Technical Report – Stealer's Shadow Investigation

1. Executive Summary

The WK001 workstation used by a.smith@megacorpone.com was compromised via a phishing email that led to the execution of a malicious HTA file. The attacker downloaded and ran a disguised .epub executable, exfiltrated sensitive data, and communicated with a command and control server.

2. Exfiltrated Files & Tools

Exfiltrated file: 101010245WK001_protected.zip (SHA-256: 0324d54b…960d9c)- Exfiltration program: captcha_privacy[1].epub (SHA-256: a88fedc9…e96ed)

3. Download & Execution Method

The malicious .epub was downloaded through IMEWDBLD.EXE (LOLBin abuse) triggered by mshta.exe. Registry hijacking allowed .epub files to run as executables.

4. Attack Chain

Summary - Phishing email → fake CAPTCHA page- Payload command retrieved via Ethereum smart contract- User tricked into running mshta.exe- HTA downloaded malware via IMEWDBLD.EXE - Registry hijack → execution of .epub malware- C2 communication and data exfiltration

5. C2 Endpoints /life (heartbeat), /send_message (exfiltration), /receive_message (commands), /feed (covert config channel).

6. Data Protection Exfiltrated ZIP encrypted with WinZip AE-2 (AES-256). Password = Machine GUID + Hostname: cc9441e5-1c80-4287-9c7a-4c03215c0969WK001

7. Compromised Credentials Credentials extracted from Chrome for Azure and Google Workspace.

8. Attacker IPs 99.91.94.11 – phishing 31.17.87.96 – blockchain RPC 145.1.0.92 – C2 & hosting

9. Timeline (UTC) 08:35 – Phishing email received 09:01 – HTA executed, malware downloaded and run 09:01+ – C2 established 09:02 – Data exfiltration completed

10. Security Recommendations Immediate: isolate WK001, reset passwords, enable MFA, block malicious IPs. Long-term: improve email filtering, block LOLBins, monitor registry changes, enhance user awareness.

11. Indicators of Compromise IPs, URLs, file hashes, blockchain contract, registry modification (.epub → exefile).

Conclusion

Stealer's Shadow used social engineering, LOLBins, and blockchain-based payload delivery to bypass defenses. Compromised cloud credentials pose significant ongoing risk