Financial Services

SECTOR RANSOMWARE SPOTLIGHTS

Investigative Cybercrime Series

A Collaboration Between

Arete

Cyentia INSTITUTE

Table of Contents

Introduction

Ransomware has continuously evolved since it first arrived on the scene in 1989. Over the past 34 years, researchers have explored the rise of ransomware fueled by its ease of distribution, shortened path to monetization, and the parallel growth of cryptocurrency.

In the first two volumes of the Investigative Cybercrime Series, we leveraged data from Arete ransomware engagements to analyze trends in cyberattacks, ransom payments, and effective controls across multiple sectors.

In this report, we will dive deeper into the financial services sector, which represents 4.7% of all events in our observation period—from May 2019 through May 2022. This data led us to explore trends in ransomware families, controls, and mitigation techniques.

The Investigative Cybercrime Series is an ongoing research effort to unmask insidious cyber threats and lessen their impact on insurers and the organizations they cover.

The data for this research comes directly from security incidents investigated by Arete and the intelligence operations supporting those investigations.

Financial Sector Ransomware Highlights

Every sector has been affected by ransomware, and financial services is no exception. The highly valuable and highlysensitive transactions core to this industry make a ransomware outbreak a potentially disastrous scenario. We offer this sector-specific analysis along with actionable insights to better equip defenders as they protect against the rising risk of ransomware attacks.

WHERE DOES FINANCIAL SERVICES STAND RELATIVE TO OTHER INDUSTRIES ON KEY RANSOMWARE STATISTICS?

When examining the chart below, follow the pink line that notes the position of the financial sector when it comes to frequency of attacks, typical demand, typical payment, and payment likelihood.

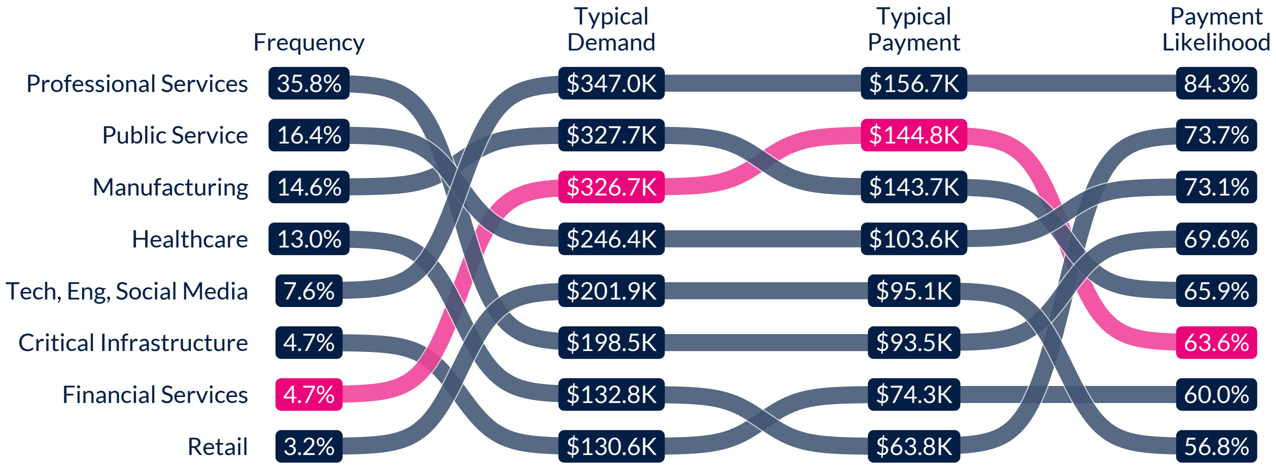

Figure 1—Sector's important values compared to others

KEY TAKEAWAYS

As Figure 1 illustrates, financial services ranks toward the bottom of all sectors when it comes to the frequency of ransomware attacks. Financial firms represented 4.7% of Arete's ransomware caseload, compared to professional services, which holds the top spot with 35.8%.

Following the pink line, we also can see that financial services rises towards the upper end of the spectrum for the typical demand ($326.7K) and even higher for the typical payment ($144.8K). We see it drop back down though, when it comes to the likelihood of paying ransoms, with 63.6%.

Typical Demands and Payments

Table 1 offers more insight into these data points. Note that the "typical" number is the geometric mean, which is what we have used in the ranking graphic in Figure 1. Table 1 also notes two additional values—average and extreme. Due to the wide range of demands within the financial services sector, the average here is skewed by a few very large demands. The "extreme" category represents the 95th percentile, which highlights the largest ransoms demanded. With all three of these values, we can create a more accurate picture of what is truly being demanded and paid.

You can also compare these values to the overall trends in Table 1 in Volume 1 on page 8.

	Typical	Average	Extreme
Demands	$326.7K	$3.0M	$9.0M
Payments	$144.8K	$1.6M	$2.3M

Table 1—Sector's summary of demands and payments

KEY TAKEAWAYS

Notably, extreme demands within financial services are among the highest of any sector—three times what we see in healthcare, for example. Extreme payments are nearly 16 times the size of typical payments, but financial firms paid less than half (44.32%) of typical ransom demands and 25.56% of extreme demands.

Controls that Reduce Payments

As the prevalence of ransomware continues to rise, many organizations work to put controls in place so that if a compromise occurs, the impact will be mitigated. These controls, including backups, multi-factor authentication (MFA), and endpoint detection and response (EDR), can all play a role in helping keep your organization safe.

Our data demonstrates that utilizing these controls affects the typical percentage of demand paid ("percent paid" in Table 2) and payment likelihood.

	Adoption Rate	Percent Paid	Payment Likelihood
Overall			
		38.7%	70.0%
Financial Services			
Multi-factor authentication	33.3%	20.0%	62.5%
Performing backups	55.9%	37.4%	66.7%
Proven recovery	29.6%	20.0%	33.3%
Endpoint detection & response	31.4%	12.5%	54.5%

Table 2—Comparing values for sector when a given control is in place

KEY TAKEAWAYS

One in three organizations in the financial services sector has MFA in place, while over half (55.9%) report performing regular backups.

Interestingly, just having an EDR platform is one of the more effective ways to decrease the payment likelihood in the financial sector. While only 33.3% of financial services organizations in our data set report having MFA in place, those that do typically pay just 20% of the demanded ransom and have a 62.5% likelihood of paying. Just under 30% demonstrated the ability to recover, and those that do typically pay only 20% of the demanded ransom and have a 33.3% likelihood of paying. Surprisingly, while over half the financial services firms in our data set performed backups, those that did typically paid 37.4% of the demanded ransom and were 66.7% likely to pay.

Having multiple controls in place will allow your organization to leverage the most negotiating power.

Our data shows having an EDR platform in place results in stronger protection and a reduced likelihood of paying a ransom. The implementation of an EDR platform can be used to help evaluate potential risk.

This data indicates that having multiple controls in place will allow an organization to leverage the most negotiating power when it comes to a ransomware incident. Just performing backups isn't enough to thwart attackers and lower payments.

Top Ransomware Families in Financial Services

With the proliferation of ransomware-as-a-service (RaaS) operations, we are seeing an increase not only in ransomware families but also in the number of “family members” within each family. We explored this development in more detail in Volume 2 of the Investigative Cybercrime Series, Reining in Ransomware.

Suffice it to say, ransomware families can be extremely volatile, changing names and shifting operations often. Due to increasing government investigations, key operators of many of these ransomware families have been arrested. However, that doesn’t diminish the threat of ransomware as a whole or the potential for new families to be created.

In Figure 2, we look at the top five ransomware families that impacted the financial services sector since 2019. The figure is color-coded according to the families’ current state of activity:

DARK BLUE	**LIGHT BLUE**	**PINK**
INACTIVE	STEADY OR DECLINING ACTIVITY	TRENDING UP

You can also compare this industry-specific figure to the overall trend, featured in Figure 2 in Volume 2.

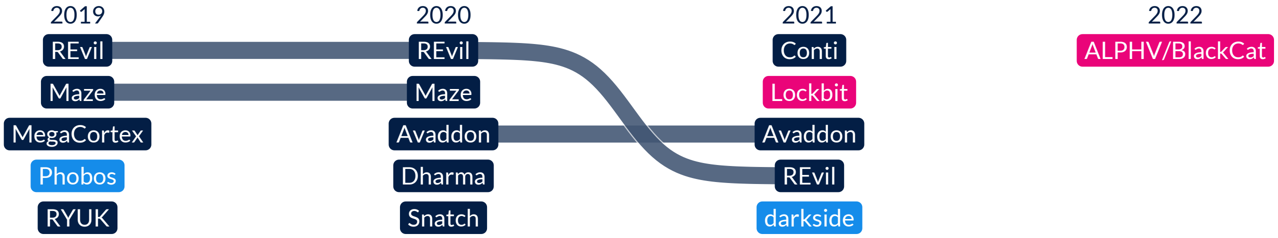

Figure 2—Most prevalent ransomware families observed in financial services incidents

KEY TAKEAWAYS

Figure 2 demonstrates an influx of new ransomware families that have arrived on the scene. The first thing that jumps out is how no family managed to stay in the top five for the entire period, but that didn’t stop them from making their presence felt.

When REvil was discovered in 2019, it was noted to be an evolution of GandCrab ransomware. In 2020, REvil launched a few high-profile attacks, including one on the law firm Grubman Shire Meiselas & Sacks that represented then–U.S. President Donald Trump, Lady Gaga, and Madonna.

> Just because a ransomware family exists one day does not mean that it will exist with the same name or operate under the same capacity the next day.

In July 2021, REvil returned to the public eye by exploiting zero-day vulnerabilities in Kaseya. Shortly after the media hype around Kaseya, REvil quietly disappeared, and their websites were taken offline. LockBit, on the other hand, was gaining traction, while Conti has become inactive over the past year. Instead, many of Conti’s members are suspected to have found homes with other ransomware groups.

ALPHV/BlackCat, one rising family of ransomware targeting the financial services industry, is known to be a haven for ex-Conti members. BlackCat is widely thought to be the first professional ransomware group that writes its code in the Rust programming language, allowing criminals the ability to easily change the code to fit their current needs. Most concerning for data-rich financial firms, the criminals using BlackCat have shown a propensity for releasing stolen data publicly.

Ransomware Techniques & Mitigations

The methods and mitigations presented in this section are based on the MITRE ATT&CK framework. This is done partly because ATT&CK is quickly becoming the common language of threat tactics and techniques used across the cybersecurity industry. Another benefit of using ATT&CK is that it enables readers to easily find definitions and examples of each technique referenced and explore a wealth of information on associated threat groups, malicious software, mitigations, attack simulations, etc.

INITIAL ACCESS METHODS

During a ransomware investigation, Arete's incident response team takes special care to, determine the initial access technique. Everything that happens afterward relies on attackers successfully introducing malware into the victim's environment, and preventing that from happening in the first place is the best way to keep your business protected. Understanding common infection vectors can help organizations focus their preventive strategies.

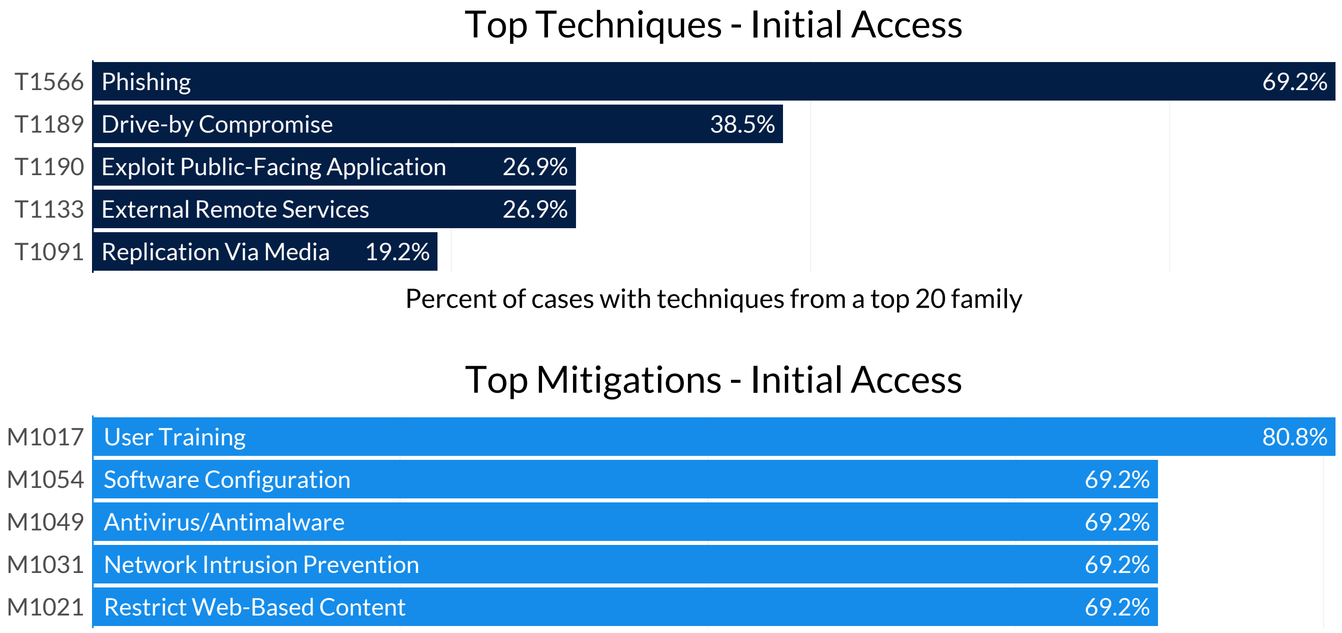

Figure 3—Sector's top initial access techniques and mitigations

Observed in 69.2% of cases, phishing is the most common way ransomware is initially introduced into financial services organizations. The second-ranked technique at 38.5% of cases, drive-by compromise, also employs deception to embed malware into web pages that are likely to be visited by users. Other top techniques for initial access, including exploiting public-facing applications, external remote services, and replication via media were utilized less frequently in 19.2 to 26.9% of cases.

The top variant impacting financial services changes from year to year, but what has not changed is that phishing is the most common way that ransomware initially finds its way into these organizations.

The second part of Figure 3 shows the recommended practices based on ATT&CK mitigations associated with the initial access capabilities exhibited by the top malware families. The percentages are based on the proportion of incidents potentially thwarted by each practice.

User training, specifically around common social engineering schemes, and promoting norms of healthy skepticism may have helped in more than 80% of these cases. The four-way tie for second place demonstrates the importance of software configuration, antivirus/antimalware, network intrusion prevention, and restricting web-based content. Note that each of these defensive measures can neutralize ransomware despite the opening of a dangerous link or attachment.

MID-EVENT TACTICS

What happens when malicious users have access to your systems? At the tactical level, these users utilize techniques to maintain persistence in the victim's environment, escalate privileges to gain more access, discover additional target systems and data, move laterally across the internal network, evade security defenses, establish command and control channels, collect and encrypt data, and other costly impacts.

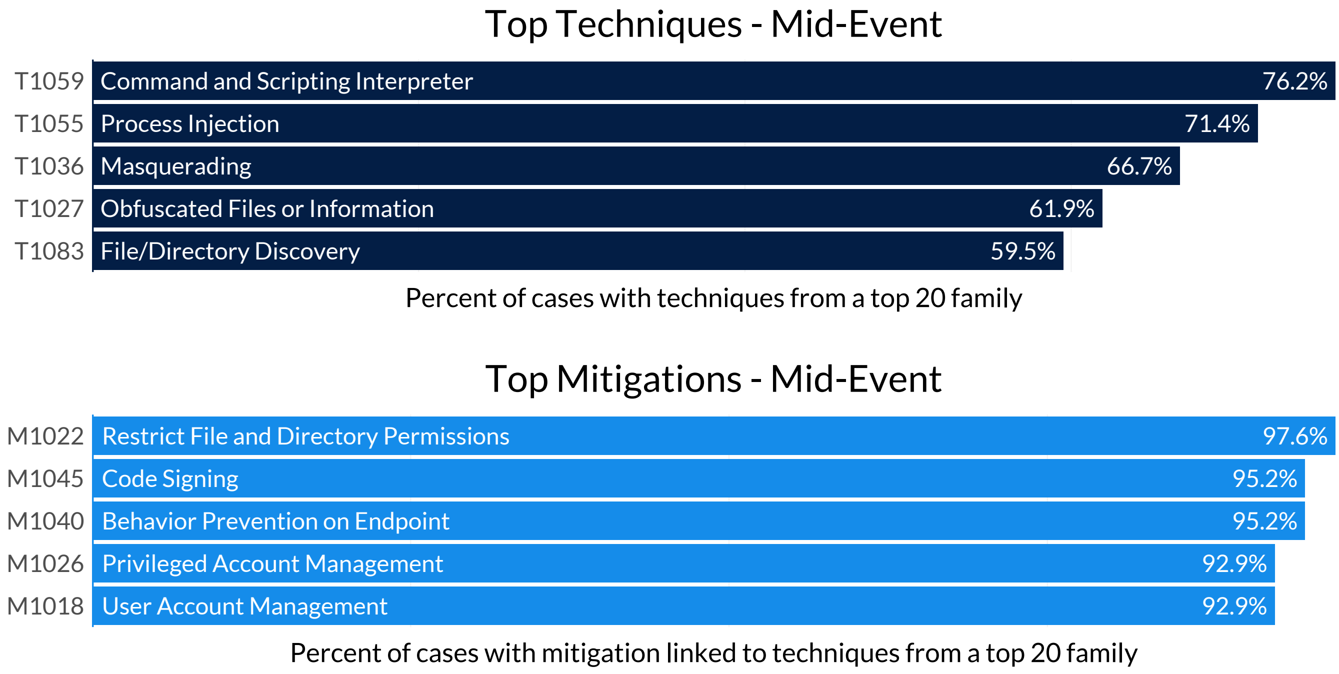

Figure 4—Sector's top mid-event techniques and mitigations

Figure 4 ranks post-compromise techniques associated with the most common ransomware strains encountered by victims in the financial sector. The percentages correspond to the proportion of cases involving ransomware possessing each capability. Since these techniques ostensibly contribute to the success of top campaigns, they offer a forewarning of what a threat actor might attempt should an infection occur in your systems.

Command and scripting interpreter techniques were quite popular among malicious users, showing up in 76.2% of cases, with process injection coming in at a close second at 71.4%.

The top mitigation techniques are all extremely close, each relevant to over 90% of ransomware cases in the financial sector. A common theme among them is trust, whether that be restricting permissions for files and directories, validating code, preventing malicious behavior on endpoints, or managing privileged and regular user accounts. These strategies that target the top post-compromise techniques can help financial services firms prevent data exfiltration and loss of availability in the event of an incident.

DATA EXFILTRATION AND IMPACT

We all know that ransomware encrypts data and holds it for ransom. However, it's becoming increasingly popular among criminals to also steal sensitive data from their victims and threaten to release it unless they pay up—see our previous report's section on payment reasons over time for more info.

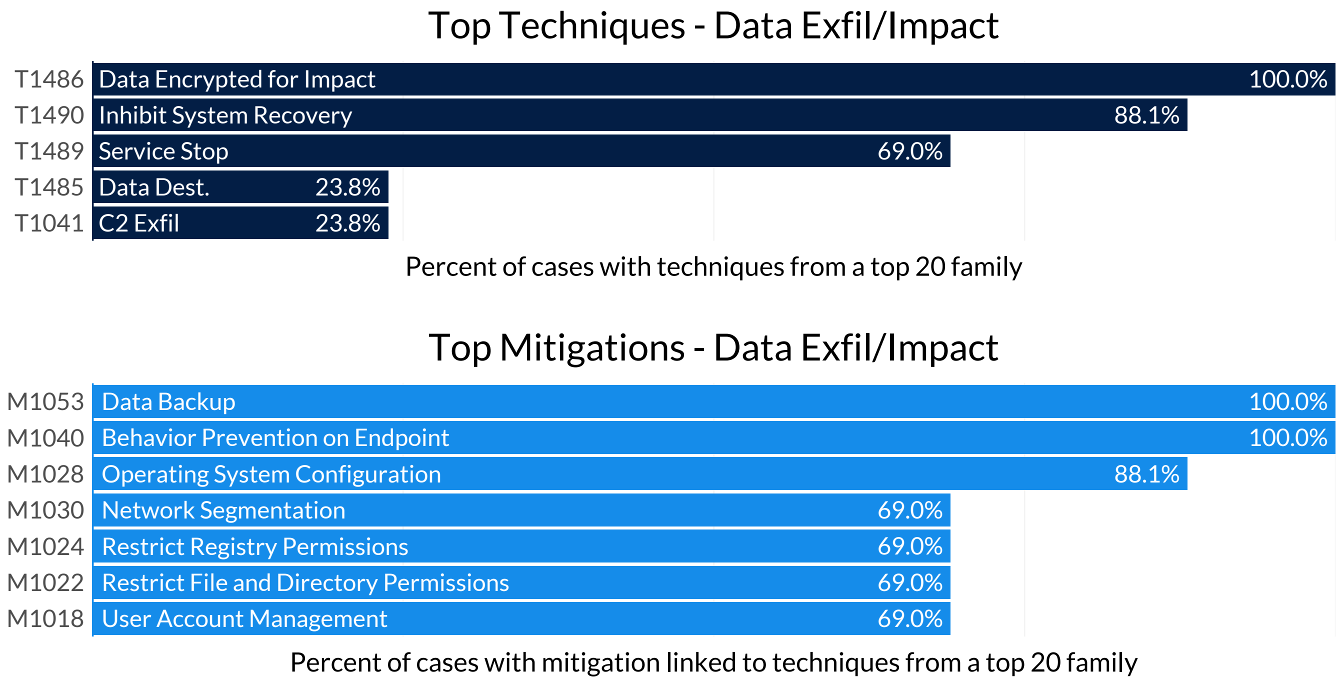

Figure 5—Sector's top data exfil/impact techniques and mitigations

Data encryption for impact was used in 100% of the ransomware cases that impacted the financial sector. The next most popular technique was inhibiting system recovery, which makes sense; in order for the criminals to make their ransom demand credible, they need to have sole access to your data.

Data encryption is the top technique used for impact. To mitigate risk of data exfiltration, user training and data backups are two key controls to consider when evaluating financial services organizations.

The top mitigation techniques are data backup and behavior prevention on endpoint. It's important to remember that demonstrating the ability to recover from backups is critical to mitigating these types of incidents and returning to business as usual. Operating system configuration is at the middle of the pack but highlights the importance of building a system that prioritizes not just efficiency but safety as well.

KEY TAKEAWAYS

Organizations are rightfully concerned about the rise and sustained dominance of ransomware as a tool of choice among cybercriminals. However, successful campaigns rely on more than one thing going right for the attacker. Defenders have more options and information about their adversaries than ever to tailor protections across multiple stages of developing incidents. It's our hope that financial services organizations can combine the insights above with their expertise to do exactly that.

LOOKING TO LEARN MORE?

While this report looks solely at how ransomware has impacted the financial services sector, we invite you to take a wider look at how these trends are impacting the overall business landscape. For additional analysis about how ransomware is impacting the world today, head over to the Investigative Cybercrime Series, Vol 1 & Vol 2.

Table of Contents
03 Key findings
04 Ransomware families
04 What are the most common ransomware families?
09 Ransomware capabilities & defenses
10 How does ransomware infect victims?
13 What does ransomware do after initial infection?
16 How does ransomware exfiltrate data?
The Investigative Cybercrime Series is an ongoing research effort to unmask insidious cyber threats and lessen their impact on insurers and the organizations they cover.
The data for this research comes directly from security incidents investigated by Arete and the intelligence operations that support those investigations.
Access Volume 1
Executive Summary
Key Findings
Reining in Ransomware
Investigative Cybercrime Series: Vol 2
A Collaboration Between
Arete
Cyentia

A collaboration between

Arete transforms the way organizations prepare for, respond to, and prevent cybercrime. With decades of experience and best-in-class technology, our team of experts provides comprehensive end-to-end services, from incident response and restoration to advisory and managed services.

The Cyentia Institute is a research and data science firm working to advance cybersecurity knowledge and practice. We pursue this goal through our data-driven products and joint research publications like this study.