

CRYPTOLOCKER

“The bleppiest virus of 2013” –Reddit user bluesoul

Andrew Tarrh
Ashley Hansberry
Allan Lasser

CS558
Network Security
2/20/14



Search 11°

Sign Up for Newsletters
Contests Your Home More

LOGIN REGISTER

Home News Sports Weather Traffic Health Boston's Best Video Audio Events Places Travel Deals Circulars Autos

Local Politics Business Health Education Consumer News

WINTER OLYMPICS: News | Results | Event Schedules |

Local

Cryptolocker Ransomware Being Described As 'The Perfect Crime'

By Chief Correspondent Joe Shortleeve, WBZ-TV

December 18, 2013 5:34 PM

Like 4.5k Tweet 290 Share 1K

Related Tags: CBS Boston, Cryptolocker ransomware, Joe Shortleeve, WBZ



Joe Shortleeve
Joe Shortleeve is chief correspondent for WBZ-TV News weekdays a... [Read More](#)



KGO-TV SAN FRANCISCO, CA

HOME

ABC7 NEWS

UREPORT

MOST POPULAR

SAN FRANCISCO

EAST BAY

SOUTH BAY

PENINSULA

NORTH BAY

CALIFORNIA

NATIONAL/WORLD

7 ON YOUR SIDE

I-TEAM

ASSIGNMENT 7

POLITICS

ENTERTAINMENT

ABC7 SPORTS & ESPN

BREAKING NEWS ▶ Amber Alert issued after carjacking, abduction at Safeway in Oakland

LIVE STREAM ▶ Watch here: ABC7 News at 11 p.m. | Watch on a mobile device

Enter search phrase

SEARCH

SEE IT ON TV? CHECK HERE

FOLLOW US



Technology

Computer virus 'CryptoLocker' kidnaps files, holds them for ransom

Friday, January 31, 2014

Share this Story

Recommend 241 people recommend this. Be the first of your friends.

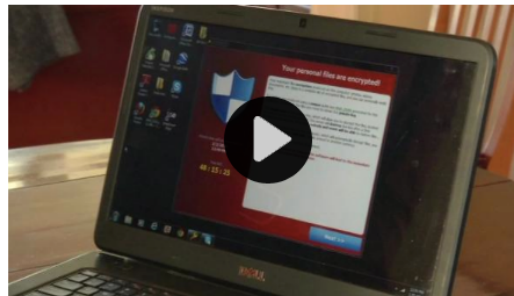
Tweet 29

+22 Recommend this on Google

News Headlines

Video

abcNEWS



EMBED

TAGS: hacking, websites, internet, technology, jonathan bloom

Comment Now Email Print Report a typo



Jonathan Bloom

More: Bio, E-mail, Facebook, Twitter, News Team

MILL VALLEY, Calif. (KGO) -- A ruthless computer virus discovered last September is still terrorizing users, and now is making millions off them in the

- Amber Alert issued after carjacking, kidnapping
- Richmond man sentenced for keeping sex slave
- New Willie Brown signs unveiled on Bay Bridge
- Lone 49ers teen receives generous donations
- Antolin Garcia-Torres indicted in Sierra LaMar's murder
- Google expanding presence to Moffett Field
- Wire fox terrier wins best in show at Westminster
- Graco recalling nearly 3.8 million child car seats
- San Jose councilmember donates stem cells to kid 33 min
- House passes debt ceiling increase
- FBI cracking down on lasers shined at aircrafts
- WEATHER: Bay Area weather forecast for Wednesday
- Get WATCH ABC for your mobile device
- ROUNDUP: New massage rules; Oakland homicide

MORE: Contact ABC7 | Watch ABC | ABC7 Mobile Apps |

Your personal files are encrypted!



Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount in another currency**.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>

HOW CRYPTOLOCKER WORKS

1. Affects Windows versions XP through 8
2. Encrypts data files using RSA and AES encryption
3. Once encryption is finished, a pop-up asking for \$100 or \$300 in Moneypack or 2 bitcoins (BTC)
4. User must pay in time in order to decrypt their files
5. If not paid within 72 hours, you pay much more



A TYPICAL CRYPTOLOCKER ATTACK



Infection



Encryption



Decryption

“I know this thing sucks and
all, but it is **really** well done”

—Reddit user olithraz



Infection

Common email subjects

USPS - Your package is available for pickup (Parcel 173145820507)	USPS - Missed package delivery ("USPS Express Services" <service-notification@usps.com>)
USPS - Missed package delivery	FW: Invoice <random number>
ADP payroll: Account Charge Alert	ACH Notification ("ADP Payroll" <*@adp.com>)
ADP Reference #09903824430	Payroll Received by Intuit
Important - attached form	FW: Last Month Remit
McAfee Always On Protection Reactivation	Scanned Image from a Xerox WorkCentre
Scan from a Xerox WorkCentre	scanned from Xerox
Annual Form - Authorization to Use Privately Owned Vehicle on State Business	Fwd: IMG01041_6706015_m.zip

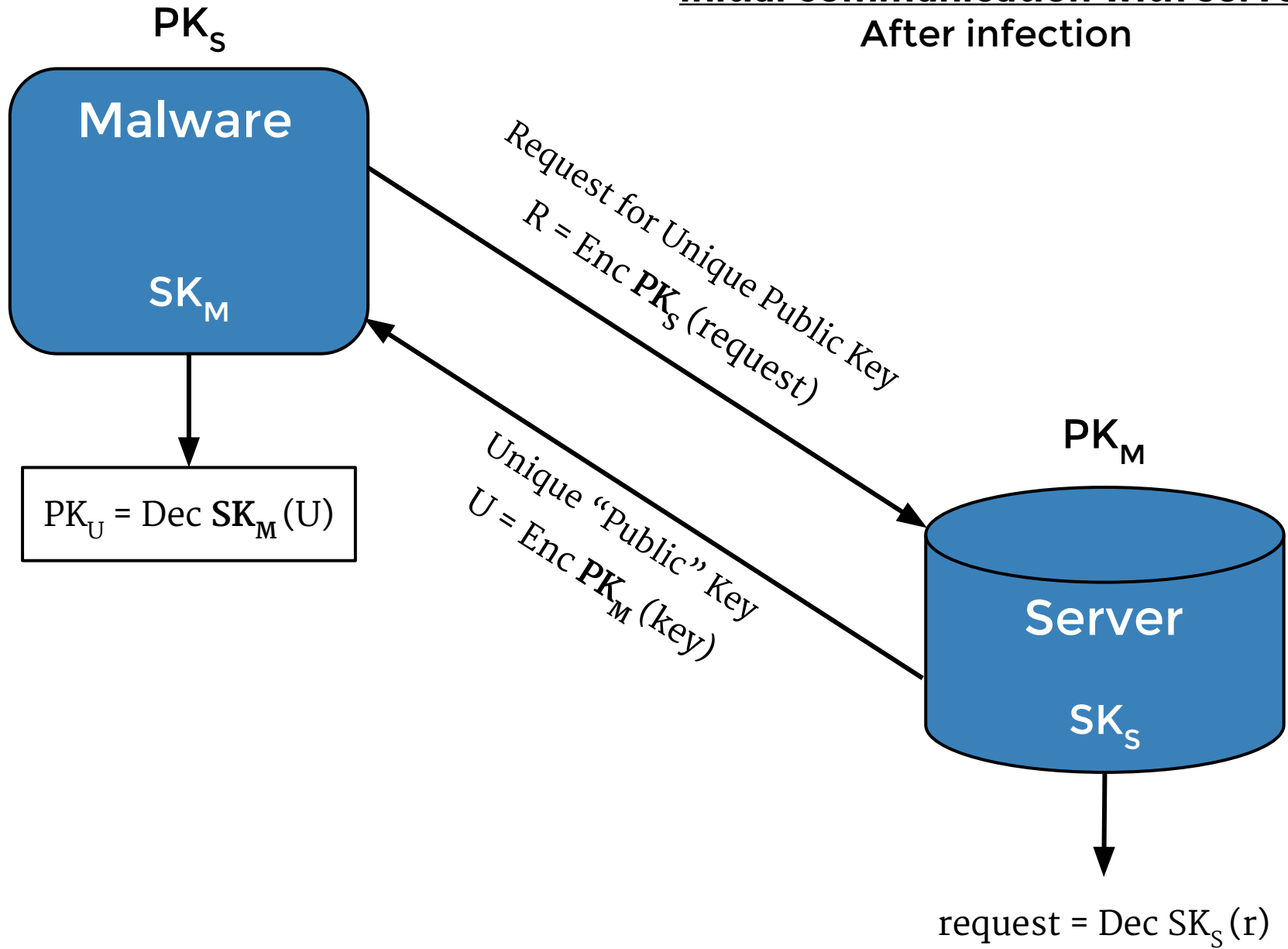
2

Encryption

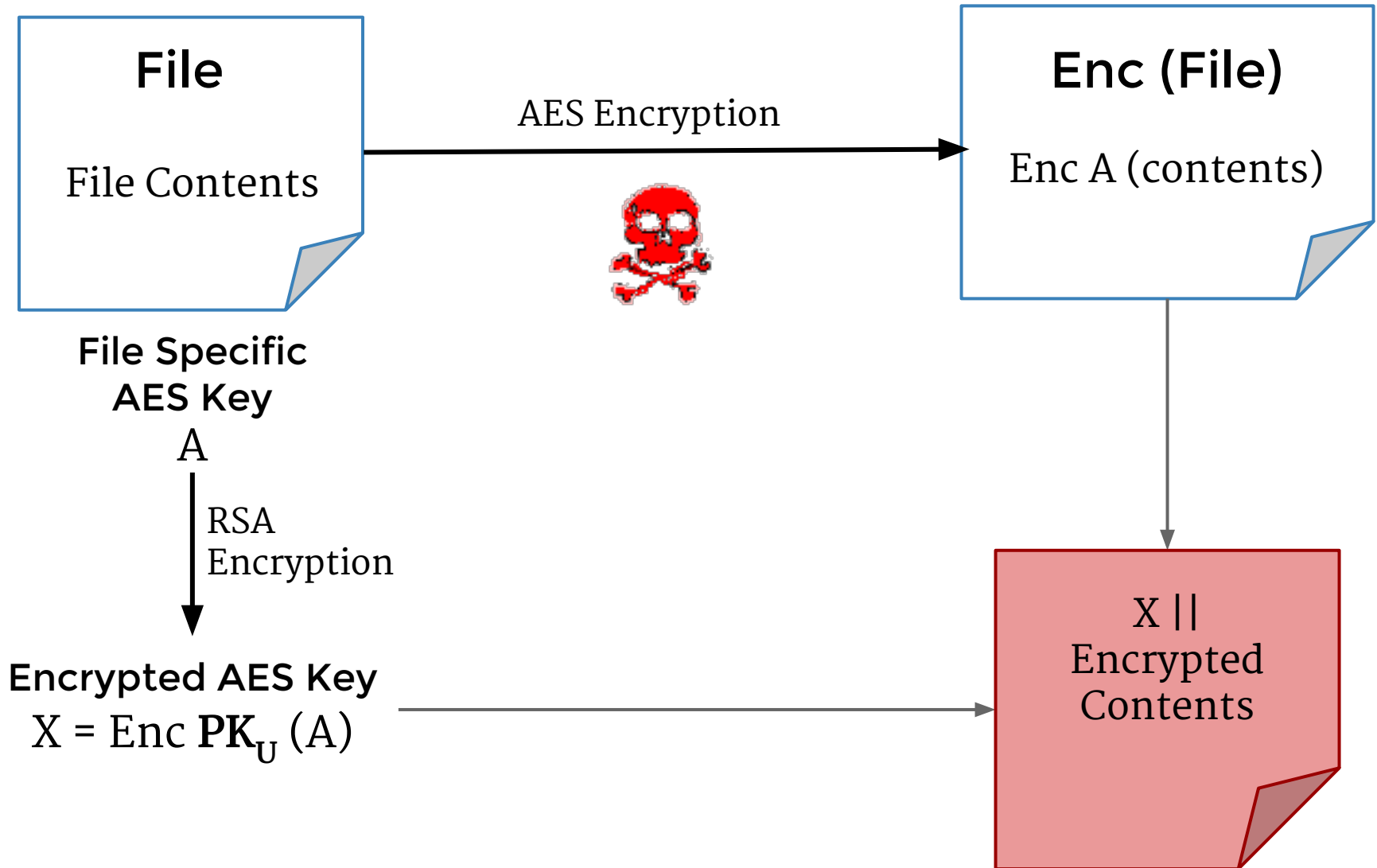
How Cryptolocker ruins your life:

1. Domain generation algorithm used to connect to server
2. Server communication encrypted with 2048-bit RSA
3. Files encrypted with 256-bit AES and RSA

Initial communication with server
After infection



CryptoLocker encrypts each file

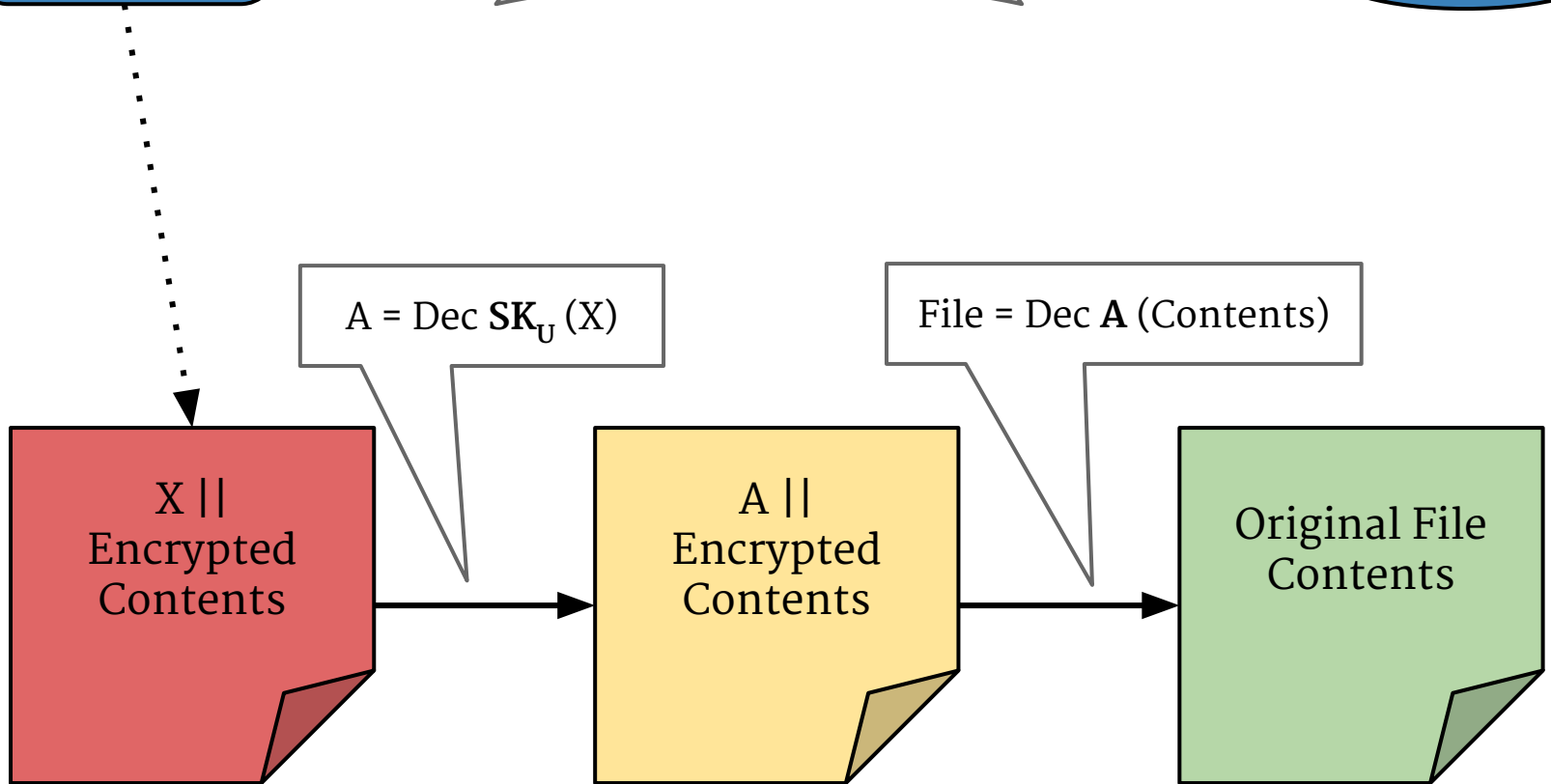
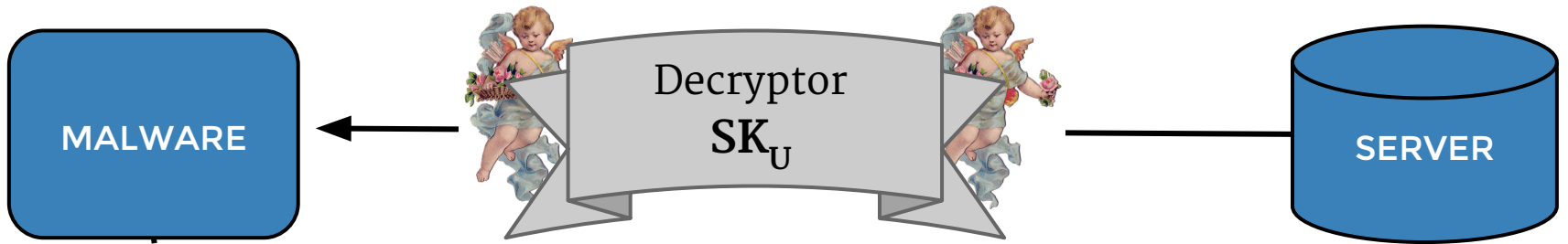


3

Decryption

Decrypting modern ransomware:

1. Brute force is impossible
2. With a cold storage backup, just delete the malware and restore the files
3. Otherwise, pay ransom of ~2 bitcoins before the timer expires



WHAT ARE THE BENEFITS CONSEQUENCES?




Bitcoin Address

Summary

Address [135N2nfAkextd6E25quXpM98qLSi2BccCb](#)

Tools [Taint Analysis](#) - [Related Tags](#) - [Unspent Outputs](#)

Transactions

No. Transactions	157	
Total Received	36,497.85154773 BTC	
Final Balance	2.10568641 BTC	

[Request Payment](#) [Donation Button](#)



- Funding criminals
- Bitcoin theft and inflation
- Temporary, perhaps permanent, loss of files
- Worm-like infection of subsequent machines
- Computer takeover! 250,000 computers infected.
 - DDoS
 - Bitcoin mining

WHAT CAN WE DO ABOUT IT?

- Once active, cannot be stopped besides payment
- **Prevention** (backups) and caution are key
- Deleting the malware will not remove the encryption and will hinder your ability to pay up—you'll have to reinfect your computer
- By creating a honeypot (large volume of garbage data) on hard drives, sysadmins have caught the malware in action



SOURCES

- [Krebs on Security](#)
- [Malware Bytes](#)
- [overview on ransomware from Symantec](#)
- [Nakedsecurity on Cryptolocker](#)
- [Cryptolocker technical analysis](#) by kernelmode
- [Cryptolocker FAQ](#) by bleeping computer
- [Reddit](#), and a [followup post](#)
- [Analysis of ransomware software from Journal of Computer Virology](#)
- [differences from CL 1.0 to 2.0](#)
- [Kaspersky - 2048 bit key\(s\)](#)
- [Police station falls victim, boston.com](#)
- [ABC news producer falls victim](#)
- [BBC infection statistics](#)

Thanks for listening!

Any questions?