FLASHPOINT

Use Cases for Physical Security

Online illicit communities are not only a place where cyber attacks are planned and the tools to commit them are traded, it's also home to emerging threats to an enterprise's physical assets, including its employees, facilities, and data. The physical element of information security often takes a backseat to the technology protecting the information. Theft, vandalism, or alteration of hardware can be equally as destructive and costly as a malware infection, and possibly even easier and more productive than a digital attack.

Flashpoint broadens the scope of cyber intelligence beyond threat detection to areas like physical security, providing the relevant context to business units not traditionally afforded the benefits of intelligence derived from illicit communities. By collecting and analyzing data from these communities and various surface web sources, Flashpoint provides customers with the trusted intelligence they need to facilitate risk assessments, the development and implementation of mitigation measures, and the ability to assess the effectiveness of those measures.

Below are examples of the types of challenges Flashpoint helps companies address:

ACTIVISM

Over the past several years, various groups initiated campaigns against the aviation industry that ranged from anti-pollution and runway expansion protests to demonstrations against deportations. Demonstration tactics included the blocking of runways, demonstrators chaining themselves to aircraft, concourse "die ins" in which protesters lie on the floor as though deceased, and general gatherings to disrupt business operations. In the past, these demonstrations in which participants impeded flight operations, by causing runway or terminal shutdowns, resulted in global flight delays and ultimately a financial impact to individual airline carriers.

By monitoring the situation and assessing tactics, techniques, and procedures (TTP's), Flashpoint was able to assess the impact of upcoming protests, and determine that these groups would likely continue to protest and attempt to impede airport construction and expansion projects through direct action. Other assessments included which protests were likely to include vandalism, economic impacts like disruption of business, and if their campaigns were gaining or losing momentum. Based on this information, Flashpoint customers were able to take actions to help control the impact to business operations, and to ensure the safety of their employees and facilities as well as the safety of those protesting.

EXECUTIVE PROTECTION

Leading up to the G20 Summit in Hamburg, Germany, which was attended by more than twenty heads of state or government and high level representatives of other organizations, Flashpoint was monitoring multiple groups that were preparing direct, violent action against the summit. These groups had called for vandalism from extreme far-left and anarchist groups and already one protest had led to several police vehicles being burned. Additionally, due to historic cyber campaigns around the G20, Flashpoint had assessed with moderate confidence that some form of nefarious cyber activity was likely to be observed.

Flashpoint monitored the timelines of these groups, identifying the peak dates where demonstrations would likely take place and which of those dates were most likely to involve vandalism and violence towards police by extremist groups. Customers were also provided profiles of the groups involved with an eye towards whether these groups were typically violent. Our analysts offered customers strategic advice in the instance of a violent protest, including how to set up emergency notification systems and physical evacuation plans. They also evaluated physical threats that would lead to cyber compromise, such as malware deployed through flash drives, and offered strategic advice on how to protect laptops and other mobile devices.

PHYSICAL FRAUD

In April 2017, a threat actor published a post titled “Diaries of a Fraudster,” detailing various fraud techniques. According to the actor, he and a team of others would purchase credit reports and then purchase matching scanned driver's licenses and Social Security Numbers. After the purchases, he claimed that: “[the] rest was simple, just memorize the information on the [credit] Report and DOB, Address etc. Then we went to [a retail store] or any stores that let you buy merchandise as a loan. “ He also claimed that their team would place small microphones in: “big construction stores . . . that any entrepreneur could go simply by telling the cashier his name and account number. “ After stealing the information, he and his team would "dress in construction clothes, make fake [IDs]," and buy less than $5,000 CAD worth of items at a time.“

Flashpoint alerted customers to these new techniques, as the advice and experience offered by actors such as this one are of immense value to other cybercriminals-–both novice and experienced-–who are seeking to enhance their operational tradecraft. This helped customers to make strategic decisions about their operational security procedures. A profile was also created on this actor to monitor his other activities on illicit communities so if he continues his diary series, Flashpoint can keep customers abreast of new TTPs as soon as other threat actors learn them.

PHYSICAL THEFT & LOSS

In June 2017, a company was fined more than £100,000 following the theft of a hard drive containing the banking details of almost 60,000 customers. The device also held limited credit card details of 20,000 customers, although CVC numbers and expiration dates are not affected. The Information Commissioner’s Office (IOC) said the device was stolen either by a member of staff of a contractor, adding that the information on it was not encrypted and the device has never been recovered.

Theft of hardware, such as company-issued laptops, cellular devices, and removable media, poses a potentially high-impact financial threat to the financial sector. The loss of employee or customer data, if decrypted or readable, will likely lead to large-scale fraud and the possibility of lawsuits and/or fines by government regulators. With Flashpoint’s help, the company could have strategically planned to protect their sensitive hardware both on a physical security level and recommendations on protecting the data on that hardware. Following a breach like this, if the company’s information were to appear on illicit communities, Flashpoint could also alert them and provide context which could assist in discovering the threat actors involved.

ABOUT FLASHPOINT

Flashpoint is the globally trusted leader in risk intelligence for organizations that demand the fastest, most comprehensive coverage of threatening activity on the internet. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across the private and public sectors to help them rapidly identify threats and mitigate their most critical security risks.

For more information, visit **https://www.flashpoint-intel.com/** or follow us on Twitter at **@FlashpointIntel**