FINALDRAFT Malware Abuses Outlook Drafts for Covert C2 Communication

Vairav Cyber Security News Report

Date: February 17, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Elastic Security Labs has identified FINALDRAFT, a sophisticated malware family used for cyber espionage. This malware exploits Microsoft Outlook drafts as a covert command-and-control (C2) channel via the Microsoft Graph API, enabling stealthy communication. The malware includes a loader (PATHLOADER), a backdoor, and multiple submodules, all designed for data exfiltration, process injection, and network proxying.

Windows and Linux variants have been discovered, indicating a well-developed cross-platform malware framework. The long-term engineering efforts and sophisticated evasion techniques suggest that FINALDRAFT is operated by an advanced and well-funded threat actor engaged in espionage operations.

DETAILS OF THE INCIDENT

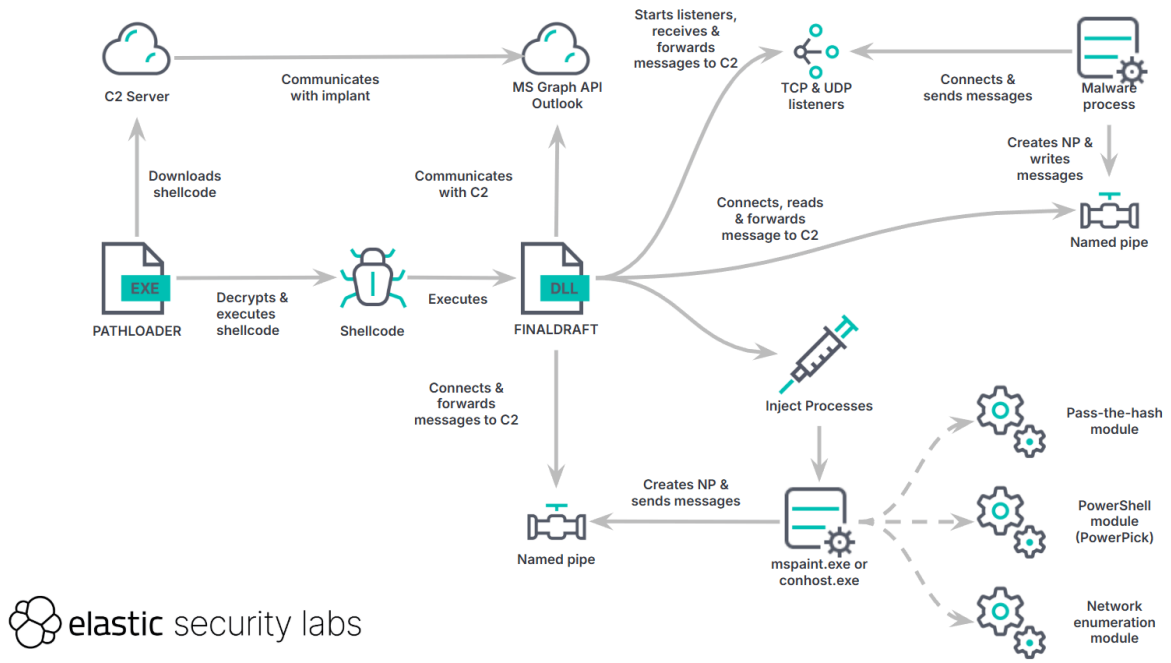

Figure 1: Infection chain

FINALDRAFT is deployed via PATHLOADER, a lightweight Windows PE executable that downloads and decrypts AES-encrypted shellcode before executing it in memory. To avoid detection, it employs API hashing, obfuscation, and sandbox evasion techniques. The malware's embedded configuration includes typosquatted domains imitating security vendors such as Check Point *(checkponit.com*) and Fortinet *(fortineat.com)* to blend malicious traffic with legitimate network activity.

A key feature of FINALDRAFT is its use of Outlook mail drafts for C2 communication, allowing it to avoid direct network connections that could trigger security alerts. The malware creates draft emails to send and receive commands, ensuring minimal network footprints. It supports various attack techniques, including process injections using VirtualAllocEx, WriteProcessMemory, and RtlCreateUserThread API calls. Additionally, the Linux variant extends its capabilities with multiple C2 transport protocols such as HTTP/HTTPS, UDP, ICMP, and DNS.

FINALDRAFT poses a severe threat due to its stealthy nature and espionage-focused capabilities. By leveraging Outlook drafts as a C2 channel, it bypasses traditional network security defenses. Its ability to inject malicious code, manipulate files, and establish proxy connections enables attackers to maintain persistent access to compromised systems. The cross-platform design also suggests a broader target scope, including enterprises running both Windows and Linux environments. If undetected, this malware can facilitate data theft, credential compromise, and long-term surveillance of high-value targets.

RECOMMENDED ACTIONS

- **Monitor Outlook API Activity** – Detect suspicious draft modifications and unauthorized use of mail services.
- **Deploy Advanced Endpoint Detection & Response (EDR)** – Identify malware persistence techniques and prevent unauthorized API access.
- **Block Known C2 Domains** – Prevent communication with attacker-controlled domains such as *checkponit.com* and *fortineat.com.*
- **Network Segmentation** – Isolate high-risk endpoints to minimize lateral movement within the network.
- **Security Awareness Training** – Educate employees about social engineering risks and phishing tactics used for initial infection.
- **Threat Hunting & YARA Rules** – Implement proactive threat-hunting measures and use YARA rules to detect anomalies in log events.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://securityonline.info/finaldraft-malware-exploits-outlook-drafts-for-covert-communication/

https://www.elastic.co/security-labs/finaldraft

https://www.elastic.co/security-labs/fragile-web-ref7707

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com