The Rise of Ransomware
Three Critical Steps to Prevent an Outbreak in Your Organization

Pez Zivic
Global Systems Engineer
CISSP, CISA
FBI Says Threat From ‘Ransomware’ Is Expected to Grow

Hollywood Hospital Hit By Ransomware Attack, FBI Investigates

Ransomware Warning Issued After Triad Company’s Files Held Hostage
Hospital pays nearly $17G in bitcoins to hackers who disabled computer network

A Los Angeles hospital paid a ransom of nearly $17,000 in bitcoins to hackers who disabled its computer network.
How do we feel?

LORD, Grant Me the Serenity to Accept the Things I Cannot Change, the Courage to Change the Things I Can, And the Wisdom to Hide the Bodies of Those People I Had to Kill Because They Pissed Me Off.
Research and Learn!
30 Active Malware Families

2005
GPCoder
The return of file-encrypting malware

2010
WinLock
Leveraging premium SMS

2013
THE REVOLUTION
Anonymous online payments with BitCoin

2012
Reveton
Appears to be a fine from law enforcement

2014
TorrentLocker
CTB-Locker
Uses Tor for command-and-control

2016
KeRanger
First targeting OS X

Locky
Delivered via Microsoft word documents

2015
PClock
Copycat ransomware, pretending to be CryptoLocker

TeslaCrypt
Goes after online gaming save files

1989
AIDS malware
First known ransomware

AndroidDefender
Fake anti virus + LockScreen

Source: Palo Alto Networks.com/solutions/initiatives/ransomware
Cooperation and Partnership in Research and Learning
CryptoWall v3 Investigation

$325M
Estimated Damages Across the Globe 44%
Victims Paid Up

30.7%
Exploit Delivery

Source: http://go.paloaltonetworks.com/cryptowall

Co-Founded by
Palo Alto Networks
Intel Security
Symantec
Fortinet
What We Learned?
To Prevent Ransomware:

1. Attack Vectors
2. Delivery Methods
3. How to Block
Hidden Attack Vectors!
1. Attack Vectors

Exploits
Macros
1. Attack Vectors

Exploits
1. Attack Vectors

Exploits

Macros
1. Attack Vectors

- Exploits
- Macros
- Exec
Delivery Methods
2. Delivery Methods
2. Delivery Methods

Exploit Kits
2. Delivery Methods

Exploit Kits

- User visits a compromised website
- Malicious code or ad redirects to exploit kit landing page
- Exploit kit page loads; determines best way to compromise user endpoint

- Ransomware encrypts data and holds it for ransom
- Exploit kit delivers ransomware
- Exploit kit compromises user endpoint
2. Delivery Methods

- Exploit Kits
- Email Attachments
Email Attachments

2. Delivery Methods

User receives targeted email with infected file

User opens file, thinking it is a legitimate document

Ransomware encrypts data and holds it for ransom

Office runs macro, downloads ransomware from URL embedded in doc
2. Delivery Methods

- Exploit Kits
- Email Attachments
- Drive-by Downloads
2. **Delivery Methods**

**Drive-by Download**

- **User visits a compromised website**
- **Website serves exploit to compromises user endpoint**
- **Ransomware encrypts data and holds it for ransom**
- **Exploit downloads ransomware**
The Problem – Prevent & Detect Ransomware

- **Multiple Attack Vectors**
- **Multiple Delivery Methods**

- **Perimeter**
- **Cloud/SaaS**
- **Endpoints**
How to Block and Detect?
3. How to Block

1. Reduce Attack Surface
2. Prevent Known Threats
3. Prevent Unknown Threats
Reduce Attack Surface

- Block unknown traffic
- Block malicious URLs
- Micro-segmentation N-S & E-W
- Stop dangerous file types

Disallow non-org access
Block dangerous file types
Extend zero-trust policies to endpoints
Extend threat intelligence from network to SaaS apps to endpoints
Prevent Known Threats

Block storage or transmission of files containing exploits
Scan cloud storage & SaaS apps for malicious files

Extend threat intelligence from network to SaaS apps to endpoints

Block malicious URLs
Block Virus & Vulnerabilities
Stop known exploits, malware & command-and-control traffic

Block execution of known malware
Block all known exploits
**Prevent Unknown Threats**

- Control unknown traffic
- Add context to threats and create proactive protections
- Detect and prevent threats in unknown files and URLs
- Block execution of unknown malware
- Block all unknown and zero-day exploits

Scan cloud storage & SaaS apps for malicious files

Extend threat intelligence from network to SaaS apps to endpoints
Automated Ransomware Prevention Across Multiple Attack Vectors and Delivery Methods is Only Possible with an Integrated Security Platform
How to Block and Detect?

Palo Alto Networks
Implementing Contextual Security

THREAT INTELLIGENCE CLOUD

Aperture

WildFire

AutoFocus

URL Filter

User-ID

Threat-ID

App-ID

NEXT-GENERATION FIREWALL

ADVANCED ENDPOINT PROTECTION

EXTENSIBLE

NETWORK

CLOUD

AUTOMATED

NATIVELY INTEGRATED
Enhancing Contextual Security with Partners
RESOURCES

Unit 42 Ransomware Report:

Ultimate Test Drives:
http://Go.PaloAltoNetworks.com/TestDrive