



# Ransomware Update

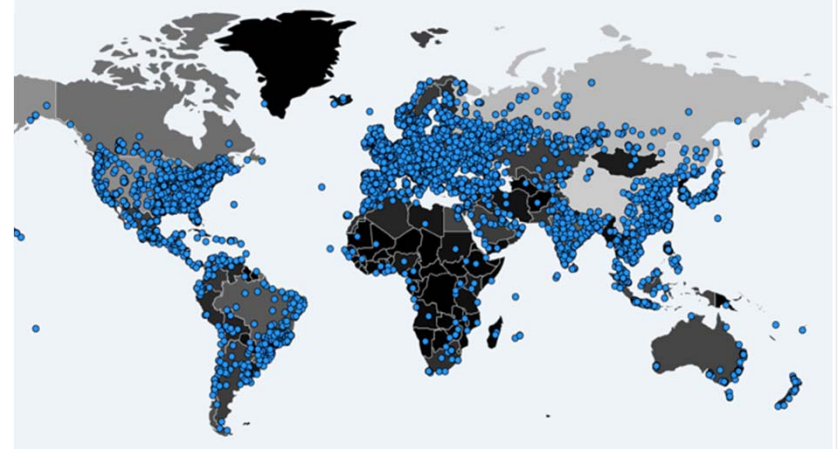
**Eric Tsoi**, CISSP, CISA, C|EH

Cyber Security Engineer  
Strategic Accounts and Global Enterprise  
Nov 2017

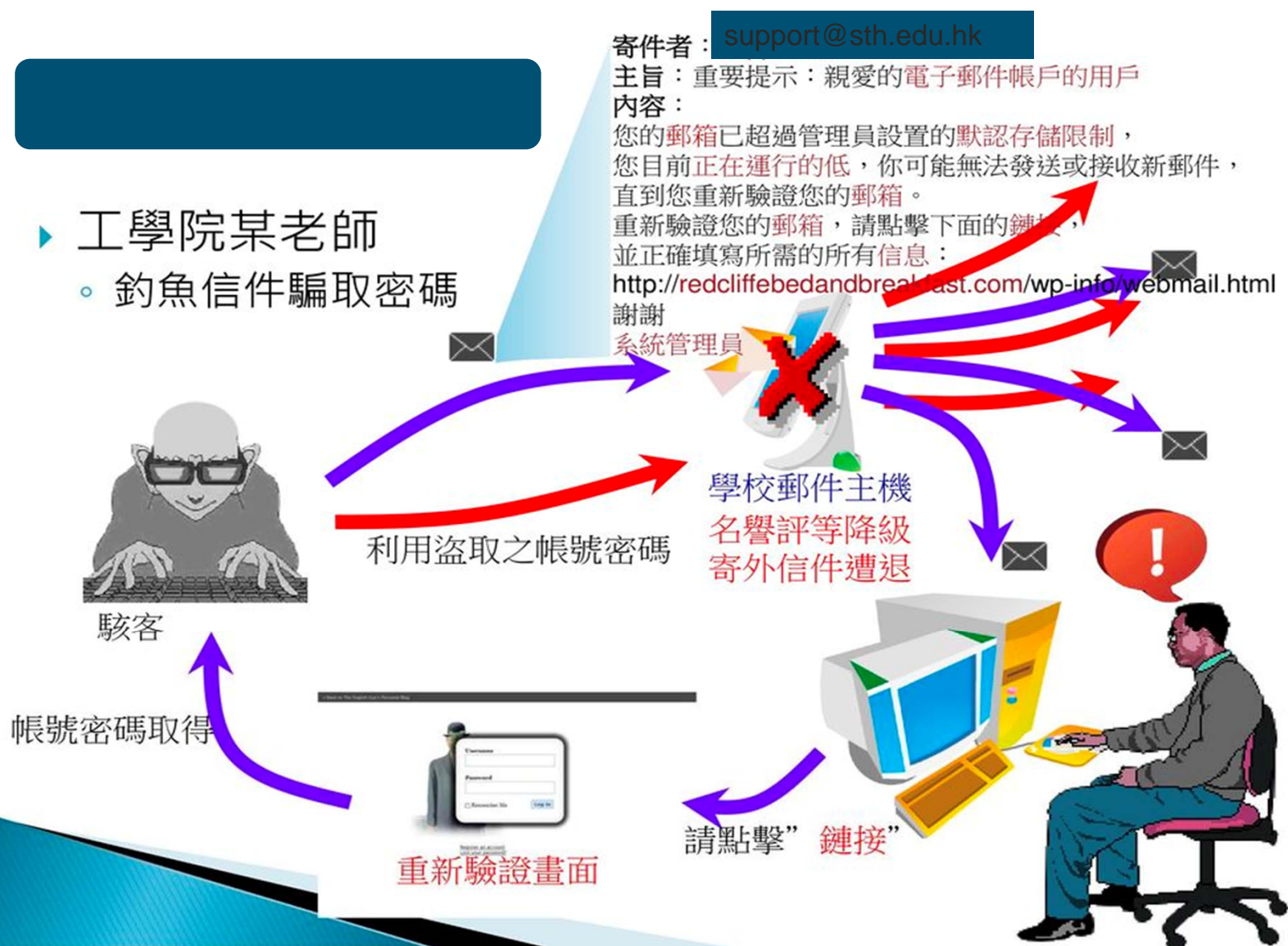
# Agenda

- Ransomware 1.0
  - Cases and impact
  - How it works?
  - Basic way to defend
  - New technology – Predictive security
- Ransomware 2.0
  - Wannacry, Neyeta, Bad Rabbit
  - Impact
  - Advance Ransomware Defense
- Material – Security Report and Ebook
- Offer – 14 days trial
- Network Academy

# Two main types of Cyber Attacks



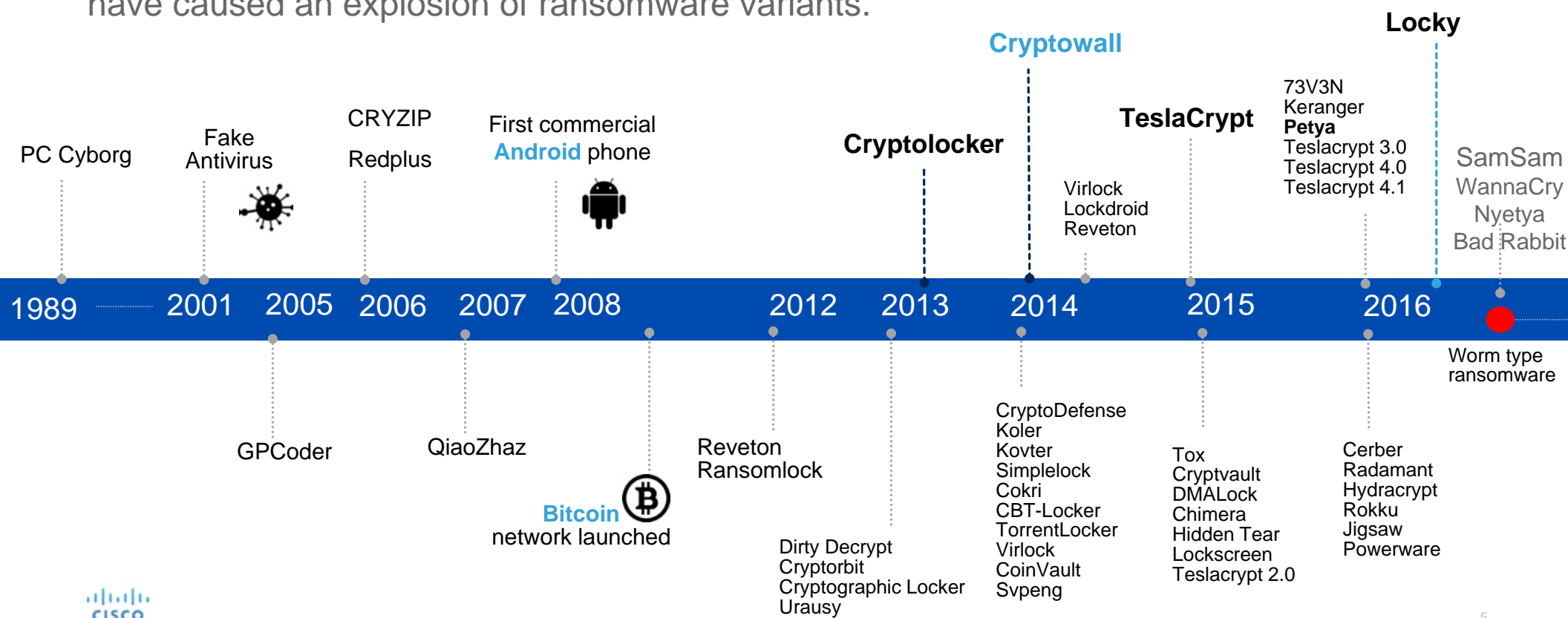
- ▶ 工學院某老師
  - 釣魚信件騙取密碼





# The Evolution of Ransomware Variants

The confluence of easy and effective encryption, the popularity of exploit kits and phishing, and a willingness for victims to pay have caused an explosion of ransomware variants.





# Ransomware in 2016: \$1 billion

Your computer files have been encrypted. Your photos, videos, documents, etc....  
But, don't worry! I have not deleted them, yet.  
You have 24 hours to pay 150 USD in Bi\_



Your computer files have been encrypted. Your photos, videos, documents, etc....  
But, don't worry! I have not deleted them, yet.  
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.  
Every hour files will be deleted. Increasing in amount every time.  
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.  
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.  
Send to the Bitcoins address specified.  
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal.  
Try anything funny and the computer has several safety measures to delete your files.  
As soon as the payment is received the crypted files will be returned to normal.

Thank you

59:59



1 file will be deleted.

[View encrypted files](#)

Please, send \$150 worth of Bitcoin here:

15fyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ

I made a payment, now give me back my files!



Email: [cryptohitman@yandex.com](mailto:cryptohitman@yandex.com)

Your files have been encrypted. We will delete files every hour.  
Ransom / Recompensa ID: 10958847  
You must pay \$150 USD in Bitcoins to the address specified below.  
Depending on the amount of files you have your Ransom can double to \$300  
If you dont pay within 36 hours.  
Take a picture of the BTC address, Ransom ID and contact email.  
We will delete files everyhour until you pay!  
If you do not have Bitcoins visit [www.localbitcoins.com](http://www.localbitcoins.com) to purchase.  
Your payment BTC Address is 19a93M9JGX377yFvZWRBs4abcUpwLFXsvE  
Everytime you restart your computer it recrypts everything. It will take a while  
for you to see the this screen again. Take a photo in case you want to contact us.  
Every time you restart the computer you run the risk of damaging the hard drive.  
Questions - email us: [cryptohitman@yandex.com](mailto:cryptohitman@yandex.com)

HITMAN

Y  
A  
T  
E  
59:52  
OS

3 files will be deleted. 3 archivos seran

[View encrypted files](#)

Send - Envie \$150 worth of Bitcoin here -

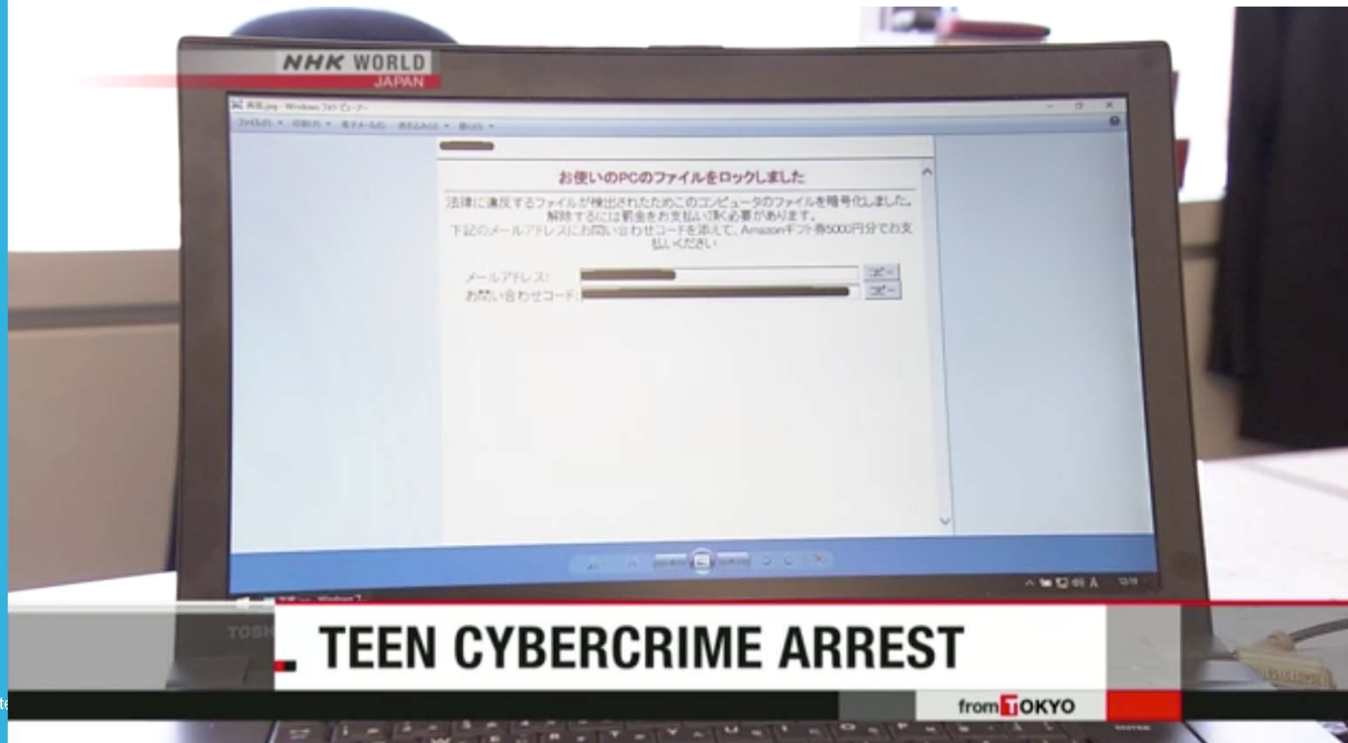
19a93M9JGX377yFvZWRBs4abcUpwLFXsvE

I made a payment, now give me back my files! Hice el pago, ahora  
devuélveme mis archivos!

Email:  
[cryptohitman@yandex.com](mailto:cryptohitman@yandex.com)

# 14-Year-Old Japanese Boy Arrested for Creating Ransomware


NHK WORLD News







 Builder  About

 Configuration  UAC Tricky  Extraction Path  DateTime  File Pumper  Exit

Path

- ☒ Select Path :  
- ☐ I use this :

Enter Folder

# RaaS

### Ransom32 - Stats

Address

1EnWwsdyrMiXPTU87bWtvW6zPL6ZozD61v

Payout ratio

75%

Installs

0

Lockscreens

0

Paid

0

Paid BTC

0

### Client download

BTC amount to ask: 0.1

Don't be too greedy or people will not pay

☒ Fully lock the computer

☒ Low CPU usage

☒ Show the lockscreen before encrypting

☒ Show a message box

☐ Critical Error

☐ Yellow Exclamation

☐ White Information

ERROR: main\_gui\_renderer.cc(237) Running without Renderer

☒ Latent Timeout

- Days: 0

- Hours: 0

- Minutes: 0

Download client scr


Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.

## RaaS: Karmen

 Hello, DevBitox! 

Dashboard







## Clients

 Settings

# Dashboard Statistics Overview



⌚ Updates

 New Design + Bug fix	22 feb
 Critical bug fixed	20 feb
 New programm design	20 feb
 Fix programm bug	18 feb
 Release new version	15 feb
 Test new version	14 feb

**Infos**

- ❗ Current version: 2.4
- ❗ Price to unlock: 1.2683 BTC
- ❗ Don't forget update you key!
- ❗ Contact jabber: devbitox@sj.ms
- ❗ Contact Telegram: @DevBitox

# Live Chat with customer services

## Padcrypt

10:45:00: Connection could not be made to the server!

50

Refresh Clear Chat Send

## CTB-Locker

Index Free decrypt Chat

Chat room

If you have any questions or suggestions, please leave a english message below. To prove that you are an administrator, you must specify the name of the secret file that is in same directory with index.php. We will reply to you within 24 hours.

RECEIVE SEND

## Jigsaw

Chat with us!

You are served by operator

Hello did you just message us

yes

1. Go to [www.LocalBitcoins.com](http://www.LocalBitcoins.com), Register and purchase Bitcoins. 2. Copy the Bitcoins address below and send the coins to that address from yourlocalbitcoins profile. 3. Click below that you paid. 4. Our system will recognize the payment instantly and unblock all your files

Type your message here ...

anWebChat





Swansea Police, Massachusetts \$750

Dickson County Police, Tennessee \$572

Tewksbury Police, Massachusetts \$500

Midlothian Police, Chicago \$500

Melrose Police, Massachusetts \$450

Melrose Police Dept, MA. \$500

Feb 2016

We have FW,  
and we have Anti-Virus



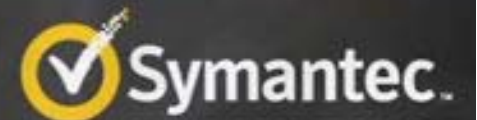
A man with short brown hair, wearing a blue shirt, is speaking in a video frame. The background is slightly blurred, showing an indoor setting with warm lighting.

Antivirus is dead

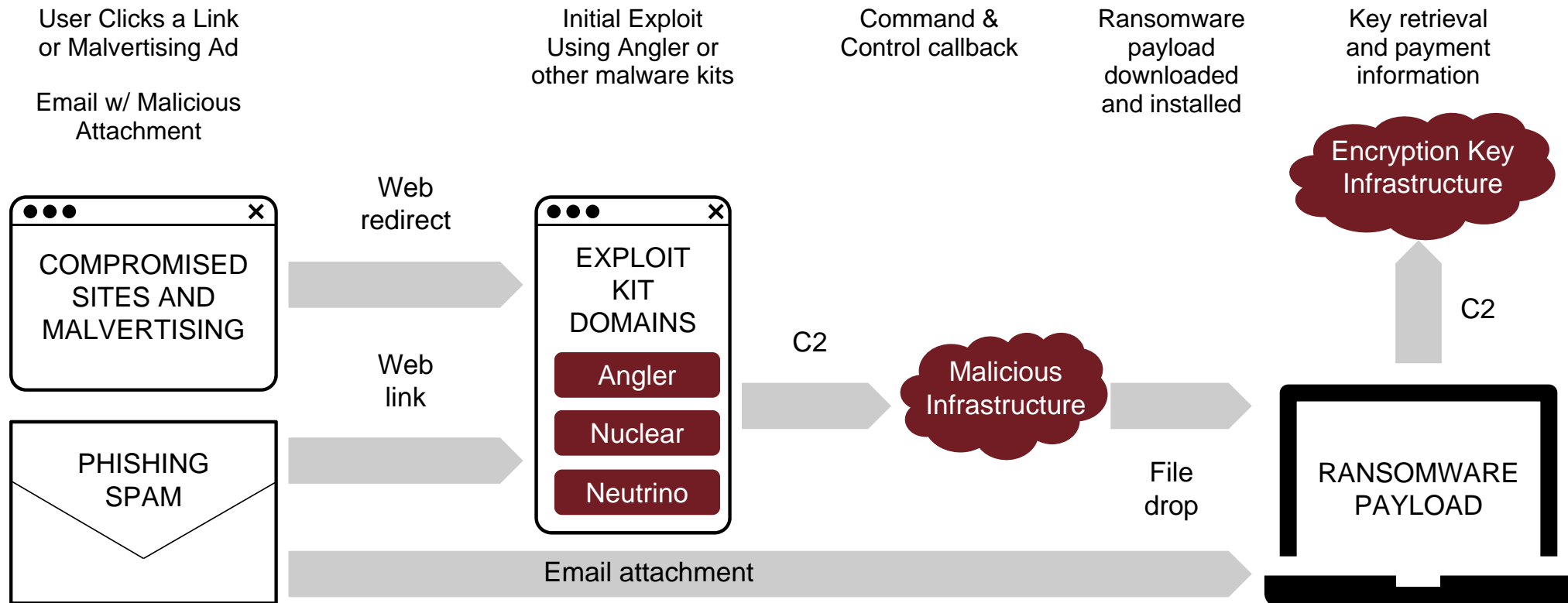
estimates traditional  
antivirus detects a  
mere 45 percent of  
all attacks.

Brian Dye

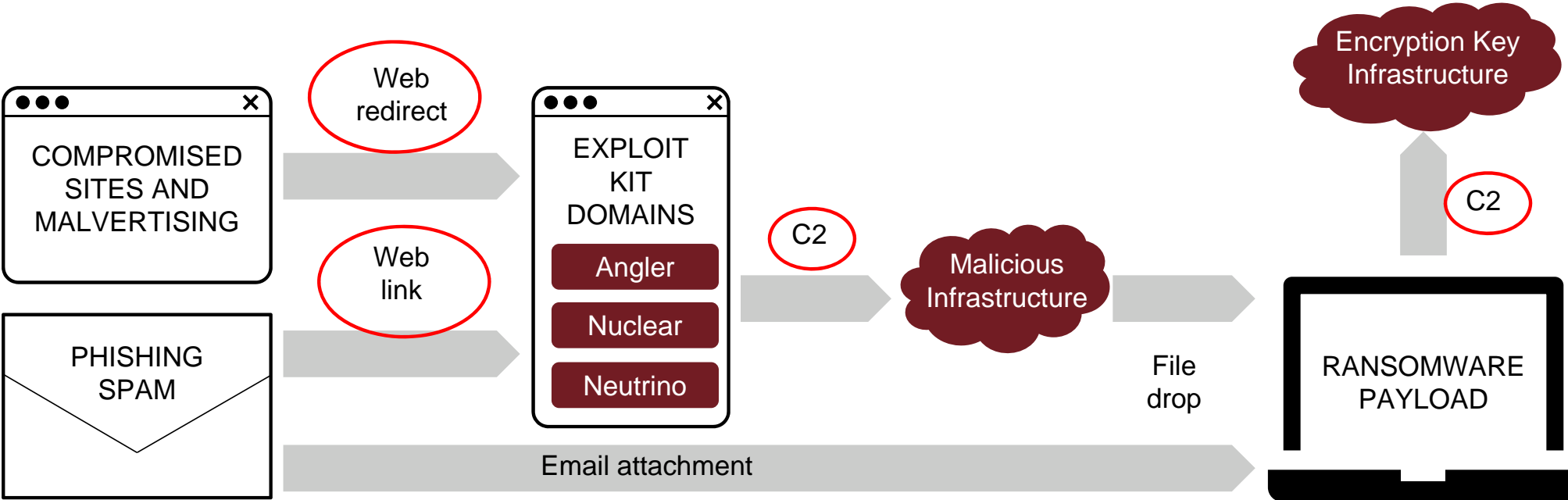
Sr. VP. of Information Security



# How Ransomware Works
















# Most Ransomware Relies on DNS and C2 Callbacks



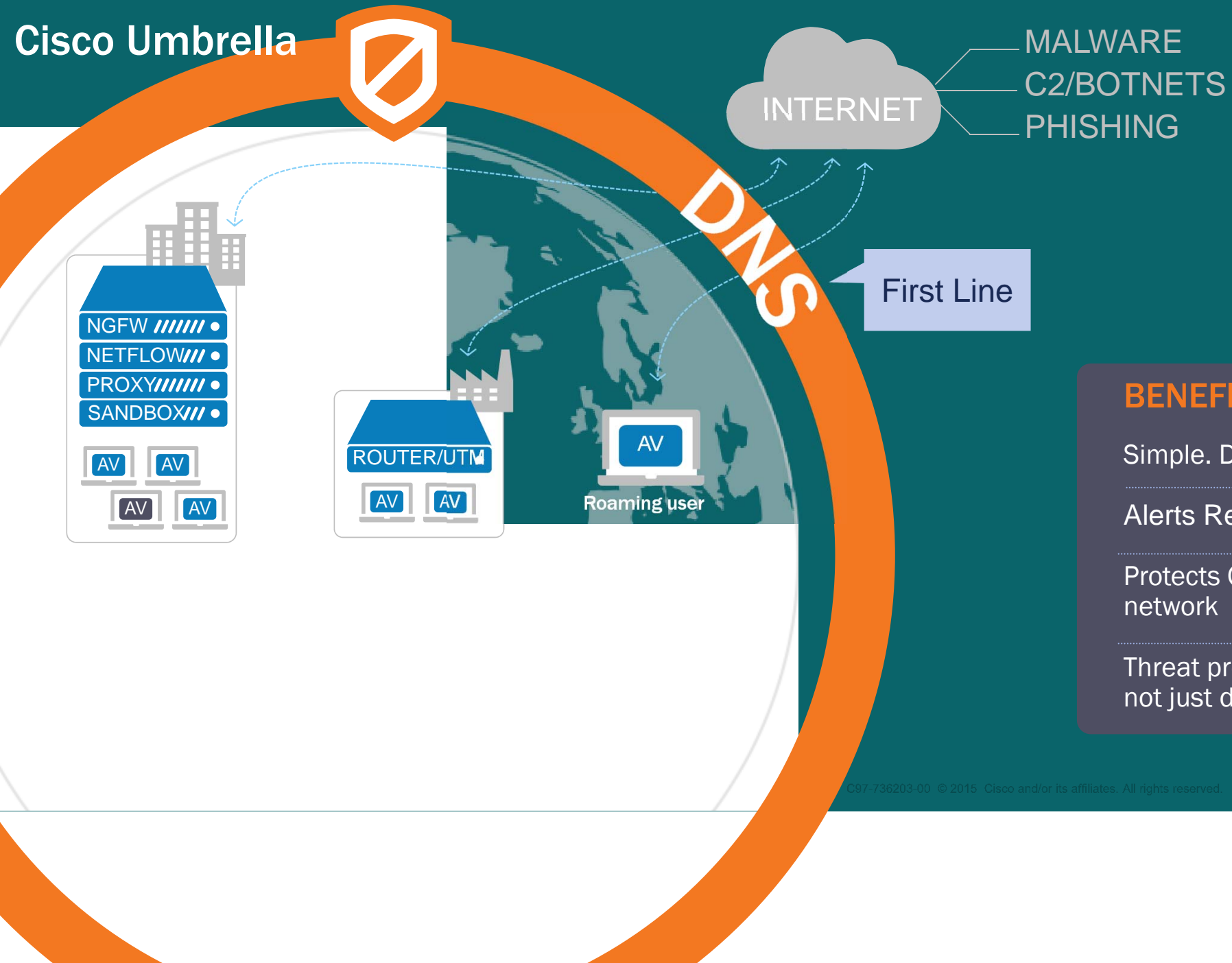
## Encryption C&amp;C

## Payment MSG

NAME	DNS	IP	NO C&C	TOR	PAYMENT
Locky					DNS
SamSam					DNS (TOR)
TeslaCrypt					DNS
CryptoWall					DNS
TorrentLocker					DNS
PadCrypt					DNS (TOR)
CTB-Locker					DNS
FAKBEN					DNS (TOR)
PayCrypt					DNS
KeyRanger					DNS







## BENEFITS

Simple. Deploy in mins!

Alerts Reduced 2-10x

Protects ON & OFF network

Threat prevention, not just detection



# Predictive

100B

requests  
per day

85M

daily active  
users

12K

enterprise  
customers

160+

countries  
worldwide

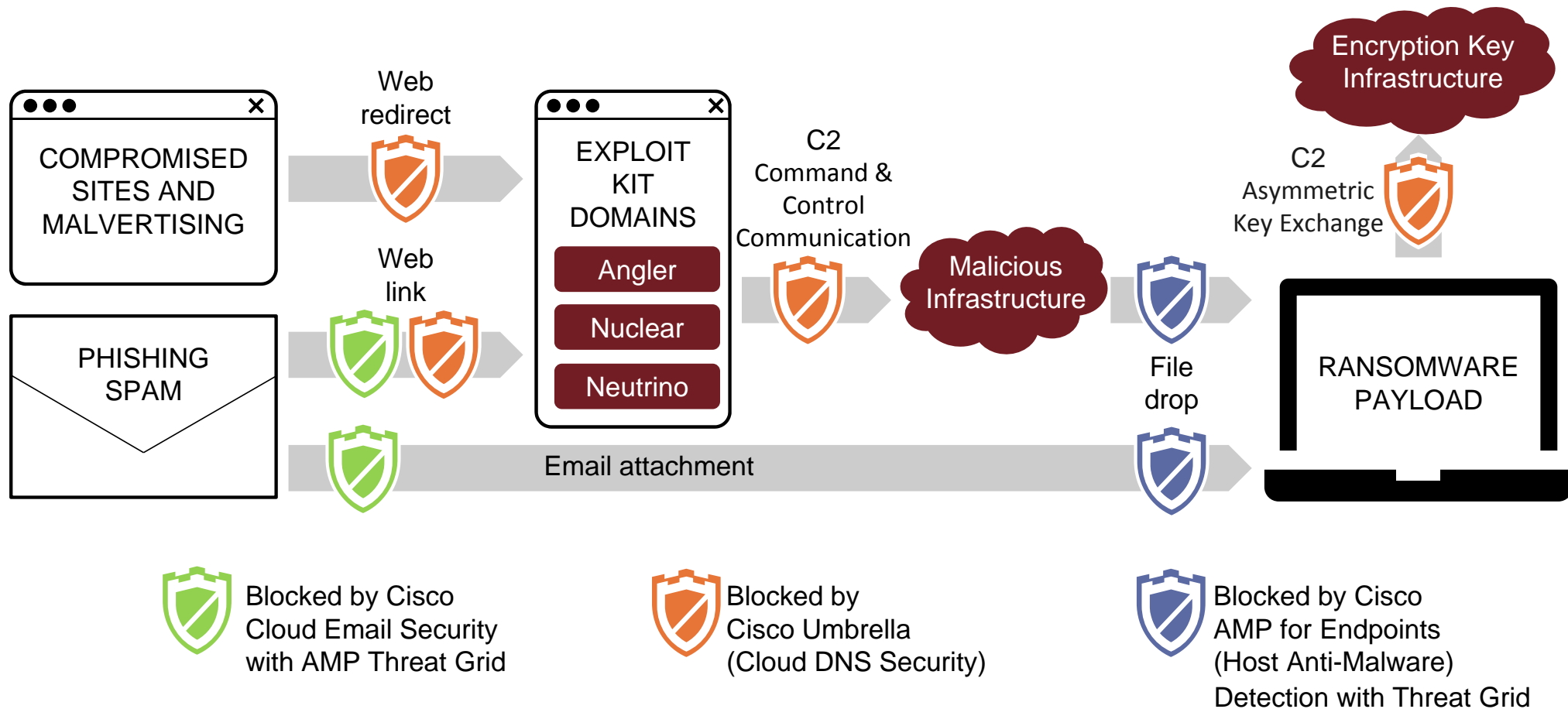


# CRYPTOLOCKER

The "Ripple Effect" by OpenDNS Research

[https://youtu.be/acwD\\_OA3QZ4](https://youtu.be/acwD_OA3QZ4)

# Basic defense: Prevent, Detect and Contain Ransomware with Cisco Email Security, Umbrella, and AMP for Endpoint



# OpenDNS Home

You're just three steps away from a safer, faster, smarter and more reliable Internet — for free!

## BENEFITS OF OPENDNS HOME

- ✓ Websites will load faster, and with OpenDNS' 100% up-time, you won't have to worry about unreachable websites and DNS outages from your ISP.
- ✓ With over 50 customizable filtering categories, OpenDNS Web content filtering keeps parents in control of what websites children visit at home.
- ✓ OpenDNS blocks phishing websites that try to steal your identity and login information by pretending to be a legitimate website. Surf the Web with confidence.
- ✓ Over 30,000,000 homes, schools, and businesses of all sizes rely on OpenDNS for a better Internet.



Looking for threat protection?

[Learn more about Cisco Umbrella](#) ➔

Already have an account? [Sign in.](#)

All fields are required.

Email address

Confirm email address

Select your country

Create password

Confirm password

[GET A FREE ACCOUNT](#)

By clicking "Get A Free Account" you agree to the OpenDNS [Terms of Service](#) and [Privacy Policy](#)

Just want DNS without creating an account? [Go right ahead!](#)

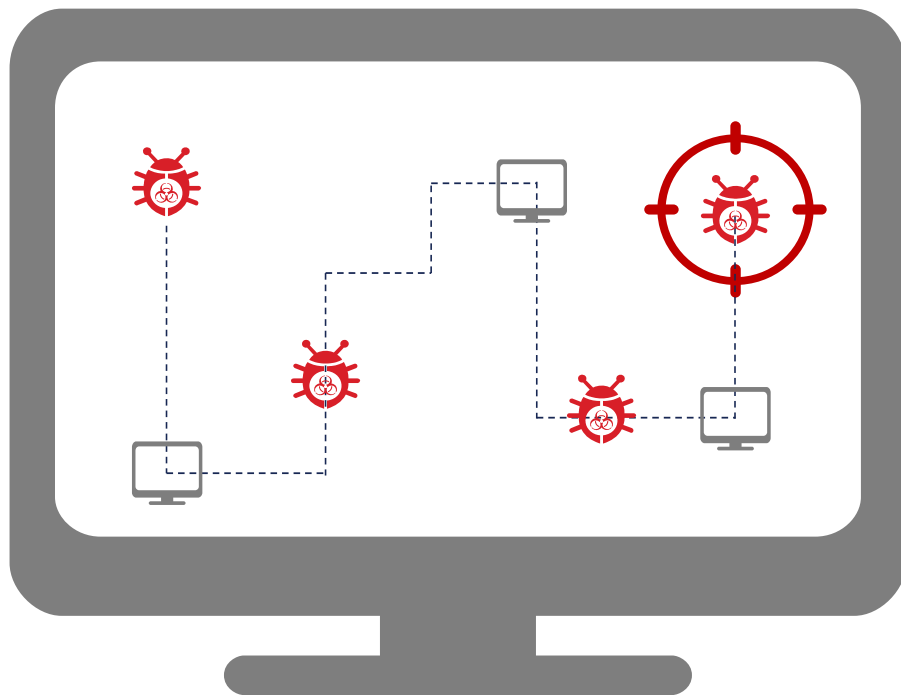


# Continuous Analysis and Retrospective Security

Only AMP for Endpoints Continuously Monitors, Records, and Analyzes All File Activity, Regardless of Disposition



● Recording





# If Something Gets in, Continuous Analysis and Retrospective Security Helps You Find Answers to the Most Pressing Security Questions



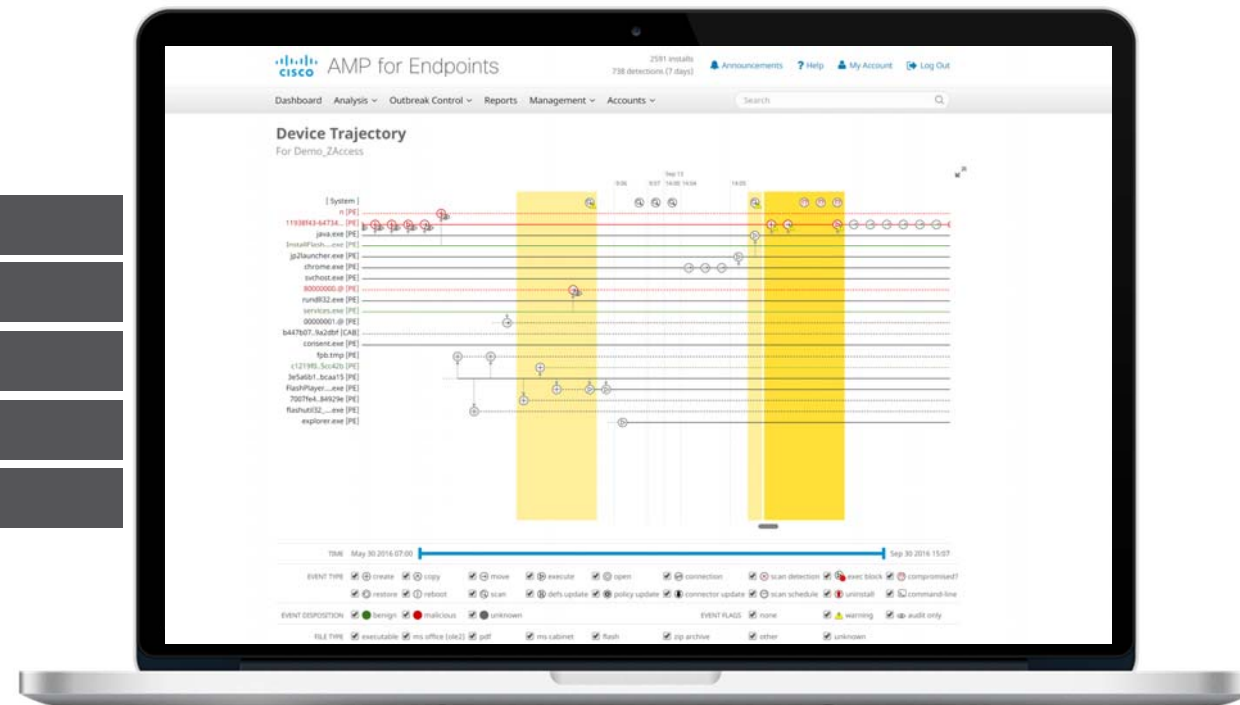
What happened?

Where did the malware come from?

Where has the malware been?

What is it doing?

How do we stop it?



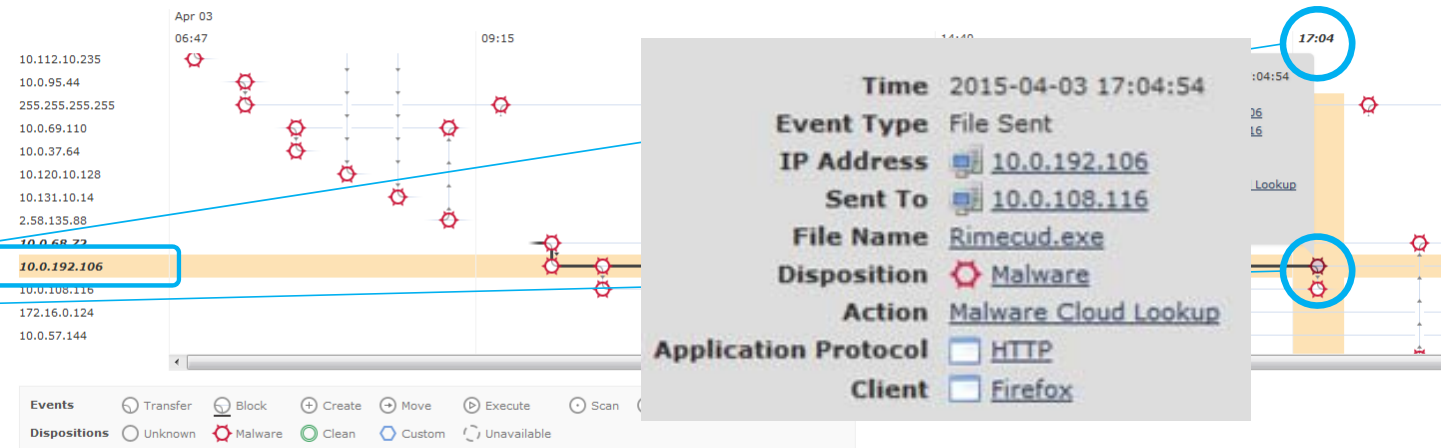
# Cisco FirePOWER AMP for Networks

## Network File Trajectory

File  
seen  
that  
about now ransomware  
likely entered the  
network and where it  
has spread

File SHA-256 5ae340af...1c8f37dc  
File Names [Alureon.exe](#), [Babonock.exe](#), [Badtrans.exe](#), [Bagle.exe](#) (+17 more)  
File Type [MSEXE](#)  
File Category [Executables](#)  
Current Disposition [Malware](#)  
Threat Score None

First Seen 2015-04-03 06:47:32 on [10.131.13.56](#)  
Last Seen 2015-04-03 19:52:50 on [10.130.10.83](#)  
Event Count 40  
Seen On 28 hosts  
Seen On Breakdown 15 senders → 21 receivers



e.g. if StealthWatch detects ransomware on host 10.0.192.106 at 5:04, FirePOWER's Network File Trajectory capability can be used to investigate the source of the infection

Time	Event Type	Sending IP	Receiving IP	File Name	Disposit...	Action	Protocol	Client
2015-04-03 09:15:42	Transfer	10.0.57.144	10.0.121.117	Pamro.exe	Malware	Malware Cloud Lookup	HTTP	Firefox
2015-04-03 09:15:42	Transfer	10.131.10.240	10.0.57.144	Badtrans.exe	Malware	Malware Cloud Lookup	HTTP	Firefox
2015-04-03 14:40:23	Transfer	10.110.10.195	10.131.15.26	Nakht.exe	Malware	Malware Cloud Lookup	HTTP	Firefox





"We received a malware alert. Within a few minutes in the AMP for Endpoints console we were able to determine the malware was using prohibited websites to mask its network traffic. AMP provides us the visibility and control on our endpoints to provide the IT security needs of the university without inhibiting academic freedom and research."

*Tim McGuffin, Information Security Officer, Sam Houston State University*

Visit [www.cisco.com/go/ampendpoint](http://www.cisco.com/go/ampendpoint) to access all customer testimonials

# What customers are saying about AMP for Endpoints

## CISCO ADVANCED MALWARE PROTECTION CUSTOMER TESTIMONIAL

“ We displaced Symantec Endpoint Protection and within 10 days, we detected over 500 new vulnerabilities in our environment, increased our threat detection by 200% and reduced our incident response time by 10 days. Overall, AMP for Endpoints has been one product that has increased our security visibility the most in the past 18 months.

— Chief Information Security Officer, Medium Enterprise Computer Software Company

Source: Chief Information Security Officer, Medium Enterprise Computer Software Company

✓ Validated Published: Apr. 11, 2017 TVID: G2E-8B4-A1A



## CISCO ADVANCED MALWARE PROTECTION CUSTOMER STATISTIC

84% of surveyed customers reduced threat detection time by 6 hours or more with AMP for Endpoints.



Source: TechValidate survey of 470 users of Cisco Advanced Malware Protection

✓ Validated Published: Apr. 7, 2017 TVID: 6EE-BF4-FD6

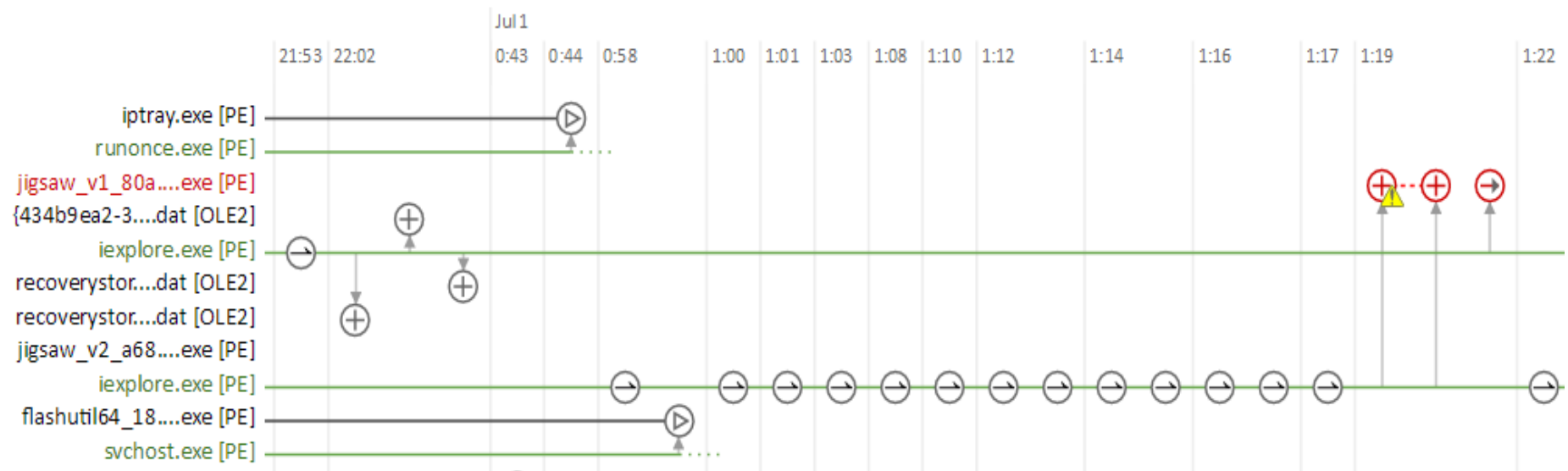


Visit <https://www.techvalidate.com/collections/amp-for-endpoints-survey-results> for more quotations and metrics



## Device Trajectory

For W7-amp10






# Ransomware 2.0

## Cryptoworm

Source: Cisco MCR and Goggle research report



**Hollywood Presbyterian Medical Center**  
**Methodist Hospital in Henderson, Kentucky**  
**Chino Valley Medical Center in Chino, Ontario, California**  
**Desert Valley Hospital in Victorville, Ontario, California**  
**Ottawa Hospital, Canada**  
**MedStar managed hospitals in Baltimore, Washington, Maryland**  
**King's Daughter's Health, Indiana**  
**Alvarado Hospital Medical Center, San Diego**  
**Chino Valley Medical Center, California**  
**Desert Valley Hospital, California**

**LA Hollywood Presbyterian Medical Center, \$17000**

May 2016





**Email, financial aid, voice mail, phone system. \$28,000 ransom**

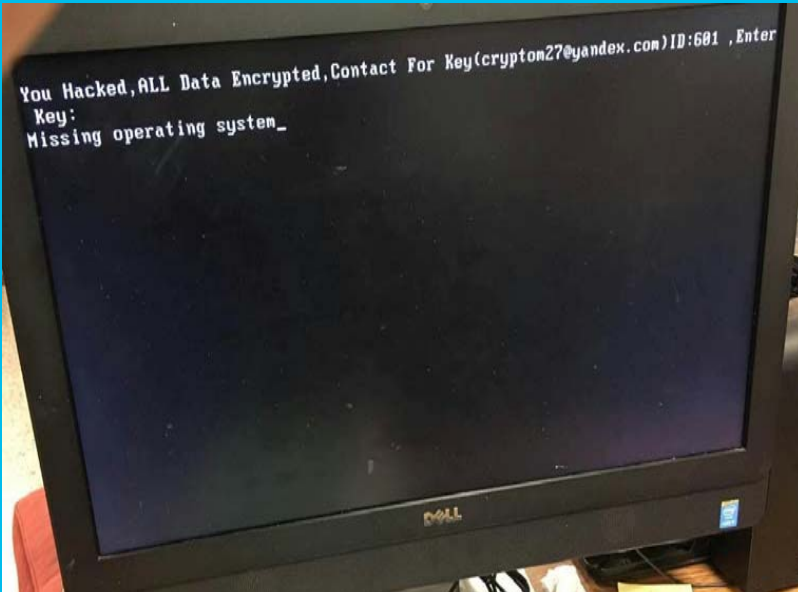
Dec 2016





**San Francisco MUNI Railway, 900 computer encrypted, demand for \$73,000**

Nov 2016







메인 사이트의 트래픽 과부화로 인해 임시 사이트를 운영하고 있습니다.

랜섬웨어 서버복구 과정에 대한 공지,

사이트 복원을 비롯한 문의 사항에 대한 응대를 진행하고 있습니다.

이용에 불편을 드려 죄송합니다.

[임시 사이트 바로가기 >](#)

[기존 사이트 바로가기 >](#)

June 2017



Due to heavy traffic on the main site, we run temporary sites.

Notice of Ransomware server recovery process,

We are responding to inquiries, including site restoration.

We apologize for the inconvenience.

[Temporary site shortcut>](#)

153 Linux servers, 3400 websites encrypted. **\$1 million US** paid

[Existing site shortcut>](#)

TALOS

WANNACRY?

12/5/2017



TALOS