QakBot Back With New Evasion Technique

LOADER, TROJAN BOTNET, STEALER, BANKING TROJAN

Vairav Advisory Report

8th January 2023

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairav.net

Executive Summary

A new Qakbot malware campaign has been identified in this recent cybersecurity incident, employing a multi-stage attack methodology. The adversary used a phishing campaign pretending to be an email from an IRS employee. Attached to the email is a PDF file pretending to be a list that says, “Document preview is not available” and then prompts the user to download the PDF to view it properly. However, when clicking the download button, recipients will download a malicious Windows Installer (.msi) file, which is digitally signed to appear legitimate.

Key Takeaways:

- The campaign utilizes various stealthy techniques, including digitally signed executables, hiding behind benign filenames, and employing processes like rundll32 to execute malicious DLL functions.
- The malware engages in registry activities, checking and potentially modifying trust settings, a tactic that could allow it to install malicious software without triggering security warnings.
- The malware establishes persistence by creating files in user directories and manipulating the system restore points. It also attempts to exploit vulnerabilities and bypass security measures by forcing the use of an older version of the console host.
- The malware connects to a command-and-control server, highlighting the importance of monitoring network traffic for suspicious activities.
- The execution of the Microsoft volume shadow copy service suggests an attempt to manipulate or disable the VSS service, hindering file recovery options for the victim.

What's New?

The new Qakbot malware has evolved and differs from the previous versions in several ways:

- **Delivery Method:** The new Qakbot campaign starts with a target receiving a PDF file from users masquerading as an IRS employee. This PDF contains a URL that downloads a digitally signed Windows Installer (.msi).
- **Digitally Singed MSI:** The Windows Installer (list.msi) downloaded from the PDF is digitally signed, which is a new tactic.
- **Uses Legitimate Processes:** The new Qakbot uses legitimate Microsoft processes like srtasks.exe, conhost.exe, wermgr.exe, vssvc.exe, and FileCoAuth.exe to blend in with normal system activity and evade detection.
- **Encryption Method:** There are minor changes to the new Qakbot DLL, including AES to decrypt the string rather than XOR in the previous version.
- **Targeting:** The new Qakbot has been observed targeting the hospitality industry.
- **Version:** The payload was configured with the previously unseen version.

Tactics, Techniques, and Procedure

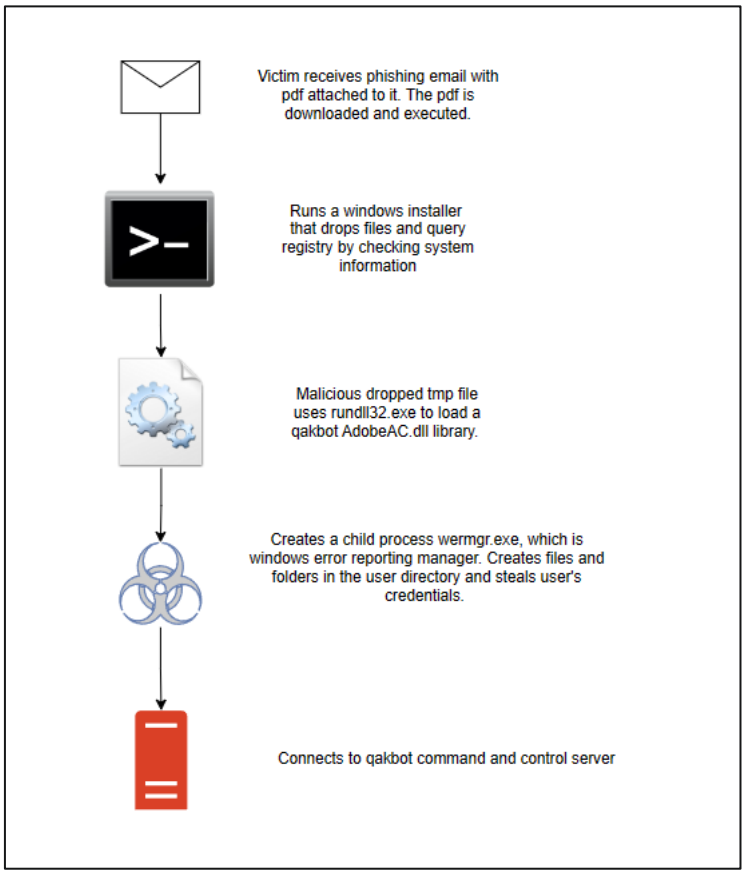

Figure 1: Infection Chain

The new campaign of Qakbot starts with the target receiving an email from users masquerading as an IRS employee. A PDF file is attached to the email that pretends to be a guest list that says, “Document preview is not available” and then prompts the user to download the PDF to view it properly.

Figure 2: New Qakbot phishing emails impersonating the IRS.

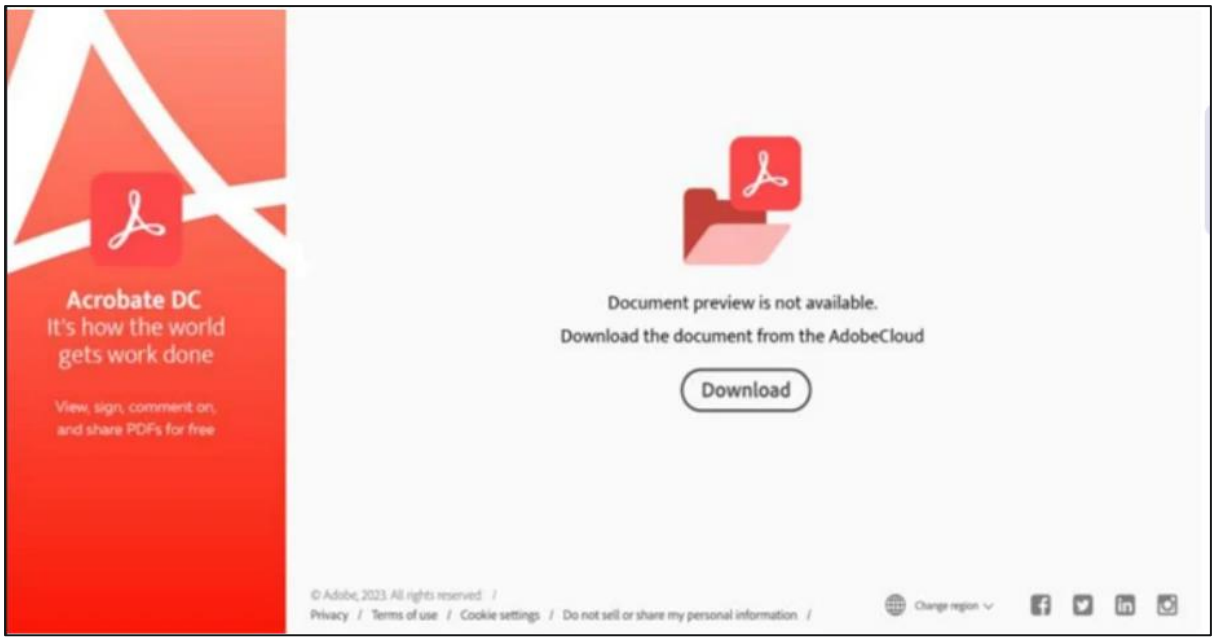

Figure 3: PDF attached to the phishing email.

Clicking on the download button, the recipients will download a digitally signed Windows Installer (.msi). The Windows Installer service (msiexec.exe) starts with /I parameter to install the msi package “list.msi”. Legitimate programs can use this command line to install software packages on a Windows system. But malicious programs can also use this command line to install malware on the victim’s system.

Following the execution process, seven files were dropped, and the security settings of Internet Explorer, software policy configurations, and proxy server information were read. All the seven dropped files have the same md5 hash 5A1F2196056C0A06B79A77AE981C7761. Checking on the virus total these files seem to be non-malicious but match with crowdsourced sigma rule set.

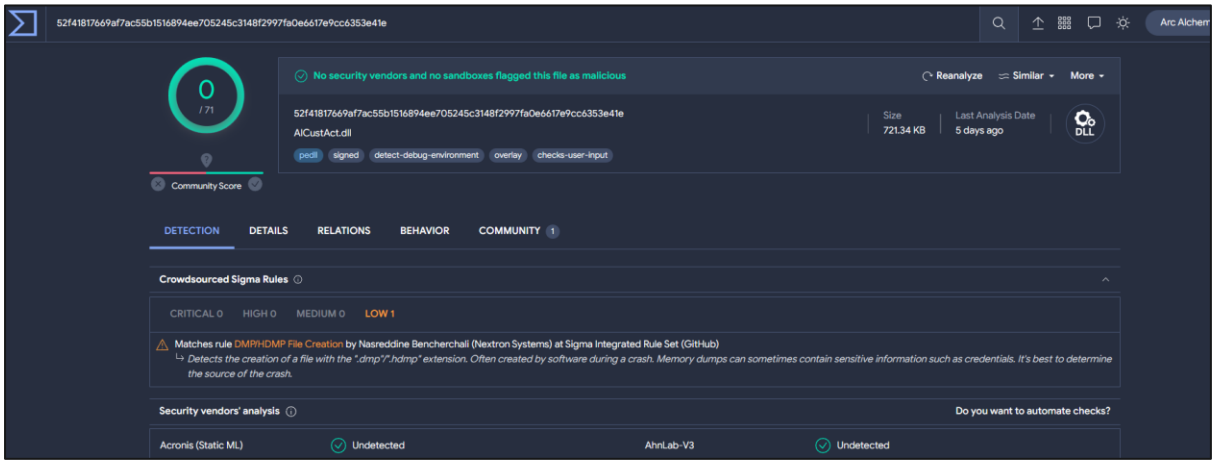

Figure 3: Checking tmp file in virus total

After dropping the files, the command “C:\WINDOWS\system32\msiexec.exe /V” executes. This command line is used to execute the Windows Installer service (msiexec.exe) in verbose mode. /V parameter can be used to hide the installation process from the user by suppressing any user interface or progress indicator. Verbose mode can also be used to gather information about the system. This process drops 3 portable executables to the Windows directory, with 2 of them having the same md5 hash as the above-dropped files 5A1F2196056C0A06B79A77AE981C7761. One of the dropped tempt files has B41E1B0AE2EC215C568C395B0DBB738A hash and the virus total verdict shows that it is malicious. Malicious users can these dropped files to execute malicious code, exploit vulnerabilities, evade detection, persistence mechanisms, and data exfiltration.

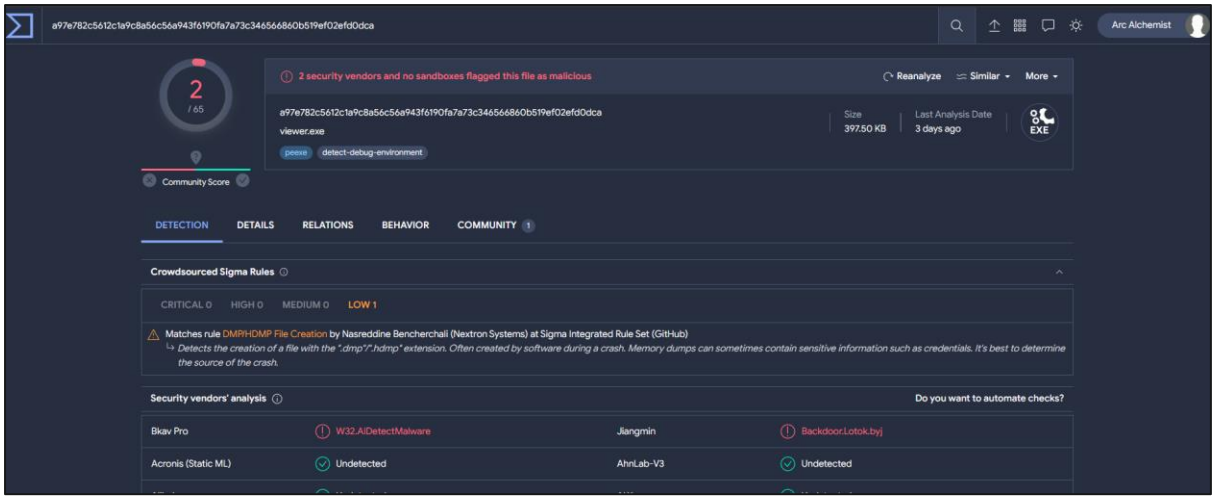

Figure 4: running the hash of the dropped file in the virus total

The command “C:\WINDOWS\system32\msiexec.exe /V” also checks the Windows trust settings HKEY_USERS\S-1-5-21-3896776584-4254864009-862391680-1000\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\WINTRUST\TRUST PROVIDERS\SOFTWARE PUBLISHING. This registry key contains information about the software publishers that are trusted by the system. Malicious users can modify the list of trusted software publishers, which could allow them to install malicious software on the computer without triggering any security warning.

After reading the software policies, and machine GUID from the registry; this process creates a file in the user directory: “C:\Users\admin\AppData\Roaming\AdobeAC.dll”

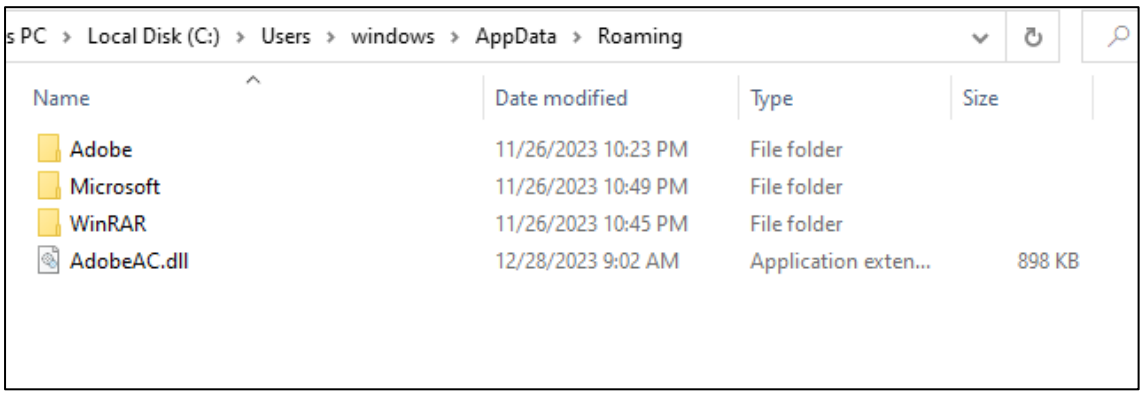

Figure 6: Qakbot dll.

File Name: AdobeAC.dll

md5: 88bbf2a743baaf81f7a312be61f90d76

The AdobeAC.dll file is executed with ""C:\Windows\System32\rundll32.exe" C:\Users\admin\AppData\Roaming\AdobeAC.dll,EditOwnerInfo" command. This command line is used to execute the rundll32.exe to load AdobeAC.dll with function 'EditOwnerInfo'. The 'EditOwnerInfo' function could be a malicious function designed to perform unauthorized actions on the system, such as modifying owner information for malicious purposes. Checking the hash of AdobeAC.dll in multiple trusted sandboxes, it was discovered that the file is a QakBot.

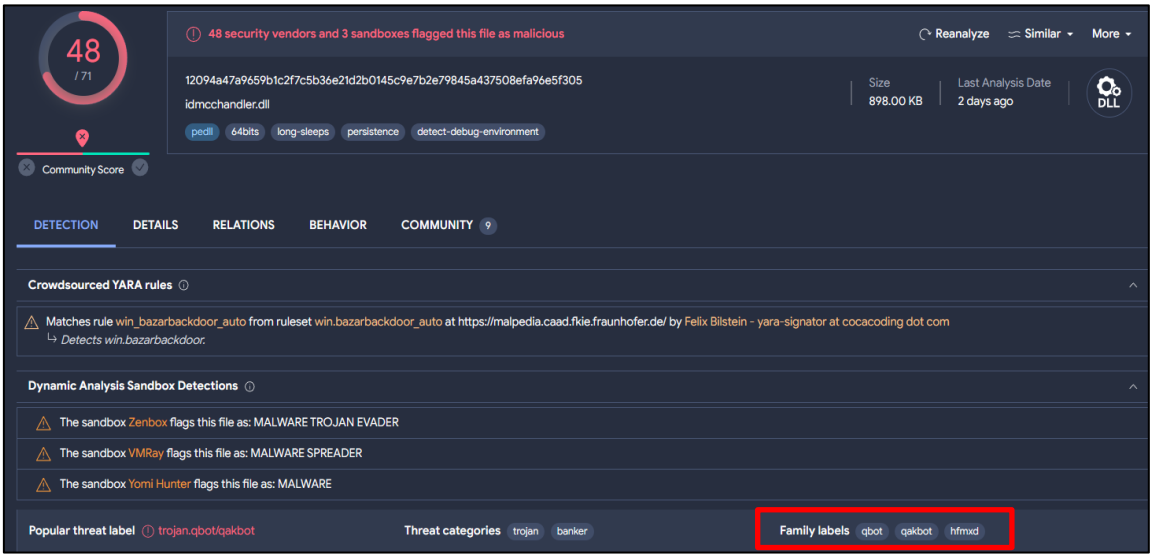

Figure 5: AdobeAC.dll virus total verdict

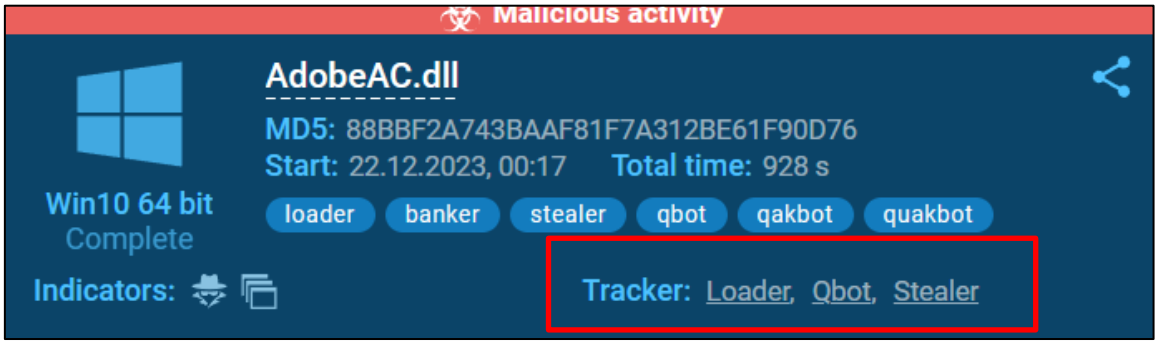

Figure 6: Any.run verdict of AdobeAC.dll

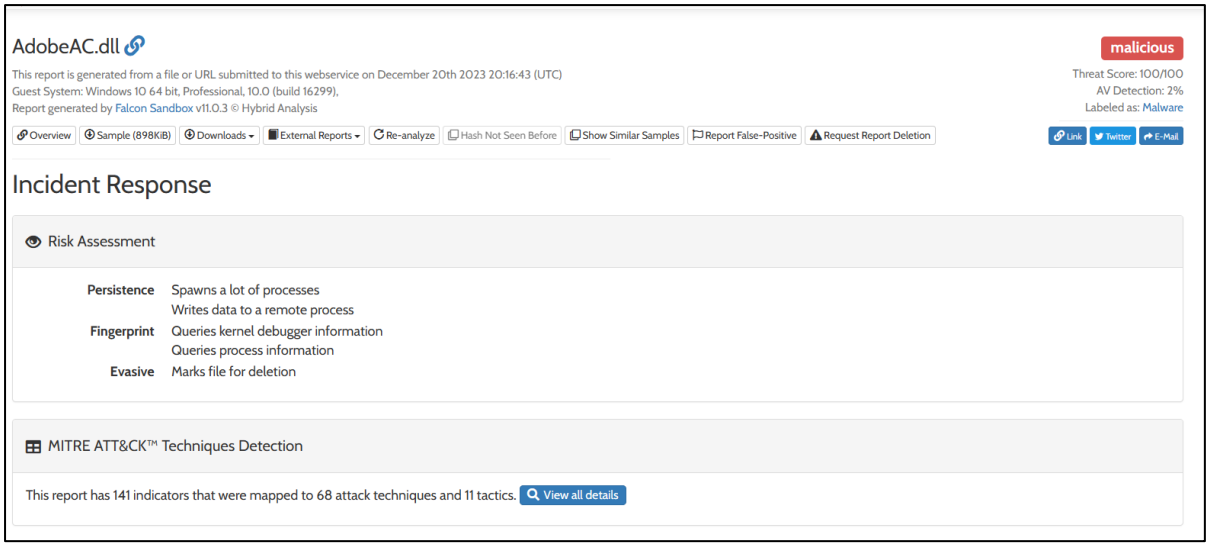

Figure 7: Verdict from hybrid analysis.

Another process executes from the msiexec.exe with the command "C:\Windows\syswow64\MsiExec.exe -Embedding A40E12B663B7C72922B2865E153457C4 C" which invokes Windows installer with (Component Object Model) COM embedding and passing with "A40E12B663B7C72922B2865E153457C4 C" identifier. Legitimate programs can use the "-Embedding" parameter to enable the Windows Installer service to run in a separate process to improve performance and stability while malicious programs can use this to execute arbitrary commands or download and install malware.

After this process, "srtasks.exe" executes with the argument "ExecuteScopeRestorePoint /WaitForRestorePoint:4" in the Windows 32 directory. Srtasks.exe is a legitimate Microsoft process known as System Protection Background Tasks. This command is used to create a system restore point and wait for the restore point to be created. The /WaitForRestorePoint:4 parameter specifies the number of minutes to wait for the restore point to be created. Malicious users with administrative privileges, can create a restore point and use it to revert the system to its previous state, potentially undoing any security measures implemented.

“\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1” process is a child process of srtasks.exe. This command line is used to execute the conhost.exe process with the argument of “-ForceV1” which can be used to force the use of an older version of the console host. With the older version, it is easier to bypass security measures and exploit vulnerabilities.

After this process, the application with the command line:

““C:\WINDOWS\Installer\MSIA5DC.tmp” /HideWindow rundll32 C:\Users\admin\AppData \Roaming\AdobeAC.dll,EditOwnerInfo” starts. This command line runs the rundll32 command to load a DLL file “AdobeAC.dll” function named EditOwnerInfo. The “/HideWindow” parameter runs the process silently without displaying any user interface or window. The function “EditOwnerInfo” could be a custom function within the DLL that performs malicious actions. It queries the registry by reading the date of Windows installation.

After the AdobeAC.dll loads, “wermgr.exe” Windows Error Reporting Manager starts. This is a genuine executable that is responsible for collecting and sending error reports to Microsoft when a program crashes or encounters an error. In this case, the process was executed by a parent process called rundll32.exe with a command line that includes a suspicious DLL file (AdobeAC.dll). This suggests that the “wermgr.exe” process may be used maliciously to hide or disguise malicious activities. It also creates files or folders in the user directory, which could indicate the installation of additional malware or the theft of personal data. It also checks proxy server information, reads software policy settings, and reads security settings of Internet Explorer, which are actions commonly performed by

malware to gather information or modify system settings. It then connects to Qakbot CnC (command and control) server (116.203.56.11 and109.107.181.8).

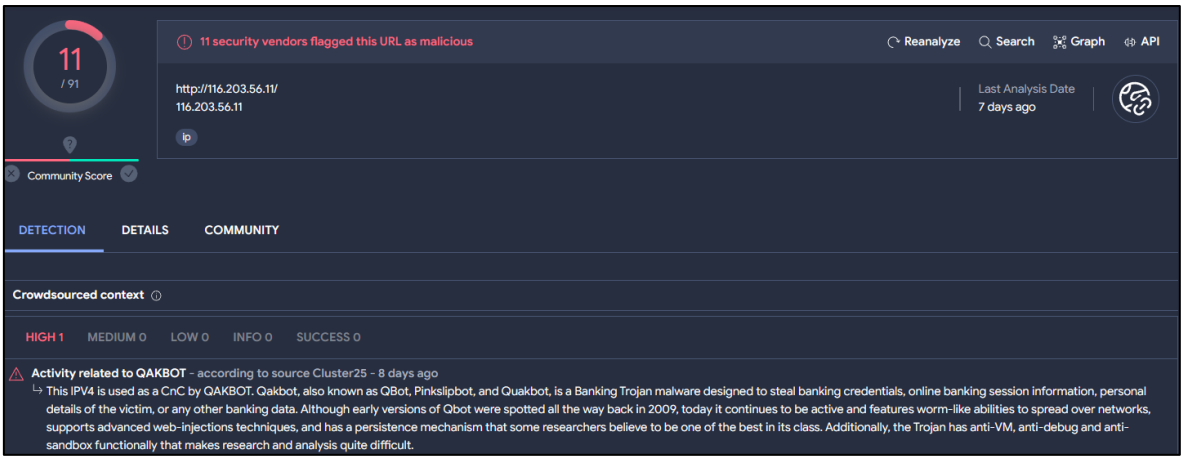

Figure 8: Virus total result

Figure 9: Threatfox result

Figure 10: Virus total result

Figure 11: Threat Fox result

Vssvc.exe (Microsoft volume shadow copy service) runs after the wermgr.exe process ends. Vssvc.exe is a Windows service that allows users to create snapshots of files and volumes,

which can be used for backup and recovery purposes. Vssvc.exe is responsible for managing the creation and deletion of shadow copies. This program might be executed to hide the malware execution or manipulate or disable the VSS service to prevent the creation of shadow copies, making it more difficult for users to recover their files in the event of an infection.

“C:\Users\admin\AppData\Local\Microsoft\OneDrive\19.043.0304.0013\FileCoAuth.exe -Embedding” command line is used to execute the “FileCoAuth.exe” program with the “-Embedding” parameter. This enables communication between different components or processes. FileCoAuth.exe is an executable file that is part of the Microsoft OneDrive software, a file hosting service and synchronization service. It is responsible for the co-authoring feature in OneDrive, which allows multiple users to work on the same document at the same time. If you are using Microsoft OneDrive, you should not remove this file. If you find that the file is malicious, you should remove it to protect your computer. In this case, the “FileCoAuth.exe” program is probably using the parameter to embed itself into another process or to enable inter-process communication. Malicious programs can use this to hide their activities or to inject malicious code into legitimate processes. By embedding themselves into another process, they can evade detection and perform malicious actions without arousing suspicion.

MITRE ATT&CK techniques

The 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)
Execution	System Services (T1569) • Service Execution (T1569.002)
Defense Evasion	System Binary Proxy Execution (T1218) • Rundll32 (T1218.011)
	Virtualization/Sandbox Evasion (T1497) • Time Based Evasion (T1497.003)
Credential Access	Unsecured Credentials (T1552) • Credentials In Files (T1552.001)
Discovery	Software Discovery (T1518)
	Query Registry (T1012)
	System Information Discovery (T1082)
	Virtualization/Sandbox Evasion (T1497) • Time Based Evasion (T1497.003)
	System Location Discovery (T1614)
Command and Control	Application Layer Protocol (T1071)

Indicator of Compromise

IP Addresses

138.91.171[.]81

116.203.56[.]11

139.178.84[.]217

52.142.223[.]178

2.18.97[.]227

109.107.181[.]8

20.231.121[.]79

23.192.153[.]142

172.64.155[.]106

50.112.202[.]115

52.165.165[.]26

13.85.23[.]206

184.30.21[.]171

2.16.241[.]19

20.50.80[.]213

Hashes

82b8bd90e500fb0bf878d6f430c5abec

88bbf2a743baaf81f7a312be61f90d76

Dropped executable file

C:\Users\admin\AppData\Local\Temp\MSI3301.tmp

52f41817669af7ac55b1516894ee705245c3148f2997fa0e6617e9cc6353e41e

C:\Users\admin\AppData\Roaming\AdobeAC.dll

12094a47a9659b1c2f7c5b36e21d2b0145c9e7b2e79845a437508efa96e5f305

C:\WINDOWS\Installer\f5422.msi

93a98b919aec23411ae62dba8d0d22f939da45dec19db2b4e7293124d8f1507f

C:\WINDOWS\Installer\MSI5D4E.tmp

a97e782c5612c1a9c8a56c56a943f6190fa7a73c346566860b519ef02efd0dca

Threat Summary	
Name	Qakbot
Threat Type	Malware, Trojan, Bazar Loader, Banker
Detection Names	BitDefender: Trojan.GenericKD.70825276, ALYac: Trojan.Agent.QakBot Antiy-AVL: Trojan[Banker]/Win64.Qbot Arcabit: Trojan.Generic.D438B53C Avast: Win63:BankerX-gen [Trj]
Symptoms	Unusual Network Activity, drops executable file, Query Registry, Uses RUNDLL32.EXE to load library, Connects to Qakbot Command and Control Server, Modified Proxy Settings, Altered Registry Values
Additional Information	It's important to keep in mind that Qakbot may not be the only malware present in an infected system. It can work in conjunction with other malicious samples and can be downloaded by notorious Trojans.
Distribution methods	Phishing techniques
Damage	Steal sensitive information, data loss, downtime, and financial loss.
Malware Removal (Windows)	Effective removal typically requires using robust antivirus or antimalware software capable of detecting and eradicating the malware components. Additionally, restoring the system to a known good state through system backups and performing a thorough analysis of network activity is recommended to ensure complete removal and mitigate potential residual threats.

Recommendations

1. **Email Security**: Implement advanced email security solutions to filter out malicious emails and prevent users from falling victim to phishing attacks. Train employees to recognize suspicious emails and links.
2. **User Awareness Training**: Regularly educate and train employees about the risks of clicking on unknown links or downloading attachments from unverified sources. Ensure they are aware of common social engineering tactics.
3. **Endpoint Protection**: Utilize robust endpoint protection software that includes features like real-time malware scanning, intrusion detection, and behavioral analysis to detect and block malware before it can execute.
4. **Patch Management**: Keep all software, including operating systems and applications, up to date with the latest security patches. Vulnerabilities in outdated software can be exploited by malware.
5. **Network Monitoring**: Implement network monitoring solutions that can detect unusual network traffic patterns or connections, helping to identify potential infections early.
6. **Firewall Rules**: Configure firewalls to block unnecessary outgoing traffic, especially on non-standard ports. This can prevent malware from communicating with its command-and-control server.
7. **Least Privilege Principle**: Limit user and system privileges to the minimum necessary to perform their tasks. This reduces the potential impact of malware if a system is compromised.

8. **File Reputation Services**: Utilize file reputation services like VirusTotal to check the legitimacy of downloaded files before they are executed, helping to identify potentially malicious content.
9. **Regular Backups**: Conduct regular backups of critical data and systems. Ensure backups are isolated from the network and periodically test restoration procedures.
10. **Incident Response Plan**: Develop and regularly update an incident response plan that outlines the steps to be taken in case of a malware infection. Ensure all team members are familiar with their roles and responsibilities.

By following these recommendations, one can significantly reduce the risk of falling victim to malware like Qakbot and strengthen overall cybersecurity defenses. Also, it is important to remember that cyber adversaries 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 and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairav.net

Website: https://vairav.net