LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Ransomware Trends 2021

06/03/2021

TLP: WHITE, ID# *202106031300*

Agenda

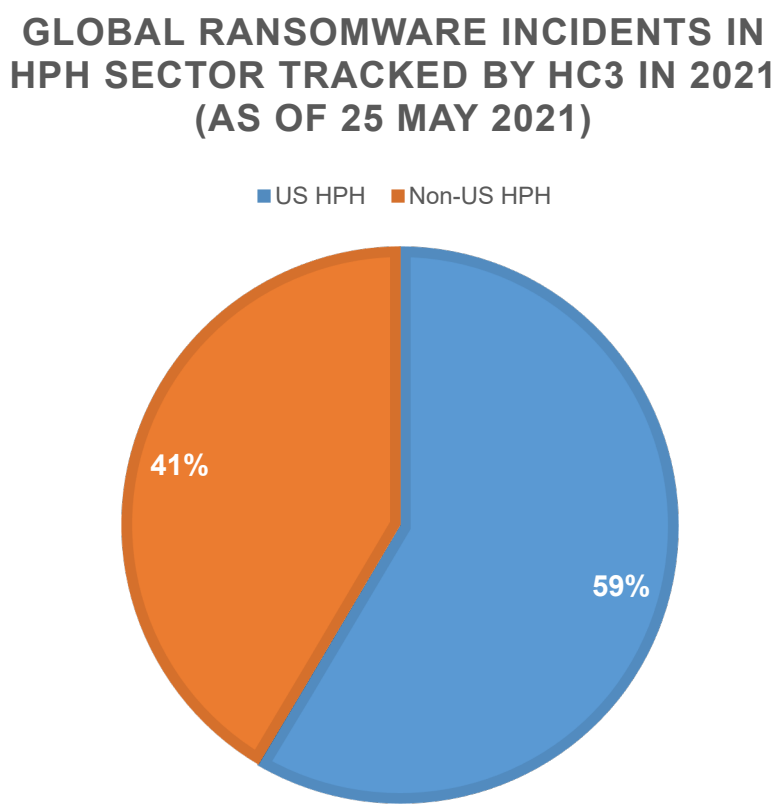
- Overview of HC3 Observations & Research
- Top Ransomware Groups Impacting Healthcare
- Healthcare Industry Victimization by Ransomware
- U.S. States with the Most Ransomware Incidents
- Data Leak Trends for the U.S. Healthcare Sector
- Sophos Ransomware in Healthcare Report
- State-Sponsored Ransomware
- DarkSide – Colonial Pipeline Attack
- DarkSide – Aftermath
- Cyber Attack on Irish Health System
- New Ransomware Capabilities
- Mitigations
- References

Slides Key:

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

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

- HC3's Cyber Threat Intelligence (CTI) team tracks notable cyber incidents affecting both US and global HPH entities, as well as attacks on non-HPH entities that may affect the HPH sector.
- Because of the HPH sector's attractiveness to ransomware actors, the HC3 CTI team pays particular attention to ransomware trends.
- As HC3 CTI's greatest priority is the US HPH sector, these findings are not representative of all incidents.
- HC3 has tracked a total of **82** ransomware incidents impacting the healthcare sector worldwide so far this calendar year, as of May 25,, 2021.
- 48 of these ransomware incidents (or nearly 60%) impacted the United States health sector.
- Findings are based primarily on observations of ransomware extortion blogs, but also open-source media reporting and breach notifications.



Top Ransomware Groups Impacting Global HPH Sector

- As of May 25, 2021, HC3 tracked 82 HPH sector ransomware incidents globally (including the United States) for the 2021 calendar year.
  - Does not include unknowns where there was an unspecified cyber incident, or where not enough data was available. (8 instances where an unknown variant was tracked.)
  - Avaddon and Conti were the most frequently observed ransomware-as-a-service (RaaS) groups impacting the healthcare sector globally so far this year. The Revil/Sodinokibi, Mespinoza/Pysa, and Babyk variants followed suit, as shown below:

Top 5 Ransomware Actors Impacting Global HPH Sector 2021		
Place	**RaaS Name**	**Number of Incidents**
1	Avaddon RaaS Operator(s)	16
2	Conti RaaS Operator(s)	16
3	REvil/Sodinokibi RaaS Operator(s)	7
4	Mespinoza/Pysa RaaS Operator(s)	6
5	Babyk RaaS Operator(s)	5

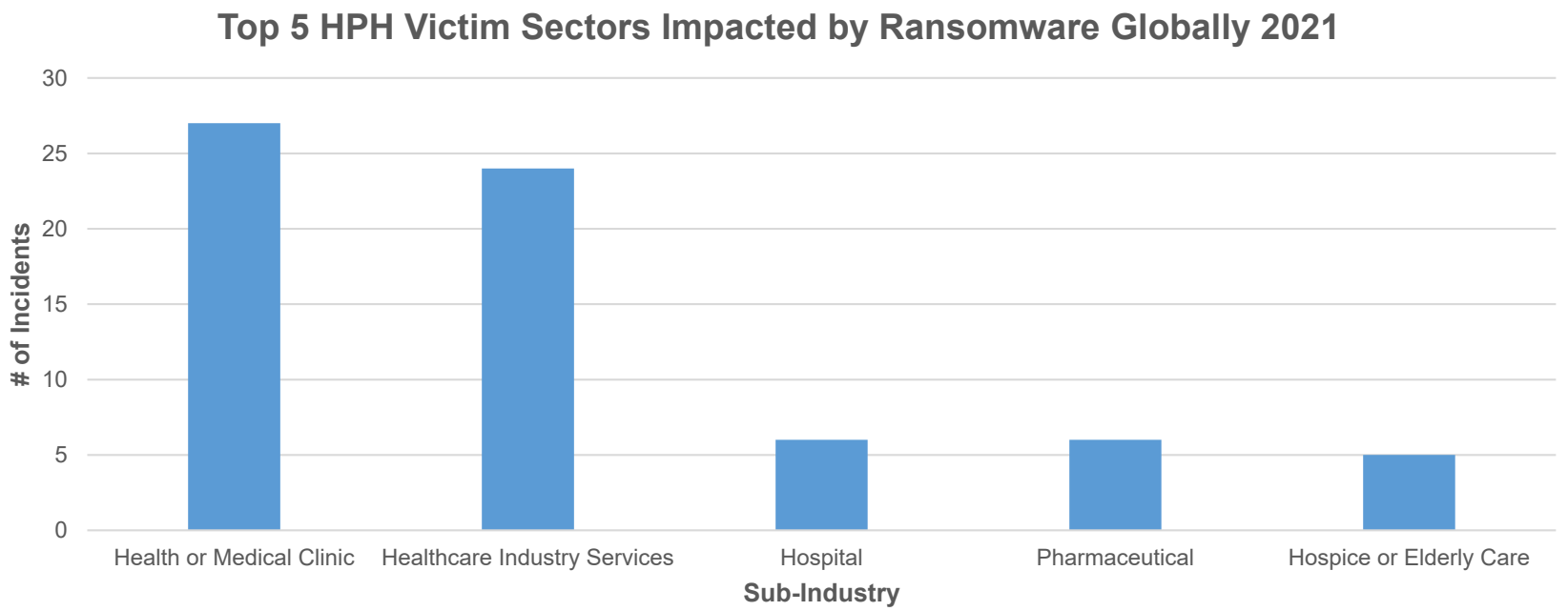
Top Ransomware Groups Impacting United States HPH Sector

- As of May 25, 2021, HC3 tracked **48 ransomware incidents targeting just the United States HPH sector** for the 2021 calendar year.
  - Does not include unknowns where there was an unspecified cyber incident, or where not enough data was available. (8 instances where an unknown variant was tracked.)
  - Conti and Avaddon continued to be the most frequently observed ransomware groups impacting healthcare. Mespinoza/Pysa, Astro, and REvil/Sodinokibi took third, fourth, and fifth place.

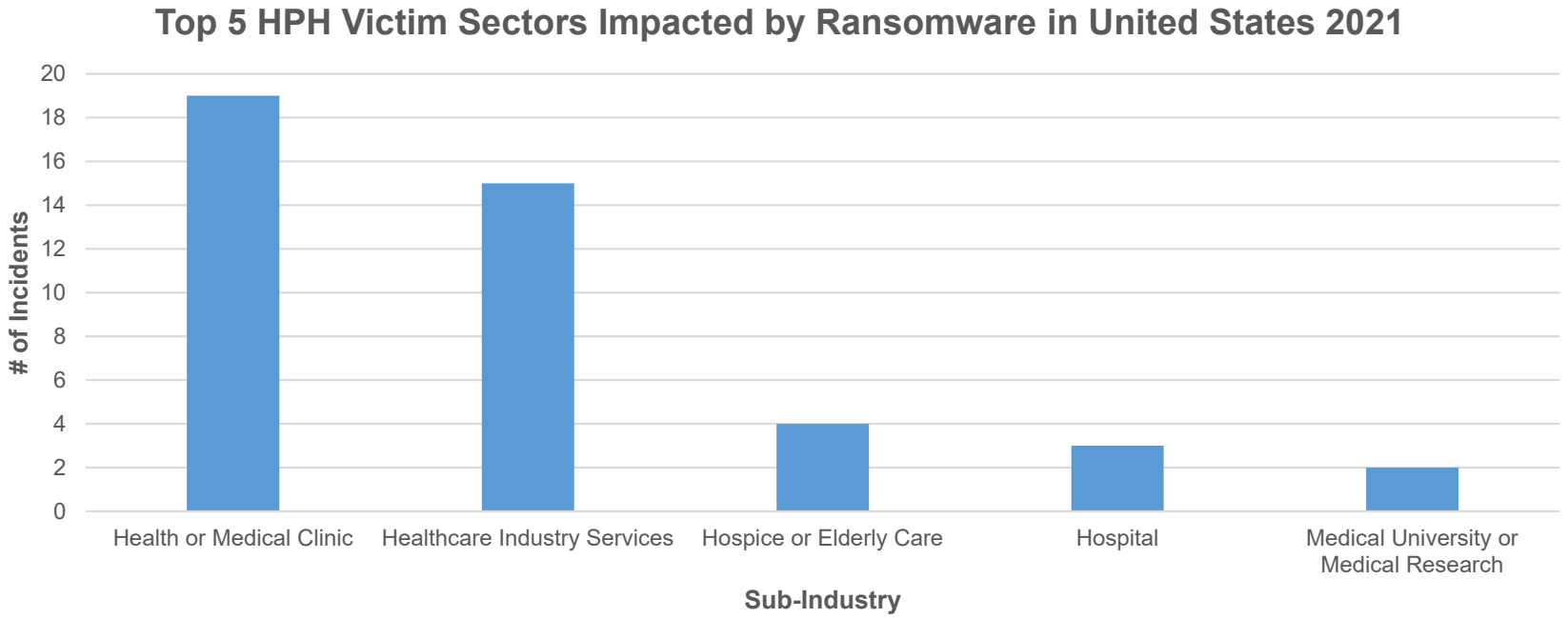
Top 5 Ransomware Actors Impacting U.S. HPH Sector 2021		
Place	**RaaS Name**	**Number of Incidents**
1	Conti RaaS Operator(s)	11
2	Avaddon RaaS Operator(s)	7
3	Mespinoza/Pysa RaaS Operator(s)	5
4	Astro RaaS Operator(s)	3
5	REvil/Sodinokibi RaaS Operator(s)	3

Healthcare Industry Victimization for Global Ransomware Incidents 2021

- Looking back at a total of **82 global ransomware incidents in the healthcare sector** tracked by HC3 in 2021 as of May 25, 2021, HC3 categorized ransomware incidents into the following sub-industries. Please note, the results below only cover the top 5 sub-industries.
- The vast majority of global ransomware incidents targeting the HPH sector so far this year impacted organizations in the Health or Medical Clinic industry, or the Healthcare Industry Services sector.

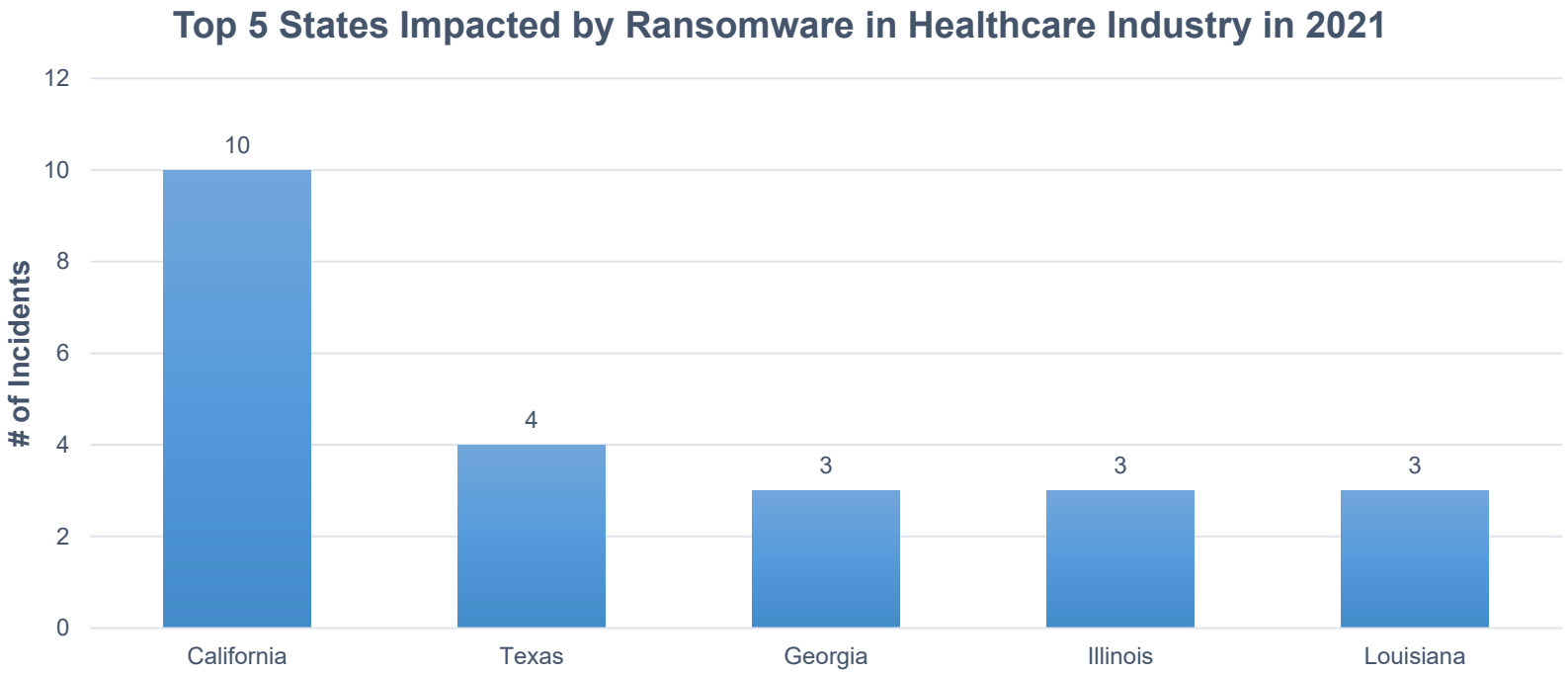


- Looking back at a total of 48 **ransomware incidents in the United States** tracked by HC3 since May 25, 2021, HC3 categorized ransomware incidents into the following sub-industries. Please note, the results below only cover the top 5 sub-industries.
- Compared to the global victimization, Health or Medical Clinics and Healthcare Industry Services organizations remained the most frequently observed victims.
- Compared to 6 total hospitals compromised by ransomware globally, 3 of them were located in the U.S.

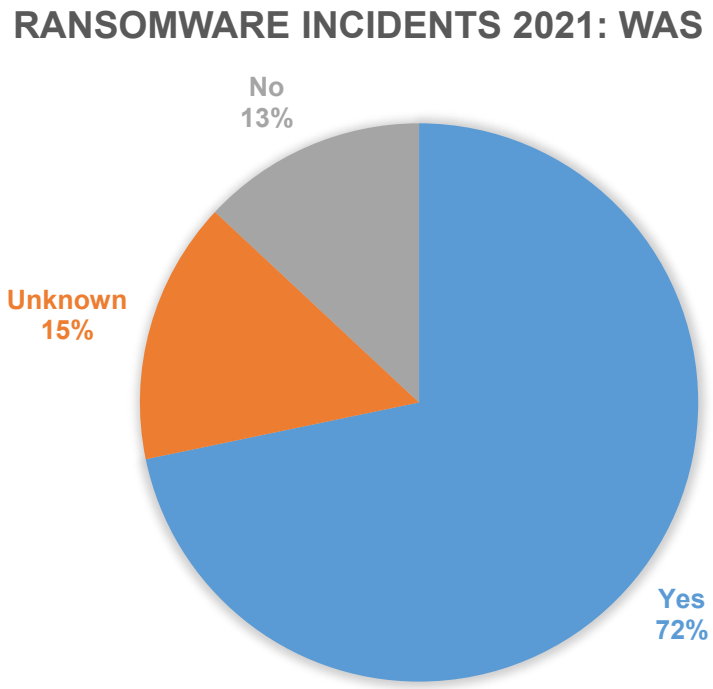


U.S. States with Most Ransomware Incidents in Healthcare

- Based on HC3 observations of ransomware extortion blogs and open-source intelligence, HC3 also determined the top 5 states that fell victim to ransomware attacks in 2021.
- Interestingly, **California** experienced the most ransomware incidents for healthcare industry victims, accounting for 12% of all U.S. ransomware incidents that we've tracked so far this year.

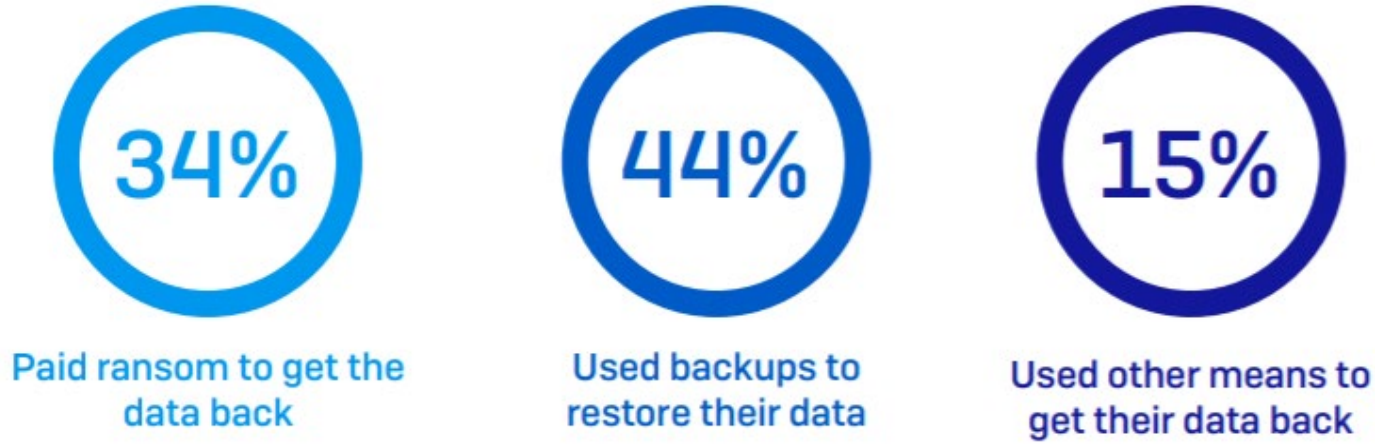


- Looking back at a total of **48 ransomware incidents in the United States healthcare sector** tracked by HC3 this year, for **at least 72%** of the ransomware incidents, victim data was leaked.
- This involved either full file dumps, screenshots, or samples.
- Based on HC3 observations of ransomware blogs, data leaks ranged from just a few screenshots to as large as Terabytes of data from the victims.

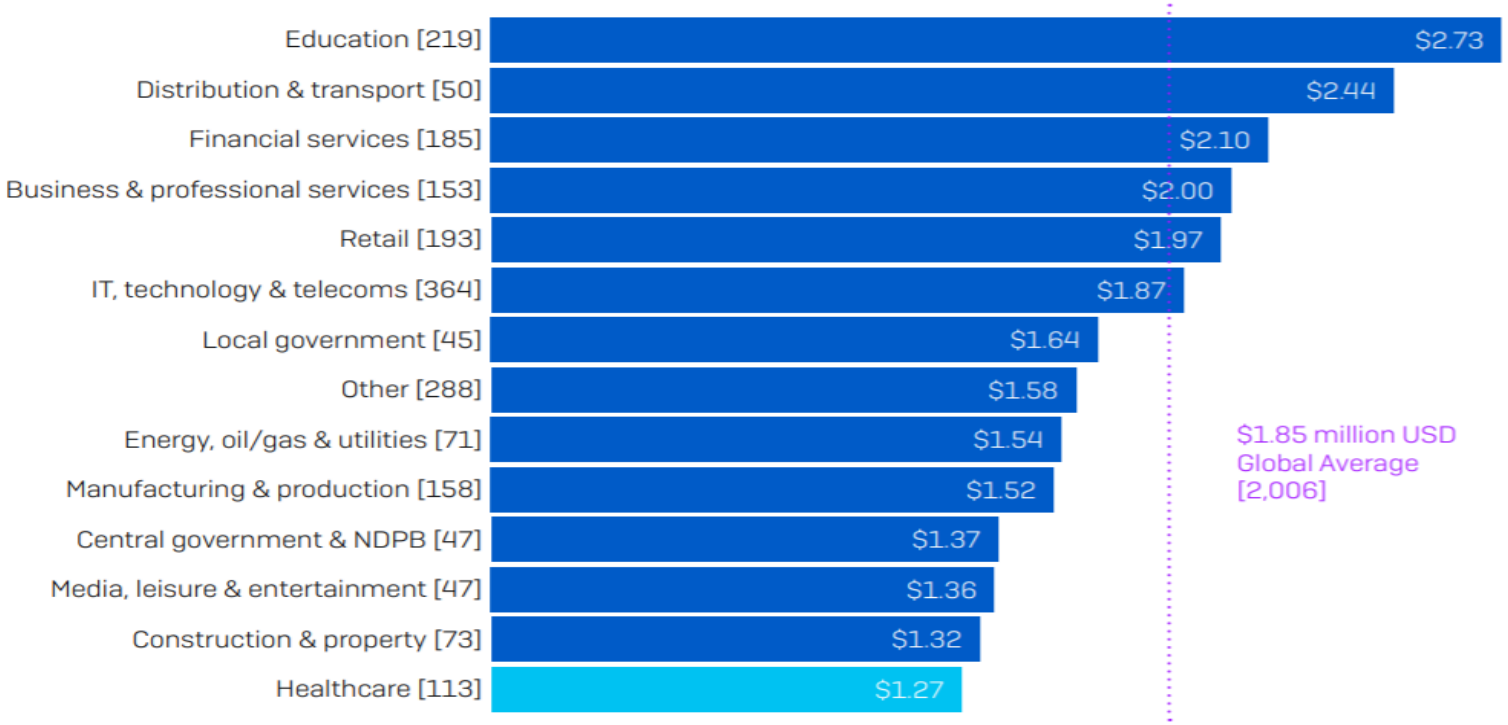


Survey of HPH organizations worldwide between January and February 2021:

- 34% of healthcare organizations were hit by ransomware in the last year.
- 65% that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack.
- 44% of those whose data was encrypted used backups to restore data.
- 34% of those whose data was encrypted paid the ransom to get their data back in the most significant ransomware attack.
- 93% of affected HPH organizations got their data back, but only 69% of the encrypted data was restored after the ransom was paid



- The average ransomware payment for the HPH sector is $131,000.
  - The average bill for rectifying a ransomware attack – considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc. – was $1.27 million.
  - While this is a huge sum, it's also the lowest among all sectors surveyed.



Average approximate cost to organizations to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) [base numbers in chart] respondents whose organization had been hit by ransomware in the last year, split by sector, Millions of US$

State-Sponsored Ransomware

- Cybersecurity firm Flashpoint reported that "Iran's Islamic Revolutionary Guard Corps (IRGC) was operating a state-sponsored ransomware campaign through an Iranian contracting company called 'Emen Net Pasargard' (ENP)."
- The project began sometime between June and September 2020.
- Flashpoint's analysis was based on three documents leaked by an anonymous entity named Read My Lips, or Lab Dookhtegan, between March 19 and April 1, 2021.
- Used a "subterfuge technique" to mimic the tactics, techniques, and procedures (TTPs) of other financially motivated cybercriminal ransomware groups so as to make attribution harder and better blend in with the threat landscape.
- Potentially financially motivated, but more likely using the appearance of financial motivation as a cover.
- Operation overlapped with deployment of Iranian state-sponsored Pay2Key ransomware targeting Israeli companies.

PAY2KEY

HELLO [redacted] USERS!

Congratulations!
Your entire network and all your informations such as computers/ employees information/ users folders/ servers/ file-servers/ applications/ databases/etc... in your network has been successfully encrypted!
Some of your important information dumped and ready to leak, in case we can't make a good deal!

Don't modify encrypted files or you can damage them and decryption will be impossible!
Don't try unofficial decryptors to recover your files or you can damage them and decryption will be impossible!

There is only ONE possible way to get back your files! Pay and contact to receive your special decryptor!
You should pay 7 BTC to receive official decryptor and easily recover your files. [redacted] special decryptor is now ready and waiting for your payment, let's do it!

You can send 4 random files from any computers and receive decrypted data, just as a proof that works!
Your UserID IS: [redacted]
Your Network ID [redacted]

| NOTICE |
Offer available until 11/08/2020. If you do not pay on time, price will be doubled!

Wallet: [redacted]

E-mail:
pay2key@tuta.io
pay2key@pm.me

Keybase:
Pay2Key

DarkSide – Colonial Pipeline Attack

- DarkSide operates a "ransomware-as-a-service" (RaaS) model
- Attack resulted in payment of $4.4 million in ransom
- Disruption to payment collection system led to shutdowns
- Perceived gas shortage led to stockpiling and panic

May 6: Colonial Pipeline is attacked

May 7: Colonial Pipeline pays ransom

May 8: Attack is announced. Colonial Pipeline shuts off servers and some pipelines

May 10: FBI confirms attack was DarkSide ransomware

May 11: Federal agencies release Alert (AA21-131A)

May 12: Colonial Pipeline restores operations and announces fuel delivery timelines

DarkSide – Aftermath

- **"Ransomware attackers are by definition liars, thieves, extortionists and members of a global criminal enterprise, and they take extreme technological measures to conceal any trace of their identity and location."** – John Reed Stark, a cybersecurity consultant and a former Chief of the Securities and Exchange Commission Office of Internet Enforcement
- DarkSide goes dark
  - Group claimed to have lost access to its servers, which are used to house and display data stolen from victims and store ransoms
  - Claimed to have lost access to some funds
  - Unlikely to be true shutdown, more likely rebranding to avoid attention
  - Avoided payouts to affiliates
  - Unlikely to have been U.S. government action
- Babyk (recently attacked DC's police department), Everest, and AKO all claim to have shut down or changed hands recently
- Several major cybercriminal forums have changed their policies about ransomware
  - Banned or discouraged discussion of ransomware
  - Banned recruiting for RaaS affiliate programs
- DHS will require companies to address ransomware in their cyber-preparedness, or face penalties
- Policy response to Colonial Pipeline will inform future ransomware policies that can affect the HPH sector
  - Infrastructure attacks can put health services in jeopardy

Attack on Irish Health System

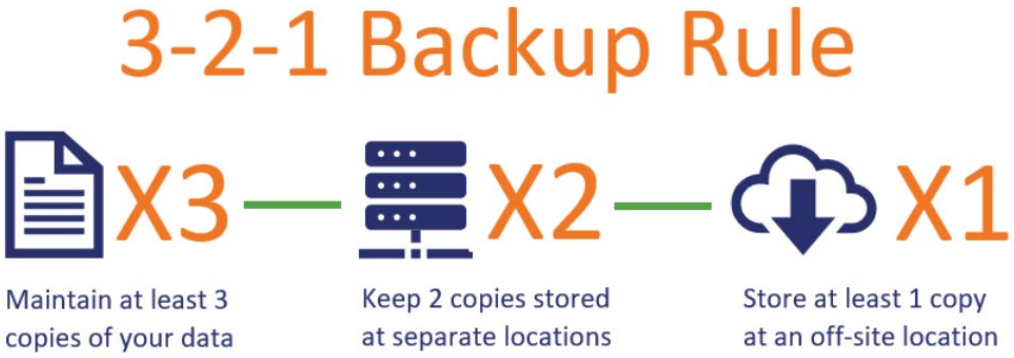
- Both the Irish Department of Health and the Health Service Executive (HSE) were attacked by Conti ransomware in May 2021
  - Within the last year, Conti has attacked 16 US HPH and first responder organizations
  - Known double-extortion practitioner
  - May use stolen credentials, RDP, or phishing campaigns to obtain initial access to a network
  - May also use Cobalt Strike, Mimikatz, Emotet, and Trickbot alongside Conti ransomware during attacks
- HSE's national clinical advisor Dr. Vida Hamilton said it was "affecting every aspect of patient care"
- Forced major cancellations to in-patient services
  - Delays in issuing birth and death certificates
  - No interruption in COVID-19 vaccination
  - Delay in processing COVID-19 tests
- Facilities forced to use pen-and-paper documentation
- Patient data was released online

New Ransomware Capabilities

- Most ransomware variants require some human direction and intervention to target and spread through networks
- Worms can spread automatically
- New Ryuk version exhibits "worm-like capabilities"
  - Allows reinfection of already-infected devices and networks
- MountLocker ransomware, which is used by AstroLocker and XingLocker, uses "enterprise Windows Active Directory APIs to worm through networks"
  - XingLocker or Xing ransomware debuted in May 2021
  - Of the 11 victims that have appeared on the Xing ransomware name-and-shame blog to date, three are part of the global HPH sector
- Triple Extortion
  - Used first by Avaddon, and is widely available to threat actors
  - Data is encrypted and exfiltrated **and** threatens a data leak **and** threatens a DDoS attack

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.



- **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 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

- "Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks," CISA, May 11, 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-131a
- Alert CP-000147-MW. "Conti Ransomware Attacks Impact Healthcare and First Responder Networks," FBI. May 20, 2021. https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf
- "A Second Iranian State-Sponsored Ransomware Operation “Project Signal” Emerges," Flashpoint Intel. April 30, 2021. https://www.flashpoint-intel.com/blog/second-iranian-ransomware-operation-project-signal-emerges/
- "Cyber-crime: Irish health system targeted twice by hackers," BBC, May 17, 2021. https://www.bbc.com/news/world-europe-57134916
- "Cyber-attack on Irish health service 'catastrophic'," BBC, May 20, 2021. https://www.bbc.com/news/world-europe-57184977
- "The State of Ransomware in Healthcare 2021," Sophos. May 2021. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf
- Abrams, Lawrence. "MountLocker ransomware uses Windows API to worm through networks," Bleeping Computer, May 19, 2021. https://www.bleepingcomputer.com/news/security/mountlocker-ransomware-uses-windows-api-to-worm-through-networks/
- Gianna. "The Colonial Pipeline Ransomware Attack: Everything We Know," Security Boulevard, May 19, 2021. https://securityboulevard.com/2021/05/the-colonial-pipeline-ransomware-attack-everything-we-know/
- Lakshmanan, Ravie. "Researchers Uncover Iranian State-Sponsored Ransomware Operation" The Hacker News. May 3, 2021. https://thehackernews.com/2021/05/researchers-uncover-iranian-state.html

- Osbourne, Charlie. "FBI identifies 16 Conti ransomware attacks striking US healthcare, first responders," ZDNet, May 24, 2021. https://www.zdnet.com/article/fbi-identifies-16-conti-ransomware-attacks-striking-us-healthcare-first-responders/
- Riley, Tonya. "The Cybersecurity 202: Ransomware groups are going underground, which could make them harder to track," The Washington Post. May 17, 2021. https://www.washingtonpost.com/politics/2021/05/17/cybersecurity-202-ransomware-groups-are-going-underground-which-could-make-them-harder-track/
- Smith, Daniel. “Welcome to the new world of triple extortion ransomware,” Security Magazine, May 18, 2021. https://www.securitymagazine.com/articles/95238-welcome-to-the-new-world-of-triple-extortion-ransomware

Questions

Upcoming Briefs

- 6/17 – Threat Hunting
- 7/8 – Conti Ransomware

Requests for Information

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

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.

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 visit us at **HHS.GOV/HC3**.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV