CYBER MANAGEMENT ALLIANCE

https://www.cm-alliance.com

WanaCry Crowdsourced Intelligence - PLEASE READ First

PLEASE share links, notes, images here. If possible, provide a summary of each link. Only add - don't delete anything - leave a comment or use the "Suggest Edits" feature.
All **legal cautions**, caveats etc apply. Before taking any action please consult with your own professionals and use common sense. We take no responsibility for the accuracy of the content and are not liable for any resulting physical, virtual or financial damage!
We apologise for not being able to attribute all the content - if you are the author of some content please let us know. We are not claiming any attribution.
NO comments that incite racism, hatred or any other illegal activity are allowed and will be deleted.

Photos/Images: some of the photos may NOT be genuine! If you know they are fake - do highlight.

1. Whatever you do - please do take an OFFLINE backup of your critical data. If your backup or DR site is always connected - you are in a for a big shock
2. This attack should be a wake up call- There is NO excuse NOT to patch! - Put another PATCH YOUR SYSTEMS immediately! No Excuses.
3. Finally - you really need to have a Cyber Incident Planning & Response strategy in place. Whatever you do PROTECTION is not the only answer. You must be prepared and ready to respond. You must have a management led Cyber Incident Planning & Response strategy.

Who is/are the attacker (s): According to my sources very likely the North Koreans! (please feel free to correct this)

Thanks to everyone who is contributing in their own way. Do please reach on LinkedIn (Amar Singh) and introduce yourself so I may add your name to the list of contributors. Thanks

New Updates: NEW ALERT - BT FAKE EMAIL- PLEASE SHARE & beware

To all the wonderful contributors - feel free to join in the debate next week. Titled Stop Blaming Russia and China for All Cyber Attacks.
https://www.brighttalk.com/webcast/14185/259269

Table of Contents

CYBER MANAGEMENT ALLIANCE

https://www.cm-alliance.com

Useful Links & Twitter Handles

Useful Information	
https://www.cm-alliance.com/hubfs/WanaCry%20Ransomware%20Incident%20Response%20Playbook.pdf	**INCIDENT RESPONSE PLAYBOOKS** WanaCry Ransomware Incident Response **Playbook** by DFLabs - Do
https://github.com/gentilkiwi/wanakiwi/releases	Wannacry- decryption tool It basically tries to retrieve the two prime numbers, used in the formula to generate encryption keys from memory. It will only work if the affected computer has not been rebooted after being infected or if the associated memory has not been allocated and erased by some other process.
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx	Actual CVE- The vulnerability
https://intel.malwaretech.com/WannaCrypt.html https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all	Live Feed by Intel Good dashboard of infected countries
https://www.joesecurity.org/reports/report-db349b97c37d22f5ea1d1841e3c89eb4.html	**Good analysis with screenshots** (not endorsing this service)
https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId=100	**Another Good analysis with screenshots** (not endorsing this service)
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/	Microsoft's Guidance on WANACRYPT
https://www.nomoreransom.org/ https://www.bleepingcomputer.com/forums/t/608858/id-ransomware-identify-what-ransomware-encrypted-your-files/ https://id-ransomware.malwarehunterteam.com	Identify your ransomware by MalwareHunterTeam
https://gist.github.com/Blevene/2ef2b808a114722e5061297a5897a710	Hashes (for more information on how to use hashes - consult with your SIEM/ AV/ Threat Intel provider)

https://github.com/countercept/doublepulsar-detection-script?files=1	Detection Rules
https://www.ncsc.gov.uk/alerts/nhs-alert	UK's National Cyber Security Centre - NHS Alert Page
https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/	Kaspersky - one of the best research teams around - must read and informative as always
https://www.ncsc.gov.uk/cisp	UK's National Cyber Security Centre - Information Sharing Platform
https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168	Similar Collection of information and details
https://www.youtube.com/watch?v=6rrY0S8x3HQ	EternalBlue looks like this :
https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ From the above link: *Finally, this attack provides yet another example of why the **stockpiling** of **vulnerabilities** by **governments** is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the **CIA** show up on WikiLeaks, and now this vulnerability stolen from the **NSA** has affected customers around the world.*	Microsoft publically pointed the finger at the NSA for the ETERNALBLUE exploit being stolen. Brad Smith - President and Chief Legal Officer at Microsoft.
https://securelist.com/blog/research/78411/wannacry-faq-what-you-need-to-know-today/	**Kaspersky Labs reporting that there is still no evidence of an initial attack over email.**
https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst	Good document from ENISA!

Other Useful Links and LinkedIn Posts	
https://www.linkedin.com/hp/update/6268854969684762624	Post by Tempest Security Intelligence
http://varlamov.ru/2370148.html	A good source from a Russian website
https://www.hedgehogsecurity.co.uk/2017/05/12/nhs-england-cyber-attack/	Very informative Post by HedgeHog Security
https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis	WCry/WanaCry Ransomware Technical Analysis

https://sidechannel.tempestsi.com/wannacry-ransomware-spreads-around-the-world-and-impacts-large-enterprises-3036550ed58f	Good source of IOCs, IP, hashes
http://go.newsfusion.com/security/item/931320	
https://blogs.technet.microsoft.com/eopfieldnotes/2015/06/05/tips-to-prevent-zero-day-malware-with-eop/	Microsoft's blog on prevent such attacks
http://blog.checkpoint.com/2017/05/14/wannacry-paid-time-off/	Questions over how the payment / decryption key distribution method could work by Checkpoint
https://www.hiddentext.co.uk/collection-of-resources-on-the-nhs-cyber-attack/	Post by Stuart Coulson
https://digital.nhs.uk/article/1491/Statement-on-reported-NHS-cyber-attack	NHS Statement
https://www.crowdstrike.com/blog/falcon-intelligence-report-wanna-ransomware-spreads-rapidly-continually-encrypts-victim-files/	CrowdStrike Intel Report
https://exchange.xforce.ibmcloud.com/collection/WCry2-Ransomware-Outbreak-8b186bc4459380a5606c322ee20c7729	IBM's X-Force threat intel feed on WanaCry
https://support.microsoft.com/en-gb/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012	How to disable SMBv1. Ransomware uses the ETERNALBLUE exploit to propagate.
https://otx.alienvault.com/pulse/5915db384da2585b4feaf2f6/ https://www.us-cert.gov/ncas/alerts/TA17-132A	IOCs for Wannacry
https://securelist.com/blog/research/78411/wannacry-faq-what-you-need-to-know-today/	YARA Rules for Wannacry by Kaspersky Lab
https://github.com/Neo23x0/signature-base/blob/master/yara/crime_wannacry.yar	YARA Rules Published by Florian Roth

Useful Twitter Handles

Feel free to your twitter handle or other's that you think everyone should be aware of.

- https://twitter.com/NCSC
- https://twitter.com/cm_alliance
- https://twitter.com/teddy_breath
- https://twitter.com/shadowbrokerss
- https://twitter.com/Naushad_IT
- https://twitter.com/SPCoulson
- https://twitter.com/MalwareTechBlog
- https://twitter.com/actual_ransom
- https://twitter.com/amisecured
- https://twitter.com/msuiche

- https://twitter.com/malwareunicorn
- https://twitter.com/ransomtracker

Speculation

Speculation: Was this attack initially designed to be launched at scale? The payment validation system appears to require human interaction on the attacker side. Obviously this wouldn't be sustainable at a global scale. Is this a smaller attack that got out of hand, or something else? *Ian Porteous*

Speculation: The "kill switch" was likely an anti-sandbox mechanism. WannaCry makes an HTTP request to a (previously) non-existent domain. Most sandboxes will respond to DNS and HTTP requests to try and discover more about the threat and reveal additional behaviours. When in a sandbox and a request for a domain that should not exist is successful, the malware quits to prevent further analysis. When @MalwareTechBlog registered this domain (hxxp://ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com) all instances of the malware with internet connectivity act as they may be in a sandbox and quit before propagating further or encrypting files. *Ian Porteous*

Speculation : the NHS was hit as they have legacy systems that cannot run on patched/upgraded/Windows 10 systems. May explain why some University Hospitals are also being hit. It would be good if we could find a copy of the infected Word document. Having seen and heard of cases in education where vendors try to charge triple the normal costs seeing government departments as cash cows, some are not able to upgrade due to the extortionate costs. Therefore they end up having to rely on legacy systems. I suspect that some of the IT infrastructure in the NHS cannot be upgraded as the software vendors don't have upgrade paths to Windows 10. *Stuart Coulson*

Link related to the above:

http://www.bbc.co.uk/news/uk-39911385

NHS Digital said that 4.7% of devices within the NHS use Windows XP, with the figure continuing to decrease.

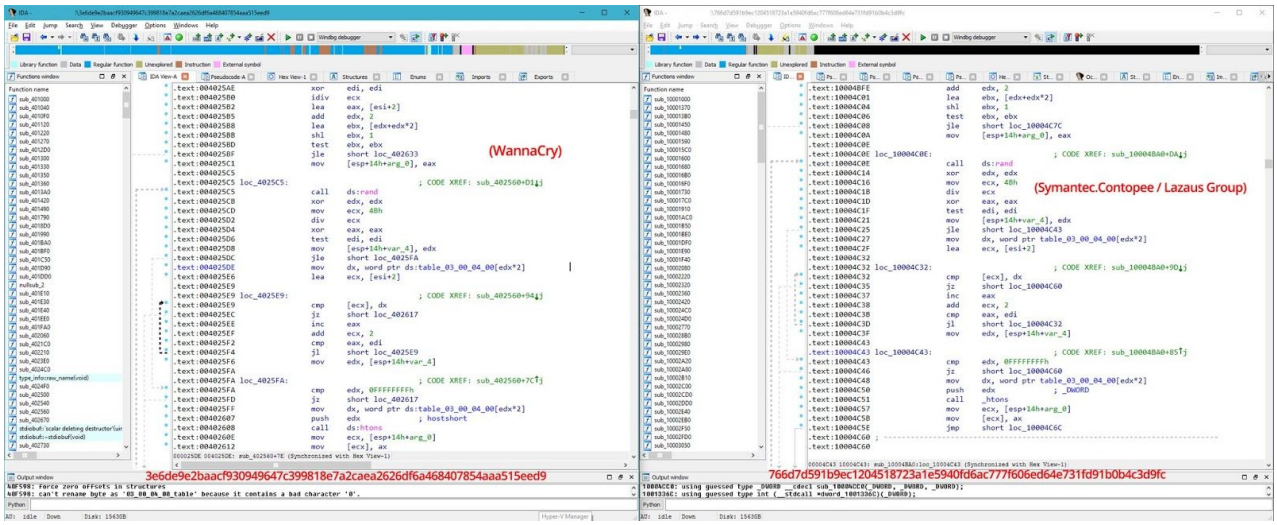
Infected Companies & Organisations

- NHS (uk) turning away patients, unable to perform x-rays. (list of affected hospitals) << why the NHS got hit so bad (N3 backbone - wot no SMB proxy?). (UK 61 NHS Organisation disrupted) (More reasons shared on why?)
- Nissan (uk) http://www.chroniclelive.co.uk/news/north-east-news/cyber-attack-nhs-latest-news-13029913
- Telefonica (spain) (https://twitter.com/SkyNews/status/863044193727389696)
- Power firm Iberdrola and Gas Natural (spain)
- FedEx (us) (https://twitter.com/jeancreed1/status/863089728253505539)
- University of Waterloo (ontario canada)
- Renault shut down several French factories after cyberattack
- Energy giant PetroChina payment systems were hit
- Russia interior ministry & Megafon (russia)
- https://twitter.com/dabazdyrev/status/863034199460261890/photo/1
- VTB (russian bank) https://twitter.com/vassgatov/status/863175506790952962
- Russian Railroads (RZD) https://twitter.com/vassgatov/status/863175723846176768
- Portugal Telecom
- Сбербанк - Sberbank Russia (russia)
- Shaheen Airlines (india, claimed on twitter)
- Train station in frankfurt (germany)
- Neustadt station (germany)
- the entire network of German Rail seems to be affected (@farbenstau)
- in China secondary schools and universities had been affected (source)
- A Library in Oman (@99arwan1)
- China Yanshui County Public Security Bureau (https://twitter.com/95cnsec/status/863292545278685184)
- Renault (France) (http://www.lepoint.fr/societe/renault-touche-par-la-vague-de-cyberattaques-internationales-13-05-2017-2127044_23.php) (http://www.lefigaro.fr/flash-eco/2017/05/13/97002-20170513FILWWW00031-renault-touche-par-la-vague-de-cyberattaques-internationales.php)
- Schools/Education (France) https://twitter.com/Damien_Bancal/status/863305670568837120
- University of Milano-Bicocca (italy)
- A mall in singapore https://twitter.com/nkl0x55/status/863340271391580161
- ATMs in china https://twitter.com/95cnsec/status/863382193615159296
- norwegian soccer team ticket sales https://www.nrk.no/telemark/eliteserieklubber-rammet-av-internasjonalt-dataangrep-1.13515245
- STC telecom (saudia arabia, more, more)
- All ATMs in india closed
- Social security department in the city of Changsha (China)
- XIT-entry bureau in Dalian (China)
- A housing fund in Zhuhai (China)
- Industry watchdog in Xuzhou (China).
- Hospital and other businesses have also been hit by the WannaCry (Japan)
- Thousands of personal computers also WannaCry effected in Japan
- Indonesia's biggest cancer hospital, Dharmais Hospital in Jakarta
- Harapan Kita hospitals (Indonesia)
- 3 Businesses hit by the bug in Australia

- A coal port in New Zealand shut temporarily to upgrade its systems
- Hitachi Ltd. said the attack had affected its systems
- More at https://en.wikipedia.org/wiki/WannaCry_cyber_attack#List_of_affected_organizations they seem to be cataloguing the infections faster/better.

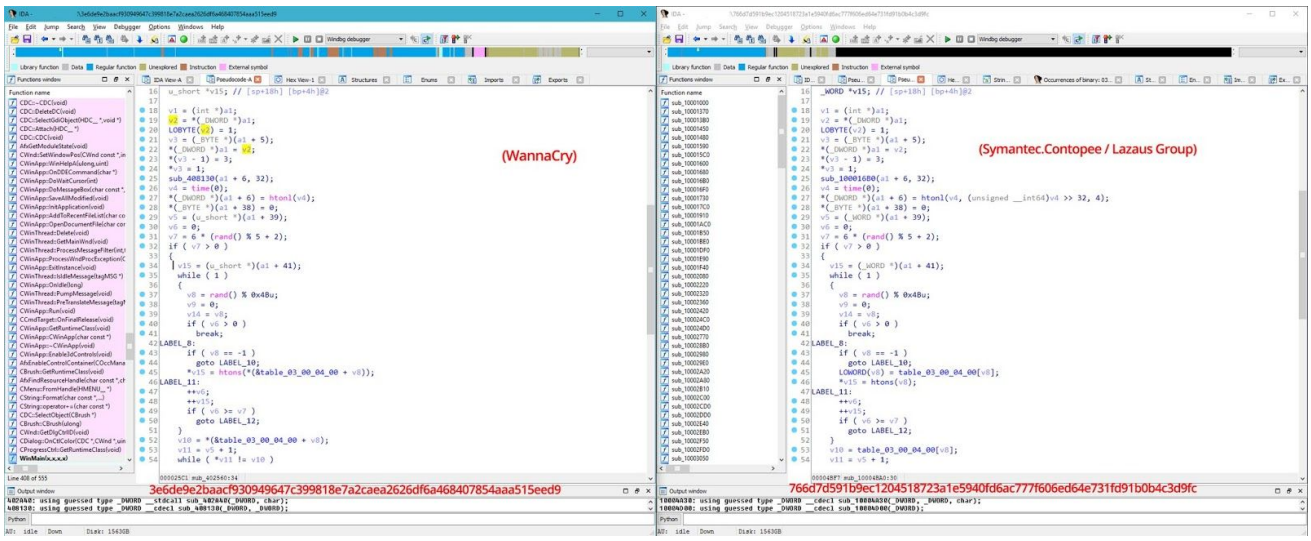
Attribution - Who Did It?

Feel free to add your comments / data.



See below tweets - from Matthieu Suiche

https://twitter.com/msuiche/status/864179805402607623



https://twitter.com/msuiche/status/864186146938605568

https://storify.com/amisecured/conversation-with-msuiche-nova6k0-oranj-zh4ck-jenv

https://twitter.com/0xSpamTech/status/864551791719055360

Background Information

WanaCry and EternalBlue: Partners in Ransom

If you thought cybercrime was an activity reserved for the shadows then Friday the 12th of May 2017 would have left you questioning your beliefs. There could be no darkness to hide in, with the limelight being shone from all media directions on what could become the world's largest coordinated ransomware attack.

Raising the Alarm
With no award for first place, it is not known who reported the attack first, however the British media was quick to report critical infrastructure within the NHS (National Health Service) having been rendered unusable. Some hospitals were turning patients away or warning people to avoid accident and emergency departments for fear of a backlog in patient care.

Some hours later it became known that this was not an attack targeting the NHS, nor the UK but had been discovered in up to 99 counties in a variety of industries. Rumour has it that the Madrid headquarters of Telefonica used their in-house announcement system to demand that users stop using their terminals until the situation had been assessed.

The Threat and its Origins
"How could this happen?" the media cried. Is it negligence? Is it underfunding? Arguing against extra funding is generally seen as counterproductive, however the it would seem that this one event has awoken the world to a problem which IT security professionals have been living in for some time. Ransomware is of course not new, in-fact its popularity (for lack of a better word) peaked in 2016, so much so that the FBI reported that global ransom payments would top $1 billion by the end of the year. It turned out they underestimated.

The ransomware variant under scrutiny in this case is a variant of the WannaCry strain. A particularly nasty ransomware which after infecting its initial host, seeks out other hosts in the network to move onto through the SMBv1 (Server Message Block) protocol. Once on a host, the ransomware encrypts files and then removes the ability to restore from tool such as system repair or volume snapshots. Finally, a message is presented on-screen demanding payment of up to $600 into a bitcoin wallet within an allotted time.

Affected operating systems include:

- Microsoft Windows Vista SP2
- Windows Server 2008 SP2 and R2 SP1
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 and R2
- Windows 10
- Windows Server 2016
- Windows XP

Update: Microsoft has released ETERNALBLUE patches for non-supported operating systems such as Windows XP.

At the time of writing, the bitcoin wallet (115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn) requesting payment has already been filling up, despite the advice of law enforcement, some have decided that the cost of payment is less than the potential loss of that host. For the latest update on the reported Bitcoin accounts being used, please visit https://twitter.com/ransomtracker.

The question therefore becomes how did this strain of known ransomware manage to penetrate so many household name brands and organisations? The answer lies in a slightly less widely reported event on the 8th of April 2017, when a cybercriminal collective known as The Shadow Brokers leaked a treasure trove of NSA (National Security Agency) spying tools. Included in this release was a tool known as ETERNALBLUE, which could exploit a flaw in Microsoft Windows operating systems and allow for files to be moved over the SMBv1 protocol without effort or authentication.

It is not known for how long the NSA had been using ETERNALBLUE, however Microsoft was unaware of the vulnerability (**However**, MS claims that they had patched this vulnerability before the Shadow broker release here) only releasing a patch six days after the Shadow Brokers' leak.

Prior to the release of Wannacry, other criminals had been using the same vulnerability to conduct cryptocoin mining, which had a secondary effect of preventing Wannacry infecting the endpoints that were already infected with Adylkuzz. And possibility that Adylkuzz might be bigger than WannaCry (https://www.itnews.com.au/news/bigger-than-wannacrypt-attackers-use-same-nsa-exploits-to-mine-cryptocurrency-461932).

Multiple variants of the original ransomware with modified kill-switch domains being seen in the wild. New sinkholes being set up by various security researchers and vendors.

Reports are currently that these are simply modified with a hex-editor, not recompiled versions of the original. Some variants with no kill-switch have also been seen, but there are apparently no reports of one with a working SMB propagation mechanism.

Unfortunate incident of sink-holes being taken down by law enforcement being reported by @MalwareTechBlog.
https://twitter.com/MalwareTechBlog/status/864186357136207873

> "*We lost two sinkhole servers due to a take-down request from law enforcement, but these were immediately replaced to ensure no downtime.*"

(Tech)Precautions, Detection & Response

- **Patch Management**
  - Ensure all Workstations and Servers have the latest Microsoft patches, especially the ones related to MS17-010.
  - Keep all the software on your computer up to date. When your operating system (OS) or applications release a new version, install it. And if the software offers the option of automatic updating, take it.

- **Back-up! Back-up! Back-up!** Have a recovery system in place so a ransomware infection can't destroy your personal data forever. It's best to follow the 3-2-1 backup method: Three backups of your data, Two that are onsite and one that is

offsite. Options include one backup set stored in the cloud (remember to use a service that makes an automatic backup of your files) and one stored physically (portable hard drive, thumb drive, extra laptop, etc.). Disconnect these from your computer when you are done. Your backup copies will also come in handy should you accidentally delete a critical file or experience a hard drive failure.

- **Operating System**
  - Disable SMBv1 this prevents Wannacry from spreading within your network.

- **Antivirus**
  - Ensure AV signatures are updated on all assets. Identify critical assets and target them first. Block IOCs on AV solution.
  - Get the details with regards to the name of the malware and verify if this malware has been detected in the logs for last 1 week.
  - **Use robust antivirus software** to protect your system from ransomware. Do not switch off the 'heuristic functions' as these help the solution to catch samples of ransomware that have not yet been formally detected.

- **IPS - Intrusion Prevention System**
  - Ensure IPS signatures are updated. Verify if the signature that can detect this vulnerability / exploit attempt is enabled and is in blocking mode.
  - Get the details with regards to the name of the Signature and verify if this Signature has been detected in the logs for last 1 week.
  - Example signature: alert tcp $HOME_NET 445 -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:2;)

- **eMail Gateway**
  - Ensure eMail Gateway solutions has all relevant updates for detecting possible mails that may bring the Trojan in the environment.

- **Proxy**
  - Ensure Proxy solution has updated database. Block IOCs for IP Address and Domain names on the Proxy.
  - Verify last one week logs for the IOCs on Proxy and take action on sources of infection.
  - Forward communication to hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com to a local IP to confirm Sinkhole of Kill Switch is always maintained if infected.

- **Firewall**
  - Block the IP addresses on Perimeter Firewall.
  - Verify logs for last one week.
  - Segment internal networks to contain outbreaks.
  - Block Port 445 (SMB)

- **Anti** - APT Solutions
  - Ensure signatures are up to date.
  - Check for possible internal sources of infection and take actions.

- **SIEM**
  - Check logs to verify if any of the IOCs have been detected in 1 week logs.
  - Integrate IOCs (Indicators of Compromise) with your SIEM

- **"Next Generation AV" / Advanced Endpoint Protection / Anti-Ransomware Products**
  - These products are designed to detect new threats without a specific update, but many are still relatively new to market and not widely adopted.

- **Detecting Vulnerable Hosts in your network**
  - All major vulnerability scanners have detection capabilities to detect hosts that are vulnerable in the network.
  - Various tools out there that can be used to see if endpoint hosts are vulnerable.
    - Nmap script to scan your network and check if endpoints are vulnerable: https://github.com/cldrn/nmap-nse-scripts/blob/master/scripts/smb-vuln-ms17-010.nse
  - A custom policy created with specific plugin id's can be used to quickly scan hundreds of subnets.

- **Trust no one. Literally.** Any account can be compromised and malicious links can be sent from the accounts of friends on social media, colleagues or an online gaming partner. Never open attachments in emails from someone you don't know. Cybercriminals often distribute fake email messages that look very much like email notifications from an online store, a bank, the police, a court or a tax collection agency, luring recipients into clicking on a malicious link and releasing the malware into their system.

- **Enable the 'Show file extensions'** option in the Windows settings on your computer. This will make it much easier to spot potentially malicious files. Stay away from file extensions like '.exe', '.vbs' and '.scr'. Scammers can use several extensions to disguise a malicious file as a video, photo, or document (like hot-chics.avi.exe or doc.scr).

- If you discover a rogue or unknown process on your machine, disconnect it immediately from the internet or other network connections (such as home Wi-Fi) — this will prevent the infection from spreading.

Repositories & Analysis (PCAPS, Code)

This section has some technical details including PCAP files

- **Full Technical and Cryptographic Analysis available for download here**
- **For an image of the WireShark Analysis click here**
- **Download the FULL PCAP for your own WireShark Analysis here** (8MB file)

https://www.joesecurity.org/reports/report-db349b97c37d22f5ea1d1841e3c89eb4.html	**Good analysis with screenshots** (not endorsing this service)

https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId=100

Another Good analysis with screenshots (not endorsing this service)

***** Cryptography Details *****

- Each infection generates a new RSA-2048 keypair.
- The public key is exported as blob and saved to 00000000.pky.
- The private key is encrypted with the ransomware public key and saved as 00000000.eky.
- Each file is encrypted using AES-128-CBC, with a unique AES key per file.
- Each AES key is generated CryptGenRandom.
- The AES key is encrypted using the infection specific RSA keypair.
- The RSA public key used to encrypt the infection-specific RSA private key is embedded inside the DLL and owned by the ransomware authors.

***** Command and Control IPs *****

- 188[.]166[.]23[.]127:443
- 193[.]23[.]244[.]244:443
- 2[.]3[.]69[.]209:9001
- 146[.]0[.]32[.]144:9001
- 50[.]7[.]161[.]218:9001
- 217.79.179[.]77
- 128.31.0[.]39
- 213.61.66[.]116
- 212.47.232[.]237
- 81.30.158[.]223
- 79.172.193[.]32
- 89.45.235[.]21
- 38.229.72[.]16
- 188.138.33[.]220
- 87[.]7[.]10[.]93
- 192[.]42[.]115[.]101
- 178[.]62[.]197[.]82
- 212[.]47[.]244[.]98
- 5[.]35[.]251[.]247
- 128[.]31[.]0[.]39
- 91[.]219[.]236[.]222
- 144[.]76[.]92[.]176
- 148[.]244[.]38[.]101
- 149[.]202[.]160[.]69
- 163[.]172[.]149[.]155
- 171[.]25[.]193[.]9
- 195[.]22[.]26[.]248
- 197[.]231[.]221[.]221
- 198[.]96[.]155[.]3
- 213[.]61[.]66[.]117
- 46[.]101[.]166[.]19
- 62[.]210[.]124[.]124
- 91[.]121[.]65[.]179
- 91[.]219[.]237[.]229
- 212[.]47[.]232[.]237:9001

- 81[.]30[.]158[.]223:9001
- 79[.]172[.]193[.]32:443
- 46[.]101[.]166[.]19
- 23[.]254[.]167[.]231

A wider set of malicious IP addresses as identified here (http://trapx.com/wannacry-thoughts-and-threat-intelligence/)

***** TOR C2 Addresses *****

- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maqm7.onion

***** Observed hash values *****

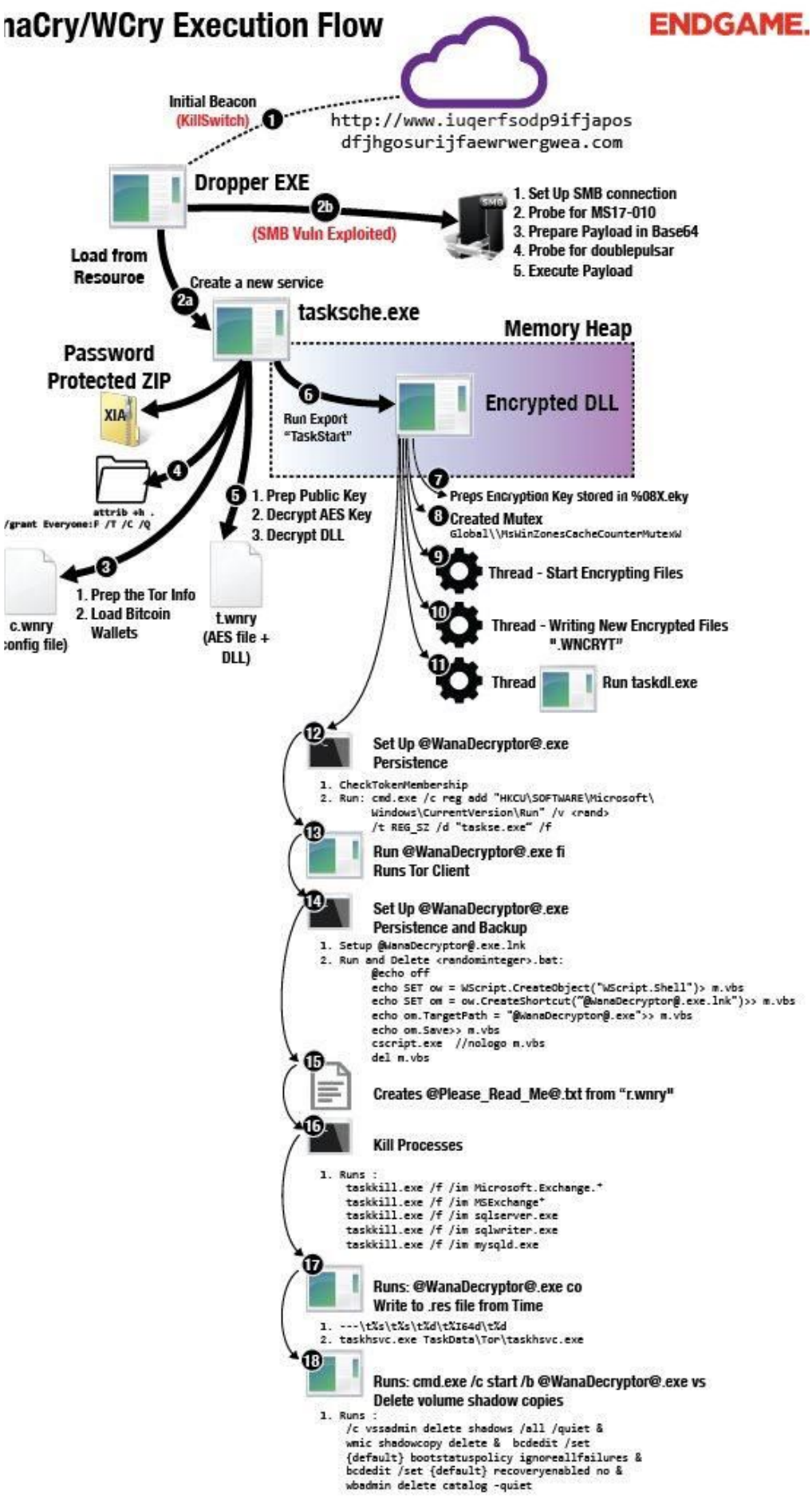
- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
- 0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
- 428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
- 5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
- 62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
- 72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
- 85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
- a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
- a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
- 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
- 2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
- 7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
- a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
- fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
- 9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- 4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa

***** List of file names encrypted by WannaCry ransomware: *****

der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds, .max, .3dm, .ods, .sxc, .stc, .dif, .slk, .wb2, .odp, .sxd, .std, .sxm, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .mdf, .ldf, .cpp, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .mkv, .flv, .wma, .mid, .m3u, .m4u, .svg, .psd, .tiff, .tif, .raw, .gif, .png, .bmp, .jpg, .jpeg, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .ARC, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .dwg, .pdf, .wk1, .wks, .rtf, .csv, .txt, .msg, .pst, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotm, .dot, .docm, .docx, .doc,

Full file is available for download here

Legal & GDPR


naCry/WCry Execution Flow
ENDGAME.
Initial Beacon
(KillSwitch)
1
http://www.iuqerfsodp9ifjapos
dfjhgosurijfaewrwergwea.com
Dropper EXE
2b
(SMB Vuln Exploited)
1. Set Up SMB connection
2. Probe for MS17-010
3. Prepare Payload in Base64
4. Probe for doublepulsar
5. Execute Payload
Load from
Resouroe
Create a new service
2a
tasksche.exe
Memory Heap
Password
Protected ZIP
XIA
6
Run Export
"TaskStart"
Encrypted DLL
4
attrib +h .
/grant Everyone:F /T /C /Q
5
1. Prep Public Key
2. Decrypt AES Key
3. Decrypt DLL
7
Preps Encryption Key stored in %08X.eky
8
Created Mutex
Global\\MsWinZonesCacheCounterMutexW
9
Thread - Start Encrypting Files
10
Thread - Writing New Encrypted Files
".WNCRYT"
11
Thread
Run taskdl.exe
3
1. Prep the Tor Info
2. Load Bitcoin
Wallets
c.wnry
config file)
t.wnry
(AES file +
DLL)
12
Set Up @WanaDecryptor@.exe
Persistence
1. CheckTokenMembership
2. Run: cmd.exe /c reg add "HKCU\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run" /v <rand>
/t REG_SZ /d "taskse.exe" /f
13
Run @WanaDecryptor@.exe fi
Runs Tor Client
14
Set Up @WanaDecryptor@.exe
Persistence and Backup
1. Setup @WanaDecryptor@.exe.lnk
2. Run and Delete <randominteger>.bat:
@echo off
echo SET ow = WScript.CreateObject("WScript.Shell")> m.vbs
echo SET om = ow.CreateShortcut("@WanaDecryptor@.exe.lnk")>> m.vbs
echo om.TargetPath = "@WanaDecryptor@.exe">> m.vbs
echo om.Save>> m.vbs
cscript.exe //nologo m.vbs
del m.vbs
15
Creates @Please_Read_Me@.txt from "r.wnry"
16
Kill Processes
1. Runs :
taskkill.exe /f /im Microsoft.Exchange.*
taskkill.exe /f /im MSExchange*
taskkill.exe /f /im sqlserver.exe
taskkill.exe /f /im sqlwriter.exe
taskkill.exe /f /im mysqld.exe
17
Runs: @WanaDecryptor@.exe co
Write to .res file from Time
1. ---\t%s\t%s\t%d\t%I64d\t%d
2. taskhsvc.exe TaskData\Tor\taskhsvc.exe
18
Runs: cmd.exe /c start /b @WanaDecryptor@.exe vs
Delete volume shadow copies
1. Runs :
/c vssadmin delete shadows /all /quiet &
wmic shadowcopy delete & bcdedit /set
{default} bootstatuspolicy ignoreallfailures &
bcdedit /set {default} recoveryenabled no &
wbadmin delete catalog -quiet

Management and Business Perspective

Here is a little analysis about ransomware. You might have been hit yourself or most likely you know someone who has been hit by a ransomware attack. This very nasty piece of malware becomes a bigger threat every day.

From a strategic point of view, you have to follow future developments of ransomware very closely. As with many previous malware and other attack vectors you can observe the development of new strains and variants. Like in business if the product proofs to be successful further development and enhancements to the product will be applied. This can be observed by the distribution and target selection of the malware. Like phishing in the past who became spear phishing attacks over time, the same is now true for ransomware. Not before long we will have specifically targeted ransomware malware. I am not talking about the attack distribution I am talking about the ransomware itself. We have done a little analysis of ransomware from a business perspective. Basically you have two options (three if doing nothing is an option). First is paying and second is not paying. We put both options on a chart. The chart contains two axis one for costs and one for time. The time axis is synonymous with complexity ranging from simple to complex.

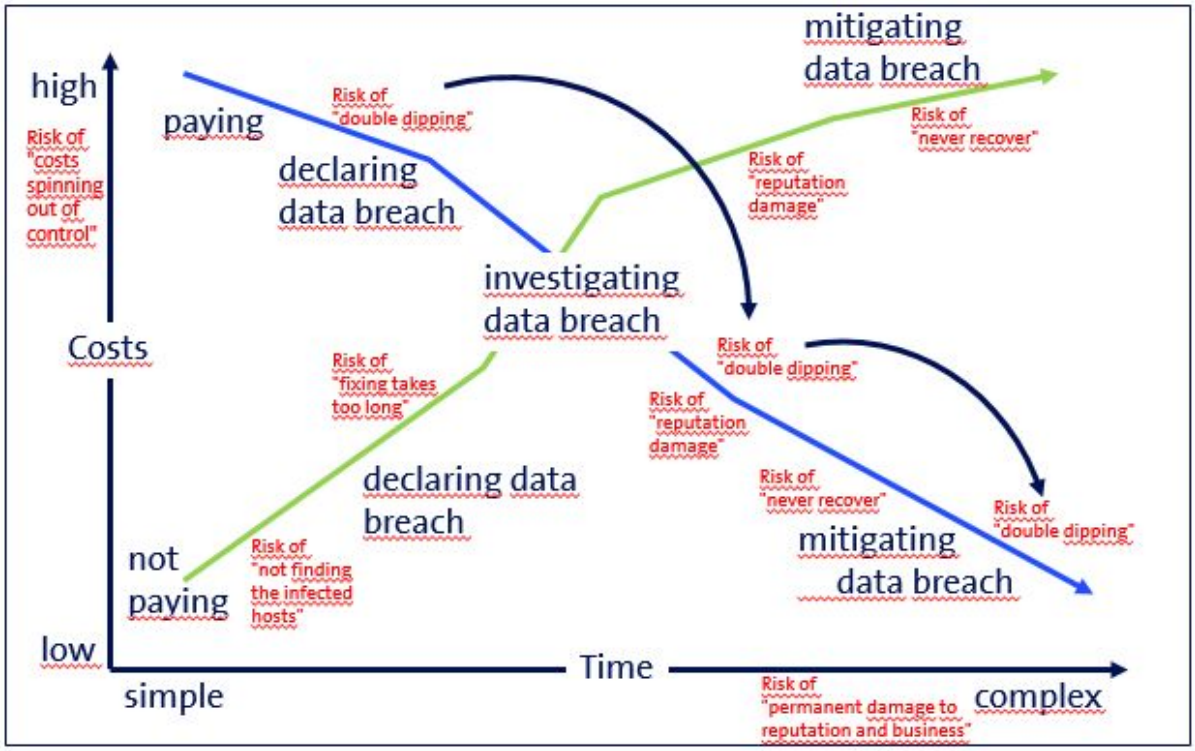
For both paths it’s the same process steps you have to walk through:

- Declaring data breach (yes it's still a data breach although nothing has been actually breached)
- Investigating data breach
- Mitigating data breach

Both paths (paying and not paying) have different risks associated with it.

Pay or don't pay?

A graphic for management to understand the process.



What you can see from the chart is: it actually doesn't matter if you pay or not the costs are very similar. The big difference is where the money comes from. If you don't have a dedicated ransomware bitcoin budget the costs will directly hit your bottom line. Unplanned and unbudgeted costs. By paying you might risk double dipping by the hackers (there are documented cases). Double dipping means after you have successfully paid the hackers they come back and ask for more money.

Since you have been a worthy payee the hackers just hit you again. In the worst case this works like a ransomware loyalty program sponsored by bitcoins. Bear in mind if you have once convinced management for paying a ransomware with bitcoins and if you then have to go back and ask for more bitcoins: oh boy I would want to do that! Without bitcoins acting as the AML hub, ransomware wouldn't be as successful as it is. Thank you digitalization for making fraud so easy.

Some ransomware protection tips:

- Time critical assessment of the situation (situation appraisal)
    a. Scope of the ransomware infection (how many and where)
    b. Risk assessment of the infection (version, detectability, expected costs (loss expectation app. 300$ per user))
    c. Partnership with service provider and specialists (i.e. outsource provider)

- Invoke your BCM and DR plan.

- If paying is an option:
    a. Decide on the point of no return (how long are going to play with backups and restore?)

   b. Who is obtaining the bitcoins and making the payment? Eventually work through a third party because of liability and compliance matters. Don't make your CFO obtain bitcoins!
   c. Get the board and management together for approving payment. Inform about the risks involved with payment.
   d. Pay and pray

4. If paying is not an option:
   a. If available inform your CERT
   b. Check your backups and secure your backups
   c. Configure firewalls, install additional segregation
   d. Update patches and antivirus
   e. Raise awareness inform staff and management
   f. Switch to whitelisting
   g. Work with your service provider
   h. Don't pay and pray

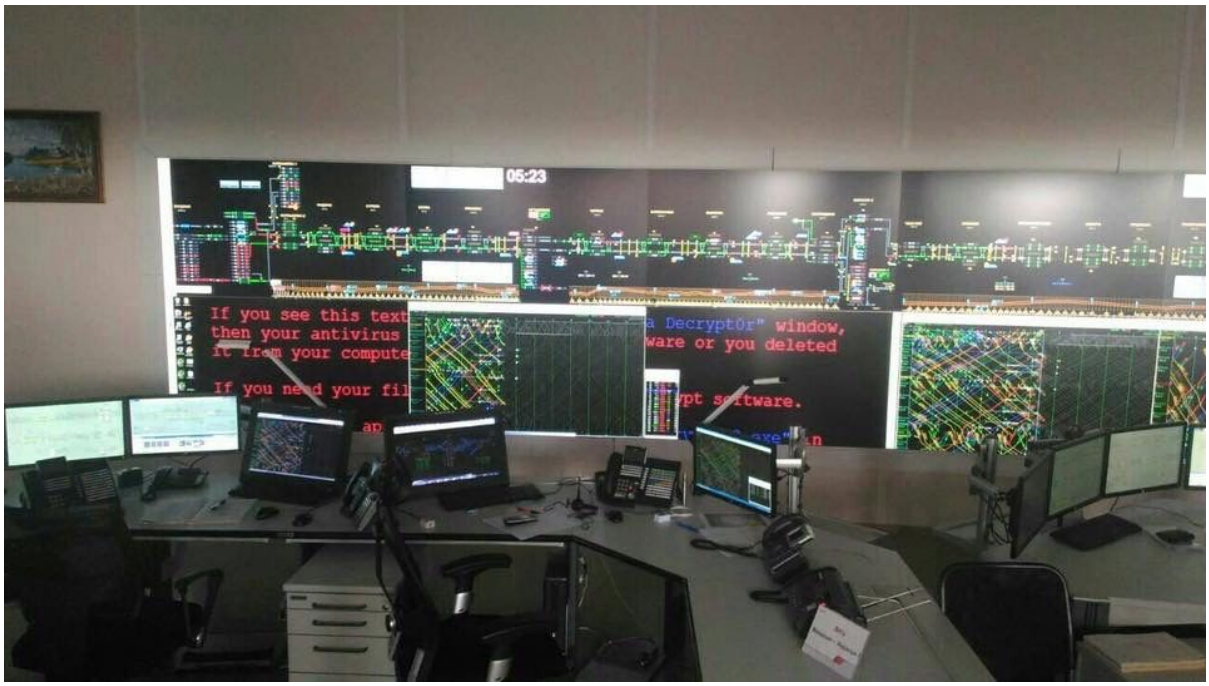
5. Join your local ransomware support group: n/a

To do before you get hit:

1. Insert ransomware scenarios into your business continuity and disaster recovery plans. Amend the BCM framework.
2. Get Bitcoins like other assets (gold, diamonds, bonds) in the company name for later use.
3. Prepare your board or senior management for quick decision making. Delegate authority accordingly. You can't put such a matter on the board meeting agenda with two weeks' preparation time.
4. Test your BCM and DR scenarios. Regulate your decision making competencies i.e. who can order the shutdown of systems and networks. What are your ramp up priorities? Which systems go online first?
   Prep like a pro. Make sure you are prepared for ransomware…soon in your neighborhood too.

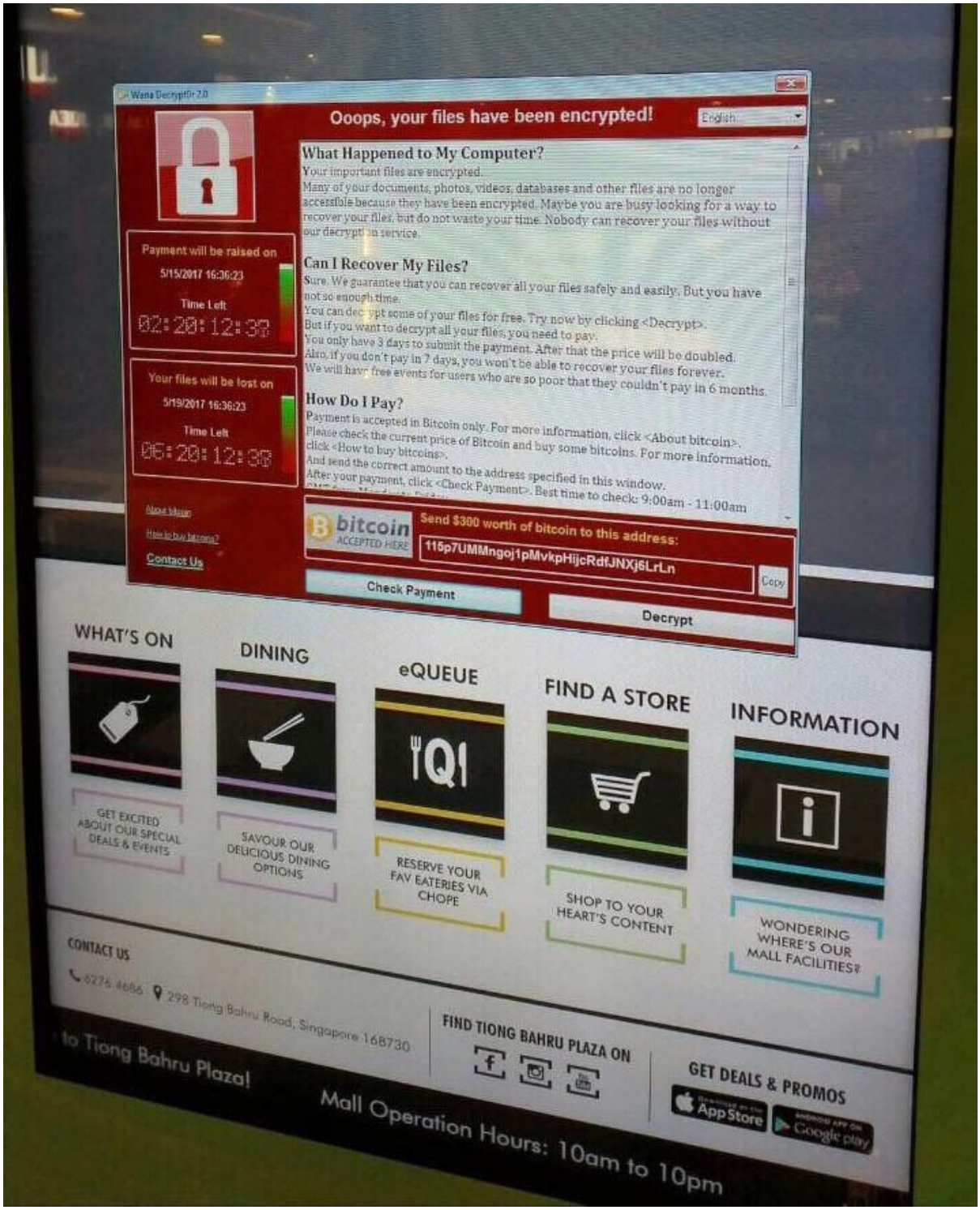
Images

Seen in a shop in Singapore

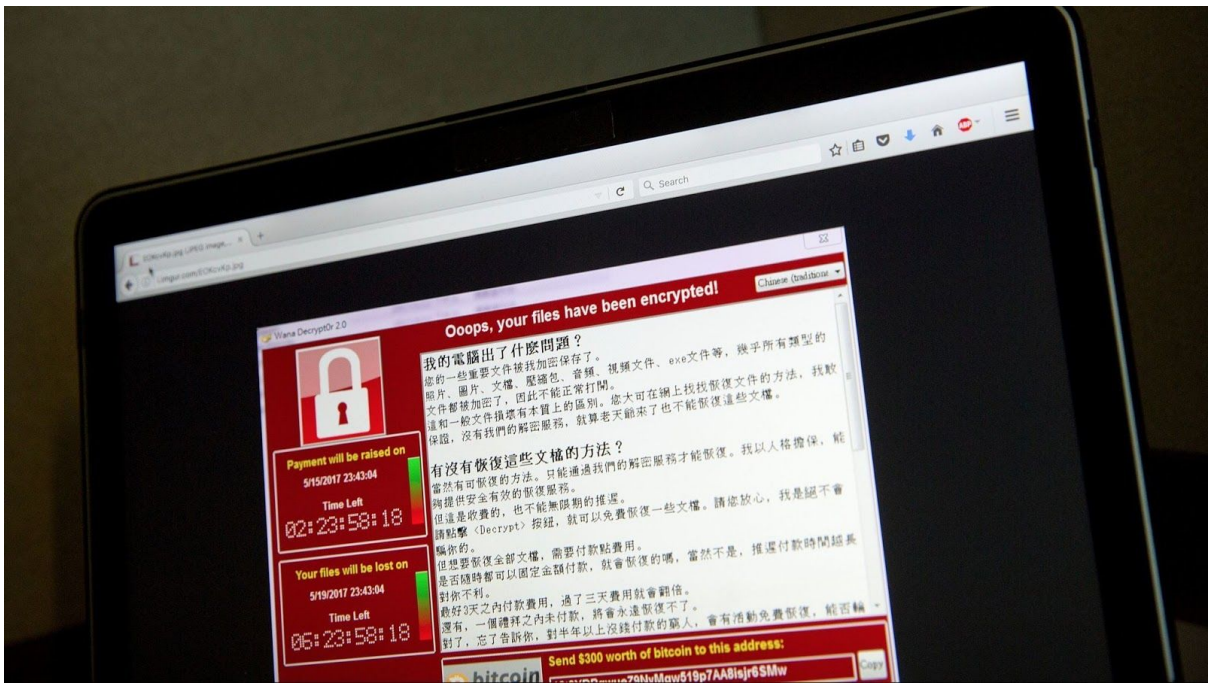


This is reported to be a russian railway control centre.


expose SMB to the internet
don't patch for months
fucking nsa
imgflip.com


Wana DecryptOr 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:36:23
Time Left
02:20:12:38
Your files will be lost on
5/19/2017 16:36:23
Time Left
06:20:12:38
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt
WHAT'S ON
GET EXCITED ABOUT OUR SPECIAL DEALS & EVENTS
DINING
SAVOUR OUR DELICIOUS DINING OPTIONS
eQUEUE
RESERVE YOUR FAV EATERIES VIA CHOPE
FIND A STORE
SHOP TO YOUR HEART'S CONTENT
INFORMATION
WONDERING WHERE'S OUR MALL FACILITIES?
CONTACT US
6276 4686
298 Tiong Bahru Road, Singapore 168730
FIND TIONG BAHRU PLAZA ON
GET DEALS & PROMOS
App Store
Google play
to Tiong Bahru Plaza!
Mall Operation Hours: 10am to 10pm

Somewhere in Thailand




加油卡自助服务终端
中国石油

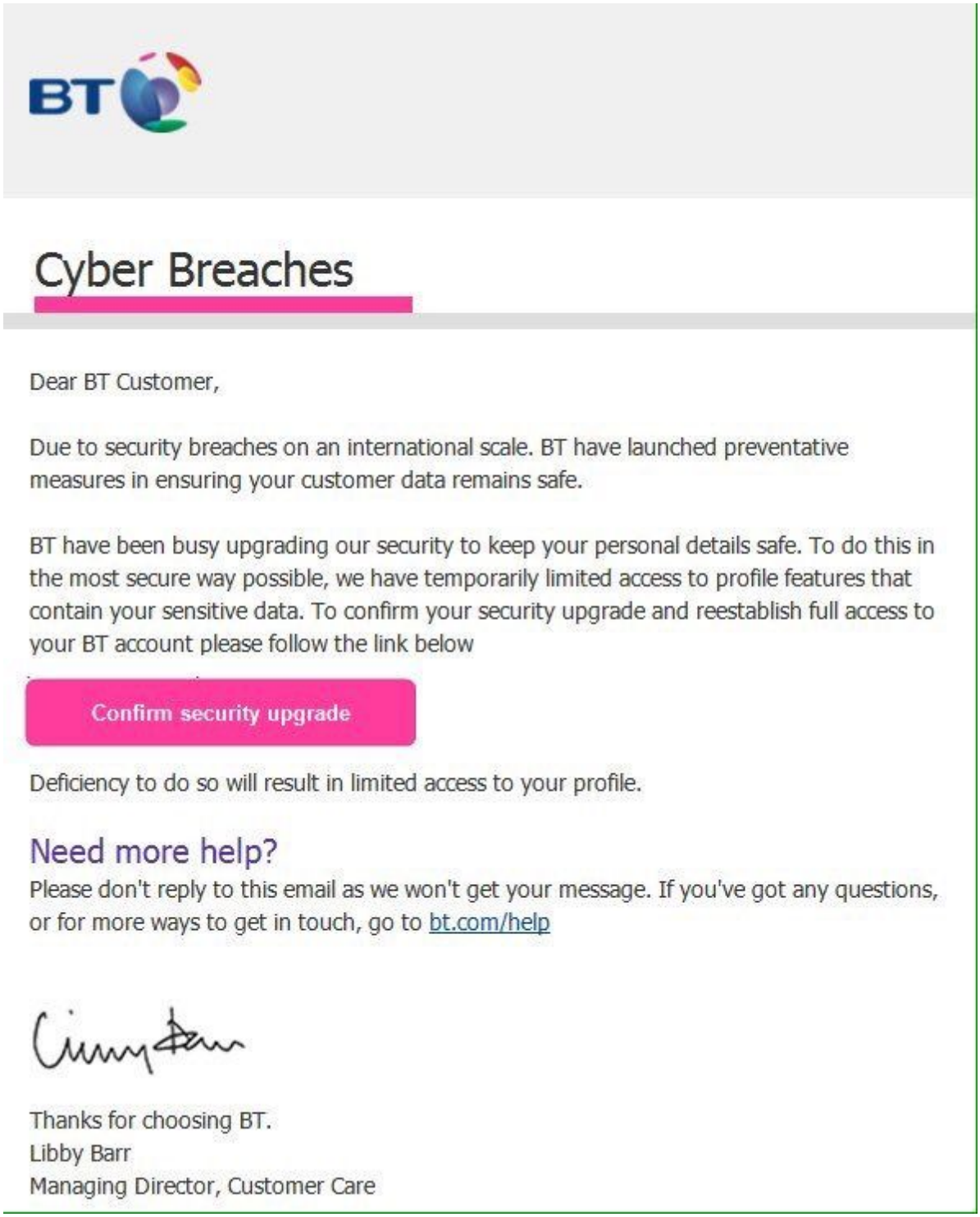
Claimed photo of a Telecoms' SoC hit by WannaCry - not sure how genuine this. Regardless, the worry breach is that someone (an employee) took a photo of a SOC and posted it on LinkedIn!

https://www.cm-alliance.com

ALERT: Fake BT email that takes advantage of the global #WannaCry ransomware attack - Fraudsters are using the global WannaCry ransomware attack as a hook to try and get people to click on the links within this clever BT branded phishing email. They claim the company has launched new measures that will protect your data. It tells you that if you click on the click you'll be safe from the attack that happened to the NHS.

Action Fraud say the email could easily catch victims out because it really does look like the real deal.

Report phishing attempts using the BT brand to phishing@bt.com



Cyber Breaches

Dear BT Customer,

Due to security breaches on an international scale. BT have launched preventative measures in ensuring your customer data remains safe.

BT have been busy upgrading our security to keep your personal details safe. To do this in the most secure way possible, we have temporarily limited access to profile features that contain your sensitive data. To confirm your security upgrade and reestablish full access to your BT account please follow the link below

Confirm security upgrade

Deficiency to do so will result in limited access to your profile.

Need more help?

Please don't reply to this email as we won't get your message. If you've got any questions, or for more ways to get in touch, go to bt.com/help

Thanks for choosing BT.
Libby Barr
Managing Director, Customer Care

https://www.cm-alliance.com

Another Phishing Attack Leveraging WannaCry:
From the LogMeIn BlogPost:

On the heels of the publicity around the WannaCry ransomware scare, we've received reports about suspicious emails that are designed to look like they are coming from LogMeIn. These e-mails have all the hallmarks of a phishing attempt. The reported emails have the same headline and text. In each case, these communications are meant to look like an alert of a computer infected with the now notorious "WannaCry" ransomware with an email subject line similar to the following: "Your computer is infected with WannaCry Ransomware." We want to make it clear that these communications did NOT come from LogMeIn and we urge recipients not to click on any such links if you receive a similar email.

Attribution link:
https://blog.logmeininc.com/phishing-alert-fake-logmein-emails-play-off-wannacry-scare/

From: LogMeIn.com Auto-Mailer [mailto:webmaster@skiundbike.de]
Sent: Wednesday, May 17, 2017 7:01 PM
To: [redacted]
Subject: Your computer is infected with WannaCry Ransomware.

LogMeIn

Computer: ID **21178268** **(status: infected)**

This emails was sent to ([redacted]).

There is a problem with your computer (ID:41942474) , Your computer is infected with WannaCry Ransomware.
If the problem persists please update the LogMeIn sofware on the affected computer. click here

Use the link bellow to connect to the infected computer.

https://secure.logmein.com/session_warning.asp?hid=21178268

Replies to this email are not monitored.
© LogMeIn Inc, 320 Summer St., Boston MA, 02210
18.05.2017

CYBER MANAGEMENT ALLIANCE

https://www.cm-alliance.com

TIPS & ADVICE

EUROPOL EC3 European Cybercrime Centre

To Prevent Ransomware from Infecting Your Electronic Devices

Ransomware is a type of malware that locks your computer and mobile devices or encrypts your electronic files, demanding a ransom payment through certain online payment methods (and by an established deadline) in order to regain control of your data.

It can be downloaded through fake application updates or by visiting compromised websites. It can also be delivered as email attachments in spam or dropped/downloaded via other malware (i.e. a Trojan).

It is a scam designed to generate huge profits for organised criminal groups. To prevent and minimise the effects of Ransomware, Europol's European Cybercrime Centre advises you to take the following measures:

DOS

UPDATE YOUR SOFTWARE REGULARLY.
Many malware infections are the result of criminals exploiting bugs in software (web browsers, operating systems, common tools, etc.). Keeping these up to date can help to keep your devices and files safe.

USE ANTI-VIRUS SOFTWARE.
Install and keep anti-virus (AV) and firewall software updated on your devices. AV can help keep your computer free of the most common malware. Always check downloaded files with AV software. You can easily find many free options on the market.

BROWSE AND DOWNLOAD SOFTWARE ONLY FROM TRUSTED WEBSITES.
Use official sources and reliable websites to keep your software patched with the latest security releases. Always use the official version of software.

REGULARLY BACK UP THE DATA STORED ON YOUR COMPUTER.
Full data backups will save you a lot of time and money when restoring your computer. Even if you are affected by Ransomware, you will still be able to access your personal files (pictures, contact lists, etc.) from another computer. There are a number of high quality data backup solutions available on the internet for free.

REPORT IT.
If you are a victim of Ransomware, report it immediately to your local police and the payment processor involved. The more information you give to the authorities, the more effectively they can disrupt the criminal infrastructure.

CONSULT YOUR ANTI-VIRUS PROVIDER ON HOW TO UNLOCK AND REMOVE THE INFECTION FROM THE DEVICE.
There are numerous official websites and blogs with instructions on how to safely remove this type of malware from your electronic devices. Always consult www.nomoreransom.org to check whether you have been infected with one of the Ransomware variants for which there are decryption tools available free of charge.

DON'TS

CLICK ON ATTACHMENTS, BANNERS AND LINKS WITHOUT KNOWING THEIR TRUE ORIGIN.
What looks like a harmless advertisement or image can actually redirect you to the website from where the malicious software is downloaded. The same can happen when opening attachments in emails received from unknown sources.

INSTALL MOBILE APPS FROM UNKNOWN PROVIDERS/SOURCES.
Always download from official and trusted resources only. In the settings of your Android device, always keep the option "Unknown sources" disabled and the "Verify Apps" option checked.

TAKE ANYTHING FOR GRANTED.
If a website warns you about obsolete software, drivers or codecs (programs that encode and decode your data) installed on your computer, do not fully trust it. It is really easy for criminals to fake company and software logos. A quick web search can tell you if your software is really out of date.

INSTALL OR RUN NON-TRUSTED OR UNKNOWN SOFTWARE.
Do not install programs or applications on your computer if you do not know where they come from. Some pieces of malware install background programs that try to steal personal data – for more information on this, see our information sheet on Identity Theft.

DO NOT PAY OUT ANY MONEY.
Paying does not guarantee that your problem will be solved and that you will be able to access your files again. In addition, you will be supporting the cybercriminals' business and the financing of their illegal activities.

Created by Europol

https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices

Contributing Authors:

- Amar Singh
- Chris Payne
- Bal Rai
- Chris Newman
- Alan Jenkins
- Ian Porteous
- Zeki Turedi
- Stuart Coulson
- Chris Rock
- Naushad (the Hacker-RedHat)
- Dario Forte
- Matthieu Suiche
- Peter Hurlimann
- Dominique Brack
- Surinder Lal
- Ed Daniel
- Chris Mavrakis
- Georgia Pulford
- John Dombrowski
- Ramandeep Bakshi
- Katalina Millan
- James Smith

Thanks to

- Peter Bassill
- Andy Robinson
- Peter Johnson
- Ed Tucker
- Jennie Williams
- Joe Shenouda
- Amanda Rousseau
- Sameh Sabry