Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

LokiBot Data Exfiltrating Trojan Targets Windows Systems

Date of Publication	Admiralty Code	TA Number
July 17, 2023	A1	TA2023301

Summary

Attack Began: May 2023
Malware: LokiBot (aka Loki PWS)
Attack Region: Worldwide
Affected Platform: Windows
Attack: LokiBot, an infamous data-exfiltrating Trojan, has maintained a prominent presence since 2015. This pernicious malware predominantly sets its sights on Windows systems, diligently striving to acquire confidential data from compromised machines.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-40444	Microsoft MSHTML Remote Code Execution Vulnerability	Windows Server & Microsoft Internet Explorer	✓	✓	✓
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (Follina)	Microsoft Windows	✓	✓	✓

Attack Details

#1

LokiBot, alternatively recognized as Loki PWS, has garnered widespread notoriety as an information-stealing Trojan operating since 2015. Its primary focus lies in targeting Windows systems with the explicit purpose of amassing delicate information from compromised machines. By leveraging the remote code execution vulnerabilities CVE-2021-40444 and CVE-2022-30190, the attackers used the ability to implant malicious macros within Microsoft documents. Once executed, these macros facilitated the deployment of the LokiBot malware onto the victim's system.

#2

There were two distinct variations of Word documents: the first type incorporated an externally linked XML file, while the second type encompassed a VBA script that promptly executed a macro upon document opening. Remarkably, both files shared an astonishingly identical and enticing image.

#3

The Word document that aimed to exploit CVE-2021-40444 included a file named "document.xml.rels" housing an external link that employed MHTML documents. Upon accessing the link, a file named "defrt.html" would be downloaded, effectively exploiting the second vulnerability, CVE-2022-30190.

#4

LokiBot is purposefully crafted to harvest sensitive information from a variety of sources, including web browsers, FTP, email clients, and numerous software tools installed on compromised systems. By leveraging a range of vulnerabilities and employing VBA macros, LokiBot orchestrates its attacks with precision. Furthermore, it harnesses a VB injector, utilizing multiple techniques to effectively evade detection or analysis.

Recommendations

To mitigate the risks posed by LokiBot, it is crucial to regularly update and **patch** all software applications, particularly those commonly targeted by the Trojan. This helps address known vulnerabilities and strengthens the system's defense against potential attacks.

Implementing robust security measures, such as deploying advanced endpoint protection solutions and conducting regular security audits, can significantly enhance the resilience of systems against LokiBot and similar information-stealing Trojans, reducing the likelihood of successful infiltration and data compromise.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1137 Office Application Startup	T1027 Obfuscated Files or Information
T1137.001 Office Template Macros	T1059 Command and Scripting Interpreter	T1010 Application Window Discovery	T1566 Phishing
T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol	T1573 Encrypted Channel	T1046 Network Service Discovery
T1082 System Information Discovery			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	95[.]164[.]23[.]2
SHA256	17d95ec93678b0a73e984354f55312dda9e6ae4b57a54e6d57eb59bcbbe3c382, 23982d2d2501cfe1eb931aa83a4d8dfe922bce06e9c327a9936a54a2c6d409ae, 9eaf7231579ab0cb65794043affb10ae8e4ad8f79ec108b5302da2f363b77c93, da18e6dcefe5e3dac076517ac2ba3fd449b6a768d9ce120fe5fc8d6050e09c55, 2e3e5642106ffbde1596a2335eda84e1c48de0bf4a5872f94ae5ee4f7bffda39, 80f4803c1ae286005a64ad790ae2d9f7e8294c6e436b7c686bd91257efbaa1e5, 21675edce1fdabfee96407ac2683bcad0064c3117ef14a4333e564be6adf0539, 4a23054c2241e20aec97c9b0937a37f63c30e321be01398977e13228fa980f29

Patch Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40444

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

References

https://www.fortinet.com/blog/threat-research/lokibot-targets-microsoft-office-document-using-vulnerabilities-and-macros

https://www.hivepro.com/unveiling-the-malicious-tactics-of-lokibot-malware/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

REPORT GENERATED ON

July 17, 2023 • 7:00 AM

More at www.hivepro.com