Read Featured Research & Threat Intel Article by Adam Meyers

crowdstrike.com/blog/ecrime-ecosystem/

August 1, 2016

CrowdStrike's New Methodology for Tracking eCrime

August 1, 2016

Adam Meyers Research & Threat Intel

At our inception, CrowdStrike coined the phrase, *"You don't have a malware problem, you have an adversary problem*." Behind every attack — whether it is the most advanced nation state conducting espionage, opportunistic criminal activity, or highly visible hacktivism — are human actors. Those humans have preferences, patterns, and flaws. Intelligence analysts who study these actors can piece little parts of the story together to first categorize — and then ultimately understand — the human actors behind these attacks. Models can help analysts organize their thoughts and observations into a transferable or communicable structure so that others may understand what they believe and why. In the cyber domain, military models such as the "kill chain," are often adopted to suit the analyst's needs. At CrowdStrike, we thought long and hard about how various models might help us convey to our customers the behaviors and organization of eCrime actors. What we found was that these actors and their interdependent relationships did not fit into an existing model.

The eCrime actor's operational profile differs greatly from that of an espionage-focused targeted intrusion actor. Historically the kill chain, derived from military targeting models, has been applied to disrupt the activity of an adversary. Approaches such as F3EAD (Find, Fix, Finish, Exploit, Analyze, Disseminate) have been applied to disrupt the adversary's kill chain in the cyber realm. The thought behind implementing this model is that an espionage actor generally operates in a closed cell: that is, they conduct their own reconnaissance, source or build their exploit, deliver/attack the target using data from the reconnaissance phase, create a beachhead to maintain persistence, and execute their actions on objectives. Disrupting the attacker at any link of this "chain" has consequences on the rest of the activities they may attempt to accomplish. Ideally, finding the link in the chain that is hardest or most expensive to change will create a negative impact for the attacker, and they will need to retool or regroup before the next attack.

In the criminal domain, this is not necessarily true, as eCrime is a vast ecosystem of interconnected services and schemes. There are complex relationships between varied individuals and groups, whose primary goal is to generate revenue. A banking trojan may be designed and built by one group that intends to build a reliable and feature-rich piece of software, and they may choose to monetize this via an affiliate model (partnerkas). With this approach, they don't necessarily know or care how their customers use the tool, how they distribute it, or what they do with the data they collect – only that they use the tool in accordance with their guidelines and pay them. The developers of such a tool may be categorized differently than their customers, but the fact remains they must rely on various criminal underground elements to be successful. They generally will market their tool to potential customers, they likely will need some resilient infrastructure to host their service, and they will potentially need to use monetization schemes to enjoy their revenue. The combination of what activities these actors engage in can be organized into a series of breadcrumbs to identify that actor. An eCrime actor's profile is a cross section of the services they offer, the services they utilize, crimes they engage in, means to monetize their activities, customers that they support, how they market themselves and to whom, the victims that they target, and ultimately their identity which they closely protect. Through the judicious investigation and analysis of these actors, CrowdStrike analysts piece together these breadcrumbs into the profile of an eCrime actor. The relationships between these actors becomes a sort of social network, a graph database of sorts where different groups and individuals are nodes with overlapping edges where they conduct commerce with each other.

As an example of this structure, CrowdStrike fully evaluated the CoreBot banking trojan malware and the people who maintain it, who we track as BOSON SPIDER. The adversary behind this threat, which was first identified in 2015, recently and inexplicably went dark in the spring of 2016, appears to be a tightly knit group operating out of Eastern Europe. They have used a variety of distribution mechanisms such as the infamous (and now defunct) angler exploit kit, and obfuscated JavaScript to reduce the detection by antivirus solutions. In addition to outsourcing their exploitation/delivery, they used bulletproof hosting services

such as Avalanche or Kol. Their key value proposition in the underground economy is providing a well-designed, man-in-the-middle browser hijacking trojan which can be used to hijack sessions or steal banking credentials. This service is delivered through an affiliate model that allows the actor to resell their malware with custom configurations to suit the needs of the affiliate customer. In one configuration, we observed the targeting of U.S. and Canadian banks, while in another smaller configuration, the customer targeted Japanese banks exclusively. As far as crimes committed, the primary purpose of the tool was to steal credentials to facilitate bank fraud against unsuspecting victims when they attempted to authenticate to a targeted financial institution. This was monetized by the actors as a botnet-as-a-service, and perhaps they too used the botnet to steal credentials for their own usage, in which they may have employed money mules from the eCrime ecosystem to extract the funds. They used some clever technical tradecraft including Domain Generating Algorithms (DGA) and disguising malicious JavaScript as legitimate Microsoft Office documents. Finally, in order to attract potential users or customers, they advertised in at least one criminal forum.

The story of BOSON SPIDER is certainly an interesting one, but for victims such as financial institutions who wish to understand the capabilities of this actor, and to monitor for changes in their behavior, a kill chain or diamond representation of their activities doesn't show the whole picture. This is the reason CrowdStrike has expanded our eCrime offerings to deliver to our eCrime Intelligence subscribers a more comprehensive understanding of the threat actors that they must deal with and ultimately how they can more effectively disrupt the activities of these actors to protect their businesses.

Conceptually the CrowdStrike *eCrime ecosystem model* takes into account the elements of the adversary that are important to understand who they are, as well as the inter-relationships with the eCrime ecosystem. CrowdStrike utilizes this model to deliver best-in-class eCrime intelligence reporting to our customers, and to fuel the CrowdStrike Falcon Platform with eCrime intelligence to protect the endpoints of customers all over the world. We have recently launched our eCrime premium intelligence subscription for customers who are plagued by financial, reputational, and data losses at the hands of the myriad of eCrime actors operating with impunity today.

For more information on the CrowdStrike Falcon Intelligence eCrime offering contact us at intelligence@crowdstrike.com. If you think you are up to the challenge of analyzing and investigating the motivations of malicious adversaries, check our job listings to join the mission!

Related Content

Who is EMBER BEAR?

A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell