CIRT.GY Guyana National Computer Incident Response Team

AL2025_12 FinalDraft Malware Abuses Outlook for Stealthy Communications (18th February 2025)

Description

A newly discovered malware, FinalDraft, has been leveraging Outlook email drafts for stealthy command-and-control (C2) communication. The malware was uncovered by Elastic Security Labs during an investigation into cyber-espionage attacks against a South American foreign ministry. By abusing Microsoft Outlook's email draft functionality, the malware avoids detection while executing various malicious activities such as data exfiltration, process injection, and network proxying.

Attack Details

The attack chain involves multiple stages, beginning with the deployment of PathLoader, a small executable designed to execute shellcode. PathLoader is responsible for injecting FinalDraft, which then establishes communication with the attacker’s command infrastructure via Microsoft Graph API. The attack starts with the execution of PathLoader on the victim’s machine, which retrieves and executes FinalDraft from the attacker’s infrastructure. Once active, FinalDraft generates a session ID and retrieves an OAuth token from Microsoft using a refresh token embedded in its configuration. This token is then stored in the Windows Registry for persistent access. For communication, FinalDraft stores commands from the attacker in Outlook drafts using a structured naming convention (r_<session-id> for requests and p_<session-id> for responses). These drafts are deleted after execution, making forensic analysis and detection significantly harder.

FinalDraft supports 37 malicious commands, including data exfiltration (extracting files, credentials, and system information), process injection (running malicious payloads in legitimate Windows processes like mspaint.exe), pass-the-hash attacks (extracting authentication credentials for lateral movement), network proxying (establishing covert tunnels for persistent access), file operations (copying, deleting, or modifying files), and PowerShell execution (running PowerShell commands without launching powershell.exe). The malware has both Windows and Linux variants, with the Linux version leveraging REST API, Graph API, HTTP/HTTPS, reverse UDP & ICMP, bind/reverse TCP, and DNS-based C2 exchange, making it equally dangerous.

Remediation

Organizations can mitigate the risks associated with **FinalDraft** by implementing the following measures:

- **Monitor Outlook Draft Activity:** Establish logging and monitoring for frequent draft creation and deletion.
- **Harden Microsoft 365 Accounts:** Enforce Multi-Factor Authentication (MFA) and restrict OAuth token reuse.
- **Enable Advanced Threat Protection:** Use Microsoft Defender for Office 365 to detect suspicious API calls.
- **Perform Regular Endpoint Monitoring:** Deploy **EDR solutions** that can detect process injection attempts and unauthorized registry modifications.

- **Network Segmentation:** Limit outbound connections to prevent unauthorized Microsoft Graph API access.
- **Use YARA Rules:** Implement YARA rules provided by Elastic Security to detect PathLoader, GuidLoader, and FinalDraft.
- **Incident Response Plan:** Establish a rapid response strategy to contain infections, revoke compromised credentials and remove malicious persistence mechanisms.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Outlook Mail Service hijacked FinalDraft malware for covert communications. (n.d.). Retrieved from Vocal media 01. https://vocal.media/01/outlook-mail-service-hijacked-by-final-draft-malware-for-covert-communications
- Toulas, B. (2025, February 15). New FinalDraft malware abuses Outlook mail service for stealthy comms. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/new-finaldraft-malware-abuses-outlook-mail-service-for-stealthy-comms/