Qakbot malware botnet exploits “Follina” vulnerability

8th June 2022

Orpheus vulnerability severity score: 73

Qakbot (also known as Qbot) malware botnet operators have started exploiting CVE-2022-30190 in their phishing efforts.

CVE-2022-30190, also known as “Follina”, is a zero-day vulnerability affecting Microsoft Office. It impacts all platforms from Windows 7 and Windows Server 2008 and, if exploited, allows an adversary to abuse Microsoft Support Diagnostics Tool to achieve remote code execution on a compromised device.

Qakbot operators send victims phishing emails from previously hijacked email threads: a common tactic they have previously deployed. The malicious messages contain an HTML attachment that, in turn, downloads a ZIP archive that holds a disk image containing a blank Word document, a shortcut file and a Dynamic Link-Library (DLL) file.

If interacted with, the shortcut file directly loads the Qakbot malware embedded within the disk image. Meanwhile, if opened and with content enabled, the Word document loads an additional HTML file that exploits CVE-2022-30190 to execute PowerShell code and drop a different Qakbot DLL payload.

Qakbot’s implementation of CVE-2022-30190 further showcases the increasing popularity the vulnerability is attracting within the threat landscape. Following its initial disclosure, we have reported on its exploitation by Chinese-linked threat actor TA413 and another, unknown, state-backed threat actor.

It also showcases how the cybercriminals behind the malware botnet are capable of changing their tactics, techniques and procedures to maximise the chances of a successful infection. In mid-April, we reported on Qakbot operators changing their delivery mechanism from Microsoft Office documents laden with malicious macros to MSI (Microsoft Installer) packages, likely in response to Microsoft's mitigation efforts against malware.

Threat Subcategory	Botnet
Threat Actor	Qakbot
Objective	Infrastructure enumeration/compromise
CVE	CVE-2022-30190
Infection Vectors	Phishing
Source	https://twitter.com/threatinsight/status/1534227444915482625 https://www.bleepingcomputer.com/news/security/qbot-malware-now-uses-windows-msdt-zero-day-in-phishing-attacks/