Russian Threat Actors Targeting the HPH Sector

February 15, 2024
Agenda

• Why Russian Threat Actors Target the United States
• Why Russian Threat Actors Target the U.S. HPH Sector
• Cyber Threat Actor Profiles
• Russian APT Profiles
• Russian Cyber Criminal Group Profiles
• Russian Hacktivists Profiles
• Russian Dark Web Forums
• Best Practices and Mitigation Tactics

• Conclusion
• Relevant HC3 Reports
• Resources
• References

Slides Key:

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

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Why Russian Threat Actors Target the United States
ODNI’s 2023 Annual Threat Assessment

• “...Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities.”

• “...Russia is particularly focused on improving its ability to target critical infrastructure in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis.”

Source: ODNI
Recent History of Attacks by Threat Actors

- Opportunistic, monetary, and geopolitical motivations
- The first offensive cyberattacks were conducted in the 2000s
- The 2016 and 2020 U.S. presidential elections
- 2020 Solar Winds hack
- 2023 DDoS attacks on the HPH sector – KillNet

Source: ZDnet
Why Russian Threat Actors Target the U.S. HPH Sector
Opportunistic Motivations

- “Soft target” due to the life-and-death nature of the industry
- Likelihood of paying ransom
- The COVID-19 pandemic exacerbated attacks on the HPH sector
  - Intellectual property
  - Clinical research
- APT28 and APT29 targeted pharmaceutical companies and clinical researchers
- Different motivations:
  - APTs motivated by access to information (more targeted)
  - Criminal groups financially motivated (prefer ransomware)
  - Hacktivists politically motivated (DDoS attacks)

Source: Science Magazine
Monetary Motivations

• Financially motivated
• Criminal activity online is easier, faster, cheaper, and less risky
• Cyber criminal groups
  ▪ February 2023: 130 orgs attacked from GoAnywhere attack (Cl0p)
  ▪ September 2023: PII stolen from U.S. cardiology organization (NoEscape)
  ▪ October 2023: Attack on one HPH entity with medical services for ~1,000 hospitals and health systems (BlackSuit)

Source: Radio Free Europe/Radio Liberty
Cost of a Data Breach by Industry

- Healthcare experiences the highest data breach costs of all industries.
- Reported the highest costs for the 13th year in a row.
- Increased from $10.10 million in 2022 to $10.93 million in 2023 (increase of 8.2%).
- The healthcare industry has had higher average data breach costs since the start of the COVID-19 pandemic.
Geopolitical Motivations

• Historical focus on government, defense, energy, utilities
• The HPH sector became significant during the COVID-19 pandemic
• 2023 Russia-Ukraine War
  ▪ KillNet DDoS attacks (January 2023)
  ▪ Other Russian hacktivist groups

Source: Air University
Cyber Threat Actor Profiles
# Cyber Threat Actor Characterization/Categorization

<table>
<thead>
<tr>
<th>TYPE</th>
<th>MOTIVATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Political Agenda</td>
</tr>
<tr>
<td>Cybercriminal Groups</td>
<td>Financial Fraud/Theft</td>
</tr>
<tr>
<td>Contractors</td>
<td>Political Agency (Host)</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Political Activism</td>
</tr>
<tr>
<td>Individuals</td>
<td>Any</td>
</tr>
</tbody>
</table>

**Examples:**
- APTs: Turla/Venomous Bear, APT29/Cozy Bear, APT28/Fancy Bear, Sandworm
- Cyber Criminal Groups: Conti, Royal, Black Basta, FIN7
- Contractors: Positive Technologies, Digital Security
- Hacktivists: KillNet, XakNet Team, Anonymous
- Individuals: Edward Snowden, Chelsea Manning

Source: RedLegg
Russian APT Profiles
Known Russian APT Profiles

- Star Blizzard
  - Source: Buzz Meter
- Turla/Venomous Bear
  - Source: CrowdStrike
- APT29/Cozy Bear
  - Source: CrowdStrike
- APT28/Fancy Bear
  - Source: CrowdStrike
- Sandworm/Voodoo Bear
  - Source: CrowdStrike
Star Blizzard/SEABORGIUM

• **Association**: FSB
• **AKA**: Callisto Group, TA446, COLDRIVER, TAG-53, BlueCharlie
• **Known Targets**: Defense and intelligence consulting companies, energy, NGOs, think tanks, and academia
• **Tactics, Techniques, & Procedures (TTPs)**: Spear phishing, credential theft campaigns, social media monitoring, active measures
• **Incidents**: Spear phishing attack campaigns in the United Kingdom and the United States in 2023

Source: Buzz Meter
The FBI’s Cyber Most Wanted: FSB

- FSB officer and co-conspirator behind the Star Blizzard spear phishing campaign against the U.S. and U.K.
  - Unauthorized access to email account credentials
  - Targeted defence, foreign affairs, security policies, and nuclear energy research and development
Turla/Venomous Bear

- **Association**: FSB
- **AKA**: KRYPTON, Waterbug, Snake, Group 88, WRAITH, Uroboros, Pfinet, TAG_0530, Hippo Team, Pacifier APT, Popeye, SIG23, and Iron Hunter
- **Known Targets**: Research organizations and entities in the pharmaceutical, academic, energy, government, military, and telecommunications sectors
- **Tactics, Techniques, & Procedures (TTPs)**: Spear phishing, watering hole attacks, and malicious tools such as Gazer, KopiLuwak, ICEDCOFFEE, Carbon backdoor, Moonlight Maze, Mosquito backdoor, Mimikatz, Outlook backdoor, and LightNeuron backdoor, active measures
- **Incidents**: Germany’s government computer network (2018); Swiss technology company (2014); U.S. Central Command (2008)

Source: CrowdStrike
APT29/Cozy Bear

• **Association:** SVR

• **AKA:** The Dukes, YTTRIUM, and Iron Hemlock

• **Known Targets:** Healthcare, pharmaceutical, academic, energy, financial, government, media, and technology

• **Tactics, Techniques, & Procedures (TTPs):** Phishing attacks; EnvyScout, BoomBox, NativeZone, and VaporRage malware, active measures

• **Incidents:** SolarWinds attack (2020); attacks on COVID-19 vaccine developers (2019-20)

Source: CrowdStrike
APT28/Fancy Bear

- **Association:** GRU

- **AKA:** Group 74, PawnStorm, Sednit, Snakemackerel, Sofacy, STRONTIUM, TG-4127, Tsar Team, and Iron Twilight

- **Known Targets:** Healthcare, aerospace, defense, energy, government, military, and media

- **Tactics, Techniques, & Procedures (TTPs):** Widely used malware such as ADVSTORESHELL, CHOPSTICK, JHUHUGIT, and Xtunnel and custom malware, active measures

- **Incidents:** Microsoft Outlook zero-day exploit (2023); data theft from the Hillary Clinton presidential campaign and the DNC (2016); data theft on World Anti-Doping Agency (2016)

Source: CrowdStrike
Sandworm/Voodoo Bear

- **Association:** GRU
- **AKA:** Sandworm Team, BlackEnergy APT Group, and ELECTRUM
- **Known Targets:** Energy, industrial control systems and SCADA, government, and media
- **Tactics, Techniques, & Procedures (TTPs):** Spear fishing to deliver malware (NotPetya, BlackEnergy, KillDisk, Industroyer), active measures
- **Incidents:** Winter Olympics in Korea (2018); worldwide NotPetya attack (2017); hacking of Ukraine power grid (2015)

Source: Wired
The FBI’s Cyber Most Wanted: GRU

- Six officers from Sandworm (GRU) behind the following cyberattack campaigns:
  - Nerve toxin poisoning investigations (2018)
  - NotPetya malware attacks on hospitals and other medical facilities (2017)
  - Spear phishing campaigns on elections in France (2017)
  - Malware attacks on the Ukrainian government and critical infrastructure (2015-2016)
Russian Cyber Criminal Group Profiles
Russian Cyber Criminal Group Threat Actors

- **Conti**
  - Source: Krebs

- **Royal**
  - Source: Logpoint

- **Black Basta**
  - Source: SOCRadar

- **REvil**
  - Source: Axel

- **LockBit**
  - Source: The Hacker News

- **ALPHV/BlackCat**
  - Source: The Record

- **Cl0p**
  - Source: HackRead

- **BlackMatter**
  - Source: BleepingComputer
Conti

- **Active Since:** 2019 (now disbanded)
- **Type:** RaaS group
- **Known Targets:** Businesses, government organizations, healthcare, financial services providers, educational institutions (organizations with more than $100 million in annual revenue)
- **Tactics, Techniques, & Procedures (TTPs):** Double extortion with aid of affiliates, phishing
- **Ransom:** As high as $25 million
- **Incidents:** Attacks on U.S. healthcare and first responder networks (2021); Health Services Executive in Ireland (2021); District Health Board in New Zealand (2020)

Source: Bank Info Security
Royal

**Active Since:** 2022 (likely a rebrand of Conti)

**Type:** Non-RaaS group (no affiliates)

**Known Targets:** Transportation, manufacturing, technology, government, healthcare

**Tactics, Techniques, & Procedures (TTPs):** Double extortion, phishing, remote desktop protocol (RDP), public-facing applications, brokers

**Ransom:** $250,000 - $2 million

**Incidents:** Attacks on the city of Dallas 911 center (2023)

**Associations:** Blacksuit?

Source: Logpoint
Black Basta

**Active Since:** 2022 (possible rebrand of Conti)

**Type:** RaaS Group

**Known Targets:** Construction, manufacturing, healthcare

**Tactics, Techniques, & Procedures (TTPs):**
Double extortion, phishing, RDP, web injections, malicious downloads

**Ransom:** $1.2 million average

**Incidents:** Attacks on U.S.-based health information technology, healthcare industry services, laboratory and pharmaceutical, and health plans organizations (2022)

**Associations:** Conti, FIN7, and BlackMatter?
LockBit

- **Active Since:** September 2019
- **Type:** RaaS group
- **Known Targets:** Small- and medium-sized businesses in education, finance, healthcare, internet software and services, manufacturing, and professional services
- **Tactics, Techniques, & Procedures (TTPs):** Phish and spear phishing, brute force attacks
- **Ransom:** $1,000 - $1 million
- **Incidents:** Papercut vulnerability (2023); dental insurer attack (2023); cancer patient data breach (2023); multi-state healthcare network (2023)

Source: The Hacker News
ALPHV

- **Active Since:** November 2021
- **AKA:** BlactCat, Noberus, AlphaV, AlphaVM, ALPHV-ng
- **Type:** RaaS Group
- **Known Targets:** Financial, manufacturing, legal, healthcare, pharmaceutical, and professional services
- **Tactics, Techniques, & Procedures (TTPs):** Triple extortion, spear phishing, brute force, stolen credentials; unpatched vulnerabilities
- **Ransom:** $400,000 - $3 million
- **Incidents:** Health IT solutions provider (2023); breast cancer patient data leak (2023)

Source: The Record
ALPHV Targeted by Law Enforcement

• Group’s victim leak site seized by joint international law enforcement effort (Dec. 19, 2023).

• Follows numerous incidents of victim site disruption in December 2023.

• Pivoting of affiliates towards other RaaS offerings.

• ALPHV claims seized infrastructure is not used and outdated.

• Significantly reduced attack tempo?

Source: The Record
ClOp

- **Active Since:** 2019
- **Type:** RaaS Group
- **Known Targets:** Banking, retail, healthcare, telecommunications, transportation
- **Tactics, Techniques, & Procedures (TTPs):** Spear phishing, zero-day exploitation, compromised RDP, ransomware, data exfiltration, and multi-extortion
- **Ransom:** As high as $220,000
- **Incidents:** GoAnywhere zero-day (2023); MOVEit zero-day (2023); papercut vulnerability (2023)

Source: IronScales
Russian Hacktivist Profiles
What is Russian Hacktivism?

• Russian hacktivism is crowd-funded cyber terrorism.

• Hacktivists present themselves as quasi-military organizations.

• Solicit donations in cryptocurrency on social media channels (i.e., Telegram).

• Administrators → Volunteers → DDoS attacks

• Typical attack duration lasts 30 minutes.

• Increase in Russian hacktivists since the start of the Russia-Ukraine War.

Source: KillNet Telegram
Russian Hacktivist Threat Actors

<table>
<thead>
<tr>
<th>KillNet</th>
<th>Anonymous Russia</th>
<th>Anonymous Sudan</th>
<th>Legion Russia Cyber Special Forces</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="KillNet Logo" /></td>
<td><img src="image" alt="Anonymous Russia Logo" /></td>
<td><img src="image" alt="Anonymous Sudan Logo" /></td>
<td><img src="image" alt="Legion Russia Cyber Special Forces Logo" /></td>
</tr>
<tr>
<td>Source: Atlas News</td>
<td>Source: Telegram</td>
<td>Source: BBC</td>
<td>Source: Telegram</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Special Forces Archangel ZRU</th>
<th>XakNet Team</th>
<th>CombatOsint</th>
<th>KillMilk</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Special Forces Archangel ZRU Logo" /></td>
<td><img src="image" alt="XakNet Team Logo" /></td>
<td><img src="image" alt="CombatOsint Logo" /></td>
<td><img src="image" alt="KillMilk Logo" /></td>
</tr>
<tr>
<td>Source: Telegram</td>
<td>Source: X (Twitter)</td>
<td>Source: Telegram</td>
<td>Source: TGStat</td>
</tr>
</tbody>
</table>
KillNet

- **Active Since:** January 2022
- **Type:** Hacktivist group
- **Motivations:** Pro-Russia; anti-U.S., NATO, and Ukraine
- **Known Targets:** U.S., NATO and allies, Ukraine, non-CIS countries
- **Tactics, Techniques, & Procedures (TTPs):** DDoS attacks, active measures
- **Incidents:** DDoS attacks on 91 U.S. HPH entities (January 2023)

*Source: Telegram (KillMilk)*
KillNet’s January 23, 2023 DDoS Attacks

Number of HPH Organizations by Trauma Level Targeted by KillNet DDoS Attack on 28JAN2023 (n=91)

Source: HC3
**KillNet’s Online Presence**

- Private military hacking company
- Affiliates and volunteers
- Active measures (COVID-19 disinformation campaign)
- Open-source situational awareness
- Memes, gifs, emojis, short edited videos
Russian Dark Web Forums
Hacking Forums and the Dark Web

• Similar to clear web counterparts (avoid surveillance or censorship).
• Outlet to coordinate, exchange information, and conduct illicit trades.
• Often hosted on the dark web.
• Structure includes:
  ▪ Marketplace section (stolen credentials, RaaS, and malware)
  ▪ Cybercrime discussion section
• 74% of ransomware revenue goes to Russia-linked threat actors. (Source: BBC)
• **Recommendation:** Monitor cybercrime forums for mentions of your organization.

Source: Peraton
Healthcare Industry Related Dark Web Posts in the United States

- 38% global rise in healthcare-related dark web posts from 2021-2022.
- Over 450 documented posts.
- In 2022, 119 U.S. healthcare industry-related posts were reported.

Source: SOCRadar

- Dark web posts targeting the U.S. HPH sector about buying, selling, and sharing illegal access to systems.
- In 70% of HPH data cases, threat actors were interested in already-compromised data.
- 27.5% of cases were focused on unauthorized access to health systems.

Source: SOCRadar
XSS.is

- **Active Since:** November 2004
- **Content:** Sections include hacking, exploits, zero-day vulnerabilities, malware, corporate access, database leaks, and competitive intelligence.
- **Utilization:** Recruitment and PR tool for RaaS groups (banned in 2021), forum for illegal topics (hacking/financial fraud)
- **Number of Posts (Past Year):** 59.7k
- **Active Users (Past Year):** 6.1k
- **Dark Web Networks:** Tor, ClearWeb
- **Predominant Language:** Russian
- **Known Actors:** ALPHV, Avaddon, Scourge, TheColorYellow, greenmount, 2fast, m1x, S0en, Bit Bond, Ezios, MartinRigz, l3g0l4s, Rakuda

Source: Security Boulevard
Exploit.in

- **Active Since:** 2005
- **Content:** Sections include hacking, scamming, marketplace (stolen credit card info, malware, zero-day exploits), and RaaS schemes
- **Utilization:** Professional network for career cybercriminals, access to U.S. critical infrastructure
- **Number of Posts (Past Year):** 67.7k
- **Active Users (Past Year):** 6.4k
- **Dark Web Networks:** Tor, ClearWeb
- **Predominant Language:** Russian
- **Known Actors:** ALPHV

*Source: Security Boulevard*
RAMP 2.0

- **Active Since:** July 2021
- **Content:** Sections include malware, partner programs for ransomware gangs, and selling access to corporate accounts.
- **Utilization:** Cybercrime-focused agenda
- **Access:** Must be an active member of Exploit or XSS for at least two months
- **Dark Web Networks:** Tor
- **Predominant Language:** Russian, Mandarin, English
- **Known Actors:** Babuk, ALPHV

Source: SOCRadar
FreeHacks

- **Active Since:** 2014
- **Content:** Sections for hacking and security, botnet, DDoS, malware and exploits, hacker world news
- **Utilization:** Key resource for Russian hacking methods to maximize efficiency
- **Access:** User skills and proficiency tested upon request
- **Active Users:** Almost 5,000 (~2018)
- **Dark Web Networks:** Tor
- **Predominant Language:** Russian
- **Known Actors:** Unknown

Source: The Guardian
Case Study: Exploit.in

- Data from more than 100 companies across 18 industries was sold on Russian hacking forums over a three-month period (1 HPH victim).
- Initial Access Brokers (IABs) operate and specialize in these forums.
- 36% of all listings were U.S. companies, often U.S. critical infrastructure.
- Average price of corporate IT access was $1,328.
- Lack of backup systems or access to backup systems often advertised in posts signalling potential ransomware attack.
- Individual threat actors often omit certain types of data and ask to use Telegram to evade law enforcement and threat intelligence providers.
Case Study: Exploit.in, cont.

• **Type/Тип доступа** – Describes the type of access obtained (RDP or VPN access)

• **Industry/Деятельность** – Describes the industry of the victim company

• **Access Level/Права** – Describes the level of privileges obtained

• **Revenue** – Describes the revenue of the victim company

• **Host Online** – Often describes the number of hosts from the victim

• **Start** – The starting price of the action

• **Step** – The bid increments

• **Blitz** – The buy-it-now price

Source: Flare
Best Practices and Mitigation Techniques
Technical Details

- Vulnerabilities known to be exploited by Russian APT groups for initial access include:
  - CVE-2023-42793 Team City software
  - CVE-2023-23397 Microsoft Outlook
  - CVE-2022-34721 Microsoft IKE Protocol
  - CVE-2021-26855 Microsoft Exchange
  - CVE-2021-34527 Windows Print Spooler
  - CVE-2020-14882 Oracle WebLogic
  - CVE-2020-0688 Microsoft Exchange

- Sophisticated tradecraft and cyber capabilities by:
  - Compromising third-party infrastructure
  - Compromising third-party software
  - Developing and deploying custom malware

- Demonstrated ability to maintain persistent, undetected, long-term access in compromised environments by using legitimate credentials.

- Targeted operational technology (OT)/industrial control systems (ICS) networks with destructive malware
CISA’s Known Exploited Vulnerabilities Catalog

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

Source: CISA
Detection and Incident Response

• Detection:
  ▪ Implement robust log collection and retention
  ▪ Look for behavioral evidence or network and host-based artifacts
  ▪ Take note of unexpected equipment behavior
  ▪ Record delays or disruptions in communication with field equipment or other OT devices

• Incident Response:
  ▪ Immediately isolate affected systems
  ▪ Secure backups
  ▪ Collect and review relevant logs, data, and artifacts
  ▪ Consider soliciting support from a third-party IT organization
  ▪ Report incidents to CISA and/or the FBI
# MITRE ATT&CK

## Reconnaissance
- 10 techniques
- Acquire Access
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned

## Resource Development
- 8 techniques
- Acquire Access
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned

## Initial Access
- 10 techniques
- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Executable File

## Execution
- 14 techniques
- Cloud Administration Command
- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Serverless Execution
- Shared Modules

## Persistence
- 20 techniques
- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- Event Triggered Execution (10)

## Privilege Escalation
- 14 techniques
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification
- Execution Guards
- Modify Authentication Processes
- Multi-Factor Authentication
- File and Directory

## Defense Evasion
- 43 techniques
- ADV (1)
- Application Token Manipulation
- BITS Jobs
- Build Image on Host
- Builder Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification
- Execution Guards
- Modify Authentication Processes
- Multi-Factor Authentication
- File and Directory

## Credential Access
- 17 techniques
- Adversary in the Middle
- Brute Force
- Credential from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Processes
- Multi-Factor Authentication
- File and Directory

## Discovery
- 32 techniques
- Account Discovery
- Application Token Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust

## Lateral Movement
- 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Service (1)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content

## Collection
- 17 techniques
- Adversary in the Middle
- Archive Collected Data
- Communication Through Removable Media
- Data Injection
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Failback Channel
- HTTPS
- Ingress Tool Transfer

## Command and Control
- 17 techniques
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository
- Data from Information Repositories

## Exfiltration
- 9 techniques
- Advanced Exfiltration
- Data Transfer Stealer
- Exfiltration Over Approved Protocols
- Exfiltration Over C2 Channel
- Exfiltration Over Other Physical Medium
- Exfiltration Over Other Medium
- Exfiltration Over Physical Medium
- Shadow Access
- Website Access

---

**Source:** MITRE ATT&CK

---

**Office of Information Security**
**Securing One HHS**

**Health Sector Cybersecurity Coordination Center**
Mitigations

• Be prepared:
  - Confirm reporting processes and minimize coverage gaps
  - Create, maintain, and exercise a Cyber Incident Response, Resilience Plan, and Continuity of Operations Plan

• Enhance your organization’s cyber posture:
  - Identity and access management
  - Protective controls and architecture
  - Vulnerability and configuration management

• Increase organizational vigilance
Conclusion
Summary

- Opportunistic, monetary and geopolitical motivations
- Will likely continue to target critical infrastructure
- Overabundance of Russian cyber threat actors
- HPH sector perceived to be weak and likely to pay ransoms
- Dark web forums will continue to sell stolen data
Relevant HC3 Reports
Relevant HC3 Reports

- HC3: Alert – BlackCat/ALPHV Ransomware Indicators of Compromise (April 26, 2022)
- HC3: Alert – Conti Ransomware Amplify Alert (September 30, 2021)
- HC3: Alert – Conti Ransomware (Update) (March 10, 2022)
- HC3: Alert – Indicators of Compromise Associated with LockBit 2.0 Ransomware and Additional Mitigations (February 7, 2022)
- HC3: Alert - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (May 9, 2022)
- HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (January 11, 2022)
- HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (March 1, 2022)
Relevant HC3 Reports, cont.

- **HC3: Analyst Note – 8Base Ransomware** (November 1, 2023)
- **HC3: Analyst Note – BlackSuit Ransomware** (November 6, 2023)
- **HC3: Analyst Note – Cl0p Poses Ongoing Risk to HPH Organizations** (March 23, 2021)
- **HC3: Analyst Note – Cl0p Poses Ongoing Risk to HPH Organizations** (November 16, 2020)
- **HC3: Analyst Note – Clop Ransomware** (January 4, 2023)
- **HC3: Analyst Note – Cyber Threat Posed by BlackMatter RaaS Reduced to Guarded (Blue)** (January 28, 2022)
- **HC3: Analyst Note – Healthcare Sector DDoS Guide** (February 13, 2023)
- **HC3: Analyst Note – Hive Ransomware** (April 18, 2022)
- **HC3: Analyst Note – KillNet’s Targeting of the Health and Public Health Sector (December 2022-March 2023)** (April 5, 2023)
- **HC3: Analyst Note – LockBit 3.0 Ransomware** (December 12, 2022)
- **HC3: Analyst Note – MedusaLocker Ransomware** (February 24, 2023)
- **HC3: Analyst Note – NoEscape Ransomware** (October 12, 2023)
- **HC3: Analyst Note – Overview of Conti Ransomware** May 25, 2021
- **HC3: Analyst Note – Pro-Russian Hacktivist Group ‘KillNet’ Threat to HPH Sector** (January 30, 2023)
Relevant HC3 Reports, cont.

- HC3: Analyst Note – Pro-Russian Hacktivist Group ‘KillNet’ Threat to HPH Sector (December 22, 2022)
- HC3: Analyst Note – Royal Ransomware (December 7, 2022)
- HC3: Analyst Note – The Russia-Ukraine Cyber Conflict and Potential Threats to the U.S. Health Sector (March 1, 2022)
- HC3: Sector Alert – Cl0p Allegedly Targets Healthcare Industry in Data Breach (February 22, 2023)
- HC3: Sector Alert – LockBit 3.0 Exploiting Citrix Bleed Vulnerability (November 22, 2023)
- HC3: Sector Alert – New Data Breaches from cl0p and LockBit Ransomware Groups (April 28, 2023)
- HC3: Sector Alert – New Phishing Campaign Launched by SOLARWINDS Attackers (May 28, 2021)
- HC3: Sector Alert – Rhysida Ransomware (August 4, 2023)
- HC3: Threat Actor Profile – Threat Actor Profile: Black Basta (March 15, 2023)
- HC3: Threat Actor Profile – Threat Actor Profile: Evil Corp (AKA UNC2165) (August 29, 2022)
- HC3: Threat Actor Profile – Threat Actor Profile: FIN11 (June 13, 2023)
- HC3: Threat Briefing – An Analysis of the Russia/Ukraine Conflict (May 17, 2022)
Relevant HC3 Reports, cont.

- HC3: Threat Briefing – APT and Cybercriminal Targeting of HCS (June 9, 2020)
- HC3: Threat Briefing – Conti Ransomware and the Health Sector (July 8, 2021)
- HC3: Threat Briefing – Demystifying BlackMatter (September 2, 2021)
- HC3: Threat Briefing – Hive Ransomware (October 21, 2021)
- HC3: Threat Briefing – LockBit Ransomware (September 23, 2021)
- HC3: Threat Briefing – Major Cyber Organizations of the Russian Intelligence Services (May 19, 2022)
- HC3: Threat Briefing – Revil/Sodinokibi Ransomware vs. The Health Sector (August 19, 2021)
- HC3: Threat Briefing – Royal & BlackCat Ransomware: The Threat to the Health Sector (January 12, 2023)
- HC3: Threat Briefing – Social Media Attacks (June 4, 2020)
Resources
### HC3 and Partner Resources

<table>
<thead>
<tr>
<th>Health Sector Cybersecurity Coordination Center (HC3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HC3 Products</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>405(D) Program and Task Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 405(D) Resources</td>
</tr>
<tr>
<td>• 405(D) Health Industry Cybersecurity Practices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Food and Drug Administration (FDA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FDA Cybersecurity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybersecurity and Infrastructure Security Agency (CISA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISA Stop Ransomware</td>
</tr>
<tr>
<td>• CISA Free Cybersecurity Tools</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Federal Bureau of Investigation (FBI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FBI Cybercrime</td>
</tr>
<tr>
<td>• FBI Internet Crime Complaint Center (IC3)</td>
</tr>
<tr>
<td>• FBI Ransomware</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Health Sector Coordinating Council (HSCC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HSCC Recommended Cybersecurity Practices</td>
</tr>
<tr>
<td>• HSCC Resources</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Health – Information Sharing and Analysis Center (H-ISAC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare</td>
</tr>
<tr>
<td>• H-ISAC White Papers</td>
</tr>
</tbody>
</table>
References


References, cont.


References, cont.


References, cont.


References, cont.

References, cont.


References, cont.


References, cont.


References, cont.

• Santos, Doel, Daniel Bunce, and Anthony Galiette. “Threat Assessment: Royal Ransomware.” Unit 42. May 9, 2023. https://unit42.paloaltonetworks.com/royal-ransomware/


References, cont.


References, cont.

Questions
FAQ

Upcoming Briefing

• March 14, 2024 – 2023 Healthcare Cybersecurity Year-In-Review and 2024 Look-Ahead

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

<table>
<thead>
<tr>
<th>Sector and Victim Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alerts and Analyst Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Briefings</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
CPE Credits

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


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.
Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV