



Ransomware: A New Era of Digital Terrorism

Richa Indu¹ and Anuj Sharma²

Department of Computer Science and Engineering, Institute of Technology Roorkee-247667, Uttarakhand, India

Abstract: This work entails the study of ten nasty ransomwares to reveal out the analytical similarities and differences among them, which will help in understanding the mindset of cyber crooks crawling over the dark net. It also reviews the traps used by ransomware for its distribution and side by side examining the new possibilities of its dispersal. It concludes by divulging inter-relationship between various distribution approaches adopted by ransomwares and some attentive measures to hinder the ransomware and supporting alertness as ultimate tool of defense at user's hand.

Indexing terms/Keywords: Ransomware, malwares, botnets, cryptography, web crawlers

Date of Publication: 2018-08-30

Volume: 01 Issue: 02

Journal: Computer Reviews Journal

Website: <https://purkh.com>



This work is licensed under a Creative Commons Attribution 4.0 International License.



1. Introduction

Computer and Internet is an inevitable partner of now a day's routine life and has been emerged as one of the largest platforms for e-commerce, file sharing and infotainment. Commencing by late 1960s, Internet has beheld a lot of progress as a network of WANs, MANs, LANs connected with different kinds of topologies, switches, routers and other devices, where each has different security structures, requirements and the levels of protection also varies indiscriminately. In nutshell, from a small-centralized structure, Internet has turned into a widely distributed yet decentralized architecture [1].

However, depending on the conduct of its users every discovery or investigation has positive and negative aspects. Similarly, informational subset of Internet known as WWW also has its counterpart known as Dark Net, an encrypted place of get together of cyber-criminals and crooks, which is free from surveillance and its contents, can only be accessed with the help of special protocols, softwares and browsers, namely; TOR (The Onion Router), Freenet [2]. Such a protected environment is widely utilized by criminals and crooks for their illegal tasks, sharing disastrous ideas, hijacking or hacking websites, stealing sensitive information such as banking and associated details and to exploit the vulnerable peepholes in any internet-enabled device as computer for injecting the infection, disturbing its normal working and affecting stored information to earn money [3]. Accordingly, cybercriminals work behind the scene to harm the device that concludes as the loss of valuable information for the victim user.

With advancement in technology, these cybercriminals also made progress and more expertize in concealing or sheathing their malware codes to safely dodge the hard to evade latest security solutions. Such a new generation of computer infection is referred to as ransomwares. Spreading the infection via multi-phase ransomware does not requires enough skills since it readily available on dark web in several thousand-dollar packages [4, 5]. Furthermore, there exists well-funded and organized groups behind the modelling of ransomware, operated and administered by different encrypted dark net zones. The criminals are so successful with their ransomwares because they continuously adapt new changes in technology into their ransomware and use them in more pace than others. For an instance, through the well-known phenomenon of social engineering and camouflaging these criminals are capable of befooling anyone by generating a real-seeming fake webpage or application, advertisement or e-mails.

Most often, the security keeping agencies are interested in stopping such cybercrimes but not the criminals. In addition to it, use of Dynamic DNS for ransomware distribution and crypto-currencies for ransom payment make it further difficult to trace their exact location. Cherry on the icing (top) is the willingness of some victims either individual or organizations in paying ransom rather than handling the burden of back-logging for several months will also praise the criminal minds and thence success [6]. However, the above facts does not conclude that no cybercriminal have been arrested yet. It is a matter of praise that some of the crooks are now behind the bars and such operation shut downed their whole ransomware family [4]. Even then, some other skilled hackers take advantage of that operative code by making some improvements and modifications and then reuse it to start their illegal business. The actual problem is not ransomware itself, but it is the ignorance regarding ransomware and its unusual spread [7]. The strong defensive techniques and a bit of alertness, is sufficient to tackle the ransomwares and get rid of it.

Today the extent up to which the Internet and Computers are involved in our lives, security is always on risk due to unawareness and low protection measures. That day is not so far when a car, a mobile phone, a Television set or any other internet enabled smart gadget will not start and shows DDoS (Distributed Denial of Service) error or ask for ransom because they are hacked by someone and one have to pay ransom in order to get access to them [8].

Organization of this paper consists of the journey of ransomware in sec. 2, new age of ransomwares in sec. 3, the view point in sec. 4 followed by the new saftey era in sec. 5.



2. JOURNEY OF RANSOMWARE

2.1 EVOLUTION OF MALWARE

In primordial format, designing a malware is only for excavating the vulnerabilities of a computer. In basic terms, malware is any malicious or mischievous software with a raffish of hacking, stealing and spying the sensitive information as well as disturbing the normal functionalities of entire system. Malware collectively includes viruses, Trojans, spywares, ransomwares, logic bombs, adware, rootkits and many more [9-11] as illustrated in figure 2.1. The first malware designed to reveal out insecurity on a PC is *Brain. A*, developed by Basit and Amjad of Pakistan that begins with infecting the boot sectors of a floppy diskette. Later on this infecting technique progressed towards rewriting, scrambling, or deleting File Tables on PC [10]. Gradually malwares initiated the use of mutation and polymorphism for increasing its potential against built-in security measures [5].

The first **VIRUS** exists even years before the commercialization of Internet in around late 1980s or in beginning of 1990s [1]. The first ever virus named as *Creeper* designed by Bob Thomas employed in BBN Technologies Lab was detected in 1971[11]. Creeper has no such coding that it perform any malicious task but merely replicates itself throughout ARPANET to broadcast the following message-

"I'm the Creeper, Catch me if you can!"

To do so it exploits the vulnerability of DEC PDP-10 computer, the first time-sharing system specially meant for ARPANET that runs on TENEX Operating System. Later detection revealed that Creeper was a worm not a virus and an antivirus called Reaper was developed to stop it from further telecasting/displaying the messages [11].

Beginning from replication, **Viruses** moved to infect boot sectors by rewriting them, destroying File Allocation Table (FAT) and finally infecting Master Boot Record (MBR). For further troubling windows Operating System, virus initiates by infecting Portable Eexecutable (PE) files and developing an ability of suiciding. Viruses have leveraged as well as affected a number of utilities in windows such as macros in microsoft office, e-mails, win 32 active programming interfaces, screensaver files and many more. The advanced variant of polymorphic viruses are capbale enough of evading auto-detection via anti-virus tools. In this journey hundreds of thousand viruses globally infected various systems but now a days, stealth viruses are prevalent.

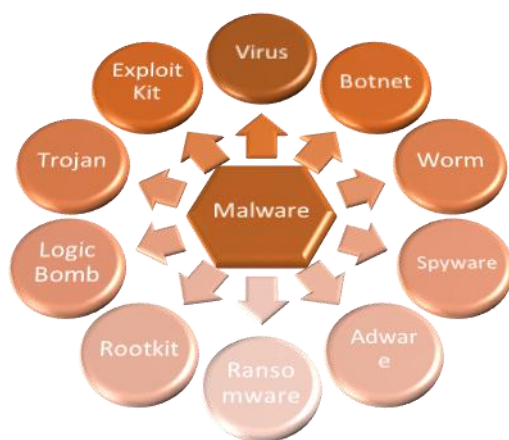




Fig 2.1 Family of Malwares

Worms has their built-in scanning algorithm that analyzes the network address to exploit any vulnerability on the device connected to IP address. Additionally, worms have a higher competence of defending against security solutions. The first worm '*Morris*' showed its existence in 1988 accidentally, which flooded the network with traffic and crashed the Internet. Some known targeted vulnerabilities exploited by worms were Microsoft SQL Server, Data Engine, Visio, Visual Studio .NET, Damage cleanup server (Trend Micro), etc.[10]. Moreover, worms are also infused with capabilities of traffic redirection, employing backdoors etc. as illustrated in figure 2.2.

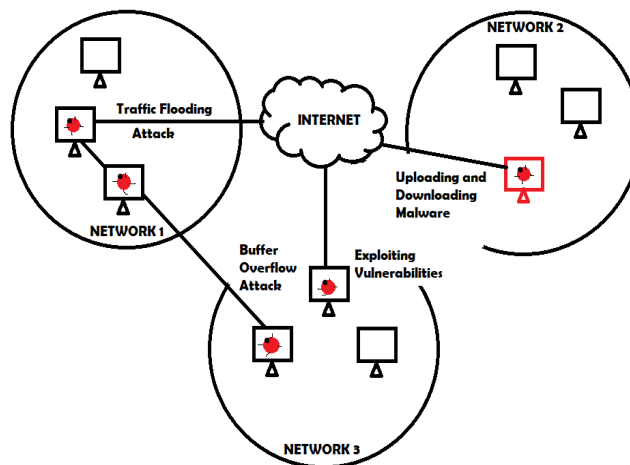


Fig 2.2 Span of Worms

Rootkits, either user mode or kernel mode, both intend to modify OS by holding system resources and keeping itself hidden to avoid detection. Rootkits have another capability of creating a botnet comprising of only victimized machines and take advantage of that botnet for further spreading other kind of infections as illustrated in figure 2.3.

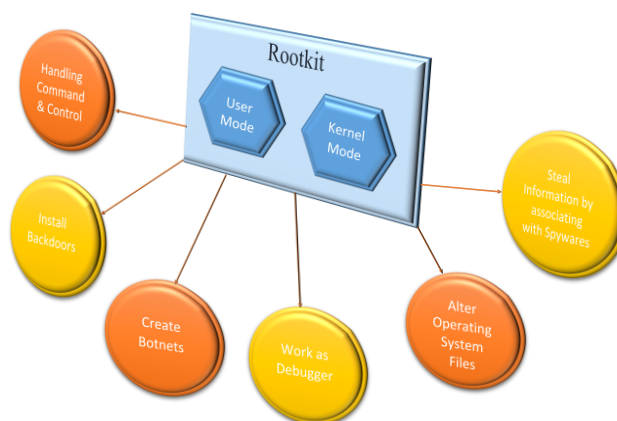


Fig 2.3 Functionalities of Rootkits

Mebroot (2008) is such rootkit that looks for security fissures of web browser to spread infections. It even appoints spying tools, which communicates with hacker to steal whatever victim types [10-11]. As an improvement, it reverts error codes or bugs to its developer to promote fixing as well as debugging.

Another well-known malware family member is **Trojan**, which describes the legitimate look like inactive program that remains dormant inside a system until a triggering event occurs to promote its disastrous



functionalities. Bundling of the most probably found spywares is not new, whether it is on cyberspace or in real world. This secret agent takes away secrets of end-user either from web-browser (Internet) or on the Personal Computer.

Adware are similar to malicious advertisements that are spoofed as legitimate ads on web pages. An adware can be injected on the website by compromising it. A click to see the tempting advertisement leads to the execution of adware, which holds a malicious payload that executes with the installation of an adware from the web or downloaded software. Usually the adware disturbs the functioning of a computer by opening a cascade of windows, which itself acts as an injector of another kind of malware [5,6].

In the modern age, the advanced malwares [10] include the deployment of such a technology, which deliberately evolves the generations of destruction, hamper smooth functioning of system and steals credible data and information. Such malwares are found active as *Stuxnet* (2010), *DoQu* and *Flame* (2012). These malwares include malevolent tools, coded in high level programming languages; namely, OOC, C++, Lua and compile with legitimate tools as Microsoft Visual Studio. It was that stint of time, when zero-day exploits and auto-response mechanism combined together with usual malwares and once the task accomplished, this malware commits suicide. These advanced malwares not only collect victims' information but also infuse with the ability of audio-video-call (skype) recording, gathering network activity and file thefts, which later on communicates to controller.

In the last month of 1989, world witnessed a great setback when the first ransomware attack invaded the digital systems via infected program stored in floppy diskette. Its programmer J. Popp, named it AIDS Trojan (also known as PC Cyborg) and placed a ransom demand of \$189 for releasing only 365 infected applications, or to disinfect the whole system the ransom amount was raised to \$378. In this way, a new member in the malware family was enrolled by merging two different anatomies: ransom and malware. Reckoned as ransomware or ransom-asking malware [4,7], **ransomware** emerged for misusing cryptographic algorithms in order to lock (encrypt) the files in the infected computer and demands huge money for unlocking (decrypting) those files.

2.2 ROLE OF OBFUSCATION TECHNIQUES IN RANSOMWARE

Obviously, malwares have a long chain of family of viruses, worms, Trojans, spywares, rootkits, adware, etc. The ransomware (a new kind of malware) being an advanced form of malware, which terrorizes its victims by misusing cryptographic techniques. Initially, the viruses in its childhood begun corrupting boot sectors and infecting computing abilities by replicating itself. Later, virus begin to develop a strong obstruction against antivirus systems by implementing sheaths, polymorphism and metamorphism.

A sheath virus evade detection by concealing the modification made during infection process of a file. For instance, if after infection the size of infected file grows from, say 841 KB to 850 KB then, this variant of virus compresses the file by 9KB to hide the possibility of detecting infection. Moving towards mutation generates the breed of polymorphic viruses that self-encrypts the body of virus multiple times during propagation and infection phase to evade sandboxing approach of detection by hiding as well as manipulating its signature via crypto-techniques. The latest approach employed by viruses is metamorphism that even possess many similarities with ransomwares. A metamorphic virus not only encrypts and compresses itself but also changes its internal codes and structure while diffusing and infecting. To achieve the ultimate goal of destruction, it even employs code obfuscation techniques like inserting garbage instructions, swapping of instructions, dead-code insertion etc. as discussed by You and Yim in their paper [12]. The increased popularity of Internet paved the way for new code obfuscation techniques in the field of malware. The Web-based malware exploited web scripts, such as java, php, asp etc. at their utmost extent for destruction and profit making. To avoid extraction of signature from web malware, its body is encrypted with key derived from URL of infected page [13].

Thus, it can be inferred that ransomware derived sheaths, polymorphic, metamorphic features as well as obfuscation from viruses. It is also probable in near future that cyber crooks will launch some tactics that



efficiently capable of hiding the behavior of malware. In the age of virtual espionage and sabotage, Modern Security Solutions has to implement advance machine-learning techniques to deal with wide range of today's challenging malware, a ransomware.

2.3 JOURNEY OF RANSOMWARE

Although till 1989, cryptography have not reached its heights. The use of mono-alphabetic symmetric encryption mechanism, hiding directories in active drive (C: drive), scrambling the file names did not initiate a substantial issue in decryption. However, the advent of a ransomware showed its footprints of a very dreadful future.

In the series of ransoms, *GPCode* (2004) A. Gazet [14] recorded its outbreak with its last variant in 2007. The devastating capabilities of *GPCode* lies in that it emerged as the senior most member of the family, which used C++ and Rivest Shamir Adleman (RSA) public-key cryptography with 660-bit key that encrypted all non-system files (user files). It is the first instance of theme-based e-mails with a pinch of spam and social engineering tactics. The theme it chose as subject for spam e-mail attachment was job application. Later the successor of *GPCode* known as *GPCode.AK* used 1024-bit key to implement RSA. Generally, the original files were deleted as soon as encryption is complete. The reason behind this task is that, the comparison of original and encrypted files paved the way towards discovering of keys, thus by deletion the malicious code eliminates any chance of reverse engineering.

In case where the PC Cyborg affected or replaced *autoexec.bat* file with a logical bomb, which counts and waits for 90 reboots before encryption. *Gpcode's* infection vector generates a thread to scan the directories and files for encryption, to locate archive and document file formats. It even modifies registry (HKEY_LOCAL_MACHINE) to remain in active state even after reboots, restarts and shutdown.

Reveton or *Police ransomware* modifies extensions in Windows/System32, displays a full window notification to the victims for not abiding the laws and asks for punishment in heavy amounts [15]. This is very first instance when hackers masquerade as legal agencies and gave birth for elaboration of locker ransomware. The primary demeanor exhibited by locker is encryption of user interface whereas the files beneath remains untouched. So, one can transfer files from infected system to another clean system with an unlocked I/O device, i.e., usually a keyboard left by ransomware so that victim can pay ransom of \$150 via Perfect Money/QIWI Visa Virtual Card Number to get the decryption key.

Year 2013 witnessed a big change in the ideology and working patterns of ransoms with the discovery of crypto-ransoms and its elaborated family. As per its name it encrypts a wide range of user's significant files with pdf, jpeg, doc, xls and many other file formats [7] using hard to guess keys coordinated by C&C server [4]. Several variants of crypto-ransoms are *Crypto-locker* and its variants, *CryptoWall* and its variants, *TelsaCrypt*, *CTB Locker*, *Crypto-blocker*, *Cerber*, *Locky*, *Powerware*, *Seftad*, *Onion-Trojan Ransom*, *Silent Crypt*, *DirCrypt* etc. [12, 13, 15].

Crypto-locker (2013) and its variant 2.0 dispersed through e-mails with an executable file that makes use of Angler Exploit kit [12-13]. The click effect leads to installation of dropper with the help of Angler kit, which manipulates internet files by escalating to administrative privileges. The hiding and scrambling of filenames is one of the key feature noticed in PC Cyborg, derived and modified by *Crypto-locker* that not only encrypts files and folders but also renames them. Using an unbreakable combination of RSA and AES cryptographic algorithm for encryption with C&C phase for key exchange as well as monitored encryption adds to its level of advancement in which C++ was replaced by C#. It first time used Tor network and bitcoins for unidentified transactions. The length of encryption key is also extended to 2048-bit, remains undetectable by anti-virus and successfully evade firewalls.

The next ransomware *Cryptowall* and its three variants; 2.0, 3.0 and 4.0 used vulnerabilities (unpatched systems, breaches or loopholes) and malware containing advertisements [12-13] along with zip, script e-mail



attachments for distribution of ransomware. On successful intrusion into *explorer.exe* and creation of copies in *AppData* directory, it provides help in manipulating registry values and ensuring ransomware reboot. To ensure the payment of ransom, the Cryptowall tries to delete volume shadow copies to remove any system restorable backup using *bcdedit* and *vssadmin* commands. For establishing C&C phase and encrypting files it uses *svchost* executable. Although any disruption during C&C or Handshaking phase can lead to failure of encryption.

Its variant *Cryptowall 2.0* have multiple propagation scheme as drive by download attack, malicious attachments and even elaborated use of TOR channel for securing handshaking phase. Further improvements visible in 2.0, is its capability to bypass emulation environment, successful conversion to 64-bit dropper from 32-bit elasticated to context switching also. Privilege snatching via exploit kits and killing active security process are quite common in *Cryptowall 3.0* as well as use of I2P to achieve ambiguity. Unlike its predecessors, *Cryptowall 4.0* re-encrypts the filenames instead of renaming them making any possibility of decryption even more difficult.

A possible reason behind using the two cryptographic algorithms for encryption in one ransomware variant may be Advanced Encryption Standard (AES) is a symmetric technique, which uses only a single key for both encryption and decryption. Thus, for eliminating any chance of obtaining the key by any means of RSA which uses two different keys for two different purposes, i.e., to open the same lock two separate keys are used. Hence, RSA is used to encrypt the AES key for further protection and the private key helpful in decryption remains on the C&C server. This private RSA key comprised of small pieces of information obtained from victim's system. It is quite common to use RSA and AES combination for encryption purpose but not a fixed venture.

Another different feature was utilized by *CTB Locker* is its ability of encrypting files without any active Internet connection by hiding C&C on TOR network. The ransomware during year 2013-15 appeared incredibly powerful that knocks down into a system through web scripts, social engineering and a wide range of exploit kits to uncover vulnerability and exploit it. These security breaches include unpatched antivirus, Operating System, Java Runtime Environment (JRE), Flash, etc. Ransomware variants were not supposed to be underestimated these days as they even employ brute force attacks to spread via terminal services, through popular games. Ransomware like *Seftad* affects MBR to disable computer from booting. Another notable point is operability of latest ransomware, which does not drive on the shoulders of a single individual but an effort of well-organized and funded team stands before it.

Some ransomwares like *Hitler* failed in terrorizing victims, which claims to encrypt files but merely removes file extension and after an hour, it crashes the PC that on rebooting deletes every single file from victimized computer. The *Fake win10 lockscreen* used decryption key visible in its code whereas *Chimera* and *Mischa* were two rival ransomwares from two different gangs. The ransomware Chimera suffered due to Mischa's creators (Janus gang) as they published some of Chimeras' decryption key online. Using this, security analyst created a decryptor for restoring all the infected files to their original state.

Hitler, Chimera, Powerware, Bart and Fakewin10 lock screen are the names of such ransomwares, which either due to their weak codes or due to rivalry, suffered setbacks [6]. So from 1989 to 2015 ransomware have travelled a long journey of setbacks, improvements, success and digitalizing the terror. Nevertheless, bundling of spywares with ransomwares for stealing sensitive information from victimized computer is also another used tactic.

Thus, ransomware a kind of advanced malware gathers its features from not only worms, viruses and rootkits but spywares and virtual destruction tools were also included within it. They exploit legitimate open source tools and techniques for evil ways of raising funds or earning money.



The long list of ransomwares their effectiveness, success and failures in past decades evidenced an all-time fear of infection among digital users giving rise to the new mode of terrorism a new challenge of ransomware to information technology.

2.4 TARGETS OF RANSOMWARES

One of the greatest responsible motivator of wide spread of ransomware is to make money or gain profit through ransom [4]. In its initial days, ransomware did not choose its target, i.e., publically distributable thus it is a matter of awareness to be one of the victims of such a high-profile member of malware family.

As history depicts, to figure out any vulnerability or flaw in the system's functionality and security malwares were designed [5, 6] so that it can be patched as soon as detected to enhance and improve system's performance and make them more obstructable against any kind of malware prevailing that time. As far today's scenario is concerned, the objective of ransomware is damage, destruction, harming victim at any state and yield as much money as possible either by hooks or crooks.

Home Users or Individuals are softest targets of ransomware due to their least fluency with technical aspects of computers. Although a home user generally does not have huge amount of data compared to corporate sector and not related to public concerns but still have extreme significance to its holder that includes reports, projects, pictures, game files, emails, etc. Extortion and pressure of ransom payment further increased by eradication of any backup files and disabling of system restore just before commencement of encryption of files by ransomwares. Reports also suggest that only 55% of home users keep a tailored backup of their files while 25 % of individual users retain either a minimum or no backup [8].

Corporate or Business Sector are most favorable target for ransomware initiators due to the presence of huge amount of confidential data regarding its consumer, sales, purchase, ledgers, journals, quotations, taxes etc. Loss of such documents can cause the whole business to shut down or bear major losses. Thus, corporate sectors opted to willfully pay ransom instead of suffering setback. The proceedings of World Congress on Engineering and Computer Sciences estimated that out of all victims, around 46% of corporations are targeted [6]. Within which, 57% were medium sized and 53% were large sized organizations that encountered threat and circumstances of ransomwares.

Now a days, hackers made a new choice to infect **Public or Government Sector machinery**. Public sector usually incorporates educational institutions, power corporations, telecommunications, law enforcement wings, hospitals, banks, transportation and all those establishments that have direct impact on public. Affecting such institutions, increases the probability of getting ransom because upkeep and maintenance of the offline digital copies of huge pile of data is difficult and denial to pay ransom will lead to setbacks in terms of minimum 3 to 6 months, i.e., another big deal of nearly a fresh start. Similarly, infecting government sector fulfil two major objectives of crooks, one to ensure the payment of ransom and if not, then steal the data regarding defense, citizens, budgets, policies etc. and sell it for money over dark net.

As of now, the ransomware attacks may be categorized into two classes; namely (1) targeted approach and (2) open (mass distributable) approach. Targeted approach is one where the ransomware especially targets similar kind of users, such as corporate sector, healthcare sector, home user or individual. Moreover, in an open attack or mass distributable attack there is no fixed target, the ransomware were launched in the wild and becoming one of the victim is all the play of vulnerability exploitation and awareness. Recently hackers have adopted a targeted approach in finding the victims to raise funds, since the reports reveal that there is a large increase in the number of attacks on corporate and public sector services such as hospitals, power stations, railways, airlines, shipping companies, etc. [8].

The primary reason behind evolving the terror of ransomware is not only willingness of victims to pay ransom but also the offerings of employing ransomware as service [4, 13]. In nutshell, the real target of ransomwares



are critical data that possess a great value to its holder and many lives are directly affected or related to it. Such kind of infection will lower the investment cost on ransomware and increases Return On Investment.

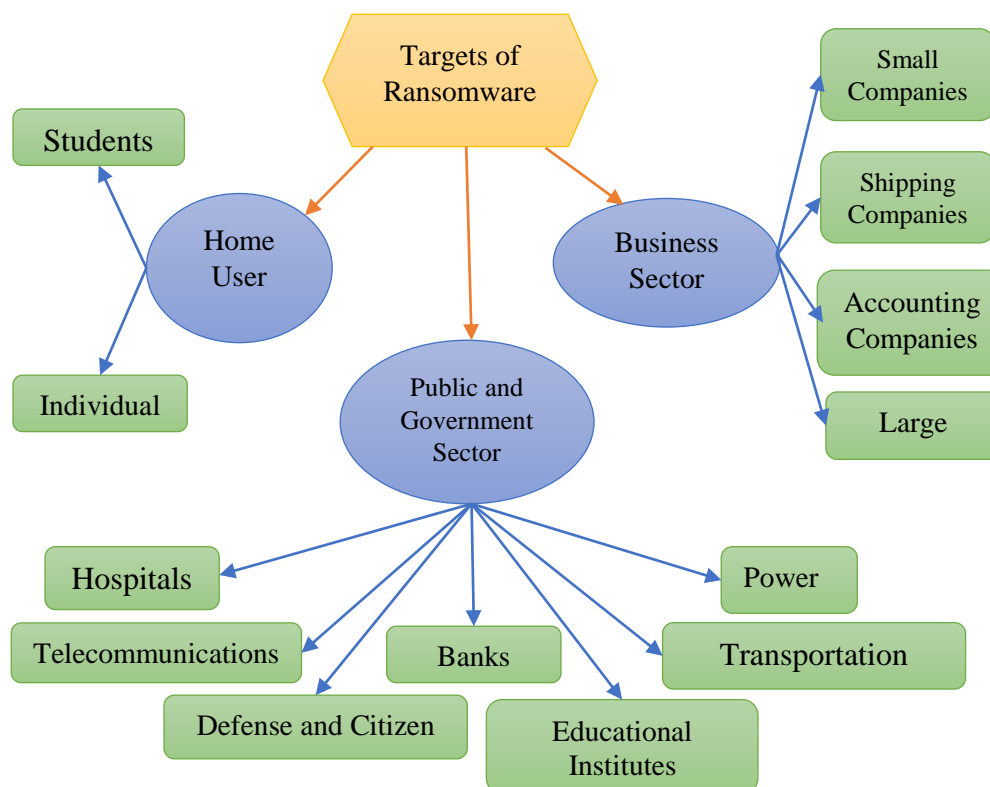


Fig 2.4 Targets of Ransomware

2.5 POPULARITY OF CRYPTOCURRENCY ON DARK NET

The term *cryptocurrency* stands for the mechanism where the identity of payer and payee remains hidden during the transaction whereas the amount and date of transaction are logged in a proper way as banks or financial institutions enforce to avoid double spending. However, there exists a claim that such structure lacks a trusted third party dealing in between two transacting parties.

One such popular cryptocurrency is *bitcoin*, proposed in 2008 by S. Nakamoto in his whitepaper [16] and take its actual form next year [17, 19]. It initiates with (\$1=□ 46.29) in 2009 to currently around (\$1200=□ 5, 59, 302.09) per bitcoin [17-22]. This rise in the value of bitcoin shows its strong grip and acceptability among customers. Although it is true that bitcoin or any other cryptocurrency like *moneypak*, *ukash*, *cashU*, *litecoin*, *dodgecoin*, *Zcash*, *monero*, *darkcoin* [17-18, 21] are fairly popular on the darknet rather than internet.

A bitcoin is made from digital signature, where transfer of coins takes place by digitally signing the hash of previous transaction and in order to avoid the chance of double spending, these transactions are publically announced as proof of transaction since the whole mechanism of bitcoins lack trusted third party. This public announcement of transaction does not compromise with privacy of clients. To achieve this, anyone who also holds bitcoin can only see that a transaction of particular amount is going on between two anonymous parties. Furthermore, for each transaction a new key pair is used. Other components involved in bitcoins are time stamp server, a network, disk space and payment verification [16]. In order to use a bitcoin, the holder



should own a virtual wallet on computer that holds all the broadcasted updates, i.e., a record of expenditure of bitcoins. Each wallet holds a public key to apply cryptographic algorithm for safeguard and anonymity of transaction. Any such wallet is operable by the person holding private key from that pair [20].

A bitcoin can be obtained in two ways: firstly, as a bitcoin miner by solving complex math puzzles, that randomly added to a transaction to maintain its anonymity and secondly, by transforming the real currency into the virtual (bit) coins [18-19, 21, 26]. Any transaction in terms of bitcoins can be carried out with the help of a public-private key pair, a digital signature, hash of previous transaction referred as *blockchain*.

This decentralized cryptocurrency, which utilizes peer-to-peer mode of communication neither ensure against loss due to disk crash holding the wallet nor any kind of fraud [16, 18-20]. Bitcoin is a widely conventional currency used as ransom to release the encrypted files also lead to new discoveries in dark market in such a way that it instigates the use of multiple signatures for verification of crypto-transaction and avoid loot.

2.6 DARK NET AND RANSOMWARE

Till now everybody is aware with the cyber term WWW (World Wide Web) which is generally understood to view or interact with Internet, but, there is yet another section it which is less known to the cyber community known as Deep Web. The Internet comprises its access publically from WWW through websites, which can be easily crawled via a large number of famous search engines such as Google, Bing, Duck Duck Go, Yacy, Startpage, Yahoo, Baidu, etc. On the other hand, the Deep Web is that part of www that does not appear in any search on Internet but do exist on the cyber space and can be accessed through special search engines like Freebase, Surfmax, IceRocket, Stumpedia, TechDeepWeb, etc. The Deep Web shares a large portion of www as compared to internet and also holds a big portion allied with digitalized crime [20].

Dark Net (a component of Deep Web) is a secret place of get together for cybercriminals such as hackers, smugglers, attackers and crooks involved in illegal or illicit trades. Dark Web, which is the informatory part of dark net that can be accessed only with the specialized web browsers, namely; Tor, Freenet, Invisible Internet Project (I2P) and other networking protocols. Dark Web is almost similar to Internet comprising of e-commerce websites, informative sites, crypto-banks, websites providing malware hosting, offering ransomware as service, etc. [2-3, 17-19].

2.7 TOOLS AND TACTICS AGAINST RANSOMWARE ATTACKS

In order to catch the ransomware, the setting up of honeypot appeared as a quite old tactics, which later on suffered from various inadequacies leading to various security challenges. Presently, ransoms are capable enough of effectively dodging such traps and efficaciously accomplish their evil tasks. Thus to defend against new age of ransoms new tools and tactics are proposed such as SDN, R-killer, Evilseed, etc. and are summarized as follows:

The SDN (Software Defined Networking) Mechanism utilizes HTTP traffic characteristics for network level detection of such file locking ransoms. In this approach, the system detects threats by studying or analyzing the HTTP traffic characteristics obtained during handshaking phase, i.e., analyzing any malicious content during communication between victimized client and C&C server. However, SDN approach assumed that protocols utilized during Handshaking phase analyzes the characteristic feature to distinguish among ransomware. To solve this purpose a three-phase process is designed consisting of learning, fine-tuning and detection phase [5]. Learning Phase includes collecting the generated network traffic and storing the extracted data in a vector resembling content size from outgoing HTTP messages and later utilizes it as input in next phase. Fine tuning phase calculates the various parameters as centroid vector, minimum and maximum Euclidean distance, limit distance etc. and adjusted them in such a way that the detection rate grows and false positive drops. Phase of detection either real time, experimental or both, examine the every incoming packet



containing HTTP traffic extract IP address or domain name to obtain C&C. If detected malicious, the data fed as input for future use [5].

R-killer (figure 2.5) is an open source modular component that can be incorporated into any e-mail client software to provide protection against those ransomwares, which use e-mails (spam or phishing) as a tool of distribution. Usually any malware analyzing tool deploy either static or dynamic analysis but R-killer is designed on the basis of deep learning mechanism of recurrent neural networking of data mining.

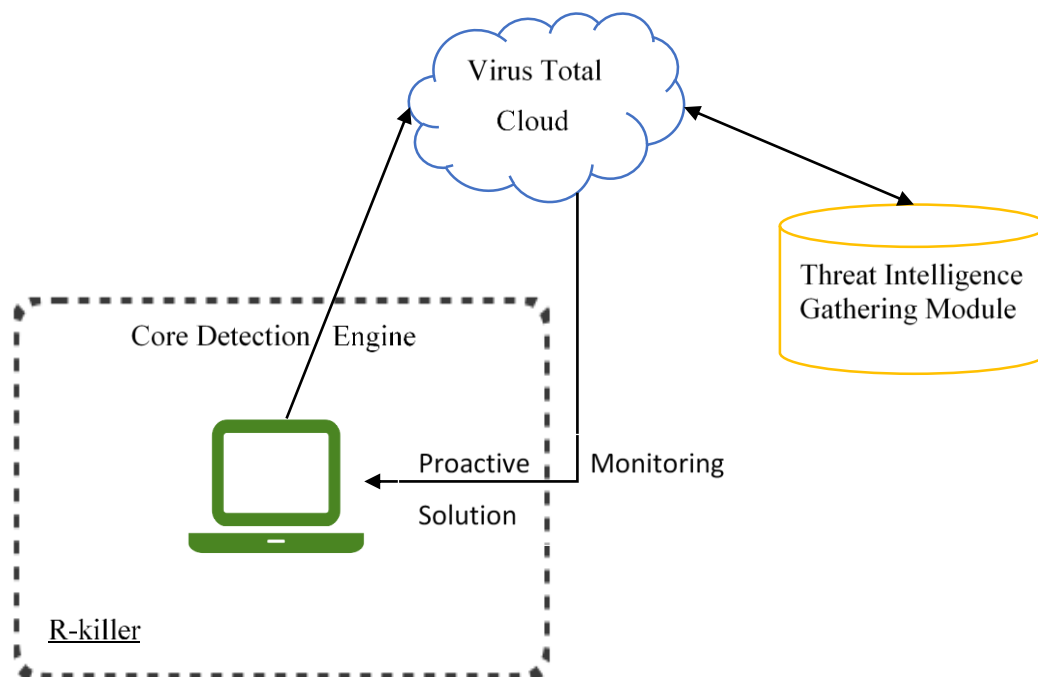


Fig 2.5 R-killer working environment

Components of R-killer include Core Detection Engine (CDE), Threat Intelligence Gathering (TIG) and Proactive Monitoring System (PMS). Analyzing URLs and attachments, blocking the defined ransomware from e-client, identify new ransom using deep learning mechanism are some tasks performed by R-killer. CDE extracts the e-mails from mailbox, attachments and web URLs embedded in the e-mail and move it to separate folder. Meanwhile continuously monitoring the activities for any suspicious content. If no doubtful content is found by engine, the e-mails are then moved back to inbox. In order to maintain the privacy and confidentiality of e-mail, only file hashes are submitted for analysis by TIG. All the threat intelligence gathered by communicating with VirusTotal cloud are returned and collected by API of R-killer to be utilized for future detection of threats. PMS monitors the currently executing process in the system for potential ransomware traces, behavior and network activities performed by attachments from non-suspicious e-mails. To identify ransomware behavior and reduce false positives, system was trained and experimented. R-killer provides an accuracy of 96% and has proven its excellence to identify new ransomware delivered through e-mails and even distinguish the variants of same family [23].

FlashGuard is a firmware level-defined approach to obstruct those ransomwares, which extorts a system by snatching the kernel or admin privileges. It is designed to support data recovery by holding the potentially encrypted data of victims and prevents them from discarding by garbage collector. It even addresses the overhead in keeping offline backups [24].



EVILSEED provides an efficient mechanism to probe for malicious pages on web and can also be deployed on search engines as pre-filters. Its ability to support the traditional web crawlers in a guided search in the neighborhood of known corpus malicious pages increases their efficiency in detection of malicious ones. The cybercriminals look for the vulnerable pages and turn them into malicious, either by manual crafting or by searching for certain keywords such as confidential, private against company names whose data they wants to hack. EVILSEED works upon two root keys, which are similarity shared between various malicious pages and availability of tools and datasets to make probing easier. The process of searching the malicious page cover three distinct stages that are collection of URL, pre-filtering and deep analysis. Crawlers perform the collection of live pointers to web pages, i.e., URL by systematic crawling, beginning from initial and move ahead to gather all possible pages by catching hyperlinks. Pre-filter even reduces the number of pages to be inspected in next phase. For performing the detailed analysis five gadgets are implemented shown in figure 2.6 [25] that employ honey clients, make use of static and dynamic tactics for examining the content of webpage either HTML or any active code, javascript or applets.

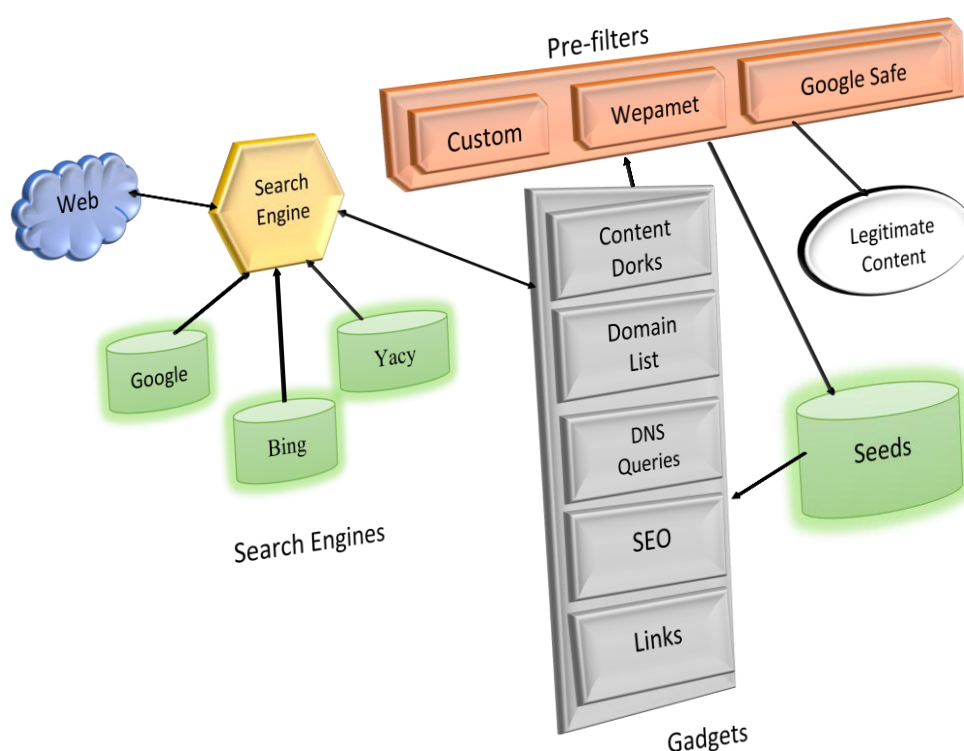


Fig 2.6 Anatomy of EVILSEED approach

Its scope of detection is confined to drive-by-download attack and social engineering tricks. It can detect only landing pages for malicious content thus any evasion attack can easily overcome EVILSEED approach establishing it as a weak safety method.

Cryptodrop actually works as an alarm that alerts user whenever a suspicious behavior is traced in comparison to normal usage traces. It is actually a complementary tool to support other security solutions running on Windows OS. The parameters utilized by Cryptodrop against ransomware includes bulk modification and deletion of data along with similarity measurements. It focuses on the point that an encrypted file has totally different contents than original file and while deleting a file ransomware targets incongruent set of files but writing a single kind ransom note. For detection purpose, it takes a snapshot of files prior to ransomware attack and monitors the behavior. If any abnormal activity as overwriting or deleting multiple files is traced, it throws an alert to suspend that initiator application. It even notifies user of any abnormal behavior and wait



for decision either to delete, quarantine, ignore, kill, lockdown or blocking it from further action [26-28]. The limitation that holds as setback for cryptodrop is inability to distinguish between user-generated or ransom generated behavior on files. Another deficiency is that its useful only after lurking of infection, i.e., while ransomware is performing encryption where only remaining files can be recovered.

Redemption is a defensive approach to make OS more powerful against ransomware threats by incorporating minor changes to record patterns of I/O requests made by several applications to access system resources. After training the model with monitored pattern, it is utilized as an offensive tool to successfully distinguish ransomware access pattern of system resources [29]. It even claims to recover the encrypted files by retracing them from transparent I/O buffer maintained at OS level.

2.8 ELUDING SECURITY WALLS

Since dark net is a favorable place of any illegal and unlawful trade. Thus is a port of such services related to crime and criminal activities. One such medium is purchasing of ransomware, exploit kits or hiring the botnets for their purpose [7, 30]. As the history suggest the botnets are used for launching spam campaigns, which even link to the page hosting exploits. Actually, exploits are not meant for destruction but for revealing flaws in the active and running applications. Meanwhile attackers mended those exploit kits to prey on Common Vulnerability Exposures (CVEs) through ransomware threats and make money.

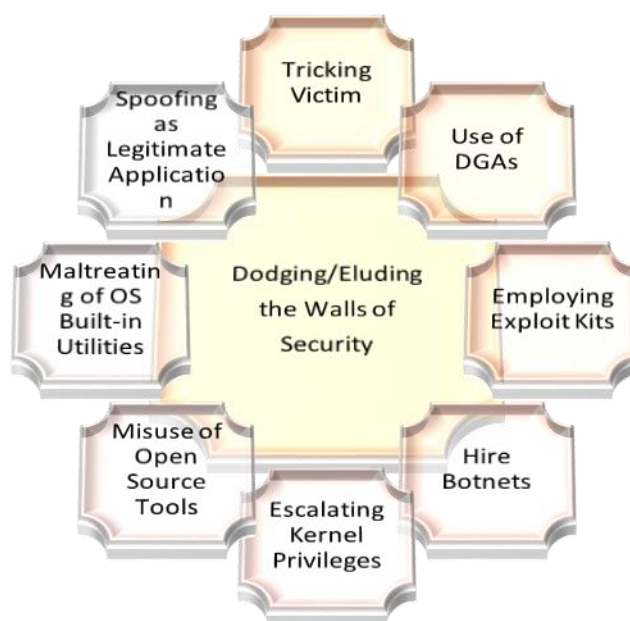


Fig 2.7 Methods adopted by ransomware to escape from security solutions

Not only this, to evade anti-malware solutions ransomware use Domain Generation Algorithms (DGAs) for a secure and tamperproof handshaking to take place between victim and assailant for exchanging victim's sensitive information (figure 2.7). Maltreating Microsoft BITS service [4] for downloading ransomware (malevolent payload) by escalating to kernel privileges are quite common tactics adopted by ransomware to bypass firewalls. Furthermore, tricking is the past strategy of attackers that is prevalent till date by spoofing as legitimate application to knock into the system with 'full permissions' granted by the victim itself by social engineering. Finally sneaking into the details of OS for modifying registry values through *regedit*, deleting volume shadow copies (backups) via *vssadmin*, ill exploit *bcdedit* for ransomware propagation and other destructive actions.



Nonetheless, some ransomwares even employ open source *diskcryptor* utility for encrypting the hard disk content. As a concluding remark, it appears that the attackers or crooks behind the ransomware are far cleverer than the general users of internet in terms of applicability of various freeware tools to earn profit.

Thus, any real time threat can only be prevented if detected and solved within time frames or restrictions. Ransomware is also a kind of real time threat with heavy malicious codes ready to intrude via networks, websites, databases and OS breaches. Even more dangerous is the ability of ransomware to evade security solutions and due to increased level of automation, it even attack critical infrastructures such as telecommunications, power and water supply etc. that if susceptible to attack can badly affect a nation's economy. Data mining can be effectively implemented in tracking self-propagation of malicious codes (*link analysis*), signature-based approach (*classification*), predict or forecast about future trends of attacks (*prediction*) [31-32]. To determine the unauthorized access web-based logs, audit trails and activity trackers (anomaly-based detection) are evaluated in the field of data mining.

2.9 ANATOMY OF ENCRYPTION ALGORITHMS

In order to avoid spill of privacy, disclosure of confidentiality and enhance a secure transmission of message between two parties the encryption tools are designed to provide safety and ensuring security goals during communication. The art of cryptography heightens with time and become stronger with each variant initiating from symmetric key cryptography to asymmetric one as well as incorporating new features of digital signatures, hashing and message digest with it. This unbreakable property of cryptographic algorithms when combined with other such algorithms attracted the attackers residing/pertaining on the dark net for exploiting and yield money from it.

Encryption is the task of transforming the actual message into the coded one with the help of keys, in such a way that it could not be determined until the key is known. During transmission to ensure privacy, the encoded message is used. For decoding the encoded message to reveal the actual content of message, the process of *decryption* is followed with the help of key.

Symmetric-Key Cryptography is also known as *Private-key cryptography* where a single variant of key is utilized for encoding the message. This key is kept secret between the two communicating parties to safeguard message confidentiality. For instance *DES*, *AES* [33-34]. *Asymmetric-Key Cryptography* is another name of *Public-key cryptography* where two different keys are used for locking and unlocking purpose. The public key is used for encoding the message is disclosed to public whereas the private key implemented for decoding purpose and kept hidden. For instance *RSA*, *Diffie-Hellman* [33-34].

The combination of two well-working algorithms AES and RSA are used for encryption in ransomwares [4, 7]. The overview and working of these algorithms is explained in [33-34] and also furnished in figure 2.10 and 2.11. Summarily, these algorithms work as follows:

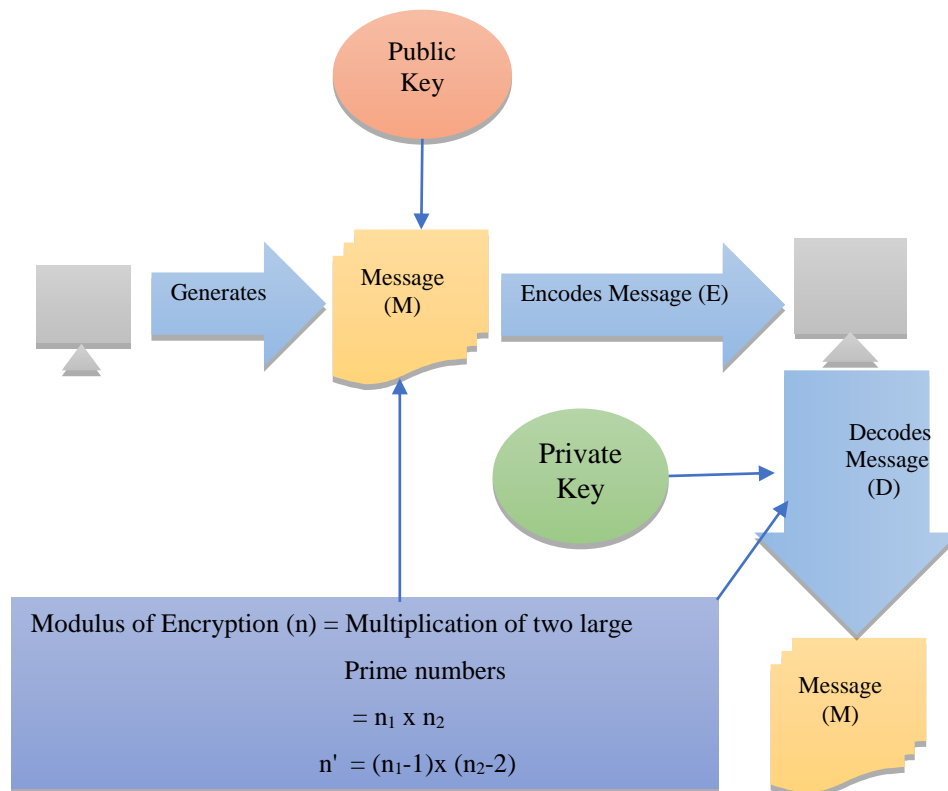


Fig 2.10 Working of RSA algorithm

The RSA algorithm chooses any two very large prime numbers used to calculate n and n' . The encoded message (E) will look like $(M) \text{ Public Key } \bmod n$ whereas decoded message (D) will appear as $(E) \text{ Private Key } \bmod n$. The Public key is chosen randomly while private key will be obtained from equation

$$(\text{Private Key}) \times (\text{Public Key}) \bmod (n') \cong 1$$

RSA algorithm is considered unsafe against brute force attack whereas AES is hardcoded against brute force, timing and such other attacks. It even support 128-bit, 192-bit and 256-bit key combinations for implementing cryptographic techniques. It works on key expansion that passes from several rounds of transformations where each round instills permutations, rotations, mix-column operations, XOR operation, expansion, etc.

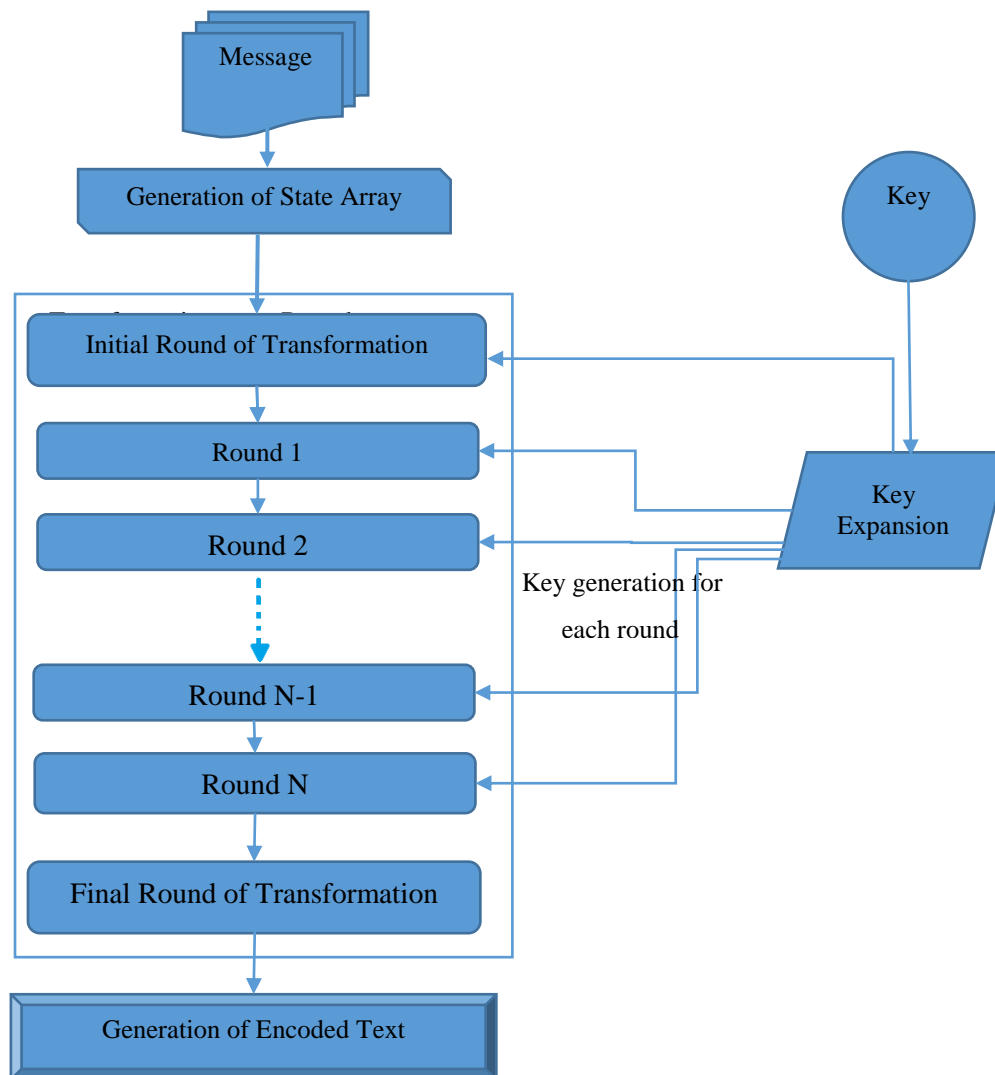


Fig 2.11 Process of Encryption in AES Algorithm

Presently, ransomware implements a nearly unbreakable combination of symmetric and asymmetric cryptographic techniques, usually AES and RSA with lengthy keys of around 2048 bit. As far as tactics and tools employed by ransoms are concerned, the increasing length of key with unbreakable combination of AES and RSA works in the favor of cyber crooks but the increasing rivalry among the botnet groups occupied for distribution of various ransomware families proves fruitful to design decryption tools.

2.10 STATE OF THE ART

The consciousness about these drawbacks prevailing in the digital systems day-to-day will definitely prove helpful in protecting the systems from those ransoms that sneaks into computers when user clicks on mischievous links in e-mails and advertisements on the web pages. Not only this, the ransomware can also silently enters the system by a drop-down payload or download by another malware. These cruxes passed the stimulus to study this topic in a little bit details.

The genesis of the existing literature suggests that most of the ransoms use spam campaigns, exploit kits to distribute themselves to other systems and command & control channels to setup a link to allow sharing of keys. Further, the latest variants of ransoms are generated by well-funded organizations, have more organized structure and are able to combine various cryptographic techniques together like AES+RSA for the purpose of encryption. The basic idea behind employing two different types of cryptographic algorithms



together for a single ransomware variant is to increase the probability of receiving payment. Such tactics offers double encryption that means encryption of files as well as of that encrypting key.

Various well known tools like Windows AppLocker, Carbon Black, Sentinel One, TripWire, etc. are based on behavior based analysis that are able to stop the detected ransomware during second phase by activity tracking when they try to access the restricted areas like volume shadow copy and disabling safe boot mode. Despite of this, the new generation of ransomware uses sheath to easily bypass security restrictions as well as firewalls. It is also nearly impossible to decrypt any file only on a hit and trial basis through reverse engineering without the actual private key.

The work embodied in this paper will mostly concentrate on working patterns on outdated; non-supported or partially updated versions of Microsoft Windows in areas like India where the usage of technology changes according to the type of institutions and their budgets. The ransomwares effectively exploit the security breaches as a path to enter the system. Therefore, it is important to patch out such vulnerabilities immediately after detection. The objectives of the work is to study the whole infrastructure of ransomware covering their each phase of lifecycle and to determine the various ways by which the users can prevent a particular ransomware to enter their systems that is from very first phase. Further, efforts are made to incorporate new findings in the field of ransomware dispersal, their interrelationship and probable layout of future attacks.

3. THE NEW AGE OF RANSOMWARES

Beginning from the least effective variants to unbeatable families of destructive programs, the ransomware has traversed a long journey till to date. As we know it has utilized the efficiency, functionalities, facilities and experience of teamwork that helped it in reaching its goal of spreading infection, generating terror and raising more and more funds. Additionally, attackers re-invoke that earned money in construction or re-construction of ransomware and progress towards selling the ransomware as facility on dark net [4-5,8].

One more property that is quite common in this era of ransomware is the reuse of previous code, i.e., inheritance. Usually the ransomwares get their name from the extension they append at the end of file after encrypting it. Those variants, which inherited the coding and reassembled the functions inspite of their different extensions, apportioned their ancestor's name, even if each has a unique feature.

Today ransomwares built on property of automation requires minimal user intervention excluding the case of knocking by drive by downloads, opening the spam or phishing e-mail attachments, visiting compromised websites and clicking malevolent ads. Use of handshaking phase, allow exchange of keys and other sensitive contents between victimized client and C&C server. Such exchange of information plays a crucial role in the success and failure of a ransomware. For patching the ransomware flaws, use of deep knowledge, practical approach and improved codes were not a new practice employed by attackers. A little bit of unawareness on Internet and trust may prove dangerous and leaves a harsh impact on their victims. Thus, people are more and more turning towards affording, enhancing and keeping security budgets and experts.

Many researchers categorize ransomware family based on their encryption ability, i.e. crypto-ransomware and locker ransomware [10, 12, 15, 41, 44]. *Crypto-ransomware* are file locking ransomwares that deletes original files and the newly encrypted version of those files are saved at that location where not only the contents of files but also their names are encrypted and an extension of that particular ransomware is appended at the end of each encrypted file. Thus, it becomes even more difficult to identify the files and estimating the amount of loss. *Locker Ransomware* are Interface locking ransomware, which leads to denial of access to the Graphical User Interface (GUI) of the device while the files beneath remains untouched. By changing the display and window properties, it allows only one window to display on the screen. It even changes the wallpaper to black or red color containing the logo of the ransomware and a message (in notepad format) that includes the procedure to make payment in terms of bitcoins to get the decryption key (figure 3.1). For some ransomware variants, it even includes demo decryption key that encrypt a single file to build victim's trust on the extortionist that if payment is made then probably most or all of the files can be restored.



Fig 3.1 Crypto v/s Locker ransomware

The new era of ransomware captivates the whole system that not only locks files but user interface as well, firstly it encrypts the files and then locks the interface following the same procedure as mentioned above. Thus, making the whole system a hostage and of no use.

3.1 THE LIFE CYCLE OF RANSOMWARES

The lifecycle varies from ransomware to ransomware, from means of distribution to exploits kits used, server accessed, keys and even the demand of ransom. The lifecycle of a ransomware admits different six phases referred to as kill chain [35-36]. However, the general trend of kill chain enforces to summarize that these stages of a ransomware can be categorized in five phases to reach its destination [4]. These phases are:

1. Knocking phase
2. Execution of infection phase
3. Handshaking phase
4. Demolition phase
5. Stipulation and demand

3.1.1 KNOCKING PHASE

This phase can also be renamed as dispersal or distribution phase, which is associated with the spread of ransomware. This phase involves tracing of various ways through which a ransomware tries to enter a user's computer (figure 3.2).

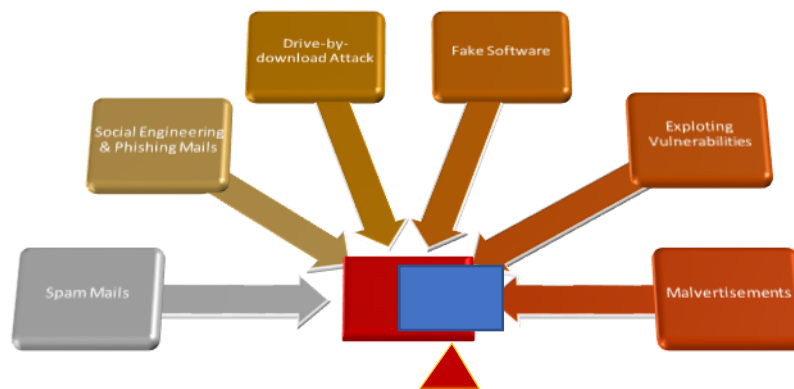


Fig 3.2 Various methods used by ransomware to enter a system

Knocking phase is the initial phase of any ransomware during which it tries to obtain anyhow the authorized permission to create space for itself into the target system, which is currently under threat. Its commonly used entry points can be described as:

(i) **Spam Attack:** Any e-mail user is aware of junk or spam folder where e-mails from untrusted source reside. Most of the ransomwares today uses spoofed electronic mails as their primary distribution method send via botnets [8, 32, 35-39]. These spams contain either a link to infected website or an attachment, which is itself a part of infection triggering code also called payload [4, 8]. One click and the infection purposefully lurks inside newly victimized PC even without user's knowledge. As an attachment, these include macro-enabled Microsoft office documents, visual basic scripts, java scripts and zip-protected files that very simply avoid from being scanned by anti-spam kits of security solutions. These may be referred to as easiest entry doors. In order to trick user the cyber crooks use current affairs, job resumes, order invoices, mail delivery notification, etc. as enticements to end-user for opening the embedded one [4, 8, 32, 35-39]. When links are concerned, they either redirect traffic to malicious websites including mischievous links or a hijacked website that will land to the page hosting the exploit kit.

(ii) **Exploiting Loopholes (Vulnerabilities):** Using the tools available on dark net or hiring the criminal services over there, assaulters deploy an exploit kit (*Rig, Neutrino, Necrus, Dridex, Angler, Nuclear, Magnitude*) [39] on a legitimate website in such a way that unnoticed ransomware creeps throughout the Internet in search of security loopholes to exploit it and enters a computer. These loopholes can be an outdated or partially updated OS, any software (*JRE, Adobe Flash, Reader, etc.*), a web browser, JBoss server etc. [8, 36-39] that are very easy to find in countries like India. For redirecting the user to exploit kit's page, an iframe is injected [10, 40]. Once an appropriate vulnerability is identified, it is utilized to make a space for ransomware in the system by dropping its infectious executable (installer) into the computer for initiating the infection. Any outdated or partially updated OS does not pose any problem until the PC is disconnected from any kind of public network but can lead to havoc if that computer is a part of an unsafe network.

(iii) **Drive-by-Download attack:** Whenever a ransomware enters a system by bluffing the user to download the latest version of a particular software such as Adobe Flash (figure 3.3), web browser (figure 3.4), Oracle JRE (figure 3.5), etc. from previously hacked website. This kind of entrance to any system is referred to as Drive-by-Download Attack [4, 35-36, 39, 41]. Furthermore, it is a subset of spam attack for providing a passage to ransomwares by means of download.

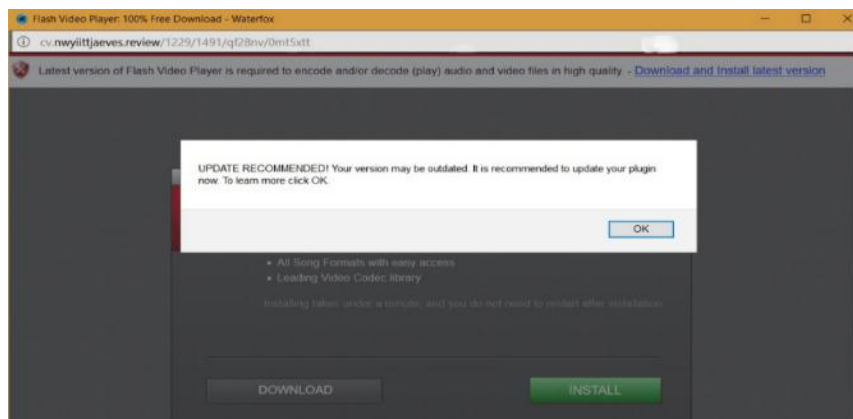


Fig 3.3 Drive-by-download attack (using fake Flash update).

Under this circumstance, the malicious executable fabricate itself as the actual software to bluff the end-user regarding its legitimacy. As the user permits to install the software, he/she unintentionally give permission to that malicious module to run on the system. Most of such come as an additional software package that resemble to be so true that even an experienced and unaware user could get trapped.

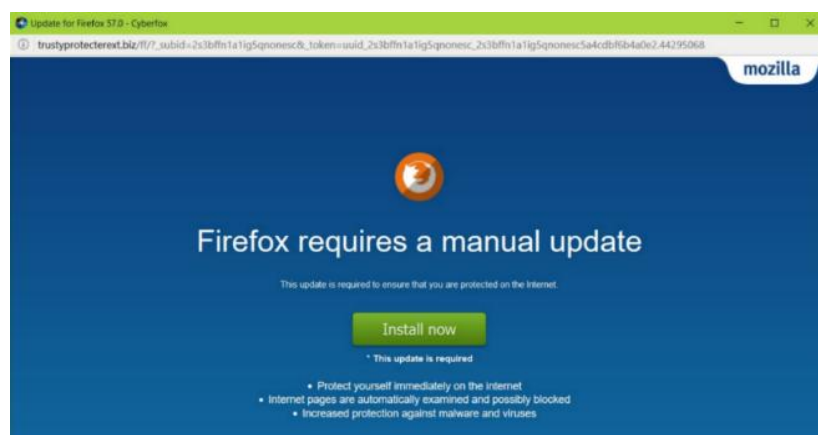


Fig 3.4 Drive-by-download attack (using web-browser update)

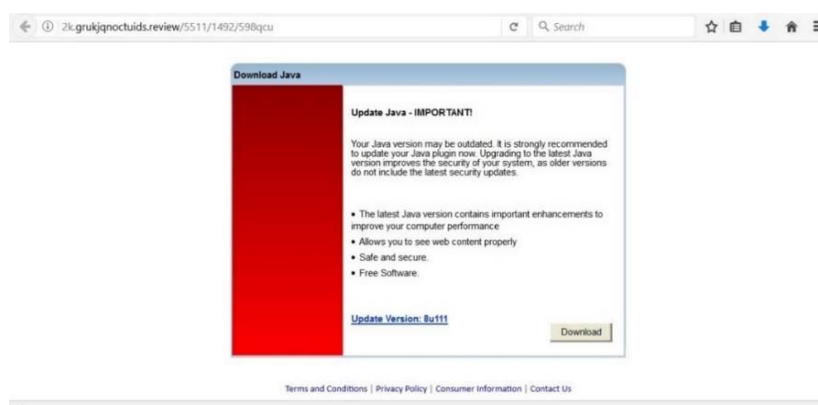


Fig 3.5 Drive-by-download attack (using JRE update)



(iv) **Malvertisements:** The word *Malvertisement* stands for malware containing advertisement or merely those advertisements that possibly cause any malicious activity to be performed on the system in which they are clicked. For distribution of ransomware, the malvertisements are made to display on the website that user visits, which contains an injected script that redirects that user to the malicious page hosting the exploit kits or initiates a downloader [4, 8, 36, 38]. In some cases, for spreading the ransomware via malvertisements bogus software bundled with adware or infectious executable is also used. Hereafter, user unintentionally provides permission to additional payload along with desired software and puts PC on risk. Another one tactic that attackers repeatedly perform with this kind of knockers is to remove the malicious codes of ads after a short interval, thus there remains no traces of past hacking or infection on that ad.

(v) **Phishing Attacks:** Phishing mails are far more different from spam mails and are finest examples of masquerading oneself as a legitimate sender [42]. For instance, those e-mails that asks for credential information such as username, passwords, Aadhaar/Credit/Debit card and bank details of recipient can be considered as phishing mails (figure 3.6 (a and b)). The information once obtained by such kind of communication is used by hackers for extorting the victim to pay a ransom, otherwise their data will be disclosed publically [4, 36]. Moreover, such kind of phishing attacks are also common in India via phone calls by fabricating as bank professionals.



Fig 3.6 (a) Phishing e-mails (Aadhaar Card)

Not only for raising the funds illicitly but the data obtained by phishing is also leveraged in probing the targets for next malware attacks. The success of any phishing attack heavily rely on user and the representation of e-mail.



Fig 3.6 (b) Phishing E-mail (Credit Card)

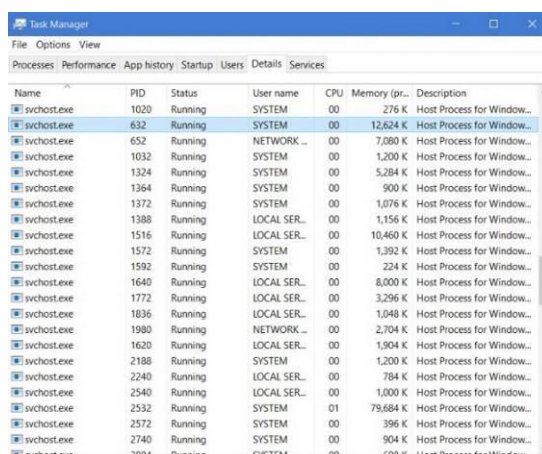


(vi) **Socialization and Tools:** The current trends represent that the new variants of ransomware successfully infused worm-like self-propagating behavior in ransomwares that enable them to move freely throughout the network of computers within an organization only by using legitimate tools after gaining authorized access to system resources. Another mechanism of dispersal employed by ransomware is use of social engineering tactics [8, 32, 38], which refers to the quantum of content of an e-mail capable to tempt the user to click the links and provide permissions to access system resources. In fact, it is the measure of the extent to which the end-user can be tricked based on human psychology and make security violations themselves. Generally, most of the dispersal methods more or less depend on social engineering for their success.

3.1.2 EXECUTION OF INFECTION PHASE

Once the user is successfully trapped during the knocking phase, it is time when previously rooted or established malicious dropper manages to download such an executable on the host system that will be able to install ransomware itself on that device by taking administrative privileges. This installation phase of a ransomware can be devised in two stages [4, 8, 35, 39, 43].

During first stage, malicious payload downloads that executable in **AppData/local/temp** folder and replicate to multiple folders. Once the ransomware successfully installs on the system, the dropper cleanly removes itself from the system leaving behind no traces. As soon as ransomware lands on the system, it begins to modify keys in Windows Registry, checking and resetting the user privileges by making changes to User Access Control (UAC) so that malicious payload obtained during knocking phase can run undetectably whenever the system boots or reboots. Moreover, it tries to kill any active security solution to establish an untraceable link with its master in next phase and gather all the required information to design the encryption key without any interruption by anti-malware tool. Henceforth, its components can silently and unnoticed work beneath antivirus products and using system's resources as a legitimate program for its installation. This phase also utilize WMIC (Windows Management Instrumentation Command Line) tools for gradually spreading from the newly infected device to other linked devices by extending WMI utility for providing non-interacting as well as interacting mode of retrieving information about the status of the system and its resources, such as computer name, model, and version of OS currently running and other setting and managing other kind of system configurations.



Name	PID	Status	User name	CPU	Memory (private)	Description
svchost.exe	1020	Running	SYSTEM	00	276 K	Host Process for Windows...
svchost.exe	632	Running	SYSTEM	00	12,624 K	Host Process for Windows...
svchost.exe	652	Running	NETWORK...	00	7,080 K	Host Process for Windows...
svchost.exe	1032	Running	SYSTEM	00	1,200 K	Host Process for Windows...
svchost.exe	1324	Running	SYSTEM	00	5,284 K	Host Process for Windows...
svchost.exe	1364	Running	SYSTEM	00	900 K	Host Process for Windows...
svchost.exe	1372	Running	SYSTEM	00	1,076 K	Host Process for Windows...
svchost.exe	1388	Running	LOCAL SER...	00	1,156 K	Host Process for Windows...
svchost.exe	1516	Running	LOCAL SER...	00	10,460 K	Host Process for Windows...
svchost.exe	1572	Running	SYSTEM	00	1,392 K	Host Process for Windows...
svchost.exe	1592	Running	SYSTEM	00	224 K	Host Process for Windows...
svchost.exe	1640	Running	LOCAL SER...	00	8,000 K	Host Process for Windows...
svchost.exe	1772	Running	LOCAL SER...	00	3,296 K	Host Process for Windows...
svchost.exe	1836	Running	LOCAL SER...	00	1,048 K	Host Process for Windows...
svchost.exe	1980	Running	NETWORK...	00	2,704 K	Host Process for Windows...
svchost.exe	1620	Running	LOCAL SER...	00	1,904 K	Host Process for Windows...
svchost.exe	2188	Running	SYSTEM	00	1,200 K	Host Process for Windows...
svchost.exe	2240	Running	LOCAL SER...	00	784 K	Host Process for Windows...
svchost.exe	2540	Running	LOCAL SER...	00	1,000 K	Host Process for Windows...
svchost.exe	2532	Running	SYSTEM	01	79,684 K	Host Process for Windows...
svchost.exe	2572	Running	SYSTEM	00	396 K	Host Process for Windows...
svchost.exe	2740	Running	SYSTEM	00	904 K	Host Process for Windows...
svchost.exe	3804	Running	SYSTEM	00	4,036 K	Host Process for Windows...

Fig 3.7 svchost executable running on the system

During second stage, that installed piece of ransomware code tries to establish itself in the process like *svchost.exe* running under *C:\Windows\System32* and illustrated in figure 3.7 so that it can delete the volume shadow copies on the system by initiating a series of light weight threads as well as disabling safe boot by using *bcdedit* [4, 44] thus curbing system restore. Whenever *svchost* is executing outside *system32* directory, it is malware under execution. This whole process of downloading the ransomware through malicious dropper then executing and establishing it successfully within system takes only few seconds.



3.1.3 HANDSHAKING PHASE:

As soon as a ransomware is successfully distributed and installed on a computer, the next action is to contact its master, i.e., extortionist. The requirements to setup a communication link between extortionist and victim is fulfilled in previous phase in the similar manner as HTTP Client/Server Model. During communication, this established link between the two can also be regarded as a master-slave connection where victim's device behaves as slave and extortionist's device as its master giving order to its slave to provide all the gathered information regarding victimized device. To access its master server the dropper either generates a list of domains (DGAs) or checks the embedded link within the payload [4]. This process is illustrated in figure 3.8.

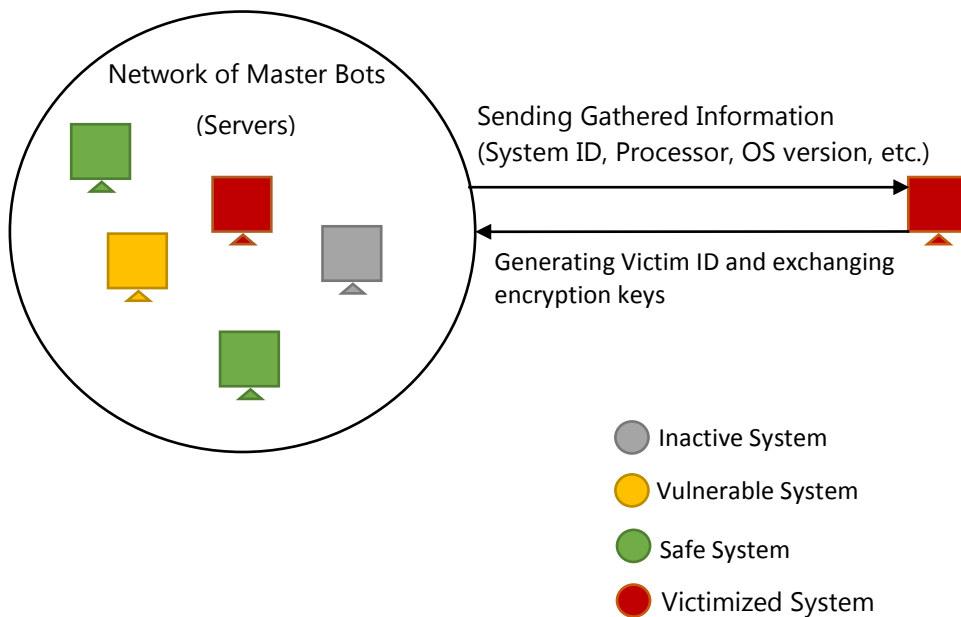


Fig 3.8 C&C channel for exchanging keys and gathered information

The initiation of this communication begins from client side (victim) where the installed ransomware scans the system and sent only those information to its master which is required enough to identify the potential of the victim. This information includes Computer name, IP Address, Domain name, Operating System (with versions of installed updates), default Web Browser, loaded antivirus product, etc. which is used to identify victim's system by generated ID [36, 45].

Since the modern ransomware uses a combination of AES and RSA cryptographic algorithms, the AES key is produced within the victim's system to encrypt files and RSA key pair is generated on the assaulter's server. The public key along with victim's ID is sent to victimized system for encrypting the AES key and private one, which is the decryption key, is kept safe on the server. In some ransomware variants, the RSA-public key, i.e., encryption key for AES-key is embedded within the payload, hence no requirement for exchanging the keys. For such variants, handshaking phase occurs after encryption of files for transferring stolen information gathered by bundled spyware with them.

3.1.4 DEMOLITION PHASE:

The initiation of demolition occurs with probing the victim's system for identifying file extensions appropriate for encryption and ends on encrypting those detected files or even the whole computer depending on the nature of ransomware. The encryption suitable formats as provided by earlier researches are pdf, doc, jpeg, png, ...[7].



During this phase, not only the infected PC is scanned but all the active cloud storage, network shares and other linked nodes are also checked to spread the ransomware infection. This phase also includes creations of various ransom notes in .html, .txt, .bmp format and pasted in each encrypted folder or even on desktop [8, 35-37, 39]. The time taken during this sequential searching depends on the number of files, folders, sub-folders currently stored on the disk. If there are millions of files saved on the disk then ransomware will take several minutes to hours whereas if a few thousand files are there then it will require only a few minutes.

Depending on the nature of ransomware, encryption of files or whole system or both is carried out. Scaife *et.al* [28] suggested the procedure of encryption in three ways [42]:

First method is used by ancient ransoms that moves all the files in a hidden folder and write new encrypted files on the disk with nearly same content. The second method moves all the identified files in a separate folder, compress it with password protection, meanwhile create new files that contains only encrypted matter, and simultaneously delete the original one. Third procedure overwrites the files one-by-one that not only erase the previous contents but make file recovery nearly impossible. The methods are time consuming and that's why these can be blocked.

As far as encryption is concerned, the AES key is used to encrypt the files while to ensure that captivated files remain irrecoverable, RSA – public key is used to further encrypt the AES-key. However, the RSA- private key, which is the decryption key, remains on the master server. In addition, the key used for encryption of files, i.e., AES-key is a MD5 Hash of obtained information, i.e., Computer name, Processor information, Volume Serial Number and OS version [45].

3.1.5 STIPULATION AND DEMAND PHASE

After the entire appropriate format files on the system are encrypted, only one decision is left in the hands of victims –pay or not. After all tasks within each phase is accomplished, ransomware swipes out all its traces and leaves a wallpaper resembling either a ransom note or logo of the infection.

Ransom note consists of message from the extortionist, instructing victim of how to make payment in the form of cryptocurrencies with the help of TOR browsers and restore all encrypted files or an encrypted system. Well, there is no guarantee that after payment all the encrypted files are back without any stolen information or even if you got the key that will definitely open the lock. The chosen payment method is a cryptocurrency, usually bitcoins [18-19] so that attackers ensure anonymity during transaction of ransom and avoid being captured by cops. All these payments are made only using TOR Browser [39].

Not only this, some ransoms even set the time limits for payment such that after the time expires either the files are deleted automatically or the price for purchasing the decryption key is doubled or tripled. The latest variants also deploy a counter that deletes fixed number of files with every passing hour [46].

3.2 MOST IMPACTFUL ATTACKS OF 2016-17

Each ransomware has unique feature that separates it from the rest ones. Some of the ransomware that gain a huge amount of profit and victims during 2016-17 and those which created nuisance in the beginning but undertaken soon are furnished below with a hierarchical chart (figure 3.9):

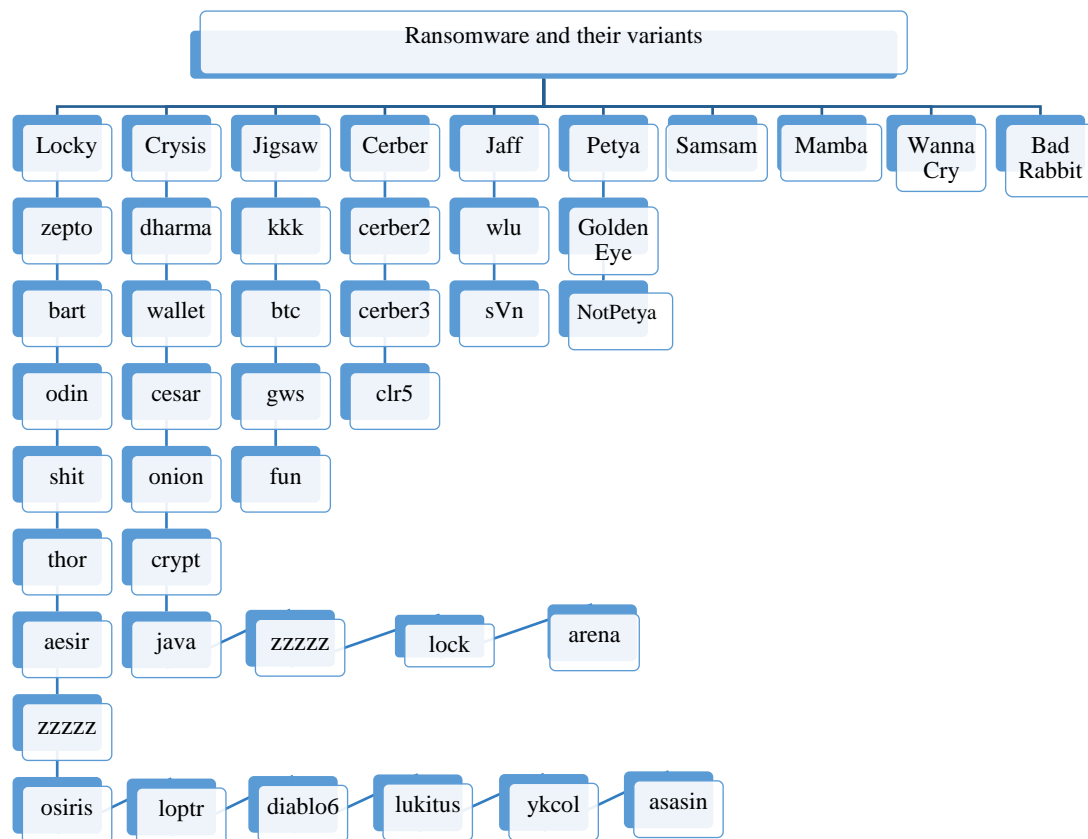


Fig 3.9 Classification of Ransomware and their variants

1. BadRabbit
2. WannaCry
3. Petya/GoldenEye/NotPetya/ExPetr
4. Locky
5. Jigsaw
6. SamSam
7. CrySiS/Dharma
8. HDDCryptor/Mamba
9. Jaff
10. Cerber

3.2.1 BADRABBIT

Year 2017 witnessed numerous ransomware attack; the third largest attack of such kind is a preplanned, well-coordinated and targeted attack that originates with Petya in July but showed its devastating effects later on Oct 24, 2017 is known as BadRabbit, which victimized large corporate networks and multinational firms [47-48].



Knocking phase: BadRabbit infection begins from compromised Russian news/media website that elevates a pop-up window to download latest version of flash player, which is actually a fake one that redirects to a website where a malicious payload dropper is waiting for the permission from visitor. It also uses WMIC and through employed EternalRomance exploit kit it further leveraged SMB (Server Message Block) vulnerability for distributing the malevolent code [47-50].

Execution of infection phase: Once the executable files get successfully downloaded another file named *infpub.dat* is dropped in C:\Windows folder which get executed using *rundll32* command [50].

Handshaking phase: The malicious file *infpub.dat* connects to its command and control server by itself behaving like client machine to download another malicious executable namely *discpi.exe*. The *discpi* is derived from open source diskcryptor utility designed to perform encryption [50].

Demolition phase: The files with appropriate extensions are searched that can be encrypted by *discpi* executable. Once all the files are located, then it is encrypted with a tamperproof combination of AES-128-CBC and RSA-2048 by downloaded *infpub.dat*. In order to encrypt the system a 32-bit long random key is produced on the system by *CryptGenRandom* function that locks down the entire system after file encryption [50].

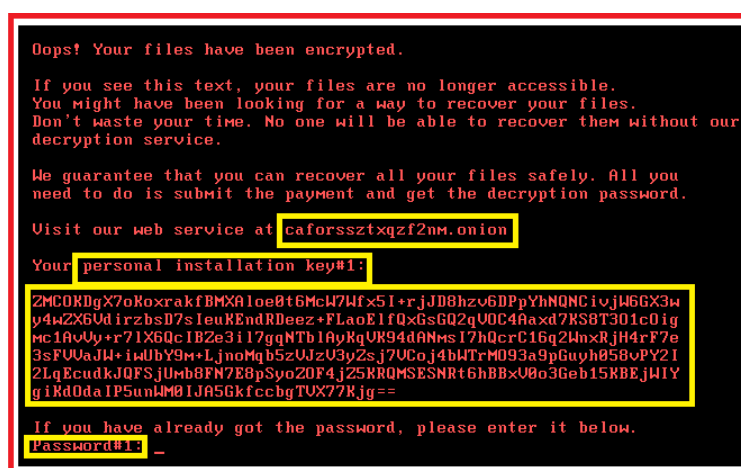


Fig 3.10 Ransom note placed by BadRabbit ransomware

Stipulation and demand phase: It displays a ransom note displaying *personal installation key #1* (figure 3.10) which varies from victim to victim and a common link that takes user to a page hosted by the darknet that informs users of the encryption.

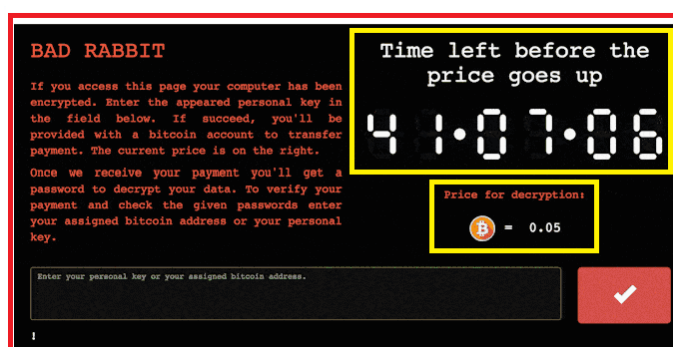


Fig 3.11 BadRabbit ransomware informing user about infection



BadRabbit demands a ransom of ≈ 0.5 , i.e., around ≈ 1 , 91,517 [48,51] to provide a password which is the decryption key to unlock the frozen screen. To create panic among the victim it deploys a countdown timer that counts the remaining time before price rises to more bitcoins illustrated in figure 3.11.

3.2.2 WANNACRY

Wannacry is considered as most scary ransomware since its first appearance in May 12, 2017 and even after upgrade within 48 hours of its initial blowout. According to Microsoft's Analysis and Report, it exploits the SMB vulnerabilities in unpatched versions of OS: XP, Vista, Win7, 8, 8.1 by using *EternalBlue* exploit kit and *Double Pulsar* backdoor [52]. Since it blocks the access to whole computer system as well as to files and even replicate itself to entire network of computers linked to the infected one via SMB due to its worm like capabilities [53]. It allows only two files to be accessed one is instruction file consisting steps to follow next and the other is a decrypt program. Above two-lakh computer are infected with Wannacry in about 150 countries while German Railway and Spanish Telecommunication Company were worst affected [52].

Knocking Phase: It spread through the unsolicited socially engineered e-mail that tricks the victim to click the link that redirects to a compromised website, where EternalBlue exploit is waiting for probing the vulnerability on visitor's computer. Once the ransomware executable is downloaded the installer extracts the password protected zip files into the same folder that include the actual mechanism used by wannacry to perform startup tasks, such as: deleting volume shadow copies, disabling win startup recover and cleaning win server backup history. [52-55].

Execution of Infection: Once the wannacry is on the system, it further searches for exploiting vulnerabilities on the system. On initializing, it creates two threads; one out of which scans hosts on the LAN and other performs replication to create 128 new threads of its kind to search for security loopholes over entire network. The scanning thread tries to establish the connection with Port 445 to access eternalblue modules for further exploitation of vulnerabilities. If this whole attempt takes more than 10 minutes, then exploitation threads is stopped along with eternalblue modules and doublepulsar backdoor is called for installation of disastrous payload with complementary intruding malwares [52-55].

Handshaking Phase: Once wannacry loader successfully setup itself inside the computer and gain full access rights, it downloads a Tor client to communicate with master C&C server to prepare infected computer for encryption. Hereafter, all the exchanges it calls *taskkill* command for terminating the connection and database.

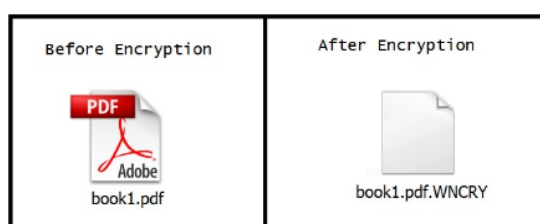


Fig 3.12 Files before and after encryption by wannacry ransomware

Demolition Phase: It is able to encrypt 176 different kinds of files using AES and RSA algorithms and finally appends *.wcry* as an extension (figure 3.12) [54]. During encryption process, it opens each file and add a WANACRY! string at the beginning and further contents are replaced with encrypted ones.

Wannacry employs two different keys for encryption: one is to actually encrypt the files that would not be decrypted without ransom payment and other one is demo key that will only encrypt those files that will be treated as bait for user to induce him/her to pay ransom. Those files which are encrypted with demo key are decrypted in demo provided to victim to infuse a believe in them for hackers. At last it runs



@WanaDecryptor@.exe program to lock the desktop main screen and paste an instruction file and a demo decryptor program.

Stipulation and Demand Phase: Wannacry hacker's demands payment of around \$300 in terms of bitcoins, i.e., around ₹19,290 per computer [51, 53-54, 56]. The ransom window (figure 3.13) has two active buttons, one for *check payment* and other is *decrypt* (demo) and a bitcoin address that varies from victim to victim. When check payment button is clicked, the ransomware connects back to TOR C&C server to check whether a payment has been made or not. If yes, it will automatically decrypts your files. If not, then a warning arises as: Only 7 days are left to recover encrypted files by making payment otherwise they delete key from the server. In some cases, it is also noticed that after every three days payment goes double [54]. Now nothing is left to victim neither GUI nor other files, but only a maroon screen with ransom note and two files.



Fig 3.13 Ransom note by Wannacry ransomware

3.2.3 PETYA/NOTPETYA

Originally *Petya* was detected during March 2016 by bundling itself with other ransomware known as *Mischa*, which means two ransoms in a box and is also named as *GoldenEye* [57-59]. Later on, it again revealed its appearance in mid of 2017, but this time all alone and without homework, and got many new names as *ExPetr*, *NotPetya*... [60-63] due to its built-in wiper.

Knocking Phase: Petya's *GoldenEye* variant is distributed via theme-based spam campaign consisting of malicious pdf regarding a job-resume with subject and file name including a German word '*Bewerbung*' [57,59]. Once clicked it downloads the fake pdf file, which is actually the malevolent dropper. Before opening that file, it elevates a window asking for user permission, if user clicks (Yes) that means providing admin access then Petya is installed on the system and gains all the rights to modify MBR. Otherwise if (No) is clicked then *Mischa* is installed on the system [57-59]. In such case, user has no other option rather than to be a victim either of Petya or *Mischa*. This bypass technique works from Win XP to 10, both on 32 as well as on 64-bit. NotPetya variant of Petya, intrudes a system by bluffing victim for initiating drive-by-download attack. This time the outbreak begins in Ukraine not targeting Germany by hijacking website that updates *MeDoc* software, a widely used Accounting and Tax paying software in Ukraine. Furthermore, it spreads through *EternalBlue* or *EternalRomance* exploit by breaching the SMB loophole [60,64].

Execution of Infection Phase: As soon as Petya make space for itself on the victimized system, it begins encrypting files one by one and appending a random extension at the end of each encrypted file, while if *Mischa* performs the encryption then it appends .7GP3 at the end of file. NotPetya's executable is made to run through *rundll32.exe* and *perfc.dat* command and works on same pattern as *GoldenEye* variant. However,



WMIC tool works simultaneously for executing malware on remote server accompanied with *Mimikatz* tool for stealing that information, which is valuable for its holder [60-62,64].

Handshaking Phase: In case of NotPetya, once the entire primary tasks before initiating encryption accomplished. The *Mimikatz* or *Windows Access Token Theft* tool performs its actual task of stealing all the credentials, user logins, passwords and whatever victim types and sends all stolen information to its master controller [60].

Demolition Phase: While the *fake chkdsk* longer appears on the display, NotPetya variant opens the file and overwrite its contents with null bytes. Both variants of Petya, not only encrypts other file formats such as .pdf, .png, .bmp, .jpg, .doc...but also encrypts .exe formats [59,61]. Finally, MBR is modified to disable normal boot into custom boot to ransom note screen. GoldenEye variant after encrypting files deploys Petya in %AppData% directory, crashes the system and reboot. While booting Petya/NotPetya begins by displaying a fake chkdsk screen in front-end and in background begins the encryption of MFT's content via *Salsa20* tool [57-59, 61].

```
You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://goldenhjqvc21ld.onion/ngWpIc5x
http://golden2uqqiqcs6j.onion/ngWpIc5x
3. Enter your personal decryption code there:
ngWpIc-5xHNJB-JFo2ap-H7gDqS-6oMbCU-PCAEbX-SAC6Ju-3Jf3oe-EiDXB3-BhuJBg-
cYDbGH-9izqGC-f28NPM-1p6a5R-DqZZH5-eKA9eh

If you already purchased your key, please enter it below.
Key: _
```

Fig 3.14 GoldenEye's ransom note

Stipulation and Demand Phase: Once the MFT and MBR are undertaken by Petya/NotPetya attack, a fake chkdsk screen ends on a yellowish screen (figure 3.14) with blinking "Press any key...". As soon as a key is pressed, a ransom note appeared on infected machine greeting with a message, two Tor links, address to feed personal decryption code and asking for a ransom of around ₹1.3, which is approximately equals to ₹ 92,393.68 [51,58]. The procedure of payment includes three distinct steps beginning from feeding personal identifier code to demand of ransom that finally ends with address of bitcoin wallet. Once the payment is received, attackers behind Goldeneye provide a decryptor program to decrypt the encrypted files [57,59].

```
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:
1Hz7153HMuXtUr2R1t70nGSdzaftNbB4K

2. Send your Bitcoin wallet ID and personal installation key to e-mail
mnmnm1h123456@posteo.net. Your personal installation key:
zRNagK-CDBHfc-pB5a14-vf8d2-14hbs-47UCzb-RYjq3E-ANg0rK-49XFX2-E42R5a

If you already purchased your key, please enter it below.
Key: _
```

Fig 3.15 NotPetya's ransom note

As the message window shows (figure 3.15), there is no sign of decreasing time frame and increasing the payment and deletion of files with NotPetya. Thus, to guarantee ransom payment and scare victims, *Mimikatz*



credential robber is leveraged. Yet, Petya asks for payment of around \$300 in terms of bitcoins, which is approximately equal to ₹19,314.00 [56].

This sudden drop in prices does not matter because neither the e-mail address (directed for sending personal installation key, varies victim to victim) nor the common address (instructed to send bitcoin) were working. Hence, NotPetya worked as a weapon of damage only (wiper) and unable to decrypt the encrypted files as directed in the ransom note left in text format [62].

3.2.4 LOCKY

Since Feb 2016, *locky* ransomware is successful in making a separate venture for itself in the herd of ransomwares. Its each and every variant discovered till Oct 2017, is well designed and coded such that neither flaws have been detected that can be turned to proceed towards development of decryption tool nor the reason of its interrupted appearance and disappearance disclosed. Furthermore, it is the most prevailing ransomware open in nature and have targeted around billions of end-users.

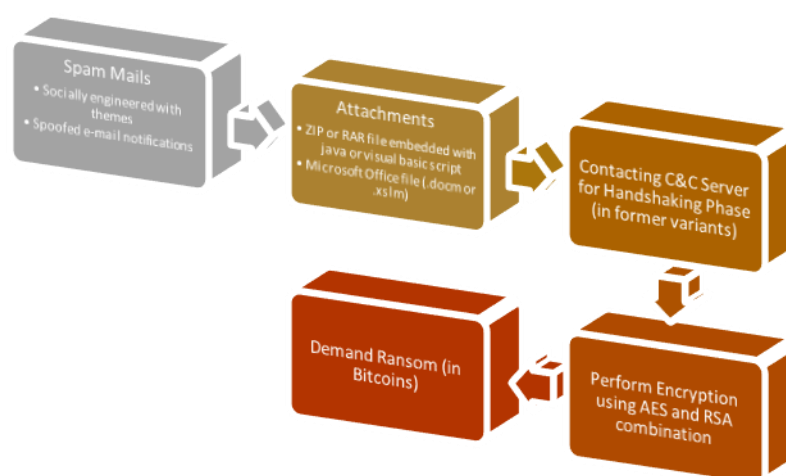


Fig 3.16 Anatomy of Locky and its variants

Knocking Phase: Initially locky's knockers are found in spam campaigns launched by Dridex and Necurs botnet in the form of attachments either macro embedded in Microsoft Office document, windows batch within document file or zip or RAR file infused with malicious javascript or visual basic script [4]. The subject baits that hackers use to tempt recipients to open infectious spam are quite common and interesting such as Invoice_(Random No.), Family Picture.jpg.js, Document, suspicious movement in A/c. XXXXXXXX...[4]. It is also observed that Locky even exploits vulnerabilities in flash and use malvertisement initiated through RIG exploit kit for befooling the user or as an attempt to enter the system. Some later variants even employ .dll file embedded in ZIP attachment for knocking purpose.

Execution of Infection: As soon as a recipient opens the attachment he/she will be greeted with a prompt to enable macros (usually in Microsoft Office 2013 or later) to view the content of the file; if spam contains macro enabled document file as attachment. Once enabled it begin downloading the PE for Locky ransomware. If attachment is mischievous javascript embedded with ZIP or RAR file, then once clicked it will call out windows script host that handles any active scripting language, which in turn changes some value in registry from 0 to 1 to begin to install locky on the PC. Not only this, locky ransomware is known to use DGA's for generating a list of domains that behave as C&C server during this phase [4].

Handshaking Phase: During handshaking phase, the PE downloaded and installed in the previous phase tries to contact one of the C&C server of hacker obtained by DGAs in previous phase. However as soon as a connection is established between C&C server and victimized client, the PE sneaked inside the PC starts to



exchange information with server initiated with system identification in order to generate a conventional private-public key pair; where the public key is sent to PE of victimized system and private key reside on server. It is also worth to mention that some later variant's of locky ransomware does not require communicating C&C server as the public key for encryption is already embedded within PE.

Demolition Phase: Before probing for appropriate extension for encryption, locky ransomware figure out any presence of backup and eliminates any chance of recovery by disabling system restore and eradicating volume shadow copies by running vssadmin process. It uses RSA-2048 bit via C&C server that further generates 128-bit AES key on the system, which actually encrypts the files and this 128-bit AES is encrypted with public RSA key that can only be decrypted by private pair of that key hold by hacker on the server.



Fig 3.17 Before and After Encryption (Locky)

The later version of locky generates 256-bit AES for file encryption. The appearance of file after encryption includes system id (generated on C&C server) and 16-bit random hexadecimal number that finally ends with .locky extension appended at the end of encrypted file name as shown in figure 3.17.

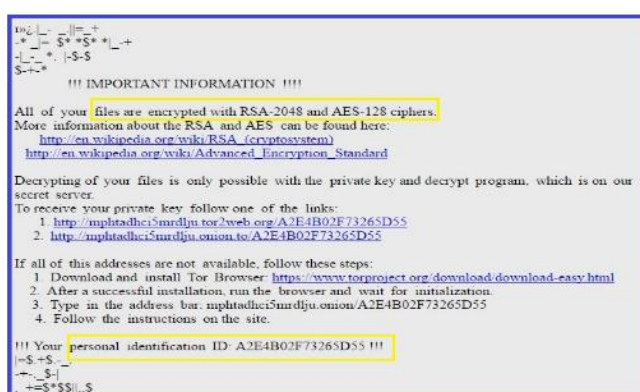


Fig 3.18 instruction.html file of Locky including ransom note

Stipulation and Demand Phase: Once the infection is successfully executed and encryption is accomplished, the desktop wallpaper switches to display ransom note (figure 3.18) that includes information regarding the infection and cryptographic algorithms used. It also incorporates a procedure to access dark net via TOR and make ransom payment of ₹ 0.5 to ₹1.0, i.e., around ₹14, 693.78 – 29,387.56 [4,51].

Variants: Locky is a biggest-sized family of these thirteen ransomwares each enriched with a new property as compared to the previous ones [65] and are arranged as follows:

(i) Zepto (Jun 27, 2016) [66]

- used *neutrino exploit kit* for distribution.
- zip attachment with embedded javascript and macro-enabled document.



- ransom demand is three times its ancestor, i.e., up to ₺3.0 .

(ii) Bart (July 2016) [67-69]

- RSA public key embedded within the malicious executable.
- Do not target the computers with Russian, Belorussian, Ukrainian language packs.
- After encryption, file name remains unchanged except the appended *.bart.zip* extension at the end.
- AVG designed a decryptor tool that performs decryption by comparing the encrypted as well as original copy of the file, if available and provided from offline backup.

(iii) Odin (Sept 26, 2016) [70]

- Spam attachment includes embedded windows script file, downloaded by communicating to exterior link and deployed in win dll via *rundll32* utility to perform encryption of files.
- It also rename files and add *.odin* extension.
- Ransom amount varies from home user to corporate user.

(iv) Shit (Oct 24, 2016) [71]

- Spam attachment will leverage all three kinds of embedded malicious scripts using windows script, javascript or html applications.
- Able to target 138 file formats for encryption.
- Name of the file containing ransom note is replaced by *_WHAT_is.html_<2-digit random number>* or *_WHAT_is.bmp*.
- It can be removed from the system in safe mode.

(v) Thor (Oct 25, 2016) [72-74]

- New visual basic script is added as new malicious embeddable, meanwhile *.shit* variant is terminated.
- Zip file includes a macro enabling excel file *'budget_xls_<random number>* with a subject line *budget forecast* for luring recipient.
- Encrypting the files, scrambling the filenames, appending *.thor* extension and represent a ransom note in *.html* and *.bmp* format.

(vi) Aesir (Nov 21, 2016) [75]

- This variant knocks as a complaint from ISP gives fake information that recipient is being used as a botnet for sending spam mails.
- The embedded malicious javascript installs itself in *%temp%* folder via *rundll32* utility for performing actual destruction.
- Distribution is initiated by *Nuclear exploit kit*.
- The ransom note file is renamed to *_instruction.html, _instruction.bmp*.



(vii) zzzzz (Nov 24, 2016) [76]

- Distributed along with .aesir variant with *order#<random number>.zip* as malicious attachment embedded with javascript by spoofing as famous e-commerce sites such as *RoyalMail, FedEx, Amazon*, etc. It works in quite similar manner as .aesir variant.
- Leveraged *GeoIP* awareness for targeting specific regions and countries.
- While performing encryption, it behaves as adware by flashing various social media ads on the screen.
- It places a ransom demand of about \$400 and majorly targeted small to medium sized businesses.

(viii) Osiris (Dec 06, 2016) [77]

- Infused with capability to bypass windows defender firewall.
- Subject of spam is order confirmation and also knocks via malvertisements employed on BBC, MSN and AOL websites.
- Ransom demand varies from $\square 0.5$ - $\square 4$ depending on the target, either home user or corporate.
- Ransom note pop-ups in web browser after encryption is done.

(ix) Loptr (May 10, 2017) [78]

- *Necurs* botnet dumped the distribution of this locky variant to encourage Jaff ransomware, but after suffering setback from *Jaff* attackers haphazardly launched .*loptr* variant out for destruction.
- Again fake invoices and social engineering tactics are leveraged to trick user but this time with two compressed files.
- Although .*loptr* variant fails due to non-debugged flaws that occur during unzipping of malicious files on win 7 or later versions, it only effects the computer working on win XP or Vista.

(x) Diablo6 (Aug 09, 2017) [79-80]

- E-mail id of sender and recipient has same domain.
- Ransom demand is reduced to $\square 0.49$ with note named as *diablo6-<randomnumber>.htm*.
- Embedded visual basic scripts are used as infection initiation vectors that lead to *greatesthits.mygoldmusic.com* domain for downloading executable to do encryption and append .*diablo6* at end.

(xi) Lukitus (Aug 15, 2017) [79-81]

- Lukitus is a French word that means locking.
- After locking the files .*lukitus* extension is appended with a ransom note named *lukitus.html* and *lukitus.bmp* is left.
- Again knockers are zip-file embedded with visual basic or javascript or macro enabling office document or spoofed notification messages. While the subjects lures are *please print, docs, pics*, etc.
- Ransom demand is same as .*diablo6* variant.



(xii) Ykcol (Sept 18, 2017) [82]

- Subject theme is changed to *status of invoice* whereas the embeddable are the same visual basic script fabricated within zip folder.
- This name is just the reverse spelling of *locky*-> *ykcol* and the ransom note appears with the same name as new extension, i.e., *ykcol.html*, *ykcol.bmp*.
- Ransom demand is further reduced to 0.25 bitcoins, equivalent to ₦65, 489.30 [58] inspite of this the value of bitcoins are increasing in comparison to other currencies.

(xiii) Asasin (Oct 10, 2017) [82]

- Suffered setback due to malformed distribution campaign and non-visibility of attachments in computers except those, which support base-64 encoding.
- Signature based e-mails are used for baiting user for legitimacy of mail by keeping in mind the increasing awareness about spam's and ransomwares among people.
- Working is similar to ykcol variant except the appended extension and ransom note, i.e., *asasin.html* and *asasin.bmp*.

3.2.5 JIGSAW

Jigsaw pioneered its presence in April 2016 in the form of a crypto-ransomware that not only lock the files by encryption but also deletes them after a fixed duration of time until the payment is made [46, 83-84]. It follows the concept of exponential growth in removing the encrypted files from the system and pressurizing victims for ransom. Jigsaw ransomware shares features of Logic Bomb, which concluded that Jigsaw is designed to run after a fixed date. As justified in [84], Jigsaw variant designed to target computers with Portuguese language pack are triggered after Apr 06, 2016 while they remain dormant from the day of intrusion, i.e., Mar 23, 2016.

Knocking Phase: Usual method adopted by Jigsaw for knocking down into a system is adware. However, apart from it, later variants of Jigsaw also spreads by victim's visit to websites containing adult contents [46]. Sumalapao [46] also analyzed the delivery of Jigsaw as a bundled file from a URL hosted by *1ficher.com* (a defame free cloud storage) and *hxxp://waldorfftrust.com* that downloads Jigsaw along with crypto-miner software.

Execution of Installation: Once malicious is dropped inside the system, it will automatically set an auto run that starts ransomware each time victim login to Windows.

Demolition- Jigsaw uses AES algorithm for encryption and append extensions as *.FUN*, *.KKK*, *.GWS*, *.BTC* depending on variant once encryption is accomplished. It scan drives for following extensions *.eps*, *.jpg*, *.wav*, *.mp3*, *.jpeg*, *.raw*, *.rar*, *.java*, *.pdf*, *.accdb*.....[84]. For terrorizing victims to pay ransom, it creates a separate button that shows the list of encrypted files (estimated while performing encryption) and bitcoin address assigned to victimized system. Both of these text files are visible in *C:\<UserProfile>\AppData\Roaming\System32* folder. Finally, it modifies the boot process in such a way that whether user restarts the system, reboot or tries to remove jigsaw, its auto run mechanism informs the C&C server and as a punishment, it deletes a thousand of encrypted files from the system [46, 83-84].

Stipulation and Demand: In order to create panic among users and ensure the payment of \$20-\$200 [46, 83-84] as ransom, which is approximately ₦1, 327-₦13,274 [56], it generates a live ransom note. In every 60 minutes, it deletes a file and even sets a counter, which is incremented with each deletion. This counter is not setup to count down the time but to increase the number of files to be deleted with every passing hour. Thus



further extorting the victim to pay ransom by declaring that only 72 hours are there to get files back unless nothing will be left, everything will be swiped clean from system, i.e., permanently deleted. When a victim sends a ransom payment, they can click on the check payment button. Once clicked, the ransomware send queries to <http://btc.blockr.io/> to see if a payment has been made to the assigned bitcoin address. If the amount of bitcoins in the assigned address is greater than the asked amount, then it will automatically decrypt the files.



Fig 3.19 (a) Jigsaw ransomware (initial variant)



Fig 3.19 (b) Jigsaw ransomware variant with modified ransom note

Variants: The first variant of Jigsaw places a picture of clown in the background (figure 3.19 (a and b)) of ransom note whereas in the next variant, the ransom note is modified. In other variant, image of the clown is replaced with pink gerbera flowers (figure 3.20). Techniques employed for probing, encryption of files remains the same in both variants and only the ransom amount varies from \$20 to \$200 [91-92].



Fig 3.20 Ransom note of jigsaw ransomware (final variant)



3.2.6 SAMSAM

Samsam or Samas ransomware was pioneered in Mar 22, 2016 and still in action. Being a ransomware, its approach to thrash out a system is entirely different that take an unusual advantage of remote execution. Its initial variant majorly captivates hospital systems, which is now extended to disturb educational and governmental sector as well. Being one of its kind it also places very high and varying ransom demands in comparison to other ransomware families. It is written in C# and manually deploy ransomware on target system rather than automatic.

Knocking Phase: Samsam ransomware uses *JexBoss*, an open source infiltration tool that exploits the vulnerabilities of unpatched *Red Hat JBoss java based web server*. Once the server is successfully enthralled, it employs another tool such as *Mimikatz* [85], *Derusbi* or *Bladabindi* [86] over it meant for stealing active personal login credentials along with collection of further data about host network.

Execution of Installation Phase: Once Samsam successfully knocks down the server, it uses *psexec* executable to spread the ransomware payload or executable on each host on the network running Windows OS [86-88]. On spreading over the entire server and to spread further to connect machines it performs web shell deployment, batch script usage and gain remote access to multiple nodes through tunneling by *Regorge* tool [87,89].

Handshaking phase: The crooks behind the Samsam ransomware generates the RSA key pair themselves and upload the public key along with ransomware to the targeted computer using batch scripts [85-86].

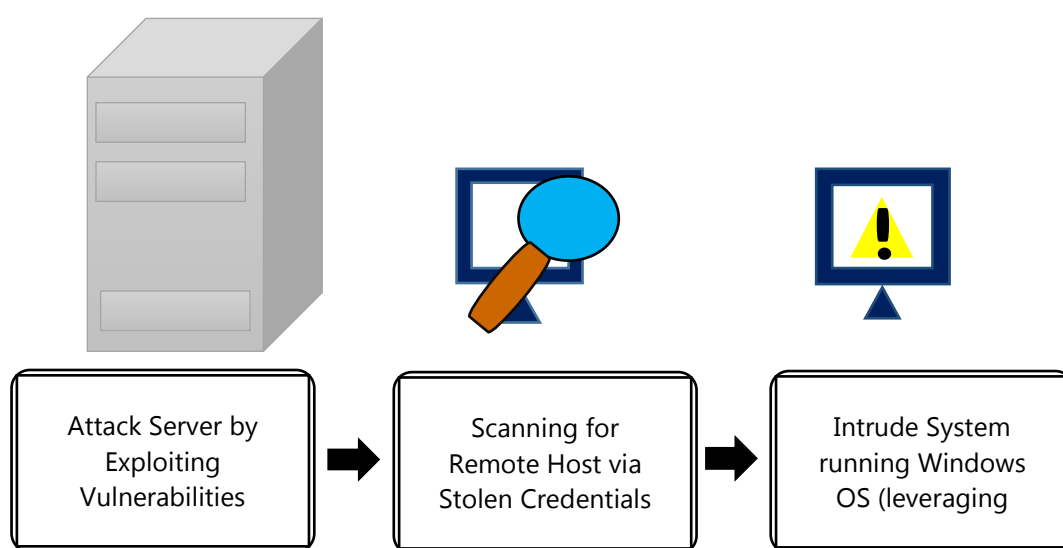


Fig 3.21 Anatomy Samsam ransomware

Demolition Phase: After deployment, it searches for the appropriate list of files that can be encrypted [90]. Along with this probing, it even runs another searching mechanism via *sqlrvtmg1* executable that searches for any locked files and map to that process under currently running and finally killing the process to ensure encryption process [88]. In order to ensure ransom payment and make victim completely helpless, it even deletes any backup, i.e., volume shadow copies and disables System Restore, Safe Mode, System Recovery and Windows Error Reporting. It even terminates any attempt to open Task Manager or *Regedit* [88]. For encrypting various file formats, AES algorithm is used and RSA-2048 key pair for encrypting the key generated for file encryption by executing *samsam.exe* that performs actual encryption [86].

Stipulation and Demand phase: The first variant of Samsam ransomware that majorly targeted healthcare services such as hospitals and demanded a fairly high amount that is 0.7-1.0 bitcoin per PC equivalent to



027, 832.25. This demand of ransom raised to 01.5 and then between 01.7 and 012, i.e., up to 03, 33,987 approximately for later variants [90]. The amount demanded as ransom is directly proportional to scope of infection. As illustrated in figure 3.22, it asks for 029 to receive all the decryption keys and for half of keys ransom amount is dropped to 014. Thus shows the perfect statistical planning of cost and profit made by actors behind the attack.



Fig 3.22 SamSam ransom note for later variant

3.2.7 CRYISIS

Crysis or Dharma ransomware is another dangerous kind of malware that can be tackled. Researchers consider dharma as successor of *TelsaCrypt* and rival of defamed Locky ransomware. The ransom note thrown by later variants of dharma suggest that it is an advanced version of *Police ransomware* [15], but actually, it resembles like a fake service utility that wants to enhance protection of our files by encrypting them as suggested by ransom note (figure 3.23).

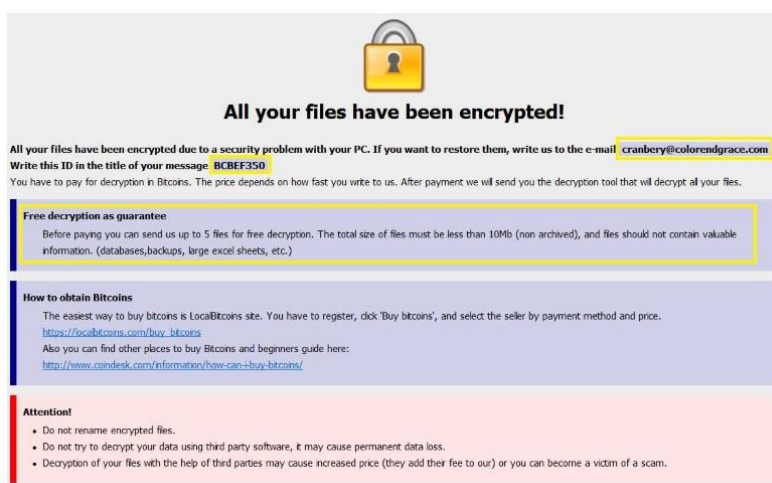


Fig 3.23 Crysis ransom note

The first registered outbreak of Crysis was in Sept 2016, which remain active until Aug 2017 with a number of different variants. It is important to notice that all the variants appeared and disappeared within short interval after renovations in previous coding. The crooks provide one or more e-mail addresses within ransom notes that are also appended with encrypted file extension, resembling that they want victim to contact them by e-



mail and make negotiation regarding ransom amount or something more is left to be stolen but goes unnoticed always.

Knocking Phase: Crysis ransomware propagates via wide range of infection vectors, i.e., firstly it employs brute force attack through *RDP (Remote Desktop Protocol)*, moving ahead it arranges distribution by sending attachments with double file extension in spam e-mails. Then it slithers into the system by adding malicious URLs in their spam campaigns and lurks through drive by download attack [91-93].

Execution of Installation phase: Once any of the above mentioned method employed by ransomware variant successfully knocks down into the system it begins to replicate, firstly in *Startup folder* and then *System32* folder [92]. Additionally, it recreates the values in windows registry to ensure uninterrupted execution of infection vector after every boot/reboot and thus make its removal difficult [91]. In some computers, it works by escalating the admin privileges to execute its malicious payload [91]. Like most of the ransomwares, it also deletes the volume shadow copies by executing *vssadmin delete shadows/all/quite* command [91-92,94].

Handshaking phase: There is no clear symptom representing any separate handshaking phase but it seemed that after encryption, the device name, list and number of encrypted files and victim's id is exchanged with notorious remote master server via HTTP protocol [91-92].

Demolition phase: Dharma is able to encrypt around 185 types of files by using a combination of AES and RSA cryptographic algorithms. The span of encryption varies from fixed to removable drives, network shares to *.dll*, *.exe* and system files that lead victimized computer to an abnormal state. What is left without encryption, is merely operating system files and those files that belong to ransomware [91-95]. One more separative task done by crooks behind Crysis, is to append e-mail id unique to each variant along with ransomware's genuine extension (figure 3.24). It is also worth noticing that some variants even perform renaming of encrypted files [92].

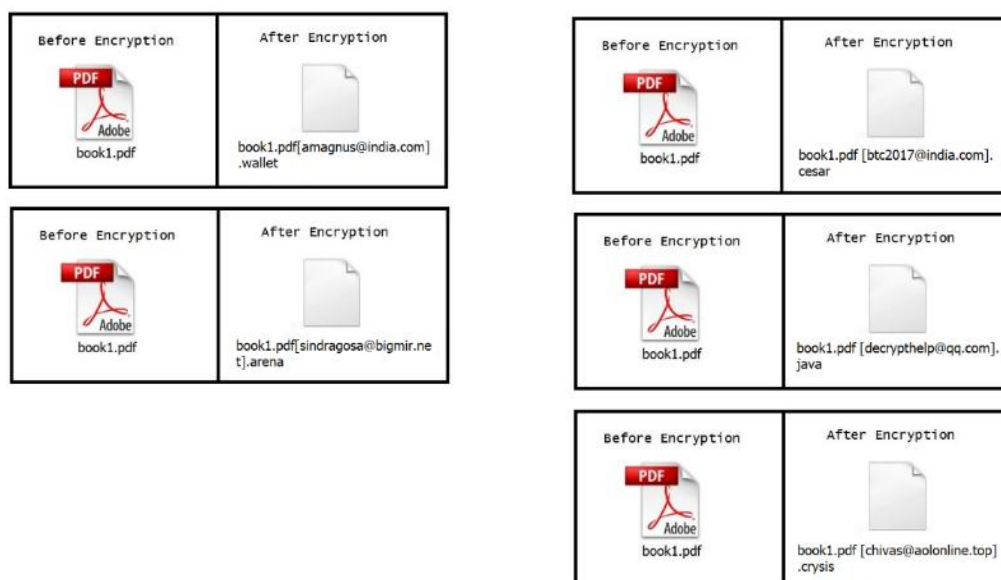


Fig 3.24 Before and after encryption (Crysis and its variants)

Stipulation and Demand phase: Usually the wallpaper changes to logo of Crysis and for infusing victim's believe on attacker, they provide a service of free decryption of five non-significant files. When such e-mail ids are contacted, they instruct victims to pay a ransom amount varying between \$400-\$1000 in the form of bitcoin crypto-currency [91,94]. Furthermore, later variants like *.wallet* tried to develop panic among victims by setting a time limit of 72 hours for payment. If failed, they claim to destroy decryption key, which results in a loss of all encrypted files [95].



Variants: During analysis, the various papers and online blogs [91-95] suggested that crysis altogether have many variants, namely; *.dharma*, *.wallet*, *.zzzzz*, *.cezar* or *.cesar*, *.java*, *.onion*, *.arena*, *.crypt*, *.lock*. Though, each variant's extension, ransom note, knocking methods and provided e-mail id possess difference but its functionality remains the same. All the variants deployed by the crysis ransomware can be decrypted by ESET [92] tool except *.arena* variant, which is still non-decryptable.

3.2.8 MAMBA

Mamba or HDD Cryptor ransomware named after a deadly snake found in Africa, was introduced in September 2016 and crippled thousands of computers of *SFMTA* (*San Francisco Municipal Transportation Agency*) in November of 2016 [96-98]. Recurrence of Mamba in August 2017 has diversified and hard-hitting approach by entangling through open-source legitimate tool *DiskCryptor*. It not only heavily affected high profile users and organizations but also places high ransom demands of around \$4000 ~ ₹ 2.5 Lakh per ₹ [97-100].

Knocking phase: It is detected that neither it uses exploit kits nor any e-mail mechanism for distribution purpose, but tried to exploit or misused RDP and illicitly accessed an organization's network of computers and then utilize *psexec* service for execution of malicious code [96,99-100]. Once it successfully enters the system, it creates a folder where it drops the files useful for encryption in next phase [101]. In some cases, mamba infection can also lurk into the system by unwitting run of malicious file. Then generation of the UAC permission prompt shown in figure 3.25 to redeem access permission for mamba to execute [101].

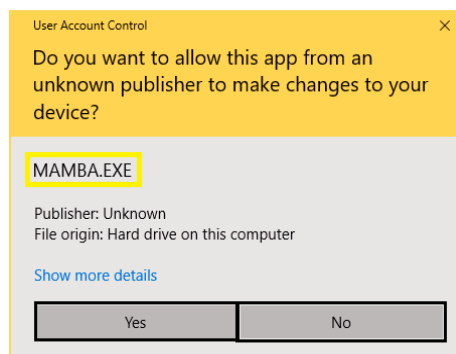


Fig 3.25 Prompt elevated by Mamba ransomware for user permission

Execution of Installation Phase: Once the malicious code successfully sneaked into the system, it begins to gather information about OS, i.e., 32-bit or 64-bit. Depending on the same, Mamba chooses the module of *DiskCryptor*, a low-level full disk encryption tool to be downloaded and dropped into a folder of active drive (C:). All these tasks execute silently and files (*dcapi.dll*, *dccon*, *dcinst*, *dcrypt*, *dcrypt.sys*, *log-file.txt*, *mount*, *netpass*) [96] required for encryption purpose are dropped at location *C:\Users\WWW* (for new variants) [96,101] or *C:\xampp\http* [99]. As soon as all the files are dropped, *dcrypt* installer is called for execution. Once *diskcryptor* is installed on the system, it generates a service with two parameters *SERVICE_ALL_ACCESS* and *SERVICE_AUTO_START*, which provide full admin control to Mamba for its destructive tasks and allows force reboot of the system [99]. It can also be said that HDDCryptor not only stealthily installing itself but also escalating to gain local system privileges and masquerading as a Windows Service, with a name Defragmentation Service [101]. Additionally, Mamba remains invisibly active even if computer is logged off.

Handshaking Phase: For employing *DiskCryptor* facility used by Mamba ransomware, it generates a password unique for each infected computer and pass it to ransomware holding crook using command line arguments. This password behaves as both encryption and decryption key for the victimized system known to the attacker only. Thus, victim has no choice rather than to pay ransom or to lose entire HDD [97,99-100,102].



Demolition Phase: Before encryption, HDDCryptor or Mamba prepares the system by replacing the actual MBR with malevolently modified or customized MBR [102]. Then compromised system faces frequent reboots and finally encryption of the HDD with the password generated in previous phase. It not only encrypts each sector of HD comprising of OS files, personal files and folders but also network shares and resources, such as Printers, Serial ports, Shared files and folders using SMB and SMB mounted devices too [98-99, 101].

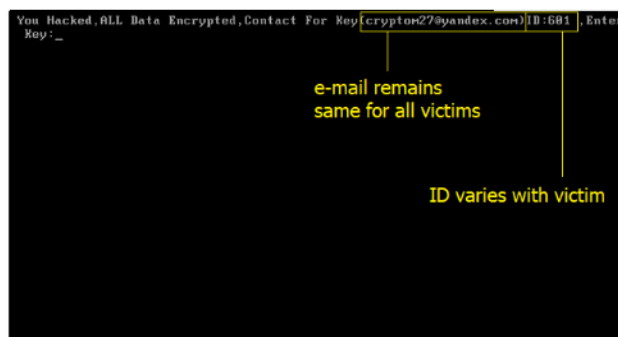


Fig 3.26 Mamba (HDD Cryptor) ransom note

Stipulation and Demand Phase: Once the encryption is done, the system reboots to a screen (figure 3.26) that informs victims that his/her HDD has been encrypted provided with victim's ID and two e-mail addresses for contacting attackers regarding payment of ransom [96,99,101-102]. As far as ransom amount is concerned, the attackers behind Mamba places the demand depending on the potential of victim. As visible from records of attack of first variant, SFMTA is asked to pay ₹100, approximately equivalent to ₹64, 27, 992.00 [98,100]. Moreover, during SMFTA attack it is also reported that around 30GB of data is filtered and sent to attacker, which is later on bargained for further extortion as to be disclosed on deep web if not paid [96]. But unfortunately, the data cannot be retrieved back even after the payment of ransom since the cracked version of DiskCryptor is employed by crooks and the code analyzed by ransomware analyst also resembles its faulty functionality that can only destruct [97,99-101].

3.2.9 JAFF

Jaff paved its way to the world of digital crime in May 11, 2017 [103-105]. However, presence of Wannacry at that phase of time overshadowed its presence but one cannot completely ignore from its occurrence and consequences. The whole infrastructure of Jaff resembles that there exists a big team behind the Jaff to support decryption once payment is made successfully. Even though its first variant is decrypted but the later needs much stronger encryption tactics.

Knocking Phase: The primary distribution source of Jaff is *Necurs botnet* that circulated a millions of infected spam mails within a day as their initial course of action to spread this ransomware [104,106-108]. This spam mail is especially designed with such subject lines as, '*print2copies*', '*document_random number*', '*reciept*', '*report*', etc. that it can easily bypass spam filters. The spam mail contain an attached zip file that includes a pdf file, namely *nm.pdf* or any *random_number.pdf* in later versions which further contains an embedded document file with extension *.docm* [103-109].

Execution of Infection phase: When user clicks the attachment to open it, the application installed to support pdf files prompts a warning message resembling the presence of embedded document file. If user permits to open the implanted *.docm* file, it will enable macros that tries to communicate with one of the ransomware server stored in the form of arrays, until it succeeds. As soon as the hidden starts receiving response, macros begins the download of intrusive malicious executable or payload [103-110].

Handshaking Phase: Thus, it is visible from above that macros play a suitable and significant role in establishing a link between ransomware dispersing server and victimized client.



Demolition Phase: After successful download and execution, jaff begins to delete any available volume shadow copies. It can encrypt more than four hundred file formats [106]. It also left a ransom note shown in figure 3.27 to inform and guide victim throughout the ransom payment process [103, 109].



Fig 3.27 Jaff's ransom note

All the encrypted files get a new name and extension of *.jaff* (with first variant), *.wlu* (for second variant) and *.svn* (for third one).

Stipulation & Demand Phase: For decrypting the victimized system, the very first variant of Jaff demands a ransom of around $\square 2.0$ approximately $\square 2$, 34, 171.80, which reduced to $\square 0.54$ BTC in next variant [104,106,108].

Variants: Jaff till date has a weakened outbreak with 3 distinct variants. Each later code is designed to overcome the flaws of previous one but unable to make its way as Kaspersky designed *Rakhini decryptor* freeware tool, which is able to successfully decrypt any variant of Jaff [104, 110]. The *.wlu* variant of Jaff has a little bit difference in knocking phase where the zip folder contains a *wsf* file infused with malicious javascript that lead to hardcoded URL of malicious executable or payload instead of pdf and embedded docm.

3.2.10 CERBER

Cerber ransomware that originated in Russia outbreak in July 2016, have seen rapid success as well as growth. It is a kind of bundled attack that employ *Betabot Trojan* [4] to steal credentials (logins and passwords), banking data and other sensitive information as much as possible. It is well-organized as well as well-funded ransomware family resembled by the task of quick patching performed when Checkpoint tried to develop decryption tool by reverse engineering encryption process [4].

Knocking Phase: Usually Cerber initiates the attack with vbscript injected macro enabled office document as spam message. This injected vbscript call out *Powershell* for downloading the malicious PE of Cerber and killing the active antivirus processes. Not only this, around 41% of Cerber attacks were launched by exploit kits as Neutrino, Rig and Magnitude. It is also noticed that Cerber is also offered as a service by its development team by sharing 60% of ransom payment with franchisee (spam campaigners or botnet masters) and 40% for themselves.

Execution of Infection: When the macro is enabled unknowingly after prompt on opening of document, the injected vbscript runs PowerShell to propagate itself throughout the network and place the downloaded payload in *%AppData%* directory or folder. Before executing further task, it checks for the installed language pack to be Russian and other defined by Liska [4], if detected to be then it stops the execution of ransomware there and removes itself from the system silently. Once successfully installing itself, Cerber disables safe boot and removes volume shadow copies to eliminate any chance of recovery and empowering the probability of



ransom payment. Then it checks for the files on victim's system to encrypt and steal via Betabot Trojan bundled with PE and finally kill any e-mail client process to ensure the encryption of their related files. In some cases Cerber also take advantage of Microsoft BITS, a legitimate application used for downloading updates in Windows OS, for downloading its PE. This allows anti-evasion by security solutions and anti-obstructive pass through firewall.

Demolition Phase: It make use of 2048-bit RSA public-private key pair to produce 256-bit to 576-bit AES key depending on variant. Again, AES key is used to encrypt victim's files and 2048-bit public key encrypts the file encryption key. After encryption appends .cerber, .cerber2, .cerber3, .c1r5 extension at the end of the encrypted file.

Handshaking Phase: Once encryption is accomplished, PE of Cerber tries to establish connection with C&C server to send all the information stolen by bundled Betabot Trojan as well as the AES key encrypted with 2048-bit RSA public key, whereas the 2048-bit RSA private key resides on the C&C server since generation with PE.

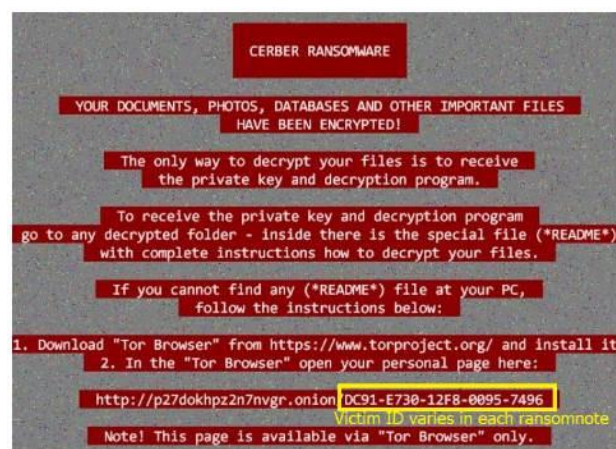


Fig 3.28 Cerber informing user of encryption

Stipulation and Demand Phase: Along with a formal ransom note illustrated in figure 3.28, Cerber also leaves a HTML document that includes embedded sound file, which plays a ransom message regarding encryption made by Cerber ransomware [4]. It asks the payment of ransom in terms of bitcoins only. Additionally, to enhance probability of ransom payment and increase panic among victims, Cerber provides a ransom payment scheme described as follows:

If advance payment is made, i.e., within 5 days of infection then victim has to pay a discounted amount of $\square 1.25$. Otherwise, if late payment is made, i.e., after 5 days of encryption then victim has to pay an increased amount of $\square 2.5$.

4. THE VIEW POINT

4.1 VICTIMS AND PERCEPTION

Finally, it may be inferred that the new era of ransomware arose with entire disk encrypting ransomwares and side-by-side leveraging brute-force and remote desktop attacks.



Fig 4.1 Facts that works against victims

Targeting more and more vulnerabilities on servers, persecuting public sector services such as healthcare, telecommunication, railways, airways, etc. containing enormous amount of critical data of relatively large mass. It is also observed that instead of paying the ransom some of the victims, relied on backup and chose to suffer a setback of some months. Once again, such incidents prove the importance of keeping regular backups. Some reasons that leads an end-user to become a ransomware victim are illustrated in figure 4.1.

4.2 RESEARCHERS' AND SECURITY ANALYSTS' OPINION

With each evolution in security and threat intelligence, cyber crooks paved a new way to increase the span of their damage. Daily millions of infectious e-mails circulate throughout the internet launched by any active botnet, many spams and phishing e-mails containing URL leading to malicious and compromised webpages. These try to infiltrate into the computer by penetrating firewalls and other employed security measures. Such an intrusion is only possible when the various security modules are not working, either partially updated or insufficient against level of attack [4]. The success or failure of any spam campaign also depends on the end-user who receive such nasty mails because it's only up to the knowledge and awareness of user to get tricked or not trapped by attackers. Having a backup but not tested can put all efforts in vain after suffering a ransomware attack. Meanwhile, Security of backup data should also be a major concern, as other members of malware family can affect them. Many security experts working in security solution tools sponsoring organizations highlighted the need of multi-tier security for computers. This includes protection from server end to minute OS processes and threads, auto-enabled patching of vulnerabilities and flaws in computer, keep and protect backup, auto-downloading of latest drivers, etc. are effective enough to cope up with any new kind of espionage and sabotage attack. Adoption of ransomware as a service [4] approach, multiple lines of attack, no or minimum scope of reverse engineering made it just a game of assumptions without evidences and proofs (figure 4.2). On the other hand, misuse of RDP provides a preliminary grip on victim's entire network [90], targeting unconcerned servers and minimal need of user intervention during an attack make prevention more challenging.

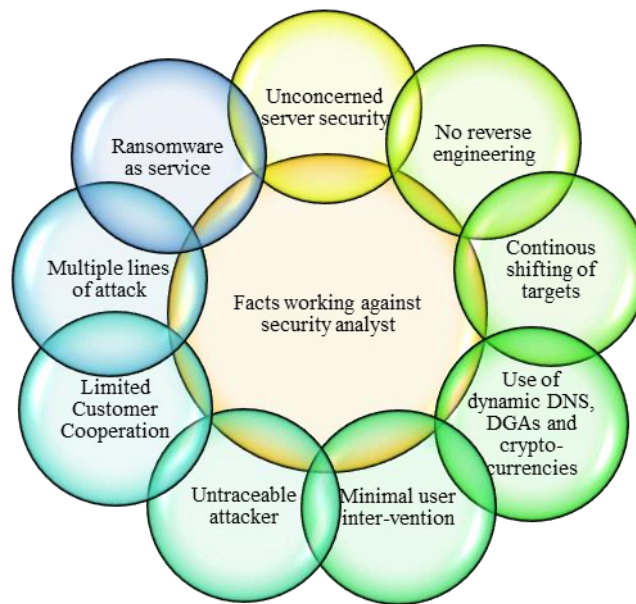


Fig 4.2 Facts that works against security analyst

4.3 ASSAULTERS' INSIGHT PERSPECTIVE

Assaulters are always excited to launch a new malware attack and surprise their targets as well as security analyst and researchers. They try to keep themselves far ahead of threat intelligence teams and thus constantly perform new experiments with their piece of code as shown in figure 4.3.



Fig 4.3 Facts that works in favor of assaulters

Before implanting any attack, an assailant should prepare hard in searching for resources, targets, methods, cost of investment and other complementary tools as well as a backup plan. Nevertheless, if one does not want too much brain exercise then implantation of infection dispersing application is also provided as provisional package on a fixed charge rate, available only on dark net portals.



5. THE NEW SAFETY ERA

5.1 FUTURE WHEELS TO CARRY ATTACK

Ironically, ransomware are most user-friendly and adjusting kind of malwares. Their new generation easily bundles themselves with spyware, adware, logic bombs, etc. with its inheritance from macro viruses and mail worms. Today spam campaigns launched by botnets widely support distribution of ransomware in the form of compressed files embedded with scripting language file or macro-enabling office documents, where embedded links lead to exploit kits and drive-by download, malvertisements; macro also enable establishing a connection to C&C and side-by-side download of malicious executable secretly. Leveraging legitimate tools as well as utilities, employing brute force attacks, hitting servers and scanning for remote targets are current techniques adopted by assailants for victim's extortion and yielding money. Some methods that may probably be ill utilized by assaulters in future for intruding a computer or their entire network are described as follows:

(i) Web Crawlers: In this era of digitalization, probing any topic is a task of few seconds, just open any search engine like google, bing, yacy, duck duck go etc., fill the search field with your query, hit enter button and millions of web links appear on the page as a result of query obtained by matching the 'keywords'. This task of providing millions of results within few seconds is effort of 'web crawler' or 'spider' that creates a centralized repository of web links by cataloging (indexing) every visited webpage yielded by simultaneously following the links within links [111-113]. As R. Ford [113] suggested web crawlers can be leveraged to search for confidential data from any poorly maintained website, which can perform as backdoor to intrude a system. Disclosure of domain registration, enterprise or organization's trash to any cyber crook proves destructive. Several consultancy firms and websites also exist on internet that include personal information of their customers in their databases, which if crawled can lead to severe instance of data leakage. For extracting such information and other credentials from internet via web crawler, hackers use particular keywords followed by or before target name such as confidential, credit or debit card, private etc.

Generally, about 80% of deep web remains inaccessible by traditional web crawlers [112-113]. In such cases, rival institutions can leverage the availability of ransomware codes or infectious payload over deep web or placed over internet, for lurking infection to their competitor's computers. Likewise if web crawlers can be malformed to index infectious links or unintentionally suffered man-in-the middle attack, where its grabbed link is converted to malicious one by minor changes. This definitely leads to hackers at gain. Though constant monitoring, maintenance and use of META TAG while designing a website [111] proves beneficial in avoiding misuse of crawled links. Till today, web crawlers are not a security concern but will be alarming in future.

(ii)Bogus pop-up message: Some ransomwares behave to be legitimate ones by asking the permission or initiate deployment through users side itself. To solve the purpose, they simply enter into the registry of the system by successfully merging themselves in OS services in such a way that they execute every time system boots and even require no internet connection for triggering. One such adware that comes into notice and quite difficult to remove from system is shown in figure 5.1. This adware usually enters a system with some freeware like registry cleaners and make necessary modifications in windows registry, i.e., HKEY_LOCAL_ so that it starts up with every boot and prompts a fake pop-up message representing a message like "---.dll or -- --.exe file crashes in C:/system32... For further assistance please call (XXX) XXX-XXX or email at :XXXX.EE@XXmail.com". Thus, behaving as a Trojan.



Fig 5.1 An adware

Any unaware or novice will easily get panic regarding something is going wrong in the system. Hence, react to the message and willingly hand-over his/her information and system to hackers who now pave their way to enter your computer system and perform extortion. In case the victim calls on the provided number for assistance, the crooks will make money with every beep while call is active and obtain personal details and other information from sufferer. Successively, this extracted information is sold over darknet for raising funds.

Now again at this stage, it cannot be predicted that the message will finally lead to a ransomware's broke out but, one cannot deny the possibility of bundling such adware with other malware like ransomware payload for remote execution.

(iii) Gathering Credentials: Ransomwares are moving towards maximizing automation and minimizing user intervention. Since as awareness regarding ransomwares is increasing, security solutions even increased their span of network security from gateway security to filtering spam. For addressing such purposes, multiple lines of attack are adopted by cyber crooks, which include a strong combination of brute force attacks, web tracking, adware and spyware that finally lead to intrude a system by taking over admin rights and lastly spread by remote execution (exploiting RDP) (figure 5.2). Moreover, such infected computer can also be transformed into botnet through rootkit approaches and accordingly further increase the span of infection.

While security analyst, use brute force attack to test the flaws in a network of organization as well as to find out password vulnerabilities, hackers use brute force attack to decrypt the locked data stolen from spied computer or hash of passwords. For this reason, it is frequently suggested to use strong passwords comprising of alphanumeric characters and symbols.

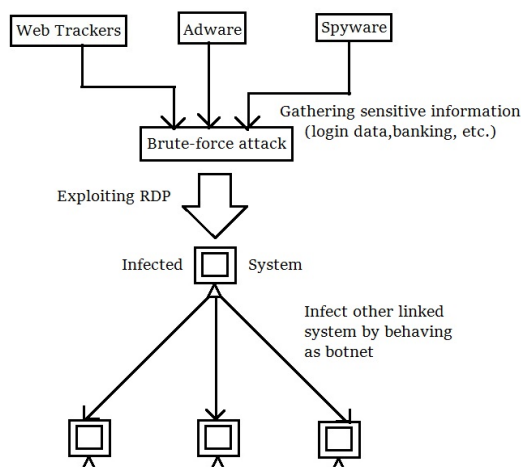


Fig 5.2 Various approaches to attack a system by exploiting RDP



In order to set up a brute force attack, special software is required that choose a best match of username and password from millions of choices. Obtaining the perfect combination requires a lot of computational resources as well as time. In fact complex is the encryption, longer is the time taken to compute the match [114-115]. Its slow success rate is its disadvantage but it is strange that still website hosted by WordPress are most vulnerable to such attacks [115]. For enhancing security, various sites including amazon (an e-commerce site) begins to use captchas that works with a criteria that if three attempts of entering wrong passwords is detected, then that request generating IP address is blocked.

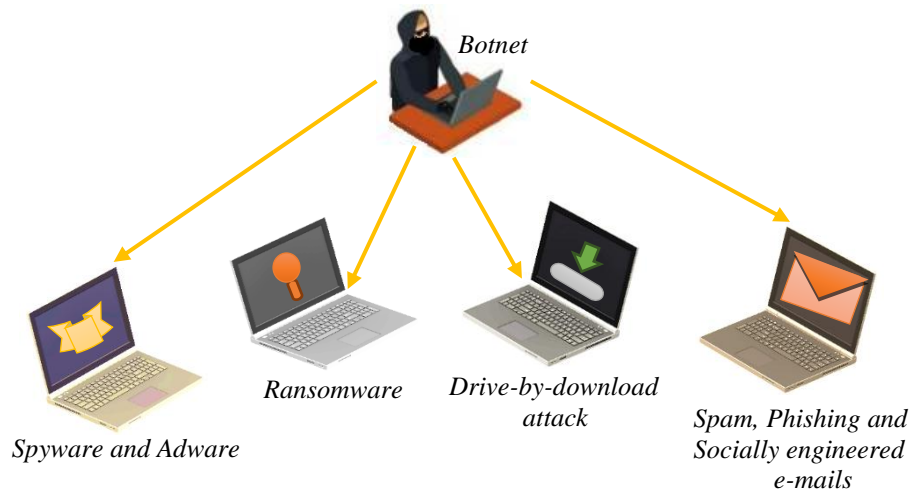


Fig 5.3 A functional botnet

In case of ransomwares, three approaches may be possible:

Firstly, via web tracking, spyware or adware a hacker collects enough information about the target to launch brute force attacks on RDP. Once attacker is successful in exploiting RDP, another low-level process hacking utility is installed on the infected system by taking over full-authorized rights to kill, modify and configure the settings. This concludes with removing volume shadow copies and backups, uploading and executing ransomware.

Secondly, leveraging web trackers to find about probable passwords followed by exploitation of RDP via brute force attack. Once access to computer resources are granted the ransomware bundled with spyware can be installed on the system, which will not only infect the computer but also steal the credentials to sell in dark market or for black mailing the victim.

Thirdly, turning the victim's system into a botnet (figure 5.3) after accessing entry through RDP.

(iv) Alliance with other malwares, pirated applications and automation: The feature of self- propagation is recently visible in WannaCry and Petya [8], but if ransomware employ such features that, they switch to dormant state during detection and can re-propagate thereafter. Then definitely, to reveal the presence of ransomware become nearly an impossible task. It is difficult to know when one's activity is under surveillance or the visit to a particular page is safe or unsafe. If a spyware is employed behind any e-commerce site by escaping its security layer then the stored information and credentials of its customer can be extracted and gathered for ill-use in spam, phishing campaigns, and socially engineered e-mails or in brute-force attacks over RDP.

In aforementioned ransomware attacks, some third-party tools like Mimikatz and Bladabindi spywares, Double Pulsar backdoor, DiskCryptor disk encrypting utility and functions derived from it, are either bundled or



deployed with ransomware payload. Automation and concealing are not new weapons of ransomwares but they begin to shift towards more camouflaging.

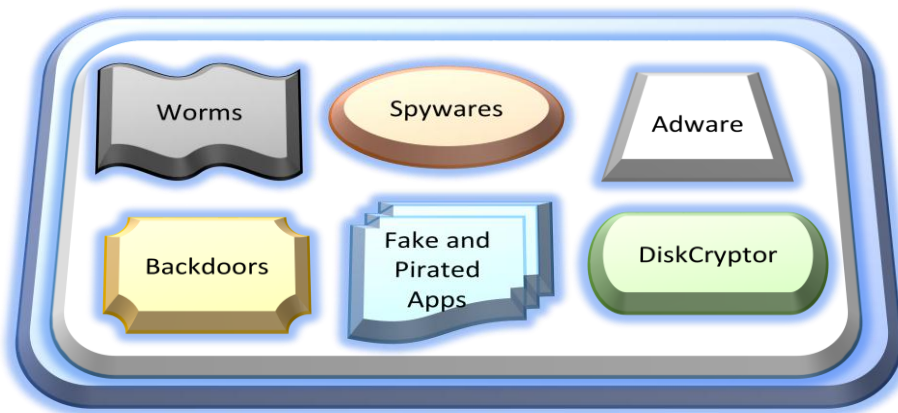


Fig 5.4 Modern ransomware payload

In near future, it is not strange to see such alliance of multiple tools for attacking win platform (figure 5.4). While pirated applications are concerned not only security is at risk but their remains a chance of being infected on every such download and installation. To achieve automation, svchost.exe, PowerShell, WMIC, BITS like services are self-executed by ransomware dropper to download and run the actual payload. Moreover, offline installing of ransoms will tend to growth of DGAs to reach C&C whenever required leading to further automation. Infusing of worm like capability for self-propagation is such another trick that fulfils two aims of attackers, one is to expand the span of infection and secondly more victims means more probability of raising profit. Thus, in days ahead it can also be possible to view modified worms that can also utilize the harvest authorized and sensitive data to bypass firewall and carry over ransomware from one vulnerable node to other to ensure more automation as well as infection.

There exists minor utilities and tools that remain unnoticed to some of the end users but are still present in system to enhance its functionality, Microsoft People is such an app that synchronize phone contacts with Windows Live Mail (Outlook) account. Now, in case due to low security measures if the system was infected, then hacker can access such an application and misuse those numbers to access Aadhar, then bank details and even finger prints in India especially. Hence, the future of ransomware is more troublesome evolved with multiple lines of attacks, embedding multiple payloads (malicious executables) in single yet compressed installer.

5.2. INTER-RELATIONSHIP AMONG MEANS OF DISPERSAL

As visible from recent and nastiest attacks that remain a disaster for victims as well as security analysts, such as Wannacry, Petya, Badrabbitt etc. An attention-grabbing feature possessed by them is a strong co-relationship (figure 5.5) that exists among various distribution strategies of ransomware following multi-level strategy of traps to circulate in such a way that if one is avoided then another will be ready for attack.

It emerges that various infection vectors deployed by ransomware to spread ransomware executable are inter-linked to each other. Consider that the ransomware is if using drive-by-download as prevailing method, which requires injection of malicious content on hijacked website. Then on failure of drive-by-download, exploit kits will continuously disperse more and more times. Bundling of spyware, adware and other malware with ransomware payload, works on drop feature that will prove helpful for an assailant to raise fund by either selling the extracted details over dark net or by blackmailing user of disclosing the obtained details over public network.

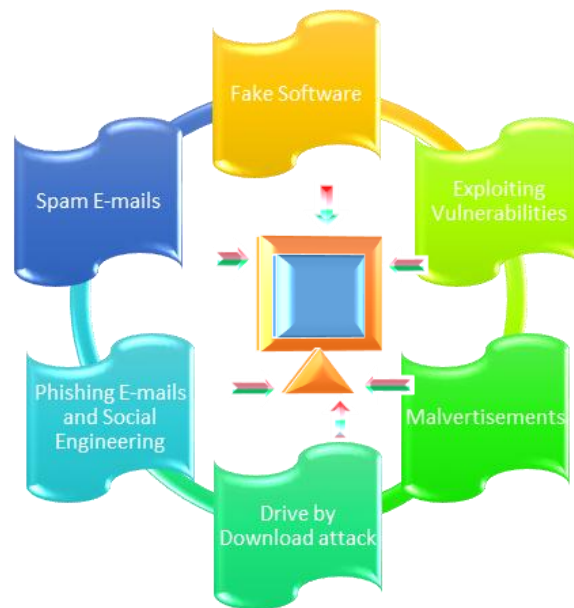


Fig 5.5 Inter-relationship among various distribution methods of a ransomware

The infectious links within the spam, phishing e-mails usually contain ads (figure 5.6) such as You Win a Lottery!!, Expensive iPhone or Branded Mobile, Brand New TV Set, Download a Video Player, etc. that tempts the user to click their links, either scrolling pictures or button like visuals. Once the click is made, they force the user to click further and further over the links and when he/she was busy in clicking links the malicious payload is being downloaded within few seconds to minutes. Their ads are of such an influence since they provide the exact location and information regarding user that an unaware user will definitely get trapped and victimized by estimating it to be real and itself opening the door for frauds or ransomwares leading to loss.

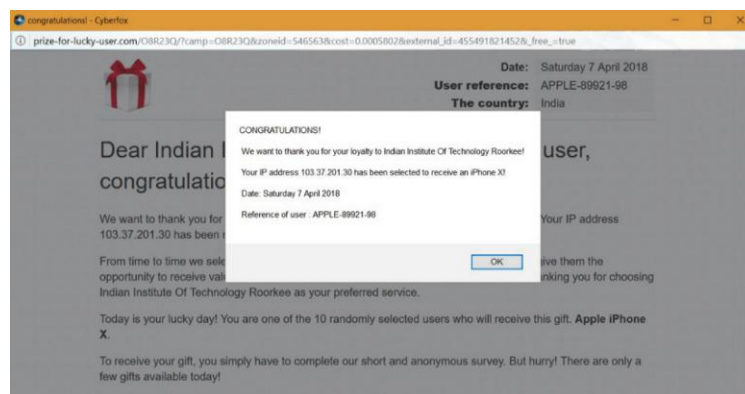


Fig 5.6 Instance of Malvertisement

Fake software tempts user to initiate drive by download attack. The route of this trap begins while a user is accessing internet and suddenly another window of the web-browser opens displaying the message that "Your Adobe Flash is out-of-date. Click Here to update!" or "To run this content you need a Adobe Flash XX.XX.XX.XX." (figure 5.7) which is an active link to the compromised website. Now, as the unaware user clicks on that link a download begins which is actually the malicious code not any genuine software. As a trick, when such malvertisements linked with such fake software are clicked the injected mischievous script redirects the user to the malicious page of exploit kit. Thereafter, it is up to the exploit kits to investigate the system and find any loophole to exploit it as entry point for ransomware.

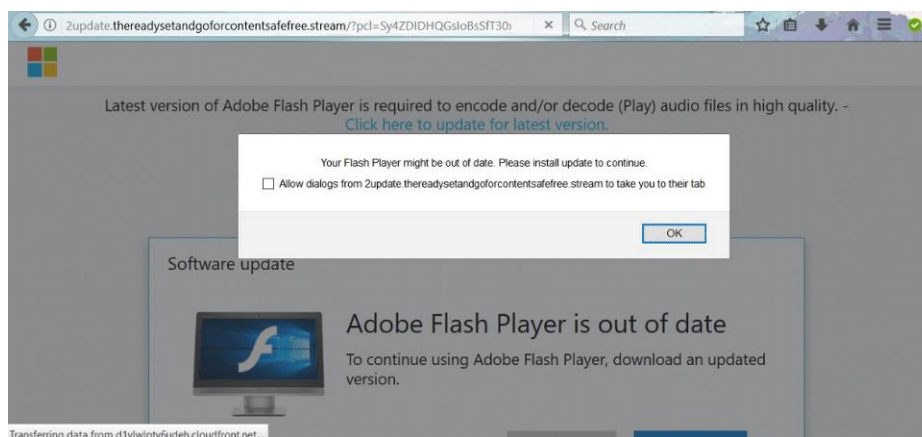


Fig 5.7 Fake software update (Adobe Flash)

Socially engineered e-mails are known for stealing saved addresses (e-mail client's address book) of victim from e-mail client and send itself to other saved e-mails in address book [116]. Nevertheless, Social engineering is closely linked with phishing e-mails and malvertisements, which further connects to exploit kit or again a drive by download attack.

5.3 AWARENESS: THE NEW HORIZONS

Some general measures are provided below that not only ensure multi-tier protection of a system but also minimizes the chances of being tricked and thwart the entry of this digital terrorist into the computer:

(i) Before downloading any software or file perform a check about its source that means whether it downloads executable or that particular file from the same site or jumps to some other one. If they jump to another ambiguous or third party source whereas it is actually available as open source software on its own site like flash, Java Runtime Environment or any web-browser then stop the download immediately and do a proper verification before downloading. One can also scan the downloaded executable or any file format with either purchased security solution or preloaded security keepers as Microsoft Security Essential (in Windows 7) and Windows Defender (in Windows 8, 8.1, 10).

(ii) While checking e-mails keep an eye on the recipient's e-mail id. Consider an example that if a bank person contacts you then why he or she should use gmail or any other anonymous e-mail address rather than the official one that is of the bank. Never respond to such e-mails; whether or not they are a source of ransom, but are definitely fraudulent e-mails.

(iii) Before responding to any legitimate looking e-mail, always inspect whether the particular organization or website is concerned to offer such services or are merely swindles. Either or not it is a ransomware dropper but definitely prevent from frauds like lottery winning.

(iv) As the text suggests, ransomware also drops through malvertisements, thus avoid careless browsing and for more protection and filtered results use pop-up blockers, ad-blockers and link checker plugins compatible with that web browser while surfing on internet.

(v) Have strict and role-based User Access Controls (UAC) and increased firewall restrictions or using limited privileges while using partially updated computers will help in reducing the chance of exploiting the vulnerability [117].

(vi) To protect important documents and images either keep an electronic file vault with extensive security features provided by some subscribed/procured security solutions. Another measure of similar safeguard is by keeping copies of such files at several locations like on e-mail server, on cloud storage and on offline backup



devices. This will provide an additional assurance that if server is under threat then you have files on offline backup and if personal computer is under attack then copies are available on server that can be retrieved in future. Along with it, these offline backups should be regularly updated and tested to assure safe restore in case of an attack. The outdated and stale documents should also be removed from backups for efficient management of available space.

(vii) Do not save credentials or any sensitive information on any website or even on web browser because such information, if leaked or tracked then can be misused in spam and phishing campaigns.

(viii) In case of noticing any suspicious activity on the computer immediately disconnect from the Internet or any other public network.

(ix) Avoid opening doubtful e-mails especially those with .doc or .docm attachment since the latest format extension is .docx and with .js format as it is not a popularly supported format to send any regular content [4,8].

(x) If one remains frequently connected with Internet then keep system up-to-date with latest security patches, operating system updates and other software updates.

(xi) Periodic full system scans as well as network scan should be incorporated in monthly activities to find any crypto-miner, bug, hidden malware or any other vulnerability in the system.

(xii) Do not allow writing permission to every application.

(xiii) Use VPN (Virtual Private Network) while accessing your desktop from unsafe network. Keep Microsoft Remote Desktop utility (figure 5.8) off when not needed.



Fig 5.8 Remote Desktop Feature in windows 10

(xiv) Use spam-filters and e-mail security solutions, to control junk mails.

(xv) Block/Uninstall unwanted IP addresses, DHCP clients and other non-compatible applications running on PC.

(xvi) In organizations, divide access rules into different departmental zones in order to have an extra layer of protection and avoid any chance of mishappening by manmade mistake [40].

(xvii) In case on any prompt appeared on the screen, carefully examine its publisher and other details before granting it any access rights.

(xviii) Set property to display extension as well as hidden files to discover any abnormal activity and extension in win explorer (figure 5.9).

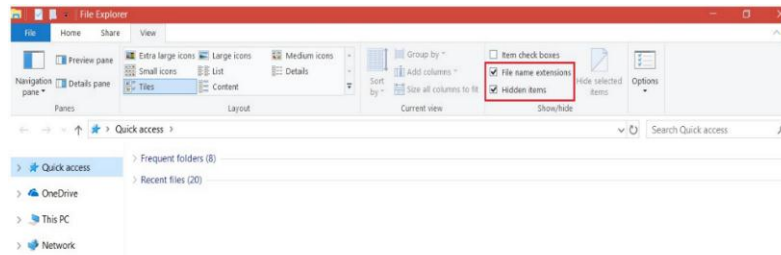


Fig 5.9 Windows Explorer

(xix) Server security should also be concerned.

(xx) Awareness campaign by various security-serving firms should be launched to teach people regarding the latest threats and importance of data safety and privacy.

REFERENCES

- [1] A. H. Weis, "Commercialization of the Internet", Internet Research 20 (4) 2010, 420-435.
- [2] G. Owen, N. Savage, "The Tor Dark Net", Global Commission on Internet Governance Paper Series No. 20, Sept 2015, 1-20.
- [3] F. Wehinger, "The Dark Net: Self-Regulation Dynamics of Illegal Online Markets for Identities and Related Services", European Intelligence & Security Informatics Conference, IEEE Computer Society, 2011, 209-213.
- [4] A. Liska, T. Gallo, "Ransomware: Defending against digital extortion", O'Reilly Media, November 2016, ISBN: 9781491967881, 190 pages.
- [5] K. Cabaj, M. Gregorczyk, W. Mazurczyk, "Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics", Computers & Electrical Engineering 66 (2018), 353-68.
- [6] S. I. Popoola, U. B. Iyekekpolo, S. O. Ojewande, F. O. Sweetwilliams, S. N. John, "Ransomware: Current Trend, Challenges and Research Directions", WCECS 1 (2017), 0958-66.
- [7] X. Luo, Q. Liao, "Awareness Education as the key to Ransomware prevention", Information System Security, 16(2007), 195-22.
- [8] K. Savage, P. Coogan, H. Lau, "The evolution of ransomware", Symantec Security Response (2015).
- [9] B. Rajesh, Y.R.J. Reddy, B.D.K. Reddy, "A Survey Paper on Malicious Computer Worms", IJARCST 3(2) 2015, 161-167.
- [10] N. Milošević, "History of Malware", Computer Security, 2014, 1-11.
<https://arxiv.org/ftp/arxiv/papers/1302/1302.5392.pdf>
- [11] M. Khari, C. Bajaj, "Detecting Computer Viruses", IJARCET 3(7) 2014, 2357-64.
- [12] I. You, K. Yim, "Malware Obfuscation Technique: A brief Survey", International Conference on Broadband, Wireless Computing, Communication and Application", IEEE 2010, 297-300.
- [13] H. U. Salvi, R.V. Kerkar, "Ransomware: A Cyber Extortion", Asian Journal of Convergence in Technology 2(3), 2016.



- [14] A. Gazet, "Comparative Analysis of Ransomware Virii", J. Computer Virology, 6(2010), 77-90.
- [15] P.B. Pathak, "A Dangerous Trend of Cybercrime: Ransomware Growing Challenge", IJARCET 5(2), (2016), 371-373.
- [16] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Whitepaper 2008, bitcoin.org
- [17] C. Telly, "A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency", Small Wars Journal, Jan 15, 2018. <http://smallwarsjournal.com/jrnl/art/coin-tsar-two-disruptive-sides-cryptocurrency/>
- [18] D. Stroukal, B. Nedvedova, "Bitcoin and Other Cryptocurrency as an Instrument of Crime in Cyberspace", 4th Business and Management Conference (Istanbul), Oct 12, 2016, 219-226.
- [19] G. F. Hurlburt, I. Bojanova, "Bitcoin: Benefit or Curse?", IT Trends (IEEE), 2014, 10-15.
- [20] K. Hegadekatti, "Regulating the Deep Web Through Controlled Blockchains and Cryptocurrency Networks", SSRN, 2016, 1-10.
- [21] M. Rutnik, "What is Cryptocurrency?", Feature: Android Authority (Online), Feb 25, 2018. <https://www.androidauthority.com/what-is-cryptocurrency-805162/>
- [22] "Rupee vs dollar: From 1990 to 2013", Business (Rediff.com), Jun 12, 2013. <http://www.rediff.com/money/slide-show/slide-show-1-rupee-vs-dollar-from-1990-to-2013/20130612.htm>
- [23] B. Lokuketagoda, M. Weerakoon, U. Madhushan, A.N. Senaratne, K.Y. Abeywardena, "R-Killer: An Email Based Ransomware Protection Tool", World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering 12 (2), 2018, 200-206.
- [24] J. Huang, J. Xu, X. Xing, P. Liu, M. K. Qureshi, "FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware", Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (2017), 2231- 44.
- [25] L. Invernizzi, P.M. Comparetti, "EVILSEED: A Guided Approach to Finding Malicious Web Pages", IEEE Symposium on Security and Privacy 2012, 428-442.
- [26] <https://www.cryptodrop.org/how-it-works.php>
- [27] P. Muncaster, "CryptoDrop Tool Spots and Stops Ransomware in its Tracks", News: InfoSecurity Magazine, Jul 14, 2016. <https://www.infosecurity-magazine.com/news/cryptodrop-spots-stops-ransomware/>
- [28] N. Scaife, H. Carter, P. Traynor, K.R.B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data", IEEE 36th International Conference on Distributed Computing Systems", 2016, 303-12.
- [29] A. Kharraz, E. Kirda, "Redemption: Real-time Protection Against Ransomware at End-Hosts" International Symposium on Research in Attacks, Intrusions, and Defenses (2017), 98-119.
- [30] N. Hachem, Y.B. Mustapha, G.G. Granadillo, H. Debar, "Botnets: Lifecycle and Taxonomy", Conference on Network and Information Systems Security (SAR-SSI) IEEE, 2011, 1-8.
- [31] B. Thuraisingham, L. Khan, M.M. Masud, K. W. Hamlen, "Data Mining for Security Applications", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (2008), 585-89.
- [32] A. Bhardwaj, V. Avasthi, H. Sastry, G.V.B. Subrahmanyam, "Ransomware Digital Extortion: A Rising New Age Threat", IJST 9(14), April 2016, 1-5.



- [33] P. Mahajan & A. Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology 13 (15) 2013, 15-22.
- [34] A. A. Hasib, A.A.M.M. Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography" 3rd International Conference on Convergence and Hybrid Information Technology (2008) IEEE, 505- 510.
- [35] Exabeam, "The Anatomy of a Ransomware Attack", White Paper (Threat Research Report) 2016, 1-13.
- [36] R. Leong, "Understanding Ransomware and Strategies to Defeat it", White Paper (McAfee Labs), 1-16.
- [37] F-Secure, "Ransomware: How to predict, prevent, detect & respond", White Paper (Threat Response), Nov 2016,1-11.
- [38] S.S. Ganorkar, K. Kandasamy, "Understanding and Defending Crypto-Ransomware", ARPN Journal of Engineering and Applied Sciences 12 (12) 2017, 3920-25.
- [39] Deloitte, "Ransomware Holding Your Data Hostage", Threat Study, Aug 12, 2016, 1-23.
- [40] M. Fimin, "Are employees part of the ransomware problem?", Computer Fraud & Security, Aug 2017, 15-17.
- [41] V.L.Le, I. Welch, X. Gao, P. Komisarczuk, "Anatomy of Drive-by Download Attack", Proceedings of the Eleventh Australian Information Security Conference 2013, 49-58.
- [42] UNB, "Spam vs Phishing Emails...what's the difference?", Blog: UNB tidBiTS, 2012. <https://blogs.unb.ca/tidbits/2012/01/11/spam-vs-phishing-emails%E2%80%A6-what%E2%80%99s-the-difference/>
- [43] R. Brewer, "Ransomware attacks: detection, prevention and cure", Network Security, September 2016, 5-9.
- [44] K.A. Gandhi, V. K. D. Patel, "Survey on Ransomware: A New Era of Cyber Attack", International Journal of Computer Application 168 (3), 2017, 38-41.
- [45] D. Kansagra, M. Kumhar, D.Jha, "Ransomware: A Threat to Cyber Security", IJCSC 7(1), Sept 2015-Mar 2016, 224-27.
- [46] J. Sumalapao, "New Crypto-Ransomware JIGSAW Plays Nasty Games", Blog: Trend Micro, Apr 19, 2016. <http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-ransomware-plays-games-victims/>
- [47] A. Perekalin, "Bad Rabbit: A new ransomware epidemic is on the rise", Blog: Kaspersky Labs, Oct 24, 2017. <https://www.kaspersky.com/blog/bad-rabbit-ransomware/19887/>
- [48] A. Greenberg, "New Ransomware Linked to NotPetya Sweeps Russia and Ukraine", Wired-Security, Oct 24, 2017; <https://www.wired.com/story/badrabbit-ransomware-notpetya-russia-ukraine/>
- [49] M. Kumar, "Bad Rabbit: New Ransomware attack Rapidly Spreading Across Europe", The Hackers News, Oct 24, 2017; <https://thehackernews.com/2017/10/bad-rabbit-ransomware-attack.html>
- [50] O. Mamedov, F. Sinitsyn, A. Ivanov, "Bad Rabbit Ransomware", Blog: Secure List, Oct 24, 2017; <https://securelist.com/bad-rabbit-ransomware/82851/>
- [51] <https://freecurrencyrates.com/en/exchange-rate-history/BTC-INR/>



- [52] CERT-MU, "The WannaCry Ransomware: Whitepaper", May 2017.
- [53] S. Mohurle, M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017", IJARCS 8(5), 2017, 1938-40.
- [54] Symantec Security Response, "What you need to know about WannaCry Ransomware?", Blog: Symantec Official, May 2017.
- [55] Symantec Security Response, "WannaCry: Ransomware attacks show strong links to Lazarus group", Blog: Security Response Symantec Official, May 2017. <https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group>
- [56] <https://www.poundsterlinglive.com/best-exchange-rates/best-us-dollar-to-indian-rupee-history/>
- [57] C. Cimpanu, "Petya Ransomware Returns with GoldenEye Version, Continuing James Bond Theme", Blog: Bleeping Computer (Security), Dec 06, 2016. <https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/>
- [58] "PETYA and Mischa: Ransomware Twins Spell Double the Trouble", Blog: Trend Micro (Security News), May 13, 2016. <https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/petya-and-mischa-ransomware-twins-double-trouble>
- [59] L. Abrams, "Petya is back and with a friend named Mischa Ransomware", Blog: Bleeping computer (Security News), May 12, 2016. <https://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/>
- [60] T. F. Brewster, "Petya or Not Petya: Why the latest ransomware is deadlier than wannacry", Blog: Forbes (Cyber Security), Jun 27, 2017. <https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/#24f0afcf532e>
- [61] Symantec Security Response, "Petya Ransomware Outbreak: Here's what you need to know", Blog: Symantec Threat Intelligence, Oct 24, 2017. <https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know>
- [62] A. Hern, "Ransomware attack 'not designed to make money', researchers claim", Blog: The Guardian (Technology), June 28, 2017. <https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia>
- [63] Solon, A. Hern, "'Petya' ransomware attack: what is it and how can it be stopped?" Blog: The Guardian (Technology), June 28, 2017. <https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how>
- [64] GReAT, "Schroedinger's Pet(ya)", Blog: Securelist, Jun 27, 2017. <https://securelist.com/schroedingers-petya/78870/>
- [65] "Locky Ransomware Information, Help Guide, and FAQ", Blog: Bleeping Computer, May 09, 2016. <https://www.bleepingcomputer.com/virus-removal/locky-ransomware-information-help>
- [66] Threat intelligence Team, "Zepto ransomware now introduces new features to better encrypt your files", Blog: Avast Threat Research, Sept 08, 2016. <https://blog.avast.com/zepto-ransomware-now-introduces-new-features-to-better-encrypt-your-files>



- [67] E. Kovacs, "Decryption Tools Released for Bart, PowerWare Ransomware", Blog: Security Week, July 22, 2016. <https://www.securityweek.com/decryption-tools-released-bart-powerware-ransomware>
- [68] L. Abrams, "Bart Ransomware being Spammed by the same devs behind Locky", Blog: Security News (Bleeping Computer) June 27, 2016. <https://www.bleepingcomputer.com/news/security/bart-ransomware-being-spammed-by-the-same-devs-behind-locky/>
- [69] V. Krustev, "Remove Bart Ransomware and Restore .bart.zip Files", Blog: Sensor Tech Forums, June 27, 2016. <https://sensoretechforum.com/remove-bart-ransomware-restore-bart-zip-files/>
- [70] Quick Heal Security Labs, "Ransomware Alert! ODIN – A new variant of Locky Ransomware", Blog: Quick Heal, September 30, 2016. <http://blogs.quickheal.com/ransomware-alert-odin-a-new-variant-of-locky-ransomware/>
- [71] L. Abrams, "Locky Ransomware's new .SHIT Extension shows that you can't Polish a Turd", Blog: Security News (Bleeping Computer), Oct 24, 2016. <https://www.bleepingcomputer.com/news/security/locky-ransomwares-new-shit-extension-shows-that-you-cant-polish-a-turd/>
- [72] L. Abrams, "Locky Ransomware switches to THOR Extension after being a Bad Malware", Blog: Security News (Bleeping Computer), October 25, 2016. <https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-thor-extension-after-being-a-bad-malware/>
- [73] B. Bilbao, ".thor Files Virus – Remove Locky's Latest Strain", Blog: Sensor Tech Forums, October 25, 2016. <https://sensoretechforum.com/thor-files-virus-remove-lockys-latest-strain/>
- [74] V. Krustev, "The .Thor Variant of Locky Virus" Latest Security News (TripWire), October 25, 2016. <https://www.tripwire.com/state-of-security/latest-security-news/thor-variant-locky-virus/>
- [75] L. Abrams, "Locky Ransomware now using the Aesir Extension for Encrypted Files", Blog: Security News (Bleeping Computer), November 21, 2016. <https://www.bleepingcomputer.com/news/security/locky-ransomware-now-using-the-aesir-extension-for-encrypted-files/>
- [76] D. Sadakov, ".ZZZZZ Ransomware is yet another Locky Variant", Latest Security News (TripWire), November 25, 2016. <https://www.tripwire.com/state-of-security/latest-security-news/zzzzz-ransomware-yet-another-locky-variant/>
- [77] Acronis Security Team, "Osiris Ransomware: New Addition to the Locky Family", Blog: Acronis, Jan 31, 2017. <https://www.acronis.com/en-us/blog/posts/osiris-ransomware-new-addition-locky-family>
- [78] C. Chimpanu, "Locky Ransomware Returns, but Targets Only Windows XP & Vista", Blog: Security News (Bleeping Computer), June 22, 2017. <https://www.bleepingcomputer.com/news/security/locky-ransomware-returns-but-targets-only-windows-xp-and-vista/>
- [79] M. Rivero, "Locky ransomware returns to the game with two new flavors", Blog: MalwareBytes, Aug 25, 2017. <https://blog.malwarebytes.com/cybercrime/2017/08/locky-ransomware-returns-to-the-game-with-two-new-flavors/>
- [80] T. Hux, "Locky Ransomware Makes a comeback with new .diablo6 and .lukitus variants", Blog: McAfee, Aug 28, 2017. <https://securingtomorrow.mcafee.com/business/locky-ransomware-makes-comeback-new-diablo6-lukitus-variants/>
- [81] S. Pilici, "How to remove Lukitus Virus (Locky Ransomware Removal)", Blog: Malware Tips, Aug 17, 2017. <https://malwaretips.com/blogs/remove-lukitus-ransomware/>



- [82] R. Abel, "Ykcol and Asasin Locky variants released within short time frame", Blog: Cybercrime (SC Media US), Oct 13, 2017. <https://www.scmagazine.com/two-new-locky-variants-released-within-a-month-of-each-other/article/700229/>
- [83] Symantec, "Jigsaw ransomware wants to play a game, but not in a good way", <https://us.norton.com/internetsecurity-emerging-threats-jigsaw-ransomware-wants-to-play-a-game-but-not-in-a-good-way.html>
- [84] L. Abrams, "Jigsaw Ransomware Decrypted: Will delete your files until you pay the Ransom", Apr 11, 2016. <https://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/>
- [85] Symantec Security Response, "Samsam may signal a new trend of targeted ransomware", Blog: Symantec Official, Apr 05, 2016. <https://www.symantec.com/connect/blogs/samsam-may-signal-new-trend-targeted-ransomware>
- [86] P. Paganini, "Why malware like the Samsam ransomware are so dangerous for hospitals?", Blog: Security Affairs, Apr 04, 2016. <http://securityaffairs.co/wordpress/45974/malware/samsam-ransomware.html>
- [87] C. Osborne, "SamSam ransomware now demands \$33,000 from victims", Blog: ZeroDay, Jun 26, 2017. <http://www.zdnet.com/article/samsam-ransomware-now-demands-33000-from-victims/>
- [88] J. Hitchcock, "SamSam Ransomware", Blog: Alert Logic Security Research, Sept 23, 2016. <https://www.alertlogic.com/blog/samsam-ransomware/>
- [89] C. Doman, "SamSam Ransomware Targeted Attacks Continue", Blog: Alien Vault, Jun 21, 2017. <https://www.alienvault.com/blogs/labs-research/samsam-ransomware-targeted-attacks-continue/>
- [90] Cisco Talos, "SamSam: The Doctor Will See You, After He Pays The Ransom", Blog: Talos Intelligence, Mar 23, 2016. <http://blog.talosintelligence.com/2016/03/samsam-ransomware.html>
- [91] Trend Micro, "Crysis Ransomware Gaining Foothold, Sets sights to Take Over TelsaCrypt", Blog: Cyber Crime & Digital Threats, Jun 08, 2016. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crysis-to-take-over-teslacrypt>
- [92] D. Perez, "New Decryption Tool for Crysis ransomware", Blog: We Live Security (ESET), Nov 24, 2016. <https://www.welivesecurity.com/2016/11/24/new-decryption-tool-crysis-ransomware/>
- [93] J. Oliver, "A Show of (Brute) Force: Crysis Ransomware Found Targeting Australian and New Zealand Businesses", Blog: Trend Micro (Ransomware), Sept 19, 2016. <http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/>
- [94] L. Abrams, "New Arena Crysis Ransomware Variant Released", Blog: Bleeping Computer, Aug 25, 2017. <https://www.bleepingcomputer.com/news/security/new-arena-crysis-ransomware-variant-released/>
- [95] J. Doevan, "Dharma ransomware virus. How to remove?", Blog: SpyWare, Dec 14, 2017, <https://www.2-spyware.com/remove-dharma-ransomware-virus.html>
- [96] S. Hilt and F. Mercês, "HDDCryptor: Subtle Updates, Still a Credible Threat", Blog: Trend Micro, Nov 30, 2016. https://blog.trendmicro.com/trendlabs-security-intelligence/hddcryptor-updates-still-credible-threat/?_ga=2.254994376.1189804836.1515322718-1117916802.1515322718



- [97] M. Mimoso, "Mamba Ransomware Resurfaces in Brazil, Saudi Arabia", Blog: Threat Post, Aug 09, 2017. <https://threatpost.com/mamba-ransomware-resurfaces-in-brazil-saudi-arabia/127325/>
- [98] Trend Micro, "Disk-Locking HDDCryptor/Mamba Ransomware Makes a Comeback" Blog: CyberCrime & Digital Threats, Aug 13, 2017. <https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/disk-locking-hddcryptor-mamba-ransomware-makes-a-comeback>
- [99] A. Ivanov, O. Mamedov, "The return of Mamba ransomware", Blog: Securelist, Aug 09, 2017. <https://securelist.com/the-return-of-mamba-ransomware/79403/>
- [100] H. Mascarenhas, "Mamba ransomware that crippled San Francisco's transit system reappears in Brazil, Saudi Arabia", Blog: IB Times, Aug 10, 2017. <http://www.ibtimes.co.uk/mamba-ransomware-that-crippled-san-franciscos-transit-system-reappears-brazil-saudi-arabia-1634381>
- [101] P. Ducklin, "Mamba ransomware strikes at your whole disk, not just your files", Blog: Naked Security (Sophos Lab), Sept 27, 2016. <https://nakedsecurity.sophos.com/2016/09/27/mamba-ransomware-strikes-at-your-whole-disk-not-just-your-files/>
- [102] NCN News Network, "WARNING: MAMBA or HDDCryptor Ransomware is back in India", News: National Computrade, Aug 17, 2017. <http://ncnonline.net/nss/warning-mamba-or-hddcryptor-ransomware-is-back-in-india.html>
- [103] B. Griffin, "In the Shadow of WannaCry, Jaff Ransomware Arrives Using Familiar Phishing Techniques", Blog: Malware Analysis, Phishing, Ransomware (Phish me), May 16, 2017. <https://phishme.com/shadow-wannacry-jaff-ransomware-arrives-using-familiar-phishing-techniques/>
- [104] S. Khandelwal, "Jaff Ransomware Decryption Tool Released – Don't Pay, Unlock Files for Free", Blog: The Hacker News, Jun 14, 2017. <https://thehackernews.com/2017/06/jaff-ransomware-decryption-tool.html>
- [105] Checkpoint research team, "JAFF – A New Ransomware is in town, and it's widely spread by the infamous Necurs Botnet", Blog: Checkpoint, May 11, 2017. <https://blog.checkpoint.com/2017/05/11/jaff-new-ransomware-town-widely-spread-infamous-necurs-botnet/>
- [106] Check Point Research Team, "Anatomy of the Jaff Ransomware Campaign", Blog: Check Point, Jun 08, 2017. <https://blog.checkpoint.com/2017/06/08/jaff-ransomware/>
- [107] Quick Heal Security Labs, "PDF files with embedded docm files now deliver Jaff Ransomware", Blog: Quick Heal, May 23, 2017. <http://blogs.quickheal.com/pdf-files-embedded-docm-files-now-deliver-jaff-ransomware/>
- [108] T.Seals, "Jaff Ransomware Targets Millions, While vCrypt1 Attacks on the Cheap", News: Info Security Magazine, May 12, 2017. <https://www.infosecurity-magazine.com/news/jaff-ransomware-targets-millions/>
- [109] L. Abrams, "Jaff Ransomware switches to the .sVn Extension", Blog: Bleeping Computer, Jun 9, 2017. <https://www.bleepingcomputer.com/news/security/jaff-ransomware-switches-to-the-svn-extension/>
- [110] D. Palmer, "Jaff ransomware demanding \$4,000 to unlock your files? Now you can get them back for free", Blog: Security ZDNet, June 15, 2017. <http://www.zdnet.com/article/jaff-ransomware-demanding-4000-to-unlock-your-files-now-you-can-get-them-back-for-free/>
- [111] R. Ford, "Googling for Gold: Web Crawlers, Hacking and Defense Explained", Network Security 2004 (1) 2004, 10-13.



- [112] S. M. Mitraheri, M.E. Dinçtürk, S. Hooshmand, G.V. Bochmann, G. Jourdan, "A Brief History of Web Crawlers", Proceedings of Conference of the Center for Advanced Studies on Collaborative Research (2013), 40-54.
- [113] S. Dhenakaran, K. T. Sambanthan, "Web Crawler-An Overview", IJCSC 2 (1) 2011, 265-67.
- [114] P. Shankdhar, "Popular Tools for Brute-force Attacks", Blog: Hacking (InfoSec Institute), May 29, 2017. <http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref>
- [115] D. Magestro, "What is a Brute Force Attack?", Blog: Stack Path. <https://blog.stackpath.com/glossary/brute-force-attack/>
- [116] C. Everett, "Social engineering emails get more Devious", Network Security 2004 (1) 2004, 1.
- [117] S. Parkinson, "Use of access control to minimize ransomware impact", Network Security, Jul 2017, 5-8.