Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare **TLP:WHITE** **Alert Id: fb2849a3** **2022-11-22 14:00:00**

This week, we dive into the European Union Agency for Cybersecurity (ENISA) Threat Landscape (ETL) report to bring you the EU perspective on what has been going on in the cyber threat landscape from the middle of 2021 to the middle of 2022. We pick out some of the more interesting and relevant findings, and we provide our analysis on how they may impact the healthcare sector.

Welcome back to *Hacking Healthcare*.

ENISA Threat Landscape (ETL) Report Takeaways

On November 3rd, the European Union Agency for Cybersecurity (ENISA) released their 2022 report on the cybersecurity threat landscape.[1] This annual report provides useful insight on what the EU's cybersecurity agency has deemed are the prime cyber threats, as well as trends and motivations among threat actors. Additionally, a comprehensive annex provides a detailed list of incidents, a breakdown of the CVE landscape, and recommendations that are tied back to ISO/IEC 27001 and the NIST Cybersecurity Framework (CSF). Despite its 150-page length, it is written in an approachable manner that non-technical audiences will largely be able to understand. The report was pulled together from data gathered between July 2021 and July 2022.

So, what are some relevant takeaways worth noting?

- Supply Chain: According to the ETL report, both state-backed threat actors and cybercriminal actors are increasingly developing an interest in supply chain attacks and the capabilities to conduct them. The ETL notes that supply chain compromises accounted for 17% of intrusions in 2021, which is a 16-percentage point increase over 2020. ENISA links this increase to lessons learned by threat actors in the aftermath of SolarWinds.

ENISA also assesses that "Cloud Service Providers (CSPs), Managed Services Providers (MSPs), and IT services organisations are prime targets for threat actors to exploit their trust relationships to conduct nefarious operations."[2] Ultimately, ENISA expects to see "cybercriminals to continue targeting the software supply chain and MSPs for the foreseeable future," and that they are "also likely to target the management tools used by MSPs such as professional services automation software (PSA) or remote monitoring and management (RMM) tools."

- Geo-Politics: The ETL report makes clear that the conflict in Ukraine has "reshaped the threat landscape," and that geopolitics continue to play an important role in cyber operations.[3] Three issues that they believe are worth highlighting are the increased hacktivist activity, the mobilization of hacktivist and cybercriminal elements to augment state capabilities, and the uptick in utilizing DDoS.

- Ransomware Rebranding: ENISA notes that it appears increasingly common for ransomware groups to attempt to rebrand ever since the Colonial Pipeline attack "resulted in increased efforts [to crack down] by law enforcement and governments worldwide."[4] The ETL report states that ransomware groups take on average 17 months before rebranding, and that their main motivations may be to:

1. Reboot their operations in case their tools, TTPs, or infrastructure were critically compromised;
2. Avoid law enforcement, media, and political attention;
3. Hinder and delay efforts to attribute an attack so that victims can pay the ransom to a non-sanctioned entity; and
4. Resolve internal disputes.

- Phishing: It is unlikely to be a surprise that ENISA found that "phishing is once again the most common vector for initial access."[5] They also highlighted that "advances in sophistication of phishing, user fatigue and targeted, context-based phishing have led to this rise," and that threat actors continue to adapt phishing campaign content to major world events in the hopes of sparking curiosity.

-

- Operational Technology: ENISA warned in last year's assessment that "the interest of state actors in targeting critical infrastructure and Operational Technology (OT) networks would certainly grow in the near future."[6] According to this year's update, the "assessment held valid as cyber operations targeting such infrastructure primarily for the collection of intelligence, deployment of newly observed ICS-targeting malware, and disruption were all observed."[7]

The ETL report heavily focuses on the threat of state-backed actors increasingly looking to develop OT-focused capabilities that could be used during crisis or conflict. ENISA warns that it is likely that those with an interest in pursuing OT targeting "will continue dedicating resources and developing extensible ICS malware frameworks because of their modularity and capability in targeting multiple victims and equipment used across multiple industries."

- Extortion Trends: One trend worth keeping an eye on according to ENISA is an increase in data theft and extortion without the use of ransomware. Extortion methods have evolved over the past several years to incorporate different tactics to maximize a victim's payout, and this particular iteration appears to be increasing in usage. ENISA notes that cybercriminals have found that they can simply request ransoms related to stolen data without having to go through the trouble of deploying ransomware.

-

- Payment Prohibition: One particularly interesting development is ENISA's call out of ransom payment prohibition legislation and regulation. The ETL report notes that in 2022, the U.S. state of North Carolina "announced that public entities were prohibited from paying ransoms," and the U.S. state of Florida followed suit with something similar for government agencies. ENISA goes on to suggest that "it remains to be seen whether these undertakings will be effective, as [Ransomware-as-a-Service] (RaaS) groups will not limit themselves because of local legislation."[8] They believe that "only in a more global context could these legal measures become more effective."

More comprehensive breakdowns on these issues can be found within the full length ETL report, which is freely available on the ENISA website. We would encourage interested members to review the report for other sections pertinent to them.

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, November 22nd:

- No relevant hearings

Wednesday, November 23rd:

- No relevant hearings

Thursday, November 24th:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

Contact us: follow @HealthISAC

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[3] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[4] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[5] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[7] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[8] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[9] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[10] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

Reference(s): treasury, Europa Analytics

Report Source(s): Health-ISAC

Sources:

https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Tags: Hacking Healthcare, ENISA, Supply Chain, Ransomware

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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