POST-INFECTION REMEDIATION:

Malware-Infected User Response Guide

SpyCloud

SpyCloud

Table of CONTENTS

OVERVIEW

Many users who have been infected with infostealer malware have unknowingly had their account passwords and full browser details recorded and stolen by cybercriminals. Information pilfered by these "botnets" is collected by cybercriminals, shared in small circles, and sometimes posted on hacking web forums for further financial gain and trouble for the individuals and organizations that the data pertains to. SpyCloud is able to recapture these botnet logs at scale, parsing out the infected victim's usernames, login URLs, passwords, and web session cookies in order to help businesses protect themselves and their consumers from account takeover, ransomware, and online fraud.

Enterprises can mitigate the risks associated with malware infections by taking swift action to inform affected users and help them fully remediate. In this guide, we'll look at what it means if information tied to your employees or consumers appears in a botnet log, and what actions you can take to help keep them safe.

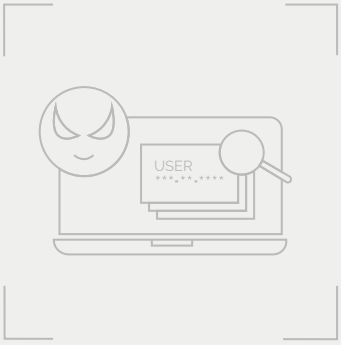
WHAT IS AN INFECTED USER?

An infected user is someone whose device has been infected with malware. Malware with keylogging components, or "infostealers," siphon information such as browser history, autocomplete data, web session cookies, screenshots, system information, crypto wallets, and login credentials. Cybercriminals use this data for a variety of malicious purposes, and there is a robust market for this type of information on the darknet. For individual victims, the results can be devastating. The losses for enterprises can be substantial if their consumers or employees are affected.

THE MALWARE ECOSYSTEM

1 Threat actor distributes malware to users. This might take the form of a phishing email or advertisement that entices the user to download a malicious file.

2 Users' infected systems send data to the threat actor's command-and-control server (C2).



3 Threat actor sees results in an admin panel, which can include stolen credentials, crypto wallet details, system information, browser data, and files.

4 Threat actor monetizes stolen data by draining accounts and selling stolen information to other criminals.

INFECTED EMPLOYEES

If SpyCloud identifies credentials from an infected employee or contractor tied to your domain(s) in our data – including your third-party workplace application domains such as VPNs, CRMs, chat services, and more – that means we have recaptured botnet logs showing that your employee used an infected device to access corporate applications with their work email address and password, most likely through an unmanaged or under-managed device.

For example, SpyCloud might identify that bob@yourcompanydomain.com was infected and his credentials and cookies were captured while logging into okta.com, dropbox.com, cloudflare.com, and other corporate applications.

What This Means For Your Enterprise

Malware with keylogging components can record your employee's every move, exfiltrating browser history, files, system information, device and web session cookies, and login data for corporate and third-party resources. While the risks of an infection on a company-owned system are obvious, infected personal devices can also endanger corporate resources — and they typically fall out of the scope of corporate security. Personal logins can reveal patterns of password reuse; plus, busy employees often blur the lines between personal and work-related device usage, meaning an infected system at home has the potential to expose corporate login credentials and data if they enable syncing their browser information on both their work and personal devices. Further, under-managed devices, such as those used by contractors to access corporate accounts or employee devices that aren't kept up-to-date with security patches, can also pose a risk as they fall outside the visibility of monitoring tools.

Whether your employee's infected system is personal or corporate, criminals may be able to use their stolen credentials and personal information for a variety of malicious purposes:

- Exploit stolen credentials to access both corporate and third-party resources, such as your corporate network, email and file sharing platforms, HR portal, cloud services, and developer resources, etc.
- Steal employee or customer data to sell on the criminal underground
- Access intellectual property or sensitive financial information
- Use corporate cloud services to host malicious infrastructure or mine cryptocurrency
- Target colleagues, customers, and partners with business email compromise (BEC) scams
- Authorize fraudulent wire transfers or change ACH details for customer payments and payroll transactions
- Escalate privileges to gain additional access and evade detection
- Use stolen personal information for blackmail, stalking, or social engineering
- Deploy ransomware to encrypt files and demand payment for the key to unlock data

Remediation Suggestions

First, check the IP and MachineID (if provided) to see if the infected system is a corporate-owned asset. If so, create a ticket to inspect or re-image the system. Also, look at SIEM logs to identify any suspicious behavior coming from that infected machine or IP address.

Infected employee or contractor records should be considered the most critical if they are corporate-owned assets or systems that have access to your corporate network. However, infected personal systems may also pose risk to your organization and should be investigated. For example, the malware may have captured your employee's logins to internal resources.

Whether the infection was personal or corporate, we advise requiring the employee to reset all corporate passwords and enabling multi-factor authentication (MFA) after remediating the device, including third-party applications and tools.

These extra steps to remediate every application exposed by malware is what we call **Post-Infection Remediation (PIR).**

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.

This approach to a 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. Learn more about these security team alerts at **SpyCloud.com**.

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

Taking these steps enables your security team to 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.

SAMPLE EMAIL: CONTACTING AN INFECTED EMPLOYEE

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>

SEND

SEE HOW TO ALERT AN EMPLOYEE WHOSE PERSONAL DEVICE HAS BEEN INFECTED IN OUR POST-INFECTION REMEDIATION GUIDE

INFECTED CONSUMERS

These are users of your consumer-facing site where botnet logs show that they were infected while entering their username and password on your login page (e.g. jim@hotmail.com was infected while logging into signin.yourcompanydomain.com). Forcing a password reset and enabling MFA or other authentication measures for the user's account is a good first step. However, as long as a consumer's system remains infected, infostealers may continue to collect their new passwords as soon as they change them. Worse, the infostealer has likely collected other authentication data (device and web session cookies) and personal information (PII, financial details) that an attacker can use for malicious purposes or sell to other criminals.

What This Means For Your Enterprise

Infected consumers are at extremely high risk of account takeover, identity theft, and online fraud. Here are just a few of the ways cybercriminals can exploit their stolen information:

- Transfer funds from crypto wallets, investment portfolios, payment applications, and other accounts
- Place fraudulent orders using credit card information or gift cards stored within accounts
- Siphon loyalty points associated with accounts
- Change shipping addresses to facilitate package theft and drop-shipping
- Sell login details, session cookies, and browser fingerprints to other criminals

Remediation Suggestions

Risk ranking varies for each SpyCloud customer and the types of consumers they are serving. Some SpyCloud customers require the end user to reset their password and also send them an email explaining why. Others choose to monitor that customer's online session(s) in a different manner and apply more scrutiny to certain transactions.

Our recommended path is to notify the customer, typically via email, and include remediation suggestions such as installing an antivirus program and running scans. Suggesting a specific antivirus program can help reduce the risk of the user unknowingly downloading additional malware disguised as antivirus software. The customer should be instructed not to go through the password change procedure until the system has been cleaned.

Additional steps such as locking the customer's account may help to prevent malicious transactions, but may be perceived as hostile or extreme by the user in the case of some types of accounts.

SAMPLE EMAIL: CONTACTING AN INFECTED CONSUMER

To: <Sparefactor Customer>

Subject: Reset Your Sparefactor Password

Hi,

One of our cybersecurity monitoring tools identified a malware infection on a device recently used to access your Sparefactor account. As a result, it is likely that the login information for your Sparefactor account might have been compromised.

We strongly encourage you to reset your password to protect your Sparefactor account. But first, we recommend installing antivirus protection to remove the malware, deleting browser and cookie history, running a scan to clean your machine, and then resetting your password on Sparefactor.com.

You can reset your password in three easy steps:
1. Go to Sparefactor.com
2. Where you would normally click to sign in, click "Forgot Password?"
3. Create a new, strong password that is unique to your Sparefactor account

We also recommend that you enable two-factor authentication (where a code is sent to you as an additional verification step) to help ensure the safety of your online accounts. You can enable this for your Sparefactor account under your Account Settings.

It's possible that the malware may have compromised your login credentials for other sites as well. You can follow the steps above for any other sites and services you use online and create a strong, unique password for each.

We take your security and privacy very seriously, and will immediately reach out if we notice anything unusual in the future.

Thank you,
<Signature>

SEND

> "With SpyCloud's botnet data, we've protected thousands of accounts representing tens of millions of dollars of funds. That's users we found in SpyCloud's botnet data, where we were able to successfully intervene and force password resets and account recoveries before an attacker was able to do something malicious."
>
> GLOBAL FINTECH COMPANY

WHAT'S THE IMPACT OF MALWARE INFECTIONS?

There's a robust market for stolen credentials and other data on the darknet, and infected users are just one source. Last year alone, SpyCloud discovered over 20 million malware-infected machines and recaptured billions of data assets exfiltrated by infostealers. We continue to collect millions of records per week ingested from malware-infected systems.

Criminals use stolen credentials and web session cookies to gain easy access to corporate systems and consumer accounts. Rampant password reuse and weak passwords make it easy for attackers to pivot from one compromised account to another, fueling a robust market for stolen credentials and other data on the darknet. And they take advantage of malware-siphoned web and device session cookies to perpetrate session hijacking, bypassing the need for credentials and MFA altogether. **Session hijacking** is an increasingly prevalent precursor to fraud and, even more frightening to the enterprise, ransomware attacks.

DISRUPTING CRIMINALS' ABILITY TO PROFIT

SpyCloud's mission is to significantly disrupt the cybercriminal economy, and ultimately make the internet a safer place for individuals and businesses.

One way we do that is through our efforts to responsibly disclose new data breaches and malware-infected user data to victim organizations when we believe they aren't already aware. We also support active investigations, such as tracking and taking down malware campaigns.

Based on that work, we have access to data that prevents criminals from profiting from your own users' data. For enterprises, the best way to disrupt the criminal economy is by understanding account takeover and session hijacking, addressing compromised credentials programmatically, and developing a process to invalidate web sessions related to infected users.

SpyCloud reveals what bad actors know about your enterprise so you can take action. Identifying exposed users and applications from malware infections on both managed and unmanaged devices helps fill the gaps left by traditional application, network, and endpoint security tools. 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.

Taking these measures as soon as possible after exposure locks criminals out and keeps them from reaping the benefits of malicious activity.

THE SPYCLOUD DIFFERENCE

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.

Access to SpyCloud's massive collection of recaptured darknet data enables enterprises to significantly shorten your exposure window for ransomware and other critical threats, and effectively stop malware exposures from becoming full-blown security incidents.

For more information, visit **spycloud.com**.