Ransomware

Prepared by:

- Author Geraint Williams
- Company GRCI Group
- Date 11 September 2019
- Version 1.0
- Restricted Public

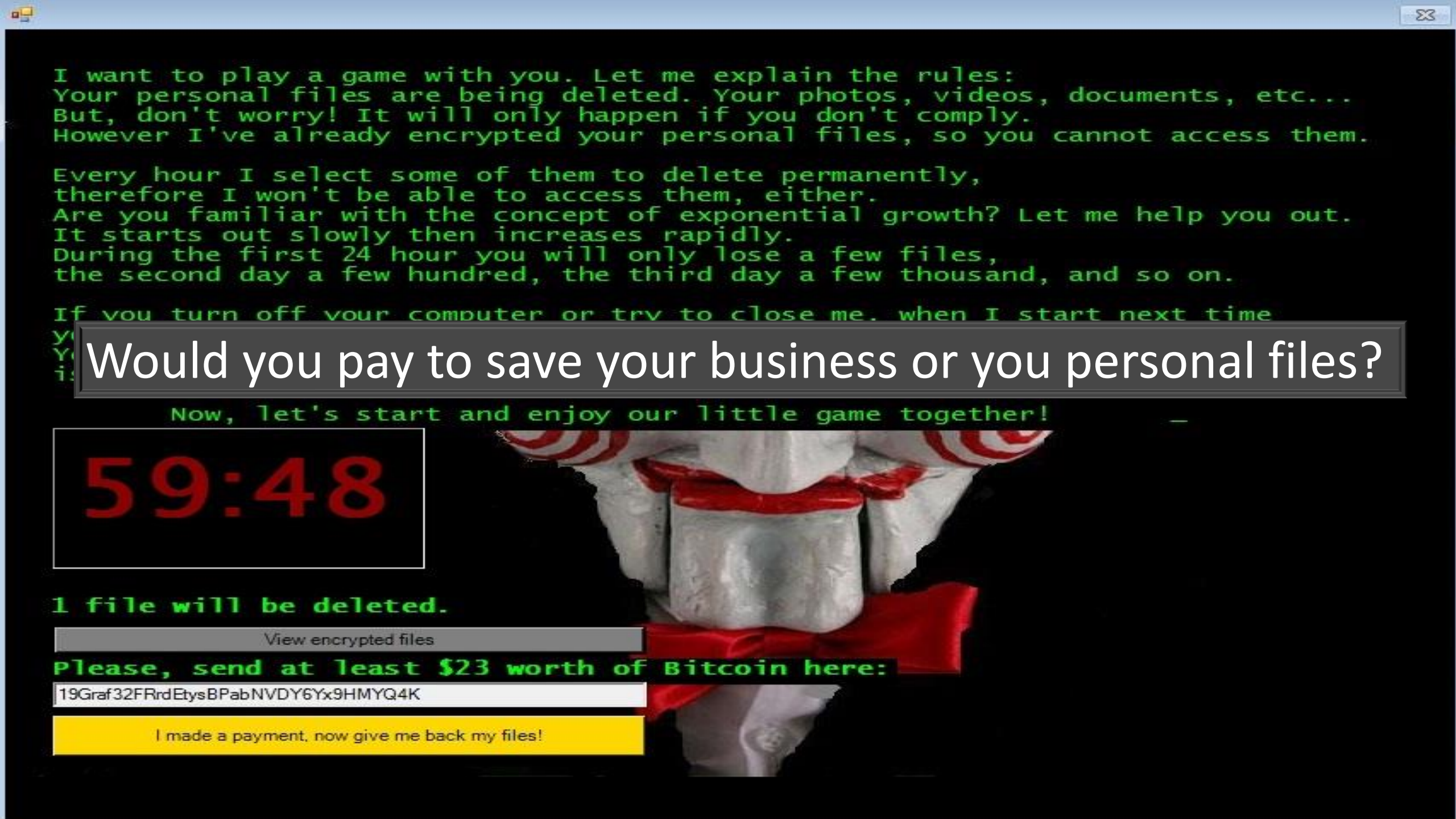
Introduction

Geraint Williams, CISO, GRC International Group

- *Taught Information Security, Ethical Hacking and Digital forensics*
- *Former Payment Card Industry Qualified Security Assessor*
- *Payment Card Industry Consultant*
- *Worked with breached companies*
- *Former Ethical Hacker*
- *Information security consultant*
- *Now Chief Information Security Officer*

Topics

- What is ransomware
- Case study
- Remediation techniques
- Incident Response
- Conclusion
- Resources

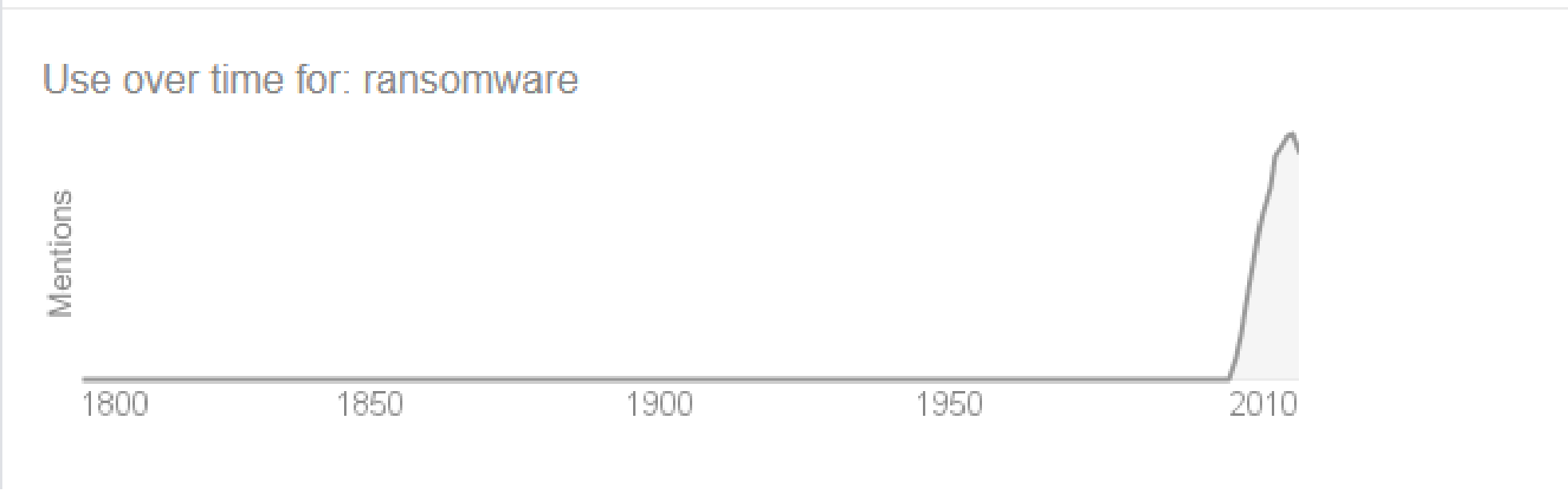


Would you pay to save your business or you personal files?

What is ransomware

Definition: Ransomware

- a type of malicious software designed to block access to a computer system or data until a sum of money is paid. (Oxford dictionary)



It is not new

- The first recorded example of ransomware was in 1989, when evolutionary biologist Dr. Joseph Popp sent floppy discs containing the PC Cyborg Trojan to hundreds of recipients under the heading “AIDS Information Introductory Diskette”.

AIG report

Fig 1 **Cyber Claims received by AIG EMEA (2018) – By reported incident**

*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations

Samples of Ransomware

Cost of Ransomware

Government puts cost of WannaCry to NHS at £92m

OSCAR WILLIAMS
EDITOR

The Department of Health and Social Care (DHSC) has estimated that WannaCry cost the NHS £92m in direct costs and lost output.

The Department's latest update on cyber resilience in health and care suggests last year's cyber-attack cost the service £20m during the outbreak and an additional £72m in the aftermath.

This includes £19m worth of lost output as a result of disruption to services – such as cancelled appointments and operations – and the shutting down of computer systems to stem the spread of the malware.

It also includes £73m in direct IT costs, which incorporates expenditure on IT support needed to recover data and restore systems affected by the attack.

SECURITY

Coordinated ransomware attack could cost global economy £148bn

30TH JANUARY 2019

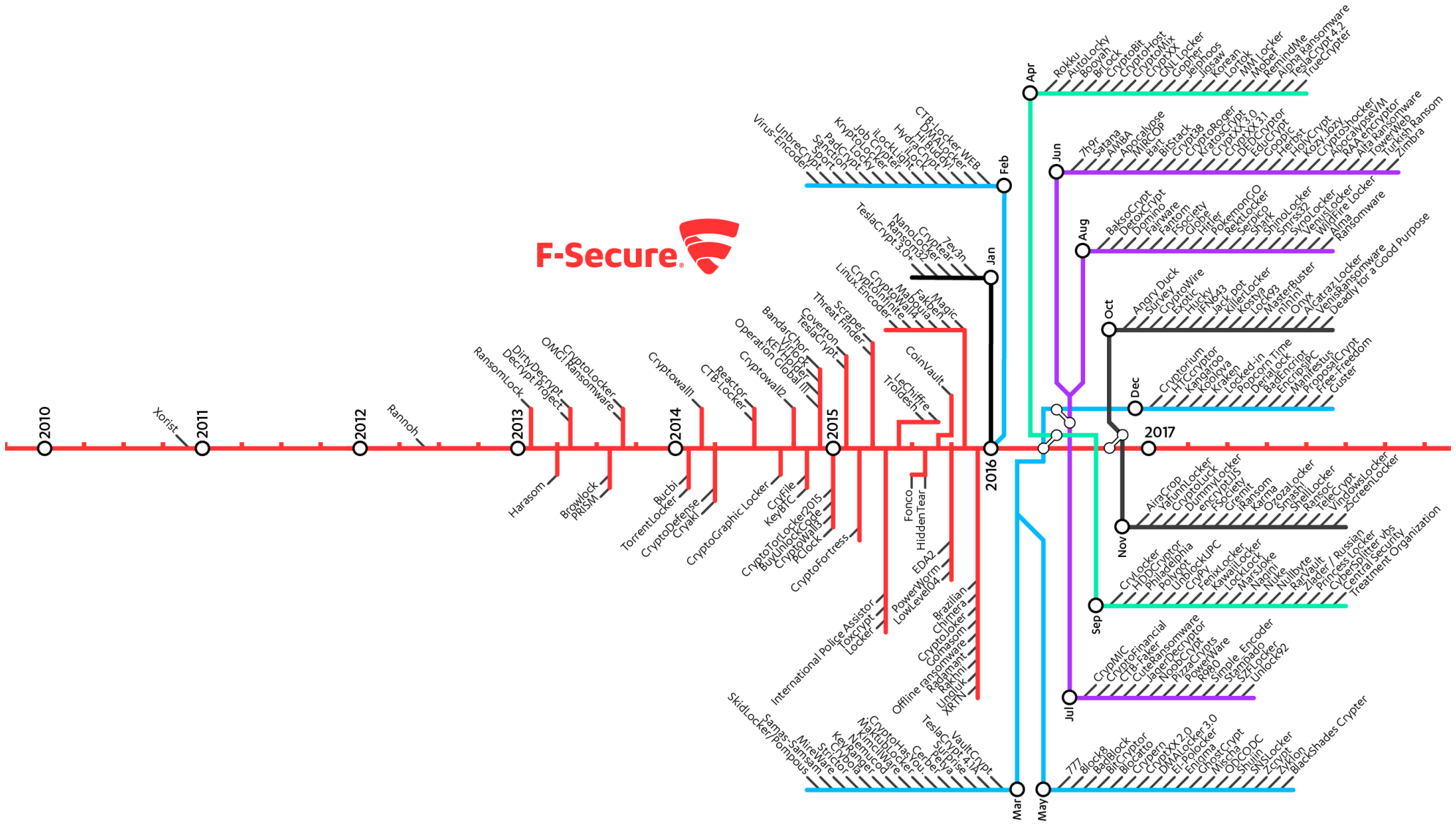
A coordinated cyber attack could hit 600,000 businesses around the world and cost the global economy as much as £148bn, according to a new report.

Researchers at Cambridge University modeled a scenario in which an attack is launched through a malware-laden email that is automatically forwarded to a victims' contacts list, encrypting data on nearly 30m devices within 24 hours.

It is predicted that the attack would have the greatest impact on the retail and healthcare sectors, which would suffer losses of £19bn each. The former would lose business due to payment systems being taken offline, while the latter would be unable to treat patients who depend on legacy IT infrastructure that cannot be easily patched, the researchers predict.

"Historically, the healthcare sector has been vulnerable to high levels of malware infection due to legacy IT infrastructure systems, which are more vulnerable to malware, and low investment in IT," they stated.

Ransomware Timeline 2010 - 2017



Encrypting ransomware

- Early techniques (ie PC Cyborg Trojan)
  - hides directories and encrypts the names of all files on drive
- Locking access to a PC
- Encrypting files
  - Symmetric Cryptography
    - Key often in the trojan
  - Asymmetric Cryptography
    - Encrypted with public key in the trojan
    - Private key held by the perpetrators

Perpetrators

- two main categories of ransomware perpetrators:

- organized criminal groups and

Hacker from Russian crime group jailed for multi-million ...
https://nationalcrimeagency.gov.uk › News
... with locking **ransomware** has been jailed for six years and five months after a ... was a member of an international, Russian-speaking **organised crime** group ...

- state actors.

North Korea cyberattacks generate $2 billion for weapons ...
https://www.dw.com › north-korea-cyberattacks-generate-2-billion-for-we...
5 Aug 2019 - **North Korea** has been supporting its weapons program using ... **North Korea** is using cyberattacks on banks and cryptocurrency .... The WannaCry **ransomware** attack infected about 300,000 computers in 150 countries in May.

Why

"That's Where the Money is..."

— Willie Sutton

Actually an urban myth

Why do they conduct attacks

- 50% of consumers said they would not pay a ransom to get their encrypted files back
- 70% of businesses that had experienced an infection had paid up

- F-Secure poll
- 8% of respondents said they'd be willing to pay a fee of more than $400 to recover lost data, 29% were willing to shell out an amount under $400

The risk

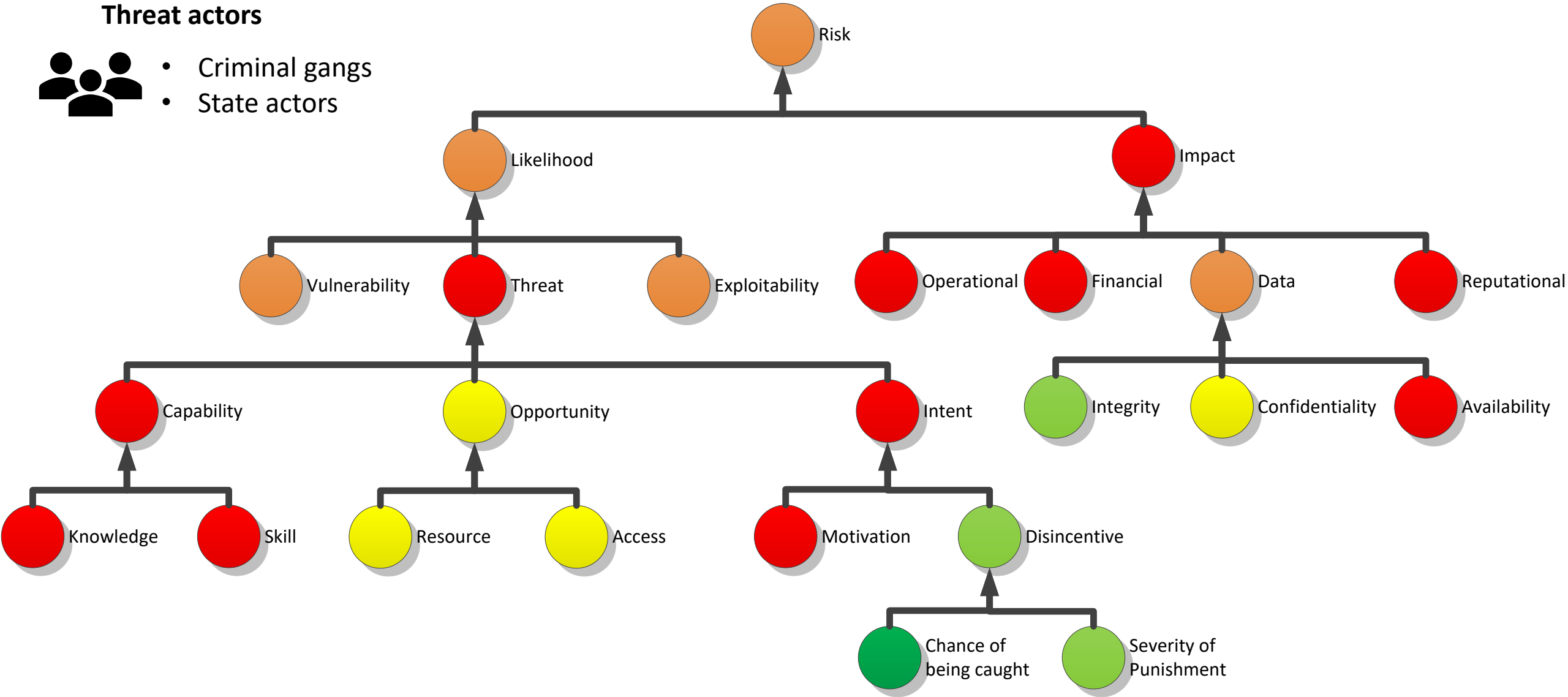
The risk

If your organisation relies on data or access to computer systems you are at risk of being impacted by ransomware

Initial Risk (Ransomware)

Threat actors

- Criminal gangs
- State actors



The kill chain

How Ransomware campaign operates

How does it work (Kill chain)

GRC international group plc™

Ransomware Attack (Campaign)

- Infection and Propagation
- Key generation and C&C
- Encryption
- Ransom alert
- Decryption and removal

Campaigns

- cybercriminals are turning to targeted ransomware attacks instead of indiscriminate campaigns.

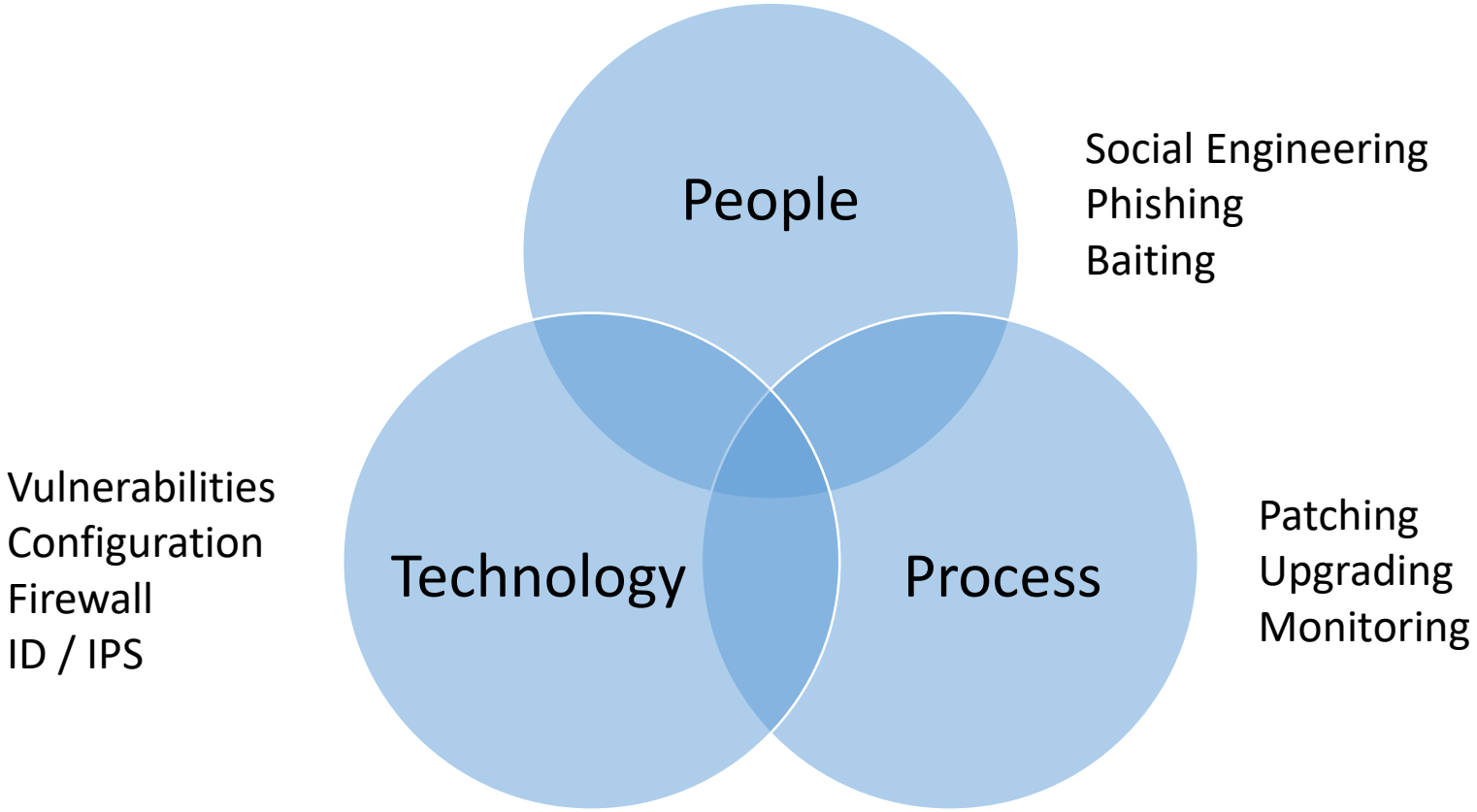
- WannaCry – 200,000 computers netted $120,000 (indiscriminate)
- River beach – single network netted $600,000 (targeted)

Infection and propagation

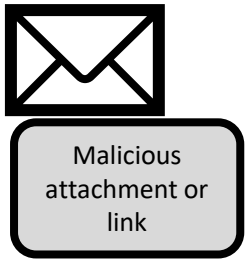
The attack starts

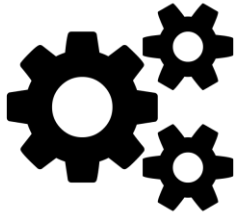
Infection and propagation

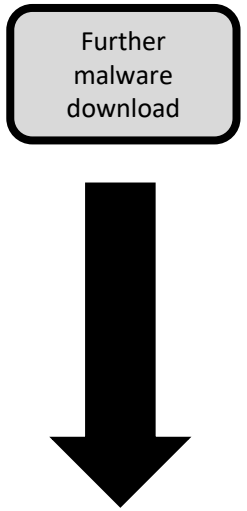
- Takes advantages of weakness

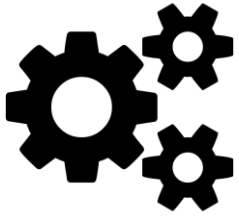


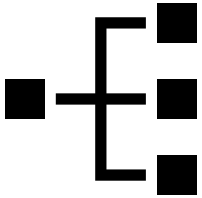
Infection and propagation











Email with attachment arrives

Macros in attachment launches malware

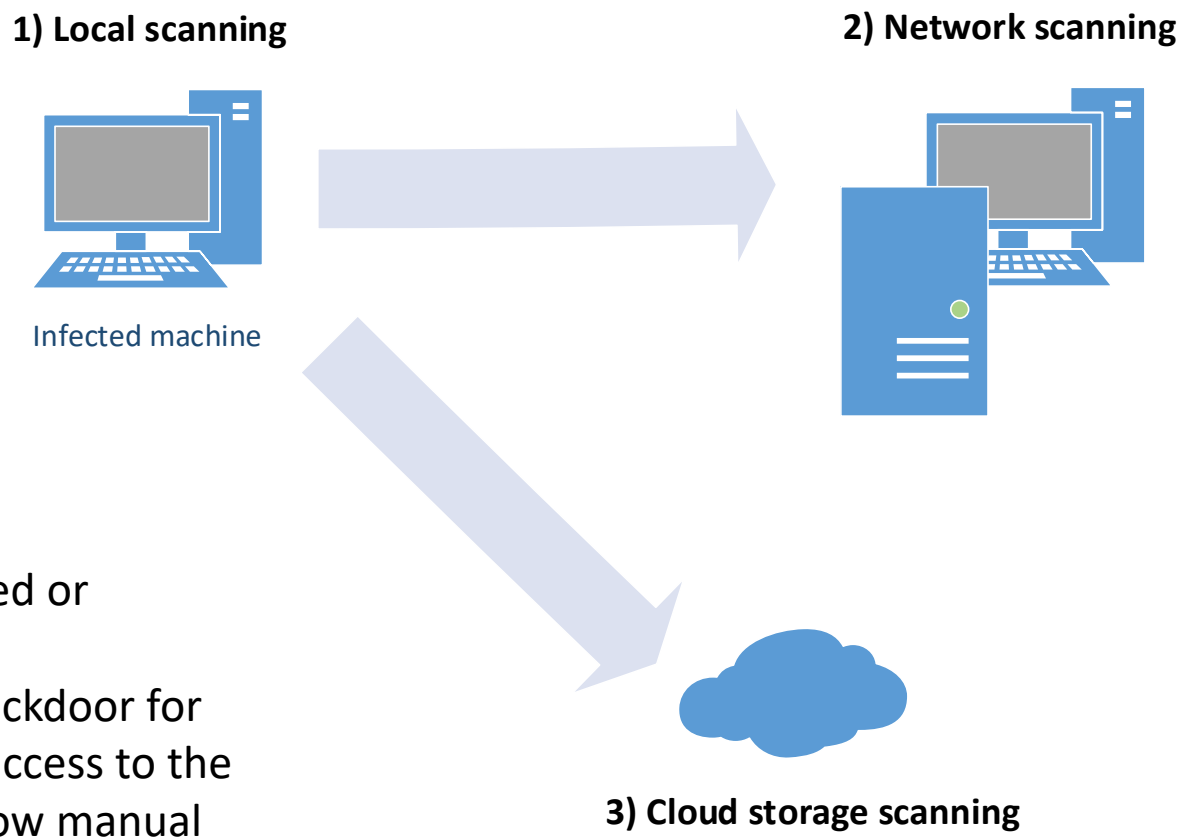
The malware executes and leverages flaws to enable its functionality

The malware connects to the internet and pulls down further modules to expand capability

Disables AV, harvests data, steals credentials,

moves lateral through the network

Lateral movement

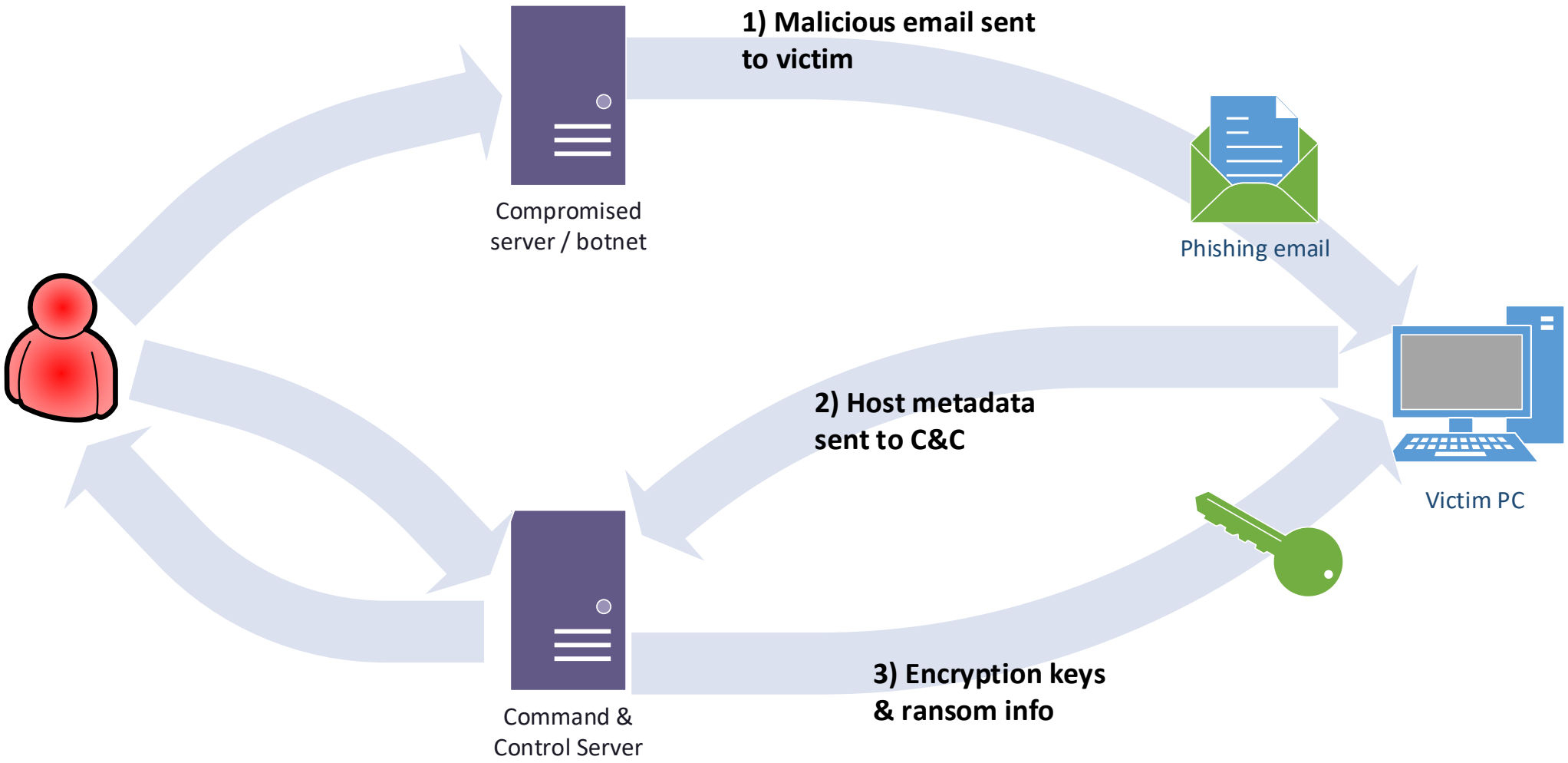


Scanning can be automated or manual.
If the malware opens a backdoor for an attacker to use to get access to the local network it would allow manual control over the lateral movement

Key generation and C&C

Once infected

Command & Control



Encryption methodologies

- Symmetric encryption ransomware
- Client asymmetric encryption
- Server Asymmetric encryption
- Hybrid encryption scheme
  - Server and Client asymmetric encryption + symmetric encryption

Encryption

Your data is attacked

Encryption

- standard and custom encryption algorithms used
  - AES
  - RSA
  - ECDH
- Since all those standard encryption algorithms can be regarded as uncrackable, the main reason why ransomware can be cracked is completely due to the improper use of standard encryption algorithms.

How Ransomware operates

- Ransomware identifies the drives on an infected system and begins to encrypt the files within each drive.
- Ransomware generally adds an extension to the encrypted files
  - such as .aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, .cryptolocker, .vault, or .petya,
- to show that the files have been encrypted—the file extension used is unique to the ransomware type.
- Once the ransomware has completed file encryption, it creates and displays a file or files containing instructions on how the victim can pay the ransom.
- If the victim pays the ransom, the threat actor may provide a cryptographic key that the victim can use to unlock the files, making them accessible.

Network shares & Ransomware

- Many ransomware families including the samples of Virlock, TeslaCrypt, and CTB-Locker also enumerate and encrypt network file shares
- Some families can find and encrypt networks shares that are unmapped
- Online file sharing such as Dropbox mapped to a drive letter on the local machine may also have saved content encrypted
- Some ransomware strains, including a variant of Virlock, use the desktop sync clients of popular cloud services to access and encrypt files stored in the cloud

Staying hidden

- Some malware sits there encrypting in the background and decrypting anything the user asks for.
  - It's silent during this phase, it only demands the ransom after everything has been encrypted.
- Others conceal their activity by using rootkits making the files appear to be OK until the process is complete.
  - By intercepting file-system calls you can change the user's view of what is actually present on the disk, making it appear that everything is still OK until its finished

Alert

It makes its demands

Alert

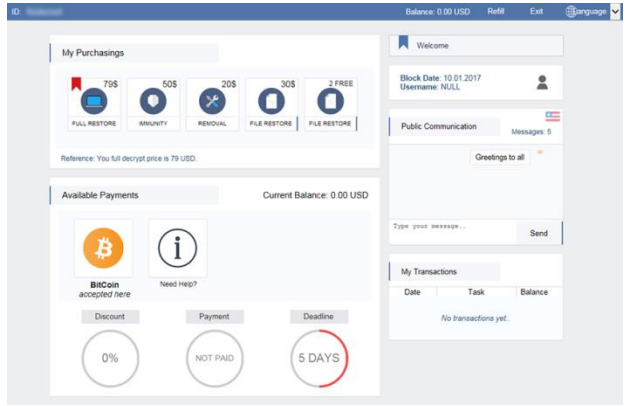
- Alerts the user to the infection
- Demands payment
- Gives details of how to make payment
- Sets the time limit to make the payment

Decryption

If you paid up

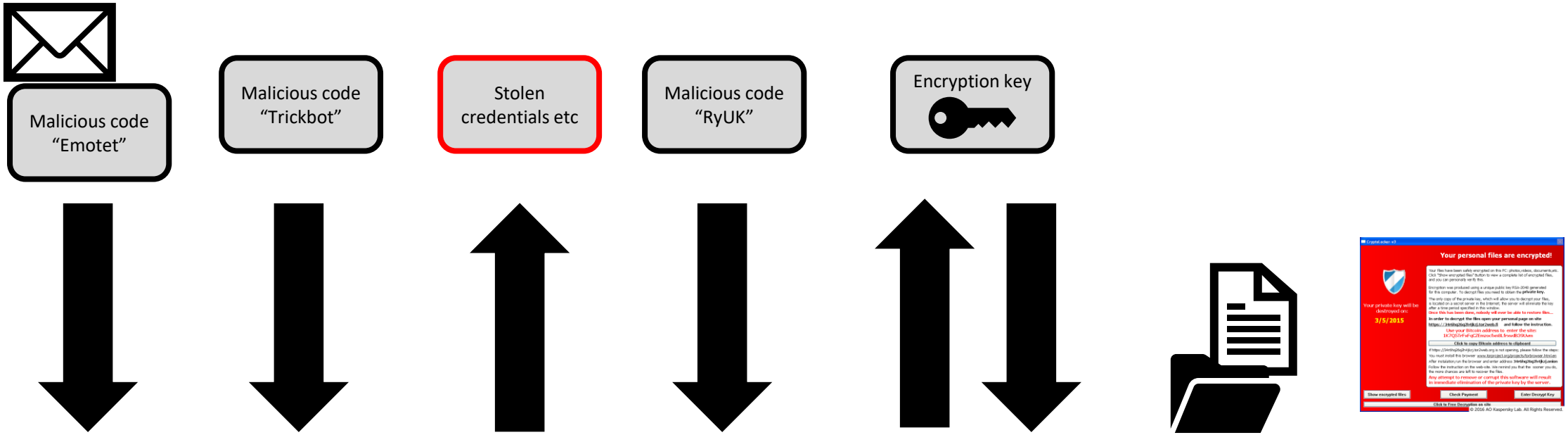
Decryption

- After payment keys will be made available
- If feasible data will be decrypted
- Your machine may be inoculated to prevent further attacks
- The ransomware may remove itself



Case study

Stages of the attack



Email with attachment arrives and is opened by recipient

Malware downloads additional code. It then propagates around the network

Malware contacts C&C servers to get instructions, download additional code and exfiltrate any stolen data

Ransomware contacts its C&C servers and gets keys for encryption

Ransomware is triggered and it encrypts data files on the network

Once encryption is complete and keys deleted it displays ransom note

Blended threat

- Ryuk ransomware has been linked to other malware families, in particular the Emotet and Trickbot banking trojans, although it could also be dropped by other malware
- Emotet is a modular banking trojan first detected in 2014, and while it has its own capability, has been increasingly used as a dropper for other trojans, facilitating the deployment of other threats.
- Trickbot, which has been targeting victims since late 2016, employs browser manipulation techniques to facilitate data theft with the aim of accessing the victims' various online accounts in order to enable further fraud and generate financial revenue for the operators.

Emotet

- Emotet is an advanced banking trojan that primarily functions as a downloader or dropper of other banking trojans.
- Its goal is to steal user credentials, card details, financial and banking information and send them back to command and control servers via cookies in http requests.
- Emotet is commonly spread by email, both using infected attachments as well as by embedded URLs in the email that download this trojan

https://www.us-cert.gov/ncas/alerts/TA18-201A

Trickbot

- The Trickbot component used to spread the infection laterally though the network.
- The infection is spread via multiple channels.
  - ExternalBlue exploit (SMB)
  - Network Shares
  - Admin Shares
  - Credential bruteforcing
  - Credential scraping

https://www.ncsc.gov.uk/news/trickbot-banking-trojan

Brute forcing credentials

- will attempt to take control of a computer by launching a brute force attack against the account login details.
- first targets normal user accounts, such as “NetUserEnum”.
  - If the login attempt fails, it then targets the device’s administrator account.
  - If the brute force attack is successful it gains access to the computer, it will then copy itself from the attacking device onto the newly infected one.

123456, password, 12345678, qwerty, 123456789, 12345, 1234, 111111, 1234567, dragon, 123123, baseball, abc123, football, monkey, letmein, 696969, shadow, master, 666666, qwertyuiop, 123321, mustang, 1234567890, michael, 654321, pussy, superman, 1qaz2wsx, 7777777, fuckyou, 121212, 000000, qazwsx, 123qwe, killer, trustno1, jordan, jennifer, zxcvbnm, asdfgh, hunter, buster, soccer, harley, batman, andrew, tigger, sunshine, iloveyou, fuckme, 2000, charlie, robert, thomas, hockey, ranger, daniel, starwars, klaster, 112233, george, asshole, computer, michelle, jessica, pepper, 1111, zxcvbn, 555555, 11111111, 131313, freedom, 777777, pass, fuck, maggie, 159753, aaaaaa, ginger, princess, joshua, cheese, amanda, summer, love, ashley, 6969, nicole, chelsea, biteme, matthew, access, yankees, 987654321, dallas, austin, thunder, taylor, matrix, william, corvette, hello, martin, heather, secret, fucker, merlin, diamond, 1234qwer, gfhjkm, hammer, silver, 222222, 88888888, anthony, justin, test, bailey, q1w2e3r4t5, patrick, internet, scooter, orange, 11111, golfer, cookie, richard, samantha, bigdog, guitar, jackson, whatever, mickey, chicken, sparky, snoopy, maverick, phoenix, camaro, sexy, peanut, morgan, welcome, falcon, cowboy, ferrari, samsung, andrea, smokey, steelers, joseph, mercedes, dakota, arsenal, eagles, melissa, boomer, booboo, spider, nascar, monster, tigers, yellow, xxxxxx, 123123123, gateway, marina, diablo, bulldog, qwer1234, compaq, purple, hardcore, banana, junior, hannah, 123654, porsche, lakers, iceman, money, cowboys, 987654, london, tennis, 999999, ncc1701, coffee, scooby, 0000, miller, boston, q1w2e3r4, fuckoff, brandon, yamaha, chester, mother, forever, johnny, edward, 333333, oliver, redsox, player, nikita, knight, fender, barney, midnight, please, brandy, chicago, badboy, iwantu, slayer, rangers, charles, angel, flower, bigdaddy, rabbit, wizard, bigdick, jasper, enter, rachel, chris, steven, winner, adidas, victoria, natasha, 1q2w3e4r, jasmine, winter, prince, panties, marine, ghbdtn, fishing, cocacola, casper, james, 232323, raiders, 888888, marlboro, gandalf, asdfasdf, crystal, 87654321, 12344321, sexsex, golden, blowme, bigtits, 8675309, panther, lauren, angela, bitch, spanky, thx1138, angels, madison, winston, shannon, mike, toyota, blowjob, jordan23, canada, sophie, Password, apples, dick, tiger, razz, 123abc, pokemon, qazxsw, 55555, qwaszx, muffin, johnson, murphy, cooper,

RyUK

- Ryuk is a type of ransomware that is used in targeted attacks against enterprises and organizations
- Ryuk is used in targeted attacks, where the threat actors make sure that essential files are encrypted so they can ask for large ransom amounts.
- The Ryuk ransomware itself does not contain the ability to move laterally within a network.
- Ryuk is a persistent infection. The malware's installer will attempt to stop certain antimalware software

https://www.ncsc.gov.uk/news/ryuk-advisory

RyUK

- Uses anti-forensic recovery techniques (such as manipulating the virtual shadow copy) to make recovering from backups difficult.
- All non-executable files across the system will be encrypted and will be renamed with the .ryk file extension.
- A ransom note will be dropped in each processed folder with the name RyukReadMe (.html or .txt).

Post mortem

- The infection would been less likely to of occurred if users where aware of how to detect phishing emails and this was tested.
- The spread of the infection would have been limited if the following had been done
  - The operating systems and applications were latest versions and patched
  - SMBv1 had been disabled
  - Segmented network with firewall enabled on hosts.
  - Restrictive firewall rules on the perimeter had been in place
- The cost of the outbreak would have been a lot less if
  - at the initial infection the network had been shutdown and rebuilt

Prevention and Remediation

Standards & Controls

- The following standards have controls that can help protect an organisation from Ransomware
  - Cyber Essentials
  - 10 steps to Cyber Security
  - ISO27001/2
  - PCI DSS
  - NIST Cybersecurity Framework
  - CIS top 20 controls

NCSC Guidance

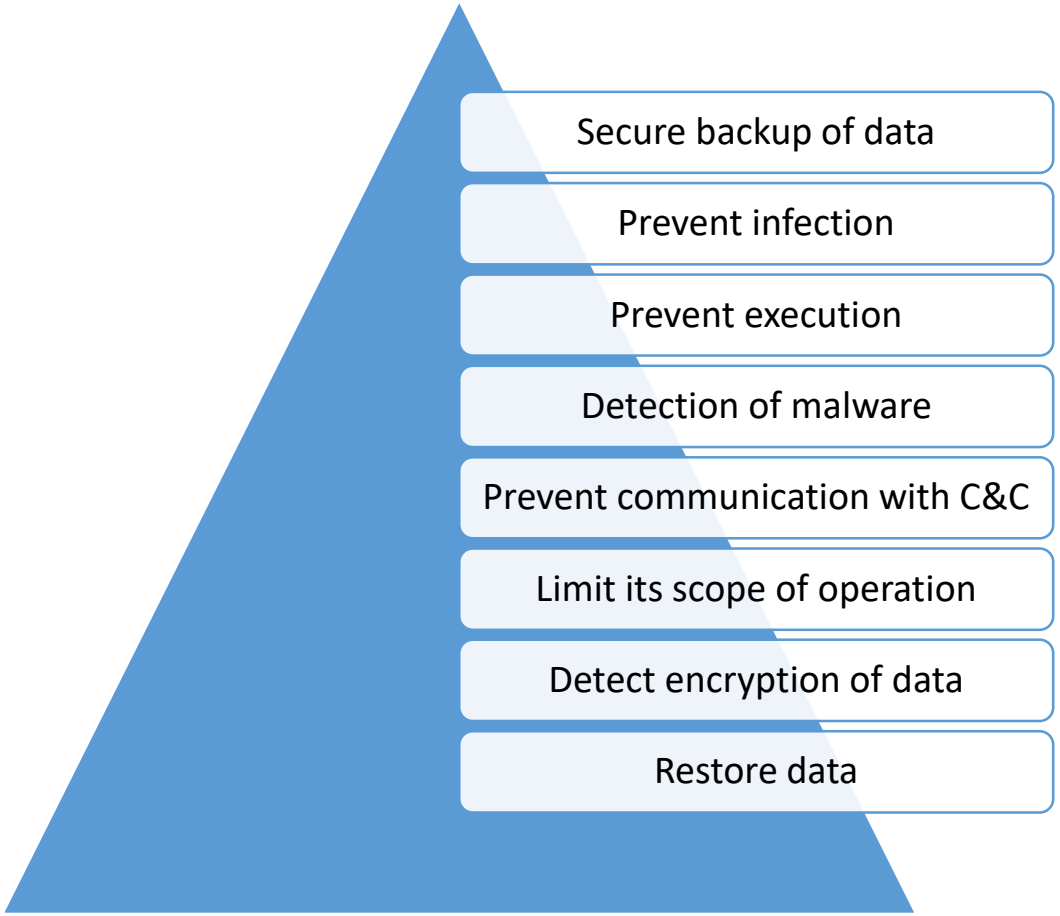
- Defend against phishing attacks
- Vulnerability management and patching
- Controlling code execution
- Filter web browsing traffic
- Control removable media access

https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Limiting the impact of a ransomware attack

- Good access control is important.
  - The compartmentalisation of user privileges
  - Understand the risks brought in by the system administration model that your IT architecture uses.
  - Re-evaluate permissions on shared network drives
  - System administrators should avoid using their admin accounts for email and web browsing.
- Ensure ransomware doesn’t have to go viral in your organisation
  - limit access to your data and file systems to those with a business need to use them.
- Have a backup of your data.
  - Organisations should ensure that they have fully tested backup solutions in place.
  - Backup files should not be accessible by machines which are at risk of ingesting ransomware.

Layered approach



15 Point Strategy

What should I be doing?

Prevention and Remediation

- **Buy Cyber Insurance**
  Cyber insurance can help pay for pay for a wide variety of costs such as third-party support, new infrastructure and potentially including the ransom. Insurers also have preferred provider relationships established with cyber incident response companies, forensic investigators, and other resources that could have been essential in an emergency.

Prevention and Remediation

- **Get a Third-Party Ransomware Risk Assessment Now**
  A thorough risk assessment can outline costs and help determining just what kind of outage is worth how much of ransom, etc. which will help guide hard decisions. Using a third party to conduct a risk assessment makes it easier to defend those decisions.

Prevention and Remediation

- **Identify Your Response Team Now**
  Identifying the incident response team before the incident makes it easier to respond when your computer screen is locked, and phones don’t work. Be defining the official chain of command, when the law enforcement should get involved, the legal notification requirements, when should attorneys and public affairs be called, who hires the third-party advisers, the forensic investigators, and any other cybersecurity specialists will speed the response and decision making process.

Prevention and Remediation

- **Awareness Training for Users**
  Most ransomware attacks happen through human error. Ensuring they are trained and supported will reduce the risk. Just by educating them can reduce the risk, but users can be bad at security. Distributing and displaying a checklist of fundamentals will create a very basic layer of security that reduces the threat of phishing and human error that have caused many a ransomware infection

Prevention and Remediation

- **Map Out Your Attack Surface**
  Mapping out all of an organisation's potential entry points especially if is distributed with many facilities, can help to define what needs to be protected. It is a case of look at what you have before you try to secure it.

Prevention and Remediation

- **More Segmentation, Less Integration**
  Part of the severity of the impact with ransomware is to with it spreading through an organisation. Reducing the spread can keep the impact manageable. By segregating the network into functional areas and separating operational systems from administrative systems it can be possible to stop ransomware infecting the whole network.

Prevention and Remediation

- **Practice Good Security Hygiene**
  It is the basic boring good security hygiene practise that will often save an organisation from a cyber-attack. The patching, updating, secure configurations are the fundamental blocks that support a cyber resilient program. Limiting administrator privileges and managing credentials properly will also help prevent the vulnerabilities that ransomware operators exploit.

Prevention and Remediation

- **Do Better Backups, with Versioning**
  By having a backup strategy and ensure employees do back up their files can make recover much easier. Versioning backup solutions enable you to return to versions of files that existed before the ransomware attack as the malware may have been dormant for a while before denotating. During the dormancy state it may of infected files to ensure it is difficult to eradicate if only immediate backups are made.

Prevention and Remediation

- **Deploy Endpoint Solutions**
  They are a number of products that offer ransomware protection across an organisations endpoints, even if the investment in a renowned ransomware protection product is too much for the whole organisation it should be considered for those that are the most sensitive or the most at risk.

Prevention and Remediation

- **Get an Incident Command System Going**
  Having an incident command system (ICS) in place can provide response teams with an action plan, a means to communicate with all staff and provide guidance and activities to staff affected by the ransomware while they are unable to access systems whilst recovery is ongoing. Reducing staff being idle during an attack.

Prevention and Remediation

- **Isolate Systems and Contain the Impact**
  The segmentation and isolation of different functions within a network can reduce the lateral movement of ransomware through an organisation localising the effect of the attack and reducing its ability to cause the whole organisation. Segregating front end systems from backend can prevent databases being infected and allow data to be access to continuing operations.

Prevention and Remediation

- **Check for Decryption Keys Online**
  Many cyber security organisation such as NoMoreRansom.org maintain a list of published decryption keys and applications to recover data from common ransomware variants in the event of an attack. Identify a strain and searching reputable organisations online can save paying a ransom to recover.

Prevention and Remediation

- **Watch What You Say to Ransomware Operators**
  If paying a ransom, negotiate, don’t pay the full price They will often be happy to get some money than no money. Make sure decryption keys work, get test files decoded where you know the contents, but they can’t be traced back to your organisation. If you are large organisation it is important not to let them find out, you could afford a bigger ransom.

Prevention and Remediation

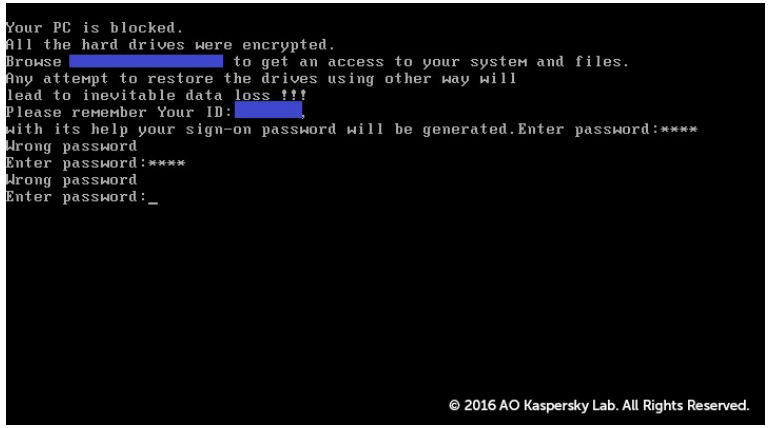
- **Be Careful with Decrypted Files**
  If files are decoded didn't just accept the files back, though carefully reintroducing files through a sheep dip process, making sure you are not introducing weaponized documents or new malware into the system.

Prevention and Remediation

- **Learn from the Experience**
  As with all incidents it is important to conduct a post-mortem and learn from the experience and implement changes to your processes to improve the response and reduce the likelihood of being infected in the future.

Incident response

If you see these prevention has failed!



NCSC advice: preventing the spread of the infection

- Immediately disconnect you computer, laptop or tablet from network. Turn off your Wi-Fi.
- Safely format or replace your disk drives.
- Whilst you're still disconnected from your network, directly connect this computer to the Internet.
- Install and update the operating system and all other software.
- Install, update, and run antivirus software.
- Reconnect to your network.
- Monitor network traffic and/or run antivirus scans to identify if any infection remains.

Triage

- an incident has been detected and you need to determine what has happened
- Once one user has a ransomware attack it is important to determine if it isolated to that machine or has spread around the network.
- With some attacks the infection has been on the network for a period of time and spread around the network before being triggered. Isolating infected machines is critical as well as examining other machines for indicators of compromise.

Communication plan

- a communication plan should be in place to communicate issues to employees using out of bands communications that don’t rely on the network.
- Calling tree
- Having calling plans that utilise a tree structure allowing messages to filter down from senior management should be in place.
- Based on company organisation chart / hierarchy

Cleansing machines

- Clean
  - Use AV tools to remove infection
  - Harden machine
  - Restore data from backups
- Rebuild
  - Rebuild from a hardened image
  - Restore data from backups

Retrieving data

- Data can be restored from backup
- Use a decrypting tool from a reputable source
- Pay ransom

To pay or not to pay, that is the question

The decision

Paying the ransom

- Possible cheapest option
- Quick return to BAU
- Funds criminal activities
- Encourages more attacks
- May not get a working key
- Data may be lost

Not paying the ransom

- Possible the more expensive option
- Longer to get back to BAU
- Discourages more attacks
- Requires data to be backed up or be re-entered
- Data may be lost

Encourages more ransomware

A recent ProPublica investigation found that insurance firms are inadvertently fueling the ransomware economy by advising cities to pay ransom demands, rather than rebuild IT networks -- as ransom payments are always cheaper for the insurance firm to cover.

This rise in the number of successful ransom payments has, in turn, attracted more ransomware gangs, breathing new life into the ransomware landscape that appeared to had died off and slowed down last year.

https://www.zdnet.com/article/ransomware-gang-wanted-5-3-million-from-us-city-but-they-only-offered-400000/

RANSOMWARE ENABLERS

The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks

Even when public agencies and companies hit by ransomware could recover their files on their own, insurers prefer to pay the ransom. Why? The attacks are good for business.

by Renee Dudley, Aug. 27, 5 a.m. EDT

https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

Law enforcement advice

- If you become infected with ransomware, the USA and UK law enforcement agencies (FBI, NCSC) encourages industry and the public not to pay the ransom. If you do pay:
  - there is no guarantee that you will get access to your data/device
  - your computer will still be infected unless you complete extensive clean-up activities
  - attackers may assume that you would be open to paying ransoms in the future
  - you will be funding criminal groups

NCSC advice

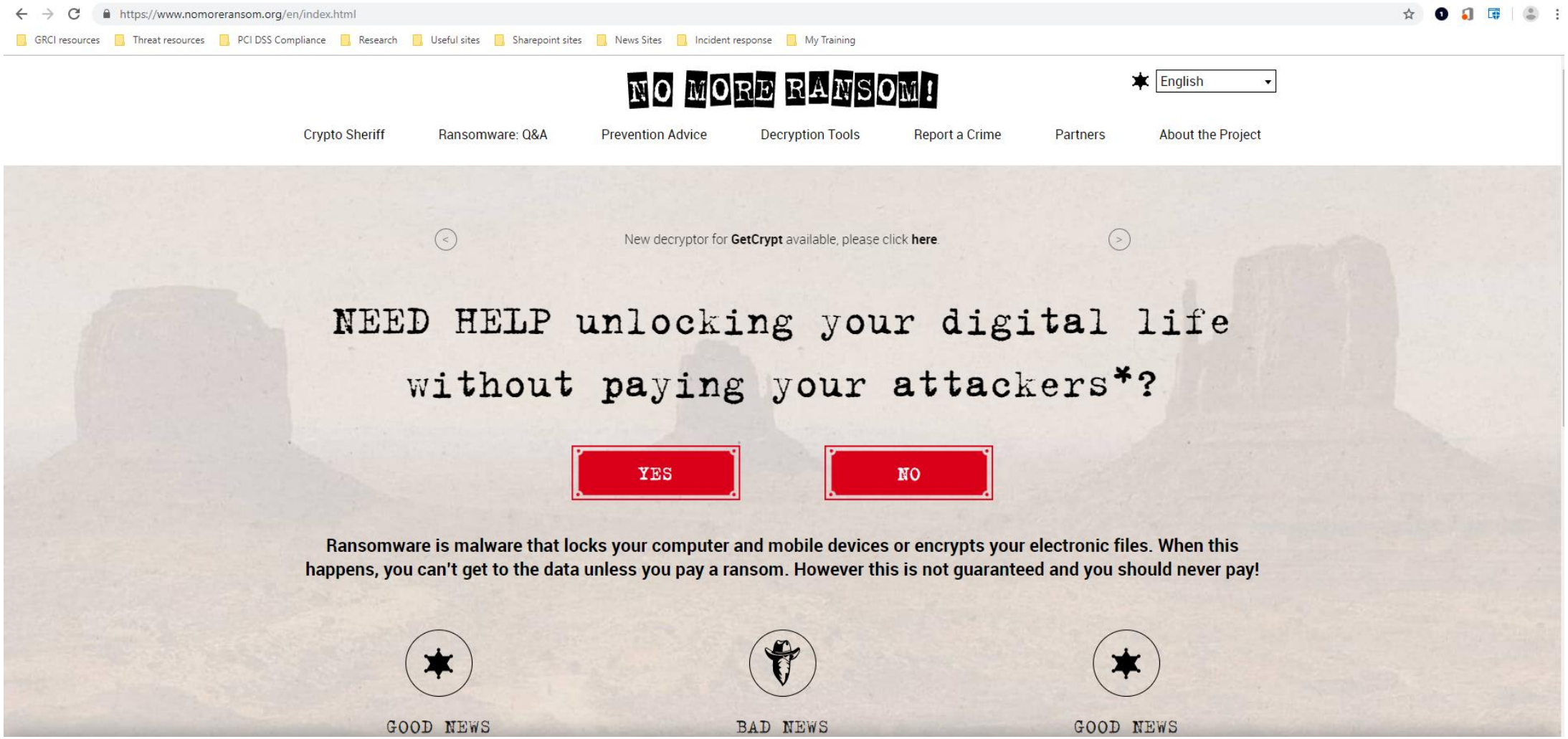
- The National Crime Agency encourages anyone who thinks they may have been subject to online fraud to contact Action Fraud at www.actionfraud.police.uk. It is a matter for the victim whether to pay the ransom.
- The National Cyber Security Centre (NCSC) runs a commercial scheme called Cyber Incident Response, where certified companies provide crisis support to affected organisations.
- The Cyber Security Information Sharing Partnership (CiSP) offers organisations in the UK a safe portal in which to discuss and share intelligence that can assist the community and raise the UK's cyber resilience. We encourage our members to share technical information and indicators of compromise so that the effects of new malware, and particularly ransomware, can be largely reduced.

Decryption tools

Typical encrypted file extensions

- Troldesh Ransomware [.xtbl]
- Crysis Ransomware [.CrySiS]
- Cryptxxx Ransomware [.crypt]
- Ninja Ransomware [@aol.com$.777]
- Apocalypse Ransomware [.encrypted]
- Nemucod Ransomware [.crypted]
- ODC Ransomware [.odcodc]
- LeChiffre Ransomware [.LeChiffre]
- Globe1 Ransomware [.hnyear]
- Globe2 Ransomware [.blt]
- Globe3 Ransomware [.decrypt2017]
- DeriaLock Ransomware [.deria]
- Opentoyou Ransomware [.-opentoyou@india.com]
- Globe3 Ransomware [.globe & .happydayzz]
- Troldesh Ransomware [.dharma]
- Troldesh Ransomware [.wallet]
- Troldesh Ransomware [.onion]
- Satan DBGer Ransomware [.dbger]

Decrypting tools



Funded by Europol

Summary

Strategy

What should I be doing?

Strategy

- Be **Hard** – harden systems, backup data
- Be **Prepared** – have an incident response plan
- Be **Quick** – detect and respond quickly

Prevention – be **Hard**

- Harden systems
  - Patch, update
  - Host based firewalls, IDS
  - AV and other anti-malware tools
- Harden data
  - Backup (3-2-1 rule)
- Harden people
  - User education

Prevention – be **Prepared**

- Incident response plan
- Test the plan
- Have detection in place

Prevention – be **Quick**

- Fast detection
- Kill the execution
- Contain the infection
- Limit the damage
- Communication

Any Questions ?

Resources

Resources

- NCSC Guidance
  - Ransomware: 'WannaCry' guidance for home users and small businesses
  - Protecting your organisation from ransomware
- NIST
  - Guide for Cybersecurity Event Recovery
- PCI SSC
  - Ransomware Resource Guide

Useful links

- Decryption tools
  - https://www.nomoreransom.org/en/index.html