The most dangerous hackers on the planet: Anonymous, Equation Group, Department 121 ... What do you know about them?

Hackers are the people with the highest level of information technology, it is sure, but not everyone can become notorious names.

Malware, malicious code, or computer viruses do not appear naturally, nor do they multiply and spread themselves as evil monsters. Every new type of malicious code is completely crafted from the magic hands of the "dark artists" hiding in the internet world full of pitfalls. All of these "artisans" are masters of computer engineering, not only know how to "manipulate" malware, they also know how to transform, making them stronger. , more dangerous, can overcome every dense security barrier and become a tool to sabotage or gain illicit profits. These people are called by their unfriendly names: Hackers, cybercriminals, or high-tech criminals. But here, we'll just call them hackers!

Hackers are the people with the highest level of information technology, that's for sure, but not everyone can become a notorious name. Simply because they are good, but there are people who are classified as 'good at good'. In the real world of security - cyber security, only a few 'elite' technologies have the right to call themselves the most dangerous hackers in the world.

Today, we will take a look at the list of some of the most dangerous hacker groups, groups and organizations today who are always in the dark, always trying to harm you. They are evil geniuses, with intelligence misplaced.

For those who are working in security - cyber security, you may find this list has a flawed aspect: The most successful cyber criminals who always know how to hide themselves first The 'hometown of the hammock' of security experts, to never be caught, exposed, or even left the smallest clues about their presence. That means most of these lists include hackers who have been careless to reveal their identity, or maybe because they want the world to know their existence.

No one can deny that the successful hack into NASA and damage more than $ 700,000 by Gary McKinnon is not a case of shocking, or denying the talent of this hacker. However, in the wider security world, McKinnon and others like me are still not the ones who can conceive of the 'upper tray' position, at least compared to SoBig's anonymous author. F Worm, malicious code has caused losses of up to 37.1 billion dollars globally. Both of them caused great damage, but the most important difference was that Gary McKinnon was exposed and captured, while the one behind SoBig.F Worm was still unknown and was living freely outside. law.

Gary McKinnon used to make NASA lose $ 700,000, but is not yet considered one of the most dangerous hackers today

So, before we go into the focus, we should correct some of the title of this list. Perhaps it should be interpreted as the list of the most dangerous hackers that humanity has ever known, and still the current threat on internet space is more accurate!

Check out the most dangerous names in the hacker world

1. Anonymous - Guys wearing Guy Fawkes masks
2. Evgeniy Mikhailovich Bogachev - Hackers are wanted by the FBI at the highest level
3. The Equation Group and The Shadow Brokers - NSA's "Daughter" and the stumbling block
4. Department 121 - President Kim's right-hand man
5. Fancy Bear - Dark bears
6. Alexsey Belan - Professional data thief
7. Unit 8200 - Jewish steel fist
8. Unit 61398 PLA - Symbol of power of the Chinese People's Army on cyberspace
9. Marcus Hutchins - The silent hero of the security world

Anonymous - Guys wearing Guy Fawkes masks

Yes, of course the first position cannot escape from Anonymous. This is probably the best hacker group in the world through extremely unprecedented 'unprecedented' missions, as well as possessing the most talented members of the hacker world.

It must be affirmed that Anonymous may not be a terrifying group of hackers or create the most serious threat, but their mere existence has proven to be a worrying sign for every security team. confidentiality, all security walls, and help visualize the picture of the terrible damage of security disasters in a world increasingly dependent on our technology today.

Founded in 2003 in the famous 4chan 'landfill' on the internet, this hacker group is known for its world-class cyber attacks, along with the fact that members are scattered throughout the world. In the world, making it more difficult to cope and find information about each individual. On the origin of the name Anonymous (anonymous) is nothing too mysterious, it originates from the original, any individual posting on the 4chan forum without setting the appropriate username will be automatically turned into Anonymous.

Guy Fawkes mask - a well-known identity of Anonymous members

However, at that time, Anonymous has not really become a true hacker group. They are merely a group of free and bored internet users, together creating harmless (or negligible) jokes on the Internet. For example, in 2006, the group planned to successfully take control of Finnish social networking site Habbo Hotel, and use a series of identical looking avatars to create a reputation. Or sometimes they also make harmless hoax calls via skype.

Anonymous did not really have the coherence and unification into a clearly targeted hacker group until 2008 with the emergence of Project Chanology - an official "war declaration" that Anonymous sent to the destination of the Scientology group. In this campaign, the Anonymous members collaborated with each other very closely and on a large scale - something they had never really done before - to deploy a series of hoax calls, tons DDoS and 'black fax' work aimed at the website of the Church of Scientology (CoS), and caused minor discomforts. The total DDoS attack launched by Anonymous later made the CoS website heavily congested with a flow of 220Mbps. Chanology is the campaign that made the first impression in the eyes of the internet user community for the existence of Anonymous and until now, when referring to Anonymous people still imagine them as hackers carrying Guy Fawkes' scary mask.

After 'shooting down' Scientology, Anonymous continued to launch another large-scale "crusade" with the "anti-copyright" Operation Payback campaign in 2010. In this campaign, Anonymous members were real. currently a series of high-intensity distributed DDoS (Denial of Service) attacks against the American Film Association (MPAA), the American Recording Association (RIAA), and the US Copyright Office to retaliate. These organizations have "taken down" the peer-to-peer network The Pirate Bay not long ago. This is a campaign that Anonymous directly confronts US public authorities, and despite the necessary victory, they also have to pay a very expensive price when the 13 key members of the campaign were FBI times. issue, arrest and prosecute with related charges.

However, this 'small' incident cannot slow down the hacking group that owns thousands of members like Anonymous. In 2011, they supported rebellions of the Arab Spring movement and Wall Street Occupation movements. In 2012, the group declared war on its founder 'Revenge Porn' Hunter Moore and forced the pornographic site to shut down shortly thereafter. In 2014, Anonymous knocked out Ferguson's internal internet system after the city police shot and killed a colored teenager Michael Brown, as well as personal information of the police officer who shot a child to death. Other colored babies: 12-year-old Tamir Rice, discovered.

In the following years, Anonymous's campaigns were still launched quite regularly, but almost exclusively targeted North Korea as well as a number of online pornography sites containing content related to children. you

However, in many cases, Anonymous has taken everything too far away from their control. Anonymous's nickname has been used by countless individuals and organizations to conceal criminal activities and at the same time discredit the social programs that have the 'righteous' purpose that the group is developing. declaration.

In 2011, an unknown hacker group knocked down the PlayStation Network system and stole user data, then left fake information as if they were Anonymous in order to distract the investigating agency, copper. the time of public opinion towards the Anonymous to depress the prestige of this organization. In 2012, someone, unknowingly or unintentionally, leaked stock of important (but old) source code of Norton Antivirus and declared himself a member of Anonymous.

Anonymous impersonations to carry out 'degrading' missions such as software piracy, stealing money and cheating people are not new stories, and will continue as long as possible. Helping the crooks find the wrong words. However, if you closely monitor the situation and style of Anonymous activities from the first days, you will find that they do not have the habit of participating in illegal frauds and with such small scale.

But because anyone can be Anonymous, due to their nature, we can hardly be sure that 'true' Anonymous members never perform the above behaviors, and the clear distinction between 'fake' and 'real' members are also not easy.

After all, Anonymous's activities are essentially illegal acts. Every hour, every minute, the members of the group are constantly being hunted around the world and they will be immediately arrested if they reveal their identity. Some people are only fined, some have to be imprisoned, but Anonymous will certainly not be 'extinguished', they exist as an entity of the internet world.

We won't be able to get rid of those Guy Fawkes masks unless we accept to stay away from the online world. That is why Anonymous is considered the most dangerous hacker group in the world, they exist in parallel with the development of the internet, simply so!

Evgeniy Mikhailovich Bogachev - Hackers are wanted by the FBI at the highest level

Do you wonder if hackers are rich? - May. So who is the richest hacker in the world? - Evgeniy Mikhailovich Bogachev. Yes, it is Evgeniy Mikhailovich Bogachev, one of the most dangerous hackers in the world, who is being wanted by the FBI at the highest level with a record amount of bonuses: $ 3 million for anyone who provides information to help catch keep this person.

FBI arrest warrant Evgeniy Mikhailovich Bogachev

The malicious codes that Evgeniy Mikhailovich Bogachev once created, the botnet that he is a co-author, or the 'unbelievable' data theft missions cause losses of up to tens of millions of dollars . all. Not only did Bogachev become the notorious name in the security world, but it also helped him to appear on the list of the most famous hackers of all time, becoming the pursuing target of many government organizations.

Russian Hacker was born on October 28, 1983, often causing people to shiver when they see nicknames like "lucky12345," "slavik," "Pollingsoon". According to the FBI, Bogachev is the most dangerous person in the hacker world today.

This statement is not without foundation when even the leading brains at the FBI and other international crime prevention organizations have taken up to two years just to find out his 'offering of rice' name. This guy, and now they give the $ 3 million figure - the biggest bonus ever given to a cyber criminal - to anyone who can help bring Bogachev to justice.

Unfortunately for the FBI, the Russian government seems to have little interest in the prize money, as evidenced by the fact that Bogachev was frequently seen appearing publicly in Anapa, a Black Sea resort town in the region. Southern Russia with dozens of luxury cars, private yachts, villas, and of course indispensable 'shadowy'.

Despite the wanted warrant, Evgeniy Mikhailovich Bogachev is living a luxurious life as a "king" in Russia.

Does such a luxurious life ever make Bogachev 'bored'? Yes. On the days of boredom, this millionaire hacker returns to his endless passion: open a computer, write malicious code, or monitor and take control of millions of computer systems all over the world. Gender also creates viruses that make master security experts 'sweaty'.

Talk a little bit about the glorious career of Evgeniy Mikhailovich Bogachev. This hacker "started out" with the role of a 'code walker', specializing in writing and selling malware on the dark web. Bogachev's professional hacker title is only truly known when he releases GameOver Zeus malware that steals bank information, and Cryptolocker malicious code with the ability to create continuous attacks. Computer systems make IT professionals unable to resist, forced to pay in exchange for 'peace'.

According to FBI statistics, Bogachev bagged hundreds of millions of dollars through his malicious activities around the world. In the United States alone, Bogachev earned more than $ 100 million from a variety of sources, mainly withdrawing bank accounts. Or as in the case of CryptoLocker, this malicious code helped Bogachev pocket $ 27 million in less than two months of deployment.

In particular, the FBI accused Bogachev of engaging in politically toxic activities since 2011. In December 2016, the hacker and five others were accused of illegal intervention in the presidential election. America.

Returning to reality, of course the Russian government never acknowledged having ever worked with Bogachev, but the refusal to arrest him, along with Bogachev's comfort and immense money certainly set out. big question.

There is no agreement between Russia and the United States on extradition law, so the FBI to Russia to arrest Bogachev is 'more difficult than heaven'. At the same time the Russian side had no reason to arrest Bogachev, at least until he violated Russian law.

The FBI's $ 3 million figure may take a long time to find the owner, or it may never be.

The Equation Group and The Shadow Brokers - NSA's "Daughter" and the stumbling block

Talking about famous, dangerous hackers without mentioning those who are sponsored by the state is a major shortcoming. The Equation Group is the typical name among them.

The Equation Group is the unofficial name of Tailored Access Operations (TAO), a confidential unit of the US National Security Agency (NSA). Due to the nature of the work, this force also uses many other codenames that are hard to list.

List of victims of The Equation Group worldwide

First established around 2001, The Equation Group is considered a state secret. The unit was extremely tight, silently carrying out countless infamous missions until it was discovered in 2015 when two types of spyware - EquationDrug and GrayFish - were brought to light and supposedly associated with an NSA unit.

The Equation Group's move is extremely tight, always kept absolutely confidential, and is sponsored by the state - these three factors have created the danger of this hacker unit. Many theories suggest that The Equation Group is the organization behind Stuxnet, the 'poison worm' that destroyed Iran's nuclear program for a long time.

Just like most other national-level special units, the main goal in all The Equation Group missions is to interfere with the opponent's system, damage or gather information to gain advantage for The United States on the negotiating table for 'hot' issues, can affect national security and interests, both domestic and foreign. Since its founding, the mission of The Equation Group revolves around Iran, Russia, Pakistan, Afghanistan, India, Syria or Mali . countries with conflicts in terms of interests and political views with the United States States

However, the appearance of The Shadow Brokers has changed all

The Shadow Brokers, who got in the way with the NSA

Until now, the true origin of The Shadow Brokers is still covered by a mysterious veil. This hacker group happened to be first discovered in 2016 via a tweet posted by the account "@shadowbrokerss", which mentioned a website and data warehouse on GitHub containing references and instructions. about how to decrypt a file's content is said to contain zero-day tools and exploits, which are used by The Equation Group, targeting enterprise firewall systems, antivirus products and Microsoft products.

In contrast to the mysterious background, the action of The Shadow Brokers has been exposed in quite a number of cases. A few months after the first disclosure of The Equation Group, the organization went into another incident when it revealed a list of information about servers, allegedly once subjected to The Equation Group '. touch ', as well as references to hack tools already in use. By April 2017, The Shadow Brokers continued to announce more hacking tools that were supposed to be NSA and password to open.

There are many cases of other information leaks of The Shadow Brokers that until now can be concluded that they are the organization behind EternalBlue, EternalRomance and a series of exploits that play an important role in created some of the world's most dangerous malware attacks, including the notorious Wannacry campaign and ransomware NotPetya. In May 2017, After infecting more than 200,000 computers in just two weeks, WannaCry extortion code used EternalBlue to launch an attack on the Server Message Block (SMB), a Windows computer network protocol, to spread itself. All have 'fingerprints' of The Shadow Brokers.

But their actions did not stop there. In the following months, The Shadow Brokers continued to reveal the list of servers and tools used by The Equation Group and provided an additional monthly data warehouse for anyone willing to pay. The move shows that The Shadow Brokers possesses unlimited access to the NSA system - a heavy "slap" on one of the world's most powerful cybersecurity agencies.

And while the 'top-of-the-line' minds at the NSA have not been able to identify the identities of those behind 'ghosts' called The Shadow Brokers that have been haunting them for years, perhaps all that We can do it here, slash the wind, and continue to make speculations for this mysterious hacker group's next attack.

Department 121 - President Kim's right-hand man

You read information online, through the media and see that Korea is an outdated, poor and underdeveloped country? Maybe, but in the field of security - information technology is absolutely not!

Department 121 - the pride of the Korean army

In fact, North Korea is in the hands of many good hackers, who have caused world shocks, and helped this country realize the urgent digital ambition in the high-tech era like The current. Unlike in other countries, most Korean hackers are on the state payroll, particularly under military control. They work day and night to ensure 'sovereignty and national status in cyberspace' and are ready to deter any goal that is thought to be detrimental to national security and survival. regime. In some cases, these hacker groups even spread chaos to their political opponents.

Among the hacker groups known in Korea, perhaps the most notorious is the Department 121 (Bureau 121) - the organization behind countless attacks and cybercrime campaigns. So how dangerous is Department 121 and how terrible are their talents? Please mention here some of the missions involving this state-level hacker organization for you to imagine:

The 121's most famous and large-scale mission is the Wannacry ransomware campaign, which has caused the world to suffer during the 2017-2018 period. billions of dollars in damage. As mentioned above, although Shadow Brokers can also be considered a 'co-founder' of this ransomware type thanks to its 'access' rights to NSA's cyberwar tools, but the truth It is the Department 121 that plays the key role in manufacturing and deploying this malicious code. Wannacry infected about 300,000 devices and caused more than $ 4 billion in damage.

Besides, this unit is also the team responsible for a huge data leak at Sony Pictures in 2014. This is a retaliatory attack after the company produced and released a The comedy is called Seth Rogen, which mainly talks about the assassinations of the Korean leader, Kim Jong Un. The North has given a drastic reaction from the beginning of the film's release, and this heavy-duty attack proves that they are not people who like to talk about it. Countless emails and personal data were leaked to the public, and eventually, Sony had to spend about $ 15 million to fix the damage.

However, working conditions of Korean hackers are also considered extremely harsh. They have to sit in front of the computer for hours every day, for several consecutive days depending on the size of each campaign, and under control to 'suffocate' to make sure there is no leaked information. Any 'change of heart' behavior will cost you a very expensive price, but this is often rare because these hackers are extremely carefully recruited. They are not only computer masters, but also have a very good and important resume that is absolutely loyal. Freedom is a luxury for members of the 121 Department, or in a softer way, it is 'freedom in the framework'.

The members of the Department of 121 are on the military staff and work as regular soldiers

Gaining foreign currency through malicious activities online is a daily job of the Korean hacker groups in general. According to a statistic (for reference), on average, each member of Bureau 121 earns 60,000 to 100,000 dollars a year through any means necessary, then they hand over this money to the state. and receive salaries like ordinary officers or soldiers depending on the specific payroll. Those who do not meet the 'target' set or appear to be inappropriateness will be immediately discarded.

Above all, they are still master hackers, and become even more dangerous under the auspices of the state. Department 121 - the name cannot be underestimated!

Fancy Bear - Dark Bear

Hearing the name of this hacker group, perhaps we have partially guessed their origins. Yes, yet another infamous name comes from faraway Russia, and of course also on the FBI's 'special interest' list.

Fancy Bear means cute bears, but in reality this hacker group is not at all friendly at all. This is considered the most elite hacker group with members possessing extremely profound knowledge in the field of security, cyber attack, and especially a clear operational policy. Fancy Bear is sometimes known as Sofacy, Pawn Storm or APT 28, this hacker group is believed to be closely related to the Russian intelligence agency GRU, and does not exclude the possibility that it is also an organization. government sponsored.

Fancy Bear has been involved in many cases affecting cybersecurity in countries around the world

Indeed, it is the Fancy Bear operations that reveal many doubts about their close connection with the Russian government, and seem to receive a great deal of support from the Kremlin in offensive campaigns. Large-scale networks are specifically targeted and filled with political motivations. It can be said that this is the most dangerous hacker organization from Russia, responsible for some hacking 'save history', not playing with the genre of 'chicken theft, dog catching' like many amateur hacker groups. other business.

Fancy Bear's first buzzing campaign took place in 2008, when the group successfully hacked Georgian government websites and networks. The attack left Georgia's online information system in serious disarray before the Russian army officially crossed the border and landed in the country.

Since that 'milestone', Fancy Bear has gradually become a respected force in the hacker world. They have been involved, and at the same time, the direct cause of numerous conflicts over cyberspace between the Russian government and rival states. From missions aimed at journalists and anti-Kremlin protesters, to German parliamentary hacking campaigns that lasted for more than six months in 2014, attacking Chinese military computer systems. States, or disable 20% of the artillery system of Ukraine ... All are done at the hands of Fancy Bear.

Fancy Bear is said to have an insatiable relationship with the Russian government

However, what makes the FBI particularly interested in this hacker organization is that it regularly interferes in the election campaigns as well as the election of a number of countries that are 'prioritized' by the Russian government. Most recently, Fancy Bear has been accused of launching attacks against the US Democratic National Committee (DNC), as well as several organizations responsible for advising the US government. Previously, the group is also said to have been involved in the networks of government organizations in many other countries, including Germany, Denmark, France and Ukraine. In general, Fancy Bear attacks usually happen before "sensitive" times, such as voting and referendum.

Despite being one of the most dangerous hacker groups in the world, Fancy Bear almost never purposefully flaunted its prestige or made a name for itself in its missions. They do not have the habit of leaving an identity behind each attack, but instead try to conceal this very carefully, causing leading security experts to 'sweat' to find out. really.

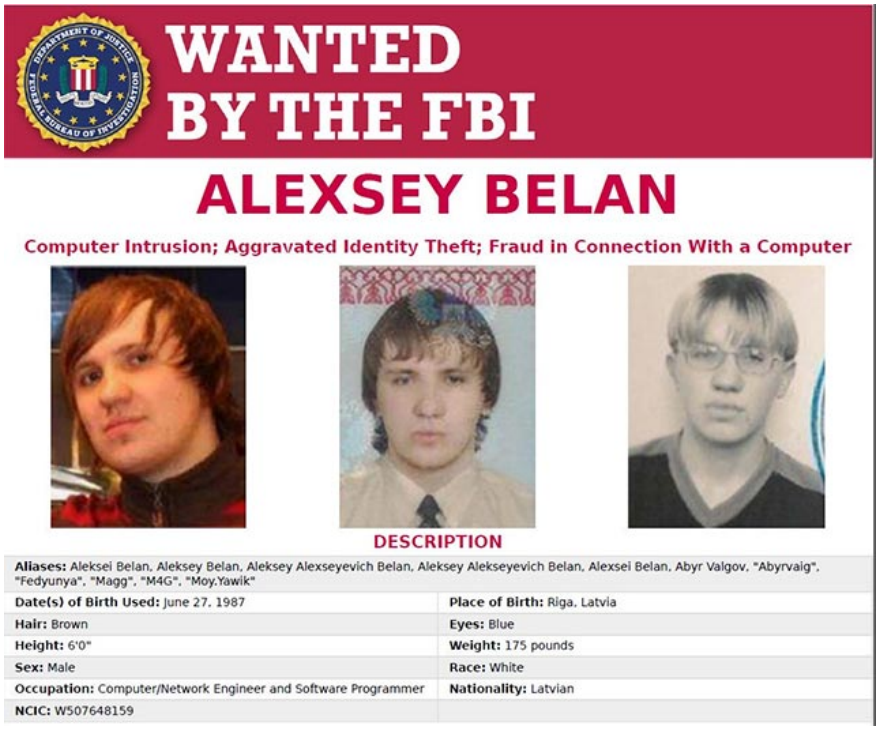
Of course, Moscow has always denied any allegations that Fancy Bear is affiliated with them in any way. However, the favor from the Russian authorities, as well as the unbelievable 'coincidence' events have left a big question mark that perhaps many people have partially guessed the answer.

The US President election, one of the most concerned political events in the world, is about to take place at the end of next year. Let's wait and see what 'fun' Fancy Bear will bring to this event!

Alexsey Belan - Professional data thief

Born in 1987, only turned 32 days old, but this Lavian hacker was a veteran name on the FBI's global wanted list.

Before performing the famous missions around the world, Alexsey Belan was already very famous in the hacking world with the nickname M4G. Alexsey Belan is one of the most active members of the unorthodox hacker community, and even runs a popular blog that sells hacking tools.



Alexsey Belan is being wanted globally by the FBI at its highest level

Alexsey Belan's identity was perfectly concealed until the hacker began to engage in more dangerous attacks, and of course more in contact with cyber security organizations around the world. After hacking and taking control of major game servers, the server crippled an Israeli-based cloud provider, as well as shut down the mass media ICQ. Alexsey Belan is starting to gain more recognition in the security world. After a while, this hacker turned to consulting for other hacker groups and actively selling personal data online. This activity helps Alexsey pocket a small amount of money, but also makes him pay more attention to the security agencies. And in 2012, Alexsey Belan was officially wanted with a long list of crimes.

Trong s? nghi?p c?a mình, Alexsey Belan ?ã th?c hi?n vô s? phi v? ?ình ?ám, tuy nhiên v? vi?c gây ti?ng vang l? n nh?t ??ng th?i c?ng ??a anh ta vào danh sách 36 hacker b? truy nã ? c?p cao nh?t có l? là v? hack Yahoo vào n? m 2013. ?ây chính là v? vi ph?m d? li?u l?n nh?t trong l?ch s? gây ra b?i m?t hacker ??c l?p, ?nh h??ng ??n g?n 3 t? tài kho?n ng??i dùng c?a Yahoo. Alexsey Belan không th?a nh?n mình có dính líu ??n v? vi?c này. Tuy nhiên ch? sau ?ó 1 n?m anh ta ?ã chính th?c b? cáo bu?c ??ng sau m?t v? t?n công khác, gây rò r? d? li?u riêng t? c?a h?n 500 tri?u tài kho?n Yahoo.

Alexsey Belan's favorite targets are US-based businesses and organizations. Alexsey Belan is believed to have been involved in a series of organized attack campaigns, which took place from 2013 to 2016, directly targeting e-Commerse sites in California and Nevada, including Yahoo already. mentioned above. During this time, he certainly hacked and stole data from a total of 700 million accounts: 500 million from Yahoo and 200 million from other sources. This is really a huge amount of private data.

Having caused such a series of criminal activities, but when international law enforcement came knocking on the door, Alexsey Belan quickly ran away for a large sum of money, and perhaps he was living. 'regal' somewhere on earth. And while no one knows for certain where Alexsey Belan could hide. Current evidence suggests that he is in Russia.

With three charges of being accused of illegal intrusion into the computer system, the FBI is ready to award $ 100,000 to anyone with information to help arrest this Latvian hacker.

Unit 8200 - Jewish steel fist

Another government-backed hacker organization appeared on the list. Unit 8200 (Unit 8200) has never been an inspirational name in the hacker world but, on the contrary, they are the ones who instill fear in any political opponents of the Jewish state of Israel. It is not wrong to say that Unit 8200 is a polity run directly by the Israeli government because it has extremely outstanding individuals, well-trained and has an organizational structure, operational plans. clearly.

Unit 8200 is the name that instills fear in any of Israel's political opponents

The effectiveness of Unit 8200 has been demonstrated in a wide range of public service assistance and terrorism prevention activities. More notably, Unit 8200 is believed to be the only hacker group with more female members than men - an interesting trait.

However, in the world of security, Unit 8200 has never been a name associated with 'cuteness'. This is the organization behind many of the most terrible malware ever known, and also a master in the implementation of information espionage campaigns, stealing data of a series of government organizations. and even civilians on an unprecedented scale. Unit 8200 is present everywhere in the world. If you want to confront them, just by proving that they pose a threat to Israel's national security, members of this organization will be able to reach you in no time.

Unit 8200 is one of the few hacker groups that were established long ago that are still active. This organization was established in 1952 as the 2nd Information Intelligence unit in Israel. However, with the rapid development of the information technology field and especially the global internet network, this unit has been expanded to be the largest and most influential force in the Israel Defense Force. .

Due to the nature of the work, most of Unit 8200's campaigns are extremely secretive, but many times their members reveal them after major hacks. The hacker organization has been accused of carrying out numerous cyber-terrorist attacks on a global scale, developing the Stuxnet virus and creating a malware called Duqu 2.0, or malicious software espionage activities. harm that Kaspersky has developed earlier. They are also the main force involved in large-scale campaigns against hacker groups from Palestine - a country hostile to Israel. The most

prominent among them is campaign #OpIsrael in 2013 that shocked the global security world.

It is no exaggeration to say that Unit 8200 is the elite of the hacker world, and this statement encapsulates the quote by Peter Roberts, senior research expert at the Royal Institute of Security: 'Unit 8200 probably It is the leading technical intelligence agency in the world and can stand on par with the NSA in every respect but size. They always put a high level of focus on each assigned task - more than the NSA - and they carry out their activities with a level of perseverance and passion that you will certainly never find anywhere else. anywhere else '.

Unit 61398 PLA - The power symbol of the Chinese People's Army on cyberspace

Earlier, we talked a lot about hacker groups that are sponsored by the government, but it would be a big mistake to ignore the name coming from the current information technology powerhouse: China..

Unit 61398 PLA is an extremely large-scale full-fledged hacker organization

Over the years, Chinese officials have held up against all allegations of being involved in illegal online activities or even owning a group of hackers operating for 'national interests'. family '. However, things changed quite dramatically in 2015 when Beijing openly admitted it was in the hands of an intensive cyber research group called Unit 61398 PLA (PLA Unit 61398), but refused to supply. Provides more details on this mysterious cybersecurity unit.

Perhaps the biggest security scandal involving this hacker organization is the Shady RAT campaign. The Shady RAT is arguably the largest state-sponsored online attack campaign ever. Over a period of five years, from 2006 to 2011, the Chinese military's Unit 61398 PLA infiltrated and stole data from more than 50 major multinational companies around the world, as well as government organizations. and non-profit organizations (mainly from the West).

However, like other sponsored hacker groups, Unit 61398 PLA's scope of activity is limited to campaigns that steal data from international actors that are crucial to government policy. China. In 2014, for example, it was accused of engaging in a serious hack that took away countless sensitive documents related to Israel's missile defense system. Recently, a series of large US businesses have become targets of Unit 61398 PLA, coinciding with the escalation of tensions in the trade war of these two countries.

Several members of Unit 61398 PLA are currently wanted by the FBI

Besides possessing extremely talented members and being 'backed by the government', the other factor that makes Unit 61398 PLA peril is the sheer size. According to estimates, this organization has no less than 1000 centralized servers, and of course that is just the tip of the iceberg. With such a large membership and large-scale infrastructure, Unit 61398 PLA can 'submerge' any force capable of threatening China's safety in cyberspace, It is worthy of being a strategic core force of the most populous country in the world in the digital age today.

Marcus Hutchins - The silent hero of the world of security

Marcus Hutchins is one of the few people who have an important (and even the most important) influence in today's world of cybersecurity. Simply because every move of this' villainous hero 'can make significant changes to the way other hackers operate in cyberspace, as well as possess the ability to' change hat colors. of them in the following years of their career.

Briefly tell the biography of Marcus Hutchins. He is a relatively reclusive cybersecurity expert, working for a small security company called Kryptos Logic at home. Two years ago, the infamous WannaCry ransomware was launched globally, making the world of security wobbly, at that time, Marcus Hutchins was on vacation with his family and received countless words' petition 'to quickly join the fight against WannaCry from many major security organizations. Marcus was pulled off the holiday to be a pioneer in this war, and indeed he did not disappoint the world by finding a method called 'kill switch', which slowly stops and eliminates. Completely this terrifying malware.

Marcus Hutchins is a hero in the campaign to fight the spread of WannaCry

Marcus Hutchins successfully prevented the biggest-scale attack campaign of 2017, became a hero of the cyber-security world and was treated like a king at DEF CON that year. (DEF CON is one of the biggest conferences of the year for hackers, the gathering place of the top faces in the field of security - cybersecurity).

However, a little while later, Marcus was arrested while still receiving praise and admiration from his colleagues after his illustrious feat. This infamous hacker is charged with 6 charges regarding his role in developing and spreading the Kronos virus, malware that could steal banking information from the browser if it successfully infects. on victim's device.

It is not clear whether Marcus Hutchins will be falsely accused, but most likely he will be the first white-hat hacker to go to jail after he has 'converted into a regular manner'. The trial of Marcus Hutchins is still being carefully watched by cybersecurity experts and even hackers worldwide, not only because Marcus is an influential figure, but also because he is arrested. under the Computer Fraud and Abuse Act, which has been a source of resentment and even anger among white-hat hackers for a long time.

Many experts believe that the Computer Fraud and Abuse Act contains too many vulnerabilities that can be misused to conduct irrational arrests against white-hat hackers, who are simply conducting operations. dynamically checking and exploiting, or writing code related to malware, even though they are essentially not maliciously damaging the network security situation. So if Marcus is found 'guilty' while deliberately creating Kronos malicious code but still jailed for his contributions, this verdict could create terrible frustration and contradiction within. the future white hat hacker world.

Marcus Hutchins has reluctantly fought a battle not only for his own freedom, but also for the future of white-hat hackers in the eyes of lawmakers. Forcing the law to be more fair to those who are fighting day and night to protect cyber peace. All we can do is hope justice will be done.

Above is a list of hackers, the most dangerous hacker group in the world. They may work for different polities, serving many different purposes, but there is only one thing in common: These are all genius minds in the digital age.