Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare ○ TLP:WHITE Alert ID : b3287e09 Feb 27, 2023, 09:27 AM

This week, Hacking Healthcare begins with an update on Russian cyber retaliation against Germany for policy decisions that supported Ukraine. We break down just how swiftly cyber capabilities were weaponized against German government and critical infrastructure, and we make the case for building resiliency against some less sophisticated types of cyberattacks. Next, we stick to the international stage as we assess the recent news of a multinational takedown of the prolific Hive cybercriminal group. Beyond summarizing the law enforcement action, we analyze the overall effect these sorts of operations have on the ransomware ecosystem, and then we provide some best practices for mitigating ransomware risks.

Welcome back to *Hacking Healthcare*.

German Support for Ukraine Leads to Cyberattacks on Critical Infrastructure

In another example of how geo-politics influences malicious cyber activity, German critical infrastructure sectors came under cyberattack soon after the German government signaled its intent to further support Ukraine. The events reiterate how cyberattacks often fall in the grey area between accepted retaliatory actions by governments, such as trade sanctions, and unacceptable ones, such as military strikes. The swiftness of the attacks and who carried them out are notable.

On January 25th, the German government agreed to send Leopard 2 tanks to aide Ukraine in their fight against Russian aggression. The German government had been resistant to the idea, in part over concerns it might increase risk to German interests. However, international pressure appears to have succeeded in changing their policy.[i] Russian cyber retaliation was swift.
Within 24 hours of the announcement, reports indicated that hacking groups aligned with the Russian government had launched attacks against a wide range of German organizations.[ii] Victims included those in critical

infrastructure sectors like transportation and finance, as well government agencies.[iii] Several pro-Russian “hacktivist” groups are said to be responsible, but their level of independence from the Russian state is an open question.[iv]

The German Federal Office for Information Security (BSI), which acts as Germany’s federal cybersecurity authority, has stated that the malicious actions were largely limited to distributed denial-of-service (DDoS) attacks.[v] These have had little serious effect, but several websites were put offline. Russia’s more serious cyber capabilities appear limited to use against Ukraine, where a new destructive wiper was seen just last week.[vi]

Action & Analysis
Included with H-ISAC Membership

FBI Seizes Infrastructure from one of Healthcare’s Largest Ransomware Attackers

The Hive ransomware group has earned a reputation for their prolific cyber operations that have victimized “more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms, and critical infrastructure.”[xi] Those operations will be disrupted, at least for a little while, due to a joint law enforcement action involving the U.S. Justice Department (DOJ) and international partners from Germany and the Netherlands. According to the DOJ, the FBI was able to successfully seize two servers in Los Angeles, California that were behind Hive’s ransomware attacks.[xii]

According to Cyberscoop, “Hive has targeted more than 1,500 victims globally since June 2021, and caused major disruptions for health care providers and hospitals during the height of the pandemic”[xiii]. Common disruptions seen because of these attacks vary from electronic system shutdowns, and cancellations of scheduled care, to ambulance diversion.

The DOJ described Hive’s activities as being “responsible for extorting and attempting to extort hundreds of millions of dollars from victims in the United States and around the world,” which is why the success of the FBI operation is behind heralded as a major win in the ongoing battle against ransomware.[xiv] In total, the FBI has distributed over 300 decryption keys to recent Hive victims, over 1,000 decryption keys for prior victims, and has prevented an estimated $130 million in ransomware payments.[xv]

Hive’s operations, while prolific, do not appear to be particularly unique. Hive reportedly operates ransomware-as-a-service (RaaS) to generate much of its revenue.[xvi] For those not ingrained in the cybercriminal world, RaaS is a business model between ransomware operators and affiliates, where affiliates pay to launch ransomware attacks that have already been developed by operators. Purchasing a readily available RaaS kit from Hive on the dark web allows affiliates that lack the skill or time to develop their own ransomware to be up and running quickly and affordably.

The DOJ, citing the Cybersecurity and Infrastructure Security Agency (CISA), further relayed that “Hive affiliates have gained initial access to victim networks through a number of methods, including: single factor logins via Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other remote network connection protocol”.[xvii] Hive is reported to be convert to the double-extortion attack method. This tactic involves extracting sensitive data before encrypting the system, enabling them to ask for ransom to both decrypt the system and to not publish the stolen information. The Department of Justice noted that Hive focused on extracting the the most sensitive data in a victim’s system to increase the pressure to pay.[xviii]

Action & Analysis
Included with H-ISAC Membership

[i] https://www.reuters.com/world/europe/germany-approves-sending-heavy-leopard-tanks-ukraine-2023-01-25/
[ii] https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/
[iii] https://www.theregister.com/2023/01/30/russian_hackers_ddos_germany/
[iv] https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/
[v] https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/
[vi] https://twitter.com/ESETresearch/status/1618960022150729728
[vii] https://foreignpolicy.com/2022/04/09/russia-putin-propaganda-ukraine-war-crimes-atrocities/
[viii] https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/
[ix] https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf
[x] https://www.hipaajournal.com/2021-saw-record-numbers-of-ddos-attacks-on-the-healthcare-industry/
[xi] https://www.cybersecuritycoalition.org/frameworks/ddos-profile
[xii] https://cyberscoop.com/fbi-europol-hive-ransomware-group/
[xiii] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
[xiv] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
[xv] https://www.nextgov.com/technology-news/2023/01/justice-hacked-hackers-hive-ransomware-stopping-130m-demands/382279/
[xvi] https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/

Congress
Tuesday, January 24th:
- No relevant hearings

Wednesday, January 25th:
- No relevant hearings

Thursday, January 26th:
- No relevant hearings

International Hearings/Meetings
- No relevant meetings

European Union
- No relevant meetings

Reference | References

The Register
US Department of Justice
Whitehouse
Nextgov
HIPAA Journal
Reuters
Twitter
Reuters

Cyberscoop
HHS
cybersecuritycoalition
foreignpolicy

Report Source(s)

Health-ISAC

Tags

Hacking Healthcare, Geopolitics, Law Enforcement, DDoS, Europe, Ransomware

---

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.
John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org