WEI INSIGHTS TECH BRIEF

PROTECT YOUR NETWORK FROM ADVANCED PERSISTENT THREATS

How do you know when you've arrived in the remote Romanian town known as Hackerville? When you see the luxury car dealerships, according to a 2011 Wired magazine article.

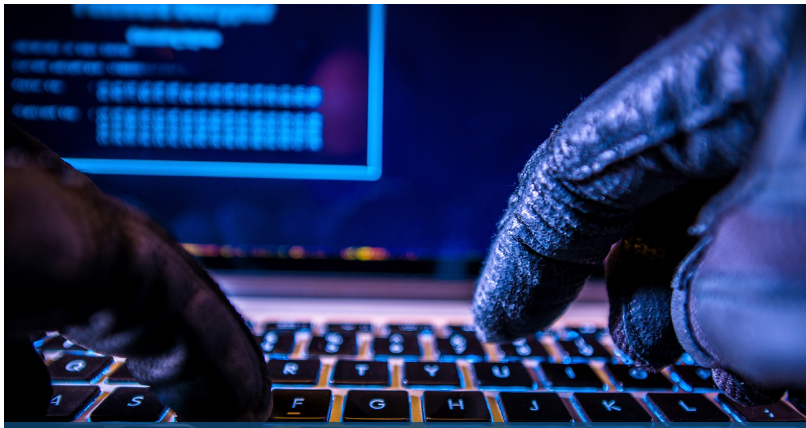
Each year, Romanian cybercriminals allegedly steal an estimated $1 billion from US consumers. Attackers based around the world, including in the US, capture more than $1 trillion annually. Cybercriminals are not typically isolated individuals working alone. Instead, they have learned to work together collaboratively, sometimes internationally, in order to distribute risk in a trend some are calling the new face of organized crime.

In the past, it was rare for a cybercriminal gang to launch the quiet, long-term attacks against enterprises and organizations known as Advanced Persistent Threats (APTs), but times are changing. The overwhelming majority of APTs are thought to be the work of nation-sponsored economic espionage teams, highly organized and focused on the long game.

How many people work on these APT teams? Does an APT team function like any software team, fussing over deadlines and monitoring budgets? Do they share pictures of their growing children as they exfiltrate data from a far away enterprise, sometimes year after year?

While the inner workings of cyberespionage teams remain largely unknown, security researchers are learning much about the attacks they launch. Consider a few recent developments:

- In a 2015 breach of the US Office of Personnel Management that affected 20+ million people, hackers were allegedly able to identify defense contractors, target the systems those people used, and steal military intelligence. Terabytes of information were stolen.
- Researchers who analyzed the 2015 Anthem health insurance breach that impacted 80 million customers confirmed that Anthem was specifically targeted and that attackers may have had a foothold in the network for seven months before they began stealing information.



Cybercriminals allegedly steal an estimated $1 billion from US consumers each year.

Typical of an APT attack, the malware acquired a foothold in the network, perhaps through a phishing scam, and phoned home to a command-and-control server which provided further instruction and additional malware to explore the Anthem network. After eight weeks of secreting information out of the network, an Anthem system administrator accidentally discovered that the hackers were using his own credentials. In part, the attackers used a fake domain and set up a structure of subdomains that mimicked the legitimate Anthem network, including a subdomain that appeared to be a

Virtual Private Network but was used by malware to steal information. The fake domain also was implicated in a separate attack against a defense contractor.

- Security firm TrapX released a 2015 report that described how attackers use unsecured diagnostic medical devices such as imaging systems and archives to launch APTs. Many such devices are running on unpatched Windows 2000 systems and use unchanged default Administrator passwords, the report said. "Based upon our experience and understanding of MEDJACK, our scientists believe that a large majority of hospitals are currently infected with malware that has remained undetected for months and in many cases years," the report said.
- In 2014, Sony's attackers stole a vast amount of data including compensation information for actors, several unreleased movies, and personal information for 6,000 employees. They then destroyed 3,000 computers and 800 servers. The FBI told a US Senate committee that the attack would have penetrated 90 percent of all companies. Researchers matched the malware to an attack two years earlier that destroyed 40,000 computers in South Korea at banks and broadcast media firms.

An APT attacker typically starts by gathering information about people who work for the targeted organization and then launch a phishing attack to get someone from within the targeted network to open a malicious attachment or website.

Once an APT has a foothold in a network, the attackers explore the network and typically begin to exfiltrate or export information outside of the organization in tiny increments over prolonged periods of time, low and slow, to avoid detection. In some cases, such as attacks against manufacturing or power facilities, an APT focuses on disrupting operations or causing physical damage.

Historically, cybercriminals and cyberespionage teams worked independent of each other. Cybercriminals tended to focus on fast moving attacks against individuals and smaller companies; cyberespionage teams slowly attacked large organizations. These groups had no easy way to sell information to each other. However, this is beginning to change with the emergence of the dark web marketplace, an area of the Internet accessed through secure, encrypted channels, where transactions are paid in a digital currency such as Bitcoin. In some APT attacks, evidence suggests that a cyberespionage team purchased and customized cybercrime malware such as ZeuS for the first attack stage. In addition, a cybercriminal who stumbles across trade secrets or other proprietary data can now more easily sell it to a cyberespionage team on the dark web. While cybercriminals are selling to cyberespionage teams, the reverse does not appear to be true at this time.

In response to the APT crisis, the security industry has produced a number of sophisticated threat protection and detection platforms that either thwart cyber attacks or allow rapid response. Companies such as FireEye, BeyondTrust, and Securlert attempt to proactively identify security vulnerabilities that were never seen before or are difficult to detect. Some platforms rely on crowdsourcing; customers submit information about threats and the platform "learns" to identify them. Other platforms overlay data from multiple sources to identify smaller weaknesses that when chained together become more serious.

A challenge with all of enterprise security platforms is the number of alerts that are generated to the team responsible for monitoring security. In the interest of defense in depth, a platform may generate too many false positives, which are normal conditions that are mistakenly identified as malicious. With too many alerts to investigate, administrators are tempted to either ignore the alerts or turn off the feature that generates them. On the other hand, a platform that attempts to eliminate false positives may fail to generate alerts for real threats.

Considering these limitations, many enterprises may be relying too heavily on technological solutions. In its 2015

Advanced Persistent Threat Awareness Annual Report, ISACA, an international professional association focused on IT Governance, revealed that enterprises tend to focus on technological solutions rather than education and training, even though it is known that most APTs gain initial entry when the trust of an employee or other insider is exploited. With a phishing scam, hackers pose as a trusted source and trick workers into opening a malicious attachment or website.

Security-minded enterprises must train all insiders in topics like safe internet surfing, safe use of social media, and telltale signs on phishing websites. In addition, these enterprises must have an ongoing awareness campaign to reinforce key concepts.

As Kevin Mandia, Chief Executive Officer of security vendor FireEye, said in a TechCrunch interview, "The advantage goes to the offense in cyber. Nation state (government) threat actors or hackers target human weaknesses, not system weaknesses."

TALK TO WEI TODAY

Our security experts want to answer your toughest questions. We can assess your current IT environment to identify security vulnerabilities and help develop a comprehensive network security plan to improve your company's security posture.

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 25 years.