**DarkWeb - Strategic Cyber Threat Intelligence**

Strategic cyber threat intelligence is information about the specific adversaries targeting your enterprise and the dangers they pose in the immediate future.

**Monitoring the underground**

The cybercriminals, cyber espionage agents, and hacktivists we have been discussing have developed an entire under- ground universe where participants:

* Exchange ideas about targets, tactics, tools, and other facets of cybercrime, cyber espionage, and hacktivism
* Share expertise on creating and using malware, exploits, spear phishing campaigns, DDoS attacks, and other malicious tools and techniques
* Plan and coordinate ideologically and politically inspired attacks and campaigns
* Buy and sell exploit kits, weaponized exploits, obfuscation and evasion tools, and other cyber-attack tools
* Provide services to other threat actors, ranging from specialized tasks (fake website design, pass- word cracking) to outsourcing of infrastructure and complex activities (hackers for hire, rent-a-botnet, DDoS-as-a-service)
* Buy and sell digital assets, including credit card and Social Security numbers, personal information, and login credentials

**Motivation and intentions**

Researchers can collect a wide variety of information in this online underground, starting with motivation and intentions. Motivation and intentions provide evidence of which adversaries are likely to attack your industry and your enterprise, and which of your assets they are most likely to target.

The motive of cybercriminals is usually obvious: to make a profit, but their intentions can vary. Some target a certain kind of financial or personal data; others focus on a specific industry.

Competitors and cyber espionage agents exhibit a wider variety of motivations and intentions. These include stealing product designs, intellectual property, and business plans, uncovering the details of bids and proposals, and obtaining political and defense-related intelligence.

Hacktivists display the widest range of motivations, from impressing friends, to advancing a cause such as environmentalism, to discrediting individuals or companies with opposing views, to harassing opponents of a government. They may even aim to shut down part of an economy or national infrastructure in the event of a political conflict. Intentions can be equally varied, including stealing information that can prove embarrassing, defacing or disabling websites, taking over social media accounts, and shutting down crucial services.

Monitoring underground forums can also produce information on threat actors’ immediate plans. Some hacktivists announce their upcoming actions online, either to promote their ideology or to coordinate the activities of like-minded individuals and groups.

Although cybercriminals and cyber espionage agents are more secretive than hacktivists, sometimes it is possible to anticipate their actions by looking at information they share. Also, analyzing the malware and services they trade in underground marketplaces can disclose their intentions, targets, and techniques provided you are able to penetrate their forums.

We are proposing to extend this dataset to use the machine learning process for quantile correlation between monitored/scraped DarkWeb Vendors and their exploits/malware posted for purchasing. With the maturation of this dataset there can and inference rating/confidence rating between these vendors and attacks occurring in “the wild”. As this Dataset progresses the machine learning will predict that probability of commonly used Attack Vectors based upon their appearance in these DarkNet Vendor boards.

It also worth noting that attackers are often found hiding in plain sight today. A frequent disclaimer - “Just for educational purposes code” is commonly used by attackers as variants to malware or exploits in their own attacks.