EnCyb

Severity: High

Advisory Type: Threat

ScarCruft (APT37) Cloud-Hosted Malware Delivery Campaign

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

ScarCruft (APT37) is actively conducting a targeted malware campaign that uses spear-phishing emails with OLE-enabled Microsoft Office documents to deliver malware. The campaign abuses trusted cloud services such as Google Drive, OneDrive, and Dropbox to download malicious payloads, helping the activity blend in with legitimate traffic and evade detection. Successful compromise enables remote access, data exfiltration, and long-term persistence on Windows systems, posing a high risk to government, research, media, and other high-value sectors.

- Active Region: Asia-Pacific (Primary), Global Potential
- Affected Sector: Government, Defense, Media, Research, NGOs
- Affected Product: Windows Endpoints
- Severity: High
- Published Date: February 09, 2026

TECHNICAL DETAILS

- **Initial Access:** ScarCruft uses targeted spear-phishing emails containing Microsoft Office documents with embedded OLE objects.
- **Execution Mechanism:** The malicious documents abuse OLE functionality to execute code **without relying on VBA macros**. Embedded OLE objects trigger **living-off-the-land binaries (LOLBins)** such as cmd.exe, powershell.exe, and mshta.exe to download and execute payloads.
- **Malware Capabilities:** The deployed malware enables remote command execution, reconnaissance, and data exfiltration. Credential harvesting may targets local storage, browsers, and sensitive files.
- **Evasion Techniques:** The campaign evades detection by leveraging **trusted cloud services** for payload delivery and command-and-control. The use of LOLBins and **minimal on-disk artifacts** reduces endpoint and forensic visibility.

IMPACT

- Attackers gain unauthorized access to sensitive documents, credentials, and internal communications
- Compromised systems may be used to alter or manipulate files and data without detection
- While not immediately destructive, compromised endpoints can be leveraged for follow-on attacks, espionage, or destructive malware deployment
- Organizations relying on Microsoft Office and cloud collaboration platforms are at heightened risk, particularly those targeted for intelligence collection

RECOMMENDATIONS

- Restrict or block embedded OLE objects in Microsoft Office documents wherever feasible.
- Enforce Protected View and block content originating from the internet by default for Office documents.
- Educate users on spear-phishing techniques and the risks associated with enabling document content.
- Implement advanced phishing detection and attachment sandboxing to analyze suspicious documents before delivery.

REFERENCE

- ScarCruft Exploits Trusted Cloud Services and OLE Documents to Deliver Malware

SECURE, SCALE, SUCCEED WITH CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com

www.encyb.com