Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

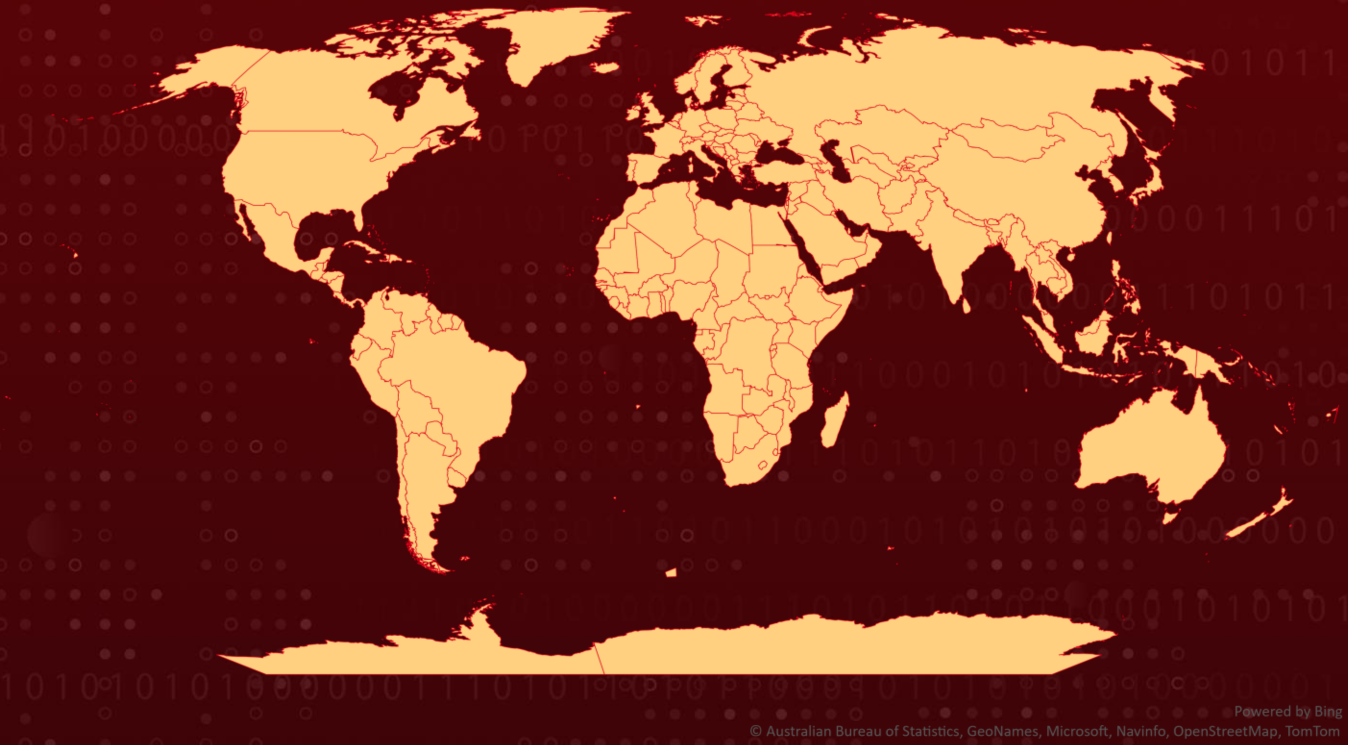
QakBot Resurges Latest Strikes with Ransom Knight and Remcos RAT

Date of Publication	Last Update Date	Admiralty Code	TA Number
October 6, 2023	July 21, 2024	A1	TA2023401

Summary

Attack Began: August 2023
Malware: Qakbot (aka QBot, QuackBot, and Pinkslipbot), Ransom Knight ransomware (aka Cyclops), Remcos backdoor
Attack Region: Worldwide
Attack: The QakBot malware has been associated with a persistent phishing campaign since the beginning of August 2023, leading to the deployment of both the Ransom Knight ransomware and the Remcos RAT. In April-2024, Qakbot malware was involved in campaigns exploiting CVE-2024-30051 as a zero-day flaw.

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-2024-30051	Microsoft Windows DWM Core Library Elevation of Privilege Vulnerability	Microsoft Windows OS	✓	✓	✓

Attack Details

#1 The threat actors orchestrating the Qakbot menace remain active, leading a renewed campaign that commenced just prior to the recent takedown by the FBI, part of an operation named Duck Hunt. This Qakbot affiliates' campaign involves the dissemination of a variant of the Ransom Knight ransomware (also known as Cyclops) coupled with the Remcos backdoor.

#2 The latest wave of malicious activity, instigated just before the takedown, begins with the deployment of a malicious LNK file, likely distributed through phishing emails. Upon activation, this file triggers the infection process, culminating in the deployment of the Ransom Knight ransomware, a recent rebrand of the Cyclops ransomware-as-a-service (RaaS) scheme.

#3 The campaign also employs a sophisticated tactic wherein ZIP archives containing the LNK files incorporate Excel add-in (.XLL) files. This integration facilitates the propagation of the Remcos RAT, providing a lasting backdoor access point to the targeted endpoints. Notably, some of the filenames used in this nefarious endeavor are written in Italian, indicative of a deliberate focus on users within that region.

#4 Despite federal actions, Qakbot continues to evolve and in late December, a new version of Qakbot emerged, featuring significant enhancements to its string encryption algorithm and the use of AES, which complicates analysis. Additionally, the updated version reinstated code specifically designed to detect and evade analysis environments.

#5 Qakbot affiliates were also observed exploiting a zero-day Privilege Escalation flaw in Microsoft Windows, CVE-2024-30051. This Windows DWM Core Library Elevation of Privilege Vulnerability, discovered in April 2024 and disclosed in May 2024, enables a local user to gain SYSTEM privileges. The flaw has been used in conjunction with Qakbot, and it is believed that multiple threat actors have had access to it.

Recommendations

Vulnerability Management: Regularly update and patch systems to mitigate vulnerabilities such as CVE-2024-30051. Prioritize the patching of devices affected with CVE-2024-30051 to prevent Qakbot infection.

Email Security: Enhance email security measures and educates users on recognizing social engineering tactics to mitigate the risk of falling prey to phishing attacks leveraging deceptive zip file attachments.

Implement Robust Endpoint Security Measures: Ensure that all endpoints have up-to-date and robust security software to detect and prevent malware infections. Employ advanced endpoint protection solutions that can identify, and block known and unknown threats.

Behavioral Anomaly Detection: Deploy advanced behavioral anomaly detection systems that can identify deviations from normal user and system behavior, flagging activities such as frequent and unusual execution of reconnaissance commands.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	T1059 Command and Scripting Interpreter	T1010 Application Window Discovery
T1566 Phishing	T1140 Deobfuscate/Decode Files or Information	T1497 Virtualization/Sandbox Evasion	T1083 File and Directory Discovery
T1018 Remote System Discovery	T1057 Process Discovery	T1082 System Information Discovery	T1055 Process Injection
T1071 Application Layer Protocol	T1105 Ingress Tool Transfer	T1588 Obtain Capabilities	T1588.001 Malware
T1068 Exploitation for Privilege Escalation			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	5e4c95b2c1b14a8a0f425576189fae60, 8aec3f3ef66e4ff118bfdab1d031eadb, 46e169516479d0614b663f302b5d1ace, 795319d48ce1f680699beb03317c6bff, De1d9ed6da4f34b4444b13442aac5033, F382d0f92221831eeb39c108f8ccfa26
SHA256	08c0af563c8c08323c195eea2068b45694d4bf83e7e4d637924cc67e4bf9806a, 0dbd6719aae8fe5b7baf0fd18e1cd744f5d347e622b27693295fa976276b643c, 12094a47a9659b1c2f7c5b36e21d2b0145c9e7b2e79845a437508efa96e5f305, 138b50f9832870157e4f0a2055d39885148c6dbe296ce6cf109d95cd4e7fc7a0, 1aa91398494318a34190460c5be2993a078ef977e9eea95e6c607a5bf5c5ba8f, 2270d9b08ecb65e01b8a490dede9b1480431bdfaa052cecc54a1231fe56e655a, 2b67128c9767fae1bbc4bd04f3a85199328b637f188a71ae6be836a81a064a55, 35ec4858f5f4f7c9c7cd27b9c48cfe3d8d4c03044974740f3fb0892bfe140a88, 3b3bd81232f517ba6d65c7838c205b301b0f27572fcfef9e5b86dd30a1d55a0d, 3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa, 3f004293165057ac40d7d2dc663cc62c877ebe29601251dcca24b6aa1062b7af, 457c622ba31de68f44d01c63de335b32cc7ef2cbbf6c48a2acdd868a28ddba97, 49220571574da61781de37f35c66e8f0dadb18fdedb6d3a1be67485069cfd4b0, 4c7d5ae6fefb8f53e0f557a241f95a677482bc4219c1d91573425ebc0cb44830, 528d81b023e374081d1d1147c9acf2adbfbc0ec8ac95f7e3131589a0c5ec0d7b, 73472cfc52f2732b933e385ef80b4541191c45c995ce5c42844484c33c9867a3, 7619db1cbeef2ec38d180fdd9fecb8dd8776c90b6c1941e4f685c0a9b03b1343, 780be7a70ce3567ef268f6c768fc5a3d2510310c603bf481ebffd65e4fe95ff3, 7ad0a845fdc8ed7843d1b65c446dc85e19cdd1e40b2e5d6ddd416c60a922100a, 8386c26ef88062db37966613ac32debe4ec5be1e44ea42ae89d8ad7fbf3f83e5, 88590eb81c23e50c1a52a49e48b37b5bc72ead1868ca45adc4ffe5c8485a9626, 90d800f250c1951c9f015b95bd590263b550af0ba56b0719325af093f184839d, 93a98b919aec23411ae62dba8d0d22f939da45dec19db2b4e7293124d8f1507f, 951cc98b54bc4d78ce4f11a3bdbfdaee7777591ffef88bb2557ebecbb1909013, a7c1c835f738e944bd88f2d5b9860b1b093c84798e73b85fef71b88c66ed6c87, a824e74f267831a500194fe885b326ca3fcc7fc4c58dff8f3eae11a969f7cb77, af6a9b7e7aefeb903c76417ed2b8399b73657440ad5f8b48a25cfe5e97ff868f, be26c5d7a70cc3ea46138c2ef3b589a381d61a9aaabd50ad9b8095d80f8260d9, cc5fa220f92319e0e063e4e19c5e09b17e2e459ee33a0b763417080b1c4ecfed, dbc198139b9f4ecbe0170b51d2e802873ac2e98db5d0f8fef6913c2f01e82e41, e88610db05636a1476435ec1f39d3651b080c8a6b8756452d421d7a822a2e115, f4833f0c2227976b4918e9999f929d22d6e9d8242dafd80f3e0619846d00939d, f4bb0089dcf3629b1570fda839ef2f06c29cbf846c5134755d22d419015c8bd2,

TYPE	VALUE
SHA256	fda2abd24764809fb36d4d2ee7ab5f6e8c06381fe6d9bb191bde62411c96ba92, 877f8a66be5c99d5a4636d74c566d61ebc1951049be5fa8968c132922ca4ba18, af5f5aa32a3e2bc802b9863c20de2eac0ca14e1002c02396e63e2aa38eb351c6, bfd2c062c12a261c4460cdc59cc9f7e80b72b455e852d08c106f12a3d657a575, d0013d23218a1aafdea792a0599b746af6966f765181c8c1dbfe7257be0cb022, d522a32eebc7f0108dbff116b7fa9dd457bf9f062465060115ec423c567c5115, e38a1648fc6494f881e3b793688ef4d69e925137c4c7494f4dd6c6604142a2bc, ec4ac7ade34402ad3757e97d03de7aa3dfee0ed53f28f32c99d8dbbb96958dcb, f2e2427107648e8d7be5f4e42341c702ceddb442191434128cbbf15c0325d8e9, 7b4d227fddcc4e93ea0cdf017026ff2dad6efd6bc7de71b689dc0595a2a4fb4d, a2c654357d790d7c4cec619de951649db31ecdb63935f38b11bb37f983ff58de, c42ad519510936f14ab46fbad53606db8132ea52a11e3fc8d111fbccc7d9ab5a, 34ea4cad8558fcab75631a44eae492a54e1cf9ae2f52e7d5fa712686acd06437, 597541041b49043bd2abd482b3bf4dd233a0dbb47d5ef704ea9ee28705d2764b, 86e96d3d22ead8f41f6a29f7bfe4b35c0d4ae5bd8da046ff0d01d9c6ea678dc2, ef74d2b8d1767667fb6817916f7d2d2c998358e07422a6af246151e0299f26aa, 006e0b5f47462c4d755b3f84e22b90f09fb6b369032a3ca72f39180e5395ed17, 19bae62fc0a3a64c80b666237c2f04706e3b89c5a6ea6be055df22122e5f8a63, 25cc64a072861840df9dfa7b2449165e4c37d57c542da8ec4ea4fffa10f1be39, 44065decc86f79ebbd56b27f1db8c7bd5843147f3fa8e577604c0ed45317b016, 6e0062ccdfa7a117a8b76d4056ac144fdf91f3a2811b32d5a3b7f31ac326181b, 75c562f9101eab86d03386fcf0ddfe3cdebec0008c2c5b5a94047c06ddeb2566, 78784c02843a518bdc546534759dcdb3ea523c54751858a51f39e0f9d1492868, 7ab8bcf9b4dc63ad3d9e1fe8eb2e8292a1545871fb2e3b5dd83c96a2b7e33b41
IPv4	89.23.96[.]203, 188.34.188[.]7

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051

References

https://blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/

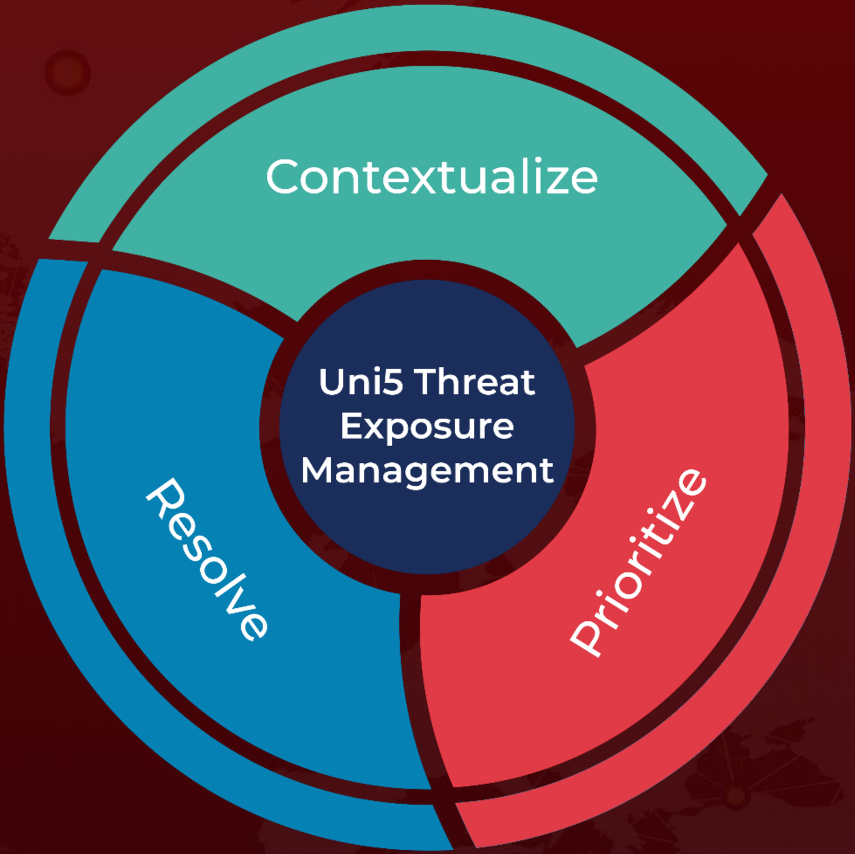
https://github.com/Cisco-Talos/IOCs/blob/main/2023/10/qakbot-affiliated-actors-distribute-ransom.txt

https://securelist.com/cve-2024-30051/112618/

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

October 10, 2023 • 5:00 AM

More at www.hivepro.com