Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

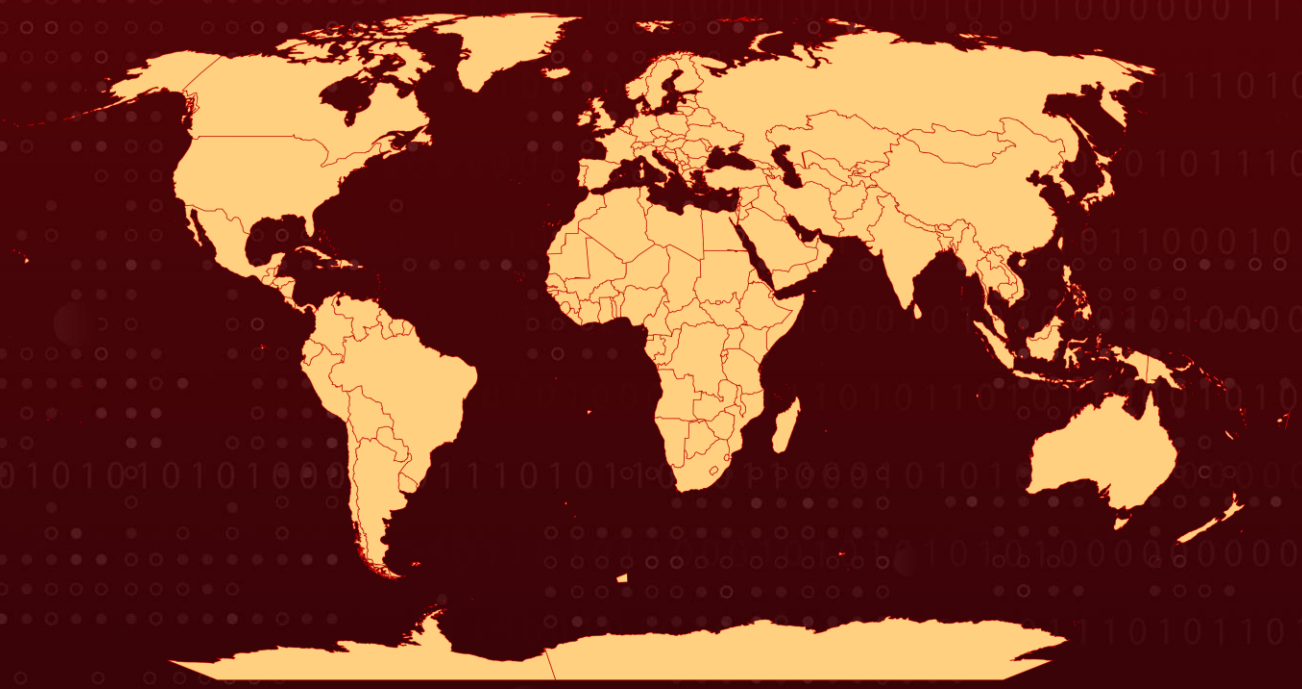
New Wave of QBot Attacks Detected via Malicious PDF Attachments

Date of Publication	Admiralty Code	TA Number
April 19, 2023	A1	TA2023194

Summary

First Appearance: April 04, 2023
Target Countries: Worldwide
Malware: QBot (also known as QakBot, QuackBot, and Pinkslipbot)
Attack: A new wave of QBot banking Trojan attacks was identified in April 2023, utilizing malicious PDF attachments in emails written in various languages.

Attack Regions



Attack Details

#1 A new wave of QBot banking Trojan attacks has been detected in early April 2023, with the malware being distributed through e-mail letters containing malicious PDF attachments. The messages are based on real business correspondence and are written in different languages, including English, German, Italian, and French.

#2 The QBot malware is capable of stealing passwords and cookies from browsers, intercepting traffic, and giving operators remote access to the infected system. The Trojan can also download additional malware, such as CobaltStrike or ransomware, and turn the victim's computer into a proxy server to facilitate the redirection of traffic, including spam traffic.

#3 The current infection chain of the QBot malware involves a PowerShell script that downloads a DLL file from remote servers, resulting in the infection of systems. Once infected, QBot is capable of extracting passwords, stealing emails, intercepting traffic, and providing remote access to compromised systems.

#4 The geography of QBot attacks during this period indicates that it was a widespread global campaign, targeting users worldwide. However, the most targeted countries during this period were Germany, Argentina, and Italy.

Recommendations

Implement multi-factor authentication (MFA) for all user accounts, especially those with access to critical systems or sensitive data. This can prevent unauthorized access even if the attacker manages to obtain user credentials through QBot's keylogging or credential-stealing capabilities.

Implement Email Sender Authentication such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocols to authenticate and verify the sender's domain in email headers. This can help prevent spoofing or impersonation of legitimate senders, which is a common tactic used by QBot and other malware to trick users.

Use web content filtering solutions to block access to known malicious websites, command-and-control (C&C) servers, and other suspicious domains. This can prevent QBot from establishing communication with its C&C servers and limit its ability to receive updates or commands from the attackers.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0002 Execution	TA0007 Discovery	TA0010 Exfiltration
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
TA0042 Resource Development	TA0001 Initial Access	T1584 Compromise Infrastructure	T1027 Obfuscated Files or Information
T1218 System Binary Proxy Execution	T1218.011 Rundll32	T1584.005 Botnet	T1566 Phishing
T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter	T1036 Masquerading	T1204 User Execution
T1204.002 Malicious File	T1059.007 JavaScript	T1059.001 PowerShell	T1132 Data Encoding
T1105 Ingress Tool Transfer			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	253E43124F66F4FAF23F9671BBBA3D98 39FD8E69EB4CA6DA43B3BE015C2D8B7D 299FC65A2EECF5B9EF06F167575CC9E2 A6120562EB673552A61F7EEB577C05F8 1FBFE5C1CD26C536FC87C46B46DB754D FD57B3C5D73A4ECD03DF67BA2E48F661 28C25753F1ECD5C47D316394C7FCEDE2

TYPE	VALUE
Domains	cica.com[.]co/stai/stai.php abhishekmeena[.]in/ducs/ducs.php rosewoodlaminates[.]com/hea/yWY9SJ4VOH agtendelperu[.]com/FPu0Fa/EpN5Xvh capitalperurrhh[.]com/vQ1iQg/u6oL8xlJ centerkick[.]com/IC5EQ8/2v6u6vKQwk8 chimpcity[.]com/h7e/p5FuepRZjx graficalevi.com[.]br/0p6P/R94icuyQ kmphi[.]com/FWovmB/8oZ0BOV5HqEX propertynear.co[.]uk/QyYWyp/XRgRWEdFv theshirtsummit[.]com/MwBGSm/lGP5mGh

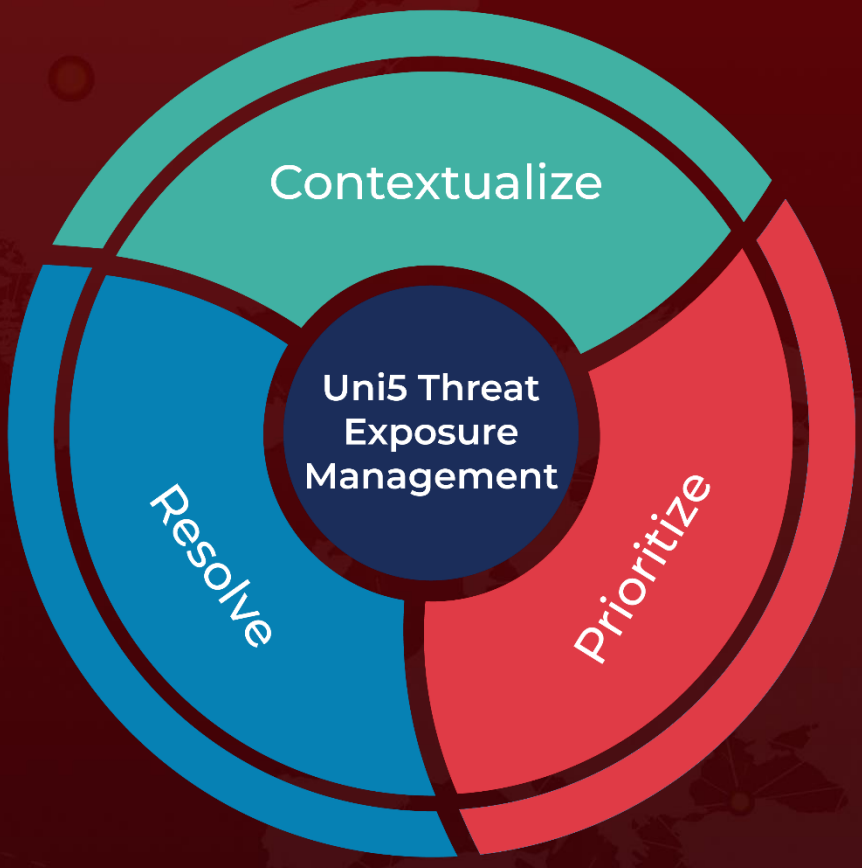
References

https://securelist.com/qbot-banker-business-correspondence/109535/

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

April 19, 2023 • 2:00 AM

More at www.hivepro.com