Incident Response: Infected User Response Guide

Overview

Many users who have been infected with 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. When SpyCloud is able to recover some of these bot logs, we parse out the infected victim's username, URL, and password in order to help consumers and organizations protect themselves.

Enterprises can mitigate the risks associated with botnet infections by taking swift action to inform affected users and help them 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 "stealers," can collect information such as browser history, autocomplete data, 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 criminal underground. 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 C&C.

3. Threat actor sees results in an admin panel, which can include stolen credentials, crypto wallets, 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 infected employees tied to your domain(s) in our data, that means we have recovered botnet logs showing that your employee has used an infected machine to log into a domain or portal with a corporate email address and provided a password to that destination. For example, SpyCloud might identify that bob@yourcompanydomain.com was infected and his credentials 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, capturing browser history, files, system information, 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 aren't monitored by 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.

Whether your employee's infected system is personal or corporate, criminals may be able to use your employee's 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
- Steal employee or customer data to sell on the criminal underground
- Use corporate cloud services to host malicious infrastructure or mine cryptocurrency
- Access intellectual property or sensitive financial information
- 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

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 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 botnet 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 *after* remediating the device, including third-party applications and tools.

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 security challenges for the user's account is a good first step. However, as long as a consumer's system remains infected, the malware will collect their new password as soon as they change it. Worse, the botnet has likely collected other personal information 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
- Commit warranty fraud using stored device information
- Change shipping addresses to facilitate package theft and drop-shipping
- Stalk or blackmail victims using browser history and other stolen data
- Sell login details and browser fingerprints to other criminals

Remediation Suggestions

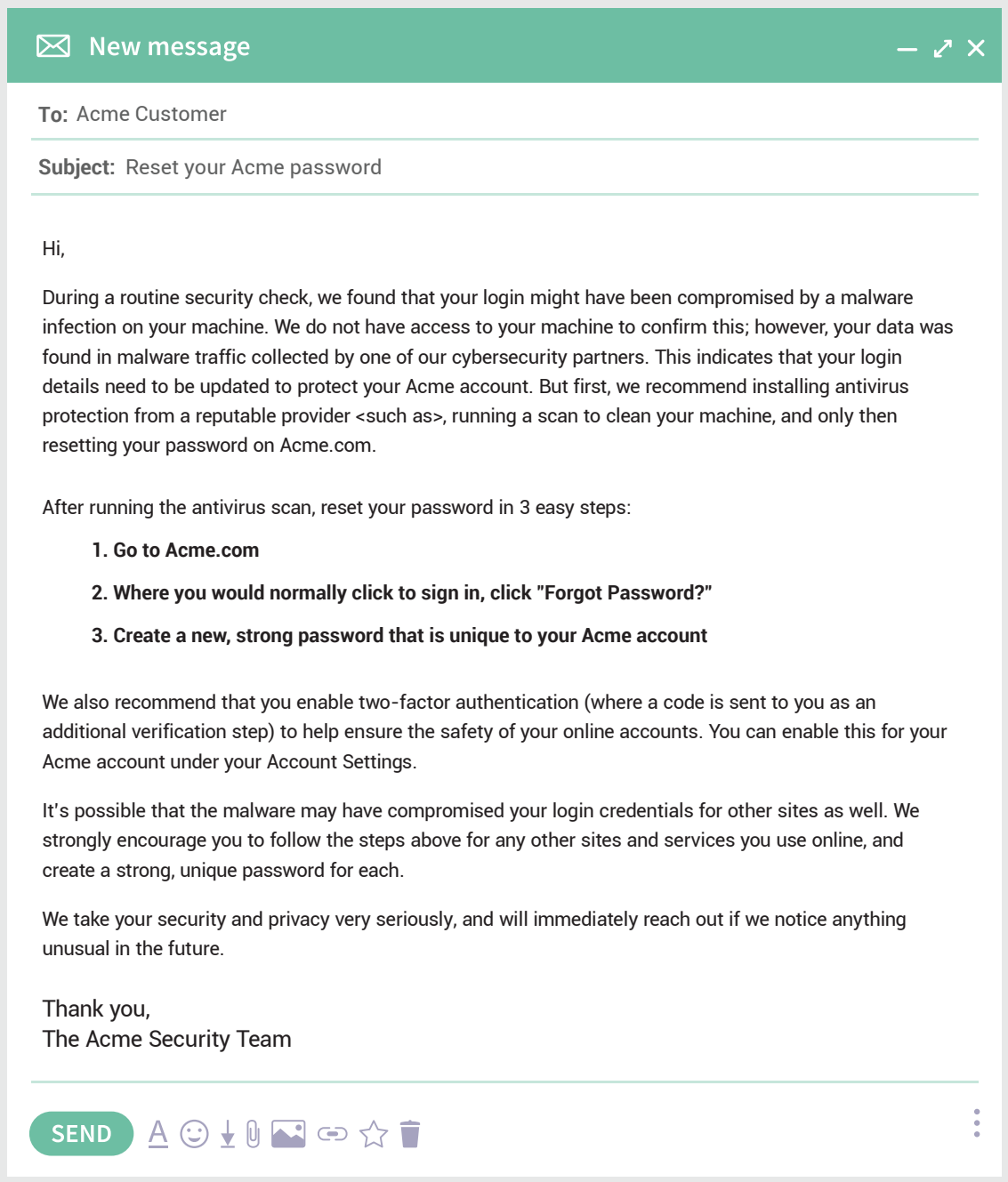
Risk ranking varies for each SpyCloud customer and the types of consumers they are serving. Some SpyCloud customers require the end user to reset their password and also send them an email explaining why. Others choose to monitor that customer's online session in a different manner and apply more scrutiny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

> *"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 with those credentials.*
>
> – Global Fintech Company

Sample Email: Contacting an Infected Consumer



New message

To: Acme Customer

Subject: Reset your Acme password

Hi,

During a routine security check, we found that your login might have been compromised by a malware infection on your machine. We do not have access to your machine to confirm this; however, your data was found in malware traffic collected by one of our cybersecurity partners. This indicates that your login details need to be updated to protect your Acme account. But first, we recommend installing antivirus protection from a reputable provider <such as>, running a scan to clean your machine, and only then resetting your password on Acme.com.

After running the antivirus scan, reset your password in 3 easy steps:

1. **Go to Acme.com**
2. **Where you would normally click to sign in, click "Forgot Password?"**
3. **Create a new, strong password that is unique to your Acme 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 Acme account under your Account Settings.

It's possible that the malware may have compromised your login credentials for other sites as well. We strongly encourage you to 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,
The Acme Security Team

SEND

> *We assume that if your credentials appear somewhere in the botnet data, your email and phone and other mechanisms for proving your identity are compromised, too. By educating customers about cybersecurity, the team hopes to help users eliminate the malware from their systems and prevent them from falling into similar traps in the future.*

– Global Fintech Company

What's the Purpose of Botnet Infections? Stolen Data Fuels the Criminal Economy

There's a robust market for stolen credentials and other data on the criminal underground, and infected users are just one source. Last year alone, SpyCloud recovered over 9 billion credentials from cybercriminal communities, including both botnet logs and data breach records, and we continue to collect millions of records per week ingested from malware-infected systems.

Criminals use stolen credentials to gain easy access to corporate systems and consumer accounts. Rampant password reuse makes it easy for attackers to pivot from one compromised account to another, fueling a robust market for stolen credentials and other data on the criminal underground.

SpyCloud's Mission: Disrupting Criminals' Ability to Profit

SpyCloud's mission is to significantly disrupt the cybercriminal economy to eliminate the loss of money, time, and reputation due to online fraud – and ultimately to make the internet a safer place for individuals and businesses.

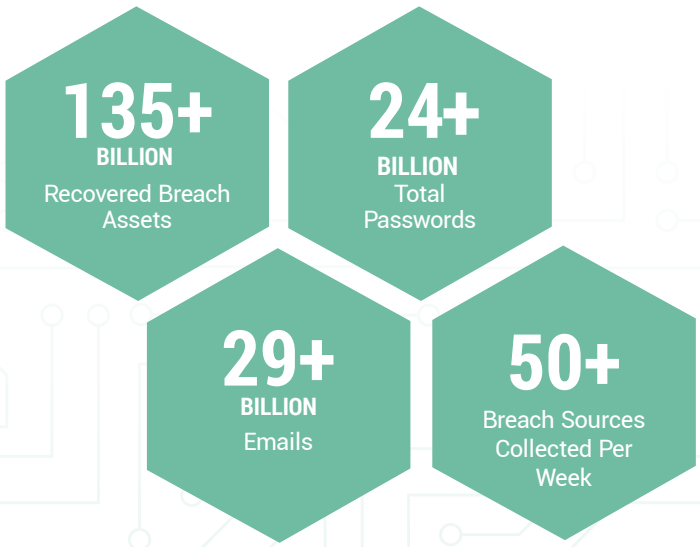
One way we do that is through our efforts to responsibly disclose new data breaches to victim organizations when we believe they aren't already aware. We also support active investigations, such as tracking and taking down malware campaigns.

Based on that work, we have access to data that prevent criminals from profiting from your own users' data. For enterprises, the best way to disrupt the criminal economy is by understanding account takeover and addressing compromised credentials programmatically. Resetting exposed passwords as soon as possible after a breach locks out criminals and keeps them from reaping the benefits of malicious activity.

The SpyCloud Difference: Current, Relevant, Truly Actionable Data

SpyCloud's solutions are backed by the largest repository of compromised credentials and PII in the world. SpyCloud researchers collect an estimated one billion new breach assets per month, infiltrating criminal communities to recover stolen data early in the breach timeline so we can notify our customers of exposures as soon as possible – often months or even years before a breach becomes public.

Access to this massive breach database enables enterprises to quickly identify and take action on exposed accounts, preventing those exposures from progressing to account takeovers.



Check Your Exposure
at spycloud.com