C

Cyber Threat Intelligence Sharing

Daniel Schlette
Chair of Information Systems, University of Regensburg, Regensburg, Germany

Synonyms

Security information sharing

Definition

Cyberattacks carried out by malicious actors often contain common elements. Tactics, techniques, and procedures (TTP) including malware and exploited vulnerabilities are reused and applied world-wide. By sharing cyber threat intelligence, organizations and security analysts can help each other to properly react to security incidents or prevent futures ones. Interorganizational Cyber Threat Intelligence (CTI) sharing is defined as the exchange and collaboration on any security information relevant to strengthen the security posture. As a subdomain of CTI, the joint undertaking of CTI sharing copes with not only technologies, data formats, but also legal elements, trust, and other human factors (Johnson et al. 2016).

Background

The intention behind cyber threat intelligence sharing is twofold. First, there is the need to react upon threats with swift response to ensure information systems' security (Pawlinski et al. 2014). Shared CTI allows organizations to skip at least some parts of time-consuming threat analysis. In conjunction with dedicated CTI sharing platforms, relevant threat information can be received automatically and applied where appropriate. Additionally, a second motivation stems from the limited analysis capabilities within an individual organization. CTI sharing supports building knowledge among information security defenders from multiple organizations. Thereby, external perspectives, insights, and complementary threat information are integrated. As the threat landscape is vast and constantly changing, CTI sharing proves to be an integral element to deal with inefficiencies and incomplete CTI (Skopik et al. 2016). Overall, it can easily be inferred that the notion "sharing is caring" applies to CTI as well. When it comes to the question of how CTI sharing is performed, a shift from informal procedures to formal, structured, and platform-centered approaches can be observed. While e-mail and other unstructured communication channels still serve as exchange mechanisms today, there

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1717-1

is a much stronger emphasis on CTI sharing platforms (Sauerwein et al. 2017). This is due to fact that the incorporated structured CTI formats limit ambiguity and support automation. CTI formats further contain favorable characteristics such as serialization rules.

Theory and Applications

The theoretical concept of CTI sharing includes CTI producers, consumers, and platform operators. On the one hand, CTI consumers subscribe to CTI feeds to receive the latest threat intelligence in a timely manner. On the other hand, CTI producers publish new CTI based on threat analysis. The platform acts as an intermediary to ensure CTI exchange and storage. It must be noted, that CTI sharing participants can hold multiple roles simultaneously. Thus, the different sharing mechanisms for CTI include a hub-and-spoke model, a publish-subscribe model with separated roles and peer-to-peer communication seen, for example, by the TAXII – Trusted Automated eXchange of Indicator Information server and client implementation (Connolly et al. 2014). MISP – Open Source Threat Intelligence Platform, another well-known open-source platform, is focused on handling CTI privacy and user participation (Wagner et al. 2016). CTI can thus be tagged according to the Traffic Light Protocol (TLP) and shared within an organization only (TLP:RED) or with specified communities. The most permissive option is public sharing (TLP:WHITE). In addition to the economic incentives for CTI sharing which often lead to industry groups (Gal-Or and Ghose 2005), intrinsic motivation and legal requirements determine participation. Mandatory for some industries (e.g., critical infrastructures), CTI sharing has to deal with trust concerns as well as regulations around sensitive data. Finally, sharing of CTI is closely linked with collaboration. For collaboration on CTI, the concept of visualization improves information accessibility (Böhm et al. 2018). As a result, various different CTI sharing platforms integrate visualizations in their implementations. By combining motivational aspects, defined processes and supportive technology, CTI sharing is effectively applied.

Open Problems and Future Directions

Cyber Threat Intelligence sharing still faces a number of challenges. Up to now, CTI sharing platforms have been based on common database technology and network protocols to allow accessibility over the Internet. Nevertheless, modern technologies might prove suitable for a range of use cases. Most notably, considerations of using Distributed Ledger Technologies (DLT) such as permissioned blockchains demand further research (Alexopoulos et al. 2020). Another open problem centers on the conflict of goals of privacy and CTI sharing for cyber defense. The most prominent issue here is how to weigh the privacy of sensitive (attacker) information (e.g., IP addresses) protected, for example, by the European Union's General Data Protection Regulation (GDPR) and the legitimate interest of secure information systems. Last but not least, despite the benefits of CTI sharing, participants can be reluctant to publish CTI and take only the role of CTI consumers. To this end, research must address types of incentives that outweigh the fear of information disclosure and attackers' adaption upon publicly available CTI.

Cross-References

▸ Cyber Threat Intelligence

References

Alexopoulos N, Vasilomanolakis E, Le Roux S, Rowe S, Mühlhäuser M (2020) TRIDEnT: towards a decentralized threat Indicator marketplace. In: Hung C-C, Cerny T, Shin D, Bechini A (eds) Proceedings of the 35th annual ACM/SIGAPP symposium on applied computing (SAC '20). SAC '20: the 35th ACM/SIGAPP symposium on applied computing. ACM, pp 332–341

Böhm F, Menges F, Pernul G (2018) Graph-based visual analytics for cyber threat intelligence. Cybersecurity (Cybersecurity) 1(1):1–16. https://doi.org/10.1186/s42400-018-0017-4

Connolly J, Davidson M, Schmidt C (2014) The Trusted Automated eXchange of Indicator Information (TAXII). MITRE. Available online at https://taxiiproject.github.io/getting-started/whitepaper/

Gal-Or E, Ghose A (2005) The economic incentives for sharing security information. Inf Syst Res 16(2):186–208. https://doi.org/10.1287/isre.1050.0053

Johnson CS, Badger ML, Waltermire DA, Snyder J, Skorupka C (2016) Guide to cyber threat information sharing. NIST Special Publication 800–150. National Institute of Standards and Technology

Pawlinski P, Jaroszewski P, Kijewski P, Siewierski L, Jacewicz P, Zielony P, Zuber R (2014) Actionable information for security incident response. European Union Agency for Network and Information Security (ENISA). Available online at https://doi.org/10.2824/38111

Sauerwein C, Sillaber C, Mussmann A, Breu R (2017) Threat intelligence sharing platforms: an exploratory study of software vendors and research perspectives. In: Leimeister JM, Brenner W (eds) Proceedings of the 13th international conference on Wirtschaftsinformatik (WI 2017). WI, pp 837–851

Skopik F, Settanni G, Fiedler R (2016) A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput Secur 60:154–176. https://doi.org/10.1016/j.cose.2016.04.003

Wagner C, Dulaunoy A, Wagener G, Iklody A (2016) MISP - the design and implementation of a collaborative threat intelligence sharing platform. In: Katzenbeisser S, Weippl E, Blass E-O, Kerschbaum F (eds) Proceedings of the 2016 ACM on workshop on information sharing and collaborative security - WISCS'16. ACM, pp 49–56