EVOLUTION OF RANSOMWARE

Advanced Protection for Modern Threats

Samuel Shiflett | Security Engineer
FIRST, A STORY

A loan officer from a large financial institution receives an email apparently from a client…

…She unknowingly downloads malware from this phishing email on her laptop.

The bank’s antivirus solution does not detect or block the incident.

Cryptolocker infects her machine
What happened when the malware got through?

What did Cryptolocker do?

- Encrypted thousands of files, including shared network storage affecting 100’s of users
- Demanded ransom in order to provide the decryption key
She lost several days of work since her last backup, and the whole department lost hours of productivity.

But, who is next?
And can we prevent it?

To best prevent future attacks, we need to know more…
Businesses Are Not Immune

Medical superbugs: Two German hospitals hit with ransomware
Infection forces patients onto phones and medicos onto faxes

Lincolnshire County Council hit by £1m malware demand

Crypto-ransomware attack encrypts entire New Jersey school district network

Horry County Schools struck by 'ransomware' virus

Major sites including New York Times and BBC hit by 'ransomware' malvertising

Patients diverted to other hospitals after ransomware locks down key software
Crypto-extortion increasingly targets bigger victims, most stay silent about it.
Overview

1. Brief History of Ransomware

2. Trends and Interesting Variants

3. What You Can Do To Protect Yourself
Lock vs Encrypt

Your computer has been locked due to the violation of the federal laws of the United States of America (Article 1, Section 8; Cause 8; Article 202; Article 210 of the Criminal Code of U.S.A.) provides for a deprivation of liberty for four to twelve years.

Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, pedophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.
You have 72 hours to pay the fine, otherwise you will be arrested.
You must pay the fine through MoneyPak:
To pay the fine, you should enter the digit resulting code, which is located on the back of your MoneyPak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fbi.gov.

MoneyPak
Walmart
CVS pharmacy
Older than you think…

A BRIEF HISTORY OF RANSOMWARE
The “AIDS” Trojan
Ransomware Theory
10 years later....
2005 to 2010
2010 to 2015

Attention!!!

The process of illegal activity is detected. According to UK law and Metropolitan Police Service and Strathclyde Police investigation your computer is locked.

The following violation is detected: your IP-address.

Exhibition websites containing pornography, child pornography, Sodom and called violence against children are, violent material toward people were visited from the IP address.

Moreover, e-mail spam was sent you’re your computer, e-mails containing terrorist materials. This locking server to stop your illegal activity.

To release your computer you should use the file in attached program.

You can:

1) Pay ransom:
   Use the details in attached program.
   In case of questions contact
   1-800-123-4567

2) Pay ransom:
   Use the details in attached program.
   In case of questions contact
   1-800-123-4567

Attention!

Your IP address is "IP_ADDRESS". The IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, images of violence and child pornography spam messages with terrorist motives were also sent from your computer.

The computer hack is aimed to stop your illegal actions.

To unlock your computer you are obliged to pay a fine of $100.

You must pay the fine through MoneyPak.

To do this, you should enter the digits resulting code in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the code to address purchase@moneypack.gov.

MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Walmart, Walgreens, CVS Pharmacy, Rite Aid, Kroger, Kroger, Longs Drugs, and Fred Meyer.
2010 to Today

CryptoLocker

Your important files encryption produced on this computer: photos, documents, etc.

You see this text, but do not see the "CryptoLocker" window. You deleted "CryptoLocker" from computer.

If you need your files, you have to recover "CryptoLocker" in the quarantine, or find a copy of "CryptoLocker" in the Internet.

You can download "CryptoLocker" from the Internet.
Mobile Ransomware
Crypto Timeline

1989
AIDS Trojan
Donated Funds to AIDS Foundation

2006
Gpcode / Troj.RANSOM.A
RSA Encryption via .EXE

2013
CryptoLocker, 2048 bit RSA key
Gaming network delivery
Payment via BitCoin

2014
CryptoWall
Malvertising / Social Engineering
$320M in BitCoin!

2015
Tesla Crypt
Utilized Angler Exploit Kit
Some with embedded key

March, 2016
KeRanger
1st Mac Crypto
TRENDS AND INTERESTING VARIANTS
FBI Says Threat From ‘Ransomware’ Is Expected to Grow

Law-enforcement agency sees problem of extortion by hackers worsening in 2016

“Ransomware” is now the #1 threat to the enterprise

by Mike Wheatley | Mar 10, 2016 | 0 comments
The Numbers are Growing…

…The Problem is Escalating
A Recent Attack – Locky - Feb, 2016

Percentage of variants identified by each AV engine

TOP 3 AVS ONLY DETECTED ~50%

+ 30 OTHERS W/ NO DETECTION

Source: First time submission to VirusTotal
How are these bypassing AV?

Exploit kits turn known into unknown

Polymorphic changes

Packing and Obfuscation

So long bankers...hello crypto lockers
We can decrypt.

Test us.
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: A5599796-2695577-

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 87-17-41, Panama 7, Panama.

Press ENTER to continue
“Educational” Ransomware

Hidden Tear 2.0 Decrypter

Password: 

Decrypt My Files

Hidden Tear decrypter 2.0
Decrypt all your files !!
CryptoHost: No C&C, No Actual Encryption

Your Computers Files have been Encrypted and Locked!

Your files have been encrypted and are unuseable and inaccessible. Don't worry, they're safe, for now.

This is unfortunate although for a small fee all of your Files will be returned to their original location as if nothing ever happened. Simply pay the recovery fee stated on this form and follow the instructions. Once the payment has been received your Files will be returned to normal. Not paying the Unlock Fee to the supplied Bitcoin Address before the Timer runs out means loss of all Files permanently.

The only payment accepted is Bitcoin. If you don't know what Bitcoin is there are instructions on how to obtain Bitcoin and pay the Fee. Just press the "How It Works" button below to learn how Bitcoin works.

This software checks the Bitcoin Network for the exact payment amount on the Bitcoin address provided. Once the amount is confirmed by clicking "Confirm Payment" your files will be returned to their original locations.

Removing this software causes permanent loss of your files! This software is the only way to get your files back!

Payment Address: 10AVFLK6BamXtpdY3kP2b5V3iJIlDpTkV

Review Locked Files

How It Works  How to Pay Unlock Fee  Check Payment Status

©2016 Check Point Software Technologies Ltd.
Locky now using Embedded RSA Key instead of contacting Command & Control Servers

By Lawrence Abrams

Zepto/Locky

~-.~=-~|...~|

!!! 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/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://mptadhci5mrdlj.u.tor2web.org/D7F6EEB0D8FC508E
2. http://mptadhci5mrdlj.u.onion.to/D7F6EEB0D8FC508E

If all of these 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: mptadhci5mrdlj.u.onion/D7F6EEB0D8FC508E
4. Follow the instructions on the site.

!!! Your personal identification ID: D7F6EEB0D8FC508E !!!
~-.~=-~|...~|
~--*.$~~-|--*$=
+++=+=++|--*~--_=+
+++*$
Pop Culture Ransomware

REMINDER
ALL EMERGENCY SERVICES
WILL BE SUSPENDED

FOR A 12-HOUR PERIOD DURING
THE PURGE
JUNE 7
SURVIVETHENIGHT

FSOCIETY
OLD PLAYERS…

…NEW TRICKS

- Ransomware events are becoming more frequent
- They have moved to target business users
- And are getting past traditional security
WHAT CAN YOU DO?
Best Practices for Protection

Blocking / Containment are crucial
- Beware new variants that encrypt off-line
- Prevent spread to more users, or network storage

Backup your data, just in case
- Not only to avoid paying
- Also because they may have bugs

Research your incidents
- To avoid additional or reinfections
- Educate users
Exploit Kits and Patching
Change Default Programs

JS

[Protected] Non-confidential content
On a more specific note....

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1 | Utilize Group Policy for Active Directory  
   Limit AppData execution, disable macros, no local admin for end users |   |
| 2 | Don’t Fall Prey to Known Attacks  
   Antimalware at the network and endpoint level, up to date and enabled |   |
| 3 | Email Security  
   No .exe, limit .zip, targeted phishing simulations |   |

Avoid paying the ransom. Decryptors are available.
Anti-Bot Technology Blocks Many, but…

SOME CRYPTOS
Don’t even need a connection to get the key…

TO STOP THESE
You Need to Prevent Malware Proactively
1st GENERATION SANDBOXES
that only detect the first instance, and block the second instance…

WILL NOT PROTECT FROM MODERN CRYPTO ATTACKS

Since damage will occur immediately…
Traditional Sandboxes are Prone to Evasion

NEW EVASION TECHNIQUES CONSTANTLY DEVELOPED

- Not activating the malware on virtual environments
- Delaying the attack…by time or action
- Different OS versions and variants
- Encrypted channels
Traditional Sandboxes are Slow

INSPECTION TAKES TIME

- As a result many sandboxes are deployed in non-blocking mode
- Allows malicious files to reach the user while the sandbox inspects the file in the background
Staying One Step Ahead of Crypto-Attacks...

- Highest Catch Rate
  Evasion-resistant malware detection

- CPU-level Detection

- Proactive Prevention
  Eliminate Malware In Documents

- Threat Extraction

Real-time Prevention Against Unknown Malware Including the Latest Crypto Variants
Family of Solutions
Staying One Step Ahead of Zero-Day Attacks

NETWORK
SandBlast Appliance
GW + Cloud Service

ENDPOINT

OFFICE 365™ EMAIL
Office 365

[Restricted] ONLY for designated groups and individuals
Sandblast Threat Extraction
Providing Clean Files Immediately for all Incoming Files

BEFORE
Malware Activated

AFTER
Malware Removed

SandBlast Agent Zero-Day Prevention

Block **CRYPTO ATTACKS** on your network and endpoints

**HIGHEST CATCH RATE**

**THREAT EMULATION**

Evasion resistant sandboxing at CPU- and OS-Level

**PROACTIVE PREVENTION**

**THREAT EXTRACTION**

Quick delivery of safe reconstructed content

**NON-INTRUSIVE**

Processing offloaded from endpoints to the cloud
Eliminate Zero-Day Malware at the Endpoint

1. Web downloads sent to SandBlast cloud
2. Sanitized version delivered promptly
3. Original file emulated in the background
Identify Infected Machines and Quarantine Them

1. Threat Intelligence continuously delivered to the Agent

2. Outgoing traffic inspected by local Anti-BOT

3. C&C traffic and data exfiltration are BLOCKED

4. Quarantine malicious process or Lockdown the entire system
Collect Forensics Data and Trigger Report Generation

1. **FORENSICS data** continuously collected from various OS sensors

2. Analysis automatically **TRIGGERED** upon detection of network events or AV

3. Advanced **ALGORITHMS** analyze raw forensics data

4. Digested **INCIDENT REPORT** sent to SmartEvent
Running Forensic Investigation

Interactive Forensics Report
- Single view of entire attack
- Tracks all attack elements
- Spans multiple reboots
- Drill-down on any element

Investigation Trigger
- Macro enabled doc

Crypter Code
- Encryptor module, connecting to C&C

Display Payment Details
- Deletes Shadow Copy
- Disables restore previous versions
- Deletes Self

Dropped File Deletion, Dangerous Execution
What to take away….

1. Ransomware isn’t going anywhere. Year over year exponential growth.

2. Use what you already have. Backups, antivirus, AD and email security.

3. Protections for the unknown. SandBlast Family of Products.

Questions?
THANK YOU