DARKReading

9/5/2019
01:20 PM

Kelly Sheridan
News
Connect Directly

Crimeware: How Criminals Built a Business to Target Businesses

A new report investigates the evolution of crimeware, how businesses underestimate the threat, and why they should be concerned.

As businesses large and small have shifted their security concerns from financial cyberattacks to sophisticated threats, criminals have been constructing a well-run crimeware organization. An enterprise of its own, this lets them develop, leverage, and distribute new infection methods.

Chronicle, the enterprise cybersecurity division under Alphabet and recent addition to Google Cloud, today published a report investigating the evolution of crimeware from 2013 to 2018. Researchers explain how crimeware, traditionally considered a "commodity threat," has grown into a highly lucrative institution fueling sophistication of malware and attack strategies.

"These guys run straight businesses," says Brandon Levene, head of applied intelligence at Chronicle and report author, explaining the services offered and analytics used. "Everything is well documented. The data is extraordinarily rich. … I think that has been a really big tell" for how organized these criminal organizations are.

Instances of crimeware have steadily grown each year, Levene says, and the prevalence and frequency of attacks have desensitized security teams. "Crimeware fatigue," as he describes it, distracts targets from malicious activity that has become inexpensive and low effort for financially motivated criminals. Once attackers are on a corporate network, they know how to conduct reconnaissance, see what's valuable to them, and where they sit in an organization.

"They are able to select their victims for maximum value," he continues. Years of deploying massive, broad attacks have taught cybercriminals how to optimize for volume and speed; now, they leverage traditional workplace standards to generate profit. A shift to consolidation and "crimeware-as-a-

service" showcases their ability to grow this business while finding new tactics.

All the while, as attackers have refined their techniques and profited off enterprise victims, law enforcement has lagged behind. Criminals model risk based on law enforcement's efforts and adjust their tactics based on the funds they generate, Levene says. Unburdened by geography and other factors that limit law enforcement's ability to find and arrest attackers, crimeware operators have had an advantage in building their capabilities to further outpace the good guys.

So, how did we get here? How have criminals adjusted their operations, and why are they leveraging their more advanced capabilities to target businesses instead of consumers?

A Snapshot of Crimeware's Evolution

In 2012 and 2013, which marked the start of Levene's research, there was a "pretty broad range" of people conducting malware operations. Over time, these parties began to consolidate, likely in response to the risks of running malware operations. Infrastructure hosting was consolidated, and malware began to consolidate as well, he explains. While we still see multiple malware families, it's typically the same four to five names instead of the 20 to 30 seen in the past.

While crimeware is generally increasing, different attacks have seen different trends. Banker malware, for example, was "relatively flat" from 2013 to 2017, then spiked 1,130% in the second quarter of 2017. Ransomware's growth track was more reliable, increasing in 13 of the 20 total quarters analyzed. Information stealers' growth was stable from 2013 to 2018. Miners were pretty uncommon until they appeared in the transition from 2017 to 2018, Levene reports.

Emotet, which is recently less active but historically has a strong relationship with the criminal community, is one example of a threat that has adjusted its technique. Its operators have moved from a banking Trojan model to running "enormous" malware spam campaigns in which they can gain, and subsequently sell, access to businesses. TrickBot has also stepped up its pace, Levene says. Emotet was used as a dropper for TrickBot, which can launch ransomware attacks.

One of the biggest shifts in technique was the transition to the "as-a-service" model. In this environment, trusted affiliates could manage malware distribution, command and control, data collection, and payouts. More criminals owned "as-a-service" platforms or bought into them, eliminating the need for people to run their own malware operations. Attackers don't need to share source code with customers, who can launch campaigns with less-advanced skills.

"Executing a well-run operation from beginning to end is much easier," Levene says, once a criminal is able to enter one of these operations or pay for a relationship to the operators. "A lot of these businesses are run on trust," he notes, and many have been around for years.

Why Businesses Should Be Worried

Today's organizations underestimate the threat of crimeware; instead, they're worried about advanced persistent threats (APTs) and advanced attacks. "One of the misconceptions is that financially motivated threat actors are not as sophisticated as these targeted intruders, nation-state intruders," he says.

APTs are low-prevalence, high-impact threats, Levene adds. Crimeware is high prevalence, high impact. Businesses that can't stop high-prevalence intrusions have no chance of stopping an APT. "The competence of financially motivated threat actors has gotten to a point where they can disrupt an organization or an enterprise just as badly as an APT."

There are two ways attackers normally try to break into a business environment. The first is sending emails laced with malicious links or attachments, which Levene calls "the bread and butter" of cybercriminals. "That accounts for the huge majority of targeting," he points out. Unlike in 2013 or 2015, when criminals used exploit kits, they now rely on social engineering.

The second is Internet-facing remote access protocols including TeamView, VNC Viewer, and Windows Desktop. All offer public-facing remote access into an enterprise server but are often protected with weak passwords. Criminals will gain access into these environments and launch tailored ransomware attacks. Levene notes this tactic, which has become prevalent in the past two years, requires more labor, knowledge, interaction, and availability to distribute malware.

He anticipates in the future, ransomware and destructive malware should be a growing concern, especially as attackers tailor access to chosen environments. Loaders will get smaller, droppers will improve, and better recon tools will be more lightweight. Recon will become a lot more routine, and organizations will be forced to quickly react when they realize data is at risk.

"I think it's going to be a shock to them, when they realize how valuable their data is," Levene says of small and large businesses alike. "This places the onus for defense on network defenders themselves, which may not be equipped to handle it."

Related Content:

- 7 Steps to Web App Security
- 3 Promising Technologies Making an Impact on Cybersecurity
- Over 47K Supermicro Corporate Servers Vulnerable to Attack
- Phishing Campaign Uses SharePoint to Slip Past Defenses

Check out The Edge, Dark Reading's new section for features, threat data, and in-depth perspectives. Today's top story: "Meet FPGA: The Tiny, Powerful, Hackable Bit of Silicon at the Heart of IoT."

Kelly Sheridan is the Staff Editor at Dark Reading, where she focuses on cybersecurity news and analysis. She is a business technology journalist who previously reported for InformationWeek, where she covered Microsoft, and Insurance & Technology, where she covered financial ... View Full Bio