DISRUPTING THE RANSOMWARE MARKET

Breaking Down Malware and the Importance of Post-Infection Remediation

SpyCloud

Ransomware is a Malware Problem

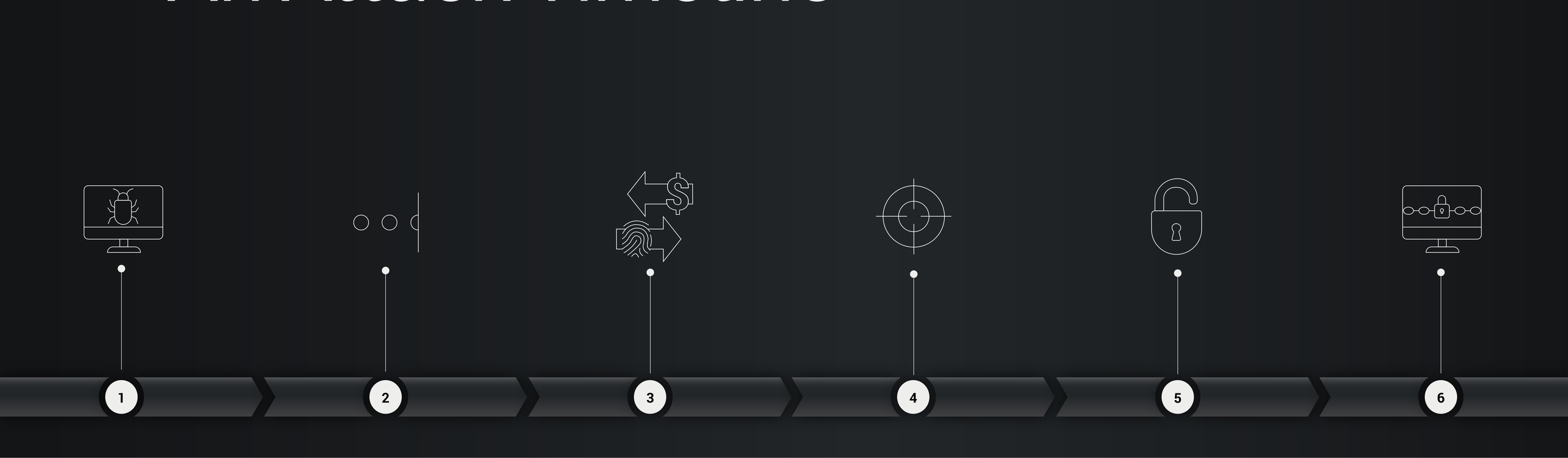
Ransomware is a pervasive problem that has become a topic of conversation at all levels of every enterprise. A **survey** of more than 400 CISOs found that ransomware is the top cyber threat most concerning to respondents. And a SpyCloud **survey** of more than 300 IT security leaders found that 90% of organizations were affected by ransomware in the past 12 months, and 50% of organizations were affected by ransomware 2-5 times within that same period.

Typical incident response playbooks often focus on the later stages of ransomware attacks because that's when it's evident that criminals have gained unauthorized access to an organization. Yet to truly understand ransomware attacks, you must identify and remediate common entry points, particularly those that fall through the cracks of traditional ransomware prevention strategies, such as infostealer malware infections.

The rise in popularity for credential-stealing malware, or **infostealers**, is especially concerning for organizations because it can steal employee authentication data right off managed or unmanaged employee devices, allowing cybercriminals to impersonate those individuals. Malware infections are so closely tied with ransomware attacks because with the freshly harvested credentials and cookies or browser fingerprint data in hand, bad actors make quick work of that information to hijack a session, bypass multi-factor authentication (MFA), access the enterprise, and start encrypting files.

To put it directly, ransomware is a malware problem. Often, bad actors use information or access that 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. Once a malware infection is detected, wiping a device isn't enough — let's walk through how malware-siphoned data serves as an entry point for ransomware and why it's so critical to understand and visualize the full scope of an infection's threat to your business.

Malware to Ransomware:
An Attack Timeline



1

Jon mistakenly downloads malware to a shared or personal device he uses to access the corporate network, sites and applications.

Employees who use personal devices to access corporate assets and applications unwittingly pose a threat to organizations. Recent data shows that unmanaged devices accessing the network are in the **top three riskiest entry points** for ransomware. Since IT security teams already struggle to stay on top of security challenges they are aware of, increasing the attack surface with devices they can't see or control puts even more burden on already overwhelmed teams.

SHINING A LIGHT ON ENTRY POINTS

SpyCloud frequently sees evidence that infected devices have been used for a combination of work and personal activities. To reduce the risk of ransomware stemming from infostealer-siphoned data, enforce security policies regarding accessing corporate applications on unmanaged devices and minimize the allowance of bring-your-own-device (BYOD) for work purposes.

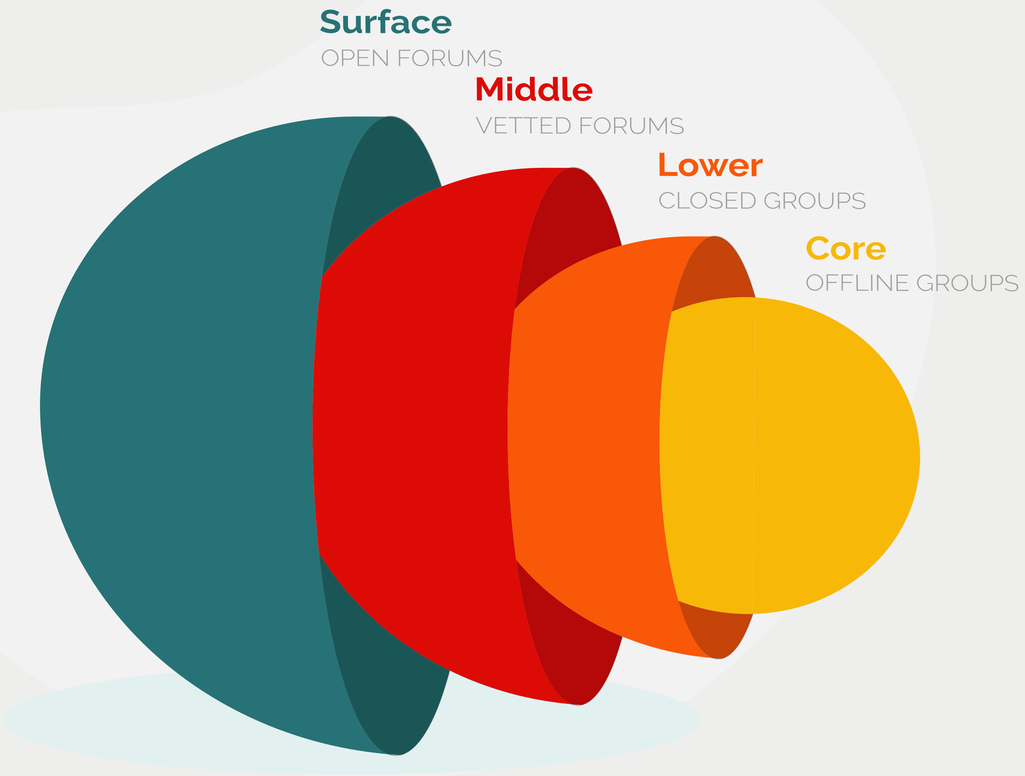
The malware siphons Jon's passwords, web session cookies, device information, browser fingerprint, and other data that allows the criminal to walk right into the corporate network.

What makes infostealers so dangerous is that the data siphoned from the device greatly increases a cybercriminal's success rate because it is current and accurate. 87% of respondents to our survey were concerned about malware on unmanaged devices being an entry point to their organization. And rightfully so, as malware becomes an increasingly popular threat vector, with more than **4 billion malware attempts** globally through the third quarter of 2022.

SHINING A LIGHT ON INFOSTEALERS

Using infostealers – malware specifically designed to harvest information from a device – cybercriminals siphon authentication data like credentials and browser fingerprints straight from the endpoint. Authentication data for third-party applications such as password managers, collaborating apps, CRM and marketing automation platforms, HR and payroll systems, and more, often fall outside the scope of traditional security monitoring tools, which leaves significant security gaps in ransomware prevention strategies.

In our recaptured malware records from **the first six months of 2022 alone,** SpyCloud discovered **6 million malware-infected devices** with, on average, up to 26 unique enterprise apps affected per device.



Jon's stolen data gets traded on the criminal underground, where initial access brokers (IABs), ransomware operators, and other bad actors can purchase it.

Thanks to the underground economy, anyone can pay for an infostealer, extract the credentials it siphoned, create a combo list (username and password combinations), and compare it against a list of targeted sites to try accessing other accounts. Or, alternatively, the same attacker may decide to sell valuable access to the highest bidder, which may be a ransomware affiliate or other financially-motivated criminal actor. But nefarious actors don't even have to go to this much trouble, with some infostealers being advertised on the darknet as a fully automated process that saves "customers" time and headaches – with all the software, front-end, and back-end components included.

SHINING A LIGHT ON THE DARKNET

The darknet is a very complex and layered world, and the value of specific darknet data varies widely, based upon the capabilities and access of the group that is collecting the information. Darknet groups and forums operate in many layers of obscurity, with each layer providing more protection for criminal actors and syndicates. Penetrating the deeper layers where high-value data is sold and traded takes significant time and investment, and only SpyCloud interacts at every layer of the darknet to gather actionable raw data, including malware data and corporate access sold by sophisticated actors, often to syndicates.

IABs identify that Jon's data includes corporate assets and sells it to ransomware operators who can use it to target Jon's employer.

Data siphoned by malware puts your organization on attackers' radar in the first place. Like any other cybercriminals, ransomware groups don't always target specific organizations but look opportunistically for targets. They may simply ask IABs for any potential targets with easy access, such as compromised credentials and cookies, that fit their desired profile. If your company is on that list, your likelihood of being the next target skyrockets.

SHINING A LIGHT ON THE PROFESSIONALIZATION OF RANSOMWARE OPERATIONS

Ransomware-as-a-Service (RaaS) operators created a market for IABs, the individuals or groups who package and sell access to networks that are guaranteed to work. The rise of IABs can be attributed to a thriving underground economy operating on many of the same principles as legitimate enterprises. Just like large enterprises, ransomware operators outsource critical business functions to specialized vendors. IABs supply the affiliates with access-as-a-service. They obtain access to organizations and then package it for sale on the same underground forums frequented by RaaS affiliates.

5

SHINING A LIGHT ON AUTHENTICATION MEASURES

Despite organizations putting more emphasis on authentication measures such as MFA, passwordless solutions, and biometrics, these forms of security still have gaps that criminals take advantage of to gain access to enterprises. While no authentication solution is a magic bullet, organizations can close those gaps by monitoring for stolen session cookies, understanding the hidden risks of malware-infected devices, and enhancing malware infection response.

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

Malware logs all the necessary credentials needed to bypass multiple layers of security, allowing criminals to move throughout your organization by changing security privileges and gaining access to business-critical information. Third-party applications serve as yet another entry point for ransomware, and concern about third-party risk is the factor impacting upcoming security investments the most, according to our survey. However, 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.

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

Despite the looming threat of ransomware becoming a "fact of life" for organizations of all sizes, the continuing escalation of this threat means security teams must close the gaps in their security controls to disrupt cybercriminals trying to harm your business.

SHINING A LIGHT ON HOW TO PREVENT RANSOMWARE

In today's threat landscape, backups, endpoint protection tools such as EDR and ASM, and anti-virus solutions alone are not enough to prevent and recover from a ransomware attack. A layered defense is required – one in which proactive monitoring for malware infections and the resulting application exposures is considered essential. Having this information can help:

- Detect threats you couldn't see coming
- Catch the warning signs of an attack
- Detect employees' infected managed and unmanaged devices
- Reduce entry points for ransomware
- Enhance malware-infection response

Disrupting Ransomware with SpyCloud Compass and Post-Infection Remediation™

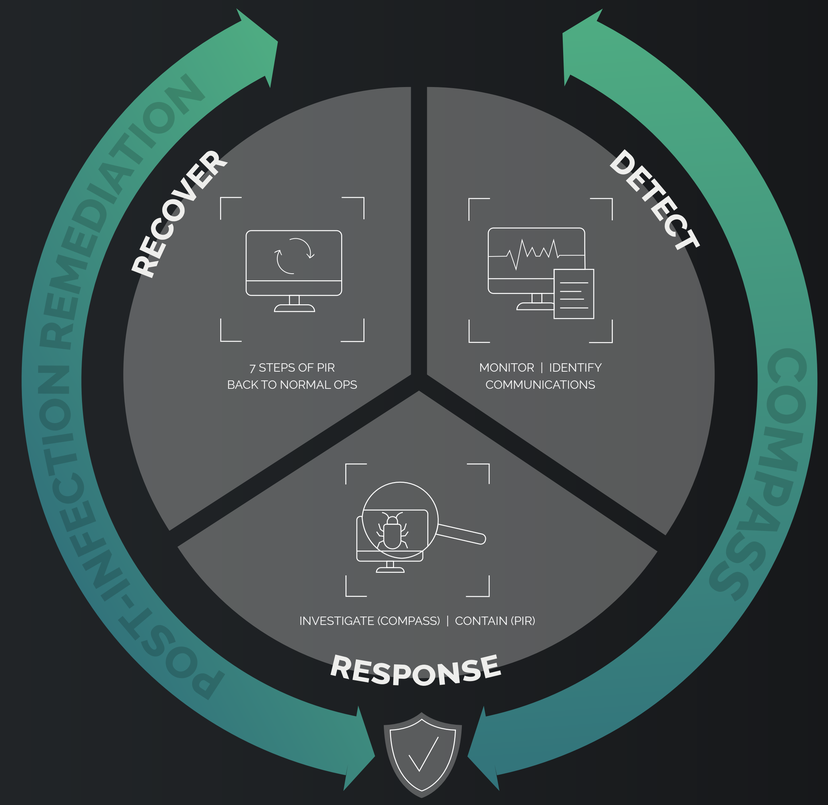
Post-Infection Remediation (PIR) is SpyCloud's innovative, critical addition to malware-infection response that exists because it's now possible to understand and visualize the full scope of the infection's threat to your business.

PIR offers a series of preventative steps designed to negate opportunities for ransomware by resetting the application credentials and invalidating session cookies siphoned by infostealer malware.

SpyCloud disrupts cybercrime by enabling proper PIR with SpyCloud Compass.

Since we monitor all layers of the darknet, SpyCloud is able to recapture malware-infected employee data, such as internal login information, third-party application logins (e.g. SSO, CRM, payroll systems, and more), and stolen device and session cookies that cybercriminals use to bypass login flows. Compass then uses this data to alert you to the infected devices, users, and applications, mapping out exactly what was exposed.

Compass fills the gaps left by traditional application security monitoring, network security, and endpoint detection and response solutions by providing detailed information on each exposure, including infection data and time, IP address, the family of malware, and more. These insights provide 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 and remediation before a full-blown ransomware incident occurs.



SpyCloud COMPASS + Post-Infection Remediation™

Find out what bad actors already know about your enterprise so you can take action.

Visit spycloud.com/ransomware