Ransomware- success stories
Triangle InfoSeCon

Karishma Mehta
MS in computer Science
Business Information Security Officer, BB&T
cs_karishma@yahoo.com

Outline

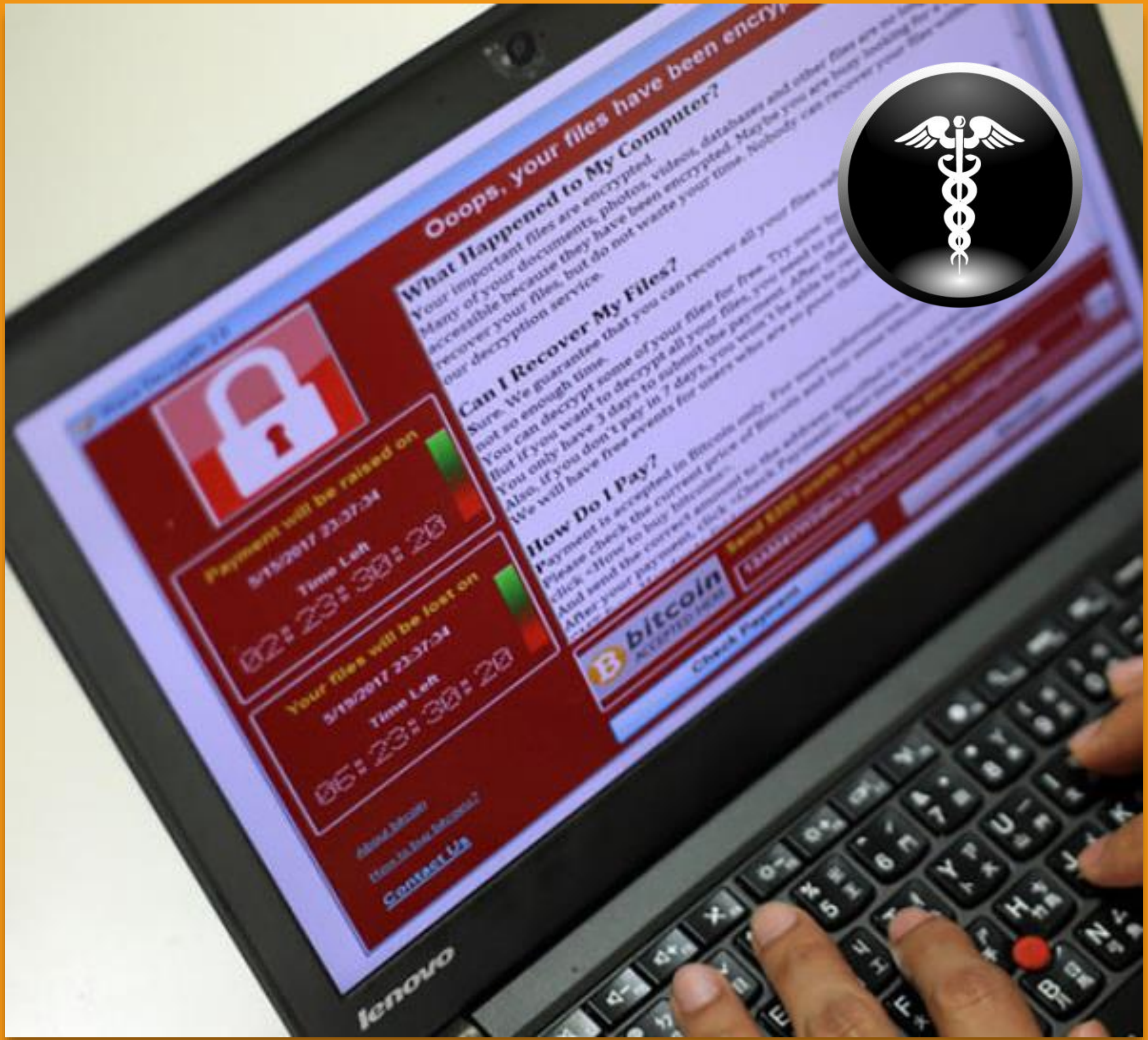
- Real life ransomware cases
- Introduction
- Trend & Statistics
- Attack vectors
- Success stories: ransomware mitigation stratergies
- Where we go from here- unknowns and future direction

Outline

- Real life ransomware cases
- Introduction
- Trend & Statistics
- Attack vectors
- Success stories: ransomware mitigation stratergies
- Where we go from here- unknowns and future direction

Case # 1 Medical Office

A dentist office in California logged on to the office computer 2018 and was greeted by this message:



Case # 2 : Law firm

Law firm in Australia fell victim to a ransomware attack, reporting that mailbox and over 44,000 files on SharePoint totaling over 5GB of data were locked down with a ransom note asking for $6,000 USD for the key to unencrypt

Case # 3 Entertainment

Tony Casala heading Children in Film works as an advocate for young actors and their families. Just before New Year's Eve, an employee opened an email attachment that appeared to be an invoice. Thirty minutes later, nobody in Casala's firm could access any of the company's 4,000+ files stored on the cloud drive

https://krebsonsecurity.com/2016/01/ransomware-a-threat-to-cloud-services-too/

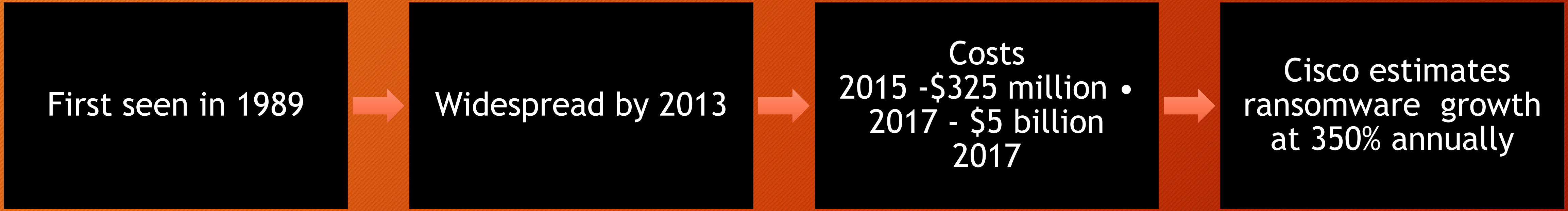
Outline

- Real life ransomware cases
- Introduction
- Trend & Statistics
- Attack vectors
- Success stories: ransomware mitigation strategies
- Where we go from here- unknowns and future direction

Pre-existing knowledge – What's Ransomware

- Ransomware
- WannaCry,Petya,CryptoLocker,and TeslaCrypt are some of the more notable examples of such ransomware.
- In general, modern ransomware are known to only encrypt user data files (e.g..xlsx,.docx,.jpg,.pptxetc.)
- Leave system files (e.g..dll) to meet the ransom demand
- The growing popularity of cryptocurrency allows ransomware developers to extort money anonymously

Quick history on Ransomware



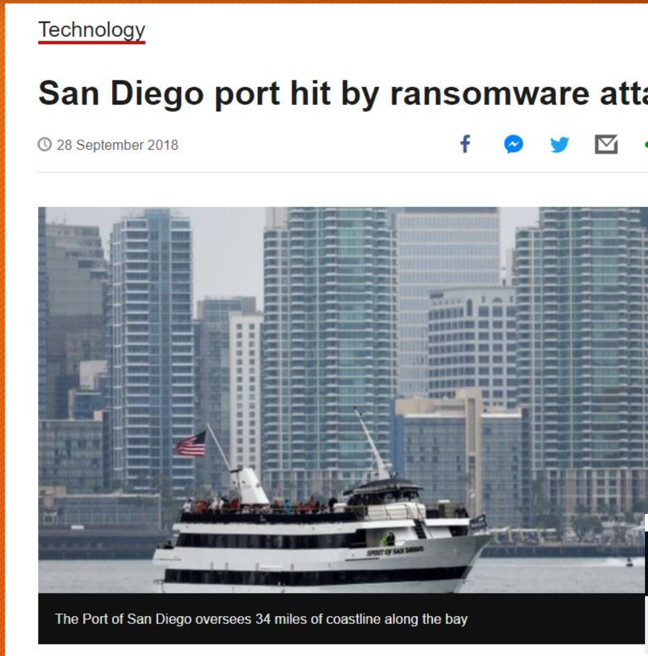
First seen in 1989

Widespread by 2013

Costs
2015 -$325 million •
2017 - $5 billion
2017

Cisco estimates ransomware growth at 350% annually

In the news

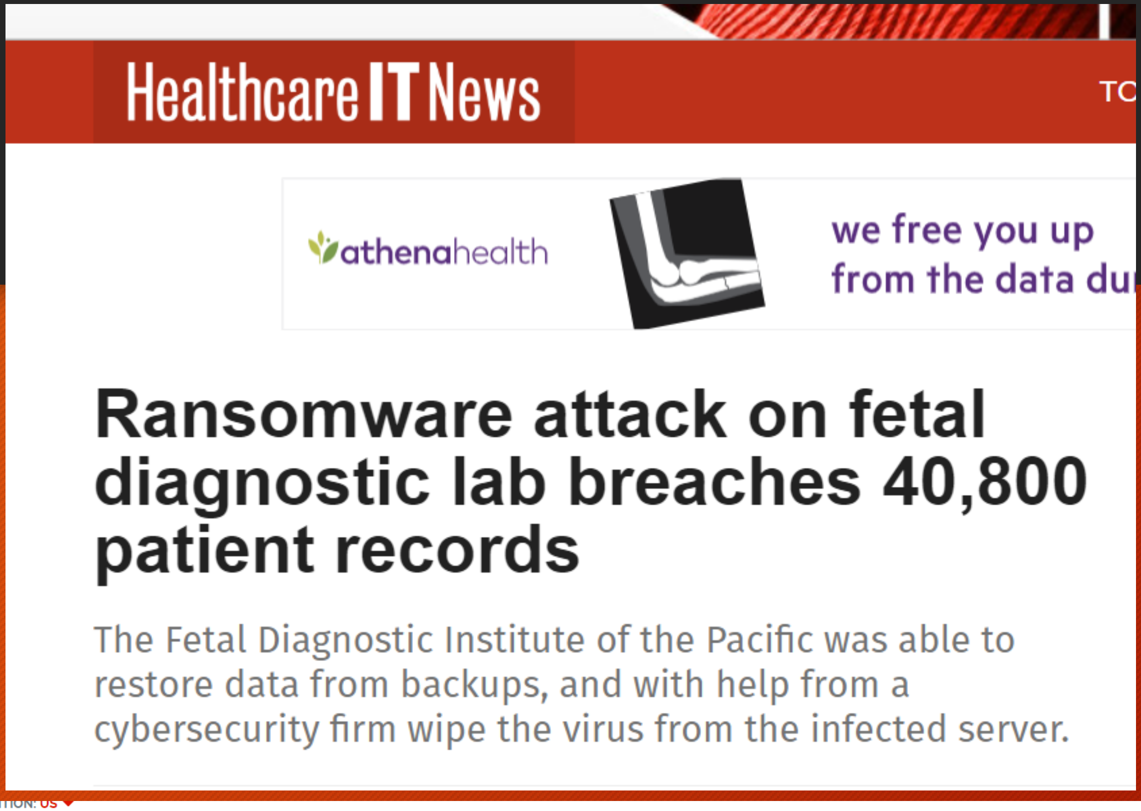


Technology

San Diego port hit by ransomware attack

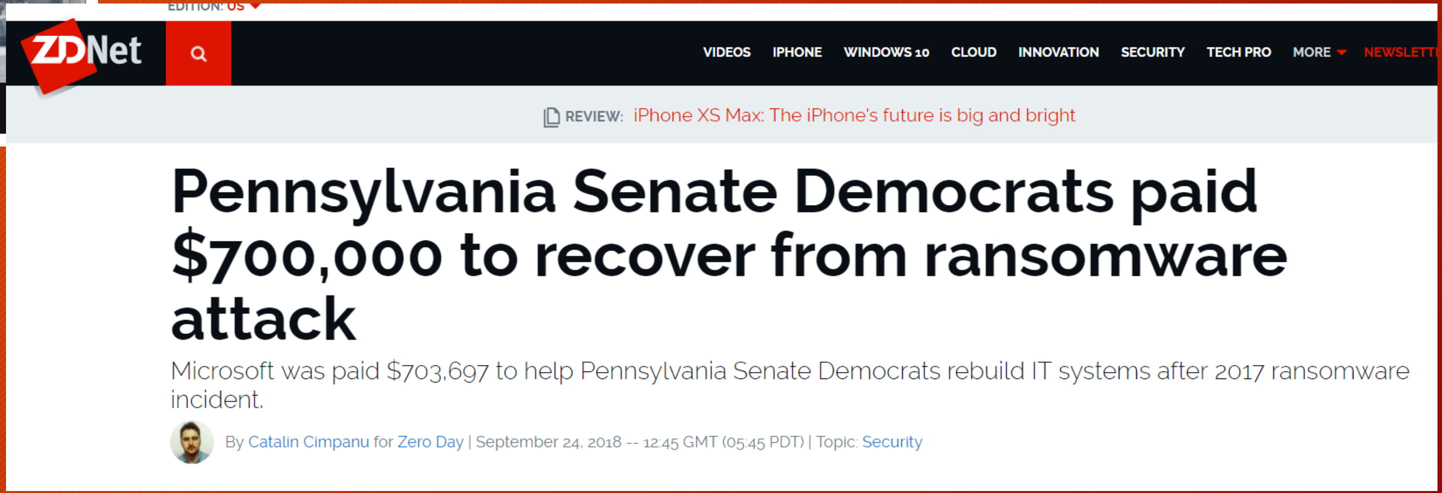
28 September 2018

The Port of San Diego oversees 34 miles of coastline along the bay



Ransomware attack on fetal diagnostic lab breaches 40,800 patient records

The Fetal Diagnostic Institute of the Pacific was able to restore data from backups, and with help from a cybersecurity firm wipe the virus from the infected server.



REVIEW: iPhone XS Max: The iPhone's future is big and bright

Pennsylvania Senate Democrats paid $700,000 to recover from ransomware attack

Microsoft was paid $703,697 to help Pennsylvania Senate Democrats rebuild IT systems after 2017 ransomware incident.

By Catalin Cimpanu for Zero Day | September 24, 2018 -- 12:45 GMT (05:45 PDT) | Topic: Security

Outline

- Real life ransomware cases
- Introduction
- Trend & Statistics
- Attack vectors
- Success stories: ransomware mitigation strategies
- Where we go from here- unknowns and future direction

Trend in Ransomware

- Ransomware will cost $6 trillion annually by 2021
- Increased attacks against Linux, Mac's and cloud based systems
- Ransomware as a service (RaaS) will gain popularity

Ransomware statistics that every business should know

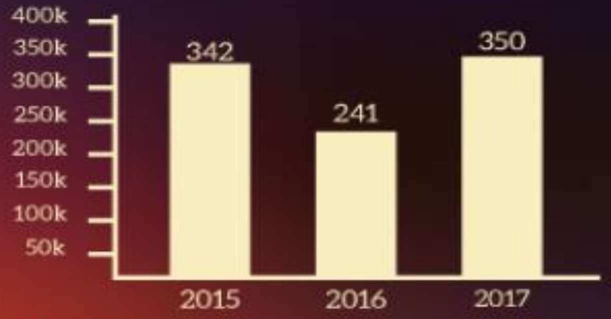
30% of
Ransomware attacks fell over the past 12 months.

In **2017**,
the number of ransomware families dropped 71%, but the number of variants increased 46%.

75% of
organizations infected with ransomware were running up-to-date endpoint protection.

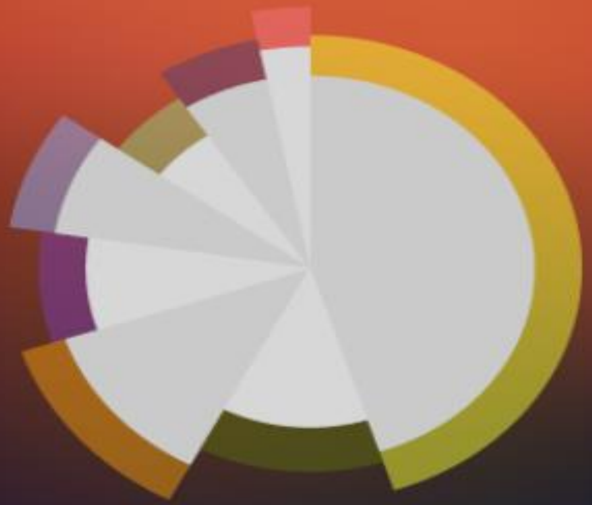
$133,000 was
the average cost per ransomware attack to businesses in 2017.

Ransomware is at a crossroads in 2018, with attacks decreasing in volume but increasing in sophistication. Here are some the latest stats and trends you need to know to ensure your company stays protected.



New Ransomeware Variants 2015 - 2017

2017 Ransomeware Incidents by Industry



■	Healthcare	45%
■	Financial	12%
■	Professional Services	12%
■	Other*	8%
■	Manufacturing	7%
■	Education	6%
■	Retail	6%
■	Hospitality	4%

Source : blog.barkly.com/ransomware-statistics-2018

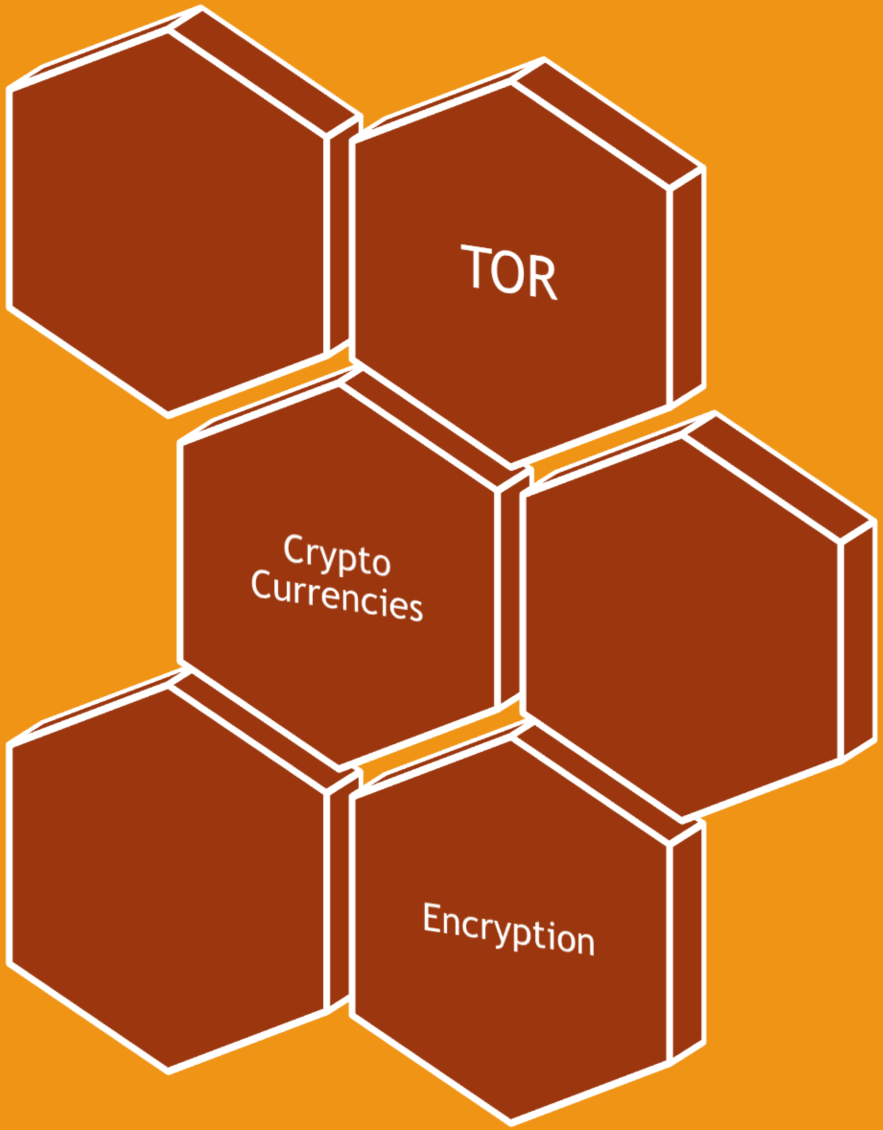
Outline

- Real life ransomware cases
- Introduction
- Trend & Statistics
- Attack vectors
- Success stories: ransomware mitigation strategies
- Where we go from here- unknowns and future direction

Attack vectors

Email	Phishing Attachments
Visiting compromised unpatched websites	Old browser Outdated plug ins
Downloading free software & games	Minecraft - mod

Basic Enablers



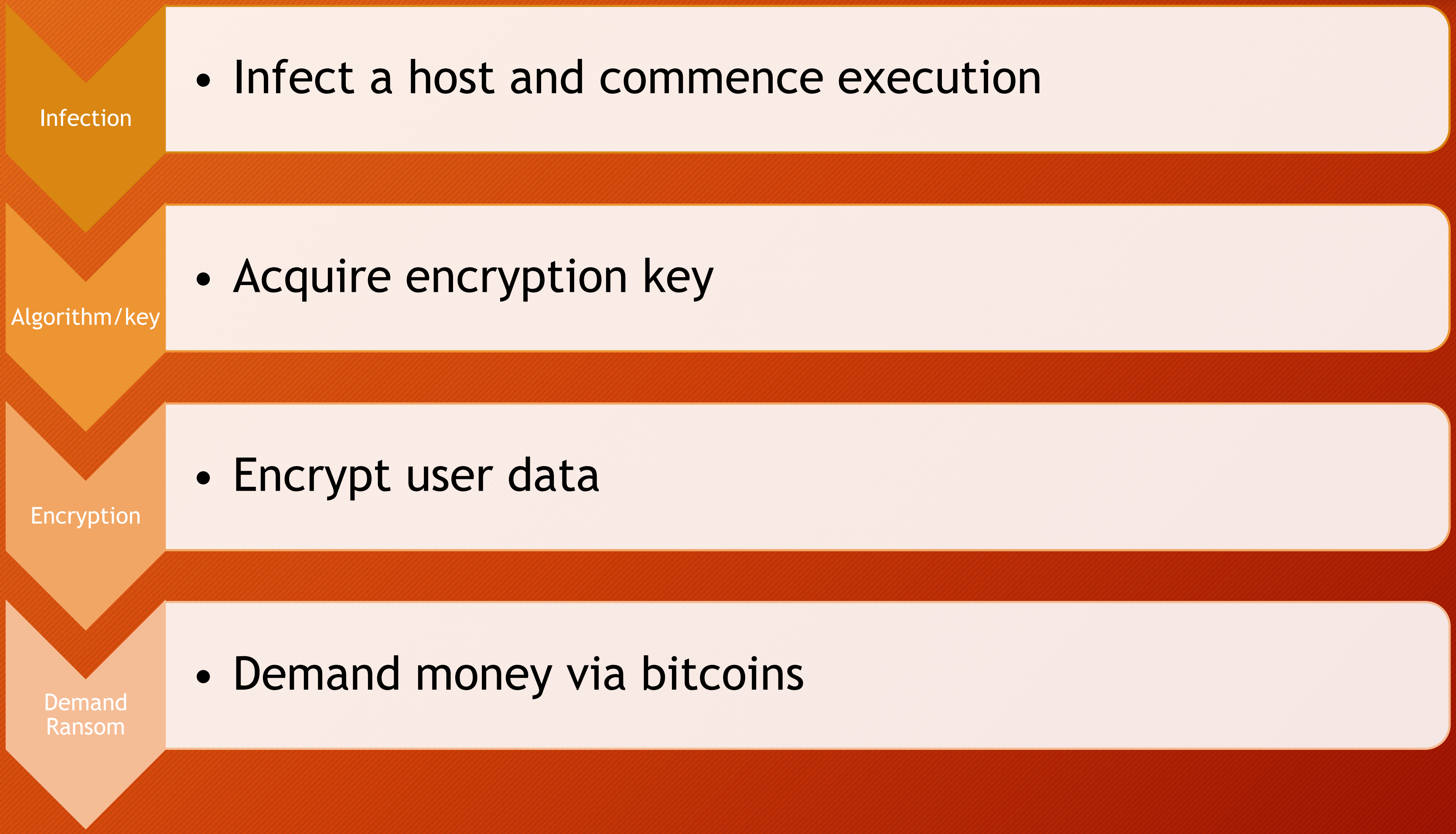
Outline

- Real life ransomware cases
- Introduction
- Trend & Statistics
- Attack vectors
- Success stories: ransomware mitigation strategies
- Where we go from here- unknowns and future direction

Lets understand Ransomware first: Key steps

- Create testbed for existing ransomware
- Understand and define types of ransomware
- Study typical ransomware behavior
- Identify tele-tell signs of ransomware
- Analyze decryption key management
- Successful creation of mitigation tools and strategies

General steps for Ransomware (summary)



Infection

- Infect a host and commence execution

Algorithm/key

- Acquire encryption key

Encryption

- Encrypt user data

Demand Ransom

- Demand money via bitcoins

Cryptodrop

- vetted by external peer reviews and selected for publication at the 2016 IEEE International Conference on Distributed Computing Systems (ICDCS)
- **Microsoft Authenticode**
- Ransim
- Av-test- based on Germany
- Detects ransomware based on its behavior against user data

Cryptodrop testbed

Test bed includes 5,099 files in 511 directories

Originally 2,663 programs labeled as ransomware were executed

2,171 programs found to be inert and modified no files

Remaining 492 programs were then classified into variants of 14 different ransomware families

All 492 ransomware programs were detected & stopped

Maximum of 33 files encrypted in a single test

Minimum of 0 files encrypted in a single test

Median number of files lost was 10, or 0.2%

Source: https://www.cryptodrop.org/

3 types of Ransomware

Class A - Overwrite Files In Place - Overwrites the contents of the original file by opening the file, reading its contents, writing the encrypted contents *in-place*, then closing the file. It may optionally rename the file.

Class B - Moves Files - Extends Class A, with the addition that the malware *moves* the file out of the user’s documents directory (e.g., into a temporary directory). It then reads the contents, writes the encrypted contents, then moves the file back to the user’s directory.

Class C - Creates New File - Reads the original file, then creates a new, independent file containing the encrypted contents and deletes or overwrites (via a move) the original file. This class uses two independent access streams to read and write the data.

Source: https://www.cryptodrop.org/

Typical Ransomware behavior

- Execute multi-infection or process injection
- Encrypt files
  - AES uses symmetric encryption that is faster. Ransomware needs to securely deploy the key for performing the encryption and then conceal the key from victim until payment is made.
  - RSA uses asymmetric encryption that is lengthy and requires more space on host machine
  - Encryption trends in modern ransomware extortions have shifted from RC4 to RSA+AES to ECDH+AES
- Establish secure communication with C&C servers

Ransomware tale-tell sign

Indicator 1 - File Type Changes

Indicator 2 - Similarity Measurement

Strong encryption should produce output that provides no information about the plaintext content. Accordingly, we assume that the output of ransomware-encrypted user data is completely dissimilar to its original content.

Range 0 to 100

Indicator 3 - Shannon Entropy

Range 0 to 8

Entropy is a simple indicator that provides information about the uncertainty of data. Some types of data, such as encrypted or compressed data, are naturally high entropy

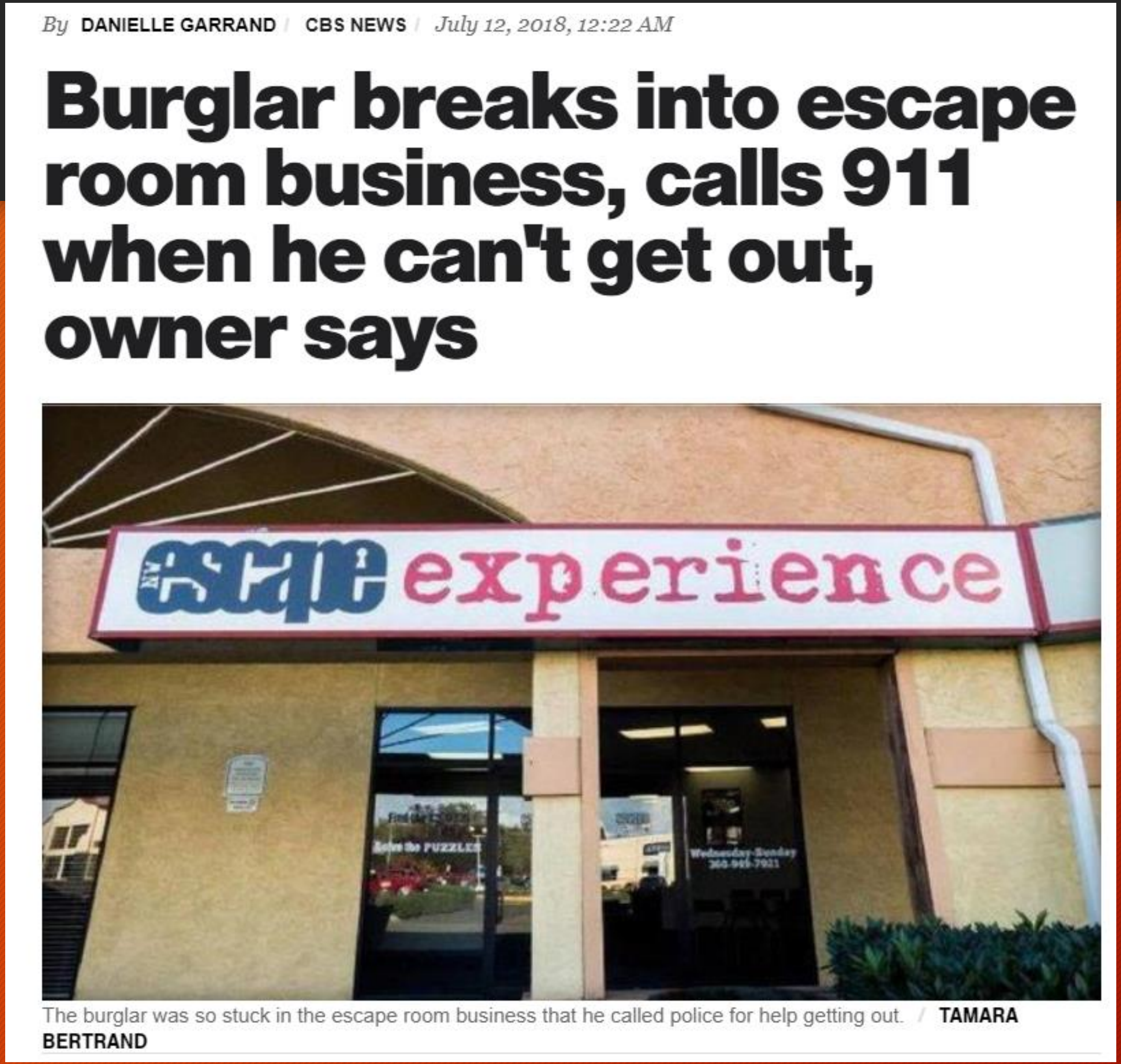
Secondary indications

Deletion

File type funneling occurs when an application reads an unusually disparate number of files as it writes.

Source: https://www.cryptodrop.org/

Clumsy Thief



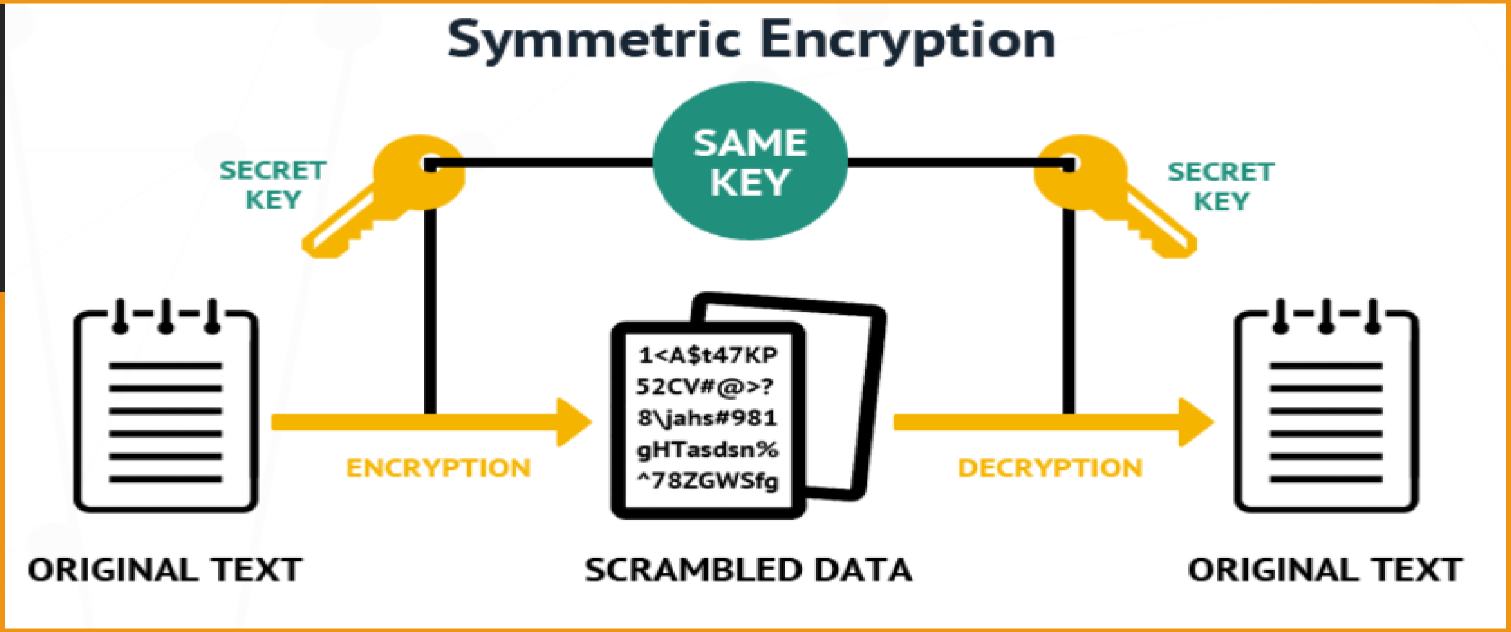
By DANIELLE GARRAND / CBS NEWS / July 12, 2018, 12:22 AM

Burglar breaks into escape room business, calls 911 when he can't get out, owner says

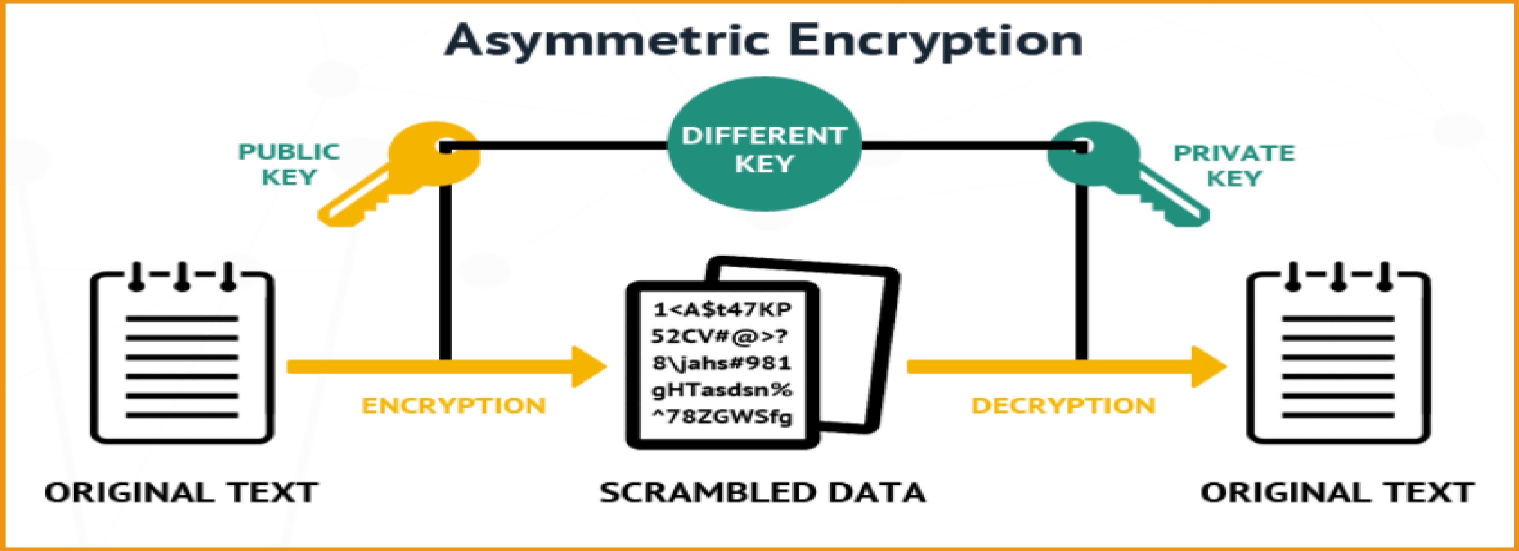
The burglar was so stuck in the escape room business that he called police for help getting out. / TAMARA BERTRAND

Analyze decryption key management

- Symmetric



- Asymmetric



Key management classification

- No key or no encryption
- Decryption key is in user domain
- Decryption key is in attacker’s domain

No key or no encryption

https://docs.apwg.org/ecrimeresearch/2018/5357083.pdf

- AnonPop and
- original variants of ConsoleCrypt
- Nemucod
- Aron WanaCrypt0r 2.0 (certain WannaCry imitators)

Decryption key in user domain

- Decryption key can be discovered by reverse engineering the ransomware code or analyzing a hidden file in the system or network where the ransomware has “secretly” stored the key.
- JigSaw – hard-coded key ransomware
- CryptoDefense – left the key on machine
- AIDS

https://docs.apwg.org/ecrimeresearch/2018/5357083.pdf

Decryption key in attacker’s domain

- Decryption key never leaves the attacker until ransom is paid
- One key pair exists
  - If one victim pays and gets the key, the rest can too☺
  - Cryptolocker
- Communication between C&C and infected host machine may or may not be encrypted
- Another approach: ransomware creates their own key at the machine and transfer the private key to the attacker
  - Cryptodefense – didn’t remove private key from the machine

https://docs.apwg.org/ecrimeresearch/2018/5357083.pdf

Sticky situation: Hybrid model

1. Ransomware compromises host
2. Cryptographic APIs available on the host to generate an encryption key such as anAES-256 key.
3. Ransomware encrypts this symmetric key with a hard-coded asymmetric key (e.g.RSA-2048) and sends encrypted symmetric key to the attacker.
4. User data is encrypted using the symmetric key.
5. Ransomware securely destroys the symmetric key on the host machine, now making the attacker the sole possessor of the decryption key.
6. A ransom note is displayed to the user while ransomware awaits payment

Decryption key distributed among peers

Breaks the keys into multiple parts, encrypting those parts, and then distributing it among a peer group such as comprised hosts

Reverse engineering is not possible here

Monitoring of communication between C&C is not possible

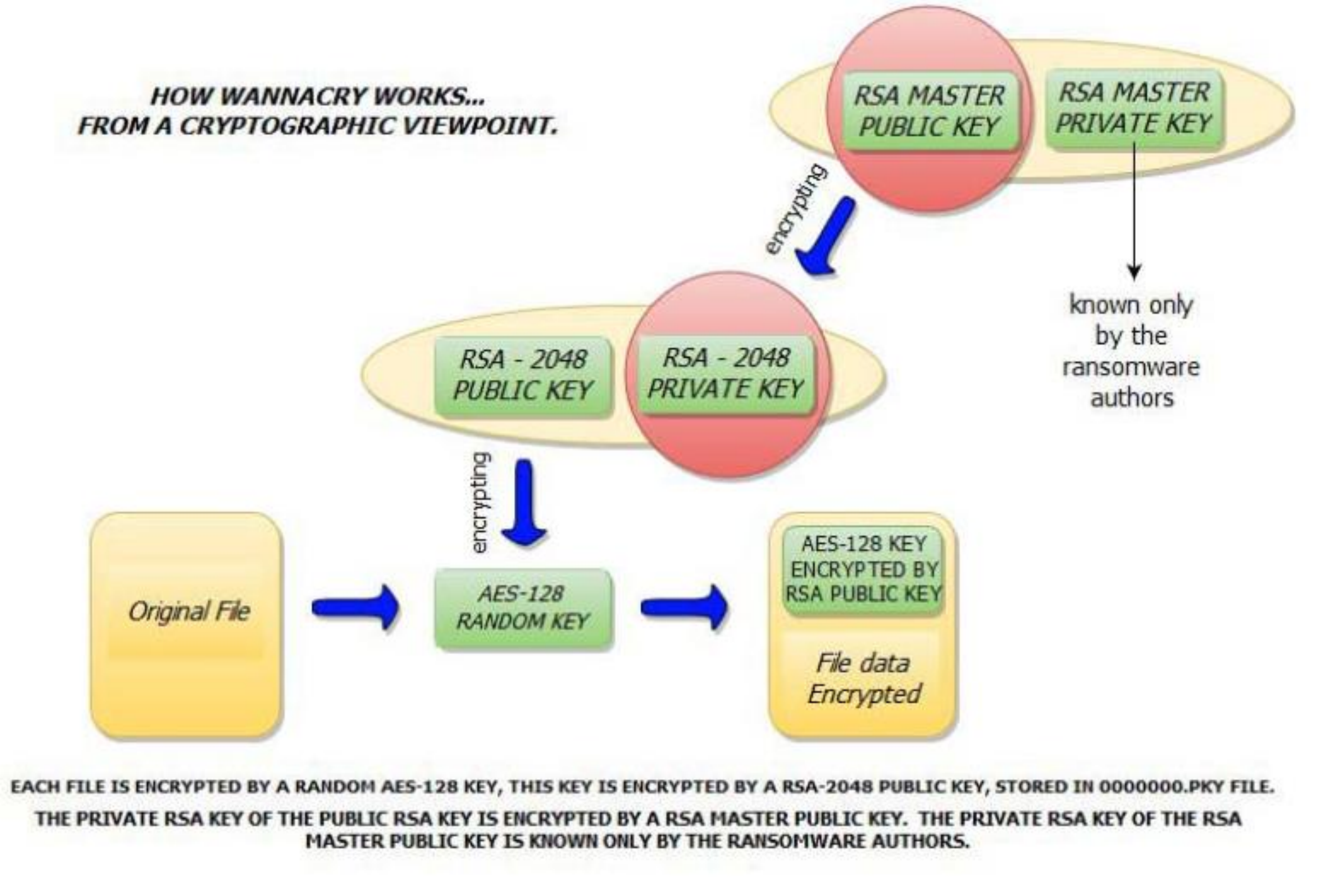
Risk : if one user restores the infected host machine successfully from backup, that part of the key is destroyed

https://docs.apwg.org/ecrimeresearch/2018/5357083.pdf

Deploy kill switch: Wannacry

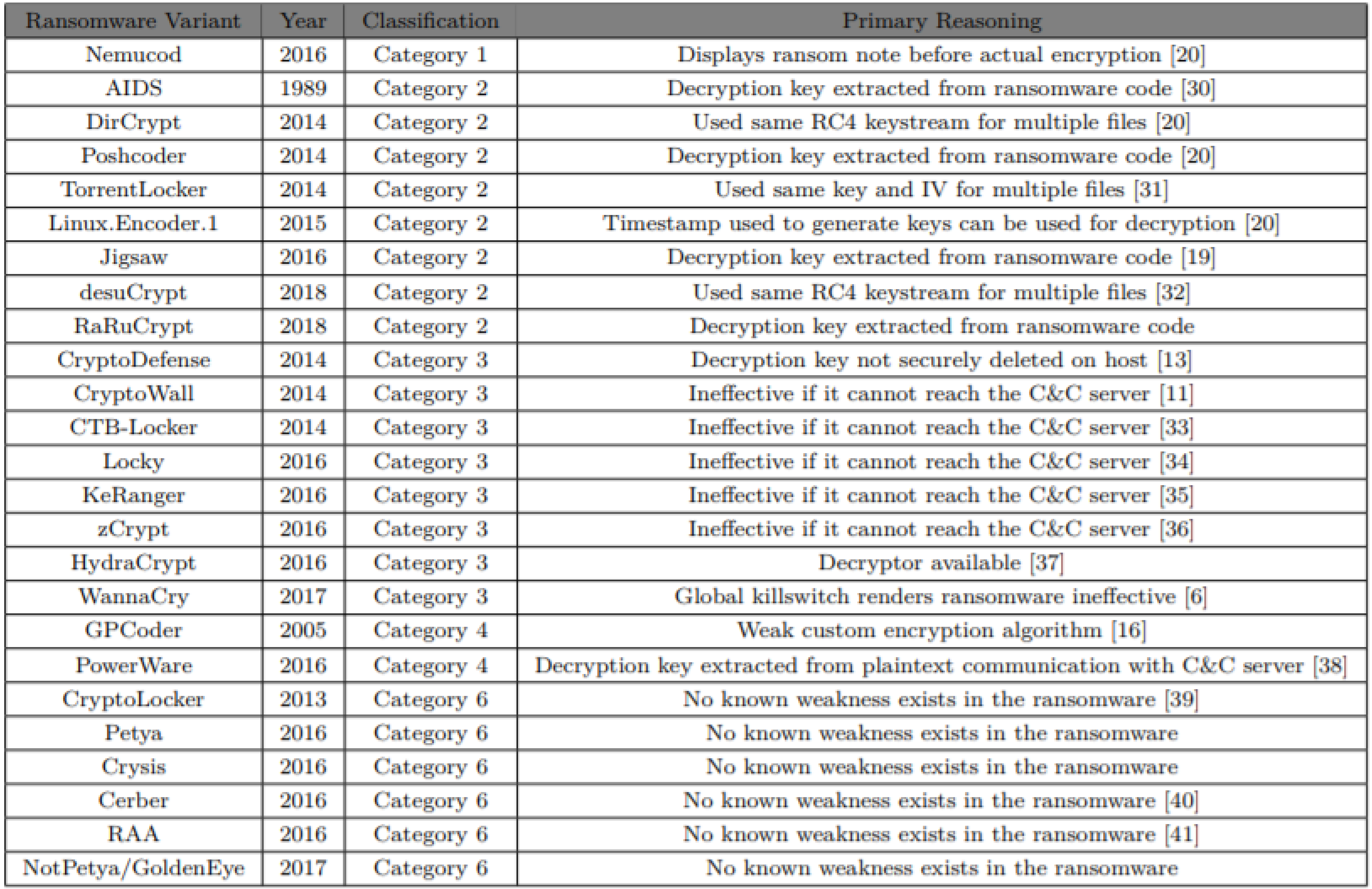
- No clicking on wrong links
- Exploited an unpatched vulnerability on a host machine and propagated like a worm

https://sensorstechforum.com/wana-decrypt0r-decrypt-files-for-free/

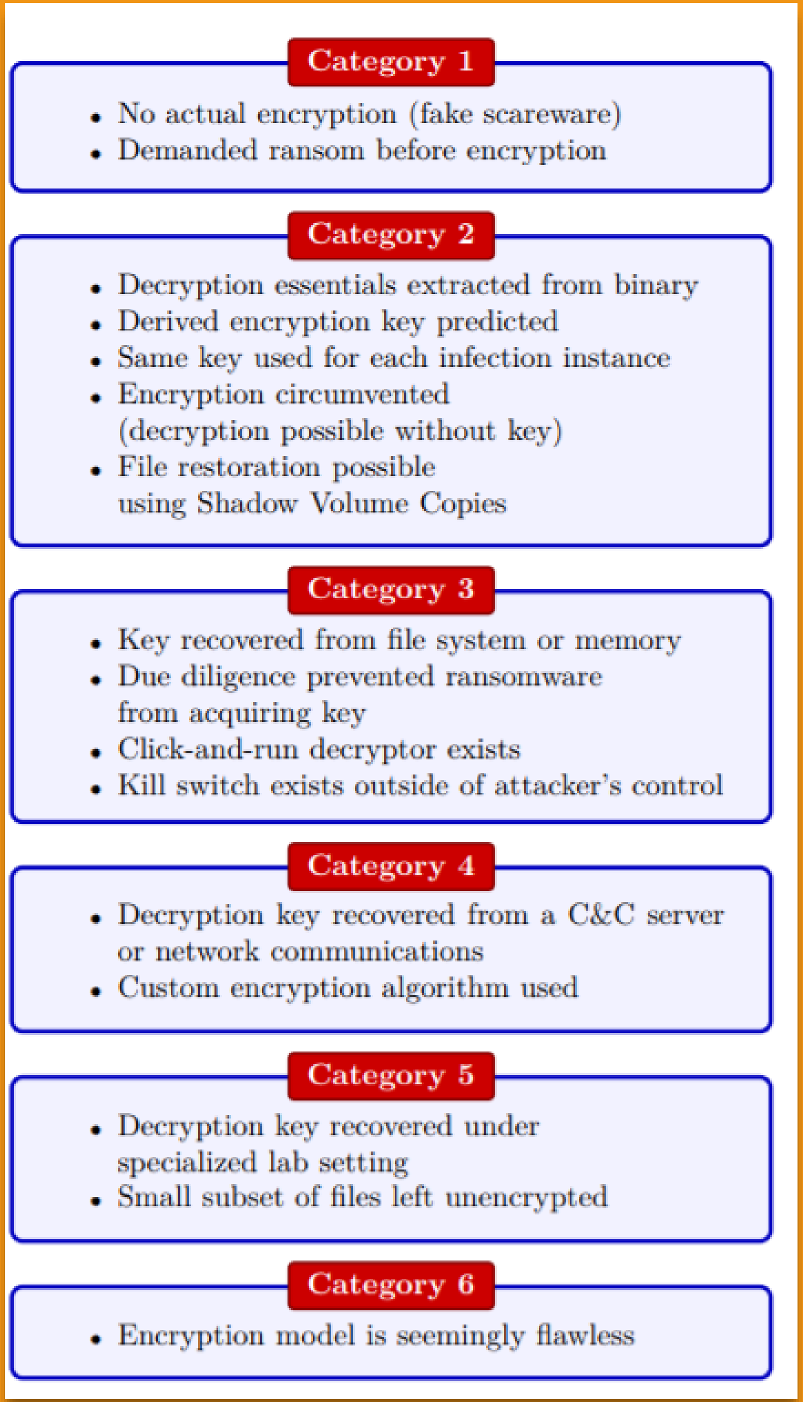


EACH FILE IS ENCRYPTED BY A RANDOM AES-128 KEY, THIS KEY IS ENCRYPTED BY A RSA-2048 PUBLIC KEY, STORED IN 0000000.PKY FILE. THE PRIVATE RSA KEY OF THE PUBLIC RSA KEY IS ENCRYPTED BY A RSA MASTER PUBLIC KEY. THE PRIVATE RSA KEY OF THE RSA MASTER PUBLIC KEY IS KNOWN ONLY BY THE RANSOMWARE AUTHORS.

Ransomware categories



Ransomware Variant	Year	Classification	Primary Reasoning
Nemucod	2016	Category 1	Displays ransom note before actual encryption [20]
AIDS	1989	Category 2	Decryption key extracted from ransomware code [30]
DirCrypt	2014	Category 2	Used same RC4 keystream for multiple files [20]
Poshcoder	2014	Category 2	Decryption key extracted from ransomware code [20]
TorrentLocker	2014	Category 2	Used same key and IV for multiple files [31]
Linux.Encoder.1	2015	Category 2	Timestamp used to generate keys can be used for decryption [20]
Jigsaw	2016	Category 2	Decryption key extracted from ransomware code [19]
desuCrypt	2018	Category 2	Used same RC4 keystream for multiple files [32]
RaRuCrypt	2018	Category 2	Decryption key extracted from ransomware code
CryptoDefense	2014	Category 3	Decryption key not securely deleted on host [13]
CryptoWall	2014	Category 3	Ineffective if it cannot reach the C&C server [11]
CTB-Locker	2014	Category 3	Ineffective if it cannot reach the C&C server [33]
Locky	2016	Category 3	Ineffective if it cannot reach the C&C server [34]
KeRanger	2016	Category 3	Ineffective if it cannot reach the C&C server [35]
zCrypt	2016	Category 3	Ineffective if it cannot reach the C&C server [36]
HydraCrypt	2016	Category 3	Decryptor available [37]
WannaCry	2017	Category 3	Global killswitch renders ransomware ineffective [6]
GPCoder	2005	Category 4	Weak custom encryption algorithm [16]
PowerWare	2016	Category 4	Decryption key extracted from plaintext communication with C&C server [38]
CryptoLocker	2013	Category 6	No known weakness exists in the ransomware [39]
Petya	2016	Category 6	No known weakness exists in the ransomware
Crysis	2016	Category 6	No known weakness exists in the ransomware
Cerber	2016	Category 6	No known weakness exists in the ransomware [40]
RAA	2016	Category 6	No known weakness exists in the ransomware [41]
NotPetya/GoldenEye	2017	Category 6	No known weakness exists in the ransomware



Category 1

- No actual encryption (fake scareware)
- Demanded ransom before encryption

Category 2

- Decryption essentials extracted from binary
- Derived encryption key predicted
- Same key used for each infection instance
- Encryption circumvented (decryption possible without key)
- File restoration possible using Shadow Volume Copies

Category 3

- Key recovered from file system or memory
- Due diligence prevented ransomware from acquiring key
- Click-and-run decryptor exists
- Kill switch exists outside of attacker's control

Category 4

- Decryption key recovered from a C&C server or network communications
- Custom encryption algorithm used

Category 5

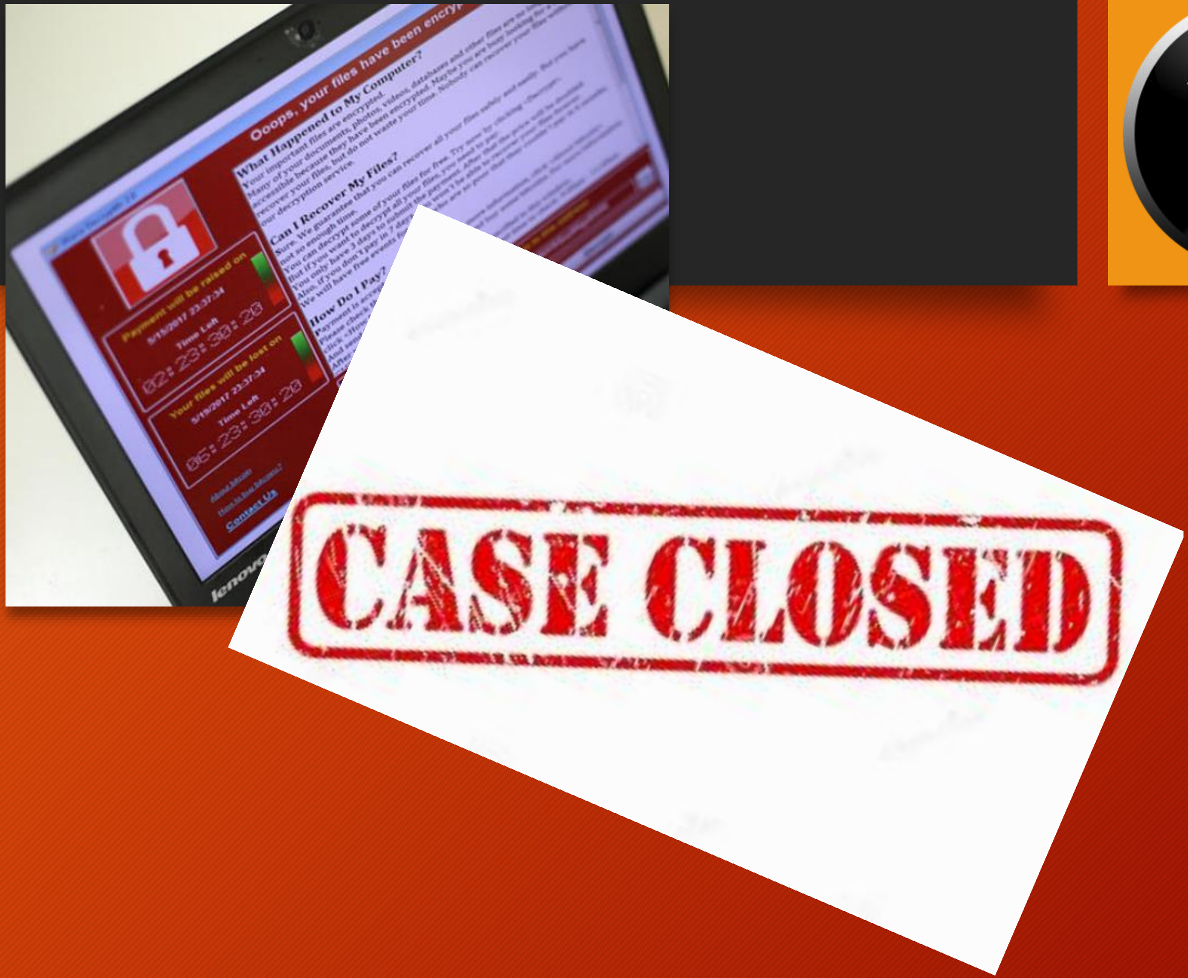
- Decryption key recovered under specialized lab setting
- Small subset of files left unencrypted

Category 6

- Encryption model is seemingly flawless

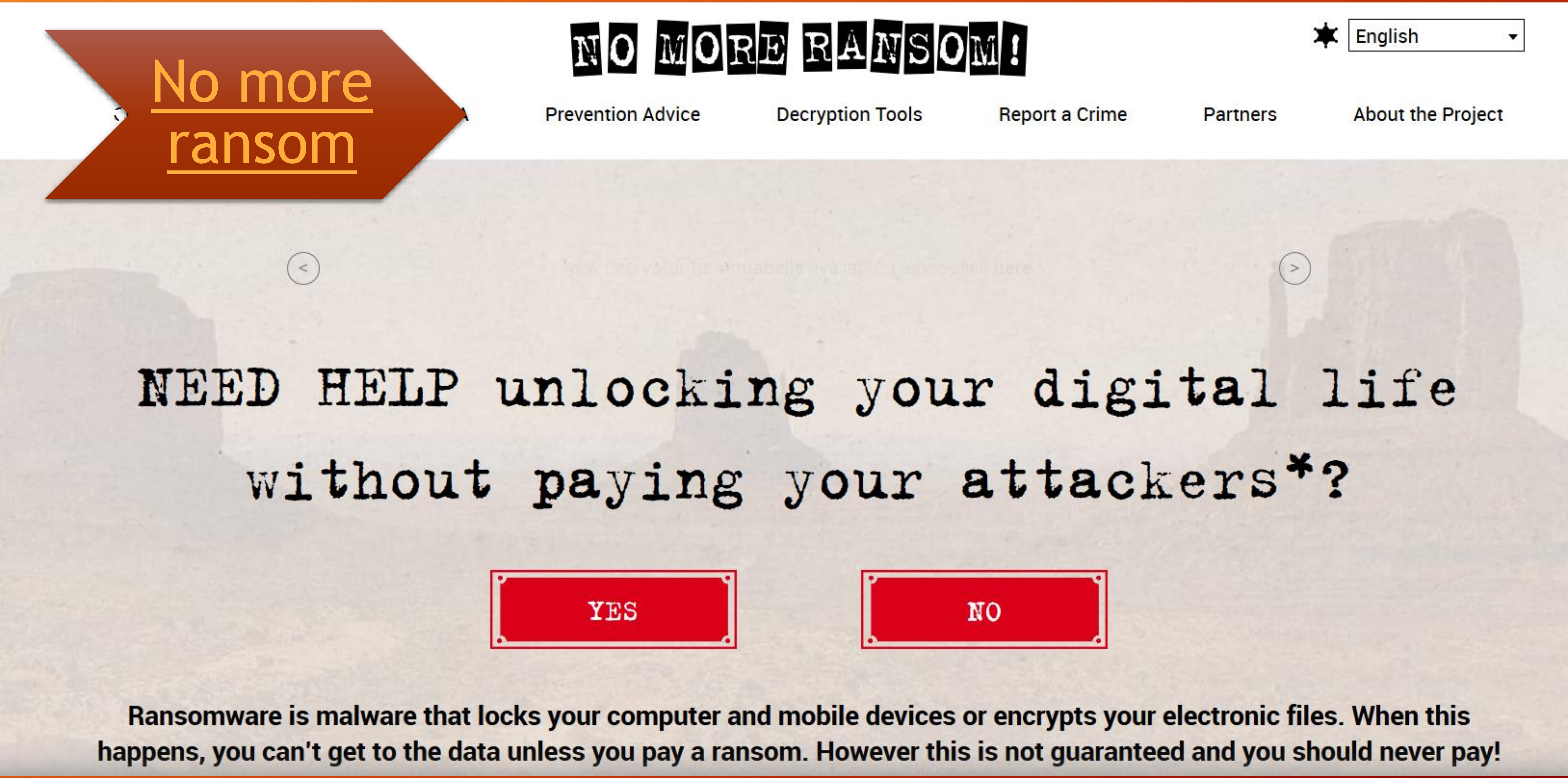
Case # 1 Medical Office

A dentist office in California logged on to the office computer 2018 and was greeted by this message:


Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
Payment will be raised on
Time Left
Your files will be lost on
Time Left
CASE CLOSED

Nomoreransom tool

No more ransom



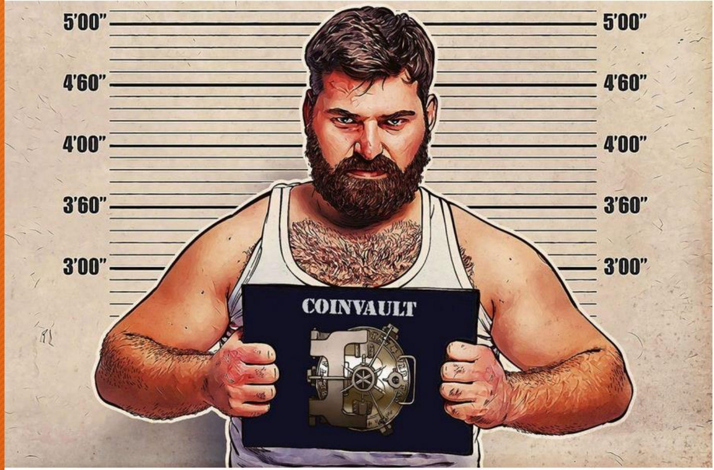
NO MORE RANSOM!

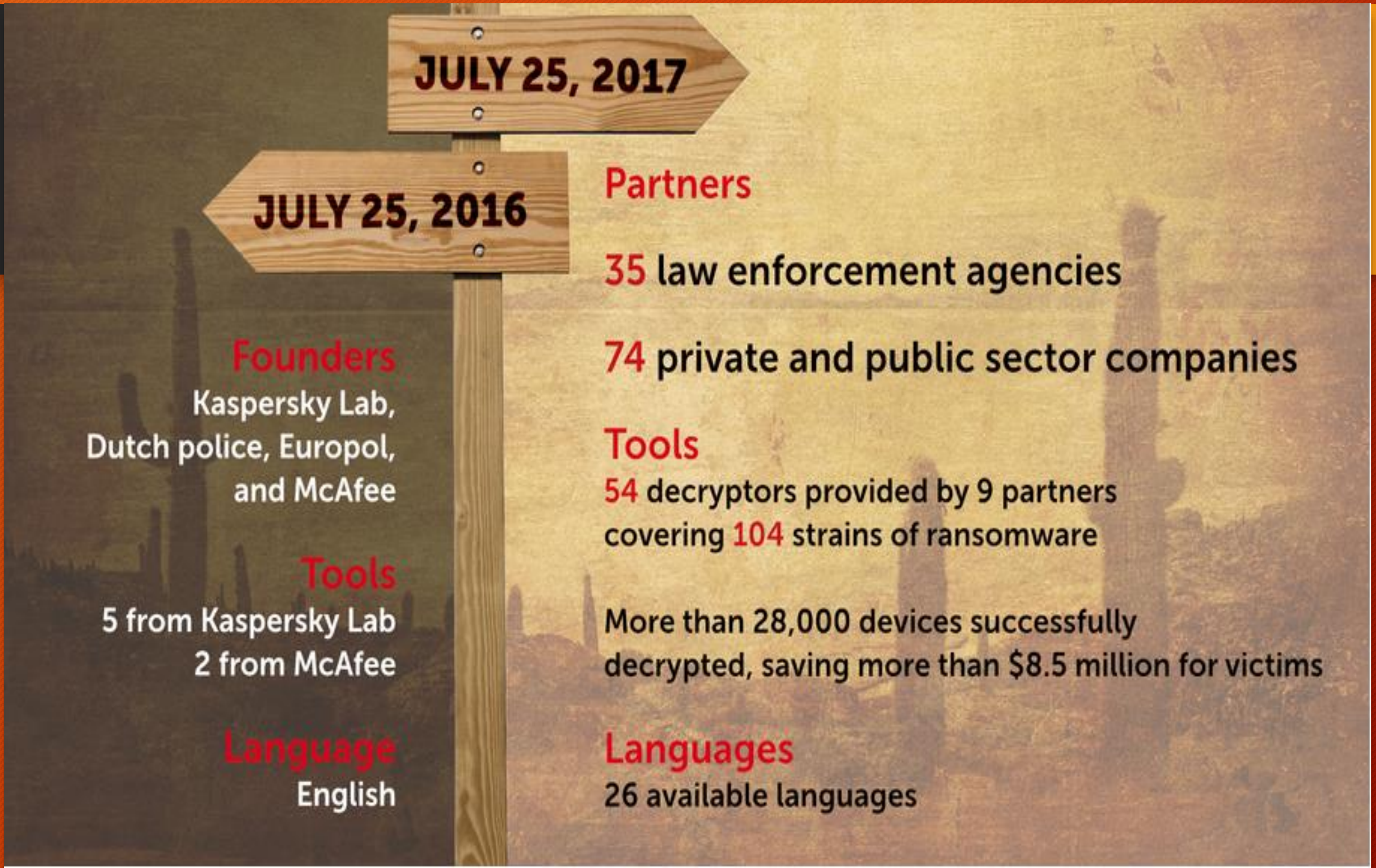
NEED HELP unlocking your digital life without paying your attackers*?

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

No more Ransom

- Success stories:





JULY 25, 2017

JULY 25, 2016

Founders
Kaspersky Lab,
Dutch police, Europol,
and McAfee

Tools
5 from Kaspersky Lab
2 from McAfee

Language
English

Partners

35 law enforcement agencies

74 private and public sector companies

Tools
54 decryptors provided by 9 partners
covering 104 strains of ransomware

More than 28,000 devices successfully
decrypted, saving more than $8.5 million for victims

Languages
26 available languages

More than 10,000 victims decrypted their files without spending a penny, using the tools from the No More Ransom platform. Most of the site visitors were from Russia, the Netherlands, the United States, Italy, and Germany.

Source: nomoreransom.org

Case # 2 : Law firm

Law firm in Australia fell victim to a ransomware attack, reporting that mailbox and over 44,000 files on SharePoint totaling over 5GB of data were locked down with a ransom note asking for $6,000 USD for the key to unencrypt

Functionally restored with preexisting cloud backup

Case # 3 Entertainment

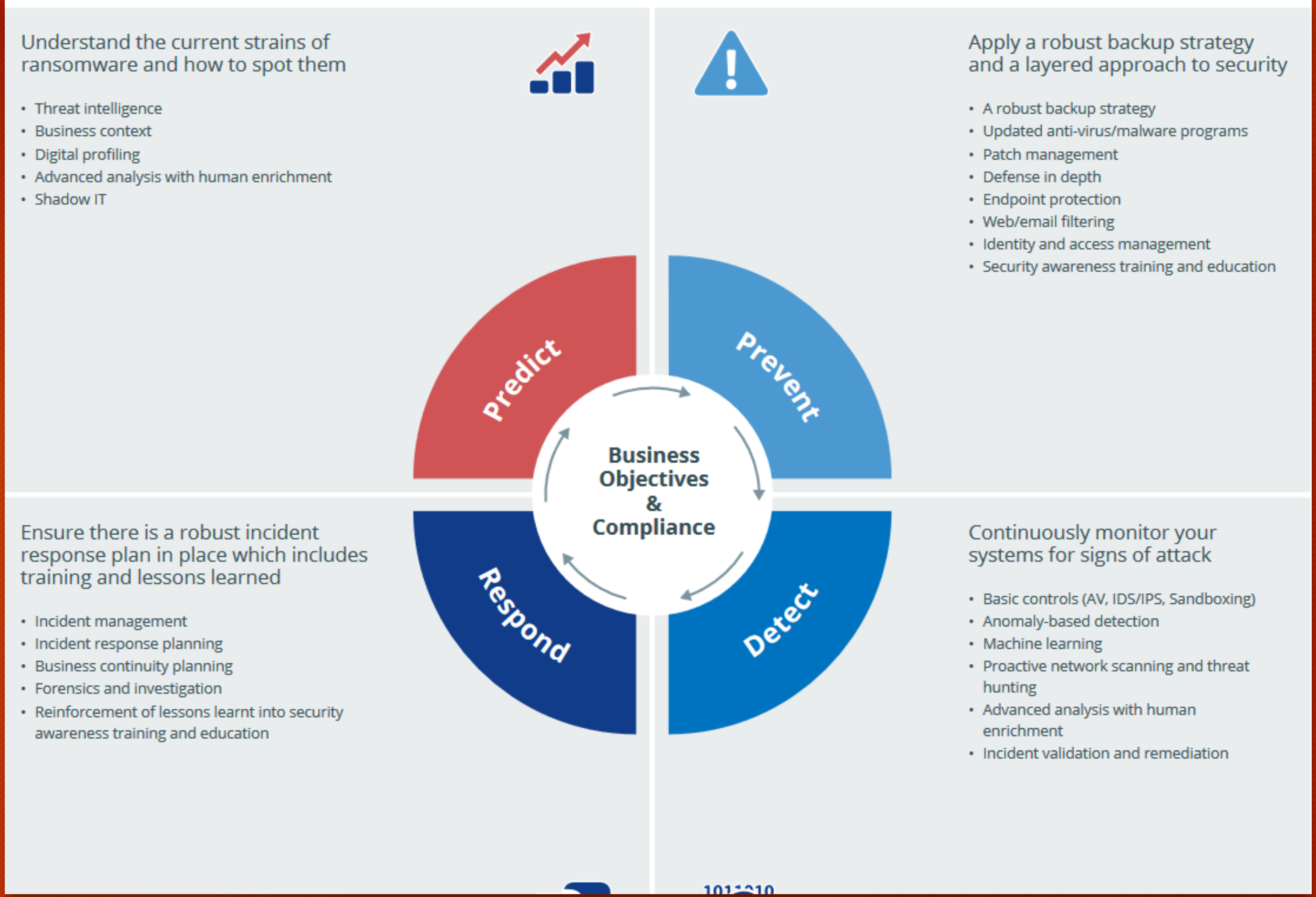
Tony Casala firm could access any of the company's 4,000+ files stored on the cloud drive

Functionally restored with community forum decryptor

https://www.bleepingcomputer.com/forums/t/575875/new-teslacrypt-version-released-that-uses-the-exx-extension/

Outline

- Real life ransomware cases
- Introduction
- Trend & Statistics
- Attack vectors
- Success stories: ransomware mitigation strategies
- Where we go from here- unknowns and future direction



Understand the current strains of ransomware and how to spot them

- Threat intelligence
- Business context
- Digital profiling
- Advanced analysis with human enrichment
- Shadow IT

Apply a robust backup strategy and a layered approach to security

- A robust backup strategy
- Updated anti-virus/malware programs
- Patch management
- Defense in depth
- Endpoint protection
- Web/email filtering
- Identity and access management
- Security awareness training and education

Ensure there is a robust incident response plan in place which includes training and lessons learned

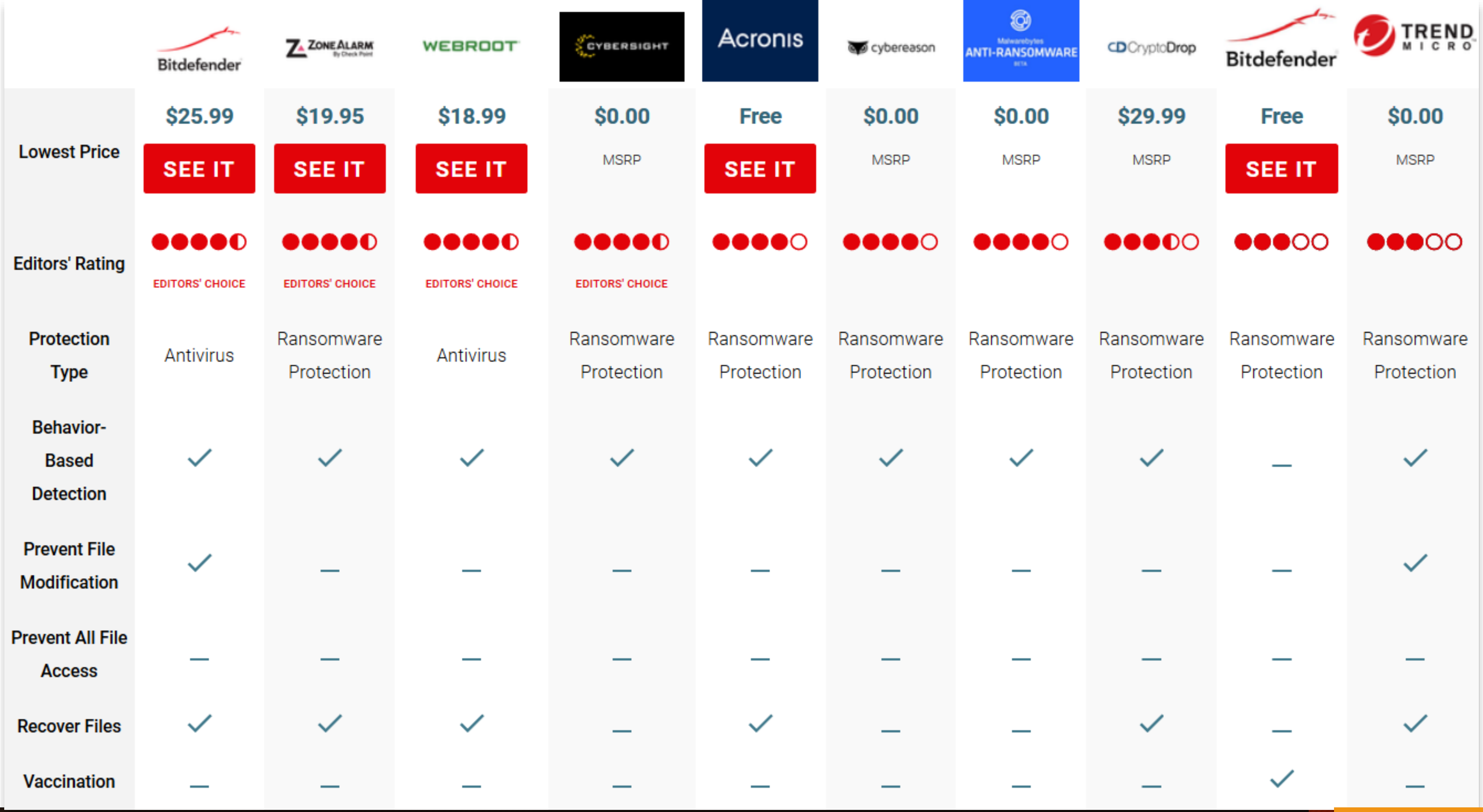
- Incident management
- Incident response planning
- Business continuity planning
- Forensics and investigation
- Reinforcement of lessons learnt into security awareness training and education

Continuously monitor your systems for signs of attack

- Basic controls (AV, IDS/IPS, Sandboxing)
- Anomaly-based detection
- Machine learning
- Proactive network scanning and threat hunting
- Advanced analysis with human enrichment
- Incident validation and remediation

Ransomware prevention strategy at a corporate level

https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl-whitepaper-ransomware-uea



	Bitdefender	ZoneAlarm By Check Point	WEBROOT	CYBERSIGHT	Acronis	cybereason	Malwarebytes ANTI-RANSOMWARE BETA	CryptoDrop	Bitdefender	TREND MICRO
Lowest Price	$25.99 SEE IT	$19.95 SEE IT	$18.99 SEE IT	$0.00 MSRP	Free SEE IT	$0.00 MSRP	$0.00 MSRP	$29.99 MSRP	Free SEE IT	$0.00 MSRP
Editors' Rating	●●●●◐ EDITORS' CHOICE	●●●●◐ EDITORS' CHOICE	●●●●◐ EDITORS' CHOICE	●●●●◐ EDITORS' CHOICE	●●●●○	●●●●○	●●●●○	●●●◐○	●●●○○	●●●○○
Protection Type	Antivirus	Ransomware Protection	Antivirus	Ransomware Protection	Ransomware Protection	Ransomware Protection	Ransomware Protection	Ransomware Protection	Ransomware Protection	Ransomware Protection
Behavior-Based Detection	✓	✓	✓	✓	✓	✓	✓	✓	—	✓
Prevent File Modification	✓	—	—	—	—	—	—	—	—	✓
Prevent All File Access	—	—	—	—	—	—	—	—	—	—
Recover Files	✓	✓	✓	—	✓	—	—	✓	—	✓
Vaccination	—	—	—	—	—	—	—	—	✓	—

Possible vendors

https://www.pcmag.com/roundup/353231/the-best-ransomware-protection

Ransomware prevention at user level

- Backup regularly
- Patch Your Software And Operating Systems Regularly
- Segment your networks
- Restrict User Administrative Access
- Don’t enable macros
- Show Hidden File Extensions On User Computers
- deploy antimalware Solutions

What can we do at each of Ransomware stage?

Reconnaissance	**Practice safe social media control**
Weaponize	**Develop secure software**
Deliver	**Guard perimeter**
Exploit	**Secure the end-points**
Install	**Patch Patch Patch**
Command&Control	**Detect and disrupt**
Execute	**Backup &Recovery**

What to do at the time of infection?

- Kill suspicious programs
- Reboot machine in safe mode
- Figure out the strain
- View file extensions
- Unplug power
- Pay or not to pay

Useful governing authority contacts

1

Elected officials
Local law enforcement, SBI, FBI

2

DIT, Chief Risk and Security Officer

919-754-6578

3

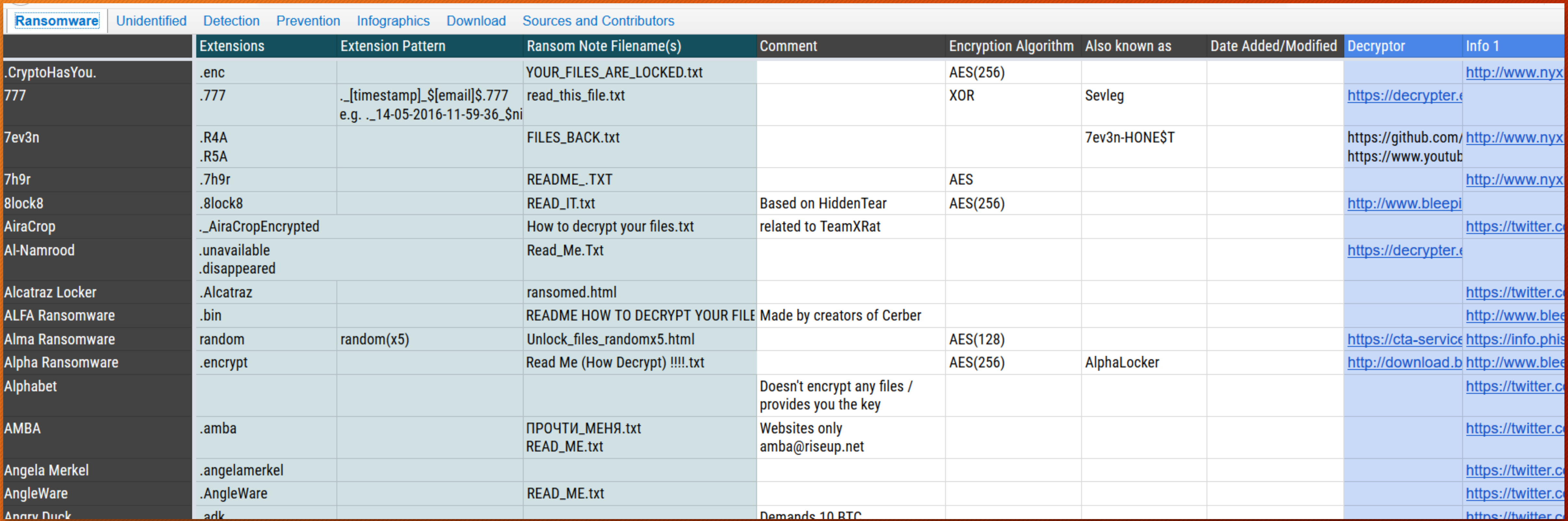
DHHS, Chief Information Security Officer

919-855-3000

4

NC Attorney General

919-716-6400



	Extensions	Extension Pattern	Ransom Note Filename(s)	Comment	Encryption Algorithm	Also known as	Date Added/Modified	Decryptor	Info 1
.CryptoHasYou.	.enc		YOUR_FILES_ARE_LOCKED.txt		AES(256)				http://www.nyx
777	.777	._[timestamp]_$[email]$.777 e.g. ._14-05-2016-11-59-36_$ni	read_this_file.txt		XOR	Sevleg		https://decrypter.e	
7ev3n	.R4A .R5A		FILES_BACK.txt			7ev3n-HONE$T		https://github.com/ https://www.youtub	http://www.nyx
7h9r	.7h9r		README_.TXT		AES				http://www.nyx
8lock8	.8lock8		READ_IT.txt	Based on HiddenTear	AES(256)			http://www.bleepi	
AiraCrop	._AiraCropEncrypted		How to decrypt your files.txt	related to TeamXRat					https://twitter.c
Al-Namrood	.unavailable .disappeared		Read_Me.Txt					https://decrypter.e	
Alcatraz Locker	.Alcatraz		ransomed.html						https://twitter.c
ALFA Ransomware	.bin		README HOW TO DECRYPT YOUR FILE	Made by creators of Cerber					http://www.blee
Alma Ransomware	random	random(x5)	Unlock_files_randomx5.html		AES(128)			https://cta-service	https://info.phis
Alpha Ransomware	.encrypt		Read Me (How Decrypt) !!!!.txt		AES(256)	AlphaLocker		http://download.b	http://www.blee
Alphabet				Doesn't encrypt any files / provides you the key					https://twitter.c
AMBA	.amba		ПРОЧТИ_МЕНЯ.txt READ_ME.txt	Websites only amba@riseup.net					https://twitter.c
Angela Merkel	.angelamerkel								https://twitter.c
AngleWare	.AngleWare		READ_ME.txt						https://twitter.c
Angry Duck	.adk			Demands 10 BTC					https://twitter.c

Overall protection strategy

Excel spreadsheets

Outline

- Real life ransomware cases
- Introduction
- Trend & Statistics
- Attack vectors
- Success stories: ransomware mitigation stratergies
- Where we go from here- unknowns and future direction

Ransom attacks on cloud

Misconfigured S3 buckets

Auto sync

Corrupted data from any Saas

Cloud nine Realtime Ransomware Attack

https://www.techrepublic.com/article/unsecured-amazon-s3-buckets-are-prime-cloud-target-for-ransomware-attacks/

Conclusion

- Ransomware is a growing concern day by day costing us billions
- The good news is that we have tools, strategies, more understanding and awareness to deal with ransomware
- Small businesses and big enterprises can benefit from adopting cybersecurity hygiene and collaboration in the community