KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | QBot phishing leverages Windows Calculator DLL hijacking

Tracker ID: TN0801 **Date:** 02/Aug/2022 **Category:** Cyber Attack **Industry:** All **Region**: All

Background

The developers of the QBot malware have been exploiting a Windows Calculator DLL hijacking vulnerability to migrate to devices and evade detection. In the early stages of a campaign, ransomware gangs deploy QBot, also known as Qakbot, a Windows malware strain that started out as a banking trojan but evolved into a malware dropper. Qakbot has been using the Windows 7 Calculator application as a target for DLL hijacking attacks since July. The tactic is still employed in phishing scams.

Qakbot's initial infection begins with a malicious spam campaign that employs a variety of themes to deceive recipients into opening attachments. This campaign's spam email is composed of a password-protected ZIP file and an HTML file with base64-encoded graphics. The password-protected zip file is placed straight away in the Downloads folder when visitors open the HTML file. The zip file's name was "Report Jul 14 47787.zip," and an HTML password was also included.

When the victim enters the password to open the zip file, another file containing an ISO image is extracted. There are four distinct parts that make up the ISO file. The ISO file mounts itself to a drive and displays the .lnk file when executed by the user. This file has been modified to look like a legitimate PDF containing critical information or a file that Microsoft Edge can open. The shortcut causes the execution of icalc.exe from the ISO file and starts the infection by running Calc.exe through the Command Prompt, visible in the options menu for the files.

The Windows 7 Calculator looks for and attempts to load the native WindowsCodecs.dll file after being launched. The DLL hard-coded locations are not searched for, though, and if a DLL with the same name is found in the same folder as the executable Calc.exe, it will be loaded. The other [numbered].dll file, carrying the QBot malware, is launched by the malicious WindowsCodecs.dll file that threat actors constructed to take advantage of this vulnerability.

When malware is loaded or deployed via a trusted program, like the Windows Calculator, some security tools could fail to detect it, allowing threat actors to escape detection. The Windows 7 version is utilized by the threat actors since the Windows 10 Calc.exe and later versions are no longer affected by this DLL hijacking vulnerability.

We may conclude that the threat actors responsible for Qakbot are active and, therefore, are constantly refining their strategies to increase their effectiveness and impact. They steal the victim's computer's login information and utilize it to do financial damage. Any victim of the Qakbot infection may also experience fraud and identity theft as a result.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | QBot phishing leverages Windows Calculator DLL hijacking

Tracker ID: TN0801 **Date:** 02/Aug/2022 **Category:** Cyber Attack **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion and Exfiltration.

Indicators of Compromise *

Please refer to the attached sheet for IOCs

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples. Validate the IOCs attached and implement the detection & prevention accordingly.
- Do not open emails from unknown or irrelevant senders.
- Avoid downloading pirated software from unverified sites.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Keep updating your passwords after certain intervals.
- Use reputed anti-virus solutions and internet security software packages on your connected devices, including PCs, laptops, and mobile devices.
- Avoid opening untrusted links and email attachments without first verifying their authenticity.
- Block URLs that could use to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solutions on employees' systems.

References

- Bill Toulas, QBot phishing uses Windows Calculator DLL hijacking to infect devices, Bleeping Computer, 24th July 2022, External Link (www.bleepingcomputer.com).
- Cyble, Qakbot Resurfaces With New Playbook, 21st July 2022, External Link (blog.cyble.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176 471 471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | QBot phishing leverages Windows Calculator DLL hijacking

Tracker ID: TN0801 **Date:** 02/Aug/2022 **Category:** Cyber Attack **Industry:** All **Region**: All

*

SHA256 Hash
cb83a65a625a69bbae22d7dd87686dc2be8bd8a1f8bb40e318e20bc2a6c32a8e
197ee022aa311568cd98fee15baf2ee1a2f10ab32a6123b481a04ead41e80eee
9887e7a708b4fc3a91114f78ebfd8dcc2d5149fd9c3657872056ca3e5087626d
8760c4b4cc8fdcd144651d5ba02195d238950d3b70abd7d7e1e2d42b6bda9751
c992296a35528b12b39052e8dedc74d42c6d96e5e63c0ac0ad9a5545ce4e8d7e