Threat Intelligence Information

Threat intelligence information is available in public and private threat intelligence feeds (e.g., AlienVault [2], Abuse.ch [1], EclecticIQ [3]), as well as from threat intelligence reports by industry (e.g., FireEye [4], Red Canary [5]). The attack artifacts are described in structured and semi-structured formats including, OpenIOC,[1] Structured Threat Information eXpression (STIX),[2] Cyber Observable eXpression (CybOX),[3] YARA,[4] etc. Given the rapid increase in the attack volume and sophistication, the attack artifacts are often descried in unstructured text (as in the CTI reports by industry).

References

[1] ABUSE, "Fighting malware and botnets," https://abuse.ch/.

[2] AlienVault, "AlienVault Open Threat Exchange," https://otx.alienvault.com/browse/global.

[3] EclecticIQ, "Intelligence at the core," https://www.eclecticiq.com/.

[4] FireEye, "Threat Intelligence Reports by Industry," https://www.fireeye.com/current-threats/reports-by-industry.html.

[5] Red Canary, "Red Canary 2021 Threat Detection Report," https://redcanary.com/threat-detection-report/.

[1] https://github.com/mandiant/OpenIOC_1.1
[2] https://stixproject.github.io/
[3] https://cyboxproject.github.io/
[4] http://virustotal.github.io/yara/