LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Qbot and Ransomware

08/05/2021

TLP: WHITE, ID# ***202108051300***

Agenda

- History of Qbot Malware
- Qbot Tactics, Techniques, and Procedures (TTPs)
- Qbot Ransomware Partners
- Q2 2021 Qbot Attacks
- Retaliation and Aftermath
- Mitigations
- References

Slides Key:

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

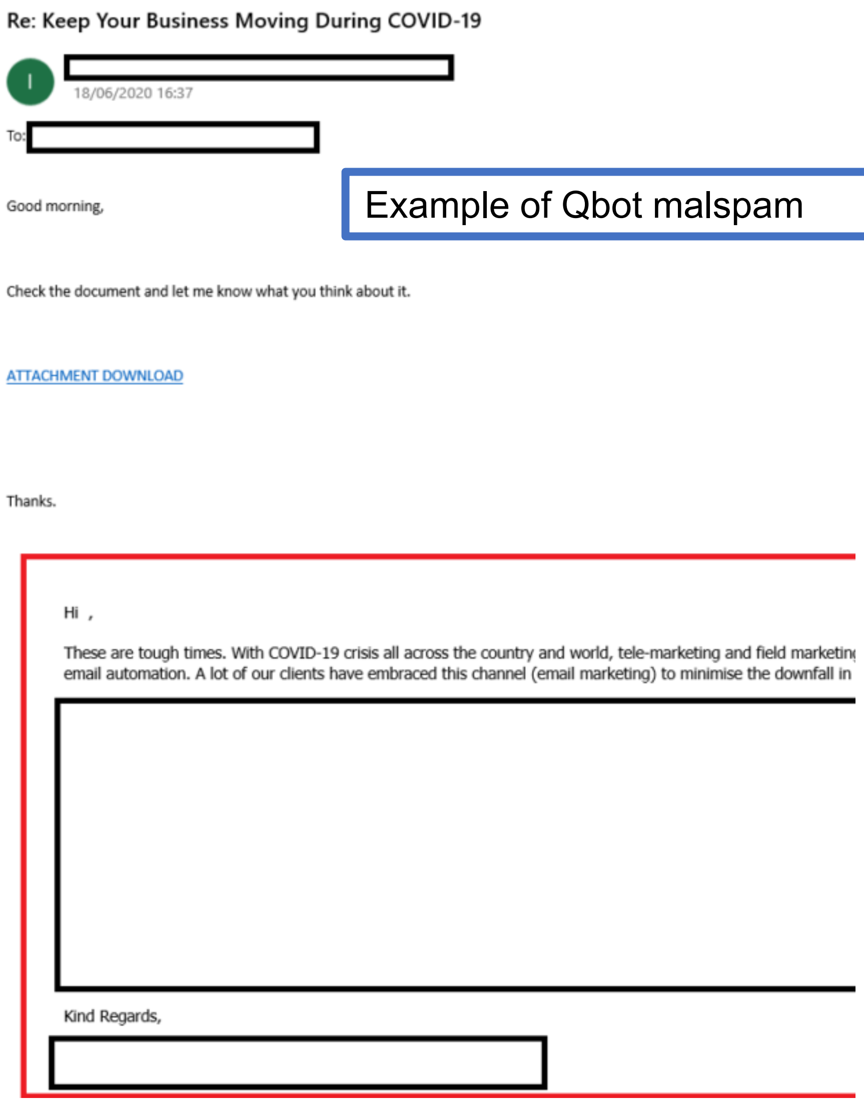
Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

History of Qbot Malware

- Qbot (also known as Qakbot or Pinkslipbot) is a banking trojan that steals financial data, browser information/hooks, keystrokes, and credentials
  - Originally developed to target financial institutions or steal financial information
  - Not exclusive to financial crimes or targets
- Discovered in 2008, gaps in operational use in the wild
- Operators are occasionally known as GOLD LAGOON
  - Not exclusively associated with any one actor or group of actors
- Trend Micro Periodic Campaign Detection Rates
  - January – May 2020 campaign contained almost 4,000 unique detections
    - 28% of detections targeted the HPH sector
  - August – November 2020
    - 8% of detections targeted the HPH sector

Qbot Tactics, Techniques, and Procedures (TTPs) – 1

- Previously distributed by Emotet, but can appear through malspam email campaigns
  - Uses email conversation thread hijacking in its campaigns
    - Replies to emails that it finds in its victim's mailboxes
    - Employs Microsoft Excel documents impersonating DocuSign-encrypted spreadsheets to deliver Qbot as an initial access vector
    - Targeted victims receive mail with a malicious attachment that when opened, drops and executes a DLL using the legitimate Windows binary, regsvr32
    - Emails contain a URL to a ZIP with a malicious VBS (Visual Basic Script) file
- Can also self-spread using an SMB brute force module that contains a list of commonly used passwords



Re: Keep Your Business Moving During COVID-19

I [redacted]

18/06/2020 16:37

To: [redacted]

Good morning,

Check the document and let me know what you think about it.

ATTACHMENT DOWNLOAD

Thanks.

Hi ,

These are tough times. With COVID-19 crisis all across the country and world, tele-marketing and field marketin
email automation. A lot of our clients have embraced this channel (email marketing) to minimise the downfall in

[redacted]

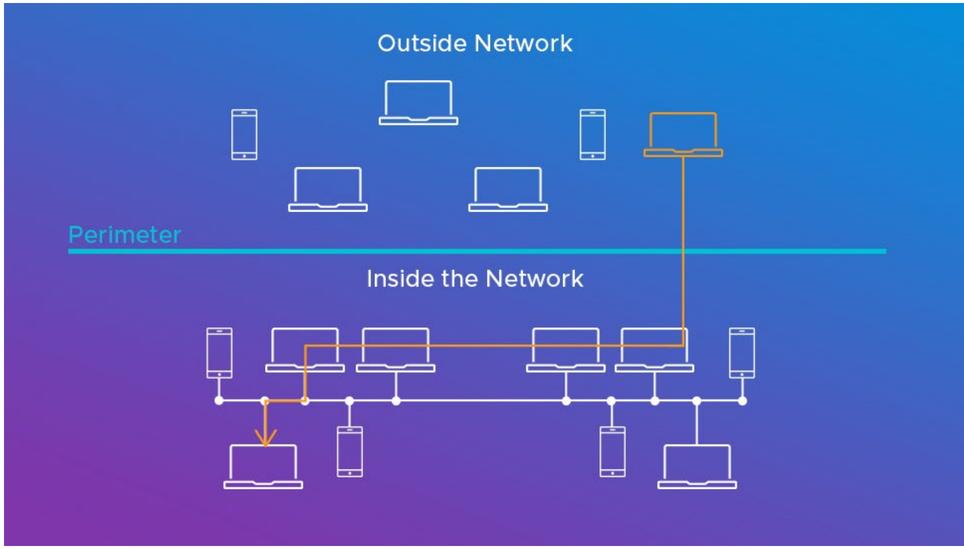
Kind Regards,

[redacted]

Example of Qbot malspam

Qbot Tactics, Techniques, and Procedures (TTPs) – 2

- Qbot's operators frequently upgrade its versions and leave version tags marked in the samples
  - The December 2020 update activates its persistence mechanism right before infected Windows devices shut down, and it automatically removes any traces when the system restarts or wakes up from sleep
    - This allows the persistence mechanism to be activated too closely to shutdown for security programs to detect
    - Gozi and Dridex have used similar techniques
- Implements multiple encryption schemes
  - This conceals its functionality and data from both potential victims and security programs
- Attempts obfuscation via legitimate process injection
- Once the victim has been infected, their computer is compromised, and they are also a potential threat to other computers in the local network because of Qbot's lateral movement capabilities

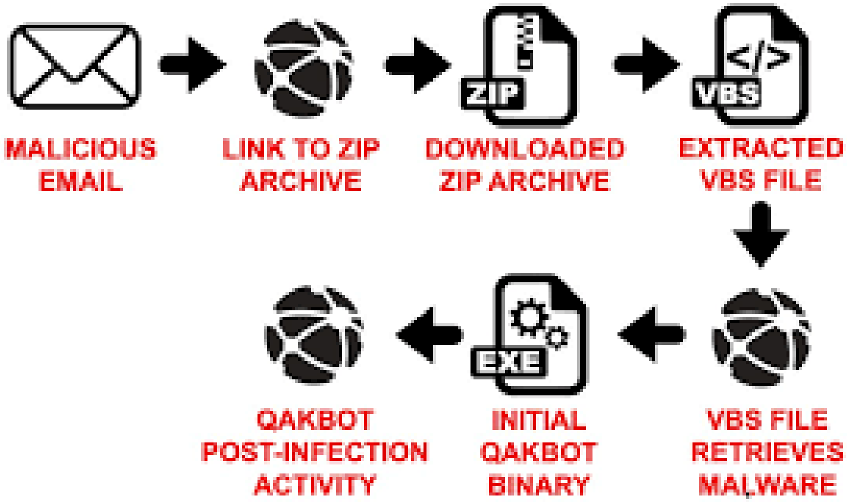


Qbot Tactics, Techniques, and Procedures (TTPs) – 3

- Universal plug-and-play (UPnP) module transforms infected hosts without direct Internet connectivity into intermediate command and control (C2) servers used for the botnet
    - C2 services begin downloading other modules
        - Password Grabber module
            - Tries to steal credentials
        - hVNC plugin
            - Allows an external operator to remote control the device, including performing bank transactions without the user’s knowledge, using a VNC connection
            - Can be used even while user is logged into computer
        - Cookie Grabber module
            - Steals cookies from popular browsers
        - Web-inject module
            - Provides the injector module with a list of websites and JavaScript code that will be injected if the victim visits any of these websites
            - Primarily for financial institutions
        - Email collection module
            - Extracts all emails from the local Outlook client
            - These emails are then used by Qbot for new phishing campaigns

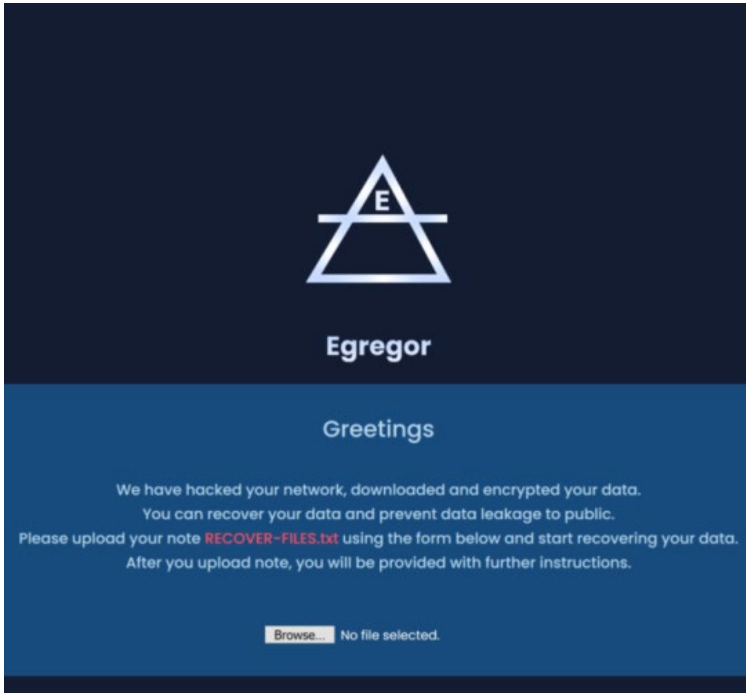
Qbot Tactics, Techniques, and Procedures (TTPs) – 4

- Known to leverage many other tools; for example, PowerShell and Mimikatz are used for self-propagation
  - 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
- Will download ransomware
  - Prolock
  - Egregor
  - REvil/Sodinokibi
- "A network infection attributed to QBot automatically results in risks associated with future ransomware attacks.“ – CEO of Advanced Intel, Vitali Kremez



Qbot Ransomware Partners – Egregor

- Variant of the Sekhmet ransomware family
- Emerged in September 2020
- Debut coincided with MAZE ransomware gang's shutdown
  - Many MAZE affiliates moved to Egregor
- Shares TTPs with ProLock
- Sold as a Ransomware-as-a-Service (RaaS), with the gang selling it or renting it to other people to use maliciously
- Uses double extortion method
  - First extortion: ransom is demanded to decrypt encrypted files
  - Second extortion: ransom is demanded to prevent ransomware operators from posting stolen data online
- Opportunistic and prolific: In their first two months of operation, targeted 69 companies around the world with 32 targets in the U.S.
- Egregor has targeted healthcare facilities and hospitals during the coronavirus crisis
- Frequently associated with Qbot

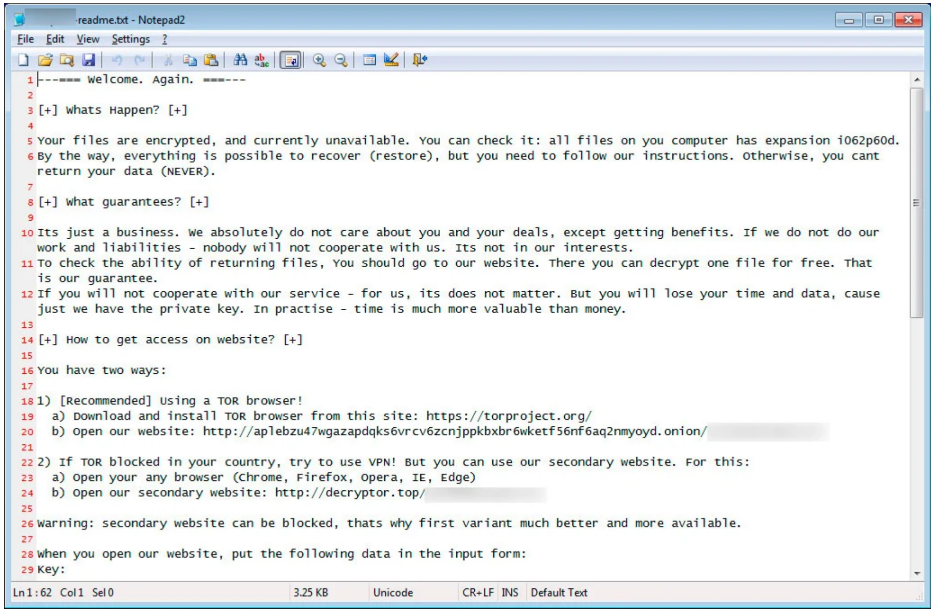


Greetings

We have hacked your network, downloaded and encrypted your data.
You can recover your data and prevent data leakage to public.
Please upload your note RECOVER-FILES.txt using the form below and start recovering your data.
After you upload note, you will be provided with further instructions.

Qbot Ransomware Partners – REvil/Sodinokibi

- The REvil ransomware operation is believed to be operated by a core group of Russian threat actors
- Launched in April 2019
- Believed to be rebranding/relaunch of GandCrab, which closed in June 2019
- Ransomware-as-a-Service
    - Maintains affiliate program to recruit partners
    - The core team earns 20-30% of all ransom payments, while the rest goes to their affiliates
- Practices double extortion
- Using the remote access provided by a trojan, the REvil infiltrates a network and spreads slowly to other devices while stealing unencrypted data
- Once they gain access to a Windows domain administrator account and have harvested any data of value, they deploy the ransomware throughout the system to encrypt devices



```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion i062p60d.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/[redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/[redacted]

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:
```

Q2 2021 Qbot Attacks

- Two major corporations affected:
  - JBS
    - Headquartered in Brazil
    - Largest meat producer in the world
    - Attacked via U.S. and Australian IT systems
  - FUJIFILM
    - Headquartered in Japan
    - A major provider of medical imaging capabilities, although there were no reports that these were compromised
- HC3 received information from a trusted third party regarding more than 50 malicious emails attempting to distribute Qbot malware to a U.S. hospital during a two-week period in June 2021

Q2 2021 Qbot Attacks – JBS

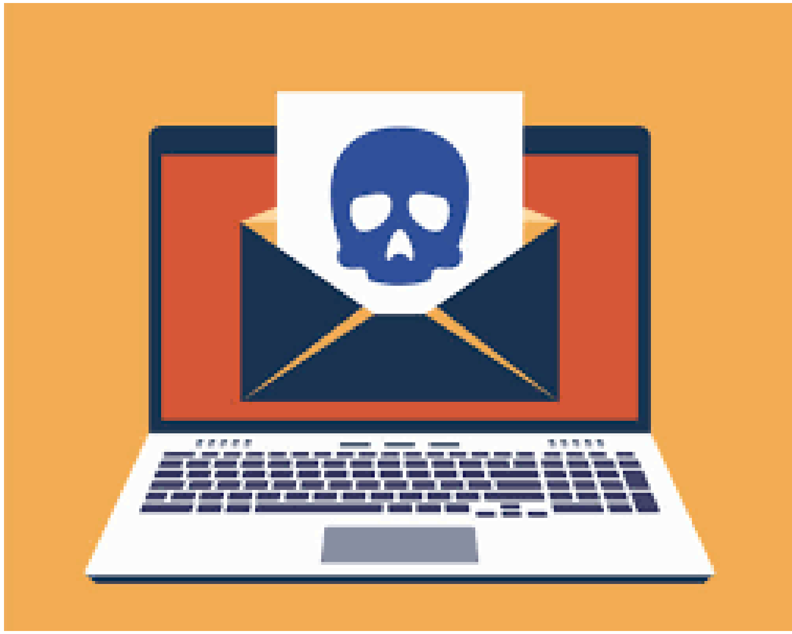
- Occurred in the early morning of May 31, 2021
- "The company took immediate action, suspending all affected systems, notifying authorities and activating the company's global network of IT professionals and third-party experts to resolve the situation." – Statement from JBS USA
- Led to shutdown of multiple food production sites due to loss of network access
  - Attack halted cattle slaughtering at all of its U.S. plants for a day
  - Extended shutdown could significantly disrupt food supply chains
- JBS claimed attack did not affect backups, but BleepingComputer reported that there were two encrypted/corrupted datasets that had prevented the company from going back online immediately
- Resulted in $11 million ransom payment
- JBS claims that “preliminary probe results show no company, customer or employee data was compromised in the attack”
- Forensic investigation ongoing

Q2 2021 Qbot Attacks – FUJIFILM

- Appeared to be infected with Qbot malware on May 15, 2021, according to CEO of Advanced Intel, Vitali Kremez
- In the late evening of June 1, 2021 (JPT), FUJIFILM became aware of the possibility of a ransomware attack. As a result, the company took measures to suspend all affected systems in coordination with various global entities.
  - "FUJIFILM Corporation is currently carrying out an investigation into possible unauthorized access to its server from outside of the company. As part of this investigation, the network is partially shut down and disconnected from external correspondence."
- On June 1, 2021, FUJIFILM USA added an alert to the top of their website stating that they are experiencing network problems that are affecting their phone and email systems.
- The company was forced to take down portions of its network worldwide
- At approximately 10:00 AM EST on June 1, FUJIFILM told employees to shut off their computers and all servers immediately, including access to email, the billing system, and a reporting system.
- Claimed to have restored normal operations by June 14
- FUJIFILM stated that the "investigations completed so far have found no evidence of information leakage to the outside world."
  - No ransomware site has posted FUJIFILM data as of this publication

Q2 2021 Qbot Attacks – U.S. Hospital

- On June 7, 2021, HC3 received information from a trusted third party regarding a malicious Qbot email campaign targeting a U.S. hospital that sees 4.3 million patients annually.
- Hospital observed more than 50 malicious emails attempting to distribute Qbot malware during a two-week period.
  - SOC noted that some of the malicious emails resembled emails from the FUJIFILM attack
    - Likely also carried out by the REvil RaaS operator(s)
  - Majority of emails leveraged invoice themes
  - Investigation revealed that a third-party vendor was most likely compromised and leveraged to distribute the malicious emails to recipients at the hospital



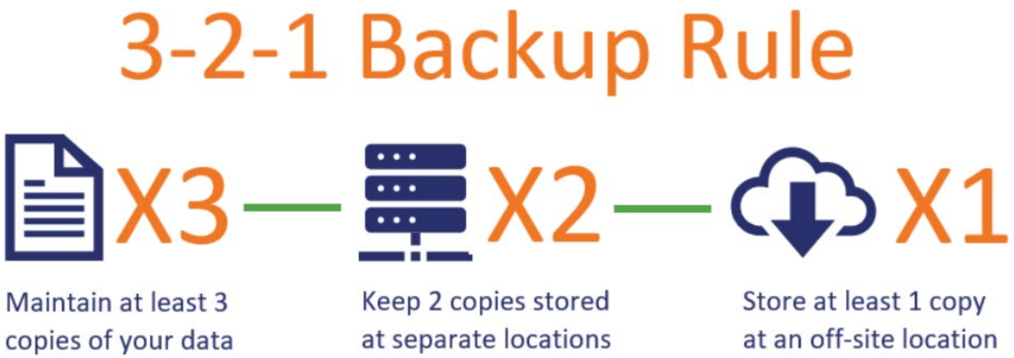
Retaliation and Aftermath

- Russian blogger Sergey RedHunt interviewed an undisclosed representative of the group behind the REvil ransomware
  - Believed to be threat actor UNKN or “Unknown”
  - Previously represented REvil on forums
- Major takeaways from the interview:
  - The representative admitted that the group attacked the food processing company JBS
  - Claimed the target was selected based on several criteria, which included the company’s very high revenue, location in Brazil, and no affiliation with critical infrastructure nor the U.S.
  - The representative claimed not to understand why U.S. officials decided to investigate the attack
  - The representative claimed that the assumption by U.S. law enforcement that all REvil members were in the Commonwealth of Independent States (CIS) region, or in Russia specifically, is false
  - As a result, the representative claimed that the REvil RaaS group lifted its ban on their affiliates attacking any U.S.-based company or organization, **including critical infrastructure,** as well as promising additional benefits for such attacks
    - As of May 13, 2021, REvil has claimed to have imposed restrictions on their affiliates: “Targeting the social sector (health care, educational institutions) is not allowed… Targeting the government sector of any country is not allowed.”
  - Interview did not acknowledge the attacks on FUJIFILM nor on the U.S. hospital

Mitigations

From **CISA's Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks:**

- **Require multi-factor authentication** for remote access to OT and IT networks.
- **Enable strong spam filters to prevent phishing emails from reaching end users.** Filter emails containing executable files from reaching end users.
- **Implement a user training program and simulated attacks for spear phishing** to discourage users from visiting malicious websites or opening malicious attachments, and re-enforce the appropriate user responses to spear phishing emails.
- **Filter network traffic** to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL block lists and/or allow lists.
- **Update software**, including operating systems, applications, and firmware on IT network assets, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program.



3-2-1 Backup Rule

X3 — Maintain at least 3 copies of your data

X2 — Keep 2 copies stored at separate locations

X1 — Store at least 1 copy at an off-site location

Mitigations, cont.

- **Block zip file attachments and disable the execution of macros.**
- **Limit access to resources over networks, especially by restricting RDP**. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require multi-factor authentication.
- **Set anti-virus/anti-malware programs to conduct regular scans** of IT network assets using up-to-date signatures. Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- **Implement unauthorized execution prevention by**:
  - **Disabling macro scripts from Microsoft Office files** transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.
  - **Implementing application allow-listing**, which only allows systems to execute programs known and permitted by security policy.
  - **Monitor and/or block inbound connections from Tor exit nodes and other anonymization services.**
  - **Deploy signatures to detect and/or block inbound connection from Cobalt Strike servers** and other post exploitation tools.

If your organization is impacted by a ransomware or Qbot incident:

- **Isolate the infected system**.
- **Turn off other computers and devices**. Power-off and segregate any other computers or devices that shared a network with the infected computer(s) that have not been fully encrypted by ransomware.
- **Secure your backups**. Ensure that your backup data is offline, secure, and free of malware.

Reference Materials

References – TLP:WHITE

- Abrams, Lawrence. “FBI: REvil cybergang behind the JBS ransomware attack,” Bleeping Computer. June 2, 2021. https://www.bleepingcomputer.com/news/security/fbi-REvil-cybergang-behind-the-jbs-ransomware-attack/
- Abrams, Lawrence. “FUJIFILM confirms ransomware attack disrupted business operations,” Bleeping Computer. June 4, 2021. https://www.bleepingcomputer.com/news/security/FUJIFILM-confirms-ransomware-attack-disrupted-business-operations/
- Asokan, Akshaya. “Qbot Banking Trojan Now Deploying Egregor Ransomware,” BankInfoSecurity. November 23, 2020. https://www.bankinfosecurity.com/qbot-banking-trojan-now-deploying-egregor-ransomware-a-15430
- Brumfield, Cynthia, “Egregor ransomware group explained: And how to defend against it.” CSO Online. February 19, 2021. https://www.csoonline.com/article/3602148/egregor-ransomware-group-explained-and-how-to-defend-against-it.html
- Bunge, Jacob. “JBS Paid $11 Million to Resolve Ransomware Attack,” Wall Street Journal. June 9, 2021. https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781
- Gatlin, Sergiu. “Qbot malware switched to stealthy new Windows autostart method,” Bleeping Computer, December 9, 2020. https://www.bleepingcomputer.com/news/security/qbot-malware-switched-to-stealthy-new-windows-autostart-method/
- Gatlin, Sergiu. “Fujifilm resumes normal operations after ransomware attack,” Bleeping Computer. June 14, 2021. https://www.bleepingcomputer.com/news/security/fujifilm-resumes-normal-operations-after-ransomware-attack/
- “GOLD LAGOON,” SecureWorks. https://www.secureworks.com/research/threat-profiles/gold-lagoon

References – TLP:WHITE

- Ilgayev, Alex. “An Old Bot’s Nasty New Tricks: Exploring Qbot’s Latest Attack Methods,” CheckPoint Security. August 27, 2020 https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/
- Insikt Group. “Egregor Ransomware, Used in a String of High-Profile Attacks, Shows Connections to QakBot,” Recorded Future. December 3, 2020. https://www.recordedfuture.com/egregor-ransomware-attacks/
- Kremez, Vitali & Yelisey Boguslavskiy, “From QBot...with REvil Ransomware: Initial Attack Exposure of JBS,” Advanced Intel. June 7, 2021. https://www.advanced-intel.com/post/from-qbot-with-REvil-ransomware-initial-attack-exposure-of-jbs
- Middelweerd, Roland and Frank de Korte. “QBOT SPAM CAMPAIGN,” Northwave Security. https://northwave-security.com/en/qbot-spam-campaign/
- Minerva Labs. “Qbot Malspam and The Rise Of Sophisticated Evasion Techniques,” Minerva Labs. February 3, 2021.
- Nair, Aishwarya. “Meatpacker JBS says it paid equivalent of $11 mln in ransomware attack,” Reuters, June 10, 2021. https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/
- Page, Carly. “FUJIFILM becomes the latest victim of a network-crippling ransomware attack,” Tech Crunch. June 3, 2021. https://techcrunch.com/2021/06/03/FUJIFILM-becomes-the-latest-victim-of-a-network-crippling-ransomware-attack
- “QakBot Big Game Hunting continues: the operators drop ProLock ransomware for Egregor,” Group-IB. November 20, 2020. https://www.group-ib.com/media/egregor/
- “QakBot reducing its on disk artifacts,” Hornet Security. December 15, 2020. https://www.hornetsecurity.com/en/threat-research/qakbot-reducing-its-on-disk-artifacts/

References – TLP:WHITE

- Santos, Doel et al. “Threat Assessment: Egregor Ransomware,” Unit 42. December 8, 2020. https://unit42.paloaltonetworks.com/egregor-ransomware-courses-of-action/?web_view=true&mid=1#cid=3037314

Questions

Questions

Upcoming Briefs

August 19 – REvil/Sodinokibi Ransomware

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

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

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current 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 presentations that provide 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 visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV