Infostealers grow in popularity as revenue-generating attack

BACKGROUND

Information-stealers, aka infostealers, are trojan-type malware that, as the name suggests, steal sensitive information from compromised systems. Typically, this information is then either sold to other threat actors for monetary gain, used to make purchases, or is used in follow-on attacks. For example, if an attacker steals login credentials, they could potentially gain access to other parts of the system or use the credentials in a separate attack to gain initial access to a more hardened target.

TOP THREATS

- Adversaries can use their preferred method to drop infostealers, whether it be phishing messages, malvertising or malicious links on forums.
- While the primary function of infostealers has traditionally been to steal data, they are also used to drop other malware or facilitate additional stages of an attack, such as lateral movement.
- Collected data may include financial information like cryptocurrency wallets, login credentials, information stored on the infected device, browser data, system environment data and more.

OUTLOOK

- Cisco Talos expects infostealers' popularity to grow as it has over the past several years.
- Infostealers will likely remain a threat regardless of new malware variants or targeting trends like stealing cryptowallets, as infostealers are highly versatile and can be used in conjunction with adversarys' preferred tools and tactics, techniques, and procedures (TTPs).
- Many infostealers are sold on the dark web using the increasingly popular "as-a-service" business model.Many infostealers are designed to be used by technically unsavvy adversaries and have cracked or free versions now widely available on underground forums, expanding their availability. These malware families can be bundled with other malware as a promotional "bonus."
- Redline, Raccoon and Impacket are popular infostealers that are currently active in the wild and have appeared in Cisco Talos Incident Response engagements this year.

AFFECTED INDUSTRIES/GROUPS

- Anyone can be a target of an information-stealer. CTIR has seen a variety of industries and organizations targeted by these threats. Infostealers can be delivered in many ways, including emails, SMS messages and malicious online advertisements.
- Adversaries have exploited many publicly available vulnerabilities to deliver infostealers, including targeting Chromium-based browsers and Microsoft's Internet Explorer browsers.

HOW ARE OUR CUSTOMERS PROTECTED?

- Cisco Secure Endpoint deploys coverage into users' environments, blocking many forms of infostealers from entering the environment.
  - Specific ClamAV signatures and Snort rules written by Cisco Talos can detect the deployment of infostealers and attempts to exploit commonly known vulnerabilities.
- Cisco Talos Incident Response can assist customers in preparing for an attack and discovering any potential points of entry.
- All organizations should enforce multi-factor authentication (MFA), such as Duo Security, across their environments, especially on all remote access applications and services, including webmail or cloud-based email.