SpyCloud Annual Report: Malware is Making Its Mark on the Darknet

March 13, 2023 Team SpyCloud Malware

It's the most wonderful time of the year, at least for us here at SpyCloud – our 4th Annual Identity Exposure Report just dropped, and yet again it doesn't disappoint.

This year's report unveils some of the latest cybercrime trends and tactics malicious actors are using to exfiltrate data and profit from the stolen information. Our researchers combed through billions of recaptured data assets from the darkweb over the course of 2022, and their analysis brought back a few familiar themes from past years, and also uncovered some alarming shifts in cybercriminal trends. The report offers insights into what this evolution means for organizations and their customers, and actionable ways to use this same data to fight back. Let's dig into our top takeaways.

Malware-Infected Devices Responsible for Nearly Half of the Exposed Credentials

Let us not bury the lead. Massive data breaches and leaks exposing millions of credentials are a yearly occurrence, leading to the popular belief that this is how passwords end up on the dark web. What many people don't realize, however, is that credential-stealing malware is just as likely to be the culprit behind these exposures – and the consequences of malware infections are much more serious when it comes to identity exposure risk and negative business impact.

> **Of the 721.5 million exposed credentials that we recovered from the darknet last year, 48.5% came from botnet logs.**

Malicious actors use botnets (aka robot networks) for large-scale deployments of a type of malware known as infostealers, designed to exfiltrate information from the infected user device. The stolen data ranges from passwords and browser cookies to personally identifiable information (PII).

Infostealers are extremely dangerous for several reasons:

- The authentication data they siphon from the infected device is current and accurate, which means cybercriminals are much more likely to succeed in impersonating the user.
- Some infostealers are designed to establish persistent presence; however, most have no idea their machines have been infected because the infostealers are stealthy and many strains are designed to destroy themselves or "dissolve" and with it goes any evidence of compromise.

Regardless, as long as the device remains infected, the bad actors will have access to the most current data and activity, which means that changing passwords continues to offer less protection than ever before.

Over the past few years, we've observed that malicious actors are more commonly using a multitude of malware-stolen data assets to impersonate identities. They are gravitating to this tactic – rather than relying on combo lists (username and password pairs) that have been circulating for a while – because it's more effective and has a greater return on investment.

The Treasure Trove of Malware Victim Data

The quantity and quality of the malware-siphoned data that is now available means this threat will not go away any time soon. But there's another reason this tactic has become popular: it enables cybercriminals to bypass multi-factor authentication (MFA) because the malware logs typically include data such as browser session cookies. Session cookies are the ultimate steal because they authenticate users on specific websites for a period of time. Cybercriminals can then import the cookies into anti-detect browsers and take over accounts without the need to log in with the username and password – hijacking the browser session to slip right into the user identity.

With our recovery of 22 billion device and session cookie records from 2022 alone, we clearly see that malicious actors are focusing on this high-quality data rather than just quantity. Session hijacking is a risk both for employees and consumers. For organizations, stolen cookies can give cybercriminals access to sensitive information and privilege escalation. On the consumer side, the bad actors can take over accounts to make fraudulent purchases, drain loyalty cards and points, and a lot more.

Another type of malware victim data are credentials for common third-party business applications such as communication and collaboration tools, human resource management apps, and customer support platforms. **Last year, we recaptured millions of third-party application credentials harvested by malware.** These included **90 of the top cloud app** subdomains that IT teams don't have visibility into. **Additionally, we recaptured 117,657 master passwords from eight leading password managers** – a reminder that even the security tools considered a best practice are not infallible, albeit still a valuable layer and resource in proper defense and user management.

Password Reuse Rates Have Not Improved

Although session cookies can trump the simple defense gate that passwords typically provide, reused passwords still pose a high risk for identity exposure – and our report shows that password reuse rates are not improving.

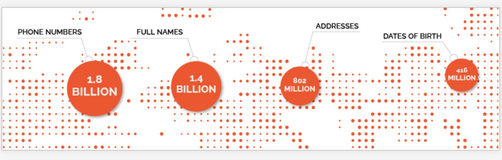
> **We found a nearly 72% reuse rate for users exposed in two or more breaches in the last year, an 8-point increase from the 64% in the previous year's report**

The combination of malware-infected devices and high password reuse rate indicates that the risk of identity exposure continues to climb. This exposure, in turn, elevates the risk of follow-on attacks like ransomware because the malware-siphoned authentication data gives ransomware operators and other malicious actors a direct path into an organization.

PII Fuels Criminal Innovation

Along with high password reuse rates, the continuous growth of exposed PII is another recurring theme in our annual report. **We recaptured 8.6 billion PII assets from the criminal underground last year, which brings the total in our database to 60 billion.**

The categories with some of the largest numbers of recaptured assets are those that malicious actors need to create synthetic identities:



Synthetic identity fraud – has become the largest form of identity theft, according to research by Pew. With synthetic identities, fraudsters can open new accounts, apply for new lines of credit, and make high-ticket purchases, among other things.

Ironically, but not surprisingly, some bad actors are now leveraging synthetic identities to get jobs that give them access to sensitive data. More traditionally, others are using these constructed identities to defraud financial institutions and even governments of large sums of money. These are all illustrations of how the abundance of stolen PII enables crafty cybercriminals to innovate and find new creative ways to perpetrate fraud.

Spotlight on Pop Culture Passwords

Each year, a highlight of the report are the insights on how pop culture influences passwords. We've seen it all from sports teams to political parties to TV shows to the latest celebrity scandals – if it's happening in the news, it's somehow finding its way into passwords.

This year was no different – making an appearance near the top of our pop culture password analysis was none other than T. Swift herself. It appears that Swifties take their love of Taylor to the next level by using her name in their passwords, or at least 186K of them did. And another pop star, Bad Bunny, Spotify's most streamed artist of the year, also showed up in 141K passwords we recaptured last year.

Significant events from last year made their way into passwords, including the passing of Queen Elizabeth and the reunion of Jennifer Lopez and Ben Affleck, aka "Bennifer." Here's a sampling of the pop culture passwords we found last year:

Final Thoughts

With the increased use of malware being a significant storyline coming out of our report analysis, we recommend security teams implement Post-Infection Remediation into their malware-infection response. This framework of additional steps to existing cyber incident response protocols is designed to negate opportunities for ransomware and other critical threats by resetting the application credentials and invalidating session cookies siphoned by infostealer malware. By incorporating this optimized remediation that includes recaptured exfiltrated data, the SOC can seamlessly and comprehensively disrupt cybercriminals before they have the chance to act on stolen data and neutralize the risk of ransomware from these exposures.

With digital identities embedded in people's personal and professional lives, securing these identities is extremely important – yet increasingly difficult. We found that the best way to stop criminals in their tracks is by using the same data they have to turn the tables on them. Organizations can use the insights into what cybercriminals know about their employees and customers to quickly identify vulnerable identities, accounts and devices and take action – effectively leveling the playing field against these sneaky bad actors.