Modern Bank Heists: The Bank Robbery Shifts to Cyberspace

Financial Institution CISOs reveal the cyber threats keeping them up at night, including Emotet, Steganography & Hidden Cobra

By Tom Kellermann, Chief Cybersecurity Officer, Carbon Black
Bill Young, Vice President Threat Management, Optiv

MARCH 2019
Executive Summary

In the second annual “Modern Bank Heists” report, Carbon Black collaborated with Optiv to survey CISOs at some of the world’s largest financial institutions to uncover cyberattack trends.

The financial sector has long been the target of some of the world’s greatest guilds of thieves, none perhaps more popular than the Dillinger gangs of the 1930s. This second annual report highlights how financially motivated criminals have evolved from stagecoaches and stickups to targeted cyberattacks.

Over the past year, cyber defenders have seen a high level of innovation from cybercriminals, who are leveraging new tactics, techniques and procedures (TTPs) to maintain persistence and counter incident response efforts.

To better determine how these cybercriminals are hiding behind invisibility cloaks to remain undetected, Carbon Black conducted a survey, comprising input from CISOs of many of the world’s largest financial institutions. The purpose of the survey is to improve telemetry for threat hunt teams and defenders.

In this survey, CISOs revealed trends in lateral movement, counter incident response, integrity attacks and the most concerning threat actors and counter incident response efforts. It’s important to note that financial institutions, relatively speaking, typically have a more robust cybersecurity posture than peers in other verticals. However, this does not make them immune to cyberattacks. There is still considerable opportunity for financial institutions to improve cybersecurity posture and go on the offensive with threat hunting teams.

We would like to thank the numerous financial institutions who participated, including four of the top 10 banks in the world. The authors would also like to thank six individuals who added valuable insights to this report: David Balcar, Paul Drapeau, Rick McElroy, Ryan Murphy, Chris Stolley and Patrick Upatham.
67% of surveyed financial institutions reported an increase in **cyberattacks** over the past 12 months.

26% of surveyed financial institutions reported they were targeted by **destructive attacks** over the past year. Destructive attacks are rarely conducted for financial gain. Rather, these attacks are launched to be punitive by destroying data. Of note, this figure represents a 160% increase over 2018 suggesting the “bank heist” is evolving into a hostage situation.

32% of surveyed financial institutions encountered **“island hopping,”** an attack where supply chains and partners are commandeered to target the primary financial institution.

21% of surveyed financial institutions experienced a **watering-hole attack** during the past year. In these attacks, financial institution and bank regulation websites are hijacked and used to pollute visitors’ browsers. This tactic is increasing in the wild as cybercriminals recognize the implicit trust consumers have in bank brands.

47% of surveyed financial institutions reported an increase in **wire transfer fraud.** These attacks are often performed by exploiting business process gaps in the wire transfer verification process or through social engineering attacks targeting customer service representatives and consumers directly.

31% of surveyed financial institutions reported an increase in **home equity loan fraud.** In these attacks, malicious actors are targeting consumers through spear phishing or making direct withdrawals from Home Equity Line of Credit (HELOC) accounts by way of exploiting business process gaps and online account compromise.

79% of financial institutions said cybercriminals have become more sophisticated, leveraging highly targeted **social engineering attacks,** advanced TTPs for hiding malicious activity, and exploiting weaknesses in people, processes and technology to gain a foothold that is persist in the network enabling the ability to transfer funds and exfiltrate sensitive data.
Emotet

One such example of sophistication with respect to attacks against financial institutions is Emotet, an advanced, modular banking trojan that primarily functions as a downloader or dropper of other banking trojans.

The developers of the Emotet trojan stole money automatically from victims’ bank accounts via automatic transfer systems (ATSs).

The Emotet trojan has a modular structure:
- Installation module
- Banking module
- Spam bot module, used for stealing address books from Microsoft Outlook
- Module for organizing Distributed Denial of Service (DDoS) attacks (Nitol DDoS bot)

Attackers are increasingly leveraging PowerShell and encrypting the URLs of the C2s used to host the second-stage payload. The Emotet trojan downloader obfuscates VBScripts using PowerShell and the Convert-To-Secure String .cmdlet, which, in the final stages, is used to decrypt the C2s and associated logic.

Emotet is among the most costly and destructive malware affecting the financial sector. Attackers continue to leverage variants of Emotet and are becoming increasingly shrewd in the techniques they employ to deliver the malware onto an infected system.

In 2018 Carbon Black’s Threat Analysis Unit (TAU) and other researchers observed the adaptation to existing methods leveraging PowerShell, where attackers were encrypting the URLs of the C2s used to host the second stage payload.

**Emotet Endpoint Behavior**
- Parent process == services.exe
- Path of System32 or SysWOW64
- New service creation
- Registry or Event Log (ID 7045)
Additional Threats Targeting the Financial Sector

According to TAU’s analysis of attacks seen across the Carbon Black customer footprint, the most prevalent threats targeting the financial sector so far in 2019 are: Adload, ATRAPS, Egguard, Emotet and GenericKD.

Adload is capable of opening a backdoor on the affected system for it to download and install adware or potentially unwanted programs (PUPs). This trojan can also gather information about the affected system, such as username and computer name, and send them to a remote location.

ATRAPS is a trojan that targets Windows platforms. ATRAPS is designed to steal confidential information from targeted computers and send it to a remote server. ATRAPS may also install additional malware onto the compromised computer and deactivate Windows system functions. ATRAPS can spread through infected file-sharing sites or corrupt video codecs, so use caution when downloading anything onto a computer.

Egguard sets a proxy accompanied with a false SSL certificate to perform a man-in-the-middle (MITM) attack.

GenericKD ransomware encrypts files stored on the affected device and demands payment of a ransom.
Evolution from Bank Robbery to Hostage Situation

Through denial of service attacks, land-and-expand attacks establishing multiple points of persistence and increased dwell time within an organization. This leads to destruction of EDR and other security logs. Malicious actors have transformed the traditional smash-and-grab attack into an ongoing siege-based hostage situation.

32% of surveyed financial institutions reported experiencing **COUNTER INCIDENT RESPONSE**. Attackers are fighting back to protect their position. Rather than just avoid detection, they are taking counter-measures to thwart responders and maintain their presence throughout the network.

21% of surveyed financial institutions reported experiencing **C2 ON A SLEEP CYCLE**. As noted by the latest Carbon Black Quarterly Incident Response Threat Report (QIRTR) cybercriminals are appearing to embrace the Eastern European tactic of deploying C2 on a sleep cycle. This allows malicious actors to minimize detection by varying their presence, appearing from different locations throughout the network at different times, and disconnecting before their access channels can be fully identified and cut off.

32% of surveyed financial institutions encountered **“ISLAND HOPPING,”** an attack where supply chains and partners were commandeered to target the primary financial institution.

Island hopping typically takes on three forms:
- Network attacks
- Watering-hole attacks
- Reverse business email compromise (BEC)
Island hopping attacks come from a wide variety of vantage points, whether it's through partner provisioned Virtual Desktop infrastructure (VDI) access, private network links and VPNs or by leveraging the compromise of partners to establish trust and perform trusted social engineering attacks.

In the case of reverse BEC, a cybercriminal commandeers a bank mail server and then conducts whaling by sending email with fileless malware (via the bank mail server) to high-profile customers, partners and subsidiaries. Due to the implicit trust placed in bank communications, this tactic is often successful.

The end result of all of these attacks is the risk of a long-term hostage siege, with the attacker setting up command posts throughout the network. Frequent threat hunting is a critical requirement to identify and mitigate these transient and obfuscated points of presence.
Steganography and C2 Obfuscation

One particular way cybercriminals can deploy C2 on a sleep cycle is via image steganography and embedding malicious traffic in seemingly normal network traffic.

Steganography (the practice of concealing data in other content types such as images, videos, network traffic, etc.) continues to play a role in modern attacks in several forms. Most uses of steganography in malware can be divided into two broad categories, concealing the actual malware contents itself and concealing the command and control communications channel.

Embedding multiple content types within a single file (by utilizing unused portions of the file format, appending data to the end of the file, etc.) has been a common technique seen in many malware droppers for some time. This technique is used to evade detection on the network wire and on the endpoint as well has hide content on disk in familiar file types such as images.

More sinister and advanced versions of this tactic have been observed, which involve covertly embedding malware code payloads in image files. One example is ZeroT’s use of BMP files, such as pictures of Britney Spears, to download in later payload stages.

Carbon Black also documented where an attacker had embedded malicious code into a set of PNG files. The PNG files were then compiled into a legitimate application, along with a function that would extract and drop the malware onto the system.

Figure 1 PNG images with Malicious Code Embedded
Additionally, attack groups recently began targeting an organization in Italy, also leveraging a form of steganography. In this attack the secondary PowerShell command and payload were encoded and embedded in a PNG file.

Steganography is also used in command and control protocols for malware, including reading content from image files available via sharing and social media sites. The network traffic and the associated downloaded images hide in plain sight among the other legitimate common uses of such services.

Tunneling C2 communications in existing protocols such as DNS and HTTP by embedding information in unused or uncommon fields is also often seen in modern malware and is a form of steganographic covert channel. This tried and true technique is seen in delivery, command and control as well as exfiltration. While traditional DNS and HTTP tunneling are still used to open C2 channels, attackers continue to find more creative ways to hide their malicious communications. For example, attackers are leveraging highly reputable domain resources, such as content delivery networks (AWS, Akami, Cloudflare, Google Cloud, etc), to open covert channels, allowing them to bypass content filters as those locations are generally trusted. This is referred to as Domain Fronting, and the traffic is often encrypted using HTTPS making it difficult to detect and prevent.

Recent Campaigns Using Steganography:
- GandCrab
- Zerp
- ZeusVM
- Triton
- Sundown Exploit Kit
- Carbanak
- VeryMal

Steganography use is suspected when:
- You see two of the same files on a hard drive and the sizes are different, sometimes significantly (double or triple the size).
- The file headers for that file type differ. Using the LSB method, the human eye cannot see the differences in color. Note: Typical JPEG files start with FF D8 and end in FF D9.
- Traffic patterns deviate from standard user activity. This can be an indication of tunneled communications and data exfiltration that is outside of the norm for the protocol in question.
Geopolitical Tension, Financially Motivated Attacks & Hidden Cobra

Geopolitical tension is manifesting in cyberspace. A few rogue nation state threat actors have been offsetting economic sanctions via attacks on Society for Worldwide Financial Telecommunications (SWIFT) and other payments systems. Hidden Cobra out of North Korea is one group that embodies this phenomenon.

Originally released as Alert (TA18-275A) from the US-CERT on October 2, 2018, the Hidden Cobra APT cybercriminal group dates back to at least 2009.

A campaign known as FASTCash targeted banks in Africa and Asia. Active since 2009, the Hidden Cobra APT group is also reportedly associated with the WannaCry ransomware and the SWIFT banking attack against a Bangladesh bank in 2016.

The Hidden Cobra APT group starts by sending out spear-phishing emails to bank employees. Once the victim clicks on the email, a Windows-based malware (Bankshot RAT) checks to see which version of the Payment Switch Application Server is in use at the bank. Following that, bank employee credentials are stolen via malware that extracts the user credentials from the windows lsass.exe. The C2 channels are hidden in openSSL channels and hides communications in false TLS handshakes.

At this point in the attack chain, legitimate credentials are used to move laterally through the bank network to gain a foothold on the Payment Switch Application Server, from which attackers begin to make ATM withdrawals.

The Hidden Cobra APT group has also utilized DDoS attacks targeting the media, aerospace and critical infrastructure around the world. These attacks are targeting CGN, NTP and DNS services going back to 2014.

*Please see [https://www.us-cert.gov/ncas/analysis-reports/AR18-275A](https://www.us-cert.gov/ncas/analysis-reports/AR18-275A) for full technical analysis of the malware samples from these attacks.
The malware being utilized in these attacks against banks targets vulnerable versions of Adobe Flash and Microsoft Silverlight.
Cyber Governance

62% of surveyed financial institution CISOs STILL REPORTED TO THE CIO. This reality represents a potential governance crisis. CISOs must be empowered with greater authorities and separate budgets in order to preserve safety and soundness in the financial sector. CISOs should report to CEOs or CROs as their defensive mindset often conflicts with the uptime, availability, and content driven goals of CIOs.

69% of surveyed financial institution CISOs are planning to INCREASE CYBERSECURITY SPENDING by 10% or more. Within that allocation of resources, 68% of these CISOs said they will be hiring additional security professionals, which may be a tough task considering the global shortage of skilled cybersecurity professionals.

47% of surveyed financial institution CISOs said their organizations are OPERATING THREAT HUNTING TEAMS – an increase of 27% from 2018.

It is imperative we move away from reactive security as the industry cannot afford to have a cybercriminal dwell on their systems for months until they are notified by law enforcement. Plausible deniability must be eliminated.

32% of surveyed financial institution CISOs said they CONDUCT THREAT HUNTS ON A MONTHLY BASIS. A handful of very proactive financial institutions said they conduct hunts daily.

Active threat hunting is an important step for organizations with mature security programs. It puts defenders “on the offensive” rather than simply reacting to the deluge of daily alerts. Strategic understanding of your environment will be key to driving a winning strategy.
Golden Rules of Threat Hunting

Threat hunting should aim to find abnormal activity on servers and endpoints that may be signs of compromise, intrusion or exfiltration of data.

**RULE I:** Go Historical—take in tactical threat intelligence of domains, hashes and IPs, and be able to search the last 30 days. Remember, it is easy for attackers to change Domains and IPs which will equate to unnecessary false positives.

**RULE II:** Move Up the Pyramid of Pain—change the threat intelligence language to move toward TTPs (actions or behaviors). The MITRE ATT&CK framework is fundamental during this stage.

**RULE III:** Move to anomaly based hunting—algorithmic threat hunting; changes in behavior versus similarities to previously seen.

70% of cybercrimes targeting surveyed financial institutions **INVOLVE LATERAL MOVEMENT**. Suppressing the adversary is imperative before they move laterally. Implement identity and patch management-based controls to minimize lateral and vertical movement. Ensure that EDR solutions are logging and reporting suspicious activity that could indicate a malicious actor moving throughout the network. Clandestinely observe the adversary and suppress their activity as we force them to become resource constrained. Decreasing dwell time requires regular threat hunting.
Conclusion

The financial sector is facing a myriad of highly sophisticated threats. Although the sector is generally more secure than other industry, it is facing the world's elite hackers, composed of organized crime syndicates and motivated nation-states. This report will be issued on an annual basis to obtain the pulse on the threats facing the sector and to educate readers on how the modern-day Dillinger gangs are evolving their tactics. For more information visit: http://carbonblack.com/finance.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leader in cloud endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint security and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 5,300 global customers, including 35 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.

Carbon Black and CB Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.

About Optiv

Optiv is the world's leading cybersecurity solutions integrator – transforming the way security is approached and consumed. Optiv develops an in-depth understanding of our clients' environments, leverages the efficiencies of cloud economics for modernized on-demand security services, and creates business-aligned solutions that are designed to deliver the clarity and assurance our clients need to effectively manage organizational risk. Optiv's approach optimizes and rationalizes existing infrastructure and operations to ensure the right balance of tools, processes, and compliance and reporting capabilities. This enables clients to build sustainable risk-centric foundations for implementing proactive and measurable security programs.