GLOBAL CYBER SECURITY CENTER

Newsletter

2018 April

Cyber Security is our mission

editorial

Time for a new national currency?

The cryptocurrency market, the exchanges in the digital money market, have induced in us different states from the excitement to the fright for a phenomenon that is still not very clear to all the people that are not in this business. We have seen the Bitcoin, in the last months, oscillating in value on the market reaching unimaginable values for a currency and then going down, a swing that has confused many fueling discordant voices about its future.

Certainly, the phenomenon of the crypto currencies is destined to remain and there are many analysts who claim that this digital currency will partly replace the national currencies because of its efficiency and independency.

Is the cryptocurrency the bank end? For sure banks need to take Bitcoin seriously, an alert that was issued also by Christine Lagarde lately. Of course, the lack of intermediaries and peer-to-peer transactions make the cryptocurrency particularly attractive for investors with the possibility of cutting the costs of financial intermediation.

Startups that offer innovative solutions in the financial sector, based on these technologies, are multiplying as well as the *Initial Coin Offering* (ICO).

The ICO tool is very widespread and is a financing way for starting new fintech companies. In short, in order to obtain funding, the project that will be implemented through Blockchain, is proposed to the public by creating "tokens" that will be sold, against a fee, to the subjects that are financing the idea. The last noisy ICO was announced by Telegram (TON), the TON platform claims to be the fastest and inherently scalable multi-blockchain architecture. This project by Telegram that is combining minimum transaction time and maximum security, may position TON as a VISA alternative for the decentralized economy.

But what's happening in Naples? The municipality has published an invitation (http://www.comune.napoli.it/blockchain) for expert in the blockchain sector to form a study group on this topic. A voluntary work group that faces a series of ambitious goals.

The local administration wants to explore the possibility of using blockchain in administrative processes and verify the feasibility of inserting cryptocurrency payments for some local services. The project aims to get a fundraising campaign through ICO and distribute a new cryptocurrency that is linked to the city's economy.

Time ripe for a new alternative currency? Could Naples be one of the laboratories? Surely this initiative could open up new interesting scenarios which will certainly be joined by a growing number of initiatives.

Enjoy your reading

Nicola Sotira
General Manager GCSEC

events

EuroCyber: Are you business-ready for GDPR?

Location: Rome, Italy
Date: May 9-10, 2018
https://skytopstrategies.com/eurocyber-2018-italy/

GDPR Implementation and its Impact on Multinational Company Compliance and Cybersecurity. The EU General Data Protection Regulation (GDPR) is set to take effect May 25, 2018 and with it comes a host of changes to personal data protection laws. GDPR aims to ensure that those processing personal data are doing so in a way that is consistent with disclosure, that data is kept safe, not kept for longer than is needed and that the person whom the data is about retains control over the data.

This full day discussion will focus on how companies are efficiently implementing and complying with GDPR and understanding the consequences of non-compliance, as well as discussing how companies based outside of the EU who do business within the EU are affected by GDPR.

Mediterranean PPP Congress

Location: Noto, Italy
Date: May 10-11, 2018
https://cybersecurity-mediterranean.it/

With the support of the most important French and Swiss Business Chambers and Associations, “Cybersecurity – Switzerland” aims to bringing together International security experts as well as Decision Makers, both from State and Private sectors. The most important role an NGO like Swiss Webacademy could play in a world full of daily cybersecurity meetings is to create a rupture event, made with security specialists covering the broadest spectrum of topics, networking and discussing with CEOs and State administration about the issues raised, in a fully international atmosphere to understand differences, practices and macro-regional needs.

Cybersecurity Summit Milano 2018
The Future of Cybersecurity in the Age

in this number

Cryptocurrency-Mining Malware

by Gianluca Bocci – CERT, Poste Italiane

According to the data provided by Clusit, the damages caused by cybercrime in Italy can be estimated in about 10 billion of euro, in 2016. A worrisome phenomenon that registered costs for 500 billion of dollars in 2017 (5-fold higher than 2011) and has involved 1 billion of people so far. Cybercrime attacks are continuously increasing, for a lot of different reasons: geopolitic interests, industrial espionage, terrorism and much more. In less than 5 years, Cyber-attacks have grown globally of more than 240%. One of the worst attacks occurred in 2017 - WannaCry – was a malware attached to an email that has encrypted and compromised sensible and personal data from many public and private companies, hospitals, schools and individual citizens. They have not always been recovered, even after paying a conspicuous amount of money in bitcoin (therefore the name "ransomware"). This is exactly why cyber criminals have paid much attention towards the cryptocurrencies in the recent years, focusing their efforts in generating "Cryptocurrency-mining malware". Moreover, the strong appreciation for the values of the cryptocurrencies, in 2017, has attracted the interests of the cybercriminals as well as that of the "traditional" investors. The Cryptocurrency-mining malware developed ad-hoc to compromise the computers; take advantage of the computing activities of the infected machines to create virtual currency as Bitcoin, Monero and Ethereum. In fact, cyber criminals are aware how much it costs to generate cryptocurrency in terms of energetic expenditure, thus have created new strategies to produce it at no costs. The researchers of Proofpoint have discovered a huge botnet (named Smominru) that using the exploit "EternalBlue SMB (CVE-2017-0144)", allows the control of the computers running Windows OS, produces the cryptocurrency Monero, illegally creating a counter value of millions of dollars. Since its activation in May 2017, the botnet has infected more than 500000 computers lacking of a patch, especially in Russia, India and Taiwan. This type of malware does not involve any download of application for the victim's computer (fileless), it requires only the presence of the malicious code in the memory and it shows a particular resistance to the antivirus programs. Recently, CrowdStrike has talked about the malware WannaMine: identified it exploits this kind of approach to create crypto currency. As it has happened for the ransom wares, also the scenario of the cryptocurrency-mining malware is evolving, and we can only imagine how many types of attacks will be developed. Another technique uses the so-called "Cryptojacking": the ad hoc JavaScript code is embedded into the not necessarily compromised websites, so it canuse the computational capacity

of Digital Transformation.
Location: Milano, Italy
Date: May 30-31, 2018
https://www.theinnovationgroup.it/events/cybersecurity-summit-2018-2/?lang=it

The "CYBERSECURITY SUMMIT 2018" will open with an EXCLUSIVE AND INVITATION event on the afternoon of 30 May, while the SUMMIT will be held on 31 May 2018 in Milan with the participation of Keynote Speaker and the best Italian and international experts. The Cybersecurity Summit by Innovation Group creates a unique opportunity to exchange experiences and networking, discuss and deepen, to understand how ICT security needs are evolving, what are the most current countermeasures to adopt, how to design and develop solutions innovations of Cyber Risk management.

news

Google to banish cryptocurrency mining extensions from official Chrome Web Store

https://securityaffairs.co/wordpress/71007/security/ban-cryptocurrency-mining-extensions.html

Google will ban cryptocurrency mining extensions from the official Chrome Web Store after finding many of them abusing users' resources without consent.

The number of malicious extensions is rapidly increased over the past few months, especially those related to mining activities.

The company has introduced a new Web Store policy that bans any Chrome extension submitted to the Web Store that mines cryptocurrency. "Until now, Chrome Web Store policy has permitted cryptocurrency mining in extensions as long as it is the extension's single purpose, and the user is adequately informedabout the mining behavior." reads a blog post published by Google

Mirai Variant Targets Financial Sector With IoT DDoS Attacks

https://threatpost.com/mirai-variant-targets-financial-sector-with-iot-ddos-attacks/131056/

A variant of the Mirai botnet was used to launch a series of distributed denial of service campaigns against financial sector businesses. The attacks utilized at least 13,000 hijacked IoT devices generating traffic volumes up to 30 Gbps, considerably less intense than the original Mirai assaults clocked at 620 Gbps.

Researchers at Recorded Future said the Mirai botnet and malware variant also exhibited characteristics that may link it to IoTroop botnet (or Reaper), first identified October 2017. The most recent attacks spotted by Recorded Future took place between Jan. 27 through 28. They reported three distinct attacks. The first attack utilized a DNS amplification technique with traffic volumes peaking at 30 Gbps.

of the computers to produce virtual currency.

```
<link rel="shortcut icon" href="/favicon.ico">
<link rel="stylesheet" href="http://localhost/css.css" type="text/css">
<link rel="stylesheet" type="text/css" href="/stdtheme.css">

<style type="text/css">
    div.html5header #header_icons #header_html5{
        background:url('img_logo_map.gif') 0 0;background-repeat:no-repeat;
    }
    div.html5header #header_icons #header_multimedia{
        background:url('img_logo_map.gif') -104px 0;background-repeat:no-repeat;
    }
    #header_text {
        font-size:120%;
```

In general, the insertion of a malicious JavaScript could occur using the vulnerabilities (low credentials) of the FTP services used to update the websites, rather than known vulnerabilities of the applicative functioning as system management that have already been patched. It has been discovered recently that Piratebay, one of the most famous website of file sharing based on the BitTorrent protocol, was infected whit such a type of code, in particular through the "embedding" of the Coin-Hive script. An interesting description of this type of attack is provided by the ENISA, the European Agency for the Security of the Network and the Information, that also makes available the list of some cases that have been identified and analysed, as well as the information on how protect your systems from the attack. The mobile devices are not safe from this attack; recently almost 50 million of Android OS-based smartphones have been infected with a malware which generates the crypto currency Monero, the only available from the mobile devices. Erroneously, this kind of malware is considered as a minor danger as it does not involve the loss of sensible and personal data, or money either; indeed they have such a behavior able to exhaust the capacity of the CPU, therefore increasing the temperature and, in case of the mobile devices, causing mechanical changes, reduction of the battery life and, even at a lower extent, damaging the “chip". It is difficult to contrast this kind of phenomena, especially if we consider also the users that, voluntarily, compute to create crypto currencies. Moreover, this kind of malware has reached a high level of sophistication to elude the protection and to work without notice: for example, it is able to deactivate the antivirus or to block the mining activities when the applications used by the legitimate owner of the computer or mobile device require computational resources that, if reduced, would generate an alert. As remembered by the ENISA, in order to prevent the "crypto jacking" attacks, it would be useful to always ask the user for the explicit consent to use the JavaScript code, install an ad-blocker to filter the spam messages and the malicious scripts used by the browser (even through the use of ad hoc extensions), to always update the operating system, to install all the suggested patches both at systemic and applicative level and remove the browser extensions that are obsolete as a future update could make them malicious.

Researchers are unsure what the volumes of subsequent attacks were.

HTTP Injector Attacks Harvest Mobile Data Connections

https://sensorstechforum.com/http-injector-attacks-harvest-mobile-data-connections/

A dangerous new malware tactic is used by hackers that are actively using a HTTP injector method that can hijack Internet access. The required tools are being sold and traded on the underground hacker markets and forums as one of the most popular items currently available. The HTTP injectors modify the sent Internet packets in order to overcome security and access measures placed by Internet service providers (ISPs) and businesses. This is one of the most widely used ways by enterprises to control overall web users. Public Wi-Fi hot spots, restaurants and hotels are among the locations where it is most likely to use captive portals. The attack begins with a mobile device loaded with a SIM card with zero carrier balance. Using the installed browser the criminals connect to a data-free site in order to avoid the captive portal connection. Using the HTTP injector tools a SSH proxy tunnel is created in order to bypass the protection.

Crooks distribute malware masquerade as fake software updates and use NetSupport RAT

https://securityaffairs.co/wordpress/71193/malware/netsupport-rat.html

Researchers at FireEye have spotted a hacking campaign leveraging compromised websites to spread fake updates for popular software that were also used to deliver the NetSupport Manager RAT. NetSupport is an off-the-shelf RAT that could be used by system admins for remote administration of computers. In the past, crooks abuse this legitimate application to deploy malware on victim’s machines. Researchers at FireEye have spotted a hacking campaign that has been active for the past few months and that has been leveraging compromised websites to spread fake updates for popular software (i.e. Adobe Flash, Chrome, and FireFox) that were also used to deliver the NetSupport Manager remote access tool (RAT).

PinkKite: The continuing threat of POS malware

https://www.scmagazineuk.com/pinkkite-the-continuing-threat-of-pos-malware/article/752891/

POS systems are unique, typically single-purpose and require limited software to function. Defenders should use this to their advantage, and enable application whitelisting to prevent unwanted or modified processes from running.

Point-of-Sale, or POS, systems are often targeted by cyber-criminals due to the high return on investment for success, potentially thousands of credit card numbers and details. Unlike many other devices targeted by criminals, POS systems are semi-unique in that they are often dedicated devices with limited resources and run specialised, and frequently non-upgradable software.

Ransomware-as-a-Service (RaaS)

by Antonio Pirozzi – Director of Malware Research Lab of CSE

Introduction

In these years, the Darknet has created new illegal business models. In fact, over the classic illegal contents, like drugs, weapons and killers, other services are born in order to allow to speculate and to earn. In information security context, you can find hacking services and illegal software development, such as malicious software. The new trend consists of platform usage that allow even the inexpert people to create ransomware on demand.

A ransomware is a malicious code that infects the victims' machines and blocks or encrypts their files, claiming a ransom. When ransomware is installed on a victim machine, it looks for and targets sensitive files and data, such as important financial data, databases and personal files. They are designed to make unusable the victims' machines. Then, the malware demands to pay a ransom for the encrypted user data showing a window or creating some text files containing the payment instructions. 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 marked the beginning of maximum spread of this kind of malware.

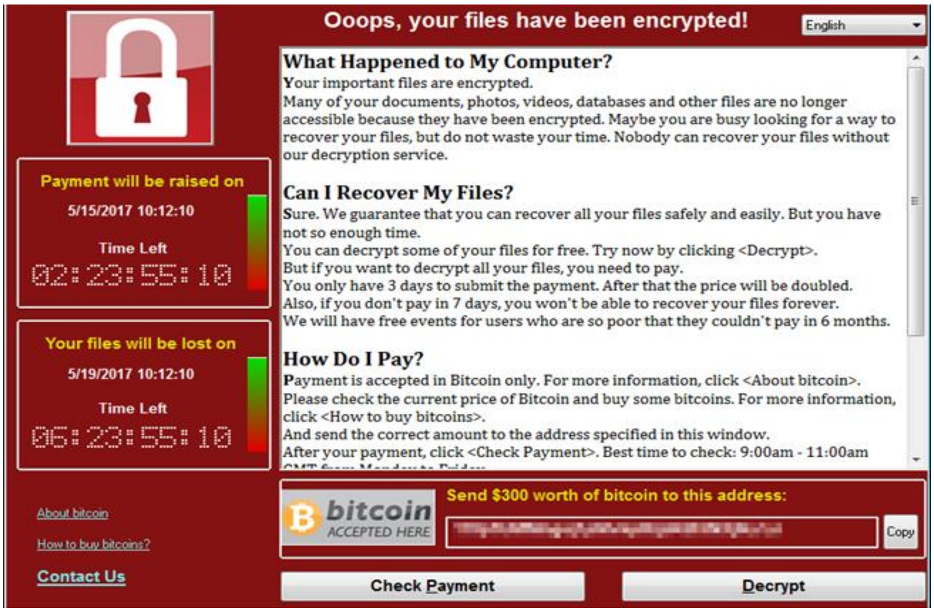
With the advent of the new anonymous payment ways in the end of 2008, such as Bitcoin, the ransomware has changed the approach of demanding ransom payment.

After many ransomware family, such as CryptoLocker, TeslaCrypt, Locky and others, in the 2017, WannaCry Ransomware Attack terrified most country in the world thanks to its worm behavior, with which the malware was able to spread in more of 230k machines exploiting a vulnerability of SMB protocol. Despite its unexpected worm behavior, WannaCry continued to encrypt the user files using the classic methods but asked a payment of 300$ in Bitcoin to send to a provided Bitcoin address.

2017 – The year of ransomware

The past year was the worst for the ransomware attacks spread in the worldwide. There were at least three ransomware attacks which made economic damages for millions of dollars.

The first one was WannaCry which hit every type of infrastructure, starting from communication companies, like Telefonica, FedEx and Deutsche Bahn until English hospital agencies. It propagated through EternalBlue, an exploit in older Windows systems released by The Shadow Brokers a few months prior to the attack. While Microsoft had released patches previously to close the exploit, many organizations that had not applied these or were using older Windows systems that were past their end-of-life..



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

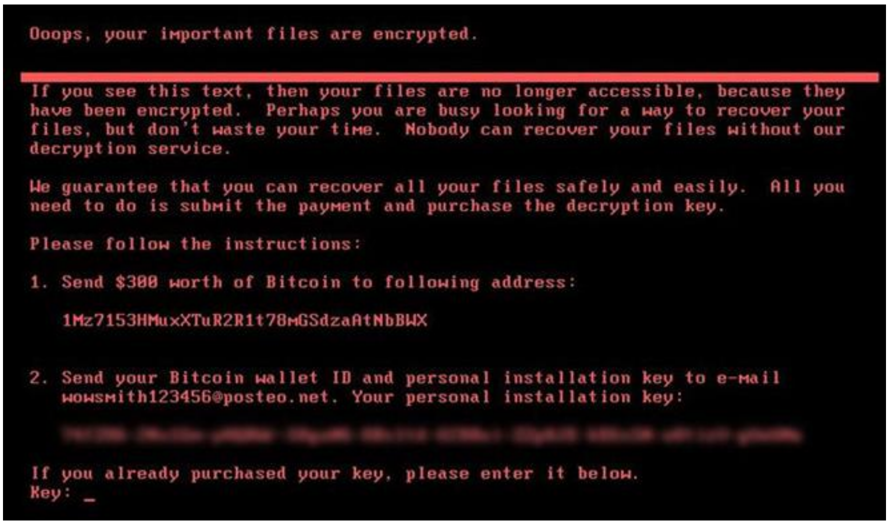
Payment will be raised on
5/15/2017 10:12:10
Time Left
02:23:55:10

Your files will be lost on
5/19/2017 10:12:10
Time Left
06:23:55:10

Send $300 worth of bitcoin to this address:
[redacted]

Figure 1 - WannaCry ransom note

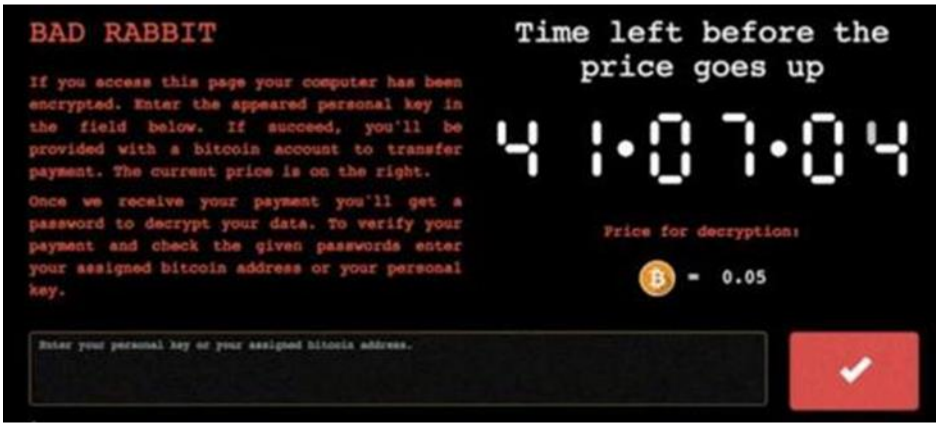
The second one is NotPetya, the evolution of another infamous ransomware, known as Petya spread in the wild in 2016. This ransomware propagates with the same exploit of WannaCry, EternalBlue. The characteristic of this malware is that it was designed not to be a ransomware, but a wiper, because it encrypts the Master Boot Record of the machine and due an algorithmic error, it was not possible to restore the previous condition and data are definitely lost.



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   [redacted]

If you already purchased your key, please enter it below.
Key: _
```

Figure 2 - NotPetya ransom note

The last terror of the computer systems was Bad Rabbit. It was the evolution of NotPetya ransomware and targeted principally Turkey, Germany, Poland, Japan, United States and other countries. But the major damage was occurred at the Odessa airport of Ukraine. It is interesting to note that the malware doesn't explicitly implement a wiper behavior, suggesting the operators are financially motivated. However, the onion website used for the payment is no longer available, this implies that victims cannot pay the ransom to decrypt the file. This behavior could be intentional and used by attackers to hide as a distraction tactic.



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

41:07:04

Price for decryption:

B - 0.05

Enter your personal key or your assigned bitcoin address.

Figure 3 - Bad Rabbit payment site

Ransomware general features

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

- 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 it was simple to bypass the ransomware lock.

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. So, 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 capabilities, in addition to the development effort. This makes ransomware an instrument for few people. To meet the needs of people who want to take revenge, make money or just for fun, new services are born to facilitate the "buying & selling" of malicious software. So, a new approach was born: **Ransomware-as-a-Service** (**RaaS**).

Ransomware-as-a-Service

The rise of the RaaS distribution model is giving would-be criminals an extremely easy way to launch a cyber-extortion business with virtually no technical expertise required, flooding the market with new ransomware strains in the process.

Ransomware-as-a-Service creates a new business model because it allows to earn both malware sellers and customers. Malware sellers, using this approach, can acquire new infection vectors and new victims which they aren't able to reach through conventional approach, such as email spamming or compromised website. RaaS customers can obtain in easy way technological weapon logging into RaaS portal, configuring the features and distributing the malware to unwitting victims. The goals can be different and are related to make easily and fastly money or to make vengeance against someone.

These illegal platforms can't be found on the Clearnet, so they are necessary 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 of ransomware creation and platform owner payment, allowing you 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 proper website in which you can engage 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. Thus, the supply of this type of service is offered substantially in two ways: the first is to hire someone to write a malware with the requirements defined by the customer and the second is to use a Ransomware-as-a-Service platform.

In the following table are synthetized the principal platforms on the Darknet of Rent-a-Hacker and Ransomware-as-a-Service.

	Rent-A-Hacker Services
X-Hacker	XHacker is a classic platform to provide a rent-a-hacker service. This hacker establishes a minimum price for a job is 200 dollars. In order to contact him, he publishes an email address attaching his PGP public key.
Hacker for Hire	It provides several hacking services, like cyber-bullism, cyber extorsion, social account hacking and more other stuff. There is a pricing list of all operations.
HXT	HXT offers an "elite hacking" services, including DDoS attacks, personal accounts' compromising, botnet and, last but not least, Ransomware on demand too. For each service the hackers show a price list and the most expensive is properly RaaS.
PirateCRACKERS	This site provides several services, such as Email and cell phones hacking, social media hacking, DDoS attacks and malicious software creation. For each service there is a price list, which makes explicit that the payment must be done in Bitcoin.
Rent-a-Hacker	He can do economic espionage, network and website compromising, DDoS attacks and hacking activity in general. Instead of pricing the hacking service types, he prices services based on the jobs dimension (small, medium and large).
	Ransomware-as-a-Service Platforms
Raasberry	In this platform there are a personal section, in which you can see statistics about your ransomware campaign, keeping track of number of infections, number of paying people and the relative monetary earning. There is a dashboard in which you can purchase new packages that include, for each plan, the same ransomware but a different subscription time to Command and Control. There are several plans, from plastic to platinum. Once you registered to platform and purchase new package, the platform assign you a personal bitcoin address and you can control statistics about your ransomware campaign and check your earning.
Ranion	This platform declares that the C&C of their "Fully UnDetectable" ransomware is established in the Darknet. In the dashboard, you can purchase new packages that include, for each plan, the same

ransomware but a different subscription time to Command and Control. There is a section of Ransomware Decrypter, in which the victim inserts the key, sent by the criminal once he has paid the ransom. After you press decrypt button, start the decryption process of files.

EarthRansomware

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 the editor area, you can create your personal ransomware in which you can set the number of bitcoins you require, email address, First payment deadline – Last payment deadline and bitcoin address. After the infection, the ransom note is shown to the victim, where are indicated the encrypted files, the deadline for payment and, obviously, the bitcoin address.

Redfox

The novelty of Redfox is that it’s hosted on the Clearnet. RedFox encrypts all user files and shared drives using BlowFish algorithm. The webpage says that the Command and Control, which is hosted over Tor, allows you to choose ransom amount, ransom note, payment mode, payment deadline and other technical features, such as the usage of binders, packers and crypters to guarantee anti-analysis of the sample.

Createyourransomware

It’s a totally-free platform. In its website you can download a ready-to-go ransomware filling only 3 form-boxes: the Bitcoin address in which you want to receive your “money cut”, the ransom amount and a simple captcha. As the website shows, the “money cut” corresponds to 90% of the ransom amount, instead the remaining amount is for the service fee. We can see some statistics about the ransomware campaign.

DataKeeper

The only platform not seized yet is DataKeeper service. When you register at the website, you have the malware configuration page, where you can choose the malware capabilities and some other configuration settings. This platform seems to be one of the more completed because it allows to specify which extension of the files to encrypt.