vmware Carbon Black

GET STARTED

Modern Bank Heists 3.0

25 CISOs from leading financial institutions reveal their thoughts on the 2020 attack landscape

Tom Kellermann, Head of Cybersecurity Strategy
Ryan Murphy, Security Strategy

May 2020

Executive Summary

This marks the third edition of the Modern Bank Heists report, which takes an annual pulse of some of the financial industry's top CISOs and security leaders. Thank you, again, for reading along and thank you to the 25 security leaders who participated in this year's survey.

This survey offers more than just data. We use the information gleaned from this report to educate the market on how modern cybercriminals are evolving; what tactics, techniques and procedures (TTPs) are emerging; and how defenders can keep pace. Perhaps most importantly, we use the information to deliver a stronger cybersecurity platform to the market.

In this year's survey, CISOs revealed what they're seeing with attack prevalence and evolution. Our questions tackled topics including lateral movement, counter-incident response, island hopping and integrity attacks. The financial sector is not a new target for criminals. Of course, the bank heist has evolved significantly—from stickups to cyberspace—but the fundamental motivation behind the attacks has remained: money. This evolution is best reflected in a conversation we recently had with Jonah Force Hill, senior cyber policy advisor and executive director of the U.S. Secret Service Cyber Investigations Advisory Board (CIAB), who told us:

"This year, while virtually all sectors of the global economy fell victim to cybercrime of one kind or another, no sector was more regularly targeted than the financial sector. At an alarming rate, transnational organized crime groups are leveraging specialist providers of cybercrime tools and services to conduct a wide range of crimes against financial institutions, including ransomware campaigns, distributed denial of service (DDoS) attacks and business email compromise (BEC) scams. **Criminals are increasingly sharing resources and information and reinvesting their illicit profits into the development of new, even more destructive capabilities.** *The growing availability of ready-made malware is creating opportunities for even inexperienced criminal actors to launch their own operations. When combined with a steady commercial growth of mobile devices, cloud-based data storage and services, and digital payment systems, cybercriminals today have an ever-expanding host of attack vectors to exploit.* **Every organization—providers of financial services, in particular—must remain vigilant in the face of these evolving threats.** *It is critical that organizations maintain a continuous dialogue with law enforcement to ensure a rapid response in the event of an incident."*

The authors would like to thank VMware Carbon Black Team Cerberus for their analytics research for this report.

Key Data

80% **of surveyed financial institutions reported an increase** in cyberattacks over the past 12 months, a 13 percent increase over 2019.

27% **of all cyberattacks in 2020 have targeted either the healthcare sector or the financial sector, according to VMware Carbon Black data.**

From **February to April 2020, amid the COVID-19 surge, cyberattacks against the financial sector** increased by 238 percent, according to VMware Carbon Black data.

82% **of surveyed financial institutions said cybercriminals have become more sophisticated**, leveraging highly targeted social engineering attacks and advanced TTPs for hiding malicious activity. These criminals exploit weaknesses in people, processes and technology to gain a foothold and persist in the network, enabling the ability to transfer funds and exfiltrate sensitive data.

64% **of surveyed financial institutions reported increased attempts of wire fraud transfer,** a 17 percent increase over 2019. These attacks are often performed by exploiting gaps in the wire transfer verification process or through social engineering attacks targeting customer service representatives and consumers directly.

33% **of surveyed financial institutions** said they've encountered island hopping, an attack where supply chains and partners are commandeered to target the primary financial institution.

25% of surveyed financial institutions said 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.

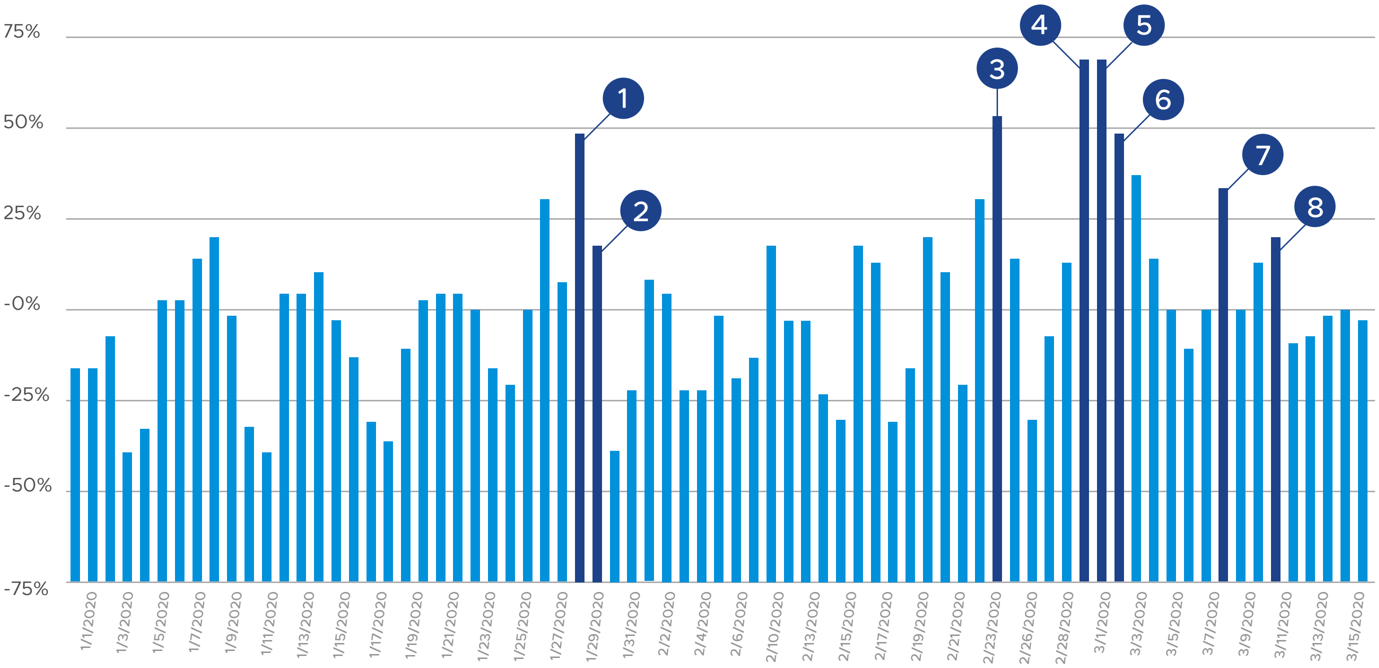
24% of surveyed financial institutions said they've encountered an **attack leveraging counter-incident response**.

20% 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 as cybercriminals recognize the implicit trust consumers have in bank brands.

Ransomware attacks against the financial sector have **increased by 9x from the beginning of February to the end of April 2020**.

Attack Prevalence and Sophistication

Each year we've produced this survey, we've been interested to see the trend with respect to attack frequency and sophistication. For this year's report, both numbers have increased over 2019. **80 percent of surveyed banks said they've seen an increase in cyberattacks over the past 12 months**, marking a 13 percent increase over 2019. And 2020 has offered a glimpse into a new world. Cybercriminals are taking advantage of COVID-19, and they are doing so in tandem with the news cycle.



1. First United States confirmed case.

2. President Trump announced entry ban on foreign nationals.

3. Announcement that 2,400+ have died globally from COVID-19 related illnesses.

4. First death in the United States.

5. Florida declares public health emergency, followed by several other states.

6. Italy COVID-19 cases surpass 2,000.

7. Italy starts lockdown.

8. WHO declares a pandemic.

FIGURE 1: Relative percentage increase and decrease by day for notable alerts observed in VMware Carbon Black data. The baseline is represented on the y-axis by 0 percent in Figure 1.

As to what specifically financial organizations are seeing, we dug into VMware Carbon Black customer data. Kryptik and Emotet continue to be among the top attacks seen across multiple sectors, including finance. These malware types are often used in longer, more complex campaigns where the end goal is to leverage native operating system tools to remain invisible or gain a foothold on one system (sometimes a supply-chain partner) to island hop to a larger, more lucrative target.

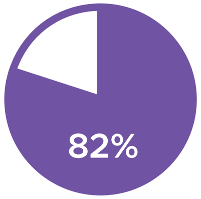
Kryptik

The Kryptik trojan attempts to target victim machines via malicious installers. It then attempts to acquire admin rights to make registry modifications, allowing it to execute each time a Windows machine boots. The Kryptik trojan can be very persistent and, without the appropriate visibility, can be difficult to detect as it attempts to delete its executable file after running.

As noted by a threat profile from the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC): “[The Kryptik trojan] queries the Windows registry for the .ini or .dat file paths. It also queries registry subkeys for the actual host, username, and password related to the specific FTP client application. Kryptik searches the registry, querying for both ftpIniName and InstallDir that hold the wcx_ftp.ini file. The trojan can recover many common FTP clients, email clients, file browsers, and file manager programs. Kryptik also can update itself and remotely download new versions.”[1]

Emotet

Emotet is a family of banking malware, which has been around since at least 2014. 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.



82 percent said attacks have become more sophisticated, a slight increase over 2019.

Kryptik was among the infections found in the notorious attack targeting the Ukrainian power grid in late 2015.

[1] New Jersey Cybersecurity and Communications Integration Cell. “*Kryptik*.” December 15, 2016.

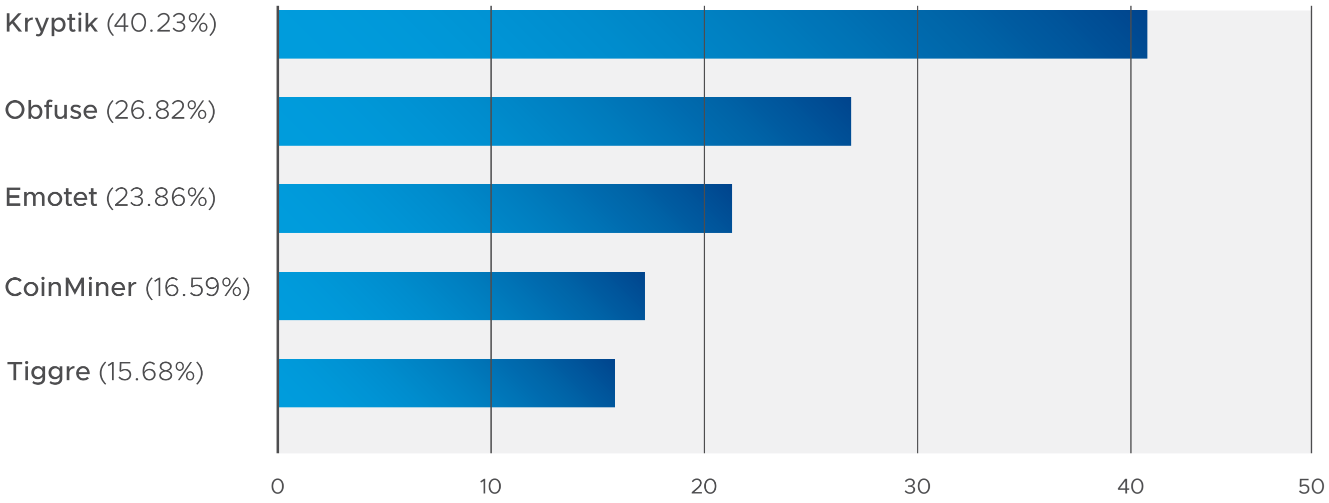


FIGURE 2: The most prevalent threats affecting the finance sector from March 2019 to February 2020.

Researchers have observed the adaptation to existing methods leveraging PowerShell, where attackers were encrypting the URLs of the command and control (C2) systems used to host the second stage payload. VMware Carbon Black has observed a spike in this type of technique being detected across customers utilizing their managed hunting services.

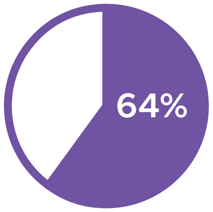
Several attacks have been observed as originating from phishing campaigns that are leveraging Microsoft Office Word documents with obfuscated VBScripts using PowerShell and the ConvertTo-SecureString cmdlet, which in the later stages is used to decrypt the C2(s) and associated logic. This represented an evolution of current macro attack techniques, where these types of cmdlets are not typically associated with phishing campaigns.

Attack Behaviors

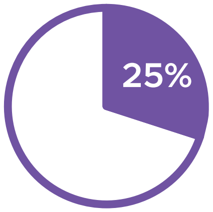
Over the past two years, we've made a concerted effort to move beyond just looking at individual pieces of malware and focus more deeply on attacker behavior. To that end, the MITRE ATT&CK framework has set an excellent standard and closely aligns with the VMware Carbon Black belief that detecting attacker behavior is exponentially more important than detecting malware alone.
With that in mind, we wanted to see what the top attacker behaviors targeting the financial sector have been over the past 12 months.

According to MITRE, "adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions." [2]

This is of particular importance in the financial sector as cybercriminals have dramatically increased their knowledge of the policies and procedures of financial institutions. They are keenly aware of the incident response (IR) stratagems being employed by IR teams and the blind spots that exist within every institution. Given the tactical shifts of the cognitive attack loop, they are maintaining and manipulating their positions within networks because of the noise created by incident response and the lack of security controls integration.



The most prevalent MITRE threat ID affecting the finance sector (64 percent of attacks) over the past year has been T1507 - Process Discovery.



Another notable threat ID (25 percent of attacks) has been T1055 - Process Injection.

[2] The MITRE Corporation. "*Process Discovery*." August 12, 2019.

According to MITRE, "process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. Malware commonly utilizes process injection to access system resources through which Persistence and other environment modifications can be made. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel." [3]

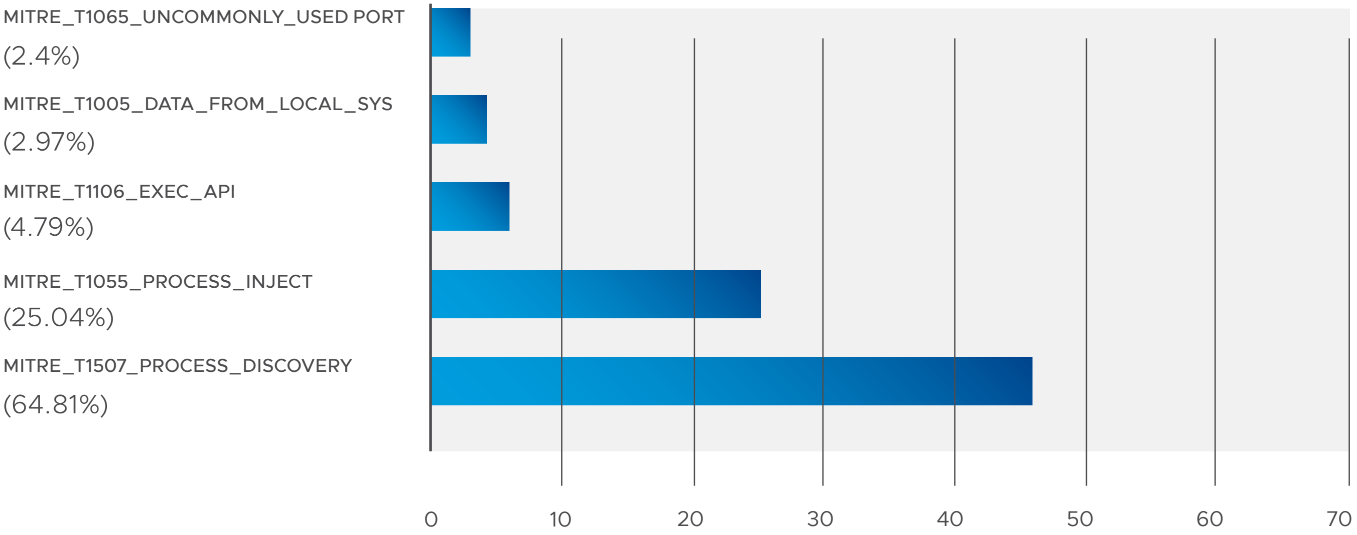


FIGURE 3: The most prevalent MITRE threat IDs affecting the finance sector from March 2019 to February 2020.

[3] The MITRE Corporation. "*Process Injection*." Anastasios Pingios, Christiaan Beek and Ryan Becwar. July 18, 2019.

A Rise in Virtual Invasions

There have been some interesting evolutions since our 2019 report. Of note, 64 percent of surveyed financial institutions reported increased attempts of wire fraud transfer, a 17 percent increase over 2019.

Wire fraud transfer 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.

Cybercriminals exhibit tremendous situational awareness regarding SWIFT messaging. This is compounded with their newfound understanding of the criticality of portfolio managers' positions.

There has been an awakening in the dark web as it relates to the value of non-public market information, which is stored on endpoints and often protected by legacy technology.

Trust and confidence can be undermined as cybercriminals appreciate that it is more valuable to commandeer the digital transformation efforts of the financial institution than to target its customers directly.

Island Hopping

33 percent of surveyed financial institutions said they've encountered island hopping, an attack where supply chains and partners are commandeered to target the primary financial institution.

There are four types of island hopping most commonly seen today

Network-based island hopping is the most frequently used form of island hopping. With network-based island hopping, attackers infiltrate one network and use it to hop onto an affiliate network.

While much less common, watering-hole attacks (one out of every five attacks targeting financial institutions) still make up a solid portion of island-hopping attacks. In these attacks, hackers target a website frequently visited by partners or customers of the organization they are trying to breach. It is important to note that watering holes are not limited to websites and can manifest on mobile applications.

There has been a newer trend in cybercrime that mainly targets the financial sector. **Reverse business email compromise attacks** occur when a hacker successfully takes over a victim's email server and executes fileless malware attacks against members of the organization as well as the board.

Island hopping as a service, or access mining is a tactic where an attacker leverages the footprint and distribution of commodity malware—in this case, a cryptominer—using it to mask a hidden agenda of selling system access to targeted machines on the dark web.

In 2019, the VMware Carbon Black Threat Analysis Unit uncovered a secondary component in a well-known cryptomining campaign. The malware had been enhanced to exfiltrate system access information for sale on the dark web. This discovery indicated a bigger trend of commodity malware evolving and will likely catalyze a change in the way cybersecurity professionals classify, investigate and protect themselves from commodity threats. Dark web forums now specialize in the sale of access to specific financial institutions via provisioning access to buyers via a remote access trojan.

Destructive attacks are rarely conducted for financial gain. Rather, these attacks are launched punitively to destroy data and dismantle subnets. It is worthy to note that cybercriminals in the financial sector will typically only leverage destructive attacks as an escalation to burn the evidence as part of a counter-incident response. According to MITRE, "Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives." It may have "worm-like features to propagate across a network by leveraging additional techniques like Valid Accounts, Credential Dumping, and Windows Admin Shares." [4] This challenges us to become more clandestine in how we conduct IR and to increase our threat hunting exercises.

25 percent of surveyed financial institutions said they were targeted by destructive attacks over the past year.

[4] The MITRE Corporation. "*Data Destruction*." July 19, 2019.

Wipers continue to trend upward as adversaries (including Iran) began to realize the utility of purely destructive attacks. Leveraging techniques across the full spectrum of MITRE ATT&CK, wipers rely heavily on defense evasion techniques (64 percent of analyzed samples).

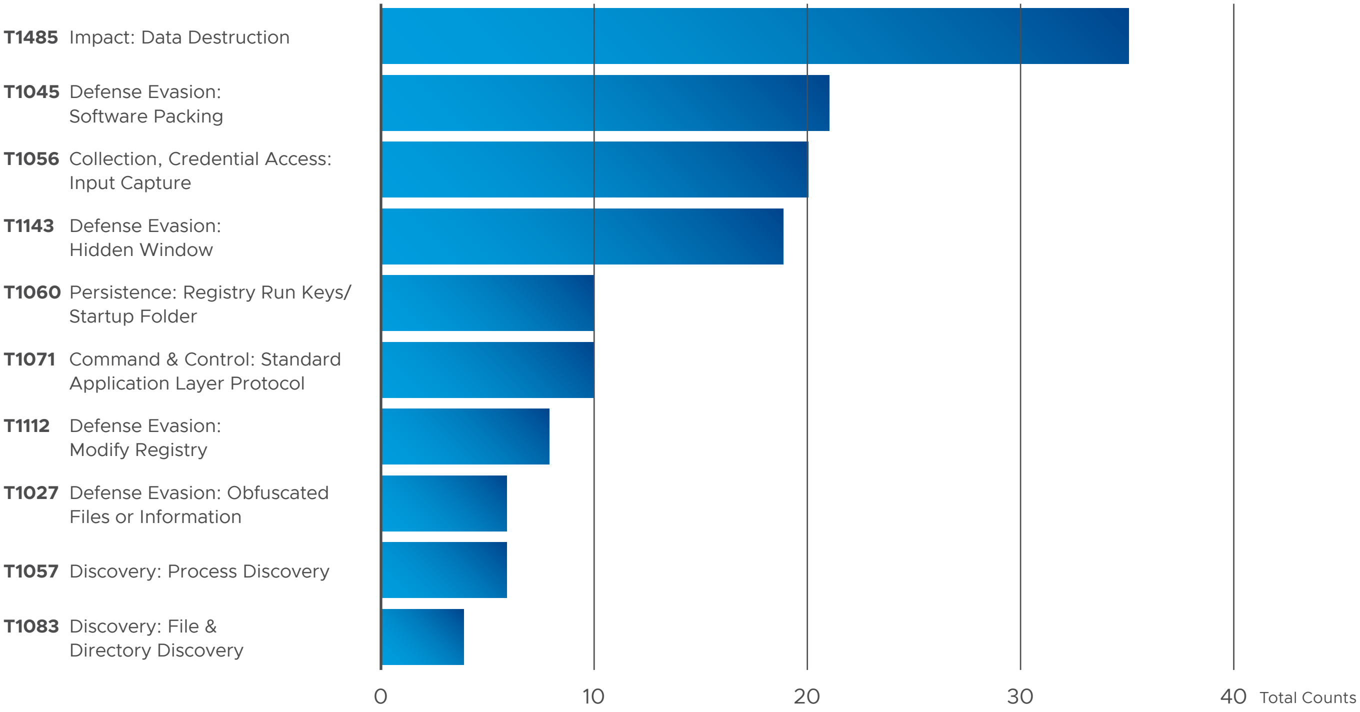


FIGURE 4: Top 10 wiper behaviors in 2019.

24 percent of surveyed financial institutions said they've encountered an attack leveraging a counter-incident response.

Figure 4 highlights the various MITRE ATT&CK TTPs associated with malware generally classified as wipers.

The most common behaviors seen across all wiper attack data mapped to the MITRE ATT&CK framework were data destruction (33 percent); software packing for defense evasion (20 percent); input capture for collection and credential access (19 percent); hidden windows for defense evasion (18 percent); and registry run keys in the startup folder for persistence (10 percent).

Bank heists are transitioning to hostage situations. Cybercriminals have no desire to leave the environment after the heist. They will fight to remain persistent on a financial institution's network. We expect this phenomenon to metastasize in 2020. Deletion of logs, manipulation of time stamps and disabling of security controls will become par for the course.

Give these realities, it's imperative we alter how we respond to incidents. Greg Foss, senior threat researcher at VMware Carbon Black, suggests the following rule of five.

1. Stand up a secondary line of secure communications.

This is vital to discuss the ongoing incident. Assume that all internal communications can be intercepted, viewed, modified and otherwise compromised by the adversary. These secondary communications should allow for talk, text and file transfer.

2. Assume the adversary has multiple means of gaining access into the environment.

Shutting off one entry point may not actually remove them from your network. This will very likely have just the opposite effect by notifying the attacker(s) that you're onto them.

3. Watch and wait.

Do not immediately start blocking malware activity and shutting off access. Do not immediately terminate the C2. To understand all avenues of re-entry, you must monitor the situation to fully grasp the scope of the intrusion to effectively develop a means of actually removing the adversary from the environment.

4. Deploy agents (if you must) in monitor-only mode.

If you begin blocking or otherwise impeding their activities, they will catch on and change tactics, potentially leaving you blind to their additional means of re-entry.

5. Deploy honey tokens or deception grids.

Especially on attack paths that cannot be hardened.

Conclusion

Cybercriminals are evolving in both attack sophistication and organization. The financial sector is the most secure industry in the world, but it is also being targeted by cybercriminals and nation-states. We must pay close attention to how we respond to these threat actors and what their ultimate goal is—hijacking your digital transformation efforts via island hopping. Cybersecurity is now a brand protection imperative. Trust and confidence in the safety and soundness of your institution will depend on it. This report should serve as a starting point for a discussion between the cybersecurity community and the defenders of the financial sector on how we might best collaborate and wage a counterinsurgency in cyberspace.

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit vmware.com/company.

Join us online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com

Item No: vmwcb-ebook-modern-bank-heists-r1 5/20