IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

Modern Bank Heist: From Smash and Grab to Hostage Situation as Cyberthieves Evolve

Tom Kellerman

Tom Kellerman
Chief Cybersecurity Officer
WMware Carbon Black

Biography

Tom Kellerman is the Chief Cybersecurity Officer for VMware Carbon Black. Prior to joining VMware Carbon Black (https://www.carbonblack.com), Tom was the CEO and founder of Strategic Cyber Ventures. On 19 January 2017, Tom was appointed the Wilson Centre's Global Fellow for Cyber Policy in 2017.

Tom previously held the positions of Chief Cybersecurity Officer for Trend Micro; Vice President of Security for Core Security and Deputy CISO for the World Bank Treasury.

In 2008 Tom was appointed a commissioner on the Commission on Cyber Security for the 44th President of the United States. In 2003 he co-authored the Book "Electronic Safety and Soundness: Securing Finance in a New Age."

Kellerman believes, "In order to wage the counter-insurgency we must spin the chess board. The kill chain is obsolete – we must measure success of disruption of attacker behaviour. Understanding root cause is paramount. Combination of TTPs define intent. Cyber is all about context and intent/cognition."

Keywords Cybersecurity, Endpoint protection, Financial services, Cloud-native, Security, Cyberattacks
Paper type Research

Abstract

VMware Carbon Black has just published the third edition of its Modern Bank Heists report, which takes an annual pulse of some of the financial industry's top CISOs and security leaders. But as the author of this article explains, the report offers more than just data. WMware Carbon Black uses 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. The financial sector is not a new target for criminals, the bank heist has evolved significantly over the years – from stickups to cyberspace – but the fundamental motivation behind the attacks has remained the same: money.

Introduction

The financial sector is historically one of the most secure industries in the world. It needs to earn trust and convince customers that their hard-earned money is safe. Nevertheless, the fact that banks are guardians of the one thing cyber criminals typically desire most (money), means security teams are under relentless pressure. Attackers are prepared to invest time, resources and collaborate to develop new and more effective ways to reach the digital vault and make off with money. Our third *Modern Bank Heist* report[1] collected the views of 25 security


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

leaders and found that attackers are evolving and getting more sophisticated as they aim to secure long-term illicit access to banking systems – and they are capitalizing on the disruption of COVID-19 to help. So, what can we learn from the data revealed in the report, and how can we combat the emerging threats?

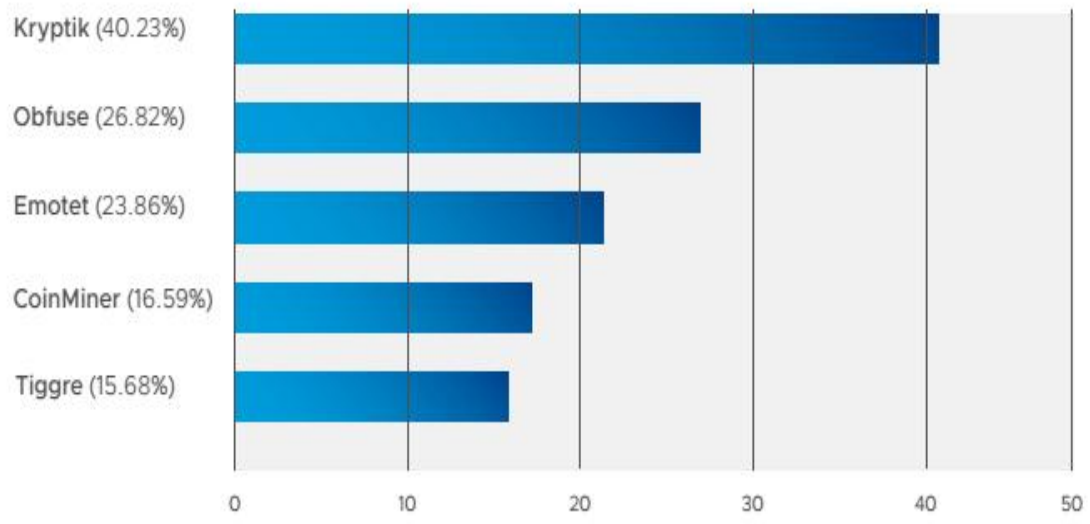
COVID-19 surge hits financial sector

Among the CISOs we surveyed, 80% said they had experienced an increase in cyberattacks over the past 12 months, up 13% compared with a year ago. Some of this is attributable to the COVID-19 surge – separate VMware Carbon Black data showed there has been an increase in attacks on finance sector targets of 238% from February to April 2020, and we saw ransomware attacks on the sector increase by a multiple of 9 during the same period. Closer analysis shows that notable alerts observed in VMware Carbon Black data spiked in correlation with significant moments in the COVID-19 news cycle, indicating that attackers are capitalizing on disruption to attack while the world looks the other way.

The majority (82%) of our CISOs noted an increase in attack sophistication over the past year, and the ways attacks are developing gives us a valuable insight into attacker behaviours that should inform our response. Overall, we are seeing attackers moving past inelegant “smash and grab” tactics, and towards more of a “hostage situation” where their motivation is to gain and retain footholds in target networks for long-term campaigns.

The Kryptik trojan and Emotet malware continue to feature among the top attack types experienced, our research has found (*see figure 1*), and these are often used in longer, complex campaigns aimed at leveraging native operating systems tools to remain undetected or gain a base to island hop to a larger and more lucrative target.

Figure 1: The most prevalent threats affecting the finance sector from March 2019 to February 2020



Source: Carbon Black, Modern Bank Heist 3.0


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Another indication that attackers are operating for the long-term is the fact that the most prevalent MITRE threat ID affecting the finance sector over the past year is T1507 – Process Discovery (comprising 64% of attacks). This shows attackers are investing in increasing their knowledge of policies and procedures in financial institutions, the better to work out how to infiltrate them undetected. They are also ramping up their awareness of incident response tactics and seeking blind spots that they can exploit to remain invisible.

Island hopping experienced by one third

Over 30% (33%) of the CISOs surveyed reported experiencing island hopping, where supply chains and partners have been unwitting vectors for attacks. The most common type of attack is network-to-network, but one fifth reported suffering watering hole type attacks, where hackers target a website frequently visited by customers of the target and attempt to gain access credentials, or the site of the financial institution itself to launch malware into visitors' browsers.

Island hopping-as-a-service is also on the rise. In 2019 our analysts uncovered a secondary component in a well-known cryptomining campaign that was designed to exfiltrate system access information that was destined for sale on the dark web. This is a significant change in behaviour that defenders need to keep on the radar as what looks like one type of attack may be cover for another.

"Virtual invasions" on the rise

Almost two thirds (64%) of those surveyed said that they had seen increased attempts at wire fraud transfer, up 17% compared with 2019. These attacks rely on attackers' knowledge of business process gaps in the verification process, or on direct social engineering of customers or customer service representatives.

Counter-incident response up as attackers evade detection

Almost a quarter (24%) of our surveyed CISOs had witnessed counter-incident response as attackers prioritize persistence and seek to retain their foothold in the financial institution's network. This is something we expect to see escalate in the coming year.

Tactics such as log deletion, manipulation of time stamps and disabling of security controls will all feature as attackers cover their tracks. Related to this are destructive wiper attacks designed to "burn the evidence" of infiltration and prevent defenders conducting forensic analysis to stop the same vectors being used in future. This has major implications for incident response: we need to get more clandestine.

Greg Foss, our Senior Threat Researcher at WMware Carbon Black has five tips for incident response to avoid alerting adversaries:

1. **Stand up a secondary line of secure communications** – This is vital to discuss the ongoing incident. Assume all internal communications are compromised and visible to the adversary.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

2. **Assume adversaries have multiple entry points** – Shutting off one entry point may not remove the attacker and may have the opposite effect by notifying the attacker you are aware of their presence.

3. **Watch and wait** – Don't immediately start blocking malware activity and access or terminating the C2. You need to monitor closely to assess the scope of the intrusion to work out exactly what to do to fully remove the adversary.

4. **Deploy agents in monitor-only mode** – If you begin blocking or otherwise impending activities, they will realize and change tactics, possibly leaving you in the dark.

5. **Deploy honey tokens or deception grids –** Particularly on attack paths that cannot be hardened.

In conclusion

The financial sector is facing a threat that evolves as fast as it can adapt. To combat the tactics adversaries are developing, we need to understand more about their behaviour. That means that kneejerk shutting down of attacks must be exchanged for a more clandestine and nuanced approach that allows us to learn, combined with our own collaborations across the cybersecurity and financial sector.

The digital vault is hostage to persistent, resilient attackers who have strategic plans for getting into and remaining in the network, so defenders need to think strategically too, if we are to stand a chance of mounting a successful counterinsurgency.

Reference

[1] https://www.carbonblack.com/resource/modern-bank-heists-3-0/