Public 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 public services sector data, which represents 16.4% 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.

Public Sector Ransomware Highlights

Every sector has been affected by ransomware, and public services more than most. 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 THE PUBLIC SECTOR STAND RELATIVE TO OTHER INDUSTRIES ON KEY RANSOMWARE STATISTICS?

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

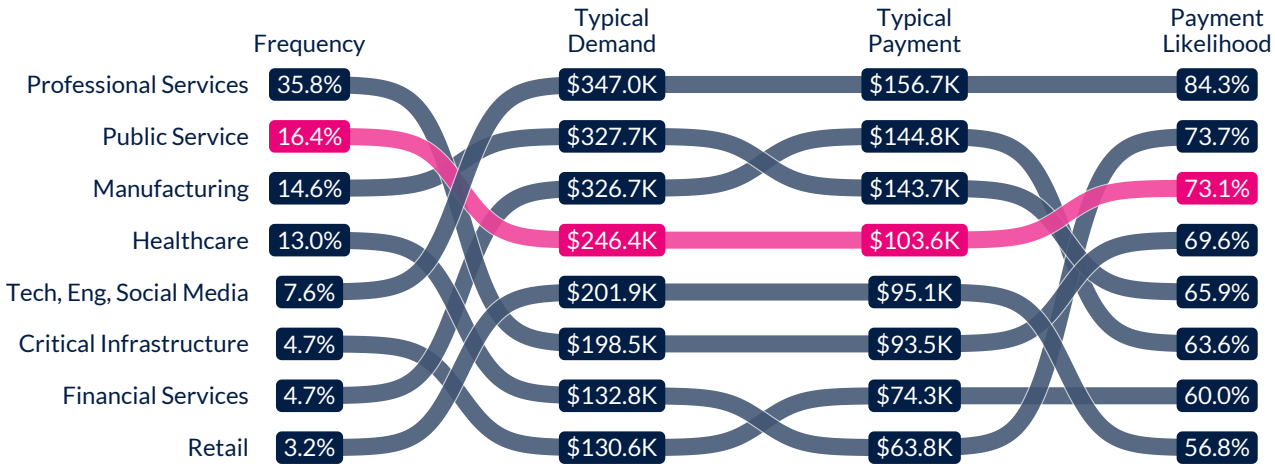


Figure 1—Sector's important values compared to others

KEY TAKEAWAYS

As Figure 1 illustrates, the public sector ranks second in the frequency of ransomware incidents, representing 16.4% of Arete's caseload. A contributing factor is the need for government organizations to be accessible to their constituency. This creates both vectors of attack and a strong incentive to avoid service disruptions, both of which cyber criminals are adept at exploiting.

Following the pink line, we can see that the public sector falls in the middle of the pack for the typical demand ($246.4K) and the typical payment ($103.6K). It rises slightly to the third spot when it comes to the likelihood of paying ransoms, with 73.1%. This demonstrates that cyber criminals typically extract more data from public agencies compared to private sector organizations.

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 public 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.

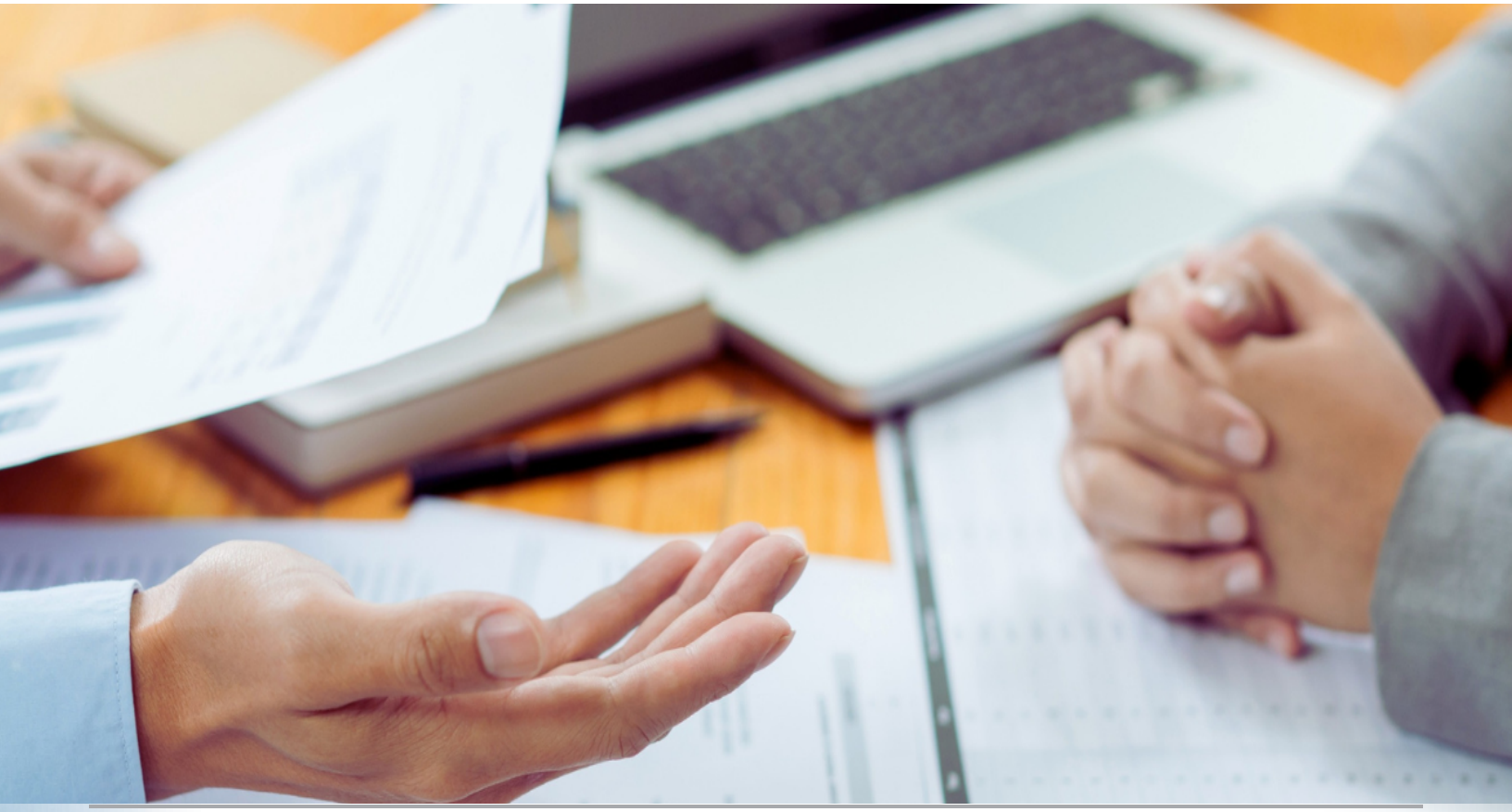
You can also compare these values to the overall trends in Table 1 in Volume 1 on page 8.

	Typical	Average	Extreme
Demands	$246.4K	$1.4M	$5.1M
Payments	$103.6K	$313.2K	$850.0K

Table 1—Sector's summary of demands and payments

KEY TAKEAWAYS

Extreme ransom demands within the public services sector are high, but still near the middle of the pack when compared to other sectors. It is worth noting the difference in demands and payments: public agencies paid 42.05% of the typical ransom demand and less than one-fifth (16.67%) of extreme demands.



Controls that Reduce Payments

As the prevalence of ransomware continues to rise, many organizations work to put controls in place to prevent the occurrence of infections and mitigate their impact. 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%
Public Service			
Multi-factor authentication	13.0%	22.8%	56.0%
Performing backups	62.0%	41.7%	80.2%
Proven recovery	24.1%	55.7%	54.8%
Endpoint detection & response	20.7%	72.7%	58.3%

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

KEY TAKEAWAYS

Only 13% of organizations in the public sector have MFA in place. Those that do, typically pay just 23% of the demanded ransom and have a 56% likelihood of paying, demonstrating that having an MFA solution is one of the more effective ways to decrease ransomware payments in the public sector.

Nearly two-thirds of public organizations (62%) report performing regular backups, yet just 24% of them demonstrated the ability to fully recover from ransomware events. Both capabilities reduce the percentage of ransom demand paid, but a proven ability to recover is more effective at lowering the likelihood of payment. EDR platforms were not common among public service agencies in our caseload, observed in just 20.7%. Interestingly, those that did have EDR did not see huge reductions in the proportion of ransoms paid and fell short of some of the other controls in payment likelihood.

This data indicates that having multiple controls in place will allow your 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.

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.

Top Ransomware Families in Public Sector

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 public sector since 2019. The figure is color-coded according to the families' current state of activity:

DARK BLUE
INACTIVE

LIGHT BLUE
STEADY OR DECLINING ACTIVITY

PINK
TRENDING UP

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

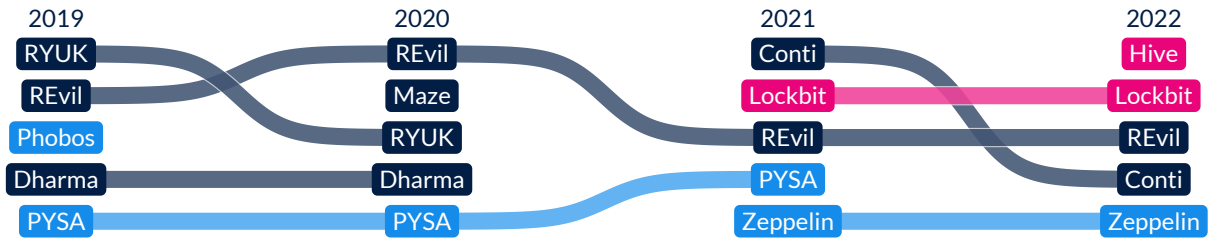


Figure 2—Most prevalent ransomware families observed in public sector incidents

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.

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, is 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.

> 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.

The Hive ransomware syndicate is one of the known havens for ex-Conti members, which is why they're among the trending ransomware families in 2022 for the public sector. However, the U.S. Department of Justice announced a successful campaign in early 2023 to disrupt the group behind Hive. This is another example of how quickly the ransomware threat landscape changes; organizations of all types need to be on top of tracking it.

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.

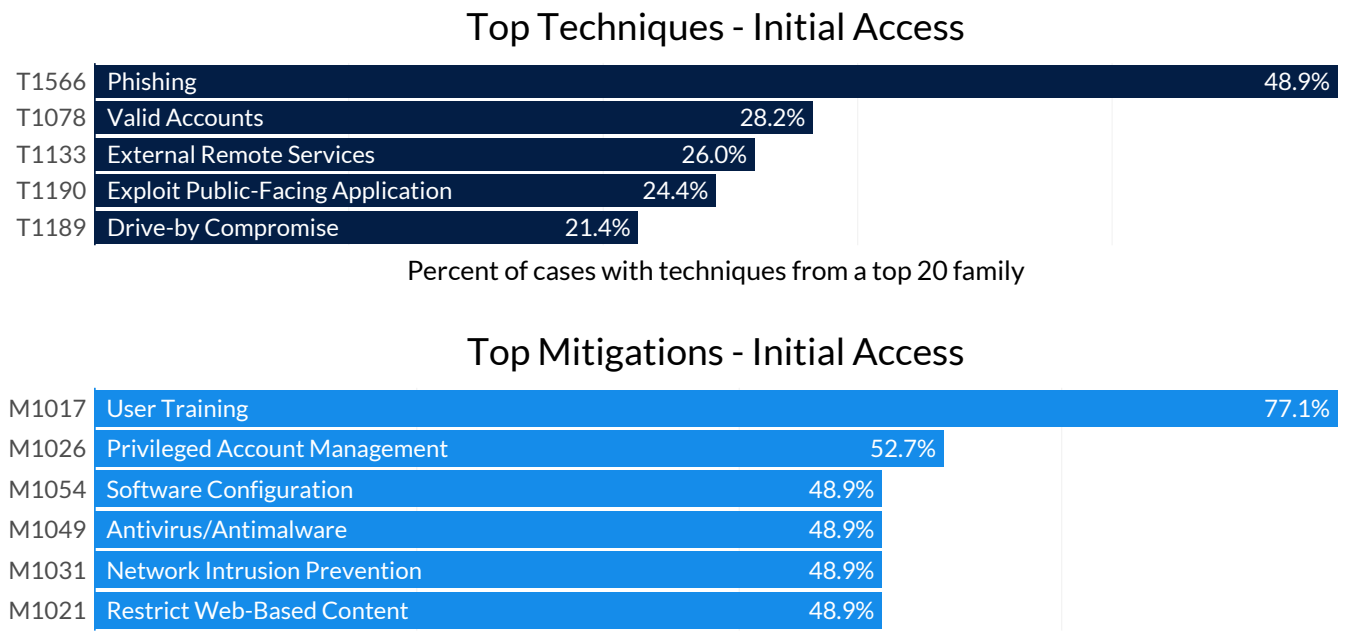


Figure 3—Sector's top initial access techniques and mitigations

Observed in 48.9% of cases, phishing is the most common way ransomware is initially introduced into government agencies. The other top techniques for initial access, including valid accounts, external remote services, exploiting public-facing applications, and drive-by compromise were utilized much less frequently in 21.4 to 28.2% of cases.

The top variant impacting the public sector 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 77.1% of these cases. Protecting privileged user accounts ranks second at 52.7% of events. The four-way tie for third 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.

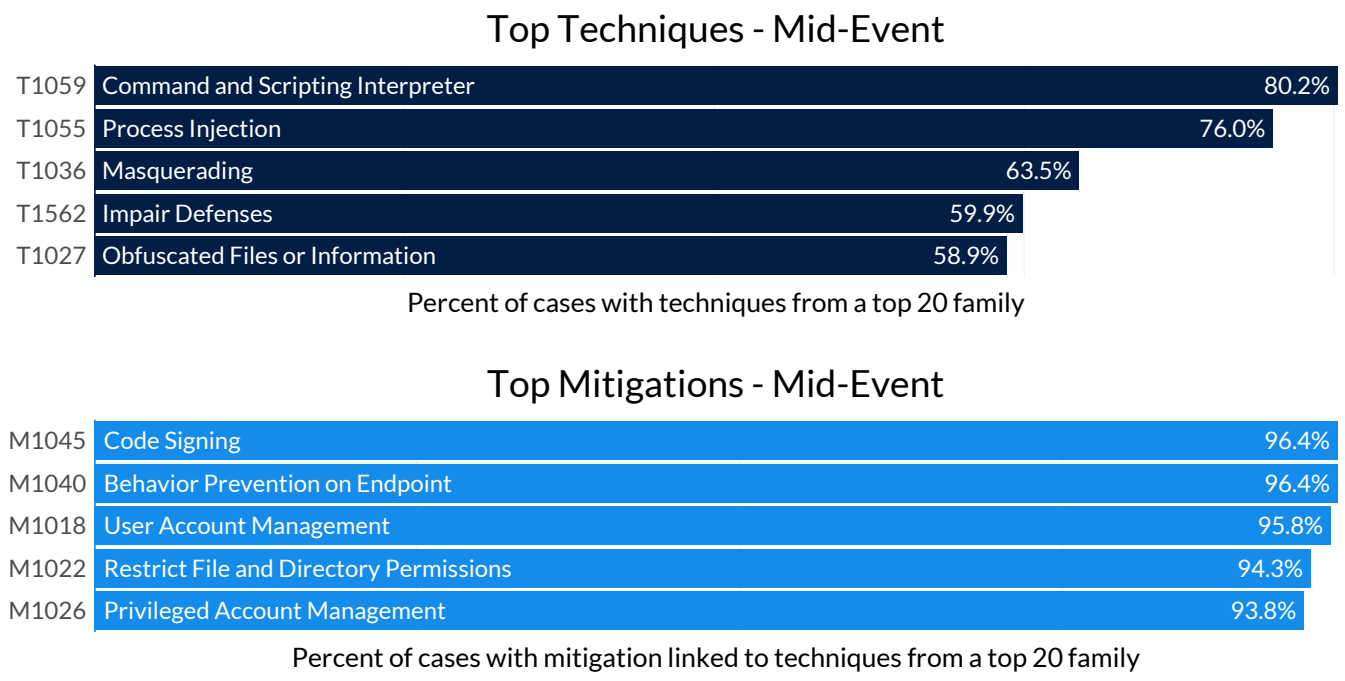


Figure 4—Sector's top mid-event techniques and mitigations

Figure 4 ranks post-compromise techniques associated with the most common ransomware strains encountered by victims in the public 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 80.2% of cases, with process injection coming in at a close second at 76%.

The top mitigation techniques are all extremely close, with the top spot at 96.4% being shared by code signing and behavior prevention on the endpoint. Still in the 90s, the "bottom" three mitigations are user account management, restricting file and directory permissions, and privileged account management. Defensive strategies that include mitigations for the top post-compromise techniques can help public agencies 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 is 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.

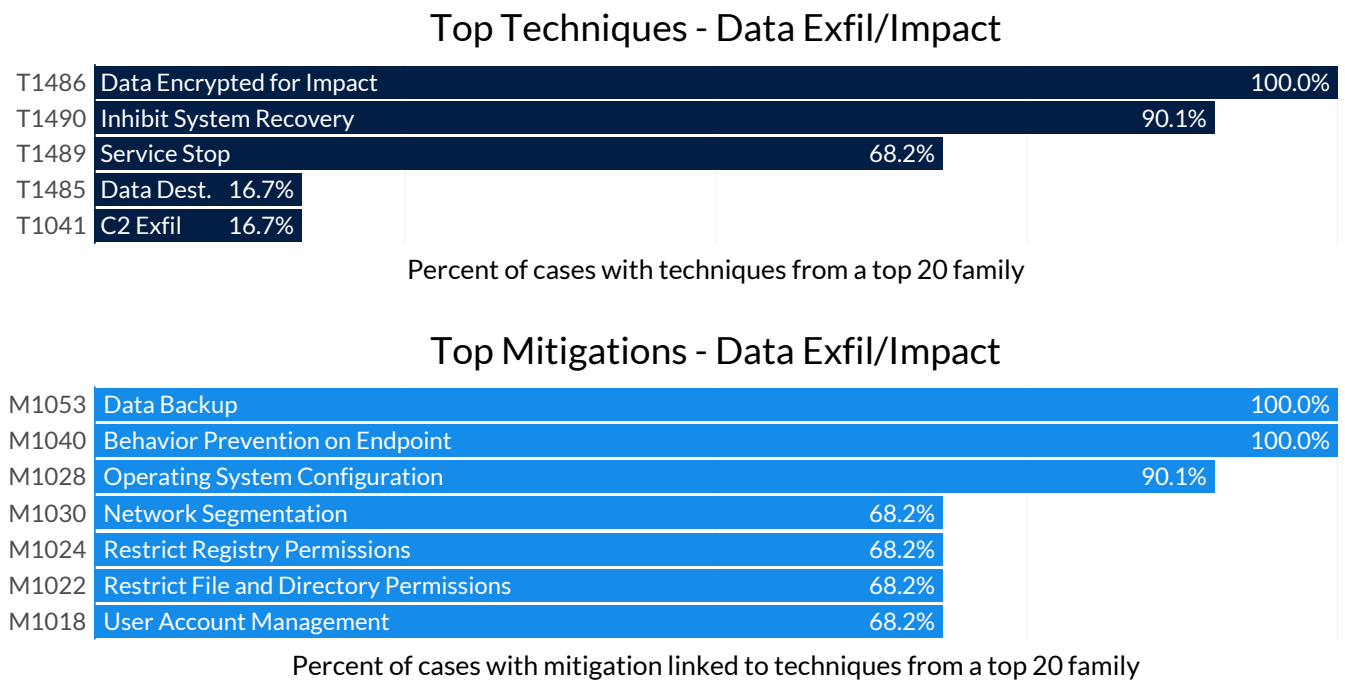


Figure 5—Sector's top data exfil/impact techniques and mitigations

Data encryption for impact was used in 100% of the ransomware cases that impacted the public 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 the risk of data exfiltration, user training and data backups are two key controls to consider when evaluating government agencies.

The top mitigation techniques are data backups and behavior prevention on endpoint. It is 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 and network segmentation highlight the importance of building systems and networks that prioritize 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 cyber criminals. 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 is our hope that public agencies 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 public sector, we invite you to take a macro 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.

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.