Carbon Black.

MAY 2018

Modern Bank Heists: Cyberattacks & Lateral Movement in the Financial Sector

40 CISOs of Major Financial Institutions Offer Perspective

Overview

The electronic finance revolution began in earnest in 1995, empowering institutional and retail clients with greater access to financial services and far lower transaction costs.

The advent of the internet and advances in wireless and satellite technologies have multiplied the possibilities for moving digital information. However, the use of these technologies is not without risk. These systems, which rely on computers and the internet, are often vulnerable to cyberattacks.

Cyberattacks against financial institutions are most often conducted for the purpose of yielding illicit financial gain. These attacks are typically undetectable, global, and instantaneous.

During the past three years, researchers have seen a tremendous amount of innovation from cybercriminals. Over the past six months specifically, the cybercriminal modus operandi has evolved. Cybercriminals are leveraging new techniques, tactics and procedures (TTPs) specific to maintaining persistence and countering incident response.

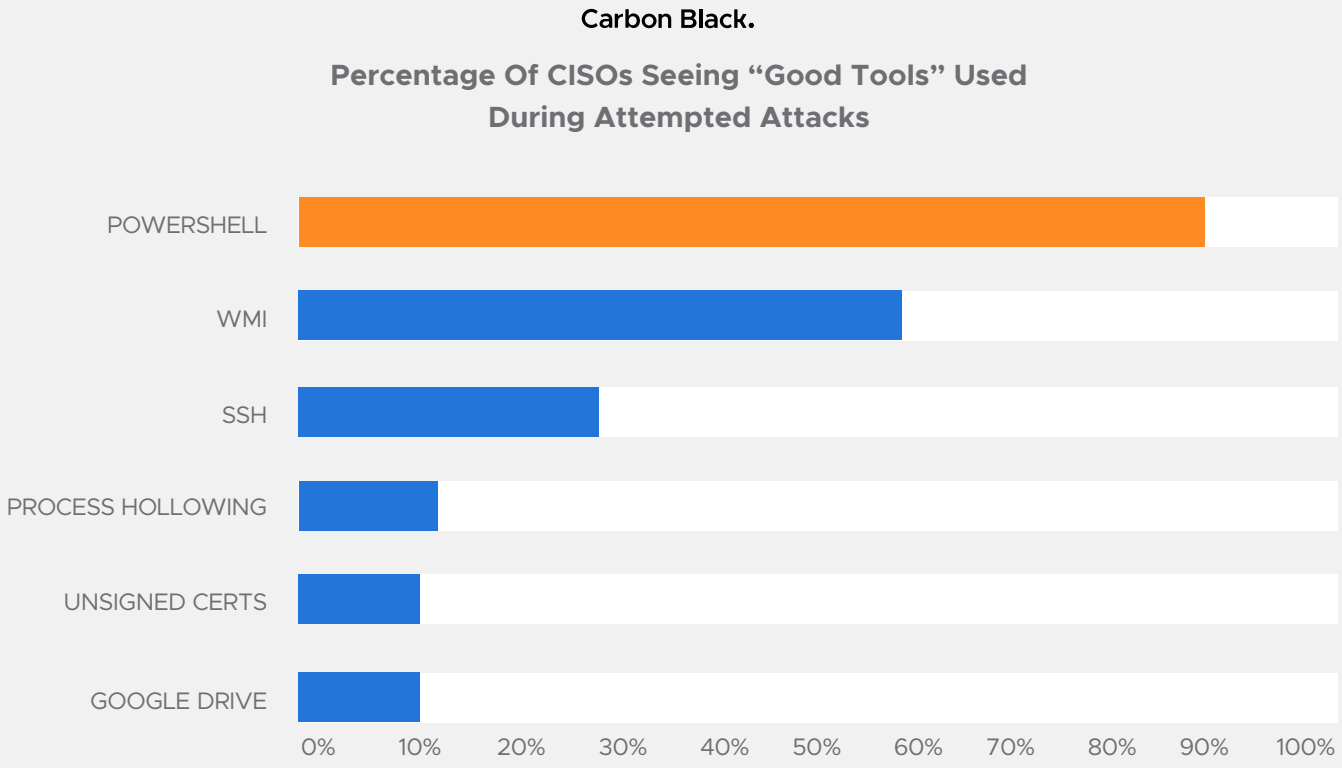
To better determine how cybercriminals are hiding behind invisibility cloaks to remain undetected, Carbon Black conducted a survey, comprising input from chief information security officers (CISOs) at 40 major financial institutions. The purpose of the survey is to improve telemetry for threat hunting teams and defenders.

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

Cybercriminals are leveraging new techniques, tactics and procedures (TTPs) specific to maintaining persistence and countering incident response.

Key Findings

Cybercriminals are continuing to hide in plain sight and move laterally leveraging non-malware attack methods. PowerShell (89%), Windows Management Instrumentation – WMI (59%) and Secure File Transfer Protocol – SSH (28%) were the top three "good tools" attackers leveraged nefariously to target financial institutions, according to our survey.



These "non-malware" (or fileless) attacks now account for more than 50% of successful breaches. With non-malware attacks, attackers use existing software, allowed applications and authorized protocols to carry out malicious activities. Non-malware attacks are capable of gaining control of computers without downloading any malicious files, hence the name. Non-malware attacks are also referred to as fileless, memory-based or "living-off-the-land" attacks.

With non-malware attacks, an attacker is able to infiltrate, take control and carry out objectives by taking advantage of vulnerable software that a typical end user would leverage on a day-to-day basis (think web browsers or Office-suite applications). Attackers will also use the successful exploit to gain access to native operating system tools (think PowerShell or Windows Management Instrumentation – WMI) or other applications that grant the attacker a level of execution freedom.

These native tools grant users exceptional rights and privileges to carry out the most basic commands across a network that lead to valuable data.

Non-malware attacks leverage a robust suite of tactics and techniques to penetrate systems and steal data without using malware at all. They have grown in prevalence in recent years as attackers have developed ways to launch these attacks at large scale.

A look at an example attack:

1. A user visits a website using Firefox, perhaps driven there from a cleverly disguised spam message.
2. On this page, Flash is loaded. Flash is a common attack vector due to its seemingly never-ending set of vulnerabilities.
3. Flash invokes PowerShell, an operating system (OS) tool that exists on every Windows machine, and feeds it instructions through the command line—all operating in memory.
4. PowerShell connects to a stealth command and control server, where it downloads a malicious PowerShell script that finds sensitive data and sends it to the attacker. This attack never downloads any malware.

Some leading attack campaigns have leveraged non-malware attack vectors to carry out nefarious actions. Almost every Carbon Black customer (97%) was targeted by a non-malware attack during each of the past two years. Their ubiquity is clear and growing.

There is a common theme why cybercriminals are increasingly leveraging non-malware attacks: they are following the path of least resistance. Financial institutions are not immune. The silver lining here is that awareness of malicious usage for tools such as PowerShell has never been higher. The fact that 90% of CISOs reported seeing an attempted attack leveraging PowerShell is a good thing. Not seeing such attempted attacks means the attacker has remained hidden.

90% of financial institutions reported being targeted by a ransomware attack during the past year. CryptoLocker. GoldenEye. Locky. WannaCry. 2017 was, perhaps, the most notorious year on record for ransomware. Even a casual news consumer can identify the menacing ransomware attacks that have cost worldwide businesses as much as $1 billion in 2017, according to FBI data. Financial institutions are clearly not immune. The overwhelming majority of CISOs in our survey reported seeing some kind of attempted ransomware attack during the past year.

of Financial Institutions Reported Being Targeted by a Ransomware Attack in 2017

Carbon Black.

This is not surprising. Last year, Carbon Black researchers monitored 21 of the largest dark web marketplaces for new, virtual offerings related to ransomware. Our research found a **2,502% increase** in the sale of ransomware on the dark web. This increase is largely due to a simple economic principle – supply and demand. Cybercriminals are increasingly seeing opportunities to enter the market and looking to make a quick buck via one of the many ransomware offerings available via illicit economies. In addition, a basic appeal of ransomware is simple: it's turnkey. Unlike many other forms of cyberattacks, ransomware can be quickly and brainlessly deployed with a high probability of profit. In our **previous report**, we found more than 6,300 estimated dark web marketplaces selling ransomware, with more than 45,000 current listings.

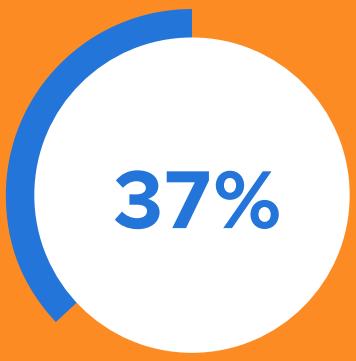
For ransomware authors, successful creation and selling of ransomware offerings appears to be fruitful. Based on our research, **some ransomware sellers are making more than $100,000 per year simply retailing ransomware**. In some instances, this is double the salary for legitimate software developers, who pull in an average of $69,000 a year, according to PayScale.com. (In Eastern Europe developer salaries are a bit lower, hovering around $45,000.)

That being said, the true untouchable hackers are becoming punitive. **Several survey respondents (1 in 10) reported encountering destructive attacks unrelated to ransomware.** The "bank heist" is becoming a hostage situation. We will continue to track this trend in future reports.

Only 37% of financial organizations have established threat hunting teams.

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.

Threat hunting aims to find abnormal activity on servers and endpoints that may be signs of compromise, intrusion or exfiltration of data. Though the concept of threat hunting isn't new, for many organizations the very idea of threat hunting is.



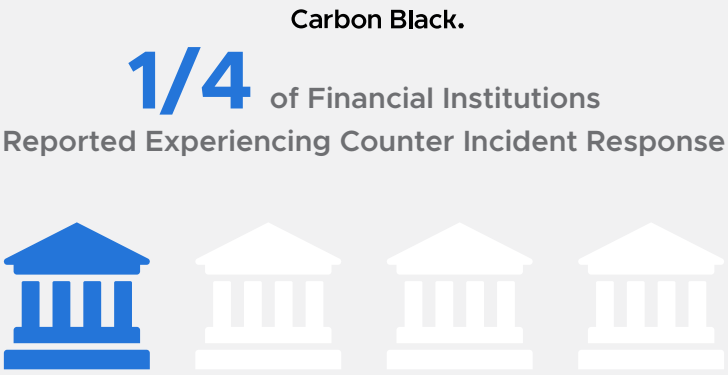
of Financial Institutions Have Established Threat Hunting Teams

Carbon Black.

The common mindset regarding intrusions is to simply wait until you know they're there. Typically, though, this approach means that an organization will be waiting an **average of 220 days** between the intrusion and the first time they hear about it. And even then, it's typically an external party such as law enforcement or a credit card company that's telling you.

With threat hunting, defenders are deployed to go out and "find the bad" versus waiting for technology to alert you. Successful threat hunting teams proactively chase down signs that intruders are present or were present in the recent past. They look for anomalies – things that don't usually happen.

1 in 4 financial institution CISOs reported experiencing counter incident response. This figure is concerning. It means cybercriminals are increasingly reacting and adapting to defenders' response efforts. Cybercriminals realize there are humans on the other end actively countering their techniques. They realize that teams are, in some cases, instrumented to detect and respond to their activities. They also realize that teams have specific IR playbooks for these types of scenarios.



Attackers are able to go off their scripts while defenders are sticking to manual and automated playbooks. These playbooks are generally based off simple indicators of compromise (IoCs). As a result, security teams are often left thinking they have disrupted the attacker, but with counter incident response, attackers maintain the upper hand. **This problem is compounded with secondary command and control (C2) present in several victims (1 in 10, according to our survey).** We forecast this will become a more prevalent tactical shift in the coming months.

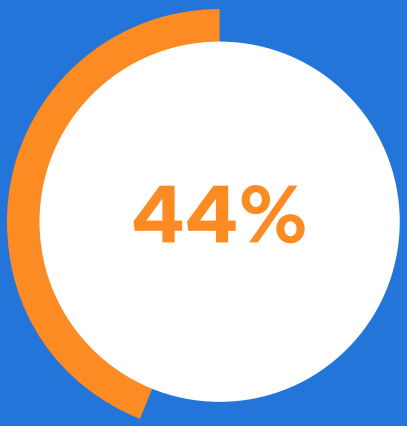
As SOC and IR teams begin to react, attackers are doing a number of things to counter the defenders.

- Changing code to evade new technology
- Targeting security analysts and engineers in separate but coordinated attacks
- Deleting logs from endpoints to hide nefarious behavior
- Executing DDoS attacks on applications and systems critical for defenders and/or the business

Cyber defense is evolving into a high-stakes game of digital chess where opponents are responding to every move made on the board. Teams should be prepared to throw out the IR playbook when necessary.

Nearly half (44%) of financial institution CISOs said they are concerned with the security posture of their Technology Service Providers (TSPs). These TSPs are regularly targeted by cybercriminals. As evidenced by the **FDIC's own inspector general**: "The FDIC's oversight process used for identifying, monitoring, and prioritizing TSPs for examination coverage needs improvement." Island hopping via information supply chains is growing. Our recommendation is for threat hunt teams and defenders to closely assess TSP security posture.

Given that 63% of financial institutions have yet to establish threat hunting teams, there should be concern regarding limited visibility into exposure created by TSPs. Cyberspace is fluid and exposure may become systemic.

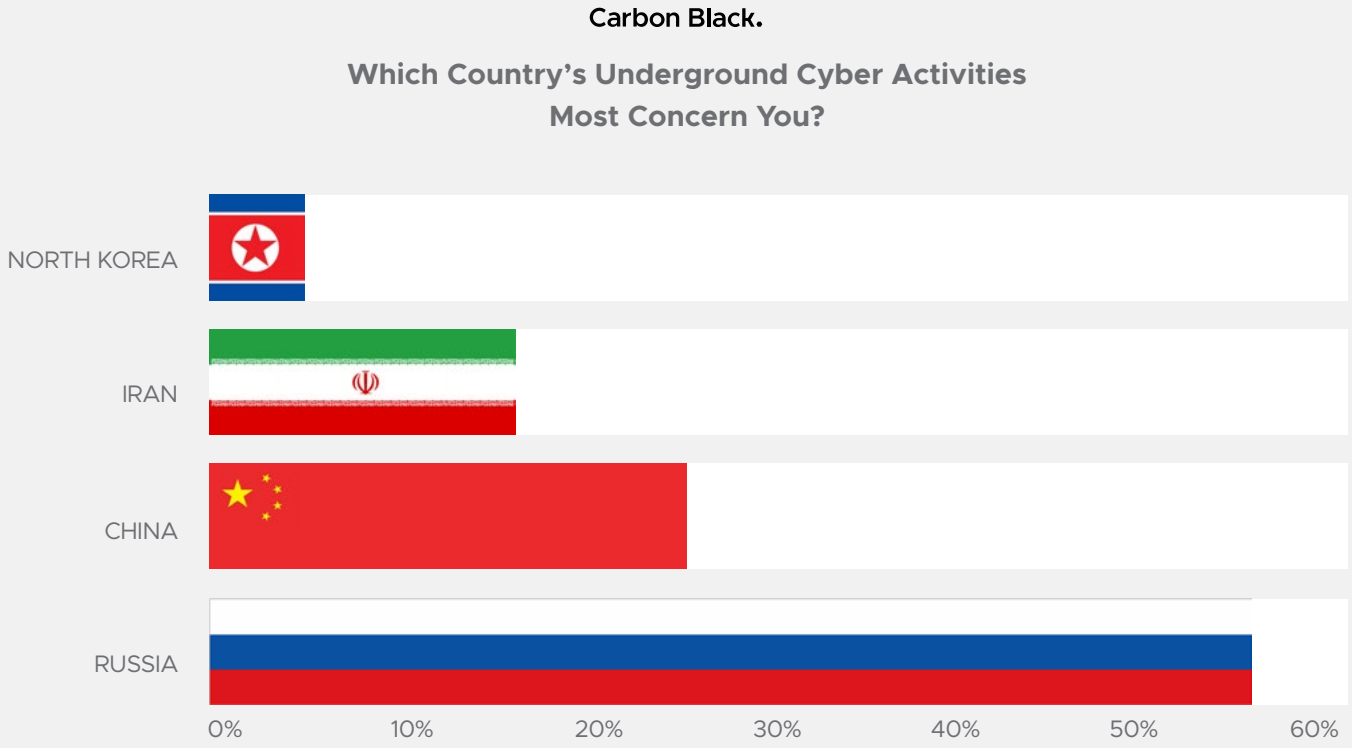


of Financial Institution CISOs Said They Are Concerned with the Security Posture of Their Technology Service Providers

Carbon Black.

Russia (59%), China (23%) and North Korea (16%) are the most concerning nation-state actors associated with cyberattacks, according to financial institution CISOs in our survey. Geopolitical tension serves as a harbinger for cyberattacks. There's perhaps no surprise with the results to this question with Russia leading the way, given the country's continued efforts to attack and influence the West, including the United States' 2016 presidential election.

The "Silicon Valley of the Dark Web" lies in St. Petersburg, Russia. Russian cybercriminals have demonstrated advanced sophistication among hacking groups. Russia's motivation for targeting financial institutions appears to go beyond financial gain or countering economic sanctions. Since 2014, many of the best cybercriminals have acted patriotically on accession to support Russia's strategic goals. Corporate espionage, sensitive data, trade secrets and personal information for executives, partners and customers all seem to be in play when it comes to Russia's cyberattack efforts.



Recommendations

Given these trends, modernizing defense in depth is imperative to preserve a high-functioning cybersecurity posture. The technological dependency of financial institutions to internet-based platforms has dramatically increased the industry's exposure to reputation, market and operational risks. The major gaps for many of these institutions revolve around visibility and time to detection. This is particularly troubling as it pertains to deterring an attacker's ability to move laterally within an enterprise post breach.

Financial institutions should aim to improve situational awareness and visibility into the more advanced attacker movements post breach. This must be accompanied with a tactical paradigm shift from prevention to detection. The increasing attack surface, coupled with the utilization of advanced tactics, has allowed attackers to become invisible. Decreasing dwell time is the true return on investment for any cybersecurity program.

Data Required to Curb Attacker Lateral Movement

Financial Institutions must have five sets of data specific to lateral movement in order to close the gap and reduce risk through rapid detection/response (this begins and ends on the endpoint):

1. High-fidelity telemetry to discern when adversaries are active in the network and on devices.
2. Correlated lateral movement telemetry with other sensors, such as egress monitoring.
3. Developing a comprehensive near-real-time "sight picture" of attacker behavior specific to internal movement and external command and control channels.
4. Rapid acquisition and automated analysis of attacker tools (and indicators of compromise), which can be vetted and communicated to existing control mechanisms through integrated workflows for automated response and defense.
5. Deploying predictive analytics to anticipate cybercriminals' movements.

Embracing intrusion suppression will allow an organization to thwart the burgeoning digital invasion. Intrusion suppression is a cybersecurity concept wherein the lateral movement of an attacker is detected in real time and the adversary's "kill chain" is disrupted and subsequently contained.

It is imperative we reevaluate vendor relationships and institute increased safeguards and oversight as information supply chain risk is here to stay. Cybersecurity investment mitigates third-party risk. Those companies who embrace brand protection as a function of comparative advantage will prevail.

Survey Methodology

In order to better determine how cybercriminals are hiding behind invisibility cloaks to remain undetected, Carbon Black conducted a survey, comprising input from CISOs of 40 major financial institutions in April 2018. Answers and CISO names were kept anonymous. In the survey, CISOs revealed trends they are seeing in lateral movement, counter incident response, integrity attacks and the most concerning threat actors their organizations continue to face.

Upcoming Research

In the coming months, Carbon Black will be working with some of the leading incident response (IR) firms in the world to determine attack trends and latest threats revealed during response engagements. If you are interested in contributing to this research, please reach out to **rmurphy@carbonblack.com**.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 33 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus.

For more information, please visit **carbonblack.com** or follow us on Twitter at @CarbonBlack_Inc.

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com