Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ | TLP:WHITE | Alert ID : c472379e | Jul 02, 2024, 03:42 PM

This week, *Hacking Healthcare*™ examines the French Cybersecurity Agency's (ANSSI) 2023 Cyber Threat Overview to gain a European perspective on how the cyber threat landscape is evolving.[i] In particular, we will look at the developments and trends that may have significant impacts on the healthcare sector throughout the rest of 2024.

2024 Fall Americas Summit: Call for Papers

While there are still many months before the Health-ISAC's 2024 Fall Americas Summit kicks off in Phoenix, Arizona, from December 2-6, 2024, time is running out to submit presentation proposals. If you are interested in sharing case studies, lessons learned, real-time strategies (best practices), or current challenges with leaders in the global healthcare community, consider submitting before the July 12 deadline.

Proposals can be submitted via the following link:

https://h-isac.org/summits/2024-fall-americas-summit/

ANSSI 2023 Cyber Threat Overview

ANSSI's third edition of its Cyber Threat Overview is a fairly comprehensive 40 pages and begins with a short summary that highlights the following:[ii]

- Cyber threats continue to increase "against a backdrop of new geopolitical tensions and France hosting international events"
- Cyber threat actors from China, Russia, and general cybercrime pose the most significant threat to critical infrastructure in France
- Strategic and industrial espionage was the primary mobilizing factor for ANSSI
- "The cybercrime ecosystem also keeps on diversifying thanks to the leaks of ransomware source codes"
- ANSSI noted an uptick in "attacks aimed at promoting a political agenda, hindering access to online content or undermining an organisation's reputation"

- Prominent international events like the 2024 Olympic and Paralympic Games may incentivize attacks

The Overview then breaks into covering three high-level issue areas:

The Changing Motivations of Malicious Actors

ANSSI focuses on three specific motivations for attacks, beginning with what ANSSI recognizes as a growing number of attacks seemingly motivated by strategic and industrial espionage. These attacks appear to primarily target policy, technology, and defense industries. More relevant to the public health sector is the second motivation — profit-oriented attacks. While ANSSI does cite more attacks against the public health sector year-over-year, the actual percentage remained constant, around 10%.[iii] The final motivation covered was related to destabilization operations in the context of geopolitical conflict. In particular, ANSSI highlights the work of pro-Russian hacktivists.

Improvement of Offensive Capabilities

ANSSI's overview reiterates the notion that while there is no shortage of tools available to less sophisticated actors looking to carry out effective operations, the higher-end malicious actors continue to adapt and increase their sophistication. This section details the growth in anonymization networks and the diversification of the cybercriminal ecosystem and cybercriminal methods. It also details a rise in the compromise of mobile devices, including those belonging to senior executives of entities tied to a wide range of politically and strategically important sectors.

Opportunities Seized by Attackers

The final section of the Overview cites how malicious actors look to take advantage of software vulnerabilities, how organizations may be taking on risk if they use a managed service provider (MSP), and how major events, such as the 2024 Olympics, can create opportunities and incentives for cyberattacks.

Action & Analysis

Included with Health-ISAC Membership

[i] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-002.pdf

[ii] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-002.pdf

[iii] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-002.pdf

[iv] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-002.pdf

[v] https://h-isac.org/health-isac-hacking-healthcare-2-23-2024/

Report Source(s)

Health-ISAC

Reference | References

Health-ISAC
CERT-FR
Health-ISAC

Tags

Hacking Healthcare, Geopolitics, EU, ANSSI, mobile, Europe

Conferences, Webinars, and Summits:

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

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@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