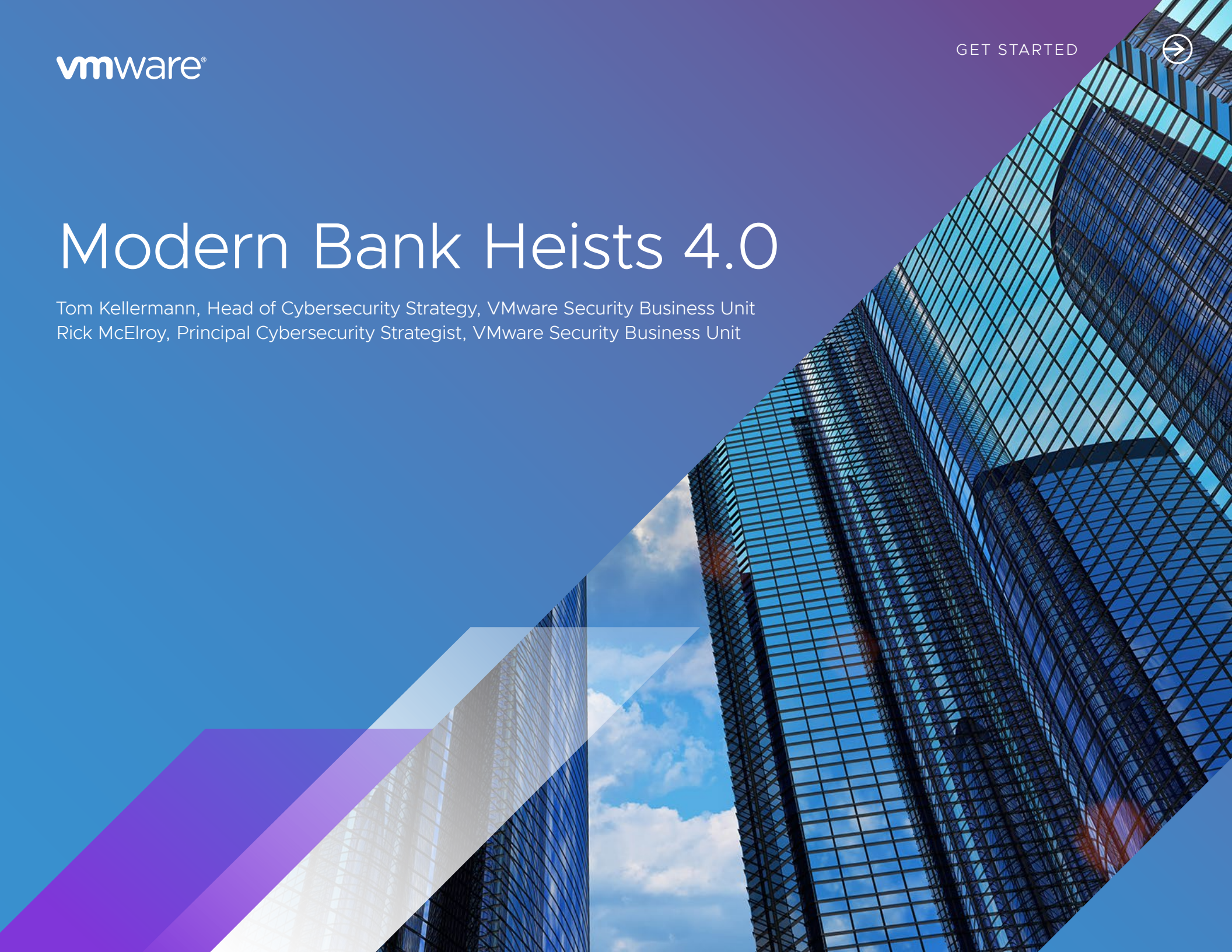
vmware

GET STARTED

Modern Bank Heists 4.0

Tom Kellermann, Head of Cybersecurity Strategy, VMware Security Business Unit
Rick McElroy, Principal Cybersecurity Strategist, VMware Security Business Unit



Executive Summary

This marks the fourth edition of the Modern Bank Heists report, which annually takes the pulse of some of the financial industry's top CISOs and security leaders. Thank you, again, for reading along, and thank you to the 126 security leaders who participated in this year's study. 48 percent of the financial institutions (FIs) are headquartered in North America, 28 percent are in Europe, 16 percent are in Asia and the Middle East, and 8 percent are based in Latin America.

We hope this report serves to provide a ground truth on the evolution of cybercriminal cartels and the defensive shift of the financial sector. In this year's report, CISOs revealed what they're seeing with attack prevalence and evolution. Our questions tackled topics including suspicious activity, counter incident response, island hopping, and integrity attacks. As evidenced by the findings, the bank heist has evolved significantly—from a heist to a hostage situation for financial institutions.

"Once again, this year's Modern Bank Heists report underscores the growing sophistication, tenacity and downright cruelty of the cybercriminal underworld. Throughout 2020, as the United States and our partners struggled to combat the COVID-19 pandemic, the world's most dangerous cybercriminals dramatically stepped up their criminal activities, redirecting their campaigns to target the most vulnerable groups in our community—the poor, the elderly, and the sick. Criminal groups launched a torrent of fraud scams, ransomware attacks, and phishing campaigns, all aimed at profiting off of the unprecedented fear and anxiety caused by a once in a lifetime public health emergency. Their actions over the past year only serve to highlight the continued urgency of forcefully investigating, prosecuting and ultimately convicting these truly reprehensible actors. The U.S. Secret Service stands ready to help ensure that these criminals are held to account."

- Jonah Force Hill, Cybersecurity Strategist, U.S. Secret Service

Headquarters of Financial Institutions Surveyed

North America
48%

Asia and Middle East
16%

Europe
28%

Latin America
8%

Key Report Findings

57% | **of surveyed financial institutions noted an increase of wire transfer fraud.**

54% | **of surveyed financial institutions experienced destructive attacks, a 118 percent increase from 2020.** These integrity attacks are burgeoning as counter incident response (IR) grows.

41% | **of surveyed financial institutions experienced an increase in brokerage account takeover.**

51% | **of surveyed financial institutions experienced attacks that targeted market strategies.** Cybercriminals have learned that the most valuable asset of a bank is nonpublic market information that can be used to facilitate digital insider trading and front running as observed by VMware cybersecurity strategists. Hacking a portfolio manager's laptop allows cybercriminals to become omniscient. This evolution of e-fraud was predicted in a World Bank report published in 2005.[1]

38% | **of surveyed financial institutions experienced an increase of island hopping,** an attack wherein an organization's information supply chain is commandeered to attack the institution from within its trusted supply chain. This represents a 13 percent increase from 2020. Cybercrime cartels have studied the interdependences of financial institutions and now understand which managed service provider (MSP) is used and who the outside general counsel is as observed by VMware cybersecurity strategists. In turn, these organizations are targeted and hacked to island hop into the bank.

41% | **of surveyed financial institutions observed the manipulation of time stamps.** Time is a fundamental element in both fintech and finance. Cybercriminals recognize they can evade detection by manipulating time. This calls for much more attention to be paid to securing the integrity of time because, if this trend continues, it could be used to alter the value of capital or trades.

1. World Bank Group. "Capital Markets and E-fraud Policy Note and Concept Paper for Future Study." May 2005.

Attack Prevalence and Sophistication

Today, financial institutions are facing a wave of custom-developed malware as well as the now prevalent fileless attack. 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.

VMware looked across our data repository with a specific focus on the financial sector (a vertical often battered by the worst the threat landscape has to offer), and found a clear change of malicious attachments and HTTP downloads between the last two weeks of January (see Figure 1) and the first two weeks of February (see Figure 4).

Note that these threats are very specific to our telemetry and are limited to the time span around the Emotet takedown operation. For a more general description of the most prevalent threats in the financial sector, see the *The 5 most prevalent threats in the finance sector* section.

Before Operation Ladybird, Emotet was definitely a major player in terms of observed downloads and attachments, followed by Hancitor, Qbot, Dridex and Valyria. With one caveat: It is often difficult to really understand the role of these threats as they often represent a vector for one another. For example, Valyria is a malicious Office document that is used to download other components, among which is Emotet itself. In other scenarios, Emotet was a conduit for Qbot. As a result, these threats often overlap and have different behaviors depending on the deployment context.

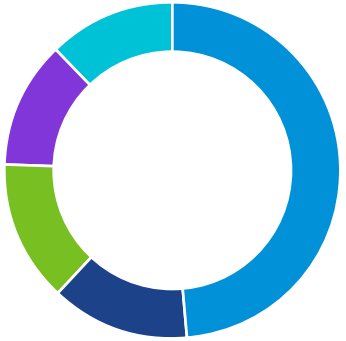


FIGURE 1: The top five malware families found in the last two weeks of January 2021.

Counter IR occurs 63 percent of the time, according to the surveyed financial institutions. Counter incident response highlights the escalation of the heist to a hostage situation. Based on the community of threat hunters who use VMware Carbon Black® EDR™, it manifests in nine ways:

1. Blocking events from hitting the security information and event management (SIEM) system
2. Disabling the Antimalware Scan Interface (AMSI) and other security tools
3. Clearing logs and the like
4. Manipulating time stamps
5. Using alternative authentication material, such as pass the hash/ticket
6. Using a signed binary proxy execution (e.g., LOLBins)
7. Using legit files to execute untrusted code
8. Deploying ransomware in a manner similar to NotPetya
9. Deploying wipers

The most visceral escalation of the modern bank heist is to leverage destructive attacks. Destructive attacks are launched punitively to destroy data and dismantle subnets. It is worth noting 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 as observed by VMware threat researchers and survey responses. Underground intelligence provider Intel 471 has observed destructive malware variants, such as ransomware and wipers, that have been leveraged against all industries, including the financial services industry.[2] Destructive malware variants seek to destroy, disrupt or degrade victim systems by taking actions, such as encrypting files, deleting data, destroying hard drives, terminating connections, or executing malicious code.

2. Intel 471. "Here's what happens after a business gets hit with ransomware." November 23, 2020.

Intel 471 has profiled threat actors and threat actor groups developing and offering these destructive malware variants on various underground forums, marketplaces, and messaging services for purchase by other financially motivated cybercriminals. Increasing in popularity since late 2019, Intel 471 has tracked the development and recruitment of ransomware-as-a-service (RaaS) variants that leverage affiliate programs to recruit other cybercriminals to deploy their custom ransomware variants and take a portion of the revenue generated by ransom payments. While ransomware has not historically been viewed as a destructive malware variant in comparison to other variants, such as wipers, they do pose considerable risk given the possibility of victims losing files or having files damaged if no backup is in place, or if decryption mechanisms render business-critical data lost or corrupted.

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."[3] It may have "worm-like features to propagate across a network by leveraging additional techniques like Valid Accounts, Credential Dumping, and Windows Admin Shares." This challenges us to become more clandestine in how we conduct IR and to increase our threat hunting exercises.

The five most prevalent threats in the finance sector

The financial sector is a high-priority target for cybercriminals looking for banking credentials and access to financial applications (such as bitcoin wallets) that can be monetized in a straightforward manner.

As it happens in many other domains, attacks are usually carried out using email as an initial vector for the execution of a trigger (usually the opening of an attachment or the clicking of a link) that activates a number of subsequent steps. This includes the downloading of additional malware components, attempts to achieve persistency, and the abuse of benign tools, such as PowerShell scripts or remote execution mechanisms, to spread laterally.

3. MITRE ATT&CK. "Data Destruction." March 27, 2020.

In our past telemetry, we have observed specific threats being particularly active in the network of our customers in the financial sectors. At the same time, we have been monitoring large-scale campaigns whose analysis has been made public.

These are the top five threats found from our threat intelligence sources:

1. Emotet – Emotet is a Trojan that mainly spreads through spam emails containing malicious macro-enabled documents or links. Emotet allows criminals to monetize attacks via information stealing, email harvesting, and ransomware distribution. Since its inception in 2014, this threat underwent a number of evolutionary steps until its network infrastructure was taken down at the beginning of 2021.

2. Dridex – Dridex is a banking Trojan that acts as a banking credential stealer, a ransomware delivering system, and a remote access control tool. This threat is often delivered through macro-enabled Office documents attached to emails.

3. Trickbot – Trickbot is a threat that targets the financial sector, providing modules that support the theft of banking credentials and cryptocurrency, as well as ransomware. This threat was the target of a takedown initiative in October 2020. Even though the threat infrastructure took a hit, the cybercriminal gang behind it recovered and restarted its activities.

4. Qbot – Qbot, also sometimes known as Qakbot, is a versatile threat that supports a number of modules (from remote access to credential theft). A notable technique recently used by this threat was to observe email threads and inject themselves in existing threads, increasing the chances that a user would deem the corresponding attachment as a legitimate one.

5. Hancitor – This less-known threat experienced a comeback at the beginning of 2021. This threat acts mostly as a delivery mechanism for a plethora of other threats, and it has often used DocuSign documents to entice the victim into activating the email's malicious attachments.

Island Hopping

38 percent of surveyed financial institutions stated they had encountered island hopping. This represents a 13 percent increase from 2020. CISOs were explicitly asked to exclude the SolarWinds campaign.

Island hopping: The four stratagems

Network-based island hopping is one of the most frequently used forms of island hopping. With network-based island hopping, attackers infiltrate one network and use it to hop onto an affiliate network. The SolarWinds attack is an example of this stratagem.

In **watering-hole attacks**, the adversary hijacks a website or mobile app used for e-finance by customers.

Reverse business email compromise (RBEC) attacks occur when a hacker successfully takes over a victim's Office 365 environment and executes fileless malware attacks against the C-suite of the financial institution and the board.

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

"Modern cybercriminals are collaborating at an unprecedented level, operating with stealth, sophistication, and ever-expanding revenue streams. Initial access brokerages are lowering the bar to entry, defense evasion tradecraft is commonplace, increasingly modular command and control frameworks, RaaS allowing for plug-and-play infection, and affiliate programs that actively reward individuals and partners for assisting in malware delivery," said Greg Foss, senior cybersecurity strategist, VMware Security Business Unit. "The industrialization of cybercrime has ignited a multitrillion-dollar industry, estimated to cost the world $6 trillion in the coming year and is expected to double by 2025. To get ahead of the threat, security leaders must understand their motivations, markets and goals. Financially motivated adversaries tend to share stolen data from breaches, both openly on marketplaces and in trusted circles, which can include email addresses and active credentials for employees. Proactively hunting for this data and correlating with asset discovery and continuous monitoring can help limit exposures via information that crimeware groups already know."

If you were impacted by an island hop attack, it is more than likely that they are moving laterally through your infrastructure. They want to commandeer an FI's digital transformation and use it to launch attacks against their customers.

75 percent of CISOs at financial institutions surveyed still report to CIOs. If we learned one thing from 2020, it's that the sustainability of telework is based in cybersecurity. CISOs should be promoted to the C-level. Of the 25 percent of CISOs surveyed who did not report to the CIO, the majority now report to the CEO.

39 percent of financial institutions stated that China posed the greatest concern followed by Russia (33 percent) and the U.S. (21 percent) underground.

Cybercriminals are evolving in both attack sophistication and organization. The financial sector is being targeted by cybercrime cartels and nation-states. Situational awareness is paramount. We must modify how we respond to these cartels and appreciate that the game has changed as mere wire transfer fraud is not their ultimate goal—rather, hijacking the digital transformation of an FI via island hopping is the new conspiracy.

Cybersecurity has become 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*.

82 percent of financial institutions surveyed plan to increase their budget by 10–20 percent. The majority of CISOs are working to address their contextual and app modernization gaps, and their investment priorities include:

1. Extended detection and response (XDR) (24 percent)

2. Threat intelligence (23 percent)

3. Workload security (21 percent)

4. Container security (18 percent)

48 percent of surveyed financial institutions conduct weekly threat hunts. Better telemetry has allowed almost half of all respondents to build hunt programs designed to disrupt, deceive and work with law enforcement around the globe to help fuel some of the largest cybercrime takedowns the world has seen.

Modern threat hunting programs have multiple outputs, and it isn't always about finding a cybercriminal. Rather, it's fueling threat intelligence. The Financial Services Information Sharing and Analysis Center (FS-ISAC) has a superior model for threat intelligence sharing that other industries can and should follow. Modern threat hunting as a best practice must be normalized.

Modern threat hunting programs are built to be proactive, contextually aware, and intelligence driven, with humans fueled by automation.

Proactive

Teams are maturing rapidly to respond to the ever-changing battlespace. Modern security teams are looking to close telemetry gaps as they hunt. It's not always about finding a cybercriminal; hunt teams are driving an enormous amount of change both at a process and technology level. Organizations with hunt teams have a better understanding of their environment and what needs to be addressed both tactically and strategically.

Contextually aware

New data sources are ingested and normalized on a regular basis, and where they aren't, they are pushing vendors to help close them. Teams have employed machine learning (ML) and AI to help determine what normal looks like. Endpoint detection and response (EDR) and network detection and response (NDR) are in use along with other sources for identity, applications and clouds.

Intelligence driven

Modern hunt teams are intelligence driven. Successful teams have automated the integration of threat intelligence into their hunt programs. Teams have started to focus on the data sets that are actually relevant to attack chains and have tailored their intelligence programs to their environments.

Humans fueled by automation

Threat hunting remains first and foremost a human-led endeavor and remains so. However, technology has substantially changed the way we hunt. Hunters are using a variety of techniques to analyze data and share those with others both inside and outside of organizations. Modern hunt teams are developing their own procedures on a regular basis and rapidly iterating to tune. These teams also automate procedures to drive better detection upstream from the hunt activity. They have employed data science and ML to help tune anomaly detection and are also employing automated red teaming and assessment technology to continually iterate.

Defending Against Modern Bank Heists: 8 Best Practices

Given the escalation to a virtual hostage situation, we must evolve how we respond to cybercrime cartels. Here are eight best practices for security teams:

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. Watch and wait. Do not immediately start blocking malware activity and shutting off access. Do not immediately terminate the command and control (C2) systems. 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.

3. 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. Ensure that you rename the agents to something innocuous.

4. Deploy honey tokens or deception grids, especially on attack paths that cannot be hardened.

5. Apply just-in-time administration.

6. Integrate your network detection and response with your endpoint protection platform.

7. Deploy workload security.

8. Conduct weekly threat hunting.

Conclusion

Cybercrime cartels are evolving in both attack sophistication and organization. The financial sector is being targeted by cybercrime cartels and nation-states. Situational awareness is paramount. The game has changed as mere wire transfer fraud is not their ultimate goal—rather, hijacking the digital transformation of an FI via island hopping is the new conspiracy. Cybersecurity has thus become a brand protection imperative. Trust and confidence in the safety and soundness in the financial sector will depend on it.

Read last year's report, *Modern Bank Heists 3.0*.

VMware January survey methodology

VMware conducted an online survey in January 2021 about evolving cybersecurity threats facing financial institutions. 126 CISOs and security leaders from around the world participated. Respondents were asked to select only one response per question. Due to rounding, percentages used in all questions may not add up to 100 percent.

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®

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