The vicissitude of Cyber Crime Threat Landscape: The past, present and the future

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both -- i.e., target computers to infect them with viruses, which are then spread to other machines and, sometimes, entire networks.

A primary impact from cybercrime is financial, and cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may target private personal information, as well as corporate data for theft and resale.

2017 was an interesting year on the cyber crime threat landscape. The WannaCry and Petya/ NotPetya attacks made headlines, but they were exceptions and masked the first indications of a shift, in the ransomware landscape in particular. While ransomware remains a major threat, it seems some ransomware criminals have been busy adding more strings to their bow: in some cases distributing financial Trojans and in other cases turning to cryptocurrency coin mining.

Some online banking threats felt the impact of major takedowns that took place in late 2016, but others managed to make a breakthrough. In particular, the Emotet (Trojan. Emotet) banking Trojan reemerged after a long hiatus. Emotet's activity ramped up in the last few months of 2017, with detections increasing by 2,000 percent in this period. At the same time, the growth of coinminers, and their use by cyber criminals, grabbed headlines.

The growth in coin mining in the final months of 2017 was immense. Overall coin-mining activity increased by 34,000 percent over the course of the year, while file-based detections of coinminers on endpoint machines increased by 8,500 percent. There were more than 8 million coin-mining events blocked by Symantec in December 2017 alone. These numbers are quite mind-boggling, but this explosion in activity may be short lived. Coin-mining activity is strongly linked to the increase in value of many cryptocurrencies; a sustained drop in their value may lead to this activity going down just as quickly as it went up.

The ransomware landscape in 2017 was dominated by the stories of the WannaCry (Ransom.Wannacry) and Petya/ NotPetya (Ransom.Petya) attacks, but they were not "typical" ransomware attacks, and don't represent the overall trend for ransomware in 2017. In fact, Petya/NotPetya was not a real ransomware, it was a destructive wiper that masqueraded as ransomware. For these reasons, we have omitted detections of these threats from our ransomware detection counts in this chapter. The impact and significance of these attacks is covered elsewhere in this report, in the article on Ransomware: More Than Just Cyber Crime.

Ransomware infections had steadily increased year-over-year since 2013, and reached a record high of 1,271 detections per day in 2016. Ransomware detections failed to break that record in 2017, but remained at those elevated levels. With WannaCry and Petya/NotPetya excluded from detection numbers, there were approximately 1,242 average ransomware detections every day in 2017, roughly the same as 2016's record-breaking number.

A stabilizing of ransomware detections on the endpoint may not necessarily be an indication of drops in activity, but could also be indicative of the impact of improved upstream protection.

Effective email filtering, Intrusion Prevention System (IPS) detection, and machine learning technology mean that ransomware activity is being blocked earlier in the infection chain. For example, in 2017 we saw a 92 percent increase in blocks of script and macro downloaders, a major source of ransomware infections. Improved detections earlier in the attack chain by Symantec mean these downloaders are being detected and blocked before they drop their final payload.

Viewing ransomware as a business, it's clear that the profitability of ransomware in 2016 led to a crowded market and clear overpricing of ransom demands from greedy criminals. In 2017, the market made a correction, with fewer new ransomware families and lower ransom demands. Ransomware authors honed their business model in 2017, seeming to find the sweet spot victims are willing to pay. The average ransom demand for 2017 was $522, which is less than half of 2016's figure of $1,070, and is also a decrease from the mid-year average, which was $544.

In 2017, 28 new ransomware families appeared, which is on par with 2014 and 2015, but a drop on 2016, when an unprecedented 98 new families were discovered.

There were also declines in activity from some of the big ransomware families in 2017. Cerber (Ransom.Cerber), Locky (Ransom.Locky), and TorrentLocker (Ransom.TorrentLocker) all but disappeared from the scene over the course of the year.

Despite this, the Necurs (Backdoor.Necurs) botnet, one of the main distributors of Locky, had a big impact on the cyber crime threat landscape in 2017. Necurs disappeared for much of the first three months of 2017—reappearing just as suddenly on March 20 when it started sending out stock spam. Its absence was immediately felt, with a major drop in email malware and spam rates for those three months. The rates steadily increased for the rest of the year, though they never quite reached 2016 levels.

On July 20, 2016, cyber attackers attempted to steal $150 million from the accounts of a bank in South Asia. Minutes later, the same thing happened to a bank in West Africa—attackers used the bank's own systems to send payment instructions to transfer $150 million to the attackers' chosen accounts. Counterparty banks spotted both sets of fraudulent messages and raised the alarm, ensuring that no funds were lost. However, the episode signaled a change in the threat facing financial systems today: not only could attackers conduct complex intrusions and manipulate payment systems within a single target bank, but they also could strike institutions on different continents simultaneously, while operating safely from the other side of the world. The threat of coordinated attacks against multiple parts of the financial system was no longer purely theoretical; malicious actors had demonstrated that they could do so, and the potential for systemic impacts was clear.

In the years since the July 2016 financial hacks, attackers have not made a habit of disrupting or manipulating the foundations of the financial system, and there has been no direct evidence of escalation. However, plenty of examples of continued attacks and other issues have increased the general cause for concern. Three long-term trends in particular emerge from this analysis and overall evolution of the threat landscape:

1. Attackers are increasingly building advanced capabilities to target core banking systems, particularly around payment messaging and transaction authorization. Once these tools are built, attackers will use them for as long as they remain effective. As security is tightened around certain technologies, such as SWIFT (an international financial communications network), they will look for and develop other routes to cash out.

2. Attackers are becoming more aggressive in disrupting their victims' ability to respond. In 2011 and 2012, attackers staged distributed denial-of-service (DDoS) attacks against U.S. banks to disrupt banking services. Though these attacks were basic and caused minimal long-term damage, the impact to the financial system was visible. Years later, the approach in the Bangladesh Bank case involved attempting to subtly hide the evidence, the equivalent of deleting security camera footage in the real world. In 2018, attackers used wiper malware across a bank's information technology systems to perform the cyber equivalent of setting the bank on fire as part of the getaway. Unfortunately, these tactics seem to work, and so attackers are likely to return to them. Where self-propagating destructive malware is used, the risk of spreading from one victim bank to others is very real.

3. Attackers continue to find ways to collaborate, bridging organized criminal gang activity across multiple geographies. Online criminal marketplaces offer tools and also services to facilitate cashing-out and money laundering. These are components of modern criminal enterprises, but the siloed nature of cyber operations and financial crime prevention make it challenging for banks to tackle these problems. The regulatory and law enforcement communities face similar challenges, compounded by the difficulty of pursuing cross-border crime.

This assessment reviews the current cyber threat to the financial system, using real-world examples from financially motivated attackers, and provides lessons to help improve sector-wide resilience and security.

In the past decade, the capability and motivation of threats to the financial sector have transformed from small-scale opportunistic crimes to efforts to compromise entire networks and payment systems. Most of the earlier attacks took advantage of low-hanging fruit, such as weak defenses and existing vulnerabilities, and did not require many resources. As hacking tools became more readily available and the services providing them became commercialized, teams of financial attackers formed and developed their own kits, and some offered their services for hire. Today, targeted intrusions have become the norm. Security vendors have raised awareness of the threat by publicizing information about high-end campaigns, but this publicity has also spread the knowledge

of how to build advanced tools and operate covertly. Proliferation-through-publication has given everyone, from the hobby hacker up to nation-state agencies, more information to develop and conduct their attacks.

Currently, the cyber threat from malicious actors looms large over the financial sector (see figure 1). Examples of recent successful attacks include the April 2018 attack against Mexico's domestic interbank payment network SPEI, in which $15 million was stolen from multiple financial institutions, and the May 2018 attack on Banco de Chile, which lost $10 million through international payment transfers. The Banco de Chile attackers also created a smokescreen for their activity by deploying wiper malware that destroyed several thousand systems on the bank's network and left banking operations unavailable for several days. In late 2018, there were further attacks—Cosmos Bank in India, Bank Islami in Pakistan, and Redbanc in Chile all suffered similar intrusions and impacts on their business operations. In February 2019, attackers compromised the payments systems of a Maltese bank and attempted to transfer €13 million from it.

The pattern of targeted institutions shows that this is mostly a problem for central and commercial banks in developing nations. Financial organizations in Latin America, Asia, and Africa have less mature cybersecurity than their counterparts in wealthier parts of the world, and attackers know this. Attacking a big Western bank with advanced security and intelligence teams is likely to end in exposure and unwanted attention from law enforcement. A stolen $1 million from a victim with poor security is worth just as much as $1 million from a top-tier investment bank, a beneficial risk-versus-reward situation that is evident to potential criminals.

However, Western financial institutions are vulnerable in their own ways, though many of the problems and incidents that they have experienced have been of their own making. In April 2018, Britain's TSB suffered a computer system meltdown as the bank attempted to migrate customer records to a new system. The issue took over a month to resolve and was estimated to have cost the bank $300 million. Two months later, Visa cardholders in Europe experienced service disruptions following a hardware failure that left them unable to carry out chip-and-PIN transactions for a few hours. Given the declining use of cash by many consumers, this system failure significantly disrupted transactions for many individuals and businesses. Legacy infrastructure is not just a problem for the financial industry; incidents with failing systems and botched upgrades have similarly disrupted transport sector firms as well as telecommunications companies. However, downtime that impacts

people's access to bank accounts and other funds has caught the eye of policymakers, and as a result the regulators are looking more closely at the sector's cyber resilience.

Attackers have improved in terms of capabilities. The prototypical modern criminal gang is a cyber crime gang. Although the resulting fall-off in bank robberies and other armed crime, with its corresponding decrease in physical violence, is to be welcomed, the potential for large-scale losses through cyber attacks continues to increase. These risks have grown as tools and information about bank systems have become more available to anyone who can pay for them. A manual on automated teller machine (ATM) security might be available for a small fraction of a bitcoin on hidden internet markets. Likewise, malware that can steal credit card information from the memory of point-of-sale systems, or provide remote access to systems behind enterprise firewalls and proxies, are available for a price online.

Cyber criminal gangs are more than isolated groups and individuals operating from the shadows. Some of these groups operate like businesses and actually are established as overt companies in order to secure the services of code developers that can build financial access tools, hosting services for launching attacks, and of course banking facilities to help with money laundering. They have a division of labor, with individuals specializing in particular areas, thus improving their productivity and overall proficiency.

The situation would be challenging enough for network defenders if criminals were the only figures of concern. Financial institutions also have to contend with adversarial nation-state groups. State actors have a disproportionate effect on the threat landscape, as they have the resources to invest in offensive cyber tools and techniques. Such capabilities raise the risk of misuse and the threat that these tools and techniques will leak into the public domain. Although nation-states may originally have developed their offensive capabilities for military conflict or espionage, these tools can be repurposed to attack financial systems—as was seen in the February 2016 Bangladesh Bank attack. Offensive cyber capabilities and knowledge are inherently leakier than traditional weapons, and cases such as the EternalBlue exploit, which enabled the May 2017 WannaCry worldwide ransomware attack, show how this can play out.