Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

QakBot Resurges Latest Strikes with Ransom Knight and Remcos RAT

Date of Publication	Admiralty Code	TA Number
October 6, 2023	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.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

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.

Recommendations

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

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	006e0b5f47462c4d755b3f84e22b90f09fb6b369032a3ca72f39180e5395ed17, 19bae62fc0a3a64c80b666237c2f04706e3b89c5a6ea6be055df22122e5f8a63, 25cc64a072861840df9dfa7b2449165e4c37d57c542da8ec4ea4fffa10f1be39, 44065decc86f79ebbd56b27f1db8c7bd5843147f3fa8e577604c0ed45317b016, 6e0062ccdfa7a117a8b76d4056ac144fdf91f3a2811b32d5a3b7f31ac326181b, 75c562f9101eab86d03386fcf0ddfe3cdebec0008c2c5b5a94047c06ddeb2566, 78784c02843a518bdc546534759dcdb3ea523c54751858a51f39e0f9d1492868, 7ab8bcf9b4dc63ad3d9e1fe8eb2e8292a1545871fb2e3b5dd83c96a2b7e33b41,

TYPE	VALUE
SHA256	877f8a66be5c99d5a4636d74c566d61ebc1951049be5fa8968c132922ca4ba18, af5f5aa32a3e2bc802b9863c20de2eac0ca14e1002c02396e63e2aa38eb351c6, bfd2c062c12a261c4460cdc59cc9f7e80b72b455e852d08c106f12a3d657a575, d0013d23218a1aafdea792a0599b746af6966f765181c8c1dbfe7257be0cb022, d522a32eebc7f0108dbff116b7fa9dd457bf9f062465060115ec423c567c5115, e38a1648fc6494f881e3b793688ef4d69e925137c4c7494f4dd6c6604142a2bc, ec4ac7ade34402ad3757e97d03de7aa3dfee0ed53f28f32c99d8dbbb96958dcb, f2e2427107648e8d7be5f4e42341c702ceddb442191434128cbbf15c0325d8e9, 7b4d227fddcc4e93ea0cdf017026ff2dad6efd6bc7de71b689dc0595a2a4fb4d, a2c654357d790d7c4cec619de951649db31ecdb63935f38b11bb37f983ff58de, c42ad519510936f14ab46fbad53606db8132ea52a11e3fc8d111fbccc7d9ab5a, 34ea4cad8558fcab75631a44eae492a54e1cf9ae2f52e7d5fa712686acd06437, 597541041b49043bd2abd482b3bf4dd233a0dbb47d5ef704ea9ee28705d2764b, 86e96d3d22ead8f41f6a29f7bfe4b35c0d4ae5bd8da046ff0d01d9c6ea678dc2, ef74d2b8d1767667fb6817916f7d2d2c998358e07422a6af246151e0299f26aa
IPv4	89.23.96[.]203, 188.34.188[.]7

References

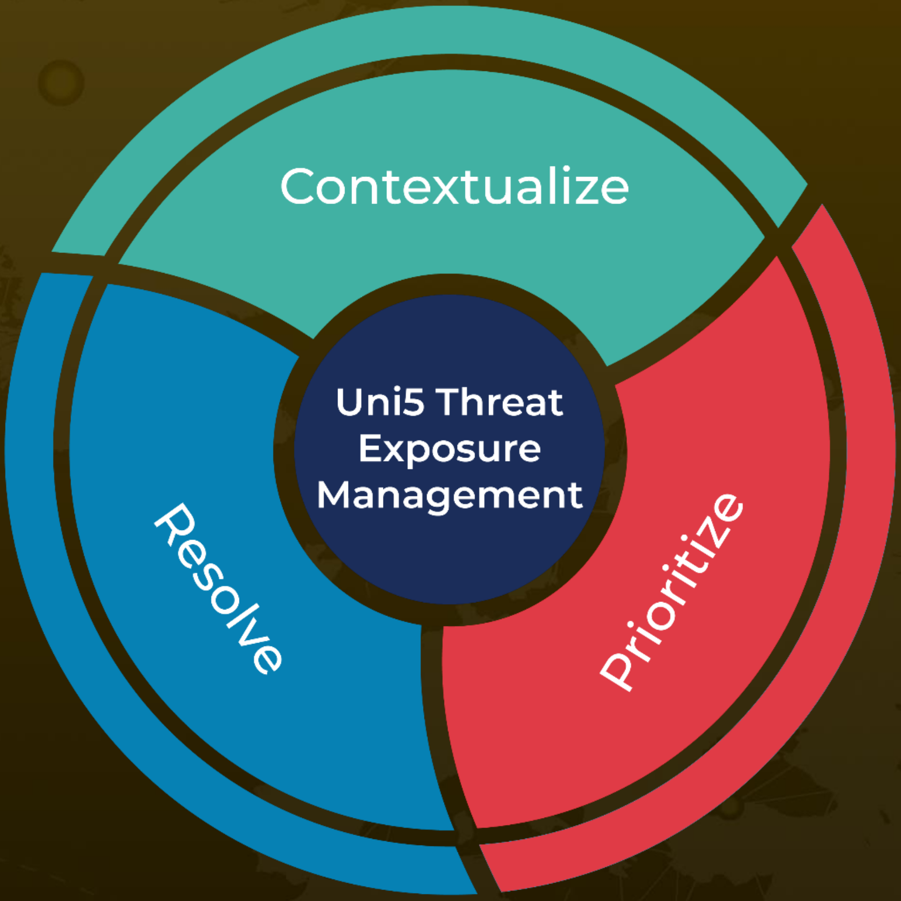
https://blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/

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

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 6, 2023 • 4:30 AM

More at www.hivepro.com