SpyCloud

Incident Response: Infected User Response Guide

Overview

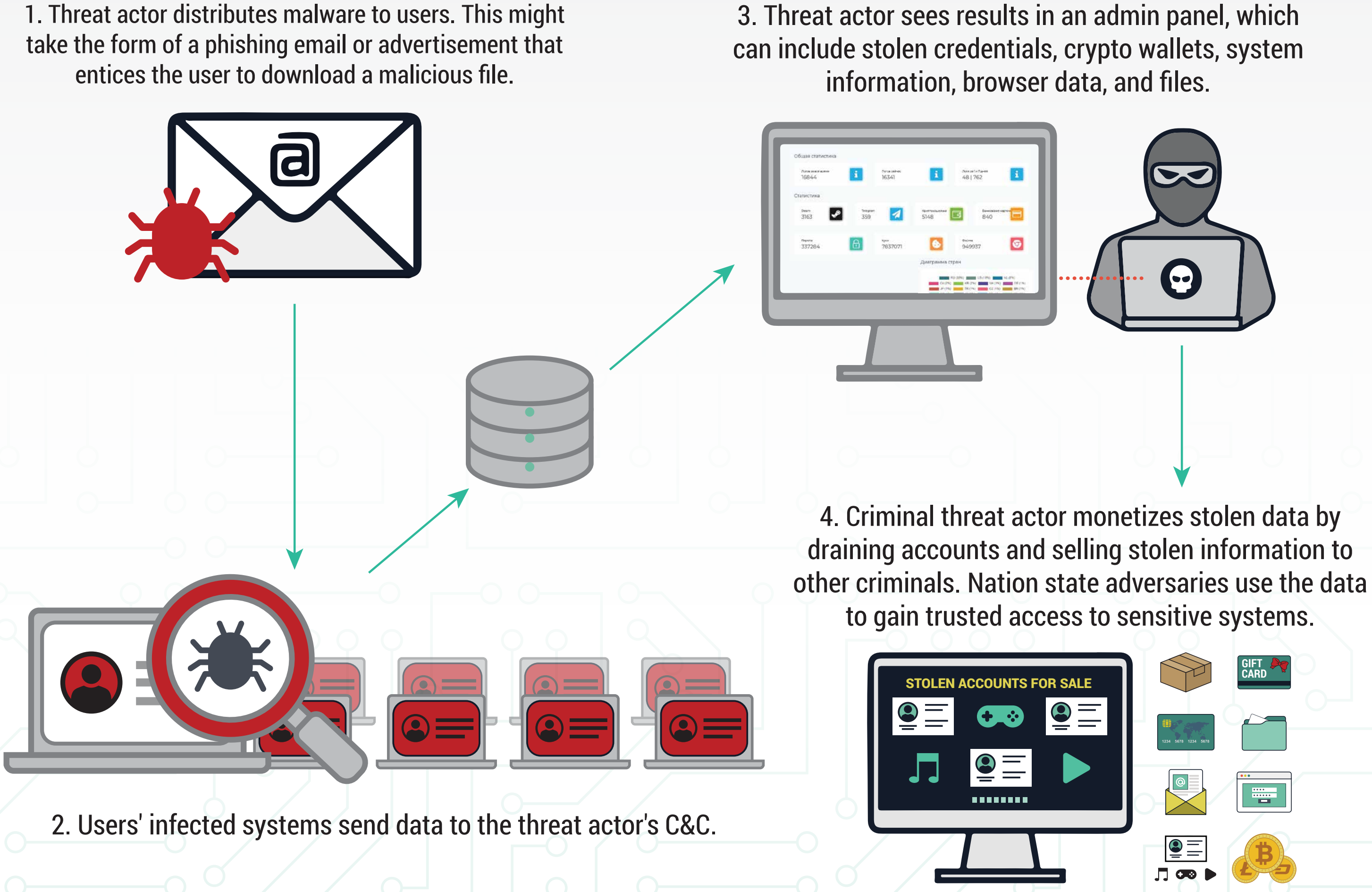
Many users who have been infected with malware have unknowingly had their account passwords and full browser details recorded and stolen by cybercriminals. Information pilfered by these "botnets" is collected by cybercriminals, shared in small circles, and often posted on hacking web forums. When SpyCloud is able to recover some of these bot logs, we parse out the infected victim's username, URL, and password in order to help citizens and organizations protect themselves.

Federal agencies 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. Adversaries 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. For agencies, costs of mitigation, loss of citizen trust, and additional audits can be painful distractions.

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. Criminal threat actor monetizes stolen data by draining accounts and selling stolen information to other criminals. Nation state adversaries use the data to gain trusted access to sensitive systems.

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 government email address and provided a password to that destination. For example, SpyCloud might identify that bob@youragencydomain.gov was infected and his credentials were captured while logging into okta.com, dropbox.com, cloudflare.com, and other COTS or GOTS applications.

What This Means for Your Agency

Malware with keylogging components can record your employee's every move, capturing browser history, files, system information, and login data for government and third-party resources. While the risks of an infection on a government-owned system are obvious, infected personal devices can also endanger government resources — and they typically aren't monitored by internal 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 agency or department login credentials and data.

Whether your employee's infected system is personal or government-owned, adversaries 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 government and third-party resources, such as your agency or department network, email and file sharing platforms, HR portal, cloud services, and developer resources
- Steal employee or citizen data to sell on the criminal underground
- Use taxpayer-funded cloud services to host malicious infrastructure or mine cryptocurrency
- Access controlled data or sensitive information
- Target colleagues, service users, and supply chain partners with business email compromise (BEC) scams
- Escalate privileges to gain additional access and evade detection
- Use stolen personal information for blackmail, stalking, or social engineering

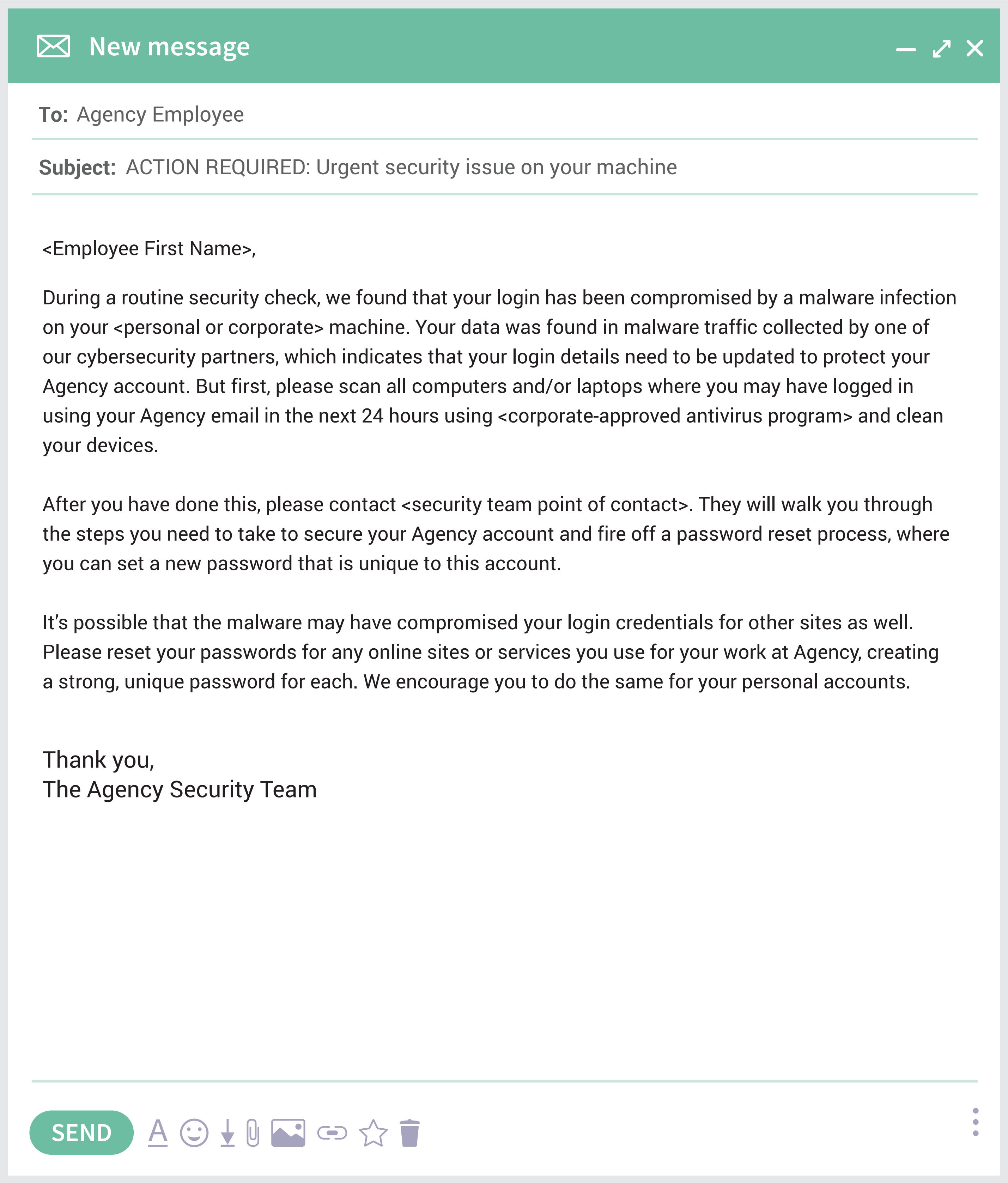
Remediation Suggestions

First, check the IP and MachineID (if provided) to see if the infected system is a government-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 government-owned assets or systems that have access to an agency or department 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 employment related, we advise requiring the employee to reset all passwords for government services after remediating the device, including third-party applications and tools.

Sample Email: Contacting an Infected Employee



To: Agency Employee

Subject: ACTION REQUIRED: Urgent security issue on your machine

<Employee First Name>,

During a routine security check, we found that your login has been compromised by a malware infection on your <personal or corporate> machine. Your data was found in malware traffic collected by one of our cybersecurity partners, which indicates that your login details need to be updated to protect your Agency account. But first, please scan all computers and/or laptops where you may have logged in using your Agency email in the next 24 hours using <corporate-approved antivirus program> and clean your devices.

After you have done this, please contact <security team point of contact>. They will walk you through the steps you need to take to secure your Agency account and fire off a password reset process, where you can set a new password that is unique to this account.

It’s possible that the malware may have compromised your login credentials for other sites as well. Please reset your passwords for any online sites or services you use for your work at Agency, creating a strong, unique password for each. We encourage you to do the same for your personal accounts.

Thank you,
The Agency Security Team

Infected Service Users

These are users of your citizen-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.youragencyservice.gov). 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 citizen'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.

What This Means for Your Agency

Infected service users are at extremely high risk of account takeover, identity theft, and online fraud. Here are just a few of the ways cybercriminals and advanced persistent threats (APTs) can exploit their stolen information:

- Transfer funds from crypto wallets, investment portfolios, payment applications, and other accounts
- Use personally identifiable information (PII) for identity theft or fraud
- Reroute government benefits intended for taxpayers
- Stalk or blackmail victims using browser history and other stolen data
- Sell login details and browser fingerprints to other criminals
- Use sensitive information for intelligence targeting

Remediation Suggestions

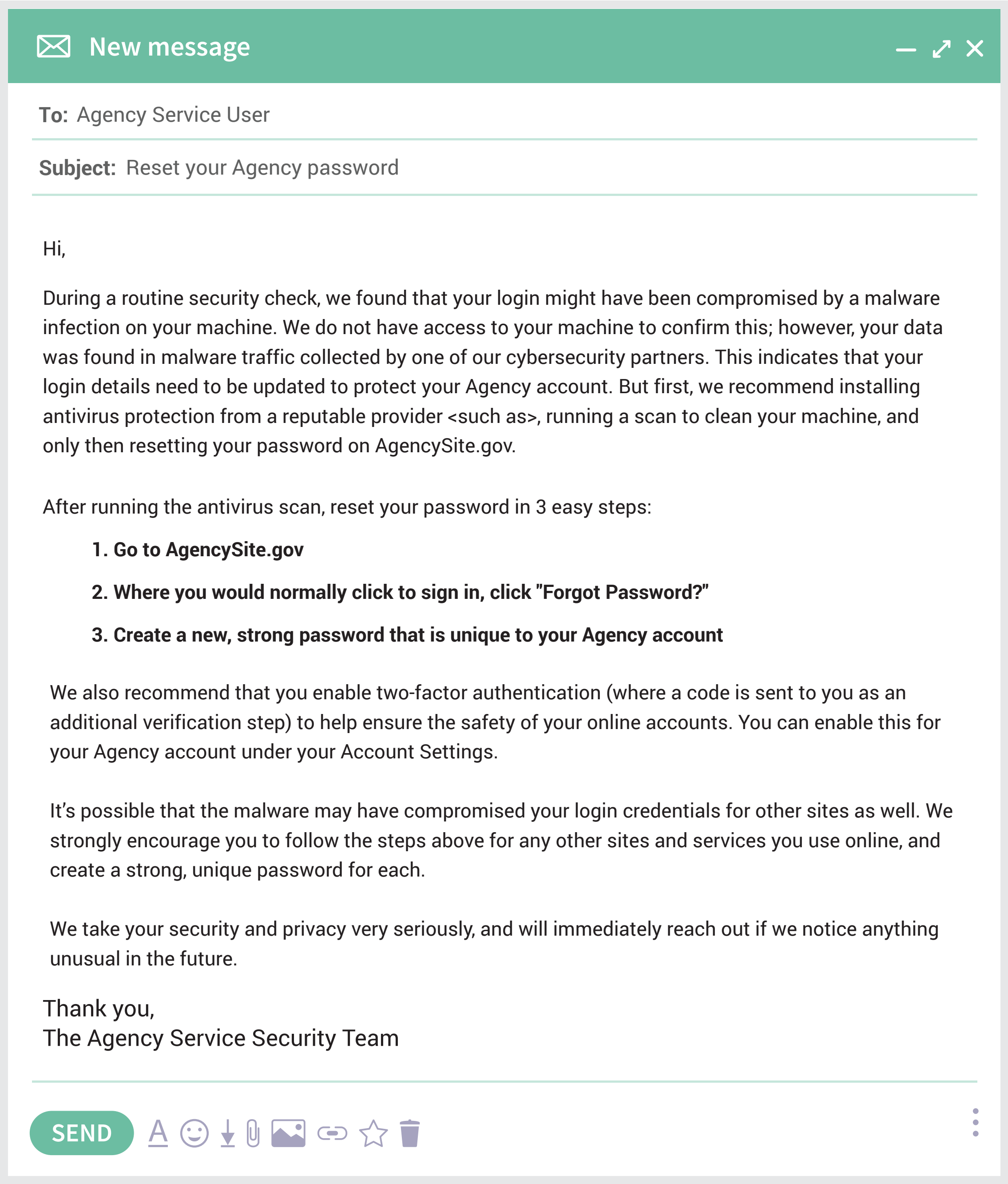
Risk ranking varies for each SpyCloud customer and the types of users they are serving. Some SpyCloud customers require the end user to reset their password and also send them an email explaining why. Others choose to monitor that user's online session in a different manner and apply more scrutiny to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

Our recommended path is to notify the user, 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 citizen should be instructed not to go through the password change procedure until the system has been cleaned.

Additional steps such as locking the user'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 Service User



To: Agency Service User

Subject: Reset your Agency 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 Agency 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 AgencySite.gov.

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

1. **Go to AgencySite.gov**
2. **Where you would normally click to sign in, click "Forgot Password?"**
3. **Create a new, strong password that is unique to your Agency 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 Agency 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 Agency Service Security Team

> *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 and government systems and user 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.

Nation state threats are also aware of how easy it is to gain access to systems through stolen credentials. They have begun using the same data to penetrate intelligence targets because it allows them to avoid research and fingerprinting, thereby obfuscating their identity and mission.

The SpyCloud Difference: Current, Relevant, Truly Actionable Breach Data

Stop cyber attacks using the most current and comprehensive repository of compromised credentials and PII in the industry, recovered from the criminal underground using Human Intelligence (HUMINT). SpyCloud's massive database of actionable open source intelligence (OSINT) includes data criminals have stolen via data breaches and through botnet infections.

SpyCloud solutions are offered as Data as a Service (DaaS), enabling agencies to act on newly-exposed data quickly without the need for increased staff.

135+
BILLION
Recovered Breach Assets

1+
BILLION
New Monthly Assets

29+
BILLION
Email Addresses

24+
BILLION
Total Passwords 90% Cracked

100+
BILLION
Chinese, Russian Records

18+
MONTHS
Prior to Exposure on Dark Web

160+
MILLION
Botnet Records

See the full power of SpyCloud's breach data to protect your agency.
Request a demo & custom test on our botnet data: **gov@spycloud.com**