PROFiT

Prevention of Fraud in Travel
www.profit.uk.com
INDUSTRY BRIEFING NOTE **no. 6**

PRINT OUT THIS DOCUMENT AND KEEP IT IN A SAFE PLACE FOR USE IN AN EMERGENCY

RANSOMWARE

Part 1 of 2

DISCLAIMER

PROFiT has put together this information in good faith using information from partners and internet sources in order to help organisations suffering a ransomware attack. We have not checked any links or websites that are mentioned and cannot verify the credentials of any organisation or website mentioned nor guarantee that any of the decrypt tools will work. Accordingly you should always proceed with caution.

Any materials, opinions and advice given in this publication are for information only based on data available to the authors and are correct at the time of publication. The authors do not accept liability for any mistakes, errors, or omissions that subsequently come to light. The contents of this publication may not reflect the views of some of the organisations listed.

BACKGROUND

The concept of ransomware is very simple. Once a computer is infected by ransomware malware it launches a 'packet' containing an algorithm which then silently encrypts (the process of converting information or data into a code) the user's data. Once the encryption is complete the ransomware displays a message demanding a payment – usually in Bitcoins – in order to obtain the key to decrypt the data.

Often the ransom demand comes with a deadline, and if payment is not received by that deadline, the ransom demanded may increase, the files may be locked permanently, or the files may be destroyed. Some types of ransomware also search for other computers to infect on the same network, scour contacts to then infect them, whilst others also infect their hosts with more malware, such as banking Trojans that steal users' online banking login credentials.

PROFiT

Prevention of Fraud in Travel
www.profit.uk.com

INDUSTRY BRIEFING NOTE

Ransomware are evolving all of the time and are an increasing threat to organisations and individuals alike many of whom remain ignorant of the potential dangers that lurk in a spam email or dodgy website. The best protection against ransomware is preventing it from ever reaching your system.

WHAT TO DO IF YOU BECOME THE VICTIM OF A RANSOMWARE ATTACK

1. **Contact Action Fraud**
   Use the hotline **0300 123 2040** for 24/7 assistance. ***Do not use the online reporting tool***.
2. **Isolate any infected devices from the network.**
   If it is possible to do so, switch it off and disconnect it in order to protect other devices which may still be unaffected.
3. **Identify the Ransomware which has infected your computer.**
   For this, you may use a free online service called Crypto-Sheriff https://www.nomoreransom.org/crypto-sheriff.php or ID Ransomware's https://id-ransomware.malwarehunterteam.com/ or Bit Defender's service https://labs.bitdefender.com/2017/09/btcware-decryption-tool-now-available-for-free/ which identifies the ransomware and recommends the best decrypt key.
4. **Check if a ransomware decrypt tool is available.**
   If you have some IT expertise or are an IT professional look up the type of ransomware infection to identify the type of ransomware that has been used.
5. **Use any good anti-virus software or anti-ransomware removal tool you already have to remove the ransomware.**
6. **Only if your anti-virus or anti-ransomware software does not work should you consider using a ransomware file decrypt tool.**
   However, if you have moved your encrypted files to another isolated secure system, you can directly use these tools.
7. Most of these decryption tools are easy to use. The ones by Emsisoft, for instance, require that ransomware victims drag and drop an arbitrary encrypted file and its original version onto the decryptor's window. With some utilities, however, more advanced tech skills are

PROFiT

Prevention of Fraud in Travel
www.profit.uk.com
INDUSTRY BRIEFING NOTE

necessary, such as the use of command prompt and the like. Furthermore, ransomware authors tend to tweak their code once in a while in order to defeat previously released decryptors. In any case, the list above should come in handy.

8. An additional recommendation is to look up the name of the ransomware on search engines, browse dedicated forums such as Bleeping Computer, and use the above-mentioned ID Ransomware and No More Ransom services. The best prevention tips are as follows: maintain regular data backups, do not open fishy email attachments, and use reliable security software that goes equipped with an anti-ransomware module.

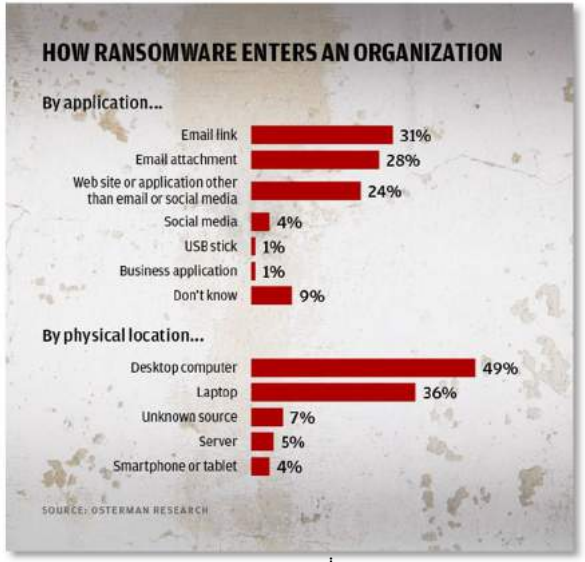
   Many of the landing pages for the decrypt keys feature more detailed descriptions of the ransomware along with technical information and descriptions of how to use the key.

HOW DO RANSOMWARE INFECTIONS OCCUR?

By far the most common source of ransomware infection is through malware in a ***spam email*** which contains a link or attachment. Organisations that do not take steps to minimise the risk of spam are effectively playing Russian roulette and hoping that all employees do not inadvertently open the door to an attack.

Other main routes of infection are through ***unlicensed, or free, software*** and also ***not keeping software updated*** so that patches designed to prevent exploitation are missed. ***Social media*** is a growing source of ransomware attack.

Very few infections are through 'brute force attacks' or other more sophisticated attacks that overcome good firewalls and anti-virus or anti-ransomware software that is kept updated.



1 SOURCE: Osterman Research[i]

PROFiT

Prevention of Fraud in Travel
www.profit.uk.com
INDUSTRY BRIEFING NOTE

HOW TO REDUCE THE RISK OF A RANSOMWARE INFECTION

Prevention Measures[ii]

Users

a) Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
b) Regularly remind all users that they should not open any spam emails or emails from unknown senders.
c) Regularly remind users that they should not download attachments or click on links in spam or suspicious emails.
d) Encourage everyone not to store important data exclusively on the PC.
e) Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed.

f) Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.

System Measures

a) Use a proactive security system that blocks cyber-attacks based on traffic analysis.
b) Use a reliable paid for anti-malware and anti-virus solution.
c) Ensure antivirus and anti-malware solutions are set to automatically update and set to conduct regular real time scans.
d) Ensure that you reduce the risk of spam emails by deploying Sender Policy Framework (**SPF**), DomainKeys Identified Mail (**DKIM**), Domain-based Message Authentication and Reporting (**DMARC**), and DNS (**Quad9**).
e) Keep the operating system, software, and firmware on digital devices updated with all of the 'patch' releases (which may be made easier through a centralized patch management system).
f) Disable macro scripts in the Microsoft Office suite to prevent infecting office files transmitted over e-mail.

g) Show file extensions and configure systems to prevent .'exe', '.vbs', and '.scr' files as these are commonly used to disguise malware.
h) Remove risky plug-ins, such as Adobe Flash, Adobe Reader, Java, and Silverlight from your browser.
i) Set all of your plug-ins to only run when you need them.
j) Adjust your browsers' security and privacy settings for increased protection.
k) Remove outdated plug-ins and add-ons from your browser.
l) Don't use the administrator account daily.
m) Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).

Business Continuity

a) Have a plan in place that allows you to continue operating if you become the victim of a ransomware attack and exercise it.
b) Back up data regularly and verify the integrity of those backups regularly.
c) Secure your backups. Make sure they aren't permanently connected to the equipment they are backing up to avoid them also becoming corrupted.
d) Keep at least 2 back-ups of your data one on an external hard drive and the other in the cloud.
e) Don't keep the cloud back-up linked to your system. Only open it when you want to back-up.

WHY ARE RANSOMWARE ATTACKS EFFECTIVE?

There are countless factors contributing to the ever-increasing popularity of ransomware among cybercriminals. Below are six of the most significant.[iii]

1. **Willingness to pay the ransoms**: Many people are willing to pay the ransom to recover their lost files, which makes ransomware a profitable business for fraudsters. The FBI recommends that you DO NOT pay the ransom.
2. **Vulnerable software**: Lack of patch management processes that identify critical systems and prioritize patches based on severity leaves software exposed to attacks.

3. **Unsecured email systems**. By not implementing SPF, DKIM, DMARC and DNS organisations are permitting spam, including malicious spam, to be delivered to users.
4. **Failure to test disaster recovery and business continuity plans**: In case of a cyber incident, it's crucial to devise a plan to continue operations during the incident response process or, at least, re-establish service as soon as possible after a data breach. Failure to regularly review and test these plans puts organizations at increased risk.
5. **Lack of backup plans**: If an organization's backup and restore strategy is not aligned with its overall disaster recovery and business continuity plans or tested regularly, it may fail unexpectedly when a cyberattack hits.
6. **Lack of security awareness training**: An educated employee is the security team's best ally. By conducting thorough and regular security training, your company will be less exposed to cyber threats. It doesn't matter how strong your security infrastructure is if your users fail to follow best practices.
7. **The underground economy**: The availability of cybercriminal tools in underground forums and marketplaces puts ransomware in the hands of nontechnical fraudsters who would otherwise lack the know-how to carry out attacks.

WHO IS BEHIND RANSOMWARE ATTACKS

Many different players are thought to be behind ransomware attacks. The most prevalent groups using ransomware are probably criminals who are after money or data to sell on or to use in criminal activity such as Janus Cybercrime Solutions or the Shadow Brokers Gang.

Some ransomware attacks are believed to have been perpetrated by Foreign Governments. It was widely reported at the time that the Wannacry attack originated in North Korea and an attack on the UK Parliamentary e-mail system was said to have originated in Iran. Whilst in 2018 UK and US Governments pointed the finger at Russia for the NotPetya attack on the Ukraine. In early 2018 the UK and US issued a joint "technical alert" warning that Russian hackers were targeting millions of devices around the world to spy, steal information, and build networks for potentially devastating future cyber-attacks.[iv]

SOME KEY DATES FOR RANSOMWARE[v]

There are two main types of ransomware: Locker ransomware, which locks the computer or device, and Crypto ransomware, which prevents access to files or data, usually through encryption.

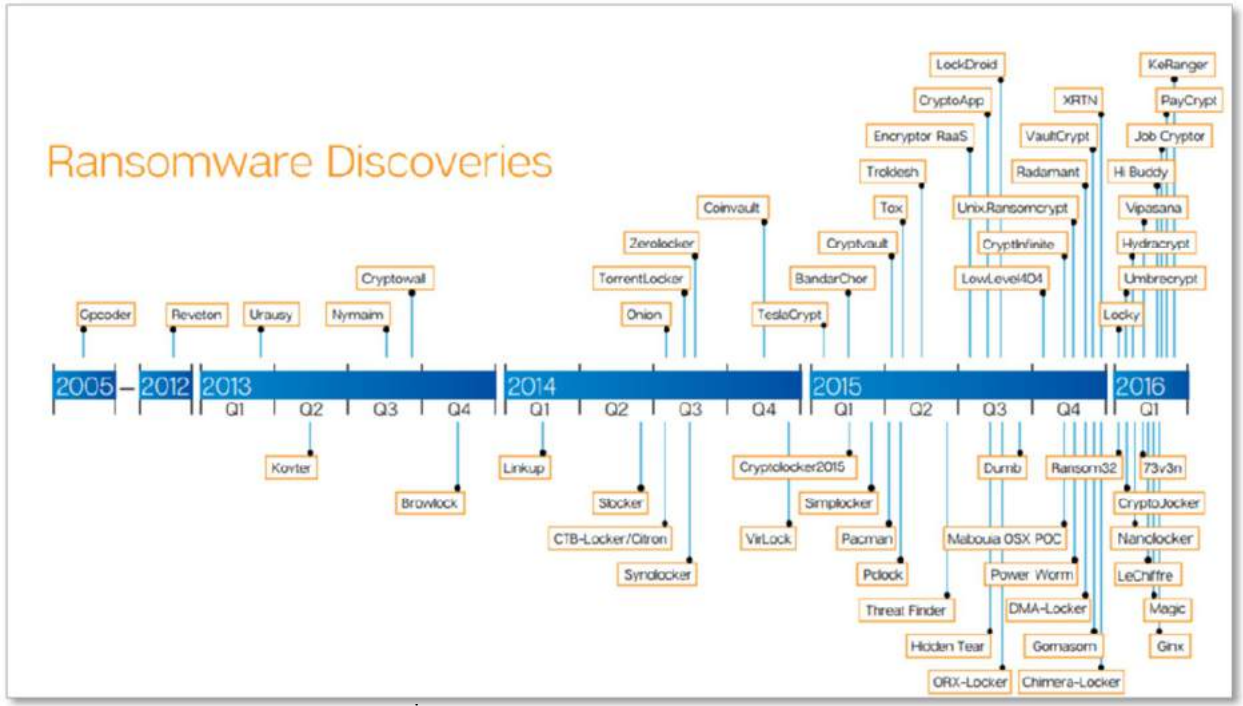
PROFiT

Prevention of Fraud in Travel
www.profit.uk.com

INDUSTRY BRIEFING NOTE

1989
The first known ransomware attack occurred was a Trojan called 'AIDS', also known as '**PC Cyborg**', which was developed by Joseph Popp. PC Cyborg locked certain files and displayed a message claiming that some software licenses had expired requiring $189 be paid to the PC Cyborg Corporation to obtain a fix.

2006
The **Archiveus Trojan** was released, the first ever ransomware virus to use RSA encryption. The Archiveus Trojan encrypted everything in the MyDocuments directory and required victims to purchase items from an online pharmacy to receive the 30-digit password. In June of that year the **GPcode**, an encryption Trojan which spread via an email attachment purporting to be a job application, used a 660-bit RSA public key.



2 Security Edge graphic from April 2016[vi]

2009
The Windows Club was launched to offer tips to Microsoft users on how to use products and before long offered advice on security and ransomware matters eventually drawing up a list of free decrypt tools.

PROFiT

Prevention of Fraud in Travel
www.profit.uk.com
INDUSTRY BRIEFING NOTE

2012
Citadel and Lyposit lead to the Reveton worm, an attempt to extort money in the form of a fraudulent criminal fine. The **Reveton** worm was the first to hold users' computers for ransom payments. Reveton locked users out of their computers unless they paid a "fine" through an online payment service.

2013
CryptoLocker came along encrypting user files and demanding a ransom to obtain the key to decrypt them. Cryptolocker used a 2048-bit RSA key pair, uploaded to a command-and-control server, and used it to encrypt files with certain file extensions, and delete the originals. It would then threaten to delete the private key if payment was not received within three days. Payments initially could be received in the form of Bitcoins or pre-paid cash vouchers.

This became the model for most subsequent types of ransomware. Cryptolocker was disabled in 2014 when the Gameover Zeus botnet upon which it relied for propagation was taken down by the U.S. Department of Justice.

Also during 2013, **CryptorBit** surfaced. Unlike CryptoLocker and CryptoDefense which only targeted specific file extensions, CryptorBit corrupts the first 212 or 1024 bytes of any data file it finds. It also seems to be able to bypass Group Policy settings put in place to defend against this type of infection.

2014
When **CryptoDefense** was released it used Tor and Bitcoin for anonymity and 2048-bit encryption. However, because it used Windows' built-in encryption APIs, the private key was stored in plain text on the infected computer.

CryptoWall also appeared and since then it has appeared in slightly different versions. One notable feature of this ransomware is that the authors offer a free single-use decryption service for one file only, apparently to prove to their victim that they do indeed hold the decryption key. CrytpoWall 4.0, released in late 2015, introduced a new "feature"; encrypting the filenames of the files it encrypts to make it harder for the victim to know what has been encrypted.

Koler.a launched in April was a police ransom Trojan infected around 200,000 Android users.

CTB-Locker dates from about mid-2014, using an affiliate program to ensure that the ransomware is propagated widely. The authors run and manage the ransomware and its command and control systems, while affiliates pay a monthly fee to access the ransomware, taking on the responsibility for finding victims through their own spam email campaigns or by running malicious web sites. The name CTB-Locker comes from Curve-Tor-Bitcoin-Locker, alluding to the Elliptic Curve encryption that the ransomware employs, the use of the anonymous Tor network for communications, and the payment demanded in Bitcoins. CTB-Locker's ransom note displays several flag icons in the top right corner so the victim can read the note in different European languages.

TorrentLocker began appearing during the same year. In addition to the standard procedure of encrypting files of multiple types and demanding a ransom in Bitcoin, this ransomware also harvests email addresses found on the machine and uses these to send further spam emails to the victim's contacts in an attempt to propagate the ransomware. TorrentLocker attempts to delete Windows volume shadow copies (which can be used to restore older, pre-encrypted versions of files) to make it less likely that users can recover their files without paying the ransom.

Bitcryptor and **CoinVault** appeared in late 2014 infecting thousands of machines before the two alleged authors were arrested in The Netherlands in 2015. During investigations, Russian security firm Kaspersky was able to get a hold of all 14,000 decryption keys that were needed to decrypt victims' files. Kaspersky subsequently created a tool that can be downloaded free to undo the damage done by both Bitcryptor and CoinVault.

2015

TeslaCrypt appeared and initially targeted and encrypted saved data and other files generated by computer games such as '*Call of Duty*' and '*World of Warcraft'*, holding them for ransom payable in Bitcoins. The first version used symmetric key encryption, and a decryption tool was made available by security researchers. Subsequent versions use more sophisticated encryption that cannot be decrypted by this tool.

In 2016, the criminals behind TeslaCrypt unexpectedly released the master decryption key for the ransomware and stopped propagating it. A free decryption tool using the master decryption key was developed and distributed by ESET, enabling victims of TeslaCrypt to recover encrypted data.

An aggressive Android ransomware strain started spreading in America. Security researchers at ESET discovered the first real example of malware that is capable of resetting the PIN of your phone to permanently lock you out of your own device. They called it **LockerPin,** and it changes the infected device's lock screen PIN code and leaves victims with a locked mobile screen, demanding a $500 ransom.

PROFiT

Prevention of Fraud in Travel
www.profit.uk.com
INDUSTRY BRIEFING NOTE

A new strain called **LowLevel04** spread using remote desktop and terminal services attacks. It encrypts data using RSA-2048 encryption and the ransom is double from what is the normal $500, demanding four Bitcoin. It is installed through a 'brute force attack' (In a **brute force attack**, automated software is used to generate a very large number of consecutive guesses until it cracks the password) on machines that have Remote Desktop or Terminal Services installed and have weak passwords.

The Ransomware-as-a-Service (RaaS) model and several strains of RaaS like **TOX**, **Fakben** and **Radamant** appeared during 2015.

2016
Locky appeared and usually infects users via malicious Microsoft Office attachments to emails. When the Office file is clicked, the file may prompt the user to enable Office macros, ostensibly to ensure that the document displays correctly, but in fact it allows the malware to run. After encrypting users' files, Locky displays a ransom note that is set as the user's desktop wallpaper. This instructs users to download the Tor Browser and visit a link specified in the note to pay the ransom.

A later version of Locky infects users via a JavaScript attachment that is automatically run by the Windows Script Host on most Windows machines when clicked, without the need for Office macros to be enabled.

A new strain of ransomware that does not encrypt files but makes the whole hard disk inaccessible, is called **Petya** and clearly Russian. As if encrypting files and holding them hostage is not enough, cybercriminals who create and spread crypto-ransomware started resorting to causing blue screen of death (BSoD) and putting their ransom notes at system start up, even before the operating system loads.

KeRanger also appeared in 2016 and is believed to be the first piece of ransomware to successfully infect Mac computers running OS X. (In 2014, a type of ransomware called FileCoder was discovered, but it was incomplete and did not function correctly.) KeRanger was injected into the installer of an open source bittorrent client called Transmission, so users who downloaded the infected installer were infected with the ransomware when they ran it.

Once infected, the ransomware waits three days and then encrypts about 300 different file types, downloading a text file containing a ransom demand of one Bitcoin and instructions on how to pay.

Cry is a sophisticated ransomware that steals and hosts personal information gathered from social networks, locates the victim on Google Maps using wireless SSID's and deletes Shadow Volume Copies among other nasty features. **Mamba**, like Petya, continues the trend of full-disk encryption ransomware but unlike Petya encrypts all data on the machine's hard drive. **Fantom** ransomware uses file and process names to set the size of the ransom demand, so if the campaign is targeting home users for example the ransom would be lower than if the target was a large enterprise.

NoMoreRansomware[vii] was set up by Kaspersky Labs and McAfee in association with Europol and the Dutch National Police the same year. The partners now provide decrypt keys for over 100 types of ransomware. **ID-Ransomware** was set up in the same year.[viii]

2017

Spora ransomware gives its victims options to just pay for file decryption, or they can pay more for immunity against future attacks. This is a sophisticated strain that collects victim data into a .KEY file, which then must be sent to the attackers who will set the ransom amount based on that data and provide decryption once paid. A new version of Spora uses an innovative way to spread itself via USB sticks.

DynA-Crypt ransomware not only encrypts data, it also attempts to steal information and even deletes files without backing them up.

WannaCry infected more than 100,000 computers in May 2017 by taking advantage of an unpatched Microsoft Windows vulnerability (MS17-010). WanaCry really caused the world to take notice of ransomware. Shadow Brokers, the hackers who leaked the NSA SMB zero-day exploit that powered WanaCry, published a manifesto threatening to release other vulnerabilities.

NotPetya attacks occurred on a large scale in France, Spain, Russia, Ukraine and other countries. It is not like normal ransomware; it's more like cyber warfare and does not come from the authors of the original Petya. It does not delete any data but simply makes it unusable by locking the files and then throwing away the key.

Newly discovered **Defray** ransomware targets healthcare, education, manufacturing and tech sectors in the US and UK, using customized spear phishing emails and demanding a hefty $5k ransom.

Another new attack by **nRansomware** demands nude pictures instead of Bitcoins in an attempt to blackmail victims multiple times. A similar attack spotted in Australia and the US claims that a virus was installed on a porn website which recorded the victim through their webcam. However, scammers are bluffing about having compromising information. These are simply fake extortion emails.

PROFiT

Prevention of Fraud in Travel
www.profit.uk.com
INDUSTRY BRIEFING NOTE

BitDefender launches its free ID tool.

A new strain called **Ordinypt** ransomware targeted victims in Germany only. Instead of encrypting users' documents, the ransomware rewrites files with random data. The **Scarab** strain was updated and spread via the Necurs botnet. In a massive 12.5 million campaign targeting .com domains, The current campaign prevents users from using third-party recovery tools, deletes Shadow Volume Copies and other default Windows recovery features.

2018
A new ransomware-as-a-service dubbed **GandCrab** showed up mid-month. This is the most prominent ransomware so far in 2018.

Zenis ransomware discovered by the MalwareHunterTeam not only encrypts your files, but also purposely deletes your backups. The latest version utilizes AES encryption to encrypt the files; unfortunately at this time there is no way to decrypt them. If you are infected with Zenis, DO NOT PAY THE RANSOM. Instead you can receive help or discuss this ransomware in Bleeping Computer's dedicated Zenis Ransomware help & support topic.

AVCrypt ransomware, discovered by BleepingComputer, tries to uninstall your existing security software (such as Anti-Virus) before it encrypts files. However, it looks like no encryption key is sent to a remote server so it's unclear whether this is true ransomware or a wiper.

Over the years ransomware has become more sophisticated and much more prolific. It is thought that today over 700 ransomware infections are being used across the internet but nobody really knows. The id-Ransomware 'malware hunter team' has identified 650 ransomware infections many of which cannot be decrypted at this time.

A full list of the identified and currently circulating ransomwares is available in Appendix A.

A table of typical ransomware variants is available in Appendix B.

Some help is available in Appendix C

For decrypt keys see the Ransomware Decryption Compendium Part 2 of 2

PROFiT

Prevention of Fraud in Travel
www.profit.uk.com
INDUSTRY BRIEFING NOTE

APPENDIX A

List of identified ransomware infections[ix]

24H Ransomware, 4rw5w, 777, 7ev3n, 7h9r, 7zipper, 8lock8, AAC, ABCLocker, ACCDFISA v2.0, AdamLocker, AES_KEY_GEN_ASSIST, AES-Matrix, AES-NI, AES256-06, Al-Namrood, Al-Namrood 2.0, Alcatraz, Alfa, Allcry, Alma Locker, Alpha, AMBA, Amnesia, Amnesia2, AnDROid, AngryDuck, Anubi, Anubis, Apocalypse, Apocalypse (New Variant), ApocalypseVM, ApolloLocker, AresCrypt, Armage, ArmaLocky, ASN1 Encoder, Atchbo, Aurora, AutoLocky, AVCrypt, AxCrypter, aZaZeL, B2DR, BadBlock, BadEncript, BadRabbit, Bam!, BananaCrypt, BandarChor, Bart, Bart v2.0, BitCrypt, BitCrypt 2.0, BitCryptor, BitKangoroo, Bitpaymer, Bitshifter, BitStak, BKRansomware, Black Feather, Black Shades, Blackout, BlackRuby, Blind, Blind 2, Blocatto, BlockFile12, Blooper, Booyah, BrainCrypt, Brazilian Ransomware, BrickR, BTCamant, BTCWare, BTCWare Aleta, BTCWare Gryphon, BTCWare Master, BTCWare PayDay, Bubble, Bucbi, Bud, BugWare, BuyUnlockCode, Cancer, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberTear, Chimera, ChinaYunLong, CHIP, ClicoCrypter, Clouded, CockBlocker, Coin Locker, CoinVault, Comrade Circle, Conficker, CorruptCrypt, Coverton, CradleCore, Creeper, Cripton, Cry128, Cry36, Cry9, Cryakl, CryFile, CryLocker, CrypMic, CrypMic, Crypren, Crypt0, Crypt0L0cker, Crypt12, Crypt38, CryptConsole, CryptConsole3, CryptFuck, CryptGh0st, CryptInfinite, CryptoDefense, CryptoDevil, CryptoFinancial, CryptoFortress, CryptoGod, CryptoHasYou, CryptoHitman, CryptoJacky, CryptoJoker, CryptoLocker3, CryptoLockerEU, CryptoLuck, CryptoMix, CryptoMix Revenge, CryptoMix Wallet, Crypton, CryptON, CryptorBit, CryptoRoger, CryptoShield, CryptoShocker, CryptoTorLocker, CryptoViki, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, CryptoWire, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, CryptXXX 4.0, CryPy, CrySiS, Crystal, CTB-Faker, CTB-Locker, Damage, DarkoderCryptor, DataKeeper, Dcrtr, DCry, DCry 2.0, Deadly, DeathNote, DEDCryptor, Defender, Defray, DeriaLock, Dharma (.cezar Family), Dharma (.dharma Family), Dharma (.onion Family), Dharma (.wallet Family), Digisom, DilmaLocker, DirtyDecrypt, DMA Locker, DMA Locker 3.0, DMA Locker 4.0, DMALocker Imposter, Domino, Done, DoNotChange, Donut, DoubleLocker, DriedSister, Dviide, DXXD, DynA-Crypt, eBayWall, ECLR Ransomware, EdgeLocker, EduCrypt, EggLocker, El Polocker, EnCrypt, EncrypTile, EncryptoJJS, Encryptor RaaS, Enigma, Enjey Crypter, EnkripsiPC, Erebus, Eternal, Everbe, Everbe 2.0, Evil, Executioner, ExecutionerPlus, Exocrypt XTC, Exotic, Extractor, Fabiansomware, Fadesoft, Fantom, FartPlz, FCPRansomware, FenixLocker, Fenrir, FindZip, FireCrypt, Flatcher3, FLKR, Flyper, FrozrLock, FRSRansomware, FS0ciety, FuckSociety, FunFact, GandCrab, GandCrab2, GandCrab4, GC47, GhostCrypt, Gibon, Globe, Globe (Broken), Globe3, GlobeImposter, GlobeImposter 2.0, Godra, GOG, GoldenEye, Gomasom, GPAA, GPCode, GPGQwerty, GX40, Hacked, HadesLocker, Halloware, HappyDayzz, hc6, hc7, HDDCryptor, Heimdall, HellsRansomware, Help50, HelpDCFile, Herbst, Hermes, Hermes 2.0, Hermes 2.1, Heropoint, Hi Buddy!, HiddenTear, HollyCrypt, HolyCrypt, HPE iLO Ransomware, Hucky, HydraCrypt, IFN643, ImSorry, Incanto, InfiniteTear, InfinityLock, InsaneCrypt, iRansom, Iron, Ishtar, Israbye, JabaCrypter, Jack.Pot, Jaff, Jager, JapanLocker, JeepersCrypt, Jigsaw, JobCrypter, JosepCrypt, JuicyLemon, JungleSec, Kaenlupuf, Karma, Karmen, Karo, Kasiski, KawaiiLocker, KCW, Kee Ransomware, KeRanger, Kerkoporta, KeyBTC, KEYHolder, KillerLocker, KimcilWare, Kirk, Kolobo, Kostya, Kozy.Jozy, Kraken, KratosCrypt, Krider, Kriptovor, KryptoLocker, L33TAF Locker, Ladon, Lalabitch, LambdaLocker, LeChiffre, LightningCrypt, Lime, LittleFinger, LLTP, LMAOxUS, Lock2017, Lock93, LockBox, LockCrypt, LockCrypt 2.0, Locked_File, Locked-In, LockedByte, LockeR, LockLock, LockMe, Lockout, Locky, LongTermMemoryLoss, Lortok, LoveServer, LowLevel04, MadBit, MafiaWare, Magic, Magniber, Maktub Locker, MalwareTech's CTF, Marlboro, MarsJoke, Matrix, MauriGo, MaxiCrypt, Maykolin, Maysomware, Meteoritan, Mikoyan, MirCop, MireWare, Mischa, MMM, MNS CryptoLocker,

Mobef, MoonCrypter, MOTD, MoWare, MRCR1, MrDec, Mystic, n1n1n1, NanoLocker, NCrypt, NegozI, Nemucod, Nemucod-7z, Nemucod-AES, NETCrypton, Netix, NewHT, Nhtnwcuf, NM4, NMoreira, NMoreira 2.0, Noblis, NotAHero, Nozelesn, NSB Ransomware, Nuke, NullByte, NxRansomware, ODCODC, OhNo!, OoPS, OopsLocker, OpenToYou, Ordinypt, OzozaLocker, PadCrypt, Paradise, PayDay, PaySafeGen, PClock, PClock (Updated), PEC 2017, Pendor, Petna, PGPSnippet, Philadelphia, Phobos, Pickles, PoisonFang, PopCornTime, Potato, PowerLocky, PowerShell Locker, PowerWare, Pr0tector, Predator, PrincessLocker, PrincessLocker 2.0, Project34, Protected Ransomware, PshCrypt, PUBG Ransomware, PyCL, PyL33T, PyLocky, qkG, QuakeWay, QwertyCrypt, R980, RAA-SEP, RackCrypt, Radamant, Radamant v2.1, Radiation, Random6, RandomLocker, Ranion, RanRan, RanRans, Rans0mLocked, RansomCuck, Ransomnix, RansomPlus, Rapid, Rapid 2.0 / 3.0, RaRansomware, RarVault, Razy, RedBoot, RedEye, REKTLocker, RemindMe, RenLocker, RensenWare, Reyptson, Roga, Rokku, RoshaLock, RotorCrypt, Roza, RSA-NI, RSA2048Pro, RSAUtil, Ruby, Russenger, Russian EDA2, SAD, SADStory, Sage 2.0, Salsa, SamSam, Sanction, Sanctions, Satan, Satana, Saturn, Scarab, Sepsis, SerbRansom, Serpent, ShellLocker, Shifr, Shigo, ShinigamiLocker, ShinoLocker, Shrug, Shujin, Shutdown57, Sifreli, Sigma, Sigrun, SilentSpring, Simple_Encoder, SintaLocker, Skull Ransomware, SkyFile, Smrss32, SnakeLocker, SNSLocker, SoFucked, Spartacus, Spectre, Spider, Spora, Sport, SQ_, Stampado, Stinger, STOP, StorageCrypter, Storm, Striked, Stroman, Stupid Ransomware, Styx, SuperB, SuperCrypt, Surprise, SynAck, SyncCrypt, SYSDOWN, SZFLocker, Team XRat, Telecrypt, TeslaCrypt 0.x, TeslaCrypt 2.x, TeslaCrypt 3.0, TeslaCrypt 4.0, TeslaWare, Thanatos, TheDarkEncryptor, tk, TowerWeb, ToxCrypt, Trojan.Encoder.6491, Troldesh / Shade, Tron, TrueCrypter, TrumpLocker, UCCU, UIWIX, Ukash, UmbreCrypt, UnblockUPC, Ungluk, Unknown Crypted, Unknown Lock, Unknown XTBL, Unlock26, Unlock92, Unlock92 2.0, Unlock92 Zipper, Useless Disk, UselessFiles, UserFilesLocker, USR0, Uyari, V8Locker, VaultCrypt, vCrypt, Velso, VenisRansomware, VenusLocker, ViACrypt, VindowsLocker, VisionCrypt, VMola, Vortex, Vurten, VxLock, Waffle, WannaCash, WannaCry, WannaCry.NET, WannaCryOnClick, WannaDie, WannaPeace, WannaSmile, WannaSpam, WhatAFuck, WhiteRose, WildFire Locker, WininiCrypt, Winnix Cryptor, WinRarer, WonderCrypter, Wooly, X Locker 5.0, XCrypt, XData, XiaoBa, XiaoBa 2.0, Xorist, Xort, XRTN, XTP Locker 5.0, XYZWare, YouAreFucked, YourRansom, Yyto, zCrypt, Zekwacrypt, Zenis, ZeroCrypt, ZeroRansom, Zilla, ZimbraCryptor, ZinoCrypt, ZipLocker, Zipper, Zyklon

APPENDIX B

Some Common Ransomware Variants[x]

TYPE	LOCKY Ransomware	DHARMA RANSOMWARE DECRYPT	DMA LOCKER Ransomware	MALWARE Data Recovery	VIRUS Encryption
EXAMPLES	**Zepto** (.zepto)	**ARENA** (.arena)	**DMA Locker 1**	**CryptoLocker**	**Crypto Virus**
	ZZZZZ (.zzzzz)	**ARROW** (.arrow)	**DMA Locker 2**	**Crypt0L0cker**	**Tesla Crypt**
	Thor (.thor)	**CESAR** (.cesar)	**DMA Locker 3**	**CryptoWall 3**	**Globe**
	Odin (.odin)	**Gryphon** (.gryphon)	**DMA Locker 4**	**CryptoWall 4**	**GlobeImposter**
	Osiris (.osiris)	**CrySIS**	**DMA Locker 5**	**CryptXXX**	**Troldesh**
	Aesir (.aesir)	**Dharma**		**Crypto Malware**	**XTBL**
	JAFF (.jaff)	**JAVA** (.java)		**Encryption Malware**	**Spora**
		BIP (.Bip)		**Satan Malware**	**Cry36**
				TorrentLocker	

Locky is a type of ransomware that uses social engineering to infect Windows PCs, and comes with powerful features to disguise itself. It can encrypt more than 160 types of files, including source code and databases.

Dharma is a type of ransomware that appends a file extension to the target data. All viruses that belong to this ransomware family differ from each other by the suffix added to documents, audio, video, images and other targeted data. Following the successful data encryption, the malware displays a specific ransom note.

DMA Locker is a type of ransomware that targets Windows OS and one known method of distribution is through Remote Desktop. Once an infection occurs and the executable is launched, DMA Locker terminates any applications used for backing up data and adds registry keys to maintain persistence. It then whitelists all system and executable files and proceeds to encrypt all other files located on local drives, mapped network shares, and even unmapped network shares. Unlike other variants, DMA Locker does not add a custom extension to encrypted files but, instead, adds an identifier into the file headers.

Malware Data Recovery is a type of ransomware that uses infected email attachments to spread across the Internet, infect Windows PCs, and lock files. Victims are then prompted to pay a ransom in order to receive a password.

Virus Encryption is a type of ransomware that prevents access to files or data, usually through **encryption**.

Crypto-ransomware (examples are ARROW and JAVA) are a type of harmful program that encrypts files stored on a computer or mobile device in order to extort money. Encryption 'scrambles' the contents of a file, so that it is unreadable. To restore it for normal use, a decryption key is needed to 'unscramble' the file. Crypto-ransomware essentially takes the files hostage, demanding a ransom in exchange for the decryption key needed to restore the files.

APPENDIX C
Some helpful people

Acronis	https://www.acronis.com/en-us/personal/free-data-protection/	A free tool said to deliver free protection from ransomware like Petya, WannaCry and Osiris, and also claims to be completely compatible with all leading anti-malware solutions.
Action Fraud	**0300 123 2040**	**City of London Police 24/7 helpline which can assist during an attack but will not recover files and data**
Bit Defender	https://labs.bitdefender.com/2017/09/btcware-decryption-tool-now-available-for-free/	The ransomware ID tool of the Bit Defender
Crypto Sheriff	https://www.nomoreransom.org/crypto-sheriff.php?lang=en	The ransomware ID tool of No More Ransom
ID Ransomware	https://id-ransomware.malwarehunterteam.com/index.php	The ransomware ID tool of the Malware Hunters Team
Malware Removal Kit	https://www.thewindowsclub.com/remove-ransomware-hitmanpro-kickstart	HitmanPro.Kickstart is a free Ransomware Removal Tool that will help you rescue a ransomed PC. It lets you start your computer from a USB flash drive to remove malware that has ransomed or locked your computer and does not allow you to access it. Hitman Pro claim this tool will find and remove viruses, trojans, rootkits, worms, spyware, fake software and keyloggers.
No More Ransom	https://www.nomoreransom.org/en/index.html	Launched by Kaspersky this site hosts a number of ransomware decrypt tools and Crypto Sheriff from various partners and is endorsed by Europol.
Ransomware Cleaner	https://www.thewindowsclub.com/kaspersky-windowsunlocker	Kaspersky WindowsUnlocker can be useful if the Ransomware totally blocks access to your computer or even restrict access to select important functions, as it can clean up a ransomware infected Registry.
Ransomware Unlock Tool	https://www.thewindowsclub.com/trend-micro-ransomware-screen-unlocker-tool	A Lock Screen ransomware may block you from entering the Normal mode only, or Normal mode as well as the Safe Mode. It is the latter which is more dangerous. But fortunately, this tool will help you both the scenarios.
Ransomware Removal & Response Kit	https://id.atlassian.com/login	Ransomware Removal & Response Kit is not a tool, but a compilation of guides and various resources relating to dealing with ransomware, that can prove to be of help. It is a 500 MB download.
TDSSKiller	https://support.kaspersky.com/5350	If you have detected any rootkits from the list on your computer, then use a special TDSSKiller tool. Win32.Trup.a,b , Rootkit.Boot.Aeon.a, Rootkit.Boot.Adrasteia.a Rootkit.Boot.Backboot.a Rootkit.Boot.Backboot.c Rootkit.Boot.Batan.a Rootkit.Boot.Bootkor.a Rootkit.Boot.Clones.a Rootkit.Boot.CPD.a,b Rootkit.Boot.Fisp.a Rootkit.Boot.Geth.a Rootkit.Boot.Goodkit.a Rootkit.Boot.Harbinger.a Rootkit.Boot.Krogan.a Rootkit.Boot.Lapka.a Rootkit.Boot.Mebusta.a Rootkit.Boot.MyBios.b Rootkit.Boot.Nimnul.a Rootkit.Boot.Nix.a Rootkit.Boot.Pihar.a,b,c Rootkit.Boot.Plite.a Rootkit.Boot.Prothean.a Rootkit.Boot.Qvod.a Rootkit.Boot.Sawlam.a Rootkit.Boot.Smitnyl.a Rootkit.Boot.SST.a,b Rootkit.Boot.SST.b Rootkit.Boot.Wistler.a Rootkit.Boot.Xpaj.a Rootkit.Boot.Yurn.a

		Rootkit.Win32.PMax.gen Rootkit.Win32.Stoned.d Rootkit.Win32.TDSS Rootkit.Win32.TDSS.mbr Rootkit.Win32.ZAccess.aml,c,e,f,g,h,i,j,k Trojan-Clicker.Win32.Wistler.a,b,c Trojan-Dropper.Boot.Niwa.a Trojan-Ransom.Boot.Mbro.d,e Trojan-Ransom.Boot.Mbro.f Trojan-Ransom.Boot.Siob.a Trojan-Spy.Win32.ZBot Virus.Win32.Cmoser.a Virus.Win32.Rloader.a Virus.Win32.TDSS.a,b,c,d,e Virus.Win32.Volus.a Virus.Win32.ZAccess.k Virus.Win32.Zhaba.a,b,c A **rootkit** is a program or a program kit that hides the presence of malware in the system.
Virus Removal Tool	http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe	If you suspect that your computer is infected with malware, then use **Kaspersky virus Removal Tool**. **Kaspersky Virus Removal Tool** is designed to scan and disinfect an infected computer from viruses and other types of malicious programs.

 1st draft released August 2018

Text References

[i] Taken from Osterman Research https://www.ostermanresearch.com

[ii] Based on the FBI https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise and Heimdal Security https://heimdalsecurity.com/blog/ransomware-decryption-tools/

[iii] Taken from Security Intelligence https://securityintelligence.com/whats-behind-the-rising-tide-of-ransomware/

[iv] Taken from The Independent https://www.independent.co.uk/news/uk/home-news/cyber-attacks-uk-launch-prepared-military-defence-intelligence-russia-iran-north-korea-a8358421.html

[v] Based on an article by Paul Rubens published in eSecurity Planet 2 March 2017. https://www.esecurityplanet.com/malware/types-of-ransomware.html

[vi] Taken from Edge-Security http://www.edge-security.com

[vii] No More Ransom https://www.nomoreransom.org/en/index.html

[viii] ID –Ransomware https://id-ransomware.malwarehunterteam.com/index.php

[ix] Taken from https://id-ransomware.malwarehunterteam.com

[x] Taken from Red Mosquito http://www.rm-ransomwarerecovery.com/?gclid=EAIaIQobChMI4rTv3djf3AIVTflRCh1hkgHVEAAYAiAAEgKulPD_BwE