

The Ransomware Epidemic and How to Protect Your Law Firm



ransomware

PRESENTERS:

Sharon D. Nelson, Esq. & John W. Simek
President and Vice President, Sensei Enterprises
703-359-0700 www.senseient.com @sharonnelsonesq

DC Bar – May 19, 2017

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?



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





- Wana Decrypt0r 2.0 (WannaCry) variation, ransom - \$300 in bitcoin
- Life and death implications
- Clock counting down – three days – then ransom doubled – after seven days, files can't be recovered

WannaCry Ransomware Worm

- No user action to launch
- 1 million IP addresses open to port 445
- SMB v1 vulnerability
- Windows XP
- 200,000 computers hit in 150 countries
- Penetration, Deployment, Crypto
- \$70,000+ in BTC payments



You don't have to be a big firm to get ransomware

- \$1200 and \$3000 – small firm ransom payments



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 Verizon data breach report



- 80% of hacking breaches - stolen passwords and/or weak passwords
- 75% of breaches - outsiders and 25% insiders
- 18% state-affiliated actors
- 51% organized criminal groups
- 73% of breaches financially motivated
- 21% of breaches - espionage
- 27% discovered by third parties

'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.

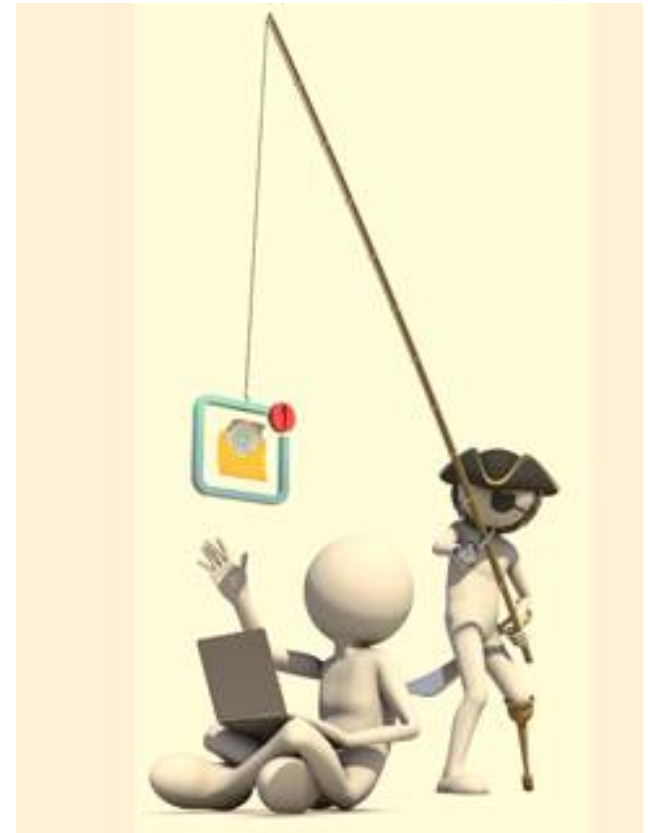
Law Firm Sues Insurance Company over Ransomware



- *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

91% of hacking attacks begin with a phishing e-mail

- 2016 PhishMe study
- Why do users click?
 - Curiosity (racy New Year's photos)
 - Fear (bar complaint attached)
 - Urgency (boss needs this today)
 - Recognition (award you've gotten)
- SonicWall and OpenDNS
- One phishing simulation (reported to employees) drops risk of phishing success by 20%



How do you spot phishing e-mails?

- Meant to induce curiosity, fear, urgency – appeal to vanity
- One letter/number off
- You weren't expecting the e-mail
- No substantive text/poor English
- Hovering over link doesn't always tell you where it goes!
- Think before clicking – pick up phone
- Give employees phishing "tests"
- Report the results



Fake LinkedIn Email (now with Malware)

From: linkedin.com <message-wk881425ffjm55@linkedin.com>
Subject: **Mark Andronas at Payroll Processing wants to connect on LinkedIn**
Date: June 2, 2011 12:55:01 PM GMT+03:00
To: Mickey Boodaei
Reply-To: message-wk881425ffjm@linkedin.com

LinkedIn

I'd like to add you to my professional network on LinkedIn.

- Mark Andronas

Neal Collins
Vice President, Strategy & Corporate Development at Payroll Processing
Greater Chicago Area

Confirm that you know Neal

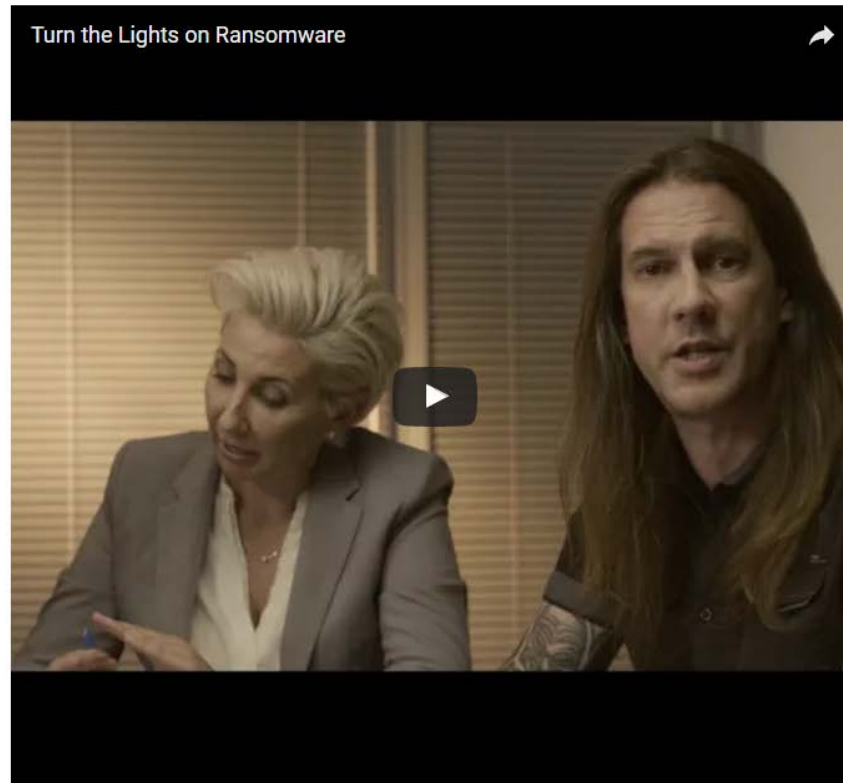
© 2011, LinkedIn Corporation

5 ½ minutes
Trend Micro

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.



It started with a targeted phishing attack

<https://www.itgovernanceusa.com/blog/anatomy-of-a-ransomware-attack-from-discovery-to-surrender/>

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

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: 2675401919

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

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



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

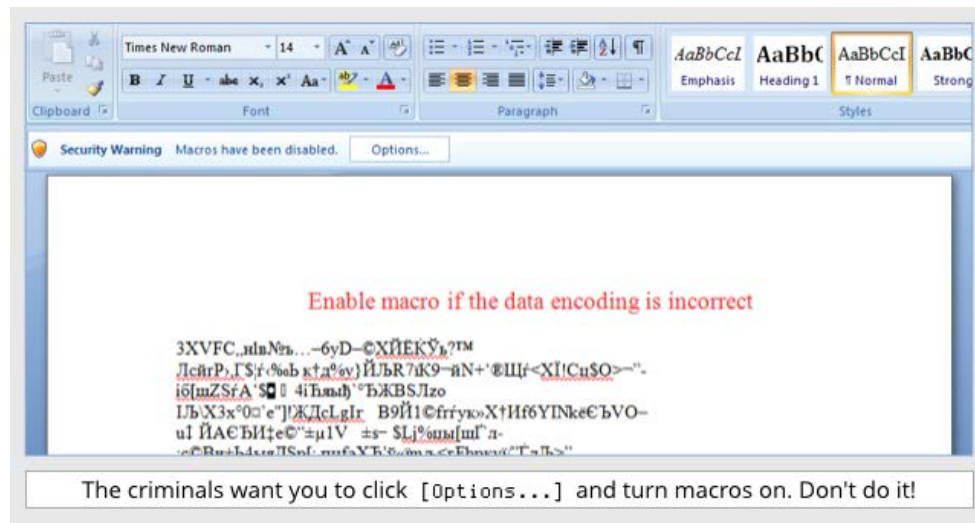
Ransomware

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



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

Your files are encrypted.
To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **20/01/15 - 16:13** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:
167h 59m 00s

Your system: Windows XP (x32) First connect IP: [redacted]  Total encrypted 2860 files.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
[How to buy CryptoWall decrypter?](#)

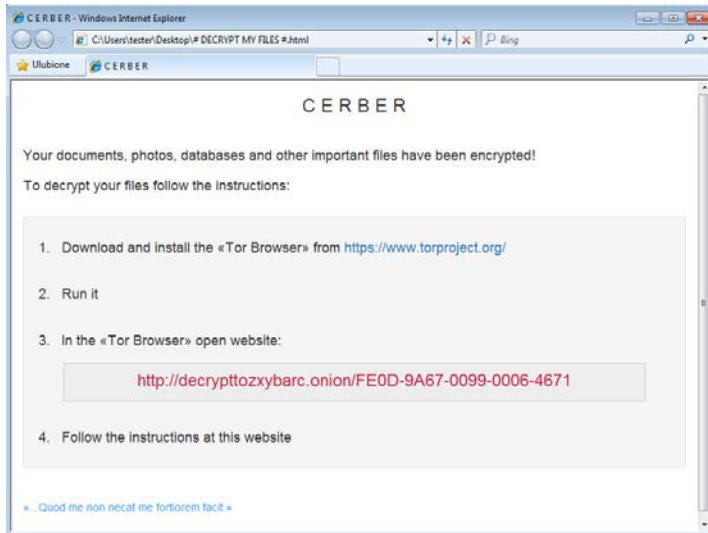


1. You should register Bitcon wallet ([click here for more information with pictures](#))

2. Purchasing Bitcoins. Although it's not yet easy to buy bitcoins, it's getting simpler every day.

- 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 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



Bitcoin

- Open source
- Real value
- 1 bitcoin = \$1,735.11 on 5/10
- 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



Commemorative Bitcoin



- Amazon Prime
- \$7.97
- .999 Gold plated

How do you get bitcoins?

- 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 a block chain?

- The equivalent of a ledger in the paper word
- Records all sales



Banks moving to block chain technology (not necessarily bitcoin transactions)

- 2016 -Citibank, Santander, Wells Fargo, HSBC, JP Morgan Chase, Bank of America, etc. working on block chain tech
- Make banking processes more efficient, timely and secure - decreasing transaction times, self-automating smart contracts, lowering transaction costs, minimizing fraud



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.](#))

Method	Coin Cafe Fee	Bank Fee	Delivery Time
Electronic Bank Transfer	1.95%	\$5 Bank fee	2-4 Days <small>(Priority Surcharge Applies)</small> 5-10 Days
Wire transfer	*4.95%	\$10 incoming wire fee	Same or Next Business Day after the transfer is received <small>Priority Service Available</small>
Cash <small>via Fedex, UPS, USPS, etc.</small>	6.95%	-	Same Business Day we receive your payment <small>Priority Service Available</small>
Cash in Person	6.95% <small>+ \$19 appointment fee</small>	-	Immediate <small>New York City only</small>
Cash at Bitcoin ATM	6.95%	-	Instant <small>New York City only</small>

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

Ransomware Impact

- Payment
- Loss of data – 15% unrecoverable
- 85% infected – offline for at least a week
- Loss of client trust



Redesigning Backups



- Hard drive based
- Encrypted
- Off-site transmission
- Backup agents
- Virtual machines

NEED HELP unlocking your digital life
without paying your attackers*?

YES

NO

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/>

Questions?

