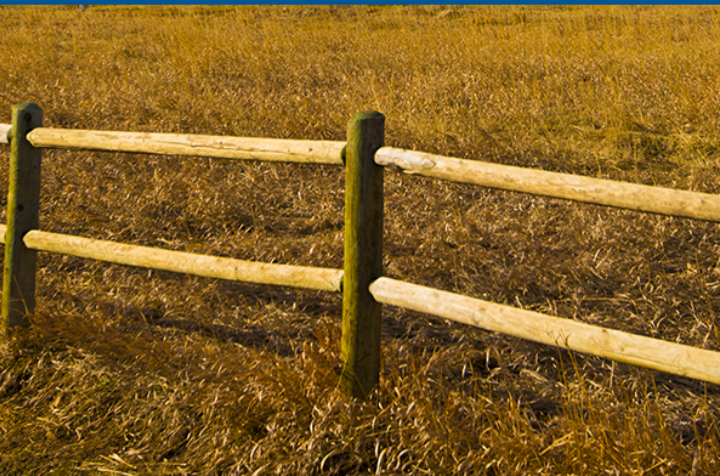




Presented and Sponsored by:



Frontier States Town Hall Meeting - Part II



MONTANA HOSPITAL ASSOCIATION

PART 2 OF THE FRONTIER STATES TOWN HALL MEETING

Cybersecurity During COVID-19: A Look Behind the Scenes

Barry Mathis
Principal, PYA, P.C.



Disclaimer



To the best of our knowledge, this information was correct at the time of publication. Given the fluid situation, and with rapidly changing new guidance issued daily, be aware that some or all of this information may have changed or no longer apply.

Please visit our COVID-19 hub frequently for the latest updates, as we are working diligently to put forth the most relevant helpful guidance as it becomes available. www.pyapc.com/covid-19-hub/

COVID-19 HUB

Because we are living through an unprecedented healthcare phenomenon, PYA is committed to sharing timely and relevant information that we hope will benefit our clients and colleagues. The COVID-19 HUB will centralize PYA's thought leadership, guidance, and resources related to the COVID-19 pandemic.

Presenter - Barry L. Mathis



- Barry has nearly three decades of experience in the information technology (IT) and healthcare industries as a CIO, CTO, senior IT audit manager, and IT risk management consultant. He has performed and managed complicated HIPAA security reviews and audits for some of the most sophisticated hospital systems in the country. Barry is a visionary, creative, results-oriented senior-level healthcare executive with demonstrated experience in planning, developing, and implementing complex information-technology solutions to address business opportunities, while reducing IT risk and exposure. He is adept at project and crisis management, troubleshooting, problem solving, and negotiating. Barry has strong technical capabilities combined with outstanding presentation skills and professional pride. He is a prudent risk taker with proficiency in IT risk management, physician relations, strategic development, and employee team building.



Barry Mathis
Principal, PYA, P.C.
bmathis@pyapc.com

Agenda

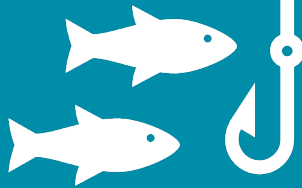


- Update on Cyber Security Threat Environment
- What are the Specific Threats in the Current COVID Environment?
- How does compromised data get used
- How to protect your data from cyber criminals

Update on Cyber Security Threat Environment



The pandemic has created what is known as an Advanced Persistent Threat (APT) to healthcare entities.



APT groups are using the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities.

Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised.

Most common forms of attack

- Phishing, using the subject of coronavirus or COVID-19 as a lure
- Malware distribution, using coronavirus- or COVID-19-themed lures
- Registration of new domain names containing wording related to coronavirus or COVID-19
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure

- To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with “Dr.” in their title.
- In several examples, actors send phishing emails that contain links to a fake email login page.
- Other emails appear to be from an organization’s human resources (HR) department and advise the employee to open the attachment.
- Malicious file attachments containing malware payloads may be named with coronavirus- or COVID-19-related themes, such as “President discusses budget savings due to coronavirus with Cabinet.rtf.”

Examples of recent phishing email subject lines include:

- 2020 Coronavirus Updates
- Coronavirus Updates
- 2019-nCov: New confirmed cases in your city
- 2019-nCov: Coronavirus outbreak in your city (Emergency)

These emails contain a call to action, encouraging the victim to visit a website that malicious cyber actors use for stealing valuable data, such as usernames and passwords, credit card information, and other personal information.

A number of cyber criminals have used COVID-19-related phishing to steal user credentials.

- These emails include previously mentioned COVID-19 social engineering techniques, sometimes complemented with urgent language to enhance the lure.
- If the user clicks on the hyperlink, a spoofed login webpage appears that includes a password entry form.
- These spoofed login pages may relate to a wide array of online services including—but not limited to—email services provided by Google or Microsoft, or services accessed via government websites.

COVID-19 Phishing to Deploy Malware



A number of threat actors have used COVID-19-related lures to deploy malware.

- In most cases, actors craft an email that persuades the victim to open an attachment or download a malicious file from a linked website. When the victim opens the attachment, the malware is executed, compromising the victim's device.
 - Many of these recent attacks deploy the “Agent Tesla” keylogger malware.
 - The email appears to be sent from Dr. Tedros Adhanom Ghebreyesus, Director-General of WHO.
 - This email campaign began on Thursday, March 19, 2020.
- Another similar campaign offers thermometers and face masks to fight the epidemic. The email appears to attach images of these medical products but instead contains a loader for Agent Tesla.

COVID-19 Smishing



- Most phishing attempts come by email but federal agencies have observed some attempts to carry out phishing by other means, including text messages (SMS).
- Historically, SMS phishing has often used financial incentives—including government payments and rebates (such as a tax rebate)—as part of the lure.
- Coronavirus-related phishing continues this financial theme, particularly in light of the economic impact of the epidemic and governments' employment and financial support packages.

Relaxed HIPAA guidance does not mean unaccountable.

- Yes, using the HIPAA waiver, you can use social video conferencing tools for telehealth visits.
- Covered health care providers will not be subject to penalties for violations of the HIPAA Privacy, Security, and Breach Notification Rules that occur in the good faith provision of telehealth during the COVID-19 nationwide public health emergency.
- This Notification does not affect the application of the HIPAA Rules to other areas of health care outside of telehealth during the emergency.
- The Notification of Enforcement Discretion does not have an expiration date. OCR will issue a notice to the public when it is no longer exercising its enforcement discretion based upon the latest facts and circumstances.

Just because you can doesn't mean you should.

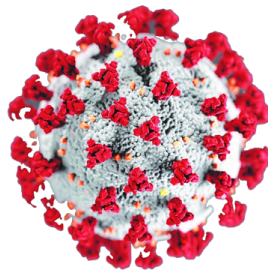
- Yes, the federal government has eased restrictions that now allow the use of FaceTime and other platforms.
- However, there are many HIPAA-compliant telehealth solutions that can be deployed within hours or days.
- Many of these solutions have full EMR integration options that could be implemented after the COVID-19 influx.



Image source: stevepb for pixnio.com, at
<https://pixnio.com/objects/tools/hammer-nail-screw-screwdriver-wood-tool-metal>

BEFORE

Before the pandemic, 1 in 10 patients in the US used telehealth, according to a J.D. Power survey from July 2019.



AFTER

One telehealth provider reports appointments are up by 70% since the virus hit the US in January, usage of the app has increased by 158% nationwide, and increased by 650% in Washington State.

Image source: Shutterstock

Telehealth Landscape Beyond 2020

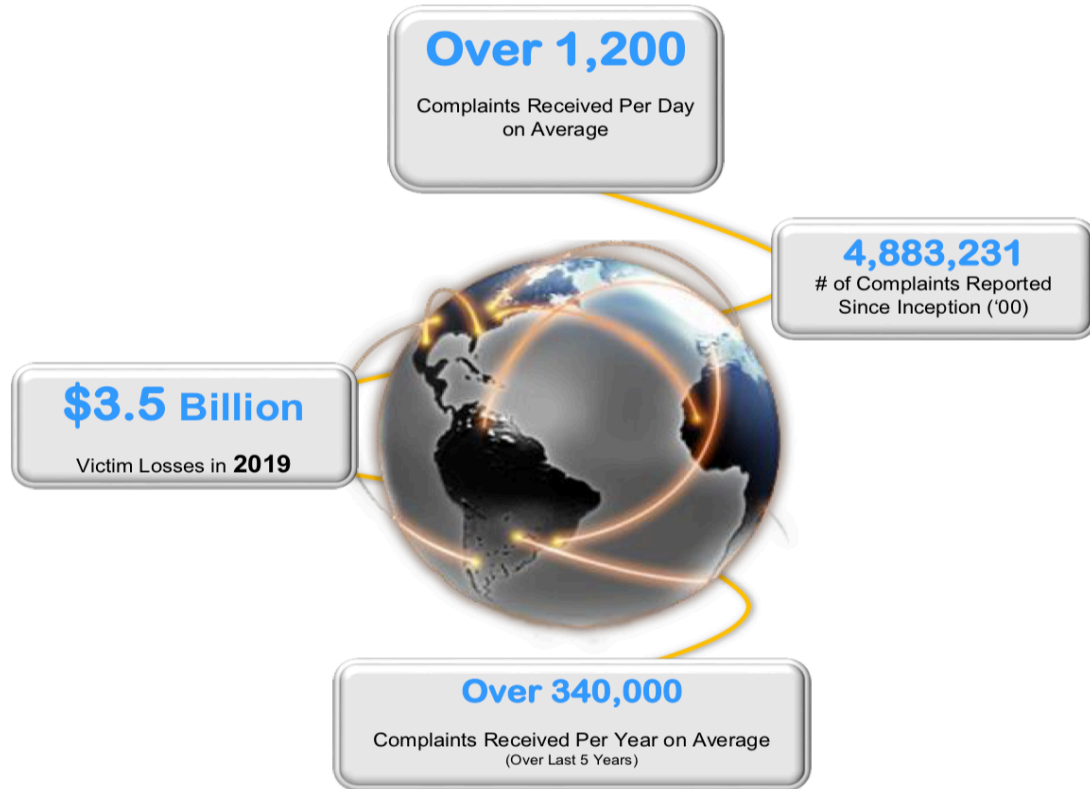


- It is said that necessity is the mother of invention, and fewer events fuel necessity more than a disaster.
- Once COVID-19 is behind us, the likelihood that telehealth will go back to its once meager beginnings is doubtful.
- First time telehealth consumers will get a taste of the technology and realize its potential and over time demand better, more accessible and flexible solutions.
- Telehealth can be a major contributor to getting patients back into the care continuum during and after COVID-19.



Image source: Shutterstock

IC3 by The Numbers



FBI's Internet Crime Complaint Center (**IC3**) which provides the public with a trustworthy and convenient mechanism for reporting information concerning suspected Internet-facilitated criminal activity.

Cyber Crime Environment



2019 Crime Types *Continued*

By Victim Loss

| Crime Type | Loss | Crime Type | Loss |
|------------------------------------|-----------------|--------------------------------|---------------|
| BEC/EAC | \$1,776,549,688 | Employment | \$42,618,705 |
| Confidence Fraud/Romance | \$475,014,032 | Civil Matter | \$20,242,867 |
| Spoofing | \$300,478,433 | Harassment/Threats of Violence | \$19,866,654 |
| Investment | \$222,186,195 | Misrepresentation | \$12,371,573 |
| Real Estate/Rental | \$221,365,911 | IPR/Copyright and Counterfeit | \$10,293,307 |
| Non-Payment/Non-Delivery | \$196,563,497 | Ransomware | **\$8,965,847 |
| Identity Theft | \$160,305,789 | Denial of Service/TDoS | \$7,598,198 |
| Government Impersonation | \$124,292,606 | Charity | \$2,214,383 |
| Personal Data Breach | \$120,102,501 | Malware/Scareware/Virus | \$2,009,119 |
| Credit Card Fraud | \$111,491,163 | Re-shipping | \$1,772,692 |
| Extortion | \$107,498,956 | Gambling | \$1,458,118 |
| Advanced Fee | \$100,602,297 | Health Care Related | \$1,128,838 |
| Other | \$66,223,160 | Crimes Against Children | \$975,311 |
| Phishing/Vishing/Smishing/Pharming | \$57,836,379 | Hacktivist | \$129,000 |
| Overpayment | \$55,820,212 | Terrorism | \$49,589 |
| Tech Support | \$54,041,053 | | |
| Corporate Data Breach | \$53,398,278 | | |
| Lottery/Sweepstakes/Inheritance | \$48,642,332 | | |

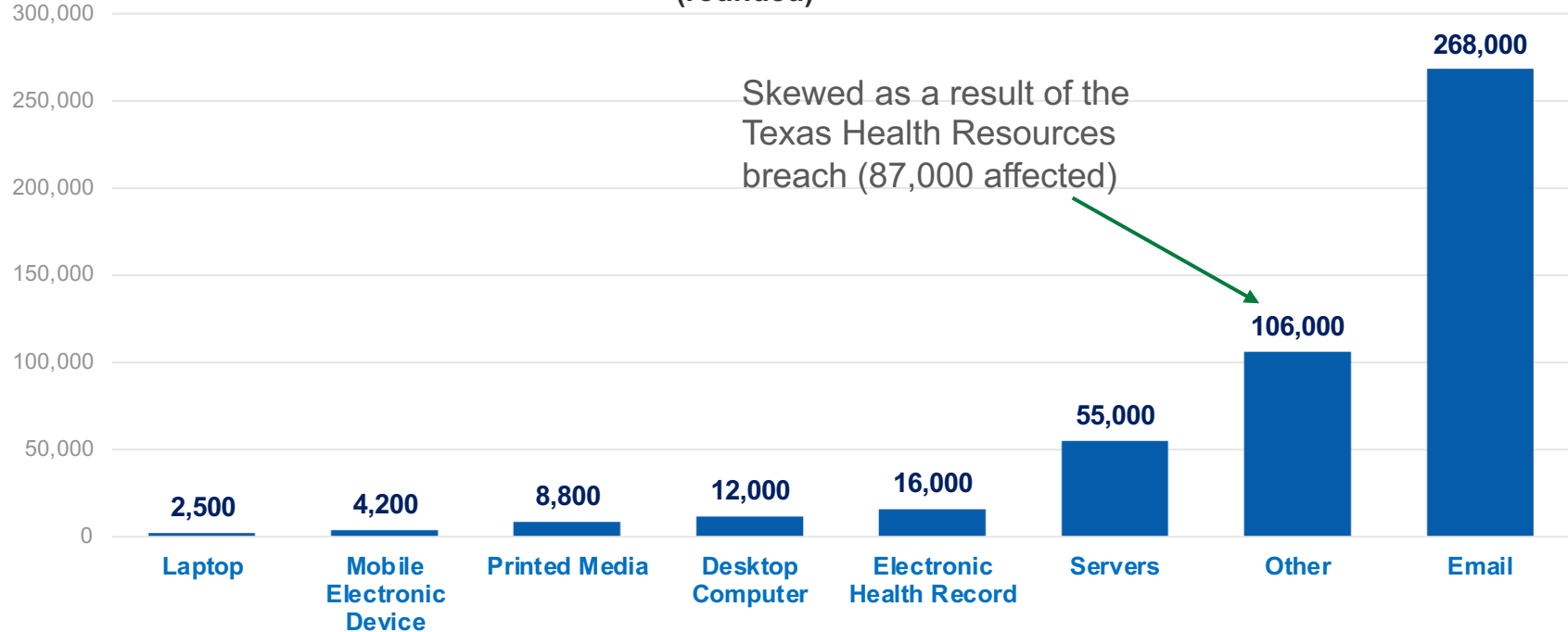
* This number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.

Source: <https://www.ic3.gov>

2019 Healthcare Breaches



**November 2019 Breaches by People Affected
(rounded)**



Source Data: <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html>

Some Terminology



Ransomware

- A type of malicious software designed to block access to a computer system until a sum of money is paid.

Bad Actor

- An entity that is partially or wholly responsible for a security incident that impacts an organization's security."

Vulnerability

- *A weakness or gap in our protection efforts.*

Attack Campaign

- Designed to bypass conventional advanced threat prevention controls and are typically executed by well-funded organizations.

Attack Vector

- A path or means by which a bad actor can gain access to a computer or network server in order to deliver a payload

Payload

- Malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.

Encryption

- Data that is scrambled using an encryption algorithm and an encryption key.

Crypto Key

- A string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.

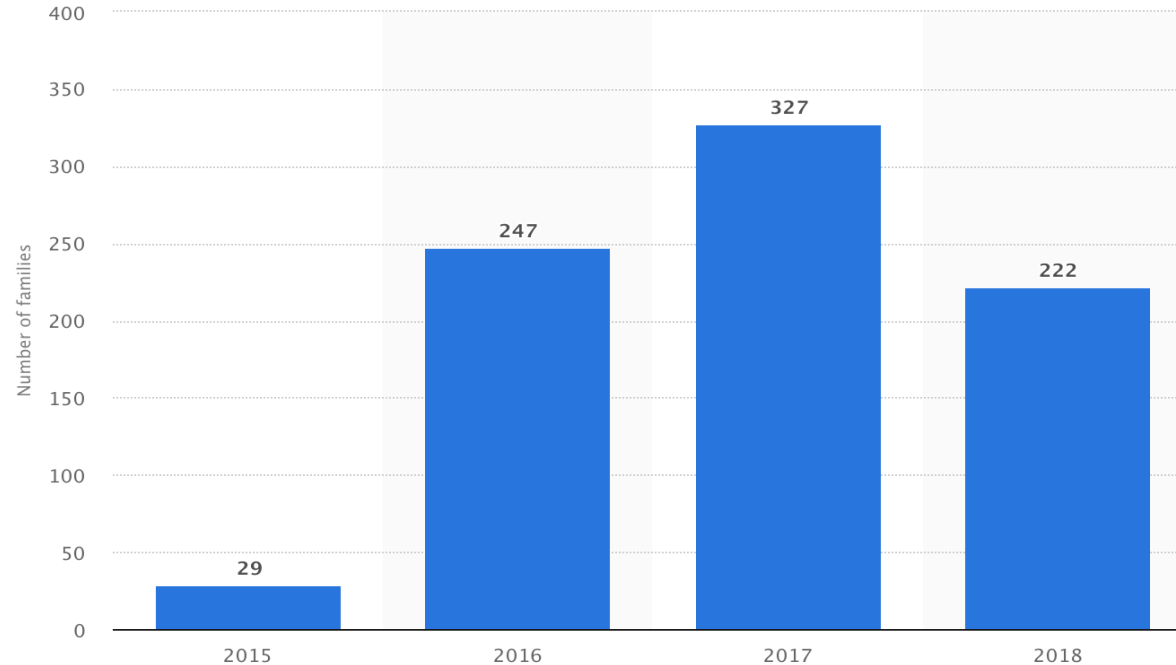
Key Logger

- A software program that logs keystrokes

Cryptocurrency

- A digital currency in which encryption techniques are used to regulate the generation currency and verify the transfer of funds

- Number of Newly Discovered Ransomware Families 2015 to 2018



Source: <https://www.statista.com/statistics/701029/number-of-newly-added-ransomware-families-worldwide/>

Ransomware Origins



- BC – Before Crypto
 - Earliest known malware classified as "Ransomware"
 - PC Cyborg Trojan – 1989, replaced Autoexec.bat
 - After boot count reached 90, hid & renamed boot directories and files.
 - Ransom: \$189
 - Extortionate ransomware became prominent in 2005
 - Limited to .JPG, .PDF, .ZIP and .DOC
 - Compressed and locked files with a password
 - Later variants locked Operating Systems and Master Boot Records
 - Ransom: \$300 to get password



Sources: <https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf>.
<https://www.pexels.com/photo/grayscale-photography-of-pedestal-balustrade-161875/>.

Ransomware Origins



- AC – After Crypto
 - Ransomware hits mainstream around 2013
 - Typically starts with a social engineering attack
 - Users tricked into launching malware
 - Files are encrypted leaving behind a ransom note
 - Payment is via crypto currency: \$500 to \$1,000
 - Becomes criminal enterprise between 2015 and 2016
 - Target shifts from individuals to businesses
 - 29 ransomware families discovered in 2015
 - 2016 saw a 752% rise to 247 ransomware families
 - More “lit fuse” strains that increase ransom over time
 - Generates \$1 billion in 2016 and 2017



Sources: <https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf>.
<https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646>.

Genealogy of Ransomware

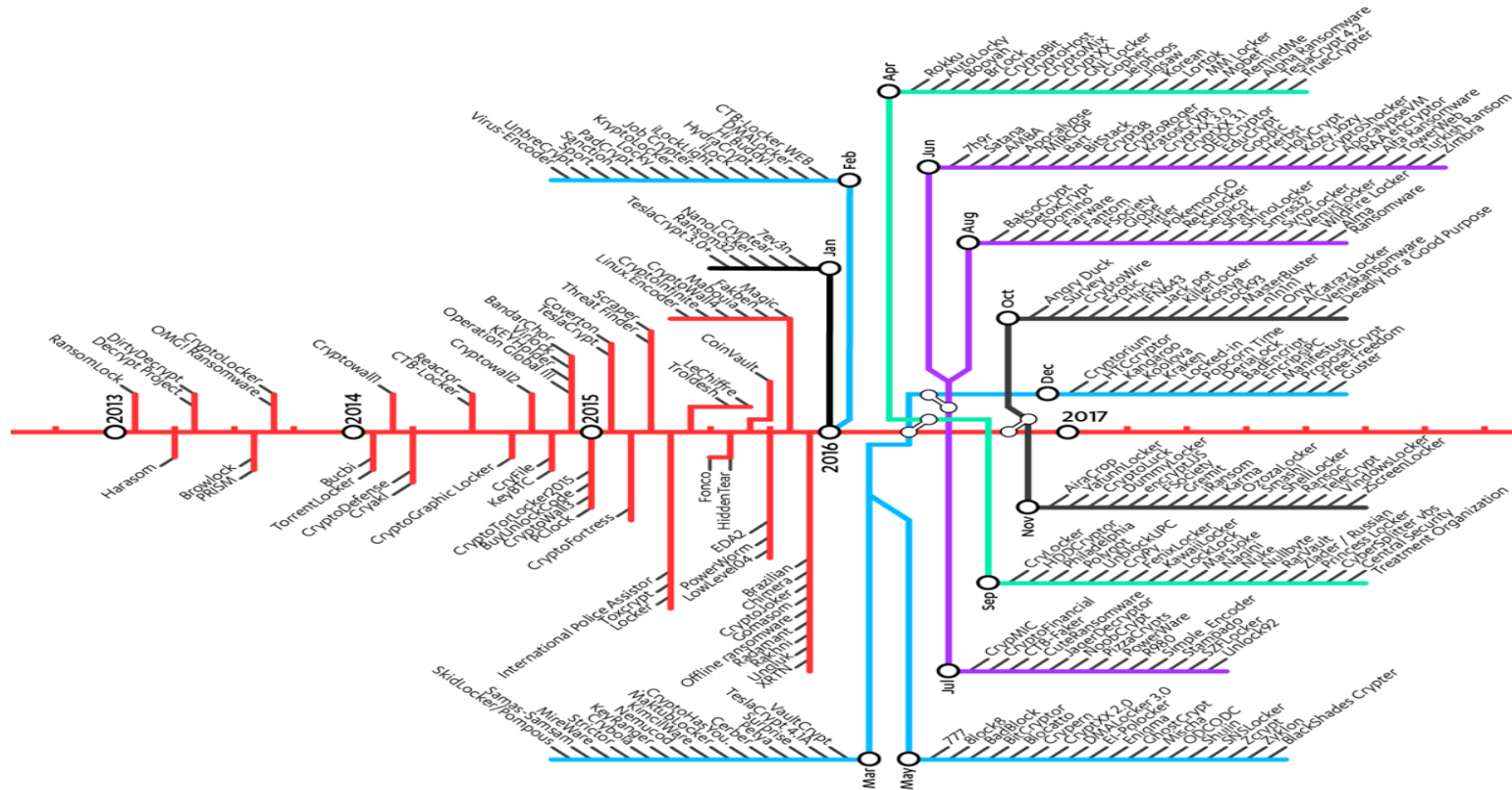
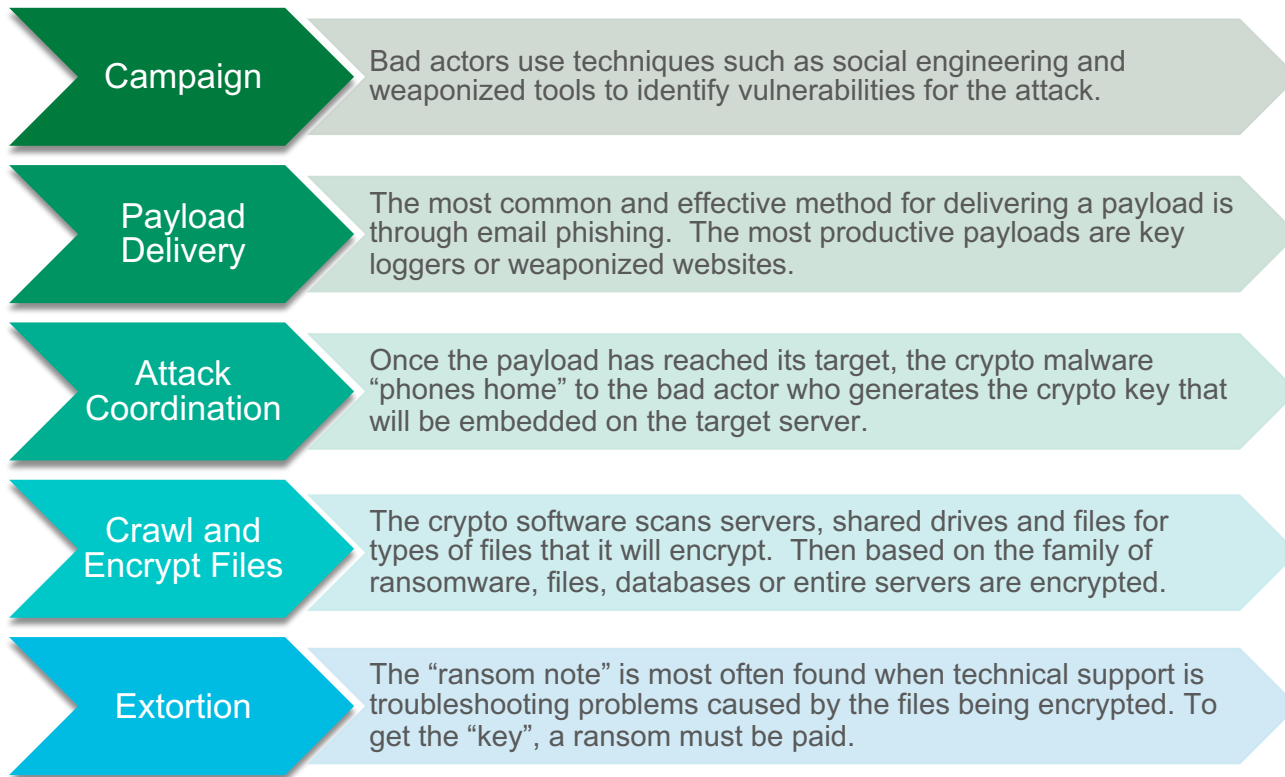


Image Source: <https://labsblog.f-secure.com/2017/04/18/ransomware-timeline-2010-2017/>

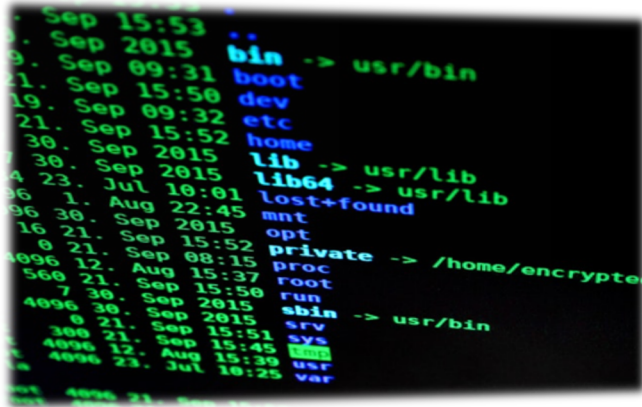
Crypto Ransomware Organized Attack



Chemistry of Crypto Ransomware



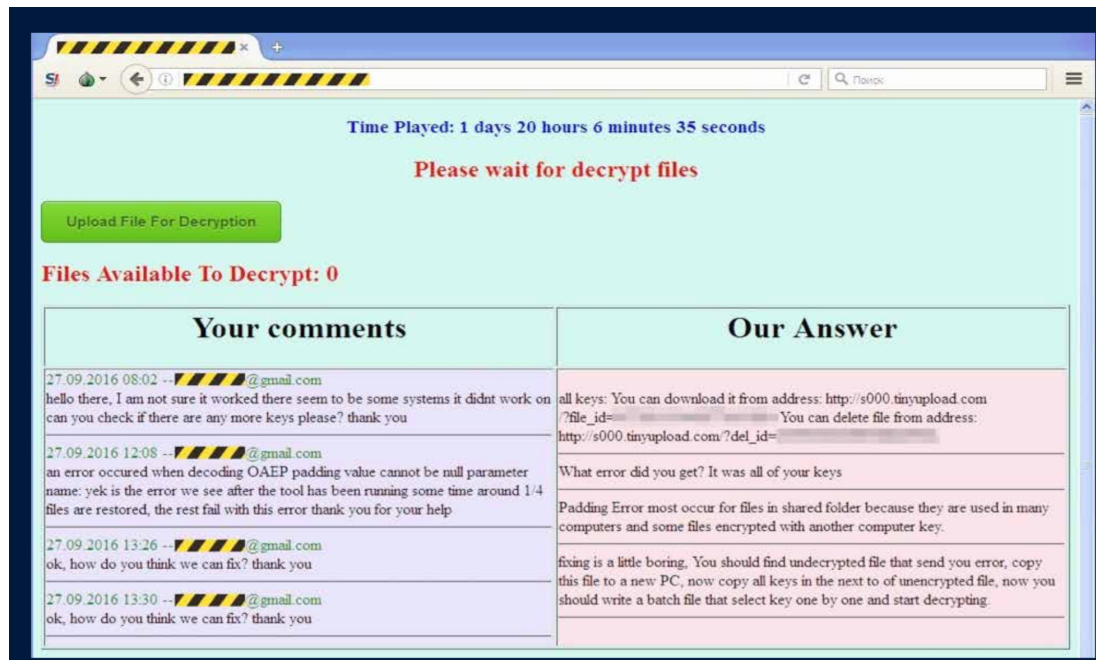
- How Ransomware interacts with the target environment.
- How we respond and interact with Ransomware.



- How Ransomware interacts with the target environment.
 - The most common injection points of successful Ransomware are through known vulnerabilities and email phishing.
 - Unpatched devices top the list of vulnerabilities
 - Social media and retail sales websites top the list for email phishing
 - The ultimate goal is to gain access to an administrator account or any account with elevated access such as an executive or system admin.

- How Ransomware interacts with the target environment (continued).
 - Once inside, the crypto malware crawls looking for common database types such as MS SQL, IBM DB2, Oracle, XML, MySQL, CACHE, MUMPS. These are high value targets as encrypting them yields a high likelihood of disruption.
 - Along with database files, the crypto malware will encrypt many common file types to cause maximum disruption.

■ Sample Ransomware Note – SamSam 2017



Time Played: 1 days 20 hours 6 minutes 35 seconds

Please wait for decrypt files

Upload File For Decryption

Files Available To Decrypt: 0

| Your comments | Our Answer |
|---|---|
| 27.09.2016 08:02 --[redacted]@gmail.com hello there, I am not sure it worked there seem to be some systems it didnt work on can you check if there are any more keys please? thank you | all keys: You can download it from address: http://s000.tinyupload.com/?file_id=[redacted] You can delete file from address: http://s000.tinyupload.com/?del_id=[redacted] |
| 27.09.2016 12:08 --[redacted]@gmail.com an error ocured when decoding OAEP padding value cannot be null parameter name: yek is the error we see after the tool has been running some time around 1/4 files are restored, the rest fail with this error thank you for your help | What error did you get? It was all of your keys Padding Error most occur for files in shared folder because they are used in many computers and some files encrypted with another computer key. |
| 27.09.2016 13:26 --[redacted]@gmail.com ok, how do you think we can fix? thank you | fixing is a little boring. You should find undecrypted file that send you error, copy this file to a new PC, now copy all keys in the next to of unencrypted file, now you should write a batch file that select key one by one and start decrypting. |
| 27.09.2016 13:30 --[redacted]@gmail.com ok, how do you think we can fix? thank you | |

Chemistry of Crypto Ransomware



Threat Finder v2.4 Total Encrypted 102400

WARNING! Your personal files are encrypted!
Don't switch off your computer and/or internet, otherwise your key will be disabled

Private key will be destroyed on

04/21/2015
23:11 AM

Time left:
71:38:41

1. You should register Bitcon wallet (<https://blockchain.info/en/wallet>)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
[LocalBitcoins.com](#) (WU) - Buy Bitcoins with Western Union
[CoinCafe.com](#) - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
[LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
[coinmr.com](#) - Another fast way to buy bitcoins
[bitquick.co](#) - Buy Bitcoins Instantly for Cash
[cashintocoins.com](#) - Bitcoin for cash.
[coinjar.com](#) - CoinJar allows direct bitcoin purchases on their site.
[zipzapinc.com](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. Send 1.25 BTC (\$300) to Bitcoin address specified below:

Send 1.25 BTC (\$300) to the following address:
or copy from QR code

Your BOT ID: **00000000** (put in NOTE field)

During the payment of 300 USD please use your Bot ID, otherwise your files will not be decrypted.

Payment via Bitcoin

Check payment

Sample Ransomware Note

- Response to Ransomware attack.
 - Timing is critical: Report to Law Enforcement (<https://www.ic3.gov>)
 - Date of Infection
 - Ransomware Variant (identified on the ransom page or by the encrypted file extension)
 - Victim Company Information (industry type, business size, etc.)
 - How the Infection Occurred (link in e-mail, browsing the Internet, etc.)
 - Requested Ransom Amount
 - Actor's Bitcoin Wallet Address (may be listed on the ransom page)
 - Ransom Amount Paid (if any)
 - Overall Losses Associated with a Ransomware Infection (including the ransom amount)
 - Victim Impact Statement

- Response to Ransomware attack.
 - Consider Behavioral Based End Point Protection
 - Assumes you will be compromised
 - Uses Machine Learning and profile templates to detect and stop abnormal behavior
 - Uses Virtual Patching (security enforcement layer analyzes transactions and intercepts attacks in transit)
 - Monitors all points of environment and not just access points
 - Not based on 3rd party malware definitions
 - More effective on Zero Day attacks.

■ **Origin:**

- In the 1960s at MIT, of the term “hacker”, where extremely skilled individuals practiced hardcore programming in FORTRAN and other older languages.
- Some may ignorantly dub them “nerds” or “geeks” but these individuals were, by far, the most intelligent, individual, and intellectually advanced people who happen to be the pioneers and forefathers of the talented individuals that are today the true hackers.

■ **Ethical Hacking:**

- An ethical hacker is an individual hired to hack into a system to identify and repair potential vulnerabilities, effectively preventing exploitation by malicious hackers. They are security experts that specialize in the penetration testing (pen-testing) of computer and software systems for the purpose of evaluating, strengthening and improving security.
- An ethical hacker is also known as a white hat hacker, red team, tiger team or sneaker.

Who Are The Hackers



Black Hat



Extraordinarily skilled at using their abilities and tools for personal gain or disruption. Dedicated to destruction.

White Hat



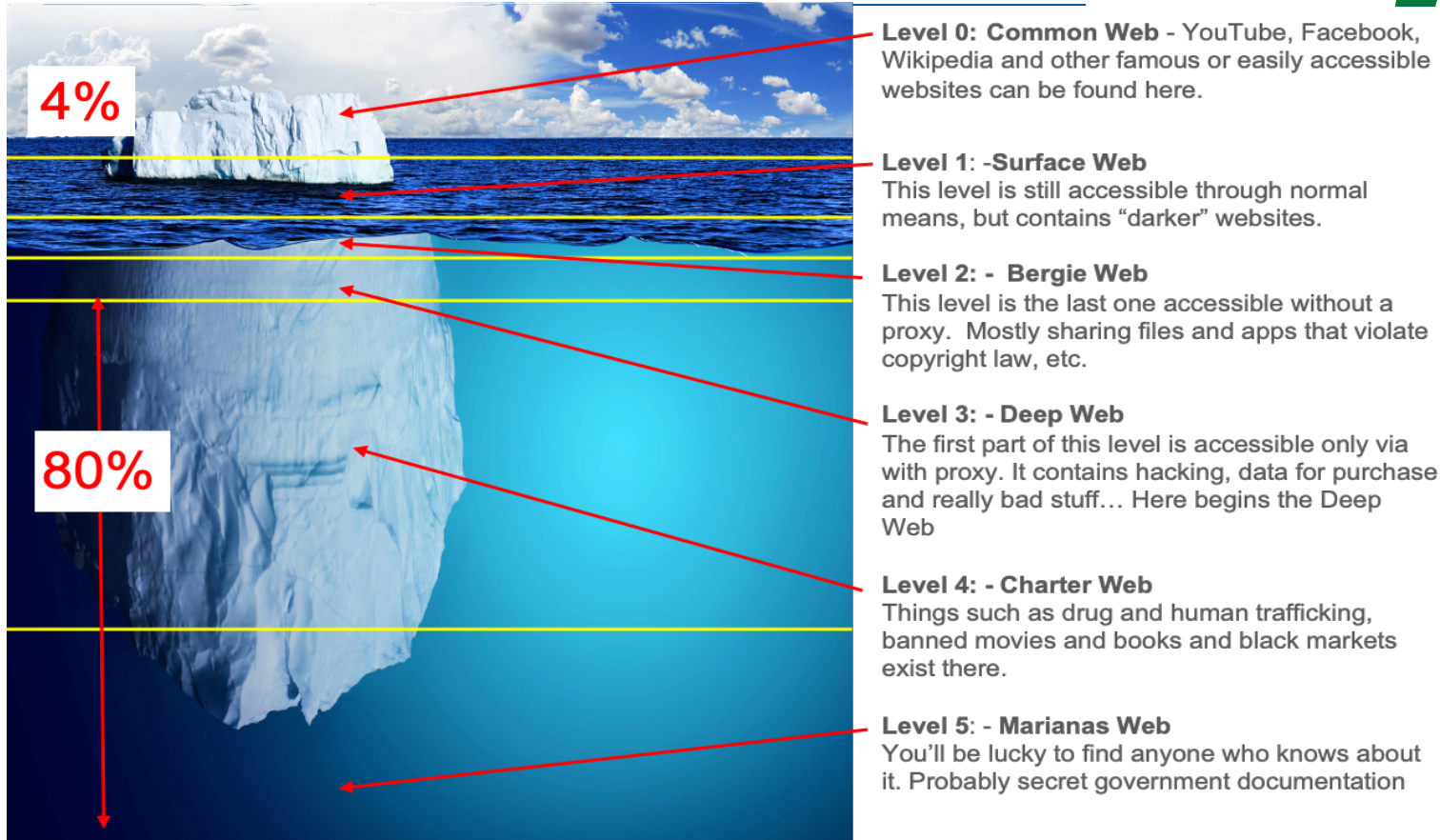
Experienced in using the same knowledge and tools as Black Hat, but use those skills to assist in education, and prevention for the common good.

Grey Hat



Mercenaries for hire. These hackers use their skills and tools for the highest bidder or to capitalize on an opportunity.

Fieldtrip into the DarkWeb



Cyber Crime: What can you do?



- Cyber Crime isn't going away
 - Many of the worst manual ransomware attacks started when the attacker discovered that an administrator had opened a hole in the firewall for a Windows computer's remote desktop. Closing these easy loopholes goes a long way to preventing these kinds of attacks. If you need to RDP, put it behind a VPN.
 - Multi-factor authentication is an amazingly effective tool for preventing the abuse of stolen credentials. If you're not using it now, you should be.
 - Administrators who manage networks should limit their use of the Domain Admin credentials to a dedicated machine or machines that are used for no other purpose.
 - Sophos Labs 2019 Threat Report
- Be diligent about what you click in emails. A Business Email Compromise is still one of the most effective ways to deliver a ransomware payload.

Image Source: <https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf>

- HIPAA requires notification in the event of a breach of unsecured PHI.
 - Notification must be made to the patient, government, and in some cases the media.
 - **Breach** → acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.
 - ePHI encrypted by ransomware has been **acquired** (i.e., unauthorized individuals have taken possession or control of the information).
 - That makes the attack a **BREACH** unless:

Low Probability of Compromise



- **Factors you must consider:**
 - Nature and extent of PHI
 - Who used the PHI or to whom the disclosure was made
 - Was PHI acquired/viewed
 - Has risk been mitigated
- **May also want to consider:**
 - Risk of unavailability of data
 - Risk to integrity of data
 - Was PHI exfiltrated
- **Must maintain documentation of the risk assessment**

Breach Incident Response



- Develop a plan before a breach occurs.
 - Create a site profile that includes contacts, legal, finance and public relations.
- The Incident Response Plan should designate:
 - Roles and responsibilities:
 - Notify your regional FBI field agent, PR firms, legal counsel, your cybersecurity insurer (only to the extent required in your policy), etc.; and
 - Identify a data forensics team to determine the source and scope of the breach and ensure vulnerable systems are patched as soon as possible.
 - Timelines
 - A communication plan for all audiences (employees, patients, board members, etc.)
 - Determine reporting obligations under federal and state law requirements.

Managing Cybersecurity Threats



- Recently HHS released a guidance document on Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)
- The purpose of the HICP is to:
 1. Raise awareness of cybersecurity;
 2. Provide vetted cybersecurity practices;
 3. Move organizations towards consistency in mitigating cybersecurity threats to the sector; and
 4. Aid health care and public health organizations to develop meaningful cybersecurity objectives and outcomes.
- HHS identified e-mail phishing, ransomware, loss or theft of equipment or data, insider, accidental, or intentional data loss, and attacks against connected medical devices as the 5 most common threats to patient health information.

Questions

