POST-INFECTION REMEDIATION GUIDE

A New Paradigm for Preventing Ransomware

SpyCloud

Table of CONTENTS

WHY WE NEED A NEW APPROACH TO PREVENTING RANSOMWARE

The cost of cybercrime to businesses in the U.S. during 2021 was nearly **$7 billion**, with ransomware a vast contributor. As a result, ransomware is on the minds of everyone from policymakers to security teams, and even boards of directors. In 2022, more than **four billion** malware attempts were recorded and ransomware attempts surpassed totals from four out of the last five years, making it clear that no company is too small or large to be targeted and no industry is immune. It has become a topic of conversation at all levels of every enterprise – and ransomware prevention is a growing portion of cybersecurity budgets.

Despite **86%** of businesses increasing their security budgets to fight these attacks, **90%** of businesses we surveyed told us they were affected by ransomware in the last 12 months, with most two or more times. Organizations realize that threats are slipping through their defenses, making ransomware attacks seemingly inevitable.

Ultimately, ransomware is a malware problem. Often, bad actors use information or access which was gathered through malware infections as the basis for ransomware attacks. Attackers are exploiting infected systems to exfiltrate data that can aid an 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. Without knowledge of infected devices, users, and applications that criminals can exploit to essentially walk right into the business, security teams cannot reduce the high risk of a successful ransomware attack.

> “Organizations may not be aware that undetected malware infections on personal devices represent a risky gap in ransomware prevention strategies. Once the siphoned data is circulated on the dark web, criminals can use it for more destructive activities – including their next ransomware attack .
>
> **TED ROSS**
> SpyCloud CEO & Co-Founder

Critical Blind Spots That Put Organizations at High Risk of Ransomware Include:

- Lack of visibility into credential and identity data circulating on the darknet, including malware-stolen authentication data for critical workforce applications that leave the door open for attackers to access, steal, encrypt, or wipe corporate data.
- BYOD policies that **allow** employees to access corporate applications on unmanaged and personal devices, as well as vendors and contractors with lax controls on managed devices, which extends the attack surface for adversaries.
- The use of shadow IT on managed and unmanaged endpoints, including productivity and development tools that house sensitive corporate data with no oversight.
- Incomplete malware infection response frameworks that end when a compromised device is reimaged.
- Browser-based synchronization functionality allows criminals to siphon sensitive enterprise credentials through employees' personal devices without ever tripping alarms.

It's clear we need a new approach to truly reduce the risk of ransomware.

In this guide, we'll shed light on how to close the gaps in malware infection response to stem the tide of costly follow-on cyberattacks. We'll start by explaining how infostealers have become the starting point in the ransomware attack lifecycle and then providing concrete steps to disrupt cybercriminals by implementing a new approach to ransomware prevention: SpyCloud Post-Infection Remediation™.

HOW INFOSTEALERS HELP CRIMINALS HARM ORGANIZATIONS

An infostealer is part of a malware toolkit that can be easily purchased and enables cybercriminals to siphon login credentials, host names from browsers and FTP clients, browser cookies, autofill data, credit card information, crypto wallet details, files with specific extensions, chat history, lists of installed programs and running processes, the machine's globally unique identifier (GUID), and more.

Once cybercriminals gain this information, they have many choices in how to operationalize it:

Sell the Logs on Darknet Marketplaces

Malware-siphoned data is extremely valuable because it's so accurate. Among other things, malware logs contain plaintext credentials and means of bypassing multi-factor authentication (MFA).

Criminals who sell this information include actors known as **Initial Access Brokers (IABs)**, a term to describe the individuals or groups who package and sell access to networks that are guaranteed to work. Their results speak for themselves; for instance, Genesis Market was **allegedly used by criminals** in June 2021 to breach Electronic Arts (EA). They purchased compromised login and cookie data, allowing the criminal to impersonate an EA employee via their Slack login and deceive IT support through social engineering. IABs also operate outside of public forums and markets, selling access directly to other criminals in Telegram, Jabber, Signal, and Discord channels or direct messages.

> **Without data from infostealers, follow-on attacks become substantially more difficult. The infostealer is the central tool in the modern criminal's arsenal.**
>
> **TREVOR HILLIGOSS**
> Former DoD Special Agent & FBI Cyber Task Force Member; Current Senior Investigator at SpyCloud

Use the Information Themselves

Malware-stolen data grants access into the victims' work and/or personal accounts for the purpose of committing fraud and perpetrating cyberattacks, including ransomware.

When a malware victim is identifiable as an employee, the criminals may set their sights on infiltrating the organization – putting the victim's data to use to become indistinguishable from the employee. This data enables easy bypass of MFA and facilitates access to corporate accounts, files, and systems.

- **Use Stolen Credentials for Account Takeover**: With the credentials siphoned from the infostealer, criminals can take over accounts not protected by secondary verification, like an authenticator app.

- **Use Stolen Cookies for Session Hijacking**: With cookies in hand, criminals can authenticate as the legitimate user, bypassing MFA to access an active web session. In 2022, SpyCloud recaptured tens of billions of cookies from the darknet – underscoring the scale of the data available to criminals – and began delivering it to customers as an **automated feed** to enable quick invalidation of compromised sessions.

Criminals are increasingly deploying malware that may allow persistent access to a device or enable a tunnel through a trusted network. When combined with the device fingerprint collected by the infostealer, attackers may also be able to simply emulate that device themselves if they don't have persistent access. They may also side-load a more persistent malware alongside a non-persistent infostealer to establish rootkits (re-attack ability).

Needless to say, malware attacks allow cybercriminals to easily bypass network defenses to encrypt and/or steal data, which results in serious financial and reputational damage. The average ransomware attack costs businesses **north of $1 million** in recovery from operational disruptions and loss of data and services. But for data breaches stemming from ransomware attacks, **IBM** reported an average cost of $4.54 million – not including the ransom.

And according to a Gartner® report, "The cost of recovery and resulting downtime in the aftermath of a ransomware attack, and the cost of the reputational damage, can amount to 10 times the amount of the ransom itself." [1]

[1 Gartner, How to Prepare for Ransomware Attacks, Paul Furtado, 16 June 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved]

WHAT'S IN A MALWARE LOG?

Infostealer malware logs provide cybercriminals with a treasure trove of stolen data siphoned from infected devices. Practically speaking, malware logs are folders of files created from information stolen off a victim's device. Some of the most common data includes device information – allowing an attacker to "fingerprint" a victim's device – as well as URLs visited, the credentials used to log into accounts, form auto-fill data, session cookies, cryptocurrency information including private keys, and other stealer-specific data. Some newer infostealers, like the Rhadamanthys Stealer, which was first observed in October 2022, even have the ability to copy files from an infected device.

INFECTED MACHINE INFORMATION

This is a robust set of data about the victim's device, including the operating system, processing power, processes running, and installed software. This helps the cybercriminal determine which systems are vulnerable to additional exploits and allows an attacker to craft a fingerprint for future emulation.

CREDENTIALS

Modern infostealers come equipped with modules that are capable of reading the databases used by browsers to store credentials. This gives the cybercriminal a wealth of data to sell or use to gain access to the network and move laterally, and/or exfiltrate sensitive corporate data.

COOKIES

Session cookies authenticate users on a given website for a period of time. By using an anti-detect browser with a browser plugin, criminals can easily import stolen cookies to hijack a user's session, bypassing MFA, and taking over the account without the need for credentials – essentially becoming a clone of that employee in your environment.

An analysis of malware logs recaptured by SpyCloud in 2022 indicated an average of 26 unique enterprise applications are exposed per employee infection.

HOW A MALWARE INFECTION LEADS TO RANSOMWARE

JON

STEP 1 MALWARE INFECTS DEVICE

Malware is mistakenly downloaded on a device used to access corporate resources.

STEP 2 DATA SIPHONED

The malware siphons Jon's passwords, cookies, device information, browser fingerprint, and other data that can be used to impersonate him.

STEP 3 DATA SOLD ON DARKNET

Jon's stolen data is bought or traded in the darknet, where initial access brokers or ransomware operators find it.

STEP 4 BUSINESS BECOMES A TARGET

Initial access brokers identify that Jon's data included personal and corporate assets. They provide the data to ransomware operators who target Jon's employer.

STEP 5 CRIMINALS INVADE COMPANY

Ransomware operators use Jon's compromised authentication data to log into corporate resources, bypass MFA, and move laterally to increase their access while evading detection.

STEP 6 RANSOMWARE DEPLOYED

Ultimately, the bad actors use their illegitimate access to deploy ransomware and demand a ransom payment in exchange for access to the enterprise's files.

SpyCloud

COMMON BLIND SPOTS IN TODAY'S MALWARE INFECTION RESPONSE

SpyCloud's most recent **Ransomware Defense Report** found a year-over-year decrease across the board in the number of respondents satisfied with their existing ransomware mitigation technologies – a growing list encompassing data backups, phishing detection, endpoint protection, UEBA, user awareness training, and threat intelligence, among others.

Threats continue to slip through, and gaps remain despite these many layers of defense. Furthermore, malware is evolving so quickly that most antivirus solutions can't keep pace with new strains that bypass regular scans. It is little surprise that most organizations feel less confident in their cyber defense strategies as ransomware attackers continue to find success.

What's not being adequately addressed in most anti-ransomware frameworks is proper malware infection response. Despite how thorough your processes may be for identifying and remediating the effects of a malware infection, you can't fix what you can't see. Most organizations lack insight into infections on unmonitored or personal devices. They often underestimate their risk from under- managed devices and the exposure of third-party applications that fall outside the visibility of existing monitoring tools.

Browser-Based Sync Functionality

All modern browsers include synchronization features to make it easy for users to move between devices and keep their bookmarks, browser history, and passwords available. While this is convenient for the user, it opens a virtually undiscoverable hole for cybercriminals to steal sensitive enterprise credentials.

Even if a work device is properly secured, if the employee enables syncing their browser information on both their work and personal devices, all saved work credentials are available on personal devices in home networks that are likely insecure. Once a home machine is infected with malware, the stealer is able to access the saved enterprise credentials through that open hole without the enterprise ever seeing anything in its EDR, SIEM, or firewall logs.

Unmanaged Devices

69% of organizations estimate that at least half of all devices on their enterprise network are unmanaged devices, outnumbering managed devices on their network three to one. Work habits have changed over the past few years, with remote work so common now that it accounts for up to **25%** of all professional jobs in North America. It's also hard to imagine employees *not* accessing work email, a sales CRM, or chat on a personal device. So it's easy to understand why in one survey, **79%** of managers reported they are extremely concerned with the risks posed by unmanaged and IoT devices, and another study found that **67%** of organizations have experienced a security incident as a result of their usage.

Under-Managed Devices

To the dismay of security teams everywhere, employees fall behind on security patches on their devices, putting them into the “under-managed device” category. As many as **40%** of workers responding to a recent survey believe it’s not their responsibility to update their work device, or cite fears of privacy violations, bugs, or preferring to wait to see if any errors result from others installing the updates before they do so – practically ensuring that some security patches are missed.

Add to this, **56%** of people admit to allowing friends and family to use their work-issued device to shop, game, or stream. Security teams are facing the reality that corporate-issued devices are increasingly used as an entry point for cyberthreats.

Third-Party Vendors and Contractors

There also exists an entire category of devices owned by third-party vendors and contractors, which may lack the protections required by the employing enterprise. Many recent ransomware attacks originate from a device not owned by the company but ones that have some level of privilege into their corporate domain, often to perform a contracted task, such as website or app development. A recent survey found that **59%** of organizations experienced a data breach or cyberattack that was caused by a third party.

If your company employs contractors or has partners or suppliers accessing the network, how confident are you in their security measures? Are they mandating system updates in a timely manner? Are they upgrading their endpoint protection regularly? Do you have visibility into their protocols and how can you enforce them?

> “
>
> **SpyCloud identified a malware infection on a device used by a contractor working remotely overseas. Their endpoint protection (EPP) was not updated, and even after updating the EPP, they did not find the malware. This confirms the risk most companies have with third-party vendors since we truly cannot measure the efficacy of the controls of such vendors who access our systems.**
>
> **- CISO**
> Financial Institution

Third-Party Applications

Password managers, security tools, collaboration apps, CRM and marketing automation platforms, chat, ticketing systems, learning platforms, HR and payroll systems – this is where work gets done. However, these applications fall outside the scope of traditional security monitoring tools and threat intel feeds that alert you to potential exposures of your owned domains – not third-party or subdomains.

Potentially even more concerning when it comes to malware are exposures of authentication data for VPN and SSO – the latter of which serves as a gateway to dozens of applications. In fact, Okta – which integrates with over 7,000 cloud, mobile, and web apps – **reports** that organizations have 89 applications deployed on average (with larger companies of 2,000+ employees using 187 on average). A single malware compromised SSO instance might be as good as an open door to the enterprise.

Shadow IT

Shadow IT continues to grow with the countless tools and applications available, such as SaaS-based productivity tools, integrations, development tools/platforms, data warehousing, and business intelligence applications. These are installed on managed and unmanaged devices without IT or security operations knowing about them, and often corporate user IDs are used to create an account. Company data stored in these applications is already problematic, existing outside of corporate control, but the risk skyrockets when the app credentials and cookies are siphoned by an infostealer.

An Incomplete Process

Going back to the idea that you can't fix what you can't see, a lack of visibility into the exposed applications resulting from infostealer infections lends itself to an incomplete malware infection response. For most security operations teams, responding to a malware infection on an employee's device is an endpoint, machine-centric process:

IDENTIFY
the malware-infected device

ISOLATE
that user and device from the network

REIMAGE
the device

But, at best, this simply severs the connection with the cybercriminal – it 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. Additionally, more malware developers are crafting their malware to steal information without leaving forensic artifacts on the victim's device to inform defenders on the type of attack encountered.

> **The result is a false sense of security that leaves the door open for attackers to access, steal, encrypt, or wipe corporate data from critical workforce applications, like code repositories, password managers, customer databases, financial systems, SSO, and more.**

And of course, the incompleteness of current malware infection response is complicated by the lack of visibility into compromised applications resulting from infections on unmanaged and under-managed devices.

So, what can be done to truly reduce your enterprise's risk of cyberattacks like ransomware stemming from malware infections?

POST-INFECTION REMEDIATION: A MORE COMPLETE APPROACH

Post-Infection Remediation (PIR) is SpyCloud's new, critical addition to malware infection response that exists because it's now possible to understand and visualize the full scope of the infection's threat to your business.

Post-Infection Remediation is a paradigm shift from a machine-centric SOC process to an identity-centric one. This is necessary because long-term ransomware risks cannot be reduced by simply wiping an infected device and closing the service ticket. Truly reducing the risk of a critical cyberattack can only occur as a result of remediating all compromised applications. That requires having a complete picture of the target URLs, stolen credentials, and session cookies siphoned from infected machines that can allow ransomware operators to "walk right into" your network.

As we shared earlier, our analysis of malware data recaptured from the darknet in 2022 reveals that 26 unique enterprise applications are affected per infected device, on average, leaving a great deal of open doors for criminals to encrypt and steal company information.

Simply put, PIR 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.

This approach to more complete malware infection response is enabled by SpyCloud. We alert security teams each time a malware infection arises on a device accessing your workforce applications. The alerts deliver definitive evidence of entry points to your organization: detailed information about the device, along with the siphoned authentication details for the applications that matter to your business – password managers, security tools, marketing and customer databases, learning and collaboration applications, and HR and payroll systems, to name a few.

As a result of Post-Infection Remediation, you can disrupt cybercriminals attempting to harm your business, significantly shorten your exposure window for ransomware and other critical threats, and effectively stop malware exposures from becoming full-blown security incidents.

WHAT ARE THE STEPS IN POST-INFECTION REMEDIATION?

The following is an addendum to your malware-infection response plan which can be incorporated into your existing runbooks.

Malware infections can have serious repercussions that last long after a device has been cleaned or reimaged. Without actioning the stolen third-party app logins to prevent their use in future ransomware attacks, the result is a false sense of security that leaves the door open for attackers.

The goal of PIR is to mitigate your organization’s risk from exposures related to the malware victim’s identity. Doing this requires your security team to evolve from a machine-centric incident response process to an identity-centric process.

To stop ransomware attacks resulting from the use of malware-stolen data, follow the steps outlined below:

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

1. ISOLATE THE DEVICE

If the detected infection has occurred on a device you can manage, disable the network access of the infected endpoint to help prevent potential lateral movement. This access can often be restricted using the quarantine features of an endpoint detection and response solution, through the corporate domain, VPN and/or SASE configuration, or may sometimes require an individual to manually disable network access. If your organization uses asset tags on corporate devices, be sure employees know they can call the listed phone number if they are locked out of their device and unsure of what to do. If you don't use asset tags, incorporate them going forward and be sure they include a "disaster recovery" phone number.

2. IDENTIFY THE TYPE, SCOPE, AND TIMELINE OF THE INFECTION

If you have access to the system, it is highly recommended to review endpoint security logs or run a modern antivirus solution to detect the specific malware family involved. Once the malware type has been identified, consult security tools (such as VirusTotal) to confirm the typical behavior of this malware and the risk it brings to your organization.

Modern malware is often immune to traditional methods of identification through Indicators of Compromise (IOCs) like hash values, as executable files are often unique to each victim and Command and Control (C2) infrastructure may be dynamic and rotate quickly. You may also need to include behavior-based detection, such as validated YARA rules, in your detection process.

Many malicious programs will attempt to spread across local domains or networks and infect other devices. Closely review the networked devices and file systems that the user and device had access to, forming an action plan to determine if, and when, the actor attempted to access other corporate resources. If you suspect lateral movement, consider expanding your scope during the isolation process.

3. CREATE AN IMAGE OF THE INFECTED SYSTEM

If this infection becomes a point of concern in a follow-on attack, it will be extremely useful to have an image of the entire system disk. Once the device has been isolated from the network, create a system image. This can be used in follow-on forensic analysis, should it be required.

4. REMOVE THE MALWARE - IF POSSIBLE

Use your company-sanctioned detection and remediation tools to remove potentially side-loaded, persistent malware like cobalt strike beacons. And while you also have the option of recovering or reinstalling the operating system, it may be best to reformat the hard disk and perform a fresh installation of the operating system or reimage the computer.

Some forms of malware are very sophisticated and move quickly, instantly installing, stealing data, including credentials from browser password managers and cookies, and uninstalling themselves before your antivirus software can catch them. If this occurs, the malware will already be gone from the device, but you will still need to remediate the exposed applications.

5. RESET PASSWORDS AND USERNAMES FOR AFFECTED APPLICATIONS

Ensure the employee signs out of all devices – particularly on corporate applications which may have privileged access into your domain. Ask the employee to use a device that isn't infected by malware to immediately reset their passwords for applications whose credentials were siphoned by the malware. Advise the employee to never use a compromised password or any variation of it again and be sure to set a unique, complex password for each application (preferably using a company-provided password manager).

If possible for high-profile users, consider the laborious effort to change compromised employee SSO usernames to reduce the impact of a potential password familiar to the threat actor from being reused by that employee in the future.

If you are a SpyCloud customer, this list of exposed applications and credentials is available via your Enterprise Protection license, and visible in the Compass module.

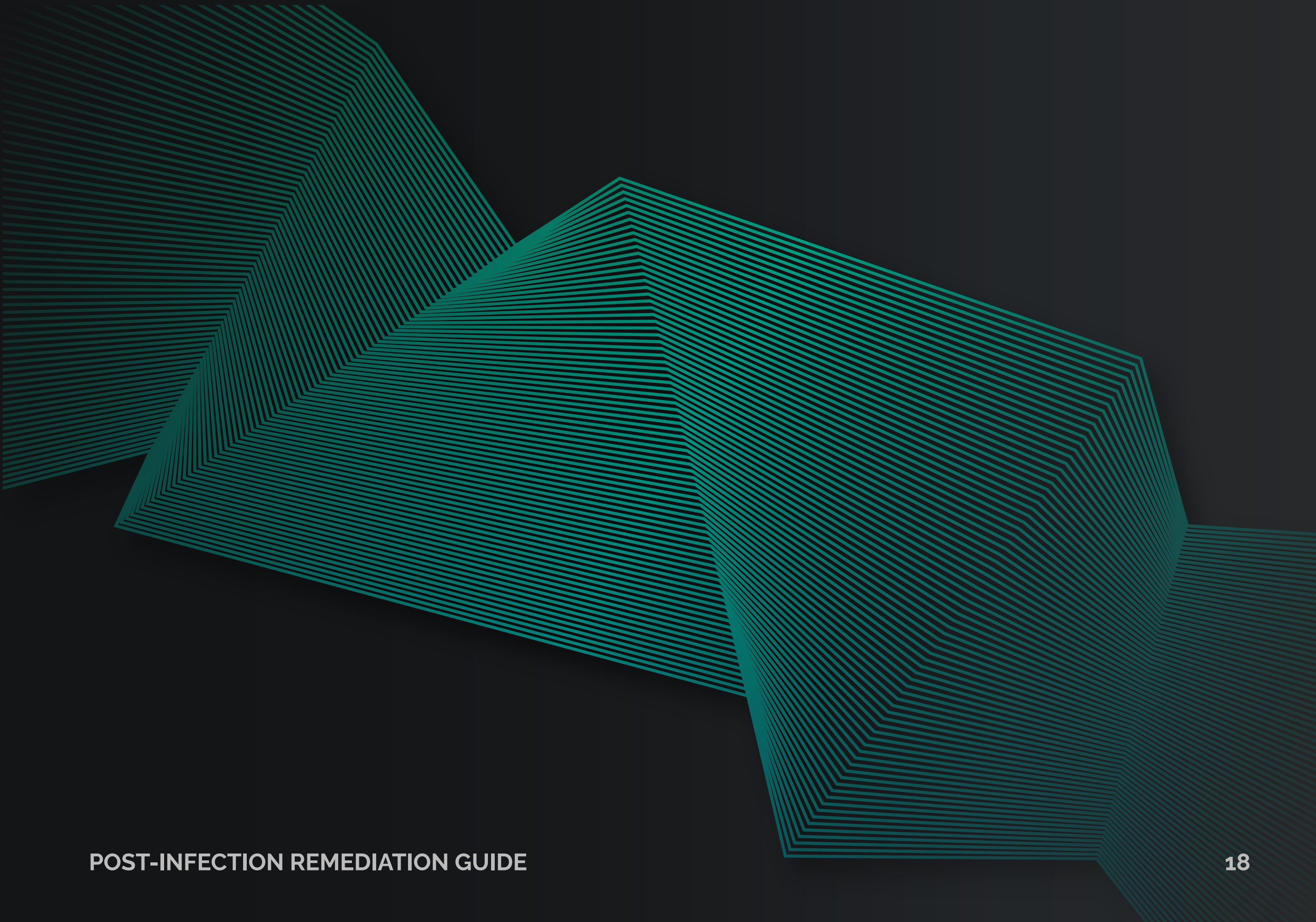
6. INVALIDATE SESSIONS

In addition to stealing credentials, information-stealing malware also siphons device and web session cookies, potentially leaving the victim's accounts vulnerable to session hijacking through device impersonation. Changing the application password does not guarantee active user sessions or trusted device tokens will be invalidated. It may be necessary to contact the third-party cloud service provider and request that the compromised user sessions be invalidated.

7. REVIEW THE INTEGRITY OF IMPACTED APPLICATIONS

Starting with the list of impacted applications outlined in steps 5 and 6, review all activity and access logs for the associated users within these applications. Confirm all detected activity is coming from expected IP address ranges and geographies, and all behavior fits the expected profile of the user. Similar analysis should be performed for all associated domain users.

Any access to sensitive data, whether it is expected or not, should be closely scrutinized and if it is determined to be unexpected, should be treated as an incident and the company's incident response plan should be activated.



EXAMPLES OF POST-INFECTION REMEDIATION WITH SPYCLOUD

#1 Invalidating Active Stolen Sessions to Prevent Session Hijacking

Scenario A: Customer Database (CRM) Exposure

A sales representative becomes infected with malware. SpyCloud alerts the security team to all session cookies that were siphoned from the device. As a part of the Post-Infection Remediation process, the security team discovers the session cookie for the organization's CRM is still active. The organization is at high risk of a cybercriminal bypassing the victim's CRM login and MFA, and gaining access to confidential customer information. The security team immediately contacts the CRM Admin and asks them to follow the steps below to secure the sales rep's account and lock out the cybercriminal. Once the sessions have been invalidated and the device has been wiped, the sales rep will be prompted to login again and a new, secure session is administered.

SpyCloud-Enabled Post-Infection Remediation Steps:

The security team should swiftly notify the employee of the malware infection and isolate their device. After removing the malware:

Invalidate Sessions and Revoke OAuth Tokens

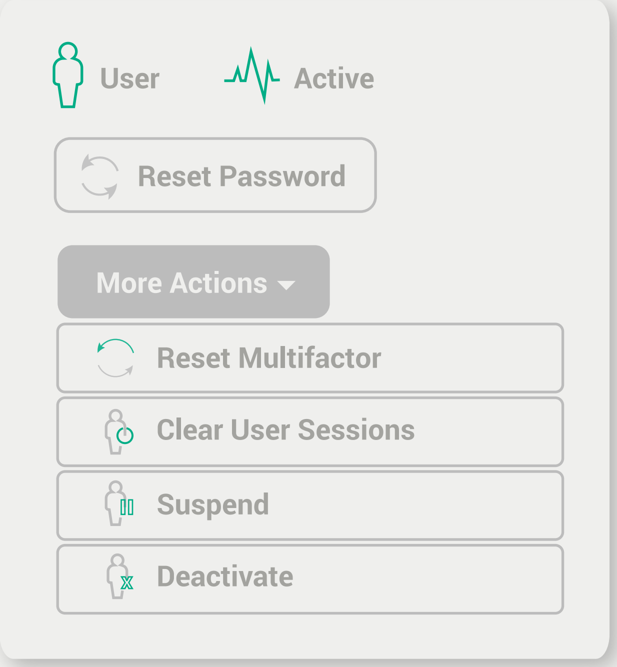
To stop a criminal from using an **anti-detect browser** and a stolen cookie to bypass authentication measures, active session cookies must also be cleared. Tokens granted from an authentication flow should also be revoked. Each CRM will have specific instructions for clearing sessions.

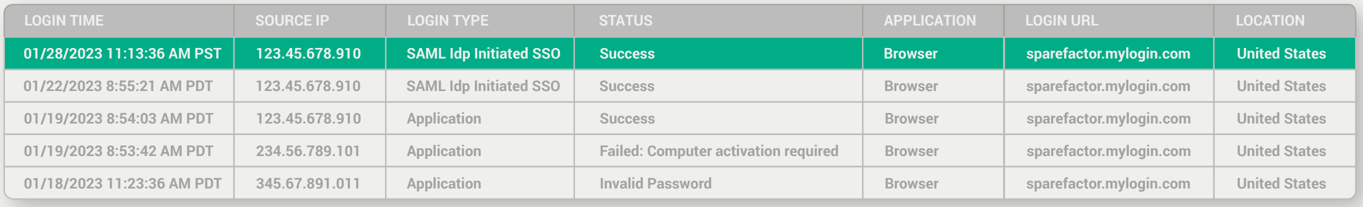
Force Password Resets and Enable MFA

Require the user to reset their password and enable MFA, if it wasn't already required.

Monitor/Review Login History

Periodically review all login attempts and activity for the user, including the date, time, IP address, and method of login (e.g. SSO) to identify attempts that appear suspicious.





LOGIN TIME	SOURCE IP	LOGIN TYPE	STATUS	APPLICATION	LOGIN URL	LOCATION
01/28/2023 11:13:36 AM PST	123.45.678.910	SAML Idp Initiated SSO	Success	Browser	sparefactor.mylogin.com	United States
01/22/2023 8:55:21 AM PDT	123.45.678.910	SAML Idp Initiated SSO	Success	Browser	sparefactor.mylogin.com	United States
01/19/2023 8:54:03 AM PDT	123.45.678.910	Application	Success	Browser	sparefactor.mylogin.com	United States
01/19/2023 8:53:42 AM PDT	234.56.789.101	Application	Failed: Computer activation required	Browser	sparefactor.mylogin.com	United States
01/18/2023 11:23:36 AM PDT	345.67.891.011	Application	Invalid Password	Browser	sparefactor.mylogin.com	United States

Scenario B: Single Sign-On Exposure

An organization leverages SSO to enable users to access many corporate applications via one set of credentials. An HR manager is infected with infostealer malware, allowing the cybercriminal to acquire a session cookie for the SSO instance, which then gives them direct access to dozens of other applications, including the payroll system, benefits service (housing sensitive employee PII), the applicant tracking application, and much more. As a result, the criminal gains access to data that can be sold to ransomware operators to use for employee impersonation, or more directly, in attempts to divert payroll to a criminal's account.

SpyCloud-Enabled Post-Infection Remediation Steps:

The security team should swiftly notify the employee of the malware infection and isolate their device. After removing the malware:

Invalidate SSO Sessions

Clear the user's sessions on all devices, which invalidates the cookie siphoned by the malware and will lock the bad actor out of the SSO portal that grants access to multiple corporate applications.

Reset SSO Password

Require the user to reset their password.

Review Access Logs

Review the user's activity and access within the scope of the application. Confirm that all access was driven by the user and coming from their expected IP addresses and devices.

Repeat Steps 1-3 for Each Application Accessible via SSO

Because the malware siphoned an active SSO session cookie that enables access to every application in the SSO portal, the organization must assume that all applications the HR manager had access to are compromised. Clear the sessions and require password resets for each, and periodically review the login histories for suspicious activity.

#2 Identifying Compromised Applications and Resetting Credentials

Scenario: Project Management Application Exposure

A project manager at an organization becomes infected with malware and SpyCloud alerts the organization that the credentials for 20 workforce applications have been exposed as a result. The security team instantly recognizes that one of the applications houses the enterprise's codebase, which includes an unreleased, game-changing product still in beta phase. Criminals put high price tags on product and engineering teams' data, knowing not all organizations back up their codebase and the losses could be catastrophic. Criminals move quickly when infiltrating networks, encrypting files, and demanding ransom, sometimes also threatening to alter or leak source code.

SpyCloud-Enabled Post-Infection Remediation Steps:

The security team should swiftly notify the employee of the malware infection and isolate their device. After removing the malware:

Check Exposed Code Base for Stolen Keys

Confirm no private keys were in any of the potentially impacted code repositories. If keys are discovered, change them.

Invalidate Sessions

Clear the user's sessions for the affected applications on all devices.

Reset Passwords

Require the user to reset their password for each affected application.

Review Access Logs

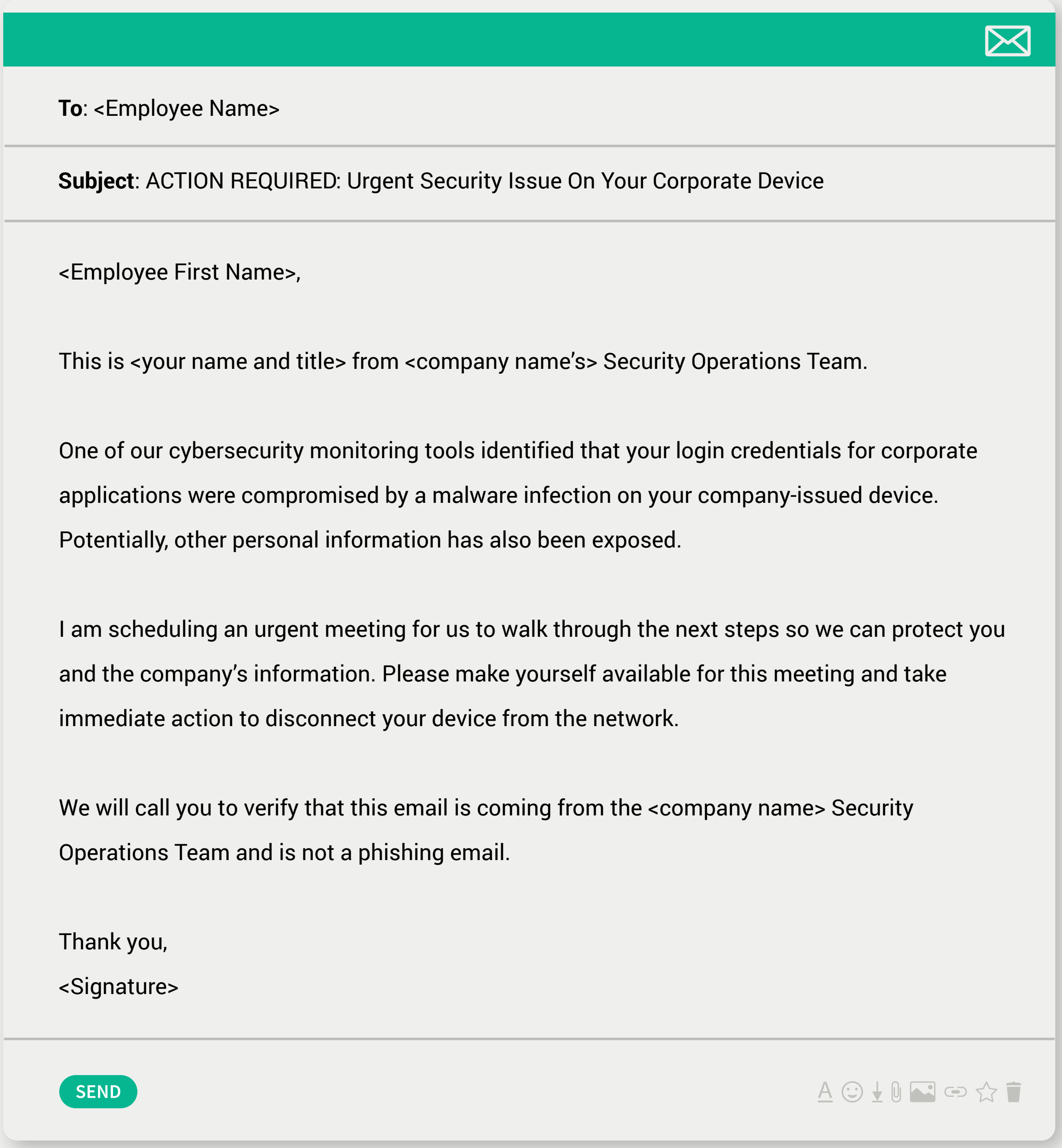
Review the user's activity and access within the scope of the application. Confirm that all access was driven by the user and coming from their expected IP addresses and devices.

It is crucial to note that resetting credentials before wiping the device is not enough. Many malware families use keyloggers to recapture the new credentials once they have been updated, creating an endless cycle of unknowingly keeping entry points to your network open.

COMMUNICATING WITH EMPLOYEES USING A MALWARE-INFECTED DEVICE

We recommend keeping templated emails on hand so you can quickly alert employees when a malware infection is detected on a device they are using to access corporate applications. Here are sample email templates to get you started.

Corporate Device Malware Infection Email Template



To: <Employee Name>

Subject: ACTION REQUIRED: Urgent Security Issue On Your Corporate Device

<Employee First Name>,

This is <your name and title> from <company name's> Security Operations Team.

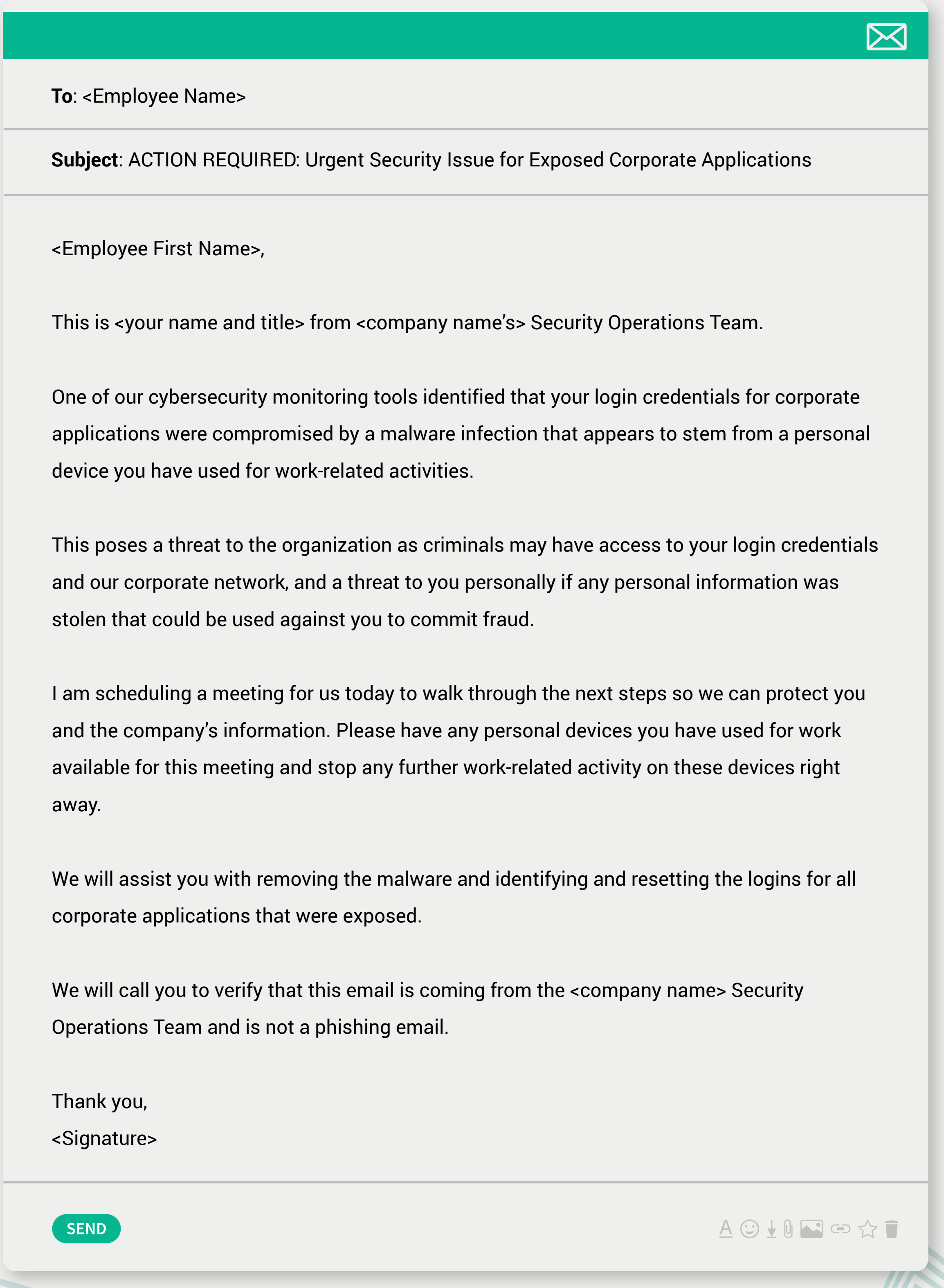
One of our cybersecurity monitoring tools identified that your login credentials for corporate applications were compromised by a malware infection on your company-issued device. Potentially, other personal information has also been exposed.

I am scheduling an urgent meeting for us to walk through the next steps so we can protect you and the company's information. Please make yourself available for this meeting and take immediate action to disconnect your device from the network.

We will call you to verify that this email is coming from the <company name> Security Operations Team and is not a phishing email.

Thank you,
<Signature>

Personal Device Infection Email Template



To: <Employee Name>

Subject: ACTION REQUIRED: Urgent Security Issue for Exposed Corporate Applications

<Employee First Name>,

This is <your name and title> from <company name’s> Security Operations Team.

One of our cybersecurity monitoring tools identified that your login credentials for corporate applications were compromised by a malware infection that appears to stem from a personal device you have used for work-related activities.

This poses a threat to the organization as criminals may have access to your login credentials and our corporate network, and a threat to you personally if any personal information was stolen that could be used against you to commit fraud.

I am scheduling a meeting for us today to walk through the next steps so we can protect you and the company’s information. Please have any personal devices you have used for work available for this meeting and stop any further work-related activity on these devices right away.

We will assist you with removing the malware and identifying and resetting the logins for all corporate applications that were exposed.

We will call you to verify that this email is coming from the <company name> Security Operations Team and is not a phishing email.

Thank you,
<Signature>

HOW SPYCLOUD DISRUPTS CYBERCRIME

Enabling Post-Infection Remediation

We created SpyCloud Compass to help security teams protect their business from ransomware and other critical threats using insights from recaptured malware data. Compass provides definitive evidence that stolen data tied to your organization is in the criminal underground, enabling you to properly remediate hard-to-detect malware infections that serve as common precursors to ransomware attacks.

Compass fills the gaps left by traditional application, network, and endpoint security tools by identifying exposed users and applications from malware infections on both managed and unmanaged devices. By mapping infected devices to exposed users and accounts, Compass provides SOC teams with the details they need to visualize the scope of each threat at-a-glance, reduce manual investigation steps, and move quickly from detection to response. This gives security practitioners everything they need to be proactive about remediation before the compromised assets can be leveraged for more sinister intent.

Only SpyCloud Compass can reveal what bad actors already know about your enterprise so you can take action.

Now your security team can truly reduce your organization's exposure to ransomware with information you *can't get anywhere else*.

PREVENT RANSOMWARE

ILLUMINATE ATTACK SURFACE GAPS

ENABLE COMPREHENSIVE MALWARE RESPONSE WITH PIR

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics to proactively prevent ransomware and account takeover, safeguard employee and consumer accounts, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include seven of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

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