Modern Bank Heists 5.0

The Escalation: From Heist to Hijack, From Dwell to Destruction

Tom Kellermann
Head of Cybersecurity Strategy, VMware

Get Started

vmware

Foreword

Foreword by Jeremy Sheridan,
Assistant Director of the U.S. Secret Service

The Secret Service, in its investigative capacity to protect the nation's financial payment systems and financial infrastructure, has seen an evolution and increase in complex cyber-enabled fraud. There are a variety of reasons for the opportunities, motives, methods, and means related to criminal activity.

At the forefront is the swelling profitability of these crimes which, of course, motivates criminal actors. The persistent, inadequate security of systems connected to the internet provides opportunity and methodology. Finally, the proliferation of digital money payment systems has created a global, instantaneous, and pseudo-anonymous means to facilitate their actions.

All of these factors have facilitated the maturation of a cybercriminal ecosystem that has not been sufficiently suppressed. We see these trends continuing into the future and utilizing greater anonymizing techniques such as peer to peer networks, privacy coins, encrypted communications, and darknet marketplaces to further expand cybercrime capabilities and reach.

Executive Summary

This marks the fifth edition of the Modern Bank Heists report, which annually takes the pulse of the financial industry's top CISOs and security leaders to provide executives with a ground truth on the changing behavior of cybercriminal cartels and the defensive shift of the financial sector. In this year's report, 130 financial sector security leaders from around the world revealed the type of attacks they're currently seeing, what threats they're most concerned about, and how they're adjusting their security strategy and spend.

The findings of the Modern Bank Heists report reflect the massive impact that the events of the past year have had, and continue to have, on financial institutions around the world. Since last year's edition published, security has become a top-of-mind issue for business leaders amid rising geopolitical tension, an increase in destructive attacks utilizing wipers and Remote Access Tools (RATs), and a record-breaking year of Zero Day exploits. The U.S. kicked off international efforts with over 30 global partners to fight ransomware by addressing the financial systems and safe harbors that make ransomware profitable, and encouraging international law enforcement collaboration to disrupt the ransomware ecosystem[1]. U.S. private-public sector collaboration also made incredible strides with the Cybersecurity and Infrastructure Security Agency's (CISA) creation of the Joint Cyber Defense Collaborative (JCDC), of which VMware is a founding member.

This continued collaboration will be key to combatting the evolving threats detailed in this year's report. Financial institutions are being hit with multiple ransomware attacks as the security industry bands together to fight back against ransomware groups like DarkSide and Conti. Cybercrime cartels are targeting market strategies, taking over brokerage accounts, and island hopping into the banks. Attackers are moving from heist to hijack, from dwell to destruction.

Key Report Findings

of financial institutions experienced an increase in destructive attacks, a 17% increase from last year. Cybercriminals in the financial sector will typically leverage destructive attacks as an escalation to burn the evidence as part of a counter incident response.

2 out of 3 (66%) financial institutions experienced attacks that targeted market strategies. Modern market manipulation aligns with economic espionage and can be used to digitize insider trading.

experienced one or more ransomware attacks and 63% of those victims paid the ransom. Ransomware has a sinister relationship with Remote Access Tools (RATs) that help adversaries gain control of systems.

are concerned with the security of cryptocurrency exchanges. The advantage for cybercriminals of targeting cryptocurrency exchanges is that successful attacks can be immediately and directly turned into cyber cash.

of financial institutions experienced an increase in island hopping, a 58% increase from last year. We've entered a new era of conspiracy where hijacking the digital transformation of a financial institution via island hopping to attack its constituents has become the ultimate attack outcome.

The majority of financial institutions plan to increase their budget by 20-30% this year. Top investment priorities include extended detection and response (XDR), workload security, and mobile security.

A Path of Destruction

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. **63% of financial institutions experienced an increase in destructive attacks, a 17% increase from last year.**

It is worth noting that cybercriminals in the financial sector will typically leverage destructive attacks as an escalation to burn the evidence as part of a counter incident response. 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.

Geopolitical tension is metastasizing in cyberspace. **The majority of financial institutions stated that Russia posed the greatest concern.** In January 2022, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) issued an unprecedented advisory on imminent Russian cyberattack campaigns detailing the modus operandi of these groups[2].

On February 23, 2022, Russian cybercrime cartels unleashed Hermetic Wiper against critical infrastructure targets[3]. HermeticWiper is a destructive payload. This malware leverages legitimate EaseUS Partition Master drivers to access the disk which in turn targets the Master Boot Record (MBR) of the disk. During execution, the attacker targets privilege escalation before targeting the Domain Controller. The attacker will utilize Active Directory; WMI and SMB to move laterally, deploy and spread to additional hosts, before corrupting the system's master boot record and displaying a fake ransomware note.

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] Destructive techniques challenge cyber defenders to become more clandestine in how they conduct IR and increase threat hunting exercises.

63%

of financial institutions experienced an increase in destructive attacks, a 17 percent increase from last year.

The majority of financial institutions stated that Russia posed the greatest concern.

Modern Market Manipulation

Although **71% of financial institutions noted an increase of wire transfer fraud this year**, our report finds that cybercrime cartels have realized that the most significant asset of a financial institution is not wire transfers or the access to capital; it's nonpublic market information. This encompasses corporate information or strategies that can affect the share price of a company as soon as it becomes public, such as earnings estimates, public offerings, and significant transactions. **2 out of 3 (66%) financial institutions experienced attacks that targeted market strategies.** This threat aligns with economic espionage, and can be used to digitize insider trading and front-run the market. Front running is the illegal practice of purchasing a security based on advance nonpublic information regarding an expected large transaction. Of the financial leaders surveyed, **25% said market data is the primary target for cybercriminal attacks.**

In addition to targeting market strategies, cybercriminals also have their sights set on taking over brokerage accounts. Access to brokerage accounts and the intelligence they contain could drastically improve the accuracy of financial bets or allow bad actors to buy or sell securities at lower prices.

63% of financial institutions experienced an increase in brokerage account takeover, up from 41% last year. As detailed by the Financial Industry Regulatory Authority (FINRA), bad actors "may access a customer's brokerage account using compromised customer information or records, such as login credentials of a customer"[5]. With organizations moving quickly to implement network segmentation, attackers have pivoted to leveraging valid credentials to gain trusted access and move freely throughout a network.

In a sector that's entirely dependent on the accuracy of the clock, more attention must be paid to securing the integrity of time. **67% of financial institutions observed the manipulation of time stamps**, an attack called Chronos named after the god of time in Greek mythology. Notably, **44% of Chronos attacks noted in our report targeted market positions.** Time is a fundamental element in finance and Chronos attacks are flourishing. Defending the integrity of time is paramount in 2022 and beyond.

71%

of financial institutions noted an increase of wire transfer fraud.

67%

of financial institutions observed the manipulation of time stamps.

Ransomware and the Resurgence of RATS

Much of the general public understands the basic profile of a ransomware attack, following attacks like the one on Colonial Pipeline that caused a shortage of gas on the U.S. East Coast in May 2021. Attackers can choose amongst a well-funded ecosystem of readymade and available ransomware kits, use the kit to compromise a network, encrypt sensitive files within the network, and present a ransom note to the victim that asks for cryptocurrency in exchange for a decryption key that will unlock access to the files.

74% of financial sector security leaders experienced one or more ransomware attacks in the past year and 63% of those victims paid the ransom. Conti ransomware was the most prevalent in these attack campaigns. VMware TAU discovered the Conti ransomware family in July 2020[6].

Chainalysis has identified over $602 million worth of ransomware payments paid in 2021 – with the Conti ransomware gang accounting for $180 million – although the true total for 2021 is likely to be much higher[7]. In a six-month span last year, FinCEN said it identified approximately $5.2 billion in outgoing bitcoin transactions potentially tied to ransomware payments[8].

Global law enforcement agencies have taken significant actions aimed at civilizing cyberspace and curbing ransomware, including mitigating the money laundering associated with cybercrime, treating ransomware attacks on critical infrastructure as a national security issue, and banning ransomware payments as they represent modern-day terror financing. Under new reporting requirements, financial institutions must immediately notify law enforcement if they suspect a ransomware transaction has taken or is taking place. Additionally, President Biden's signing of the Cyber Incident Reporting Act requires owners and operators of critical infrastructure to report cyber incidents to the U.S. Department of Homeland Security (DHS) and CISA within 72 hours and ransomware payments within 24 hours[9]. To further the progress made in fighting ransomware, forfeiture laws must be modernized to disrupt the dark web economy of scale, and seized funds should be allocated toward improving cybersecurity across critical infrastructure.

74%

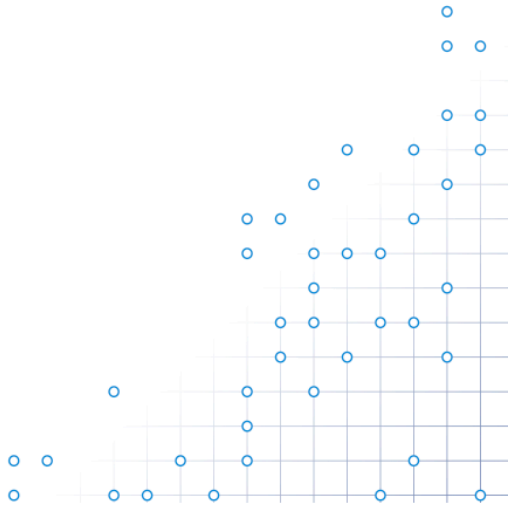
of financial sector security leaders experienced one or more ransomware attacks in the past year, and 63 percent of those victims paid the ransom.

A technical analysis provides a view into the proliferation of ransomware and how Remote Access Tools (RATs) help adversaries gain control of systems. 2022 is the year of the RAT given ransomware's sinister relationship with these tools. Remote control allows bad actors to persist within the environment, establishing a staging server that they can use to pivot and target additional systems.

A recent VMware Threat Analysis Unit report exposed just how agile attackers have become by weaponizing RATs in Linux-based environments in particular[10]. One of the primary implants used by attackers is Cobalt Strike, a commercial penetration testing and red team tool, and its recent variant of Linux-based Vermilion Strike. Since Cobalt Strike is such a ubiquitous threat on Windows, the expansion out to the Linux-based operating system demonstrates the desire of threat actors to use readily available tools that target as many platforms as possible.

"The additional threat by RATs such as Cobalt Strike is that they are developed by trustworthy businesses for legitimate usage," said Brian Baskin, manager of threat research at VMware. "They are often sold to vetted customers for the use of redteaming organizations to discover vulnerabilities for mitigation. However, as was seen with the Conti group leaks, criminal groups can bribe businesses to purchase a license on their behalf, giving the threat actors access to mature and powerful attack tools. Threat actors can then create their own malware, compatible with Cobalt Strike, to compromise Linux-based environments."

In a large-scale analysis of threat actors using RATs, VMware TAU discovered more than 14,000 active Cobalt Strike Team Servers on the Internet between February 2020 and November 2021. The total percentage of cracked and leaked Cobalt Strike customer IDs was 56%, meaning that of those observed, more than half of these Cobalt Strike users may be using Cobalt Strike illicitly or quite possibly for the purpose of cybercrime. The fact that RATs like Cobalt Strike and Vermilion Strike have become a commodity tool for cybercriminals poses a significant threat to enterprises.



"The advanced usage of RATs to deploy ransomware is a greater threat, even to larger organizations that have their own security operations," added Baskin. "While some threat actors rely upon simple and fast ransomware that is launched from email, such threats are easily identified and prevented with modern security controls. An actor leveraging sophisticated RATs to manually assess the environment, deploy custom payloads, and target specific systems for attack, can hide under the radar of many competent security teams until it is too late to stop."

Once an adversary has gained this beachhead using a RAT, they will need to find a way to monetize this limited access by relying on the victim's data to either monetize using ransomware for extortion, double extortion, and triple extortion, or monetize through stealing resources from cloud services using cryptojacking attacks.

Fast Facts: Ransomware Terms to Know

REvil – Originally known as "Sodinokibi" with the Linux version released in 2021

DarkSide – Initially used REvil but now created their own ransomware and is responsible for the Colonial Pipeline attack

BlackMatter – Evolution of DarkSide to distance themselves from the backlash created by the Colonial Pipeline attack

Conti – Ransomware group known for its ransomware-as-a-service (RaaS) structure

Defray – Also known as Defray777 and explicitly targets VMware ESXi™ virtual machines (VMs)

HelloKitty – Threat evolving from Windows to target Linux-based systems and ESXi servers

ViceSociety – Spinoff of HelloKitty, possibly from the same code base, and targeting SME businesses

Erebus – An old multilanguage threat targeting Linux-based systems

GonnaCry – Open source ransomware sample written in Python and C, with the C version actively used in the wild

eCh0raix – Ransomware targeting QNAP NAS devices and end users rather than businesses

Cracking Down on Crypto Exchanges

The advantage for cybercriminals of targeting cryptocurrency exchanges is that successful attacks can be immediately and directly turned into cyber cash. Cybercriminals get instant reward without the need to perform cumbersome scams using stolen information, such as personal data, or by having to interact with victims of ransomware. In the past decade, $2.6 billion USD has been stolen from cryptocurrency exchanges[11]. It is the digital version of a bank robbery.

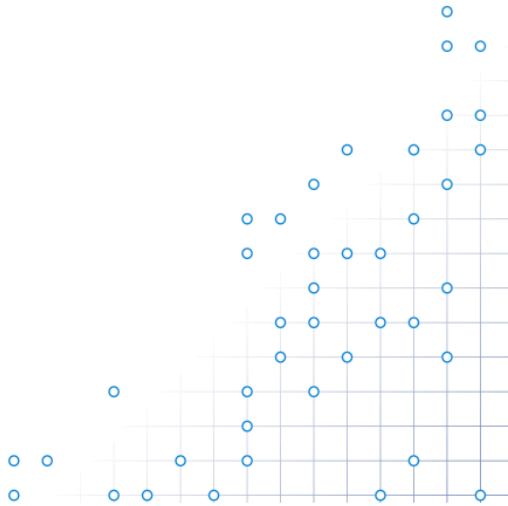
83% of respondents expressed concern over the security of cryptocurrency exchanges. While many cryptocurrency exchanges rely on blockchain for enhanced security, this technology will not stop cybercriminals from stealing funds if they gain access to a "hot wallet" that is connected to the internet. In December 2021, cybercriminals stole $196 million from Bitmart by accessing "hot wallets" on the cryptocurrency exchange[12]. Four months later in March 2022, cybercriminals successfully executed a social engineering attack on Axie Infinity and made off with $620 million worth of cryptocurrency in one of the largest cryptocurrency hacks on record[13]. The security posture of cryptocurrency exchanges must be improved to combat cybercrime.

"Cryptocurrencies are real currencies, but consumers often treat them as if they're not," said Rick McElroy, principal cybersecurity strategist at VMware. "People trust exchanges that are new to the game even though they aren't providing adequate protection to their currency or even their own admin accounts. In a crypto-based world, consumers should assume a certain level of responsibility in the protection of their cryptocurrency. There are no assurances that cybercriminals won't target the exchanges, the warm wallets or cold storage. Assume wherever the money is, there will also be criminals trying to steal it."

In addition to targeting wallets hosted on exchanges for quick cash, many cybercriminals prefer to use cryptocurrency exchanges and digital currencies for ransomware payouts because of their obvious ephemeral nature. This was evidenced by the ransomware attack against JBS USA which led to an $11 million ransom payment in Bitcoin using the Gemini cryptocurrency exchange[14]. However, governments are beginning to take action against these exchanges that facilitate financial transactions for ransomware attackers, as demonstrated with the landmark sanctions against the Suex

83%

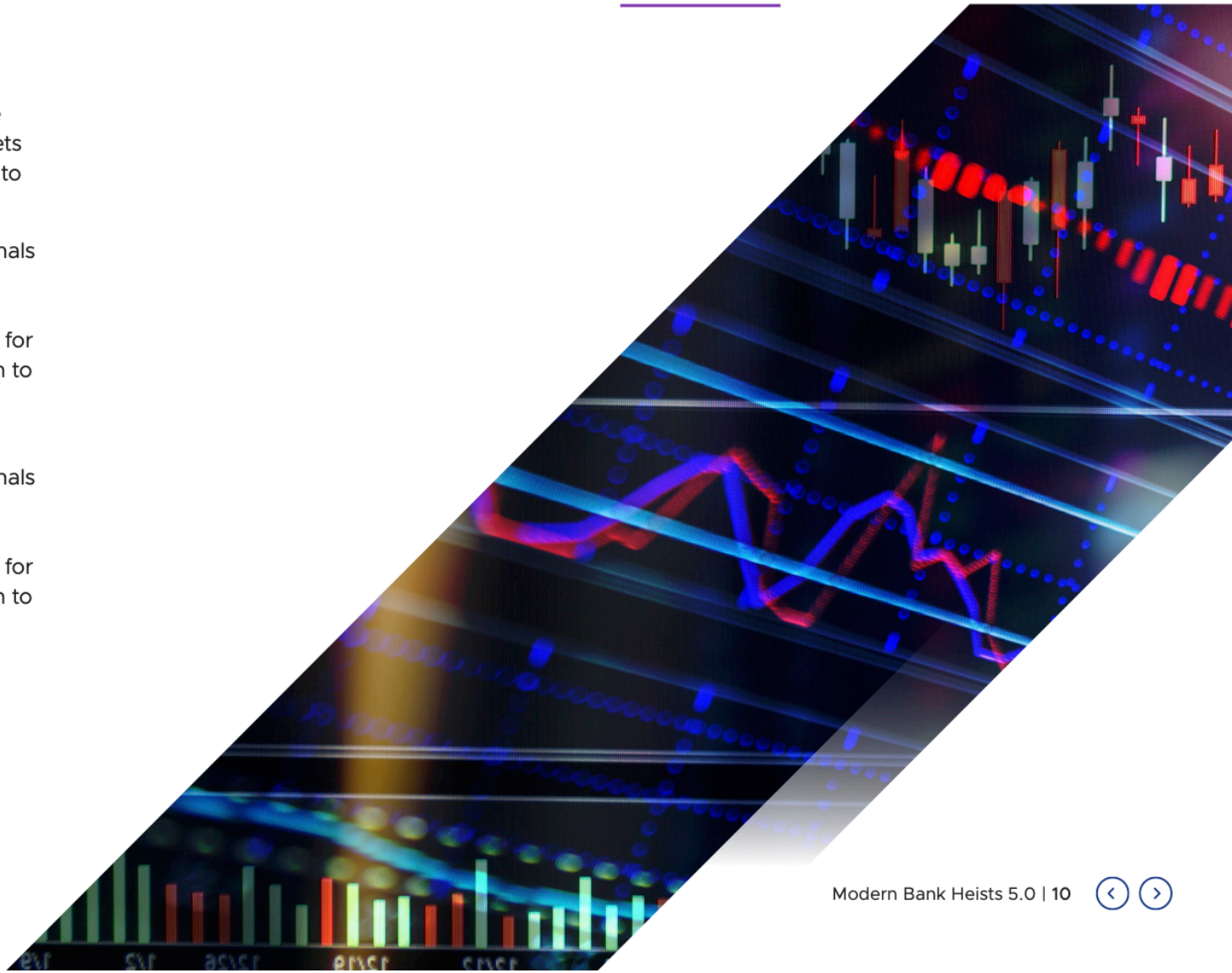
of respondents expressed concern over the security of cryptocurrency exchanges.



cryptocurrency exchange in September 2021. The executive order on Ensuring Responsible Development of Digital Assets that was issued by President Biden on March 9, 2022 helps to counter modern-day money laundering.

Without proper regulations, it has been easy for cybercriminals to cash in with nefarious exchanges and virtual currency fueling the surge in modern-day attacks, especially amid current geopolitical tensions. Eventually, the goal should be for any illicit funds seized under coordinated government action to be redeployed to help fund the protection of critical infrastructure from cyberattacks.

Without proper regulations, it has been easy for cybercriminals to cash in with nefarious exchanges and virtual currency fueling the surge in modern-day attacks, especially amid current geopolitical tensions. Eventually, the goal should be for any illicit funds seized under coordinated government action to be redeployed to help fund the protection of critical infrastructure from cyberattacks.



Island Hopping

The financial sector is being targeted by cybercrime cartels and nation-states that are evolving in both attack sophistication and organization. Cyber defenders must modify their response to these cartels and embrace situational awareness. These are not the bank heists of old, as mere wire transfer fraud is no longer the ultimate goal. We've entered a new era of conspiracy where hijacking the digital transformation of a financial institution via island hopping to attack its constituents has become the ultimate attack outcome.

60% of financial institutions experienced an increase in island hopping, a 58% increase from last year. 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 TAU. In turn, these organizations are targeted and hacked in order to island hop into the bank.

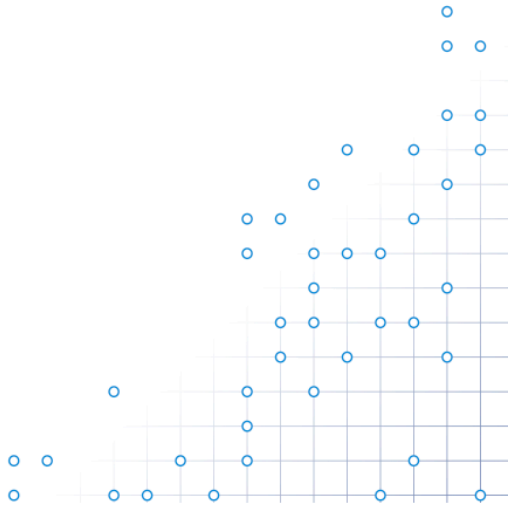
87% of financial institutions are concerned with the security posture of their shared service providers. Shared services providers, when compromised, pose a systemic risk to the financial sector as their infrastructure can be polluted to attack dozens of financial institutions at a time. This type of island hop is very concerning.

59% witnessed an increase in application attacks in 2021. Notably the top ten application attacks have evolved to include[15]:

1. Broken access control
2. Cryptographic failures
3. Injection
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-side request forgery

60%

of financial institutions experienced an increase in island hopping, a 58% increase from last year.



The 5 Stratagems of Island Hopping

API Attacks - APIs associated with FinTech are being targeted by cybercriminals due to their inherent accessibility and the reality that these APIs become a gateway to the FinTech platforms. 94% of financial security leaders experienced attacks on an API associated with FinTech. APIs have become the data plane—essentially the central nervous system—which carries critical information and data from one part of the application to another. In other words, APIs have become an essential and core component of modern applications. Thus, they make a perfect target for cybercrime cartels. As such, managing and securing modern applications cannot take place without managing and securing APIs.

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.

Watering-hole attacks take place when 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 using it to mask a hidden agenda of selling system access to targeted machines on the dark web.

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

API Security Best Practices:

1. Ensure API segmentation
2. Conduct an API assessment per vulnerability to OWASP10
3. Automate the discovery of API calls
4. Map communication patterns
5. Baseline normal patterns
6. Detect anomalous behaviors

The State of Play

80% of CISOs at financial institutions surveyed still report to CIOs. In this age of anywhere work and heightened security risks, we must provide CISOs with a direct line of access to the CEO and greater authority and resources. In CISA's Shields Up guidance, developed with input from security experts in the JCDC partnership of which VMware is a founding member, the need to empower CISOs is the top recommendation for corporate leaders and CEOs to better protect their organizations. As detailed in CISA's guidance, "In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term."

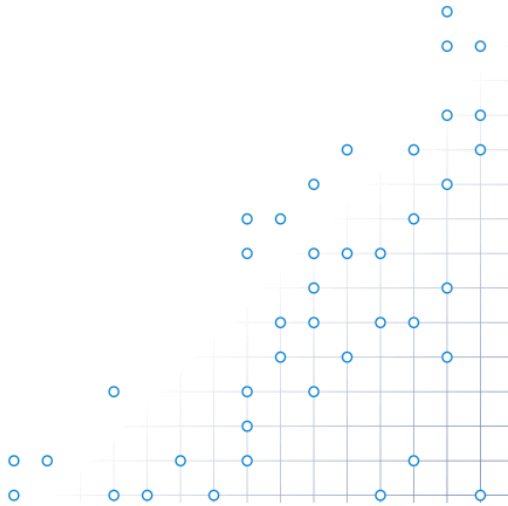
7 out of 10 financial institutions interviewed by VMware for this report are not spending more than 12% of the overall IT budget on security. **However, the majority of financial institutions plan to increase their budget by 20-30% this year.**

CISOs ranked their top security investment priority as:

1. XDR (24%)
2. Workload security (22%)
3. Mobile security (21%)
4. Threat intelligence (15%)
5. Managed detection and response (11%)
6. Container security (8%)

51% of financial institutions are conducting weekly threat hunts. The key difference between threat hunting and incident response is that threat hunting is proactive, whereas incident response is reactive. Threat hunting focuses on the pursuit of attacks and the evidence attackers leave behind.

Modern threat hunting on a weekly basis should be adopted as a best practice by security teams. Threat hunting programs have multiple outputs, and it isn't always about finding a cybercriminal – rather fueling threat intelligence. The Financial Services Information Sharing and Analysis Center (FS-ISAC) has a superior model for threat intelligence sharing.



Defending Against Modern Bank Heists: The Big 10

1 **Integrate your NDR with your EDR**

Detection and response technology employs real-time, continuous monitoring of systems to detect and investigate potential threats. A detection and response system then uses automation to contain and remove those threats.

2 **Apply micro-segmentation**

Limit an adversary's ability to move laterally within the organization. Forcing intruders to cross trust boundaries provides an improved opportunity for detection and prevention.

3 **Automate vulnerability management**

so security teams have improved risk-prioritization and can focus on vulnerabilities that are actually exploitable.

4 **Deploy decoys**

also known as deception technology, to divert the intruder.

5 **Activate application control in high enforcement**

to prevent unauthorized change and help stop malware, ransomware, Zero Day, and non-malware attacks.

6 **Deploy workload security**

to reduce the attack surface, increase visibility across environments, and secure workloads against emerging threats.

7 **Conduct weekly threat hunting**

Security teams should assume attackers have multiple avenues into their organization. Threat hunting on all devices can help security teams detect behavioral anomalies as adversaries can maintain clandestine persistence in an organization's system.

8 **Implement DevSecOps and API security**

to keep modern applications secure.

9 **Apply just-in-time administration**

to reduce the attack surface to only the times when privileges are actively being used.

10 **Ensure backups are viable and periodic**

to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack.

Cybersecurity has become a brand protection imperative. Trust and confidence in the safety of your institution depends on effectively avoiding, mitigating and responding to modern cyber threats. This report should serve as a starting point for a discussion between the cybersecurity community and the defenders of the financial sector on how best to collaborate.

Financial Security Leaders Voice Their Concerns

"At present, a network problem that I am concerned about is how to effectively avoid telecom fraud and fraud from network links."

"Continued API attack concerns. The end of 2021 was scary."

"We are most concerned about data leaking from the cloud, particularly with a high proportion of our company still working from home."

"Ransomware tops the list for us, having paid out a steep sum last year."

"Customer and client fraud. Social manipulation is hard to control and defend against."

"Cyberattacks on our records is a major concern."

"Account takeover fraud and phishing, both will lead to significant financial and reputational damage."

Sources

1. The White House Briefing Room, "Ongoing Public U.S. Efforts to Counter Ransomware," October 13, 2021.
2. Joint CISA-FBI-NSA Advisory, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," January 11, 2022.
3. VMware, "Hermetic Malware: Multi-component Threat Targeting Ukraine Organizations," March 4, 2022.
4. MITRE | ATT&CK, "Destruction Data," March 27, 2020.
5. VMware, "TAU Threat Discovery: Conti Ransomware," July 8, 2020.
6. FINRA, "FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud," September 17, 2020.
7. Chainalysis, "As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict," February 10, 2022.
8. The Record, "US Treasury said it tied $5.2 billion in BTC transactions to ransomware payments," October 15, 2021.
9. Congress.gov, "Strengthening American Cybersecurity Act of 2022," March 2, 2022.
10. CoinDesk, "Crypto Exchange BitMart Hacked With Losses Estimated at $196M," December 4, 2021.
11. CNET, "Axie Infinity's Ronin Network Loses Over $600M in One of the Largest Crypto Hacks on Record," March 31, 2022.
12. Confirm, "Live-Tracking BTC Ransom Paid by JBS to REvil Cyberattackers," June 28, 2021.
13. VMware, "Exposing Malware in Linux-Based Multi-Cloud Environments," February 9, 2022.
14. HedgewithCrypto, "Cryptocurrency Exchange Hacks," March 22, 2022.
15. Open Web Application Security Project, "OWASP Top Ten Application Security Risks 2021."

VMware Report Methodology

VMware conducted an online survey in February 2022 about evolving cybersecurity threats facing financial institutions. 130 financial sector CISOs and security leaders from around the world participated. 41 percent of the financial institutions (FIs) are headquartered in North America, 29 percent are in Europe, 16 percent in Asia-Pacific, 12 percent in Central and South America, and 2 percent in Africa. Respondents were asked to select only one response per question.

About VMware

VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control. As a trusted foundation to accelerate innovation, VMware software gives businesses the flexibility and choice they need to build the future. Headquartered in Palo Alto, California, VMware is committed to building a better future through the company's 2030 Agenda. For more information, please visit www.vmware.com/company.

This report may contain hyperlinks to non-VMware websites that are created and maintained by third parties who are solely responsible for the content on such websites.