Ransomware & Cyberthreat Intelligence Analysis

Mihoko Matsubara

CSO Japan, Palo Alto Networks K.K.

Today's talk

- Introduction
- When you talk to non-technical people
- The environment in the digital age
- Ransomware problems
- Prevention/Best practices
- Leadership involvement
- Summary

Introduction

CSO Team & Unit 42

unit 42

Rick Howard : CSO

Ryan Olson: Intelligence Director

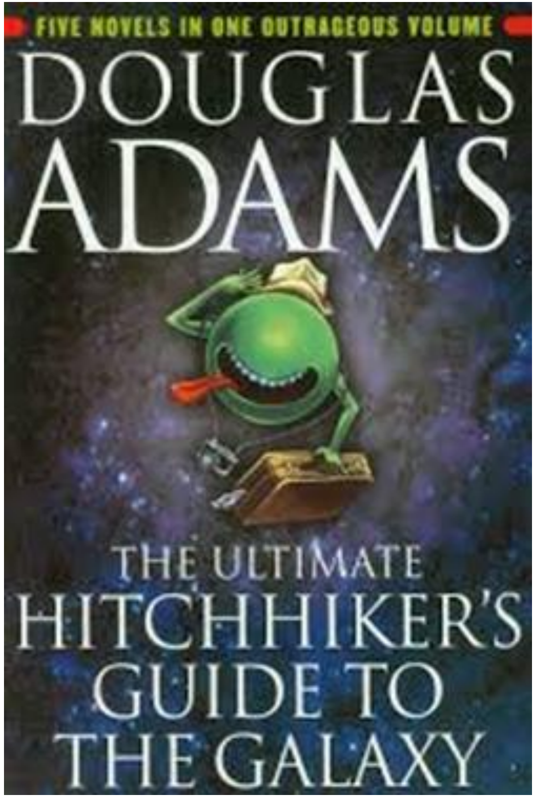
Phil
Da Silva

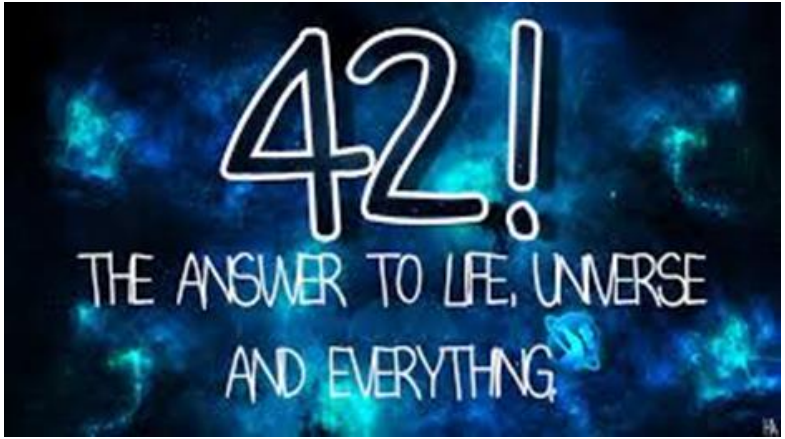
Vishaal
Hariprasad

Rob
Downs

Jen
Miller-Osborn

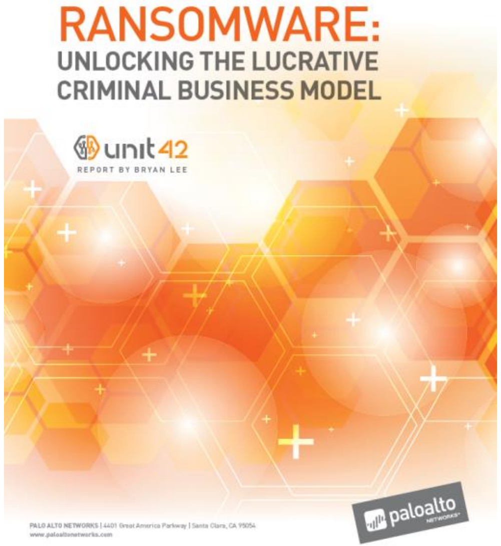
Unit 42


FIVE NOVELS IN ONE OUTRAGEOUS VOLUME
DOUGLAS ADAMS
THE ULTIMATE HITCHHIKER'S GUIDE TO THE GALAXY


42!
THE ANSWER TO LIFE, UNIVERSE AND EVERYTHING

Unit 42's research

- Whitepaper: "Ransomware: Unlocking the Lucrative Criminal Business Model" https://www.paloaltonetworks.com/resources/research/ransomware-report
- Unit 42 blogs: researchcenter.paloaltonetworks.com/unit42

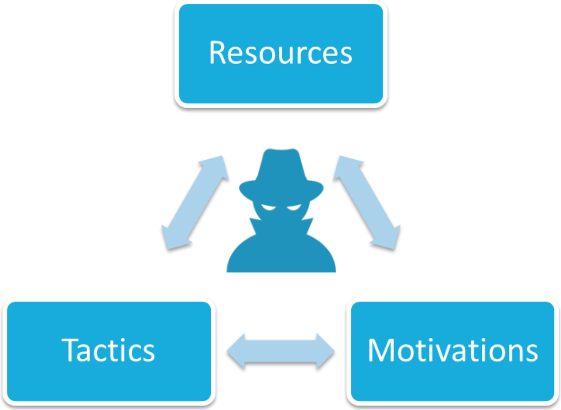


RANSOMWARE:
UNLOCKING THE LUCRATIVE
CRIMINAL BUSINESS MODEL

unit42
REPORT BY BRYAN LEE

PALO ALTO NETWORKS | 4401 Great America Parkway | Santa Clara, CA 95054
www.paloaltonetworks.com

paloalto NETWORKS



Resources

Tactics

Motivations

Unit 42's 10 recent blogs

- The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor
- New Wekby Attacks Use DNS Requests As Command and Control Mechanism
- Operation Ke3chang Resurfaces With New TidePool Malware
- Ransomware Is Not a "Malware Problem" – It's a Criminal Business Model
- KRBanker Targets South Korea Through Adware and Exploit Kits
- Bucbi Ransomware Is Back With a Ukrainian Makeover
- Prince of Persia: Infy Malware Active In Decade of Targeted Attacks
- Afraidgate: Major Exploit Kit Campaign Swaps Locky Ransomware for CryptXXX
- New Poison Ivy RAT Variant Targets Hong Kong Pro-Democracy Activists
- Python-Based PWOBot Targets European Organizations

When you talk to non-technical people

When you talk to non-technical people…

- They are more interested in financial impacts than technical details.
- They want to know what the problem is in non-technical terms.
- They also want to know what action they need to take for what reason.

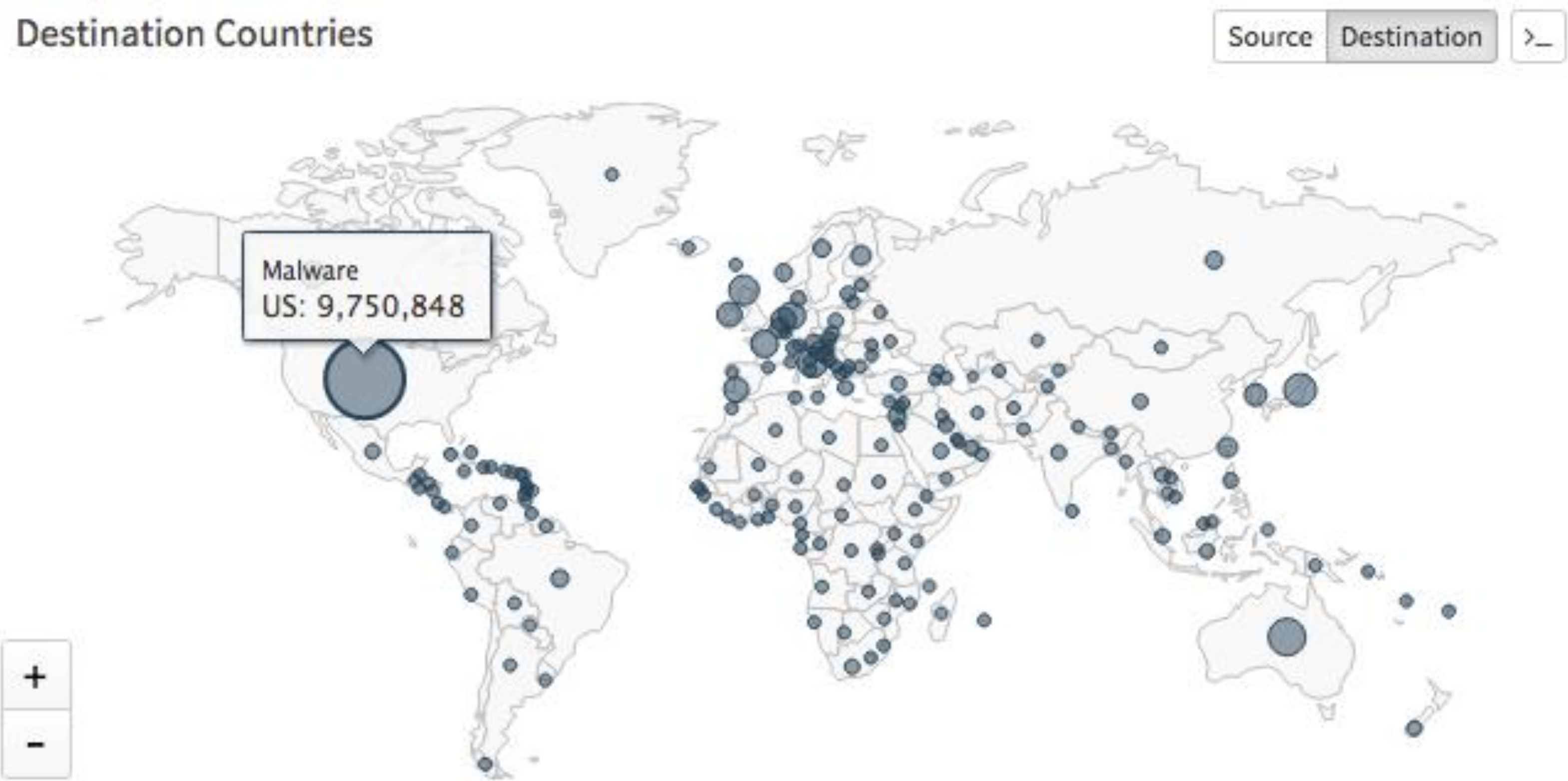
What is ransomware?

ransom

n. ran·som /rǽns(ə)m/

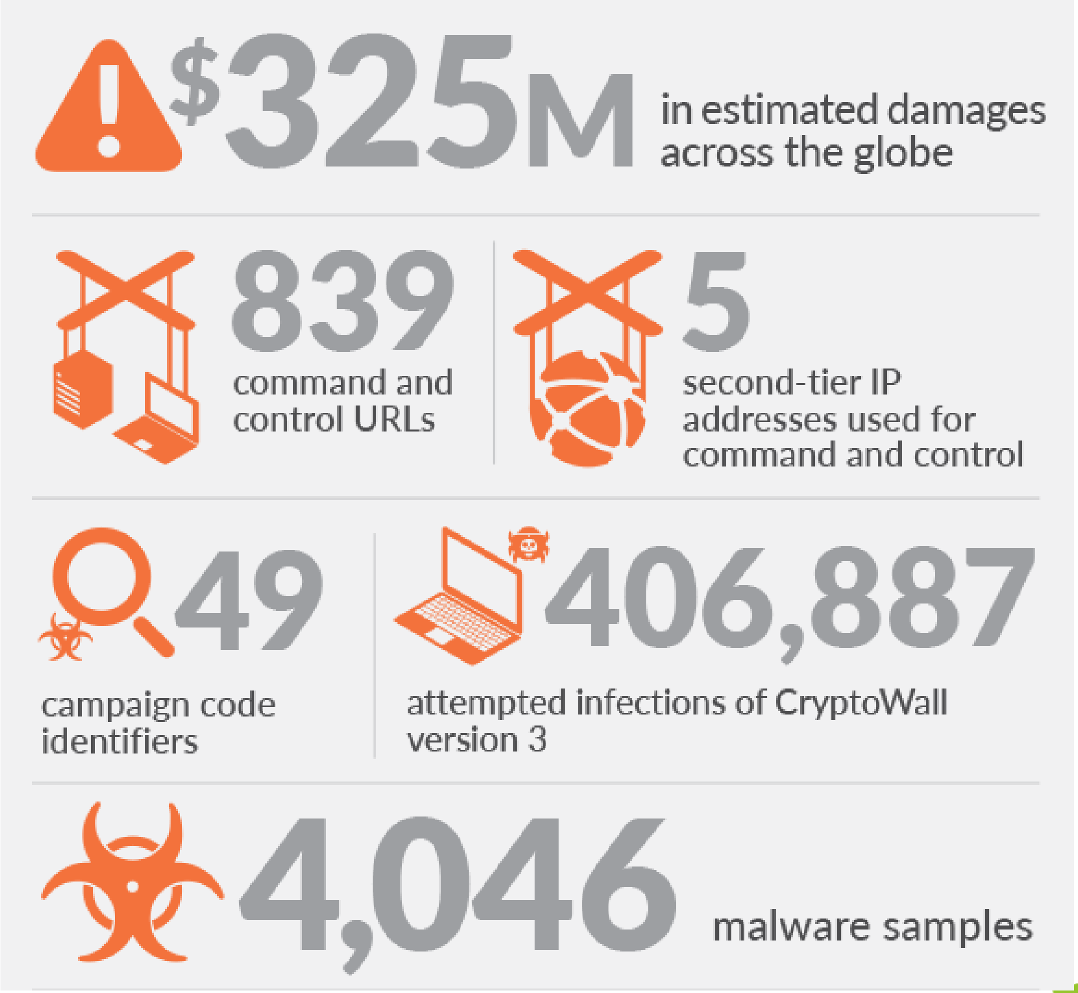
A consideration paid or demanded for the release of someone or something from captivity

Ransomware



Destination Countries

CryptoWall Threat



$325M in estimated damages across the globe

839 command and control URLs

5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples

The environment in the digital age

We live in the digital age

International Data Corporation (IDC) estimates

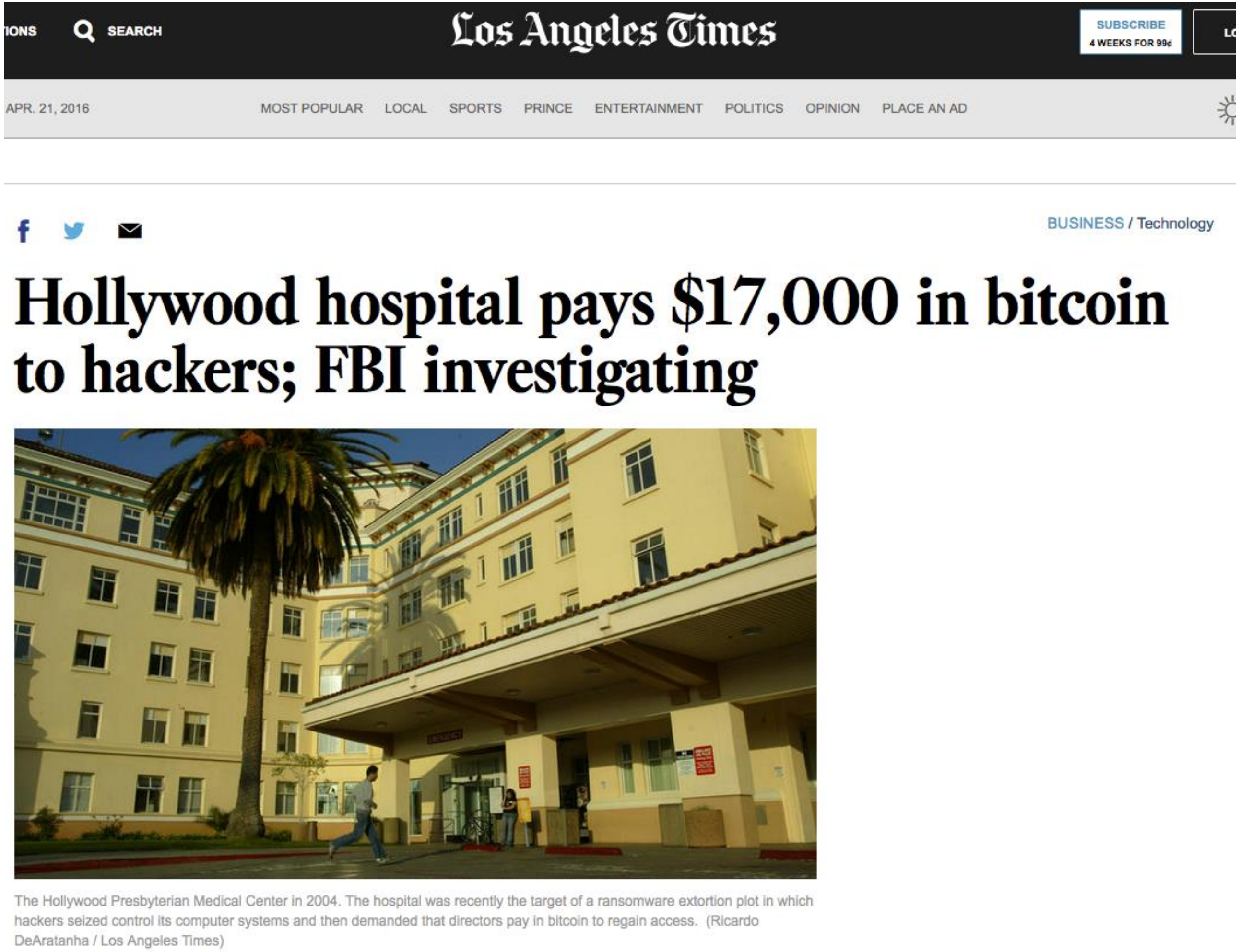
655.8 billion USD in 2014 → 1.7 trillion USD in 2020

Bad guys are also taking advantage of digitization…

Trust is the foundation of our digital world

Ransomware problems

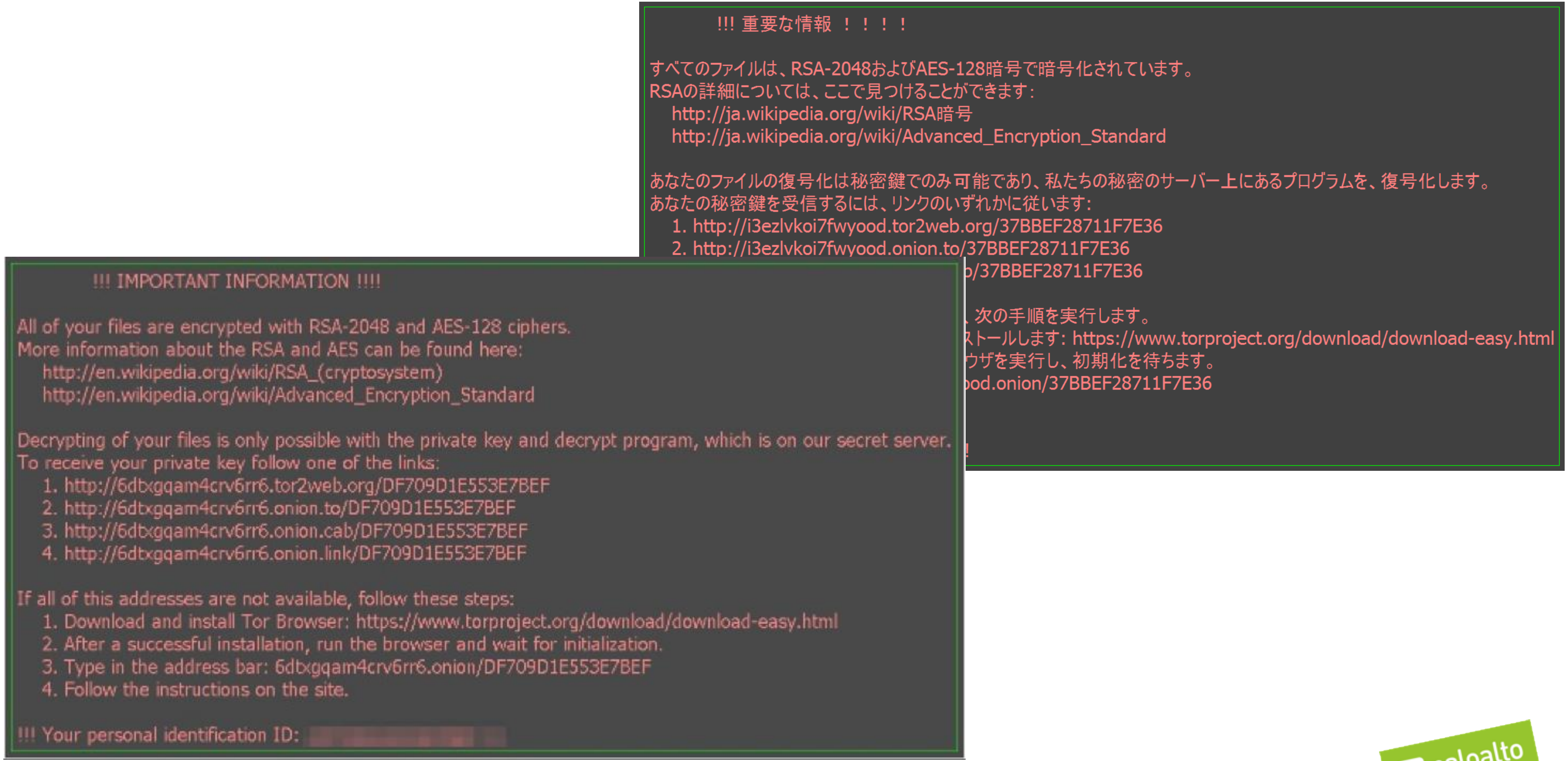
Ransomware can suspend your biz operations…



Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

The Hollywood Presbyterian Medical Center in 2004. The hospital was recently the target of a ransomware extortion plot in which hackers seized control its computer systems and then demanded that directors pay in bitcoin to regain access. (Ricardo DeAratanha / Los Angeles Times)

Ransomware used for the hospital case - Locky



!!! 重要な情報 ！！！！

すべてのファイルは、RSA-2048およびAES-128暗号で暗号化されています。
RSAの詳細については、ここで見つけることができます：
http://ja.wikipedia.org/wiki/RSA暗号
http://ja.wikipedia.org/wiki/Advanced_Encryption_Standard

あなたのファイルの復号化は秘密鍵でのみ可能であり、私たちの秘密のサーバー上にあるプログラムを、復号化します。
あなたの秘密鍵を受信するには、リンクのいずれかに従います：
1. http://i3ezlvkoi7fwyood.tor2web.org/37BBEF28711F7E36
2. http://i3ezlvkoi7fwyood.onion.to/37BBEF28711F7E36
o/37BBEF28711F7E36

、次の手順を実行します。
ストールします: https://www.torproject.org/download/download-easy.html
ウザを実行し、初期化を待ちます。
ood.onion/37BBEF28711F7E36

!

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

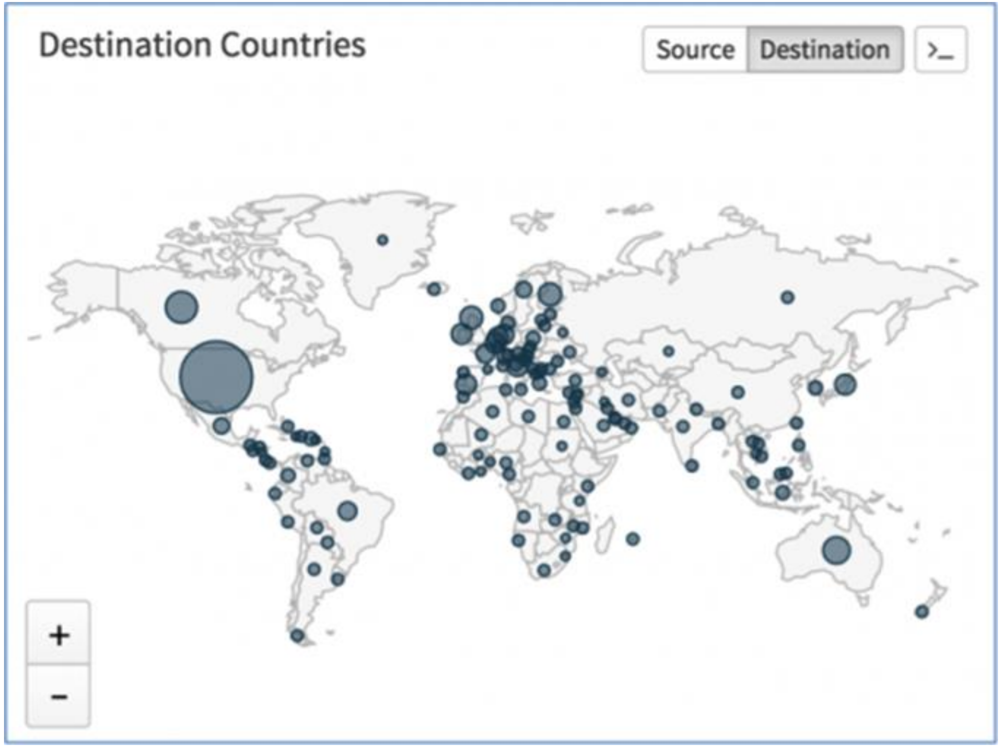
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://6dtxgqam4crv6rr6.tor2web.org/DF709D1E553E7BEF
2. http://6dtxgqam4crv6rr6.onion.to/DF709D1E553E7BEF
3. http://6dtxgqam4crv6rr6.onion.cab/DF709D1E553E7BEF
4. http://6dtxgqam4crv6rr6.onion.link/DF709D1E553E7BEF

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dtxgqam4crv6rr6.onion/DF709D1E553E7BEF
4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted]

Ransomware used for the hospital case - Locky

- First discovered in February 2016
- Covers multiple languages, including Chinese and Japanese



Source: AutoFocus

http://researchcenter.paloaltonetworks.com/2016/02/locky-new-ransomware-mimics-dridex-style-distribution/

Five steps taken by ransomware users

1. Take control of a system or device

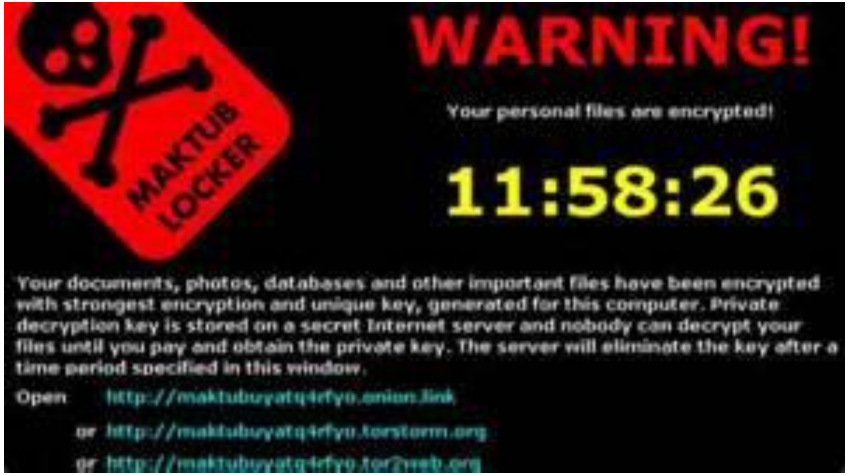
SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

Five steps taken by ransomware users

2. Prevent the owner from accessing it

Five steps taken by ransomware users

3. Alert the owner that the device has been held for ransom, indicating the method and amount to be paid



WARNING!

Your personal files are encrypted!

11:58:26

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://maktubuyatq4rfyo.onion.link

or http://maktubuyatq4rfyo.torstorm.org

or http://maktubuyatq4rfyo.tor2web.org

Five steps taken by ransomware users

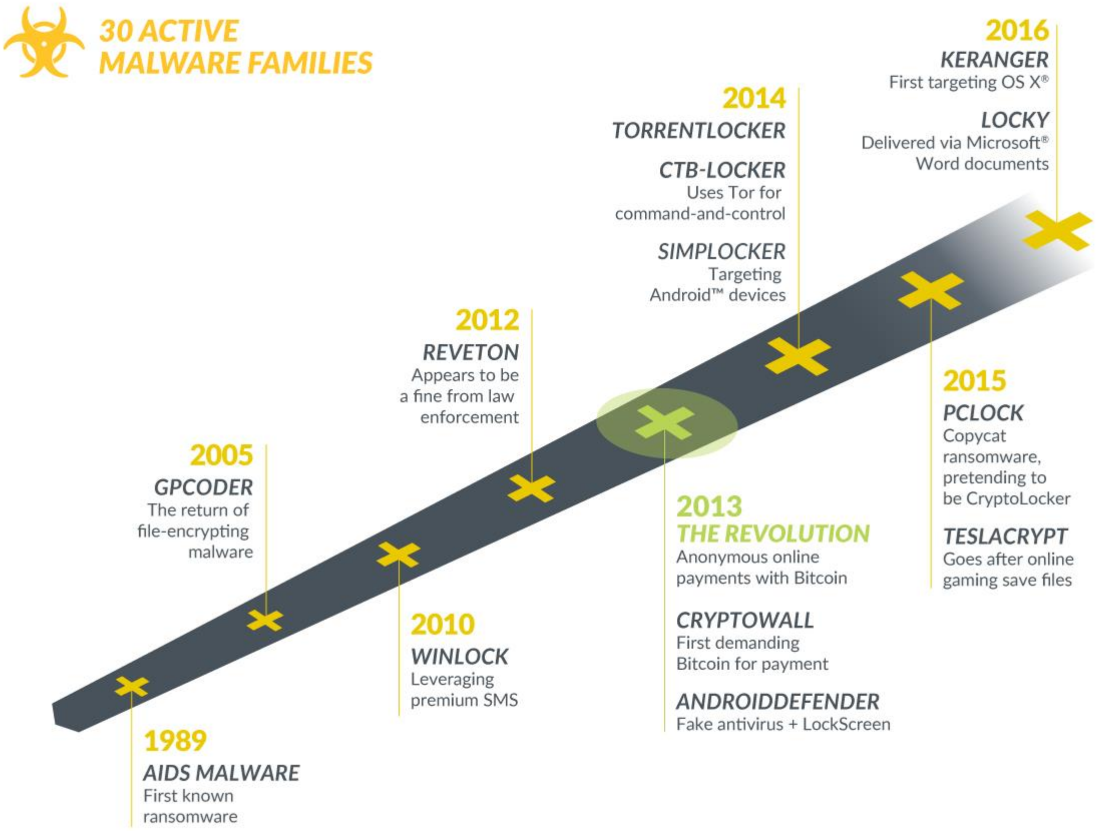
4. Accept payment from the device owner

Five steps taken by ransomware users

5. Return full access to the device owner after payment has been received

History

THE RISE OF RANSOMWARE



30 ACTIVE MALWARE FAMILIES

1989
AIDS MALWARE
First known ransomware

2005
GPCODER
The return of file-encrypting malware

2010
WINLOCK
Leveraging premium SMS

2012
REVETON
Appears to be a fine from law enforcement

2013
THE REVOLUTION
Anonymous online payments with Bitcoin

CRYPTOWALL
First demanding Bitcoin for payment

ANDROIDDEFENDER
Fake antivirus + LockScreen

2014
TORRENTLOCKER

CTB-LOCKER
Uses Tor for command-and-control

SIMPLOCKER
Targeting Android™ devices

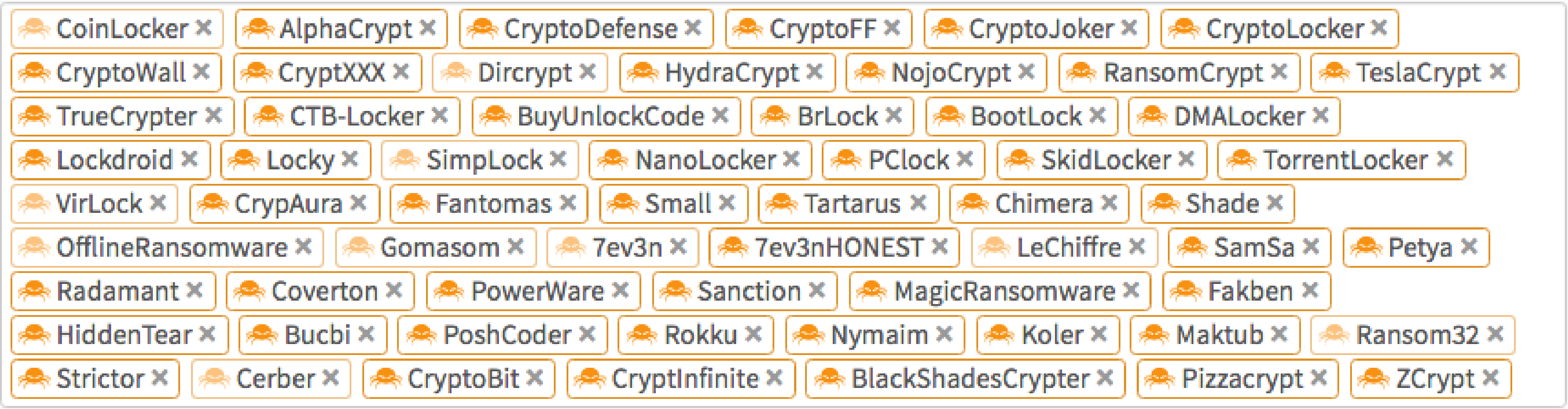
2015
PCLOCK
Copycat ransomware, pretending to be CryptoLocker

TESLACRYPT
Goes after online gaming save files

2016
KERANGER
First targeting OS X®

LOCKY
Delivered via Microsoft® Word documents

More than 60 ransomware families (types) exist as of 2016



CoinLocker × AlphaCrypt × CryptoDefense × CryptoFF × CryptoJoker × CryptoLocker ×

CryptoWall × CryptXXX × Dircrypt × HydraCrypt × NojoCrypt × RansomCrypt × TeslaCrypt ×

TrueCrypter × CTB-Locker × BuyUnlockCode × BrLock × BootLock × DMALocker ×

Lockdroid × Locky × SimpLock × NanoLocker × PClock × SkidLocker × TorrentLocker ×

VirLock × CrypAura × Fantomas × Small × Tartarus × Chimera × Shade ×

OfflineRansomware × Gomasom × 7ev3n × 7ev3nHONEST × LeChiffre × SamSa × Petya ×

Radamant × Coverton × PowerWare × Sanction × MagicRansomware × Fakben ×

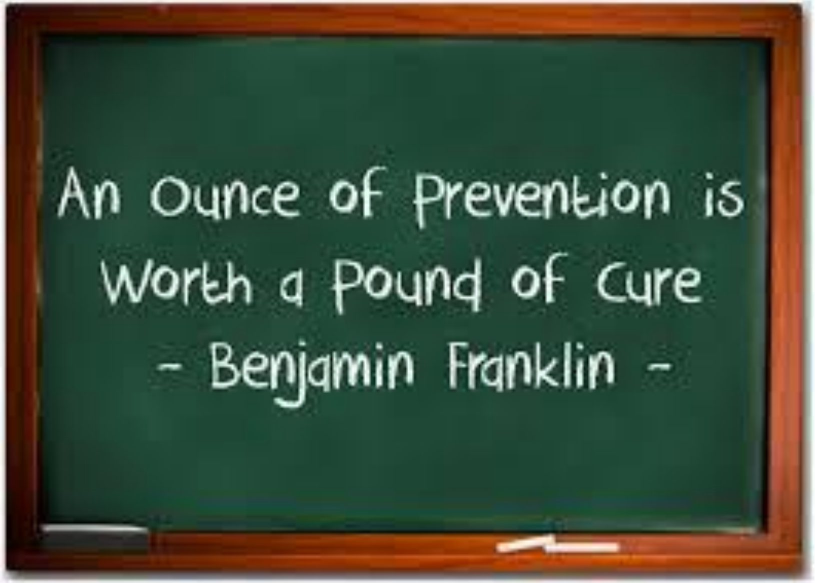
HiddenTear × Bucbi × PoshCoder × Rokku × Nymaim × Koler × Maktub × Ransom32 ×

Strictor × Cerber × CryptoBit × CryptInfinite × BlackShadesCrypter × Pizzacrypt × ZCrypt ×

By Palo Alto Networks research

Prevention/Best practices

Prevention



An Ounce of Prevention is Worth a Pound of Cure

- Benjamin Franklin -

SingCERT: “The best solution for ransomware is to prevent it from happening.“

Best practices

- Best practices – Reduce the attack surface
  - File blocking policy
  - URL filtering
  - Uncategorized domain downloads
- Regular backups of important data
- Stay aware of new malware and their indicators

Involvement of Leadership

Business leadership needs to be involved

New York Stock Exchange/Veracode found:

- 80% of board of directors say cybersecurity is discussed in most meetings.
- Top concern: brand damage due to customer loss

Summary

Summary

- Cybersecurity work is awesome.
- You talk to different types of people – technical, non-technical, government, company, academia, etc.
- Know your audience and tailor your presentation.
- Both technical and non-technical expertise is required.

Cybersecurity Jobs are hot

- Grace Hopper Celebration of Women in Computing, Houston, Texas, in October 2016
- Launched in 1994.
- This year, 15,000 women and 1,000 men participated.

Joy Osborne, “Palo Alto Networks Celebrates Women in Computing at Grace Hopper Celebration 2016,” Palo Alto Networks Blog, October 31, 2016, http://researchcenter.paloaltonetworks.com/2016/10/palo-alto-networks-celebrates-women-computing-grace-hopper-celebration-2016/.

Q&A