ultraviolet

THREAT REPORT:

Tracking QakBot

Services Performed By:
UltraViolet Cyber
Casey Latham
(443) 351-7630
info@uvcyber.com

Published Date:
05/15/2024

Contents

1 Executive Summary 2
2 Technical Analysis 2
3 What UltraViolet Cyber is Doing 3
4 What Customers Can Do 3
5 References 3

1 Executive Summary

QakBot, originally billed as a modular banking trojan, has been utilized as an information stealer since 2008 and has been upgraded over the years to become a ransomware delivery agent. A major break in successfully combating QakBot came when the FBI and CISA released a joint advisory alert (and subsequent cybersecurity advisory) on August 30, 2023, that released indicators of compromise of the QakBot infrastructure. However, QakBot persists, and on May 14, 2024, Microsoft released a patch within its security updates. *Bleeping Computer* reported: "Tracked as CVE-2024-30051, this privilege escalation bug is caused by a heap-based buffer overflow in the DWM (Desktop Window Manager) core library. Following successful exploitation, attackers can gain SYSTEM privileges."[i] Connecting the dots, *Bleeping Computer* showed that the Microsoft security update for CVE-2024-30051 also combats QakBot.

2 Technical Analysis

The joint FBI and CISA advisory defined QakBot as follows: "Originally used as a banking trojan to steal banking credentials for account compromise, QakBot—in most cases—was delivered via phishing campaigns containing malicious attachments or links to download the malware, which would reside in memory once on the victim network. QakBot has since grown to deploy multiple types of malware, trojans, and highly destructive ransomware variants targeting the United States and other global infrastructures, including the Election Infrastructure Subsector, Financial Services, Emergency Services, and Commercial Facilities Sectors."[ii] A review of the MITRE ATT&CK framework shows over 50 tactics and techniques used by QakBot to complete its malicious mission.[iii]

The fight continues against QakBot, and the investigation trail reads like a spy novel, involving cyber criminals, US Government agencies, and top researchers. The FBI and CISA have done a fantastic job with getting the information out on QakBot; however, as indicated by Microsoft's May Security Updates including a patch for CVE-2024-30051, it is apparent that the affected systems (listed in the CVE) have had a readily available exploit friendly to QakBot through the DWM core library. The FBI's website includes a very exciting read, which includes their take: "FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown."[iv] This could be a seminal event in cybersecurity as the "Operation marks one of the largest-ever U.S.-led enforcement actions against a botnet."[v]

Every cybersecurity department should immediately review the CISA and FBI's Joint Advisory on QakBot Infrastructure as it contains in-depth matter that relates to the malicious infrastructure. UltraViolet recommends that all affected systems be patched against CVE-2024-30051 with Microsoft's May security updates.

3 What UltraViolet Cyber is Doing

UltraViolet Cyber regularly:

- Updates our IOC database to ensure alerting is up to date.
- Monitors commands that are associated with malicious activity from threat actors.
- Monitors network logs for traffic to known malicious sites.

4 What Customers Can Do

- Review the Joint Advisory from the FBI and CISA about QakBot.
- Patch affected systems against CVE-2024-30051 with Microsoft's May security updates.
- Maintain a mature system update cycle against operating system vendors' patch releases.
- Educate users on phishing email, since QakBot can find initial access in this manner.

5 References

CISA and FBI Publish Joint Advisory on QakBot Infrastructure | CISA. (2023, August 30). Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/news-events/alerts/2023/08/30/cisa-and-fbi-publish-joint-advisory-qakbot-infrastructure

Critical Patches Issued for Microsoft Products, May 14, 2024. (n.d.). CIS. https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-may-14-2024_2024-053

FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown. (2023, August 29). Federal Bureau of Investigation. https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown

Gatlan, S. (2024a, May 14). Microsoft fixes Windows Server bug causing crashes, NTLM auth failures. *Bleeping Computer*. https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-server-bug-causing-crashes-ntlm-auth-failures/

Gatlan, S. (2024b, May 14). Microsoft fixes Windows zero-day exploited in QakBot malware attacks. *Bleeping Computer*. https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-zero-day-exploited-in-qakbot-malware-attacks/

Identification and Disruption of QakBot Infrastructure | CISA. (2023, August 30). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-242a

Security Update Guide - Microsoft Security Response Center. (n.d.-a). https://msrc.microsoft.com/update-guide/releaseNote/2024-May

Security Update Guide - Microsoft Security Response Center. (n.d.-b). https://msrc.microsoft.com/update-guide/

[i] https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-zero-day-exploited-in-qakbot-malware-attacks/
[ii] https://www.cisa.gov/news-events/alerts/2023/08/30/cisa-and-fbi-publish-joint-advisory-qakbot-infrastructure
[iii] https://attack.mitre.org/software/S0650/
[iv] https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
[v] https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown