Gli specialisti italiani della Cyber Security

ZLAB Malware Analysis Report

Ransomware-as-a-Service platforms

CSE CyberSec Enterprise SPA
Via Giovanni Battista Martini, 6, Roma, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Ransomware-as-a-Service (RaaS)

Introduction

Across the years, the diffusion of darknets has created new illegal business models. Along with classic illegal goods such as drugs and payment card data other services appeared in the criminal underground, including hacking services and malware development. New platforms allows crooks without any technical skills to create their own ransomware and spread it.

A ransomware is a malicious code that infects the victims' machines and blocks or encrypts their files, requesting the payment of a ransom. When a ransomware is installed on a victim machine, it search for and targets sensitive files and data, including financial data, databases and personal files. Ransomware are developed to make unusable the victim' machine, the user has only two options: pay the ransom without having the guarantee of getting back the original files or format the PC disconnecting it from the Internet.

Ransomware history

The first ransomware was born in 1989, when 20000 floppy disks were dispatched as "AIDS Information-introductory Diskettes" and after 90 reboots, the software hid directories and encrypted the names of files on the customer's computer, claiming a ransom of $189. The payment had to be done depositing the request amount at a post office box in Panama.

After many years, in May 2005, GpCode, TROJ.RANSOM.A, Archiveus, Krotten and others appeared and in the threat landscape-

With the advent of the new anonymous payment method, such as Bitcoin, at the end of 2008, the ransomware has adopted mew payment methods.

Many ransomware families such as CryptoLocker, TeslaCrypt and Locky compromised an impressive number of systems worldwide, but the WannaCry Ransomware Attack is currently considered the most devastating cyber-attacks.

In a few hours after the discovery, the malware was able to infect more then 230k machines exploiting a vulnerability in the SMB protocol. Despite its unexpected worm-like behavior, WannaCry continued to encrypt the user files using the classic methods but asked a payment of 300$.

The samples related to the last ten years attacks, could be grouped in two different categories:

- Locker-ransomware: is a ransomware that locks users out of their devices
- Crypto-ransomware: is a ransomware that encrypts files, directories and hard drives

The first type was used between 2008 and 2011. It was discarded because it was quite simple to eliminate the infection without paying the ransom. In fact, the locker-ransomware has the weakness to show a window that deny the access to the computer, but the ransomware lock was easy to bypass.

The second type hasn't got this problem because crypto-malware hits directly the users files, let free the usage of system to the victim. Obviously, the user can't access to the information contained into the crypted files.

Then, the next ransomware uses the same crypting approach of the second ones, but they involve a combination of advanced distribution efforts and development techniques used to ensure evasion and anti-analysis, as Locky and WannaCry attest.

Obviously, the creation of a ransomware needs specific and advanced skills, but the great interest of criminal organization in the extortion model implemented by this kind of malware pushed the creation of new services that allows crooks to create their ransomware without having specific knowledge. Welcome to the **Ransomware-as-a-Service** (**RaaS**) business model.

Ransomware-as-a-Service

The raise of the RaaS business model is giving wannabe criminals an extremely easy way to launch a cyber-extortion campaign without having technical expertise, and it the root cause for flooding the market with new ransomware strains.

Ransomware-as-a-Service is a profitable model for both malware sellers and their customers. Malware sellers, using this approach, can acquire new infection vectors and could potentially reach new victims that they aren't able to reach through conventional approach, such as email spamming or compromised website. RaaS customers can obtain in easy way a ransomware via RaaS portals, just by configuring a few features and distributing the malware to unwitting victims.

Obviously, RaaS platforms can't be found on the clearnet, so they are hidden into the dark side of Internet, the Dark Web.

Surfing the dark web, through unconventional search engines, you can find several websites that offer RaaS. Each ones provides different features for their ransomware allowing users to select the file extensions considered by the crypting phase, the ransom demanded to the victim and other technical functionality that the malware will implement.

Furthermore, beyond the usage of RaaS platforms, the purchase of custom malicious software can be done through crime forums or websites where you can hire a hacker for the creation of your personal malware. Historically, this commerce has always existed, but it was specialized into cyber attacks, like espionage, hack of accounts and website defacement. Only when hackers understood it could be profitable, they started to provide this specific service.

The supply of this type of service is offered substantially in two ways: hiring someone to write a malware with the requirements defined by the customer or using a Ransomware-as-a-Service platform.

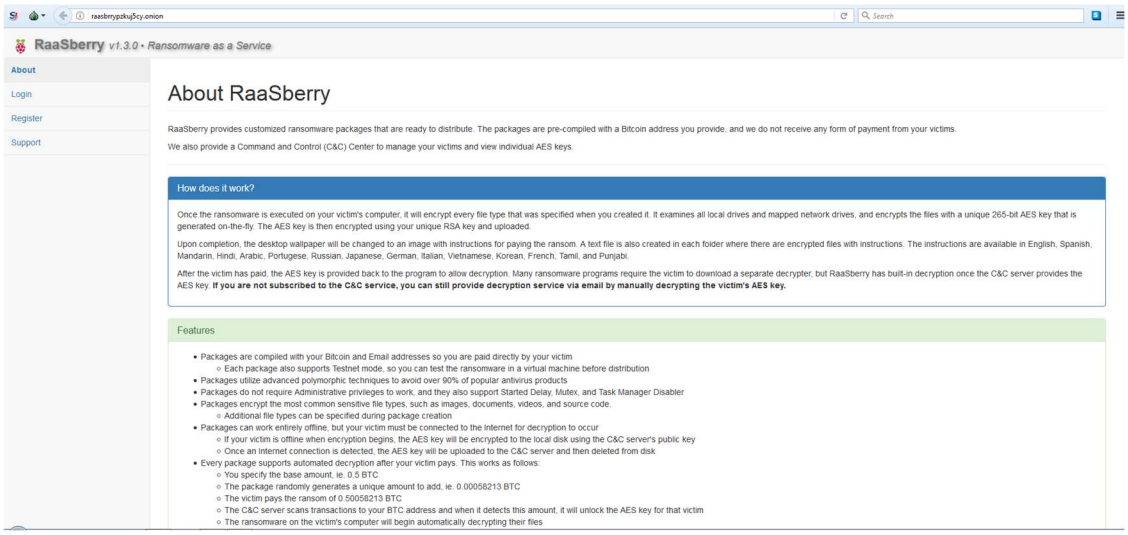
Raasberry

RaaSberry provides customized ransomware packages that are ready to be distributes. The packages are pre-compiled with a Bitcoin address provided by the customers, and the platform creators do not receive any form of payment from your victims.

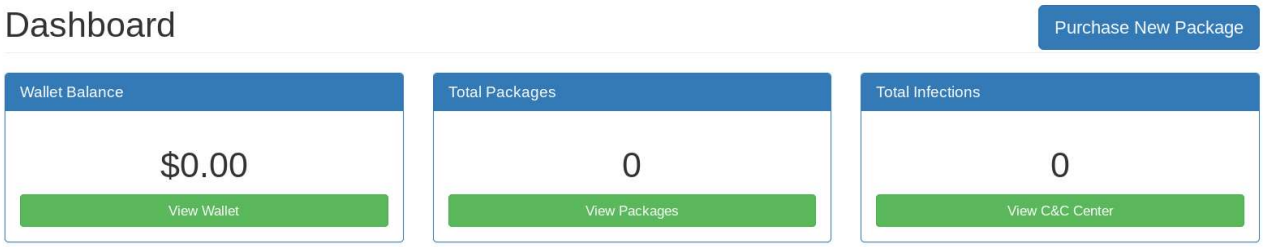
Once the ransomware is executed on your victim's computer, it will encrypt every file type that was specified when you created it. It examines all local drives and mapped network drives, and encrypts the files with a unique 265-bit AES key that is generated on-the-fly. The AES key is then encrypted using your unique RSA key and uploaded.

Upon completion, the desktop wallpaper will be changed to an image with instructions for paying the ransom. A text file is also created in each folder where there are encrypted files with instructions. The instructions are available in English, Spanish, Mandarin, Hindi, Arabic, Portuguese, Russian, Japanese, German, Italian, Vietnamese, Korean, French, Tamil, and Punjabi.

After the victim has paid, the AES key is provided back to the program to allow decryption. Many ransomware programs require the victim to download a separate decryptor, but RaaSberry has built-in decryption once the C&C server provides the AES key. If you are not subscribed to the C&C service, you can still provide decryption service via email by manually decrypting the victim's AES key. In this website there are several sections: About, Login, Register and Support. In the About section is described how you can create your personal ransomware.



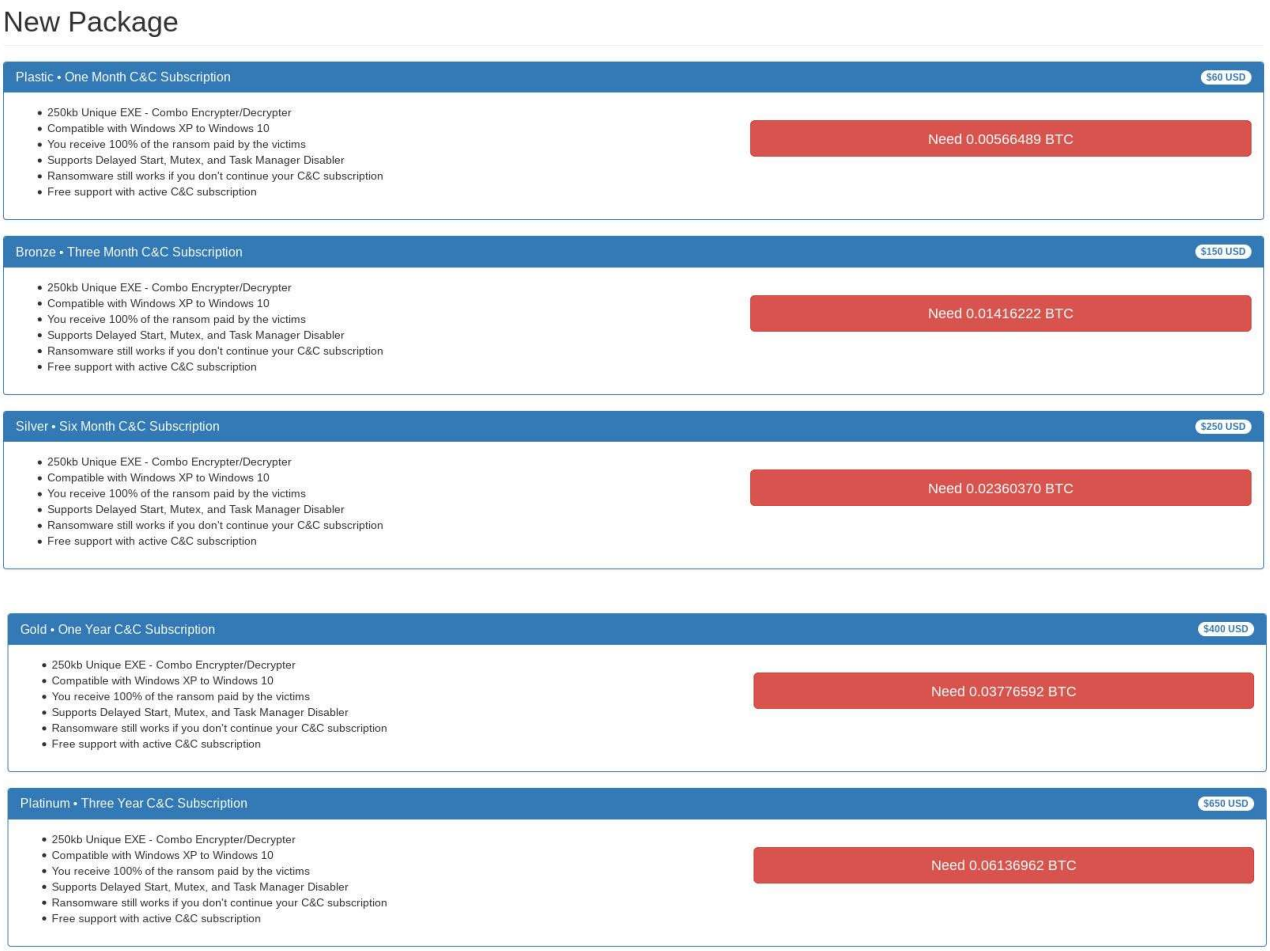
In the user's personal section are available a set of statistics about the ransomware campaign, keeping track of number of infections, number of paying people and the relative monetary earning.



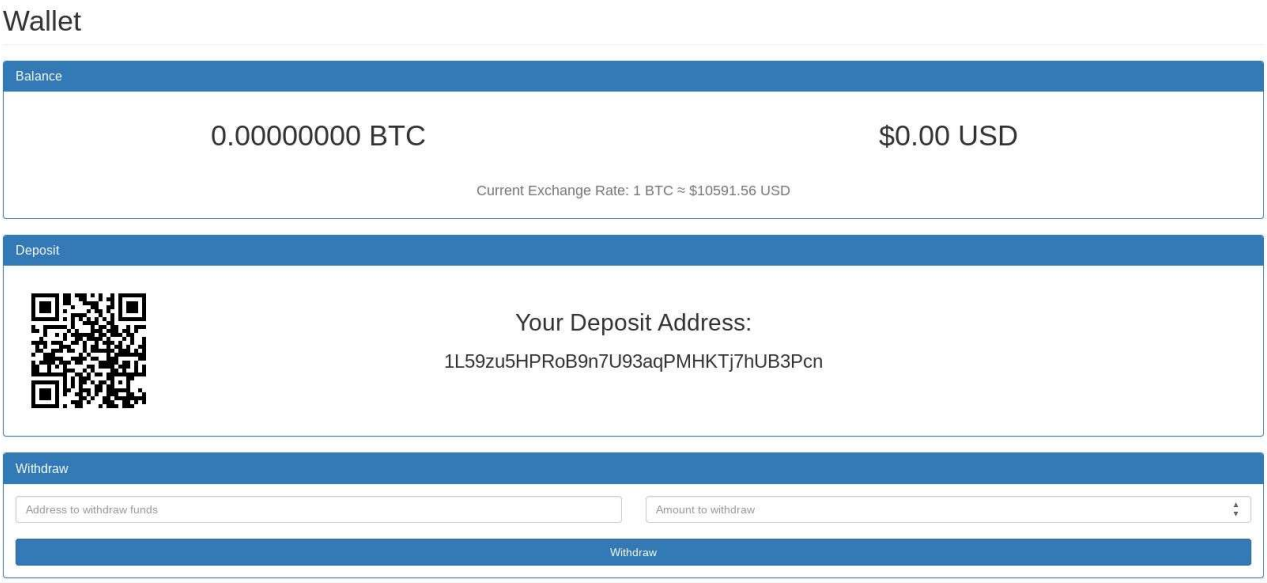
In this dashboard, you can purchase new packages that include, for each plan, the same ransomware but a different subscription time to Command and Control. As shown in the following figure, there are several plans:

- Plastic: One-month C&C subscription - $60
- Bronze: Three-month C&C subscription - $150
- Silver: Six-month C&C subscription - $250

- Gold: One-year C&C subscription - $400
- Platinum: Three years C&C subscription - $650



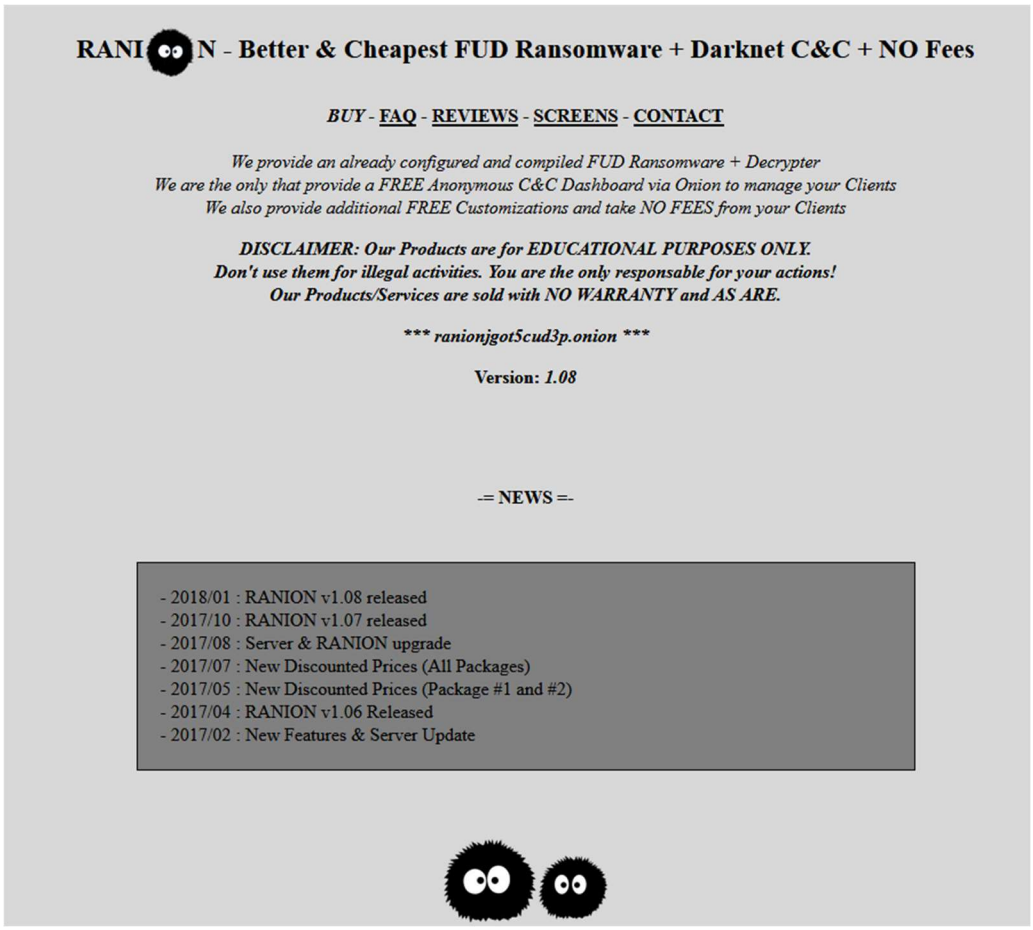
Once the users registered to platform and purchase new package, the platform assigns them a personal bitcoin address and they can control statistics about the ransomware campaign and check their earning.



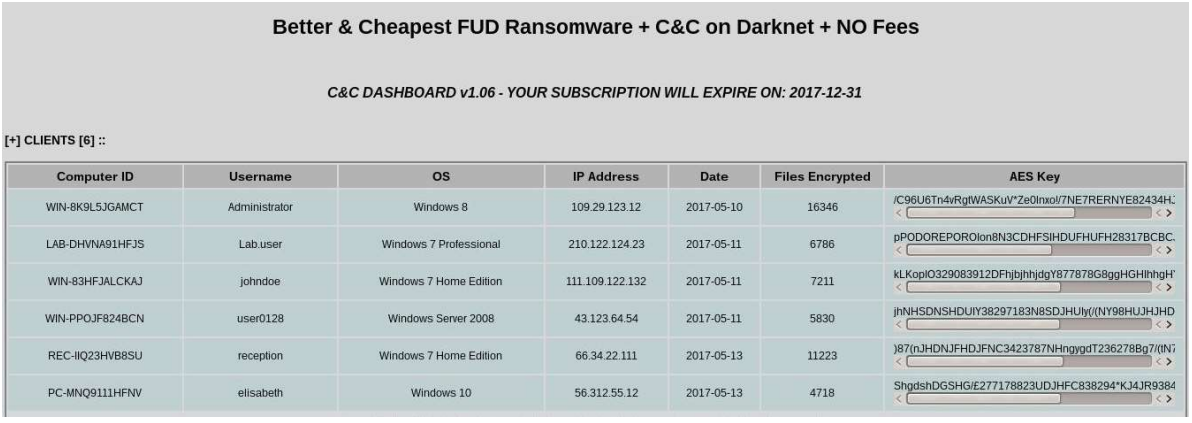
Furthermore, you can ask for assistance to the creator of this platform, sending an ad hoc email.

Ranion

Another platform that offers a similar service is Ranion. The novelty is that the Ranion team declares that the C&C of their “Fully UnDetectable”ransomware is established in the Darknet. This site is continuously updated by their operators.

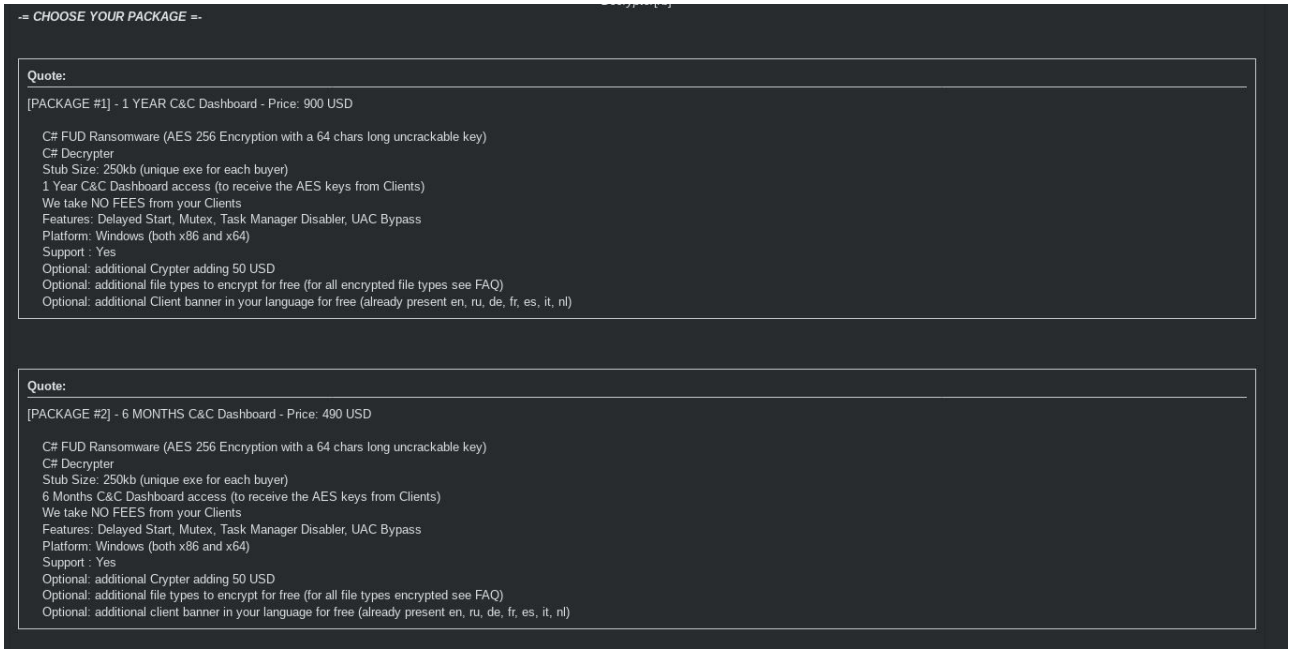


On their website, Ranion team shows an example of C&C dashboard. In the next figure, we can observe the subscription time and when it expires and also the infected machines classified by Computer ID, username of the victim, operation system, IP Address, date of infection, number of encrypted files and the relative encryption key.



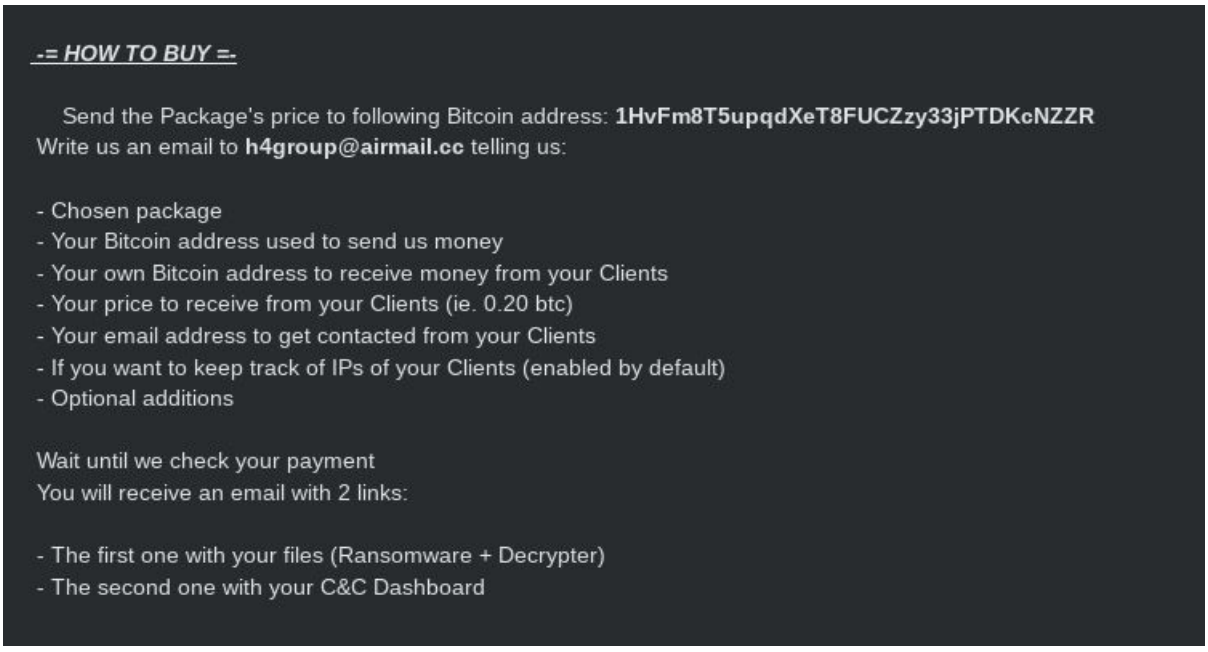
In this dashboard, users can purchase new packages that include, for each plan, the same ransomware but a different subscription time to the Command and Control. As shown in the next figure, there are two plans in which the

ransomware is the same, but there is a different subscription time to the C&C dashboard, and with, obviously, different prices.



In the next figure, is explicit the Bitcoin address, who send the package's price and email to contact, in that you must be declared:

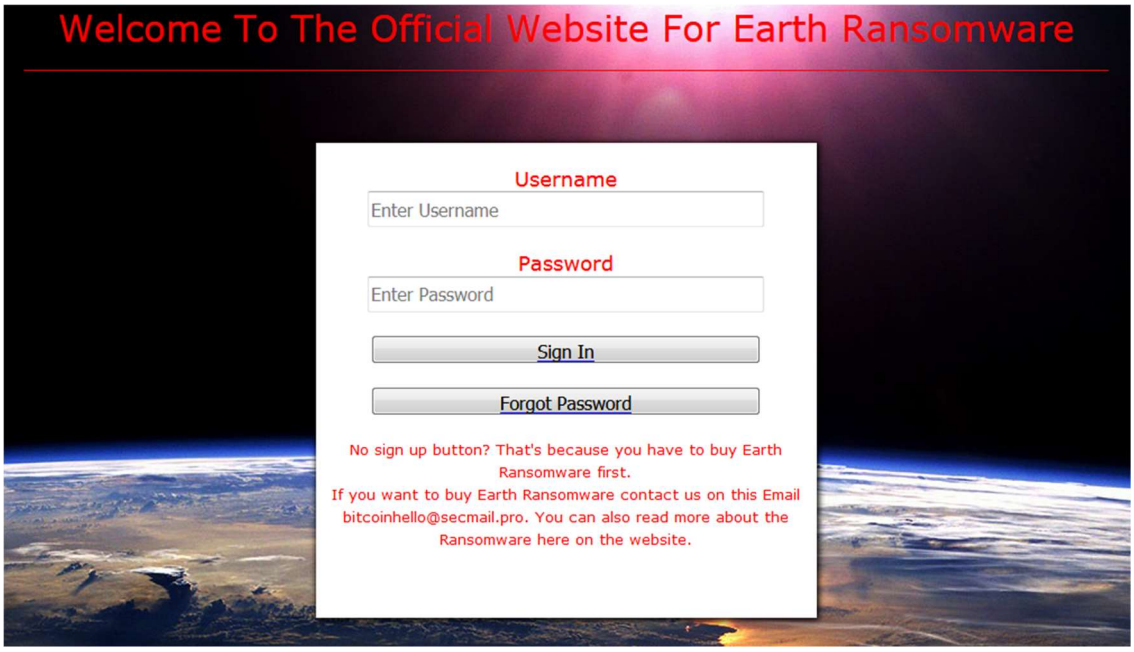
- Chosen package
- Your bitcoin address used to send money
- Your own Bitcoin address to receive money from your Clients
- Your price to receive from your Clients
- Your email address to get contacted from your Clients
- If you want to keep track of IPs of your Clients (enabled by default)
- Optional additions



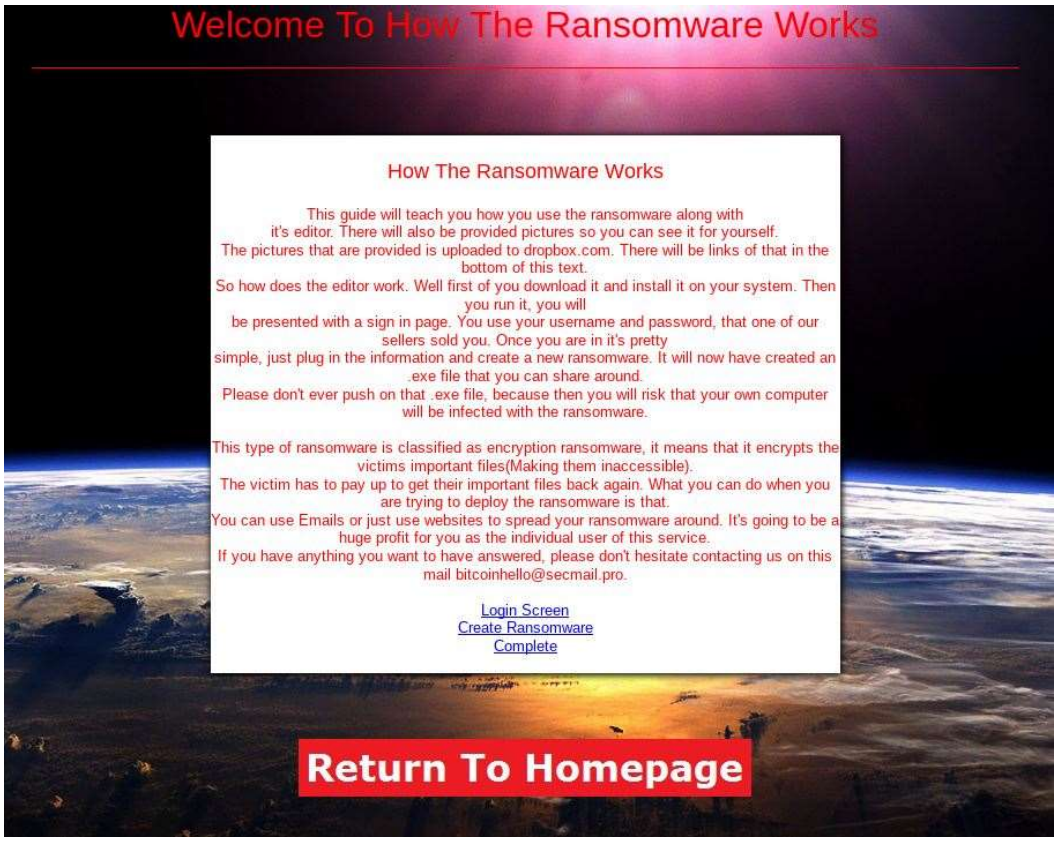
In the next figure is shown the Ransomware Decrypter, used by the victims to decrypt files with the key sent by the criminals once they have paid the ransom. Pressing the “decrypt my files” button, the decryption process of files starts.

EarthRansomware

Another RaaS platform is earthRansomware, the following page shows home page of the site, customers can login in the platform after buying their personal ransomware contacting EarthRansomware team by email.



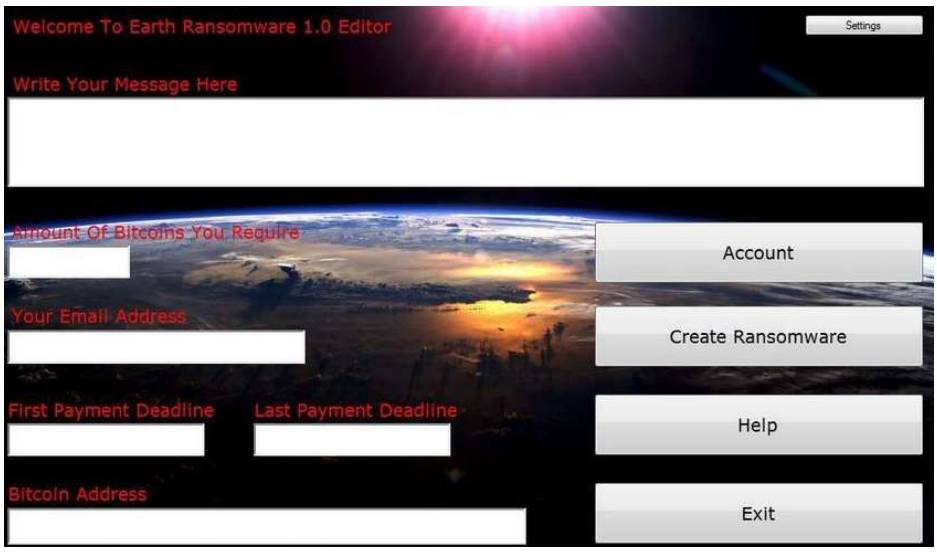
The web site included a session that provided step by step tutorial for services.



Unlike the previous RaaS, this one offers the fixed-rate service at the price of 0.3 BTC. When the customer pays the quote to the bitcoin address indicated in the mail, he obtains his credentials to enter in the personal section.

In this area of the site, users can customize their ransomware setting:

- Amount of bitcoins you require
- Your email address
- First payment deadline – Last payment deadline
- Bitcoin address



CSE CyberSec Enterprise SPA
Via Giovanni Battista Martini, 6, Roma, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

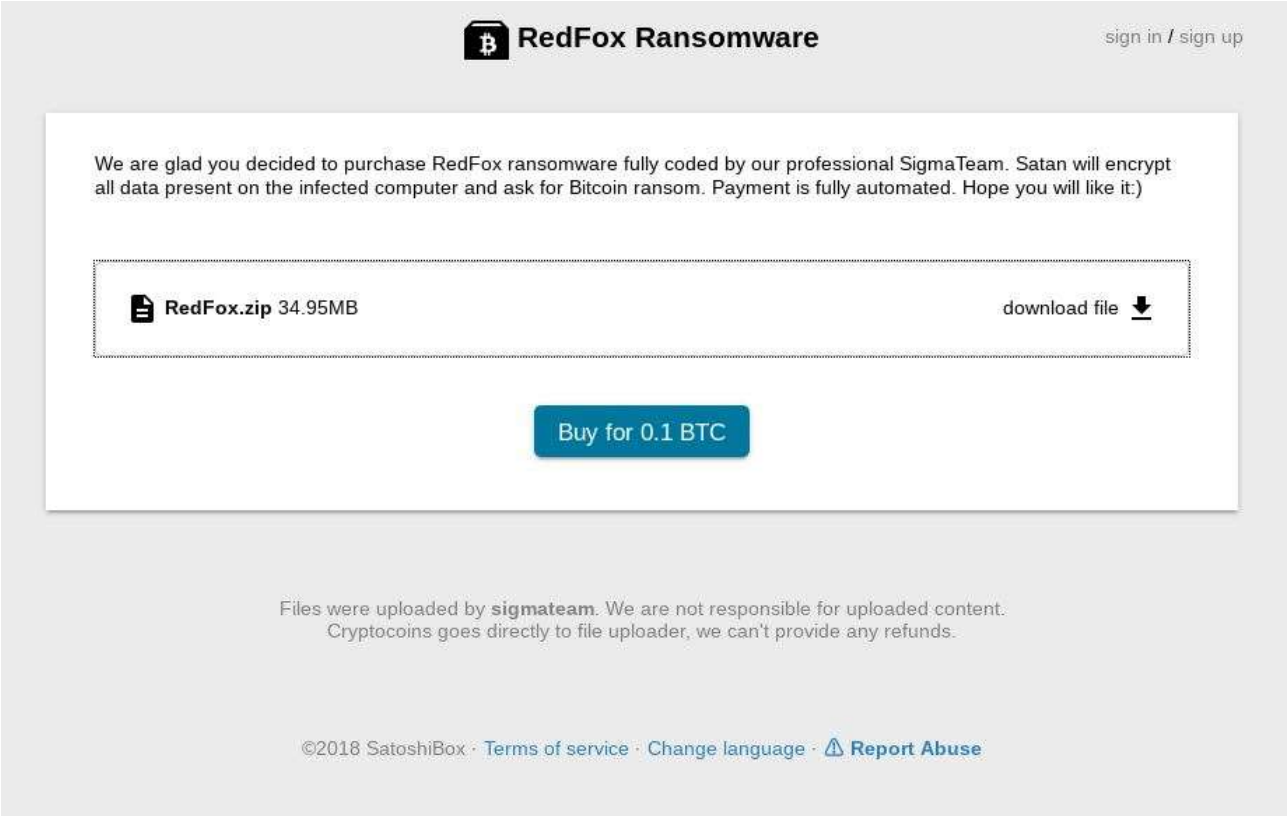
Once infected a system, the malware will show the ransom note notifying victims the deadline for the payment and instructions to pay the ransom.

Redfox ransomware

Redfox is singular Ransom-as-a-service platform because differently to the others it is hosted on the Clearnet. This ransomware, according the description provided by the developing team, is the most advanced and customizable malware. RedFox encrypts all user files and shared drives using the BlowFish algorithm.

The webpage says that the Command and Control, which is hosted in the Tor network, allows users to choose the ransom amount, the payment mode, payment deadline, personalize the ransom note and other technical features. The RaaS allows its customers to choose the usage of binders, packers and crypters to guarantee anti-analysis of the sample.

The website does not contain examples or tutorials about the command and control usage, however users can pay and download all the stuff needed to build up the criminal infrastructure.

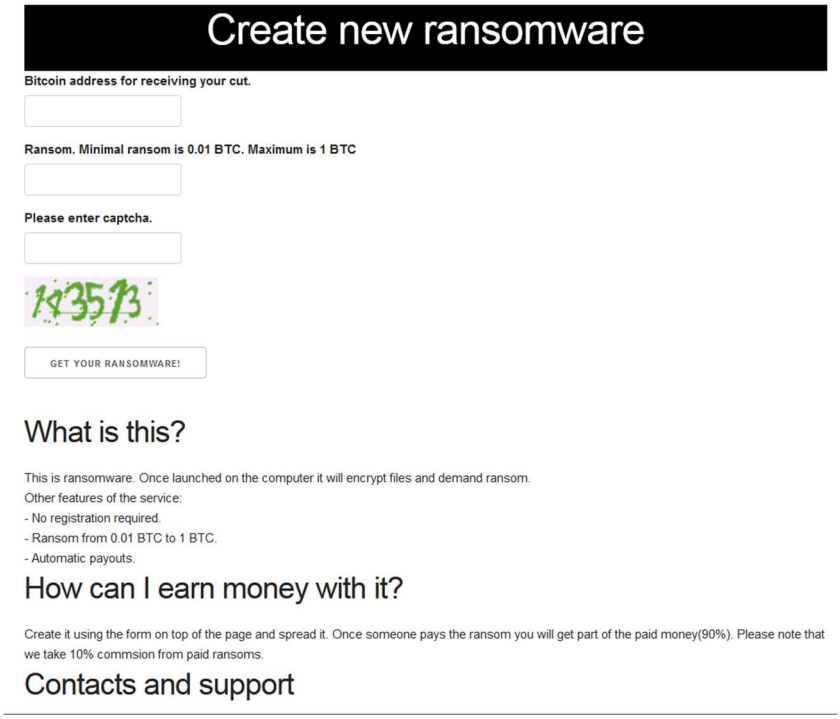


Createyourownransomware

A totally-free platform, found in the darknet, is Createyourownransomware, its website allows users to download a ready-to-go ransomware filling only 3 boxes in a form:

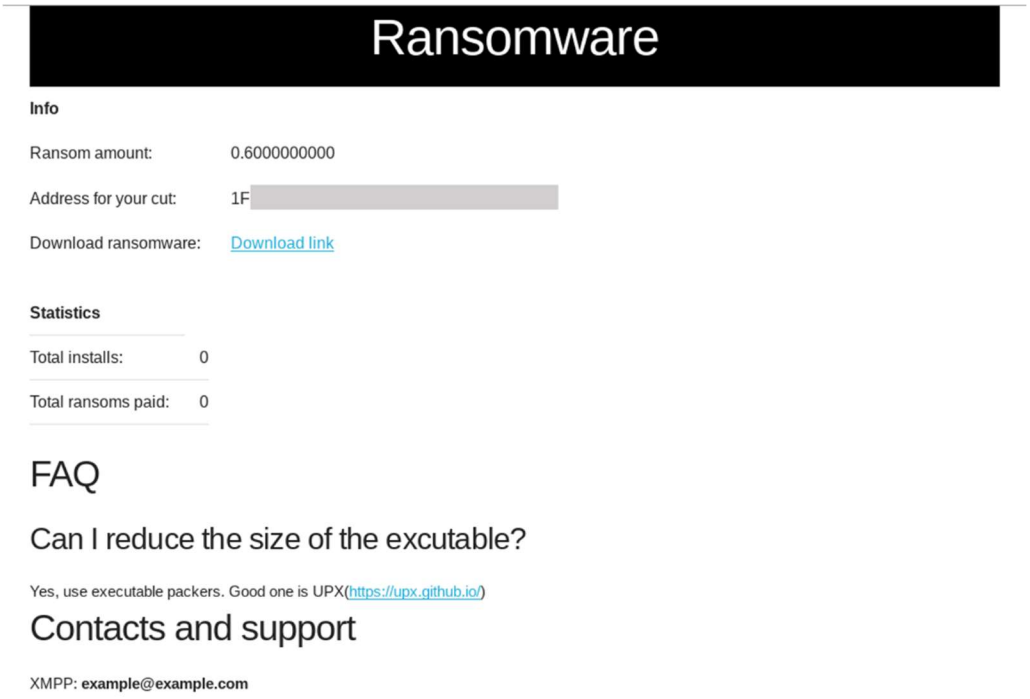
- the Bitcoin address in which you want to receive your “money cut”
- the ransom amount
- a simple captcha.

The “money cut” corresponds to 90% of the ransom amount, the remaining amount is the fee that RaaS administrators keep for them to provide the service.



Once the users have filled the form, the platform will instantly build a new sample and show the link to download the malware. Furthermore, a second webpage shows some statistics about the ransomware campaign, such as the number of infected machines and the number of the paid ransoms.

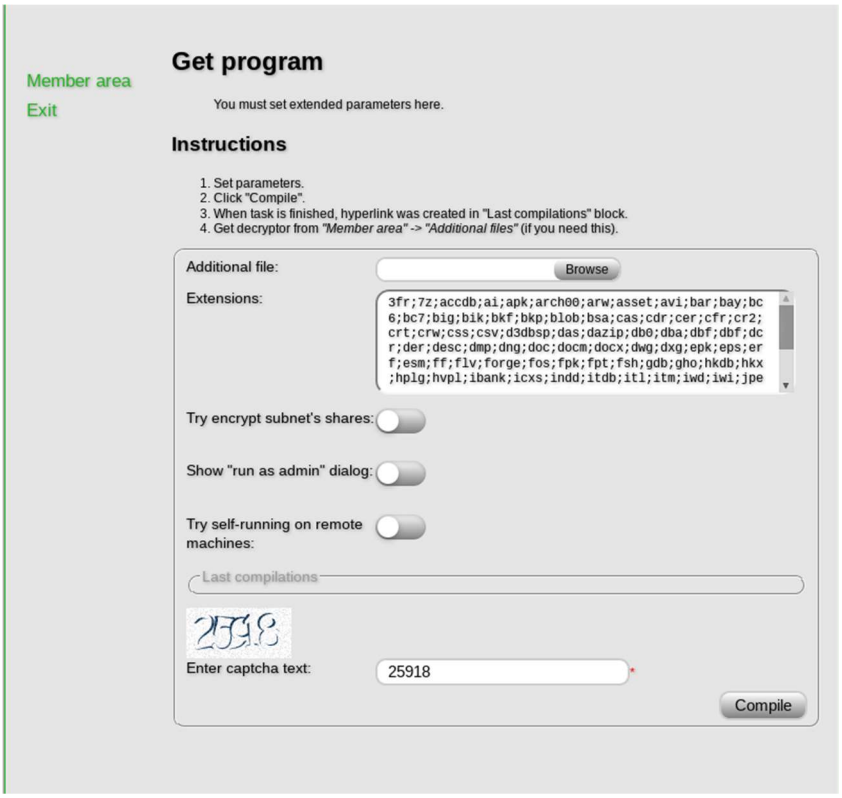
The user interface of the RaaS, unlike the previous platforms, is very minimal and provides only a few features.



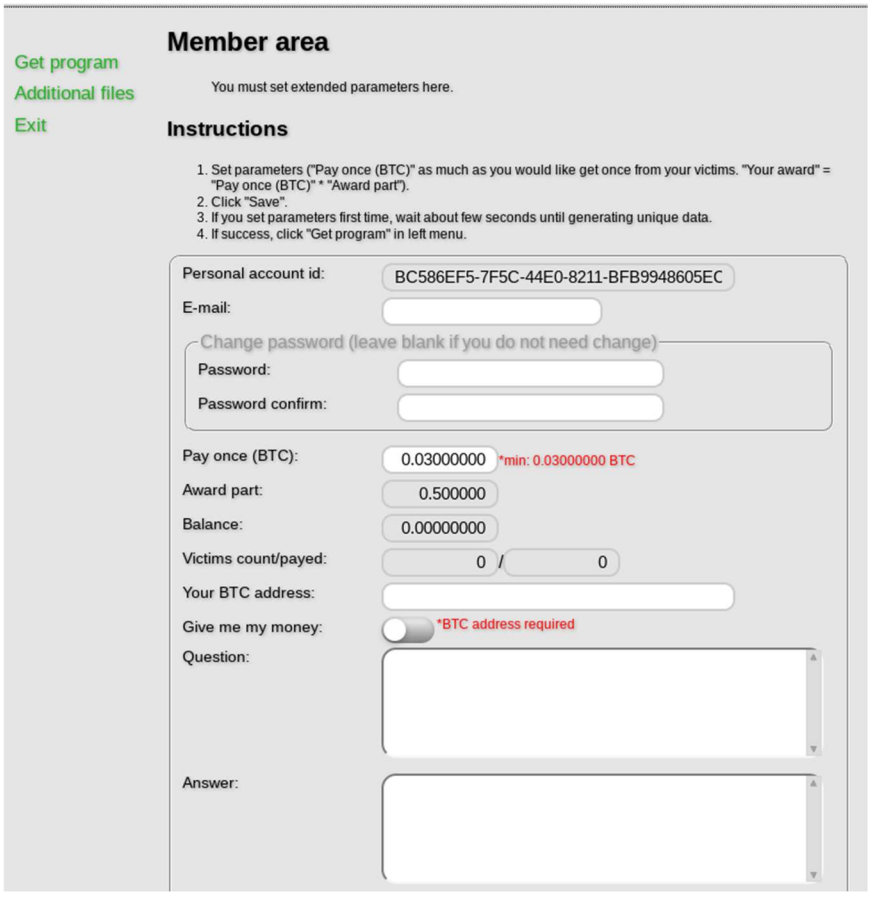
Datakeeper

Datakeeper, along with GandCrab and Saturn, is one the most recent RaaS platforms appeared in the threat landscape. The ransomware created through these platforms infected many machines at the beginning of the 2018 demonstrating the increasing interest in the use of the Ransomware-as-a-Service platforms. Currently, only Datakeeper service was not blocked by law enforcement.

When users register at the website, they can configure their ransomware by choosing a set of features. This platform seems to be one of the more completed because it allows to specify which extension of the files to encrypt.

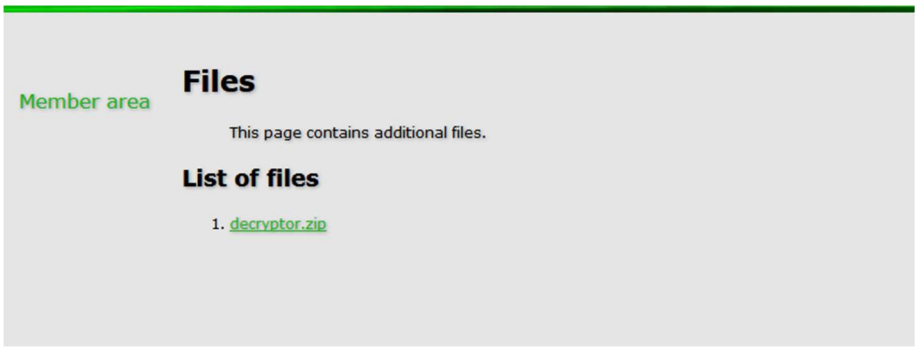


Datakeeper team holds 0.5 bitcoin as service fee for each infection.

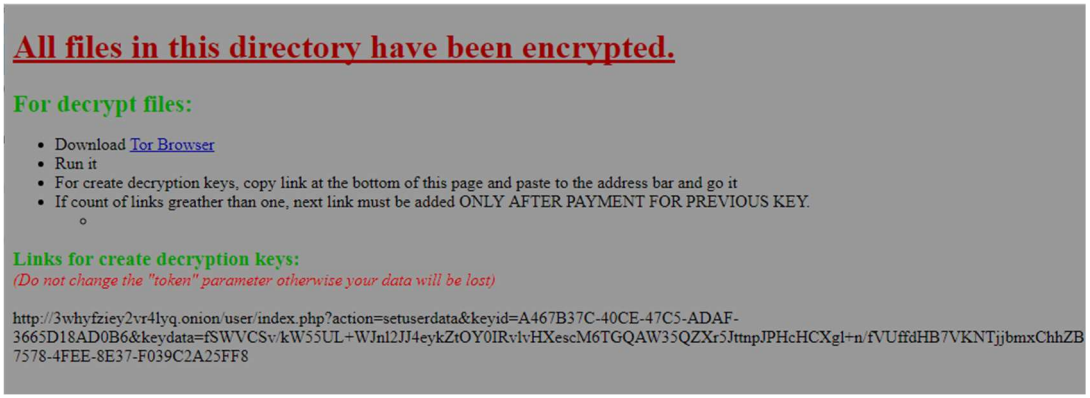


CSE CyberSec Enterprise SPA
Via Giovanni Battista Martini, 6, Roma, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

In the “Additional files” section, users can download the utility to decrypt the ciphered files.



The following figure shows an example ransom note dropped on the victim’s machine.



CSE CyberSec Enterprise SPA
Via Giovanni Battista Martini, 6, Roma, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com