IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

RAAS: Ransomware-as-a-Service

Harshada Umesh Salvi

Department of MCA, Finolex Academy of Management & Technology, Ratnagiri

Corresponding Author: harshada.salvi@famt.ac.in

DOI: https://doi.org/10.26438/ijcse/v7i6.586590 | Available online at: www.ijcseonline.org

Accepted: 10/Jun/2019, Published: 30/Jun/2019

***Abstract*—** Ransomware is a kind of malicious code, or malware, designed to deny access to a computer system or data till a ransom is paid. It generally spreads through phishing emails or by inadvertently visiting associate infected web site. Ransomware is not a brand new threat to the cyber world. Its origins dates back a few years. Over time, this threat has become more and more vicious and harmful. While people were contending with this cyber threat, cybercriminals moved one step further by providing ransomware-as-a-service (RAAS). This paper presents the overview of the RaaS kits. It focuses on the general working of the RaaS, five RaaS kits – Philadelphia, Stampado, Frozr Locker, Satan, Jokeroo. Nowadays it has become increasingly easy to create and launch ransomware, irrespective of skill. Anyone with an ill intent and access to the dark net can advertise the ransomware kits the way an online retailer promotes clothing or toys. This paper provides different defensive measures against ransomwares to individuals and organizations that they can adopt to protect themselves from the threat of ransomwares.

***Keywords*—** Ransomware, WannaCry, EternalBlue, Affiliates, Philadelphia, Stampado, FrozrLocker, Satan, Jokeroo

I. Introduction

Software as a Service (SaaS) is a cloud service model in which software is centrally hosted, licensed and distributed on a subscription basis.

With the rapid growth of the larger cloud computing market, SaaS can provide remarkable advantages in the business environment. But today criminals are exploiting this trend, which has led to the creation of Ransomware as a Service (RaaS), a growing threat to business.

Ransomware as a service (RaaS) is an online subscription-based ransomware distribution model in which third-party criminal entrepreneurs offers hackers and malicious users a platform tool for the purposes of using ransomware to hold computer files, information or systems hostage. Even the criminal with little technical skill can launch ransomware attacks without much difficulty using this model. For example, WannaCry caused severe loss across the world by using the NSA EternalBlue cyberattack exploit leaked by the Shadow Brokers hacking group [1].

RaaS is gaining popularity as it allows attackers lacking in coding skills to partner with ransomware creators who may not want to launch attacks themselves. Creators earn cash for writing and adapting code, while attackers can rent Ransomware.

II. Working of RaaS

Generally the working of Raas is as follows:-

1. RaaS creators host their ransomware code on a dark web portal.
2. This code can then be installed by RaaS affiliates (other cybercriminals) from a simple dashboard.
3. After installation affiliates can configure their new ransomware campaign, like the amount of ransom, the time intervals at which the ransom amount increases etc.
4. Affiliates then use their own means of infection.

Many ransomware codes are free to deploy. The RaaS creators shares in the affiliates' earnings. This works in the same way as the legitimate software affiliate program. When victims pay ransom in bitcoins to decrypt their data, payments are often delivered to the RaaS creator's account, who then distributes a share to the affiliates. The shares of affiliate can range from 60 to 80 percent. Indubitably this makes RaaS a very lucrative business for both RaaS creators and affiliates.

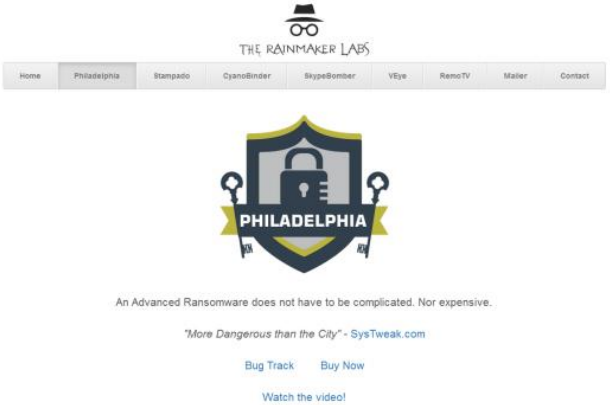
But nowadays RaaS creators are taking a more aggressive approach in advertising their offerings. While previously RaaS could be found on the Dark Web, attackers are now being bolder with promoting their RaaS Kits out in the open. They have started to use professionally produced video advertisements and a heavily designed website, to promote their latest RaaS offering. This aggressive advertising has only further highlighted how extensive this approach to ransomware is becoming.

III. TYPES OF RAAS

RaaS has almost certainly facilitated the global ransomware menace grow worse, and the number of available RaaS kits will only increase with time. Some of the notable RaaS are described below:

A. Philadelphia

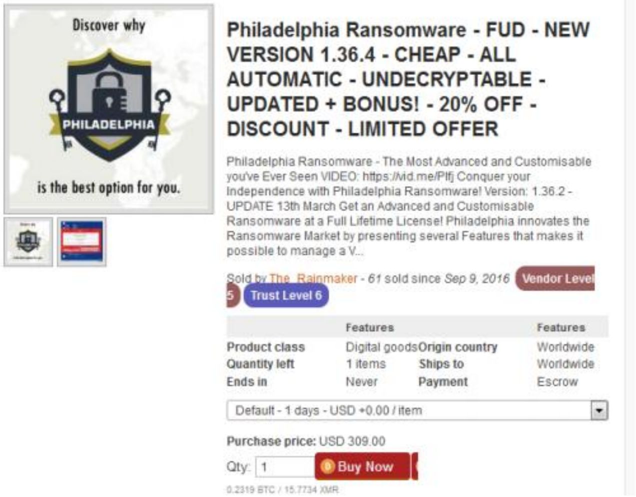
Philadelphia, the product of "The Rainmaker Labs" is one of the slickest example of RaaS which is sold for $389 to would-be cybercriminals [1]. The Rainmaker Labs have even created pretty aggressive advertising campaign and even includes a nicely made YouTube video showcasing Philadelphia's many features and customization. They advertise Philadelphia along with their other products.



An Advanced Ransomware does not have to be complicated. Nor expensive.

"More Dangerous than the City" - SysTweak.com

Fig. 1 The Website of Rainmakers Labs [1]



Discover why is the best option for you.

Philadelphia Ransomware - FUD - NEW VERSION 1.36.4 - CHEAP - ALL AUTOMATIC - UNDECRYPTABLE - UPDATED + BONUS! - 20% OFF - DISCOUNT - LIMITED OFFER

Philadelphia Ransomware - The Most Advanced and Customisable you've Ever Seen VIDEO: https://vid.me/Plfj Conquer your Independence with Philadelphia Ransomware! Version: 1.36.2 - UPDATE 13th March Get an Advanced and Customisable Ransomware at a Full Lifetime License! Philadelphia innovates the Ransomware Market by presenting several Features that makes it possible to manage a V...

Sold by The_Rainmaker - *61* sold since *Sep 9, 2016* Vendor Level 5

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	1 items	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 309.00

Qty: 1

0.2319 BTC / 15.7734 XMR

Fig. 2 Advertisement of Philadelphia Ransomware on AlphaBay offering a discount [1]

When attacker buys Philadelphia ransomware they get an executable file called Philadelphia headquarter. They have to set a username and a password. Using this credentials, they can access Philadelphia headquarter. Attackers then need to generate a PHP scripts called Bridges which run on web server chosen by them to setup a Philadelphia campaign. These Bridges will store the encryption key, information about the victim and used for the communication between attacker and the victim. They are also used to check if a ransom payment has been made.

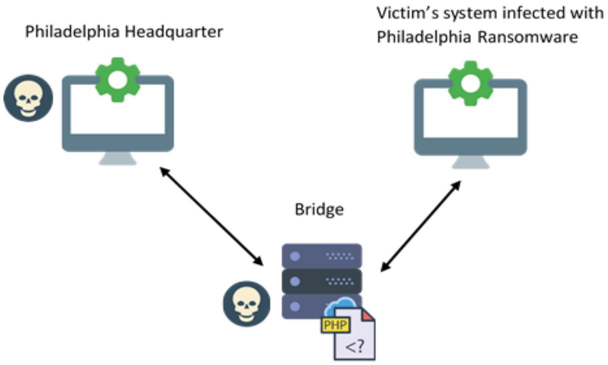
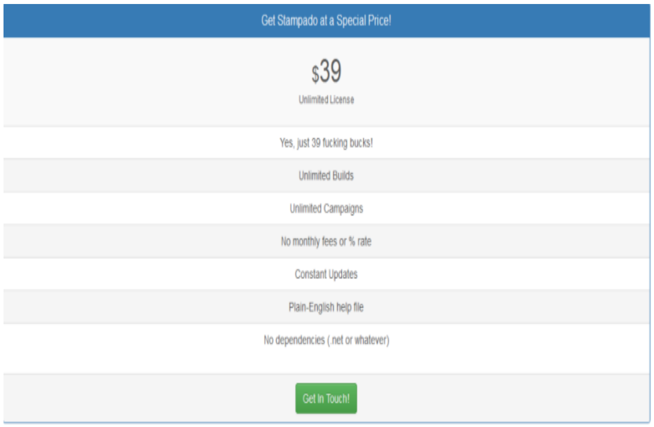


Fig. 3 Three systems and the communication channels between them

After the bridge is successfully set up, the attacker can generate ransomware samples called as agents. Several options to customize the generated ransomware are provided by the headquarter. Once all the features are set the ransomware can be generated. The result is a compiled AutoItscript.

B. Stampado

This RaaS which targets Windows OS was the first RaaS product of Rainmaker Labs launched in 2016. They started selling lifetime licenses for the low price of $39 offering customers the ability to customize various elements of the ransomware. It was promoted through aggressive advertising campaigns on the Dark web.



Get Stampado at a Special Price!

$39

Unlimited License

Yes, just 39 fucking bucks!

Unlimited Builds

Unlimited Campaigns

No monthly fees or % rate

Constant Updates

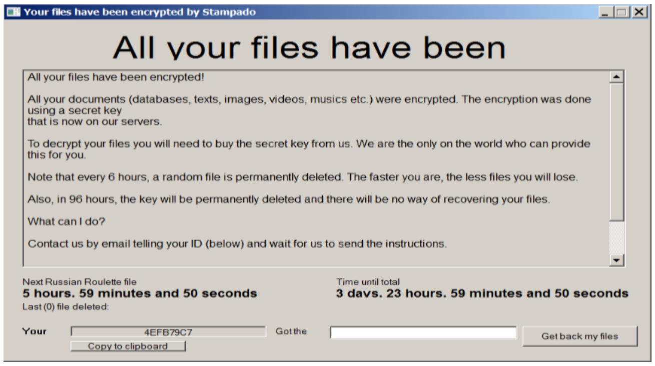
Plain-English help file

No dependencies (.net or whatever)

Fig. 4 Advertisement of Stampado on Rainmakers Lab website[2]

It sends malicious file to victims in one of the following file formats: *.exe*, *.bat*, *.dll*, *.scr*, and *.cmd [3]*. Stampado does not require administrator privileges to execute on victims' machines. It appends. locked to encrypted files, and gives victims 96 hours to pay the ransom before permanently deleting the decryption key.

It displays two countdown timers. One timer called as "Time until total loss" which is set to 96 hours displays the amount of time remaining until all of the encrypted data on the computer, decryption key will be deleted. The other timer called "Next Russian Roulette file deletion" which is set to 6 hours displays the amount of time remaining until a randomly selected encrypted file will be deleted if ransom amount is not paid. Each time this countdown timer reaches 0, the number of encrypted files deleted will be doubled.



Your files have been encrypted by Stampado

All your files have been

All your files have been encrypted!

All your documents (databases, texts, images, videos, musics etc.) were encrypted. The encryption was done using a secret key
that is now on our servers.

To decrypt your files you will need to buy the secret key from us. We are the only on the world who can provide this for you.

Note that every 6 hours, a random file is permanently deleted. The faster you are, the less files you will lose.

Also, in 96 hours, the key will be permanently deleted and there will be no way of recovering your files.

What can I do?

Contact us by email telling your ID (below) and wait for us to send the instructions.

Next Russian Roulette file
5 hours. 59 minutes and 50 seconds
Last (0) file deleted:

Time until total
3 davs. 23 hours. 59 minutes and 50 seconds

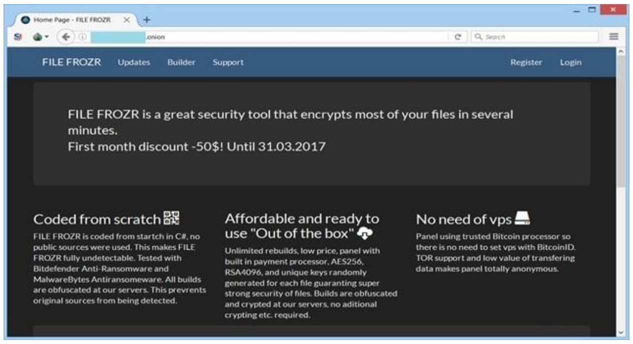
Your: 4EFB79C7

Got the:

Fig. 5 Stampado Lock Screen[4]

C. FrozrLock

A RaaS became available on the Dark Web in 2017, named FrozrLock. It was advertised under the tagline of "FILE FROZR is a great security tool that encrypts most of your files in several minutes. All that you earn yours, you pay once for a license, all further inspection are free." and was made available for only $50 discount on sales start according to the note of the advertising that the creator of FileFrozr did on sites, such as sinister.ly [5]. If the computer system is infected with this ransomware, then files with around 250 different extensions will get encrypted.



FILE FROZR is a great security tool that encrypts most of your files in several minutes.
First month discount -50$! Until 31.03.2017

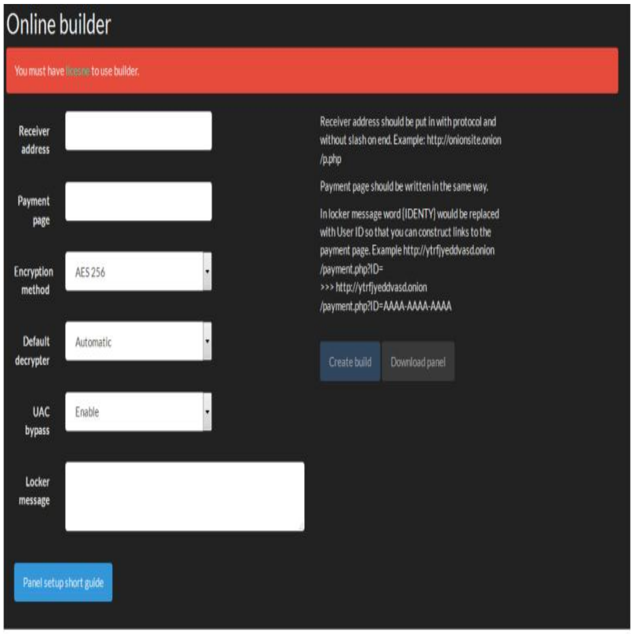
Coded from scratch
FILE FROZR is coded from startch in C#, no public sources were used. This makes FILE FROZR fully undetectable. Tested with Bitdefender Anti-Ransomware and MalwareBytes Antiransomeware. All builds are obfuscated at our servers. This prevrents original sources from being detected.

Affordable and ready to use "Out of the box"
Unlimited rebuilds, low price, panel with built in payment processor, AES256, RSA4096, and unique keys randomly generated for each file guaranting super strong security of files. Builds are obfuscated and crypted at our servers, no aditional crypting etc. required.

No need of vps
Panel using trusted Bitcoin processor so there is no need to set vps with BitcoinID. TOR support and low value of transfering data makes panel totally anonymous.

Fig. 6 FrozrLock Home page

Any attacker has to register on the site to gain access to an account. Once the account is created, they get access to the ransomware's web-based builder interface. According to the note on the Frozr Locker page people must acquire a license currently worth 0.14 Bitcoin (around $220) to use the builder and produce a fully-working ransomware [2]. It uses Twofish256, AES256, and RSA4096 encryption algorithms to encrypt the victim's files. This RaaS allows criminals to create as many ransomware builds as they want.



Online builder

You must have license to use builder.

Receiver address:

Payment page:

Encryption method: AES 256

Default decrypter: Automatic

UAC bypass: Enable

Locker message:

Receiver address should be put in with protocol and without slash on end. Example: http://onionsite.onion/p.php

Payment page should be written in the same way.

In locker message word [IDENTY] would be replaced with User ID so that you can construct links to the payment page. Example http://ytrfjyeddvasd.onion/payment.php?ID=
>>> http://ytrfjyeddvasd.onion/payment.php?ID=AAAA-AAAA-AAAA

Fig. 7 FrozrLocker configuration window

D. Satan

Satan is a ransomware that when executed in windows encrypts all the file and then demands a ransom for the decryption tools. The criminal who wants to launch ransomware attack has to sign up first. Then after login into the account he can create his own customized version of ransomware by configuring various settings of the Satan Ransomware like the ransom amount, by how much ransom amount should increase after a certain number of the days, and the number of days after which the ransom payment should increase, and infect as many systems as he wants. The Satan creators take 30% share of the ransom amount paid by the victims. Their share will vary depending upon the number of infections and ransom payments.

This RaaS also provides assistance to the criminals to distribute ransomware via spam or other means by providing tools to create malicious Microsoft Word Macros or CHM installer. They also provide translate facility to translate ransom notes into whichever language they want and help tips.

Once Satan ransomware is installed and executed it will inject itself into TaskHost.exe and start encrypting the data on the victim's computer. After encrypting files, it scrambles file name and append. stn extension to the file. At the same time, it creates a ransom note called HELP_DECRYPT_FILES.html in each folder containing encrypted files. It then wipes all data from the unused space on the C: Drive. At the last it displays ransom note showing victim's unique ID and URL to a TOR payment site [6].

E. Jokeroo

In February 2019 a new Ransomware-as-a-Service called Jokeroo was promoted on underground hacking sites and via Twitter. This RaaS allows criminals to allegedly gain access to a fully functional ransomware and payment server.

The affiliate has to pay to join a particular membership package. Different types of packages range from $90 USD to $300 and $600 packages. Affiliates can change and customize the ransomware and ransom note. The dashboard shows list of victims, time of infection, status of ransom payment, victim's IP addresses, Windows version, and geographic location [7].

IV. Defensive measures

While Ransomware-as-a-Service (RaaS) is a concoction and one of the latest threats to target on digital users, it is important to take some defensive measures to prevent this attacks. In addition to other basic security measures, you can also rely on advanced antimalware programs for better secure you against this threat. Paying a ransom does not guarantee the victim will restore their data. Despite paying ransom amount many victims are never provided with decryption keys.

Following are the defensive measures against ransomware in general:

- Take a backup regularly and keep a recent backup copy off-site - keep your information backed up in a safe area that hackers cannot easily access on i.e. an external hard drive and in the cloud like Dropbox/Google Drive/etc. Cloud backups add an extra layer of protection.
- Install a security software with the best defence against ransomware - Ransomware protection software will help to identify potential attacks. Windows Group Policy allows you to define how a group of users can use your system. It blocks the execution of files from your local folders like temporary folders and the downloads folder. This stops attacks that start by placing malware in a local folder which then opens and infects the computer system.
- Do not enable macros in document attachments received via email - Disable execution of macros in Office 2016. If company for some reason needs to run macros from Office documents, then set the settings to only allowed signed macros.
- Do not open unsolicited attachments – Do not open an email with the attachments .exe, .vbs, or .scr, even from a trusted source. Filter out and reject incoming mail with executable attachments. Configure your mail server to reject addresses of known spammers and malware.
- Update systems early and often. The system updates improve how well your computers work, and repair vulnerable spots in computer security. This way you can keep out attackers who might try to exploit software vulnerabilities in your system.
- Educate users by creating a cybersecurity culture – Train employees to recognize the signs of a phishing attack. Keep yourself and your employees updated on the latest cyber-attacks and ransomware. Make sure they know not to click on executable files or unknown links.

V. Conclusion

Ransomware has evolved as a serious threat to home users and organization and as a challenge to cyber security professionals, researchers with the development of cybersecurity. The paper presented a comprehensive overview of major ransomware as a service kits.

Despite the potential risks, the RaaS scheme remains highly attractive to criminals with limited skills. The would-be attackers with limited skills want to take advantage of the offerings, while malware authors continue to share their products for the most potential income. In the aftermath of the highly remarkable WannaCry and NotPetya attacks, we can expect the RaaS trend to gain even more popularity in 2019 as hackers look to get in on the action.

References

[1] D. Palotay, *Ransomware as a Service (RaaS): Deconstructing Philadelphia*. 2019, p. 3.

[2] B. Brenner, "5 ransomware as a service (RaaS) kits – SophosLabs investigates", *Naked Security*, 2017.

[3]A. ZAHARIA, "Security Alert: New and Cheap Stampado Ransomware for Sale on the Dark Web", *Heimdal Security Blog*, 2016.

[4] "Free Ransomware Decryption Tools | Unlock Your Files | Avast", *Avast.com*.

[5] "Ransomware FILEFROZR", *Sinister.ly*.

[6]L. Abrams, "New Satan Ransomware available through a Ransomware as a Service.", *BleepingComputer*, 2017.

[7] L. Abrams, "Jokeroo Ransomware-as-a-Service Offers Multiple Membership Packages", *BleepingComputer*, 2019.

Authors Profile

Miss. H U Salvi pursed Bachelor of Science from University of Mumbai, in 2005 and Master of Computer Application from from University of Mumbai in year 2008. She is currently working as Assistant Professor in Department of MCA, Finolex Academy of Management and Technology since 2008. Her main research work focuses on Ransomware, Cryptography Algorithms, Network Security, Cloud Security and Privacy. She has 11 years of teaching experience.