INFOSTEALER IDENTIFIED

A USE CASE FOR IDENTIFYING CREDENTIAL-STEALING MALWARE THROUGH DARK WEB MONITORING

INTRODUCTION

Infostealer malware has emerged as a rapidly growing threat in recent years, with 2024 research showing a 266 percent year-on-year increase[1] in infostealer activity. Data theft and leak incidents also rose to 32 percent of cyberattacks in the same year, moving past "extortion" as the attack type that has the largest impact.

The rise in infostealer incidents highlights the thriving market for stolen credential data, which cybercriminals sell to facilitate further cyberattacks. It can also be linked to the growth of Malware-as-a-Service (MaaS), which has made infostealers readily available on the dark web and lowered the technical barrier for entry for hackers.

Infostealers are a specific type of malware that are designed to be persistent and benign while collecting sensitive information from infected devices. The data they collect varies but typically includes the normal targets of data-driven cybercrime like personal details, financial information, and login credentials, to name but a few.

User devices are often initially compromised by phishing emails with infostealers embedded in harmful attachments, fake software, or malicious advertisements on legitimate websites such as social media.

266% YEAR-ON-YEAR **INCREASE IN INFOSTEALER ACTIVITY**[1]

Once installed, this type of malware is built to bypass anti-virus detection. Masquerading as legitimate applications, they reside within a compromised device for a period of time sufficient enough to collect and transfer user data to a server operated by the attackers.

The stolen data is then packaged up and exported, ready to be used for financial gain. We regularly observe this type of data being sold on dark web markets (known as autoshops) relatively cheaply, usually in the region of $10. If the infostealer has collected very valuable information, prices can increase to several hundred dollars.

This report takes a real life example of an infostealer infection of an international professional services firm to demonstrate the challenges this type of malware creates for cybersecurity teams and how they can be overcome through dark web monitoring.

[1] https://www.ibm.com/reports/threat-intelligence

MARCH 2023

- An employee downloads corrupted software, infecting their device with an infostealer.
- The corrupted software is shared among the team in the office, whose data is harvested and published on the dark web.

JANUARY 2024

- The company procures Searchlight Cyber's dark web monitoring solution, which immediately identifies the stolen credentials on the dark web.
- Remediative action is immediately undertaken to protect the impacted employee's accounts.
- An investigation finds that a fake TeamViewer application infected with Raccoon Stealer was the source of the leak.
- Security team removes malware and updates security policy to increase staff awareness and reduce the risk of future incidents.

UNCOVERING DARK WEB EXPOSURE

A professional services firm with offices across the globe partnered with us to understand and mitigate their dark web risk.

In January 2024, the firm used the external attack surface management (EASM) capability in the Searchlight Cyber dark web monitoring platform to map their external attack surface and pull together an inventory of their digital assets, including IPs, domains and subdomains and identify any vulnerabilities, misconfigurations, and exposed credentials.

Our platform combines traditional EASM with dark web monitoring, for a more holistic external view of the attack surface. In this case, it allowed the firm to identify a data breach that hadn't been identified with their other cybersecurity tools: leaked credentials related to one of the organization's branches that were available for sale on a dark web forum.

IDENTIFYING AN INFOSTEALER INFECTION

Identifying the leaked credentials immediately allowed the organization to implement mitigation efforts, such as password changes and additional security for the impacted staff members - who were all based in the same regional office.

However, the next step was for the organization to identify the source of the data leak because - if it was a result of malware - there was a high likelihood that the machines were still infected and further data breaches would occur unless the malware was remediated. Understanding the origin of leaked credentials allows businesses to contain the threat and prevent it from impacting the business again or even spread further.

In this case, our dark web monitoring solution allowed the professional services firm to determine that the credential leak originated from an infostealer infection, specifically from the malware strain Raccoon Stealer.

Reviewing the details of the logs, the security team determined that all of the infected devices were compromised on the same date in March 2023. Due to the nature of infostealers, the malware was able to remain undetected until January 2024 when the firm used Searchlight Cyber for their asset discovery.

ABOUT RACCOON STEALER

First observed in April 2019, Raccoon Stealer is a relatively inexpensive infostealer, commonly sold through a Malware-as-a-Service (MaaS) model to cybercriminals. Its payload is a modular C/C++ binary designed to infect 32-bit and 64-bit Windows-based systems for only $75 per week, or $200 monthly. It is known to target infected users' browser autofill passwords, history, cookies, credit cards, usernames, passwords, and crypto wallets.

INVESTIGATION AND REMEDIATION

Once the infostealer strain was determined, the company's cybersecurity team were able to track the introduction of the infostealer malware to one person's device and establish that the initial compromise occurred when an employee inadvertently downloaded a fake copy of TeamViewer from an unreliable source. The Racoon malware embedded in the corrupted application and compromised the employee's device.

After further exploration, it was discovered that the employee had shared the link to the fake website with other colleagues in the office, who then proceeded to download the malware-infected software onto their devices.

With the ability to see which of the team's credentials had been compromised, the security team took action to remove the malware from all of the infected devices before any other cybersecurity incidents could occur. Without the intelligence on the infostealer infection, the malware would have laid dormant within the devices and more credentials could have been harvested in the future.

> “WITHOUT THE INTELLIGENCE ON THE INFOSTEALER INFECTION, THE MALWARE WOULD HAVE LAID DORMANT WITHIN THE DEVICES AND MORE CREDENTIALS COULD HAVE BEEN HARVESTED IN THE FUTURE.

CONTINUED SECURITY IMPROVEMENT

The professional services company now uses Searchlight to continuously monitor the dark web for leaked credentials and other cybersecurity threats. This enabled the security team to assess that the clean up process of the infected devices had been successful and means that they will be more proactive in catching the next attack. This proactive monitoring of the dark web is important because the sooner a breach is identified, the quicker the threat can be mitigated and the less damage that can be inflicted on the organization.

The organization has also used this incident to inform other cybersecurity procedures, including employee training and the creation of a central repository for trusted applications to avoid other instances of malicious software being downloaded by employees.

SUMMARY

This example demonstrates the importance of proactive dark web monitoring and actionable intelligence in preventing cyberattacks.

Identification

The professional services firm was able to identify leaked credentials, trace the source of the breach to infostealer malware, and pinpoint the infected devices.

Continuous Monitoring

Searchlight Cyber allowed the security team to continuously monitor the dark web for leaked credentials, to ensure all infiltrated devices were cleaned during the remediation process.

Process

Understanding the source of the infostealer infiltration allowed the organization to implement new security policies and procedures that will enable a better security posture.

USE SEARCHLIGHT TO MONITOR FOR INFOSTEALERS AND LEAKED CREDENTIALS

Searchlight Cyber empowers organizations to proactively identify early warning signs of cyberattacks by monitoring the dark web for indications of compromised data, malicious activity, or targeted threats.

DARK WEB MONITORING

Automatically monitor for hidden dark web threats and cybercriminal activity before it escalates. Searchlight Cyber's dark web monitoring tool detects, categorizes, and alerts organizations to imminent threats so security teams can take quick preventative action.

COMBINED WITH EASM

EASM and dark web monitoring work together to create a more holistic view of cybersecurity threats. While EASM focuses on identifying vulnerabilities within an organization's public-facing digital assets, dark web monitoring helps to detect if any sensitive data or credentials has been compromised and shared on the dark web in forums, marketplace or by Initial Access Brokers.

COMPREHENSIVE DARK WEB DATASET

Searchlight Cyber draws from the world's most comprehensive dark web dataset. With 15 years of data, organizations can have access to - and can gather intelligence from - live and historical dark web marketplaces and forums. This ensures organizations can see the full picture when conducting dark web investigations.

SEARCHLIGHT.
CYBER

VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE OR BOOK A DEMO NOW.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
200 Massachusetts
Avenue Northwest,
Washington, DC 20001
United States