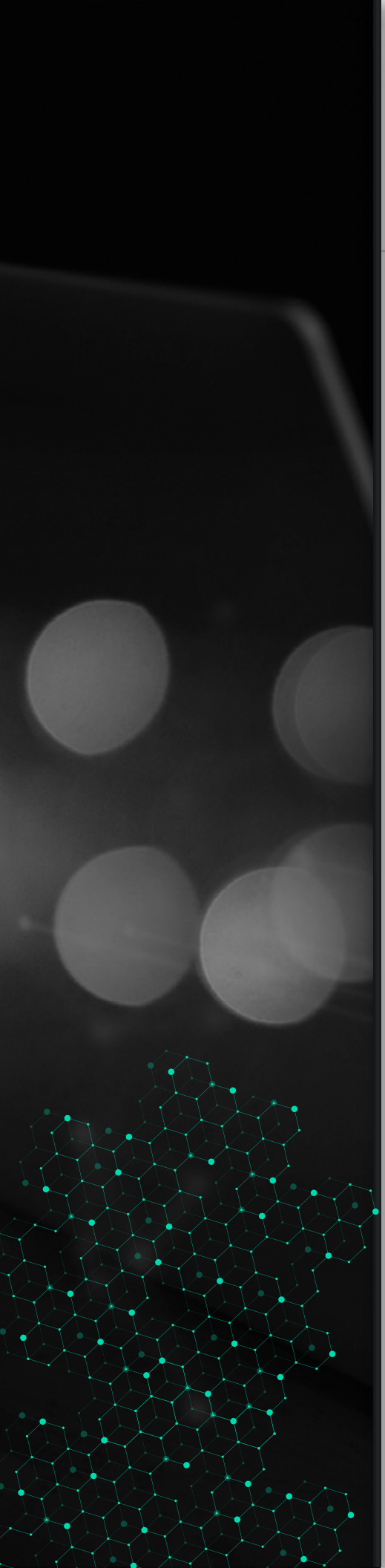
SpyCloud

MALWARE READINESS & DEFENSE **REPORT**

2023



SpyCloud

TABLE OF CONTENTS

GLOSSARY OF TERMS

AUTHENTICATION (OR SESSION) COOKIES OR TOKENS

When you log into a site or application, the server sets a temporary session cookie or token in your browser. This lets the application remember that you're logged in and authenticated. Many authentication cookies last a surprisingly long time (months or longer).

POST-INFECTION REMEDIATION

A critical addition to malware infection response playbooks, with steps that take remediation beyond clearing the device. By resetting the credentials and invalidating the active web sessions of exposed applications, the goal is negating entry points for ransomware by acting on initial access exfiltrated from the infected device and being sold to ransomware operators.

UNDER-MANAGED DEVICES

Corporate devices that aren't current on security updates, such as endpoint protection or anti-malware solutions.

SpyCloud

GROWING EXPOSURE FROM MALWARE INFECTIONS

Our digital-first lives, both personal and professional, fuel the rapid growth of information about each of our identities online – from credentials and other forms of authentication to personally identifiable information (PII). Despite us creating this world and the ever-evolving technology within it, keeping up with the fast pace of digital expansion seems to be humanly impossible – and organizations and individuals alike continue to fall behind in securing new ways of doing business. But cybercriminals don't have the problem of speed or agility; they innovate their technology and tactics as fast as the digital landscape evolves, including advanced ways to exfiltrate data and access quickly, long before their actions raise any red flags.

This criminal innovation has created a cybercrime epidemic that plagues organizations of all sizes. The cost of cybercrime is projected to **more than double** in the next five years, skyrocketing from an estimated $11.5 trillion globally in 2023 to $23.82 trillion in 2028. Cyber incidents not only **rank at the top** of business risks, but are also the most feared factor that causes business interruption. Much of this fear stems from the risk of ransomware.

Ransomware's potential to wreak havoc has **far-reaching implications**, and perhaps that's why it ranks as the **top cyber threat** that keeps security leaders up at night. However, devoting more resources to the problem doesn't seem to solve it. SpyCloud's **2022 Ransomware Defense Report** found growing pessimism among surveyed security professionals about their prospects of avoiding an attack, while the number of organizations that have been hit by ransomware in the past 12 months increased significantly.

GLOSSARY OF TERMS

SESSION HIJACKING (NEXT-GENERATION ATO)

In traditional **account takeover (ATO) attacks**, criminals use another person's login credentials, most often by leveraging reused or similar passwords from previously breached sites, to gain access to existing accounts. Increasingly, criminals are gaining access to accounts via **session hijacking** – or "next-generation account takeover." Using stolen authentication cookies exfiltrated from malware-infected devices to bypass any form of credential, from passwords to passkeys and even multi-factor authentication (MFA), criminals can impersonate the employee and gain access to private information with ease.

SHADOW DATA

Similar to the concept of shadow IT, this refers to sensitive data that is created, shared, or stored outside of the purview of the IT security team and is therefore not governed by corporate security policies. Shadow data can include corporate documents created on personal devices, sensitive data saved on external devices, or data stored from an application that is no longer in use, to name a few.

One of the biggest reasons for this losing battle is the proliferation of malware attacks, which reached **5.5 billion** last year. Malware-infected employee devices create a direct path into an organization as infostealer malware exfiltrates fresh, accurate data from target URLs, login credentials, passkeys, and authentication cookies/tokens to device and system information that enables easy impersonation. With this data, attackers can mimic employees' access with a high degree of success and perpetrate cybercrimes like account takeover, session hijacking, and ransomware attacks. Nearly half the darknet-exposed data that SpyCloud recaptured last year **came from botnets** (a common method for deploying infostealers) – and this trend is growing rapidly.

Although data siphoned by malware creates entry points for ransomware and is sold to ransomware operators as "initial access," most organizations stop short of remediating the full scope of malware infections. The lack of comprehensive Post-Infection Remediation can keep organizations exposed longer as malicious actors exploit still-valid exfiltrated data to launch targeted attacks.

In this report, we examine how organizations are currently addressing malware infections and identify opportunities to fill the gaps. As we note in our findings, the digital environment we all operate in increases the risk of malware while decreasing security teams' visibility into a growing attack surface. In addition to presenting the survey results, this report discusses the overlooked aspects of Post-Infection Remediation and what organizations can do to reduce their risk of the most damaging attacks resulting from malware exposure.

ABOUT THE SPYCLOUD SURVEY

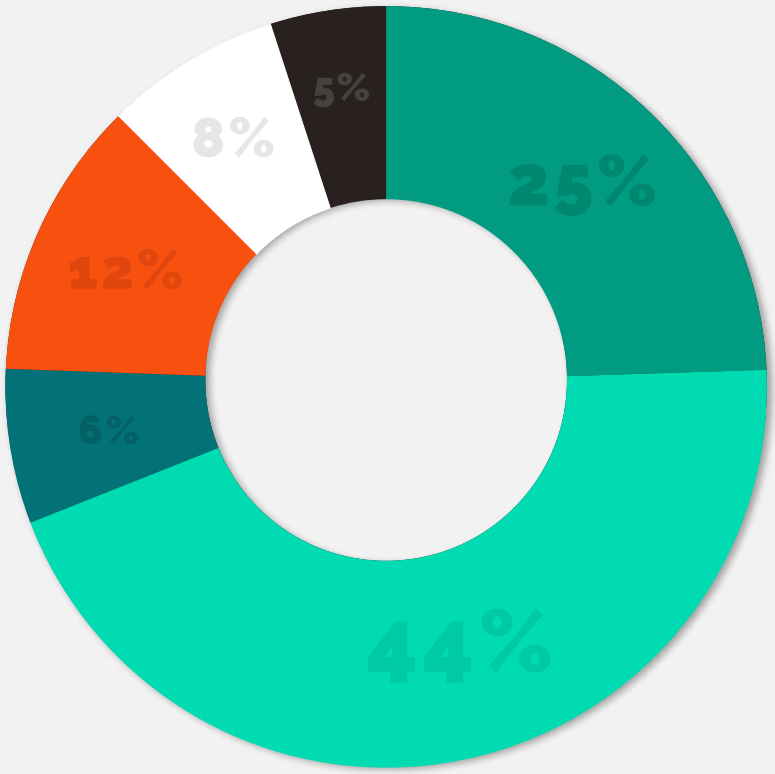
Our goal was to gain insights into current malware remediation practices and priorities among cybersecurity leaders and practitioners. We surveyed 317 individuals across the US and UK in active IT security roles at organizations ranging from 500 employees to more than 25,000.

The survey examined areas such as:

- Concerns about cybersecurity threats and malware exposure
- Security measures and incident response protocols
- Post-Infection Remediation capabilities and best practices

We solicited responses from practitioners including IT security analysts and incident responders, director+ leaders, and CISOs. Nearly a third of participants were security practitioners and others outside of leadership roles (Figure 1).

SpyCloud Figure 1 ▶

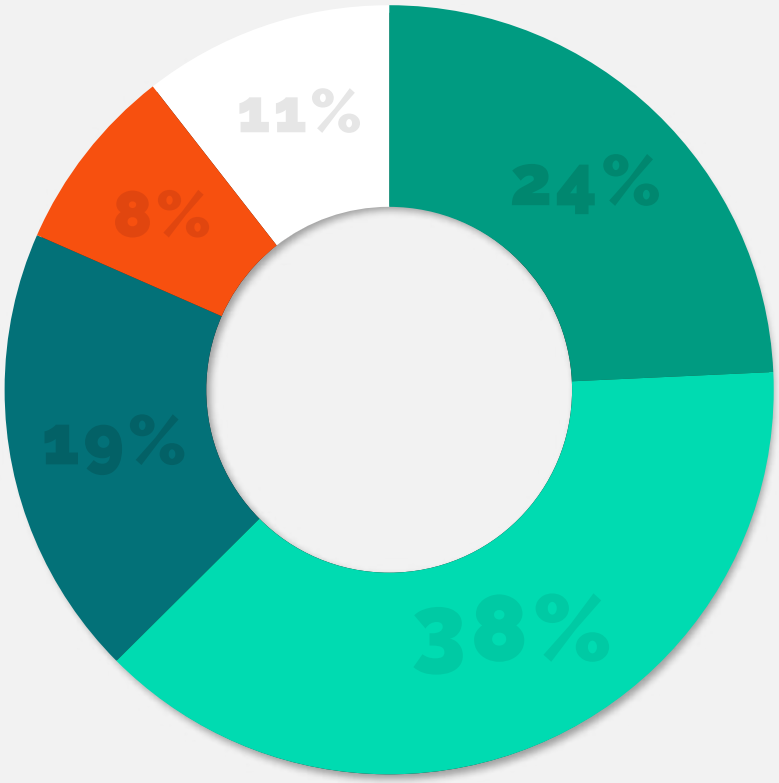


SURVEY PARTICIPANTS BY ROLE

- CIO, CISO, or IT security executive
- IT security director, manager, or team lead
- IT security architect / engineer
- IT security operator / analyst / incident responder
- IT security administrator
- Other role in IT security

Participants represented a cross-section of organization sizes, from mid-sized to very large enterprises, with organizations of 1,000-4,999 representing the largest cohort at 38% (Figure 2).

SpyCloud Figure 2 ▶



SURVEY PARTICIPANTS BY SIZE OF ORGANIZATION

- 500 – 999
- 1,000 – 4,999
- 5,000 – 9,999
- 10,000 – 25,000
- More than 25,000

KEY FINDINGS

1. Human behavior – intentional and unintentional – is the core risk driver.

With ransomware still looming as a top threat for security teams, our survey found that phishing is the second-highest threat that concerns organizations, indicating awareness that the human factor plays a big role in exposure. However, the lack of robust security practices and resources leaves gaps in defenses. The modern workforce expects ease and convenience, including the ability to access applications and data from anywhere with limited friction. Unfortunately, providing this convenience often sacrifices security. We found that many organizations continue to allow poor security practices, such as access to business applications by unmanaged or shared devices and the ability to sync browser data between corporate and personal devices.

2. The shifting digital environment creates a high risk of malware infections.

The shift to a digital- and cloud-first environment has changed the way employees work. In their quest for efficiency and improved productivity, they embrace a variety of third-party tools, but some of this adoption takes place outside of IT's control. Our survey discovered that more than 50% of organizations have employees setting up applications and systems without IT's consent. These "**shadow IT**" resources, coupled with a rise in employees and contractors accessing corporate resources on unmanaged and under-managed devices, create blind spots for security – not only in the context of access and application controls – but also in creating "shadow data." Consequently, organizations have limited or no visibility into these devices, nor into critical access and sensitive data that spans outside their control.

3. Organizations are worried about malware infections but lack adequate measures to remediate them.

An overwhelming 99% of those surveyed agreed that their organization is concerned about malicious actors' use of malware-exfiltrated data to perpetrate follow-on attacks such as account takeover and ransomware. However, many enterprises have gaps in their malware remediation or antiquated incident response practices that limit the scope of complete infection resolution, stopping short of critical steps like invalidating vulnerable web sessions for exposed applications and resetting passwords. Without visibility into malware on every device used by employees, contractors, and vendors – and without the people, tools, and time to properly respond to infections – security teams cannot keep up with this threat, which leaves the door open for malicious actors to attack again and again.

4. Infostealers are a growing concern – and a prevailing tactic that should be on every SecOps team's radar.

Security Operations (SecOps) teams appear alert to the infostealer trends: survey respondents ranked infostealers as their third top concern. Additionally, 98% agreed that better capabilities for gaining a clear picture of business applications at risk of infostealer-infected devices would significantly improve their security posture. Designed specifically to steal credentials and other forms of access from infected machines, infostealers are becoming increasingly common due to their ease of deployment, ability to scale, and high success rate. And recent reports regarding security **investigations** and incident remediations have found that malicious actors used stolen credentials more frequently in 2022 compared to the previous year, with an increased prevalence in both the use of infostealers and the purchasing of stolen credentials.

5

5. Current malware response practices leave gaps in Post-Infection Remediation.

Although awareness about the risk of infostealers is high, the same can't be said for organizations' ability to minimize the potential damage caused by this type of malware. Wiping clean a device doesn't completely eliminate the damage caused by such a malware infection. According to SpyCloud research, every infection exposes access to an average of 26 business applications. Detecting and acting on these exposures quickly is critical to disrupting malicious actors attempting to harm the organization. Yet this final step is a weak spot – organizations rank their ability to identify application exposure below other remediation steps. Our survey also found that more than a third of organizations don't reset application passwords and more than a quarter don't even review the application logs for signs of compromise.

THE RISK AND IMPLICATIONS OF MALWARE INFECTIONS

Ransomware has become such a severe problem in the past couple of years that **80%** of security leaders surveyed by the World Economic Forum called it an evolving and dangerous threat to public safety. And the **cost is escalating**: at $4.5 million, the average cost of a ransomware attack is higher than that of a data breach ($4.35 million), and that's not even counting the ransom.

Although **some research** suggests that ransomware attack rates have remained level in the past year, this hasn't eased the concerns of security leaders and practitioners. Our survey respondents ranked **ransomware as the top threat, followed by phishing/spear-phishing and infostealers** (Figure 3).

It's worth noting that these three threats go hand-in-hand: malicious actors may execute infostealer malware onto a device through a user falling prey to a malicious link or image in an email phishing campaign, and once devices are infected and user data or valuable corporate data is extracted, they can initiate the more complex ransomware attack – or sell that data to other threat actors who then do so.

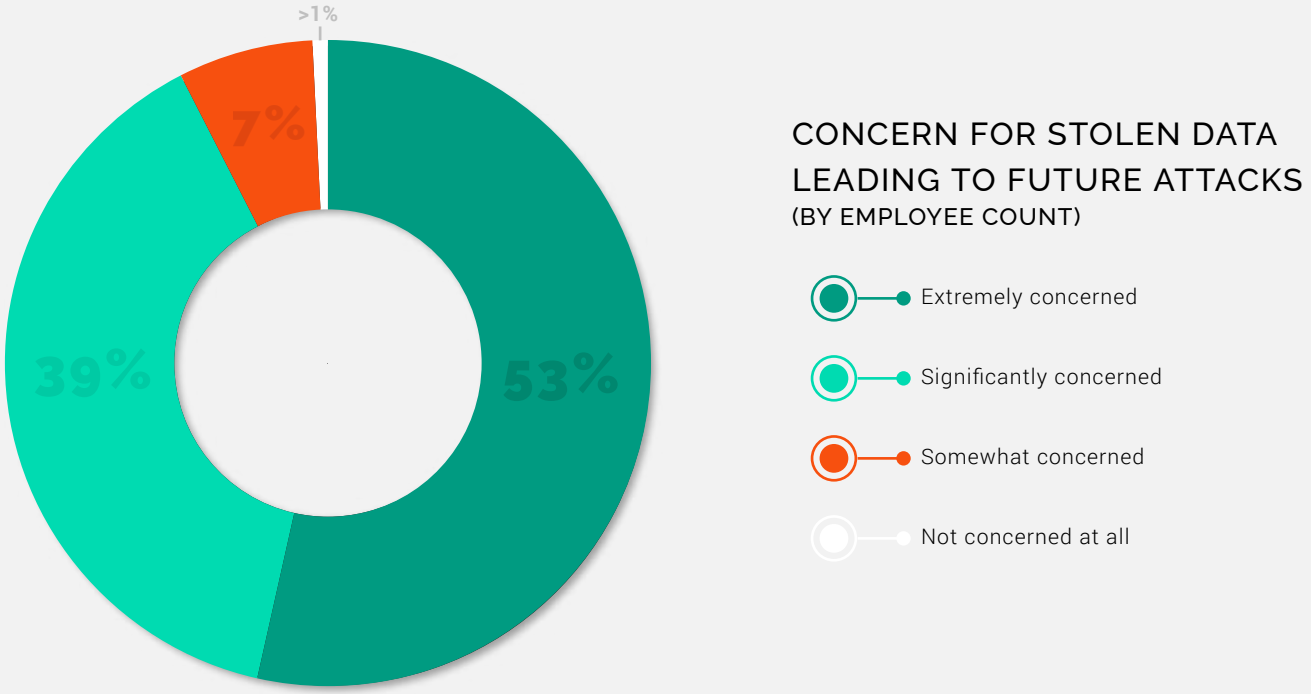
Furthermore, infostealer logs that contain stolen access to enterprise applications ranging from SSO instances to financial systems, customer databases, and code repositories have become abundant on the criminal underground, and entire marketplaces specialize in this type of "offering." One market alone, Genesis Marketplace, offered more than 430,000 stolen identities in 2022 alone, our research found. While shut down by law enforcement in early 2023, over the last 6 years Genesis provided stolen data to the tune of **80+ million** account access credentials specifically catering to initial access brokers (IABs), who sell guaranteed direct access via this stolen data to ransomware operators.

SpyCloud Figure 3 ▶

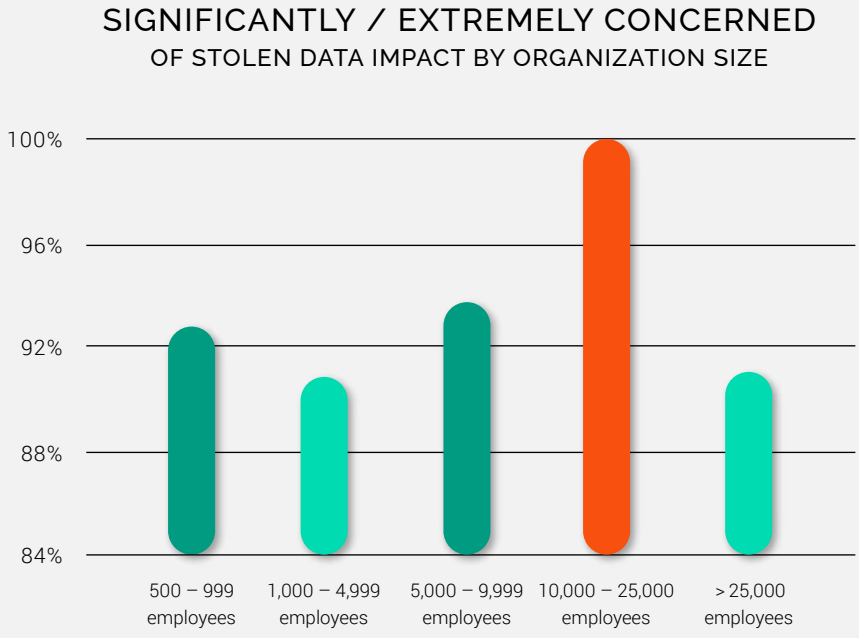
Malware a Big Concern for Organizations

Organizations have no illusions about the potential harm of malware, as our survey indicates. Less than 1% of survey respondents said they are not concerned about more harmful future attacks stemming from authentication, identity, session, and other data exfiltrated from infected devices, and 53% said they are extremely concerned (Figure 4).

SpyCloud Figure 4 ▶



While larger organizations often have better defenses due to more resources and more sophisticated practices, size doesn't appear to make a difference here: compared to the average across all size categories, respondents from enterprises with 25,000 or more employees were only slightly less concerned about stolen data leading to future attacks (Figure 5).



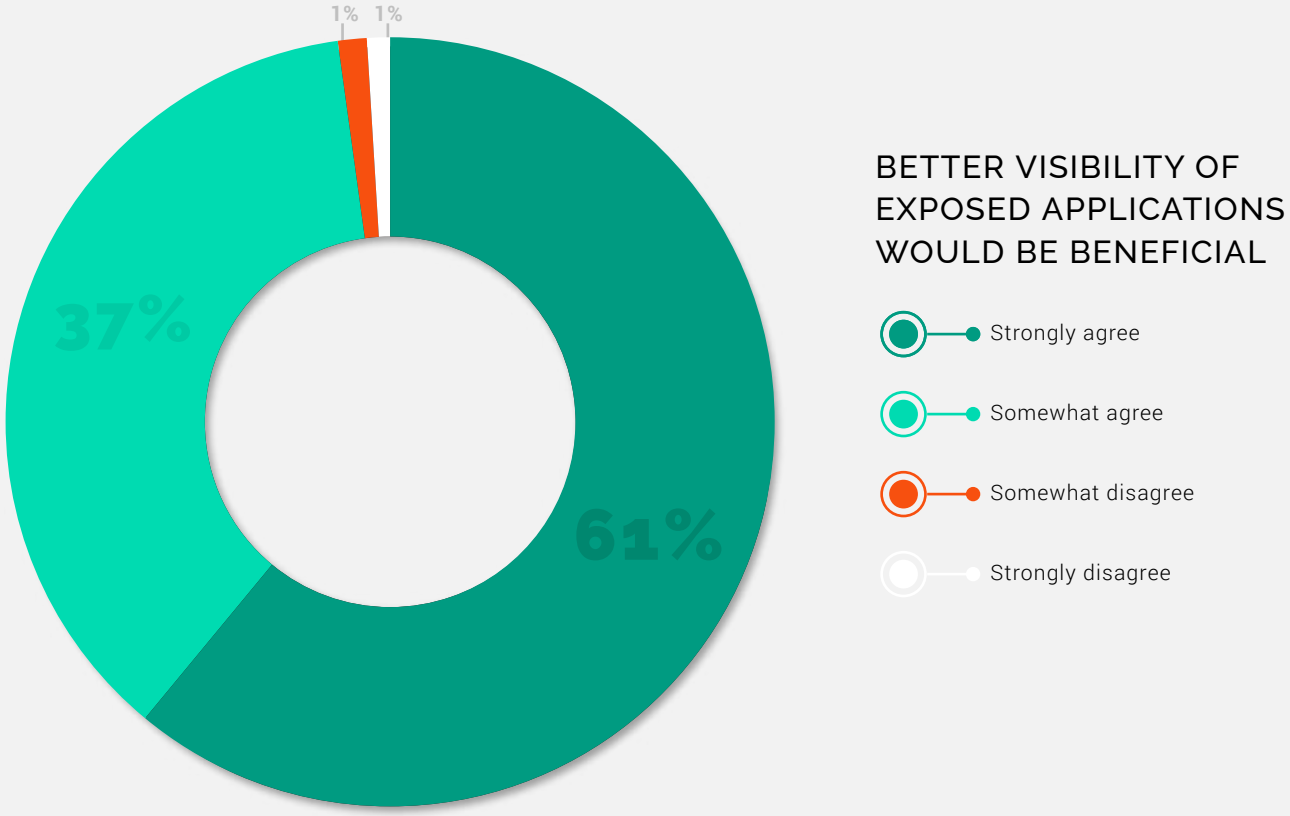
SpyCloud Figure 5 ◀

This fear is not unfounded. Last year, SpyCloud researchers recovered 721.5 million exposed usernames and password combinations from the criminal underground, with **48.5%** exfiltrated from malware-infected devices (and the remaining leaked in third-party breaches). In addition, malware logs contain other credentials including authentication cookies – which enable malicious actors to **hijack a session** without providing a password, passkey or second factor – impersonating the employee, gaining unfettered access to valuable systems and networks, and creating opportunities to perpetrate costly, damaging cyberattacks.

Lack of Visibility Hinders Progress

While concern is high, visibility into this risk seems low: 98% of respondents agreed that having better visibility into the business applications exposed by an infostealer infection would increase security posture (Figure 6). This is an area where organizations need to prioritize. They must figure out how to solve the visibility problem, because any efforts to reduce the risk of exposure will remain ineffective for as long as this gap exists.

SpyCloud Figure 6 ▶



HUMAN FACTOR: THE COMMON THREAD

AS WE HIGHLIGHTED IN KEY FINDINGS, human behavior – intentional or not – is at the core of every organization's risk. Malicious insiders still raise concern for security leaders, but our survey participants ranked them as the fifth highest threat behind unwitting insider threats from employees, contractors, and other trusted insiders who could potentially cause a lot of harm simply by being careless. All it takes is for an internal user to click on the wrong email link while not paying attention for cybercriminals to take full advantage of the access they have. Adversaries are counting on this cavalier behavior: the number of phishing attacks has grown by **150%** every year since 2019, with 2022 a record year for phishing.

In this robust age of hybrid work, actions that may seem benign to employees, such as accessing corporate applications from a personal device or downloading an app without IT's permission, also open the door to ransomware and other attacks.

Next-Generation Account Takeover Is Here and Not Going Away Soon

We were surprised to learn that account takeover is not a big concern for organizations, ranking second-to-last out of nine categories. Ransomware may be holding much of security teams' attention, but next-generation account takeover (ATO) resulting from malware infections should still be considered a high risk. Session hijacking – a form of next-generation ATO – originates from the takeover (or "hijack") of a session using a stolen, still-valid authentication cookie to appear as a verified clone of a legitimate employee. This method goes beyond traditional credential exposure and expands the data criminals can now use to assume the access of an authenticated user. Criminals leverage these active sessions to exfiltrate data, and monitor and mimic user behavior patterns. **Last year alone, SpyCloud researchers recaptured 22 billion stolen cookie records**, which indicates criminals are shifting tactics to steal, buy, and trade this highly accurate and highly valuable data, minimizing their need for larger breach data sets that may be clouded with old, out-dated, and for their purposes, somewhat useless data.

Personal or shared devices, for example, typically have much weaker security than those managed by the organization.

If an employee unsuspectingly logs into corporate applications from a personal device infected with an infostealer, the malware will siphon all credentials, whether personal or business, along with other identity and device data that bad actors can use to impersonate the employee and infiltrate the organization. All this activity flies under the SecOps team's radar – and a serious cyberattack like ransomware may be the first sign that something was amiss.

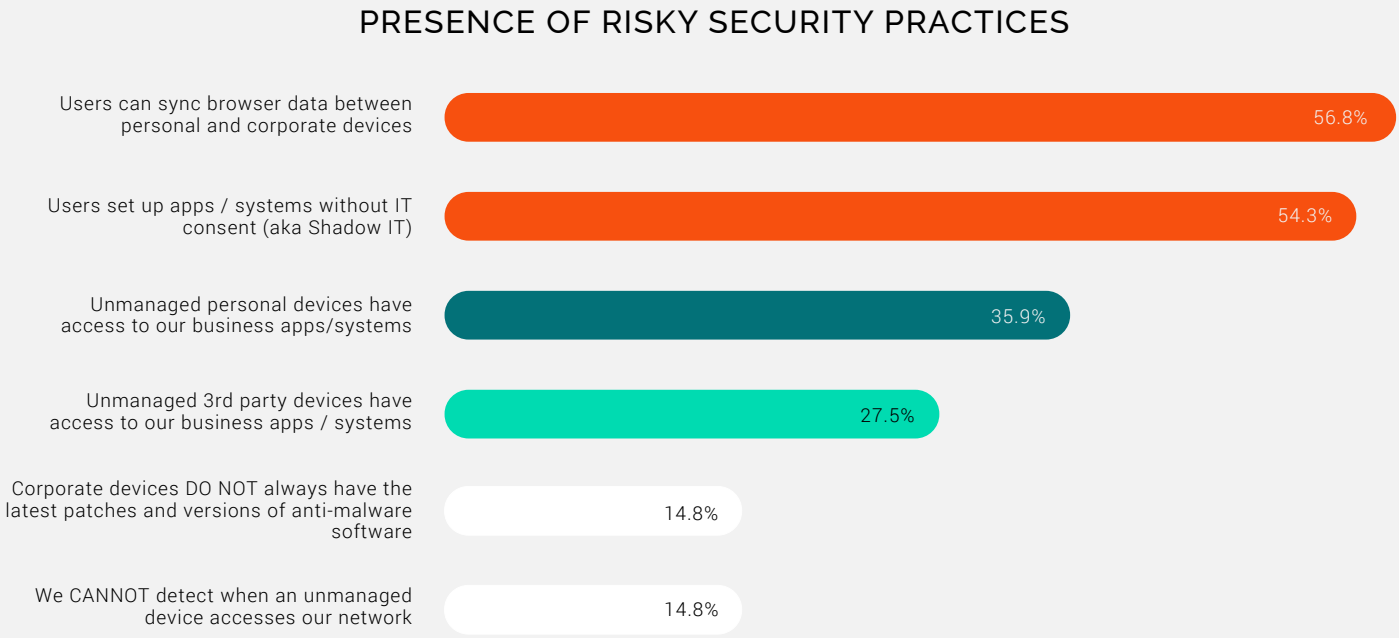
Employee security awareness and education programs are a common tactic for organizations looking to fortify their human defenses. Unfortunately, these programs don't seem to be making enough impact: while employees may be aware of threats and best practices, it doesn't mean they're changing behaviors and it really falls back to the IT and security teams to make sure they have stopgaps in place at every stage.

OVERLOOKED ENTRY POINTS THAT LEAVE ORGANIZATIONS EXPOSED

The lines between personal and professional spaces have been blurred the last 3+ years, with no end in sight. **More than 70%** of surveyed employers have shifted to hybrid work models, where it's easier for risky cyber practices to slip through the cracks. Digital workplaces continuously heighten security risks due to the fast-paced changes in technology. As tech evolves, employees' digital-first lives – which call for convenience, ease, and minimal friction – are scaling beyond the IT and security teams' control and impacting security posture.

Our survey reflects these trends, indicating that security teams struggle to keep pace with the evolving workplace (Figure 7). In particular, we found that:

- **57% of organizations allow employees to sync browser data between personal and corporate devices.** While this practice provides convenience for users, it allows malicious actors to steal corporate credentials (including authentication cookies) through infected personal devices without being detected and without the user even being aware this is the entry point to begin with.
- **54% of organizations struggle with shadow IT due to employee adoption of applications and systems without IT's consent.** Not only does IT lack visibility into these unsanctioned tools, oftentimes employees use consumer-grade apps that don't have basic security controls and corporate policies are not strong enough or non-existent to minimize or stop this access.
- **36% of organizations allow unmanaged personal devices to access business applications and systems, and 27% do the same for third-party devices.** Both of these practices are risky because of the lack of IT and security control, as well as the high likelihood that the unmanaged devices have lax security measures, such as removed or non-existent authentication requirements – increasing an already sprawling attack surface.



'Good Enough' Really Isn't

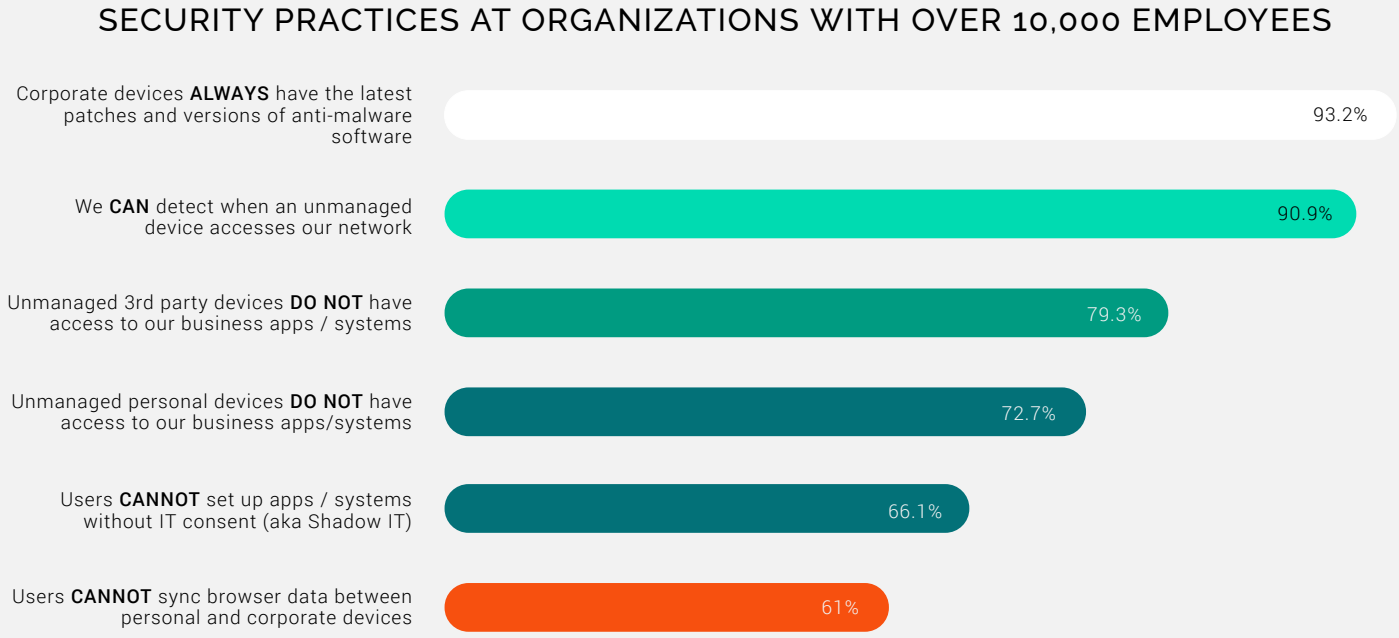
While 85% of organizations believe their corporate devices have the latest patches and anti-malware software, that leaves 15% who don't, according to the SpyCloud survey respondents (Figure 7). Patching and keeping devices up-to-date is a critical best practice, yet security teams shouldn't allow themselves to have a false sense of security simply because they have checked that box. "Checking the box" solutions and practices may have been good enough in the past, but can no longer keep pace with the evolving threats and criminal tactics.

Having the latest patches doesn't necessarily mean the organization is safe. According to recent SpyCloud research, for the first 6 months of 2023, **20% of all SpyCloud recaptured malware logs had an antivirus program installed at the time of successful malware execution** – meaning the tool did not in fact stop the infection (also known as producing a false negative). While these tools serve a valuable purpose in the first line of defense, they are not, and never will be, a stopgap for criminals who are deploying advanced infostealer malware that is purpose-built to bypass anything from basic antivirus to robust authentication methods like MFA and passkeys.

Large Enterprises: More Mature, But Still at High Risk

Larger organizations do have a little better control over their exposure (Figure 8), which reflects a more mature security strategy. But having better control doesn't eliminate risk, especially since bigger organizations are a bigger target for attackers. Additionally, with enterprises' greater use of third-party vendors and contractors and the ability for employees to leverage personal devices for corporate access, unmanaged or under-managed devices increase the risk because a single malware-infected device can give attackers access to dozens of corporate applications.

SpyCloud Figure 8 ▶



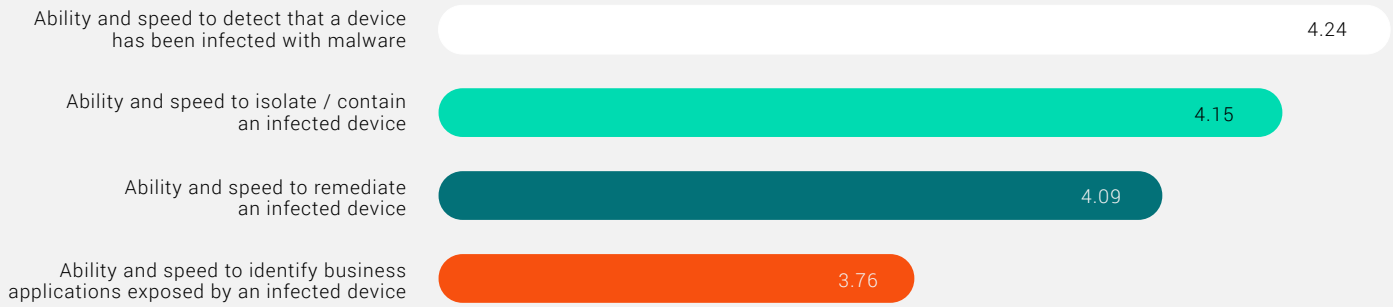
Gaps in Malware Response Capabilities

Despite exposure from malware, organizations have limited ability to identify business applications affected by an infection. Our survey found that organizations have much stronger capabilities in malware detection and the first phases of response than in the later stages of remediation (Figure 9), which includes identifying what third-party business applications have had credentials exfiltrated by an infostealer.

SpyCloud Figure 9 ▶

MALWARE DETECTION AND RESPONSE CAPABILITIES

SCALE OF 1 (LOWEST) TO 5 (HIGHEST)

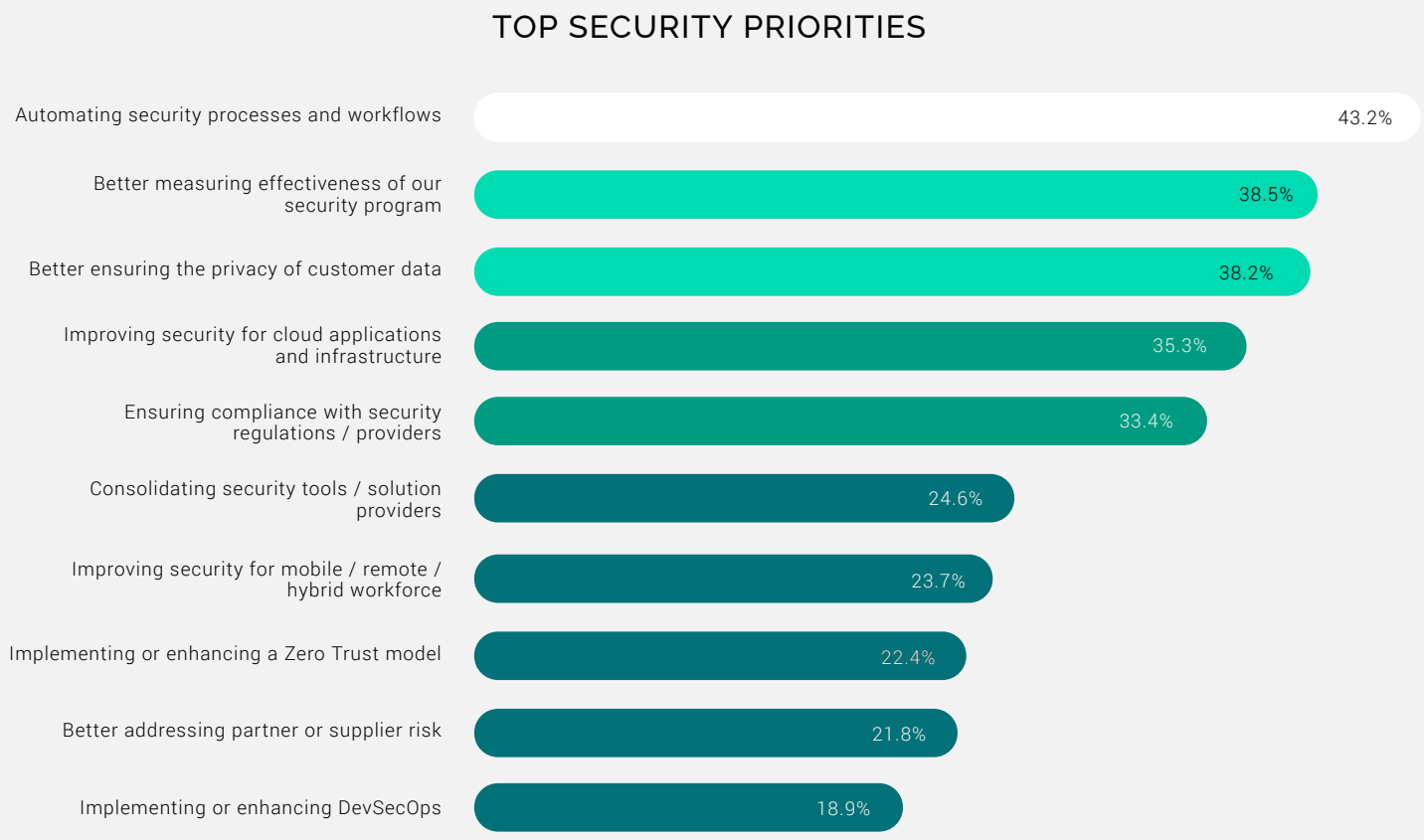


SecOps survey participants may feel good about their ability to work with their IT counterparts to detect an infected device, isolate, and remediate it as they understand it today; however, with digital identities at the center of today's workplace, remediation shouldn't stop at the device. A "reset it and forget it" mentality is no longer a viable option. To truly reduce the risk of ransomware, organizations must move beyond the traditional, machine-centric malware response to an identity-centric approach that encompasses complete Post-Infection Remediation steps that reduce risk associated with compromised applications.

POST-INFECTION REMEDIATION PRIORITIES AND CAPABILITIES

Workflow automation has been a growing priority for SecOps in past years, and the current economic conditions may further emphasize that need. A recent survey of CISOs found that economic uncertainty has negatively impacted security budgets for **58%** of organizations. Given this environment, we were not surprised to see automation of security processes and workflows rank as the highest priority in the next 12 to 18 months, identified by 43% of our survey participants (Figure 10). Even with the difference in priorities between leaders and practitioners, automation is in the top three for each group.

SpyCloud Figure 10 ▶



In addition to automation, the other top two priorities – better measurements of security effectiveness and better customer data protection – suggest that security teams are highly interested in improving outcomes and boosting security efficiencies. To get there, organizations must first eliminate silos across teams, systems, and data – and doing so requires converging technologies to obtain a single source of truth, leading to better prevention and remediation.

Security leaders and practitioners ultimately want the same thing – better security – yet they see different paths for getting there. And it seems quite clear that their larger role-based objectives of strategic versus tactical goals mirror our findings. We found that:

- Leaders are focused more on better measurement of security effectiveness, better customer data privacy, and automation, while SecOps practitioners and admins place more emphasis on compliance, cloud security, and automation.

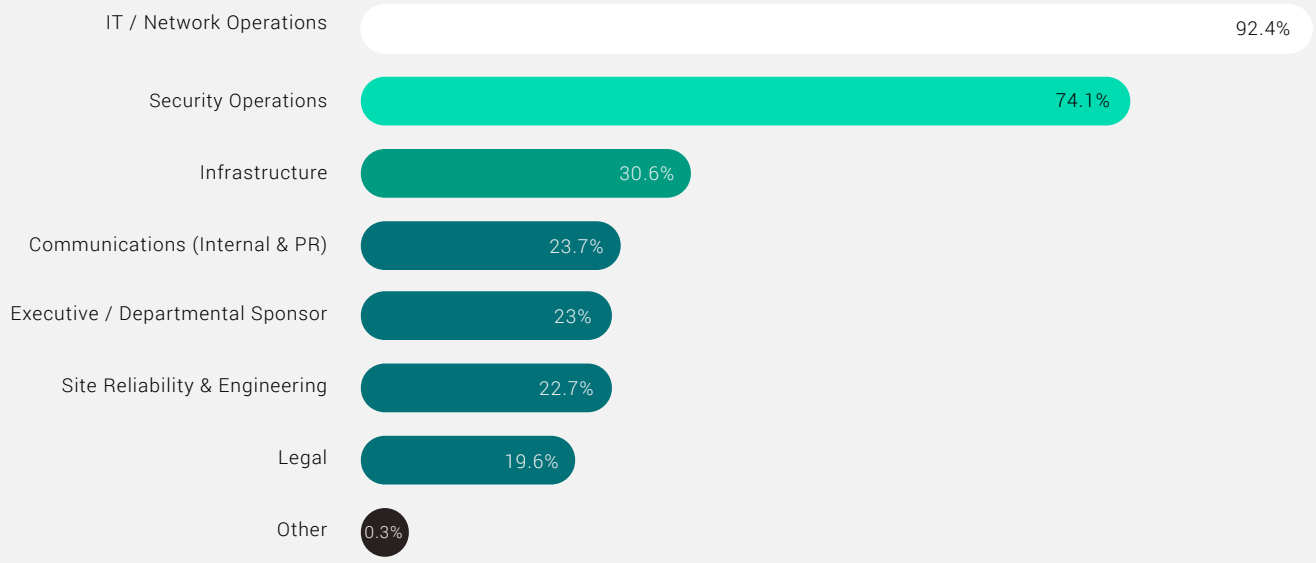
- Security architects and engineers, by far, prioritize improving cloud application and infrastructure security (60%). Last year, SpyCloud recovered millions of third-party application credentials harvested by malware that give access to over 56,000 popular cloud-based applications such as communication, collaboration/project management, and common human resources tools. This data emphasizes that the cloud continues to be top of mind in organizations' quest for digital transformation, but cloud-based applications also create higher risk in workplaces that embrace a digital experience; therefore, organizations must prioritize cloud security.

We were surprised to see third-party risk receive such little attention from our survey participants, landing second to last on the list of priorities. This ranking shows a disconnect with the malware concerns discussed earlier, especially considering how many organizations have third-party devices connecting to their applications and systems. Research shows that **59%** of surveyed organizations have experienced a cyberattack or data breach due to a third party. But organizations lack visibility into a commonly overlooked supply chain component: under-managed vendor devices that access their valuable systems, networks, and applications. To mitigate risk stemming from vendors' or contractors' malware-infected devices, security teams need the same level of visibility outside their organization as they have inside.

Traditional Malware Drains Resources

For most organizations, malware response is not limited to SecOps. It's a team effort that requires the involvement of multiple core business areas, from IT, network operations and engineering to compliance and legal (Figure 11). With a minimum of seven departments involved in this process, the cost can add up quickly – which perhaps explains why automation is such an urgency for organizations. Streamlining remediation can free up headcount and cost center resources, as well as protect organizations from the unseen costs of an attack, such as damage to brand reputation and loss of business.

PERSONNEL / TEAMS INVOLVED IN MALWARE RESPONSE PROCESS



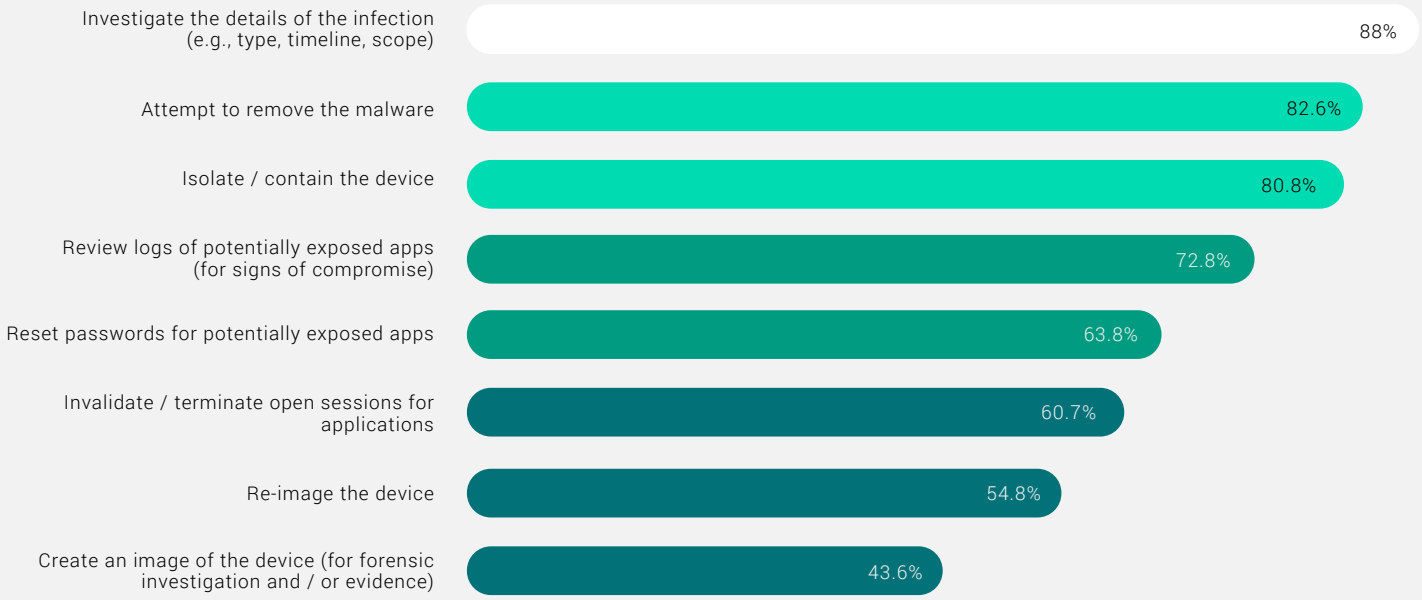
Routine Responses to Malware Infections – What's Missing?

Attacker dwell time has been **growing** according to recent research, providing malicious actors ample time for actions like operationalizing data exfiltrated by malware. One of the best ways to decrease mean-time-to-discovery (MTTD) and mean-time-to-remediation (MTTR) is by gaining a complete picture of all applications compromised by an infection, including the target URLs, siphoned sessions cookies/tokens, and stolen credentials. Taking action on the exact access stolen by attackers can shorten the time the business is at risk of additional data exfiltration and disrupt cybercriminals' ability to launch follow-on attacks, as well as lessen the burden of malware infection response on cross-team resources.

However, many organizations struggle in this area. We found that **27% don't routinely review their application logs for signs of compromise, 36% don't reset passwords for potentially exposed applications, and 39% don't terminate session cookies at the sign of exposure** (Figure 12).

SpyCloud Figure 12 ▶

ROUTINE RESPONSES TO MALWARE INFECTIONS



Compounding the problem is the lack of visibility across the environment in the first place. As we noted earlier, nearly a third of organizations don't have a good handle on their corporate managed devices, to say nothing of those that are unmanaged and under-managed. The BYOD trend may be saving operating costs and boosting employee productivity, but if the cost is compromised security, are the net gains truly beneficial in the long term?

CHANGING THE PARADIGM

Ransomware is a multi-faceted problem that remains a consistent threat. In their **2023 Data Breach Investigations Report,** Verizon found that ransomware appeared to stay statistically steady, involved in just under a quarter (24%) of breaches in comparison to last year, and persists regardless of existing layers of defense organizations have in place to combat it. But many organizations don't realize that ransomware is *really* a malware problem.

Bad actors are exploiting infected systems to exfiltrate data that can aid a ransomware attack, identify potential entry points to corporate resources, and deliver executable files. The challenge is that businesses lack visibility into infostealer malware infections on managed, under-managed, and unmanaged devices accessing the network – and the workforce applications that are exposed as a result.

Remediating applications compromised by malware infections can greatly improve the ability to stop malicious actors in their tracks. However, traditional malware response practices are not standing up to the fast-paced evolution of the threat landscape, technology, and the digital workforce.

For most SecOps teams, responding to a malware infection on an employee's device is about the endpoint itself – a machine-centric process that involves identifying the malware-infected device, isolating the user and device from the network, and reimaging the device. At best, this severs the initial connection with the cybercriminal, but doesn't account for the stolen credentials, cookies, and other means of access that are already in adversary hands and will make their way onto darknet markets – perpetuating the cycle of cyberattacks long after the device is clean. Additionally, more malware developers are crafting their malware to steal information without leaving forensic artifacts on the victim's device, otherwise known as non-persistent malware, which leaves little to no trace – and therefore nothing that would inform defenders about the type of infection encountered.

To borrow from a famous quote, **organizations simply can't do the same things yet expect different results.** It's time for a paradigm shift from machine-centric to identity-centric remediation.

An identity-centric approach disrupts ransomware and other attacks by going beyond traditional malware response to remediate exposure beyond the device, with affected users and applications at the forefront. **Post-Infection Remediation** is a series of additional steps in a malware infection response framework designed to negate opportunities for ransomware and other critical threats by resetting the application credentials and invalidating session cookies siphoned by infostealer malware.

But what's required for this to work is visibility into exactly what access has been stolen, so security teams can direct their efforts (in an automated way) to slamming the door on malicious actors and thwarting the opportunity for cybercrimes against the business. Doing so minimizes resource and budgetary constraints with a more concerted effort that takes the best and most effective protocols from existing playbooks and enhances them to stay one step ahead of cybercriminals and the growing underground market.

POST-INFECTION REMEDIATION STEPS

1. ISOLATE THE DEVICE
2. IDENTIFY THE DETAILS
3. CREATE AN IMAGE
4. REMOVE THE MALWARE
5. RESET CREDENTIALS
6. INVALIDATE SESSIONS
7. REVIEW APPLICATION INTEGRITY

FINAL THOUGHTS

When all was said and done, survey respondents made it clear that organizations view infostealer malware as a threat, but gaps remain to achieve a properly robust and comprehensive response:

- Malware is one of the top three threats organizations face, along with ransomware and phishing/spear phishing, all of which can be used in concert with each other to harm your business.
- The most overlooked entry points for malware are synced browser data across personal and corporate devices, shadow IT, and unmanaged devices accessing business applications.
- When it comes to malware response, organizations are most confident in the first phases of response aligned to the device, but less confident in the latter stages of response related to the risk from exposures tied to the malware victim's identity.

While security leaders and practitioners are aware of the threat of malware, organizations remain at risk due to the use of unmanaged and under-managed devices that can greatly impact ransomware defenses. As our digital lives continue to expand and the human element remains a key factor in malware attacks, SOC teams struggle to keep up with the innovative ways criminals gain access to their organization through tactics like session hijacking using malware-exfiltrated authentication cookies.

Almost all of our survey respondents agree: having full visibility into the business applications at risk from infostealer-infected devices would enhance their security framework. Yet, organizations ranked the ability to identify what third party business applications have had credentials exfiltrated by an infostealer *last* in their malware detection and response capabilities. This disconnect validates the need for complete Post-Infection Remediation, which involves not only wiping and reimaging the device, but also ensuring that all compromised access resulting from the infection is addressed.

With full visibility into an infostealer infection and the ability to act on stolen authentication data, enterprises can find power and process to remediate infections with confidence, proactively prevent ransomware, and sleep a little more soundly at night.

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, protect their business from consumer fraud losses, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to nearly 200 cybersecurity experts whose mission is to make the internet a safer place.

To learn more and see insights on your company's exposed data, visit **spycloud.com**.