RedLine Stealer: Incident Analysis, Detection, and Mitigation Report

A Threat Assessment of a Credential-Stealing Malware-as-a-Service Infostealer

Rishan Tamrakar

***Abstract*—This report examines RedLine Stealer, an infostealer that was apprehended in October 2024 by international law enforcement authorities during Operation Magnus. It categorises the threat, identifies the endpoint and identity vulnerabilities exploited, highlights indicators of detection, and provides recommendations by ranking controls from most to least significant, including the importance of symmetric encryption and proper handling of keys for securing credential information.**

***Key Terms*—Infostealer, Malware-as-a-Service (MaaS), Indicators of Compromise (IoC), Endpoint Detection and Response (EDR), Symmetric Encryption**

I. INTRODUCTION

Credential-stealing software is one of the most dangerous types of malware affecting organisations, as it connects ransomware and business email compromise via the initial-access-broker economy. The analysis of RedLine Stealer throughout this report is based on the material covered in the first to fourth lectures and practicals of Weeks 3–4.

II. INCIDENT OVERVIEW AND THREAT CLASSIFICATION

RedLine Stealer, identified in 2020, operates as a malware-as-a-service (MaaS) infostealer. By 2024, it had become the most prevalent form of credential-stealing malware [4]. On October 28, 2024, Operation Magnus, a coordinated effort by the Dutch National Police, the FBI, Eurojust, and international partners, resulted in the seizure of three servers and two domains. This operation disrupted an infrastructure estimated to comprise over 1,200 servers globally. Concurrently, the US Department of Justice unsealed charges against an alleged developer associated with the malware [9].

Adopting the threat management framework outlined by the ACSC [2], RedLine is categorised as credential-stealing spyware or Trojan malware. Its primary objective is financial gain, achieved by exfiltrating sensitive data such as login credentials, browser cookies, VPN access details, and cryptocurrency wallet information. This harvested data is compiled into "stealer logs" and subsequently sold on cybercriminal marketplaces or to initial access brokers. The affected assets typically include end-user endpoints and browser credential stores; indirectly, any corporate systems accessible via compromised credentials are also at risk. The primary impact on the CIA triad (Confidentiality, Integrity, Availability) is a severe loss of confidentiality due to the extensive exfiltration of authentication data. Integrity is compromised when session cookies are leveraged for account takeover. Availability is affected only indirectly, often as a precursor to further attacks such as ransomware deployment enabled by the compromised access.

III. ATTACK PATH AND VULNERABILITY ANALYSIS

Figure 1 summarises the four stages of a typical RedLine Stealer compromise, from initial dissemination through to the endpoint and identity vulnerabilities that are ultimately exploited.

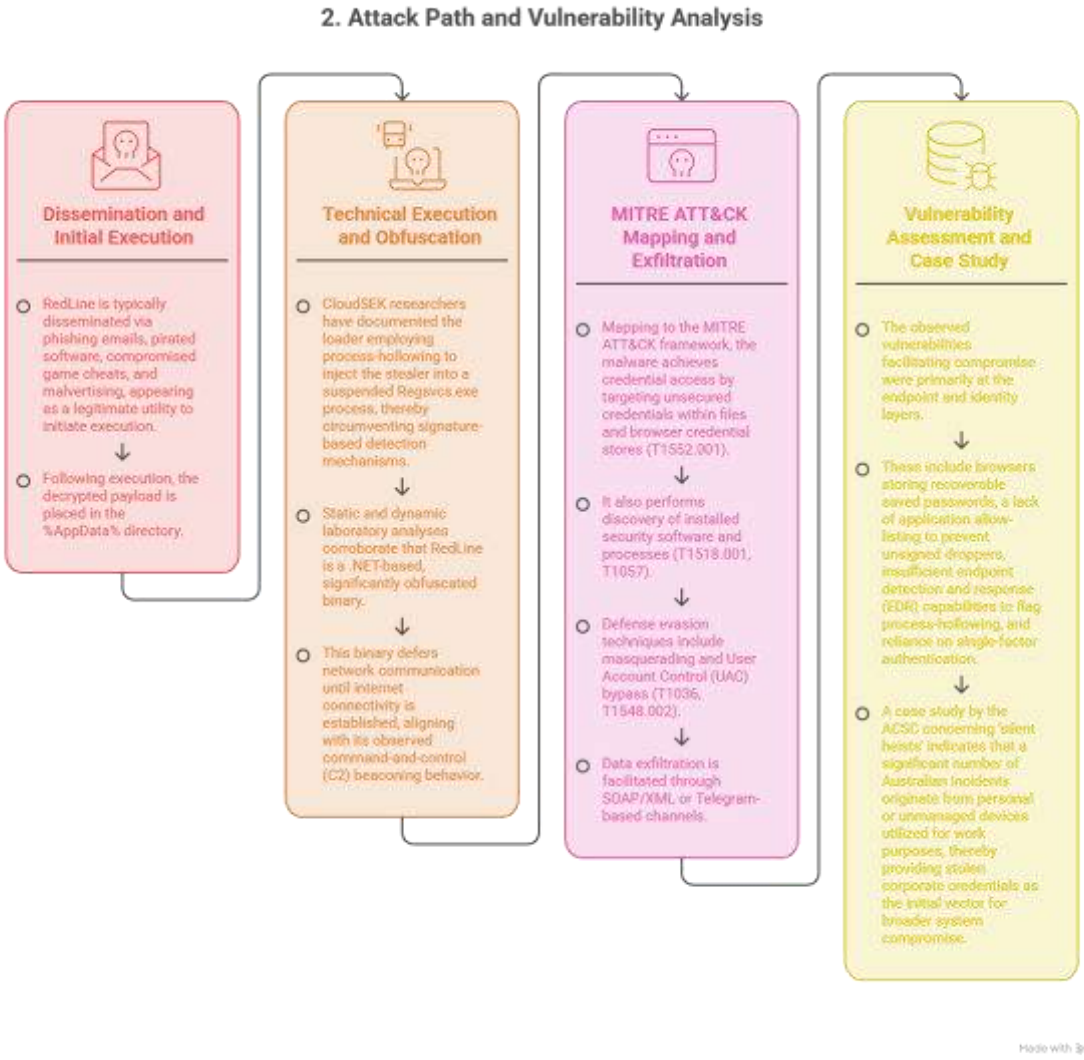

Fig. 1. Attack path and vulnerability analysis for a RedLine Stealer compromise.

IV. DETECTION EVIDENCE AND IMMEDIATE RESPONSE

Four indicators are commonly associated with RedLine compromise. The first is anomalous child-process behaviour, where a trusted binary such as Regsvcs.exe is initiated in a suspended state and then hollowed out — a phenomenon detectable via EDR process-lineage telemetry. The second involves Windows Security Event ID 4663, which logs unusual processes accessing browser credential and cookie database files; this event is identified by the Splunk Threat Research Team as a critical detection point for stealer malware activity [8]. The third indicator is unexpected outbound connections to unfamiliar domains or Telegram infrastructure, often transmitting structured exfiltration traffic shortly after execution. Finally, the fourth indicator is the appearance of a new, unsigned executable in the %AppData% directory, characterised by a mismatched or randomised filename and lacking any legitimate installation record.

In response to these indicators, immediate actions are recommended. These include isolating the affected endpoint from the network to prevent further data exfiltration. Additionally, all credentials and cached session cookies on the device should be considered compromised, necessitating a forced reset and re-authentication process, as stolen session tokens can circumvent standard password resets. Before undertaking remediation, capturing forensic memory and disk images is crucial for preserving evidence and facilitating root-cause analysis. Lastly, consulting threat intelligence sources for the device or associated domains within known stealer-log marketplaces can help ascertain the scope of the compromise.

The provided information does not include details on the deployment or operation of the malware itself, in keeping with the assessment requirements.

V. SECURITY CONTROLS AND SYMMETRIC CRYPTOGRAPHY

Figure 2 outlines the recommended security controls and cryptographic practices for mitigating the risks posed by RedLine Stealer and similar credential-stealing malware.

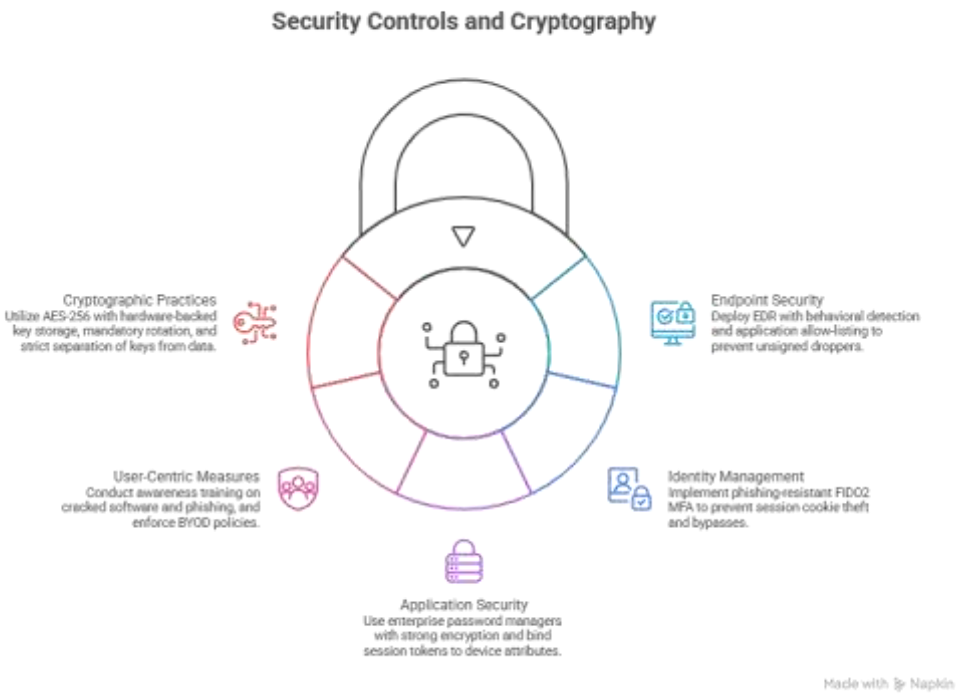

Fig. 2. Security controls and cryptographic practices for mitigating RedLine Stealer risk.

VI. CONCLUSION

The primary vector for RedLine-style compromises appears to be the execution of obfuscated dropper malware, often distributed through phishing campaigns or compromised software, on endpoints lacking robust security controls. Critical deficiencies include the absence of application allow-listing and the use of authentication methods that are not resistant to phishing. The most significant business impact stems from the silent, widespread exfiltration of credentials and session cookies, which facilitates undetected initial access for subsequent ransomware attacks or business email compromise schemes.

To mitigate this threat, organisations should prioritise three key actions. First, implement multi-factor authentication (MFA) that is resistant to phishing attacks, and immediately rotate or revoke all active sessions and credentials associated with compromised devices. Second, deploy endpoint detection and response (EDR) solutions that incorporate behavioural detection capabilities, in conjunction with application allow-listing. Third, establish and enforce clear policies governing Bring Your Own Device (BYOD) and software usage, reinforced through mandatory security-awareness training programs.

REFERENCES

[1] Australian Cyber Security Centre. (2024, September 2). The silent heist: Cybercriminals use information stealer malware to compromise corporate networks. Cyber.gov.au. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/silent-heist-cybercriminals-use-information-stealer-malware-compromise-corporate-networks

[2] Australian Cyber Security Centre. (n.d.). Information stealer malware. Cyber.gov.au. https://www.cyber.gov.au/threats/types-threats/malware/information-stealer-malware

[3] CloudSEK. (n.d.). Technical analysis of the RedLine stealer. https://www.cloudsek.com/blog/technical-analysis-of-the-redline-stealer

[4] MITRE ATT&CK. (n.d.). RedLine Stealer, Software S1240. https://attack.mitre.org/software/S1240/

[5] National Institute of Standards and Technology. (2020). Recommendation for key management: Part 1 – General (NIST SP 800-57 Part 1 Rev. 5). U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final

[6] Ramadan, F., & Hikmah, I. R. (2023). Redline stealer malware analysis with surface, runtime, and static code methods. In 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs) (pp. 205–211). IEEE. https://doi.org/10.1109/ICoCICs58778.2023.10276709

[7] SecurityScorecard. (2026, May 20). A detailed analysis of the RedLine stealer. https://securityscorecard.com/research/detailed-analysis-redline-stealer/

[8] Splunk Threat Research Team. (2023, June 1). Do not cross the 'RedLine' stealer: Detections and analysis. Splunk. https://www.splunk.com/en_us/blog/security/do-not-cross-the-redline-stealer-detections-and-analysis.html