A Brief Overview of DJVU Ransomware Family

Chaitanya Kapre

¹Department of Computer Science and Engineering, Shri Ramdeobaba
College of Engineering and Management, Nagpur, India

ABSTRACT

In today's world the use of internet and computer are not just restricted to sending emails and retrieve information. Instead all large and small enterprises, health institutions, financial institutions, government officials all are shifting from offline data management to online data management. There are now various softwares for paying Income Tax return, bills, e-banking, airways and railways ticket booking, movie ticket, etc. By the substantial increase in growth of usage of cloud services, there has been exponential growth of cyber threats and cyber attacks incidents [Peter W. Singer, Allan Friedman, 2014]. Malware had been the primary tool used by the hackers to do malicious activity. The most used malware is ransomware and, in that also DJVU/STOP family viruses are the most common. These viruses will not only affect the big companies, but also small scale startups or businesses and even common people [K.A. Francis, 2019]. According to the University of Maryland, Hackers attack every 39 seconds, which results in an average of 2,244 times a day. So, considering the need of awareness, this paper has been written to give the all information about this type of ransomware. Moreover, this paper will also cover the discussion on -how virus has entered into system (that is the way/entry point), working of the virus (that is how it affects the system), processes to remove the virus correctly, various methods to recover the data and the preventive measures to avoid such virus attacks. This paper is for the people who are the victim of such viruses or having keen interest in learning new viruses. Also, this paper motivates the readers to use this for further research.

KEY WORDS: ONLINE DATA MANAGEMENT, CLOUD SERVICES, MALICIOUS ACTIVITY, RANSOMWARE, RECOVER DATA.

INTRODUCTION

As the technology evolved and use of internet got more robust which enabled digital advertising, marketing in wider area, etc., many large enterprises are taking interest in using and developing cloud services for efficient and safe online data management systems. If we consider safety of data, they have to verify that their clients/users data is safe and protected. According to the report of the

Information Systems Security Association (ISSA), the big problem is 82% of employers lack cybersecurity skills. Hence many large enterprises are spending nearly \$1 million annually on data and cybersecurity. This shows the need of awareness about cybersecurity. Hence cyber security issue should not get restricted to company/personal issues but it should be considered as a national issue. Cyber security ensures no illegal access, unauthorized modification of data and protect the files from malware.

Data breaching/sealing is an unethical method to access someone's data without their permission. Hackers generally use this technique for cyber threats and crimes with the help of their primary tools which are - 'malwares'. Computer malwares can simply termed as a computer software/program which secretly enters into our system with or without concern and can duplicate itself to carry out many vulnerable activities like accessing

ARTICLE INFORMATION

*Corresponding Author: kaprecp@rknec.edu
Received 18th Oct 2020 Accepted after revision 29th Dec 2020
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

NAAS Journal Score 2020 (4.31)
A Society of Science and Nature Publication,
Bhopal India 2020. All rights reserved.
Online Contents Available at: <http://www.bbrc.in/>
Doi: <http://dx.doi.org/10.21786/bbrc/13.14/58>

and modifying our private ,as well as system files which can lead to encryption of data , lose all data or system abnormal behaviour 'ILOVEYOU' virus which is considered as one of the most popular and worst viruses spread through emails.They sent the mail with the subject 'I LOVE YOU' and the attachment 'LOVE-LETTER-FOR-YOU.txt.vbs'.After opening the file the virus will quickly try to hide itself after modifying the different types of files like jpg / jpeg (image) , mp4 (video) , .mp3(audio),etc and sends the copy of the email(infected) to the first 50 contacts of the Windows Address Book.This virus has affected nearly 10% of internet-connected computers in the world. During this Pandemic one thing has been proved ,that ransomware cases crossed over 20% around the world in the first half of 2020 itself.[Refer fig<a>]

*New template refers to new and unique COVID 19 phishing template.

*3 parts are made according to the intensity, being lowest -Wave 1 and highest - Wave 3

As Cybercriminals are taking advantage of this pandemic by tricking the common people with the subject of COVID-19 and make them click the ad which steals their information.Also, the another reason for the rise in cyber threats could be that most of the people were working from home so they had weaker IT security than corporate network security.

fig<a> :New phishing (scam) covid templates by week
Image Courtesy: www.beazley.com
Source:knowBe4

Types of Malwares

- **Adware:** Adware is a program which redirects the user to advertisement pages while the user is surfing on the web or even connected to the internet.
- **Spyware:** Spyware is deployed by hackers into the systems to keep a check of the system files, personal information, login credentials and also intellectual properties.
- **Trojan:** Trojan or Trojan horse is a type of malware which can secretly enter our system with some legitimate software and gain access to our system files.It can also copy /modify/block or even delete

the data.

- **Ransomware:** It is a malicious software which infects the system and the only way to open the system/ access our files is to give the ransom as demanded by the hackers.
- **Viruses and worms:** It can be defined as malicious software that has the ability to self duplicate themselves via local/network resources without any concern of the owner of the system.Also worms can directly penetrate the computer memory and then execute the worm code , coded by the hackers.
- **Bots:** Bots are nothing but robots which are used to do repetitive tasks like spamming requests to a particular website server to make their server down,steal personal information, gain total access over the computer.These infected systems are commonly referred to as zombies.
- **Bugs:** A software bug is deployed to gain unauthorized access to certain system.It exploits data integrity,data confidentiality,authorization of users to access the rights and other entities.
- **Rootkits:** It is a malicious software which allows an unwanted and unauthorized user to access and restrict the access of the data.When rootkits enter they first gain the administrative access and then they steal the administrative credentials and privileges. The most common observed this year was ransomware and that too of DJVU/STOP family. DJVU(family of specific viruses cryptoware encrypts the user files by using the AES-256 algorithm and put the extension of its own.

Related Work: DJVU/STOP4 is a family of viruses which contains more than 240+ variants.These viruses use AES(advanced encryption standard)-256 algorithm(CFB mode).CFB mode stands for Ciphertext feedback mode. These types of viruses can't encrypt the whole file , but approximately encrypts nearly 5MB of the beginning. KASP virus belongs to DJVU/STOP4 ransomware family. [Brendan Smith, 2020].The Kasp ransomware can only encrypt the first 150KB of files. So if you have a big mp4 file you can play it through media players(for example Winamp) but the first 3-6 seconds(the encrypted portion) would be missing.

Some of the common variants of viruses are: COPA Virus (.copa extensions),KOLZ VIRUS (.kolz extensions) ,Ogdo Virus (.ogdo extensions),KASP Virus (.KASP extensions) ,Boop Virus Ransomware(.BOOP extensions),Vari Virus (.VARI extensions),OONN VIRUS (.oonn extensions) .The best part is that the working of these viruses are nearly the same which makes it easy to remove it and recover data.My pc was infected with .kasp and at that time I was unaware of this ransomware so didn't find any other alternative rather than formatting the pc.But by doing research I found out some working methods which I proposed below - to identify the mode of virus, remove the virus ,and also to recover data. Following are the associated files:%LocalAppData%\[guid]\[random_numbers]tmp.exe ,%LocalAppData%\[guid]\4.exe,%LocalAppData%\[guid]\2.exe,%LocalAppData%\[guid]\3.exe, %LocalAppData%\[guid]\updatewin.exe.

Proposed Methods

How does the virus enter?

1. Many users experienced that the cryptoware is injected after downloading unethical/crack version of applications, games, modded apks, pirated softwares/torrent files, and even crack key of MS Windows / MS Office (example: KMSPico, KMSAuto Net, etc.) distributed by the hackers through dark/pirated websites. The other means can be weak RDP (remote desk protocol) configuration which enables remote connection to other system, via email spam and infected attachments, downloads from malicious/infected websites, exploits, web injectors, fake/faulty updates, etc. [Brendan Smith, 2020]
2. The below-mentioned extensions can be encrypted by these viruses. MS Office or OpenOffice documents, .PDF and .txt (text files), databases, photos (jpg/jpeg), mp3 (music), mp4 (video), archives, .exe (application files), etc.
3. After infection these types of files will be stored in all folders which demand ransom in exchange for the decryption key. In this file they give their contact information for obtaining ransom (490\$ to 980\$ for this type DJVU/STOP) !!!OPEN_ME!!!, _readme.txt or _open_\DATA_FILES.txt, !!!CLICK_ME!!!

*In my case it was _readme.txt.

Working of the viruses [DJVU/STOP family]

- Command-and-Control [C&C] server is a method in which systems can be controlled by a cybercriminal. This cyber criminal sends commands and in return it receives stolen data from a target system/network using cloud-based services, such as file-sharing services, webmail.
- C&C servers also serve as the headquarters for infected machines in a botnet. The systems used by botnets follow these three models: the centralized model, the peer-to-peer [P2P] model, and the random model.
- Besides this just the presence of C&C the applications may also crash and the resources/data files can be misused.

Detection whether the decryption is offline/online

- Open PC in safe mode >>> uncheck the hide system file option of This PC folder options (view menu) >>> Open the PersonalId on location C:\SystemId\PersonalId
- If the file contains the codes with ending t1 that means the encryption key is offline otherwise online.
- ex: *****t1 (* can be any character/number) - offline.
- If the encryption key is online try to avoid internet connection till the virus is not removed. Also the retrieval of the original file is impossible even the super computer will take 1,00,000 years to decrypt the files. But you can recover the useful data.
- If the encryption key is offline, data recovery is comparatively easy.

Virus Removal method: To remove viruses there are two methods - Auto and Manual (for offline decryption). Auto method involves installing the well-paid anti malware software like MalwareBytes, Emsisoft anti malware. Just run the scan it will detect the viruses and just remove them. Now your system is free from viruses.

Antivirus scan reports (trojan names): Api.2ip.ua, Morgem.ru ; Antivirus detection: Troj/Emotet-CNM, Trojan.Agent.EWXA, Trojan.Agent.EWXL, Trojan.Agent.EWXC, Win32/Emotet.CB, Trojan.Emotet.ALX, Trojan-Banker.Win32.Emotet.pef, MSIL/Kryptik.XWJ, Trojan:MSIL/NanoBot.D!MTB

Manual Methods:

Disclaimer: As we are going to delete the malicious programs manually make a restore point because we are dealing with system and registry files. Also if in case you delete the incorrect file you should keep the scope to correct the mistake.

a. Manually deleting method:

Delete the following files

i. Go to location >> C:\Windows\System32\drivers\etc\hosts and delete the last added IP (internet protocol).

ii. Open Task scheduler >> If the Time Trigger task is present delete it.

Open Task Manager >> In startup disable all malicious programs >> go to the file location change the access from the properties and delete it.

iii. Click windows button + R >> Use command regedit to open registry editor and delete the unwanted registry files which are added by the virus from the following locations.

```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SysHelper
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOne
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

b. If you have restore point (which should obviously be before the infection date), Then your work becomes easy you can directly restore the system to that restore point date (mean your restore point will work as a checkpoint). Just select the date and click restore. Your system will now become the past system i.e malware free. In this process if you had made any changes, downloads between the restore point date and till now then that progress will also be lost. [The above method is applicable only for offline decryption because when the decryption is online it deletes all the restore points].

Results And Discussions:

By following procedure we can decrypt the files and recover the data:

Data Recovery / Decrypt files

Offline files decryption: Just install Emsisoft decrypter tool like a normal software from. Open it and select the drive where your encrypted files are present. Then choose the target location where the recovered files would be stored. Recommended : external drive like pendrive ,harddisk,etc.

> System Restore point (is available)

If this is the case then download shadow explorer and install it. Then open it and select the appropriate restore point. By this all the files which contain images ,videos,docs,etc will change to that specified date files and would easily get decrypted.

> Generalised Methods(for offline as well as online decryption)

i] Using PhotoRec software: In beginning remove the extension which was imposed by the virus in my case it was .kasp. For example img.jpg.kasp>>>img.jpg. Then download and install the testdisk software and then run qphotorec application qphotorec. It can recognize and recover 480 file extensions (which are nearly about 300 file families) including jpg,mp3,mp4,docs,.pdf,etc. Choose the target location where the recovered file would be saved. [Recommended : Use an external disk to take recovered files like hard disks,pen drives,etc].

ii] For recovering pdf files: You can just go to ILOVEPDF website where a pdf repair tool is present where we have to import the pdf file removing the malicious extension. Then download it and save it in an external disk. It will now open like before.

iii] For recovering psd,word,sql,excel,zip files using DataNumen: Just remove the malicious extension and now install DataNumen. Select the file and location and click on repair. Now go to any certain online editing website according to the files(extensions)

Example: For a psd file I will go to a photo editing website like photopea from there I will select the recovered psd file(output of datanumen) then I can download it or store it on the cloud.

Note: PhotoRec recognizes .word pdf .pdf extension as well but still I mentioned a particular method that is DataNumen and iLovePDF website for efficiency.

CONCLUSION

As we learned many types of viruses some can be removable,irremovable,mendable or even irremediable

so it is better to be on the safe side and practice the following measures to remain away from malwares.- When infected just take the system disc backup because it takes time to affect/modify data files.-Employ multi-factor authentication on all remote access points into an enterprise network to secure or disable remote desktop protocol (RDP) access[Thomas Roccia, 2020].-Use penetration testing to identify weak points in networks..-Backup all your important files, and store them independently from your system (e.g. in the cloud, on an external drive).-Always check and verify that you are on a company's legitimate website before entering your login details/sensitive information.-Ensure you have the latest legit anti-virus software installed on your computer and mobile devices.-Ensure secure email gateways to thwart threats via spam;Make your home network secure.-Disable third-party or outdated components of programs that could be entry points for malwares; Check regularly and update the privacy settings on your social media accounts.-Update passwords and ensure they are strong enough (a mix of uppercase, lowercase, numbers and special characters).-Do not click on links or open attachments in emails which seem unfamiliar to the subject /sender.

REFERENCES

- Brendan Smith, About DJVU/STOP Ransomware, September 2020.
- Brendan Smith, KASP Virus (.KASP File) Ransomware – How to Remove & Decrypt Files. Datanumen.com/download.
- Encyclopedia.kaspersky.com/knowledge/viruses-and-worms/ Emsisoft product download.
- Emsisoft:ransomware-decryption-tools/download/stop-djvu, Oct, 18, 2019.
- Enterprise.comodo.com-Rootkits definition. Ilovepdf.com/repair-pdf.
- K.A. Francis, How Has the Internet Impacted Businesses? | Small Business - Chron.com, February 12, 2019.
- Kaspersky.com/resource-center/threats/trojans.
- Kaspersky- What is Ransomware? Malwarebytes-download.
- Margaret Rouse,What is AES Encryption and How Does it Work?
- Norton.com internet security-malware-what-are-bots, Jan. 18, 2018.
- Peter W. Singer, Allan Friedman , Cybersecurity: What Everyone Needs to Know-2014, pg3-5.
- Photopea | Online Photo Editor.
- Photorec|File Support.
- Security Primer – Remote Desktop Protocol.
- Shadow Explorer Downloads.
- TestDisk Download.
- Thomas Roccia , Cybercriminals Actively Exploiting RDP to Target Remote Organizations , May 06, 2020
- Wikipedia-Bugs