Roses Are Red(Line): Why Credential-Stealing Malware is Giving SOC Teams the Blues

Ransomware continues to take a toll on businesses across the globe, with 66% of organizations hit by ransomware in 2021, compared to 37% the prior year. A common precursor to ransomware attacks is malware infections, which came in as the second highest breach action last year with over 30% involving some type of malware. There have been more than 2.8 billion malware attacks recorded in the first half of this year alone.

One of the biggest ransomware prevention challenges for Security Operations Center (SOC) teams is the lack of visibility into malware infections, which essentially give the adversary a pathway into your organization. Malware-infected devices present high-risk because they enable threat actors to siphon employee credentials, cookies (even from SSO instances), and other data that helps them infiltrate your business via ATO or session hijacking.

But your existing tools won't surface every malware infection alert, and if you have a bring-your-own-device (BYOD) environment that allows the use of unmanaged employee devices, you won't have visibility of all malware infections. That's why prevention must be the critical focus for SOC teams.

Let's dive into what you need to know about credential-stealing malware and its tie to ransomware attacks,

How InfoStealers Create Exposure

Credential-stealing malware is a type of infostealer that was designed for (surprise!) stealing credentials, but can also siphon other data, such as browser fingerprints and session cookies, from the infected device. Using this stolen data and anti-detect browsers, adversaries can log into an employee's accounts like a legitimate user and bypass multi-factor authentication (MFA) while the session cookies are still fresh.

RedLine Stealer, an infostealer that first appeared for sale in the criminal underground in March 2020, quickly became wildly popular among cybercriminals. For instance, half of the stolen data logs on the underground marketplace "2easy" – which experienced rapid growth recently – came from RedLine Stealer. SpyCloud researchers found that RedLine Stealer was one of the most commonly used infostealers for Windows last year.

One example of a RedLine Stealer-related incident involved stolen virtual private network (VPN) credentials. The breached company provided a VPN to remote employees for accessing the corporate network, and one of the employees saved the VPN login in a web browser. Their anti-malware software didn't detect RedLine Stealer, which harvested data from the infected device. Three months later, threat actors used the leaked VPN credentials to breach the company's network.

Unfortunately, saving logins in the browser is a common behavior among employees. And RedLine Stealer doesn't stop at browsers – it can siphon credentials from other apps. While stolen credentials may seem of little value if you have MFA deployed, that's not the case with infostealers since the adversary can bypass MFA using stolen session cookies, session tokens, and other digital fingerprinting data that helps impersonate the user.

Like typical malware, RedLine Stealer is often deployed through phishing email campaigns with malicious attachments, as well as through links in social media comments and direct messages. This infostealer can be found easily on the criminal underground for as little as $100 a month or an $800 "lifetime" subscription. The more recent versions include new capabilities and features, along with support, indicating that the RedLine operators intend to continue developing the malware. RedLine Stealer has a very low barrier of entry, as subscriptions come with all the tools needed to deploy it – which may be another reason why it's so popular.

Why RedLine Stealer Should Steal Your SOC's Attention

Ransomware operators typically outsource the first stage of their attack, the initial foothold, to specialized groups called initial access brokers. These brokers look for the easiest way in, often by impersonating an insider using stolen credentials and other data. That's why infostealers like RedLine Stealer are so effective for cybercriminals – the credentials and cookie data are straight from the endpoint, increasing the attackers' odds of success.

For your SOC team, RedLine Stealer is a problem for several reasons:

- Your anti-malware solution won't always catch credential-stealing malware. Even if you detect the malware and remediate the infection, the damage is done and the stolen data is already exposed, inviting future attacks. And you may not even know about malware-stolen credentials and cookies until they show up on the dark web. But most teams don't take post-remediation steps such as invalidating active web session cookies to address long-term ransomware risks.
- Your team needs to know what systems, applications, and users have been compromised, and what kind of data the malware has stolen as close to real time as possible so you can remediate quickly. But if you have a BYOD policy and unmanaged devices tied to your environment, you have no visibility into those devices and your ability to scope the threat is limited.
- If an employee logs into (or uses a cookie to get into) SSO, the adversary will get free rein over all the user's critical workforce applications. With the SSO instance in the attacker's hands, access will persist even if the session is terminated because applications within the same portal will launch authentication sessions with their own session cookies.

Red Flags to Watch For

To proactively prevent ransomware attacks, we suggest one key recommendation for each of the above mentioned entry points.

Unusual behavior

SOC teams should know normal traffic patterns and behavior for application installation, usage, authentication attempts, etc. Having that baseline will help you spot when something's outside of typical parameters.

Unusual DNS queries

Since malware in your network will beacon to the master server or the command-and-control site, unusual DNS domain requests, unusual query failures, abnormal volumes, and other unusual DNS activity should be investigated.

Application or file changes

Tools for monitoring file integrity can help detect unexpected changes to applications or files on laptops and servers, which are another indicator of malware presence.

To defend against infostealers and other forms of malware, we suggest:

- Implementing strong security policies around passwords to reduce the fallout from stolen credentials
- Properly maintain and monitor your attack surface by restricting the use of personal devices for accessing corporate assets
- Taking swift action to prevent unauthorized access when cookies from critical workforce services – such as a corporate Okta instance – are stolen from employees' infected personal or corporate devices

Locking down access has been a major theme for anyone paying close attention to headlines in the past year. If your team is blind to what malware-stolen data is in criminal hands, responding proactively will remain a challenge. Knowing what users are doing and what's executed on their endpoints is the first critical piece for anyone who wants to stand any chance of catching credential-stealing malware and preventing ransomware attacks.

Recent Posts

The Most Overlooked Ransomware Defenses
September 22, 2022

Three Common Entry Points for Ransomware
August 31, 2022

Don't Get Schooled by Cybercriminals: Back to School Cybersecurity Tips
August 25, 2022

Making the Internet a Safer Place: Celebrating Six Years of SpyCloud
August 9, 2022

Consumer or Fraudster? A Q&A with Fraud Prevention Experts
July 12, 2022