CYBER DEFENSE MAGAZINE

eMAGAZINE

MARCH 2026

FROM CONTROLS TO CREDIBILITY

From Controls To Credibility: Cybersecurity Leadership In AI-Augmented Environments

Entropy as Infrastructure: The Missing Layer in Post-Quantum Security

The Hidden Security Debt That Kills Deals After Letter of Intent (LOI)

...and much more...

MORE INSIDE

Inside the Infostealer Economy

By Mike Wilson, Founder & CTO, Enzoic

Passwords are a perennial security vulnerability, but threat actors' means of accessing this information has historically been relatively stagnant. Capitalizing on widespread credential reuse, exploiting vulnerabilities in websites and apps, or initiating phishing campaigns have proved extremely fruitful for hackers to obtain credential data. While these methods remain effective, infostealer malware has emerged in recent years to not only offer a compelling alternative but also suggest a permanent change in the credential theft ecosystem.

Breaking Down the Threat

Infostealers extract browser "autofill" field data, cookies, information stored in password managers, and numerous other forms of sensitive information. Once an infostealer has infected a system with access to corporate data, breaching individual accounts, VPNs, or internal websites is child's play. As such, the malware provides "keys to the kingdom" access to customer databases, financial records, sensitive IP data—and the list goes on. While infection volumes are lower than traditional database breaches, the value, immediacy, and usability of this stolen information are far higher. And the extracted data is typically packaged and sold as logs on the Dark Web, enabling cybercriminals to exploit this information in near real-time.

How Do Infostealers Spread?

There are a variety of tactics threat actors utilize to spread the malware, including:

· Embedding the software in a document and sending it as an attachment in a phishing email, enticing recipients to open it

· Building a phishing site that mirrors the domain or logo of an established organization. With AI making it increasingly simple to replicate design details, it's easy to trick people into believing it's a legitimate app and unknowingly downloading the infostealer

· Adding the code to a mobile app or browser extension, and making that app available for download

· Promoting download links on social media and streaming sites, claiming to share copies or add-ons for video games or other types of free software

The Enterprise Impact

Any employee with privileges to install software on a corporate device can fall victim to infostealers via these threat vectors. Particularly in today's remote and hybrid work environments, in which people frequently access corporate networks from their personal devices, it's difficult for organizations to mitigate the threat.

The Password Problem(s)

Once a device has been infected, password managers are an obvious target. These solutions generally link the URL where the respective credential is utilized, meaning infostealers gain access not only to the plain text credential but also all of the sites and services associated with it. This can fuel credential stuffing and password spraying attacks against additional sites and organizations, and lead to major reputational headaches for the company found to be the source of the breach.

Another password issue is that people typically practice terrible security hygiene and use the same one for numerous work and personal accounts. This means that there is an enterprise threat even if an employee only uses a password manager for the latter, as there's a possibility the credential is the same or very similar to their corporate passwords.

Bypassing MFA

Infostealers are also upending multi-factor authentication's reputation as an effective password hardening tool. MFA is often skipped if the device has previously logged into the account and is trusted, which is generally accomplished by session tokens stored in the cookies. The malware can be used to steal this stored data, rendering MFA ineffective. This unauthorized access can result in further extraction of corporate data or the deployment of ransomware, which can cause significant financial loss and reputational damage.

The Path Forward

As with all security vulnerabilities, there is no single solution for combating infostealers. Rather, companies must deploy a layered strategy that comprises the following considerations:

- **Education:** Ongoing guidance about how to discern the differences between a legitimate site or service and a fake one is vital. As mentioned above, AI has simplified the process of replicating logos and designs, and it's also enabling the creation of more legitimate-sounding emails and website copy. Urge employees to check whether a website is using SSL/TLS certificates, understand what source the link is coming from, and ensure that the "Contacts" section contains a physical address and phone number.

- **Anti-Malware and Endpoint Detection and Response (EDR):** Modern EDR tools and anti-malware capabilities are evolving to combat infostealers by focusing on both prevention and post-compromise detection. It's critical that enterprises invest in these solutions, but they should also recognize their limitations. EDR can generate false positives, and acting on alerts effectively depends heavily on the security team's skill and capacity. Zero-day exploits and other attacks that use novel code or new behaviors can also evade detection entirely.

- **Look Outside the Perimeter:** Arguably the largest gap in both EDR and anti-malware is that they cannot identify threats outside of the network. As such, another important component is understanding what information exists on the Dark Web—before it can be weaponized against employees or organizations. By identifying credential exposure, companies can act to protect accounts before threat actors can exploit infostealer data.

The infostealer landscape is rapidly evolving, but the malware's popularity underscores that hacker behavior is shifting from scale to precision. In this environment, early warning is especially valuable as infostealers compress the timeline between credential theft and account takeover. Strong endpoint controls and user training remain essential, but they are most effective when paired with rapid detection of leaked access data. Organizations must evolve their cybersecurity postures accordingly, or risk the massive fallout associated with modern data breaches.

About the Author

Mike Wilson is the founder and CTO of Enzoic, a leading provider of compromised credential detection and account takeover prevention solutions. Mike has spent 20 years in software development, with 15 years specifically in the information security space, at companies like Webroot and LogicNow. Mike started his career in the high-security environment at NASA, working on the mission control center redevelopment project. Apart from his security experience, Mike also founded several successful startups over the years. Connect with him here and on Twitter and LinkedIn.