



# Types of Cyber Threat Actors That Threaten Healthcare

June 8, 2023





# Agenda

---

- Cyber Threat Actors: An Overview
- Types of Cyber Threat Actors Threatening Healthcare:
  - Cybercriminals
  - Hacktivists
  - Nation State Actors
  - Cyberterrorists
  - Script Kiddies
  - Insider Threats

## Slides Key:



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



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



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# **Cyber Threat Actors: An Overview**

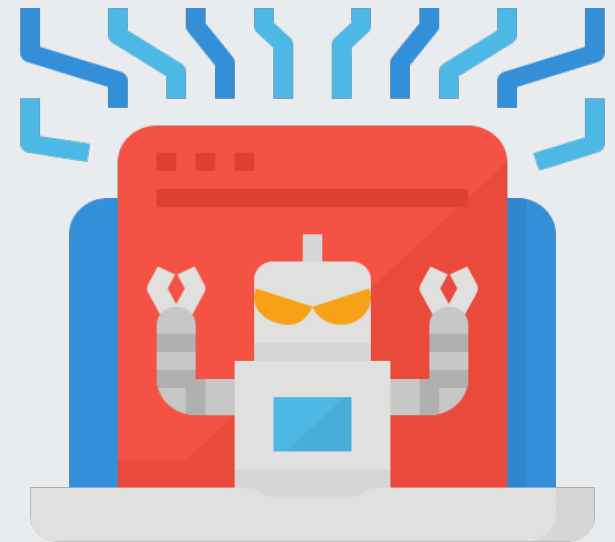
---



# Cyber Threat Actors

## Who They Are and How They Achieve Their Objective

- Malicious groups or individuals who aim to exploit weaknesses in an information system, or to exploit its operators to gain unauthorized access to or otherwise affect victims' data, devices, systems, and networks.
- They pursue their objectives by exploiting technical vulnerabilities, using social engineering, and by creating, disseminating, or amplifying false or misleading content online to influence individuals' behavior and beliefs.



Office of  
**Information Security**  
Securing One HHS



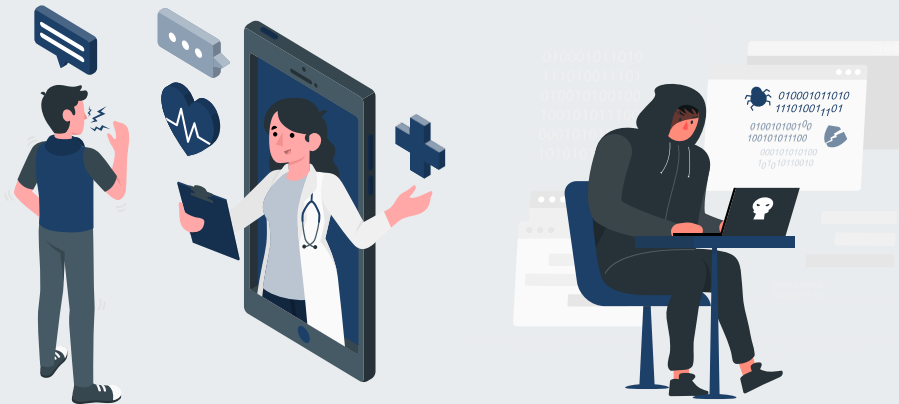
**Health Sector Cybersecurity  
Coordination Center**



# Cyber Threat Actors, cont.

## Why the Healthcare Industry Is Targeted

- Ease of network intrusion
- The information is good



## Potential Cost

- To Customers/Patients:
  - Hackers can make use of the stolen data for identity theft, financial gain, targeted blackmailing, and insurance fraud.
  - If the hackers don't make use of the information themselves, they can make a profit off it on cybercriminal forums.
- To Healthcare Entities:
  - Financial burden
  - Legal ramifications
  - Reputational damage



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Top Attacks Utilized by Cyber Threat Actors

---

- 1. Social Engineering:** The practice of obtaining sensitive information by manipulating legitimate users, often using the telephone or Internet.
- 2. Phishing:** Mainly conducted through email spoofing and text messages, a common method by which threat actors disguise themselves as a trustworthy entity with the intent to lure many recipients into providing information such as login credentials, banking information, and other personally identifiable information. Phishing is an example of a social engineering technique.
  - **Business Email Compromise (BEC):** Emails designed to trick an employee of the target organization into directly providing PII, credentials, etc. to cyber threat actors.
- 3. Distributed Denial of Service (DDoS):** A DoS attack that originates from numerous machines at once; can be controlled by a group of threat actors working together or be part of a botnet acting under the direction of a single threat actor.
- 4. Botnet:** A group of compromised devices that are coordinated by a threat actor; can be used for distributed denial of service (DDoS ), spreading ransomware and malware, sending spam, diverting traffic, stealing data, and/or more.





# Top Attacks Utilized by Cyber Threat Actors, cont.

---

## 5. Zero-day Vulnerability/Exploit

- Zero-day Vulnerability: A vulnerability that is not yet known by the vendor, and therefore has not been mitigated by a patch.
- Zero-day Exploit: An attack directed at a zero-day vulnerability.

## 6. Person-in-the-Middle (PITM) (also known as Man-in-the-Middle): A technique by which a threat actor intercepts a communication between two parties, such as a victim and a web server, without the victim's knowledge.

### The 'wares

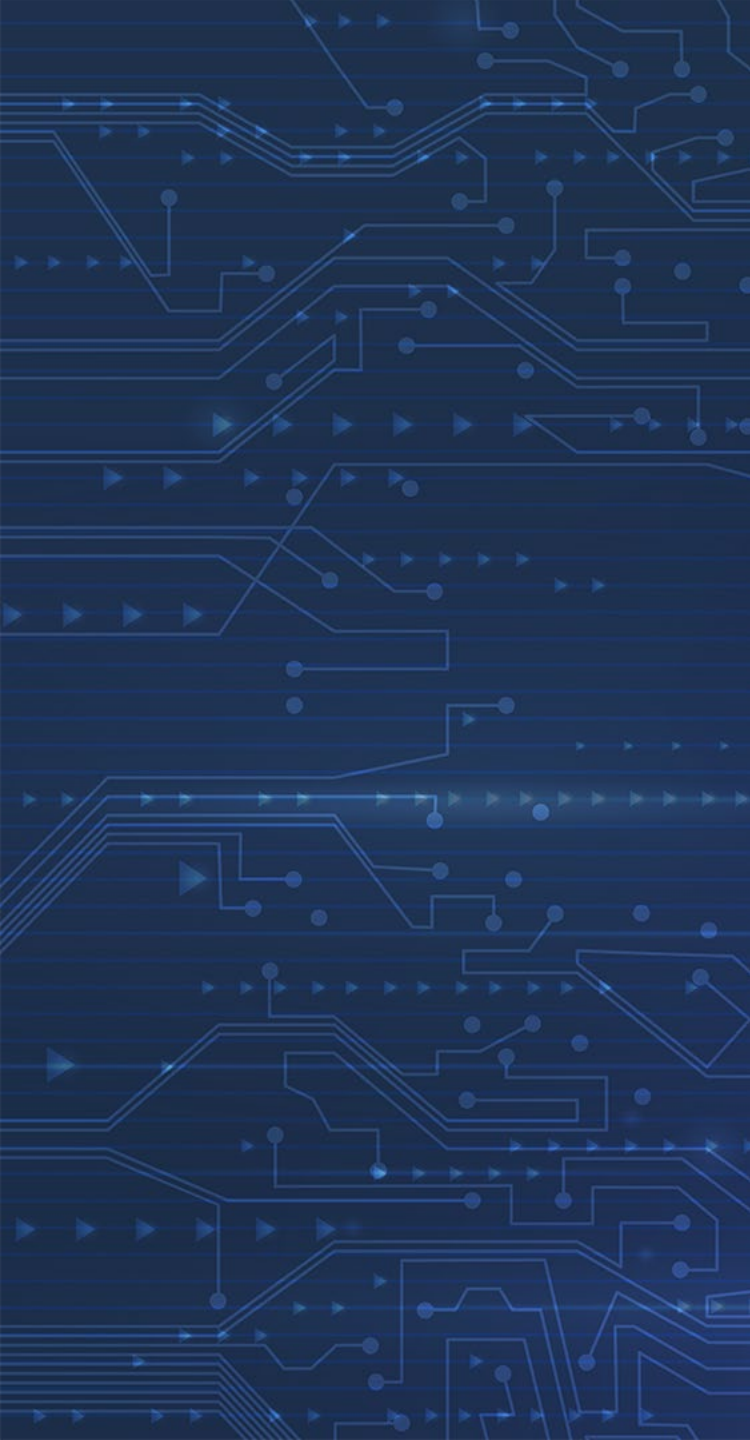
## 7. Malware: Short for malicious software; any software or code designed to infiltrate/damage a computer system.

- Wipers: Malware designed to completely wipe the hard drive of infected devices.

## 8. Adware: Short for “advertising software”; browser-based and application-based adware tracks and gathers user and device information, including location data and browsing history; can lead to exploitation of security settings, users, and systems.

## 9. Ransomware: Malicious software that restricts access to or operation of a computer or device, restoring it following payment.





# **Types of Cyber Threat Actors Threatening Healthcare**

---





# Cybercriminals

---



# Cybercriminals

---

- Threat actors or hackers that target organizations through extortion or the disclosure of compromised data for financial or personal gain.
- Responsible for targeting organizations for their own personal gain via extortion, blackmail, or revealing sensitive information.
- Cybercriminals are able conduct complex and sophisticated campaigns using cyber tools and services available through illegal online markets.
- A cybercriminal group can be an individual or a large group from different criminal enterprises working together.
- Responsible for stealing billions of consumer and business dollars annually and have a dominant presence in the media.
- Liable to purchase software and attack tools from the dark online community, like script kiddies and hacktivists.
- Engage in selling, purchasing, and trading sensitive intellectual property.
- Known to use tactics such as ransomware and DDoS attacks against healthcare organizations.



Office of  
**Information Security**  
Securing One HHS

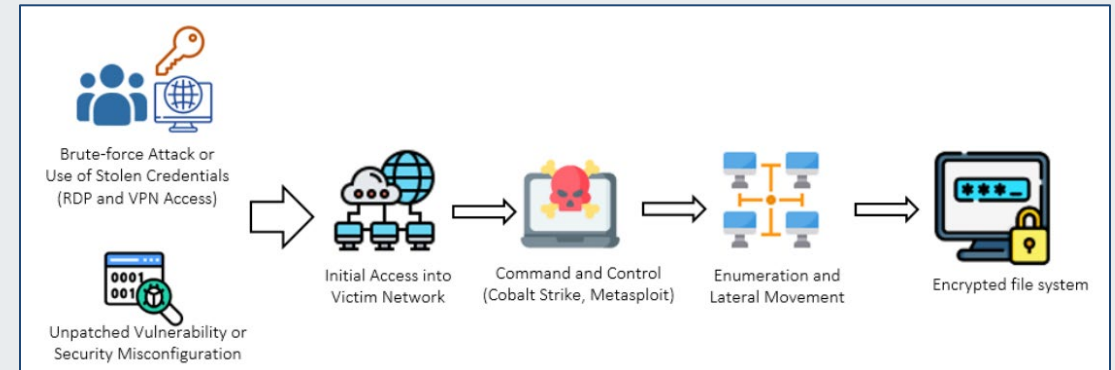


**Health Sector Cybersecurity  
Coordination Center**



# LockBit 3.0 Ransomware as a Service

- LockBit 3.0 (LockBit Black) discovered June/July 2022
- Newest version of the LockBit ransomware
- This malware sometimes requires a unique, 32-character password each time it is launched, making analysis difficult for researchers
- Financially motivated
- **Notable Victims:** A CRM company, HPH
- **Related HC3 Products:** [LockBit 3.0](#), [EMRs Still a Top Target for Threat Actors](#), [New Data Breaches from CIOp and Lockbit Ransomware Groups](#)



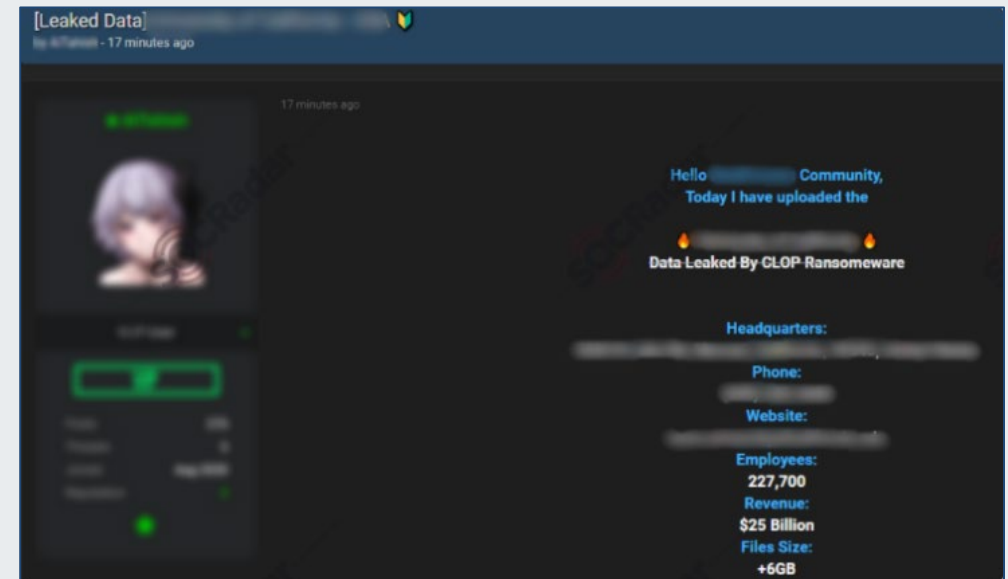
An overview of a typical LockBit operation.  
(Source: SOC Radar / Australian Cyber Security Center)





# ClOp Ransomware as a Service

- Russia-linked ransomware group
- First observed in February 2019
- Mostly targets Windows systems, but also Linux servers
- Known to target organizations with a revenue of \$5 million U.S. Dollars (USD) or higher. Operators have seen payouts of up to \$500 million USD.
- **Notable Victims:** Microsoft; also claimed responsibility for a mass attack on more than 130 organizations, including those in the healthcare industry.
- **Related HC3 Products:** [ClOp Allegedly Targets Healthcare Industry in Data Breach](#); [ClOp Ransomware](#)



An alleged database leaked by ClOp is detected in a hacker forum monitored by SOCRadar.  
Source: SOCRadar



Office of  
**Information Security**  
Securing One HHS

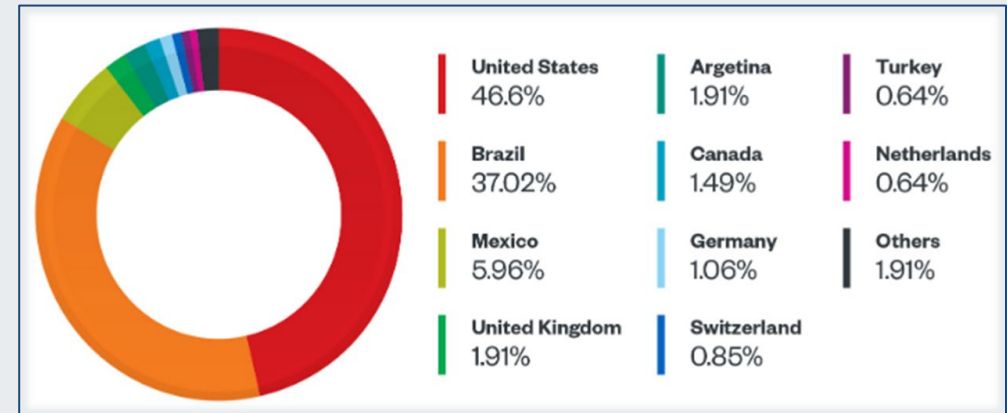


Health Sector Cybersecurity  
Coordination Center

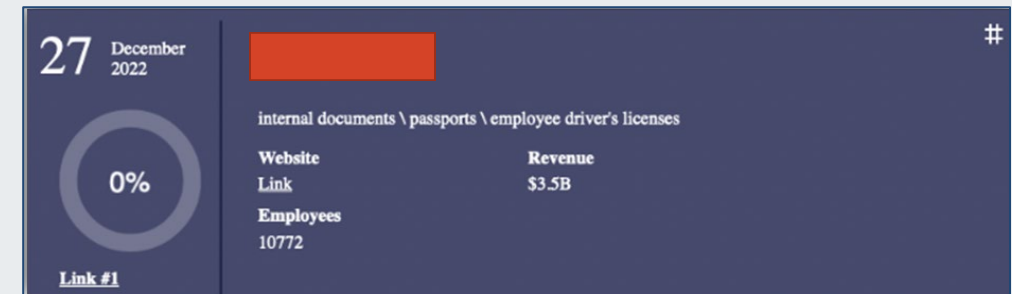


# Royal Ransomware as a Service

- First observed in early 2022 and believed to have very experienced operators previously belonging to other infamous cybercriminal groups, including Conti Team One.
- The United States tops their victim list
- 64-bit executable, written in C++
- Targets Windows systems, encrypts files and appends “.royal” or “.royal\_w” extensions to filenames; creates a "README.TXT" ransom note.
- **Notable Victims:** *US Telecom, UK Racing Circuit*
- **Related HC3 Products:** [Royal Ransomware Analyst Note](#); [Royal & BlackCat Ransomware: The Threat to the Health Sector](#)



Percentages of Royal ransomware attacks by country.  
Source: Trend Macro



Royal ransomware website showing a U.S. telecom company as a victim.  
Source: Bleeping Computer



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# BianLian Ransomware as a Service

- Emerged in August 2022
- Healthcare is among the top industries targeted by this threat actor group
- Financially motivated
- Known for researching victims before an attack
- **Notable Victims:** California healthcare facility, Virginia public entity
- Actions to mitigate cyber threats from BianLian ransomware and data extortion:
  - Strictly limit the use of RDP and other remote desktop services.
  - Disable command-line and scripting activities and permissions.
  - Restrict usage of PowerShell, and update Windows PowerShell or PowerShell Core to the latest version.
- **Related HC3 Products:** [EMRs Still a Top Target for Threat Actors](#)

CYBERSECURITY ADVISORY

## #StopRansomware: BianLian Ransomware Group

Release Date: May 16, 2023

Alert Code: AA23-136A

### Summary

*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](https://stopransomware.gov) to see all #StopRansomware advisories and learn more about other ransomware threats and no-cost resources.*

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Australian Cyber Security Centre (ACSC) are releasing this joint Cybersecurity Advisory to disseminate known BianLian ransomware and data extortion group IOCs and TTPs identified through FBI and ACSC investigations as of March 2023.

May 2023 Joint Cybersecurity Advisory (FBI, CISA): BianLian Ransomware Group  
Source: CISA



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Hacktivism

---



# Hacktivism

- Hack + Activism = Hacktivism
- **Hacktivist:** An individual who performs an act of hacktivism.
- Often targets government entities and organizations located within countries seen as enemies.
- Actions aim to cause significant reputational harm to their targets.
- Once decentralized collectives made up of private individuals, they are now coordinated organizations that are better organized, more structured, and more sophisticated.



Source: NBC News



Office of  
**Information Security**  
Securing One HHS



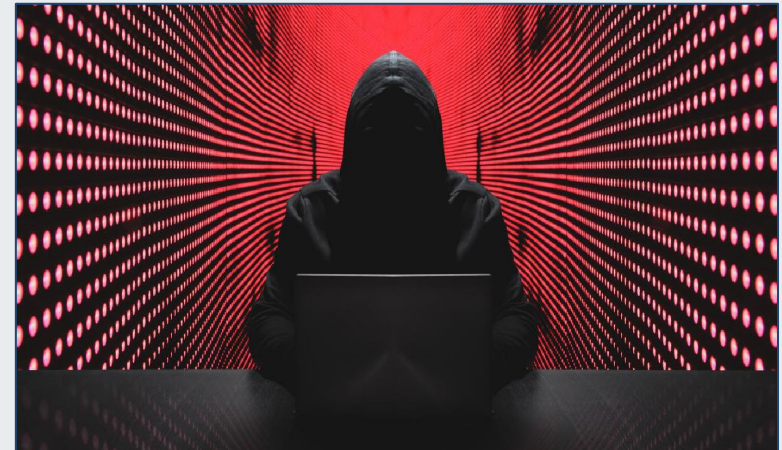
**Health Sector Cybersecurity  
Coordination Center**





# Lapsus\$

- First made headlines with a ransomware attack against the Brazilian Ministry of Health in December 2021, compromising the COVID-19 vaccination data of millions within the country.
- Known for their high-profile cyberattacks on government and corporate targets, as well as their use of sophisticated malware, encryption techniques, and other techniques to hide their tracks and evade detection.
- **Notable Attack:**
  - Targeted a major healthcare provider in 2020; during this attack, the group was able to access and steal the sensitive personal information of millions of patients.
- **Related HC3 Products:** [Lapsus\\$ and the Health Sector](#)



Source: Reversing Labs



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# KillNet

- Launched around the end of February 2022.
  - More than 89,000 subscribers on their Telegram channel, organized in a military-like structure with a clear top-down hierarchy.
  - Consists of multiple specialized squads to perform attacks, all answering to the main commandment.
- Currently around a dozen sub-groups, the main one being Legion.
  - **Subgroups:** Legion, Jacky, Mirai, Impulse, Sakurajima, Rayd, Zarya, Vera, Phoenix, Kajluk, Sparta, and DDOSGUNG
  - All these groups were led by a hacker called KillMilk, now believed to be led by a hacker called Blackside.
  - Legion and the squads are referred to as Killnet's special forces, with Legion referred to as its Cyber Intelligence Force.
- **Notable Attacks:**
  - In February 2023, launched daily DDoS attacks against nearly one hundred different healthcare entities, including pharmaceutical companies, hospitals, health insurance and health services.
- **Related HC3 Products:** [20230405 KillNet](#), [20230130 KillNet](#), [20221222 KillNet](#)



Source: SOCRadar



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Nation State Actors

---



# Nation State Actors

---

- Nation state actors sponsor threat groups that launch attacks against foreign governments and organizations to advance their geopolitical objectives.
- Frequently the most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination.
  - Designated as an APT, or an Advanced Persistent Threat
  - APTs are considered capable of composing and executing state-of-the-art attacks using the most modern malware-obscuring techniques.
- The activities of state-sponsored cyber threat actors include:
  - Espionage against governments, organizations, and individuals
  - Disrupting critical systems
  - Influencing and shaping public discourse
  - Building networks of compromised devices to enable further cyber threat activity
  - May also pursue financially motivated threat activity



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# North Korea

## Silent Chollima

- Reported to operate in support of the Reconnaissance General Bureau (RGB) of the Democratic People's Republic of Korea (DPRK).
- Recognized as one of the subgroups of the notorious and widely publicized Lazarus group.
- **Aliases:** Andariel
- **Targets:** Financial services, healthcare, defense, technology, and more
- **Notable Attacks:** 2022 Maui Ransomware attacks on healthcare organizations



Source: CrowdStrike



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# China

## Wicked Panda

- Wicked Panda is a Chinese APT who has been around since at least 2007.
- Observed to use spear phishing, watering holes, and supply chain attacks to gain initial access to a victim; also deploys backdoors through tools such as China Chopper.
- **Aliases:** APT 41, Barium, Double Dragon, Winnti, Wicked Spider, and Bronze Atlas
- **Targets:** Healthcare, pharmaceuticals, retail, travel, media, and more
- **Notable Attacks:** USAHerds
- **Related HC3 Products:** [APT41 and Recent Activity](#)



Source: CrowdStrike



Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center



# Cyberterrorists

---



# Cyberterrorists

- Cyberterrorists target systems to disrupt or destroy critical services and infrastructures of a specific nation, sector or organization.
- They are different from cyber-criminals because of their motivation: criminals are motivated by the reward, while terrorists act because of the possible effects.



Office of  
**Information Security**  
Securing One HHS



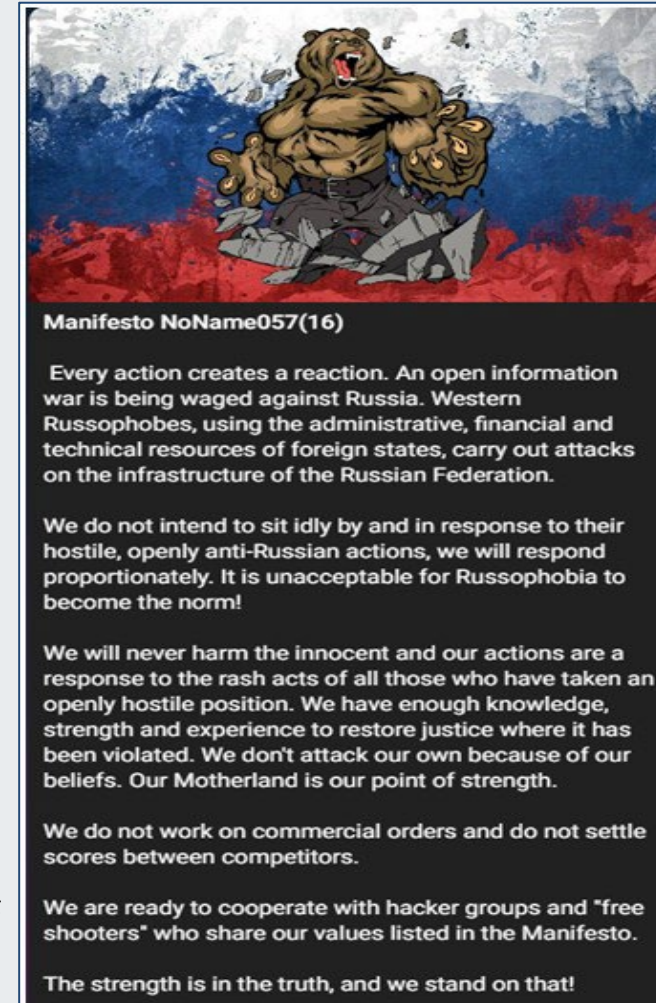
**Health Sector Cybersecurity  
Coordination Center**





# NoName057(16)

- Established March 2022
- Pro-Russia cyberterrorist hacktivist group primarily focused on disrupting websites important to nations critical of Russia's invasion of Ukraine.
- Originally targeted Ukrainian news and media websites but has since shifted to targeting critical infrastructure sectors whose operations are vital to NATO and NATO-associated targets.
- Overall, their motivations center around silencing anything the group deems to be anti-Russian.
- **Notable Attack:** The website of the Finnish Parliament in August 2022



NoName057(16) manifesto.  
Source: Check Point



Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center



# Script Kiddies

---



# Script Kiddies

---

- The term “script kiddie” first appeared in forums, blogs, message boards and Internet Relay Chat in the mid-1990s; the term is used to describe people who downloaded a tool without necessarily knowing or caring how it worked.
- The typical script kiddie uses existing, well-known techniques, programs and scripts to find and exploit weaknesses in internet-connected computers.
- Their attacks are random and with little understanding of the tools they are using, how they work, and the harm they cause.
- Script kiddies purchase, trade, and use tools and malware developed by larger attackers to gain access to vulnerable systems.
- Motivated by personal or simple reasons like seeking attention, having fun, creating chaos, or revenge.
- Denial of Service, Social Engineering, and Website Defacement are some low-skill but potentially detrimental exploits that script kiddies are known to pull off.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Hackers vs. Script Kiddies

---

- **Hackers:**

- More experienced
- Skilled and knowledgeable
- Well-researched
- Persist through challenges
- Use off-the-shelf exploits, but can code their own exploits and adapt methods to challenges



- **Script Kiddies:**

- Inexperienced
- Limited knowledge and skills
- Launch exploits without knowing much about them
- Apt to quit when challenged
- Use off-the-shelf and beginner programs written by other people



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Cybercrime Forums

---

- Internet forums specializing in computer crime and online fraud activities.
- During the 2nd Quarter of 2022, FortiGuard Labs released a list validating the reliability of threat actors.
  - 24 adversaries were identified as being credible.
- Most popular and active darknet cybercrime forums: XSS, Exploit, Breached Forums (aka BreachForum), Helium Forum
- **Threat actors promoted to 'Credible' in Q2 2022:** inthetmatrix, Pirat-Networks, Mont4na/pumpedkicks, Yesdaddy, NetFlow, spectre123, kelvinsecurity/teamkelvinsec, Network Battalion 65, Breached, Netsec, RedLineVIP, PieWithNothing, SebastianPereiro, TopFuel, zanko, pompompurin, zirochka, pixe1, black\_palm, We Leak Database/GuntherMagnuson, Weaver, DragonForce Group/impossible1337, Krustywise, r1z



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**

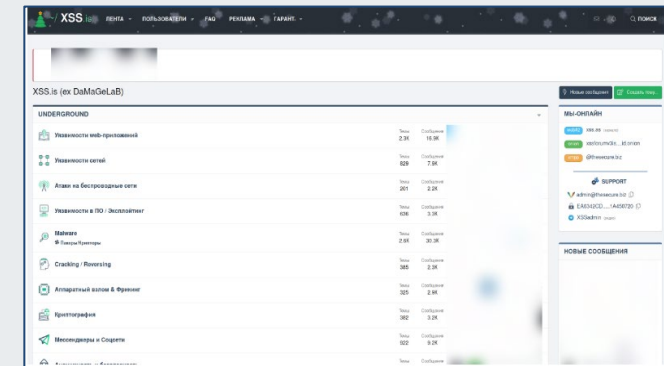


# Cybercrime Forum: XSS

- Formerly known as damagelab.org (stylized as DaMaGeLaB)
- Dating back to 2013, one of the earliest and most popular Russian language forums
- Rebranded and relaunched in September 2018 as xss[.]
- Name derived from cross-site scripting, a security vulnerability in web applications that bypasses access controls.
- A popular Russian language forum, hosting discussion topics including hacking, programming and technology, and a marketplace section where users can directly purchase primarily digital products.

*Provides custom membership groups on the forum:*

- **Legend Group:** Long time forum members or those sharing highly sensitive data can join.
- **Premium Group:** Members can change nicknames, access to all hidden links, can change nicknames, and have unlimited message editing privileges.
- **PR Group:** Members of this group are responsible for posting new content. Moderators only give access to this account after the member's credibility has been proven.
- **Member Group:** This is for members who join for free.



Snippet of the XSS.is forum homepage, which hosts different sections under the label of “Underground.”  
Source: Security Boulevard



Office of  
**Information Security**  
Securing One HHS

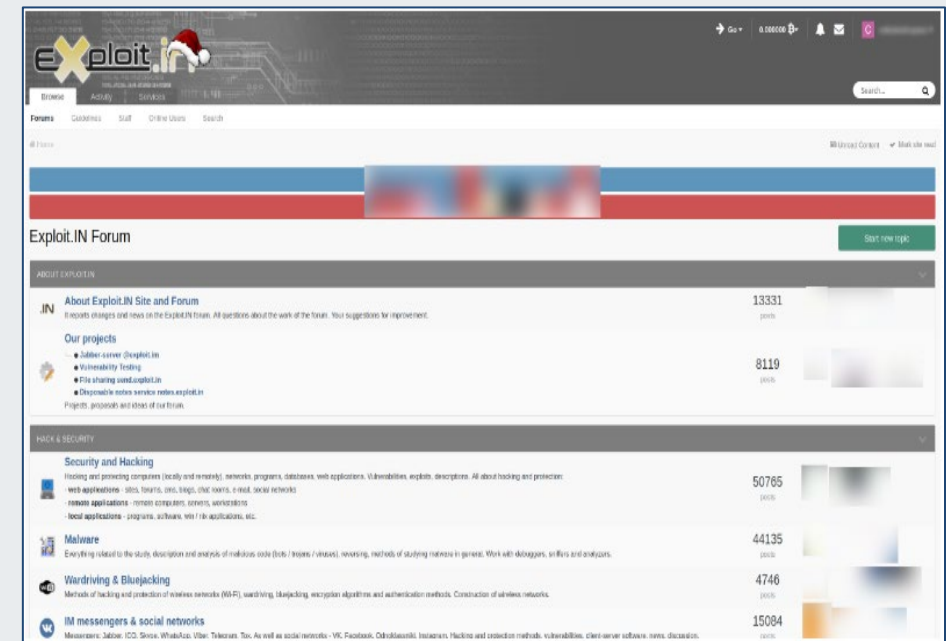


**Health Sector Cybersecurity  
Coordination Center**



# Cybercrime Forum: Exploit

- An invitation-only cybercrime forum; can also be joined with a paid registration.
- To register on Exploit without paying a registration fee, users need to fit at least one of these criteria:
  - Have their own service on other reputable forums that are over a year old; must be a member of the administration or the forum team.
  - Must be a specialist in C/C++, Assembler, Delphi, Pascal, .NET, Kylix, Python, Visual Basic, etc. (Can also specialize in web-based languages, such as PHP, Perl, ASP, JavaScript, XML, XSL, MySQL, MsSQL, etc.)
  - Potential member's account on similar forums must be at least two years old.
  - Potential member must specialize in malware, exploits, bundles, crypto, or automated transfer systems.



This snippet of the Exploit.in forum homepage screenshot shows an “About” section and different categories for posts about hacking.  
*Source: Security Boulevard*



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Cybercrime Forum: Breached Forums (aka BreachForum)

- Mentioned a handful of times in the Telegram group chat “LAPSUS\$ Chat”-- owned and managed by the data breach and extortionist group “LAPSUS\$.”
- Relatively new, with the incentives offered to former Raid Forums users.
- Successor to Raid Forums and has near identical appearance and functionality to Raid Forums.
- Owned and operated by the well-known and reputable former Raid Forums user, pompompurin.
- Site could reach or exceed its predecessor as the most popular clearnet hacking forum.



Source: HackRead



Office of  
**Information Security**  
Securing One HHS



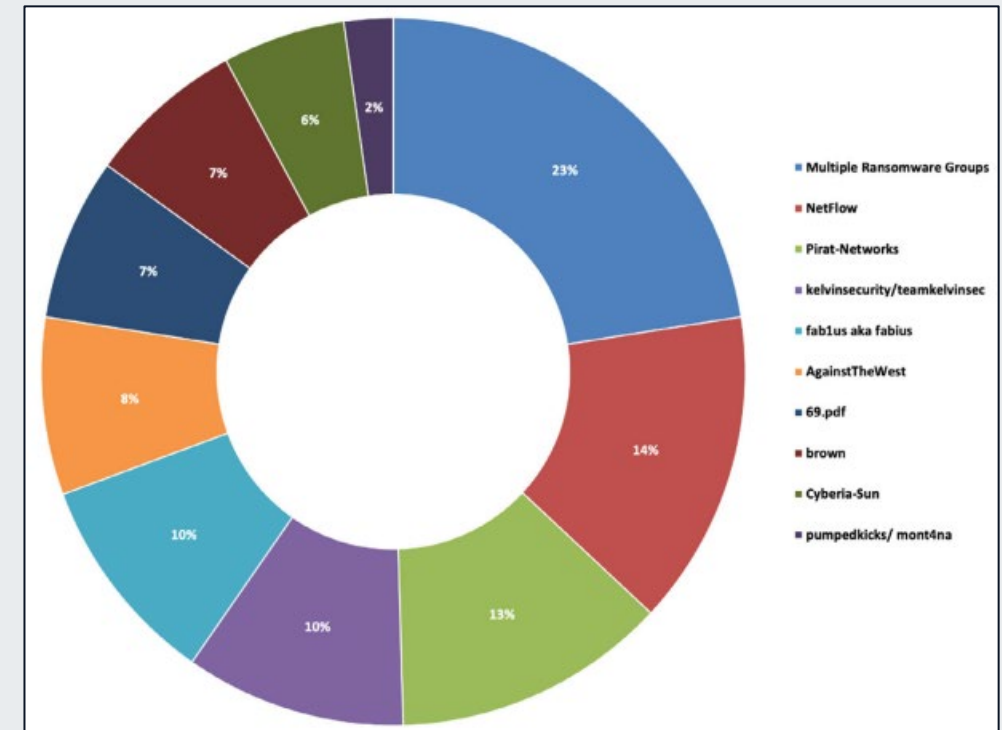
**Health Sector Cybersecurity  
Coordination Center**





# mont4na

- Top threat actor targeting the healthcare sector.
- Skillset is primarily exploiting SQL injection vulnerabilities, primarily on login panels.
- Actively selling vulnerabilities and asking buyers to access the database.
- Over time, activities include posting login accesses, and databases in some cases.
- Targeted companies are across the globe and well-known.
- Industries include aviation, banking, government, and the health sector.
- Inactive for about 10 months until late November 2021.
- Deletes advertisement once the vulnerability or the access is sold.



Top 10 Threat Actors Targeting the Healthcare Sector  
Source: Fortinet



Office of  
**Information Security**  
Securing One HHS

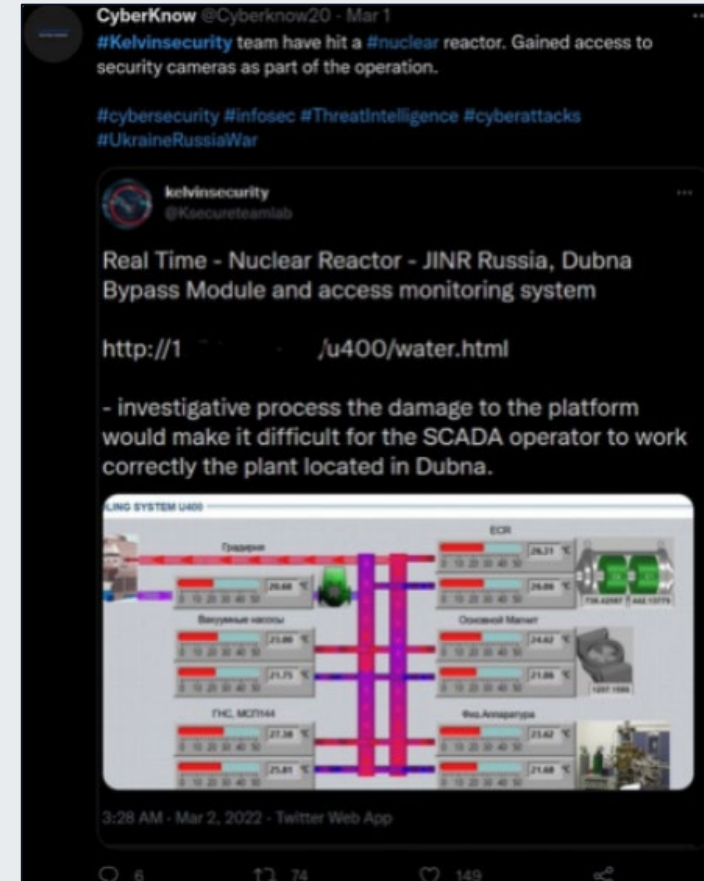


**Health Sector Cybersecurity  
Coordination Center**



# KelvinSecurity

- KelvinSecurity is a Telegram channel where cybercriminals share information.
- This channel targets the military of the target countries, financial services, government agencies, management, aviation, casinos and gaming, communications, education, energy, health, and transportation.
- KelvinSecurity shares their actions and leaks data from their Telegram accounts, like other hacker groups with Telegram channels.
- Breached a Russian nuclear reactor in March 2022 during the Russia-Ukraine war and shared their actions publicly on their Twitter accounts and Telegram channels.



An announcement tweet about KelvinSecurity hacking the nuclear reactor.  
Source: SOCRadar



Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center



# IntelBroker

- An initial access broker also known as “thekilbob.”
- Highly active BreachedForum member with an 9/10 reputation score.
- Later banned from BreachedForum for violating the site’s criminal code of ethics.
- Claimed responsibility for several high-profile leaks in the past year.
- **Notable Victims:** T-Mobile, UScellular, an online delivery platform, a health insurance company, and U.S. government agencies

The screenshot shows a forum post on IntelBroker. The post title is "SOLD [ ] DC.gov Database" and it was posted by IntelBroker on Monday, March 6, 2023, at 03:33 AM. The post content includes a redacted area, a "Buyer Information" section stating "user count: 170K" and "Compromised data:", and a list of data fields: "Subscriber ID, Member ID, Policy ID, Status, First Name, Last Name, SSN, DOB, Gender, Relationship, Benefit Type, Plan Name, HIOS ID, Plan Metal Level, Carrier Name, Premium Amount, Premium Total, Policy APTC, Policy Employer Contribution, Coverage Start, Coverage End, Employer Name, Employer DBA, Employer FEIN, Employer HBX ID, Home Address, Mailing Address, Work Email, Home Email, Phone Number, Broker, Race, Ethnicity, Citizen Status, Plan Year Start, Plan Year End, Plan Year Status". There is also a "Sample!" section with a redacted image and a "Pricing" section stating "I am looking for undisclosed amount in XMR crypto currency. contact me on keybase @ IntelBroker Middleman only!!". The user profile for IntelBroker is visible on the left, showing a profile picture of a red cat, the name "UwU Mishka-san", and statistics: 542 posts, 134 threads, joined in Oct 2022, and a reputation of 2,295.

U.S. House members' data up for sale.

Source: Bleeping Computer



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Insider Threats

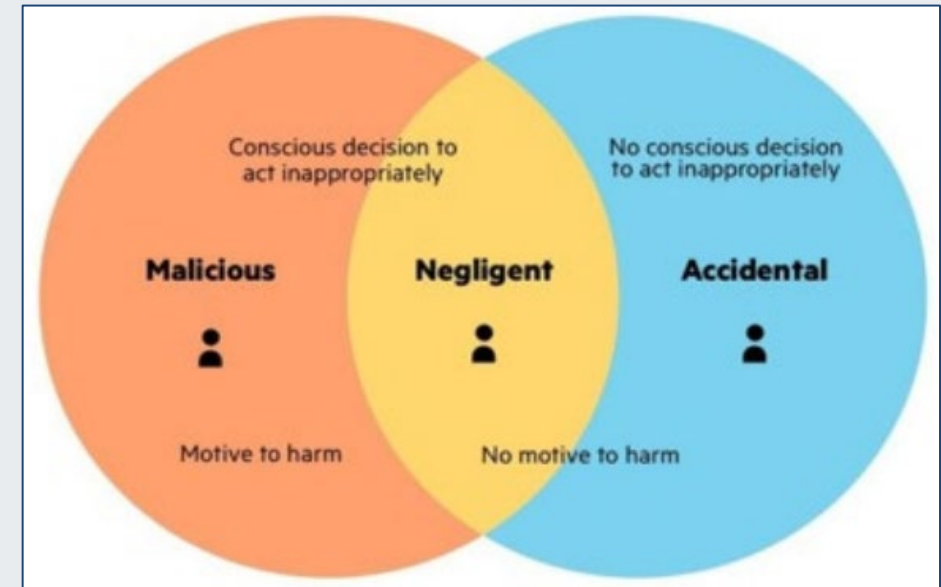
---



# Insider Threats

An insider threat in the Healthcare and Public Health (HPH) sector is a person within a healthcare organization, or a contractor, who has access to assets or inside information concerning the organization's security practices, data, and computer systems. The person could use this information in a way that negatively impacts the organization. There are several types of insider threats within an organization, all with different goals. Some insider threats are as follows:

- Careless or negligent workers
- Malicious insiders
- Inside agents
- Disgruntled employees
- Third parties





# Insider Threats, cont.

---

According to the Ponemon Institute 2022 Cost of Insider Threats report:

- These incidents have increased by almost 50% over the last two years and have become more frequent.
- The larger the organization, the more insider threat incidents.
- Critical business data and sensitive information can be found in employees' emails.
- Cost of credential theft to organizations increased by 65%.
- The average containment time for an insider incident increased from 77 to 85 days. Incidents that took over 90 days to contain cost organizations \$17.19 million on average.
- More than half of the attacks were caused by negligence, while 1 out of 4 was by malicious insiders; the rest involved credential theft.
- 3 out of 4 respondents mentioned that malicious insiders use corporate email to steal sensitive data.
- Advanced technologies, such as user behavior-based tools, AI, and machine learning, are important to prevent, investigate, contain, and remediate insider incidents.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Data Theft by Hospital Employee

---

## What happened?

- A former employee of a hospital downloaded private data from the medical center's systems to a USB drive the day after quitting. The employee still had access, which made it difficult for security software to initially detect the breach.

## What were the consequences?

- Patients' test results, names, and dates of birth were leaked.
- Patients who were victims of this breach were provided services including free credit monitoring and identity restoration.





# Conclusion



HHS HC3



HHS 405(d)



CISA



Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center





Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Reference Materials



# References

- “#StopRansomware: BianLian Ransomware Group,” CISA. 16 May 2023. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a>
- “7 Examples of Real-Life Data Breaches Caused by Insider Threats,” Ekran. N.d. <https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches>
- “2022 Ponemon Cost of Insider Threats Global Report,” Bank Info Security. 24 August 2022. <https://www.bankinfosecurity.com/whitepapers/2022-ponemon-cost-insider-threats-global-report-w-10798>
- “2023 INSIDER THREAT REPORT [GURUCUL],” Cybersecurity Insiders. N.d. <https://www.cybersecurity-insiders.com/portfolio/2023-insider-threat-report-gurukul/>
- Alcántar, Miguel. “Cybersecurity: Nation-State Actors, Encrypted Cybercrimes and Man-in-the-Middle Attacks,” ACAMS Today. 19 September 2017. <https://www.acamstoday.org/nation-state-actors-encrypted-cybercrimes-man-in-the-middle-attacks/>
- Akasaka, Yuzuka. “Top Cybercrime Forums to Monitor in 2023,” Security Boulevard. 16 May 2023. <https://securityboulevard.com/2023/05/top-cybercrime-forums-to-monitor-in-2023/>
- “Andariel, a Lazarus subgroup, expands its attacks with new ransomware,” Kaspersky. 09 August 2022. [https://www.kaspersky.com/about/press-releases/2022\\_andariel-a-lazarus-subgroup-expands-its-attacks-with-new-ransomware](https://www.kaspersky.com/about/press-releases/2022_andariel-a-lazarus-subgroup-expands-its-attacks-with-new-ransomware)
- “APT Profile: Cozy Bear / APT29,” SOCRadar. 17 March 2023. <https://socradar.io/apt-profile-cozy-bear-apt29/>
- Azure Network Security Team. “KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks,” Microsoft. 17 March 2023. <https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/>
- Behling, Dana. “LockBit 3.0 Ransomware Unlocked,” VM Ware. 15 October 2022. <https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html>
- “BianLian: A new golan based cross functional ransomware in action,” SecureBlink. 16 September 2022. <https://www.secureblink.com/threat-research/bian-lian-a-new-golan-based-cross-functional-ransomware-in-action>





# References

- Burgess, Matt. “Hacktivism Is Back and Messier Than Ever,” WIRED. 27 December 2022. <https://www.wired.com/story/hacktivism-russia-ukraine-ddos/>
- Burt, Jeff. Maui ransomware linked to North Korean group Andariel,” The Register. 10 August 2022. [https://www.theregister.com/2022/08/10/maui\\_ransomware\\_andariel/](https://www.theregister.com/2022/08/10/maui_ransomware_andariel/)
- Chavez, Ivan Nicole, Byron Gelera, Monte de Jesus, Don Ovid Ladores, Khristian Joseph Morales. “Conti Team One Splinter Group Resurfaces as Royal Ransomware with Callback Phishing Attacks,” TrendMicro. 21 December 2022. [https://www.trendmicro.com/en\\_us/research/22/1/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html](https://www.trendmicro.com/en_us/research/22/1/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html)
- “Cyber Criminals Target Remote Workers to Corner Stores,” Insurance Journal. 15 August 2021. <https://www.insurancejournal.com/magazines/mag-features/2021/08/16/627096.htm>
- Cybereason Global SOC & Cybereason Security Research Teams. “Royal Rumble: Analysis of Royal Ransomware,” Cyber Reason. 14 December 2022. <https://www.cybereason.com/blog/royal-ransomware-analysis>
- Dark Web Profile: LockBit 3.0 Ransomware,” SOCRadar. 27 April 2023 <https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/>
- Davis, Jessica. “Hacktivist vs. cyberterrorist: Understanding the 5 enemies of healthcare IT security,” Healthcare IT News. 22 January 2016. <https://www.healthcareitnews.com/news/hacktivist-vs-cyberterrorist-understanding-5-enemies-healthcare-it-security>
- Flessas, Christos. “Biggest Insider Threats of 2022: Lessons Learned and Key Takeaways for 2023,” Computer Society. 31 March 2023. <https://www.cybervigilance.uk/post/cyber-weekly-digest-2023-week-6>
- Fraser, Nalani, Fred Plan, Jacqueline O’leary, Vincent Cannon, Raymond Leong, Dan Perez, Chi-En Shen. “APT41: A Dual Espionage and Cyber Crime Operation,” Mandiant. 07 August 2019. <https://www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation>
- Gatlan, Sergui. “Royal ransomware claims attack on Intrado telecom provider,” Bleeping Computer. 28 December 2022. <https://www.bleepingcomputer.com/news/security/microsoft-notorious-fin7-hackers-return-in-clop-ransomware-attacks>





# References

- Guibernau, Francis. “Emulating the Politically Motivated North Korean Adversary Andariel,” AttackIQ. 22 December 2022. <https://www.attackiq.com/2022/12/22/emulating-the-politically-motivated-north-korean-adversary-andariel/>
- Gyongyoşi, Livia. “Major Healthcare Data Breach Impacts U.S. House Members,” Heimdal. 9 March 2023. <https://heimdalsecurity.com/blog/healthcare-data-breach-us-house-members/>
- Hall, Susan. “Healthcare lessons learned from 'hactivist' attack,” Fierce Healthcare. 1 August 2014. <https://www.fiercehealthcare.com/it/healthcare-lessons-learned-from-hactivist-attack>
- “Healthcare Data Security,” Fortinet. n. d. <https://www.fortinet.com/resources/cyberglossary/healthcare-data-security>
- Hegel, Tom. “NoName057(16) – The Pro-Russian Hactivist Group Targeting NATO,” SentinelLabs. 12 January 2023. <https://www.sentinelone.com/labs/noname05716-the-pro-russian-hactivist-group-targeting-nato/>
- Huddleston, Tom. “What is Anonymous? How the infamous ‘hactivist’ group went from 4chan trolling to launching cyberattacks on Russia,” CNBC. 25 March 2022. <https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html>
- “Insider Threat Statistics for 2023: Reports, Facts, Actors, and Costs,” Ekran. 26 April 2023. <https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures>
- Kopecky, Tom. “Why Insider Threats Will Rise In 2023 (and How To Fight Them),” Security Informed. N.d. <https://www.sourcesecurity.com/insights/insider-threats-rise-2023-fight-co-1607083835-ga.1669872931.html>
- Kovacs, Eduard. “U.S. State Governments Targeted by Chinese Hackers via Zero-Day in Agriculture Tool. Securityweek”. Mar 8, 2022. <https://www.securityweek.com/us-state-governments-targeted-chinese-hackers-zero-day-agriculture-tool>
- Lutkevich, Ben. “script kiddie,” Tech Target. N.d. <https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie>
- Maxted, Kathleen. “Cyber Weekly Digest - 2023 Week #6,” Cyber Vigilance. 10 February 2023. <https://www.computer.org/publications/tech-news/trends/key-takeaways-from-2022-cyberthreatseaways-for-2023>





# References

---

- McGee, Marianne Kolbasuk. “Preparing for Hacktivism Tied to US Supreme Court's Ruling,” Gov Info Security. 09 May 2022. <https://www.govinfosecurity.com/interviews/preparing-for-hacktivism-tied-to-us-supreme-courts-ruling-i-5068>
- “Microsoft Azure Warns on Killnet's Growing DDoS Onslaught Against Healthcare,” DarkReading. 17 March 2023. <https://www.darkreading.com/attacks-breaches/microsoft-azure-killnet-dos-onslaught-healthcare>
- Montalbano, Elizabeth. “APT Charming Kitten Pounces on Medical Researchers,” Threat Post. 31 March 2021. <https://threatpost.com/charming-kitten-pounces-on-researchers/165129/>
- Moules, Danny. “A history of hacking and hackers,” Computer Weekly. 25 October 2017. <https://www.computerweekly.com/opinion/A-history-of-hacking-and-hackers>
- Newman, Lily Hay. “Hacktivists Are on the Rise—but Less Effective Than Ever,” WIRED. 2 May 2019. <https://www.wired.com/story/hacktivism-sudan-ddos-protest/>
- “Pro-Russian Hacktivism and Its Role in the War in Ukraine,” Intel471. 19 October 2022. <https://intel471.com/blog/pro-russian-hacktivism-and-its-role-in-the-war-in-ukraine>
- Raja, Sanjay. “2023 Insider Threat Report Finds Three-Quarters of Organizations are Vulnerable to Insider Threats,” Cybersecurity Insiders. N.d. <https://www.cybersecurity-insiders.com/2023-insider-threat-report-finds-three-quarters-of-organizations-are-vulnerable-to-insider-threats/>
- “Silent Chollima,” CrowdStrike. N.d. <https://prod.adversary.crowdstrike.cloud.jam3.net/en-US/adversary/silent-chollima/>
- “Slack security update,” Slack. 9 January 2023. <https://slack.com/intl/en-au/blog/news/slack-security-update>
- SOCRadar Research. “Dark Web Profile: Killnet – Russian Hacktivist Group,” SOCRadar. 16 December 2022. <https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/>





# References

- “Technical details of MoonBounce Implementation,” Kaspersky. N.d. [https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/01/19115831/MoonBounce\\_technical-details\\_eng.pdf](https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/01/19115831/MoonBounce_technical-details_eng.pdf)
- “THE NEW ERA OF HACKTIVISM – STATE-MOBILIZED HACKTIVISM PROLIFERATES TO THE WEST AND BEYOND,” CheckPoint. 29 September 2022. <https://research.checkpoint.com/2022/the-new-era-of-hacktivism/>
- “The Top 10 Dark Web Telegram Chat Groups and Channels,” SOCRadar. 1 June 2023. <https://socradar.io/the-top-10-dark-web-telegram-chat-groups-and-channels/>
- “Threat Intelligence Report,” Fortinet. N.d. <https://www.hipaajournal.com/security-alert-bianlian-ransomware-extortion-group/>
- Uchill, Joe. “Founder of pro-Russian hacktivist Killnet quitting group,” SC Media. 29 July 2022. <https://www.scmagazine.com/analysis/cybercrime/founder-of-pro-russian-hacktivist-killnet-quitting-group>
- Van Arsdale,Carolynn. “The Week in Security: Is Lapsus\$ back in action?,” Reversing Labs. 22 September 2022. <https://www.reversinglabs.com/blog/the-week-in-cybersecurity-lapsus-back-in-action>
- Vijayan, Jai. “US Lawmakers Face Cyberattacks, Potential Physical Harm After DC Health Link Breach,” Dark Reading. 09 March 2023. <https://www.darkreading.com/application-security/us-lawmakers-cyberattacks-physical-harm-dc-health-link-breach>
- WAQAS. “Breach Forums to Remain Offline Permanently,” HackRead. 21 March 2023. <https://www.hackread.com/breach-forums-offline-permanently/>
- “What is a DDoS Attack?,” Digital Attack Map. N.d. <http://www.digitalattackmap.com/understanding-ddos/>
- “What is Hacktivism?,” Check Point.” N.d. <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism/#:~:text=Derived%20from%20combining%20the%20words,politically%20or%20socially%20motivated%20purposes>



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# Questions



# FAQ

---

## Upcoming Briefing

- 07/13 – Artificial Intelligence and Its Application to Healthcare Cybersecurity

## 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](mailto: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.



Office of  
**Information Security**  
Securing One HHS



Health Sector Cybersecurity  
Coordination Center





# 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.



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**

# 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 Current Activity](#)
- [CISA Free Cybersecurity Tools](#)
- [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](#)



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**



# 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**



Office of  
**Information Security**  
Securing One HHS



**Health Sector Cybersecurity  
Coordination Center**

# Contacts



**HHS.GOV/HC3**



**HC3@HHS.GOV**