BLACKSWAN
CYBERSECURITY

# THREAT ADVISORY

July 20, 2023

## LokiBot Malware Exploits Microsoft Word Vulnerabilities for Widespread Distribution

### OVERVIEW

Researchers recently uncovered a LokiBot info-stealer campaign exploiting well-known Microsoft Office related vulnerabilities.

First observed in May 2023, researchers found that threat actors exploited two remote code execution vulnerabilities (CVE-2021-40444 and CVE-2022-30190) embedding malicious macros in Microsoft documents, specifically Word documents. Infected files were named "document.xml.rels" and had an MHTML link. Executing this file triggered the deployment of exploits for the second vulnerability.

More recent versions of this attack include an embedded VBA script within the Word document. The VBA script generates an INF file that calls a DLL file, which then downloads a second-stage code injector from a specific URL. The code injector is capable of evasion techniques and will execute the LokiBot malware in the final stage.

Researcher's examination of the command-and-control (C2) traffic showed that the LokiBot version (March'23) deployed in these campaigns has an MD5 hash that acts as a mutex to prevent multiple instances of the malware from running concurrently.

### INDICATORS OF COMPROMISE

*Command and Control:*

- 95[.]164[.]23[.]2

*Related Files:*

- 17d95ec93678b0a73e984354f55312dda9e6ae4b57a54e6d57eb59bcbbe3c382

- 23982d2d2501cfe1eb931aa83a4d8dfe922bce06e9c327a9936a54a2c6d409ae

- 9eaf7231579ab0cb65794043affb10ae8e4ad8f79ec108b5302da2f363b77c93

- da18e6dcefe5e3dac076517ac2ba3fd449b6a768d9ce120fe5fc8d6050e09c55

- 2e3e5642106ffbde1596a2335eda84e1c48de0bf4a5872f94ae5ee4f7bffda39

- 80f4803c1ae286005a64ad790ae2d9f7e8294c6e436b7c686bd91257efbaa1e5

- 21675edce1fdabfee96407ac2683bcad0064c3117ef14a4333e564be6adf0539

- 4a23054c2241e20aec97c9b0937a37f63c30e321be01398977e13228fa980f29

## RECOMMENDATIONS

• Patch Management – Patch and Update all instances of Microsoft Office.

• Training and Awareness - Educate users about the risks associated with opening suspicious email attachments or clicking on untrusted links.

• Cybersecurity Controls (End-Points) – Deploy and effectively manage and monitor advanced endpoint protection solutions that include anti-malware, intrusion detection, and prevention systems.

• Cybersecurity Controls (Network) – Deploy 24x7 Network Traffic Monitoring capabilities to identify and block suspicious communication with command-and-control (C2) servers.

• Email Filtering: Enable all available capabilities to scrutinize incoming emails, blocking malicious attachments and links commonly used in malware distribution.

• Multi-Factor Authentication (MFA): Enforce the use of MFA for all sensitive accounts and systems to provide an additional layer of protection against unauthorized access. This helps mitigate the risk of LokiBot stealing credentials.

## REFERENCES

- https://www.fortinet.com/blog/threat-research/lokibot-targets-microsoft-office-document-using-vulnerabilities[1]and-macros
- https://thehackernews.com/2023/07/cybercriminals-exploit-microsoft-word.htm