November 2nd, 2021

TLP White

This week, *Hacking Healthcare* begins by taking a look at how government sanctions have apparently forced one major cybercrime group to routinely alter its identity in order to carry out attacks. Next, we break down a multinational guidance document on machine learning and artificial intelligence in medical devices that doesn't shy away from cybersecurity. Finally, we examine a new EU cybersecurity report and pull out three considerations for H-ISAC members.

Please note that Hacking Healthcare will be taking next week off but will return the week of November 16.

Welcome back to *Hacking Healthcare*.

1. **Sanctions Incentivize Ransomware Obfuscation**

   While Evil Corp has been a criminal entity for quite a while, they rose to prominence in cybersecurity circles a few years ago. The Russia-based cybercriminal group became famous for "the development and distribution of the Dridex malware," which it used to "infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries," allegedly netting them over $100 million.[1] If you haven't heard their name pop up recently, it's not because they haven't been active, but it may be because they've been trying to skirt U.S. sanctions by using other names.

   According to reports, Evil Corp has resorted to "limited use ransomware operations under various names such as WastedLocker, Hades, Phoenix Locker, and PayloadBin."[2] They have also been suspected of linkages to DoppelPaymer, and a new iteration called Macaw Locker that recently impacted Sinclair Broadcast Group and medical technology company Olympus.[3, 4] Their avoidance of claiming attacks under the Evil Corp banner appears to be a product of U.S. government sanctions that were levied by the Treasury Department back in 2019.

   On December 5th of that year, the Treasury Department's Office of Foreign Assets Control (OFAC) made Evil Corp, 17 individuals, and six other organizations designated entities. This designation orders their assets to be frozen and prohibits U.S. persons from conducting transactions with them.[5] The ramifications of this designation, such as victims becoming unwilling to pay ransom to them over fear of violating federal

sanctions, have apparently concerned Evil Corp to the extent that they have taken on numerous other monikers to avoid suspicion from victims of their ransomware activities.

Action & Analysis
Included with H-ISAC Membership

2. Multinational Guidance Principles for Medical Device Machine Learning Released

Last week, the U.S. Food and Drug Administration (FDA), Health Canada, and the United Kingdom's Medicines and Healthcare products Regulatory Agency (MHRA) jointly released a two-page guidance document to "help promote safe, effective, and high-quality medical devices that use artificial intelligence and machine learning (AI/ML)."[6] Importantly, security was a key topic emphasized in the guidance.

As the concise document explains, "Artificial intelligence and machine learning technologies have the potential to transform health care. . . . But they also present unique considerations due to their complexity and the iterative and data-driven nature of their development."[7] Understandably, the paragraph-length guiding principles are not highly detailed, but they do "identify areas where the International Medical Device Regulators Forum (IMDRF), international standards organizations, and other collaborative bodies could work to advance [good machine learning practices]."[8]

The authors' vision is that the 10 principles may be used to:[9]

- Adopt good practices that have been proved in other sectors
- Tailor practices from other sectors so they are applicable to medical technology and the healthcare sector
- Create new practices specific for medical technology and the healthcare sector

In total, the principles are:

1. Multi-disciplinary expertise is leveraged throughout the total product life cycle
2. Good software engineering and security practices are implemented
3. Clinical study participants and data sets are representative of the intended patient population
4. Training data sets are independent of test sets
5. Selected reference datasets are based upon best available methods
6. Model design is tailored to the available data and reflects the intended use of the device

7. Focus is placed on the performance of the human-ai team
8. Testing demonstrates device performance during clinically relevant conditions
9. Users are provided clear, essential information
10. Deployed models are monitored for performance and retraining risks are managed

Action & Analysis
Included with H-ISAC Membership

3. 2021 ENISA Threat Landscape Report Released

The ninth edition of the European Union Agency for Cybersecurity's (ENISA) Threat Landscape report was released last week. The annual report details "the status of the cybersecurity threat landscape," including "prime" threats, major trends, threat actors, and attack techniques.[10] The report's findings provide a European perspective on the cyber threat environment and are tailored to be most useful to those in strategic decision-making roles.

Based on data and analysis from April 2020 through July 2021, some of the most relevant conclusions from the report are:

- Ransomware remained the primary threat during this time period, and there has been a noted rise in "triple extortion" attacks
- COVID-19 is "still the dominant lure in campaigns for e-mail attacks"
- ENISA noted a "surge" in healthcare sector-related data breaches
- COVID-19's spread appears to correlate with a "spike in non-malicious incidents"
- Sophisticated supply chain compromises proliferated
- Cybercrime is increasingly targeting critical infrastructure entities

Action & Analysis
Included with H-ISAC Membership

November 2nd, 2021

Congress

Tuesday, November 2nd:

- No relevant hearings

Wednesday, November 3rd:

- Senate – Homeland Security and Governmental Affairs Committee: Business meeting to consider a number of cybersecurity related bills
- House of Representatives – Committee on Homeland Security: "Evolving the U.S. Approach to Cybersecurity: Raising the Bar Today to Meet the Threats of Tomorrow."
- House of Representatives - Committee on Financial Services - Cyber Threats, Consumer Data, and the Financial System"
- House of Representatives - Committee on Transportation and Infrastructure - "The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure."

Thursday, November 4th:

- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits –

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

Contact us: follow @HealthISAC, and email at contact@h-isac.org

---

[1] https://home.treasury.gov/news/press-releases/sm845

[2] https://www.bleepingcomputer.com/news/security/evil-corp-demands-40-million-in-new-macaw-ransomware-attacks/

[3] https://www.bleepingcomputer.com/news/security/olympus-us-systems-hit-by-cyberattack-over-the-weekend/

[4] https://www.bleepingcomputer.com/news/security/evil-corp-demands-40-million-in-new-macaw-ransomware-attacks/

[5] https://home.treasury.gov/news/press-releases/sm845

[6] https://www.fda.gov/media/153486/download

[7] https://www.fda.gov/media/153486/download

[8] https://www.fda.gov/media/153486/download

[9] https://www.fda.gov/media/153486/download

[10] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021