Threat Intelligence and Intelligence Sharing

Angela Milova

Palo Alto - Secure the Future

1. Identify two specific cybersecurity threat intelligence sources you should monitor and explain why they are valuable to the industry as a whole.

Nowadays, companies have more help in staying safe from online threats. There are both fancy tools for big businesses and some free ones for everyone. Two really good free tools I've found are the MITRE ATT&CK Framework and the Abuse.ch project.

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework serves as a comprehensive knowledge base delineating the actions and behavior of threat actors. It has a special part called TTPs (Tactics, Techniques, and Procedures), providing a detailed mapping of the methods threat actors may employ across different stages of the cyber kill chain (Xiong, Legrand, Åberg, et al., 2022). This map is super useful for companies because it helps them understand how attackers could try to get into their systems, aiding them in assessing the security of their systems and formulating effective response strategies. It's like having a guide to check if your systems are safe and what to do if they're not. MITRE ATT&CK is not just a standalone resource but a widely adopted framework within the cybersecurity community, fostering collaboration among organizations. Its broad usage makes it an excellent collaborative tool for sharing insights, mitigating risks, and collectively enhancing incident response capabilities. On the other hand, Abuse.ch is a research project hosted by the Institute for Cybersecurity and Engineering at Bern University, offering diverse platforms tailored to the needs of various companies and organizations (Abuse.ch, n.d). Focused primarily on real-time threat feeds related to malicious activities such as malware, phishing, and botnets, Abuse.ch provides invaluable platforms starting with 1. Malware Bazaar: This platform facilitates the exchange of information about malwares used by malicious actors, including malware samples.

Organizations can leverage this to test the impact of malwares in their environment and enhance their security measures. 2. Feodo Tracker: A tracker for botnet command and control (C2), this resource assists organizations in monitoring their systems for the presence of threats like Emotet, Dridex, and TrickBot. Threat Fox is another great platform they offer, showing a wealth of indicators of compromise (IOCs), Threat Fox helps organizations identify patterns indicative of security incidents (Haircutfish, 2022). An IOC is a piece of evidence or artifact observed on a network or system that indicates a security incident. It reveals a pattern suggesting that a compromise or malicious activity has occurred. Common examples of IOCs include malicious IP addresses or file hashes, which have been used and are now documented for their activity. TTPs refer to methods and tactics that adversaries can use to achieve their objectives. Examples of TTPs would be social engineering tactics malicious actors use to reach their goals (Cyberseer, n.d.). Having information regarding IOCs and TTPs can be an invaluable resource for organizations to stay updated on security risks.

In conclusion, these free resources, exemplified by MITRE ATT&CK and Abuse.ch, are pivotal in empowering organizations to fortify their cybersecurity posture, providing insights, collaborative opportunities, and real-time threat intelligence crucial for effective defense against evolving threats.

2. Describe some of the regulatory or compliance standards for your sector that would impact the types of information you would share with your intelligence community in the future.

In the health sector, numerous compliance standards significantly impact the types of information that can be shared with the intelligence community. To begin with, the Health Insurance Portability and Accountability Act (HIPAA) serves as a guardian of patient privacy, placing strict restrictions on information sharing without patient consent (Bodie, 2022 p.118). Even in the context of sharing threat data, where user medical and personal information might not be immediately relevant, the health sector must exercise the utmost caution to ensure that shared intelligence data remains void of patient data. Additionally, the General Data Protection Regulation (GDPR), a European regulation with global influence, extends its rigorous requirements regarding the processing and transferring of personal data to organizations worldwide (Regulation, G. D. P., 2018). While GDPR primarily applies to European citizens, compliance with GDPR is crucial for those in the health sector due to the potential presence of personal data belonging to European citizens. Similarly, the Federal Information Security Management Act (FISMA), which primarily deals with government data, emphasizes the need for prudence when sharing threat intelligence data to maintain regulatory compliance and uphold the security and integrity of government information (Taylor, 2013). The Drug Enforcement Administration (DEA) regulations, governing controlled substances in the healthcare sector stress the prohibition of unauthorized access, compelling organizations to exercise extreme care in sharing information to prevent any compromise in the handling of controlled substances (Sacco, 2014). Lastly, the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework by the health sector, while not healthcare-specific regulation, reflects a

commitment to robust cybersecurity practices, aligning with a widely recognized standard that enhances overall cybersecurity resilience (Plan, N. P. A, n.d). These compliance standards are integral components of the health sector's unwavering commitment to patient privacy, data security, and ethical information handling in the face of evolving cyber threats.

References

Abuse.ch. BFH. (n.d.). https://www.bfh.ch/en/research/reference-projects/abuse-ch/

Bodie, M. T. (2022). HIPPA. *Cardozo L. Rev. De-Novo*, 118.

From IOC to TTP - Cyberseer. (n.d.).

Haircutfish. (2022, December 6). TryHackMe threat intelligence tools - task 4 abuse.ch,.Medium.

Plan, N. P. A. National Institute of Standards and Technology (NIST). Retrieved from.

Regulation, G. D. P. (2018). General data protection regulation (GDPR). Intersoft Consulting, Accessed in October, 24(1).

Sacco, L. N. (2014). Drug enforcement in the United States: History, policy, and trends (Vol. 7). Washington, DC: Congressional Research Service.

Taylor, L. P. (2013). FISMA compliance handbook. Newnes.

Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, *21*(1), 157-177.