Russian Threat Actors Targeting the HPH Sector

February 15, 2024

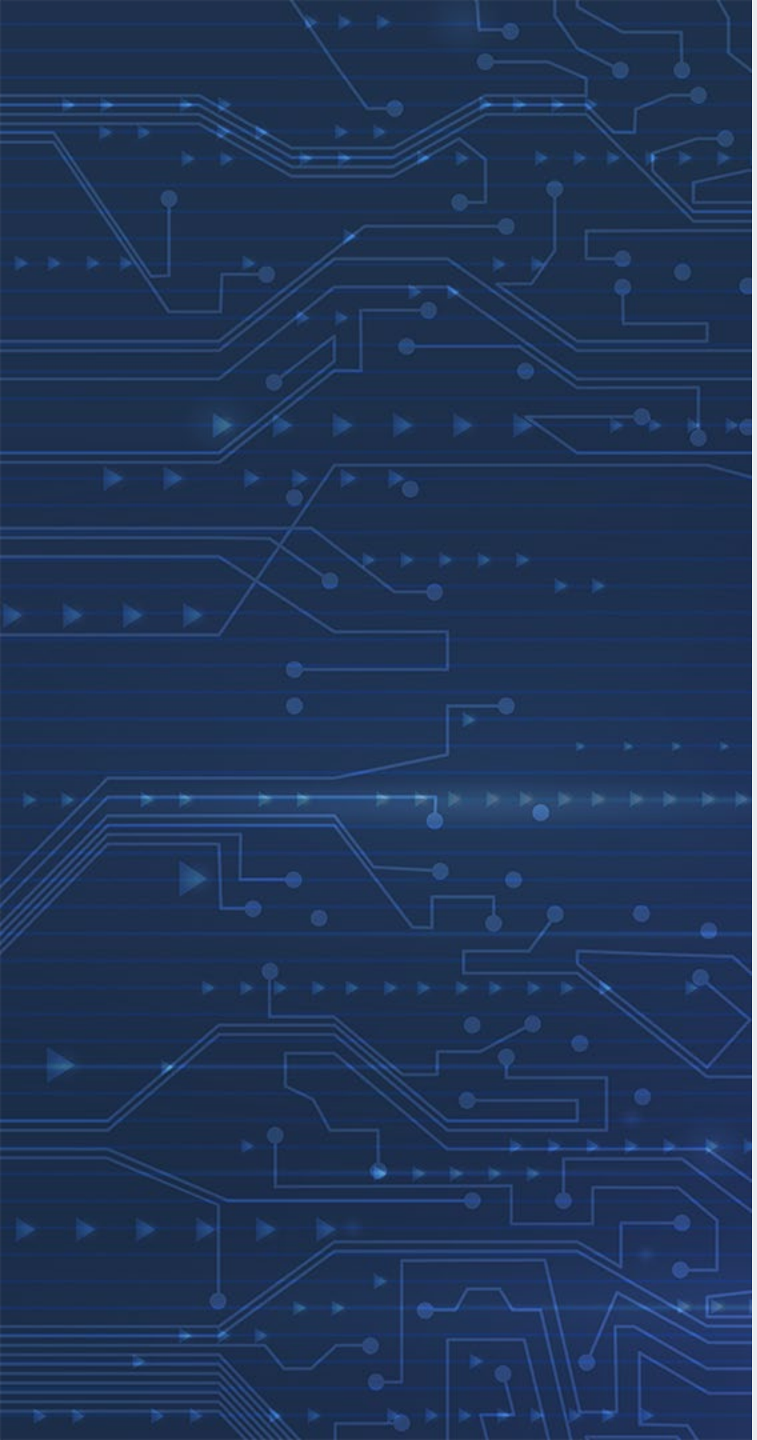
Agenda

- 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)

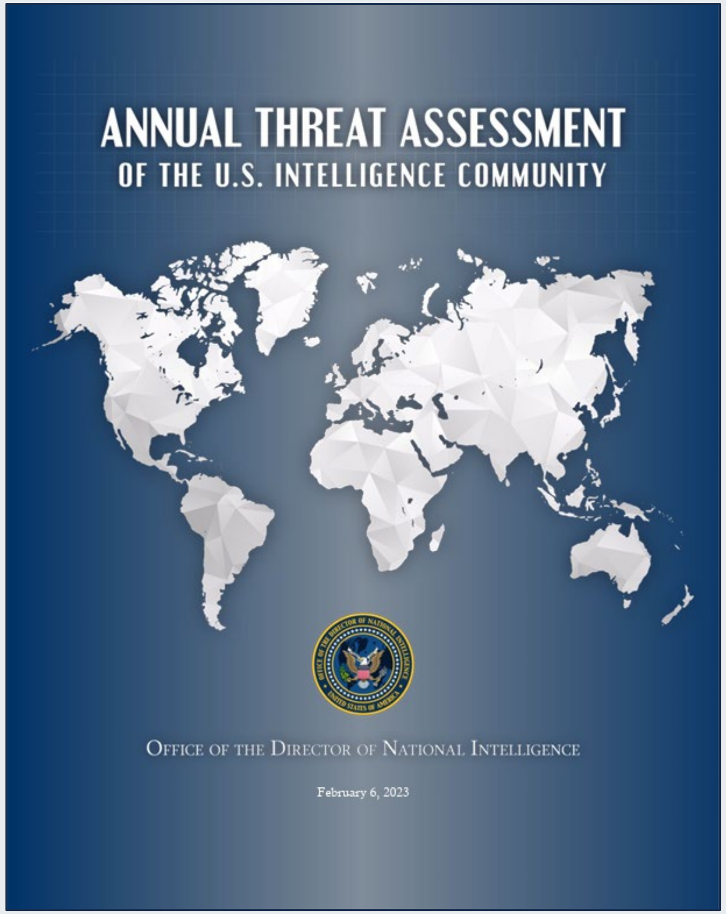
Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



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.”



ANNUAL THREAT ASSESSMENT

OF THE U.S. INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence

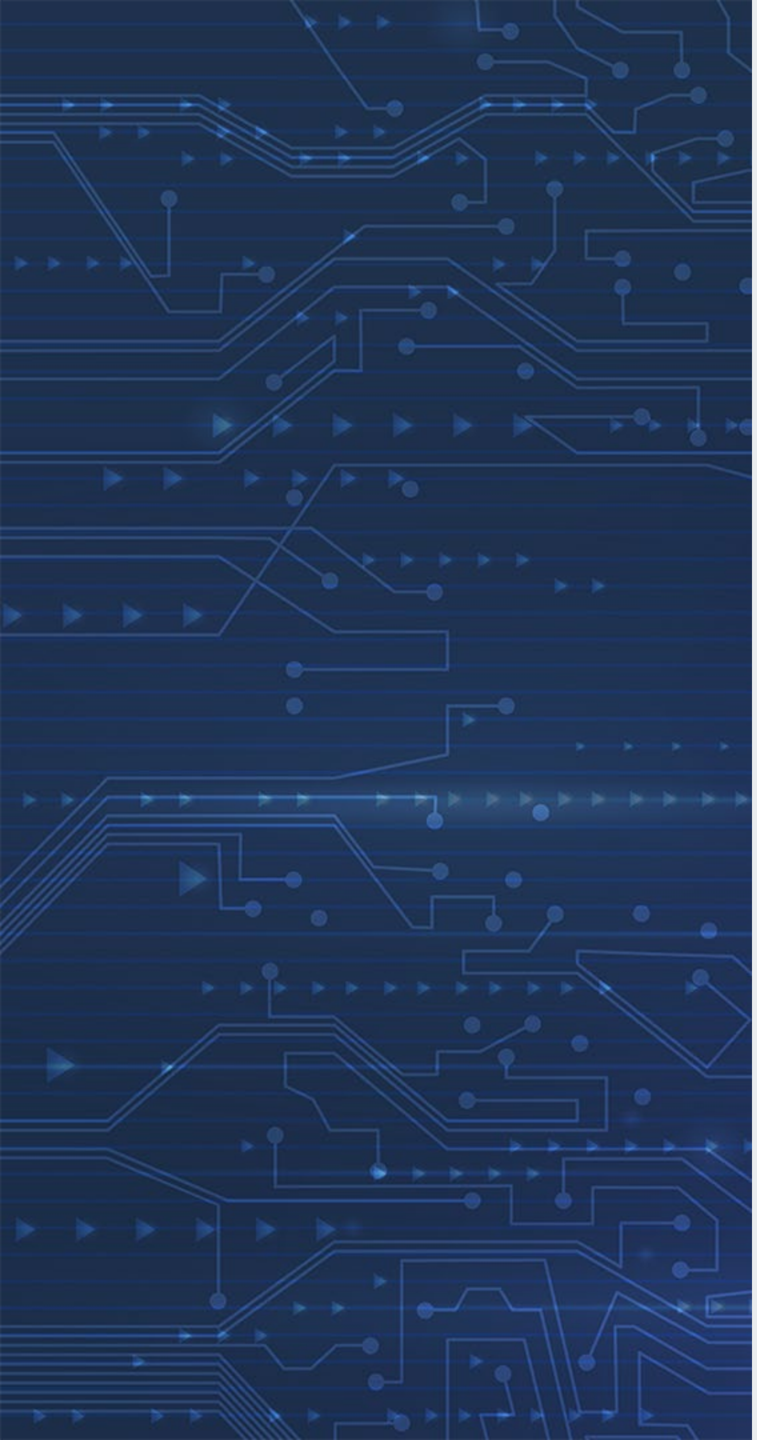
February 6, 2023

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.

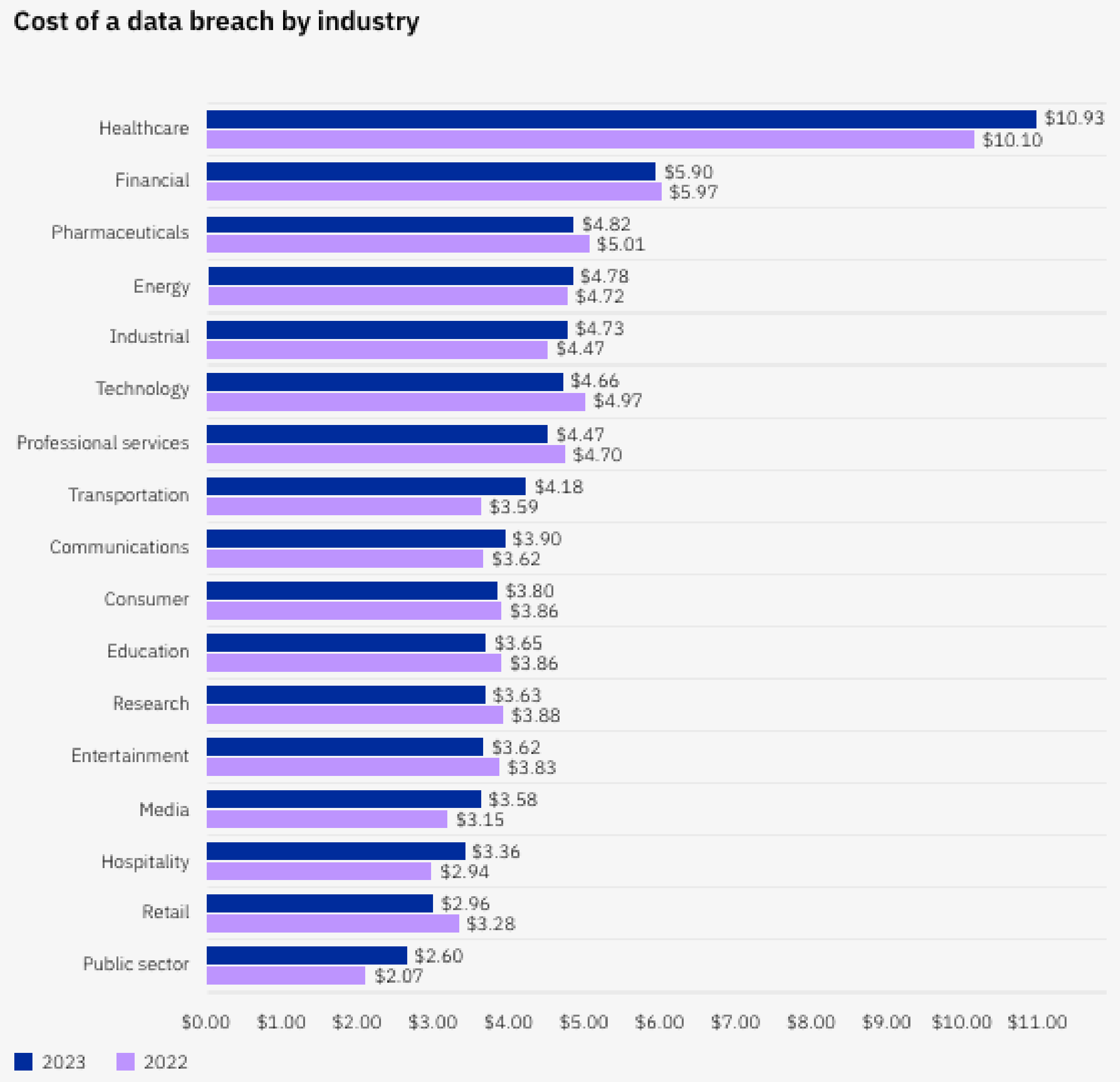


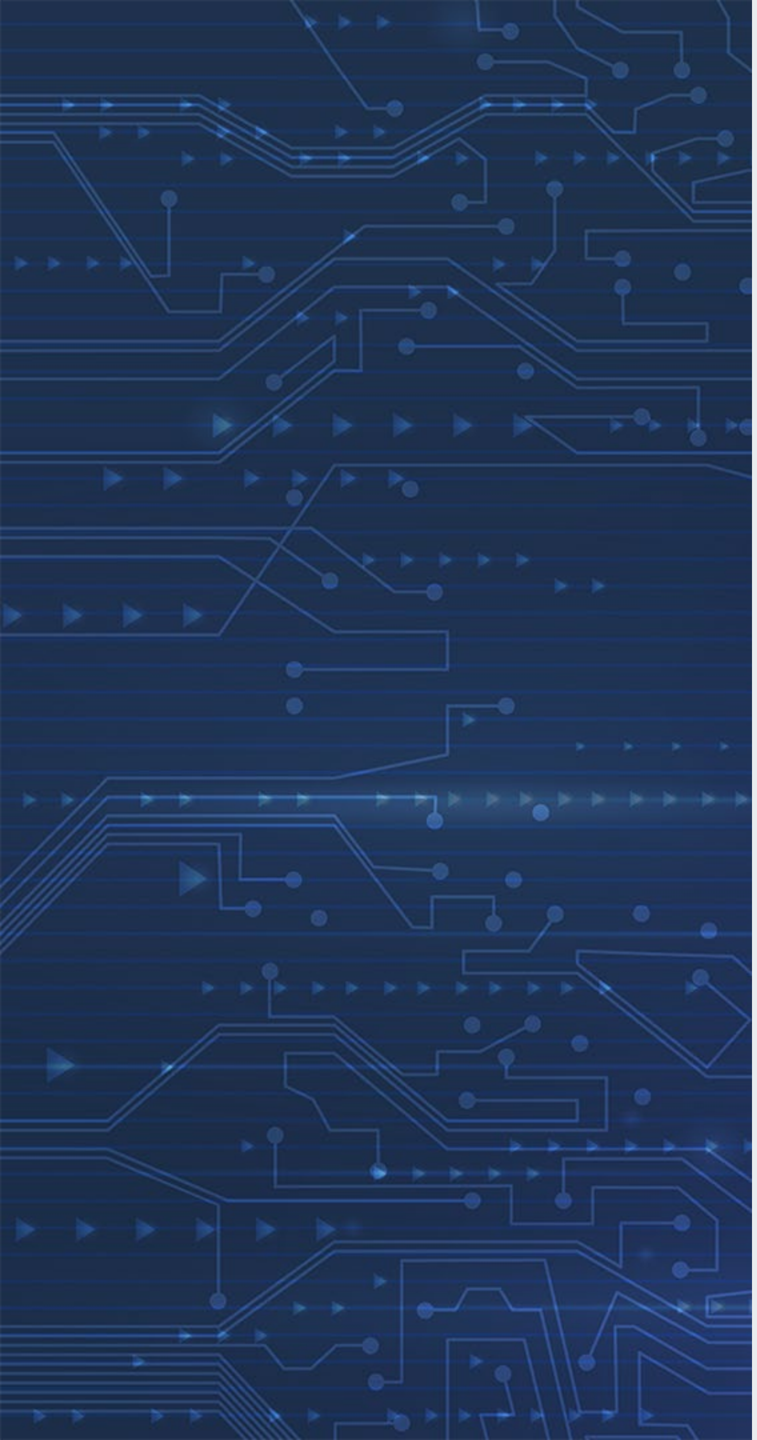
Figure 4. Measured in USD millions

Source: IBM – "Cost of a Data Breach Report 2023"

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



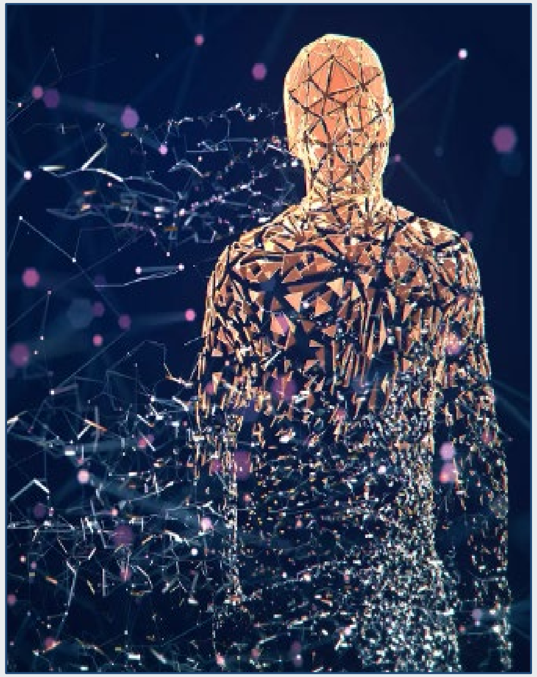
Cyber Threat Actor Profiles

Cyber Threat Actor Characterization/Categorization

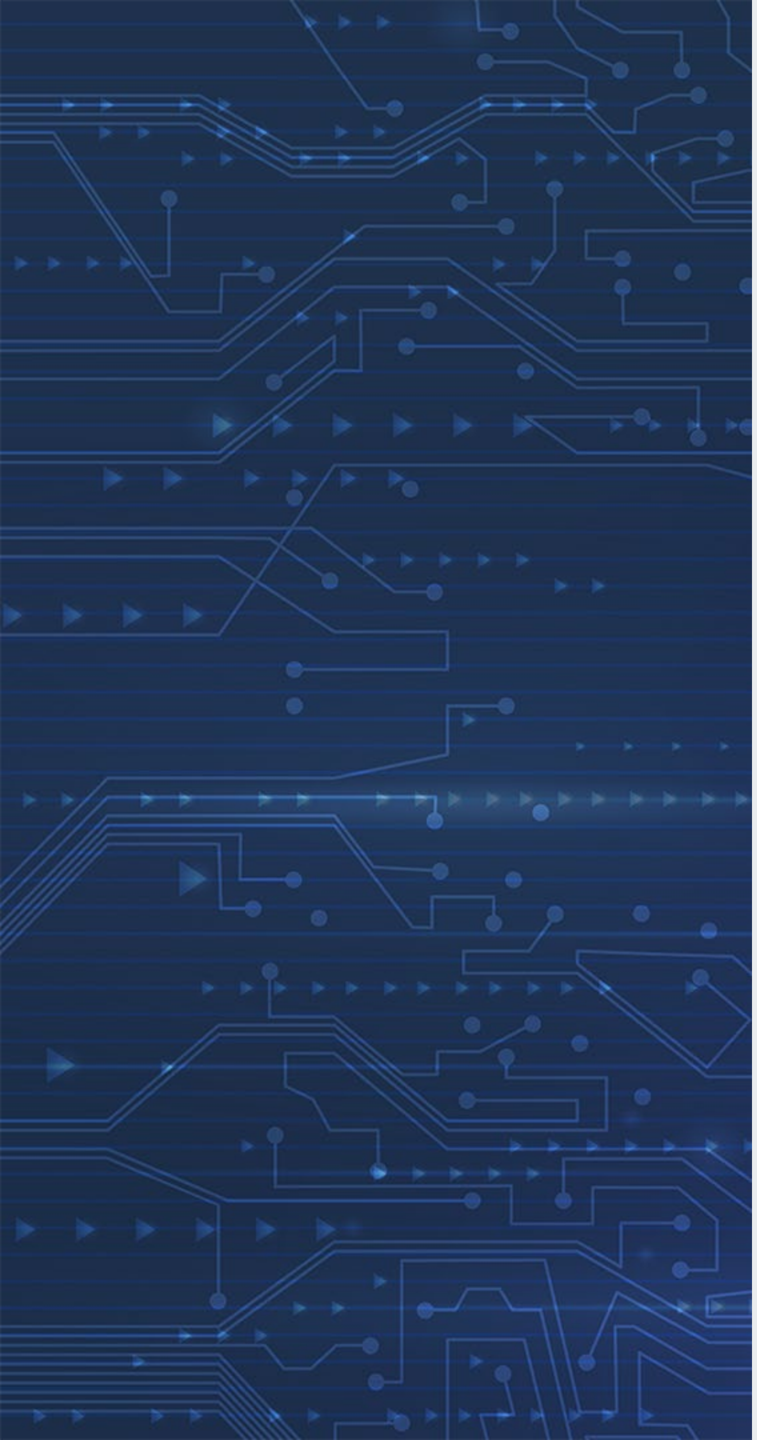
TYPE	MOTIVATION
Advanced Persistent Threat	Political Agenda
Cybercriminal Groups	Financial Fraud/Theft
Contractors	Political Agency (Host)
Hacktivists	Political Activism
Individuals	Any

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

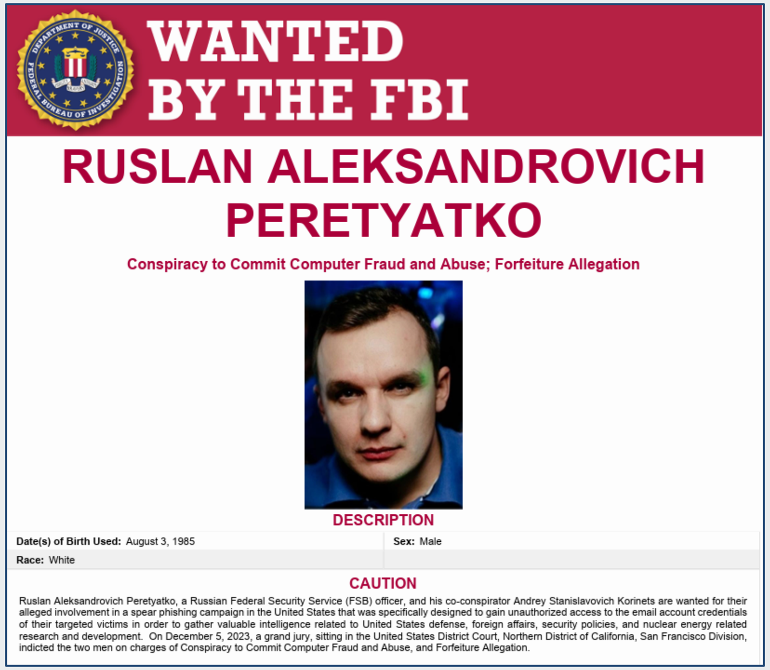
Star Blizzard/SEABORGIUM

- **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



WANTED BY THE FBI

RUSLAN ALEKSANDROVICH PERETYATKO

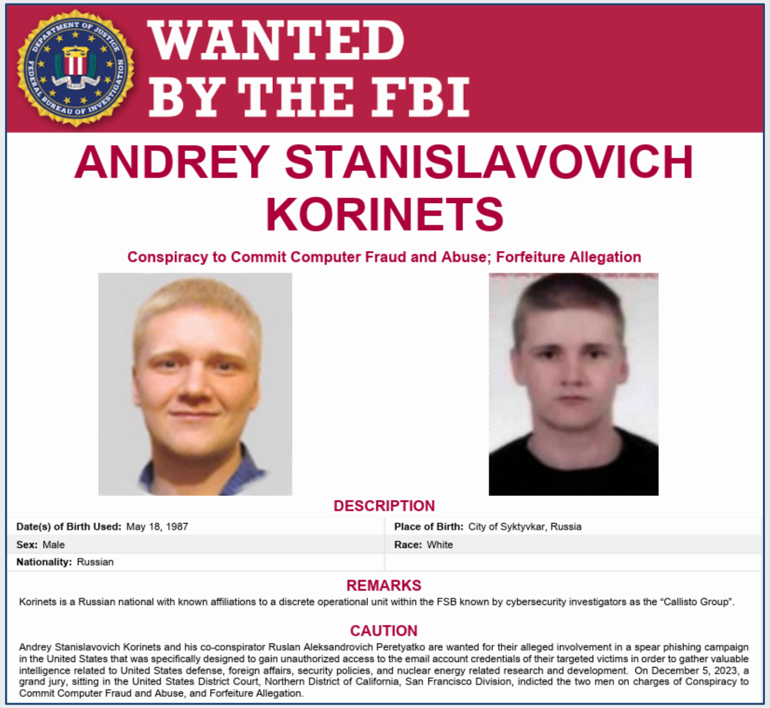
Conspiracy to Commit Computer Fraud and Abuse; Forfeiture Allegation

DESCRIPTION

Date(s) of Birth Used: August 3, 1985	**Sex:** Male
Race: White	

CAUTION

Ruslan Aleksandrovich Peretyatko, a Russian Federal Security Service (FSB) officer, and his co-conspirator Andrey Stanislavovich Korinets are wanted for their alleged involvement in a spear phishing campaign in the United States that was specifically designed to gain unauthorized access to the email account credentials of their targeted victims in order to gather valuable intelligence related to United States defense, foreign affairs, security policies, and nuclear energy related research and development. On December 5, 2023, a grand jury, sitting in the United States District Court, Northern District of California, San Francisco Division, indicted the two men on charges of Conspiracy to Commit Computer Fraud and Abuse, and Forfeiture Allegation.



WANTED BY THE FBI

ANDREY STANISLAVOVICH KORINETS

Conspiracy to Commit Computer Fraud and Abuse; Forfeiture Allegation

DESCRIPTION

Date(s) of Birth Used: May 18, 1987	**Place of Birth:** City of Syktyvkar, Russia
Sex: Male	**Race:** White
Nationality: Russian	

REMARKS

Korinets is a Russian national with known affiliations to a discrete operational unit within the FSB known by cybersecurity investigators as the "Callisto Group".

CAUTION

Andrey Stanislavovich Korinets and his co-conspirator Ruslan Aleksandrovich Peretyatko are wanted for their alleged involvement in a spear phishing campaign in the United States that was specifically designed to gain unauthorized access to the email account credentials of their targeted victims in order to gather valuable intelligence related to United States defense, foreign affairs, security policies, and nuclear energy related research and development. On December 5, 2023, a grand jury, sitting in the United States District Court, Northern District of California, San Francisco Division, indicted the two men on charges of Conspiracy to Commit Computer Fraud and Abuse, and Forfeiture Allegation.

Turla/Venomous Bear

- **Association**: FSB
- **AKA**: KRYPTON, Waterbug, Snake, Group 88, WRAITH, Uroburos, 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

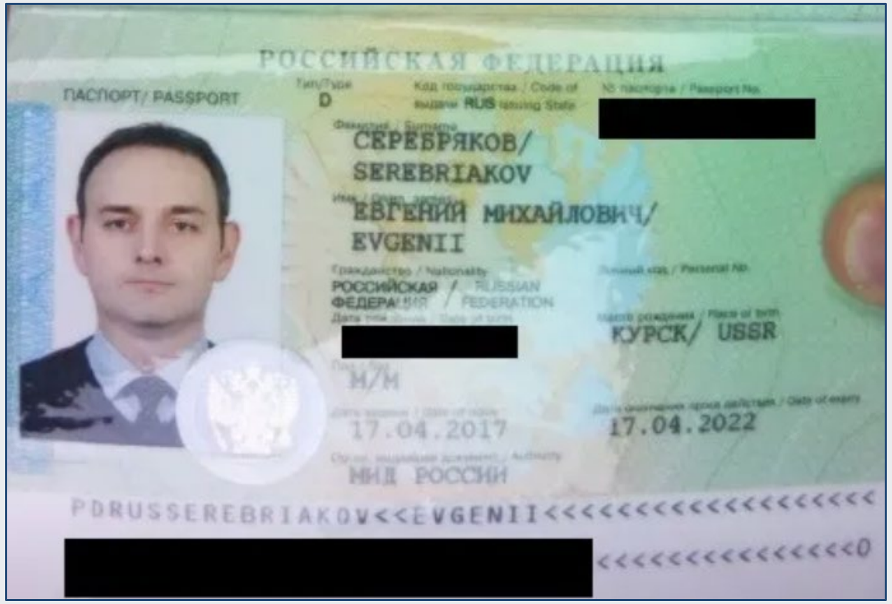
APT28/Fancy Bear

- **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)



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАСПОРТ/ PASSPORT

Тип/Type
D

Код государства / Code of
выдачи RUS issuing State

№ паспорта / Passport No.
[redacted]

Фамилия / Surname
СЕРЕБРЯКОВ/
SEREBRIAKOV

Имя / Given names
ЕВГЕНИЙ МИХАЙЛОВИЧ/
EVGENII

Гражданство / Nationality
РОССИЙСКАЯ / RUSSIAN
ФЕДЕРАЦИЯ / FEDERATION

Личный код / Personal No.

Дата рождения / Date of birth
[redacted]

Место рождения / Place of birth
КУРСК/ USSR

Пол / Sex
М/M

Дата выдачи / Date of issue
17.04.2017

Дата окончания срока действия / Date of expiry
17.04.2022

Орган, выдавший документ / Authority
МИД РОССИИ

PDRUSSEREBRIAKOV<<EVGENII<<<<<<<<<<<<<<<<<<<

[redacted]<<<<<<<<<<<<<<<<0

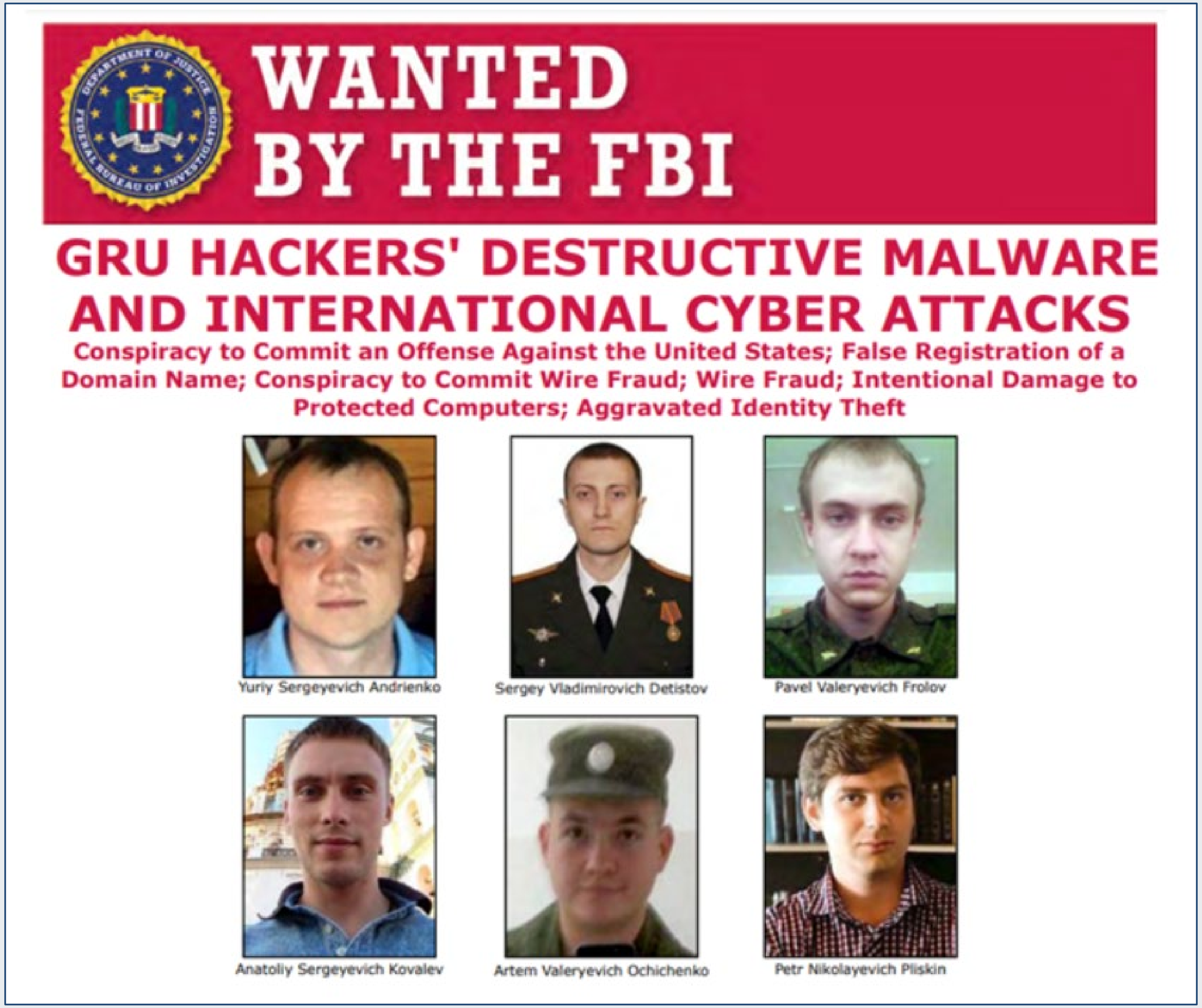
Source: Wired

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

The FBI’s Cyber Most Wanted: GRU

- Six officers from Sandworm (GRU) behind the following cyberattack campaigns:
  - Nerve toxin poisoning investigations (2018)
  - Olympic Destroyer malware attacks on PyeongChang Winter Olympics (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)



WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

Yuriy Sergeyevich Andrienko

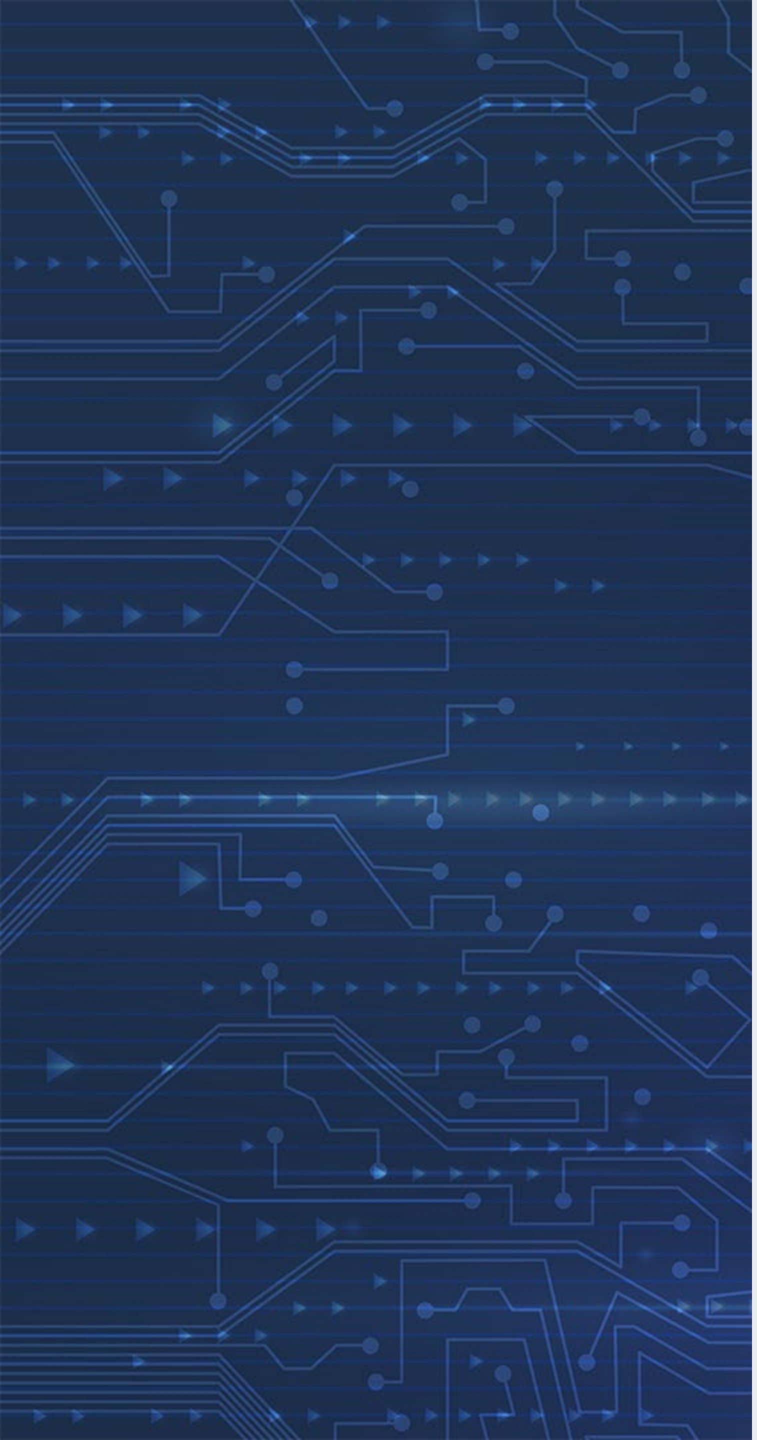
Sergey Vladimirovich Detistov

Pavel Valeryevich Frolov

Anatoliy Sergeyevich Kovalev

Artem Valeryevich Ochichenko

Petr Nikolayevich Pliskin



Russian Cyber Criminal Group Profiles

Russian Cyber Criminal Group Threat Actors

Conti

Source: Krebs

Royal

Royal

Please read carefully the "readme" file you got from us.
If you still have a problem, use our contact form.

Source: Logpoint

Black Basta

Source: SOCRadar

REvil

Source: Axel

LockBit

Source: The Hacker News

ALPHV/BlackCat

Source: The Record

Cl0p

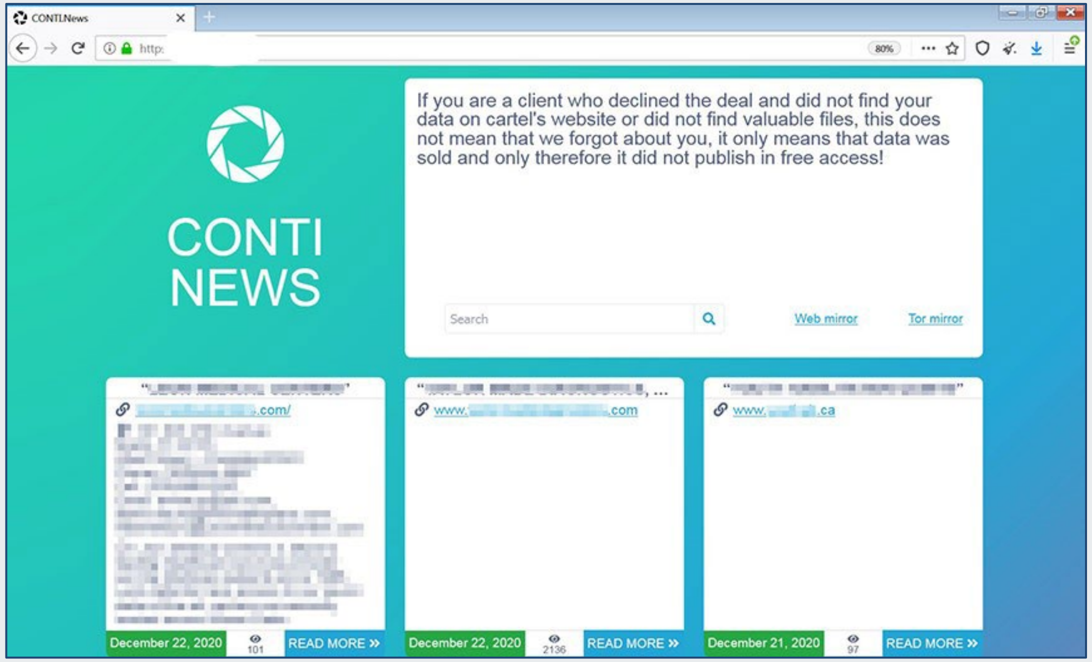
Source: HackRead

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)



If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

"[redacted]" [redacted].com/ [redacted] December 22, 2020 101 READ MORE »

"[redacted], ... www.[redacted].com December 22, 2020 2136 READ MORE »

"[redacted]" www.[redacted].ca December 21, 2020 97 READ MORE »

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?

Royal

:ase read carefully the "readme" file you got from us.
you still have a problem, use our contact form.

Source: Logpoint

Black Basta

Active Since: 2022 (possible rebrand of Conti)

Type: RaaS Group

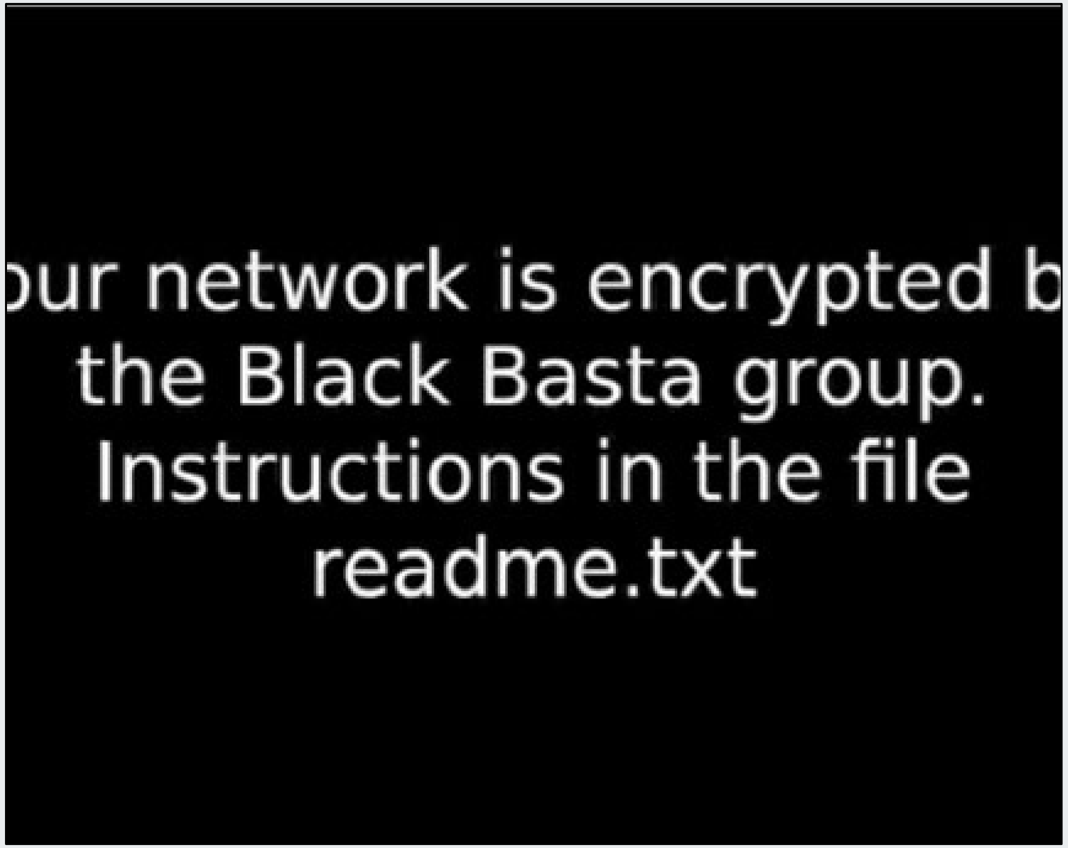
Known Targets: Construction, manufacturing, healthcare

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?



our network is encrypted b the Black Basta group. Instructions in the file readme.txt

Source: TrendMicro

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

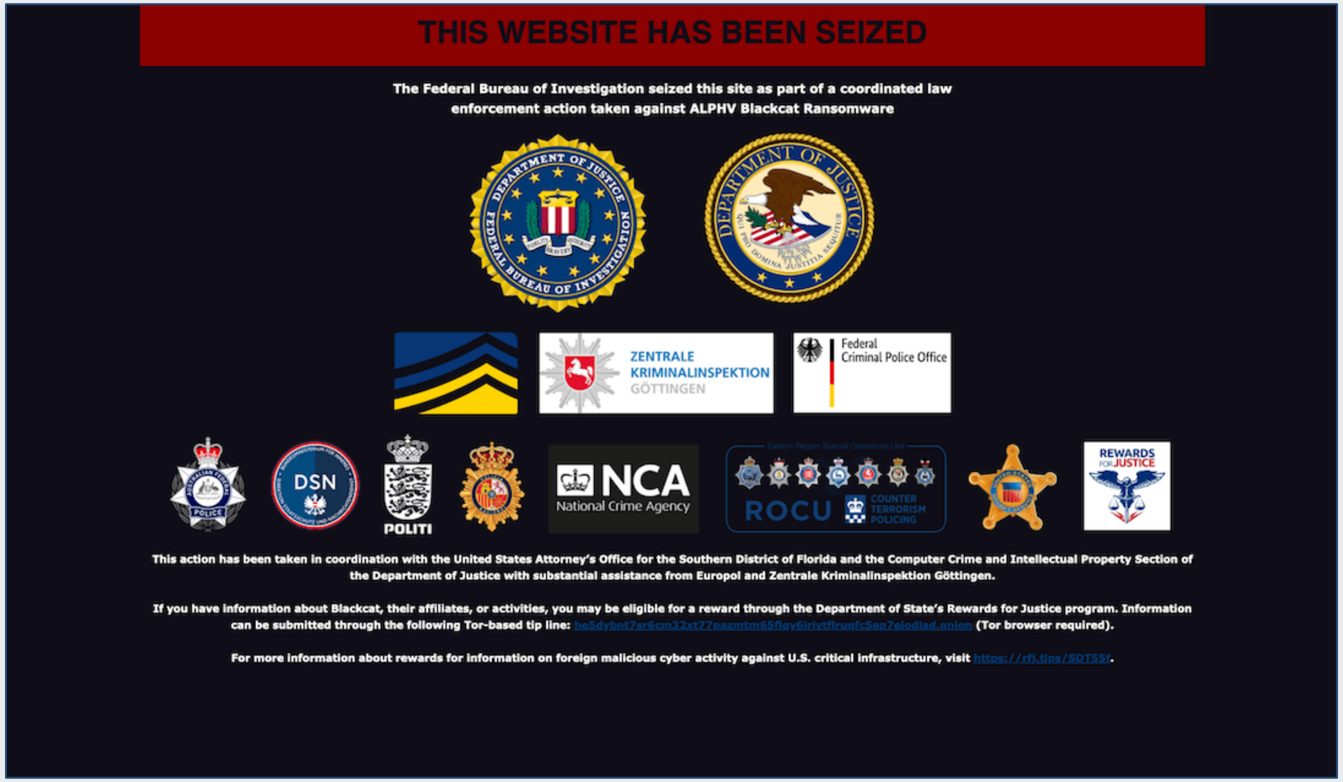
ALPHV

- **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?



THIS WEBSITE HAS BEEN SEIZED

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware

ZENTRALE KRIMINALINSPEKTION GÖTTINGEN
Federal Criminal Police Office
DSN
POLITI
NCA National Crime Agency
ROCU
COUNTER TERRORISM POLICING
REWARDS FOR JUSTICE

This action has been taken in coordination with the United States Attorney’s Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

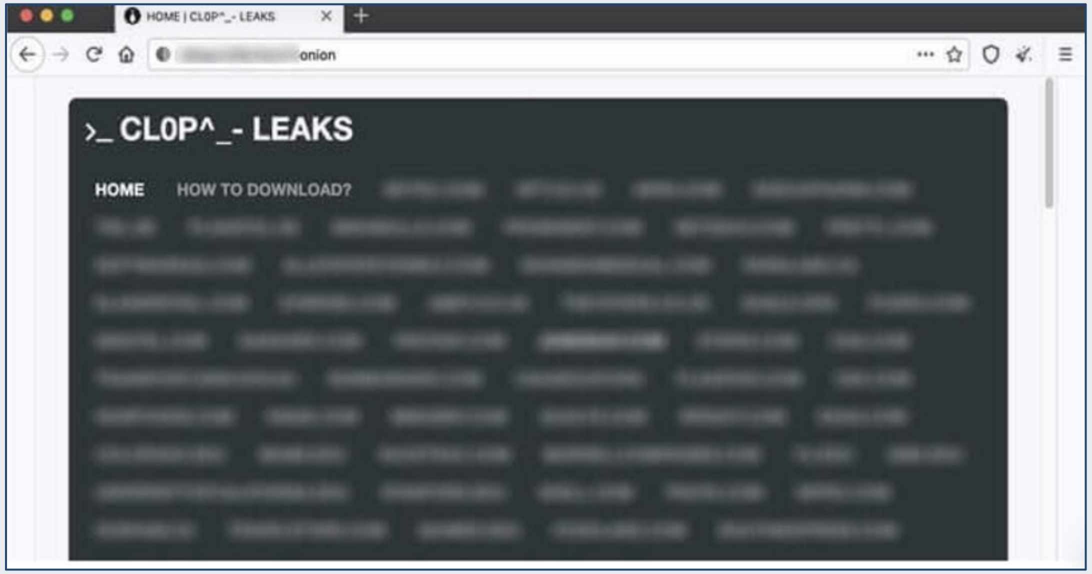
If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State’s Rewards for Justice program. Information can be submitted through the following Tor-based tip line: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion (Tor browser required).

For more information about rewards for information on foreign malicious cyber activity against U.S. critical infrastructure, visit https://rfj.tips/SDT55f.

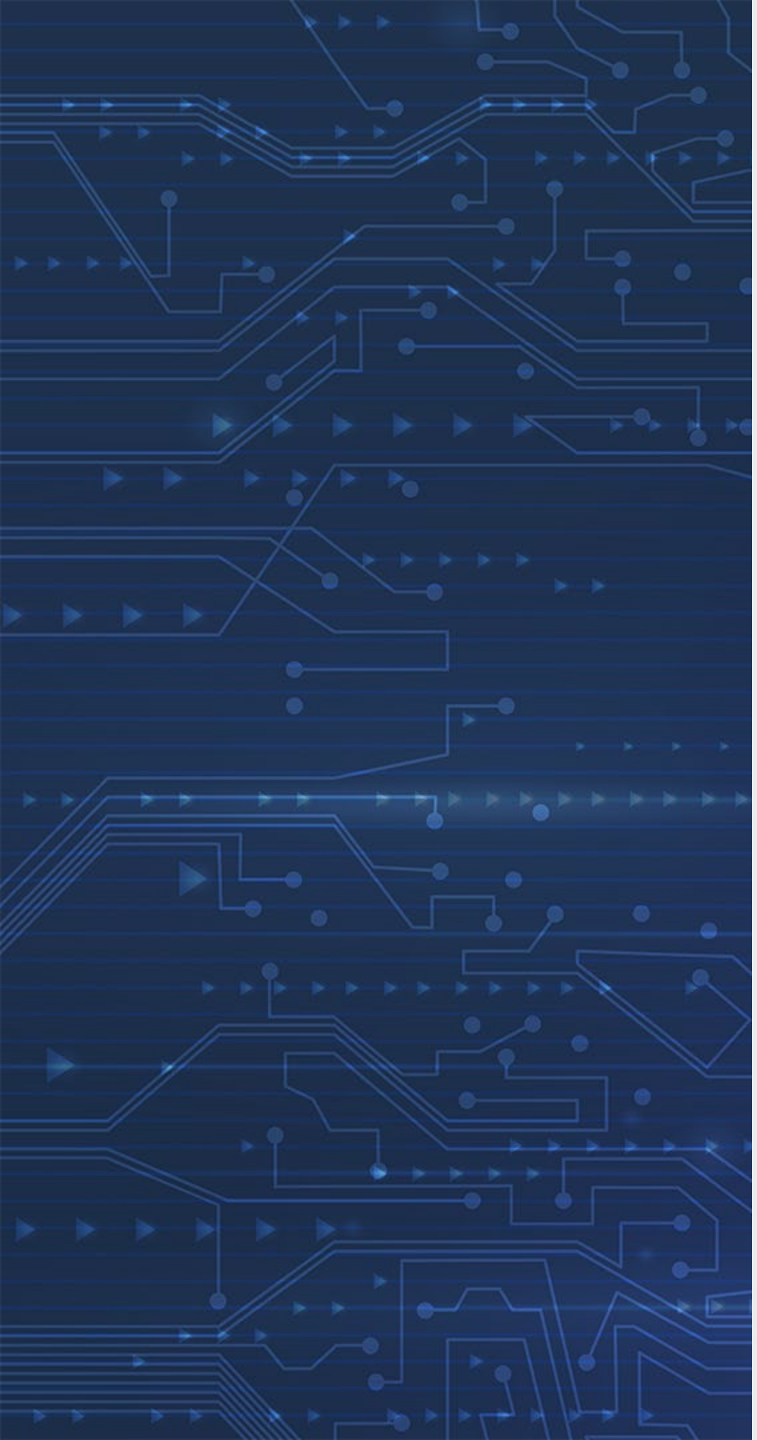
Source: The Record

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)



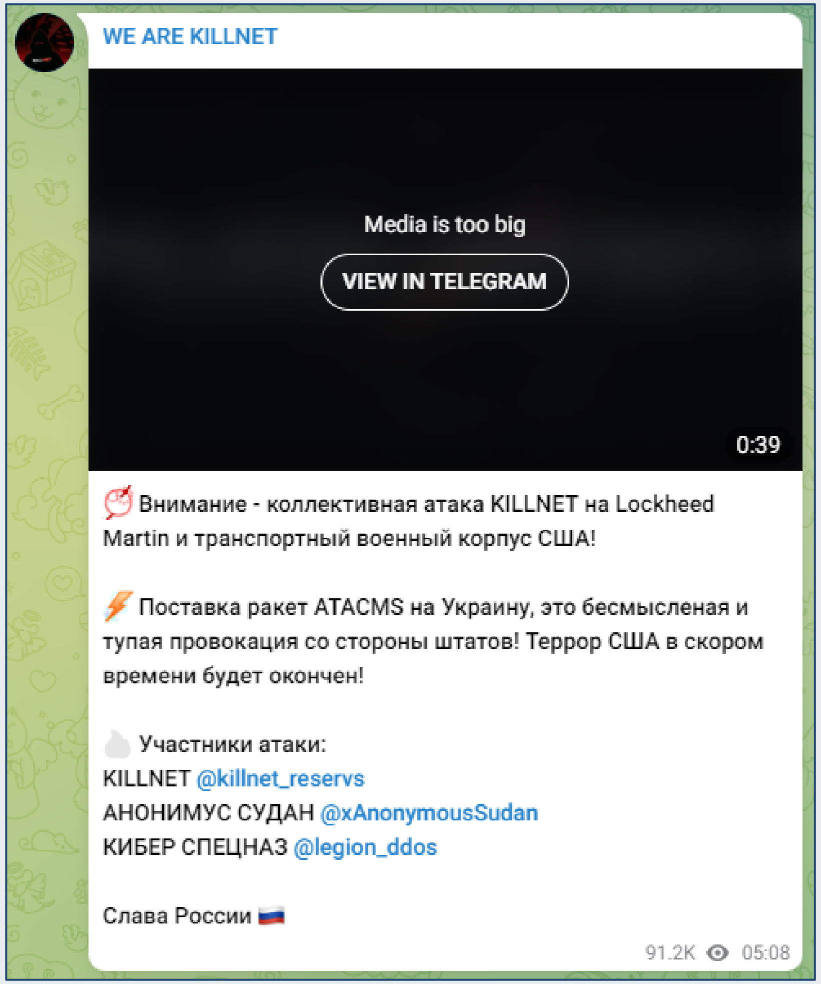
Source: IronScales



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.



WE ARE KILLNET

Внимание - коллективная атака KILLNET на Lockheed Martin и транспортный военный корпус США!

⚡ Поставка ракет ATACMS на Украину, это бесмысленая и тупая провокация со стороны штатов! Террор США в скором времени будет окончен!

Участники атаки:
KILLNET @killnet_reservs
АНОНИМУС СУДАН @xAnonymousSudan
КИБЕР СПЕЦНАЗ @legion_ddos

Слава России

91.2K 05:08

Source: KillNet Telegram

Russian Hacktivist Threat Actors

KillNet

Source: Atlas News

Anonymous Russia

Source: Telegram

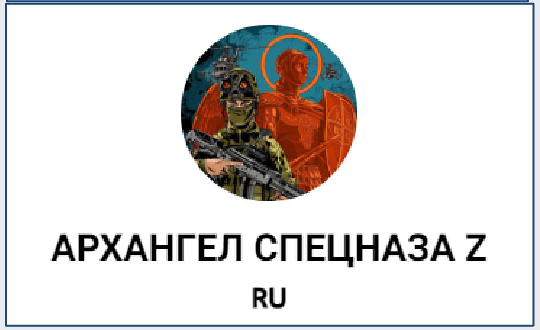
Anonymous Sudan

Source: BBC

Legion Russia Cyber Special Forces

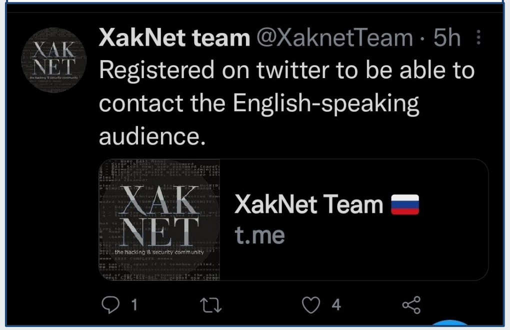
Source: Telegram

Special Forces Archangel ZRU



Source: Telegram

XakNet Team



XakNet team @XaknetTeam · 5h

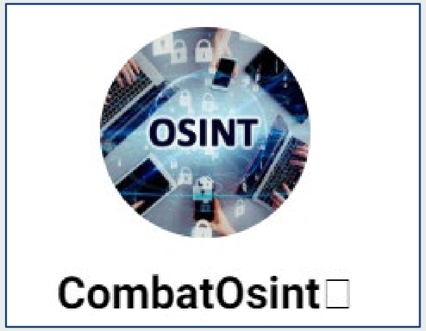
Registered on twitter to be able to contact the English-speaking audience.

XakNet Team 🇷🇺

t.me

Source: X (Twitter)

CombatOsint



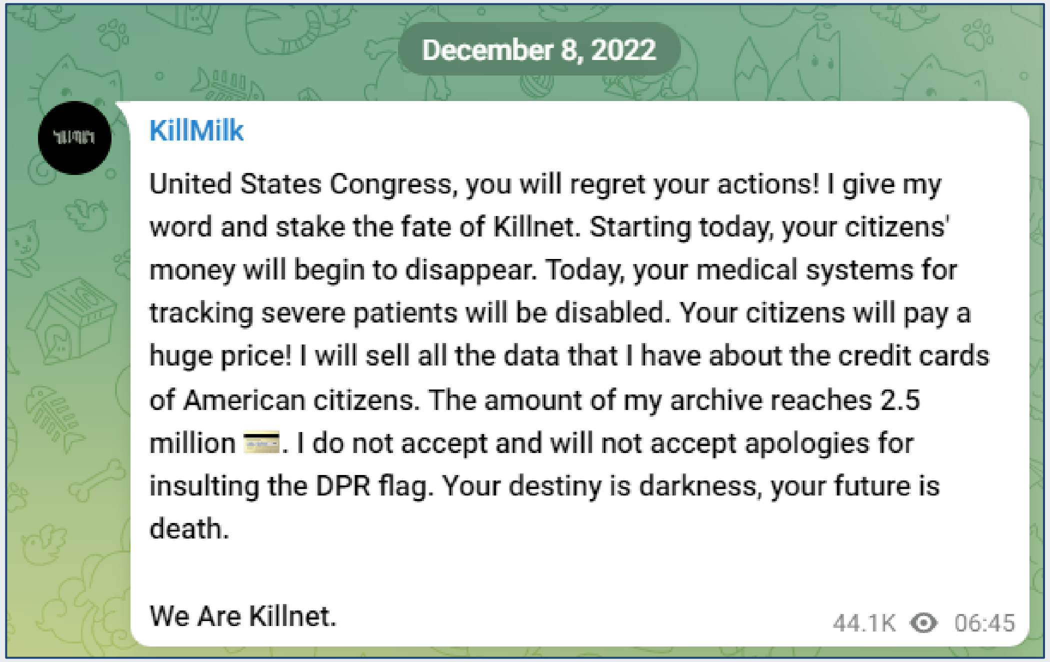
Source: Telegram

KillMilk

Source: TGStat

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)



December 8, 2022

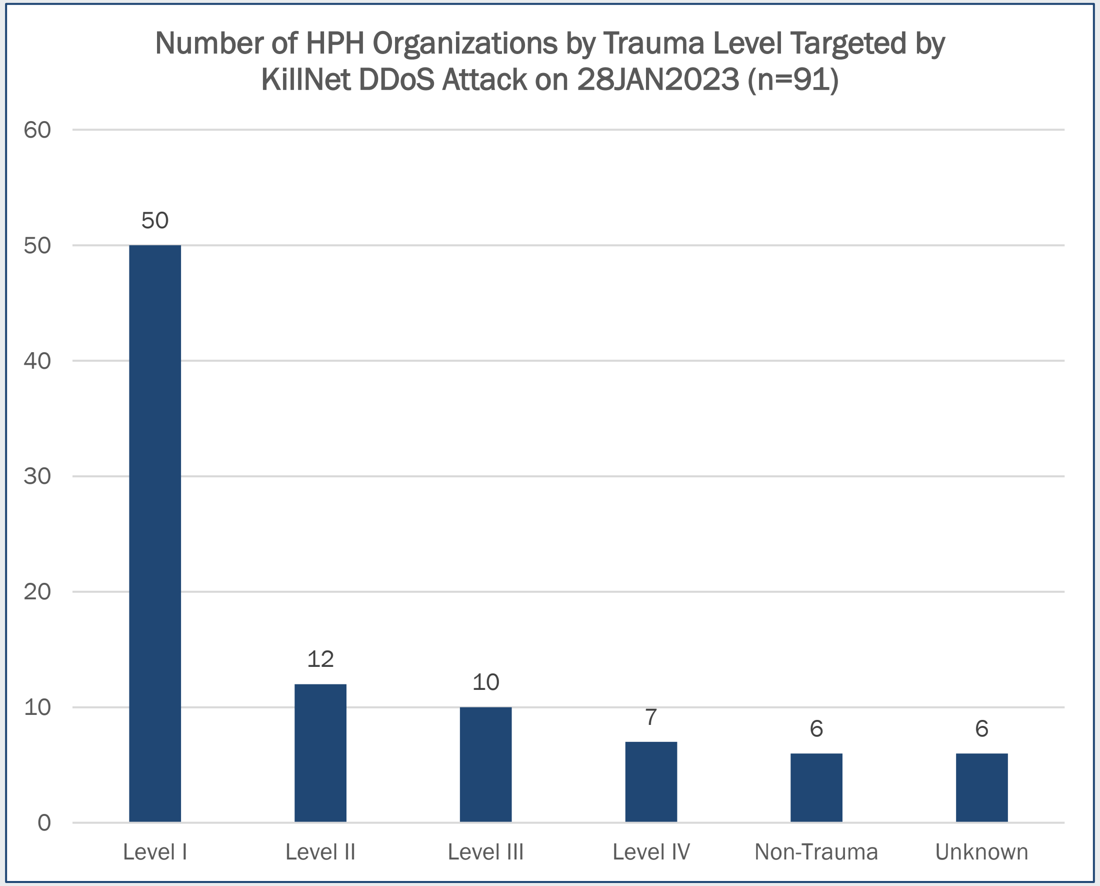
KillMilk

United States Congress, you will regret your actions! I give my word and stake the fate of Killnet. Starting today, your citizens' money will begin to disappear. Today, your medical systems for tracking severe patients will be disabled. Your citizens will pay a huge price! I will sell all the data that I have about the credit cards of American citizens. The amount of my archive reaches 2.5 million 💳. I do not accept and will not accept apologies for insulting the DPR flag. Your destiny is darkness, your future is death.

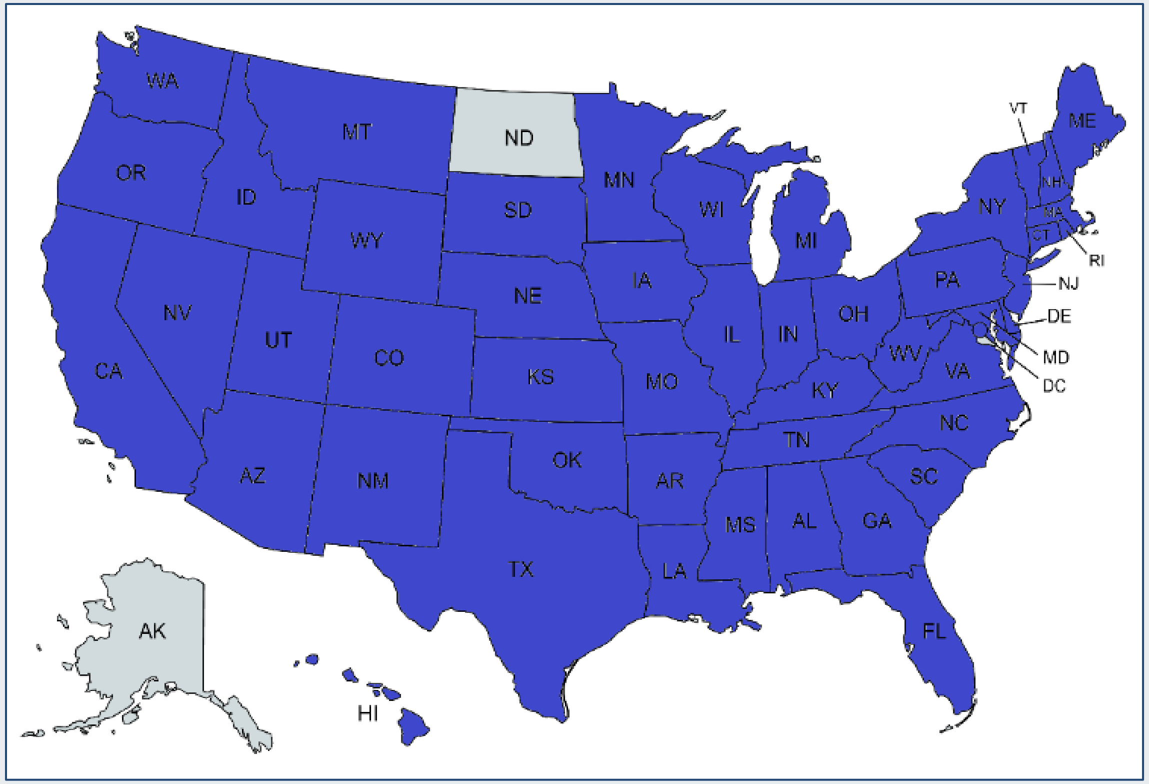
We Are Killnet.

Source: Telegram (KillMilk)

KillNet’s January 23, 2023 DDoS Attacks



Source: HC3



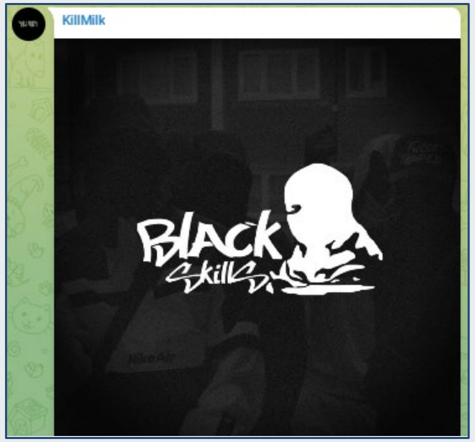
Source: HC3

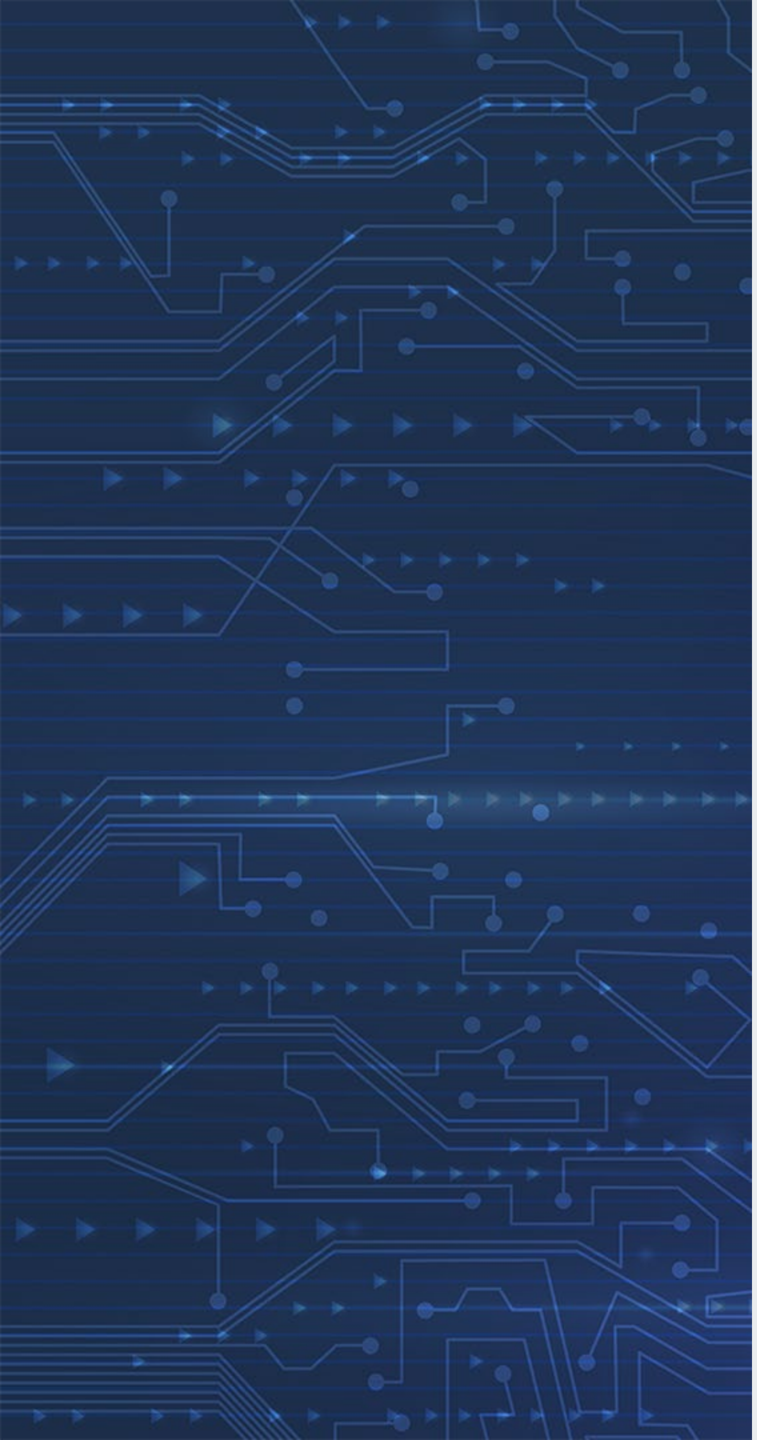
Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

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

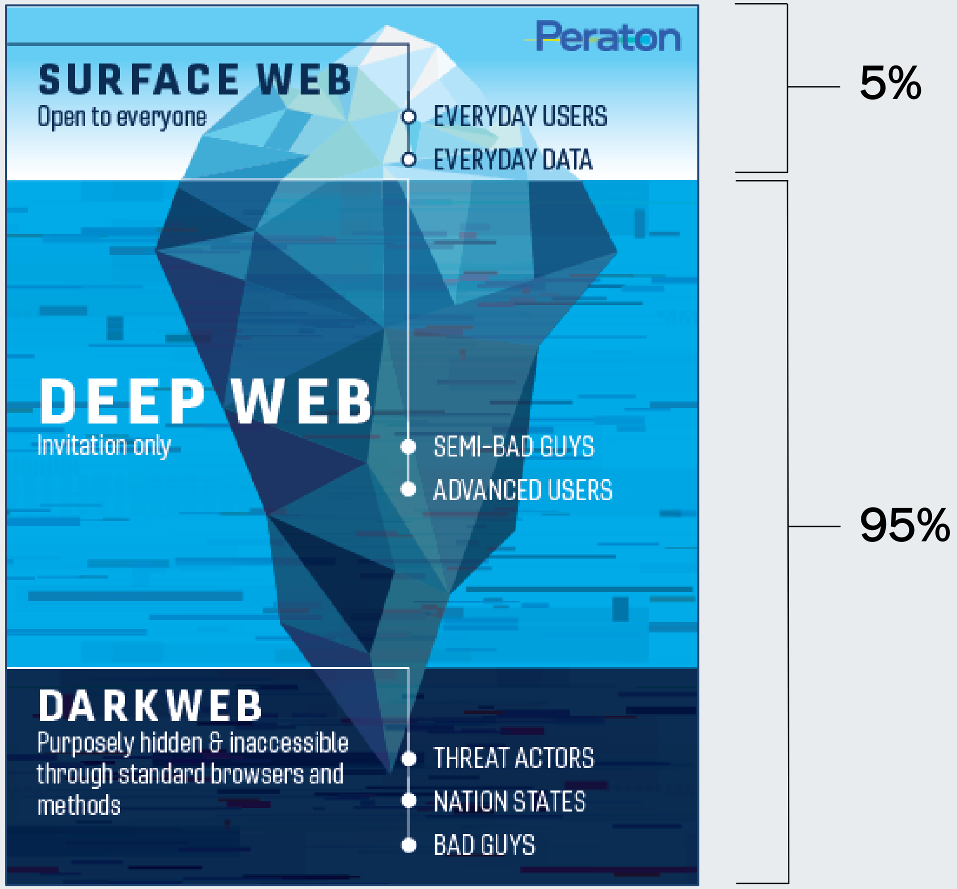




Russian Dark Web Forums

Hacking Forums and the Dark Web

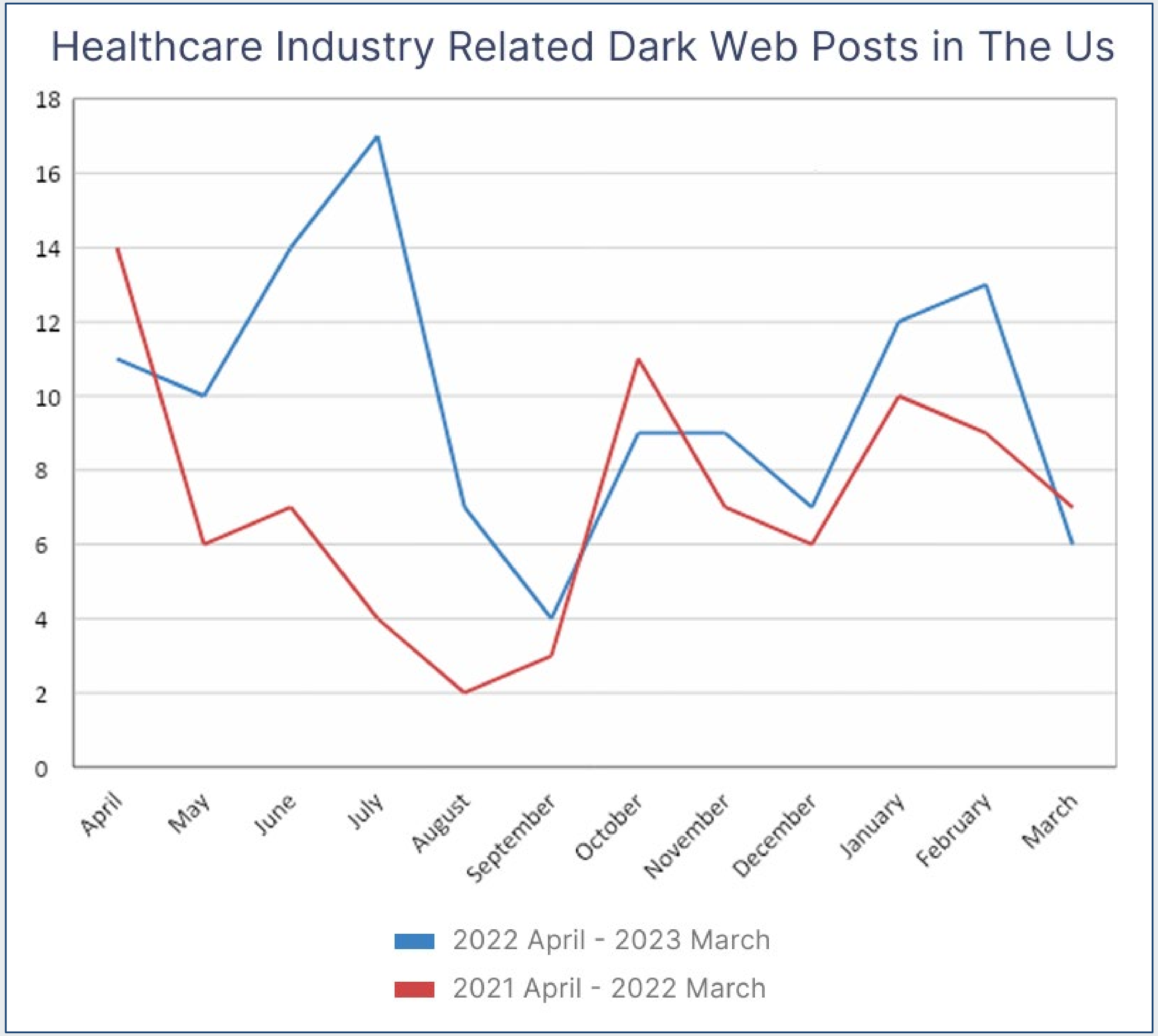
- Similar to clear web counterparts (avoid surveillance or censorship).
- Outlet to coordinate, exchange information, and conduct illicit trades.
- Often hosted on the dark web.
- Structure includes:
  - Marketplace section (stolen credentials, RaaS, and malware)
  - Cybercrime discussion section
- 74%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



Source: Peraton

Healthcare Industry Related Dark Web Posts in the United States

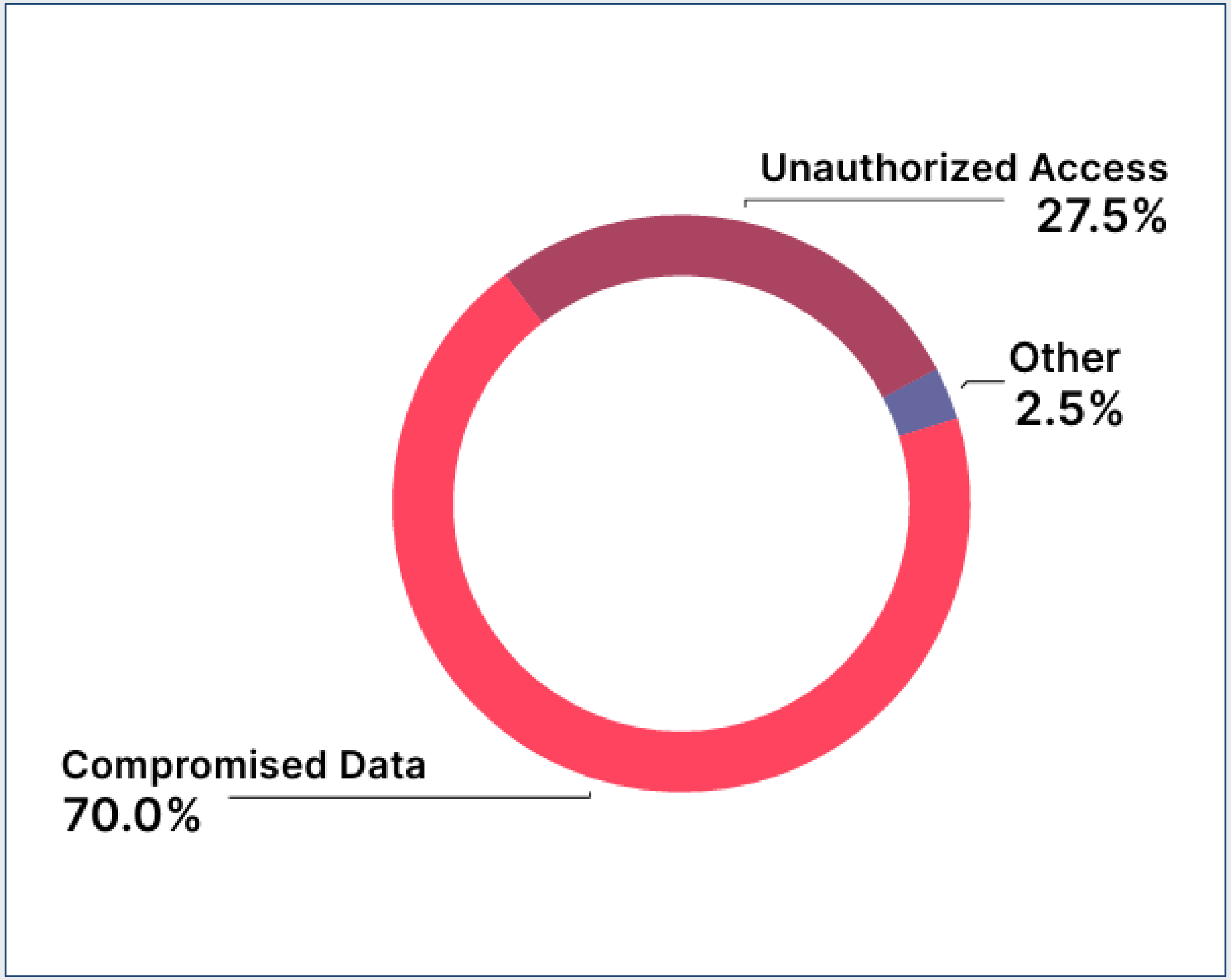
- 38% global rise in healthcare-related dark web posts from 2021-2022.
- Over 450 documented posts.
- In 2022, 119 U.S. healthcare industry-related posts were reported.



Source: SOCRadar

Healthcare Industry Related Dark Web Posts in the United States, cont.

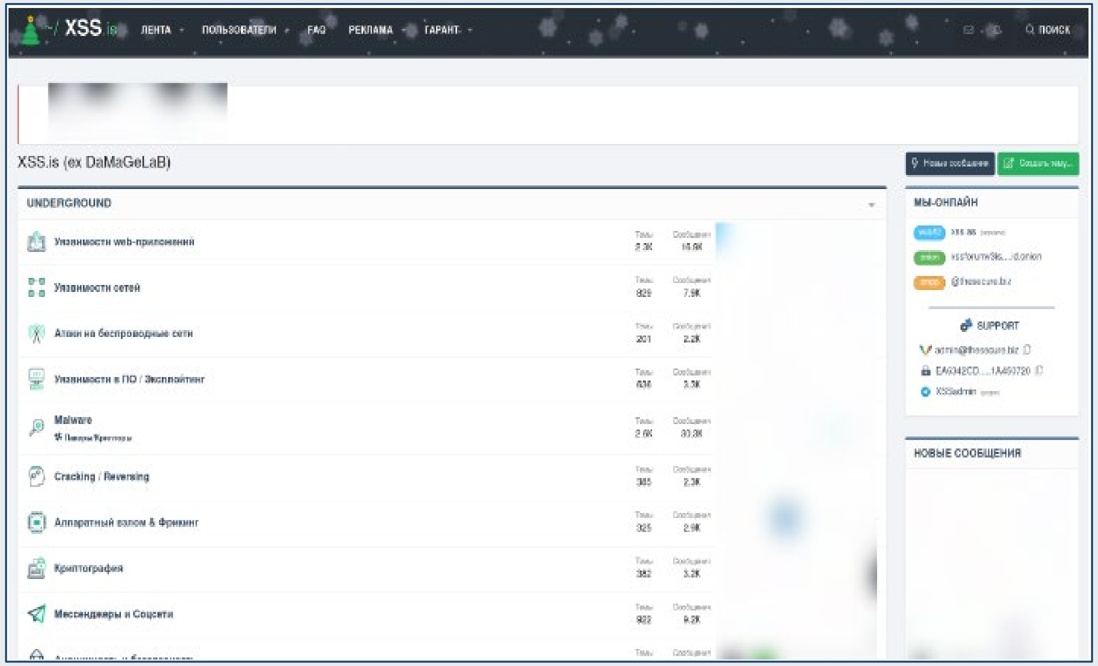
- Dark web posts targeting the U.S. HPH sector about buying, selling, and sharing illegal access to systems.
- In 70% of HPH data cases, threat actors were interested in already-compromised data.
- 27.5% of cases were focused on unauthorized access to health systems.



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, l3g0las, Rakuda



XSS.is (ex DaMaGeLaB)

UNDERGROUND

	Темы	Сообщения
Уязвимости web-приложений	2.3K	16.6K
Уязвимости сетей	829	7.9K
Атаки на беспроводные сети	201	2.2K
Уязвимости в ПО / Эксплойтинг	636	3.3K
Malware Лоадеры/Крипторы	2.6K	30.3K
Cracking / Reversing	385	2.3K
Аппаратный взлом & Фрикинг	325	2.9K
Криптография	382	3.2K
Мессенджеры и Соцсети	922	9.2K

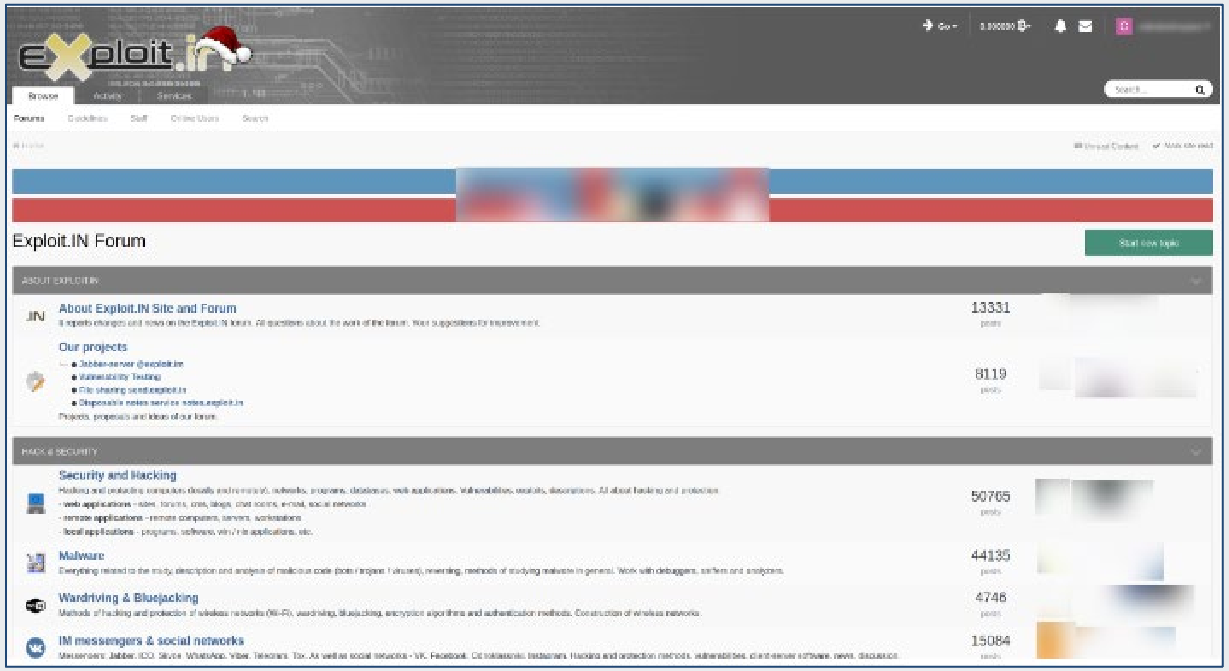
xss.is
xssforumv3is...d.onion
@thesecure.biz

admin@thesecure.biz
EA6342CD....1A450720
XSSadmin

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



Exploit.IN Forum

ABOUT EXPLOIT.IN

About Exploit.IN Site and Forum — 13331 posts
It reports changes and news on the Exploit.IN forum. All questions about the work of the forum. Your suggestions for improvement.

Our projects — 8119 posts
- Jabber-server @exploit.im
- Vulnerability Testing
- File sharing send.exploit.in
- Disposable notes service notes.exploit.in

Projects, proposals and ideas of our forum.

HACK & SECURITY

Security and Hacking — 50765 posts
Hacking and protecting computers (locally and remotely), networks, programs, databases, web applications. Vulnerabilities, exploits, descriptions. All about hacking and protection.
- **web applications** - sites, forums, cms, blogs, chat rooms, e-mail, social networks
- **remote applications** - remote computers, servers, workstations
- **local applications** - programs, software, win / nix applications, etc.

Malware — 44135 posts
Everything related to the study, description and analysis of malicious code (bots / trojans / viruses), reversing, methods of studying malware in general. Work with debuggers, sniffers and analyzers.

Wardriving & Bluejacking — 4746 posts
Methods of hacking and protection of wireless networks (Wi-Fi), wardriving, bluejacking, encryption algorithms and authentication methods. Construction of wireless networks.

IM messengers & social networks — 15084 posts
Messengers: Jabber, ICQ, Skype, WhatsApp, Viber, Telegram, Tox. As well as social networks - VK, Facebook, Odnoklassniki, Instagram. Hacking and protection methods, vulnerabilities, client-server software, news, discussion.

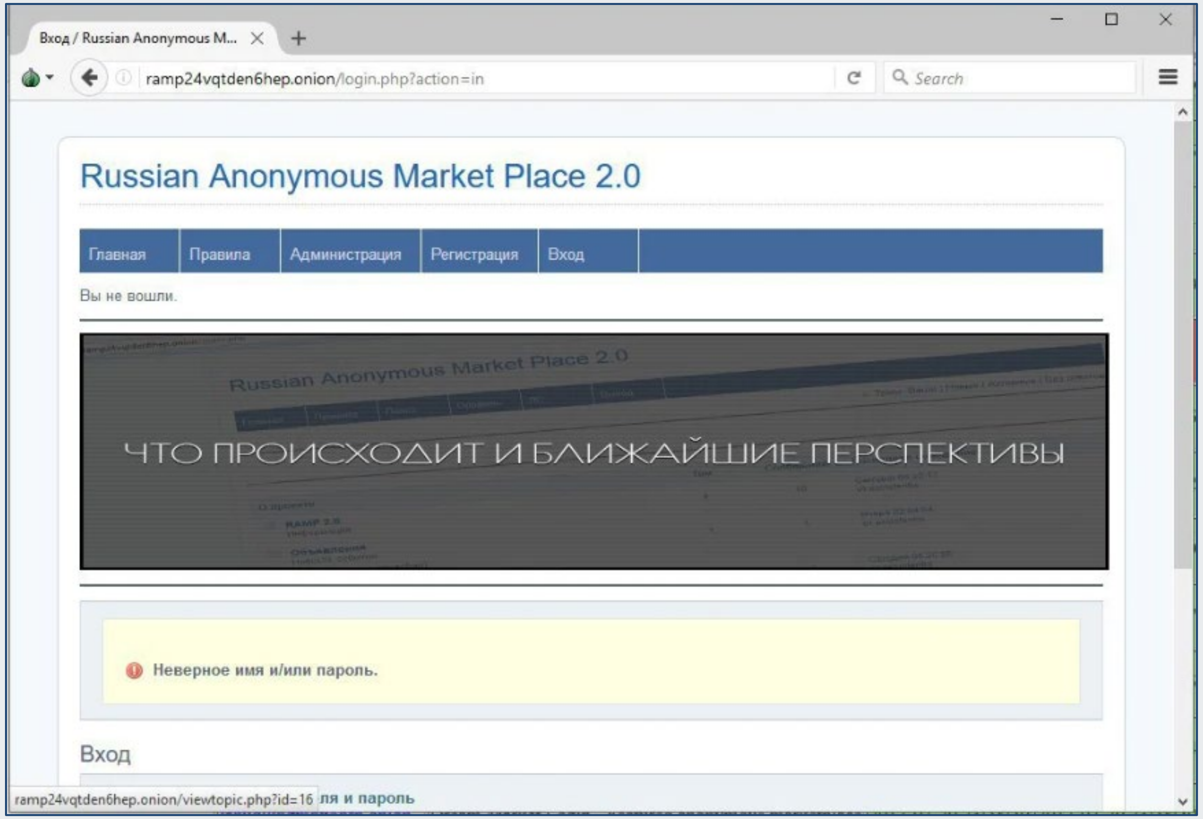
Source: Security Boulevard

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

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



Вход / Russian Anonymous M...
ramp24vqtden6hep.onion/login.php?action=in
Search
Главная
Правила
Администрация
Регистрация
Вход
ramp24vqtden6hep.onion/viewtopic.php?id=16

Russian Anonymous Market Place 2.0

Вы не вошли.

ЧТО ПРОИСХОДИТ И БЛИЖАЙШИЕ ПЕРСПЕКТИВЫ

Неверное имя и/или пароль.

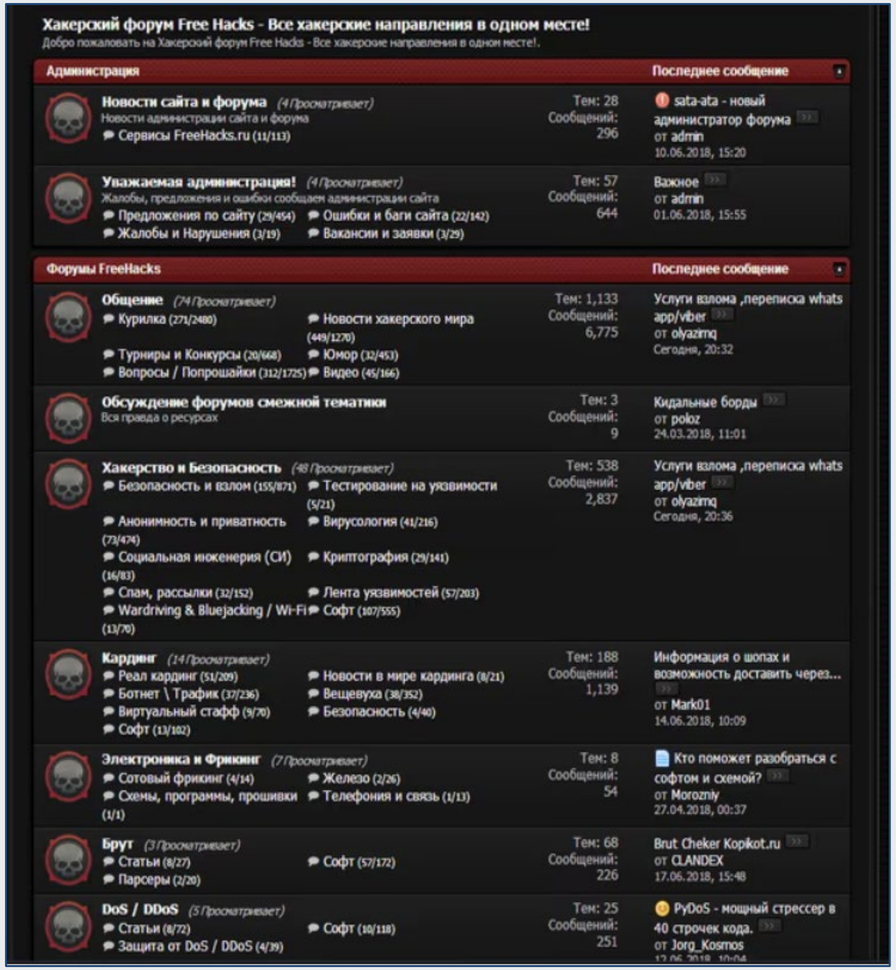
Вход

ля и пароль

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



Хакерский форум Free Hacks - Все хакерские направления в одном месте!

Добро пожаловать на Хакерский форум Free Hacks - Все хакерские направления в одном месте!.

Администрация		Последнее сообщение
Новости сайта и форума *(4 Просматривает)* Новости администрации сайта и форума Сервисы FreeHacks.ru (11/113)	Тем: 28 Сообщений: 296	sata-ata - новый администратор форума от admin 10.06.2018, 15:20
Уважаемая администрация! *(4 Просматривает)* Жалобы, предложения и ошибки сообщаем администрации сайта Предложения по сайту (29/454) Ошибки и баги сайта (22/142) Жалобы и Нарушения (3/19) Вакансии и заявки (3/29)	Тем: 57 Сообщений: 644	Важное от admin 01.06.2018, 15:55

Форумы FreeHacks		Последнее сообщение
Общение *(74 Просматривает)* Курилка (271/2480) Новости хакерского мира (449/1270) Турниры и Конкурсы (20/668) Юмор (32/453) Вопросы / Попрошайки (312/1725) Видео (45/166)	Тем: 1,133 Сообщений: 6,775	Услуги взлома ,переписка whats app/viber от olyazimq Сегодня, 20:32
Обсуждение форумов смежной тематики Вся правда о ресурсах	Тем: 3 Сообщений: 9	Кидальные борды от poloz 24.03.2018, 11:01
Хакерство и Безопасность *(48 Просматривает)* Безопасность и взлом (155/871) Тестирование на уязвимости (5/21) Анонимность и приватность (73/474) Вирусология (41/216) Социальная июкенерия (СИ) (16/83) Криптография (29/141) Спам, рассылки (32/152) Лента уязвимостей (57/203) Wardriving & Bluejacking / Wi-Fi (13/70) Софт (107/555)	Тем: 538 Сообщений: 2,837	Услуги взлома ,переписка whats app/viber от olyazimq Сегодня, 20:36
Кардинг *(14 Просматривает)* Реал кардинг (51/209) Новости в мире кардинга (8/21) Ботнет \ Трафик (37/236) Вещевуха (38/352) Виртуальный стафф (9/70) Безопасность (4/40) Софт (13/102)	Тем: 188 Сообщений: 1,139	Информация о шопах и возможность доставить через... от Mark01 14.06.2018, 10:09
Электроника и Фрикинг *(7 Просматривает)* Сотовый фрикинг (4/14) Железо (2/26) Схемы, программы, прошивки (1/1) Телефония и связь (1/13)	Тем: 8 Сообщений: 54	Кто поможет разобраться с софтом и схемой? от Morozniy 27.04.2018, 00:37
Брут *(3 Просматривает)* Статьи (8/27) Софт (57/172) Парсеры (2/20)	Тем: 68 Сообщений: 226	Brut Cheker Kopikot.ru от CLANDEX 17.06.2018, 15:48
DoS / DDoS *(5 Просматривает)* Статьи (8/72) Софт (10/118) Защита от DoS / DDoS (4/39)	Тем: 25 Сообщений: 251	PyDoS - мощный стрессер в 40 строчек кода. от Jorg_Kosmos 12.06.2018, 10:04

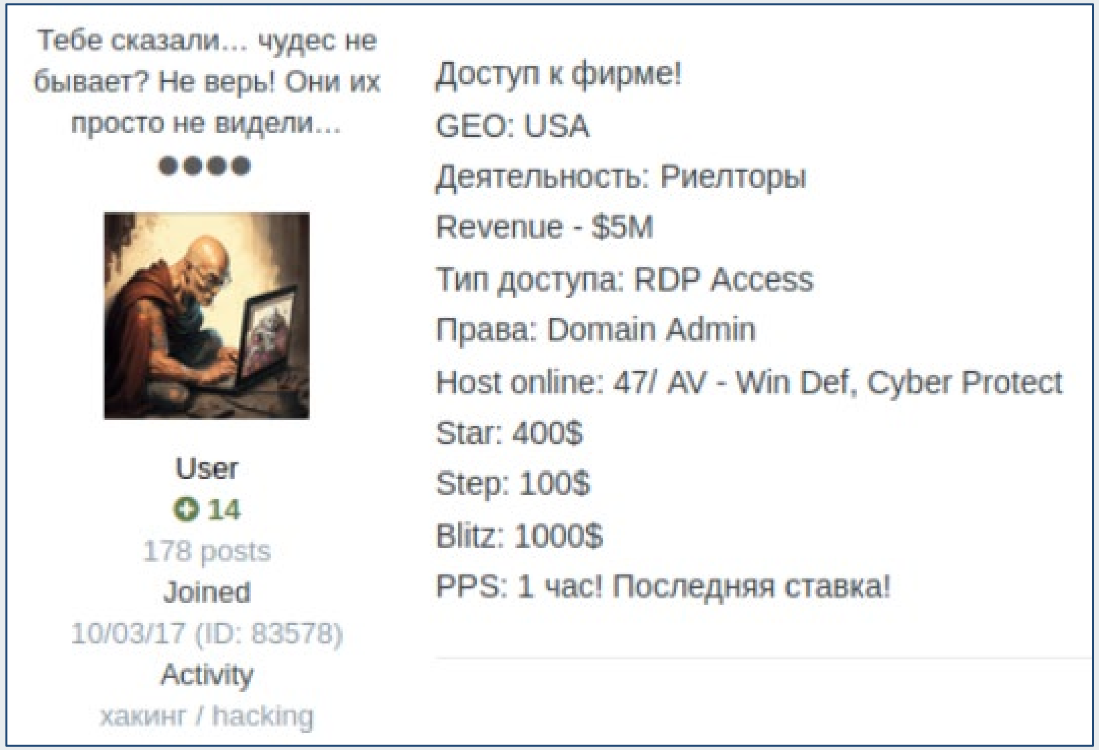
Source: The Guardian

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



Тебе сказали... чудес не бывает? Не верь! Они их просто не видели...

●●●●

User

14

178 posts

Joined

10/03/17 (ID: 83578)

Activity

хакинг / hacking

Доступ к фирме!

GEO: USA

Деятельность: Риелторы

Revenue - $5M

Тип доступа: RDP Access

Права: Domain Admin

Host online: 47/ AV - Win Def, Cyber Protect

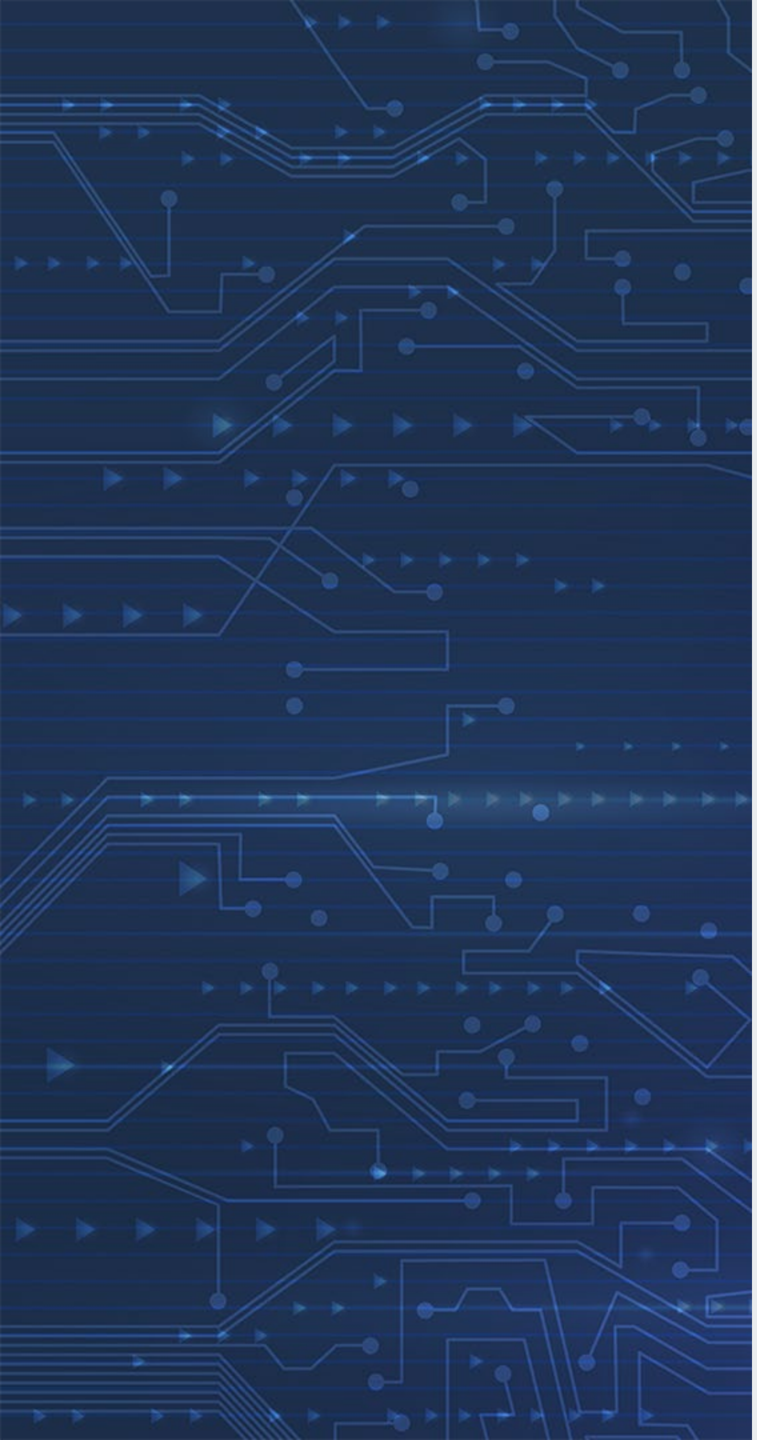
Star: 400$

Step: 100$

Blitz: 1000$

PPS: 1 час! Последняя ставка!

Source: Flare



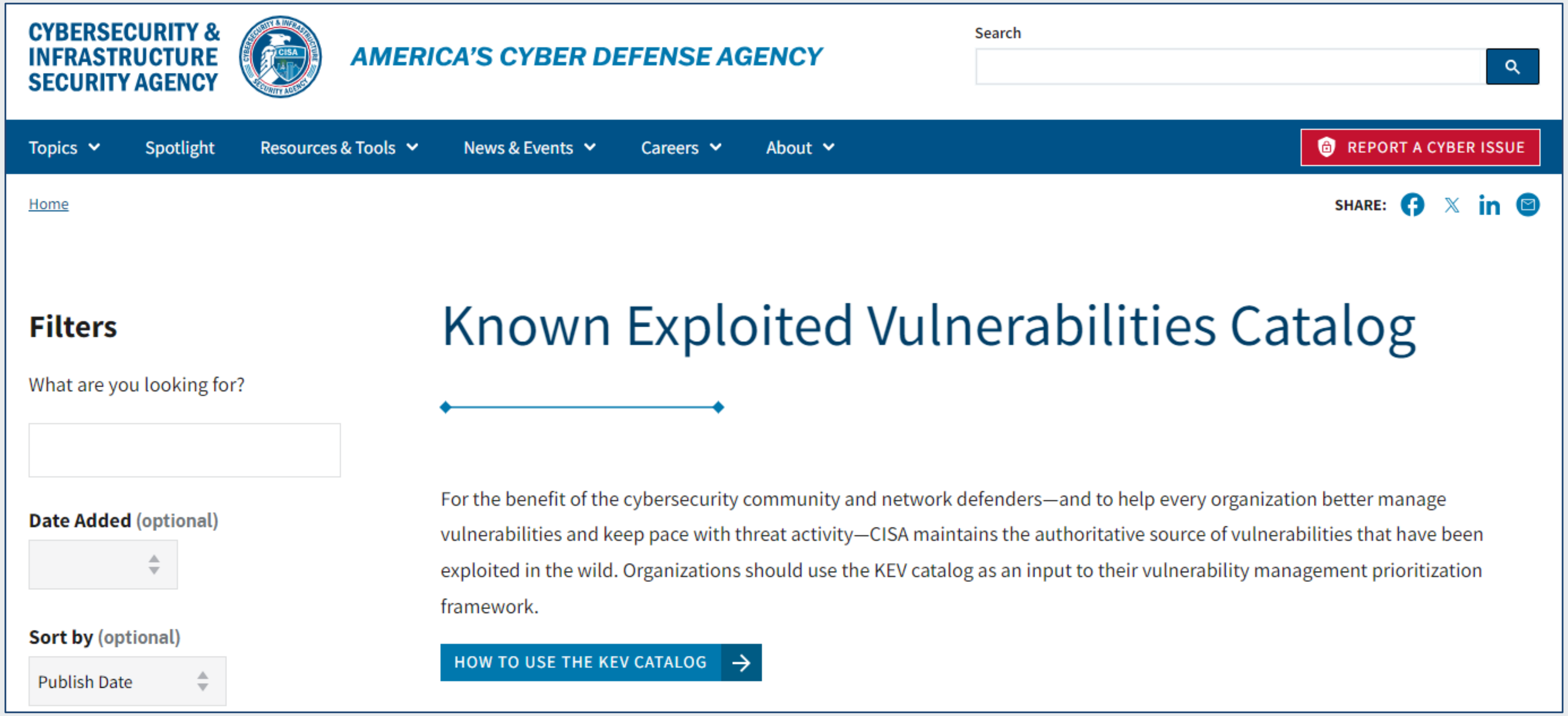
Best Practices and Mitigation Techniques

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



Known Exploited Vulnerabilities Catalog

Filters

What are you looking for?

Date Added (optional)

Sort by (optional)

Publish Date

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.

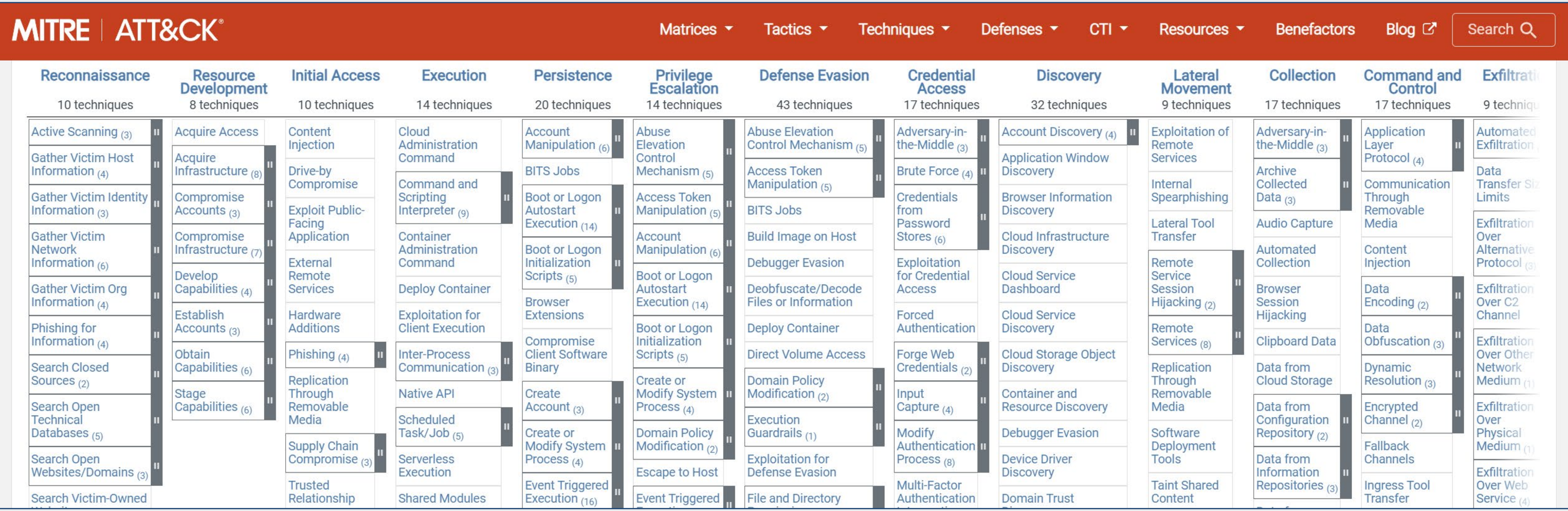
Source: CISA

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

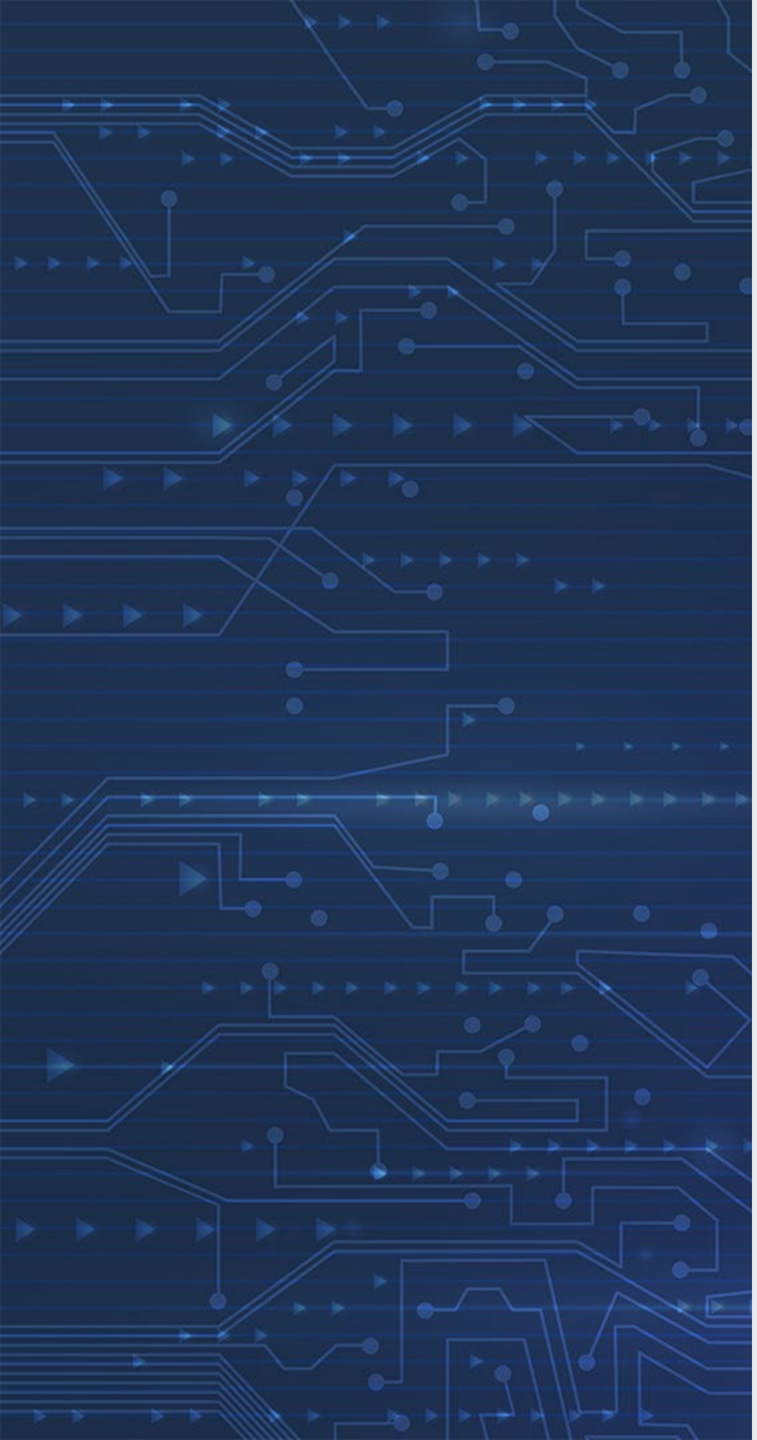


Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltrati
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniqu
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Si Limits
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered	Domain Policy Modification (2)	Multi-Factor Authentication	Debugger Evasion		Data from Information Repositories (3)	Ingress Tool Transfer	
Search Victim-Owned			Shared Modules			Execution Guardrails (1)		Device Driver Discovery				
						Exploitation for Defense Evasion		Domain Trust				
						File and Directory						

Source: MITRE ATT&CK

Mitigations

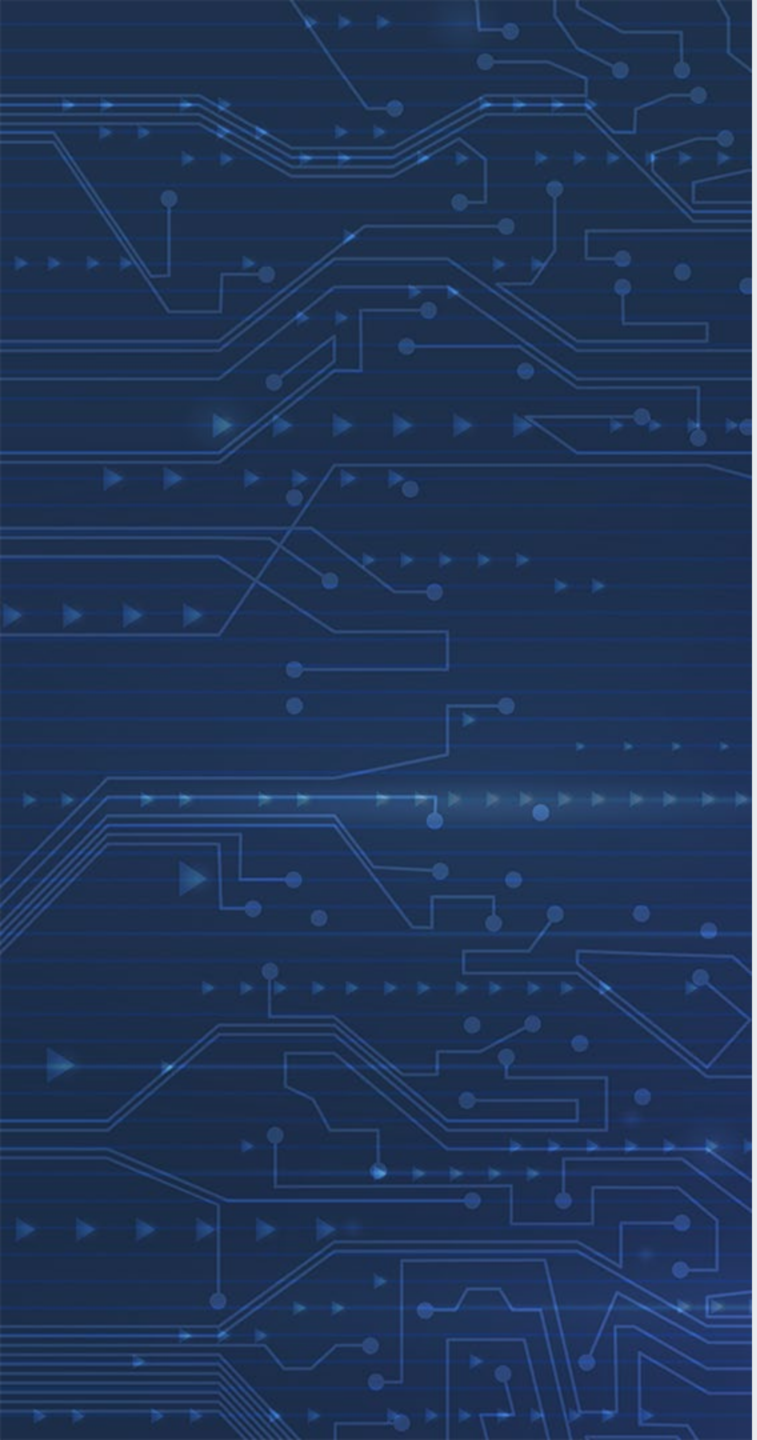
- Be prepared:
  - Confirm reporting processes and minimize coverage gaps
  - Create, maintain, and exercise a Cyber Incident Response, Resilience Plan, and Continuity of Operations Plan
- Enhance your organization’s cyber posture:
  - Identity and access management
  - Protective controls and architecture
  - 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 Hive Ransomware (August 25, 2021)
- HC3: Alert – Indicators of Compromise Associated with LockBit 2.0 Ransomware and Additional Mitigations (February 7, 2022)
- HC3: Alert – Joint CISA/NSA/FBI BlackMatter Ransomware Amplify Alert (October 19, 2021)
- HC3: Alert – Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (April 26, 2022)
- HC3: Alert - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (May 9, 2022)
- HC3: Alert – Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability (March 16, 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.

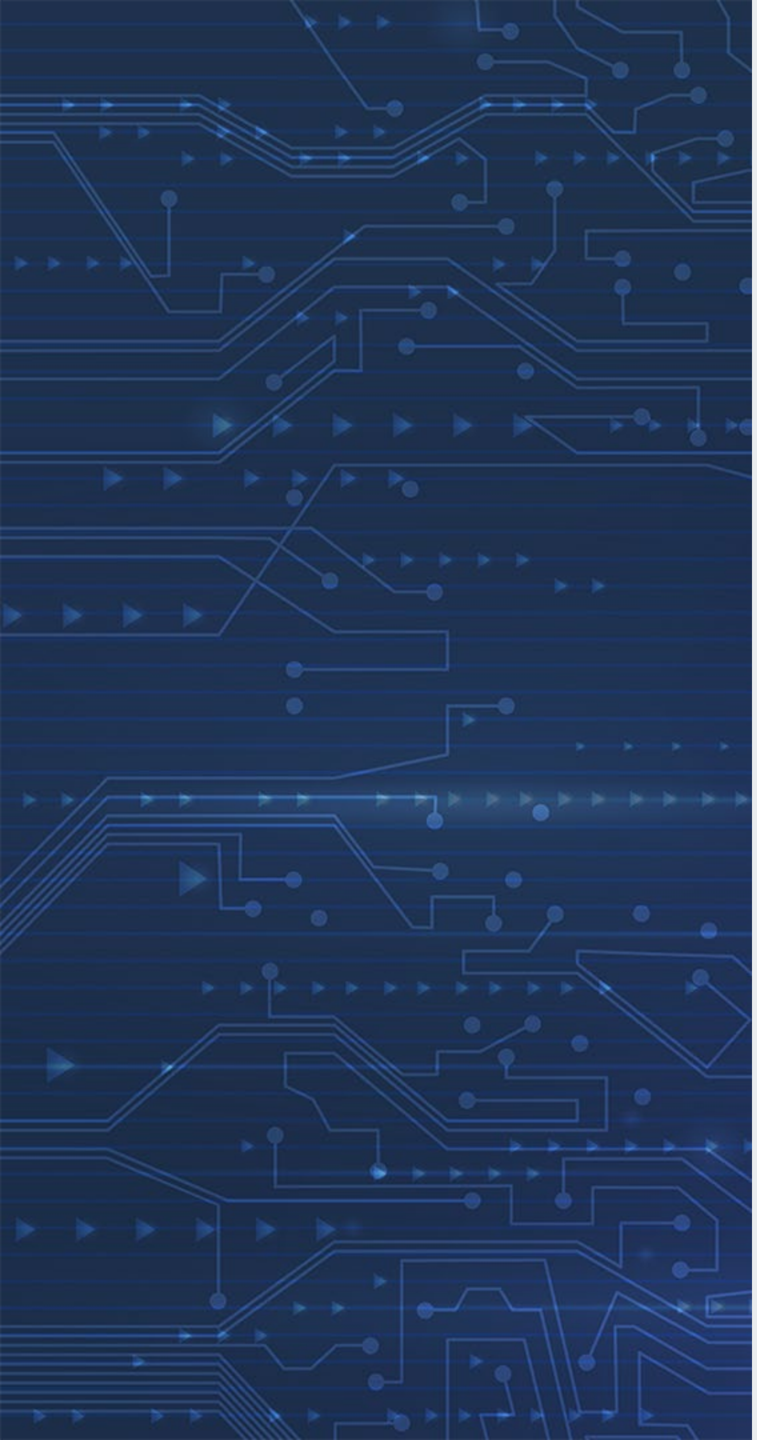
- HC3: Analyst Note – 8Base Ransomware (November 1, 2023)
- HC3: Analyst Note – BlackSuit Ransomware (November 6, 2023)
- HC3: Analyst Note – Cl0p Poses Ongoing Risk to HPH Organizations (March 23, 2021)
- HC3: Analyst Note – Cl0p Poses Ongoing Risk to HPH Organizations (November 16, 2020)
- HC3: Analyst 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: Analyst Note – Threat Actor ‘Orange’ and Groove Data Leak Site Targets U.S. HPH Sector (October 28, 2021)
- HC3: Analyst Note – SolarWinds Critical Remote Code Execution Flaws (October 25, 2023)
- HC3: Sector Alert – ClOp 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 – COVID-19 Related Nation-State and Cyber Criminal Targeting of the Healthcare Sector (May 14, 2020)
- 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

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

Reference Materials

References

- “5 Key Dark Web Forums to Monitor in 2023.” Flare. April 6, 2023. https://flare.io/learn/resources/blog/dark-web-forums/
- Abrams, Lawrence. “BlackMatter ransomware claims to be shutting down due to police pressure.” BleepingComputer. November 3, 2021. https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-claims-to-be-shutting-down-due-to-police-pressure/
- Ahmed, Deeba. “Cl0p Ransomware Gang Leaks MOVEit Data on Clearweb Sites.” HackRead. July 24, 2023. https://www.hackread.com/cl0p-ransomware-moveit-data-clearweb-sites/
- “Annual Threat Assessment of the U.S. Intelligence Community.” Office of the Director of National Intelligence. February 6, 2023. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf
- “APT Profile: Cozy Bear / APT29.” SOCRadar. March 17, 2023. https://socradar.io/apt-profile-cozy-bear-apt29/
- “APT Profile: Sandworm.” SOCRadar. March 22, 2023. https://socradar.io/apt-profile-sandworm/
- “APT Profile: Turla.” SOCRadar. June 29, 2023. https://socradar.io/apt-profile-turla/

References, cont.

- “BlackCat Malware (AKS ALPHV).” BlackBerry. Accessed December 18, 2023. https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/blackcat#:~:text=BlackCat%20is%20operated%20as%20a,speaking%20group%20of%20cybercrime%20actors.
- Burgess, Matt. “Russian ‘Hacktivists’ Are Causing Trouble Far Beyond Ukraine.” Wired. July 11, 2022. https://www.wired.com/story/russia-hacking-xaknet-killnet/
- Burky, Annie. “Attack by notorious ransomware group compromise personal data of 8.9M dental insurance members.” Fierce Healthcare. June 1, 2023. https://www.fiercehealthcare.com/health-tech/attack-notorious-ransomware-group-compromises-personal-data-89-million
- Clay, Eric. “Report – Initial Access Brokers, Russian Hacking Forums, and the Underground Corporate Access Economy.” Flare. August 16, 2023. https://flare.io/learn/resources/initial-access-brokers-russian-hacking-forums-the-underground-corporate-access-economy/

References, cont.

- “Conti Ransomware: In-Depth Analysis, Detection, Mitigation.” SentinelOne. Accessed December 12, 2023. https://www.sentinelone.com/anthology/conti/
- “Cost of a Data Breach Report – 2023.” IBM Security. 2023. https://www.ibm.com/downloads/cas/E3G5JMBP
- Curran, Dylan. “My terrifying deep dive into one of Russia’s largest hacking forums.” The Guardian. July 24, 2018. https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety
- “Cyber operations and the Russian intelligence services.” United Kingdom Foreign, Commonwealth & Development Office. Updated December 7, 2023. https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet
- “Dark Web Threat Profile: CLOP Ransomware.” SOCRadar. July 21, 2023. https://socradar.io/dark-web-threat-profile-clop-ransomware/
- “A Deep Dive into the Russian Cybercrime Forums Shaping 2023’s Landscape.” Munitio. February 23, 2023. https://munit.io/a-deep-dive-into-the-russian-cybercrime-forums-shaping-2023s-landscape/

References, cont.

- “Fancy Bear and Venomous Bear: What’s the difference between the two threat groups?” Cyware Social. July 28, 2019. https://cyware.com/news/fancy-bear-and-venomous-bear-whats-the-difference-between-the-two-threat-groups-430d9985
- “FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks.” Federal Bureau of Investigation. May 20, 2021. https://www.cisa.gov/sites/default/files/publications/Conti%2520Ransomware%2520Healthcare%2520Networks.pdf
- “FBI Most Wanted: Andrey Stanislavovich Korinets: Conspiracy to Commit Computer Fraud and Abuse; Forfeiture Allegation.” Federal Bureau of Investigation. Accessed December 15, 2023. https://www.fbi.gov/wanted/cyber/andrey-stanislavovich-korinets
- “FBI Most Wanted: Ruslan Aleksandrovich Peretyatko: Conspiracy to Commit Computer Fraud and Abuse; Forfeiture Allegation.” Federal Bureau of Investigation. Accessed December 15, 2023. https://www.fbi.gov/wanted/cyber/ruslan-aleksandrovich-peretyatko
- “Feds Warn Health Sector of Top Russia-Backed APT Groups.” Health-ISAC. May 20, 2022. https://h-isac.org/feds-warn-health-sector-of-top-russia-backed-apt-groups/

References, cont.

- Fox, Andrea. “Russian who deployed ransomware against hospitals are charged.” Healthcare IT News. September 11, 2023. https://www.healthcareitnews.com/news/russians-who-deployed-ransomware-against-hospitals-are-charged
- Freed, Benjamin. “Ransomware gang that hit Dallas an offshoot of Conti group, researchers say.” StateScoop. May 9, 2023. https://statescoop.com/ransomware-gang-dallas-offshoot-conti-group/
- Gatlan, Sergiu. “Dallas says Royal ransomware breached its network using stolen account.” BleepingComputer. September 22, 2023. https://www.bleepingcomputer.com/news/security/dallas-says-royal-ransomware-breached-its-network-using-stolen-account/
- Greenberg, Andy. “This is the New Leader of Russia’s Infamous Sandworm Hacking Unit.” Wired. March 15, 2023. https://www.wired.com/story/russia-gru-sandworm-serebriakov/
- Greig, Jonathan. “More than $100 million in ransom paid to Black Basta gang over nearly 2 years.” The Record. November 30, 2023. https://therecord.media/blackbasta-ransom-payments
- Hickman, Richard. “Conti Ransomware Gang: An Overview.” Unit 42. June 18, 2021. https://unit42.paloaltonetworks.com/conti-ransomware-gang/

References, cont.

- Hill, Jason. “BlackCat Ransomware (ALPHV).” Varonis. April 14, 2023. https://www.varonis.com/blog/blackcat-ransomware
- “LockBit Ransomware: Inside the World’s Most Active Ransomware Group.” FlashPoint. June 20, 2023. https://flashpoint.io/blog/lockbit/
- Lopez, C. Todd. “In Cyber, Differentiating Between State Actors, Criminals Is a Blur.” U.S. Department of Defense. May 14, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/
- “The ‘Main Enemy:’ Russian Active Measures in the United States.” The Cipher Brief. July 16, 2017. https://www.thecipherbrief.com/main-enemy-russian-active-measures-united-states-1090
- Matsygaya, Shingo. “Ransomware in 1H 2023: LockBit, BlackCat, and Clop Prevails as Top RaaS Groups.” TrendMicro. September 21, 2023. https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-blackcat-and-clop-prevail-as-top-raas-groups-for-1h-2023#:~:text=in%201H%202023-,LockBit%2C%20BlackCat%2C%20and%20Clop%20Prevail%20as%20Top%20RAAS,Groups%3A%20Ransomware%20in%201H%202023&text=We%20delve%20into%20three%20of,LockBit%2C%20Clop%2C%20and%20BlackCat.

References, cont.

- McGee, Marianne Kolbasuk. “Russian APTs: Why Stakes Are So High for Healthcare Sector.” Gov Info Security. January 12, 2022. https://www.govinfosecurity.com/russian-apts-stakes-are-so-high-for-healthcare-sector-a-18298
- Meyers, Adam. “CrowdStrike’s January Adversary of the Month: VOODOO BEAR.” CrowdStrike. January 29, 2018. https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/
- Nikolsky, Alexey. “Russian Meddling in the United States: The Historical Context of the Mueller Report.” Center for Strategic & International Studies. March 27, 2019. https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report
- Olenick, Doug. “How Conti Ransomware Works.” Bank Info Security. January 14, 2021. https://www.bankinfosecurity.com/how-conti-ransomware-works-a-15763
- Paganini, Pierluigi. “LockBit Threatens to Leak Medical Data of Cancer Patients Stolen from Varian Medical Systems.” Security Affairs. August 9, 2023. https://securityaffairs.com/149307/cyber-crime/varian-medical-systems-lockbit-ransomware.html

References, cont.

- “The Practitioner’s Guide to the Dark Web.” Searchlight Cyber. Accessed December 19, 2023. https://www.slcyber.io/dark-web-hub/?loader=false#hacking_forums
- “Ransomware is Big Business for REvil Hacker Group.” Axel. November 27, 2020. https://www.axel.org/2020/11/27/ransomware-is-big-business-for-revil-hacker-group/
- “The rise and fall of the Conti ransomware group.” Global Initiative. June 27, 2023. https://globalinitiative.net/analysis/conti-ransomware-group-cybercrime/#:~:text=Over%20the%20coming%20months%2C%20Conti%27s,websites%20were%20no%20longer%20working.
- “Russian Cyber Threat Overview and Advisories.” Cybersecurity & Infrastructure Security Agency. 2023. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia
- “Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns.” Cybersecurity & Infrastructure Security Agency. December 7, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a

References, cont.

- Santos, Doel, Daniel Bunce, and Anthony Galiette. “Threat Assessment: Royal Ransomware.” Unit 42. May 9, 2023. https://unit42.paloaltonetworks.com/royal-ransomware/
- Schappert, Stefanie. “Summit Health network hit by possible ransom attack.” Cybernews. November 15, 2023. https://cybernews.com/news/summit-health-lockbit-ransomware-/
- “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace.” U.S. Department of Justice. October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and
- Soldatov Andrei and Irina Borogan. “Russian Cyberwarfare: Unpacking the Kremlin’s Capabilities.” Center for European Policy Analysis. September 8, 2022. https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/
- Standish, Reid. “Study Shows How Russian, Chinese Disinformation About COVID-19 Evolved During The Pandemic.” RadioFreeEurope RadioLiberty. December 2, 2021. https://www.rferl.org/a/russia-china-covid-disinformation-campaigns/31590996.html

References, cont.

- Sussman, Bruce and David Steinberg-Zwirek. “Cyber’s Most Wanted: FBI is Hunting 10 Russian Threat Actors.” BlackBerry. December 9, 2022. https://blogs.blackberry.com/en/2022/12/cybers-most-wanted-is-10-russian-threat-actors
- “Threat Profile: Black Basta.” Health Sector Cybersecurity Coordination Center. March 15, 2023. https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf
- Tidy, Joe. “74% of ransomware revenue goes to Russia-linked hackers.” BBC. February 14, 2022. https://www.bbc.com/news/technology-60378009
- “Under the Spotlight: RAMP Forum.” SOCRadar. July 7, 2022. https://socradar.io/under-the-spotlight-ramp-forum/
- “Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.” Cybersecurity & Infrastructure Security Agency. March 1, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a
- “U.S. Healthcare Threat Landscape Report.” SOCRadar. Accessed December 22, 2023. https://socradar.io/wp-content/uploads/2023/06/US-Healthcare-Industry-Threat-Landscape-Report.pdf

References, cont.

- YouTube User: Фейгин Live. “Активные мероприятия. Беседа с Сергеем Жирновым.” YouTube. 2021. https://www.youtube.com/watch?v=a_5HtIaE9IA
- Wahlen, Mattias. “Russian Hacktivism.” Truesec. August 11, 2022. https://www.truesec.com/hub/blog/russian-hacktivism
- “What is ‘Star Blizzard’ in the News?” Buzz Meter. December 7, 2023. https://buzzmeter.in/what-is-star-blizzard-in-news
- “Who Wrote the ALPHV/BlackCat Ransomware Strain?” KrebsonSecurity. January 28, 2022. https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/
- Winder, Davey. “What is ALPHV/BlackCat?” TechFinitive. November 3, 2023. https://www.techfinitive.com/explainers/what-is-alphv-blackcat/
- “ZeroFox Intelligence Flash Report – Anonymous Russia Announces War Against NATO.” ZeroFox. December 14, 2023. https://www.zerofox.com/advisories/22551/

? 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

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.

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.

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV