SANS

Analyst Program

Survey

Ransomware and Malware Intrusions in 2022 (And Preparing for 2023!)

Written by **Matt Bromiley**

March 2023

CrashPlan

Executive Summary

The year 2022 confirmed one thing (if it wasn't confirmed already): *Ransomware is here to stay*. Whether we like it or not, adversaries continue to find success in deploying malware and locking up access to enterprise resources. As with prior years, 2022 continued to see high-profile ransomware attacks on critical organizations such as K–12 education[1] and life-saving healthcare networks.[2]

When breaches occur, there's plenty of blame to go around: vulnerabilities left unpatched, passwords stolen or easily cracked, access to resources left wide open. Information security is the job of many, and security teams are working hard to mitigate these vulnerabilities, protect their networks, and minimize business impact. And many of them are having success.

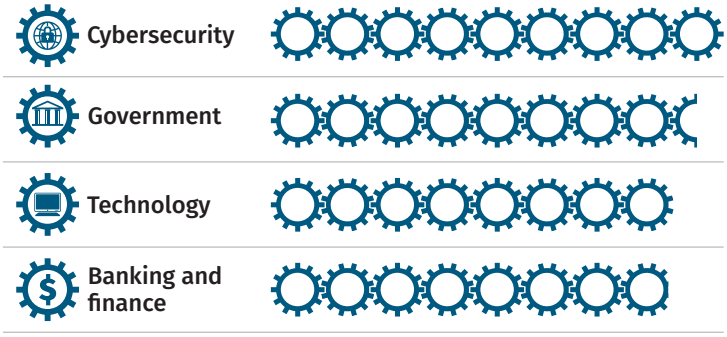
In this survey, we wanted to understand what the past year looked like for our respondents. Taking an incident response (IR) viewpoint on malware and ransomware intrusions, our survey focused on key points in the investigation lifecycle, and how our various teams dealt with the challenges they faced. Some of our key takeaways included:

- Approximately 79% of respondents felt that their organization was actively targeted by ransomware threat actors, likely prompting action and security expenditures.
- Having an IR plan, utilizing third-party tools for incident detection, and providing an in-house security operations center (SOC) with appropriate telemetry were the biggest ransomware mitigation steps.
- Respondents reported that IT, customers, and information security would be the top three areas impacted by a ransomware attack.
- Despite the "best" efforts by adversaries, our respondents indicated that at least 75% of incidents with ransomware objectives did not result in a ransom—a win for security!
- Approximately 61% of respondents said that restoring from a backup was their solution to responding to a ransomware intrusion—highlighting the need for resiliency and a backup solution.

Thank You to Our Respondents!

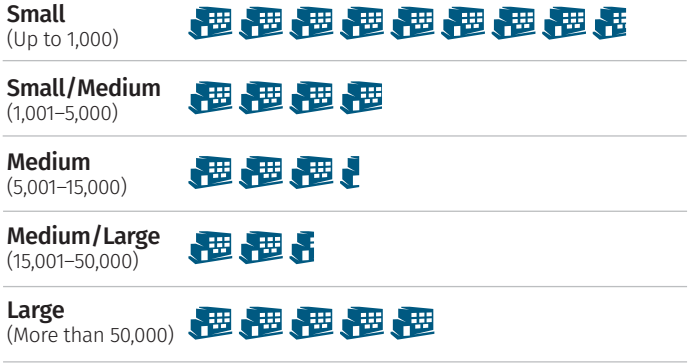
This year saw a wide range of survey respondents from upper management and C-suite to junior analysts and consultants. This respondent pool provided us insight across a wide range of professions and geographies, providing a diverse look at the past year of malware and ransomware intrusions. See Figure 1 on the next page for a more detailed breakdown of our respondent pool.

Top 4 Industries Represented



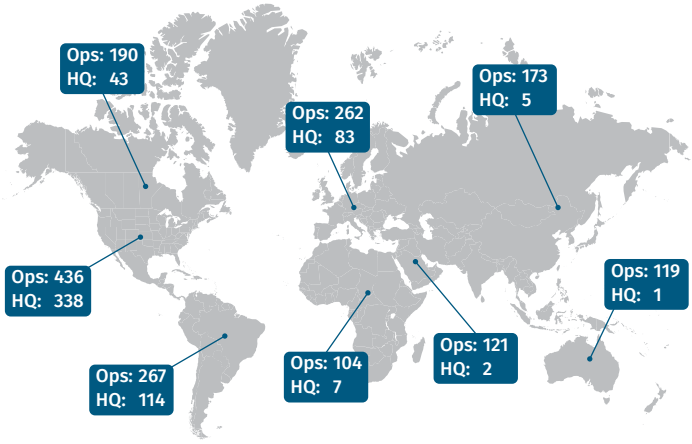
Each gear represents 10 respondents.

Organizational Size

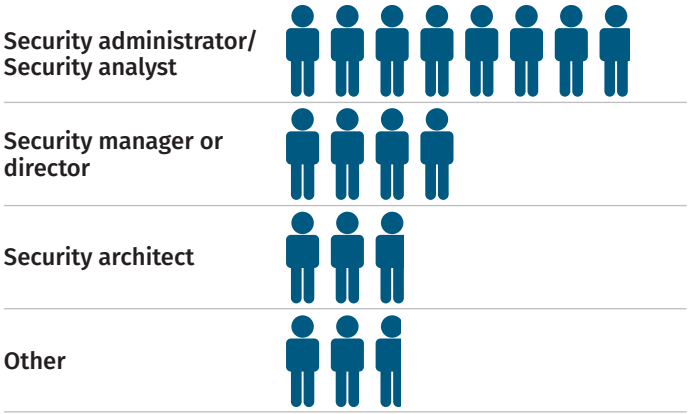


Each building represents 25 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 20 respondents.

Figure 1. Survey Demographics

Ransomware Threat Profiling

Every time malware/ransomware intrusions are brought up in the media, it's all doom and gloom. The popular phrase "It's not *if*, but *when*..." has loomed over many board meetings and driven security decisions for many years now. However, there are plenty of organizations that have never experienced an event. Are they supposed to wait for the "when" forever? Or have they made investments to lessen that risk?

We began this survey by asking whether ransomware posed a credible threat to our respondent organizations, and an overwhelming 95% responded yes.

However, perhaps more interestingly, we also asked whether they felt their organization was actively targeted by ransomware threat actors (see Figure 2). Approximately 79% of our respondents felt that they were actively targeted, with 21% answering in the opposite.

Do you think your organization is actively targeted by ransomware threat actors?

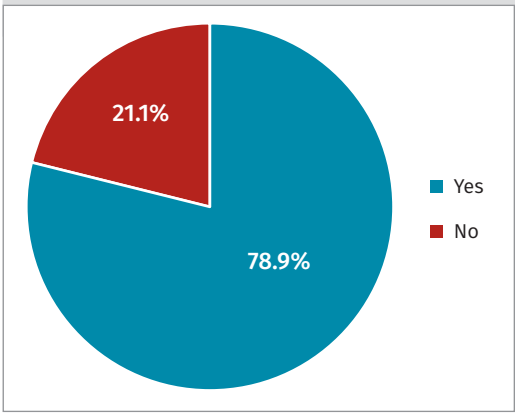


Figure 2. Perceived Threat Risk

We feel that this breakdown represents a unique dissection of threats and risk management. If we are to believe media reports and FUD-claiming blog posts, then every organization should be prepared for an attack—now! However, we cannot expect all teams to remain on high alert *forever*. Instead, the security team must make an informed decision as to whether they feel actively threatened and then formulate a response based on that decision.

Our findings suggest that with informed threat intelligence and/or perhaps a robust security posture, maybe 21% of our respondents can confidently assess that they do not feel targeted.

Continuing to explore this thread further, we also asked our respondents to expand on this level of confidence. Figure 3 shows what investments were made to mitigate the threat of ransomware, might shed light on the source of such confidence.

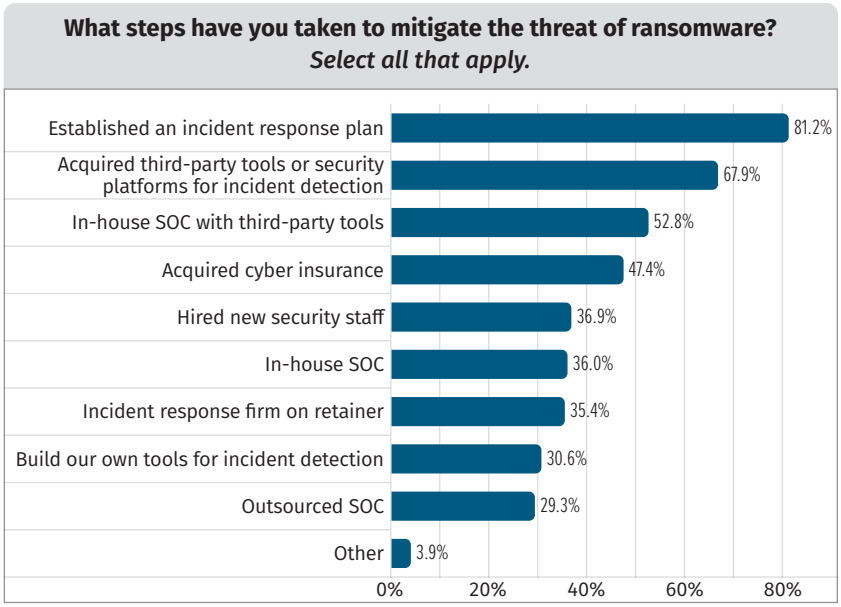


Figure 3. Threat Mitigation Activity

The top three answers, establishing an incident response plan (81%), acquiring third-party tools (68%), and establishing an in-house SOC with third-party tools (53%), are in line with our expectations. We have been saying for years that organizations should invest in their own security programs and have a plan in place. Concurrently, we have seen organizations make investments in their security posture for years, and those investments are paying off. (In the next section, we'll evaluate some of this in our incident lifecycle walkthrough.) Having an incident response (IR) plan and increasing telemetry within your organization are critical steps to erecting effective malware and ransomware defenses.

On the topic of enterprise preparedness, we also asked our respondents what areas would be most impacted by a ransomware attack. Figure 4 provides these results.

Figure 4. Potential Ransomware Impact

Approximately 80% of our respondents selected IT as an impacted area, the largest representation. Second and third place were customers and information security, respectively. These statistics align with our own expectations, which would see an attack like ransomware spread throughout an organization. Additional areas expected to be affected included accounting and the C-suite.

This is an important consideration for any organization—just how and where would ransomware impact the organization? We did not expect customers to come in as the second-highest area represents a unique viewpoint—even though it is the organization that must recover from the attack, it is the customers who may suffer most due to lack of available services, inability to connect to the victim organization, or long-tail effects of loss of trust and reliance. Furthermore, it is tougher to insulate customers against the effects of a malware/ransomware attack, despite the security team's best efforts.

A Year of Incident Response

Most of our survey focused on questions from an incident detection and response perspective. We did this intentionally—we wanted to track how security teams respond and how adversaries act at each step of the investigation lifecycle. For reference, we will use the high-level diagram shown in Figure 5 to explore these results.

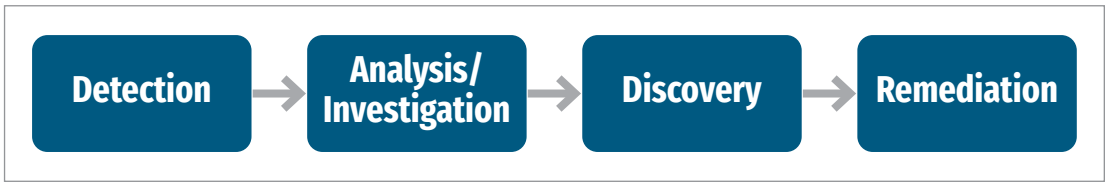


Figure 5. Investigation Workflow, from Incident Detection to Remediation

We also wanted to know just how many incidents our respondents have responded to in the past year. Figure 6 shows the results.

More than 50% of our respondents reported that their incident count was low—no more than five throughout the past 12 months, which provides ample opportunity for response and remediation efforts. The other results no more than that our respondent pool had a wide range of incident counts in the past year.

Finally, we drilled down one more step, asking our respondents how many of the incidents they reported were determined to have ransomware elements. Figure 7 has these details.

Note that between Figures 6 and 7, approximately 51% of respondents had one or more ransomware-related incidents, bolstering our statement that ransomware remained a top threat for many organizations. As seen in Figure 7, some organizations had multiple incidents with ransomware elements. Again, we will use these results to help examine additional questions and responses, which focus on key investigation lifecycle steps.

How many incidents have you or your team responded to in the past 12 months?
(Note: These are incidents responded to, however you may confirm them. This is not a count of detections over the past year.)

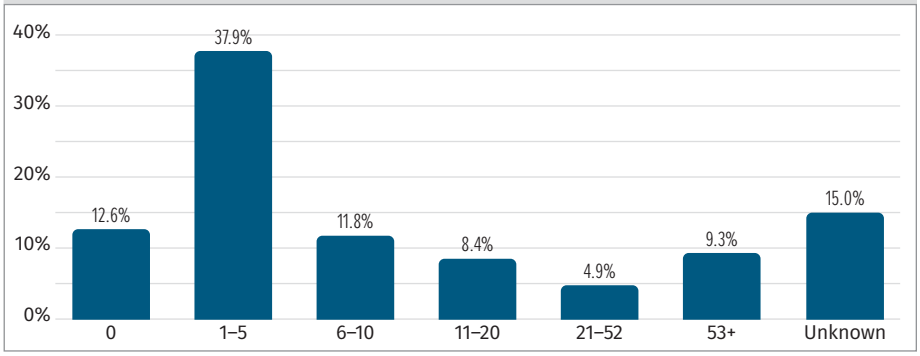


Figure 6. Security Incidents in the Past Year

How many of these incidents were determined to have ransomware elements, whether file contents were encrypted or not?

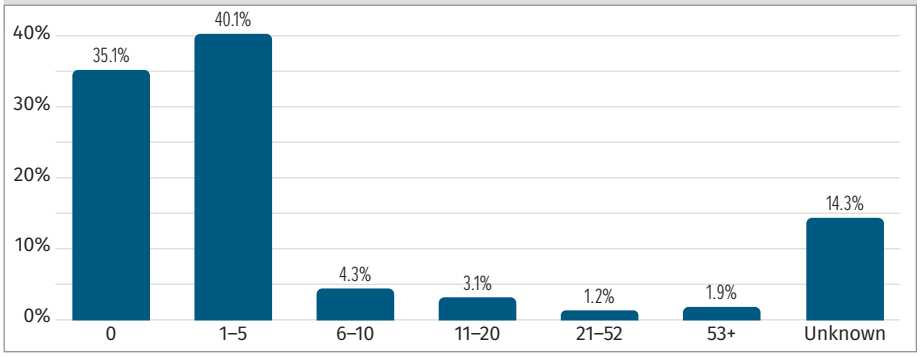


Figure 7. Incidents with Ransomware Elements

How to Use These Stats

One of the most important things any security team can do is maintain statistics and reporting for posterity. Our survey captures some of these points for our respondents; however, we encourage your security team to maintain the same level of statistics that we will examine in subsequent sections.

Incident Detection

The first step in our investigation workflow looks at incident detection. A myriad of means may be used for initial incident detection, ranging from custom detections to third-party notifications or "ransom note" detections. Figure 8 looks at how incidents were initially detected.

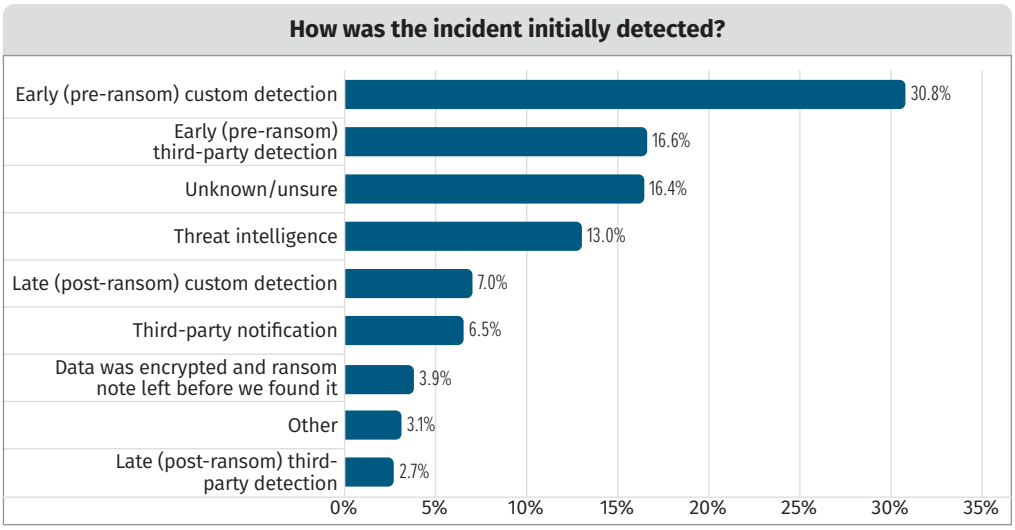


Figure 8. Detection Methods

A healthy portion of detected incidents, approximately 31%, were pre-ransomware custom detections. The second-highest detection method, also pre-ransom, was third-party detection. We are huge proponents of "the earlier the better," and these results confirm that our respondents have taken note—this gives the security team a huge advantage in stopping adversary activity prior to any ransom-related impact.

The third-highest category for this question was "Unknown/unsure," which is always a troublesome category for SANS surveys. As mentioned previously, we encourage organizations to retain as much data as possible for posterity, incident correlation, and organic security growth from incident to incident. Organizations that are unsure or do not know how incidents are detected are leaving a significant amount of critical data unchecked. Security teams absolutely need to know how incidents have been detected, and we encourage them to make these changes going forward.

Far too often we see organizations lose institutional knowledge that could have easily answered some questions. Tracking incidents within an organization is critical to understanding the threats it is facing, determining how detections correlate with one another, and informing future staff of past events, so they can make informed decisions.

With less representation, but still critical to our analyses, are the post-ransom detections. Frankly, post-ransom is too late for these types of intrusions. Once an adversary has encrypted data, they have already impacted operations—the security team is now far behind the curve. One goal with easy metrics that these teams should strive for is earlier, pre-ransom detection.

Within this phase, we are curious to understand how an adversary may have gained entry into an organization. It is important to track and understand adversary entry vectors to ensure that open vulnerabilities and/or access means are patched before they can be re-exploited.

As you can see in Fugure 9, nearly three-quarters of our respondents indicated that they did know the adversary's entry vector. This is one of the most important pieces of information about an intrusion that any security team can obtain. Knowing how an adversary broke into an environment is critical to knowing how to fix that security gap.

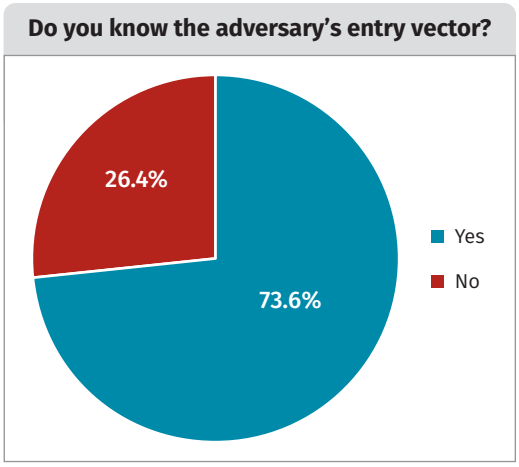


Figure 9. Vector Entry

We also asked our respondents what the adversary's entry vector was. Figure 10 displays the results, mostly expected.

It should come as no surprise to anyone who has been observing information security over the past decade that spearphishing was the primary entry factor. However, the sheer amount by which spearphishing led—nearly three times as often as the second method—was astounding.

Coming in at a distant second and third were external vulnerability and remote access, at 29% and 27%, respectively. The top three entry vectors don't surprise us (although, yet again, the dominance of spearphishing is something to marvel at). In fact, industry experience and recent threat reports have indicated that adversaries will show no preference for one entry vector if another is available, is cheaper, and/or is more reliable.

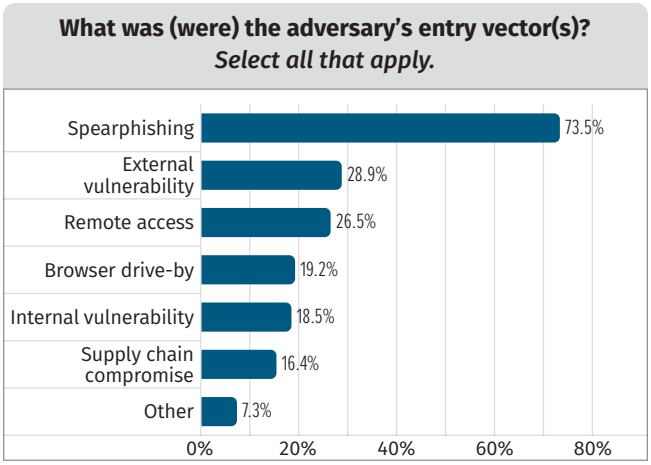


Figure 10. Entry Vectors Identified

Knowing how adversaries got into your organization is one thing, but knowing how they *could* get in is another. Our survey proves one thing: Attack surface management, or knowing your perimeter, is a critical step in gaining control back from adversaries, who may have options you don't even know about yet.

Adversary Actions

Once adversaries have gained a foothold in the environment, their next step is often a mix of different post-exploitation steps. The steps taken by adversaries who have ransomware in mind are often predictable. Remember, their goal is to spread ransomware throughout the victim environment. For this reason, we often see threat actors repeat the same steps from target to target.

Depending on the types of permissions, accounts, systems, locations, and a blend of other factors, adversaries may need to:

- **Escalate privileges**, seeking higher privileges to execute commands or perform another task
- **Harvest credentials**, gaining access to other account(s), for persistence purposes or to jump to another account with higher privileges
- **Move laterally**, looking for additional systems to compromise and/or encrypt as part of a ransomware attack

We asked our respondents whether, during their investigations, they discovered that adversaries had to do any of these three items. Figure 11 provides insight into those results.

First off, an overwhelming majority of respondents indicated that all three actions were needed in observed incidents. Although harvesting credentials is by far the most common post-exploitation act, privilege escalation and lateral movement were not far behind. Figure 11 also shows that, in some situations, it was not necessary for an adversary to take these post-exploitation steps.

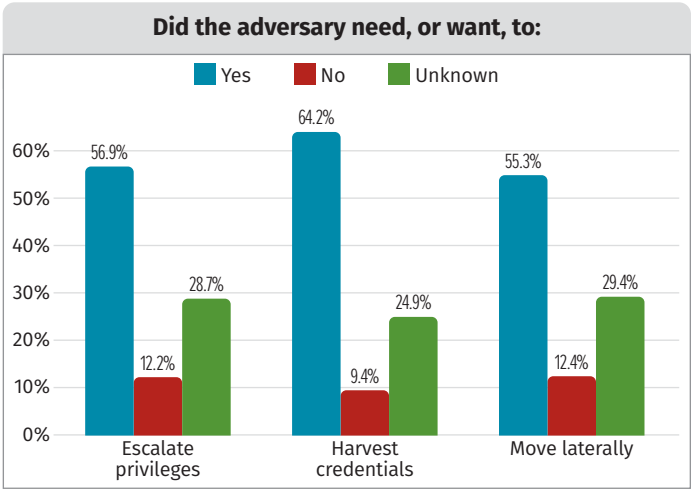


Figure 11. Post-Exploitation Steps Taken

We did not pull further on this thread; however, we have seen in industry experience time and time again where adversaries compromise an account or system that they "need." Consider, for example, a brief case study where an adversary compromises a vulnerable Exchange email server (as we have seen in recent years due to publicized vulnerabilities). Depending on how the server was configured or account exposure, the adversary may gain the system and account they need on the first hit and not need to execute additional post-exploitation commands.

When an adversary gets lucky like this, it can make incident response significantly more difficult, especially in malware/ransomware cases. The security team might rely on detections for certain predictable adversary events, such as the three activities we identified previously; however, if an adversary never has to do those things, then the detection may never fire. Furthermore, in situations where an exploit is outside the bounds of telemetry, a compromised system and/or account may go unnoticed for a long period of time.

For our respondents who answered "unknown" for this question, we reference you back to our earlier comments on *not* tracking incident details from your investigations. We can say with certainty that security teams do well with historical data and context, especially to help train future analysts. As you're reading this survey and you find yourself in the "unknown" category, we highly recommend that you utilize some sort of incident tracking system (even if it's simply a text file with notes in it) so that you will have an enduring record.

We pressed further, wondering about adversary objectives, asking if investigated incidents resulted in encrypted data. Figure 12 has those results (organized by number of incidents).

Through the next two figures, we begin to see a "funnel" forming in our respondents' answers. Figure 12 shows that approximately 64% of incidents did not result in encrypted data—a strong testament to the detection and response capabilities of those organizations. These respondents likely fit within the pre-ransom detection groups we reviewed earlier. Furthermore, without data encryption, it is unlikely that the adversary made a ransom demand, as shown in Figure 13.

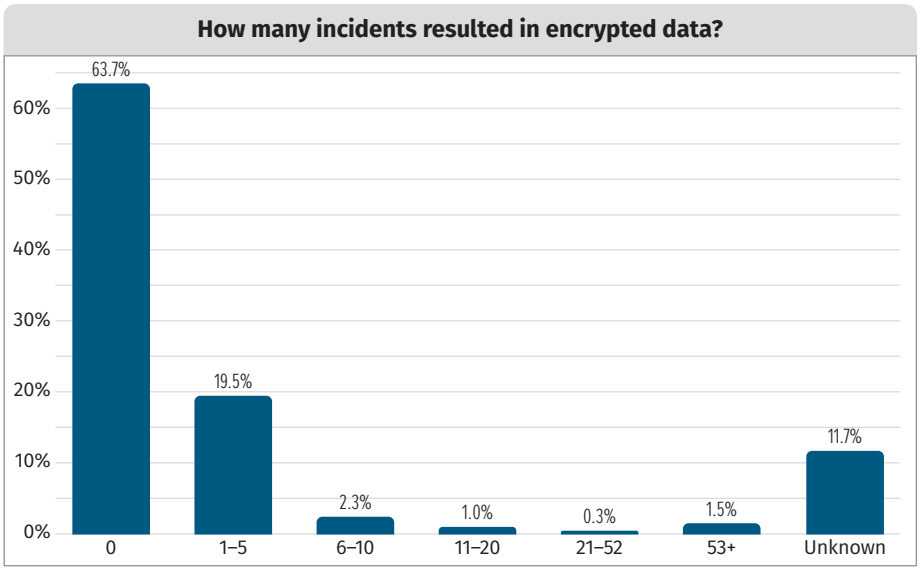


Figure 12. Encrypted Data Incidents

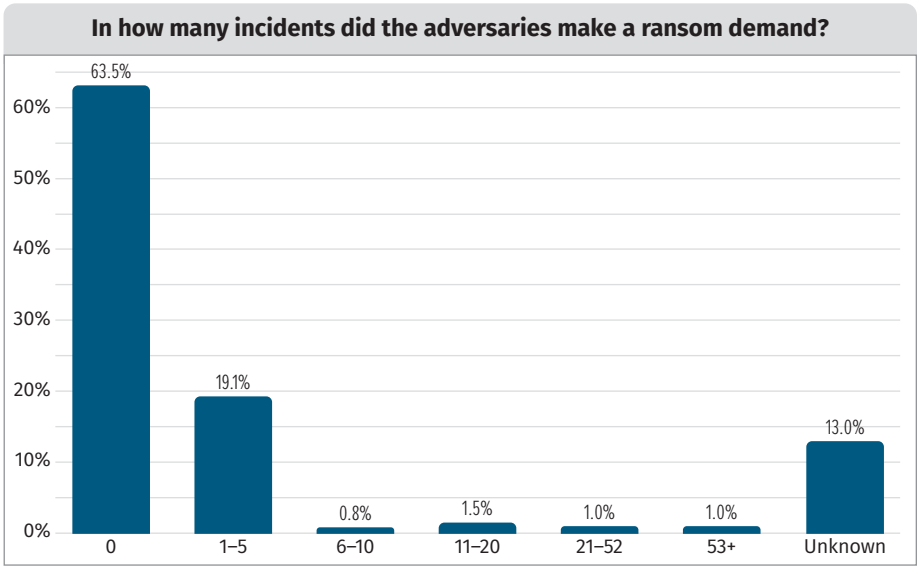


Figure 13. Ransom Demand

The results from Figures 12 and 13 are almost identical, aligning security teams that did not have encrypted data with those that had no ransom demands—nearly 64% in both cases. However, approximately 19% did see between one and five incidents that resulted in both encrypted data *and* a ransom demand, indicating that adversaries succeeded a small number of times.

For the previous two data sets, we also saw an interesting (albeit single-digit) representation in the 20-plus categories. Teams that are facing multiple incidents per year and see at least 20 turn into data encryption and ransom demands need to revisit some of their security technologies, incident response plans, or incident recovery plans—which we'll examine next.

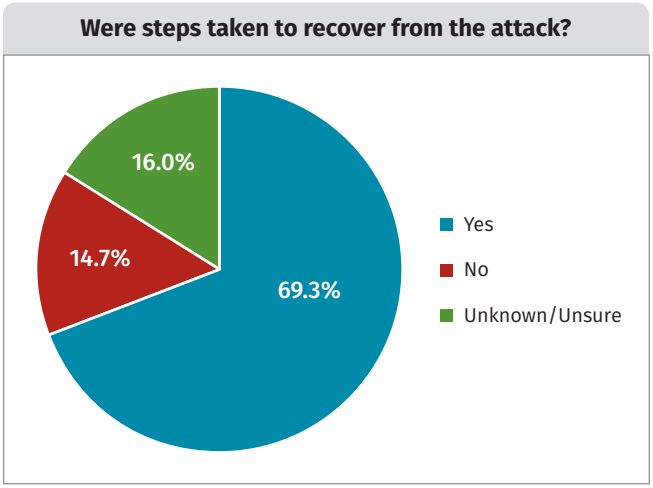


Figure 14. Recovery Remediation

Incident Recovery

The final stage of the incident response lifecycle is remediation and recovery. This is one of the most critical steps, especially in the aftermath of a ransomware event, because this is where security teams hope to get the business back to normal. As seen in Figure 14, nearly 70% of organizations did take steps to recover from the attack.

Admittedly, we expected the "yes" number to be higher—approximately 15% of respondents indicated that they had not, or did not need to, take steps to recover. We must ask then: What happened? Is the incident still ongoing, or was the environment stripped down and rebuilt?

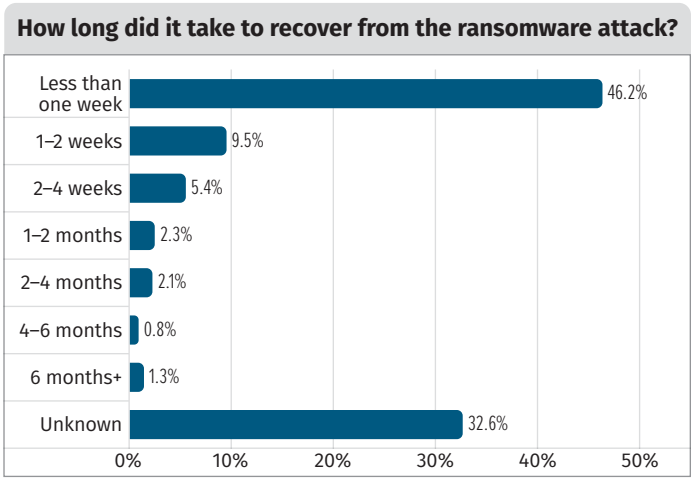


Figure 15. Recovery Duration

Any intrusion can take weeks or months to recover from, depending on environment size, impact, and adversary capabilities/infection rate, to name a few factors among many. Ransomware intrusions can prove to be especially tricky because they impact the environment and disrupt business in a way that is not so easy to recover from. For those that did pursue recovery options, Figure 15 looks at that time frame.

Nearly half—approximately 46%—of our respondents indicated that recovery took less than one week. This is one of the most promising statistics in this entire survey. A week is a very quick time frame to recover from an attack, especially ransomware incidents. We're making an assumption that incident recovery achieved within a week was done properly and the organization got back to normal before too much was impacted.

The latter set of statistics is where security teams can find the most difficulty. When an incident takes weeks or months to recover from, it could have long-lasting and damaging effects on the security team and the organization overall. No team likes to be stuck in IR mode for too long. Although we want to do the job right, time frames that last for multiple weeks or months (as we saw with some of our respondents) cover dangerous ground. We highly recommend that if you find yourself in that category, make every effort to let your team resolve this incident and get the enterprise back to normal.

For those security teams that did pursue remediation options, we asked what steps were taken to recover from the attack. Figure 16 has those details.

The top three steps that we saw in this question were predictable and align with some of the most common incident recovery steps. Resetting passwords (63%), restoring from backups (61%), and modifying policies to prevent further abuse/access (54%) are critical steps for general security hygiene—and especially important during incident recovery!

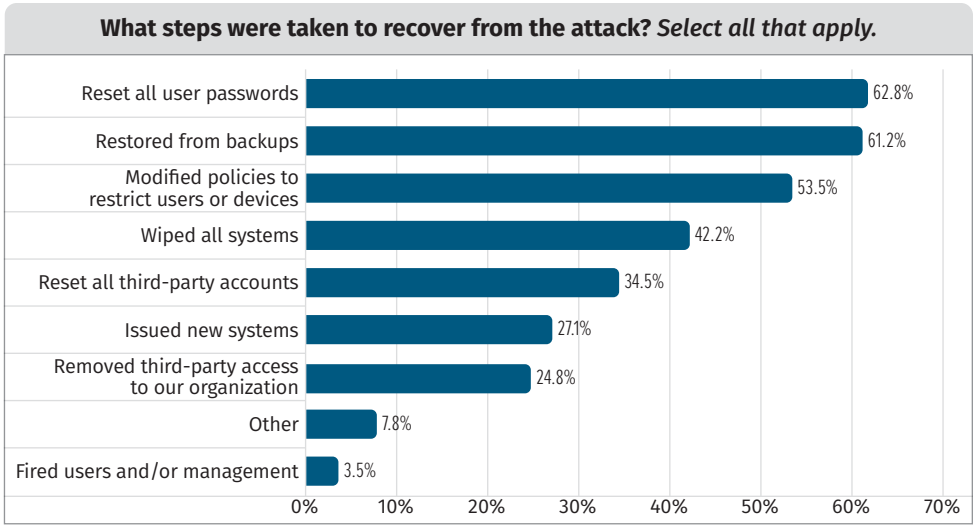


Figure 16. Recovery Remediation Path

Notably, some of our respondents do take different—maybe even more drastic—routes when recovering from an incident. Approximately 42% of our respondents wiped all systems, whereas 27% issued new systems! Without knowing the full scope of an incident, we cannot say whether these steps were necessary; however, any organization that must issue completely new systems is likely recovering from a fairly devastating attack.

Finally, one question we were curious about, but that provided no insight into ongoing incidents, was whether a threat actor had returned to an environment or was there for the first time. Of course, this question relies very heavily on our respondents knowing enough details to confirm whether an adversary had been in the environment before or not. (We have already stressed the importance of retaining investigation details, so we won't stress it again.) Figure 17 looks at details around returning adversaries.

Our examination of the survey results does not dig too much into third-party or supply chain compromises. However, we did observe that the remediation steps taken to recover from an attack did include a healthy percentage of resetting or removing third-party accounts or access to an environment. An important takeaway here is that, even though third-party access is not a major factor, it is still an important consideration and should be part of any security audit.

There is a very interesting, and pretty even, split among three notable results in this question. Approximately 31% indicated that none of their adversaries were first-timers. Approximately 32% indicated that an adversary had returned, suggesting that they had enough details to confirm that in at least one to five incidents, an adversary was back. Finally, approximately 31% indicated that it was unknown. We expected such results. It is not always easy for an IR or a security team to know with certainty whether an adversary was there for the first time.

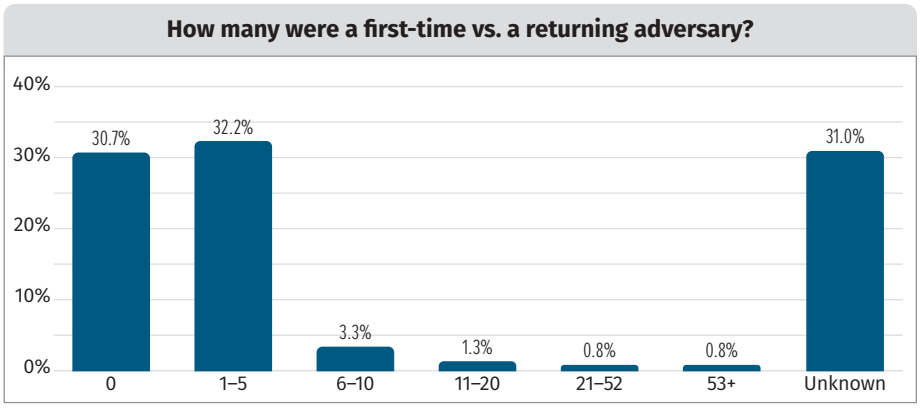


Figure 17. First-Time vs. Returning Adversaries

The Year Ahead

The latter part of our survey looked at how security teams have learned from these malware/ransomware intrusions and what steps were taken for future security posturing. We had two specific questions in mind: Did you acquire technology based on a ransomware attack, and do you plan to acquire any more? We'll look at each question separately, beginning with Figure 18.

Did your organization, or an organization you worked for, acquire any new technologies or make investments based on a ransomware attack?

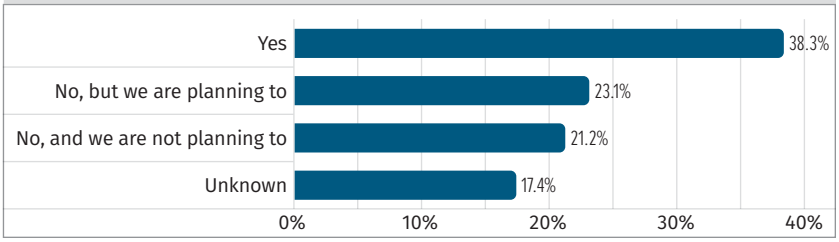


Figure 18. New Technologies/ Investments Driven by a Ransomware Attack

Only 38% of respondents said that they needed to acquire new technology, and 23% indicated that they had intentions to do so. These results offered an interesting split, suggesting that each environment had to make considerations about (1) how the intrusion occurred and (2) whether additional investments were necessary. For example, if an organization suffered an incident but the adversary never proceeded past an entry vector, then additional technology spending might not be required. Conversely, for organizations that ended up paying a ransom, new technology was likely purchased during the incident response.

For our respondents who indicated that they were planning to purchase new technology, or for respondents planning to purchase technology in general, our final question looked at what types of investments they would be making. Figure 19 provides our results.

What investments are you likely to make because of a ransomware attack?
Select all that apply.

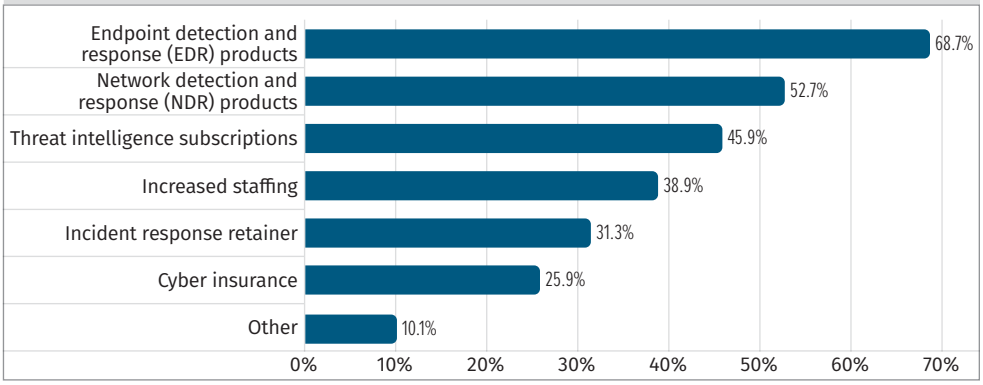


Figure 19. Planned Investment(s) Based on Ransomware Attack

It should come as no surprise that some of the most sought-after technology in any enterprise is detection and response products; in this case, preferences for endpoint and network, respectively. Nearly 70% of our respondents indicated that they were seeking endpoint detection and response (EDR) products, while almost 53% indicated that they were planning to acquire network detection and response (NDR) products. EDR and NDR technologies make up some of the most critical types of telemetry that any enterprise can have, because they offer deep insight and critical IR capabilities.

We were also pleased to see that some organizations plan to expand their staff (approximately 39%) and/or obtain an incident response retainer (approximately 31%) to help them navigate future potential uncertainties. Respondents in the "other" category included some critical investments, such as:

- Network segmentation plans
- Backups
- Cloud-focused security tools
- SIEM/security orchestration, automation, and response (SOAR)/cloud access security broker (CASB)
- Hardening the IT/OT boundary

Regardless, our survey provided unique insight that can help our readers and respondents determine where they might have critical security gaps, and what tools/technologies can be of assistance.

Parting Thoughts

The threat of malware and ransomware intrusions is something that security teams must face daily. Some may feel the pressure of a looming threat more than others; however, that does not disqualify the fact that all organizations should be ready for whatever may arrive at their door. However, amid all that preparation, how many organizations stop to take a good look at their defenses and see how their security investments are paying off for them?

In this survey, this question is something we kept at the center of our analysis. How can we assess the efficacy of a security team or their ability to respond to intrusions? More pointedly—how can we determine if malware/ransomware threats are reaching their final stages? To that end, we focused this survey on asking respondents about critical stages of an investigation, from initial access to actual data encryption.

As always, our survey provided unique insight into the current state of many organizations. Malware and ransomware threats are ever-present, but how teams prepare for, detect, and respond to these incidents differs from organization to organization. Our results showed that although adversaries might find certain levels of success, mindful security teams are watching closely and preparing for the next attack.

Sponsor

SANS would like to thank this paper's sponsor:

CrashPlan