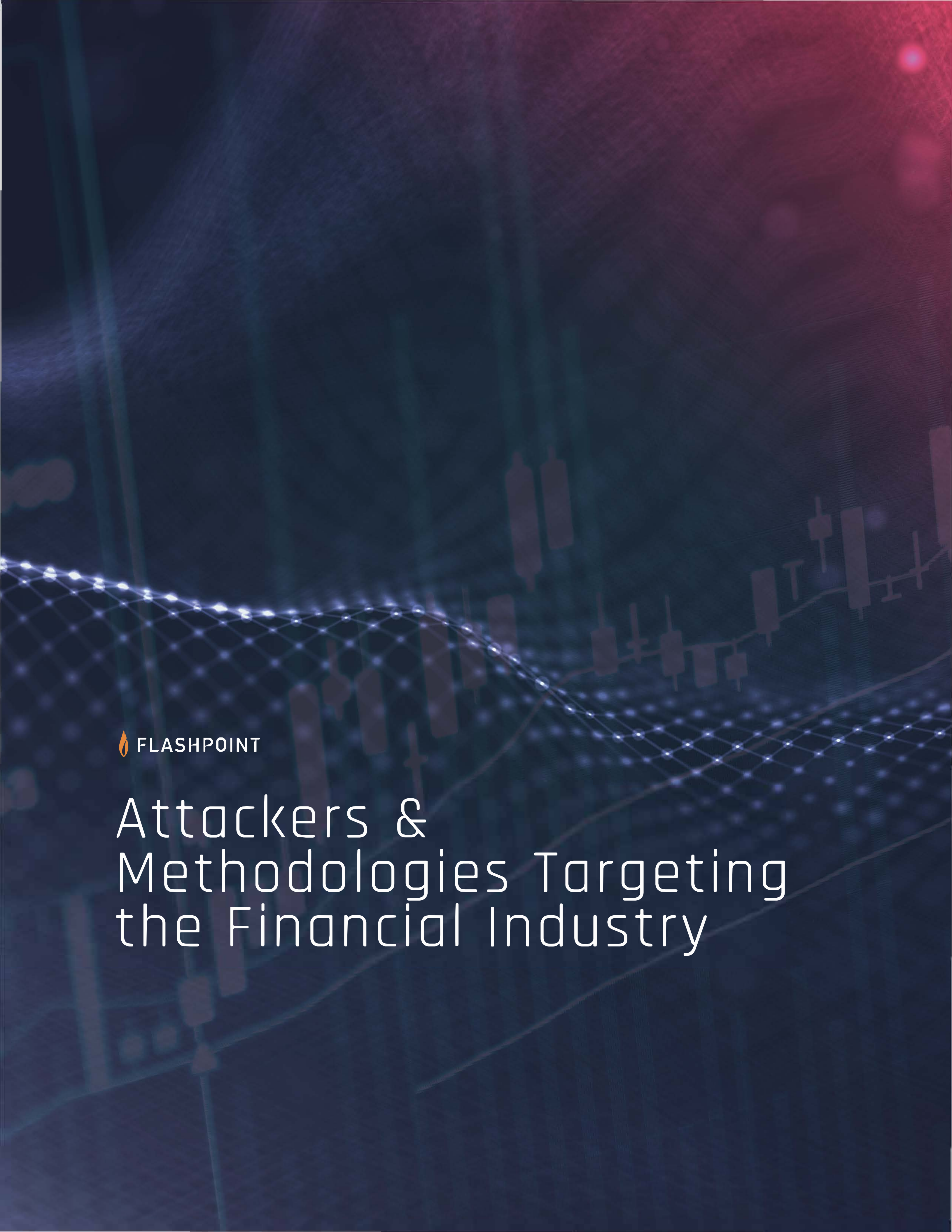


FLASHPOINT

Attackers & Methodologies Targeting the Financial Industry

ABSTRACT

The heavily regulated financial industry has long been considered a bleeding-edge investor in security technology and a forerunner in the area of policy, all with the goal of protecting customers' money from determined hackers. Unfortunately, financial services institutions are not immune from the decades-long cat-and-mouse game with threat actors.

Attackers have the luxury of not having to adhere to regulations, laws, and industry standards, and are free to pivot as they see fit in order to turn a profit. Financial services, meanwhile, is almost forced to be in a perpetual reactive state when it comes to defense, in particular against emerging threats.

In the past two years, the financial and credit sectors have been saturated with attacks from a growing roster of criminal and state-sponsored elements targeting banks with a holster full of known and unknown vulnerabilities and exploits.

This paper will examine the long line of threats banks and credit institutions must contend with and the challenges they face from cybercriminals and advanced persistent threat actors, both of which are equally likely to use targeted attacks, social engineering, phishing, and insiders to obtain their malicious objectives.

INTRODUCTION

Whiplash. That's what it's like to be a security and risk professional in the financial services and credit industries. Necks snapping back and forth on a dime as cybercriminals converge from one direction, nation-states from another. Ransomware here, stolen credentials there, zero-days at 12 o'clock. It's a dizzying windmill of threats that does not abate no matter how much professionals in this highly regulated industry invest in technology and lead the way in policy formulation and execution.

Bad guys are still coming for the money, and this is where money lives.

What's changing is that it's not just customers' money the crooks want; it's also their goal to live on a financial network, pivoting from system to system, using stolen passwords and exploiting vulnerabilities to maintain persistence on the most coveted of networks. Attackers have progressed from almost exclusively targeting banking customers, to stealing money straight from the source.

The collection of attacks used against financials reads like a who's-who of the malware world: cryptocurrency miners, ransomware, phishing, banking Trojans, fileless malware. The roster of attackers, meanwhile, has also expanded to include state-sponsored groups such as the Lazarus Group, Sofacy, and others, in addition to dozens of organized cybercrime groups. And much of it is aimed at institutions including banks, credit unions, wealth management firms, and the SWIFT banking network.

THE ABCS OF APTS AND FINANCIAL ATTACKS

The SWIFT banking network, or the Society for Worldwide Interbank Financial Telecommunication, is the primary means of secure, reliable communications between financial institutions. The global network processes transactions and messaging between banks and it's been a sweet spot for limited targeted attacks carried out by APT groups since at least 2016 to the tune of tens of millions of dollars in fraud.

This is an about-face for state-sponsored APT activity when taken into consideration that these groups are considered the elite among threat actors and generally well funded by governments or organizations loyal to states.

Yet in the early half of this decade, some of the elite—and near-elite—decided to turn a profit and begin to self-fund operations by attacking financial institutions and the infrastructure supporting them. An appealing target was the SWIFT network given the percentage of the global economy moving through its pipes on a daily basis.

The network was attacked on numerous occasions and in different geographies with the largest reported loss coming in a February 2016 attack against the Bangladesh Bank, below, that resulted in more than $850 million in fraudulent SWIFT-based transactions ($81 million of which were not recovered). Attackers alleged to have ties to North Korea's Lazarus Group, a.k.a. Hidden Cobra, are believed to also have attacked other financial institutions, financial trade software development companies, cryptocurrency markets, and casinos. The Bluenoroff group, as identified by BAE Systems and Kaspersky Lab, is a splinter group of Lazarus whose function is to self-support the rogue nation's APT-based espionage activity.

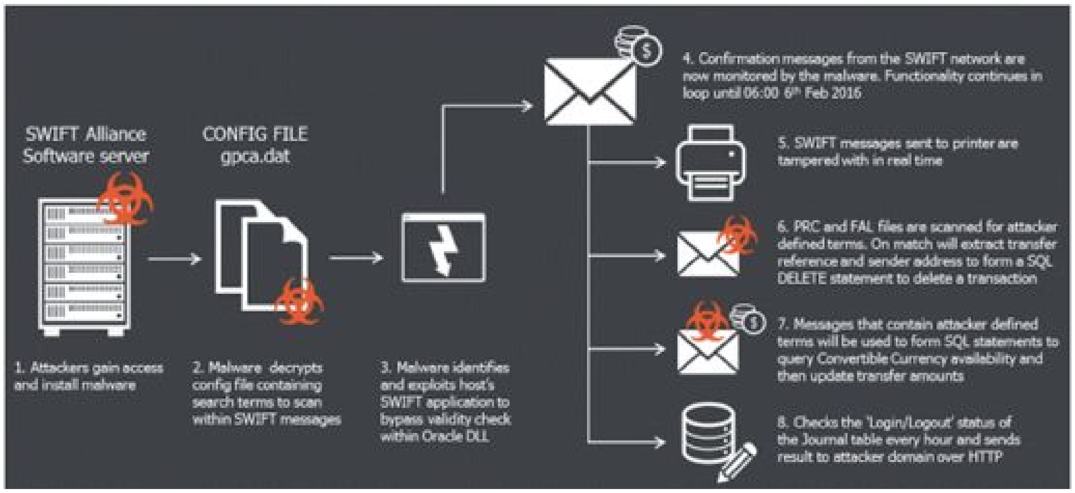

SWIFT Alliance Software server
CONFIG FILE gpca.dat
1. Attackers gain access and install malware
2. Malware decrypts config file containing search terms to scan within SWIFT messages
3. Malware identifies and exploits host's SWIFT application to bypass validity check within Oracle DLL
4. Confirmation messages from the SWIFT network are now monitored by the malware. Functionality continues in loop until 06:00 6th Feb 2016
5. SWIFT messages sent to printer are tampered with in real time
6. PRC and FAL files are scanned for attacker defined terms. On match will extract transfer reference and sender address to form a SQL DELETE statement to delete a transaction
7. Messages that contain attacker defined terms will be used to form SQL statements to query Convertible Currency availability and then update transfer amounts
8. Checks the 'Login/Logout' status of the Journal table every hour and sends result to attacker domain over HTTP

Image 1. Anatomy of the 2016 SWIFT attack against the Bangladesh Bank.

Attacks against the SWIFT network (others were also reported in Poland, Vietnam and in South America) are not straightforward, and often require attackers to invest time and money learning how the network operates and where exploitable vulnerabilities may be found. APTs with the ability to use purpose-built malware to target the network, for example, could gain access to sensitive databases, modify SWIFT transactions and messaging between parties, and bypass controls in order to leave few clues behind after an attack.

SWIFT reacted by providing advice to protect the client side of SWIFT network-related transactions, insisting that its network and core messaging services were intact. Customers can also receive a daily validation report of their transactions on a separate communication channel in order to verify the days transactions and get an immediate inkling of whether their interaction with the SWIFT network was at all compromised.

Carbanak:

Then there's Carbanak, which is also known as the Fin7 group and also Cobalt. Carbanak's activities were disclosed in 2015 but it's activities date back at least two years prior. The group is believed to be Russian-speaking and its capabilities harken to those of an APT group in its resourcefulness and sophistication.

Carbanak is alleged to have stolen more than $1 billion from as many as 100 banks across the globe using a custom-built backdoor and known penetration-testing tools to steal credentials and access financial networks. Once the group had access to admin machines, it would transfer money to mule accounts, install malicious code that instructs ATMs to remotely dispense money at certain intervals where mules would be present to collect it, and it also manipulated transactions across the SWIFT network and other payment systems to make payments to designated accounts.

The group's use of known pen-testing tools such as Metasploit, Mimikatz, and Cobalt Strike among others allows it to hide malicious activity among innocuous and seemingly legitimate network traffic. Cobalt Strike is an exploit kit that pen-testers use to stress test enterprise networks against vulnerabilities and known exploits. It was used in targeted attacks against financials throughout 2017, including a $1B ruble ($17M USD) robbery targeting Russian credit institutions. The goal was either to fraudulently cash out using ATMs or phony payment card processing where fraudulently obtained cards are transferred to mules with an attacker having the ability to raise withdrawal limits or card balances.

On Aug. 1, the U.S. Department of Justice announced the arrest of three individuals key to the Fin7 operation and were alleged to have been involved in attacks against more than 100 companies in 47 states and the theft of millions of credit card numbers. It's unclear what kind of dent the arrest may put into the illicit organization.

APTs also have targeted brokerage firms given the sensitive investment data they maintain for large clients; that data can be monetized in a number of ways, including being sold to competitors or held for ransom on the Deep & Dark Web (DDW). The data stolen from wealth management companies may include intelligence on potential human targets, adversary economic data, and information that can help guide economic, political, or diplomatic decisions. Attacks against data warehouses and repositories serving these firms are rare, but interest may be climbing to do so, in particular as attacks against data stored in other cloud-based storage systems prove successful because of weak access controls or poor configuration management decisions.

Insiders are also a threat to wealth management houses given their privileged access to data on thousands of clients, which has value on the DDW. Brokerage firms are also susceptible to the same vulnerabilities and attacks common across industries, including technical remote compromises via Remote Desktop Protocol bugs, web server or web application vulnerabilities, brute-force attacks, and compromised credentials. Executives may also be targeted via business email compromise schemes, which are largely social engineering attacks where decision makers are lured into making fraudulent wire transfers or downloading malware onto sensitive systems.

Mitigations:
Organizations are urged to maintain vigilance against phishing via employee training, maintain up-to-date antivirus and intrusion prevention system signatures, and install software on ATMs to detect and prevent unauthorized third-party program execution. Security vendors and threat intelligence companies provide indicators of compromise that can be integrated into security systems for monitoring of specific attacks and connections to external servers that could be part of a command-and-control infrastructure.

PARADOX OF CYBERCRIME: COMPLEX ATTACKS AND LOW-HANGING FRUIT

While APTs have made financial networks and infrastructure the center of their activity, cybercriminals continue to concentrate on attacking, defrauding, and stealing from customers and online banking consumers.

Banking malware continues to be developed, bought, sold and traded at will, focusing on desktop and mobile platforms alike in an attempt to defeat heightened security controls implemented by financial and credit institutions and increased awareness of security by consumers.

Nonetheless, malware families such as Zeus, Dridex, Dyre and their offspring such as Trickbot and IcedID remain in heavy circulation, today racking up hundreds of millions of dollars in losses.

Trickbot:
Trickbot, a successor to the Dyre, or Dyreza, family of banking malware that disappeared in 2015 and has been used to attack financial institutions worldwide has been updated continuously and includes new modules that make it difficult to detect the malware's activity. Trickbot, however, employs human fraud operators in conjunction with its automated capabilities to infect and steal data from machines to present defenders with an imposing opponent.

Recently, Flashpoint analysts revealed that the operators behind Trickbot were collaborating with the operators of IcedID, sharing victims and profit, and forming a formidable criminal operation.

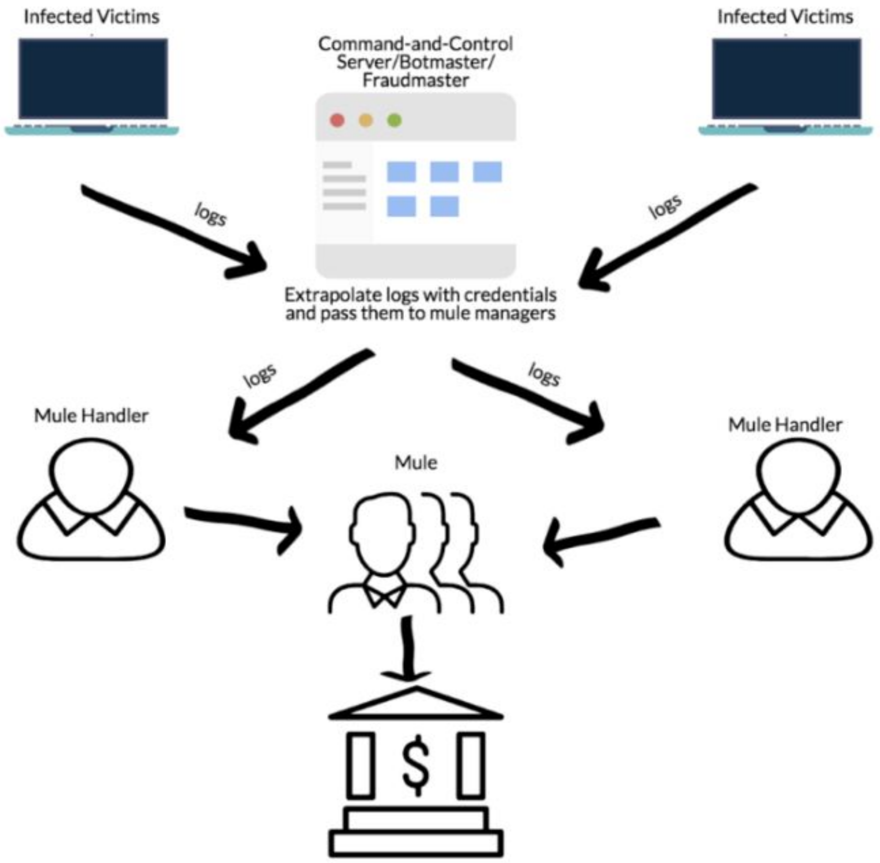


Image 2. A typical fraud ecosystem that involves IcedID/TrickBot cash-outs.

These attacks are complex and involve the use of token grabbers, redirection attacks, and webinjects to steal banking credentials. There are also other modules at the operators' disposal that allow them to have deep coverage of a victim's machine (below is an example of its backconnect proxy) and expand the breadth and scope of an attack, thereby allowing them to derive additional potential sources of profit from a successful compromise.

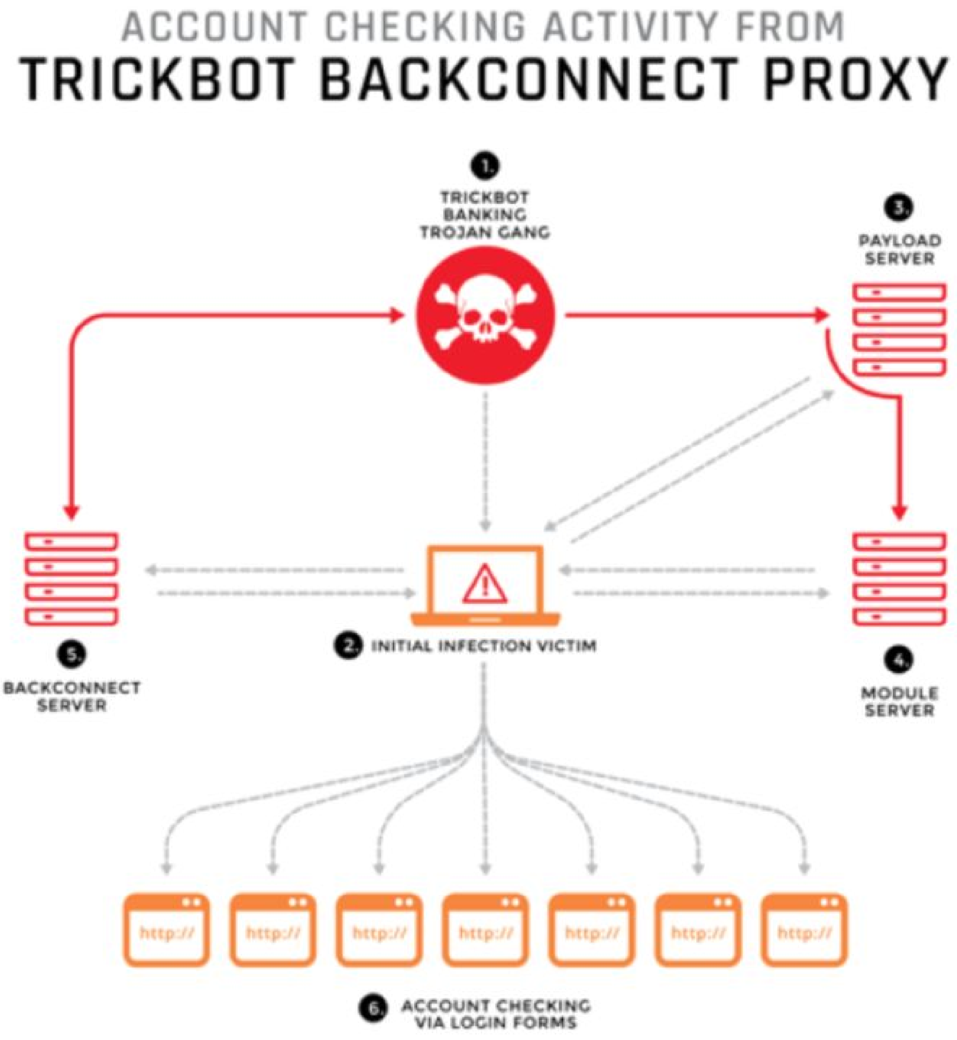

ACCOUNT CHECKING ACTIVITY FROM
TRICKBOT BACKCONNECT PROXY
1. TRICKBOT BANKING TROJAN GANG
3. PAYLOAD SERVER
5. BACKCONNECT SERVER
2. INITIAL INFECTION VICTIM
4. MODULE SERVER
http://
6. ACCOUNT CHECKING VIA LOGIN FORMS

Image 3. Overview of Trickbot's backconnect proxy account checking activity.

Key to this complete coverage is the ability to carry out account checking, or credential stuffing, in order to determine the value of a victim's machine and their access. Attackers can leverage higher value targets for network penetration, for example, while attackers can use other compromised targets for cryptocurrency mining.

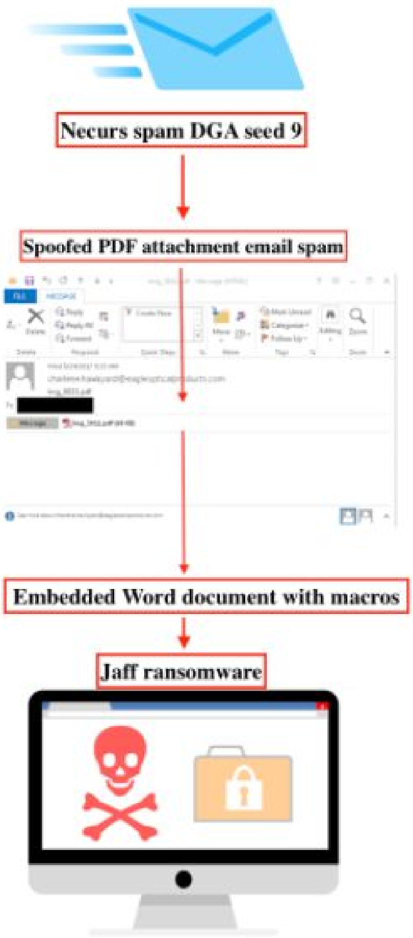
IcedID:

IcedID has been in the wild since April 2017 and was originally known as BokBot; this malware is exclusively a threat to Windows. Emotet was associated with this malware, and operators used it mainly as a loader and to maintain persistence in order to install and execute additional malware, including a virtual network computing (VNC) module for remote management and an antimalware bypass module.

IcedID creates proxies that are used to steal credentials for a host of websites that are mainly in financial services, though some sites also correspond to the retail and technology sector. The local proxy intercepts traffic and uses a webinject that steals login data from the victim.

Ransomware:

A report published recently by a security and storage company said that 90 percent of financial organizations were targeted with ransomware. This type of malware has wreaked havoc for the past three years, locking down and encrypting critical systems regardless of industry. The most notable attacks in recent memory, WannaCry and NotPetya, targeted healthcare and other industries—including financials—indiscriminately on a global scale; NotPetya included a destructive capability that would overwrite a victim's hard drive, wiping it clean and rendering it unusable going forward.


Necurs spam DGA seed 9
Spoofed PDF attachment email spam
Embedded Word document with macros
Jaff ransomware

[redacted]

Image 4. The Necurs-Jaff delivery chain reveals heavy usage of PDF attachments.

Often, attackers are likely to spam out banking malware that includes a ransomware payload as well. The Necurs botnet has at different intervals spammed out banking malware along with the notorious Locky ransomware and its predecessor, Jaff ransomware. The malware is hidden inside an attachment, including macro-based executables where a victim is tricked into enabling macros in order to read an alleged invoice or shipping order attached to an email.

Ransomware encrypts locally stored drives, and some samples have the capability of seeking out network shares and encrypting machines on those drives as well. The data stored on the drive held for ransom, and instructions are provided on how to remit payment in cryptocurrency. Authorities advise against paying ransoms in these instances and instead advise users to frequently backup systems and store those backups securely, as well as maintain up-to-date antivirus signatures.

Other threats to financials:

Business email compromise (BEC) doesn’t specifically target financial institutions, but losses attributed to these scams dwarf those tied to ransomware, for example. BEC targets executives and other individuals inside an organization, usually those with close ties to moving money and authorizing wire transfers and other payments. Financial and lending institutions have suffered heavy losses, along with other sectors including real estate and law firms. After a bit of reconnaissance, a phishing email is sent to the targeted higher-up that either is laced with malware that affords the scammer access to the exec’s inbox, or socially engineers the executive into trusting the malicious party on the other end of the message.

From the executive's inbox, the criminals learn about the target's relationships, activities, interests, and travel plans, then scrape the target's email addresses and check for correspondence or keywords that would indicate a wire transfer. The fraudsters additionally forge the sender's email address as displayed to the recipient, so that it appears to be from a legitimate contact when it is actually a spoofed domain. The fraudulent emails are then sent to employees, requesting that they transfer funds to foreign banks.

Insider threats:

Privileged access afforded to a critical insider is like a magnet to an attacker targeting a financial or credit institution. Insiders who are disgruntled and have access to critical internal systems can engineer fraudulent transfers and cover them up in order to avoid triggering alarms or leaving clues in logs. Insiders have been responsible for elaborate schemes where money is moved to fraudulent companies or accounts controlled by outside accomplices. Insiders understand how internal systems work, know which vulnerabilities exist, and how to clean up after themselves. One bank employee withdrew money from customers' accounts and backfilled them with funds from other accounts in a Ponzi-like scheme, while another incident featured a bank employee who knew how much to withdraw from client accounts—allegedly on the client's behalf—without triggering internal alarms and forging signatures in order to cover his tracks. Greed eventually did in this particular insider who withdrew a sum that tripped the bank's threshold.

Mitigations:

Malware and vulnerability exploits require the same care and vigilance whether it's an emerging threat or a commodity attack. Basic security blocking and tackling are fundamental to combating malware; timely patching of vulnerable systems, reliable and available backups, and updated antivirus signatures are a must. All of this combined with finished intelligence culled from a presence on the DDW and human analysis of current and impending threats help risk managers and security professionals combat a majority of threats.

CONCLUSION

Financial services and credit institutions yield potentially high profits for cybercriminals meaning they will likely continue as a valuable target. Given that banks and lenders tend to be leaders in cybersecurity and other relevant protections, cybercriminals and APTs face a challenge gaining access to these sensitive networks and figure to profit most from targeting customers.

Successful attacks against institutions are predominantly in regions with lower security awareness that lack the infrastructure to aptly protect their financial data. The range of sophistication required to steal from these locations varies, and advanced attackers have the time, resources and patience to target these locales, especially if they're doing so to fund their own operations.

Due to the self-reported nature of cyberattacks, the full economic impact of cyberattacks on a company's parent institution cannot be assessed from attacks targeting their holdings. The attacks that are publicized are likely to encourage small groups of technically sophisticated threat actors. However, the recent news of high-profile cybercriminal arrests are likely to also deter several threat actors from future targeting.

CREDITS

The primary author of this report is Mike Mimoso. A special thanks to the entire Flashpoint intelligence analyst team for their dedication and contributions to this report. Contributors to this report include Carles Lopez-Penalver, Luke Rodeheffer, and Leroy Terrelonge III.

ABOUT FLASHPOINT

Flashpoint delivers Business Risk Intelligence (BRI) to empower organizations worldwide with meaningful intelligence and information that combats threats and adversaries. The company's sophisticated technology, advanced data collections, and human-powered analysis uniquely enables large enterprises and the public sector to bolster cybersecurity, confront fraud, detect insider threats and build insider threat programs, enhance physical security, improve executive protection, and address vendor risk and supply chain integrity.

For more information, visit **www.flashpoint-intel.com** or follow us on Twitter at **@FlashpointIntel**.