Protecting Your Firm from Ransomware Attacks

Jason McNew
John Simek
What is ransomware?
Is ransomware always a data breach? Do you have to report it under data breach notification laws? Do you have to tell your clients?
First Ransomware

- Appeared in 1989
- PC Cyborg
- Hid folders
- Encrypted files on C:
- $189/$378 ransom
- Distributed via floppy disc
- Healthcare industry
- 90 computer boots
2017 Verizon data breach report

• 42,000 security incidents, nearly 2,000 breaches, 84 nations
• 61% of victims have fewer than 1,000 employees
• 1 in 14 users fall for phishing e-mails. 25% of them fall more than once
• 51% of breaches involved malware. Ransomware now the 5th most common form of malware and the first in what the report calls the Crimeware pattern
• 66% of malware installed via malicious e-mail attachment
• 62% of breaches involved hacking

“I suppose I’ll be the one to mention the elephant in the room.”
2017 Internet Security Threat Report

• April 2017 from Symantec
• In 2016, average ransom demand $1,077, up from $294 in 2015
• 36% increase in ransomware in 2016 over 2015
• Ransomware kits $10 - $1,800
• Exploit kits on compromised website – exploits your browser vulnerabilities to deposit ransomware
2017 Internet Security Threat Report

• In 2016, only 34% of victims paid ransom
• 47% of those got the decryption key
• Primary business target? SMBs
• High value data
• Far less data protection than larger entities
2017 – The Year of Ransomware

• Consumer attacks up more than 93%
• Business attacks increased 90%
• September 2017 – 700% increase over 2016
• Three major outbreaks
  • WannaCry
  • NotPetya
  • BadRabbit
How Is Ransomware Delivered?

- Malicious links
- Malicious attachments
- Phishing attacks
- Lateral spread
- Smishing
Attack Vector

• Local drives
• External USB drives
• Network shares
• Mapped drives
• Boot sector
• Cloud storage
Cloud Applications not Immune

- 42% of MSPs report infection
- Dropbox – 76%
- Office 365 – 32%
- G Suite – 21%
- Box – 5%
- Salesforce – 2%
So what is the motive?

• Usually, financial gain
• Can be political (WannaCry)
• Cryptocurrency manipulation
• Disguise other activities
• Vandalism
RaaS – Ransomware as a Service

• Sales
• Support
• Updates, too!
RaaS – Ransomware as a Service

- Sales
- Support
- Updates, too!

Features

- Packages are compiled with your Bitcoin and Email addresses so you are paid directly by your victim
  - Each package also supports Testnet mode, so you can test the ransomware in a virtual machine before distribution
- Packages utilize advanced polymorphic techniques to avoid over 90% of popular antivirus products
- Packages do not require Administrative privileges to work, and they also support Started Delay, Mutex, and Task Manager Disabler
- Packages encrypt the most common sensitive file types, such as images, documents, videos, and source code.
  - Additional file types can be specified during package creation
- Packages can work entirely offline, but your victim must be connected to the Internet for decryption to occur
  - If your victim is offline when encryption begins, the AES key will be encrypted to the local disk using the C&C server's public key
  - Once an Internet connection is detected, the AES key will be uploaded to the C&C server and then deleted from disk
- Every package supports automated decryption after your victim pays. This works as follows:
  - You specify the base amount, i.e., 0.5 BTC
  - The package randomly generates a unique amount to add, i.e., 0.00058213 BTC
  - The victim pays the ransom of 0.50058213 BTC
  - The C&C server scans transactions to your BTC address and when it detects this amount, it will unlock the AES key for that victim
  - The ransomware on the victim's computer will begin automatically decrypting their files
Detection

- Hard disk activity
- Visual message
- File extensions
- Inaccessible files
Prevention

• Security software
• Cryptoprevent
• White listing
• Restrict application installation
• Install updates
You don’t have to be a big firm to get ransomware

- $1200 and $3000 – small firm ransom payments
‘Cryptolocker’ Virus Holding Law Firm Data For Ransom

By Y. Peter Kang

Law360, Los Angeles (March 9, 2015, 6:49 PM ET) -- A California law firm was the victim of a “Cryptolocker” cyberattack in which unknown hackers attempted to hold data for ransom, according to a notice recently filed with the California Attorney General’s office.

Ziprick and Cramer LLP reported the breach to the attorney general’s office on March 2. In late January, hackers used malicious software believed to be a new variant of Cryptolocker, a type of “ransomware” that encrypts files on a victim’s computers until they pay a ransom, according to a Feb. 27 letter sent to clients. Typically, if the ransom is not paid, the hackers then destroy the data.

The virus infected an attorney’s work computer possibly through a phishing email and made its way to an in-house server containing client information, said the Redlands, California-based firm, which contacted the FBI and brought in a specialist to assess the situation.
Law Firm Sues Insurance Company over Ransomware

• The Providence Journal reported May 2017
• Moses Afonso Ryan Ltd sued Sentinel Insurance Co. - breach of contract and bad faith
• Denied the firm's lost billings claim ($700,000) over 3 months when documents were encrypted by ransomware – 10 lawyers could barely work
• Criminal demanded $25,000 in bitcoin for decryption key – law firm paid - had to re-negotiate after the initial decrypt key failed to work
• Insurer: Only coverage for loss or damage caused by a computer virus was under one clause – paid maximum amount of $20,000 – additional coverage for physical damage to computers but not for data damage
• Therefore business losses not covered. Suit ongoing
If it could happen to DLA Piper . . .

• One of the largest firms in the world, #1 by revenue
• June 27, 2017 – e-mail and phones down, some of their network – some computers shut down as a precaution
• GoldenEye/NotPetya malware – appeared at first to be ransomware, real intent to destroy data (exploited NSA tools published by the Shadow Brokers)
• July 3rd statement – e-mail back up, bringing up other systems
• Mum as to source of problem
May 12, 2017 – 12 countries and 16 UK health institutions hit!

• British National Health Services – hospitals - other facilities
• Exploited vulnerability in Microsoft software discovered by the NSA and stolen by the “Shadow Brokers” who dumped NSA hacking tools online
• Microsoft had a patch (MS17-010) but many hadn’t updated
WannaCry Ransomware Worm

- No user action to launch
- 1 million IP addresses open to port 445
- SMB v1 vulnerability
- Unpatched Windows 7
- 200,000 computers hit in 150 countries
- Penetration, Deployment, Crypto
- $70,000+ in BTC payments
Anatomy of a ransomware attack – from discovery to surrender

Marika Samarati | August 11, 2016

Have you ever been in a situation where your company was hit by ransomware? Watch the video Turn the Lights on Ransomware, filmed by Trend Micro, to discover how ransomware hit a company and how they coped with it.

Ransomware

- How do you get your data back?
- How do you engineer backups that are impervious to ransomware?
- FBI says it is 1 BILLION dollar a year business
Ransomware

- CryptoLocker & variants
- Attacks logical drives
- Encrypts data
- Ransom payment
- Bitcoin
- Decryption key
- How backup has changed
Ransomware attacking mobile devices

• Began in 2015 and growing
• Downloading apps from unsanctioned app stores
• One example: SimpleLocker
  • Runs until all data on phone is encrypted
  • Sets a time limit for payment
  • No payment? All files erased
Locky

- Constantly changing
- First used Word macro
- Second most prevalent (11/2016)
- Offline encryption (no C&C)
- Delivered via e-mail attachment
- 30 different languages
- Unique RSA keys per machine
CryptoWall

- Started as CryptoLocker
- Regularly updated
- Scrambles file names
- Deletes system restore points
- Delivered as zipped attachment
Cerber Ransomware

- Dodges machine learning
- Separate “harmless” components
- Dynamically injects into a running process
- Distributed via e-mail link
- Self-extracting Dropbox file
- Checks if running in a sandbox
Ransomware Impact

• Payment
• Loss of data – 15% unrecoverable
• 85% infected – offline for at least a week
• Loss of client trust
Financial Impact of NotPetya

• Nuance Communications
• 2017 NotPetya attacks – lost $98 million in revenue
• Increased loss going into 2018
• Primarily healthcare
• Transcription services
• Attack started 6/27/2017
• Final recovery 8/4/2017
Latest Generation Ransomware

- Annabelle ransomware
- Autostart on Windows login
- Terminates Process Hacker, Process Explorer, Msconfig, Task Manager, Chrome, etc.
- Configures Image File Execution registry entries – prevents launching Notepad++, Notepad, IE, Chrome, etc.
- Attempts to spread using autoru.inf files
Annabelle Ransomware

• Encrypts with static key
• Appends .ANNABELLE extension to file name
• Reboots computer
• Upon login – lock screen launched
• Replaces master boot record
Never Seen Features

- GandCrab ransomware
- First to use DASH
- Uses high-level domain NameCoin.BIT
- .bit domains used by C&C servers
- Decryption tool available at No More Ransom
Identification

- Nomoreransom.org
- ID Ransomware
  - [https://id-ransomware.malwarehunterteam.com/](https://id-ransomware.malwarehunterteam.com/)
  - Ransom note
  - Sample encrypted file
  - E-mail address
Redesigning Backups

• Hard drive based
• Encrypted
• Off-site transmission
• Cloud
• Backup agents
• Virtual machines
Ransomware Detection Programs

• Trend Micro RansomBuster
• Bitdefender Anti-Ransomware Tool
• Cybersight RansomStopper
• Cybereason RansomFree
• Windows Defender
Decryption tools

- Kaspersky
  - [https://noransom.kaspersky.com/](https://noransom.kaspersky.com/)
- McAfee
- Avast
  - [https://www.avast.com/ransomware-decryption-tools](https://www.avast.com/ransomware-decryption-tools)
NEED HELP unlocking your digital life without paying your attackers?*

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

https://www.nomoreransom.org/
Best Practices

• Disable macros
• Apply patches and software updates
• Run in least privilege mode
• Train end-users about malware
• Encourage users to report ransomware infections
• Limit BYOD – approved devices and policies
• Test backups
Bitcoin

- Open source
- Real value
- 1 bitcoin = $10,601.7 on 2/28/18
- German ruling
- Banned in Thailand
- Regulated financial instrument? Yup.
- $1 billion lost in attack on BIPS, a Bitcoin processor – Nov. 2013
- BitStamp $5.4 million – Jan. 2015
- June 2016 BTCC introduced new physical titanium bitcoins with private key with one bitcoin attached
- Coincheck $500 million in cryptocurrency – Dec. 2017
How do you get virtual currency?

• Private transaction
• At an exchange
• Peer-to-peer – e.g. paid for work completed directly from a crypto wallet
• By mining (processing transactions) for which you are paid
• ATM
What is blockchain?

• The equivalent of a ledger in the paper word
• Records all sales
Ransomware Payments

- EFT
- Wire transfer
- Cash
- ATM

https://coincafe.com/

Bitcoin Delivery Times and Fees

Background:
We ran a fee-free service for months, but now we have to start charging for our service as the reality of hundreds of thousands of hits on our web server and our ability to pay rent on our retail location in New York City has sunk in.

We still believe in the powerful potential of cryptocurrency and want to help as many regular folks obtain Bitcoins as possible.

Thanks so much for supporting us in our mission!

-Coin Cafe Team

Bitcoin Delivery Times and Fees

*Click for high-volume rates
(Also, email us for our preferred service plan for high-volume clients and resellers.)

<table>
<thead>
<tr>
<th>Method</th>
<th>Coin Cafe Fee</th>
<th>Bank Fee</th>
<th>Delivery Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Bank Transfer</td>
<td>1.90%</td>
<td>$0 Bank fee</td>
<td>2-4 Days (priority last name applies)</td>
</tr>
<tr>
<td>Wire transfer</td>
<td>*4.95%</td>
<td>$10 incoming wire fee</td>
<td>Same or Next Business Day after the transfer is received</td>
</tr>
<tr>
<td>Cash via FedEx, UPS, USPS, etc.</td>
<td>6.95%</td>
<td>-</td>
<td>Same Business Day we receive your payment</td>
</tr>
<tr>
<td>Cash In Person</td>
<td>6.95% + $15 appointment fee</td>
<td>-</td>
<td>Immediate New York City only</td>
</tr>
<tr>
<td>Cash at Bitcoin ATM</td>
<td>6.95%</td>
<td>-</td>
<td>Instant New York City only</td>
</tr>
</tbody>
</table>

https://coincafe.com/
Questions?
• YOU play the most important part in keeping TECHSHOW exciting. *Please complete the Speaker evaluation before you leave.*

• Reserve the dates!

TECHSHOW 2019: February 27 – March 2, 2019