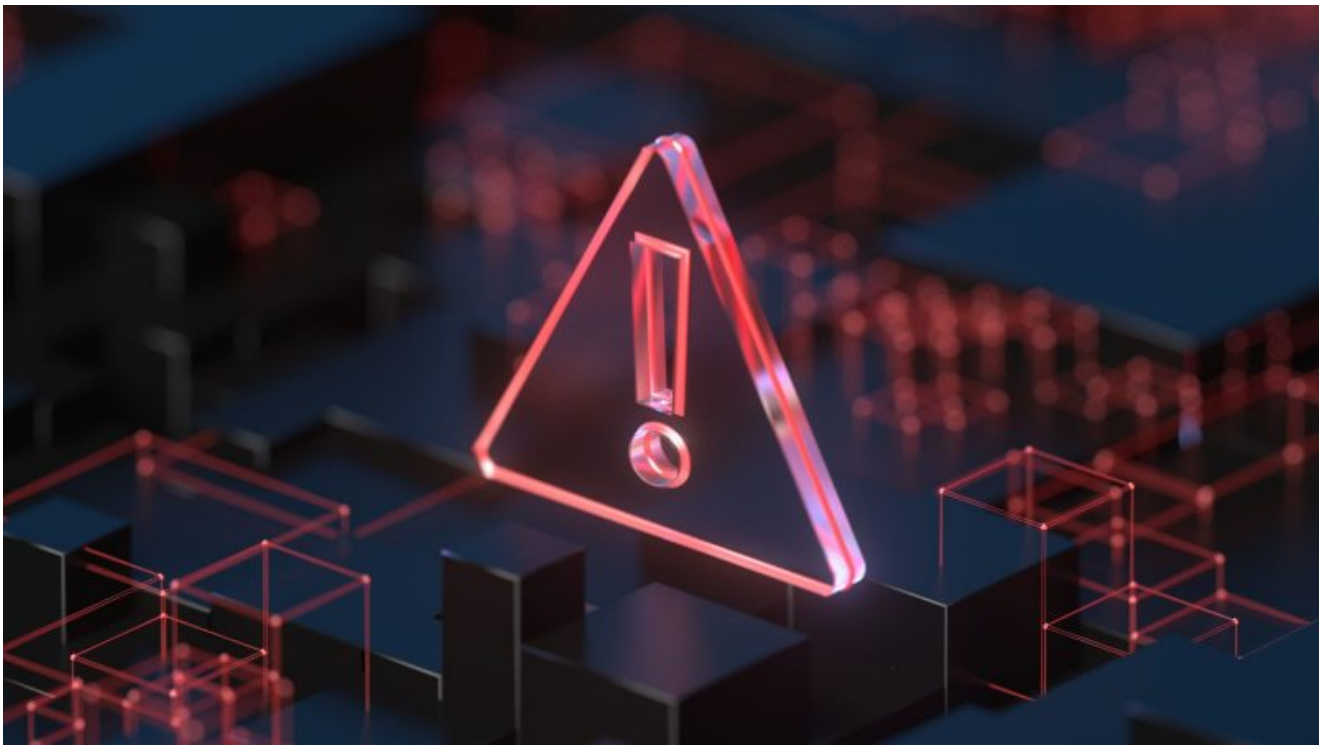
QakBot attacks with Windows zero-day (CVE-2024-30051)

securelist.com/cve-2024-30051/112618

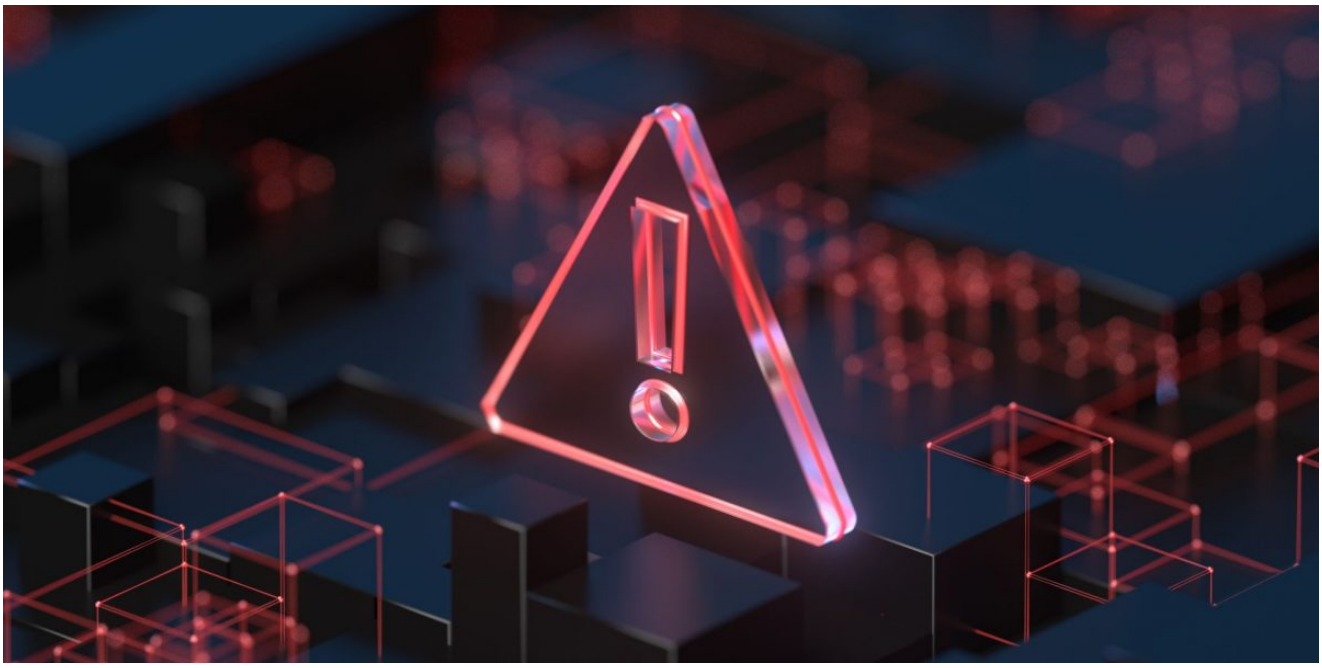


Software

Software

14 May 2024

minute read



Authors

-  Boris Larin
-  Mert Degirmenci

In early April 2024, we decided to take a closer look at the Windows DWM Core Library Elevation of Privilege Vulnerability CVE-2023-36033, which was previously discovered as a zero-day exploited in the wild. While searching for samples related to this exploit and attacks that used it, we found a curious document uploaded to VirusTotal on April 1, 2024. This document caught our attention because it had a rather descriptive file name, which indicated that it contained information about a vulnerability in Windows OS. Inside we found a brief description of a Windows Desktop Window Manager (DWM) vulnerability and how it could be exploited to gain system privileges, everything written in very broken English. The exploitation process described in this document was identical to that used in the previously mentioned zero-day exploit for CVE-2023-36033, but the vulnerability was different. Judging by the quality of the writing and the fact that the document was missing some important details about how to actually trigger the vulnerability, there was a high chance that the described vulnerability was completely made up or was present in code that could not be accessed or controlled by attackers. But we still decided to investigate it, and a quick check showed that this is a real zero-day vulnerability that can be used to escalate privileges. We promptly reported our findings to Microsoft, the vulnerability was designated CVE-2024-30051, and a patch was released on May 14, 2024, as part of Patch Tuesday.

After sending our findings to Microsoft, we began to closely monitor our statistics in search of exploits and attacks that exploit this zero-day vulnerability, and in mid-April we discovered an exploit for this zero-day vulnerability. We have seen it used together with QakBot and other

malware, and believe that multiple threat actors have access to it.

We are going to publish technical details about CVE-2024-30051 once users have had time to update their Windows systems.

Kaspersky products detect the exploitation of CVE-2024-30051 and related malware with the verdicts:

- PDM:Exploit.Win32.Generic;
- PDM:Trojan.Win32.Generic;
- UDS:DangerousObject.Multi.Generic;
- Trojan.Win32.Agent.gen;
- Trojan.Win32.CobaltStrike.gen.

Kaspersky would like to thank Microsoft for their prompt analysis of the report and patches.

- CVE-2024-30051
- Microsoft Windows
- QakBot
- Vulnerabilities
- Vulnerabilities and exploits
- Zero-day vulnerabilities

Authors

-  Boris Larin
-  Mert Degirmenci

QakBot attacks with Windows zero-day (CVE-2024-30051)

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

---

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm

(Required)

Reports

APT trends report Q1 2024

The report features the most significant developments relating to APT groups in Q1 2024, including the new malware campaigns DuneQuixote and Durian, and hacktivist activity.

ToddyCat is making holes in your infrastructure

We continue to report on the APT group ToddyCat. This time, we'll talk about traffic tunneling, constant access to a target infrastructure and data extraction from hosts.

DuneQuixote campaign targets Middle Eastern entities with "CR4T" malware

New unattributed DuneQuixote campaign targeting entities in the Middle East employs droppers disguised as Total Commander installer and CR4T backdoor in C and Go.

HrServ – Previously unknown web shell used in APT attack

In this report Kaspersky researchers provide an analysis of the previously unknown HrServ web shell, which exhibits both APT and crimeware features and has likely been active since 2021.

Subscribe to our weekly e-mails

The hottest research right in your inbox

(Required)

Subscribe to our weekly e-mails

The hottest research right in your inbox

(Required)