Oakbot

Threat: **Banking Trojan**

Author: **Jeffrey Farnan** Date Originally Published: **February 28th, 2023**

1. SUMMARY

- Qakbot is a Banking Trojan or a modular information stealer which has been known to steal financial data (banking credentials, online banking session information, victim's personal details, etc.) and has been activate since 2007. It is distributed through phishing emails containing malicious documents, attachments, or password-protected archives. The attachments usually involve a document that downloads the Qakbot payload. Qakbot is often used as a gateway entry point, similar to TrickBot or Emotet campaigns leading to post exploitation operations such as the delivery of Ransomware. Qakbot is recognised as one of the top malware strains of recent times.

2. MALWARE FAMILY

- **Type** = Banking Trojan.
- **Sub-type** = Backdoor, Worm, Remote Access Trojan (RAT) .
- Classified as a Banking Trojan, Worm and a Remote Access Trojan (Rat), Qakbot steals sensitive data and attempts to self-propagate to other systems on the network. Qakbot can provide backdoor capabilities, allowing an attacker to perform manual attacks to achieve secondary objectives such as scanning the compromised network or injecting ransomware.
    - **Banking Trojan:** Malicious Software designed to gather user information from a victim's system, information used to login into a system, such as usernames and passwords. When this information is gathered it is sent back to the attacker system via email or over a network.
    - **Backdoor:** Gain unauthorized access to the application/system/network while bypassing all the implemented security measures and proceed to install other types of malware.
    - **Worm:** attempts to self-propagate to other systems on the network.
    - **Remote- Access-Trojan (RAT):** Malware used by an attacker to gain full administrative privileges and remote control of a target computer.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Unknown.
- **First seen date/period** = January 2007.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = February 20th, 2023.

4. MALWARE HISTORY

- Oakbot is also known by other names such as Qbot or Pinkslipbot and has been active since 2007. it was initially known as a Banking Trojan and a loader using C2 servers for payload delivery.
- Initially Qakbot was distributed by Emotet malware, but currently the major infection vector is malspam email campaigns with multiple variants. It has been identified as a key “malware installation-as-a-service” botnet enabling many of today’s campaigns.
- In March 2020, Qakbot had evolved and spread through email thread hijacking allowing the threat actors to insert malicious replies into the middle of existing email conversations and compromising the accounts of other infection victims.
- With its modularity and flexibility development it also became capable of spying of financial operations and redirecting users to fake banking sites. It also sold access to affected devices to other threat actors, who used this access for a wide range of activities from deploying other trojans to ransomware.

5. MALWARE DESCRIPTION

- Qakbot modular nature allows it to persist in today’s computing landscape because it enables attackers to pick and choose the “building blocks” they need for each attack chain depending on the network environment the malware lands on. Attack methods can come in many different forms, the most common:
    - **Email:** The QakBot email lures are not the most sophisticated. The lure text is not well written, but it has been effective enough to convince people to open the attachment. The messages in these email campaigns typically consist of one- or two-sentence lures (for example, “please see attached” or “click here to view a file”). Such brevity provides sufficient information and a call to action for the target users but little for content security solutions to detect.
    - **Malicious links:** The email campaigns we observed delivering Qakbot typically include the URLs that download the malware on target devices in the message body.
    - **Embedded Images:** A recent evolution, Qakbot arrives via an email message that only contains an embedded image in its body, the image is designed to *look* like the message body. The image instructs recipients to type the URL directly in their browser to download an Excel file that eventually leads to Qakbot.
- Most recently, threat actors have transformed their techniques to evade detection by using ZIP file extensions, enticing file names with common formats, and Excel (XLM) 4.0 to trick victims into downloading malicious attachments that install Qakbot. Embedded as commonly named attachments, Qakbot leverages ZIP archive file having embedded files such as Microsoft Office files, LNK, Powershell, and more.
- Qakbot campaigns use Highly Evasive Adaptive Threat (HEAT) techniques:
    - **Excel 4.O Macros:** This campaign uses Excel 4.0 macros to add commands into spreadsheet cells and then send the email attachment to the intended targets. When the victim opens the XLS document, they are asked to enable the macro to execute the Excel 4.0 macros containing the commands. These commands downloads and executes the payload from the C2.
    - **Follina Exploit:** A windows vulnerability referred to as **CVE-2022-30190 leveraged to deliver Qakbot on compromised networks for initial access by several cybercriminal groups.** When executed, the

document containing the exploit calls out to external HTML file that uses ms-msdt URL protocol to execute PowerShell code.

- **Email Lure with Hyperlink:** This technique uses a compromised domains to host malicious payloads. The attackers would send an email with a link to the victim, which would download a password-protected ZIP file contain the Qakbot Trojan. The ZIP file would contain a link file which can easily provide PowerShell or JavaScript commands to execute. When opened this link file downloads the JS file and then downloads the Qakbot payload.
- **HTML Smuggling:** This campaign uses specially crafted HTML attachments and web pages to build malware directly on endpoint devices behind the firewall. The victim would open and HTML email attachment, while the HTML file would then construct the payload through a decoding process. A password-protected ZIP file would then be created, when extracted, would drop an ISO file (Report Jul 1471645.iso) containing the Qakbot payload onto the endpoint machine.

- Qakbot can provide remote code execution (RCE) capabilities, allowing an attacker to perform manual attacks to achieve secondary objectives such as scanning the compromised network. However, its developers have also developed functionalities that allow to evade detection and debugging, and install additional malware or injecting ransomware on compromised machines.
- Qakbot is still a dangerous and persistent threat to organizations and has become one of the leading Banking Trojans globally.

6. POTENTIAL CUSTOMER DEFENSE

- QakBot is still a dangerous malware and it seems like the threat group behind it keeps evolving its techniques throughout the years. Qakbot campaigns could look strikingly different on each affected device, significantly impacting how defenders respond to such attack. Having a first layer of defence in place is critical. Security teams need to update their defences preventing threats from reaching their endpoints.
- Some tips for user protection from this infection:
  - Do not open email attachments if they come from unknown sources.
  - Minimize your attack surface by using an email filtering system.
  - Do not activate macros (“Enable Content”) when opening a Word or Excel document.
  - When using Microsoft OneDrive especially when dealing with password-protected ZIP archives, do not follow any links to OneDrive even coming from a supposedly trustworthy source.
  - Report suspicious emails to your Cybersecurity team.
  - Update security software regularly specially browser protection.
- Some tips for enterprise protection from this infection:
  - The most effective way to protect against this malware is with Advanced Threat Protection for email. This will block the receipt of dangerous email attachments on your email gateway, including Office documents with macros.
  - Block access to known Qakbot botnet C&C servers on your security perimeter (e.g. firewall, web proxy, etc.). Lists can be found in various security forums.
  - Block access on your security perimeter (via firewall, web proxy, etc.) to websites that are currently being used to spread malware. Lists can be found in various security forums.

Research Sources:

- https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/vorsicht_e-mails_2.html
- https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot
- https://www.cyfirma.com/outofband/html-smuggling-a-stealthier-approach-to-deliver-malware/
- https://www.microsoft.com/en-us/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/
- https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html
- https://cybersecurity.att.com/blogs/labs-research/the-rise-of-qakbot
- https://www.menlosecurity.com/blog/an-anatomy-of-heat-attacks-used-by-qakbot-campaigns/
- https://www.huntress.com/blog/threat-advisory-qakbot-activity-is-rising