



Major Cyber Organizations of the Russian Intelligence Services

May 19, 2022





Agenda

- Russian Intelligence Services' Structure
- Russian Intelligence Services' Mandates
- Turla
- APT29
- APT28
- Sandworm
- Conclusion
- Questions

Slides Key:



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



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



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



Assessed Structure of Russian Cyber Programs



M // ©2021 Mandiant



Source: Mandiant

Russian Intelligence Services' Structure



Office of Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



The Federal Security Service (FSB)

FBI equivalent

Collect on domestic intelligence and security, plus foreign intelligence from Russia's Near Abroad.



The Foreign Intelligence Service (SVR)

CIA equivalent

Collect foreign intelligence from military, strategic, economic, scientific, and technological targets; conduct active measures.



The Main Intelligence Directorate of the General Staff of the Armed Forces (GRU)

DIA equivalent

Collect foreign intelligence focusing on military issues; also conducts information operations and destructive cyber attacks.

Source: Mandiant

	Political intelligence	Economic intelligence	Military intelligence	Active measures	Counter-intelligence	Political security	Law enforcement
Federal Security Service (FSB)	●			●	●	●	●
Foreign Intelligence Service (SVR)	●	●	●	●	●	●	
Main Intelligence Directorate (GRU)	●	●		●	●		

Source: European Council on Foreign Relations

Russian Intelligence Services' Mandates



Office of Information Security
Securing One HHS



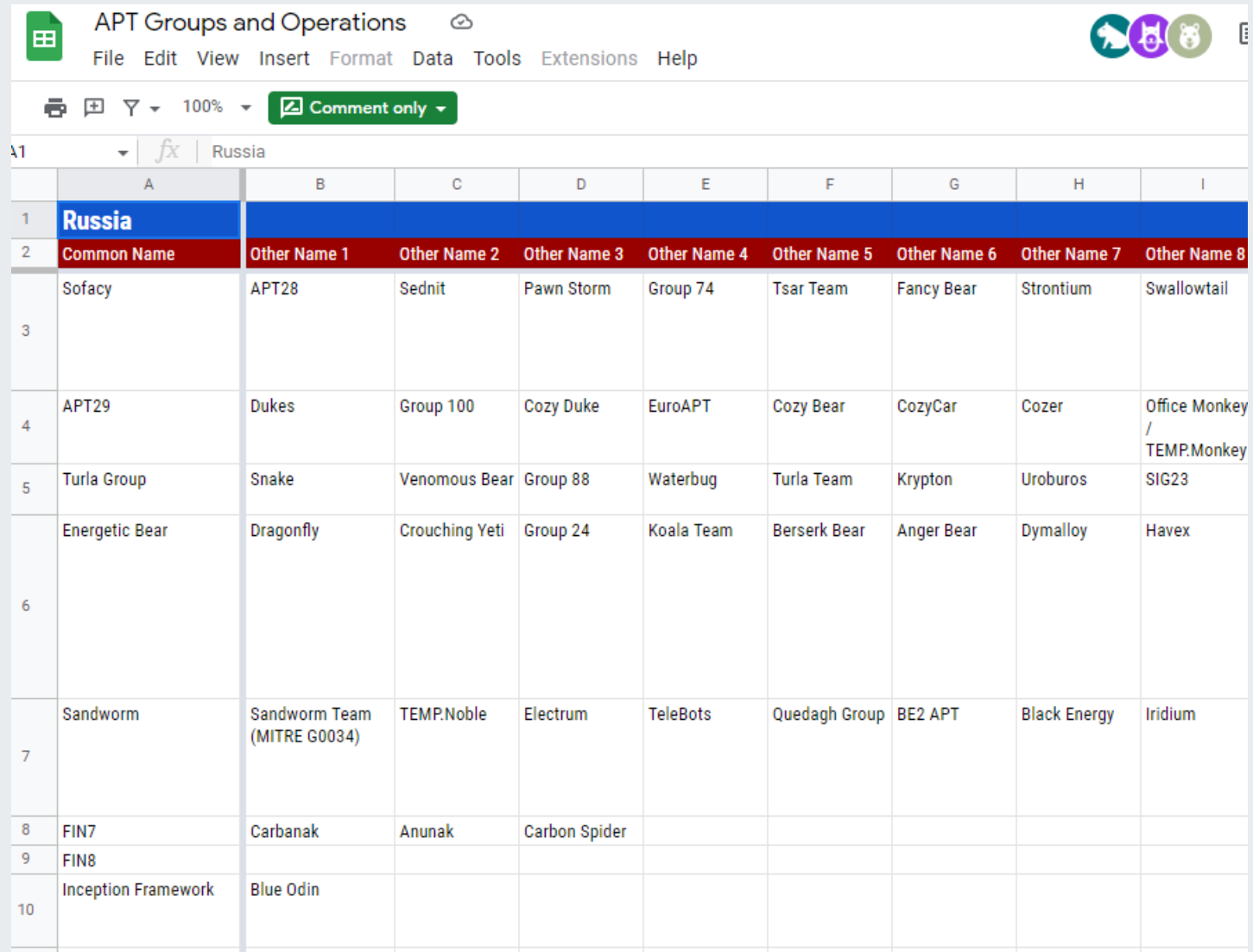
Health Sector Cybersecurity
Coordination Center

Disclaimer

Organizations track cyber threat actors using varying methodologies

In this presentation we have:

- Used Mandiant's designation to refer to the actor
- Used CrowdStrike's visual depiction of the actor, known as "bears"
- Gone back to the earliest suspected activity we could find



The screenshot shows a Google Sheets spreadsheet with the following data:

	A	B	C	D	E	F	G	H	I
1	Russia								
2	Common Name	Other Name 1	Other Name 2	Other Name 3	Other Name 4	Other Name 5	Other Name 6	Other Name 7	Other Name 8
3	Sofacy	APT28	Sednit	Pawn Storm	Group 74	Tsar Team	Fancy Bear	Strontium	Swallowtail
4	APT29	Dukes	Group 100	Cozy Duke	EuroAPT	Cozy Bear	CozyCar	Cozer	Office Monkey / TEMP.Monkey
5	Turla Group	Snake	Venomous Bear	Group 88	Waterbug	Turla Team	Krypton	Uroburos	SIG23
6	Energetic Bear	Dragonfly	Crouching Yeti	Group 24	Koala Team	Berserk Bear	Anger Bear	Dymalloy	Havex
7	Sandworm	Sandworm Team (MITRE G0034)	TEMP.Noble	Electrum	TeleBots	Quedagh Group	BE2 APT	Black Energy	Iridium
8	FIN7	Carbanak	Anunak	Carbon Spider					
9	FIN8								
10	Inception Framework	Blue Odin							

Source: Cyb3rops



Turla



Source: CrowdStrike

- **Attribution:** Russia's FSB
- **Earliest suspected activity:** 2004
- **AKA:** Venomous Bear (CrowdStrike), CTG-8875 (SCWX CTU), ITG12 (IBM), KRYPTON (Microsoft), Waterbug (Symantec), Iron Hunter (Secureworks)
- **Targeted Industries:** Academic, Embassies, Energy, Government, Military, Telecommunications, Research and Pharmaceutical Companies



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



Turla: Noteworthy Attacks

- U.S. Central Command (2008)
- Former Soviet Union Prime Minister's office (2012)
- G20 attendees (2017)
 - Embedded a malware dropper in a meeting invite
 - Dropper installed a JavaScript decryptor, which in turn installed the KopiLuwak backdoor
- Germany's government computer network (2018)



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



Turla Malware & Tactics, Techniques, and Procedures (TTPs)

- Known Associated Malware:
 - Carbon-DLL, ComRAT, Mosquito, Nautilus, Neuron, PoisonFrog, PyFlash, Skipper, Snake, Tavidig
 - LightNeuron
 - Sophisticated backdoor that has targeted Microsoft Exchange servers since 2014
- Tactics, Techniques, and Procedures (TTPs)
 - Largely focused on former Eastern Bloc countries
 - Uses novel and sophisticated techniques to maintain OPSEC
 - Espionage-focused actor in search of diplomatic intelligence
 - Distinct command and control network probably supported by SIGINT assets
 - Started using a second, simple, limited-functionality backdoor to maintain persistence if primary backdoor was discovered



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



APT29



Source: CrowdStrike

- **Attribution:** Russia's SVR
- **Earliest suspected activity:** 2008
- **AKA:** Cozy Bear (CrowdStrike), The Dukes (F-Secure), YTTTRIUM (Microsoft), Iron Hemlock (Secureworks)
- **Targeted Industries:** Academic, Energy, Financial, Government, Healthcare, Media, Pharmaceutical, Technology, Think Tanks



Office of
Information Security
Securing One HHS

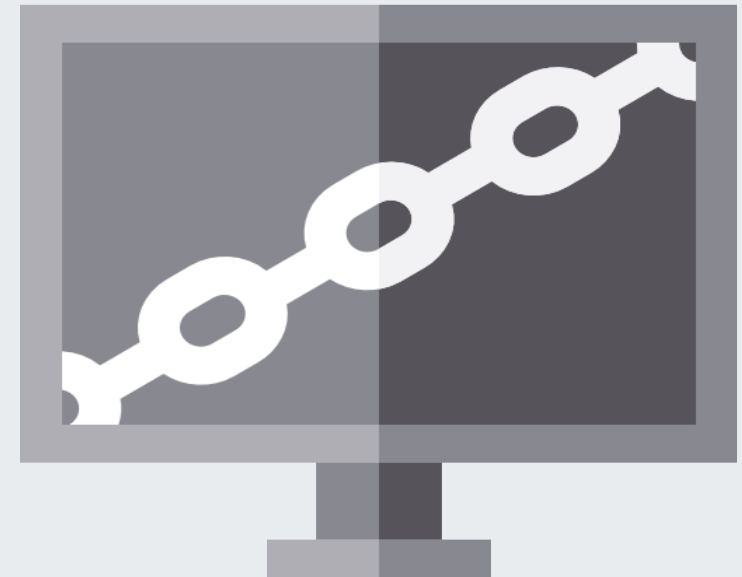


**Health Sector Cybersecurity
Coordination Center**



APT29: Noteworthy Attacks

- Pentagon (2015)
- COVID-19 vaccine developers (2020)
- SolarWinds Orion attack (2020)
 - Used a trojanized version of SolarWind's Orion software updates to distribute SUNBURST backdoor
 - Leveraged lateral movement and stole data
 - 18,000 affected — including a U.S. hospital



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



APT 29 Malware & Tactics, Techniques, and Procedures (TTPs)

- Known Associated Malware:
 - CosmicDuke, CozyCar, CozyDuke, HAMMERTOSS, LiteDuke, MiniDuke, OnionDuke, PolyglotDuke, RegDuke, SeaDuke
 - FatDuke
 - Flagship backdoor
 - Generally dropped by the MiniDuke backdoor but also using lateral movement such as PsExec
- Tactics, Techniques, and Procedures (TTPs)
 - Primarily targets European and NATO countries
 - Leverages large-scale spear phishing campaigns
 - Especially persistent and focused on specific targets
 - Prefers stealthy, long-term operations
 - Often reuses tools and techniques from previous attacks
 - Steals information, but doesn't leak it like APT28





APT28



Source: CrowdStrike

- **Attribution:** Russia's GRU, 85th Main Special Service Center, Military Unit 26165
- **Earliest suspected activity:** 2004
- **AKA:** Fancy Bear (CrowdStrike), Group 74 (Talos), PawnStorm (Trend Micro), Sednit (ESET), Snakemackerel (iDefense), Sofacy (Palo Alto), STRONTIUM (Microsoft), TG-4127 (SCWX CTU), Tsar Team (iSight), Iron Twilight (Secureworks)
- **Targeted Industries:** Aerospace, Defense, Energy, Government, Healthcare, Military, Media, Dissidents



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



APT28: Noteworthy Attacks

- World Anti-Doping Agency (2016)
 - Posed as hackers
 - Stole and manipulated the data in their systems
 - Act of revenge
- U.S. Democratic National Committee and the Clinton Campaign (2016)
 - Stole a great amount of data, including 19,252 emails from DNC staffers and members of Clinton's campaign
- German and French Elections (2016-2017)
- International Olympic Committee (2018)





APT28 Malware & Tactics, Techniques, and Procedures (TTPs)

- Known Associated Malware:
 - DEALERSCHOICE, DOWNDDELPH, EVILTOSS, HIDE DRV, LOJACK, POWERSHELL EMPIRE, SCARAMOUCHE, SCONATO, SEDKIT EXPLOIT KIT, SHARPFRONT, SOFACY DOWNLOADER, X-AGENT, X-TUNNEL, ZEBROCY
 - SEDUPLOADER
 - Simple tool used to facilitate download and persistence of next-stage tool
 - Collects system information and metadata, probably to tell sandbox environments apart from real targets
- Tactics, Techniques, and Procedures (TTPs)
 - Primarily focuses on NATO countries
 - Uses password spraying techniques
 - Uses malware unique to APT28 and leverages proprietary tools and droppers
 - Employs phishing and credential harvesting
 - Targets conventional computers and mobile devices
 - Steals and leaks information for publicity to further Russia's political interests
 - Conducts “noisy” cyber attacks





Sandworm



Source: CrowdStrike

- **Attribution:** Russia's GRU, Main Center for Special Technologies, Unit 74455
- **Earliest suspected activity:** 2007
- **AKA:** Voodoo Bear (CrowdStrike), CTG-7263 (SCWX CTU), ELECTRUM (Dragos), Hades/OlympicDestroyer (Kaspersky), IRIDIUM (Microsoft), IRIDUM (Microsoft), Qudedagh (F-Secure), Sandworm Team (Trend Micro), Telebots (ESET), Iron Viking (Secureworks)
- **Targeted Industries:** Energy, Government



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



Sandworm: Noteworthy Attacks

- Ukrainian Government and Critical Infrastructure (2015-2016, 2022)
- Georgian websites prior to Russian invasion (2008)
 - Used DDoS attacks
 - 54 targets including government, financial, and media outlets
- NotPetya attacks (2017)
 - Hijacked Ukrainian accounting software MeDoc (the TurboTax of Ukraine)
 - Corrupted the update so that if you had a copy of MeDoc, you had a copy of NotPetya
 - Shut down a pharmaceutical manufacturer in the U.S.
 - Affected the medical record systems of dozens of U.S. hospitals.



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



Sandworm Malware & Tactics, Techniques, and Procedures (TTPs)

- Known Associated Malware:
 - BadRabbit, BlackEnergy, GCat, GreyEnergy, KillDisk, NotPetya, PSCrypt, TeleBot, TeleDoor, xData
 - Industroyer
 - Speaks several industrial communication protocols that are used worldwide in critical infrastructure systems
 - Uses a wiper module to make systems unbootable; erases system crucial registry keys and overwrites files
- Tactics, Techniques, and Procedures (TTPs)
 - Particular focus on Ukraine
 - Targets ICS and computer systems for destructive purposes, such as shutting down power plants or deleting data
 - Most destructive of the “Bears” and seemingly not concerned with 2nd/3rd order effects of attacks (i.e., NotPetya)





Mitigations

- Update software, including operating systems, applications, and firmware, on IT network assets
- Reviewing the CVEs for all Public Facing Systems – CISA regularly updates and maintains a full list of CVEs that are known to be exploited: [CISA: Known Exploited Vulnerabilities Catalog](#)
- Enforce MFA to the greatest extent possible and require accounts with password logins, including service accounts, to have strong passwords
- If you use RDP and/or other potentially risky services, secure and monitor them closely
- Provide end-user awareness and training to help prevent successful targeted social engineering and spear phishing campaigns
- As part of a longer-term effort, implement network segmentation to separate network segments based on role and functionality
- HHS 405(d) program provides the Healthcare and Public Health (HPH) sector with useful, impactful, and vetted resources, products, videos, and tools that help raise awareness and provide cybersecurity practices, which drive behavioral change and move toward consistency in mitigating the most relevant cybersecurity threats to the sector. They offer advice for small, medium, and large healthcare organizations: [405\(d\) Health Industry Cybersecurity Practices \(HICP\)](#)
- For more information on preparing for cyber incidents, identity and access management tips, protective controls and architecture, and vulnerability and configuration management, see the CISA joint cybersecurity advisory [Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure](#)



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



Conclusion



Source: Euro Maidan Press



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



Reference Materials



References I

- Alexander, Keith B. “Disinformation: A Primer in Russian Active Measures and Influence Campaigns,” U.S. Senate. 30 March 2017. <https://www.intelligence.senate.gov/sites/default/files/documents/os-kalexander-033017.pdf>.
- “APT 29,” Malpedia. https://malpedia.caad.fkie.fraunhofer.de/actor/apt_29.
- “Assembling the Russian Nesting Doll: UNC2452 Merged into APT29,” Mandiant. 27 Apr 2022. <https://www.mandiant.com/resources/unc2452-merged-into-apt29>.
- ATTACKIQ. “The CISO’s Guide to APT29,” ATTACKIQ. 2020. https://go.attackiq.com/rs/041-FSQ-281/images/CISO_Guide_APT29.pdf.
- Baker, Sara. “Turla threat group targets G20 Summit attendees,” SecurityBrief. 21 Aug 2017. <https://securitybrief.asia/story/turla-threat-group-targets-g20-summit-attendees>.
- Bowen, Andrew S. “Russian Cyber Units,” Congressional Research Service. 2 Feb 2022. <https://crsreports.congress.gov/product/pdf/IF/IF11718>.
- Chyursin, Alexander. “The Cold War “Russian Bear” image is back,” Euromaiden Press. 27 Sept 2014. <https://euromaidanpress.com/2014/09/27/the-cold-war-russian-bear-image-is-back/>.
- CrowdStrike. “Cozy Bear,” CrowdStrike. <https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/>.
- CrowdStrike. “Fancy Bear,” CrowdStrike. <https://adversary.crowdstrike.com/en-US/adversary/fancy-bear/>.
- CrowdStrike. “Venomous Bear,” CrowdStrike. <https://adversary.crowdstrike.com/en-US/adversary/venomous-bear/>.
- CrowdStrike. “Who is FANCY BEAR (APT28)?,” CrowdStrike. 12 February 2019. <https://www.crowdstrike.com/blog/who-is-fancy-bear/>.
- CrowdStrike. “CrowdStrike’s January Adversary of the Month: VOOODOO BEAR,” CrowdStrike. 29 January 2018. <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-vooodoo-bear/>.





References II

- Cybersecurity Help. “The story of the four bears: Brief analysis of APT groups linked to the Russian government,” Cybersecurity Help. 17 January 2022. <https://www.cybersecurity-help.cz/blog/2507.html>.
- Cybersecurity Help. “The story of the four bears: Brief analysis of APT groups linked to the Russian government (Part 2),” Cybersecurity Help. 25 January 2022. <https://www.cybersecurity-help.cz/blog/2509.html>.
- Cybersecurity Help. “The story of the four bears: Brief analysis of APT groups linked to the Russian government (Part 2),” Cybersecurity Help. 31 January 2022. <https://www.cybersecurity-help.cz/blog/2510.html>.
- Cyware Hacker News. “Turla threat actor group: An insight into the threat group’s cyber-espionage activities,” Cyware. 29 June 2019. <https://cyware.com/news/turla-threat-actor-group-an-insight-into-the-threat-groups-cyber-espionage-activities-f7e97192>.
- Darczewska, Jolanta and Piotr Żochowski. “Active Measures: Russia’s Key Export,” Center for Eastern Studies. June 2017. https://www.osw.waw.pl/sites/default/files/pw_64_ang_active-measures_net_0.pdf.
- Department of Justice. “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” DOJ. 19 October 2020. <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>.
- “FatDuke,” Malpedia. N.a. <https://malpedia.caad.fkie.fraunhofer.de/details/win.fatduke>.
- Galeotti, Mark. “Putin’s Hydra: Inside Russia’s Intelligence Services,” European Council on Foreign Affairs. May 2016. [https://ecfr.eu/archive/page/-/ECFR_169_-_INSIDE_RUSSIAS_INTELLIGENCE_SERVICES_\(WEB_AND_PRINT\)_2.pdf](https://ecfr.eu/archive/page/-/ECFR_169_-_INSIDE_RUSSIAS_INTELLIGENCE_SERVICES_(WEB_AND_PRINT)_2.pdf)





References III

- Holt, Rene. “Sandworm: A tale of disruption told anew,” WeLiveSecurity. 21 March 2022. <https://www.welivesecurity.com/2022/03/21/sandworm-tale-disruption-told-anew/>
- Hultquist, John. “Anticipating and Preparing for Russian Cyber Activity,” BrightTALK. 20 January 2022. <https://www.brighttalk.com/webcast/7451/527124>
- “LightNeuron,” MITRE. 28 June 2019. <https://attack.mitre.org/software/S0395/>
- “Mitre ATT&CK Groups,” Mitre ATT&CK. <https://attack.mitre.org/groups/>
- O’Leary, Lizzie. “Russia’s Invisible War on Ukraine,” Slate. 25 February 2022. <https://slate.com/technology/2022/02/ukraine-russia-cyberwar-sandworm-gru.html>.
- Roth, Florian. “APT Groups and Operations,” 26 Dec 2015, Google Sheets. <https://apt.threattracking.com>.
- Roth, Florian. “The Newcomer’s Guide to Cyber Threat Actor Naming.” Medium. 25 March 2018. <https://cyb3rops.medium.com/the-newcomers-guide-to-cyber-threat-actor-naming-7428e18ee263>.
- “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure,” CISA. 20 Apr 2022 <https://www.cisa.gov/uscert/ncas/alerts/aa22-110a>.
- “Seduploader,” Malpedia. N.a. <https://malpedia.caad.fkie.fraunhofer.de/details/win.seduploader>.
- Then, Ewdison. “SolarWinds Hack Also Affected A Hospital, Major Tech Companies,” Slash Gear. 22 December 2020. https://www.slashgear.com/solarwinds-hack-also-affected-a-hospital-major-tech-companies-22652129?utm_campaign=clip
- “Threat Profiles,” SecureWorks. N.a. <https://www.secureworks.com/research/threat-profiles?filter=item-russia>





Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**



Questions



FAQs

Upcoming Briefing

- June 2, 2022 – The Return of Emotet

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.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



About HC3

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



Office of
Information Security
Securing One HHS



**Health Sector Cybersecurity
Coordination Center**

What We Offer

Sector and Victim Notifications

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

Alerts and Analyst Notes

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

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center

Contacts



[HHS.GOV/HC3](https://www.hhs.gov/hc3)



HC3@HHS.GOV