Name

Cryptojacking

Date of Birth

2011

Origin

Clues point to Russia.

Modus Operandi

Cryptojacking uses other people's devices without permission to mine cryptocurrencies illegally.

Attackers make use of malware to take over computers, tablets, or smartphones and take advantage of their processing power to mine cryptocurrencies in secret, using the devices' energy resources.

Most cryptojacking attacks use CoinHive code to mine cryptocurrencies

Arrest

This threat has already been arrested and neutralized by Panda Security.

But if you are not a Panda Security client and you catch sight of it on the company network, contact us immediately to facilitate its capture.

info@pandasecurity.com

Criminal Record

Smominru

At the start of 2018, Smominru was discovered. It is a piece of malware used to mine Monero, and which had infected over half a million machines since May 2017, mainly in Russia, India and Taiwan. It is estimated that the cybercriminals had already made up to $3.6 million.

Adylkuzz y Wannamine

One of the most problematic vulnerabilities in 2018 has been EternalBlue, which was also used by WannaCry. This vulnerability was how Adylkuzz got onto systems. This malware was used to generate Monero, and infected thousands of computers all around the world. In fact, it is believed to have affected even more computers than WannaCry.

Attack on DoubleClick

Towards the end of January 2018, YouTube was found to be affected when it was discovered that, hidden within its ads was malicious code, putting numerous users at risk. In this case, the advertising platform DoubleClick was the victim of an attack that hid the CoinHive cryptojacking code in YouTube adverts..

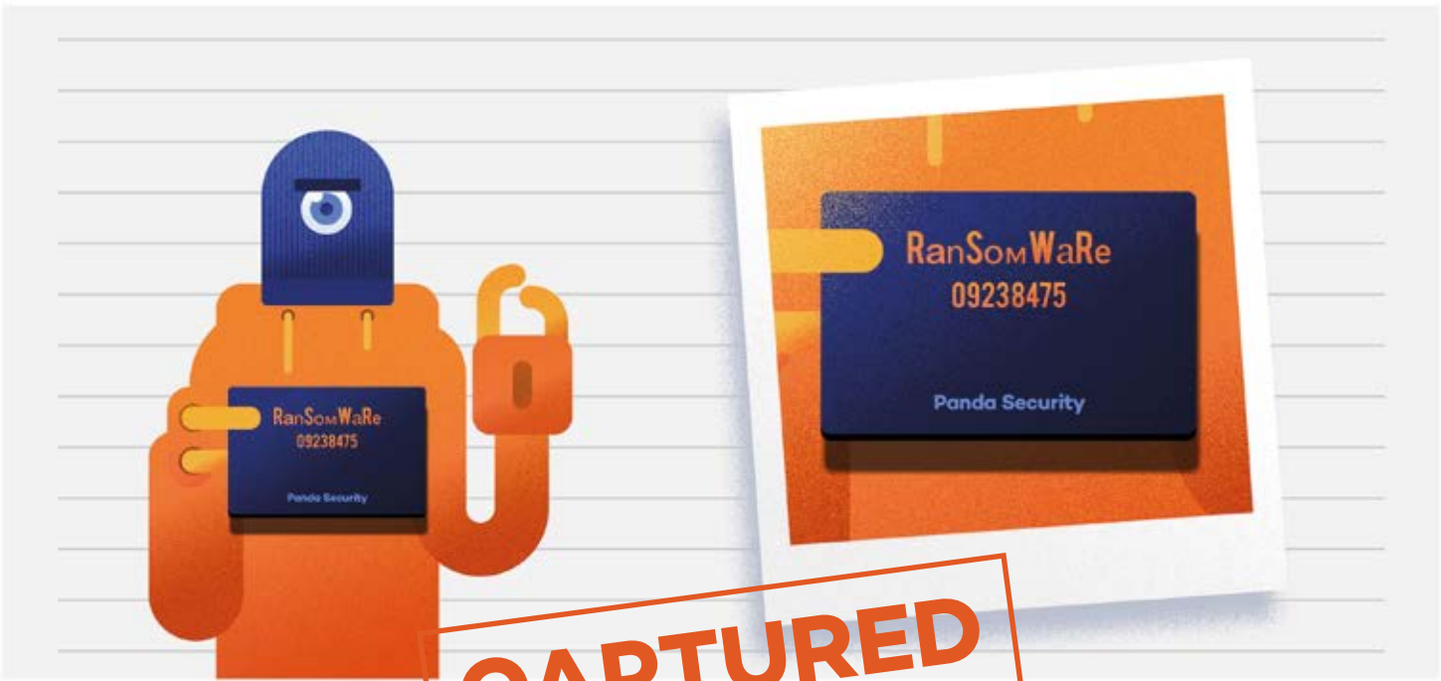
WinstarNssmMiner

In May 2018, another particularly dangerous piece of malware called WinstarNssmMiner infected half a million computers in three days. This malware got in using phishing emails and infected websites. Once on a system, it used all of the computer's power to mine cryptocurrency

HiddenMiner

Discovered in March 2018, HiddenMiner managed to make its way onto mobile devices via applications downloaded from third party (i.e., non-official) app stores.

One of the reasons it was so dangerous is that, in older versions of Android, it was almost impossible to get rid of. Once inside, it used all the device's resources, making it overheat and crash.



Name

Ransomware

Date of Birth

1989

Origin

USA

Modus Operandi

This kind of cybercrime encrypts the files on a computer, and keeps them blocked until the required ransom is received, generally in the form of bitcoin, an untraceable virtual cryptocurrency.

Don't trust it, and never agree to pay the ransom, because it in no way guarantees that your files will be freed.

Arrest

This threat has already been arrested and neutralized by Panda Security.

But if you are not a Panda Security client and you catch sight of it on the company network, contact us immediately to facilitate its capture.

info@pandasecurity.com

Criminal Record

Wannacry

On 12 May 2017, a piece of ransomware with a network worm functionality affected certain Microsoft Windows systems, taking advantage of an old vulnerability. In this way, it managed to encrypt all the files on the affected computers and on the computers that were connected to the same network drive, infecting the rest of the vulnerable Windows systems on that network.

The process finished with a demand for a ransom in return for the decryption of the files. More specifically, a payment of $300 for each computer freed, to be paid in Bitcoin.

WannaCry has been described as an unprecedented threat in terms of size, infecting over 230,000 computers in more than 150 countries. Its total cost was around 5 billion dollars.

GoldenEye/Petya

27 June 2017 a new ransomware attack struck, paralyzing large companies all over the world. This large-scale attack was carried out new variant from the ransomware family GoldenEye. A replica of the dreaded WannaCry.

Petya was run on computers, encrypting certain files while blocking the compromised system's boot sector. This way it blocked the user from accessing their own computer unless they entered an access key, after having paid a ransom.

Something that was new compared to WannaCry was the fact that this cyberattack was able to turn off the computer, or program a task to turn it off after a certain time.

Name

APTs (Advanced Persistent Threats)

Date of Birth

1989

Origin

Moscú

Modus Operandi

This is a set of stealthy, complex and continuous computer hacking processes orchestrated by organized groups of cybercriminals, and generally targeting governments, large companies or institutions.

They are called advanced due to their coordination and their use of sophisticated techniques to penetrate into victims' IT systems, using vulnerabilities and backdoors in operating systems.

ATPs are characterized by their intention to stay hidden for as long a time as possible, in order to steal as much information as they can. They search for the companies' and organizations' most valuable asset: their most sensitive corporate information, and the data that will allow them to monetize the attack immediately.

Arrest

This threat has already been arrested and neutralized by Panda Security.

But if you are not a Panda Security client and you catch sight of it on the company network, contact us immediately to facilitate its capture.

info@pandasecurity.com

Criminal Record

GhostNet

Large-scale attack discovered in March 2009. Its origin is most likely the People's Republic of China.

GhostNet infiltrated the computers of political, economic and media targets in more than 100 countries.

Operation Aurora

A series of cyberattacks launched in 2009 originating in China. It used a Zero-day exploit to install a Trojan designed to steal information.

In 2010, Google revealed these attacks, alleging that other companies had also been attacked.

Among these companies were leading banks, defense contractors, security providers, oil and gas companies, as well as other tech companies.

Stuxnet

Computer worm that affected computers running Windows, discovered in June 2010. It was the first worm known to spy on and reprogram industrial systems.

The target of this worm was Iran's nuclear infrastructures that used Siemens control systems. Some media outlets attributed it to the US and Israeli secret services.

Red October

In October 2012, a malware program was discovered that was designed to steal confidential information from governments and research organizations.

It is believed that it had been operating all over the world for at least five years before its discovery, stealing sensitive information from diplomatic, commercial, military, aerospace and research organizations in Russia, Iran, the USA and at least 36 other countries.

Name

Phishing

Date of Birth

1995

Origin

Clues point to the USA.

Modus Operandi

This is one of the most well-known scams of the 90s, and to this day continues to be one of the resources most commonly used by cybercriminals. Over 90% of the malware in the world arrives via email.

Phishing consists of sending emails that, seemingly come from reliable sources (for example, banking institutions), and which try to obtain the user's confidential data, which is then used to commit some kind of fraud.

The appearance and tactics of this attack vary, but the objective is always the same: to get data using fake messages, in order to access a user's personal or corporate accounts.

Arrest

This threat has already been arrested and neutralized by Panda Security.

But if you are not a Panda Security client and you catch sight of it on the company network, contact us immediately to facilitate its capture.

info@pandasecurity.com

Criminal Record

Operation Phish Phry

In 2009, American banks suffered a phishing attack, Phish Phry, that affected over 500 people with losses of $1.5 million. More than 100 people in the USA and Egypt were charged for this operation.

The financial institutions affected were Bank of America and Wells Fargo. To date, it is the largest international phishing campaign ever carried out

Attack on the RSA

In March 2011, the RSA reported that it had been attacked by a phishing campaign. The attack exploited an unpatched vulnerability in Adobe Flash. The email that was used read: "I forward this file to you for review. Please open and view it", and had a file called '2011 Recruitment plan' attached.

Dyre Phishing Scam

In October 2014, the phishing campaign Dyre infected more than 20,000 users and managed to steal over a million dollars. Most of the emails sent claimed to be from a tax auditor in order to make the victim download the malicious software.

Phishing on Snapchat

In July 2018, a phishing attack managed to get hold of 50,000 Snapchat users' credentials. The report contained a publicly available list, embedded on a phishing website called klkviral.org. It included 55,851 Snapchat accounts, along with their usernames and passwords.

Name

Zero days

Date of Birth

2010

Origin

Unknown

Modus Operandi

'Zero Day' is the name given to any attack that is launched using the window of opportunity provided by recently discovered vulnerabilities. In other words, a rapid attack, deployed by cybercriminals before security providers are able to repair the vulnerability or even before they've heard of it.

They are one of the most commonly used resources for certain governments when it comes to undermining other countries' critical systems or the companies that developed these systems

Arrest

This threat has already been arrested and neutralized by Panda Security.

But if you are not a Panda Security client and you catch sight of it on the company network, contact us immediately to facilitate its capture.

info@pandasecurity.com

Criminal Record

Stuxnet

Computer worm that affected computers running Windows, discovered in June 2010. It was the first worm known to spy on and reprogram industrial systems.

The target of this worm was Iran's nuclear infrastructures that used Siemens control systems. Some media outlets attributed it to the US and Israeli secret services

Sony Pictures attack

In 2014, Sony Pictures suffered one of the worst attacks in its history. The hacking group known as 'Guardians of Peace" used a zero day attack to bring Sony's corporate network to a standstill and, over several weeks, steal sensitive information from the company.

The data included personal information about employees and their families, confidential emails, information about company executives' salaries, and copies of unreleased films. A large part of this information was published online.

Democratic National Committee

Thanks to six vulnerabilities in Microsoft Windows 10, Adobe Flash and Java, in 2016, Russian hackers backed by intelligence agencies managed to infiltrate the system of the Democratic National Committee (the US Democratic Party's formal governing body).

In order to exploit these vulnerabilities, phishing emails were sent to different members of the DNC and other political targets, aiming to steal their passwords.

The data obtained was mainly leaked by WikiLeaks.