LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY


# The Evolution of Ryuk

**04/08/2021**

TLP: WHITE, ID# ***202104081030***

# Agenda

- What is Ryuk?
- A New Ryuk Variant Emerges in 2021
- Progression of a Ryuk Infection
- Infection Chains
- Incident: Late September Attack on a Major US Hospital Network
- Incident: Late October Attack on US Hospitals
- UNC1878 – WIZARD SPIDER
- Danger to the HPH Sector
- Mitigations and Best Practices
- References

**Slides Key:**

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

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

# What is Ryuk?

- A form of ransomware and a common payload for banking Trojans (like TrickBot)
- First observed in 2017
- 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
- SonicWall researchers claimed that Ryuk represented a third of all ransomware attacks in 2020
- In March 2020, threat actor group WIZARD SPIDER ceased deploying Ryuk and switched to using Conti ransomware, then resumed using Ryuk in mid-September
- As of November 2020, the US Federal Bureau of Investigation (FBI) estimated that victims paid over USD $61 million to recover files encrypted by Ryuk

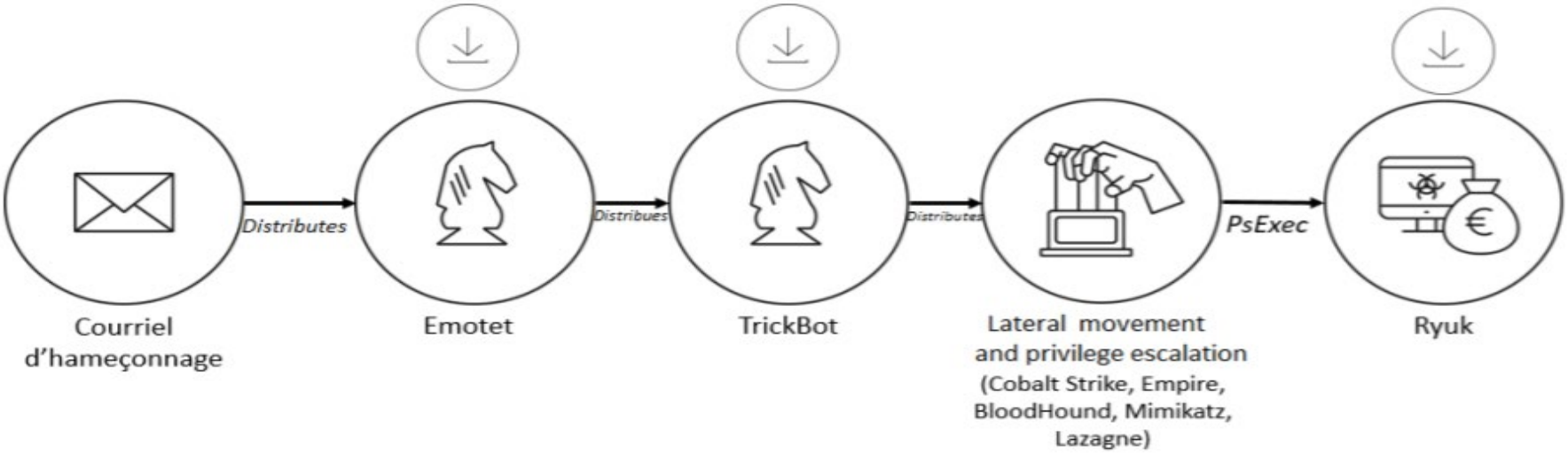
# A New Ryuk Variant Emerges in 2021

- Previous versions of Ryuk could not automatically move laterally through a network
  - Required a dropper and then manual movement
- A new version with “worm-like” capabilities was identified in January 2021
  - A computer worm can spread copies of itself from device to device without human interaction or the need to attach itself to a specific software program
  - The new Ryuk variant can spread automatically/without intervention through infected networks
  - Currently, ability is limited to Windows machines

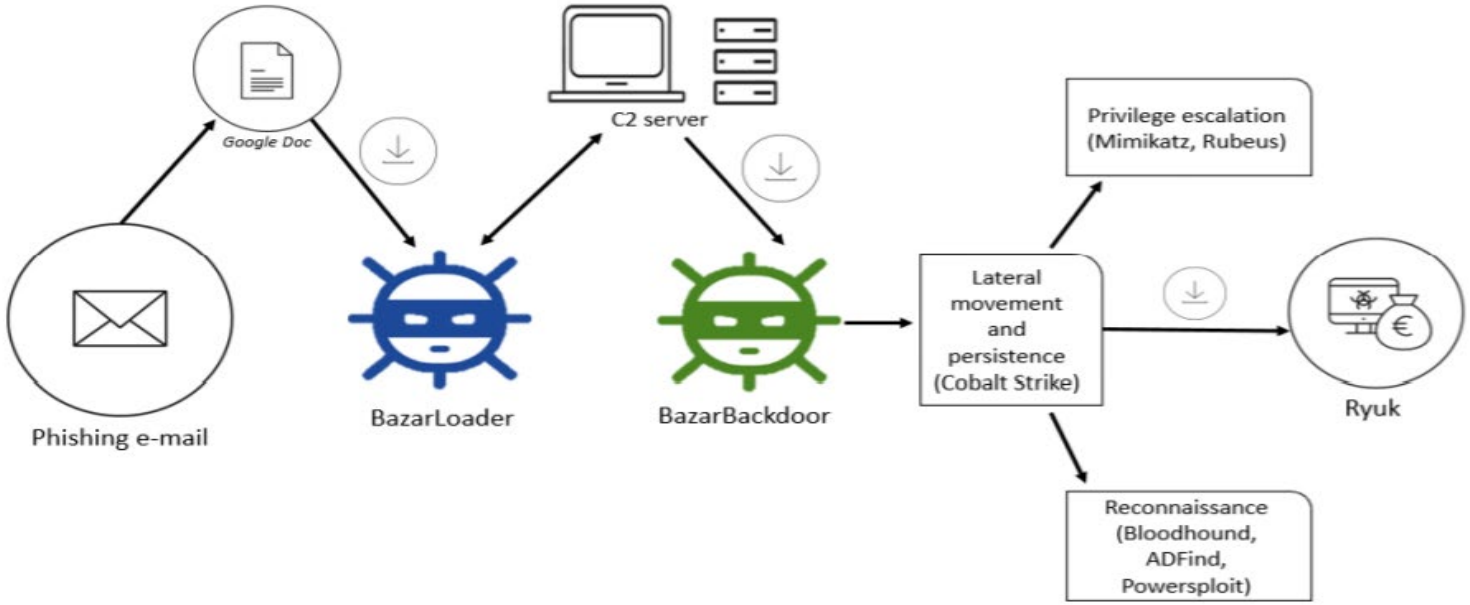
# Progression of a Ryuk Infection

- The French National Agency for the Security of Information Systems (ANSSI) identified the initial infection point as a privileged domain account
- As the new variant moves through the network, it scans for network shares and copies a unique version of the ransomware executable to each of them as they are found
  - Uses Wake-on-LAN feature to automatically remotely turn on other machines on the same network
- Uses the filename lan.exe or rep.exe
- Encrypts files with the AES256 algorithm of Microsoft's CryptoAPI, and a unique AES key wrapped with an RSA public key stored in the binary code for each file
- Files will be encrypted and appended with .RYK
- Files RyukReadMe.txt and RyukReadMe.html will appear in affected directories
  - These ransom notes direct victims to contact the ransomware operators at two specific email addresses and provide a Bitcoin wallet for ransom payment
- No ransomware site
  - Victims are identified from press releases, press coverage, and cryptocurrency transactions with known Ryuk-affiliated wallets

- Classic: TrickBot Chains
  - TrickBot → Ryuk
  - Emotet → TrickBot → Ryuk
  - TrickBot activities disappeared in March 2020 and reemerged in July 2020
  - Disrupted by US government-led Fall 2020 action against TrickBot infrastructure
    - Action did not completely destroy TrickBot, and botnet is still active



- Emerging: BazarLoader Chains
  - BazarLoader → BazarBackdoor → Ryuk
  - Began in September 2020
  - More expensive than TrickBot, but less detectable, according to security researchers at Advanced Intel
  - Uses process hollowing to hide within legitimate Windows processes and run every time the computer is turned on



# 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 CSO
  - Phones and medical IoT (radiology machines) 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 alerts, hospitals took strong measures to minimize Ryuk exposure
- **Even with these measures, Ryuk was reportedly responsible for 75% of attacks on the American healthcare sector in October 2020**

# UNC1878 - WIZARDSPIDER

- Documented involvement in TrickBot → Ryuk infection chains starting in January 2020 and BazarLoader → Ryuk infection chains starting in September 2020
- Alleged to be affiliated with Russian cybercrime ring; some members were part of the group that operated the banking Trojan malware Dyre, which ceased operating in 2015 following a crackdown from Russian authorities
- Infects targets extremely quickly
    - Time between initial infection and encryption recently reduced from a few (two to five) days to three hours
- May not be behind all Ryuk infections
- Believed to be behind October 2020 attacks on US HPH sector
    - Researchers generally characterize UNC1878's tactics, techniques, and procedures (TTPs) as opportunistic and indiscriminate
- According to FireEye, a fifth of all ransomware-related intrusions in 2020 are due to Ryuk. 83% of them are the work of UNC1878, of which 27% were successful

- 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"
- 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
- Groups using Ryuk, including UNC1878, have previously targeted US HPH organizations

**Due to the tenacity of the new Ryuk variant, prevention is a more effective tool than mitigation or remediation once Ryuk takes hold in a system**

- The new variant also lacks any exclusion mechanisms, such as a Mutual Exclusion Objection (MUTEX), to prevent multiple Ryuk processes from running on a single machine
    - Reinfection of the same device is possible once the initial infection is cleared

Because Ryuk infections most commonly begin with the deployment of a form of "dropper" malware as a foothold in the victim's machine, we include these mitigations 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 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 and air gaps, 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**

# Reference Materials

# Key References


- “Alert (AA20-302A),” Cybersecurity and Infrastructure Security Agency. October 28, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- “Ransomware: What It Is & What To Do About It,” The National Cyber Investigative Joint Task Force (NCIJTF). February 4, 2021. https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf
- “The Ryuk Ransomware,” French National Agency for the Security of Information Systems. March 1, 2021. https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-006/

# References


- “A Bazar start: How one hospital thwarted a Ryuk ransomware outbreak,” Red Canary, October 29, 2020. https://redcanary.com/blog/how-one-hospital-thwarted-a-Ryuk-ransomware-outbreak/
- Abrams, Lawrence. “BazarLoader used to deploy Ryuk ransomware on high-value targets,” BleepingComputer, October 12, 2020. https://www.bleepingcomputer.com/news/security/bazarloader-used-to-deploy-ryuk-ransomware-on-high-value-targets/
- “Alert (AA20-302A),” Cybersecurity and Infrastructure Security Agency. October 28, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- Associated Press. “German Hospital Hacked, Patient Taken to Another City Dies,” Security Week, September 17, 2020. https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
- Artnz, Peter. “Ryuk ransomware develops worm-like capability,” MalwareBytes. March 2, 2021. https://blog.malwarebytes.com/malwarebytes-news/2021/03/ryuk-ransomware-develops-worm-like-capability/
- “A Tsunami of Ryuk Ransomware Attacks Hits U.S. Hospitals,” CISOMAG. October 29, 2020. https://cisomag.eccouncil.org/ryuk-ransomware-targeting-us-hospitals/
- Bing, Christopher and Joseph Menn. “Building wave of ransomware attacks strike U.S. hospitals,” Reuters, October 28, 2020. https://www.reuters.com/article/uk-usa-healthcare-cyber/fbi-probes-string-of-recent-ransomware-attacks-on-u-s-hospitals-idUKKBN27D36P
- Davis, Jessica. “Update to Ryuk Ransomware Variant Adds Network Worming Capability,” HealthITSecurity. March 2, 2021. https://healthitsecurity.com/news/update-to-ryuk-ransomware-variant-adds-network-worming-capability

# References II


- Davis, Jessica. “UPDATE: UHS Health System Confirms All US Sites Affected by Ransomware Attack,” Health IT Security, October 3, 2020. https://healthitsecurity.com/news/uhs-health-system-confirms-all-us-sites-affected-by-ransomware-attack
- Felegy, Amy. “'Unusual network activity' at Ridgeview Medical Center,” SW News Media, October 27, 2020. https://www.swnewsmedia.com/chanhassen_villager/news/local/unusual-network-activity-at-ridgeview-medical-center/article_5fc12f6e-c320-59d4-9ad4-24f5cb985a36.html
- Jercich, Katie. “UHS says all U.S. facilities affected by apparent ransomware attack,” Healthcare IT News, October 2, 2020. https://www.healthcareitnews.com/news/uhs-says-all-us-facilities-affected-apparent-ransomware-attack
- Krebs, Brian. “FBI, DHS, HHS Warn of Imminent, Credible Ransomware Threat Against U.S. Hospitals,” Krebs On Security, October 28, 2020. https://krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/
- Lemos, Robert. “Trickbot Tenacity Shows Infrastructure Resistant to Takedowns,” DarkReading, October 20, 2020. https://www.darkreading.com/threat-intelligence/trickbot-tenacity-shows-infrastructure-resistant-to-takedowns/d/d-id/1339217
- Muncaster, Phil. “Red Alert as US Hospitals Are Flooded with Ryuk Ransomware,” Information Security Magazine, October 29, 2020. https://www.infosecurity-magazine.com/news/red-alert-us-hospitals-flooded
- Palmer, Danny. “This new Trickbot malware update makes it even harder to detect,” ZDNet, May 29, 2020. https://www.zdnet.com/article/this-new-trickbot-malware-update-makes-it-even-harder-to-detect/
- Seals, Tara. “Ryuk Ransomware: Now with Worming Self-Propagation,” ThreatPost. March 2, 2021. https://threatpost.com/ryuk-ransomware-worming-self-propagation/164412/

# References III


- Swindell, Bill. “Sonoma Valley Hospital Hit by Cybercriminals with Ransomware,” Press Democrat, October 30, 2020. https://www.pressdemocrat.com/article/news/sonoma-valley-hospital-hit-by-cybercriminals-with-ransomware-attack/?sba=AAS
- Ta, Van and Aaron Stephens. “Spooky Ryuky: The Return of UNC1878,” SANS, October 28, 2020. https://www.youtube.com/watch?v=BhjQ6zsCVSc
- Umawing, Joel. “Threat spotlight: the curious case of Ryuk ransomware,” MalwareBytes. December 12, 2019. https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/
- “What is a computer worm, and how does it work?,” Norton LifeLock. August 28, 2019. https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html
- “WIZARD SPIDER Update: Resilient, Reactive and Resolute,” CrowdStrike, October 16, 2020. https://www.crowdstrike.com/blog/wizard-spider-adversary-update/

# Questions

## Upcoming Briefs

- April 22nd: Cyber-SCRM

### *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.**

### *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

### *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

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 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