LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Ryuk Update

01/30/2020

Report #: 202001301000

Agenda

- Overview
- Functionality
- Shifting Attribution
- Blacklisting capabilities – Further attribution?
- Threat Actors
- Historic Activity
- Emotet => TrickBot => Ryuk delivery
- Ransom Demands
- Prominent Ryuk Activity and Alerts in the Last Year
- Ryuk Defense and Mitigations
- Indicators of Compromise (IOCs)
- References
- Questions

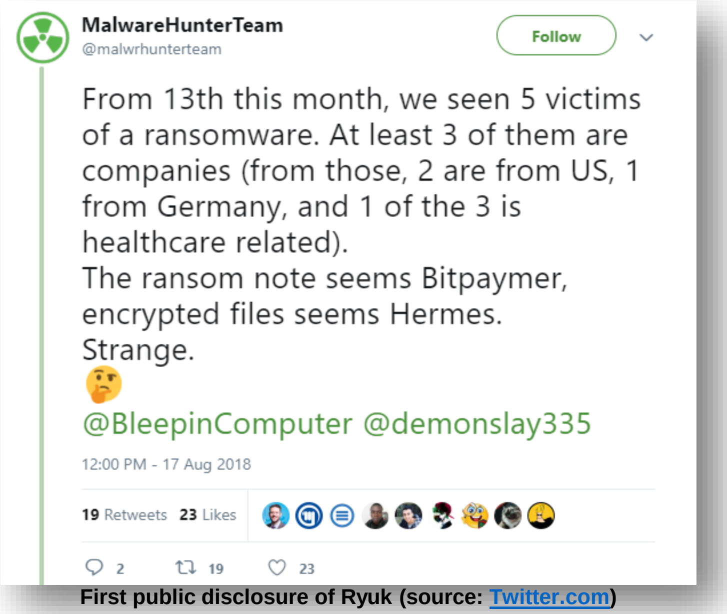
Image courtesy of Bleeping Computer

Slides Key:

👤	Non-Technical: managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

- Ryuk
  - Ransomware
    - First identified in 2018
    - Initially thought to be Hermes
- Modified version of Hermes 2.1
  - Similar code
  - Similar functionality
- Likely utilized by Russian criminal groups
  - Originally attributed to North Korea
- Often deployed with other weapons
  - TrickBot
  - Emotet
- Used against big targets (big game hunting)
  - Known for high ransom remands
  - Encryption scheme built for small-scale operations
- Why the name "Ryuk"?
  - Fictional character in Japanese comic book series, Death Note



MalwareHunterTeam
@malwrhunterteam

From 13th this month, we seen 5 victims of a ransomware. At least 3 of them are companies (from those, 2 are from US, 1 from Germany, and 1 of the 3 is healthcare related).
The ransom note seems Bitpaymer, encrypted files seems Hermes.
Strange.
🤔
@BleepinComputer @demonslay335

12:00 PM - 17 Aug 2018

19 Retweets 23 Likes

2 19 23

First public disclosure of Ryuk (source: Twitter.com)

Photo credit:
http://www.rayphillips.co.uk

Functionality

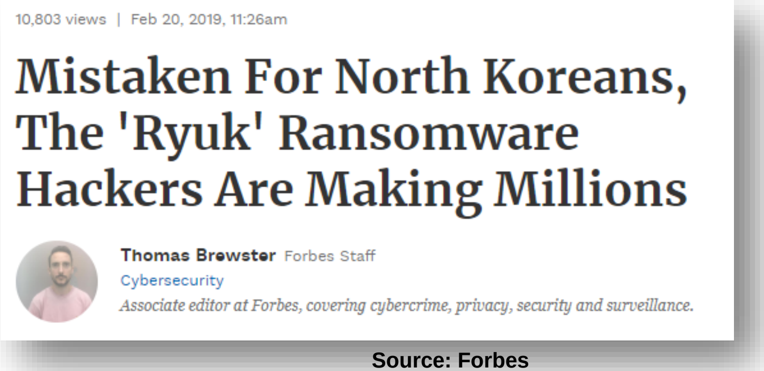
- Establishes persistence by modifying registry
- Injects itself into running processes
- Encrypts files using RSA-2048 and AES-256
- Can download additional exploitation tools
- Can steal credentials
- In one case, the ransomware appears to have used unsecured or brute forced Remote Desktop Protocols (RDPs) to gain access.
- Stores keys in the executable using the proprietary Microsoft SIMPLEBLOB format
- Capable of targeting beyond immediate system devices: Encrypts network-connected devices, mounted devices and remote hosts
- Conceals its tracks - deletes many files related to the intrusion, makes it challenging to identify infection vector
- Most recently, Wake-on-LAN allows for the targeting of systems that are in standby/sleep mode and it would otherwise have no ability to reach and ARP pinging allows for the identification of more systems on a network

Image source: Bankinfosecurity.com

Image source: Reactionary Times

Shifting Attribution

- Original attribution: North Korea
  - Hermes-related code
    - Similar call flows
    - Marker code is identical
    - Lazarus Group and APT 38 has history of use
      - Targets: International banking/SWIFT
- Updated attribution linked to Russian cyber criminal groups
  - CrowdStrike: medium-high confidence Ryuk is used by Russian threat actors
  - FireEye: “most likely hypothesis” Ryuk operators are Russian cybercriminals
    - Why?
      - Hermes has been seen for sale on the dark web
      - Uploaded files related to Ryuk to file-scanning website from Russian IP
      - Does not work on systems with Russian, Ukrainian or Belarusian language enabled
- Use by various APTs and criminal group threat actors
  - CrowdStrike: Grim Spider
  - FireEye: TEMP.Mixmaster



10,803 views | Feb 20, 2019, 11:26am

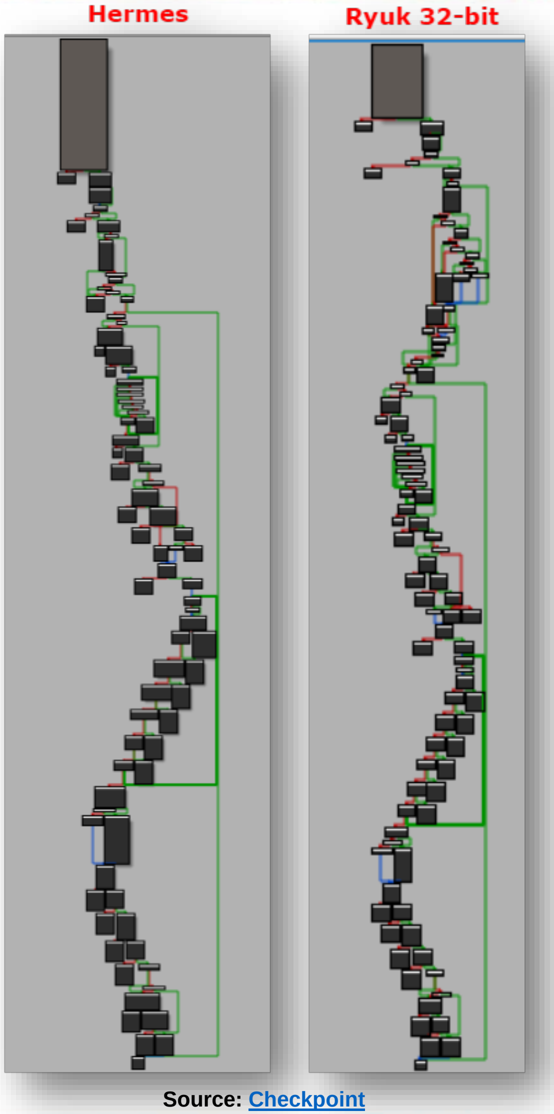
Mistaken For North Koreans, The 'Ryuk' Ransomware Hackers Are Making Millions

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Source: Forbes

Shifting Attribution

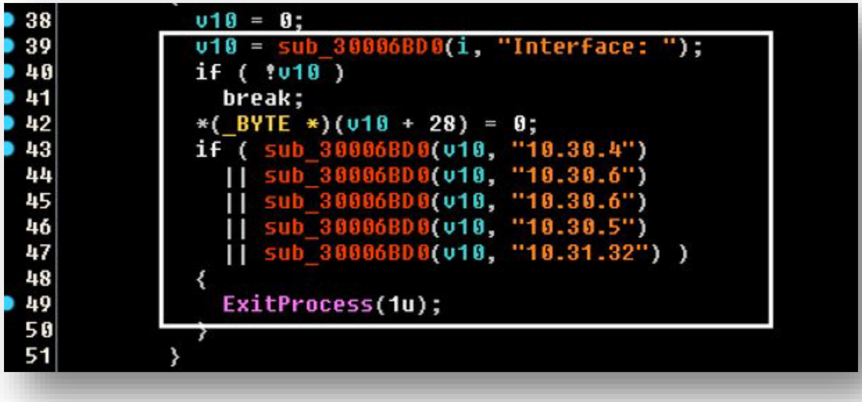
- A comparison of call flow diagram of the encryption functions of Ryuk and Hermes
  - Both instances of malware have similar code structure
  - Both instances of malware have similar flow



Source: Checkpoint

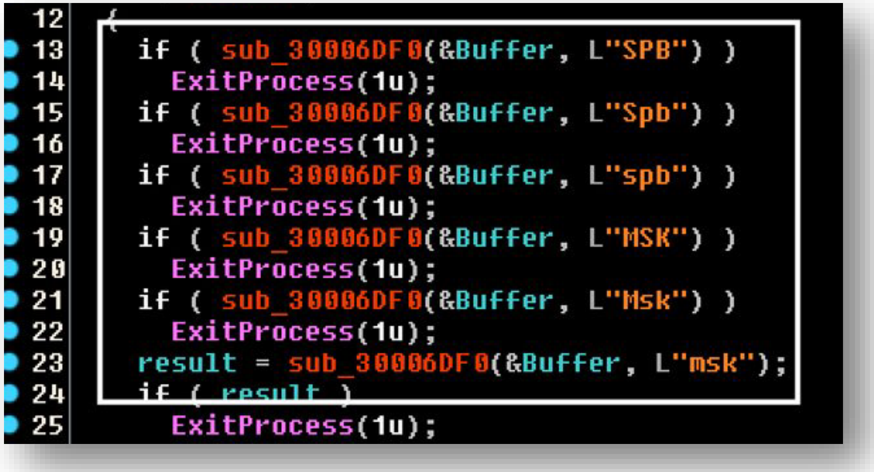
Blacklisting Capabilities – Further Attribution?

- June 2019, a new Ryuk variant was discovered which makes checks before encryption:
    - Ryuk will not encrypt systems on the subnets 10.30.4, 10.30.5, 10.30.6, or 10.31.32



```
      v10 = 0;
      v10 = sub_30006BD0(i, "Interface: ");
      if ( !v10 )
        break;
      *(_BYTE *)(v10 + 28) = 0;
      if ( sub_30006BD0(v10, "10.30.4")
        || sub_30006BD0(v10, "10.30.6")
        || sub_30006BD0(v10, "10.30.6")
        || sub_30006BD0(v10, "10.30.5")
        || sub_30006BD0(v10, "10.31.32") )
      {
        ExitProcess(1u);
      }
    }
```

- Ryuk will not encrypt systems that contain certain strings ("SPB", "Spb", "spb", "MSK", "Msk", and "msk“)
    - These blacklisting capabilities were likely added to avoid encrypting systems in Russia.

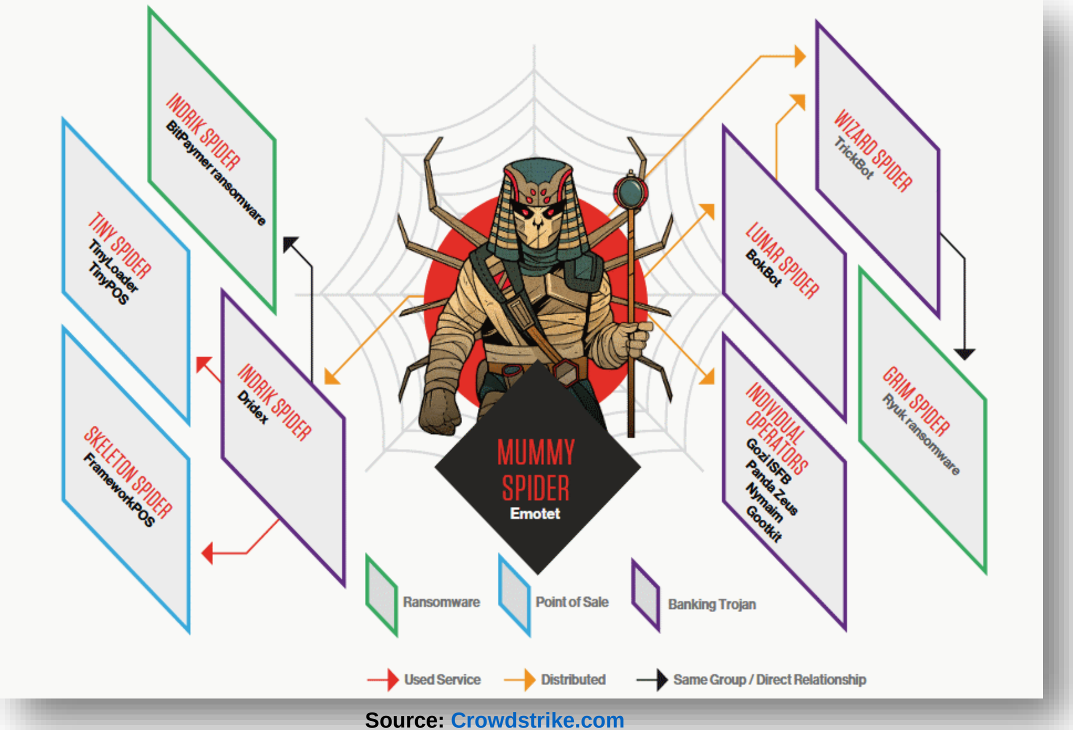


```
{
  if ( sub_30006DF0(&Buffer, L"SPB") )
    ExitProcess(1u);
  if ( sub_30006DF0(&Buffer, L"Spb") )
    ExitProcess(1u);
  if ( sub_30006DF0(&Buffer, L"spb") )
    ExitProcess(1u);
  if ( sub_30006DF0(&Buffer, L"MSK") )
    ExitProcess(1u);
  if ( sub_30006DF0(&Buffer, L"Msk") )
    ExitProcess(1u);
  result = sub_30006DF0(&Buffer, L"msk");
  if ( result )
    ExitProcess(1u);
```

Images courtesy of Bleeping Computer

Threat Actors

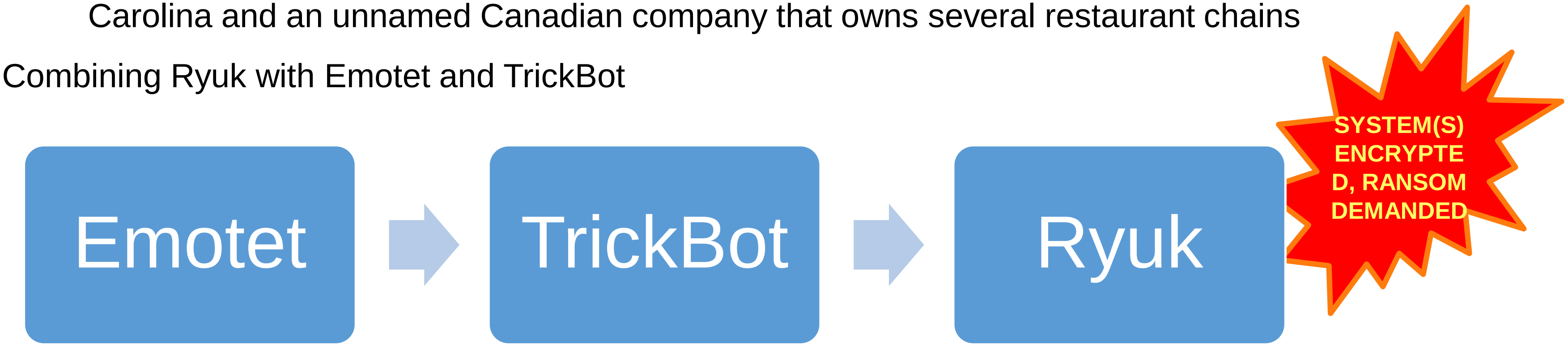
- FireEye: TEMP.MixMaster
  - “…financially-motivated activity that involves the interactive deployment of Ryuk ransomware following TrickBot malware infections”
  - Not concluded to be a single threat group
  - “…proven to be highly successful at soliciting large ransom payments from victim organizations”
- CrowdStrike: GRIM SPIDER
  - cell of WIZARD SPIDER
    - Developer of TrickBot
    - Wizard Spider cell of Mummy Spider (Emotet)



Source: Crowdstrike.com

Threat Actors

- Initial activity
  - August 2018 to Jan 2019: $4.7M USD in BTC acquired
  - Used in cyberattacks targeting various newspapers in December (slight delays in delivery but no significant operational impact):
    - San Diego Union-Tribune
    - Los Angeles Times and Tribune Publishing
      - Includes Chicago Tribune, New York Daily News, Baltimore Sun and Orlando Sentinel
  - Used to attack cloud hosting provider Data Resolution, Onslow Water and Sewer Authority in North Carolina and an unnamed Canadian company that owns several restaurant chains
- Combining Ryuk with Emotet and TrickBot



Emotet

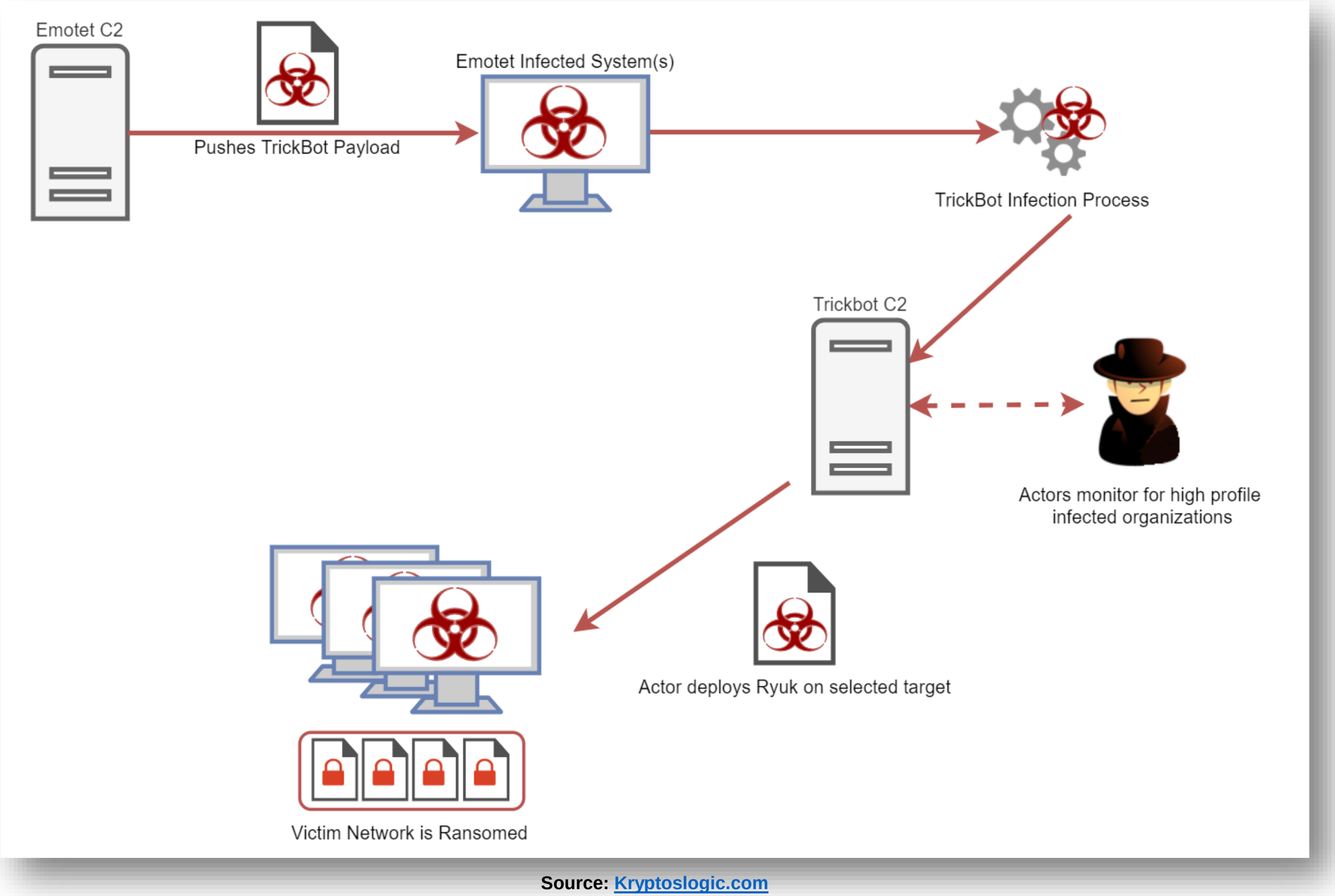
TrickBot

Ryuk

SYSTEM(S) ENCRYPTED, RANSOM DEMANDED

  - “Along with Emotet, TrickBot has become one of the most versatile and dangerous pieces of modular malware hitting enterprise environments.” – HelpNet Security
  - “Interactive deployment of ransomware” to conduct reconnaissance and ultimately “maximize their disruption of business operations” - FireEye

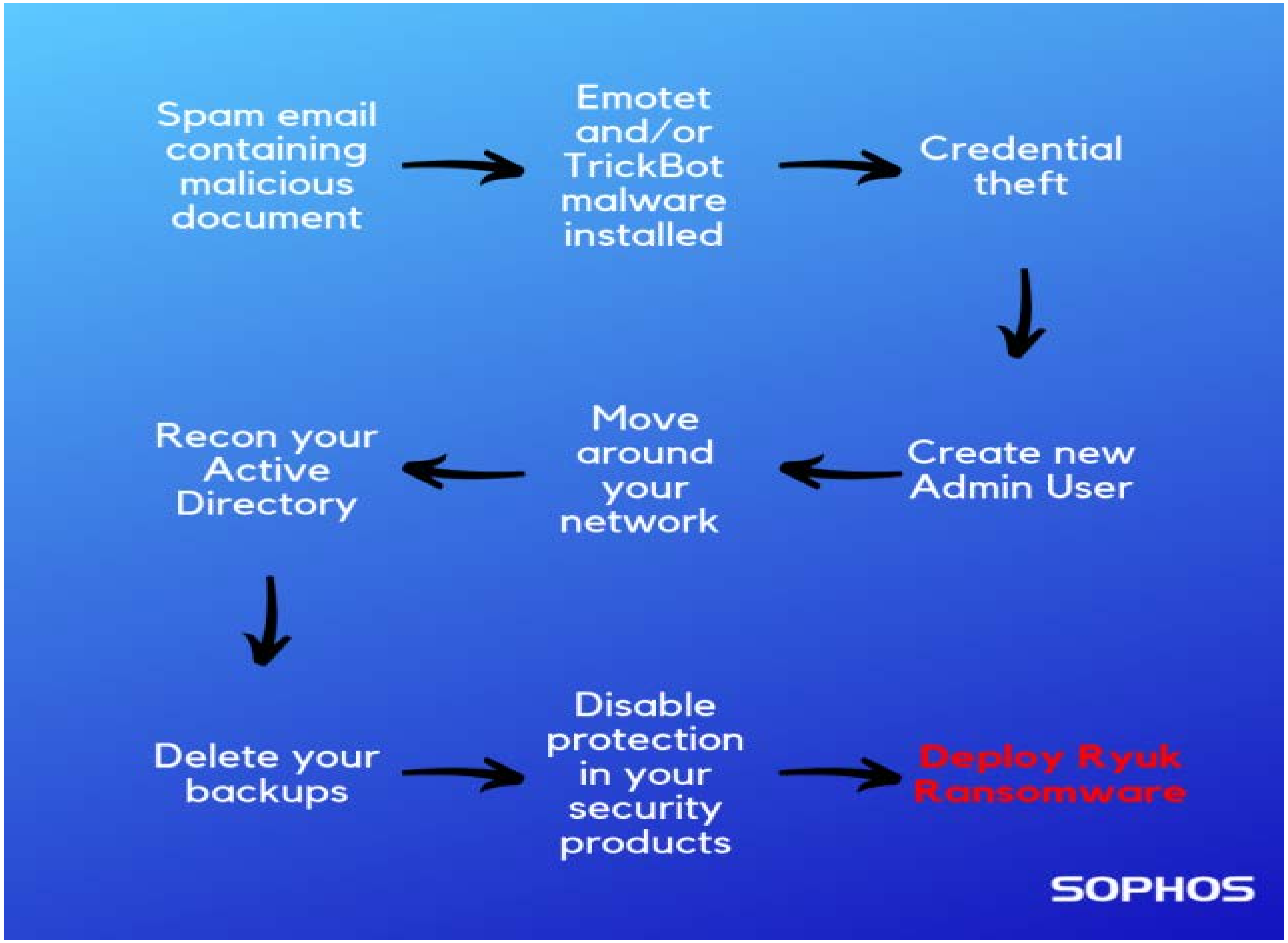
Emotet ➡ TrickBot ➡ Ryuk Delivery


Emotet C2
Pushes TrickBot Payload
Emotet Infected System(s)
TrickBot Infection Process
Trickbot C2
Actors monitor for high profile infected organizations
Actor deploys Ryuk on selected target
Victim Network is Ransomed

Source: Kryptoslogic.com

Emotet ⇨ TrickBot ⇨ Ryuk Delivery

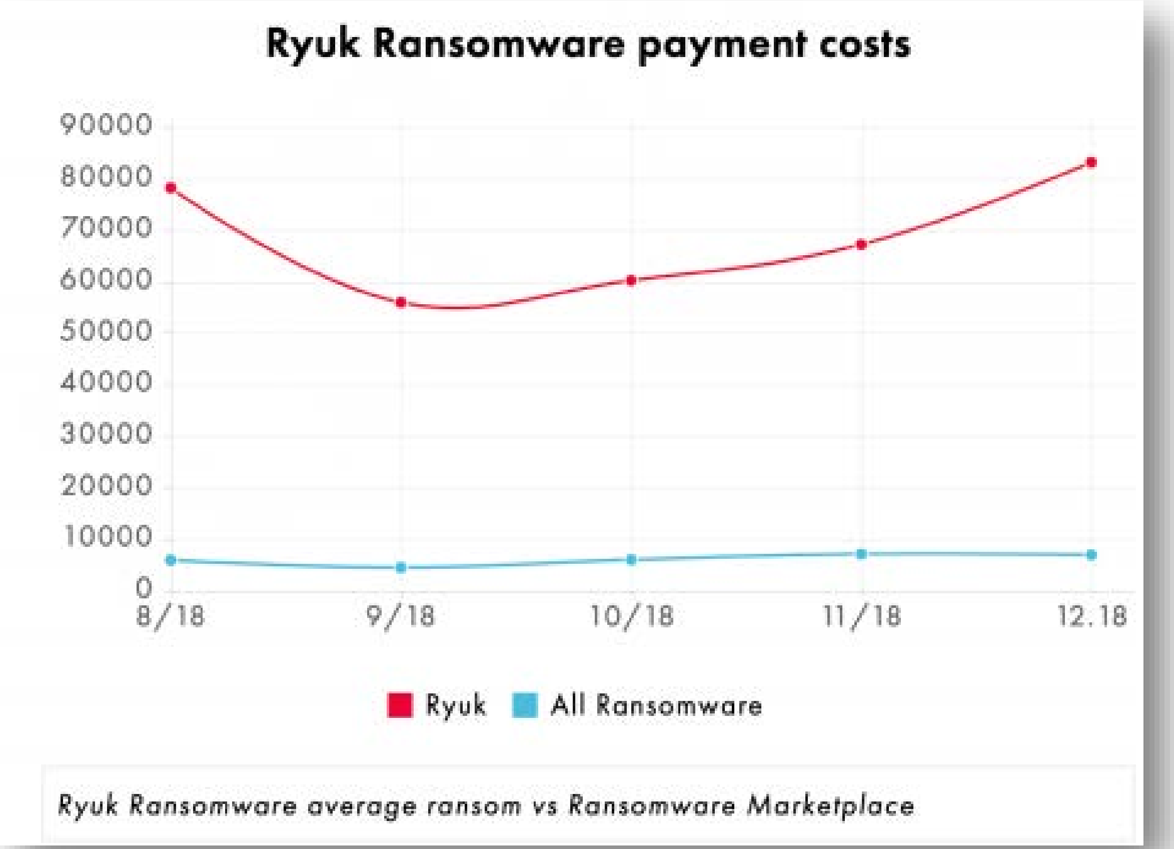
Another example of the workflow of Emotet, TrickBot and Ryuk when used together



Spam email containing malicious document → Emotet and/or TrickBot malware installed → Credential theft → Create new Admin User → Move around your network → Recon your Active Directory → Delete your backups → Disable protection in your security products → Deploy Ryuk Ransomware

Ransom Demands

- Ryuk is known to be one of the most costly ransomware families
  - According to Coveware, Ryuk payments are often 10 times more than its peers



Prominent Ryuk Activity and Alerts in the Last Year

- March 2019:
  - IT systems for Jackson County, Georgia attacked. They paid $400,000 (most IT systems except website and 911 knocked down)
- May 2019:
  - Disrupted operations of C.E. Niehoff & Co., a manufacturing firm
- April 2019:
  - Stuart, Florida, attacked with Ryuk
  - Imperial County, California, refused to pay $1.2M Ryuk ransom demand but suffered downtime
- June 2019:
  - Key Biscayne, Florida, attacked with Ryuk
  - Lake City, Florida, paid ~$460K in Ryuk attack ransom
  - British GCHQ releases warning about global Ryuk campaign
  - Georgia’s Administrative Office of the Courts attacked
- July 2019:
  - La Porte County, Indiana, attacked, paid $130,000 ransom
  - Chinese company Tencent releases report on Ryuk attacking targets in China
  - Coveware report notes dramatically increasing ransomware ransom demands, identifies Ryuk as one of the reasons
  - New Bedford, Massachusetts, attacked. Refused to pay ransom and rebuilt.
  - Several Louisiana school districts attacked with Ryuk

Prominent Ryuk Activity and Alerts in the Last Year

- August 2019:
  - Rockville Centre school district (Long Island, New York) paid nearly $100,000 ransom for a Ryuk attack
- September 2019:
  - Ryuk-related malware observed exfiltrating sensitive military and financial files
- October 2019:
  - DCH Health System in Alabama were attacked, shut down and temporarily stopped admitting new, non-emergency patients
- November 2019:
  - Ransomware attack on Louisiana Office of Technology Services, likely Ryuk based on publically-released
  - Multinational Spanish security company, Prosegur temporarily shut down IT network after Ryuk attack
  - Ryuk attack on Cadena SER (Spain’s largest radio station)
  - Ryuk attack on T-System, a provider of end-to-end IT solutions for emergency and urgent healthcare providers, allegedly the infection spread to public segments such as their demilitarized zone, extranet, and even their helpdesk
- December 2019:
  - Ryuk used to attack IT network of a federally regulated maritime facility
- January 2020:
  - Ryuk used to attack several oil and gas facilities
  - Coveware again reports dramatically increasing ransomware demands, identifies Ryuk as one of the reasons

Prominent Ryuk Activity and Alerts in the Last Year

- January 2020:
  - Ryuk used to attack several oil and gas facilities
  - Coveware again reports dramatically increasing ransomware demands, identifies Ryuk as one of the reasons

Ryuk Defense and Mitigations

- 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 applicable patches and updates immediately after testing; Develop and maintain patching program if necessary. **[7.S.A], [7.M.D]**
- Implement Intrusion Detection System (IDS). **[6.S.C], [6.M.C], [6.L.C]**
- Implement spam filters at the email gateways. **[1.S.A], [1.M.A]**
- Block suspicious IP addresses at the firewall. **[6.S.A], [6.M.A], [6.L.E]**
- Implement whitelisting technology on appropriate assets 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 Remote Desktop Protocol (RDP) or, if absolutely needed, restrict its use applying the principle of least privilege and monitor/log its usage. **[7.S.A], [7.M.D]**

We suggest contacting local law enforcement in the case of a cyberattack. Also, the FBI's Internet Crime Complaint Center (IC3) can be reached here:

https://www.ic3.gov/complaint/default.aspx/

Prominent Ryuk Activity and Alerts in the Last Year

- Please note several things about the indicators of compromise (IOCs) on the following slides:
  - There is a significant quantity of indicators of compromise related to Ryuk available on the public Internet. We have attempted to include as many as possible in this presentation. However, **there may be some available to the public not included here**.
  - Upon being released to the public, IOCs may become “burned” which is to say that 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**.

Indicators of Compromise

Command and control:

47.49.168.50	42.115.91.177	199.227.126.250	68.4.173.10	
190.145.74.84	137.74.151.18	24.113.161.184	72.189.124.41	
185.251.38.208	71.94.101.25	197.232.50.85	74.134.5.113	
188.68.208.240	206.130.141.255	94.232.20.113	105.27.171.234	
24.247.181.155	92.38.163.39	190.145.74.84	182.253.20.66	
174.105.235.178	74.140.160.33	47.49.168.50	172.222.97.179	
185.80.148.162	65.31.241.133	64.128.175.37		
181.113.17.230	140.190.54.187	24.227.222.4		
174.105.233.82	24.247.181.226	213.183.63.245		
71.14.129.8	46.149.182.112	103.110.91.118		
216.183.62.43	213.32.122.246	24.119.69.70		

Indicators of Compromise (Continued)

Hashes:	
1354ac0d5be0c8d03f4e3aba78d2223e	
29340643ca2e6677c19e1d3bf351d654	
5ac0f050f93f86e69026faea1fbb4450	
86c314bc2dc37ba84f7364acd5108c2b	
958c594909933d4c82e93c22850194aa	
c0202cf6aeab8437c638533d14563d35	
cb0c1248d3899358a375888bb4e8f3fe	
d348f536e214a47655af387408b4fca5	

Reference Materials

References

- Ryuk Ransomware, Exploring the Technical and Human Connections
  - https://www.coveware.com/blog/2019/2/19/ryuk-ransomware-exploring-the-technical-and-human-connections
- 2017 Cylance Threat Report
  - https://pages.cylance.com/2018-03CylanceThreatReport2017.html
- 2018 Global Threat Report: Blurring the Lines Between Statecraft and Tradecraft, Crowdstrike
  - https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf
- TEMP.MixMaster group infects with Trickbot and delayed Ryuk ransomware combo
  - https://www.scmagazine.com/home/security-news/financially-motivated-threat-actorsreferred-to-as-temp-mixmaster-are-infecting-victims-with-trickbot-malware-before-deploying-the-infamous-ryuk-ransomware/
- Ryuk ransomware linked to Emotet and TrickBot trojans; suspicions shift to cybercriminal group
  - https://www.scmagazine.com/home/security-news/ryuk-ransomware-linked-to-emotet-and-trickbot-trojans-suspicions-shift-to-cybercriminal-group/
- Ryuk ransomware earns hackers $3.7M in Bitcoin over 5 months - 52 known ransom transactions were recorded, the highest worth 99 BTC
  - https://thenextweb.com/hardfork/2019/01/14/ryuk-bitcoin-ransomware/
- Ryuk Ransomware Crew Makes $640,000 in Recent Activity Surge
  - https://www.bleepingcomputer.com/news/security/ryuk-ransomware-crew-makes-640-000-in-recent-activity-surge/

References

- Ryuk ransomware gang probably Russian, not North Korean
  - https://www.zdnet.com/article/ryuk-ransomware-gang-probably-russian-not-north-korean/
- Cloud Hosting Provider Dataresolution.net Hit by Ryuk Ransomware
  - https://www.securitysw.com/blog/cloud-hosting-provider-dataresolution-net-hit-by-ryuk-ransomware
- CrowdStrike 2018 Global Threat Report: Blurring the Lines Between Statecraft and Tradecraft
  - https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf
- Trojan.TrickBot
  - https://blog.malwarebytes.com/detections/trojan-trickbot/
- TrickBot Banking Trojan Takes Center Stage in 2018
  - https://blog.barkly.com/trickbot-trojan-2018-campaigns
- HHS HCCIC cybersecurity alert: New Ryuk ransomware quickly racking up damage
  - https://www.healthcareitnews.com/news/hhs-hccic-cybersecurity-alert-new-ryuk-ransomware-quickly-racking-damage
- Notorious Ryuk Ransomware Adds Trojans to Cyberattack Method
  - https://healthitsecurity.com/news/notorious-ryuk-ransomware-adds-trojans-to-cyberattack-method
- Emotet re-emerges after the holidays
  - https://blog.talosintelligence.com/2019/01/return-of-emotet.html
- The Unholy Alliance of Emotet, TrickBot and the Ryuk Ransomware
  - https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

References

- Cybercrime and Other Threats Faced by the Healthcare Industry
  - https://www.trendmicro.com/content/dam/trendmicro/global/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf
- Ryuk ransomware targets big businesses: New ransomware group waits and gathers intel before attacking large enterprises
  - https://www.techradar.com/news/ryuk-ransomware-targets-big-businesses
- Computer virus hits newspapers coast-to-coast
  - https://www.nbcnews.com/news/us-news/computer-virus-hits-southern-california-newspapers-n953001
- Ryuk Ransomware: A Targeted Campaign Break-Down, CheckPoint Research
  - https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/
- Ryuk ransomware targets big businesses
  - https://www.techradar.com/news/ryuk-ransomware-targets-big-businesses
- United States Department of Homeland Security Cybersecurity and Infrastructure Security Agency Alert (TA18-201A) Emotet Malware
  - https://www.us-cert.gov/ncas/alerts/TA18-201A
- Research Suggests Russian-Based Hackers Behind Ryuk Ransomware's $2.5 Million Gains
  - https://finance.yahoo.com/news/research-suggests-russian-based-hackers-131700487.html
- Long Island Ransomware Attack: New York School Pays $100,000
  - https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/ryuk-hits-rockville-centre/

References

- Ransomware hits computer networks of North Carolina water utility, CyberScoop
  - https://www.cyberscoop.com/ransomware-hits-onwasa-computer-network-north-carolina-water-utility/
- Media Release: Cyber-Criminals Target Critical Utility in Hurricane-Ravaged Area, Onslow Water and Sewer Authority
  - https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A
- Origin of virus that hobbled newspapers still unclear - The origins of a suspected computer attack that disrupted the Los Angeles Times and Tribune Publishing newspapers remain unclear
  - https://abcnews.go.com/US/wireStory/origin-virus-hobbled-newspapers-unclear-60083516
- Meet CrowdStrike’s Adversary of the Month for February: MUMMY SPIDER
  - https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/, February 8, 2018
- North Korea APT(?) and recent Ryuk Ransomware attacks
  - https://blog.kryptoslogic.com/malware/2019/01/10/dprk-emotet.html
- US Coast Guard Warns Over Ryuk Ransomware Attacks
  - https://www.bankinfosecurity.com/us-coast-guard-warns-over-ryuk-ransomware-attacks-a-13563
- Georgia county pays a whopping $400,000 to get rid of a ransomware infection
  - https://www.zdnet.com/article/georgia-county-pays-a-whopping-400000-to-get-rid-of-a-ransomware-infection/
- Informations Concernant Les Rancongiciels Lockergoga Et Ryuk
  - https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf
- Cybereason Researchers Discover a 'Triple Threat' Attack Utilizing Emotet to Deploy TrickBot Which Steals Data and Spreads Ryuk Ransomware
  - https://www.benzinga.com/pressreleases/19/04/p13470755/cybereason-researchers-discover-a-triple-threat-attack-utilizing-emote

References

- Ryuk Ransomware Adds IP and Computer Name Blacklisting
  - https://www.bleepingcomputer.com/news/security/ryuk-ransomware-adds-ip-and-computer-name-blacklisting/
- US Coast Guard - Marine Safety Information Bulletin
  - https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf
- Wizard Spider Upgrades Ryuk Ransomware to Reach Deep into LANs
  - https://threatpost.com/wizard-spider-upgrades-ryuk-ransomware/149853/
- U.S. Coast Guard Says Ryuk Ransomware Took Down Maritime Facility
  - https://www.bleepingcomputer.com/news/security/us-coast-guard-says-ryuk-ransomware-took-down-maritime-facility/
- Mistaken For North Koreans, The 'Ryuk' Ransomware Hackers Are Making Millions
  - https://www.forbes.com/sites/thomasbrewster/2019/02/20/mistaken-for-north-koreans-the-ryuk-ransomware-hackers-are-making-millions/#6d47034775f4
- Ryuk Ransomware, Exploring the Technical and Human Connections
  - https://www.coveware.com/blog/2019/2/19/ryuk-ransomware-exploring-the-technical-and-human-connections
- Stuart's city hall ransomware attack "more than likely" caused by phishing email scam
  - https://www.tcpalm.com/story/news/local/martin-county/2019/04/22/city-halls-ransomware-attack-may-linked-phishing-email-scam-ryuk/3540067002/
- 7 Florida municipalities have fallen prey to cyber attacks since last year
  - https://www.naplesnews.com/story/news/crime/2019/08/20/7-florida-municipalities-have-fallen-prey-cyber-attacks-ryuk-ransomware-phishing/2065063001/
- Tampa Bay Times hit with Ryuk ransomware attack
  - https://blog.malwarebytes.com/ransomware/2020/01/tampa-bay-times-hit-with-ryuk-ransomware-attack/

References

- Cyber attack: Virus Ryuk disrupts The Watertown Daily Times' Sunday paper delivery
  - https://www.ibtimes.sg/cyber-attack-virus-ryuk-disrupts-watertown-daily-times-sunday-paper-delivery-30503
- How a Manufacturing Firm Recovered from a Devastating Ransomware Attack
  - https://www.darkreading.com/attacks-breaches/how-a-manufacturing-firm-recovered-from-a-devastating-ransomware-attack/d/d-id/1334760
- Florida LAN: Someone clicks link, again, giving Key Biscayne ransomware
  - https://arstechnica.com/information-technology/2019/06/is-there-something-in-the-water-third-florida-city-hit-by-ransomware/
- New Warning on Ryuk Ransomware
  - https://www.darkreading.com/document.asp?doc_id=1335101
- La Porte County Pays $130,000 Ransom To Ryuk Ransomware
  - https://www.bleepingcomputer.com/news/security/la-porte-county-pays-130-000-ransom-to-ryuk-ransomware/
- China on Ryuk Virus alert: Deadly ransomware sneaks through the country’s computer systems
  - https://www.cryptopolitan.com/china-on-ryuk-virus-alert/

Ryuk, Sodinokibi Ransomware Responsible for Higher Average Ransoms
https://www.bleepingcomputer.com/news/security/ryuk-sodinokibi-ransomware-responsible-for-higher-average-ransoms/

Ryuk Related Malware Steals Confidential Military, Financial Files
https://www.bleepingcomputer.com/news/security/ryuk-related-malware-steals-confidential-military-financial-files/

Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

References

- Rolling back Ryuk Ransomware
  - https://news.sophos.com/en-us/2019/10/04/rolling-back-ryuk-ransomware/
- DCH Hospital Pays Ryuk Ransomware for Decryption Key
  - https://www.bleepingcomputer.com/news/security/dch-hospital-pays-ryuk-ransomware-for-decryption-key/
- Louisiana was hit by Ryuk, triggering another cyber-emergency
  - https://arstechnica.com/information-technology/2019/11/louisiana-was-hit-by-ryuk-triggering-another-cyber-emergency/
- Security firm Prosegur: We've shut our IT network after Ryuk ransomware attack
  - https://www.zdnet.com/article/security-firm-prosegur-weve-shut-our-it-network-after-ryuk-ransomware-attack/
- Cash-moving giant Prosegur knocked offline by Ryuk ransomware
  - https://www.csoonline.com/article/3504492/cash-moving-giant-prosegur-knocked-offline-by-ryuk-ransomware.html
- New ransomware rakes in $4 million by adopting a “big game hunting” strategy: Ryuk lies in wait for as long as a year, then pounces on only the biggest prey
  - https://arstechnica.com/information-technology/2019/01/new-ransomware-rakes-in-4-million-by-adopting-a-big-game-hunting-strategy/
- A Nasty Trick: From Credential Theft Malware to Business Disruption
  - https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html

References

- Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware
  - https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
- Hackers Demand Bitcoin Ransom in Cyberattack on Big Canadian Restaurants
  - qhttps://www.cbc.ca/news/business/ransomware-hack-recipe-unlimited-restaurant-cyberattack-1.4847487
- Ryuk Ransomware Is Making Victims Left and Right
  - https://www.bleepingcomputer.com/news/security/ryuk-ransomware-is-making-victims-left-and-right/
- Ryuk: Cult Character to Ransomware Villain
  - https://securityboulevard.com/2019/12/ryuk-cult-character-to-ransomware-villain/
- Hermes ransomware distributed to South Koreans via recent Flash zero-day
  - https://blog.malwarebytes.com/threat-analysis/2018/03/hermes-ransomware-distributed-to-south-koreans-via-recent-flash-zero-day/

Questions

Questions

Upcoming Briefs

- Artificial Intelligence – Application to the Healthcare Industry
- Electronic Health Record systems
- PyXie RAT

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.**

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

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.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV