole data in more than half of these ransomware attacks.

Ransomware in Healthcare (cont.)

Based on available open-source data, the ransomware threat in the U.S. struck 24 healthcare providers. Despite the small number, the impact is much more significant, potentially affecting as many as 289 hospitals. The most notable healthcare entity attacked runs more than 140 hospitals, exposing the data of 623,000 patients. Emsisoft researchers say that hackers stole files including Protected Health Information (PHI) in 17 incidents, amounting to nearly 70% of those incidents affecting healthcare providers in the U.S.

Healthcare Ransomware Incidents in 2022 with Data Exfiltration (Source: Emsisoft)



LockBit, BlackCat, and Hive Most Observed

- The FBI's Internet Complaint Center last year (2022) received 870 complaints that indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack.
- The top strain of ransomware observed in those 870 incidents affecting critical infrastructure (including healthcare) reported to the FBI was LockBit, followed by ALPHV/BlackCat and Hive.
- Two caveats are that many more attacks have hit organizations outside critical infrastructure, and that the findings do not factor in unknown victims.

Image source: IC3

Healthcare Data Breaches Still Higher Than Pre-Pandemic Levels

- While the number of data breaches affecting healthcare providers declined in the second half of 2022, consistent with a downward trend over the past two years, breach totals are still higher than pre-pandemic levels.
- Breaches are affecting more individuals and hackers are shifting tactics to attack weak links in the healthcare system supply chain, most notably attacking EHR systems, according to Critical Insight.
- Healthcare data breaches had the greatest impact in the second quarter of 2022 compared to previous years, with a 35% increase in the number of patient records affected.

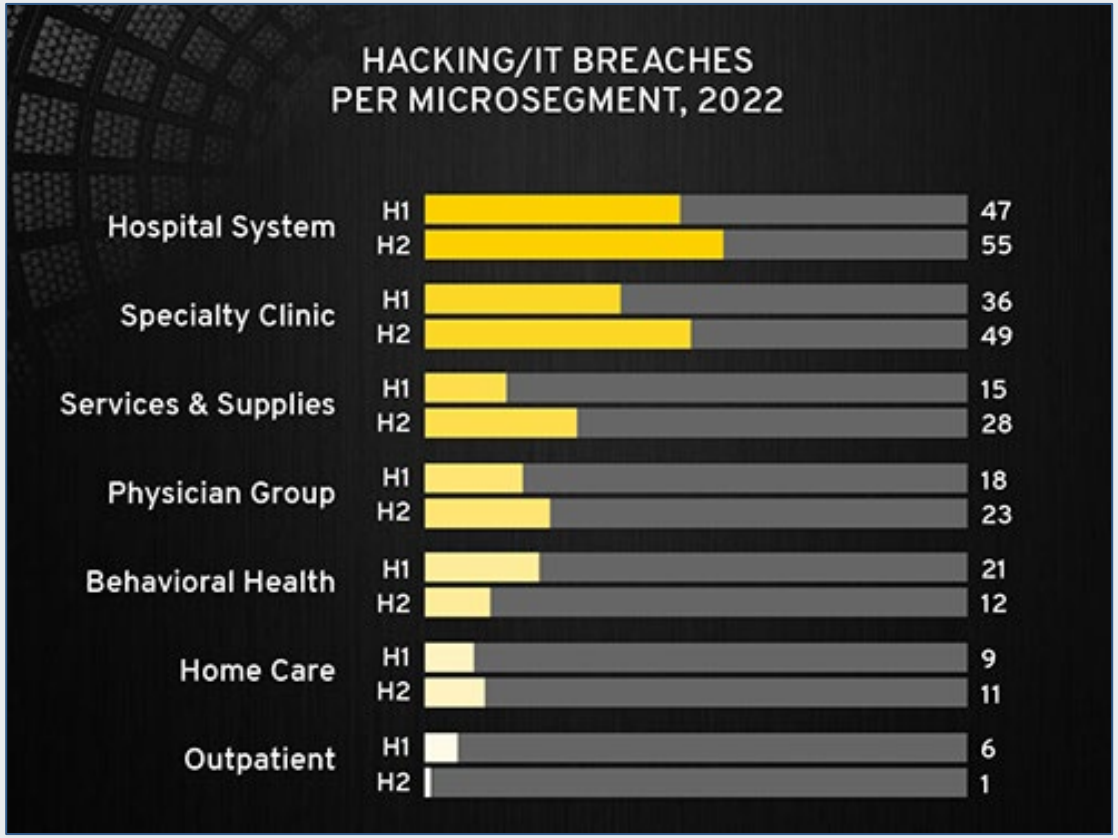


Image Source: Critical Insight

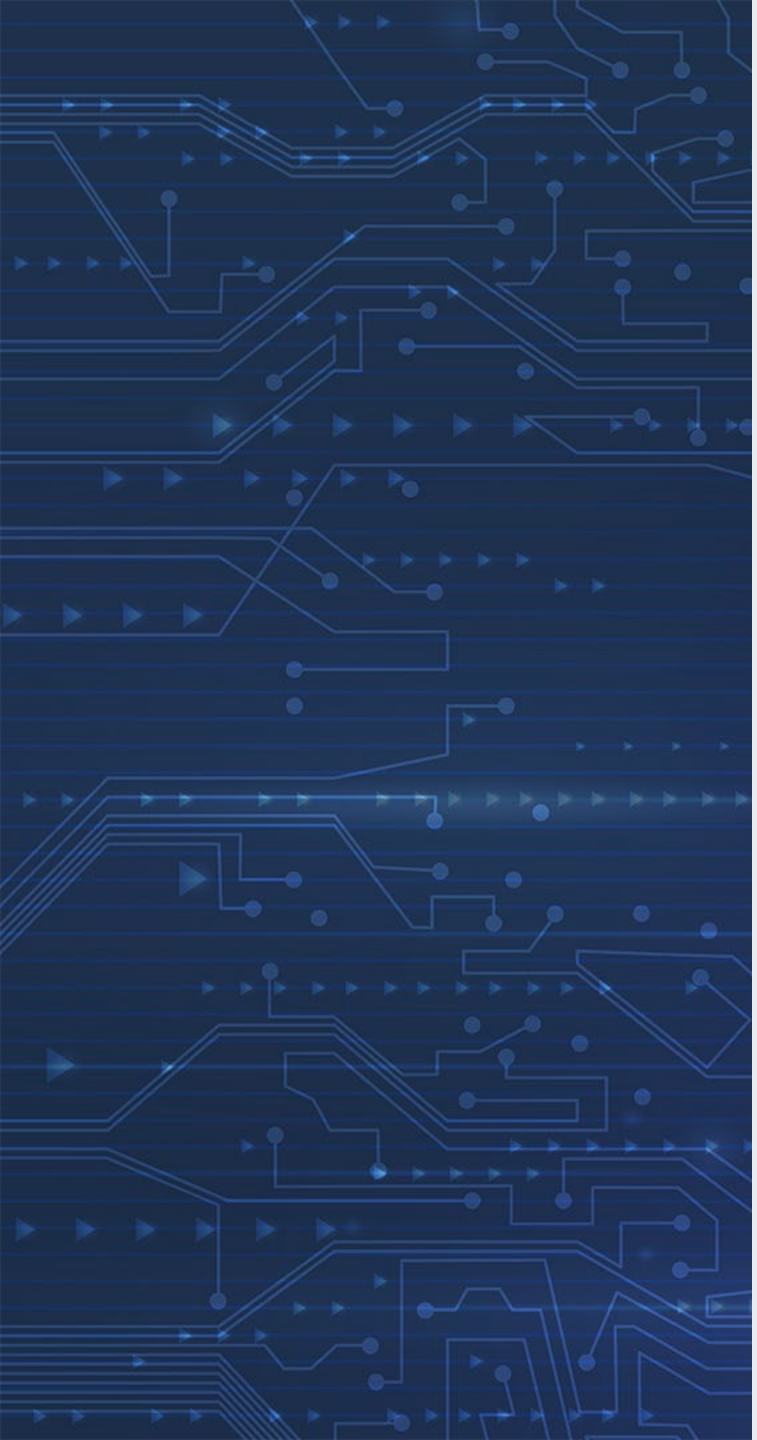
Example: Data Exfiltration at a U.S. Hospital

- On December 29, 2022, an Arkansas-based hospital published a news release stating that the hospital had discovered suspicious activity on its network earlier that month, and that an unknown actor alleged they stole data from the hospital's network. The ongoing investigation found an unknown actor had access to the hospital's network from mid-November to early December and may have stolen certain files. The hospital is still reviewing the at-risk files to identify affected patients and employees. Data potentially breached during the incident includes names, contact information, birth dates, and Social Security numbers. Employees may also have had their direct deposit bank account information breached.

HIPAA Breach Notification Rule

- HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414
- “A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.”
- Notification must be provided to affected individuals, the Secretary, and, in certain circumstances, to the media.
- Breaches affecting 500 or more individuals must notify the Secretary no later than 60 days following a breach.
- Financial consequences of violating HIPAA depend on the level of negligence, and fines for a HIPAA violation can be applied even if no breach of PHI has occurred.
- More info: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Image source: Compliancy Group

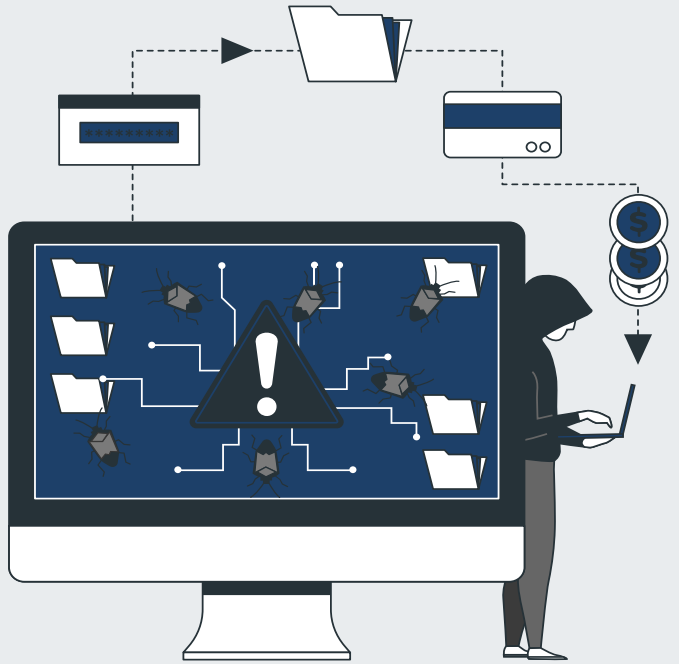


Deep Dive Into Data Exfiltration

Numerous Threats Involve Data Exfiltration

There are numerous cyber threats that involve data exfiltration. These cover various threat actors and Tactics, Techniques, and Procedures (TTPs). This section on “Deep Dive Into Data Exfiltration” will cover the following topics:

- Information Stealers
- Ransomware
- Custom Data Exfiltration Tools and Methods
- Cyber Espionage for Intelligence Collection
- Cloud Threats
- Insider Threats



Cyber Kill Chain – Data Exfiltration

Stage 7: Actions on Objectives

- After cybercriminals have developed cyberweapons, installed them onto a target's network, and taken control of their target's network, they begin the final stage of the Cyber Kill Chain: carrying out their cyberattack objectives. While cybercriminals' objectives vary depending on the type of cyberattack, some examples include weaponizing a botnet to interrupt services with a Distributed Denial of Service (DDoS) attack, distributing malware to **steal sensitive data** from a target organization, and using ransomware as a cyber extortion tool.

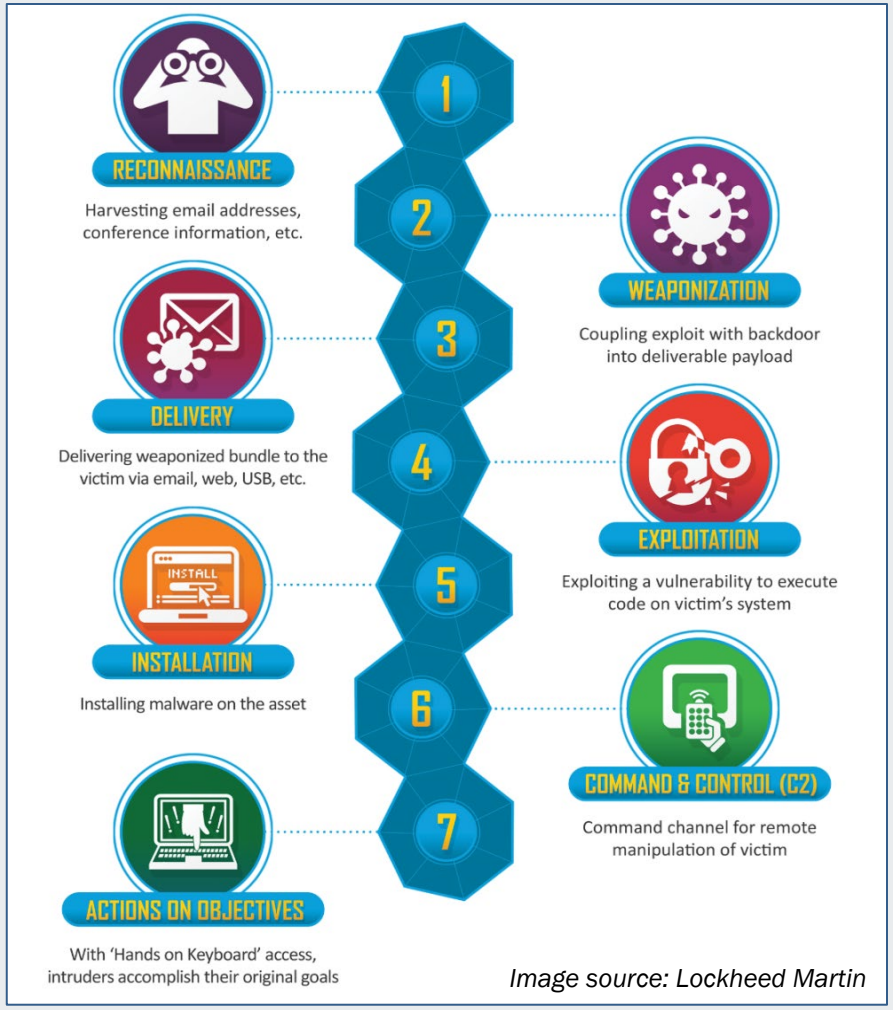
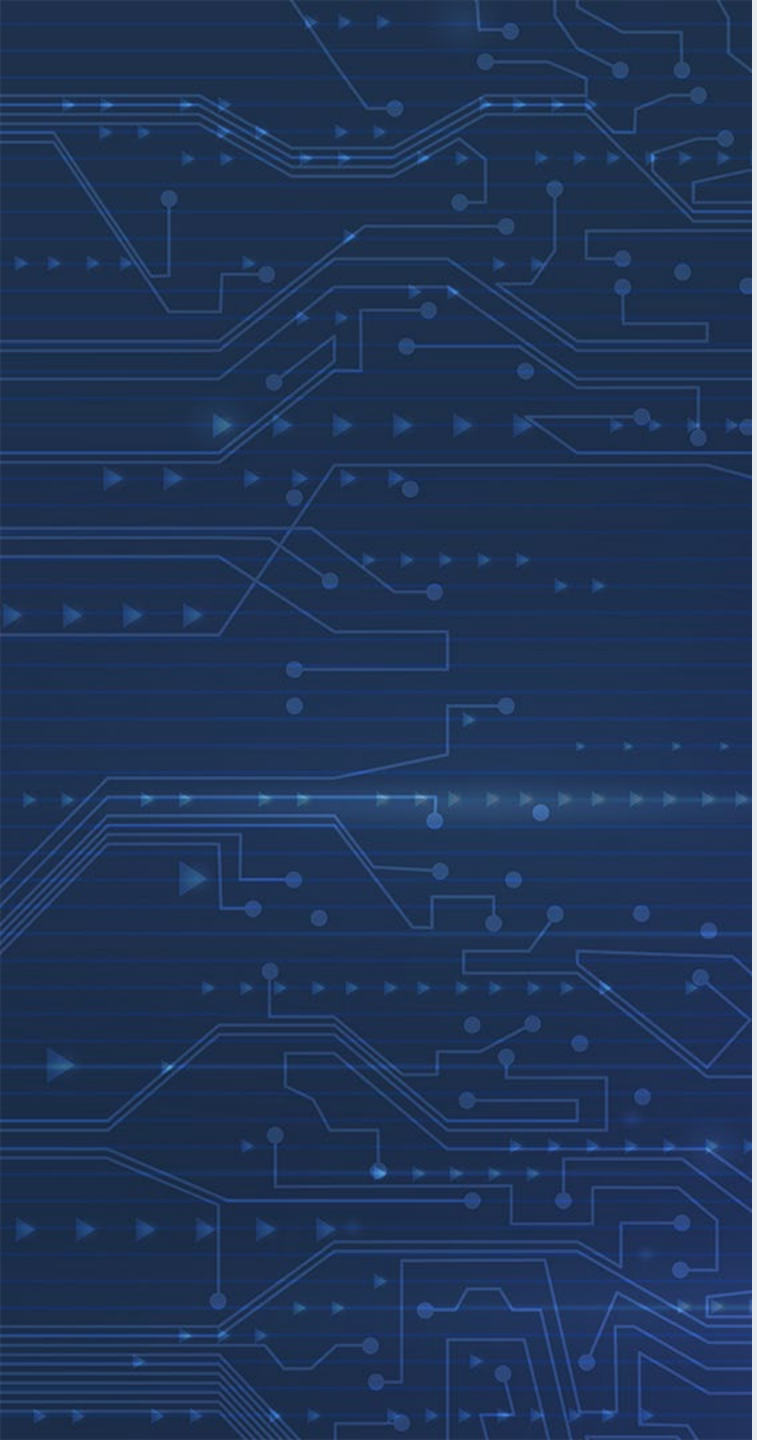


Image source: Lockheed Martin



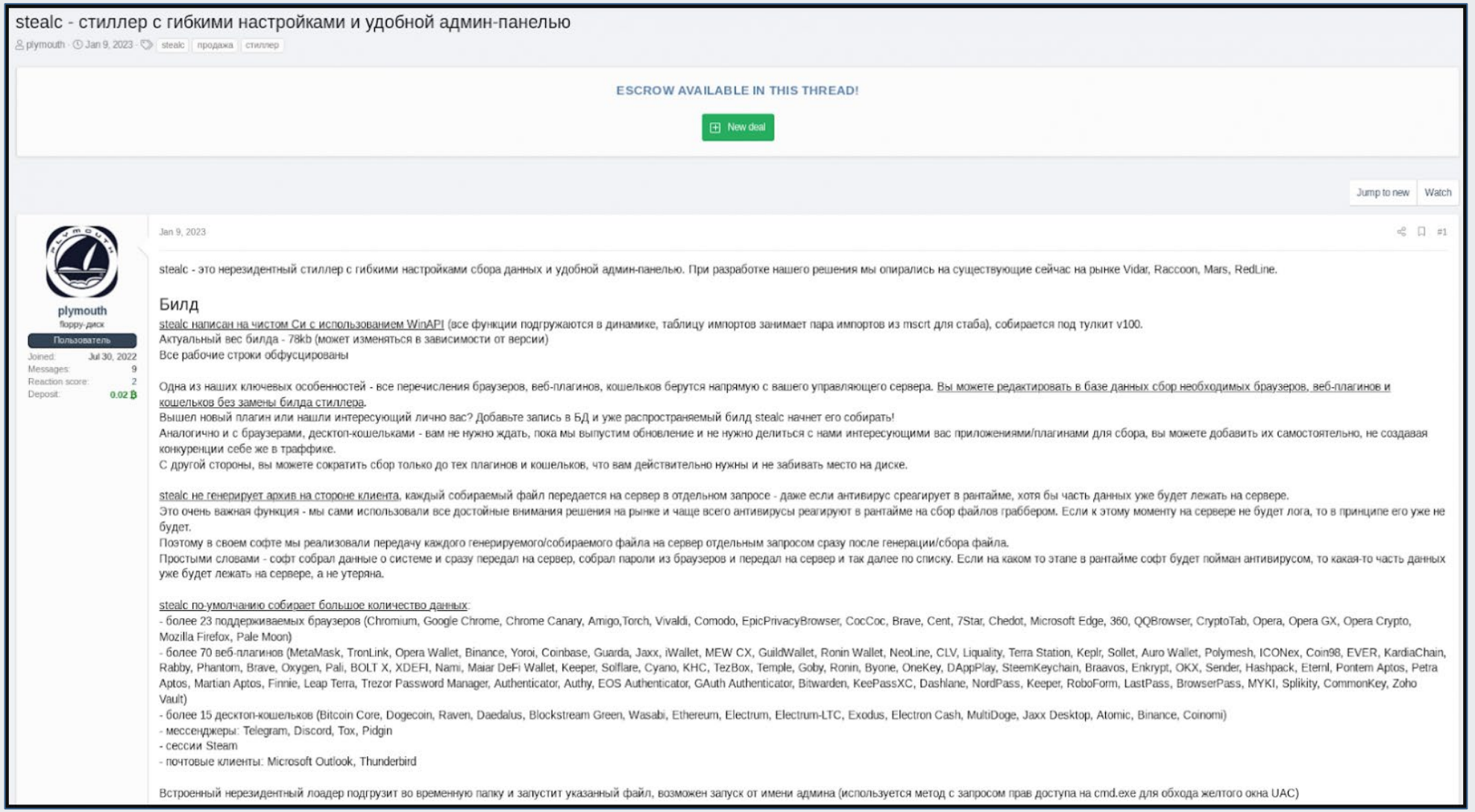
Information Stealers

Information Stealers Leveraged for Initial Access

Information stealers are designed to steal credentials and other data from a computer and can be leveraged to find further high-value data to steal from an organization with minimal technical skillset.

Popularity spiked towards the end of 2022 for information stealers on the dark web, including:

- **Mars**: Extracts data from most popular web browsers, including 2FA plugins and multiple cryptocurrency extensions and wallets.
- **Raccoon**: Targets users' browsers and crypto wallets (cookies, login details, credit cards).
- **Redline**: Previously leveraged by LAPSUS$ group to obtain passwords and session tokens.
- **Vidar**: Over 1,300 fake AnyDesk sites push Vidar info-stealing malware in January 2023.
- **StealC**: New stealer similar to Vidar, Raccoon, Mars, and Redline active in February 2023 with customizable file-grabbing and loader capabilities.



stealc - стиллер с гибкими настройками и удобной админ-панелью

plymouth · Jan 9, 2023 · stealc · продажа · стиллер

ESCROW AVAILABLE IN THIS THREAD!

New deal

Jump to new · Watch

plymouth
floppy-диск
Пользователь
Joined: Jul 30, 2022
Messages: 9
Reaction score: 2
Deposit: 0.02 Ƀ

Jan 9, 2023 · #1

stealc - это нерезидентный стиллер с гибкими настройками сбора данных и удобной админ-панелью. При разработке нашего решения мы опирались на существующие сейчас на рынке Vidar, Raccoon, Mars, RedLine.

Билд

stealc написан на чистом Си с использованием WinAPI (все функции подгружаются в динамике, таблицу импортов занимает пара импортов из mscrt для стаба), собирается под тулкит v100.
Актуальный вес билда - 78kb (может изменяться в зависимости от версии)
Все рабочие строки обфусцированы

Одна из наших ключевых особенностей - все перечисления браузеров, веб-плагинов, кошельков берутся напрямую с вашего управляющего сервера. Вы можете редактировать в базе данных сбор необходимых браузеров, веб-плагинов и кошельков без замены билда стиллера.
Вышел новый плагин или нашли интересующий лично вас? Добавьте запись в БД и уже распространяемый билд stealc начнет его собирать!
Аналогично и с браузерами, десктоп-кошельками - вам не нужно ждать, пока мы выпустим обновление и не нужно делиться с нами интересующими вас приложениями/плагинами для сбора, вы можете добавить их самостоятельно, не создавая конкуренции себе же в траффике.
С другой стороны, вы можете сократить сбор только до тех плагинов и кошельков, что вам действительно нужны и не забивать место на диске.

stealc не генерирует архив на стороне клиента, каждый собираемый файл передается на сервер в отдельном запросе - даже если антивирус среагирует в рантайме, хотя бы часть данных уже будет лежать на сервере.
Это очень важная функция - мы сами использовали все достойные внимания решения на рынке и чаще всего антивирусы реагируют в рантайме на сбор файлов граббером. Если к этому моменту на сервере не будет лога, то в принципе его уже не будет.
Поэтому в своем софте мы реализовали передачу каждого генерируемого/собираемого файла на сервер отдельным запросом сразу после генерации/сбора файла.
Простыми словами - софт собрал данные о системе и сразу передал на сервер, собрал пароли из браузеров и передал на сервер и так далее по списку. Если на каком то этапе в рантайме софт будет пойман антивирусом, то какая-то часть данных уже будет лежать на сервере, а не утеряна.

stealc по-умолчанию собирает большое количество данных:
- более 23 поддерживаемых браузеров (Chromium, Google Chrome, Chrome Canary, Amigo,Torch, Vivaldi, Comodo, EpicPrivacyBrowser, CocCoc, Brave, Cent, 7Star, Chedot, Microsoft Edge, 360, QQBrowser, CryptoTab, Opera, Opera GX, Opera Crypto, Mozilla Firefox, Pale Moon)
- более 70 веб-плагинов (MetaMask, TronLink, Opera Wallet, Binance, Yoroi, Coinbase, Guarda, Jaxx, iWallet, MEW CX, GuildWallet, Ronin Wallet, NeoLine, CLV, Liquality, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh, ICONex, Coin98, EVER, KardiaChain, Rabby, Phantom, Brave, Oxygen, Pali, BOLT X, XDEFI, Nami, Maiar DeFi Wallet, Keeper, Solflare, Cyano, KHC, TezBox, Temple, Goby, Ronin, Byone, OneKey, DAppPlay, SteemKeychain, Braavos, Enkrypt, OKX, Sender, Hashpack, Eternl, Pontem Aptos, Petra Aptos, Martian Aptos, Finnie, Leap Terra, Trezor Password Manager, Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Bitwarden, KeePassXC, Dashlane, NordPass, Keeper, RoboForm, LastPass, BrowserPass, MYKI, Splikity, CommonKey, Zoho Vault)
- более 15 десктоп-кошельков (Bitcoin Core, Dogecoin, Raven, Daedalus, Blockstream Green, Wasabi, Ethereum, Electrum, Electrum-LTC, Exodus, Electron Cash, MultiDoge, Jaxx Desktop, Atomic, Binance, Coinomi)
- мессенджеры: Telegram, Discord, Tox, Pidgin
- сессии Steam
- почтовые клиенты: Microsoft Outlook, Thunderbird

Встроенный нерезидентный лоадер подгрузит во временную папку и запустит указанный файл, возможен запуск от имени админа (используется метод с запросом прав доступа на cmd.exe для обхода желтого окна UAC)

Image source: SEKOIA

Ransomware & Custom Data Exfiltration Tools

Ransomware & Custom Data Exfiltration Tools

- In 2022, HC3 observed multiple RaaS groups upgrade their data exfiltration tools in attempts to improve the capabilities of the ransomware and evade detection.
- In addition to using ubiquitous tools such as Rclone, MegaSync, and FileZilla, ransomware and extortion groups have crafted custom exfiltration tools tailored to their operations.
- The continued development and use of these custom tools is a testament to their success, often simplifying and accelerating data exfiltration.
- Some examples include Exbyte (BlackByte), Exmatter (BlackMatter), StealBit (LockBit), and Ryuk Stealer (Ryuk).

Case Study 1

Hive Leverages Rclone and Mega.nz to Exfiltrate Data

Hive: Transfer Data to Cloud Account (T1537)

- Hive actors have previously exfiltrated data likely using a combination of Rclone and the cloud storage service Mega.nz.
- Rclone is an open-source, multi-threaded, command-line computer program (written in Go) to manage or migrate content on cloud and other high latency storage. Its capabilities include sync, transfer, crypt, cache, union, compress and mount. The Rclone website lists supported backends which include S3 and Google Drive.
- Rclone has been used in a number of ransomware campaigns, including those associated with the Conti and DarkSide Ransomware-as-a-Service operations.

Case Study 2

October 2022: Exbyte Data Exfiltration Tool Used by BlackByte Ransomware

Exbyte: Custom Data Exfiltration Tool Used by BlackByte Ransomware

- The Exbyte exfiltration tool is written in Go and designed to upload stolen files from compromised Windows devices to the Mega cloud storage service.
- The BlackByte ransomware modifies firewall settings to enable linked connections to support data exfiltration.
- Upon execution, the tool performs anti-analysis checks to determine if it is running in a sandboxed environment and checks for debuggers and anti-virus processes.
- If tests are clean, Exbyte enumerates all document files on target system and uploads them to a newly-created folder on Mega using hardcoded credentials.
- Full report with publicly available Yara Rules to detect BlackByte Exfiltration can be found here.

Case Study 3

September 2022: BlackCat/ALPHV Ransomware Data Exfiltration Tool Gets An Upgrade While Information-Stealing Malware Steals Credentials Stored by Cloud Backup Software

Exmatter: Custom Data Exfiltration Tool Used by Noberus (aka BlackCat, ALPHV) Ransomware

- Ransomware variant linked to FIN7 attacks.
- Heavily updated version of Exmatter data exfiltration tool observed in August 2022 ransomware attacks.
- Designed to optimize its operation and expedite exfiltration of a sufficient volume of high-value data in as short a time as possible.
- Updated version limits the number of file types it attempts to exfiltrate to increase speed.
- Adds FTP as an exfiltration option in addition to SFTP and WebDAV, among other features.
- Use of Eamfo information-stealing malware designed to steal credentials stored by Veeam backup software.
- Full report with IOCs can be found here.

Case Study 4

December 2021: LockBit Ransomware's StealBit Data Exfiltration Tool

StealBit: LockBit Ransomware's Data Exfiltration Tool

- LockBit group provides StealBit to affiliates as part of the group's ransomware affiliate program.
- Targets all files except specific, blacklisted items. Avoids common system files and programs.
- Leverages RC4 and XOR for obfuscation and data encryption.
- Uses HTTP PUT method for exfiltration.
- C2 infrastructure identified during analysis by Accenture was hosted by nine (9) unique hosting services or ASNs.
- Full report with TTPs and IOCs can be found here.

Comparative Analysis of Custom Data Exfiltration Tools

- Based on comparative analysis of the tools, while data exfiltration is the consistent operational objective, the path to achieve that objective and the supporting functionality of each exfiltration tool varies slightly based on configuration, implementation details, and the operational environment. These variations can create challenges for network defenders.
- ExMatter adopts a more targeted approach to file discovery and exfiltration, while StealBit casts a wider net, especially for newer versions with geolocation restrictions removed.
- StealBit uses the HTTP PUT method for exfiltration, while ExMatter uses SFTP, SOCKS5, or WebDAV for exfiltration.
- C2 infrastructure supporting StealBit identified during analysis by Accenture was distributed across nearly ten (10) unique hosting services, while 85% of C2 infrastructure connected to ExMatter was hosted by a single ASN.

Ransomware Shift to Data Exfiltration and Extortion

Ransomware Shift to Data Exfiltration and Extortion

- 2022 saw a 20% increase in the number of adversaries conducting data theft and extortion campaigns.
- Over the past year, HC3 has observed new threat actors join the scene, engaged in pure data exfiltration and extortion without encrypting files.
- Recent examples of threat actors engaged in this activity include the Donut Leaks, Karakurt, and the Lapsus$ data extortion groups.

Threat Actors Conducting Data Exfiltration and Extortion

Donut Leaks (aka D0nut)

- First surfaced in August 2022, launching double-extortion attacks on enterprises.
- In November 2022, the 'Donut Leaks' data extortion group claimed the compromise of a North Dakota-based healthcare entity, as well as an Illinois-based medical device manufacturer in September 2022.
- The threat actor emails URLs of the Tor site to the victim's business partners and employees.
- Multiple ransomware groups, including Hive and Ragnar Locker, have also claimed victims that appeared on the Donut Leaks blog.
- The group was also confirmed to be using its own customized ransomware in November 2022.

Threat Actors Conducting Data Exfiltration and Extortion (Part 2)

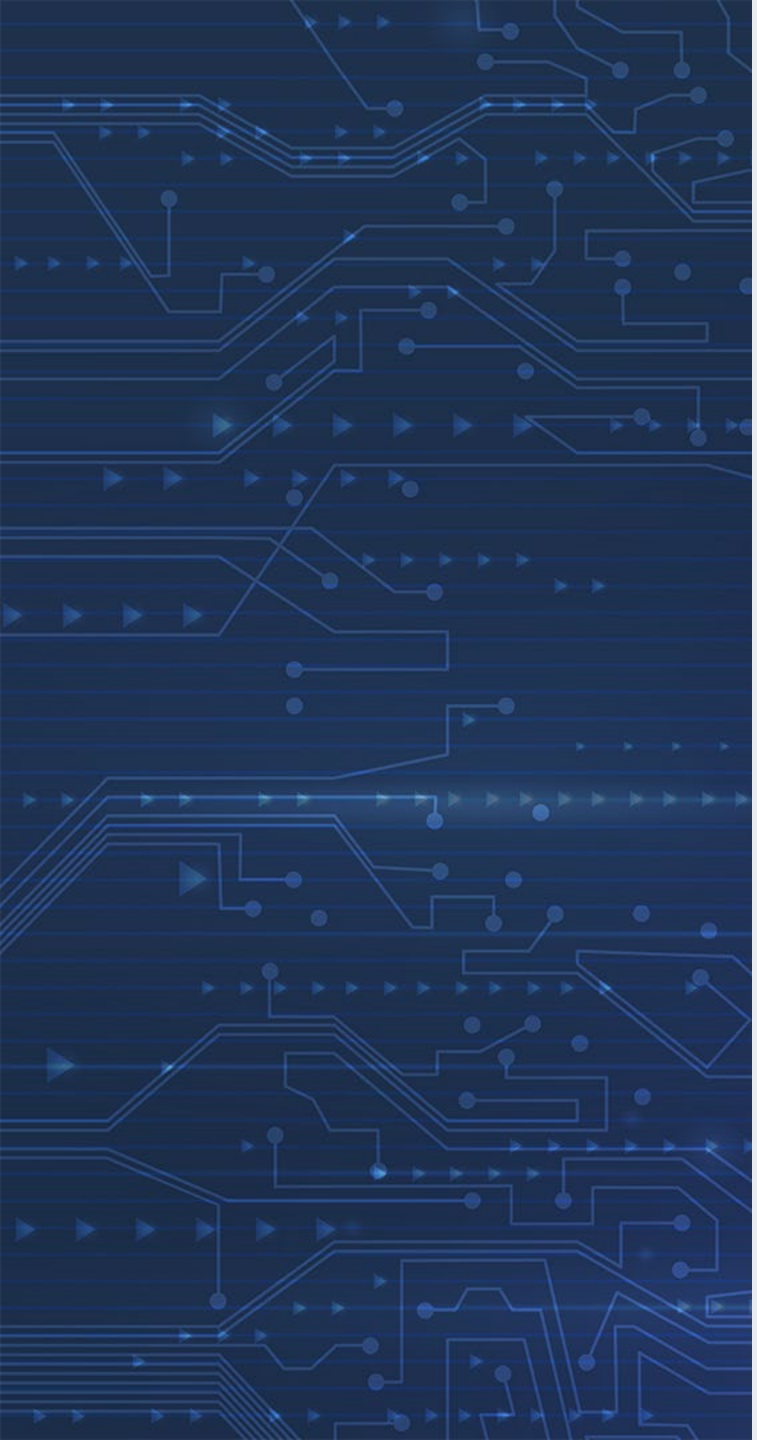
Karakurt (aka UNC3316)

- In November 2022, the Karakurt data extortion group claimed the compromise of a surgical and rehabilitation healthcare facility located in Kansas. The threat actors claimed to possess 200 GB of corporate data from the victim.
- Karakurt actors compress (typically with 7zip) and exfiltrate large sums of data—and, in many cases, entire network-connected shared drives in volumes exceeding 1 terabyte (TB)—using open-source applications and File Transfer Protocol (FTP) services [T1048], such as Filezilla, and cloud storage services including rclone and Mega.nz [T1567.002].
- Karakurt was revealed to be a data extortion arm of Conti in April 2022.
- June 02, 2022 – CISA Cybersecurity Advisory: AA22-152A

Threat Actors Conducting Data Exfiltration and Extortion (Part 3)

Lapsus$ (aka DEV-0537, SLIPPY SPIDER)

- A data extortion gang that claimed responsibility for a breach affecting a U.S.-based authentication company used by millions, as well as other critical companies.
- After gaining privileged access, Lapsus$ exfiltrates data from their target for future attacks and deletes the target's resources both on premises and in the cloud.
- Known to perform SIM swapping and recruit insiders.
- Several members arrested in March 2022 with just two eventually charged, failing to significantly disrupt Lapsus$ operations.



Cyber Espionage

Cyber Espionage and Data Exfiltration

State-sponsored threat actors are motivated by military, economic, or political interests, typically employing malicious cyber campaigns to gain access to sensitive assets for competitive advantage.

- Well-funded, experienced teams of hackers that target high-value organizations for data collection.
- Advanced Persistent Threats (APTs) may fly under the radar for years undetected.
- General techniques include watering holes, spear-phishing, zero-day exploits, and recruiting insiders.
- State-sponsored actors posing a threat to the U.S. HPH sector include Russia, China, Iran, and North Korea.

Case Study 5

No Pineapple! – DPRK Targeting of Medical Research and Technology Sector

- Q4 2022 cyber espionage campaign targeting medical research and technology sector attributed to Lazarus by WithSecure.
- Threat actor exfiltrated ~100GB of data but took **no destructive action** by the point of disruption.
- **SSH** connections where large volumes of data were moved out of the network and in one case '**pscp**' (Putty Secure Copy command) was used to transfer a file from the victim network to the actor infrastructure.
- Some data was also staged on the **Zimbra** server (possibly from the mail server itself) and then exfiltrated by the threat actor using a **webshell.**
- Some webshells used by the actor included **base.jsp** and **carbon.jsp**.
- Other tools leveraged in the attack included Cobalt Strike, Mimikatz, Stunnel, Plink, 3Proxy
- Full report with IOCs can be found here.

Case Study 6

Hydrochasma: Previously Unknown Group Targets Medical Laboratories in Asia for Intelligence Gathering with Publicly Available and Living-Off-The-Land Tools

- The threat actor ‘Hydrochasma’ has not been linked to any previously identified group but appears to have a possible interest in industries that may be involved in COVID-19-related treatments or vaccines.
- Tools used include Gogo scanning tool, Process Dumper (lsass.exe), Cobalt Strike Beacon, AlliN scanning tool, Fscan, Dogz proxy tool, SoftEtherVPN, Procdump, BrowserGhost, Gost proxy, NtImrelay, Task Scheduler, Go-strip, and HackBrowserData.
- The lack of custom malware used in this attack is notable. Relying exclusively on living-off-the-land and publicly available tools can help make an attack stealthier, while also making attribution more difficult.
- This activity is ongoing since at least October 2022.
- Full report with IOCs can be found here.

Are Cloud Backups Safe?

Backups Increasingly Targeted

- Mandiant research indicates that threat actors are increasingly targeting backups to inhibit reconstitution after an attack.
- Threat actors known to leverage Eamfo, an information-stealing malware designed to steal credentials stored by the Veeam cloud backup software.
- FIN12 used living-off-the-land-techniques to manually delete volume shadow copies.
- Operators and users of Conti ransomware have deployed malware capable of deleting shadow copies, backups, virtual machines, and snapshots.
- Other ransomware families such as LockBit, Ryuk, and Babuk contain functionality to automatically delete volume shadow copies and stop services related to backup solutions.

Backups Increasingly Targeted (cont.)

Off-site backups have also been targeted by threat actors in multiple cases. For example:

- A cloud backup system used by hundreds of dental offices in the U.S. was impacted by Sodinokibi ransomware in 2019.
- A cloud-hosting provider fell victim to ransomware in 2020, which affected 200,000 patients from numerous providers.

Source: oshamanual.com

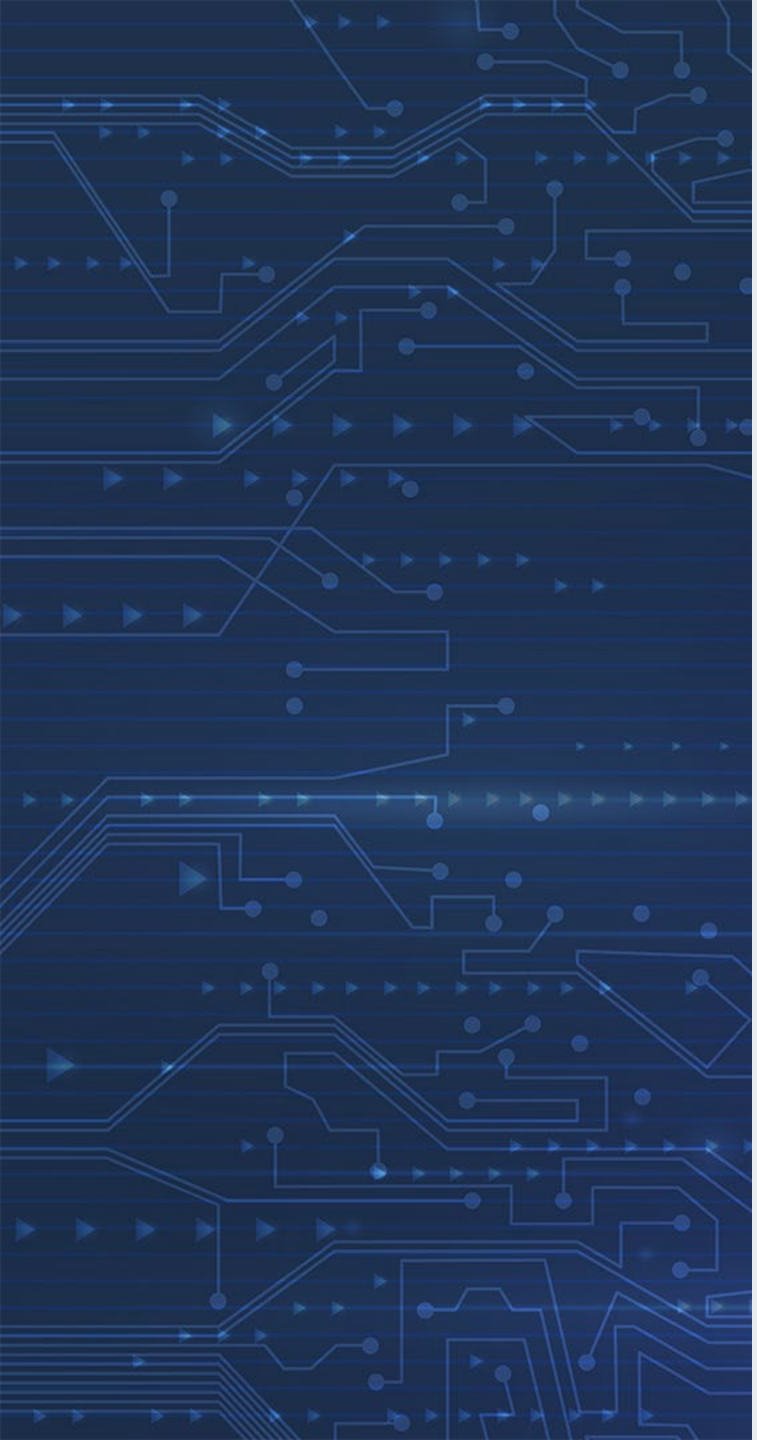
Insider Threats

- CISA defines an insider threat as an insider using their authorized access, wittingly or unwittingly, to do harm to the department's mission, resources, personnel, facilities, information, equipment, networks, or systems.
- This threat can manifest as damage to the department through the following insider behaviors: Espionage, Terrorism, Unauthorized disclosure of information, Corruption, Sabotage, Workplace violence, and Intentional or unintentional loss or degradation of departmental resources or capabilities.
- For more info, see Defining Insider Threats by CISA.

Case Study 7

Insider threat leads to data exfiltration at major pharmaceutical company:

- In November 2021, a U.S.-based pharmaceutical company filed a federal court lawsuit against a defendant for uploading more than 12,000 files with trade secrets related to its COVID-19 vaccine, including analysis of vaccine studies, operational goals, and development plans for new drugs.
- The company said in the complaint that it believed the defendant was going to another pharmaceutical company, and that the employee provided a “decoy” laptop when confronted about subsequent downloads of the information. The complaint stated that the company detected the employee transferring 12,000 files from a corporate laptop to an online Google Drive account across a three-day window.
- The employee had signed a confidentiality agreement as part of their employment, and the company had already disabled USB access in 2019 to prevent unauthorized file transfers. In October 2021, the company also implemented a technology that monitors when employees upload files to cloud-based platforms like Google Drive, according to the complaint.



Mitigations

Six Common Insider Threat Indicators

1. Unusual data movement
2. Use of unsanctioned software and hardware
3. Increased requests for escalated privileges or permissions
4. Access to information that is not core to their job function
5. Renamed files where the file extension does not match content
6. Departing employees

Resources:

[HC3 Brief on Insider Threats in Healthcare]

[CISA Insider Threat Mitigation Guide]

Data Loss Prevention (DLP)

- Data loss prevention (DLP) is a part of a company's overall security strategy, which focuses on detecting and preventing the loss, leakage or misuse of data while helping comply with regulations such as HIPAA. A comprehensive DLP solution provides the information security team with complete visibility into all data on the network, including:
    1. **Data in use**: Securing data being used by an application or endpoint through user authentication and access control.
    2. **Data in motion**: Ensuring the safe transmission of sensitive, confidential or proprietary data while it moves across the network through encryption and/or other e-mail and messaging security measures.
    3. **Data at rest**: Protecting data that is being stored on any network location, including the cloud, through access restrictions and user authentication.

Centralized Log Management for Data Exfiltration

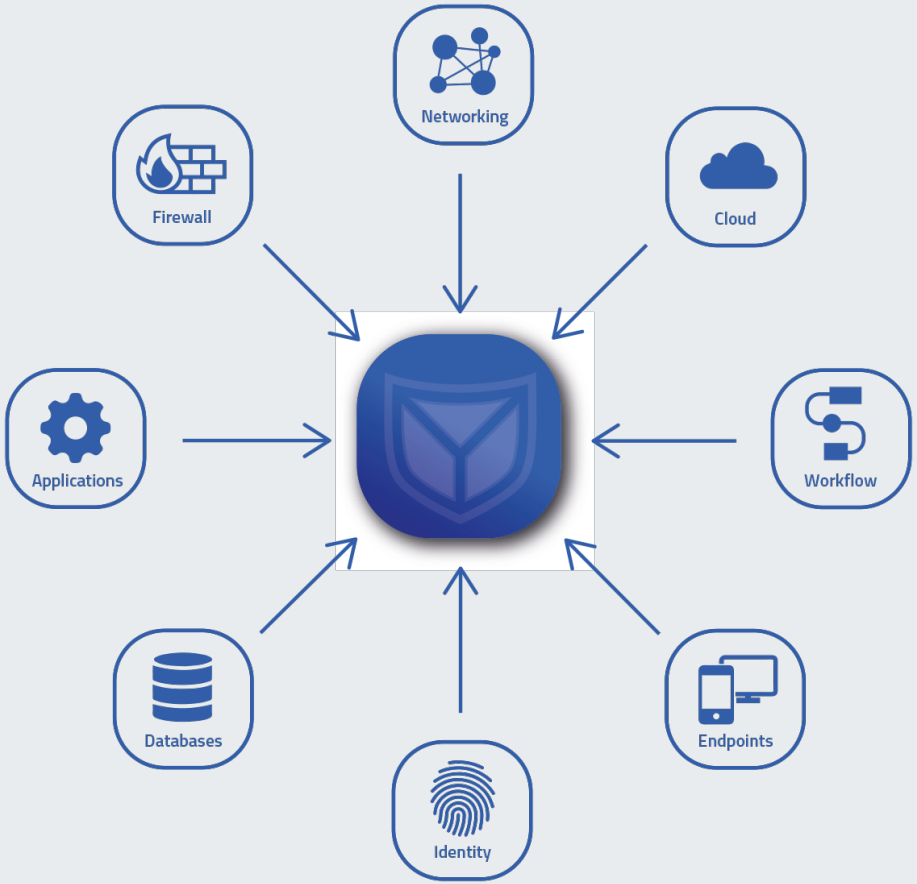


Image source: SECUINFRA

Goal: Collect, Analyze, Correlate & Search Event Log Data

Various log sources:

- Network
- Workstations
- Servers (Email, etc.)
- Systems
- Databases
- Web Applications
- Firewalls
- Authentication Services
- Cloud

Confronting Data Exfiltration Risks in the Cloud

- Securing data in the cloud requires new security approaches and methods of auditing data access.
- When securing data in the cloud, design an architecture to minimize downtime and limit the effects to the rest of your system in the event of a security compromise.
- Cloud providers also introduce explicit chokepoints, such as bastion host for communication with fleets of VMs, network proxy servers, network egress servers, and cross-project networks. These measures can reduce the risk of data exfiltration but cannot eliminate it completely.
- Establish a strong detection and response infrastructure for data exfiltration events.
- Resource: Google Cloud Data Loss Prevention

Exfiltration (TA0010)

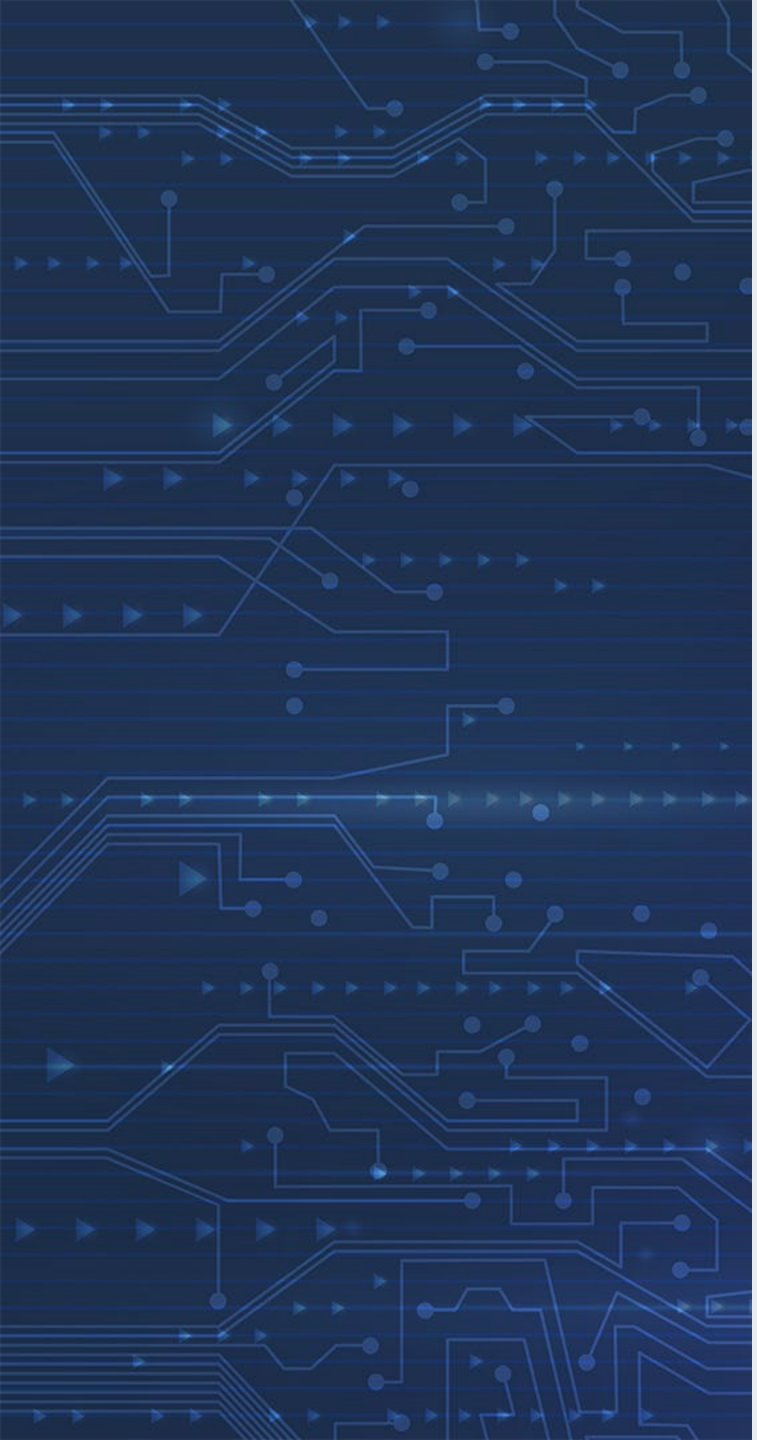
Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control (C2) channel, or an alternate channel, and may also include putting size limits on the transmission.

MITRE ATT&CK

- T1020: Automated Exfiltration
- T1030: Data Transfer Size Limits
- T1048: Exfiltration Over Alternative Protocol
- T1041: Exfiltration Over C2 Channel
- T1011: Exfiltration Over Other Network Medium
- T1052: Exfiltration Over Physical Medium
- T1567: Exfiltration Over Web Service
- T1029: Scheduled Transfer
- T1537: Transfer Data to Cloud Account

High-Level Mitigations

- To reduce the risk of data exfiltration, organizations must integrate security awareness and best practices into their culture.
- Consistently evaluate the risks of every interaction with computer networks, devices, applications, data, and other users.
- Organizations may also decide to institute periodic audits to verify that best practices are followed.



Major Takeaways

Major Takeaways

- Various classifications of threat actors performing data exfiltration continue to impact healthcare organizations and patients.
- Data, including PHI, was exfiltrated in at least 70% of ransomware incidents affecting healthcare delivery organizations, with a 35% increase in the number of patient records affected in 2022.
- Threat actors continue to evolve TTPs for successful data exfiltration and defense evasion.
- Mitigations are available to help defend against the risk of sensitive data leaving your organization.

Reference Materials

References

- The Rise of Data Exfiltration and Why It Is a Greater Risk Than Ransomware (August 23, 2022) https://thehackernews.com/2022/08/the-rise-of-data-exfiltration-and-why.html
- 2023 THIRD PARTY DATA BREACH REPORT (January 31, 2023) https://blackkite.com/whitepaper/2023-third-party-breach-report/
- Healthcare data breaches still higher than pre-pandemic levels (February 20, 2023) https://www.helpnetsecurity.com/2023/02/20/data-breaches-affecting-healthcare-providers/
- The Shift from Ransomware to Data Theft Extortion, https://www.blackfog.com/shift-from-ransomware-to-data-theft-extortion/
- Donut extortion group also targets victims with ransomware (November 22, 2022) https://www.bleepingcomputer.com/news/security/donut-extortion-group-also-targets-victims-with-ransomware/

References

- Hydrochasma: Previously Unknown Group Targets Medical and Shipping Organizations in Asia (February 22, 2023) https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering
- Centralized Log Management for Data Exfiltration (August 2, 2022) https://www.graylog.org/post/centralized-log-management-for-data-exfiltration/
- What is Data Loss Prevention (DLP)? (September 27, 2022) https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/
- What Are Some Potential Insider Threat Indicators? (January 27, 2023) https://securityboulevard.com/2023/01/what-are-some-potential-insider-threat-indicators/
- Centralized Log Management for Data Exfiltration (August 2, 2022) https://www.graylog.org/post/centralized-log-management-for-data-exfiltration/

References

- Healthcare Most Hit by Ransomware Last Year, FBI Finds (February 27, 2023), https://www.bankinfosecurity.com/healthcare-most-hit-by-ransomware-last-year-fbi-finds-a-21315
- Cyber Intelligence Part 3: Cyber Intelligence Collection Operations (June 27, 2015), https://www.newamerica.org/cybersecurity-initiative/blog/cyber-intelligence-part-3-cyber-intelligence-collection-operations/
- #StopRansomware: Hive Ransomware (November 25, 2022) https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-321a
- Cyber Extortionists' Newest Ploy: Skipping the Encryption (February 28, 2023) https://www.govtech.com/security/cyber-extortionists-newest-ploy-skipping-the-encryption
- LAPSUS$: AN IN-DEPTH LOOK AT DATA EXTORTION GROUP (April 26, 2022) https://www.avertium.com/resources/threat-reports/in-depth-look-at-lapsus

References

- Exbyte: BlackByte Ransomware Attackers Deploy New Exfiltration Tool (October 21, 2022) https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackbyte-exbyte-ransomware
- BlackCat ransomware's data exfiltration tool gets an upgrade (September 22, 2022) https://www.bleepingcomputer.com/news/security/blackcat-ransomware-s-data-exfiltration-tool-gets-an-upgrade/
- THREAT ANALYSIS REPORT: Inside the LockBit Arsenal - The StealBit Exfiltration Tool (December 16, 2021) https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool
- Stealc: a copycat of Vidar and Raccoon infostealers gaining in popularity – Part 1 (February 20, 2023) https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/

Questions

FAQ

Upcoming Briefing

- April 6 – Electronic Medical Records Still a Top Target for Cyber Threat Actors

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

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

Threat Briefings

Presentations that provide 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.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

HHS.GOV/HC3

HC3@HHS.GOV