Ransomware Update

Garrick Ng

Cyber Security Professionals Awards – Gold Winner

Smart City Consortium Security SIG Chairman

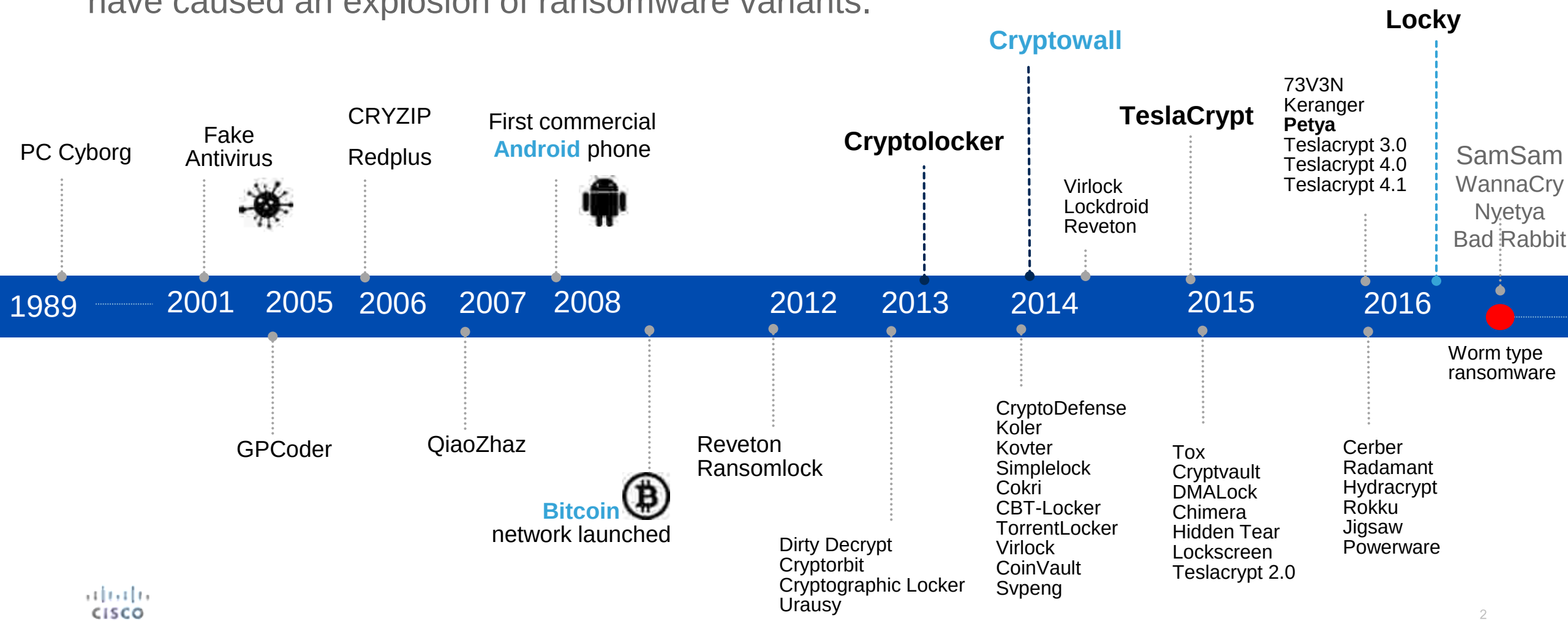
Chief Technology Officer

Cisco Hong Kong, Macau, Taiwan

Nov 2017

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

Locky, Cerber, CryptXXX, Cryptowall, …

Source: Cisco MCR and Goggle research report


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 or 24

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

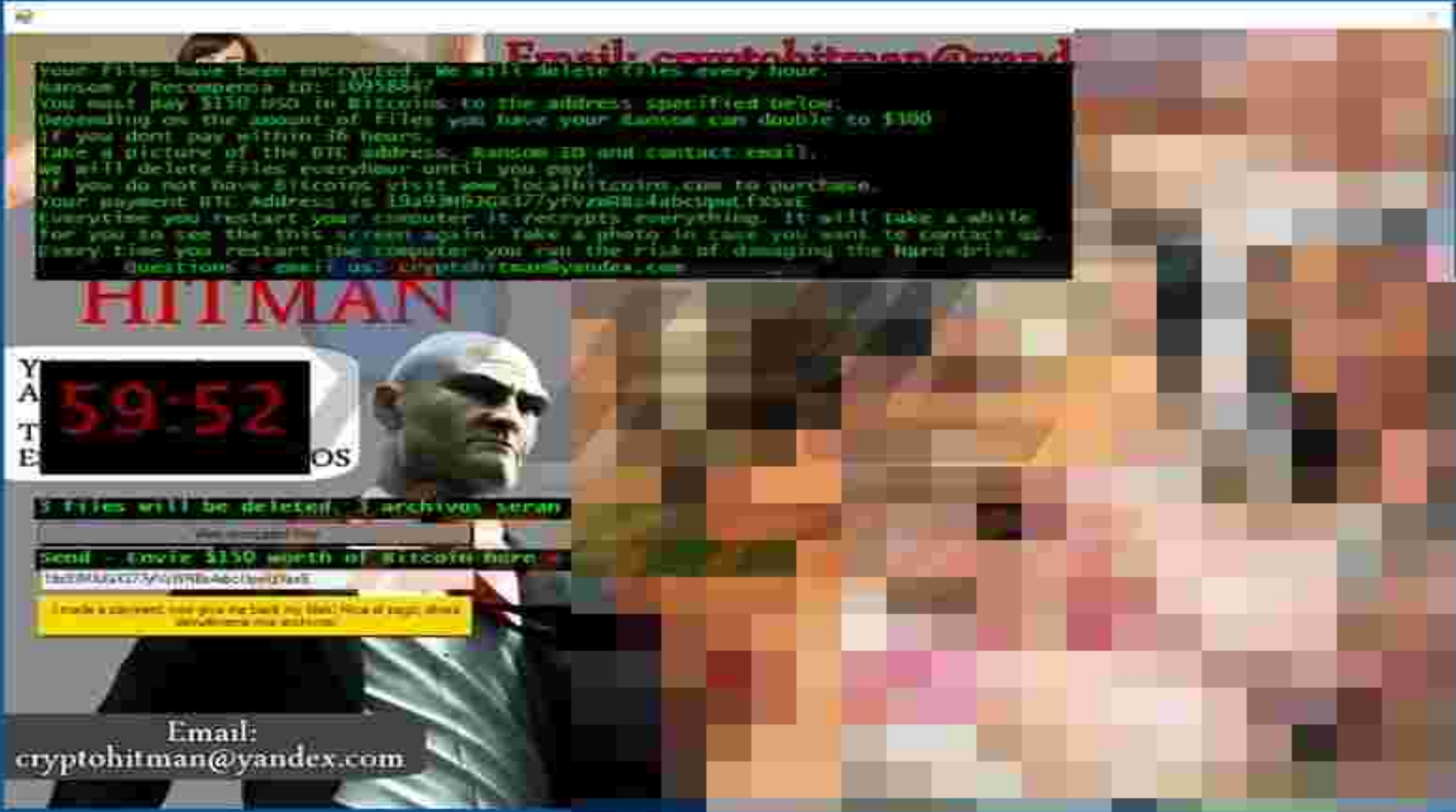
1 file will be deleted.

View encrypted files

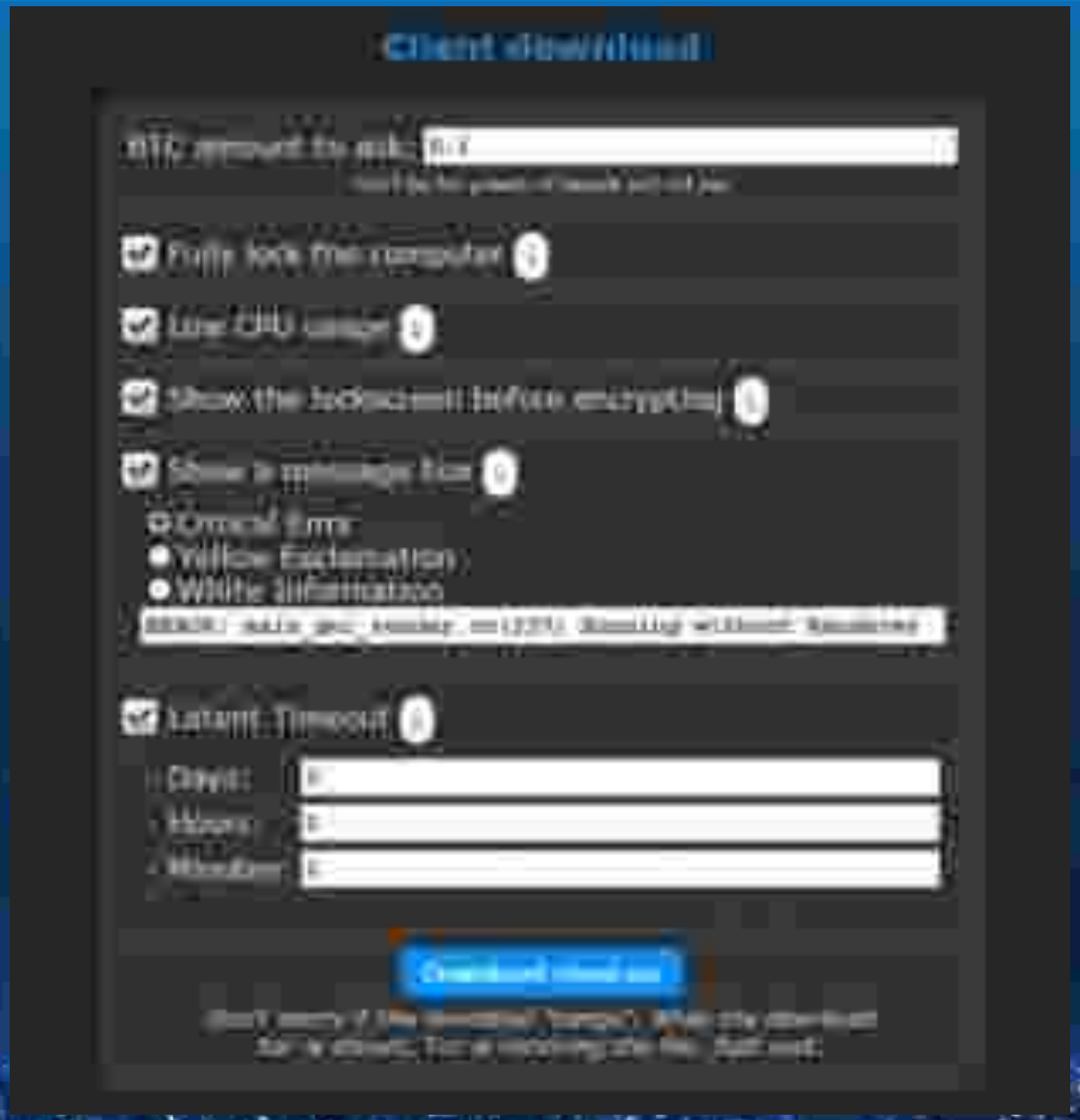
Please, send $150 worth of Bitcoin here:

15fbyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ

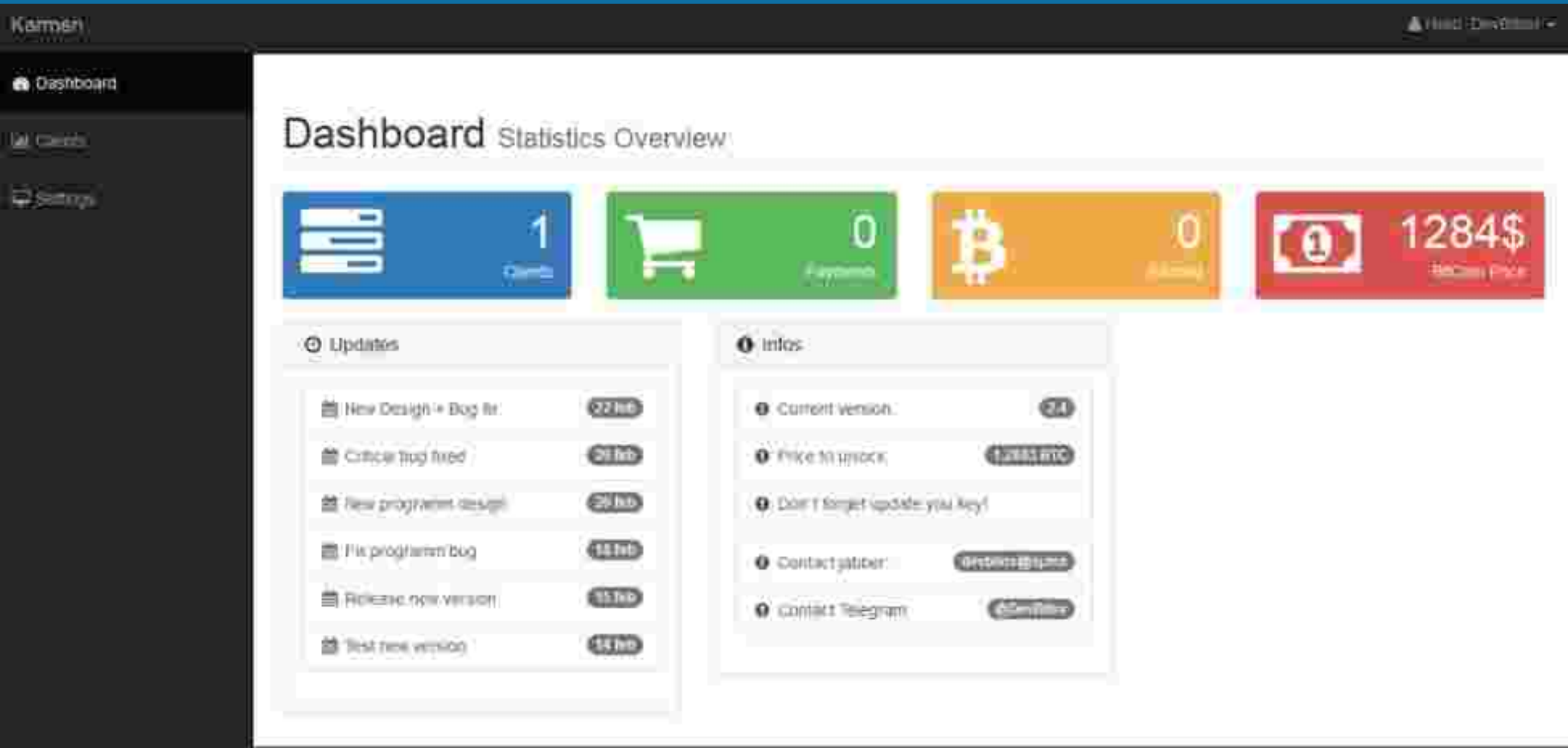
I made a payment, now give me back my files!


Your files have been encrypted. We will delete files every hour.
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 to purchase.
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.
HITMAN
59:52
files will be deleted
Send - Envie $150 worth of Bitcoin here
Email:
cryptohitman@yandex.com

RaaS

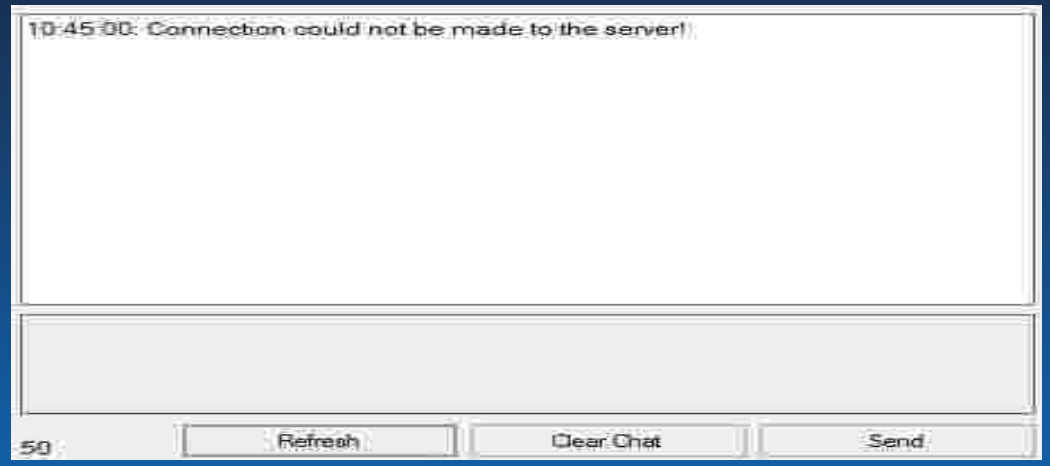


RaaS: Karmen

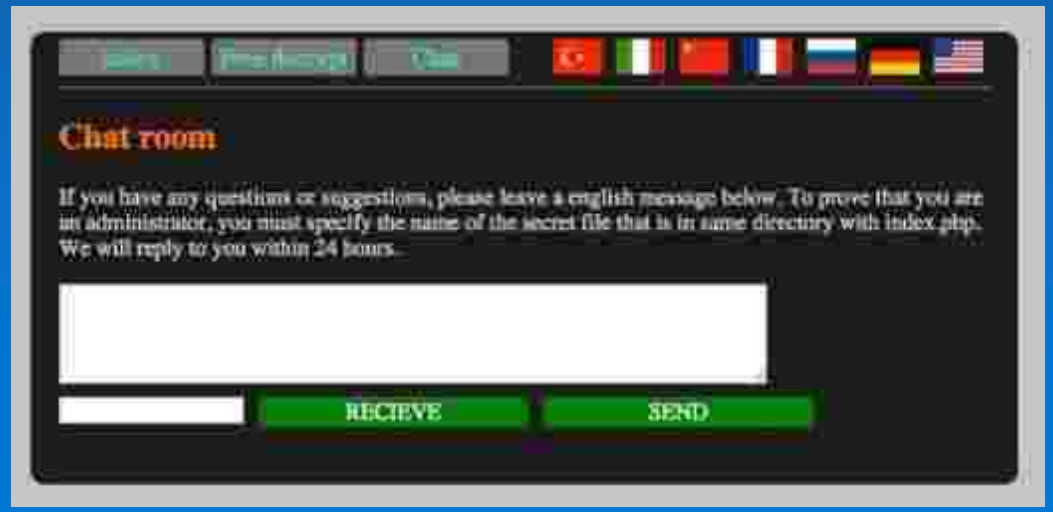

Karmen
Dashboard
Dashboard Statistics Overview
1
0
0
1284$
Updates
Infos

Live Chat with customer services

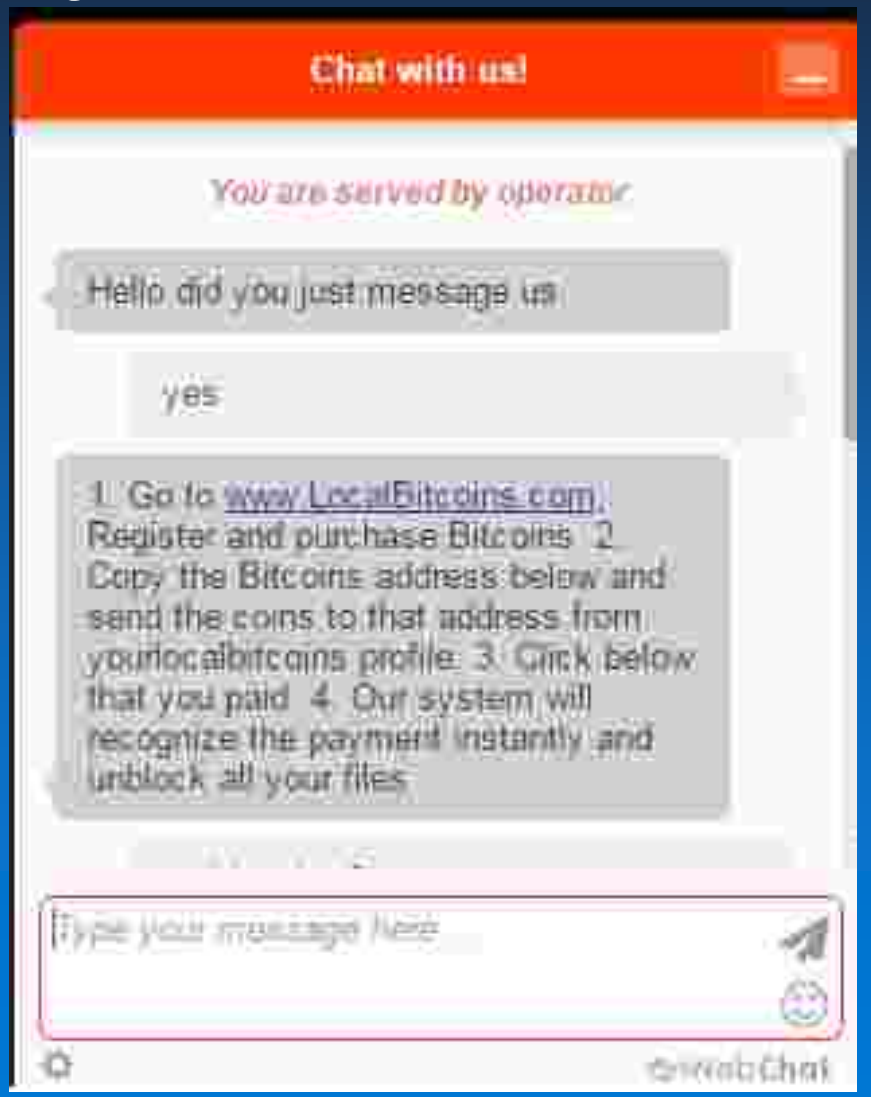
Padcrypt



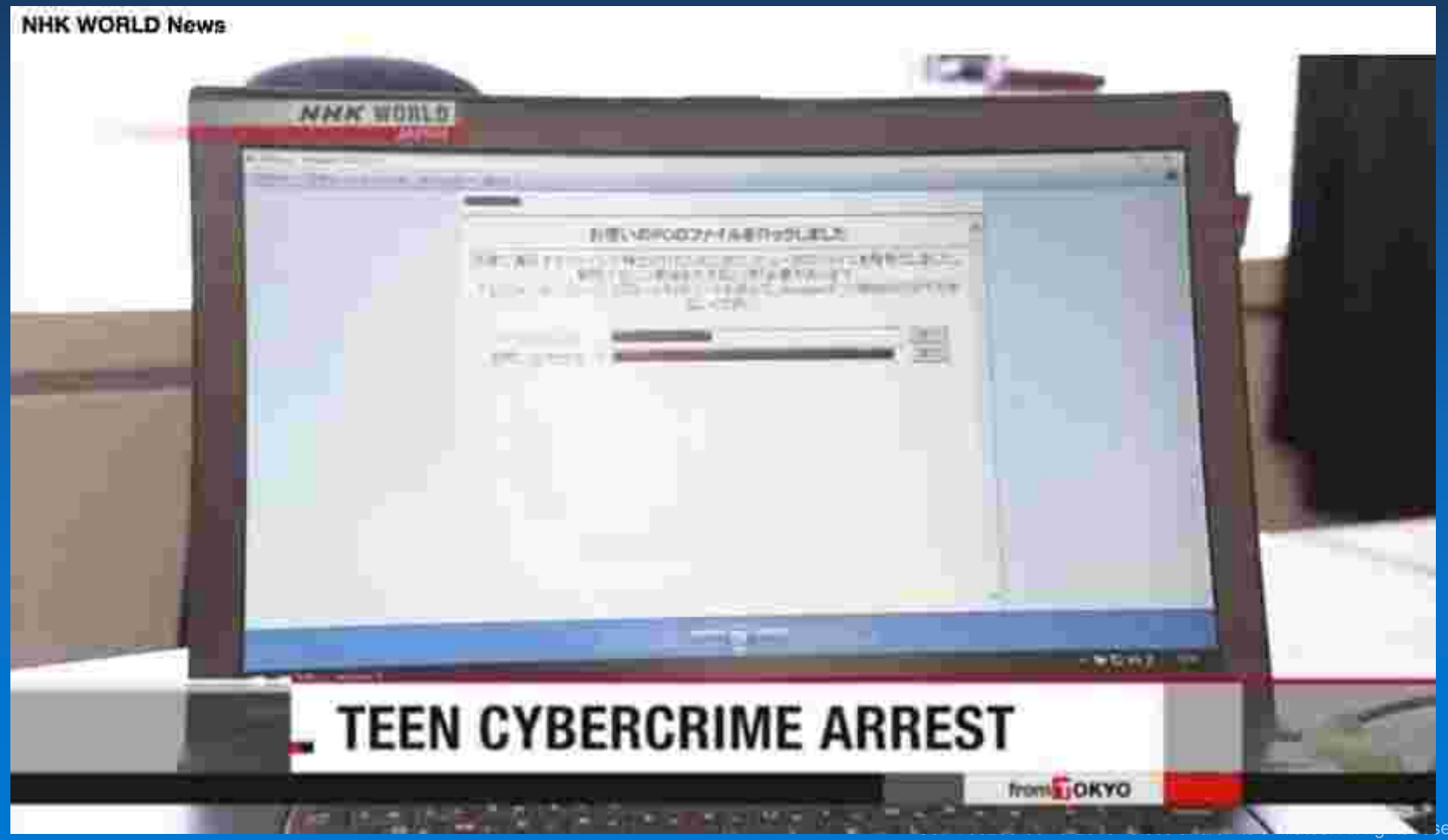
CTB-Locker

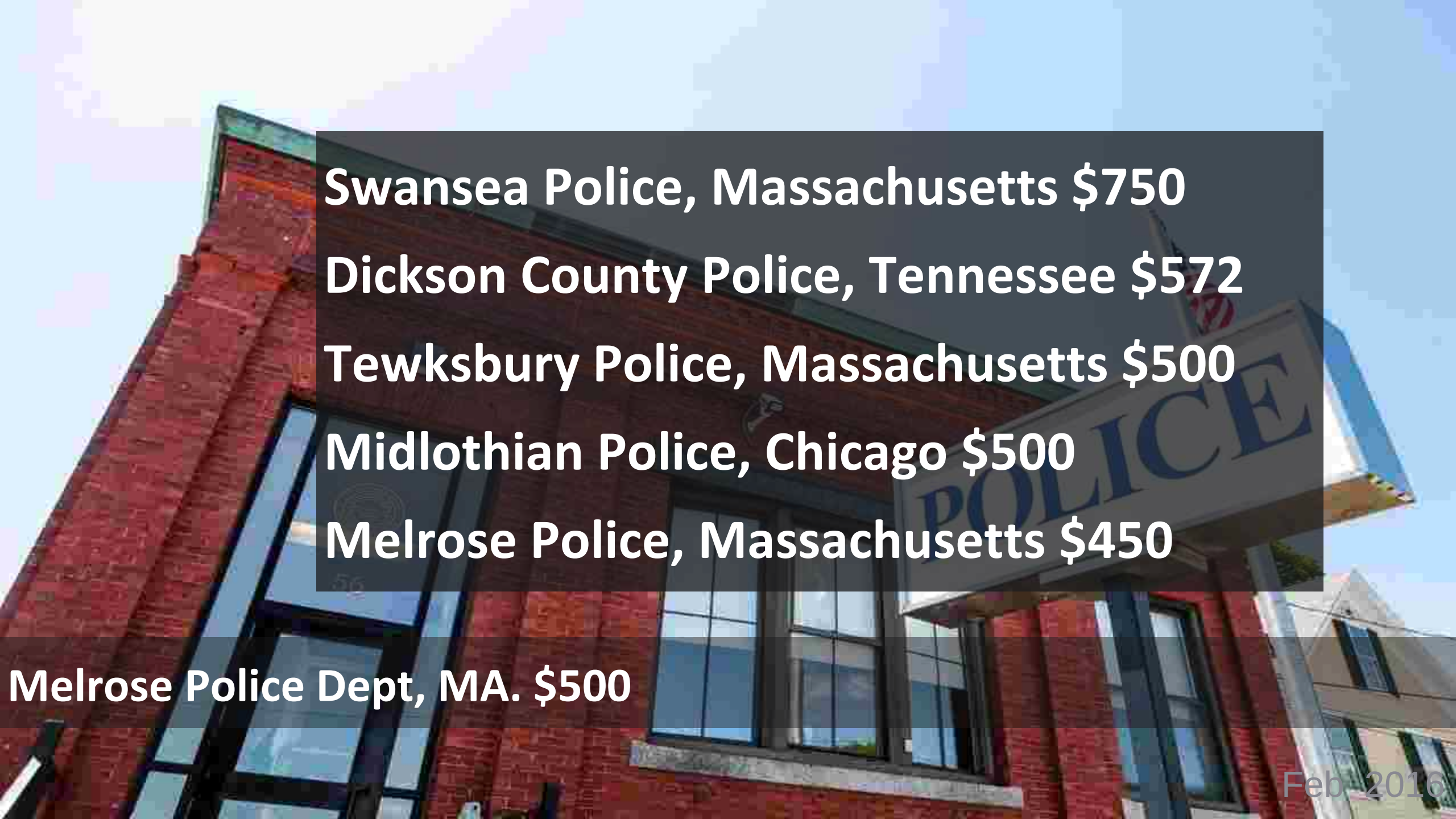


Jigsaw



14-Year-Old Japanese Boy Arrested for Creating Ransomware





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

[redacted]

- 工學院某老師
  - 釣魚信件騙取密碼

寄件者：support@sth.edu.hk
主旨：重要提示：親愛的電子郵件帳戶的用戶
內容：
您的郵箱已超過管理員設置的默認存儲限制，
您目前正在運行的低，你可能無法發送或接收新郵件，
直到您重新驗證您的郵箱。
重新驗證您的郵箱，請點擊下面的鏈接，
並正確填寫所需的所有信息：
http://redcliffebedandbreakfast.com/wp-info/webmail.html
謝謝
系統管理員

駭客

利用盜取之帳號密碼

學校郵件主機
名譽評等降級
寄外信件遭退

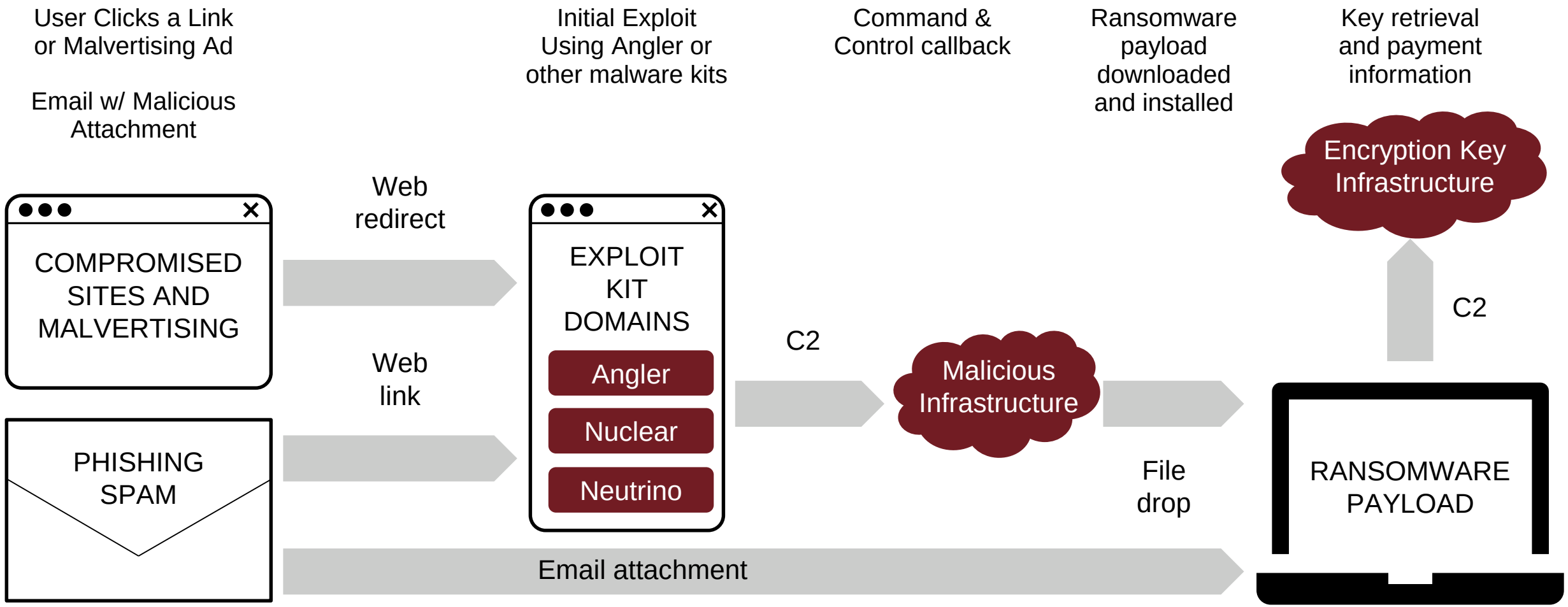
請點擊” 鏈接”

重新驗證畫面

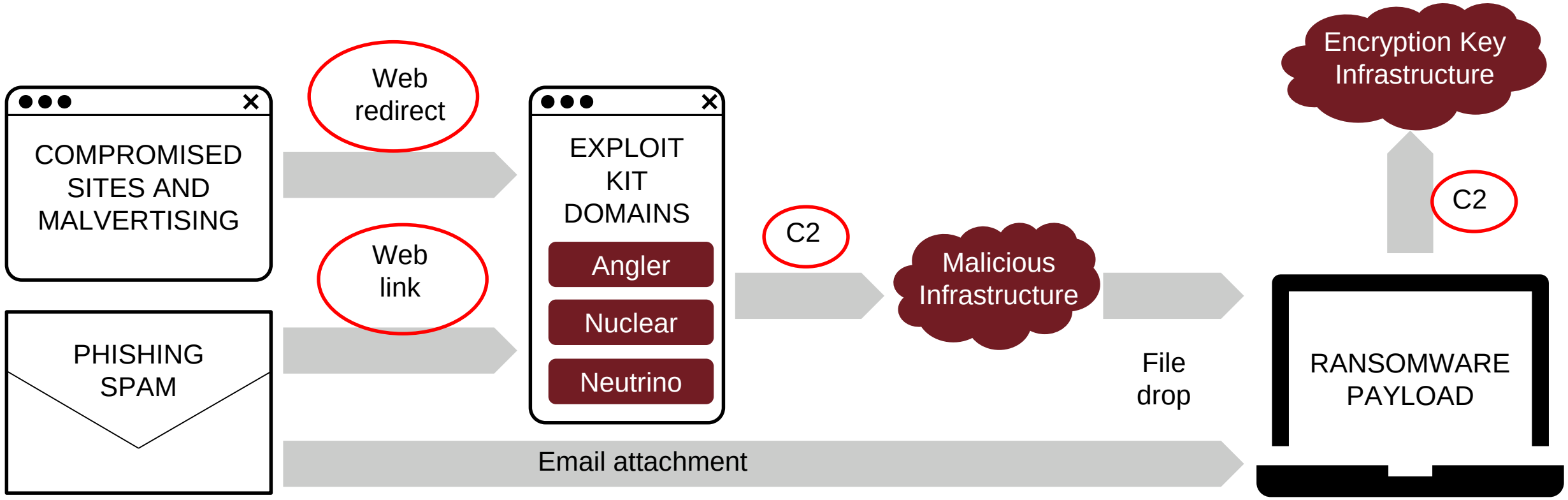
帳號密碼取得

We have FW,
and we have Anti-Virus

How Ransomware Works



Most Ransomware Relies on DNS and C2 Callbacks



	Encryption C&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

Predictive

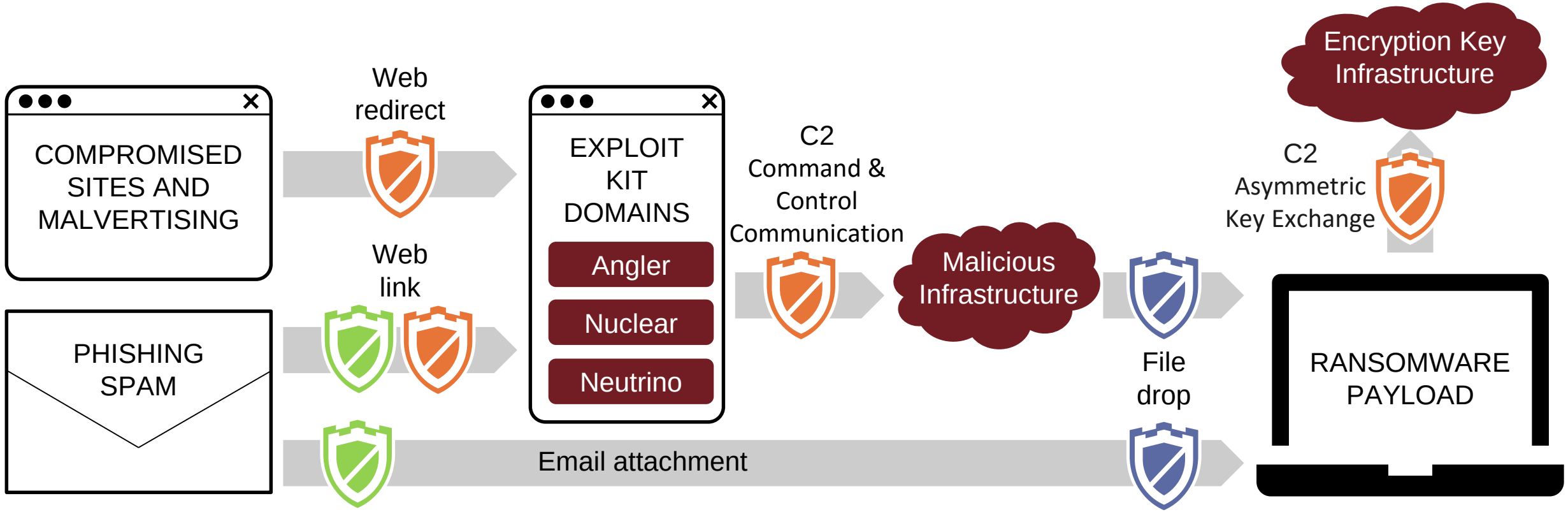
100B	85M	12K	160+
requests per day	daily active users	enterprise customers	countries worldwide

CRYPTOLOCKER

The "Ripple Effect" by OpenDNS Research

https://youtu.be/acwD_OA3QZ4

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



Blocked by Cisco Cloud Email Security with AMP Threat Grid

Blocked by Cisco Umbrella (Cloud DNS Security)

Blocked by Cisco AMP for Endpoints (Host Anti-Malware) Detection with Threat Grid

14 Day Free Trial of Cisco Umbrella

Get started in 30 seconds

No credit card or phone call required

WHAT IS INCLUDED?

- Threat protection like no other – block malware, C2 callbacks, and phishing.
- Predictive intelligence – automates threat protection by uncovering attacks before they launch.
- Worldwide coverage in minutes – no hardware to install or software to maintain.
- Weekly security report – get a personalized summary of malicious requests & more, directly to your inbox.

All fields are required

First name

Last name

Company Email

Company Phone

Company Name

Select your country

Are you an MSP, IT services provider or reseller? No

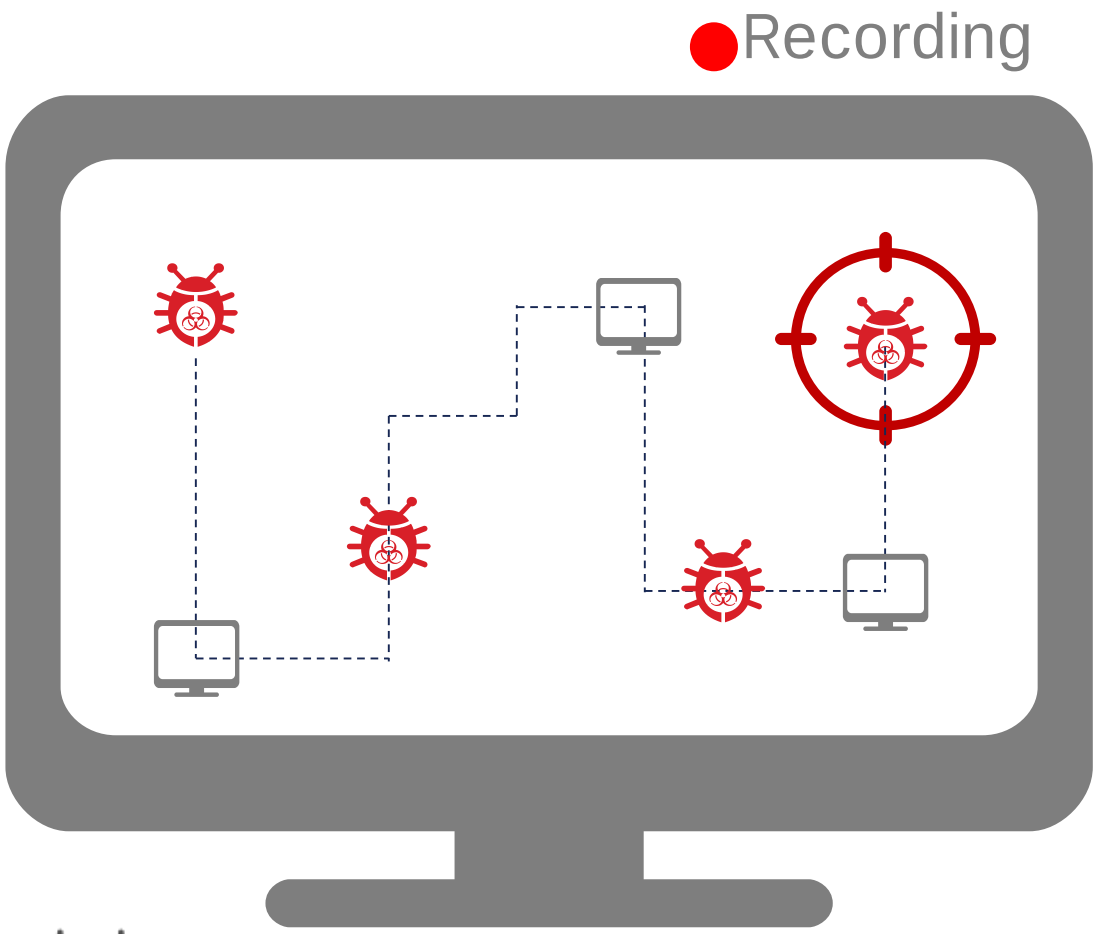
CREATE MY TRIAL

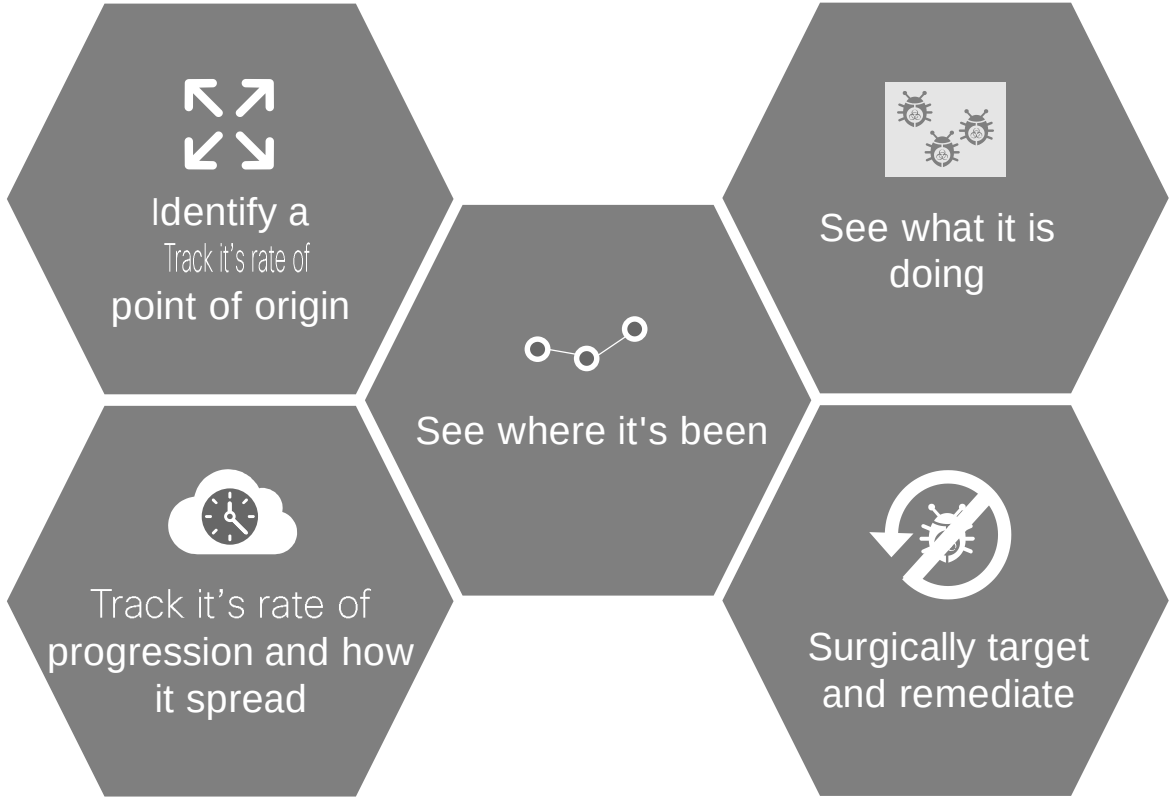
By clicking "Create my trial", you agree to the Umbrella Terms of Service and Privacy Policy and you understand that your personal information may be transferred for processing outside your country of residence, where standards of data

Continuous Analysis and Retrospective Security

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

Monitor
+
Detect

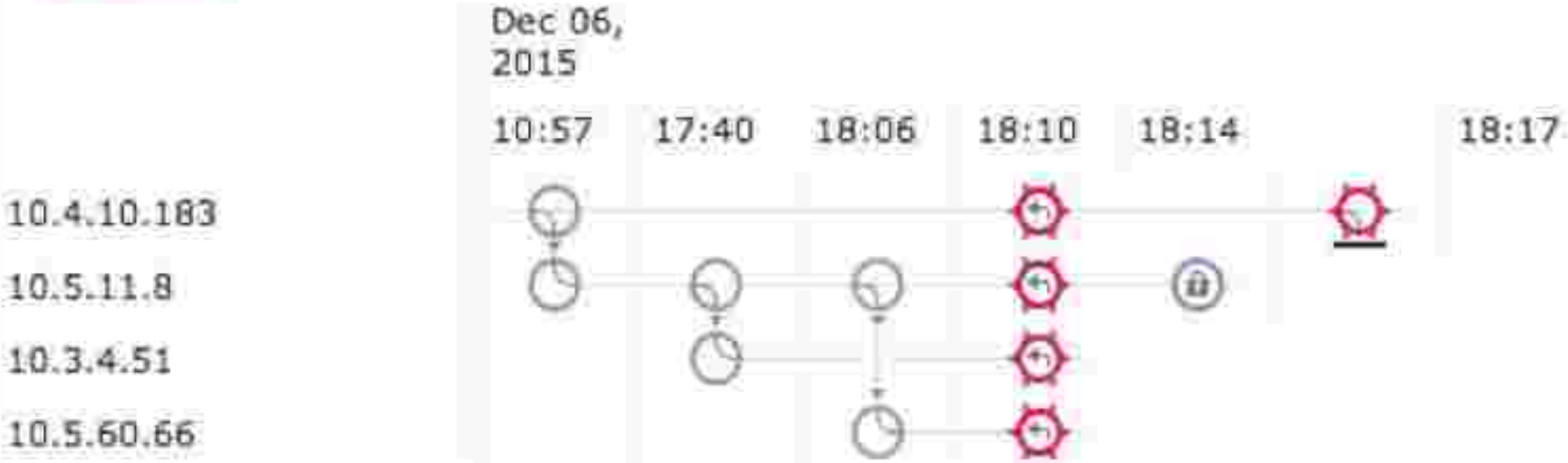




Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High
First	
Last	
Event	
Seen	
Seen	

Trajectory



What customers are saying about AMP for Endpoints

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

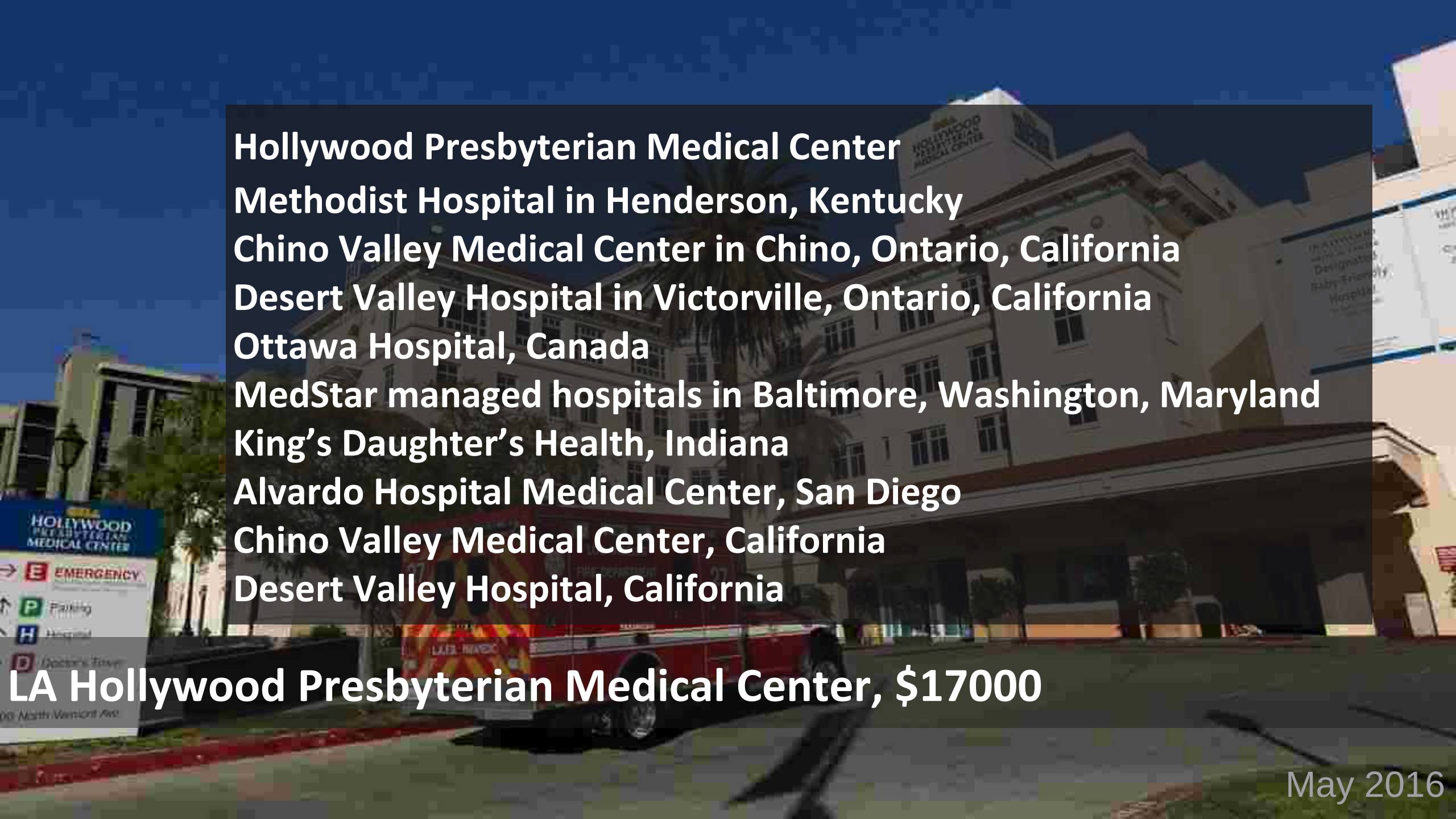
CISCO

Ransomware 2.0

Targeted Ransomware (APT)

Crytoworm

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
Alvardo 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


Out Of Service
tickets
Out Of Service
tickets


You Hacked,ALL Data Encrypted,Contact For Key(crypton27@yandex.com)ID:601 .Enter
Key:
Missing operating system_


SFMTA
muni
METRO
FREE
A
B
C
D
E
F
G
H
I
J
▼CANCEL
▼TAP BELOW

ov 2016

NAYANA

COMMUNICATION

메인 사이트의 트래픽 과부하로 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>

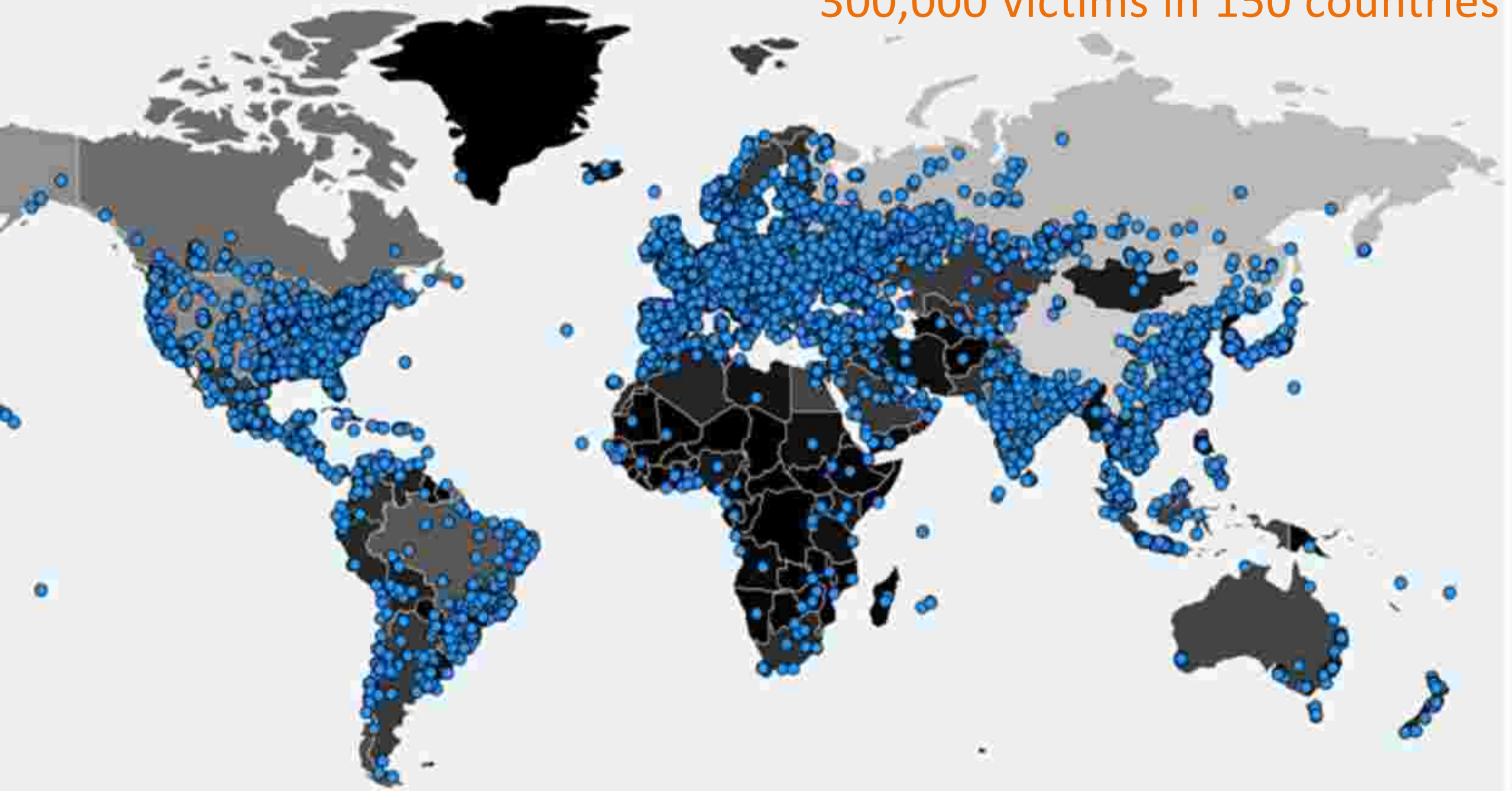
12/5/2017


We're currently experiencing significant problems with our IT and telephone network
DELL

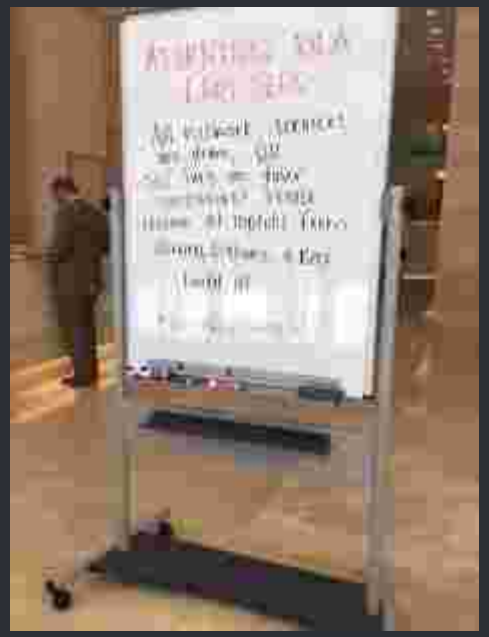

Abfahrt
Linie
Nach
Gleis
Über
Qlbernhau
Hbf
(S) Hbf
g-B. Süd
Aue (Sachs)
Dresden Hbf


Deaigua

300,000 victims in 150 countries



NotPetya / Petrwrap / Nyetya



27/6/2017

Reckitt Benckiser - $117 million

Maersk - $200-$300 million

Fedex and TNT: $300 million

Merck: $310 million

Why so powerful?

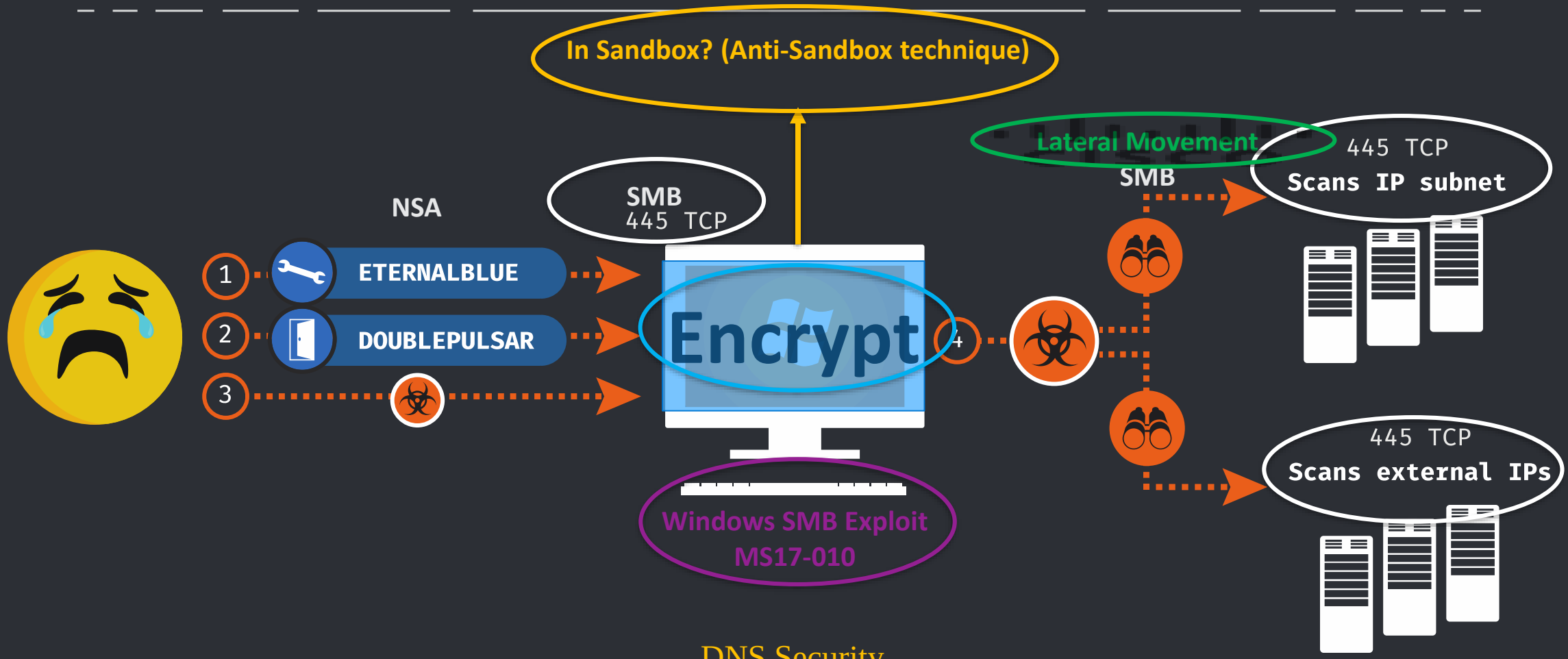
WannaCry = Ransomware + Exploit + Worm

WannaCry

In Sandbox? (Anti-Sandbox technique)
Check domain (Kill Switch)

Windows SMB Exploit
MS17-010

WannaCry Defense



NGFW/IPS/AMP

Email Security

DNS Security

Endpoint security

NGFW/IPS/AMP

Identity, Posture & SD-Segmentation

Network Visibility, Behavior Analysis

Timeline of 'WannaCry' Ransomware Defense

Microsoft Security Bulletin
March 14th, 2017

On March 14th, Microsoft released a patch (MS17-010) for a new SMB vulnerability.

Cisco NGFW | Meraki MX
March 14th, 2017

On the same day, Cisco Talos released Snort signature #41978 to detect vulnerabilities identified in MS17-010.

Shadow Brokers
April 14th, 2017

A group known as "The Shadow Brokers" released a set of vulnerabilities allegedly sourced from the National Security Agency (NSA) that go by the names of Eternal Blue and Double Pulsar.

Cisco NGFW | Meraki MX
April 25th, 2017

Talos releases Snort signatures #42329, #42332, #42340 for Double Pulsar and Anonymous SMB shares.

TALOS

Cisco TALOS

With more than 250 world class researchers around the globe and a global network of intelligence and data sources, Cisco continues to monitor, research, and protect customers against "WannaCry" and other emerging threats.

Cisco Umbrella
May 12th, 2017 | 10:12 UTC

Cisco Umbrella adds attribution of the attack type to ransomware and moves the kill switch domain to the malware category.

Cisco AMP
May 12th, 2017 | 9:33 UTC

Approximately 80 minutes after the first seen samples, AMP detected the ransomware. Threat was detected via automatic analysis rules and low prevalence methods.

AMP successfully detected and blocked on endpoints, email and web gateways and network security.

Cisco Umbrella
May 12th, 2017 | 7:43 UTC

Cisco Umbrella pushes kill switch domain globally into Newly Seen Domains categories which resulted in protection against the ransomware and spreading of the worm.

Cisco Investigate
May 12th, 2017 | 7:30 UTC

MalwareTech Blog releases information about a new attack dubbed "WannaCry" on Twitter and the blog.

Cisco Investigate screenshot was included in the blog as it was used as a part of the intelligence collection and discovery.

Best Practices – Things I Can Do!

1. Do you have good disaster recovery (People/Process/Tools)? Train to implement it on a regular basis.
2. Do you have good offline back ups? Test them regularly.
3. Patch your systems, update your AV ASAP
4. Additional layer of defense such as DNS (Umbrella) and Anti-malware solution
5. End of life hardware / software?
6. Educate users on emails with links and attachments

Ransomware Defense for Dummies

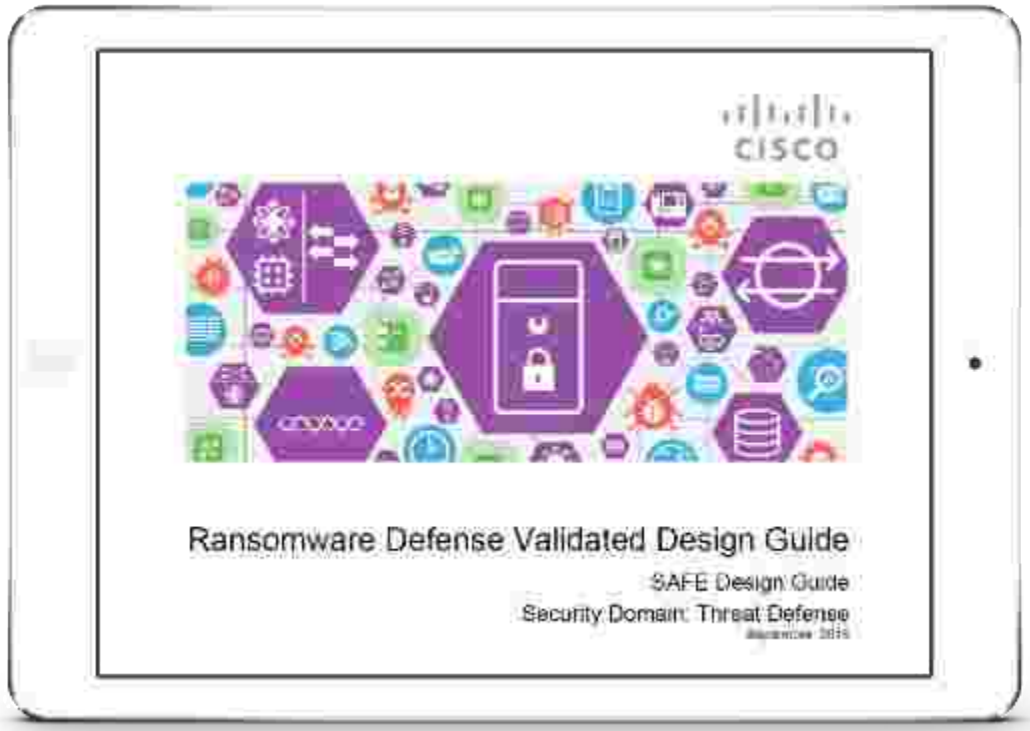
www.cisco.com/go/ransomware

Ransomware Defense Prevention Validation

Tested against >20 REAL Ransomware Attack families to validate the solution

- Cisco Umbrella
- Cloud Email Security w/AMP
- AMP for Endpoints
- AMP ThreatGrid

Cloud and software solution that enables quick deployment and protection



www.cisco.com/go/safe

https://mkto.cisco.com/Security-Scholarship.html

$10 Million in Cisco Global Cybersecurity Scholarships!

In our digital era, organizations are relying increasingly on cybersecurity to protect themselves, enable trust, move faster, add value, and grow. As the volume and sophistication of cyberattacks rises, organizations are experiencing a significant shortage of IT professionals with cybersecurity skills.

To help close this security skills gap, Cisco is introducing the Global Cybersecurity Scholarship program. Cisco will invest $10 million in this program to increase the pool of talent with critical cybersecurity proficiency. Cisco also has enhanced its Security certification portfolio with a new CCNA Cyber Ops certification.

Thank you very much for your interest in the Cisco Global Cybersecurity Scholarship program. We will reopen registration for the Cybersecurity Scholarship in the fall of 2017. Please fill out the form below if you are interested in applying for the scholarship program, and we will notify you of next steps when registration opens.

Cisco Networking Academy,

a Cisco Corporate Social Responsibility program, is an IT skills and career building program available to learning institutions and individuals worldwide.

The Networking Academy Learning Portfolio

Current & Planned

Aligns to Certification

Instructor Training required

Self-paced

* Available within 12 months

Collaborate for Impact

Introduction to Packet Tracer | **Packet Tracer** | **Hackathons** | **Prototyping Lab** | **NetRiders** | **Internships**

	Exploratory	Foundational	Career-Ready
Networking		**Networking Essentials** **Mobility Fundamentals**	**CCNA R&S:** Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks **CCNP R&S:** Switch, Route, TShoot **Emerging Tech Workshop:** Network Programmability*
Security	**Introduction to Cybersecurity**	**Cybersecurity Essentials** **IoT Security***	**CCNA Security** **CCNA Cyber Ops***
IoT	**Introduction to IoT**	**IoT Fundamentals:** Connecting Things, Big Data & Analytics Hackathon Playbook	
OS & IT	**NDG Linux Unhatched**	**NDG Linux Essentials** **IT Essentials**	**NDG Linux I** **NDG Linux II**
Programming		**CLA: Programming Essentials in C** **CPA: Programming Essentials in C++** **PCA: Programming Essentials in Python*** **Emerging Tech Workshop:** Collaboration / Spark API*	**CLP: Advanced Programming in C*** **CPP: Advanced Programming in C++***
Business	**Be Your Own Boss**	**Entrepreneurship**	
Digital Literacy	**Get Connected**		

Specifically for Self-Paced Courses

Networking

- Packet Tracer 101
- Packet Tracer 101 Mobile
- Introduction to Packet Tracer

IoT

- Introduction to IoT
- Introduction to the Internet of Everything

Security

- Introduction to Cybersecurity
- Cybersecurity Essentials

Business Literacy

- Entrepreneurship

Digital Literacy

- Get Connected

To get this slide and more about NetAcad Program, pls leave your contact by scanning this QR code:

Garrick Ng - CTO: garng@cisco.com
Shania Ting - Security Sales Manager: hoting@cisco.com
Tommy Mak - Security Consultant : tomak@cisco.com
Eric Tsoi - Security Consultant: eritsoi@cisco.com

Garrick Ng - CTO: garng@cisco.com
Shania Ting - Security Sales Manager: hoting@cisco.com
Tommy Mak - Security Consultant : tomak@cisco.com
Eric Tsoi – Security Consultant: eritsoi@cisco.com