
Ransomware Under The Microscope A Closer Look

GHA Compliance Officers Roundtable Retreat
September 6, 2018

Presented by:

Robert M. Keenan III
King & Spalding
Partner, Healthcare

Barry L. Mathis
PYA
Consulting Principal

KING & SPALDING



Rob Keenan, Partner Healthcare

Rob Keenan is a partner with the Healthcare Practice Group of King & Spalding in Atlanta, Georgia. He is a graduate of the University of Illinois and of the University of Georgia School of Law. Rob advises health industry clients on a wide variety of regulatory, contracting and transactional matters, with considerable focus on HIPAA and health information privacy and cybersecurity issues. He is a member of the American Health Lawyers Association and is a past president of the Georgia Academy of Healthcare Attorneys.

Barry Mathis, Consulting Principal

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 security reviews and audits for some of the most sophisticated hospital systems in the country.

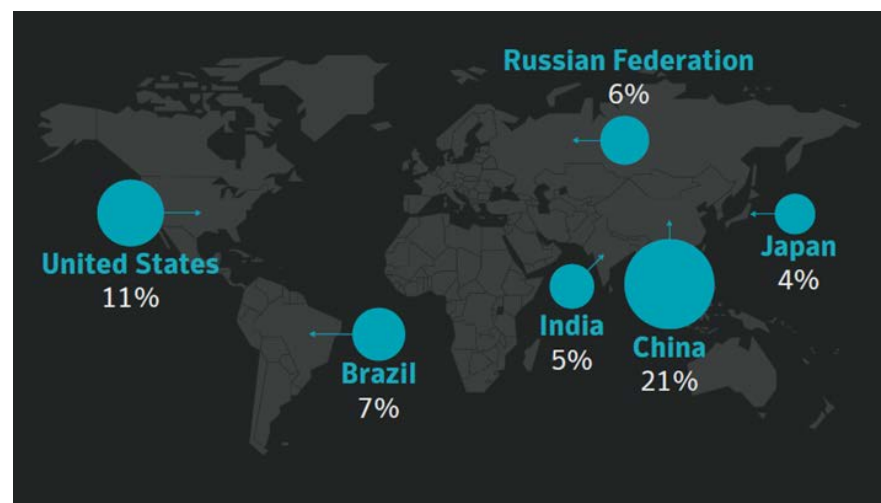
Barry is a creative senior level healthcare executive who is visionary and results-oriented, with demonstrated experience in planning, developing, and implementing complex information technology solutions to address business opportunities while reducing IT risk and exposure. He is adept at project and crisis management, trouble shooting, problem solving, and negotiating.

Cybersecurity Landscape (Ransomware)

- Number of ransomware detections per day



- Attack origins



The numbers

\$522

Avg. Ransom Demand

\$133,000

Avg. Cost to Companies

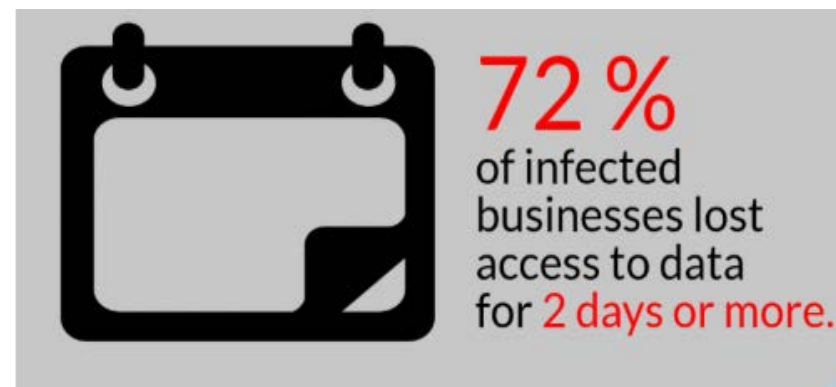
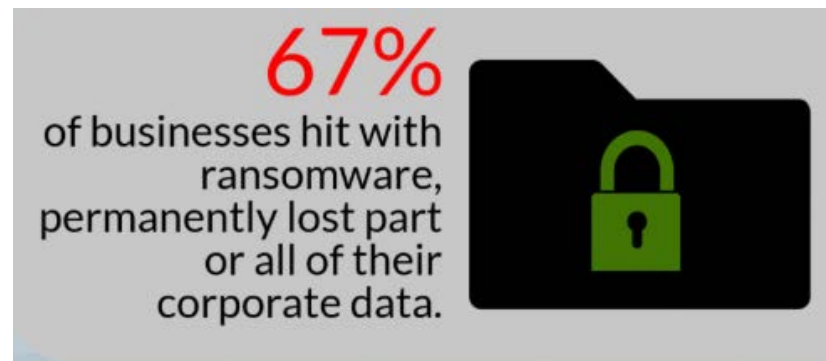
\$8B

Global Cost to Companies

Sources: Symantec Internet Security Threat Report 2018, The State of Endpoint Security Today, Sophos Survey, A Sophos Guide, Jan. 2018

Cybersecurity Landscape (Ransomware)

- Sobering statistics



Sources: Symantec Internet Security Threat Report 2018, "12 Terrifying Ransomware Statistics for 2018", Cyber Security,

Topics

- 1 Genealogy of Ransomware
- 2 Anatomy of Crypto Ransomware
- 3 Chemistry of Crypto Ransomware
- 4 HIPAA and State Law Considerations
- 5 Case Study
- 6 Future Ransomware



<https://pixabay.com/en/books-education-school-literature-484766/>

Before We Begin: Some Terminology

Ransomware <ul style="list-style-type: none">• a type of malicious software designed to block access to a computer system until a sum of money is paid.	Bad Actor <ul style="list-style-type: none">• an entity that is partially or wholly responsible for a security incident that impacts an organization's security."	Vulnerability <ul style="list-style-type: none">• a weakness or gap in our protection efforts.	Attack Campaign <ul style="list-style-type: none">• designed to bypass conventional advanced threat prevention controls and are typically executed by well-funded organizations.	Attack Vector <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.	Encryption <ul style="list-style-type: none">• data that is scrambled using an encryption algorithm and an encryption key.	Crypto Key <ul style="list-style-type: none">• a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.	Key Logger <ul style="list-style-type: none">• a software program that logs keystrokes	Cryptocurrency <ul style="list-style-type: none">• a digital currency in which encryption techniques are used to regulate the generation currency and verify the transfer of funds,

Genealogy of Ransomware

- 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

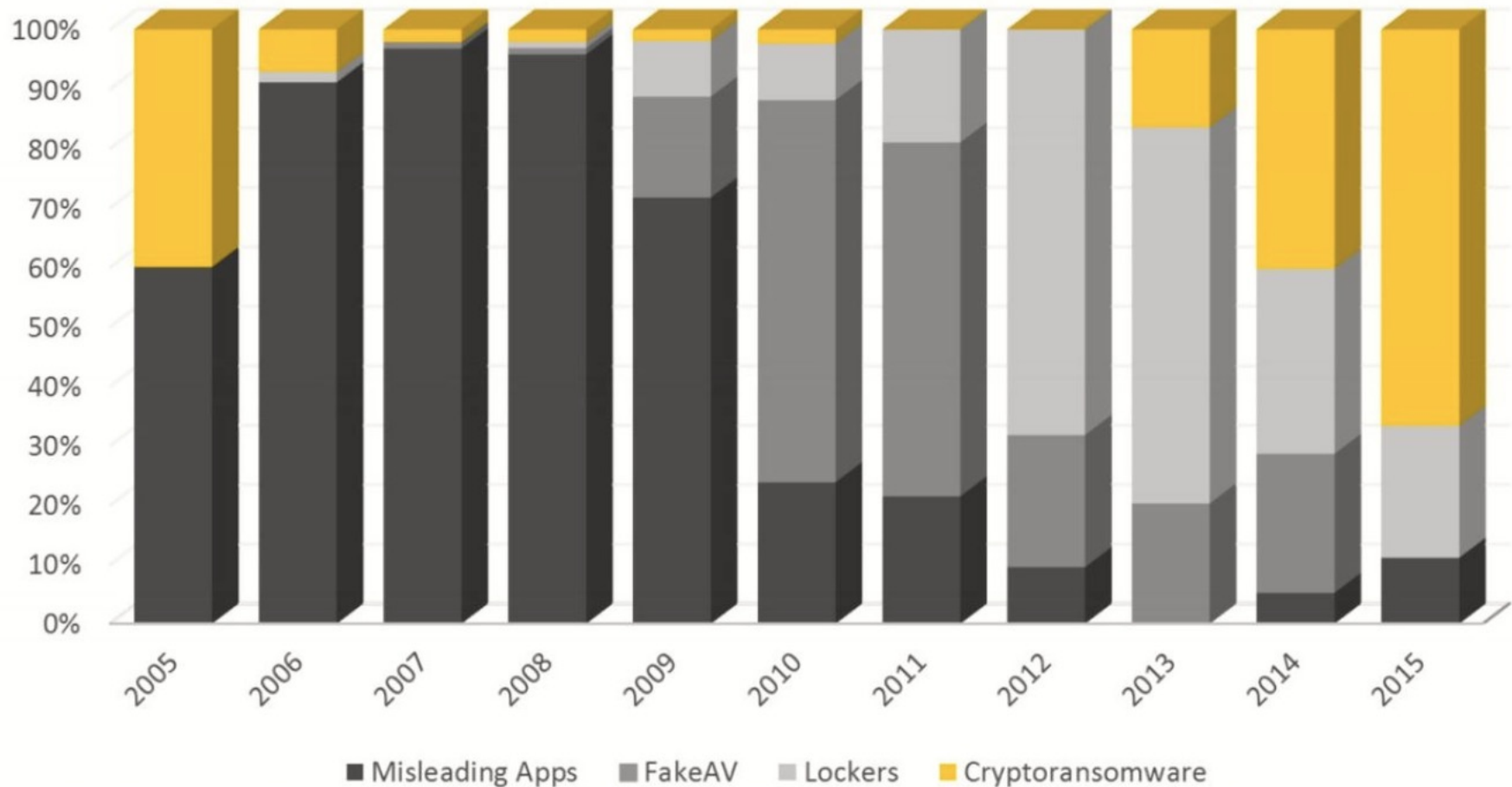


Genealogy of Ransomware

- 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

Source: <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



A percentage breakdown of new ransomware varieties by type, 2005-2015.

Genealogy of Ransomware

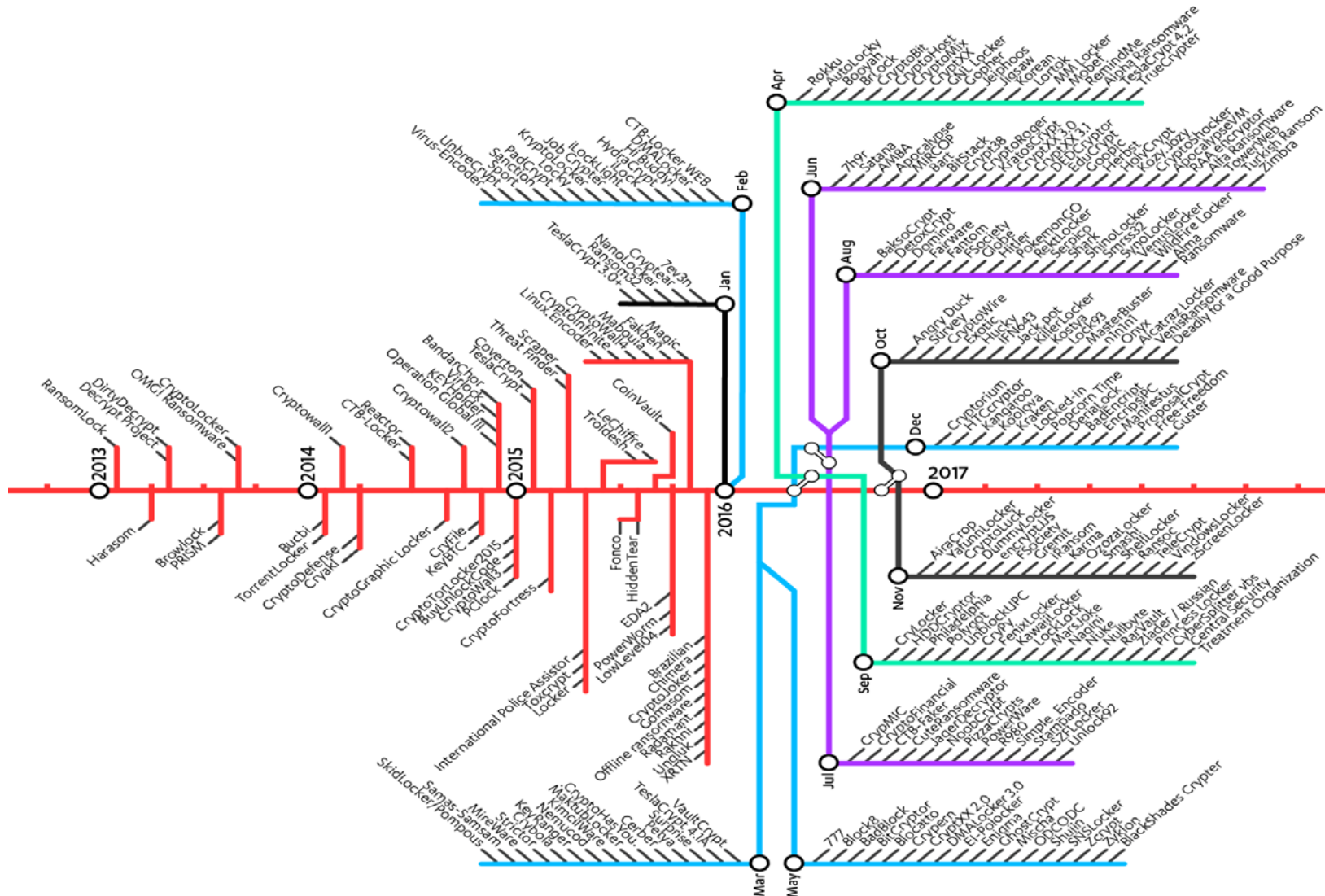
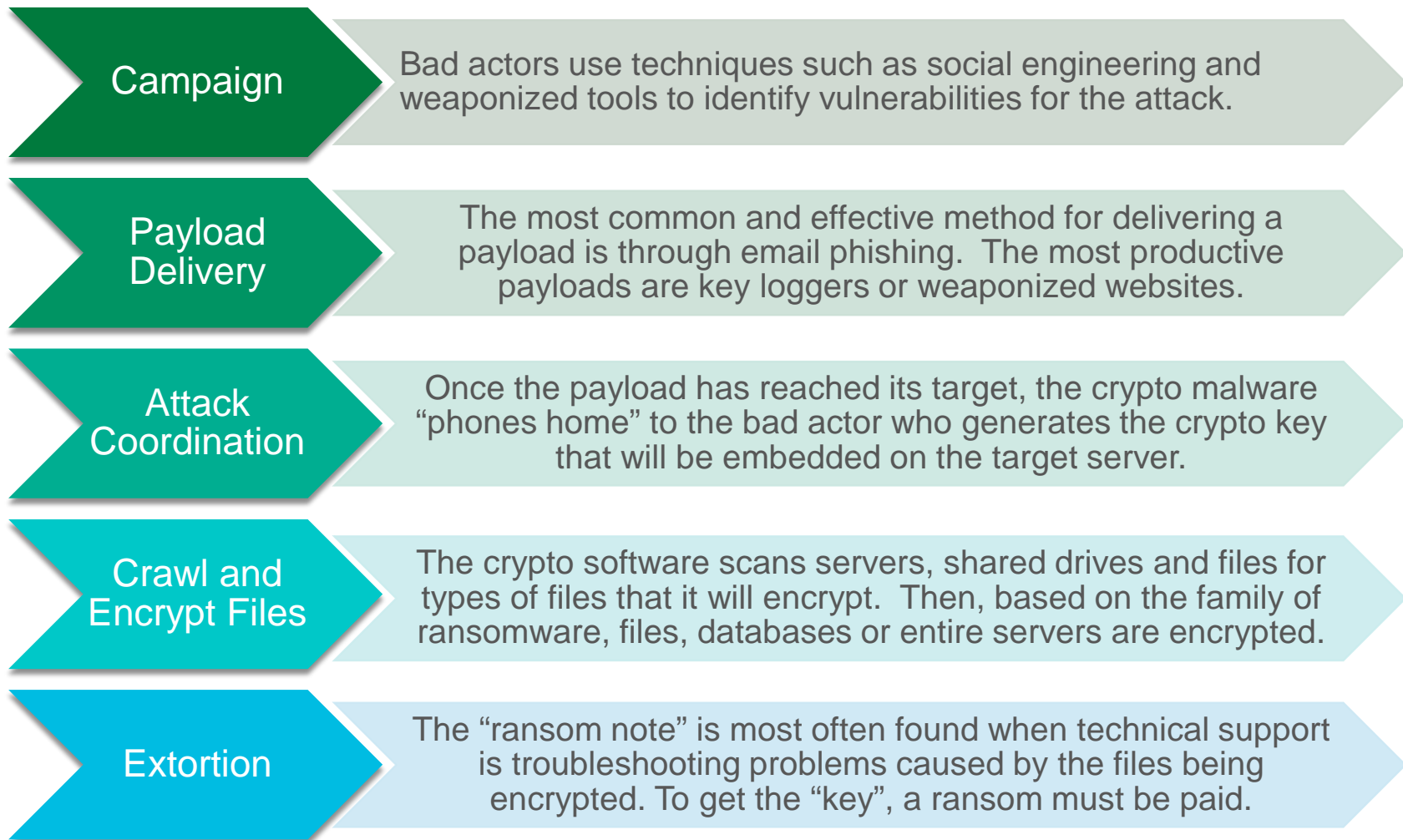


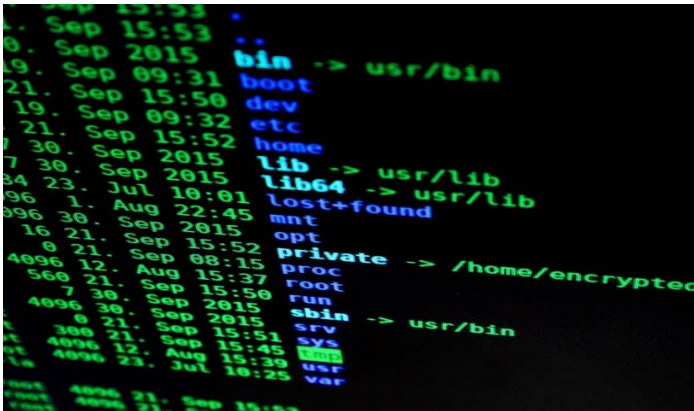
Image Source: <https://labsblog.f-secure.com/2017/04/18/ransomware-timeline-2010-2017/>

Anatomy of Crypto Ransomware



Chemistry of Crypto Ransomware

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



<https://www.pexels.com/photo/blur-bright-business-codes-207580/>

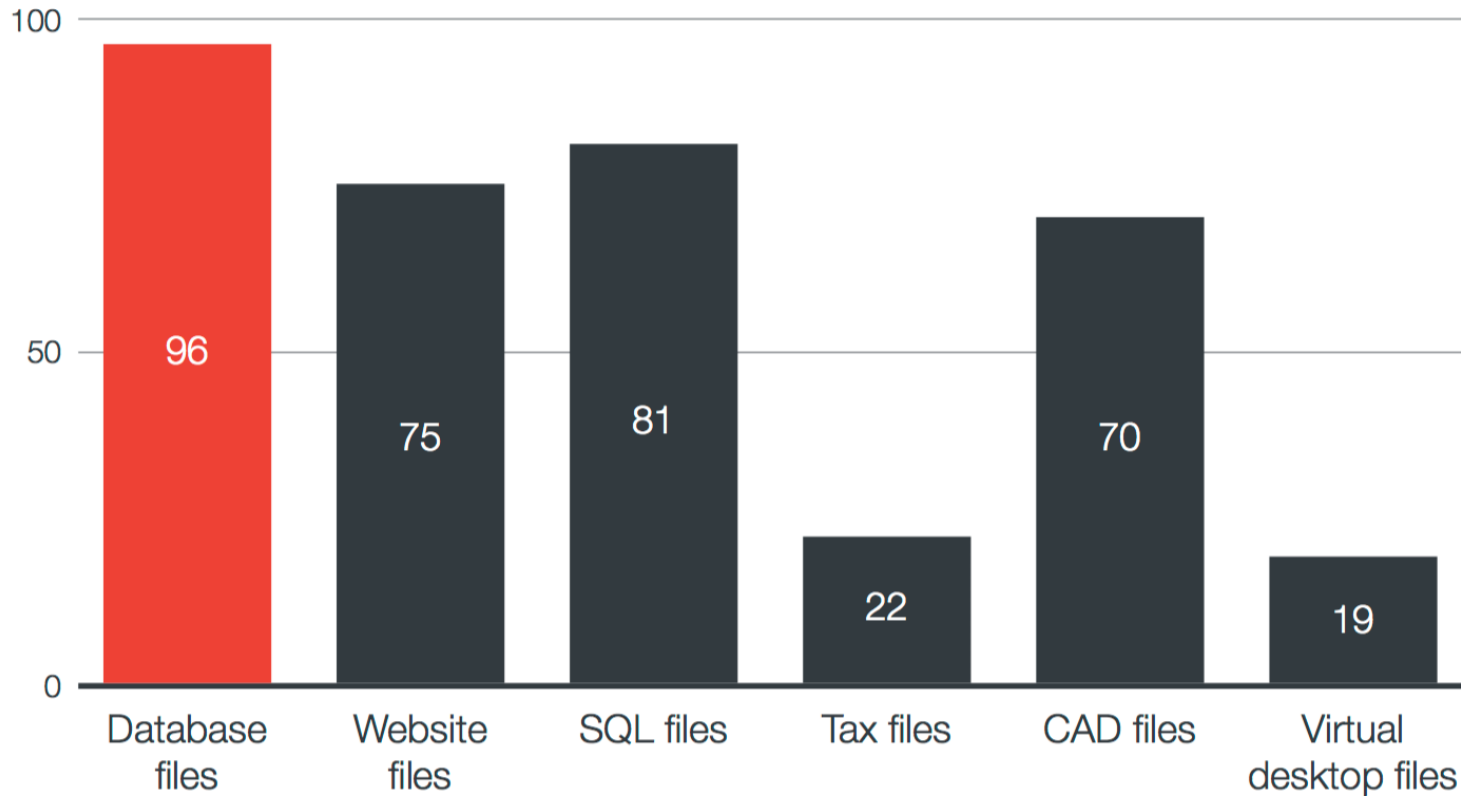


<https://www.pexels.com/photo/men-working-at-night-256219/>

Chemistry of Crypto 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.
 - 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.

Chemistry of Crypto Ransomware



Number of known ransomware families that encrypt business-related files, 2016

Image Source: <https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf>:Figure 5

Chemistry of Crypto Ransomware

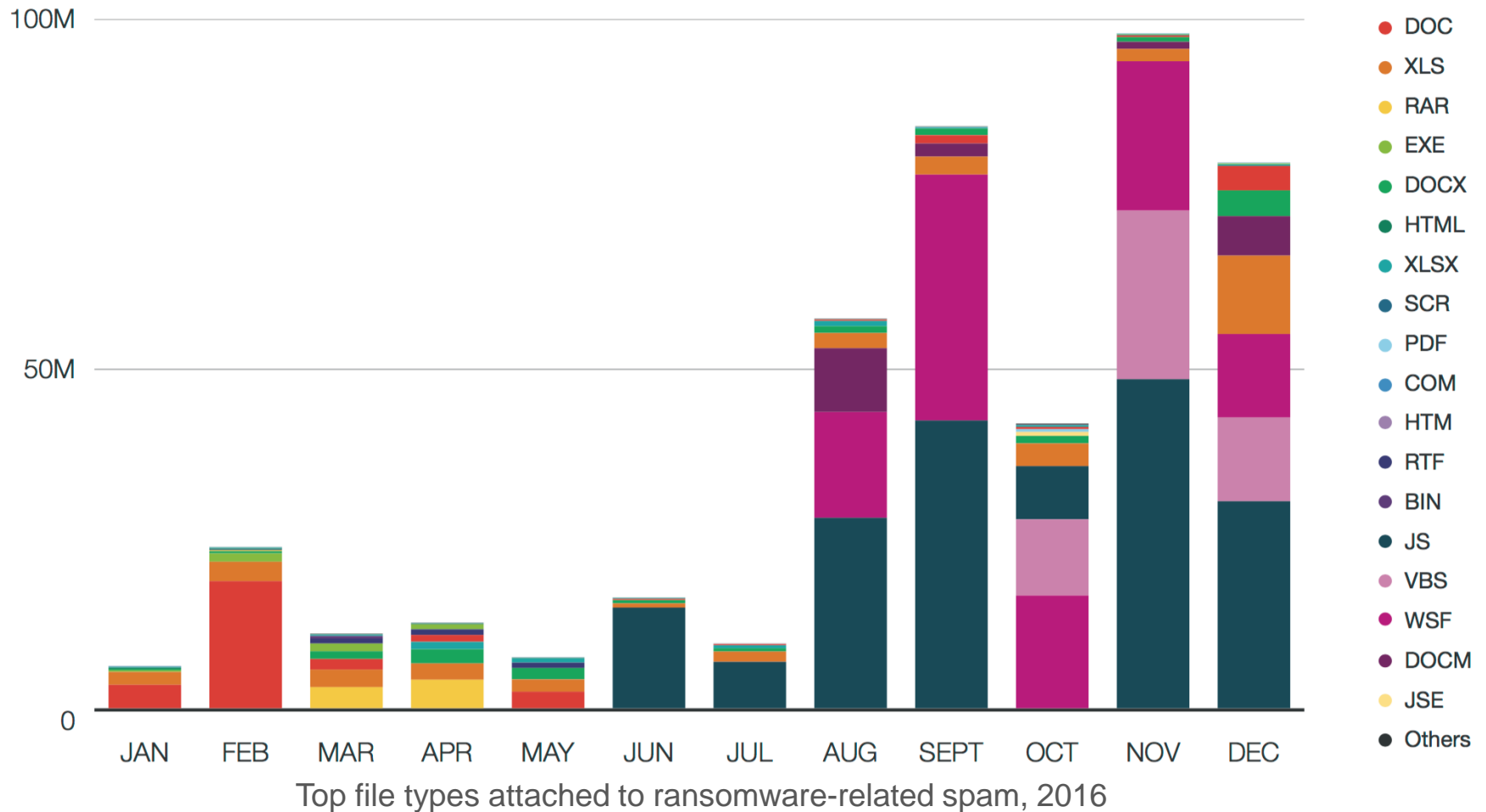
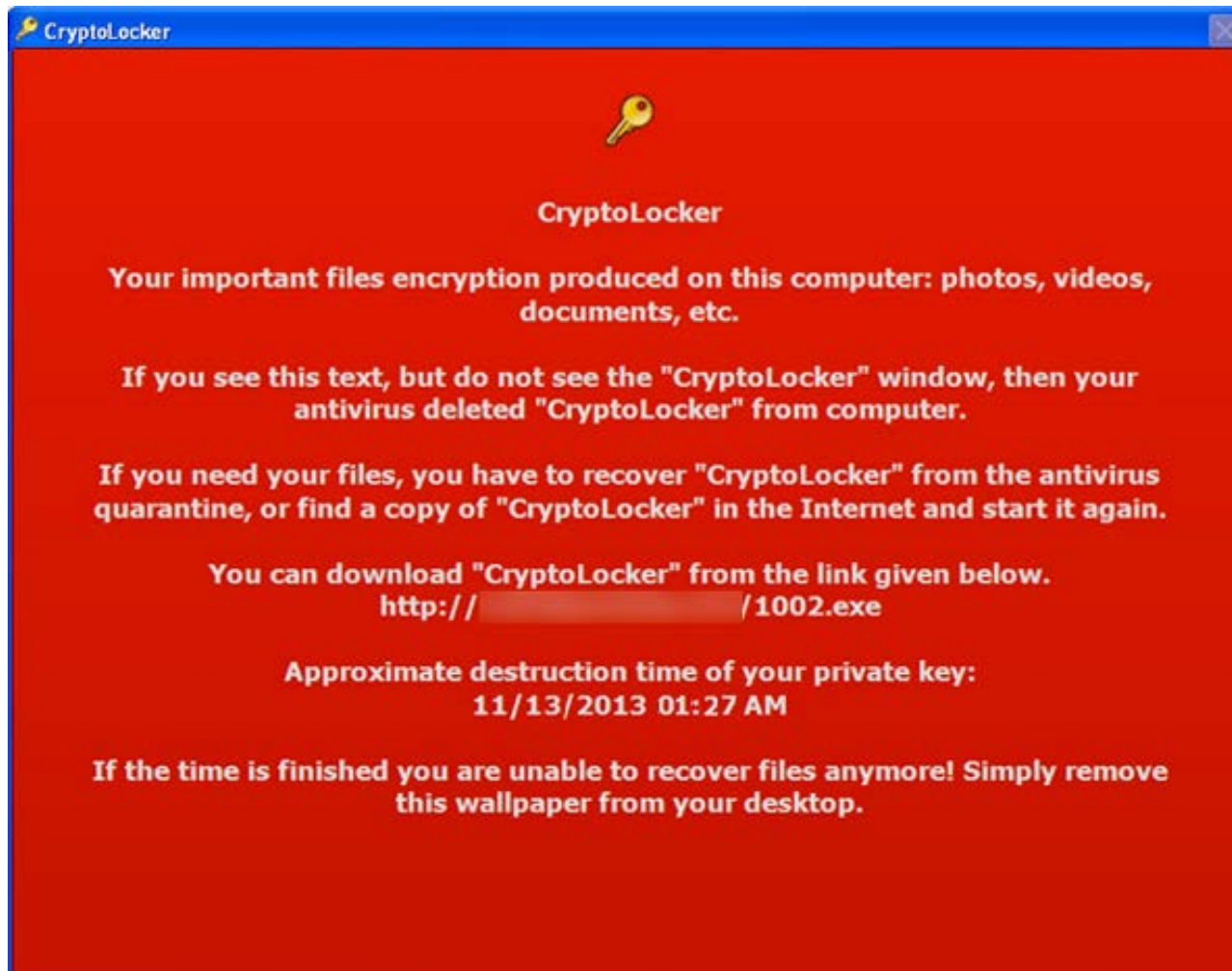


Image Source: <https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf>:Figure 4

Chemistry of Crypto Ransomware

- Sample Early Ransomware Note - 2013



Chemistry of Crypto Ransomware

■ Sample Later Ransomware Note - 2016

YOUR PERSONAL INFORMATION ARE ENCRYPTED by 7ev3n

All your documents, photos, databases, office projects and other important files have been encrypted with strongest encryption algorithm and unique key, original files have been overwritten, recovery tools and software will not help.

Private key is stored on a server and nobody can decrypt your files until you pay and obtain the private key.

You have only 96 hours to make a payment. If you do not send money within provided time, private key will be destroyed, and all your files will be lost.
Follow the instructions:

1. Pay amount of 13 bitcoin (~4980 USD) to address: 
this unique address generated only for you.

2. Transaction will take about 50 minutes to accept and confirm the payment, decryption and uninstalling of this software will start automatically. Usually decryption will take about 1-3 hours, average decrypt speed 9gb per hour.

Bitcoin is a digital currency that you can buy on 'ebay.com', 'localbitcoins.com', 'anxpro.com', 'ccedk.com' and many others online and physical exchangers through credit card, bank account, using paypal and many others payment methods.

warning, do not try to get rid of this program, any action taken will result in decryption key being destroyed, you will lose your files forever, one way to get you files is to follow the instructions. In case of non-payment reserve the right to publicly publish all encrypted files.

PRIVATE KEY WILL BE DESTROYED : 24/01/2016 24:04

Chemistry of Crypto Ransomware

- Response to Ransom ware 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

Chemistry of Crypto Ransomware

- Response to Ransom ware 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.

Chemistry of Crypto Ransomware

- Much more sophisticated and even autonomous.
 - Machine learning that embeds and makes attack decisions based on analytics gathered.
 - Minor changes to backup and recovery resources for months ending in unrecoverable backups.
 - Rifle vs. shotgun approach targeting only the most critical files.
 - Very few human factors in deployment, injection and encryption.



Image Source: <https://www.pexels.com/photo/business-businessmen-classroom-communication-267507/>

Chemistry of Crypto Ransomware

- Much more than just encrypting files
 - Imagine if payroll was held hostage or stolen
 - Malware that specifically targets payroll transactions
 - Happening in UK now
 - Trade secrets
 - Captures, encrypts and allow data owner to bid with other on release of the data
 - Happening in China now
 - Reputation ransom
 - Malware crawls for months collection every letter, photo, email, financial transaction or social media post (public and private) that might be considered unethical, immoral or illegal
 - Demands ransom with countdown before going public
 - Happening in US now (distributed through malvertising traffic and targeting Internet Explorer on Windows and Safari on OS X)

HIPAA and State Law Considerations

- OCR Fact Sheet: Ransomware and HIPAA
 - Posted July 2016
 - <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>
- OCR Discussion Points:
 - Prevention
 - Recovery
 - Detection
 - Response
 - Breach analysis
 - Unauthorized disclosure
 - Benefit of CE/BA encryption

HIPAA and State Law Considerations

- State laws
- Standard PII definition
- Expanded definitions
- Future trends?
 - North Carolina proposed legislation – Act to Strengthen Identity Theft Protections

Short Ransomware Case Study

- Entity

- US-based healthcare facility considered medium size provider
- Up-to-date antivirus
- Above average protection on firewall
- Had completed multiple risk analyses from multiple outside firms
- Had completed internal assessments
- Had completed penetration testing and vulnerability scanning

- What happened

- Random JBoss attack on known vulnerability
 - **JBoss** is an open-source, cross-platform Java application server developed by **JBoss**, a division of Red Hat Inc.
- Allowed crypto locker to gain access to JBoss server
- Impacted primary EHR, SANS, Lab Systems, Radiology Systems, ED system, OB systems, Clinic Systems and 600+ devices

Short Ransomware Case Study

- What went wrong
 - JBoss vulnerability showed up on multiple scans and reports but was not clearly understood in terms of impact and severity
 - No action was taken
 - Once attack began, focus was on who was attacking vs. limiting the exposure
 - Almost 8 hours before sr. administration involved
 - 1 week before law enforcement was involved
 - Systems down for more than 2 weeks because backup files were also impacted.
 - FBI insisted they not pay ransom
 - Had to pay after two week just to get primary clinical systems back
 - Ransom less than \$100k
 - Impact in lost revenue for two weeks undetermined
 - Insurance claim filed and partially denied

Thank you!



Robert M. Keenan III
King & Spalding, LLP
Partner, Healthcare
RKeenan@KSLAW.com

KING & SPALDING
1180 Peachtree Street, NE Suite
1600
Atlanta, GA 30309
[404. 572 .4600](tel:404.572.4600)



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


PERSHING YOAKLEY & ASSOCIATES, P.C.
800.270.9629 | www.pyapc.com