The cybercriminal underground hasn't forgotten about financial services

intel471.com/blog/financial-cybercrime-2021-jackpotting-atm-malware

It is a well-worn cliche in cybersecurity: criminals prey on banks and financial services because that's where the money is. In 2021, that remains a fact. However, while the overall crime remains the same, who is responsible for it and the method by which the crimes are carried out have been modified.

While the financial services sector has undoubtedly increased security procedures and adopted advanced technologies to deter attacks, underground actors continue to adapt and develop new methods of evading anti-fraud systems to gain access to sensitive information that financial businesses and organizations collect, store and transmit. With the world having to adjust to the global pandemic in 2020, financial services are now exposed to new risks and threats that attackers are taking advantage of. In the past six months, Intel 471 has observed actors on the cybercriminal underground establish their reputation using a variety of goods, products and services that have specifically targeted financial services.

One door closes, two doors open

There have been significant actions taken to undercut cybercrime this year, with each event weakening criminals' ability to target financial services. One was Joker's Stash, the prolific carding dump shop, which announced its closure in January 2021. That announcement came after law enforcement allegedly seized proxy servers used in connection with the site's blockchain-based domains. Another law enforcement action in 2021 successfully disrupted the Emotet botnet, which featured a modular loader that could steal credentials and bank details from infected users, as well as distribute other malware.

While each of these takedowns kneecaps criminal activity, there are actors on the underground who move to fill in the void left by the law enforcement actions. With each of the above examples, Intel 471 has seen other actors quickly move to establish a bigger presence in the market.

With regards to Joker's Stash, we have observed the creation of and updates to numerous payment card data shops. An updated shop Intel 471 has been tracking offered payment card information, particularly card verification values (CVVs) and dumps that included the data copied from payment card magnetic stripes. As of mid-December 2020, the shop allegedly contained 1,200 compromised payment card records and about 21,000 dumps for sale.

With regards to malware-as-a-service, Intel 471 has seen two actors sell access to malware that targets the Android operating system in an effort to pull bank credentials. One service, first advertised in October 2020, includes the ability to intercept, send and receive text

messages; grab payment card data and two-factor authentication (2FA) codes; and steal online banking payment details through web-injects. Another actor, a relative newcomer to the cybercriminal underground, started advertising an Android-focused MaaS that could intercept, send and receive text messages; record an infected device's screen; grab payment card data; and steal online banking credentials through web-injects. The service allegedly also supported a socket secure internet protocol (SOCKS5) proxy and keylogging modules.

Access is everything

Without obtaining credentials, a cybercriminal's attempt to steal money or sensitive information is exceedingly difficult. Credentials are a crucial cog for actors, serving as the tool that paves the path to ill-gotten gains. Financial institutions are already a heavily targeted sector, so this threat has the capability to impact those at both an individual and organizational level.

Intel 471 has observed a number of actors advertise possession of personal bank account login credentials, an organization's employee credentials, as well as system access credentials over the past few months. In the closing months of 2020, we observed one actor offering bank logins with credit card information from a Spanish financial institution, while also claiming to have bank logins available from a French bank and an online bank popular in Europe. Additionally, another actor being tracked by Intel 471 offered to sell compromised account credentials to the control panel of business process management software used by an undisclosed insurance company.

On the network access side, one actor Intel 471 is tracking tried to sell unauthorized access to an undisclosed bank in Africa, claiming to have administrator-level access to the organization's domain controller, access credentials to some databases, the source code of undisclosed applications the organization used, and the bank's customer data. As recently as January 2021, another actor monitored by Intel 471 offered to sell unauthorized access to the network of a France-based company that deals in hardware and software for PoS systems, including automatic coin mechanisms, cash registers, management systems and payment software. The compromised account allegedly included domain administrator privileges and enabled access to the company's product source codes, GitHub software development platform accounts, Amazon Web Services (AWS) accounts, employee email accounts and lists of customer email addresses.

While an organization can help individuals recover from compromised payment cards or bank logins, bouncing back from network compromise is much more difficult and therefore presents a much larger threat.

Criminals make money machine go BRRR

When not going after the users or company itself, cybercriminals have turned their attention to the next best thing: the machines that hold the money. The act of using malware to force ATMs to malfunction and empty their cash — known as "jackpotting" — has been around for some time, but actors are finding novel ways to get around baked-in defenses. Intel 471 observed one actor selling ATM malware that allegedly could be deployed using a specially-crafted Raspberry Pi kit computer and be controlled remotely via a smartphone or a laptop.

ATMs aren't the only hardware in criminals' sights. Point-of-sale (PoS) malware also is being sold on underground markets, taking advantage of flaws in the devices used to process card payments at retail locations to steal sensitive information. Intel 471 observed an actor in February 2021 selling PoS malware dubbed "ATM & POS Malware Injector" that allegedly operated as a data sniffer without requiring additional action from the user. The malware features included payment transaction data output in a result box that included Track 1 and Track 2 data, as well as the personal identification number (PIN) code for the compromised payment card. Data collected via this kind of malware has the capability to be used in further fraudulent activity or offered for sale as a product on underground forums or via dump shop services.

While the global economy took a hit over the last year as it recovers from the pandemic, the underground marketplace continues to flourish with new opportunities as the potential victim pool grows with the increase of people using online services. The buying, selling and trading of products, goods and services used for crimes has fueled several attack schemes, with many developed specifically to target the financial services sector. It's apparent that several threat actors leveraged multiple products, goods and services together to maximize potential impact and profit. The target on financial services has remained a large one, with new actors constantly developing ways to pry money away from its rightful owners.