LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

TrickBot, Ryuk, and the HPH Sector

11/12/2020

Report #: 202011121030

Agenda

- Who or What is WIZARD SPIDER?
- What is TrickBot?
- What Connects TrickBot and Ryuk?
- What is Ryuk?
- The Future of TrickBot and Ryuk
- Fall 2020 Action Against TrickBot
- Incident Example: Major US Hospital Network
- Incident Example: Ongoing Ransomware Attack Against US Healthcare and Public Health (HPH) Sector
- Danger to the HPH Sector
- Mitigations
- References

Slides Key:

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

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

Who is WIZARD SPIDER?

- TrickBot is run by cybercriminal group “WIZARD SPIDER” (named by CrowdStrike), UNC1878, or “Team9”
- Alleged to be affiliated with Russian cybercrime rings
- Affiliated with GRIM SPIDER, LUNAR SPIDER, and MUMMY SPIDER
- Some members were part of the group that operated the banking Trojan malware Dyre (Dyreza)
- Dyreza ceased operating in November 2015 after Russian law enforcement raided the entertainment company believed to be behind it
- Toolset covers the entire attack chain and frequently uses the combination of Emotet > TrickBot > Ryuk

Source: CrowdStrike

What is TrickBot?

- Why does the HPH sector care about a banking Trojan?
- At this point, TrickBot is a “fully-fledged information stealer, as well as providing backdoor access to infected machines, enabling cyber criminal groups to use it as gateway for delivering other malware onto already compromised networks” and can act as a botnet
- Uses EternalBlue to move laterally around a network (despite EternalBlue being over 3 years old)
- Run from memory to leave no trace behind
- TrickBot uses standard attack vectors for infection:
  - Malvertising – The use of advertising – legitimate or fake – to surreptitiously deliver TrickBot to victim system
  - SpearPhishing – E-mails with malicious links or attachments that specifically target organizational leadership
  - Network vulnerabilities – SMB (Server Message Block) and RDP (Remote Desktop Protocol) are common
  - Secondary payload – Sometimes dropped by other malware (second stage), often Emotet
- Nothing TrickBot does is unique, but its aggregate capabilities and modular flexibility make it a powerful tool

Emotet

- Delivered via spam, phishing, or RDP exploit, delivers TrickBot

Source: Hershey

TrickBot

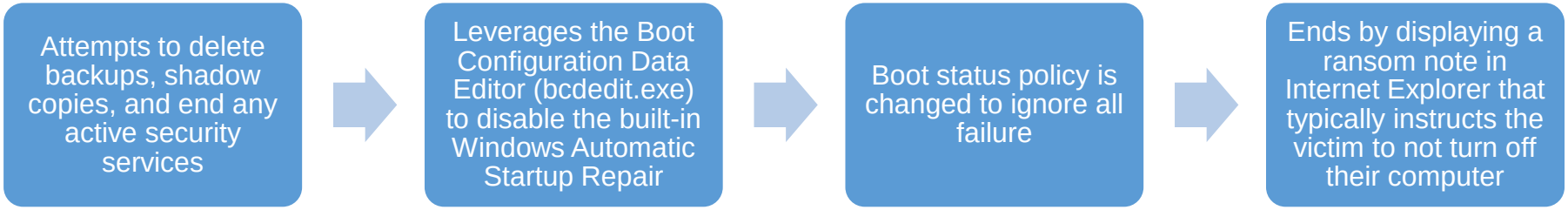
- Used to conduct reconnaissance via Cobalt Strike Beacon and deliver Ryuk

Ryuk

- Ransomware

What is Ryuk?

- A form of ransomware and a common payload for banking Trojans (like TrickBot)
- Originally based on Hermes(e) 2.1 malware but mutated since then
- Ryuk actors use commercial “off-the-shelf” products to navigate victim networks
  - Cobalt Strike, Powershell Empire
- Exploits trusted Windows processes to inject malicious logic to evade detection
- Early versions would sometimes also encrypt key Windows processes, “bricking” the machine
- Research from SonicWall claims that Ryuk now represents a third of all ransomware attacks so far in 2020
- In March 2020, WIZARD SPIDER ceased deploying Ryuk and switched to using Conti ransomware, then resumed using Ryuk in mid-September
- US Federal Bureau of Investigation (FBI) has estimated that victims have paid over USD $61 million to recover files encrypted by Ryuk



- File names RyukReadMe.html or RyukReadMe.txt, contains email addresses to contact for ransom payment
- No ransomware site

The Future for TrickBot and Ryuk

- A new threat emerges: BazarLoader/BazarBackdoor aka KEGTAP replaces TrickBot
- Security researchers at Red Canary have identified a new attack pattern
  - BazarLoader > Cobalt Strike > Ryuk
- BazarLoader uses business-themed emails containing a link to a Google Docs file
- BazarLoader's backdoor component is capable of executing arbitrary payloads, batch and PowerShell scripts, exfiltrating files from a victim, and terminating running processes
- Unlikely that WIZARD SPIDER will completely abandon TrickBot

Fall 2020 Action Against TrickBot

- Undertaken to preserve US election integrity, among other benefits
- Led by Microsoft
- Used a “persistent and layered approach” to thwart TrickBot operators’ attempts to establish new C2 servers
- Ultimately only partially successful:
  - “The botnet's operators have all the IT support of legitimate enterprises — continuity planning, backups, automated deployment, and a dedicated workforce — that allow them to quickly react to disruptive measures.” – Microsoft
- “Technical takedowns are neither a sufficient nor an efficient solution.” – Intel471
- “Strategies to shutdown Trickbot for good would need to include arrests, financial asset seizures — of cryptocurrency wallets, for example — coordinated and global infrastructure takedowns, and potentially even offensive action against Trickbot infrastructure [that] isn't able to be taken down.” – Intel471

Incident: Late September Attack on a Major US Hospital Network

- Network of over 400 hospitals in the US and UK
- All 250 facilities in the US were affected in one of the largest medical cyberattacks in history
  - Did not affect UK facilities
- Attack began around 2AM Sunday, September 27, 2020. First news of compromise appeared on Reddit
  - Employees confirmed that files were being encrypted with the .Ryuk extension, indicating Ryuk
  - “Once on an infected host, [Ryuk] can pull passwords out of memory and then laterally moves through open shares, infecting documents and compromised accounts” – Ordr
  - Phones and medical IoT were also affected
  - Some facilities were forced to return to pen-and-paper documentation, although no loss of life was reported
- Company confirmed three weeks later that all systems were back online
  - Victim organization claims “no indication that any patient or employee data had been accessed, copied or misused”
  - Unclear how much the hackers demanded in ransom, nor whether the health system paid the demand

Incident: Late October Attack on US Hospitals

- CISA, FBI, and HHS released alert based on “credible information of an increased and imminent cybercrime threat to US hospitals and healthcare providers”
- Multiple confirmed hits across the US, including in:
  - California
  - Minnesota
  - Oregon
  - New York
- A doctor at an affected facility told Reuters that the “facility was functioning on paper after an attack and unable to transfer patients because the nearest alternative was an hour away.”
- Deemed “a coordinated attack designed to disrupt hospitals specifically all around the country.”
- “While multiple ransomware attacks against healthcare providers each week have been commonplace, this is the first time we have seen six hospitals targeted in the same day by the same ransomware actor.” – Recorded Future
- Based on early alert, hospitals took strong measures to minimize Ryuk exposure
- “Hundreds” of hospitals have not been targeted…yet

Danger to the HPH Sector

- High stakes: threat actors know the costs of a ransomware or malware attack to a hospital's operations
  - Research by Coveware claims "ransomware attacks spur 15 days of EHR downtime, on average"
- Example: September 2020 ransomware attack on Dusseldorf University Hospital
  - Widely considered to be first death directly attributable to ransomware
  - Hospital likely not the intended target, but incident was unable to be resolved in time to prevent loss of life
- Valuable data: medical data is easy to sell and commands a high price
  - Organizations engaged in coronavirus response may have information related to vaccine research or other intellectual property

From **CISA's Alert (AA20-302A)** on **Ransomware Activity Targeting the Healthcare and Public Health Sector**

- ***Patch operating systems, software, and firmware as soon as manufacturers release updates.***
- Check configurations for every operating system version for HPH organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Audit logs to ensure new accounts are legitimate.
- Scan for open or listening ports and mediate those that are not needed.
- Identify critical assets such as patient database servers, medical records, and teleheatlh and telework infrastructure; create backups of these systems and house the backups offline from the network.
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

- Regularly back up data, air gap, and password protect backup copies offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.
- Focus on end user awareness and training about ransomware and phishing.
- Ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently.

Additional best practices and next steps can be found at **CISA's Alert (AA20-302A)** on **Ransomware Activity Targeting the Healthcare and Public Health Sector**

Recent IOCs, including IP addresses, domains, and SHA-256, were released by RiskIQ and can be found on their website under **Ryuk Ransomware: Extensive Attack Infrastructure Revealed** (included in the references)

Reference Materials

References

- CISA's Alert (AA20-302A) on Ransomware Activity Targeting the Healthcare and Public Health Sector
  - https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- JOINT CYBERSECURITY ADVISORY, Ransomware Activity Targeting the Healthcare and Public Health Sector AA20-302A
  - https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
- RiskIQ, Ryuk Ransomware: Extensive Attack Infrastructure Revealed
  - https://community.riskiq.com/article/0bcefe76
- Microsoft, New action to combat ransomware ahead of U.S. elections
  - https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/
- Intel471, Global Trickbot disruption operation shows promise
  - https://public.intel471.com/blog/global-trickbot-disruption-operation-shows-promise/
- DarkReading, Trickbot Tenacity Shows Infrastructure Resistant to Takedowns
  - https://www.darkreading.com/threat-intelligence/trickbot-tenacity-shows-infrastructure-resistant-to-takedowns/d/d-id/1339217
- The CyberWire, "TrickBot's return is interrupted. Election rumor control. Supply chain security. Securing the Olympics. NSS Labs closes down."
  - https://thecyberwire.com/podcasts/daily-podcast/1198/transcript
- SANS, Spooky Ryuky: The Return of UNC1878
  - https://www.youtube.com/watch?v=BhjQ6zsCVSc

References

- Krebs On Security, FBI, DHS, HHS Warn of Imminent, Credible Ransomware Threat Against U.S. Hospitals
  - https://krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/
- ZDNet, This new Trickbot malware update makes it even harder to detect
  - https://www.zdnet.com/article/this-new-trickbot-malware-update-makes-it-even-harder-to-detect/
- Press Democrat, Sonoma Valley Hospital Hit by Cybercriminals with Ransomware
  - https://www.pressdemocrat.com/article/news/sonoma-valley-hospital-hit-by-cybercriminals-with-ransomware-attack/?sba=AAS
- SW News Media, 'Unusual network activity' at Ridgeview Medical Center
  - https://www.swnewsmedia.com/chanhassen_villager/news/local/unusual-network-activity-at-ridgeview-medical-center/article_5fc12f6e-c320-59d4-9ad4-24f5cb985a36.html
- Red Canary, A Bazar start: How one hospital thwarted a Ryuk ransomware outbreak
  - https://redcanary.com/blog/how-one-hospital-thwarted-a-Ryuk-ransomware-outbreak/
- Information Security Magazine, Red Alert as US Hospitals Are Flooded with Ryuk Ransomware
  - https://www.infosecurity-magazine.com/news/red-alert-us-hospitals-flooded
- Reuters, Building wave of ransomware attacks strike U.S. hospitals
  - https://www.reuters.com/article/uk-usa-healthcare-cyber/fbi-probes-string-of-recent-ransomware-attacks-on-u-s-hospitals-idUKKBN27D36P
- Security Week, German Hospital Hacked, Patient Taken to Another City Dies
  - https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies

References

- Security Week, German Hospital Hacked, Patient Taken to Another City Dies
  - https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
- CrowdStrike, WIZARD SPIDER Adversary Update
  - https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
- Healthcare IT News, UHS says all U.S. facilities affected by apparent ransomware attack
  - https://www.healthcareitnews.com/news/uhs-says-all-us-facilities-affected-apparent-ransomware-attack
- Health IT Security, UPDATE: UHS Health System Confirms All US Sites Affected by Ransomware Attack
  - https://healthitsecurity.com/news/uhs-health-system-confirms-all-us-sites-affected-by-ransomware-attack

Questions

Upcoming Briefs

- Chinese State-Sponsored Cyber Activity (11/19)
- Disinformation and the Healthcare Sector (12/3)

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.

HC3 Customer Feedback

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.**

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.

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

Products

Sector & Victim Notifications

Directed 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.
Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV