Integrated Cyber Threat Intelligence

Technical Intelligence Analysis Report

Name: Seerat E Marryum

Bytewise Limited Cyber Security Track

Submitted to: Sir Tayyab

Submission date: 4 September, 24

Contents

1. Introduction

This report provides a detailed technical analysis of the malware "SpecterDrop" and "ShadowFrost," both part of the Specter APT group's multi-stage attack. The report includes an in-depth examination of infection methods, persistence mechanisms, obfuscation techniques, and ransomware encryption strategies. Additionally, comprehensive indicators of compromise (IOCs) and recommended technical controls for detection and mitigation are outlined.

1. Detailed Malware Behavior

SpecterDrop

- **Infection Methods:**
  - Delivered primarily via phishing emails containing malicious attachments or links to compromised websites.
  - Exploits common vulnerabilities (e.g., CVE-2021-40444) in Microsoft Office and web browsers to execute malicious code on the target system.
- **Persistence Techniques:**
  - Creates registry keys to launch on startup (e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Run).
  - Installs scheduled tasks to periodically re-execute the malware if removed.
  - Uses fileless persistence by injecting code into legitimate processes such as svchost.exe.
- **Obfuscation Strategies:**

- Heavily obfuscated PowerShell scripts and shellcode are used to evade detection by static analysis tools.
- Uses dynamic API resolving techniques to load functions at runtime, making reverse engineering more difficult.
- Encrypts payloads with AES-256, decrypting them only in memory during execution.

ShadowFrost

- **Infection Methods:**
  - Propagates within the network by exploiting SMB vulnerabilities and brute-forcing weak admin credentials.
  - Uses lateral movement techniques such as Pass-the-Hash and exploits known vulnerabilities in outdated software versions (e.g., EternalBlue).
- **Persistence Techniques:**
  - Installs backdoors and creates hidden user accounts with elevated privileges.
  - Manipulates Group Policy Objects (GPOs) to ensure continuous access to compromised systems.
  - Modifies boot scripts to launch malicious binaries during system startup.
- **Obfuscation Strategies:**
  - Encrypts communication channels with command-and-control (C2) servers using TLS to avoid detection.
  - Implements process hollowing, replacing the memory of legitimate processes with malicious code.

- Employs polymorphic code, altering itself with each infection to evade signature-based detection.

2. Indicators of Compromise (IOCs)

SpecterDrop IOCs:

- **File Hashes:**
  - MD5: 1a2b3c4d5e6f7g8h9i0jklmnopqrst
  - SHA256: abcd1234efgh5678ijkl9101mnopqrstuvwxyza1234567890bcdef123456789
- **Registry Keys:**
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SpecterDrop
- **Network Indicators:**
  - Communication with suspicious IPs: 192.168.0.100, 203.0.113.50
  - C2 domain: malicious-domain.example.com

ShadowFrost IOCs:

- **File Hashes:**
  - MD5: abcdef1234567890abcdef1234567890
  - SHA256: 123456abcdef7890abcdef123456abcdef123456abcdef7890abcdef123456
- **Registry Keys:**
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ShadowFrost
- **Network Indicators:**
  - C2 traffic over TLS to shadowfrost-c2.example.com

- Malicious SMB connections from IP: 10.0.0.5

FrostLock Ransomware IOCs:

- **File Extensions:** .frostlock
- **Ransom Note:** README_FROSTLOCK.txt
- **Network Indicators:**
  - Outbound connections to known ransomware C2 servers, e.g., frostlock-decrypt.example.com

3. Technical Controls and Detection Strategies

1. Network Monitoring:

- Deploy intrusion detection/prevention systems (IDS/IPS) to monitor for C2 traffic and detect unusual outbound communications.
- Implement firewall rules to block known malicious IP addresses and domains associated with SpecterDrop and ShadowFrost.

2. Endpoint Detection:

- Use endpoint detection and response (EDR) solutions to identify abnormal process behavior and registry modifications indicative of SpecterDrop.
- Monitor for fileless malware execution and PowerShell script abuse.

3. Ransomware Mitigation:

- Deploy automated backup solutions and isolate critical systems to minimize ransomware impact.
- Use decryption tools, if available, to recover encrypted files; otherwise, ensure comprehensive incident response planning to avoid paying ransoms.

4. Network Segmentation and Least Privilege:

- Enforce network segmentation to contain the spread of malware like ShadowFrost.

- Apply the principle of least privilege to minimize exposure and reduce the risk of lateral movement.

4. Regular Software Updates:

- Ensure all systems are patched and up to date to prevent exploitation of known vulnerabilities.
- Use vulnerability scanners to identify and prioritize critical security gaps.

5. Conclusion

SpecterDrop and ShadowFrost pose significant threats to organizations due to their sophisticated infection methods, persistence techniques, and obfuscation strategies. By implementing the recommended detection strategies and technical controls, organizations can enhance their defenses against these advanced malware variants and mitigate their impact.
