LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

An Analysis of the Russia/Ukraine Conflict

03/17/2022

TLP: WHITE, ID# ***202203171300***

Agenda

- Russo-Ukrainian War: A Timeline
- Roots of the Conflict
- The World Responds…
- … As Does Hacktivist Group Anonymous…
- …And the Conti RaaS Group
- Russian Attacks on Healthcare in Recent History: NotPetya
- Russian Attacks on Healthcare in Recent History: FIN12
- Russian Attacks on Healthcare in Recent History: Ryuk
- Russian Cyber Operations Against Ukraine
- HermeticWiper
- WhisperGate
- Potential Impact on the U.S. HPH
- Best Practices and Mitigations
- Russian Tactics, Techniques, Procedures

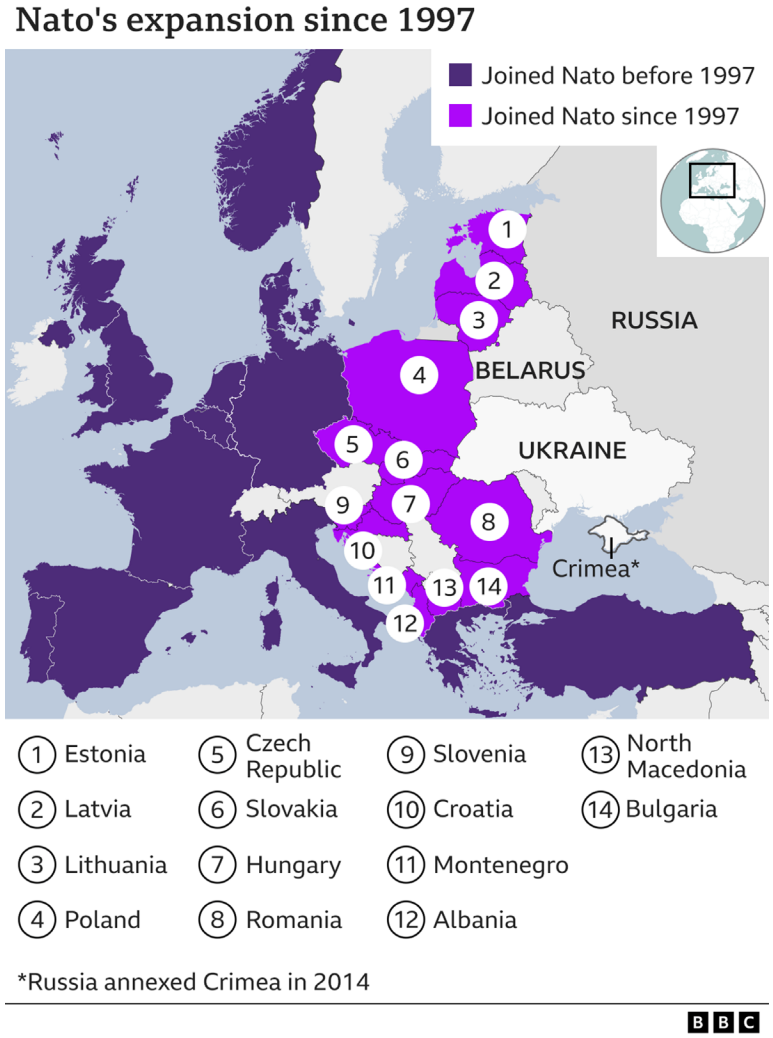
Slides Key:

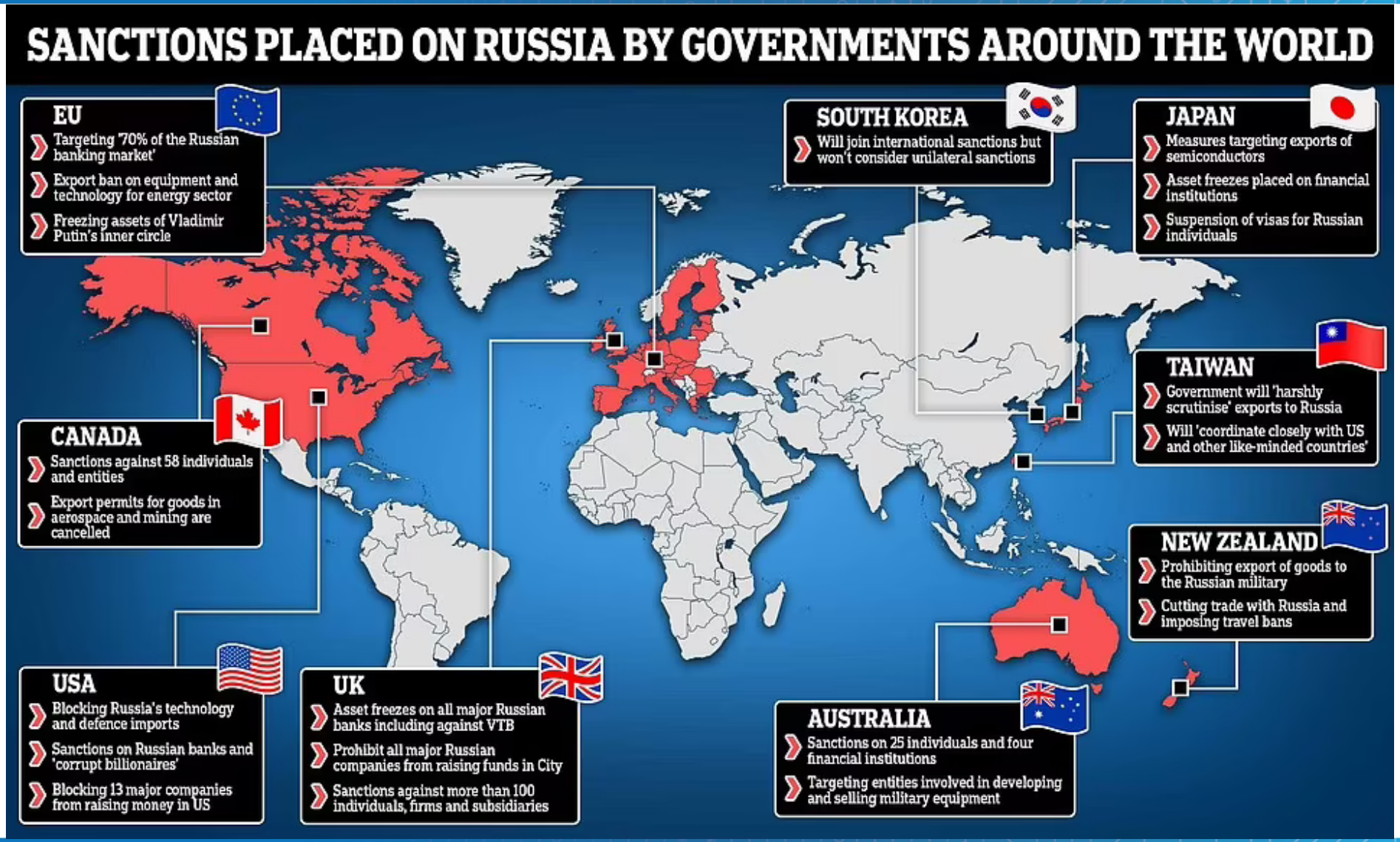
Non-Technical: Managerial, strategic and high-level (general audience)

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

- 2014 Action in Crimea
  - The Russian military crossed into Ukrainian territory after an uprising replaced the Russia-friendly Ukrainian president with a pro-Western government.
  - Russia then annexed Crimea and inspired a separatist movement in the east.
  - Although a cease-fire was negotiated in 2015, fighting continued.
- Tensions escalate again in October 2021
  - Russia began moving troops and military equipment (including armor, missiles, and other heavy weaponry) near its border with Ukraine with no explanation.
- 2022 Conflict
  - On February 24, Russia invaded Ukraine. In response, Ukraine declared a 30-day state of emergency as cyberattacks knocked out government institutions and Ukrainian President Volodymyr Zelenskyy declared martial law. The foreign minister called the attacks “a full-scale invasion” and called on the world to “stop Putin.”

- Complicated topic impossible to fully cover or explain here.
- Russia considers Ukraine within its sphere of influence and has grown unnerved at Ukraine's closeness with the West, as well as the prospect that the country might join NATO or the European Union. Some Russian political figures view Ukrainian sovereignty as illegitimate or as a relatively recent invention.
- Putin said he was acting after receiving a plea for assistance from leaders of Russian-backed separatist territories, citing false accusations.
- Putin claimed that his goal was to protect people subjected to bullying and genocide and aimed for the "demilitarization and de-Nazification" of Ukraine.



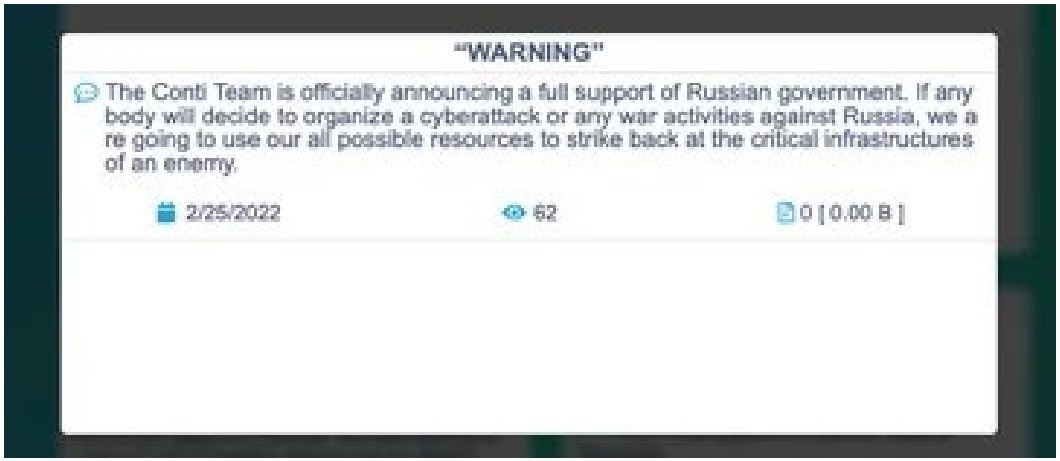

SANCTIONS PLACED ON RUSSIA BY GOVERNMENTS AROUND THE WORLD
EU
Targeting '70% of the Russian banking market'
Export ban on equipment and technology for energy sector
Freezing assets of Vladimir Putin's inner circle
SOUTH KOREA
Will join international sanctions but won't consider unilateral sanctions
JAPAN
Measures targeting exports of semiconductors
Asset freezes placed on financial institutions
Suspension of visas for Russian individuals
TAIWAN
Government will 'harshly scrutinise' exports to Russia
Will 'coordinate closely with US and other like-minded countries'
CANADA
Sanctions against 58 individuals and entities
Export permits for goods in aerospace and mining are cancelled
NEW ZEALAND
Prohibiting export of goods to the Russian military
Cutting trade with Russia and imposing travel bans
USA
Blocking Russia's technology and defence imports
Sanctions on Russian banks and 'corrupt billionaires'
Blocking 13 major companies from raising money in US
UK
Asset freezes on all major Russian banks including against VTB
Prohibit all major Russian companies from raising funds in City
Sanctions against more than 100 individuals, firms and subsidiaries
AUSTRALIA
Sanctions on 25 individuals and four financial institutions
Targeting entities involved in developing and selling military equipment

… As Does Hacktivist Group Anonymous

- On February 24, members of Anonymous announced on Twitter that they would be launching attacks against the Russian government.
- The hacktivists defaced some local government websites in Russia and temporarily took down others, including the website of Russian news outlet RT.
- The group claimed on February 25 that it would leak login credentials for the Russian Ministry of Defense website.

…And the Conti RaaS Group

- On February 25, the Conti RaaS group announced it was supporting Russia and the Russian people.
- Conti is well known to hit organizations where IT outages can have life-threatening consequences, including HPH organizations. The group is connected to more than 400 cyberattacks worldwide, approximately 300 of which were against U.S.-based organizations. Demands can be as high as $25 million.
- Conti later walked back the statement after receiving criticism from members and the cybercriminal community.
- A Ukrainian nationalist member of the RaaS group leaked internal chats, source code, and stolen data in retaliation.
- “Greetings,” one tweet began. “Here is a friendly heads-up that the Conti gang has lost its s****.” The message included a link that would allow anyone to download almost two years of private chats. “We promise it is very interesting,” the tweet added.

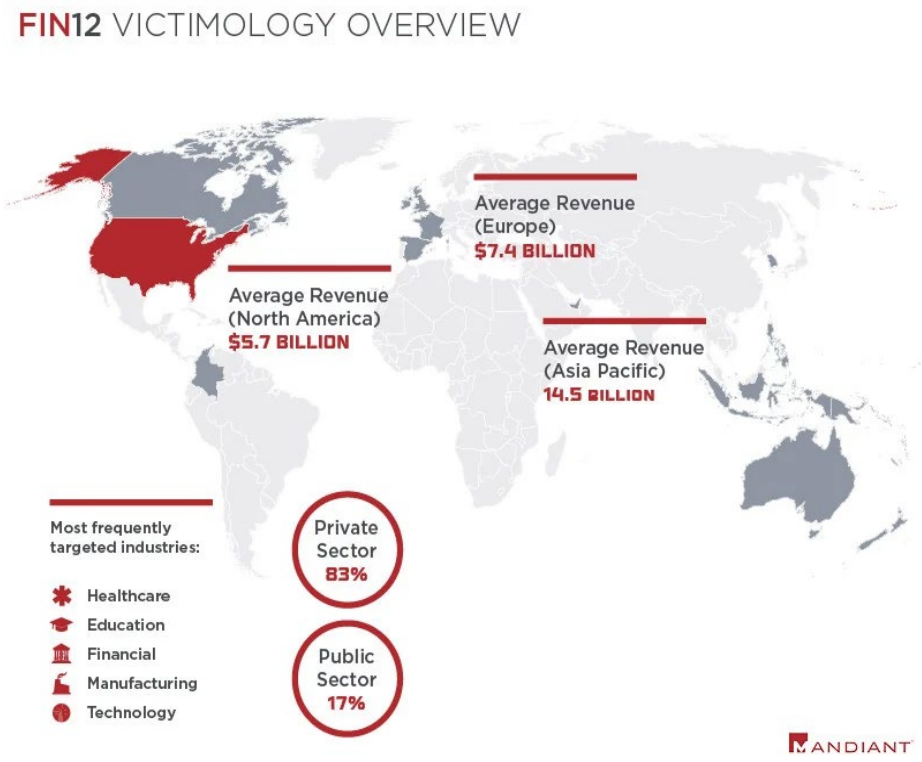


Russian Attacks on Healthcare in Recent History: NotPetya

- NotPetya ransomware is an evolved strain of the Petya ransomware.
- Ransomware is malware where the threat actors make sure that essential files are encrypted so they can ask for large ransom amounts.
- It is more noteworthy due to a few major tweaks, one being the use of EternalBlue – a Windows Server Message Block (SMB) exploit, in which the attack method is the same exploit that allowed WannaCry to spread so rapidly. It is also combined with password-harvesting tools based on Mimikatz, which allowed NotPetya to propagate between devices in a wormable fashion, spreading across businesses and corporate networks even without human interaction.
- NotPetya made it so that it was technically impossible to recover the victim's files after the payload had been executed.
- Initially launched against Ukraine in June 2017.
- Subsequently spread globally, disrupting operations at a major U.S. pharmaceutical company, a major U.S. health care communications company and U.S. hospitals.

Russian Attacks on Healthcare in Recent History: FIN12

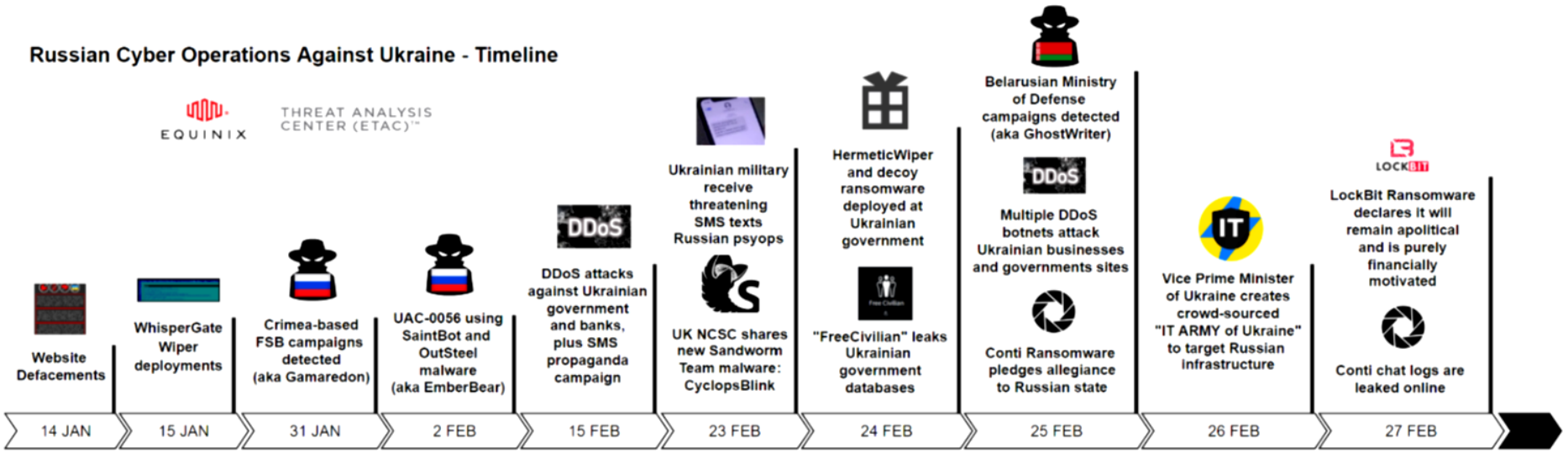
- FIN12 is a Russian-speaking cybercriminal group known to target hospitals and health care groups across North America using ransomware.
- Annual revenue of more than $300 million.
- One in five of FIN12's victims are healthcare groups; FIN12 is responsible for multiple major attacks on the U.S. healthcare system.
- The group remains focused purely on ransomware, moving faster than its peers and hitting big targets/high-revenue victims.
- For more information on FIN12, consult HC3's threat brief from December 2021:
  - Threat Brief 12/02/2021: FIN12 as a Threat to Healthcare



Russian Attacks on Healthcare in Recent History: Ryuk

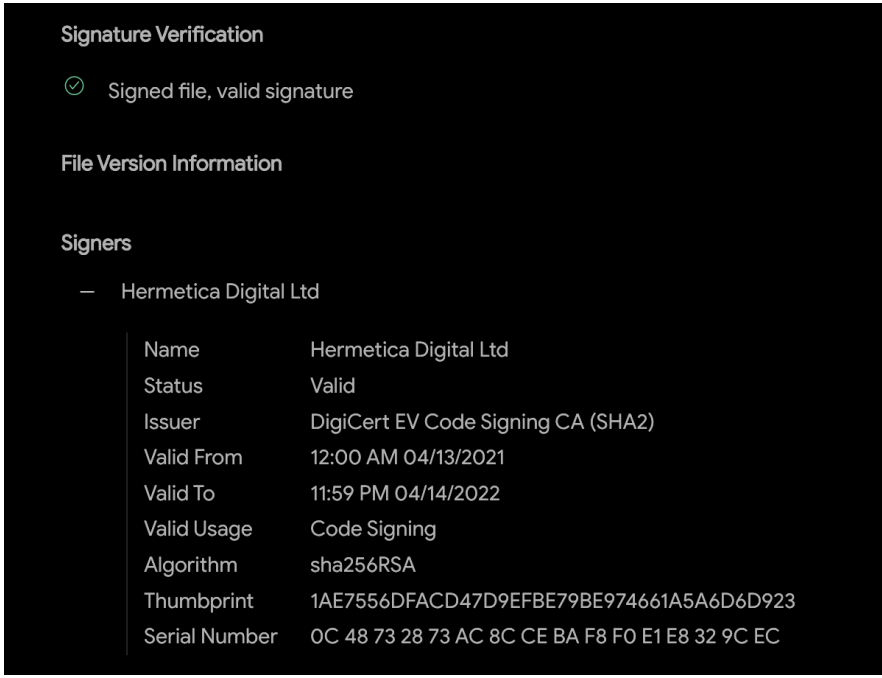
- Ryuk is one of the first ransomware variants to include the ability to identify and encrypt network drives and resources, as well as delete shadow copies on the endpoint.
  - Attackers can disable Windows System Restore for users, making it impossible to recover from an attack without external backups or rollback technology.
- Since 2018, the Ryuk ransomware attack has wreaked havoc on at least 235 hospitals and inpatient psychiatric facilities, as well as dozens of other healthcare facilities.
  - The result: suspended surgeries, delayed medical care, and the loss of millions of dollars (as of June 2021).
- HC3's previous coverage of Ryuk can be found at:
  - Threat Brief 04/08/2021: Ryuk Variants
  - Threat Brief 11/12/2020: Trickbot and Ryuk
  - Threat Brief 01/30/2020: Ryuk Update

Russian Cyber Operations Against Ukraine



HermeticWiper

- HermeticWiper is a new form of disk-wiping malware that was used to attack organizations in Ukraine shortly before the launch of the Russian invasion.
- Some quick facts about the HermeticWiper:
  - It leverages a signed driver, which is used to deploy a wiper that targets Windows devices, manipulating the master boot record in such a way that causes boot failure.
  - It uses a digital certificate issued under the Cyprus-based company called “Hermetica Digital Ltd” – which is a company that likely does not exist or is not operational if it does.
  - The certificate is valid as of April 2021, but it does not appear to be used to sign any files.



- WhisperGate is a new form of disk-wiping malware that is believed to operate in three stages/parts:
  - A bootloader that corrupts detected local disks
  - A Discord-based downloader
  - A file wiper
- WhisperGate has been observed attacking organizations in Ukraine shortly before the launch of the Russian invasion on February 24, 2022.
- The WhisperGate bootloader complements its file-wiper counterpart. Both irrevocably corrupt the victim's data and attempt to disguise themselves as ransomware operations.
- More about HermeticWiper and WhisperGate can be found in the HC3 Sector Alert published on March 1, 2022, entitled The Russia-Ukraine Cyber Conflict and Potential Threats to the US Health Sector.

```
Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us  $10k via bitcoin wallet
1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23'
054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

- Three concerns:
  - That hospitals and health systems may be targeted directly by Russian-sponsored cyber actors.
  - That hospitals and health systems may become incidental victims of Russian-deployed malware or destructive ransomware.
  - That a cyberattack could disrupt hospitals' services.

- Be prepared.
  - Confirm reporting processes and minimize personnel gaps in IT/OT security coverage.
- Create, maintain, and exercise a cyber incident response plan, resilience plan, and continuity of operations plan so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline. Hospitals and health systems should implement 4- to 6-week business continuity plans and well-practiced downtime procedures.
- Enhance your organization's cyber posture.
  - Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.
  - Increase staff awareness of the greater risk for receiving malware-laden phishing emails.
  - Check network and data backups and make sure that multiple copies exist – off-line, network segmented, on-premises, and in the cloud, with at least one immutable copy.
- Geo-fencing for all inbound and outbound traffic originating from, and related to, Ukraine and its surrounding region, as well as identifying all internal and third-party mission-critical clinical and operational services and technology. SANS is offering tips on how to do this: Geoblocking When You Can't Geoblock.
- Increase organizational vigilance. Stay current on reporting on this threat.
- Check out CISA's Shields-Up for more information on guidance, mitigations, and reporting on malicious activity that may be associated with the conflict.

Russian Tactics, Techniques, Procedures

- Russian state-sponsored advanced persistent threat (APT) actors have used common but effective tactics—including spear phishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security—to gain initial access to target networks.
- Vulnerabilities known to be exploited by Russian state-sponsored APT actors for initial access include:
  - CVE-2018-13379 FortiGate VPNs
  - CVE-2019-1653 Cisco router
  - CVE-2019-2725 Oracle WebLogic Server
  - CVE-2019-7609 Kibana
  - CVE-2019-9670 Zimbra software
  - CVE-2019-10149 Exim Simple Mail Transfer Protocol
  - CVE-2019-11510 Pulse Secure
  - CVE-2019-19781 Citrix
  - CVE-2020-0688 Microsoft Exchange
  - CVE-2020-4006 VMWare (note: this was a zero-day at time.)
  - CVE-2020-5902 F5 Big-IP
  - CVE-2020-14882 Oracle WebLogic
  - CVE-2021-26855 Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

Reference Materials

References

- Barr, Luke and Mallin, Alexander. “DOJ official warns companies 'foolish' not to shore up cybersecurity amid Russia tensions,” 17 February 2022. ABC News. https://abcnews.go.com/Politics/doj-official-warns-companies-foolish-shore-cybersecurity-amid/story?id=82959520.
- Constantin, Lucian. “Conti gang says it's ready to hit critical infrastructure in support of Russian government,”CSOOnline 25 February 2022. https://www.csoonline.com/article/3651498/conti-gang-says-its-ready-to-hit-critical-infrastructure-in-support-of-russian-government.html.
- Duell, Mark. “Russia sanctioned by the world: How world leaders putting the financial thumbscrews on Putin have done nothing to halt his forces rampaging across Ukraine... as India and China refuse to stop trading,” DailyMail. 25 February 2022. https://www.dailymail.co.uk/news/article-10550811/How-Russia-sanctioned-world-Ukraine-invasion.html.
- “Conflict in Ukraine,” Council on Foreign Relations. 8 March 2022. https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine.
- Greig, Jonathan. “Anonymous hacktivists, ransomware groups get involved in Ukraine-Russia Conflict,” ZDNet. 25 February 2022. https://www.zdnet.com/article/anonymous-hacktivists-ransomware-groups-get-involved-in-ukraine-russia-conflict/.
- Gwengoat. “Ukraine vs Russia stock photo,” iStock. 25 June 2019. https://www.istockphoto.com/photo/ukraine-vs-russia-gm1158059333-316205199.
- Henderson, Jennifer. “Watch Out for Cyberattacks Following Russia's Invasion of Ukraine,” MedPage Today. 25 February 2022.https://www.medpagetoday.com/special-reports/exclusives/97385#:~:text=Since%202018%2C%20the%20Ryuk%20ransomware,Street%20Journal%20reported%20last%20June.

References

- Hickman, Richard. “Conti Ransomware Gang: An Overview,” Unit42. 18 June 2021. https://unit42.paloaltonetworks.com/conti-ransomware-gang/.
- Ilascu, Ionut. “FIN12 hits healthcare with quick and focused ransomware attacks,” Bleeping Computer. 7 October 2021. https://www.bleepingcomputer.com/news/security/fin12-hits-healthcare-with-quick-and-focused-ransomware-attacks/.
- Kirby, Paul. “Why has Russia invaded Ukraine and what does Putin want?,” BBC News. 7 March 2022. https://www.bbc.com/news/world-europe-56720589.
- Ma, Alexandra. “Switzerland breaks neutral status to sanction Russia over Ukraine invasion,” Business Insider. 28 February 2022. https://www.businessinsider.com/switzerland-sanctions-russia-breaks-neutral-status-ukraine-invasion-2022-2.
- Matt. “Scared Hamster,” Know Your Meme. 29 January 2019. https://knowyourmeme.com/memes/scared-hamster.
- McKeon, Jill. “AHA: Russia’s Invasion of Ukraine Could Lead to Healthcare Cyberattacks,” Health IT Security. 22 February 2022. https://healthitsecurity.com/news/aha-russias-invasion-of-ukraine-could-lead-to-healthcare-cyberattacks.
- Miller, Maggie. “Russian-speaking hacking group scaling up ransomware attacks on hospitals,” The Hill. 7 October 2021. https://thehill.com/policy/cybersecurity/575787-russian-speaking-hacking-group-scaling-up-ransomware-attacks-on?rl=1.
- Pitrelli, Monica Buchanan. “Global hacking group Anonymous launches ‘cyber war’ against Russia,” CNBC. 1 March 2022. https://www.cnbc.com/2022/03/01/how-is-anonymous-attacking-russia-disabling-and-hacking-websites-.html.

References

- "Russia-Ukraine War," The New York Times. 8 March 2022. https://www.nytimes.com/news-event/ukraine-russia.
- Riley, Charles. "What is SWIFT and how is it being used against Russia?," CNN. 28 February 2022. https://www.cnn.com/2022/02/28/business/swift-sanctions-explainer/index.html.
- "Ryuk ransomware," Malwarebytes. n.d. https://www.malwarebytes.com/ryuk-ransomware.
- Shepherd, Adam. "What is NotPetya?," ITPro. 8 October 2021. https://www.itpro.com/malware/34381/what-is-notpetya.
- Temple-Raston, Dina. "Inside Conti leaks: The Panama Papers of ransomware," The Record. 8 March 2022. https://therecord.media/conti-leaks-the-panama-papers-of-ransomware/.
- "The Russia-Ukraine Cyber Conflict and Potential Threats to the US Health Sector," HC3: Analyst Note, 202203011700 (1 March 2022): 1-10. https://www.hhs.gov/sites/default/files/russia-ukraine-cyber-conflict-analyst-note-tlpwhite.pdf
- Toh, Ardan. "Ryuk Ransomware," Proficio. n.d. https://www.proficio.com/ryuk-ransomware/.
- "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," CISA. 11 January 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-011a.

Questions

Upcoming Briefs

- 4/7 – BazarBackdoor as a Threat to the U.S. Health Sector
- 4/21 – Insider Threats and the Healthcare Industry

Requests for Information

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

Product Evaluations

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

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. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & 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.

White Papers

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

Threat Briefings & Webinar

Briefing 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.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV