International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Emerging Threats of 2017: Ransomware, IOC's

Pradeep Bihola*, Ravi Sheth
Department of IT & Telecommunication, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

In this present era of the internet the cybersecurity has became an immense part of the world and as the continue to expand ransomware is becoming number one peril. Primary motivation of the ransomware is financial gain. Unlike malware that allows the hacker or criminals to pilfer valuable data of the user ransomware attacks directly on owner's data by keeping the computer file's locked until ransom is paid. The startling sophistication of ransomware marks the model shifting cyber ecosystem. In this review paper an overview of malware and ransomware, different types of ransomware, different types of techniques ransomware emerging in 2017, top ransomwares of 2017 with its countermeasures in details and their IOC's are reviewed.

Keywords: Malware, Ransomware, Top Threats of 2017, Ransomware IOC's.

I. INTRODUCTION

What if, all of a sudden, the files on your mobile or computer became unusable? Every picture, financial document, music file, video file-you name it-essentially disappeared or encrypted or useless. How did that happen? What did you do to deserve this?
Welcome to the world of malware.
If you download pirated software online rather than pay for the genuine version. You are welcoming the ransomware in your machine just by opening an email attachment or clicking on a link given in email without thinking. Cybercriminals use these tricks to spread malicious code, or malware to their victims.

And among the various types of malware there is ransomware getting more spotlight recently due to its high impact on economy of various countries.

In old days, people gathered information from the system which is used for crime like identity theft. Now days are changed cybercriminal became more aggressive they hold victims device and data as hostage and demand the ransom this type of attack is known as ransomware.

II. RANSOMWARE

What is ransomware?

Ransomware is a type of a malware which restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) in order to remove the restrictions.

How does ransomware work?
If you download pirated software online rather than pay for the genuine version. Opening an email attachment or clicking on a link in an email without thinking will infected your computer, the ransomware encrypts files and documents and then demands a ransom virtual currency, to unlock the files using digital key. If you won't keep backup of your files then either you have to pay ransom or forget about data.

The basics of ransomwares:
Ransomware is a type of malware designed to hijack computers and force victims to pay ransoms to have their files decrypted. Hackers infect your computer by prompting you to download a malicious email attachment or visit a code-carrying website, which ultimately encrypts your critical files or denies access to your computer. Two main forms of this malware are currently popular:

A. Crypto ransomware:

The goal of crypto ransomware is to encrypt your critical data, like pictures, videos or documents while leaving more basic computer functions untouched. This generates a sense of panic, because you can see your

files, but you can't access them. Crypto creators often include a countdown in their ransom demand: If you don't pay by the deadline, all your files will be deleted. With many users unaware of the need to make multiple file backups across cloud and physical storage devices, crypto ransomware can be devastating and lead many victims to pay the ransom in the hopes of getting back their digital assets. Examples include CryptoLocker, Locky, CrytpoWall and more.

B. Locker ransomware:

This type of malware locks users out of basic computer functions. For example, you can be denied access your desktop, while your mouse and keyboard functions can be partially disabled. You'd still be able to interact with the ransom demand to make payment, but otherwise your computer would become essentially useless. The good news is locker malware typically avoids encrypting critical files in favor of simply locking you out, meaning there's less chance of total data destruction. Examples include the police-themed ransomware or Winlocker.

The first modern ransom malware emerged in 2005 with Trojan.Gpcoder. In 2015, more than 58 percent of corporate PCs were attacked with malware, and cryptolocker attacks doubled, according to Kaspersky Labs. Locker ransomware made up approximately 20 percent of ransomware.

Up to 2017 saw a number of new ransom malware types emerge:

Linux Server threats: Several web security firms discovered Linux malware designed to lock out Web administrators from Linux servers and prevent them from accessing necessary website support functions. While a predictable encryption key workaround was discovered, new variants of the malware appeared, and they didn't respond to the decryption tool. Hackers were asking for one Bitcoin to release critical files.

Cryptowall 4.0: A new version of the popular Windows-based CryptoLocker is now being distributed via the Nuclear Exploit kit, according to Threat post.
The major change in 4.0 is that it now encrypts file names along with data in an effort to further obfuscate its processes and make it more tough for victims to recover information without paying.

TeslaCrypt: This Cryptowall competitor also released a new version in 2015. Security firms tracked a massive spam campaign delivering this malware through infected email attachments that claim to be overdue invoices.

Locker: In summer 2015, locker ransomware lay dormant until May 25 when it activated, locked files and demanded a 0.1 Bitcoin ransom, which increased to 1 Bitcoin after 72 hours.
Oddly enough, after less than a week, malware creator "Poka Bright Minds" made a Pastebin apology and decrypted all infected computers. Any Bitcoins paid were not returned.

Android Malware: Mobile ransom malware has yet to reach the same volumes as its PC-based counterparts, but 2015 saw a significant rise in ransom code across Android devices.

A variant of Android malware denied users access to their devices and claimed users had been illegally viewing adult content. The cost of freedom? $500 in a MoneyPak voucher.

The Future of Digital Extortion

This year certainly won't be the last for ransomware, so what does the future hold for digital extortion? According to me, this are a few likely scenarios. Vehicle-based ransom malware is one option, since researchers have already demonstrated that it's possible to hijack and take total control of a moving vehicle. Smart home technology, such as security cameras, door locks and thermostats are also a possible avenue, because these devices require Wi-Fi and many are poorly secured against brute-force attacks. There's also the risk of health-based ransomware, which targets devices such as pacemakers, implants or health monitors. The burgeoning Internet of Things (IoT) offers a host of connective possibilities and is short on security standards.

Ransom malware is here to stay. Its form and targets may change, but the method is tried and true. If you're infected, try not to panic: Look for help online, don't pay up, and consider the use of real-time security protection moving forward to help detect and quarantine ransom threats before they lock you out.

III. EXAMPLES

The top 10 worst ransomware attacks of 2017 (Ref:1)

1) **NotPetya**: NotPetya is starting as a fake Ukrainian tax software update, NotPetya infected hundreds of thousands of computers in more than 100 countries within just a few days. This ransomware is a variant of an older attack dubbed Petya, except this time the attack uses the same exploit behind WannaCry.
2) **WannaCry**: WannaCry was the first to use EternalBlue, which exploits a vulnerability in Microsoft's Server Message Block (SMB) protocol.
3) **Locky**: 2016's most popular ransomware is alive and well in 2017. New variants of Locky, called Diablo and Lukitus, surfaced this year, using the same the phishing email attack vector to initiate their exploits.
4) **CrySis**: CrySis is the king of Remote Desktop Protocol (RDP) compromise started last year in Australia and New Zealand. Remote Desktop Protocol is one of the most common ways to deploy ransomware because cybercriminals can compromise administrators and systems that control entire organizations.
5) **Nemucod:** Nemucod arriving in the form of a phishing email that looks like a shipping invoice, it's downloads malware and encryption components stored on compromised websites. Nemucod would have been the most malicious phishing email if Locky hadn't reignited in August. The Nemucod ransomware family has been active since at least 2015.
6) **Jaff**: Jaff arose in May 2017, and heavily mimics tactics used by Locky. It uses the Necurs botnet to send millions of spam emails to targets globally over just a few hours, and demands victims pay 1.79 Bitcoins—currently more than $6,000. Similar to Locky, new variants of Jaff ransomware continue to leverage phishing emails and embody characteristics associated with other successful malware.
7) **Spora**: Cybercriminals hack legitimate websites to add JavaScript code to distribute this ransomware. Then, a pop-up alert prompts user to update their Chrome internet browsers to continue viewing the webpage. Once users follow the "Chrome Font Pack" download instructions, they become infected.
8) **Cerber**: One of the multiple attack vectors Cerber utilizes is called RaaS (RaaS means ransomware-as-a-service). Through this "service," cybercriminals package up ransomware and then give other criminals the tools to distribute how they see fit.
9) **Cryptomix**: This ransomware is one of the few that does not have a type of payment portal available on the dark web. Instead, users have to wait for the cybercriminals to email them instructions to pay a heavy amount in Bitcoin.
10) **Jigsaw**: Another carryover from 2016, Jigsaw embeds an image of the clown from the "Saw" movies into a spam email. Once a user clicks, the ransomware not only encrypts files, but it also deletes files if a user takes too long to make the ransom payment of $150.

IV. WANNACRY RANSOMWARE: (REF:2)

Sign: WannaCrypt, WanaCrypt0r 2.0, WCry, WCrypt, and Wanna Decryptor
Damage Level: High, May 12, 2017
Attack vector: EternalBlue Server Message Block (SMB) Exploit Kit
Destruction Zone: 150+ Countries, attacked Britain's health service and companies in Spain, Russia, the Ukraine and Taiwan
Inception: March 2017 but attacked in May 2017
Ransom: $300-$600
Method of Propagation:
There are two scenarios that are highly possible explanations for the spread of this ransomware:

- ✓ Arrival through social engineering emails designed to trick users to run the malware and activate the worm-spreading functionality with the SMB exploit.
- ✓ Infection through SMB exploit when an unpatched computer is addressable from other infected machines.

Dropper:
The threat arrives as a dropper Trojan that has the following two components:

1. A component that attempts to exploit the SMB CVE-2017-0145 vulnerability in other computers
2. The ransomware known as WannaCrypt

The dropper tries to connect the following domains using the *API InternetOpenUrlA()*:

- ✓ www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- ✓ www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- ✓ www[x].iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]test

If connection to the domains is successful, the dropper does not infect the system further with ransomware or try to exploit other systems to spread; it simply stops execution. However, if the connection fails, the threat proceeds to drop the ransomware and creates a service on the system.

WannaCrypt ransomware

The ransomware component is a dropper that contains a password-protected .zip archive in its resource section. The document encryption routine and the files in the .zip archive contain support tools, a decryption tool, and the ransom message.
When run, WannaCrypt creates the following registry keys:

- ✓ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\<random string> = "<malware working directory>\tasksche.exe"
- ✓ HKLM\SOFTWARE\WanaCrypt0r\\wd = "<malware working directory>"

It changes the wallpaper to a ransom message by modifying the following registry key:

- ✓ HKCU \ Control Panel\Desktop\Wallpaper: "<malware working directory>\@WanaDecryptor@.bmp"

It creates the following files in the malware's working directory:

- ✓ 00000000.eky
- ✓ 00000000.pky
- ✓ 00000000.res
- ✓ 274901494632976.bat
- ✓ @Please_Read_Me@.txt
- ✓ @WanaDecryptor@.bmp
- ✓ @WanaDecryptor@.exe
- ✓ b. wnry
- ✓ c.wnry
- ✓ f. wnry
- ✓ m.vbs
- ✓ msg\m_bulgarian.wnry
- ✓ msg\m_chinese (simplified).wnry
- ✓ msg\m_chinese (traditional). wnry
- ✓ msg\m_croatian.wnry
- ✓ msg\m_czech.wnry
- ✓ msg\m_danish.wnry
- ✓ msg\m_dutch.wnry
- ✓ msg\m_english.wnry
- ✓ msg\m_filipino.wnry
- ✓ msg\m_finnish.wnry
- ✓ msg\m_french.wnry
- ✓ msg\m_german.wnry
- ✓ msg\m_greek.wnry
- ✓ msg\m_indonesian.wnry
- ✓ msg\m_italian.wnry
- ✓ msg\m_japanese.wnry
- ✓ msg\m_korean.wnry
- ✓ msg\m_latvian.wnry
- ✓ msg\m_norwegian.wnry
- ✓ msg\m_polish.wnry
- ✓ msg\m_portuguese.wnry
- ✓ msg\m_romanian.wnry
- ✓ msg\m_russian.wnry
- ✓ msg\m_slovak.wnry
- ✓ msg\m_spanish.wnry
- ✓ msg\m_swedish.wnry
- ✓ msg\m_turkish.wnry
- ✓ msg\m_vietnamese.wnry
- ✓ r. wnry
- ✓ s. wnry
- ✓ t. wnry
- ✓ TaskData\Tor\libeay32.dll
- ✓ TaskData\Tor\libevent-2-0-5.dll
- ✓ TaskData\Tor\libevent_core-2-0-5.dll
- ✓ TaskData\Tor\libevent_extra-2-0-5.dll
- ✓ TaskData\Tor\libgcc_s_sjlj-1.dll
- ✓ TaskData\Tor\libssp-0.dll
- ✓ TaskData\Tor\ssleay32.dll
- ✓ TaskData\Tor\taskhsvc.exe
- ✓ TaskData\Tor\tor.exe
- ✓ TaskData\Tor\zlib1.dll
- ✓ taskdl.exe
- ✓ taskse.exe
- ✓ u. wnry

WannaCrypt may also create the following files:

- ✓ %SystemRoot%\tasksche.exe
- ✓ %SystemDrive%\intel\<random directory name>\tasksche.exe
- ✓ %ProgramData%\<random directory name>\tasksche.exe

It may create a randomly named service that has the following associated Image Path: "cmd.exe /c "<malware working directory>\tasksche.exe"".

It then searches the whole computer for any file with any of the following file name extensions: .123, .7z , .jpg , .rb , .602 , .jpeg , .rtf , .doc , .js , .sch , .3dm , .jsp , .sh , .3ds , .key , .sldm , .3g2 , .lay , .sldm , .3gp , .lay6 , .sldx , .ldf , .slk , .accdb , .m3u , .sln , .aes , .m4u , .snt , .ai , .max , .sql , .ARC , .mdb , .sqlite3 , .asc , .mdf , .sqlitedb , .asf , .mid , .stc , .asm , .mkv , .std , .asp , .mml , .sti , .avi , .mov , .stw , .backup , .mp3 , .suo , .bak , .mp4 , .svg , .bat , .mpeg , .swf , .bmp , .mpg , .sxc , .brd , .msg , .sxd , .bz2 , .myd , .sxi , .c , .myi , .sxm , .cgm , .nef , .sxw , .class , .odb , .tar , .cmd , .odg , .tbk , .cpp , .odp , .tgz , .crt , .ods , .tif , .cs , .odt , .tiff , .csr , .onetoc2 , .txt , .csv , .ost , .uop , .db , .otg , .uot , .dbf , .otp , .vb , .dch , .ots , .vbs , .der" , .ott , .vcd , .dif , .p12 , .vdi , .dip , .PAQ , .vmdk , .djvu , .pas , .vmx , .docb , .pdf , .vob , .docm , .pem , .vsd , .docx , .pfx , .vsdx , .dot , .php , .wav , .dotm , .pl , .wb2 , .dotx , .png , .wk1 , .dwg , .pot , .wks , .edb , .potm , .wma , .eml , .wmv , .fla , .ppam , .xlc , .flv , .pps , .xlm , .frm , .ppsm , .xls , .gif , .ppsx , .xlsb , .gpg , .ppt , .xlsm , .gz , .pptm , .xlsx , .h , .pptx , .xlt , .hwp , .ps1 , .xltm , .ibd , .psd , .xltx , .iso , .pst , .xlw , .jar , .rar , .zip , .java , .raw.

WannaCrypt encrypts all files it finds and renames them by appending .WNCRY to the file name.

This ransomware also creates the file @Please_Read_Me@.txt in every folder where files are encrypted. The file contains the same ransom message shown in the replaced wallpaper image

After completing the encryption process, the malware deletes the volume shadow copies by running the following command:

cmd.exe /c vssadmin delete shadows /all /quiet wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet

Behavior Post Infection:

The ransomware infects your system using vulnerability and then it encrypts your files and folders using resource selection from dropper. After encryption it will display a ransom message on display and demand for ransom.

V. PETYA RANSOMWARE (REF:3)

Sign: Petya, Petrwrap, June 27, 2017

Attack vector: EternalBlue Server Message Block (SMB) Exploit Kit

Damage Level: High

Destruction Zone: Organizations in Europe and the US

Method of Propagation:

Firstly, Petya used to attempt installation and execution of the dropped file "C:\Windows\perfc.dat" on other devices to spread laterally. The dropped file, if managed to get the Administrator privileges, will encrypt the Master File Tree (MFT) tables for NTFS partitions and overrides the Master Boot Record (MBR) with a custom bootloader making the system unusable. Further the malware creates a scheduled task via schtasks /at to reboot the system one hour after infection. After the system is reloaded the malware downloads its code from MBR and encrypts data on the hard drive.

In case the fail to get the privileges rewrite MBR, the files are encrypted without a system reload.

The list of file types that are encrypted:

3ds, 7z, accdb, ai, asp, aspx, avhd, back, bak, c, cfg, conf, cpp, cs, ctl, dbf, disk, djvu, doc, docx, dwg, eml, fdb, gz, h, hdd, kdbx, mail, mdb, msg, nrg, ora, ost, ova, ovf, pdf, php, pmf, ppt, pptx, pst, pvi, py, pyc, rar, rtf, sln, sql, tar, vbox, vbs, vcb, vdi, vfd, vmc, vmdk, vmsd, vmx, vsdx, vsv, work, xls, xlsx, xvd, zip.

IOC's:

IP:

95.141.115.108

IP-dst:

185.165.29.78, 84.200.16.242, 111.90.139.247

DOMAIN:

coffeinoffice.xyz

french-cooking.com
sundanders.online

URL:
http[:]//french-cooking[.]com/myguy[.]exe
http[:]//84[.]200[.]16[.]242/myguy[.]xls
http://84[.]200[.]16[.]242/Profoma[.]xls
http://84[.]200[.]16[.]242/Lucky[.]exe
http://185.165.29.78/~alex/svchost.exe

sha256:
02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f
78734761d8edbdcd9f
eae9771e2eeb7ea3c6059485da39e77b8c0c369232f013
34954fbac1c186c998
64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599
a31d418c7c69e94b1
027cc450ef5f8c5f653329641ec1fed91f694e0d2299289
63b30f6b0d7d3a745
fe2e5d0543b4c8769e401ec216d78a5a3547dfd426fd47
e097df04a5f7d6d206
ee29b9c01318a1e23836b949942db14d4811246fdae2f4
1df9f0dcd922c63bc6
22053C34DCD54A5E3C2C9344AB47349A702B8CF
DB5796F876AEE1B075A670926
1FE78C7159DBCB3F59FF8D410BD9191868DEA1B
01EE3ECCD82BCC34A416895B5
EEF090314FBEC77B20E2470A8318FC288B2DE19A
23D069FE049F0D519D901B95

md5:

9B853B8FE232B8DED38355513CFD4F30
CBB9927813FA027AC12D7388720D4771
a809a63bc5e31670ff117d838522dec433f74bee
bec678164cedea578a7aff4589018fa41551c27f
d5bf3f100e7dbcc434d7c58ebf64052329a60fc2
aba7aa41057c8a6b184ba5776c20f7e8fc97c657
0ff07caedad54c9b65e5873ac2d81b3126754aac
51eafbb626103765d3aedfd098b94d0e77de1196
078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
7ca37b86f4acc702f108449c391dd2485b5ca18c
2bc182f04b935c7e358ed9c9e6df09ae6af47168
1b83c00143a1bb2bf16b46c01f36d53fb66f82b5
82920a2ad0138a2a8efc744ae5849c6dde6b435d

FILENAME:
C:\0487382a4daf8eb9660f1c67e30f8b25.hta
petwrap.exe
C:\027cc450ef5f8c5f653329641ec1fed91f694e0d2299
28963b30f6b0d7d3a745.bin.dll
Order-20062017.doc
myguy[1].hta
myguy.xls
dllhost.dat named pipe: {df458642-df8b-4131-b02d-
32064a2f4c19}

EMAILS:
wowsmith123456@posteo.net
wowsmith123456@posteo.net
iva76y3pr@outlook.com
carmellar4hegp@outlook.com
amanda44i8sq@outlook.com

Who is behind the attack?
It is not clear, but it seems likely it is someone who wants the malware to masquerade as ransomware, while actually just being destructive, particularly to the Ukrainian government. Security researcher Nicholas Weaver told cybersecurity blog Krebs on Security that 'Petya' was a "deliberate, malicious, destructive attack or perhaps a test disguised as ransomware". Pseudonymous security researcher Grugq noted that the real Petya "was a criminal enterprise for making money," but that the new version "is definitely not designed to make money.

"This is designed to spread fast and cause damage, with a plausibly deniable cover of 'ransomware,'" he added, pointing out that, among other tells, the payment mechanism in the malware was inept to the point of uselessness: a single hardcoded payment address, meaning the money can be traced; the requirement to email proof of payment to a webmail provider, meaning that the email address can be – and was – disabled; and the requirement to send an infected machine's 60-character, case sensitive "personal identification key" from a computer which can't even copy-and-paste, all combine to mean that "this payment pipeline was possibly the worst of all options (sort of 'send a personal cheque to: Petya Payments, PO Box … ')".

Behavior Post Infection:
Infected computers display a message demanding a Bitcoin ransom worth $300. Those who pay are asked to send confirmation of payment to an email address. However, that email address has been shut down by the email provider.

The "Petya" ransomware has caused serious disruption at large firms in Europe and the US, including the advertising firm WPP, French construction materials company Saint-Gobain and Russian steel and oil firms Evraz and Rosneft. The food company Mondelez, legal firm DLA Piper, Danish shipping and transport firm AP Moller-Maersk and Heritage Valley Health System, which runs hospitals and care facilities in Pittsburgh, also said their systems had been hit by the malware.

If the system reboots with the ransom note, don't pay the ransom – the "customer service" email address has been shut down so there's no way to get the decryption key to unlock your files anyway. Disconnect your PC from the internet, reformat the hard drive and reinstall your files from a backup. Back up your files regularly and keep your anti-virus software up to date.

VI. LOCKY RANSOMWARE (REF: 4)

Damage Level: High
Attack vector: Spam Email
Destruction Zone: 28+ Countries, top 10: France, Italy, Germany, Spain, USA, Great Britain, Poland, Japan, Czech Republic, and Canada.
Inception: February 2016
Ransom: $400-$800

Features: Locky uses all "top class" features, such as a domain generation algorithm, custom encrypted communication, TOR/Bitcoin payment, strong RSA-2048+AES-128 file encryption and can encrypt over 160 different file types, including virtual disks, source codes and databases.

Method of Propagation:

You receive an email containing an attached document (Trojan/DocDl-BCF). The document advises you to enable macros "if the data encoding is incorrect."

If you enable macros, you don't actually correct the text encoding (that's a subterfuge); instead, you run code inside the document that saves a file to disk and runs it. The saved file (Trojan/Ransom-CGX) serves as a downloader, which fetches the final malware payload from the crooks. The final payload could be anything, but in this case, is usually the Locky Ransomware (Trojan/Ransom-CGW).

- ✓ Locky scrambles all files that match a long list of extensions, including images, videos, source code, and Office files.
- ✓ Locky even scrambles wallet.dat, your Bitcoin wallet file, if you have one.
- ✓ Locky also removes any Volume Snapshot Service (VSS) files, also known as shadow copies, that you may have made.
- ✓ Shadow copies are the Windows way of making live backup snapshots without having to stop working – you don't need to logout or even close your applications first – so they are a quick and popular alternative to a proper backup procedure.
- ✓ Once Locky is ready to hit you up for the ransom, it makes sure you see the message by changing your desktop wallpaper.
- ✓ It scrambles any files in any directory on any mounted drive that it can access, including removable drives that are plugged in at the time, or network shares that are accessible, including servers and other people's computers, whether they are running Windows, OS X or Linux.

Behavior Post Infection:

After ransomware attacked on system then locky ransomware rename all files and folders extensions to .locky and made it to not usable. it doesn't just rename your files, it scrambles them first, and – as you probably know about ransomware – only the crooks have the decryption key. You can buy the decryption key from the crooks via the so-called darkweb.

Summary:

Locky ransomware is currently a big player in the malware sphere. When looking into Locky, we can see all top features, such as a time-based DGA system, huge spam email campaigns, various scripting languages, generic PE packers, server-side encryption key generation and Tor/Bitcoin payment.

The authors of Locky are skilled and are developing Locky further. They reacted to the AV industry blocking their C&C server infrastructure by changing the DGA algorithm and also patched some minor bugs in the newer version.

File encryption malware is currently very popular and can be very profitable. We therefore predict new ransomware families will emerge next years.

VII. COUNTERMEASURES: (REF:5)

What Managed Service Providers (MSPs) and small- to medium-sized businesses can do to protect devices from ransomware:

Deploy Security Solution: Purchase and deploy a top-rated security solution. Look for cybersecurity solutions that provide protection from multiple attack vectors, without affecting user experience by slowing devices during scans.

Keep your security software up to date: Firmware and patches are how vendors push out important security updates. Keep both devices and operating systems up-to-date and create a process for patch management.

Backup and restore: Backup sensitive data. Generally, ransomware only has the means to encrypt files stored locally on a user's system. Backup data to a hard, offline location. In the case of equipment failure or ransomware, you can access your backup and get back to business as usual.

Strong password policies: Implement a strong password naming convention. A strong password policy limits the likelihood of Remote Desktop Protocol (RDP) breaches.

What home users can do to protect computers from ransomware:

Use genuine antivirus: Use a reliable antivirus software. A good solution should protect your data while providing a seamless user experience.

Back up your data: Proactively backing up your files can not only save you thousands, it can save your favorite vacation photos, videos of your kids' piano recitals, and sensitive information.

Take precautions while browsing: Use good judgement. Be extra vigilant about the websites you visit, the URLs you follow, and the applications and mobile apps you use.

VIII. CONCLUSION

In this review paper, we presented a review of ransomware-attacks along with the possible countermeasures in computer systems. From this paper we can say that ransomware families are made more and more advance day by day. 2017 is a year where attacked by more powerful ransomwares done. In this we have tried to give the insight of the ransomware and its type, working of ransomware and method they applied and most useful information's like its IOC'S and method of propagation are explained in detailed. Countermeasure for home users and small-medium scale organization is provided.

IX. WEB REFERENCES

[1]. https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/

[2]. https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

[3]. http://www.cyberswachhtakendra.gov.in/alerts/petya_ransomware.html

[4]. http://www.blog.avast.com/malware/malwareanalysis/research/Locky/A_closer_look_at_the_Locky_ransomware.pdf

[5]. https://www.webroot.com/us/en/about/press-room/releases/webroot-top-10-nastiest-ransomware