TOP 10 RANSOMWARES

SECURITY PLAN FOR IDENTIFICATION PROTECTION AND DEFENSE FROM RANSOMWARES

Prepared by: (TEAM G)

ANUSHKKA DHAMIJA
SHLOK SHARMA
MD HAMID MURTUZA
SHRUTIKA SONI
SAURABH CHAUHAN
MUGILAN ELUMALAI

REPORT 3

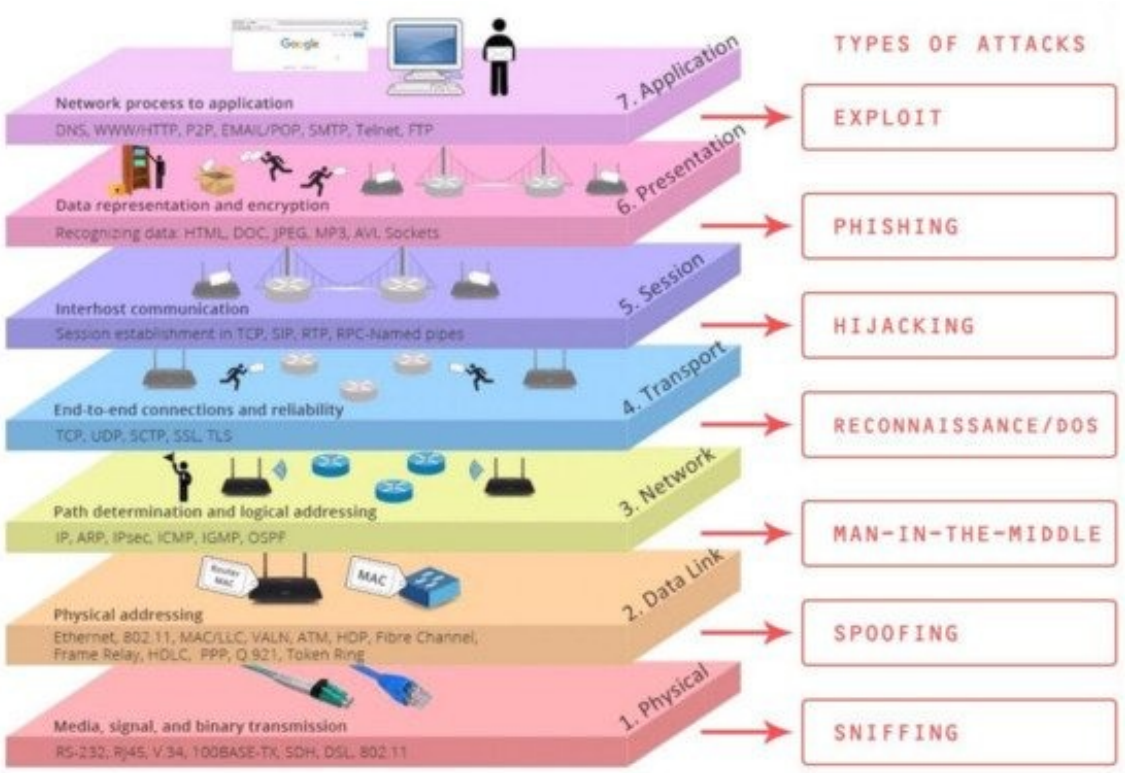
MILESTONE : IoC (Indicator of Compromise)

This report contains the IoC's and hashes of various ransomware attacks

OVERVIEW

Indicators of Compromise (IoCs) are the evidence that a cyber-attack has taken place. IoCs give valuable information about what has happened but can also be used to prepare for the future and prevent against similar attacks. Antimalware software and similar security technologies use known indicators of compromise, such as a virus signature, to proactively guard against evasive threats. Indicators of compromise can also be used

DETAILS ABOUT IoC



How Do Indicators of Compromise Work?

When a malware attack takes place, traces of its activity can be left in system and log files. These IoCs present the activity on your network that you may not otherwise be able to see in real-time and that could suggest potentially malicious activity is taking place. If a security breach is identified, the IoC or "forensic data" is collected from these files and by IT professionals. Modern antimalware systems use known indicators of compromise to detect malware infections

IoC's of WannaCry

HASHES :

- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
- 0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
- 428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
- 5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6

DOMAIN :

When this sample was initially discovered, the domain "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com" was not registered, allowing the malware to run and propagate freely. However within a few days, researchers learned that by registering the domain and allowing the malware to connect, it's ability to spread was greatly reduced. At this time, all traffic to "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" is re-directed to a monitored, non-malicious server, causing the malware to terminate if it is allowed to connect. For this reason, we recommend that administrators and network security personnel not block traffic to this domain.

IP(INTERNET PROTOCOL):

WannaCry utilizes this exploit by crafting a custom SMB session request with hard-coded values based on the target system. Notably, after the first SMB packet sent to the victim's IP address, the malware sends two additional packets to the victim containing the hard-coded IP addresses 192.168.56.20 and 172.16.99.5.

IoC's of WannaCry

DROPPER :

(5bef35496fcbdbe841c82f4d1ab8b7c2

EXTENSION :

Can people start adding to the list below for known file extensions on Wannacry. Here's what I have so far:

- .wnry
- .wcry
- .wncry
- .wncryt
- . uiwix

It'll help the community in the short term

IoC's of GoldenEye

HASHES :

- Order-20062017.doc (RTF) -> myguy.xls (HTA) -> myguy.exe ->
- Using a python script (rtfdump.py) for dumping the contents of a rtf, we can extract the embedded link object from the sample (101cc1cb56c407d5b9149f2c3b8523350d23ba84-Order-20062017.doc).
- Contents dumped contains this string (URL): "84.200.16.242/myguy.xls"
- The file continues to be downloaded because of the known vulnerability CVE-2017-0199 that leverages and exploits Office Documents/RTF.After the download, we have sample 736752744122a0b5ee4b95ddad634dd225dc0f73-myguy.xls. According to the description of the vulnerability CVE-2017-0199, Mshta.exe will parse the myguy.xls and find a script.

DOMAIN :

This latest attack, much like WannaCry, has hit some major targets:

- Maersk (Danish energy and transportation company)
- Rosneft (Russian oil company)
- The Kiev metro system (Ukraine)
- Chernobyl's radiation monitoring system (Ukraine)
- Boryspil airport (Ukraine)
- National Bank of Ukraine
- DLA Piper (British law firm)
- WPP (British advertising and PR firm)
- Merck (US pharmaceutical company)

This is a preliminary list that is likely to grow, but it reveals the global scale of the outbreak even in this early stage.

IP(INTERNET PROTOCOL):

- 14FLqrYVveGEdW6LYYNcCe1
- 84.200.16..242
- 95.141.11..108
- 111.90.139..247

IoC's of GoldenEye

DROPPER :

- X2KM_GOLDENEYE.A
- aac
- accdb
- aepx
- ai
- aif
- amr
- ape

EXTENSION :

GoldenEye ransomware is predominantly distributed by malicious email attachments that employ deceptive methods. The email attachment will typically consist of a.zip file or fake document file. If files from the .zip file are manually extracted it will unpack a JavaScript file. When the JavaScript file is manually executed by the user it will cause the malware to spread across the machine.

.mid, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .tar.bz2, GoldenEye ransomware encrypts files that match certain file extensions with encryption ciphers. The encryption process will render the files inaccessible to the user. The encrypted files are appended a new 8 character file extension to the end of the file and file type by the ransomware. A ransom note (or series of ransom notes) named YOUR_FILES_ARE_ENCRYPTED.TXT will then be placed in every folder the virus encrypted files in and on Windows desktop. In addition, the ransomware will modify the user's MBR (Master Boot Record) with a custom boot loader. The boot loader will forcibly restart the user's computer and enters a stage where it proceeds encrypting the user's hard drive MFT (Master File Table), which makes it impossible to access any files on the hard disk. During the process a fake chkdsk screen will be displayed.

Ioc's of Bad Rabbit

HASHES :

- 0b2f863f4119dc88a22cc97c0a136c88a0127cb026751303b045f7322a8972f6
- 16605a4a29a101208457c47ebfde788487be788d
- 1d724f95c61f1055f0d02c2154bbccd3
- 2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035
- 301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcfe347c
- 3d05f09fb436c0e4dea85a8c6a12d47502016795df6ea5c8844da1655f1657b4
- 413eba3973a15c1a6429d9f170f3e8287f98c21c
- 4f61e154230a64902ae035434690bf2b96b4e018
- 579FD8A0385482FB4C789561A30B09F25671E86422F40EF5CCA2036B28F99648
- 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da
- 682ADCB55FE4649F7B22505A54A9DBC454B4090FC2BB84AF7DB5B0908F3B7806
- 7217fae6f3634cde7d54eba3858e8958eb1e5e85e2c36d968818cdce75a3fae9
- 79116fe99f2b421c52ef64097f0f39b815b20907
- 80c336a30aa746f5a05a21056e36328b9527c4ace59cd9e2fbb5211e87e5841d
- 84ac3d2f1ca70bc83149bec52b00009639e9006f941caed3ca83e4e8e47f64bd
- 8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93
- 8fd96bb2ce94146f1b0271d18ba52f176d4ebf8fabd275f1d16d59ed9d91d2da
- afeee8b4acff87bc469a6f0364a81ae5d60a2add
- b14d8faf7f0cbcfad051cefe5f39645f
- de5c8d858e6e41da715dca1c019df0bfb92d32c0
- fbbdc39af1139aebba4da004475e8839

DOMAIN :

Spreading via SMB

Win32/Diskcoder.D has the ability to spread via SMB. As opposed to some public claims, it does not use the EternalBlue vulnerability like the Win32/Diskcoder.C (Not-Petya) outbreak. First, it scans internal networks for open SMB shares. It looks for the following shares:

- admin
- atsvc
- browser
- eventlog
- lsarpc
- netlogon
- ntsvcs
- spoolss
- samr
- srvsvc
- scerpc
- svcctl
- wkssvc

Ioc's of Bad Rabbit

IP(INTERNET PROTOCOL) :

185.149.120.3

DROPPER :

630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da

EXTENSION :

- 1dnscontrol.com
- caforssztxqzf2nm.onion
- 185.149.120.3/scholargoogle
- 1dnscontrol.com/flash_install.php
- Argumentiru.com
- www.fontanka.ru
- grupovo.bg
- www.sinematurk.com
- www.aica.co.jp
- spbvoditel.ru
- argument.ru
- www.mediaport.ua
- blog.fontanka.ru
- an-crimea.ru
- www.t.ks.ua
- most-dnepr.info
- osvitaportal.com.ua
- www.otbrana.com
- calendar.fontanka.ru
- www.grupovo.bg
- www.pensionhotel.cz
- www.online812.ru
- www.imer.ro
- novayagazeta.spb.ru
- i24.com.ua
- bg.pensionhotel.com
- ankerch-crimea.ru

IoC'S of LOCKY

HASHES :

- 7a23368ee84781d7584e058a9922f324
- 74dde1905eff75cf3328832988a785de
- d9df60c24ceca5c4d623ff48ccd4e9b9
- e7aad826559c8448cd8ba9f53f401182
- e95cde1e6fa2ce300bf778f3e9f17dfc6a3e499cb0081070ef5d3d15507f367b
- 5466fb6309bfe0bbbb109af3ccfa0c67305c3464b0fdffcec6eda7fcb774757e
- fde84a9e721c55675452ed2d2f12f224e19a0a24116d3a47efe1633b1c6b404c
- f689391b0527fbf40d425e1ffb1fafd5c84fa68af790e8cc4093bcc81708c11b
- f317cd282eabf150e660619a686ac9c2af11ac59d103abaea2756c221d33af45
- f196a81eab51eadbcf3c5171c3c23ce35a7320a8434676ac9265dda2c0aec229
- eead04036eccb12ea4e27c38047bbad6899ada4cc1e9e9154c5ac1dfdedd38cc
- df255af635a2dde04c031db95862f11e1bf44fe5cfc10d3b20bd4678ed818567

DOMAIN :

- ecoledecorroy.be/1/1.exe
- onigirigohan.web.fc2.com/1/1.exe
- killerjeff.free.fr/2/2.exe
- lasmak.pl/2/2.exe
- animar.net.pl/3/3.exe
- uponor.otistores.com/3/3.exe
- premium34.tmweb.ru/4/4.exe
- suicast.de/4/4.exe
- bebikiask.bc00.info/5/5.exe
- ratgeber-beziehung.de/5/5.exe
- proteusnet.it/6/6.exe
- test.rinzo.biz/6/6.exe
- avp-mech.ru/7/7.exe
- luigicalabrese.it/7/7.exe

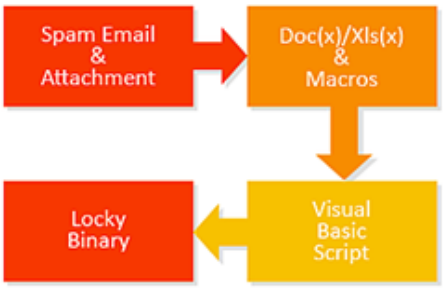
IP(INTERNET PROTOCOL):

- 95.181.171.58
- 185.14.30.97
- 195.22.28.196
- 195.22.28.198

IoC'S of LOCKY

DROPPER :

Locky is spreading via spam email campaigns that are similar to those used by the Dridex botnet. They use similar file names, obfuscation, email content and structure of download URLs.



EXTENSION :

The Locky Diablo6 Ransomware will target the following file types:
.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .backup, .backupdb, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx,

IoC 'S of RYUK

HASHES :

- d971827d974effedaeaf7d62b619b1dd
- c3a846eb04e2fe765e56fa15a0d5c1eb650ccba3
- 1d8b7faf5f290465cc742e07abca78fac419135b191071cc77912263cd1dde1d
- a90d500745a1ce2417c01fecefbc2851
- 42a0c34ac3ef479ace2c8a6222ebe8312a1959cc

DOMAIN :

- havemosts.com
- apps-testing-dev02.com

IP(INTERNET PROTOCOL):

- 88.119.171.94

DROPPER:

c3a846eb04e2fe765e56fa15a0d5c1eb650ccba3

EXTENSIONS :

PEXE - PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows

IoC'S of PETYA

HASHES :

- 71b6a493388e7d0b40c83ce903bc6b04
- a1d5895f85751dfe67d19cccb51b051a
- 7e37ab34ecdcc3e77e24522ddfd4852d
- e285b6ce047015943e685e6638bd837e
- fe2c47fbb22139f790287272e9a9e365
- E595c02185d8e12be347915865270cca
- a809a63bc5e31670ff117d838522dec433f74bee
- bec678164cedea578a7aff4589018fa41551c27f
- d5bf3f100e7dbcc434d7c58ebf64052329a60fc2
- aba7aa41057c8a6b184ba5776c20f7e8fc97c657
- 0ff07caedad54c9b65e5873ac2d81b3126754aac
- 51eafbb626103765d3aedfd098b94d0e77de1196
- 078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
- 7ca37b86f4acc702f108449c391dd2485b5ca18c
- 2bc182f04b935c7e358ed9c9e6df09ae6af47168
- 1b83c00143a1bb2bf16b46c01f36d53fb66f82b5

DOMAIN :

http://mischapuk6hyrn72.onion/
http://petya3jxfp2f7g3i.onion/
http://petya3sen7dyko2n.onion/
http://mischa5xyix2mrhd.onion/MZ2MMJ
http://mischapuk6hyrn72.onion/MZ2MMJ
http://petya3jxfp2f7g3i.onion/MZ2MMJ
http://petya3sen7dyko2n.onion/MZ2MMJ
http://benkow.cc/71b6a493388e7d0b40c83ce903bc6b04.bin
http://french-cooking.com/

IP(Internet Protocol) :

- 95.141.115.108
- 185.165.29.78
- 84.200.16.242
- 111.90.139.247

IoC'S of PETYA

DROPPER :

- http://mischapuk6hyrn72.onion/
- http://petya3jxfp2f7g3i.onion/
- http://petya3sen7dyko2n.onion/
- http://mischa5xyix2mrhd.onion/MZ2MMJ
- http://mischapuk6hyrn72.onion/MZ2MMJ/
- http://petya3jxfp2f7g3i.onion/MZ2MMJ
- http://petya3sen7dyko2n.onion/MZ2MMJ

EXTENSION :

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 8.1 RT
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008R2
- Windows Server 2012
- Windows Server 2012R2
- Windows Server 2016
- Windows Server Core
- Windows Embedded Standard 2009
- Windows Embedded POSReady 2009

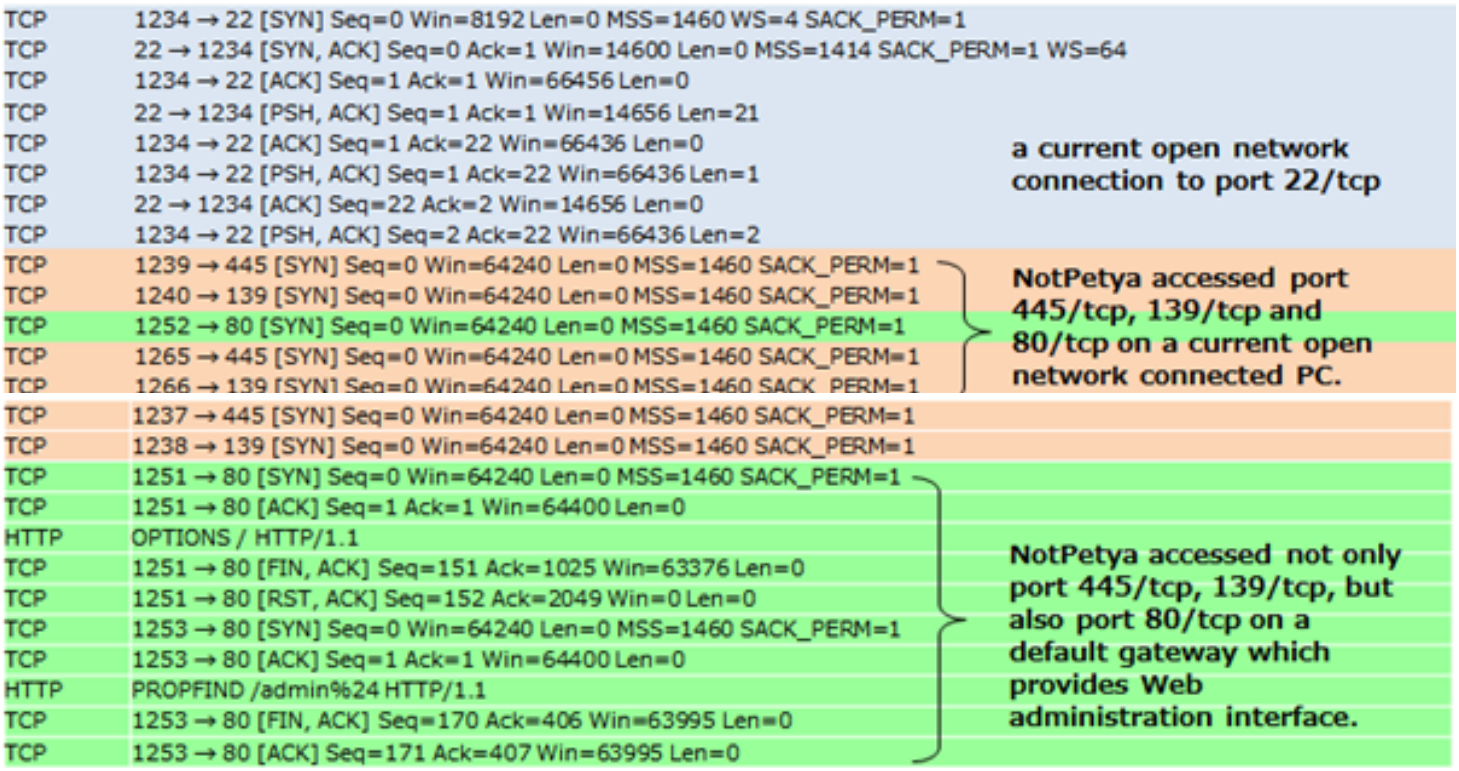
There is no evidence that Windows 10 is targeted.

IoC'S of NOT-PETYA

HASHES :

- 0x6403527E ’n avp.exe associated with Kaspersky AV
- 0x23214B44 ’n ns.exe associated with Norton Security
- 0x651B3005 ’n ccSvcHst.exe associated with Symantec
- AEEE996FD3484F28E5CD85FE26B6BDCD
- F8DBABDFA03068130C277CE49C60E35C029FF29D9E3C74C362521F3FB02670D5

DOMAIN :



IP(Internet Protocol) :

- 95.141.115.108
- 185.165.29.78
- 84.200.16.242
- 111.90.139.247

IoC'S of NOT-PETYA

DROPPER :

- 52dd60b5f3c9e2f17c2e303e8c8d4eab

EXTENSION :

- 52dd60b5f3c9e2f17c2e303e8c8d4eab
- PE32 executable for MS Windows (DLL) (console) Intel 80386 32-bit
- .text48,640c5bd3bb710ae377938b17980692b785b
- .rdata 34,304 46418e52b546c1f696eb8a524f18c56e
- .data 20,992 5216f0c62d1fd41b1d558e129e18d0fe
- .rsrc 247,808 f07e68575f50a62382d99e182baa05d5
- .reloc 3,584 c5d1d4cdade7dcfbe14ec10dcf66cfb1
- + 0x57000 6,008da2b0b17905e8afae0eaca35e831be9e

GandCrab

HASHES :

- http://172.96.14.134:5471/3306.exe
- https://camputononaunerytyre.info/vcword6.tmp
- http://13.76.158.123/Malware/ALY/Windows6.1-KB3102810-x86.exe
- http://13.76.158.123/Malware/KS/GandCrab.exe
- http://13.76.158.123/Malware/SL/GandCrab.exe
- http://13.76.158.123/Malware/ALF/GandCrab.exe
- http://13.76.158.123/Malware/GandCrab.exe
- http://13.76.158.123/Malware/CT/GandCrab.exe
- http://talsasd.ru/r78hjsd.exe
- http://sdfsd14as2334d.ru/rhjg345kj.exe

DOMAIN :

- havemosts.com
- apps-testing-dev02.com

IP(INTERNET PROTOCOL):

- 88.119.171.94

DROPPER:

c3a846eb04e2fe765e56fa15a0d5c1eb650ccba3

EXTENSIONS :

PEXE - PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows

IoC'S of Shade/Troldesh

HASHES :

- 01a47aefed5ad89958df66ceaaece3eb1028f5eb339b5fc405c365bf016652ae
- 04d08fed39c68ff27751497d6cb543d8a7d082cd2efdda0515853a9fa0f8d70c
- 053eb4558f17ff9d2e8af9fc171f279b1a43be35a309ca1298f581eb332a8790
- 07e7472cce0ba35d0f9548372f2b93d56e5fe7597a8de0de337c3a2d96f2c69c
- 093b450519424959l522a9bed6abfc24d9911d4a64c89a51a46ac75d41a0f3a4
- 2AC1A572DB6944B0A65C38C4140AF2F4aac72FB617C
- 2AC1A572DB6944B0A65C38C4140AF2F4aac72FB6588
- 2AC1A572DB6944B0A65C38C4140AF2F4aac72FB63E8
- 2AC1A572DB6944B0A65C38C4140AF2F4aac72FB6428
- 2AC1A572DB6944B0A65C38C4140AF2F4aac74C2310C

DOMAIN :

- voluptuous[.]googleresearcher[.]xyz
- ad3[.]dogfunnyvideos[.]xyz
- todaymale[.]xyz
- ertagov[.]com

IP(INTERNET PROTOCOL):

- 85[.]17.197.100
- 5[.]23.49.200
- 185[.]56.233.186
- 72[.]52.179.174

IoC's of Shade/Troldesh

DROPPER :

- 708a99e2151e1130_wsrgb.icc
- c4730063925f77d4_usercache.bin
- eb2f5c1edd5d7090_wscrgb.icc
- HA-1: E6B0FEF60562A33B68B5A3CDCAC9856756A5E883

EXTENSION :

- ASCII text, with CRLF, LF line terminators
- .xtbl
- .ytbl
- .breaking_bad
- .heisenberg
- .da_vinci_code

HASHES :

- 642e0acdbece0f1e99604f63488e2d0ae4845080adba80ecfc55cbc95db05bc5
- 73fcbb6f10cd849bff109dd05cf89d9b612302faed9c382791d6df4d024bc009
- 7e98f0308fd88e97e4f80b1e2c6845e18186e07d2a27d936bccadad719114334
- 809f403efb1c7f19a30cfdd62841b898ebfbc1e91626928bb372ad630d8d9b81
- 81dc5726d4af65258dec6ccf0dda1327fcacb9b950539992fff82859c6645a27
- 85506de211f0441c3bbf0e98668a7d3d1c2a62aadc07ef82968245644fca4b00
- 8ef7ee2b458b006e3364f972a744031cb99c9a9d7bb4329b4a41e6d0e1cbb784

DOMAIN :

- time[.]microsoft[.]akadns[.]net
- ynefefyopqvu[.]com

IP(INTERNET PROTOCOL):

- 51[.]141[.]32[.]51
- 14.33.133.188
- 14.32.0.0
- 14.33.166.39

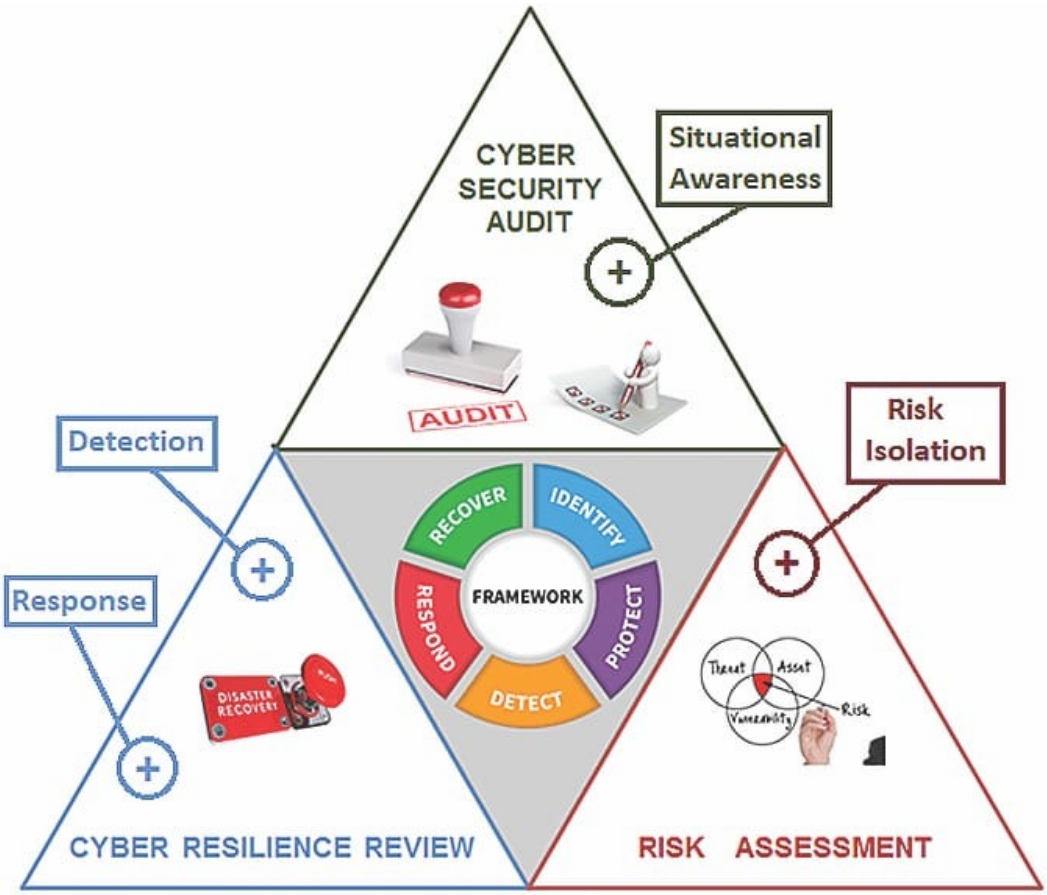
DROPPER :

- 708a99e2151e1130_wsrgb.icc
- c4730063925f77d4_usercache.bin
- eb2f5c1edd5d7090_wscrgb.icc
- HA-1: E6B0FEF60562A33B68B5A3CDCAC9856756A5E883

EXTENSION :

- To collect email addresses to spread itself, the worm looks on drives from C: to Z for address in files with the following extensions-
- .asp
- .bat
- .cfm
- .com
- .com
- .csv
- .doc
- .eml
- .exe
- .htm
- .txt
- .wab
- .xls

CONCLUSION



- Cybersecurity is a public concern receiving insufficient awareness.
- Cybersecurity is complex, intangible and hard to grasp.
- Paradoxes are identified complicating policy-making.
- Evidence-based framing can result in societal and political awareness.
- Framing strategies for creating societal and political awareness are presented
- With this 3rd milestone complete we get to know the in depth knowledge on our end about the attack

REFERENCES

- Malwarebytes LABS: WanaCrypt0r ransomware hits it big just before the weekend
- Malwarebytes LABS: The worm that spreads WanaCrypt0r
- Microsoft: Microsoft Security Bulletin MS17-010
- Forbes: An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak
- Reuters: Factbox: Don't click - What is the 'ransomware' WannaCry worm?
- GitHubGist: WannaCry|WannaDecrypt0r NSA-Cyberweapon-Powered Ransomware Worm
- Microsoft: Microsoft Update Catalog: Patches for Windows XP, Windows 8
- Cisco: Player 3 Has Entered the Game: Say Hello to 'WannaCry'
- Washington Post: More than 150 countries affected by massive cyberattack
- www.techrepublic.com
- support.threattracksecurity.com
- www.dsci.in
- www.securonix.com
- https://socprime.com/blog/security-advisory-bad-rabbit-ransomware-worm/
- https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/
- https://blog.avast.com/a-closer-look-at-the-locky-ransomware
- https://blog.malwarebytes.com/threat-analysis/2016/03/look-into-locky/
- https://www.proofpoint.com/us/threat-insight/post/Dridex-Actors-Get-In-the-Ransomware-Game-With-Locky
- https://blogs.blackberry.com/en/2017/11/threat-spotlight-locky-ransomware
- https://habrahabr.ru/post/331762/
- https://blog.sucuri.net/2019/08/troldesh-ransomware-dropper.html
- https://blog.malwarebytes.com/threat-analysis/2019/03/spotlight-troldesh-ransomware-aka-shade/
- https://www.cybereason.com/blog/exploit-kits-shade-into-new-territory#iocs
- https://blog.talosintelligence.com/2019/08/threat-roundup-0802-0809.html
- https://www.f-secure.com/v-descs/brontok_n.shtml
- https://rstcloud.net/profeed

THANK YOU