Ransomware Under The Microscope
A Closer Look

HCCA
Regional Compliance
Conference
March 2, 2018

Presented by:
Barry L. Mathis
PYA, P.C.
Consulting Principal

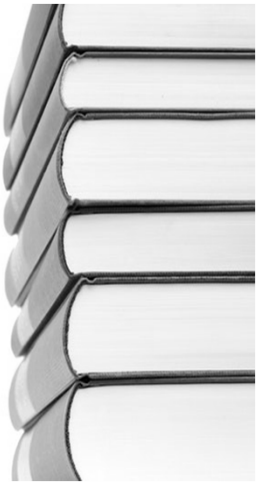
About the Speaker

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.

Topics

1. Genealogy of Ransomware
2. Anatomy of Crypto Ransomware
3. Chemistry of Crypto Ransomware
4. Future of Ransomware



Before We Begin: Some Terminology

Ransomware	Bad Actor	Vulnerability	Attack Campaign	Attack Vector
• A type of malicious software designed to block access to a computer system until a sum of money is paid.	• An entity that is partially or wholly responsible for a security incident that impacts an organization's security."	• *A weakness or gap in our protection efforts.*	• Designed to bypass conventional advanced threat prevention controls and are typically executed by well-funded organizations.	• 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	Encryption	Crypto Key	Key Logger	Cryptocurrency
• Malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.	• Data that is scrambled using an encryption algorithm and an encryption key.	• A string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.	• A software program that logs keystrokes	• 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

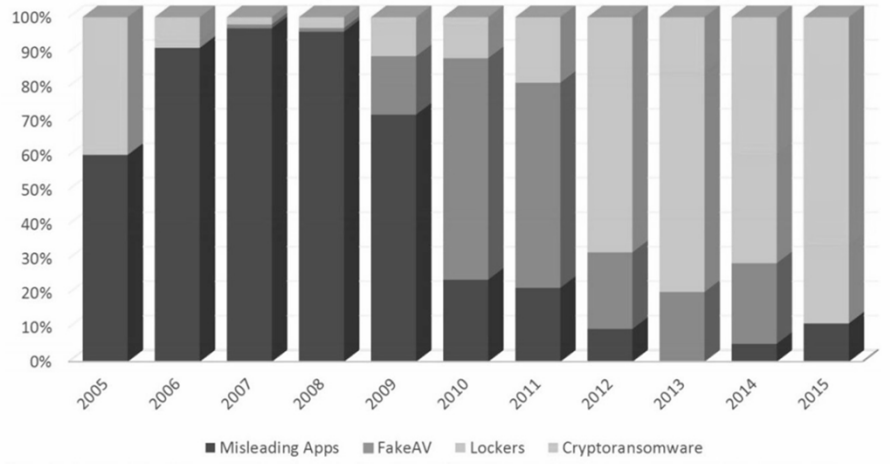
Source: https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf https://www.pexels.com/photo/grayscale-photography-of-pedestal-balustrade-161875/

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.

Image Source: http://www.latimes.com/business/hiltzik/la-fi-mh-2016-is-the-year-of-ransomware-20160308-column.html

Genealogy of Ransomware

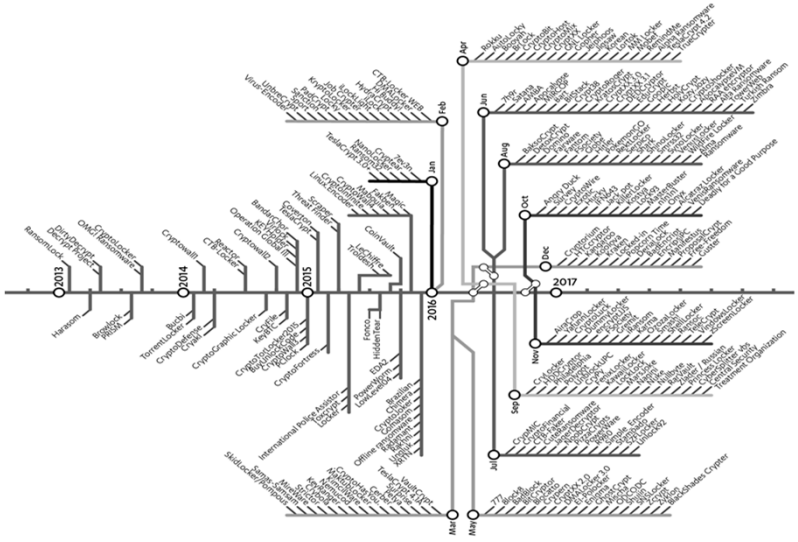


Image Source: https://labsblog.f-secure.com/2017/04/18/ransomware-timeline-2010-2017/

Anatomy of Crypto Ransomware

Campaign	Bad actors use techniques such as social engineering and weaponized tools to identify vulnerabilities for the attack.
Payload Delivery	The most common and effective method for delivering a payload is through email phishing. The most productive payloads are key loggers or weaponized websites.
Attack Coordination	Once the payload has reached its target, the crypto malware "phones home" to the bad actor who generates the crypto key that will be embedded on the target server.
Crawl and Encrypt Files	The crypto software scans servers, shared drives and files for types of files that it will encrypt. Then based on the family of ransomware, files, databases or entire servers are encrypted.
Extortion	The "ransom note" is most often found when technical support is troubleshooting problems caused by the files being encrypted. To get the "key", a ransom must be paid.

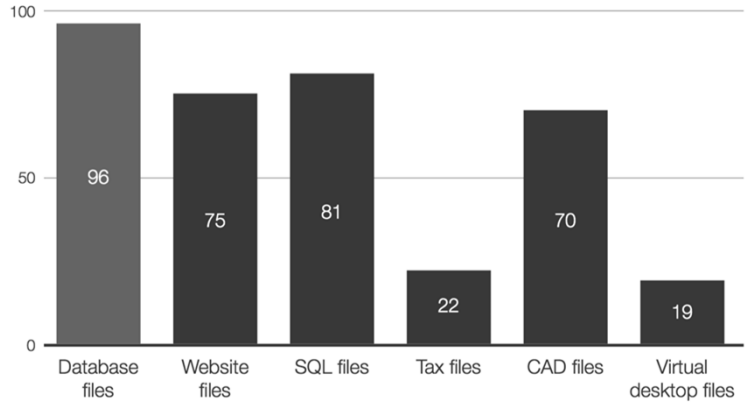
Chemistry of Crypto Ransomware

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

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 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.

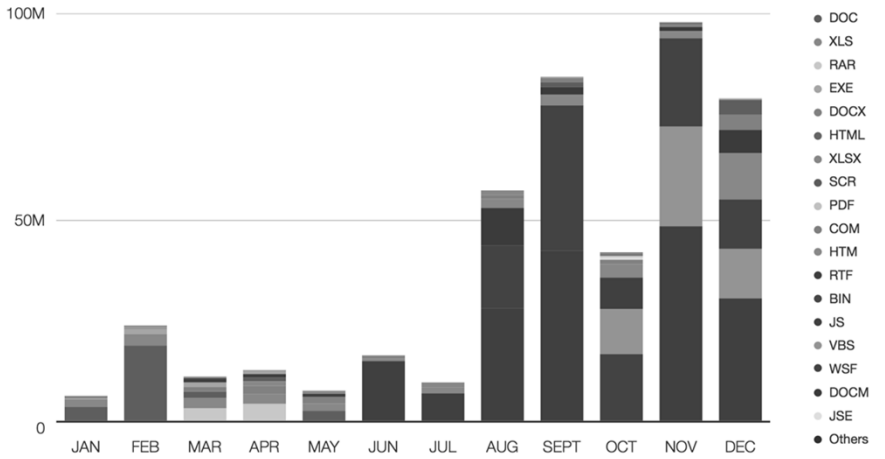
Chemistry of Crypto Ransomware



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

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

Chemistry of Crypto Ransomware



Top file types attached to ransomware-related spam, 2016

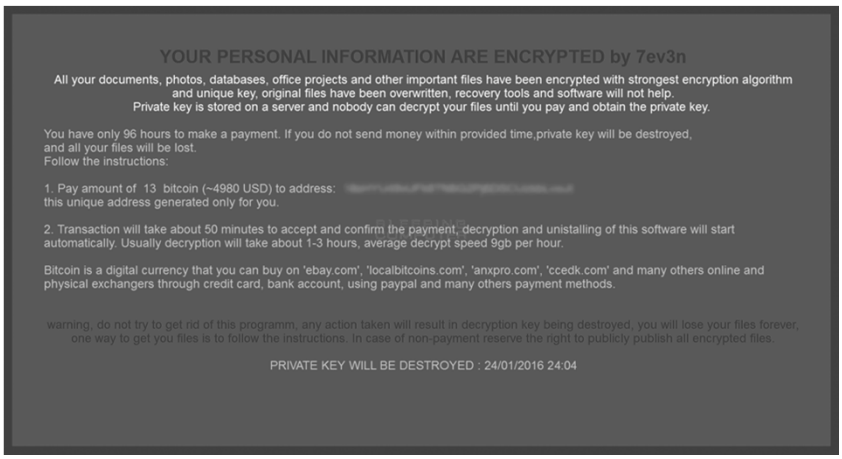
Image Source: https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf:Figure 4

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: [redacted]
this unique address generated only for you.

2. Transaction will take about 50 minutes to accept and confirm the payment, decryption and unistalling 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 programm, 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 craws 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)

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

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 Analysis 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

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

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

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

Thank you!

Barry L. Mathis
Principal
bmathis@pyapc.com

PYA, P.C.
800.270.9629 | www.pyapc.com

ATLANTA | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA