NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

SEO Poisoning

What is an information stealer?

An information stealer, or infostealer, is a type of malware designed to covertly collect sensitive data from a victim's device and send it to threat actors. This malware can steal personal information such as usernames and passwords, financial details, browser history, and other data on a system.

How does infostealer malware function?

Infostealers are typically compact and have limited functionality compared to other malware, allowing them to execute quickly, steal data, and self-delete. They frequently abuse trusted system processes or legitimate software, such as browsers or email clients, mimicking normal activity to evade detection. Developers often make slight code changes to avoid signature-based detection, with polymorphic versions continuously altering their code to bypass antivirus software that relies on static signatures.

How do information stealers get on my device?

- *Malicious email attachments*: A user receives an email with an attachment that appears to be legitimate such as an invoice. When the user downloads and opens the attachment, they might be downloading an infostealer.
- *Malicious links*: A user clicks on a seemingly legitimate link within a phishing email. When clicked this link could lead the user to download an infostealer.
- *SEO Poisoning or Malvertising*: This occurs when legitimate services (e.g., Google, Bing, Facebook) unknowingly host harmful search results or advertisements. When users click on these, they are often redirected to a site that prompts them to download and install an infostealer disguised as legitimate content.
- *Greyware*: also known as potentially unwanted programs (PUP), refers to software that provides a legitimate function, like PDF conversion or media editing, but may also include hidden malicious features. Some browser extensions, for instance, have been found to contain information stealing capabilities alongside their advertised functionality.

What is the goal of information stealing malware?

The primary goal of information-stealing malware is to collect sensitive data from victims, such as login credentials, financial information, browser history, or system details, and then exfiltrate it to the attacker. This stolen data is often sold on dark markets by Initial Access Brokers. Initial Access Brokers act as intermediaries, providing this stolen access to other cybercriminals, such as ransomware operators, who can exploit the victim's data further. Ultimately, infostealers serve as a key component in larger cybercrime ecosystems, enabling further attacks.

If you suspect or discover an infostealer on your machine -

- Use a separate computer to change all passwords on a clean device, especially for critical accounts (email, banking, healthcare etc.).
- Check for unusual activity on all accounts and systems.
- Enable multi-factor authentication (MFA) on all accounts where possible.
- If possible, restore your system from a backup created before the infection.
- Continue to monitor for signs of continued compromise or suspicious behavior.

Prevention tips -

- Be cautious about opening unexpected email or social media message attachment or links.
- Use anti-malware solutions.
- Only download from trusted sources, avoid illegitimate or pirated software, applications, and games. These areas the main source of info stealing malware.
- Enable MFA on accounts – this makes it harder for cybercriminals to utilize stolen credentials.