October 2018

group-ib.com

HI-TECH CRIME TRENDS 2018

TABLE OF CONTENTS

1. KEY FINDINGS

Hardware and BIOS/UEFI vulnerabilities

- Last year, cybersecurity experts were hit by the WannaCry, NotPetya, and BadRabbit epidemics. At the beginning of 2018, a new global IT security threat emerged and involved side-channel attacks and vulnerabilities that were discovered in processors sold by various vendors. These vulnerabilities cannot be effectively eliminated with software updates and as such they create new opportunities for attackers. It is likely that in the space of a few years they will seriously affect the cyber security market.
- To exploit certain hardware vulnerabilities, hackers can simply run a JavaScript code, as in the case of the Spectre and Glitch vulnerabilities.
- Exploits for hardware and UEFI vulnerabilities are ready-for-use Proof of Concepts (PoCs), although their exploitation in real attacks has yet to be demonstrated. However, this does not mean that they are not used by attackers today: at present, there are no solutions on the cybersecurity market that would be able to detect such threats.
- Conducting research in this area and developing real exploits are both labour-intensive and expensive processes, which means that such vulnerabilities are not yet exploited by “ordinary” cybercriminals. However, government-backed groups are both interested in and capable of investing in such research and tools.

Sabotage and espionage

- The focus of innovations and research relating to the creation of complex malware and the organisation of multi-layered targeted attacks has shifted from financially motivated cybercriminals to state-sponsored threat actors. Their actions are aimed at achieving long-term presence in critical infrastructure networks for the purpose of sabotage and espionage. They target companies in sectors such as power, nuclear energy, commerce, water, aviation, and more.
- A significant number of the attacks focused on the energy sector. Threats to electric grid security include Industroyer, the first specialised software for attacks on power grids, discovered in 2016, and Triton, a framework that targets the Safety Instrumented System (SIS) manufactured by Schneider Electric.
- In 2017 and 2018, two threats with a fuzzy target were identified: Bad Rabbit ransomware and a router malware called VPNFilter. Both threats have been linked to the BlackEnergy group. The most large-scale and high-profile aspect of the BadRabbit attack was that it was designed to cover up the targeted disabling of devices compromised in advance. VPNFilter was discovered at the preparation stage of the attack. Its goals are still unclear, but one of the VPNFilter modules is designed to detect SCADA systems.
- In February 2018, an attack using malware called Olympic Destroyer took down the official website of the Pyeongchang Olympics, shut off the stadium’s Wi-Fi, and interrupted the live broadcast of the opening ceremony. The incident demonstrates the risks that cyber attacks can represent for not only infrastructure facilities, but also a country’s image.
- Banks are also considered to be part of critical infrastructure, which is why the availability of tools and experience in disrupting bank systems are priorities for attackers. Such tools are actively used by two groups in particular: BlackEnergy and Lazarus.
- In addition to self-developed tools, many hacker groups started using open-source penetration testing tools and new techniques to cover up the interaction of infected devices with a C&C server, which significantly complicated their forensic analysis and attribution.
- Hackers are actively developing tools for not only Windows platforms but also Mac OS and mobile operating systems.
- Increasingly often, state-sponsored hackers are focusing on vulnerabilities in home routers. This allows them to not only spy on users without infecting their devices, but also maintain a more extensive and dynamic infrastructure.
- Southeast Asia is the most actively attacked region. In just one year, 21 state-sponsored groups were detected in this area, which is more than in the United States and Europe combined.

- Information about attacks carried out by APT groups becomes public on a case-by-case basis and only after a long delay. Every year, new details around past attacks conducted by already known groups come to light. When new threat actors are discovered, it turns out that they have been active for several years but remained unnoticed for various reasons (for example, Orangeworm and the Slingshot group, linked to the United States). Moreover, in many countries, data relating to the activity of state-sponsored hackers appears only in the event of security breaches (WikiLeaks publications, hacking of the NSA's contractor Equation Group, etc.). This puts potential victims in the position of forever having to catch up and complicates detecting and responding to threats, all the while making it easier for criminals to ensure their long-term presence in the networks of their targets.

Targerted attacks on banks

- Group-IB has identified four criminal APT groups that pose a real threat to the financial sector. They are able to not only penetrate a bank's network and access isolated financial systems, but also withdraw money via SWIFT, AWS CBR, card processing systems, and ATMs. These groups are Cobalt, MoneyTaker, and Silence (all three led by Russian-speaking hackers), as well as the North Korean state-sponsored group Lazarus.
- On average, one to two Russian banks per month are successfully attacked by cybercriminals. Average losses are estimated at $2 million.
- Group-IB experts have observed that the number of targeted attacks against banks which has resulted in illicit SWIFT payments has has tripled over the reviewed period. In the previous period, three such attacks were tracked — in Hong Kong, Ukraine, and Turkey. In this period, however, 9 successful attacks have already taken place in Nepal, Taiwan, Russia, Mexico, India, Bulgaria, and Chile. Only two hacker groups target the SWIFT interbank transfer system: Lazarus and Cobalt. At the end of 2017, the latter carried out the first successful attack on a bank using SWIFT in the history of Russia's financial sector. When committing thefts via SWIFT, Cobalt and Lazarus carefully prepared the cash-out scheme and stole funds from two banks simultaneously, likely to reduce the costs associated with cash withdrawal. The good news is that in the case of SWIFT, most unauthorised transfers can be stopped in time.
- Withdrawing money through AWS CBR (Automated Work Station Client of the Russian Central Bank) is a tactic employed by MoneyTaker. In November 2017, the group managed to withdraw $104,000, while in summer 2018, the gang successfully stole $865,000 from Russia's PIR Bank. In 2017 and 2018, the Cobalt and Silence groups ignored AWS CBR, even in cases where they managed to get access to it. Their attention is now drawn to more reliable theft schemes, i.e. through ATMs and card processing systems. That being said, Cobalt is also interested in local systems of interbank transfers abroad.
- Attacks on card processing systems remain one of the main theft methods and are actively used by hackers from Cobalt, MoneyTaker, and Silence. In February 2018, members of Silence conducted a successful attack on a bank and stole money via the card processing system; they managed to withdraw $522,000 from cards via a partner bank's ATMs. The focus of attacks on ATMs and card processing systems has reduced the average amount of damage caused by one attack. However, it helps attackers conduct such attacks more securely for money mules, who cash out the stolen money: the attackers are in one country, their victim (the bank) is in another, and the cashing out takes place in a third country.
- In the designated period, only Cobalt conducted attacks on payment gateways. In 2017, they used this method to steal money from two companies, but no attempts were made in 2018. During one of their attacks, they received help from members of the Anunak group, which had not conducted an attack of this kind since 2014. Despite the gang leader's arrest in Spain in spring 2018, Cobalt continues to be one of the most active and aggressive groups, steadily attacking financial organisations in Russia and abroad two to three times per month.
- Attacks targeting ATM networks were conducted by Cobalt and Silence. In May 2018, MoneyTaker also started attacking ATMs.

Attacks on bank clients — Russia

- The number of threats caused by banking PC Trojans in Russia has been decreasing since 2012. Attacks on private clients are a thing of the past, but the damage to companies was estimated at $8,3 million, down by 12% during the reporting period.

- At present, only three criminal groups — Buhtrap2, RTM, and Toplel — steal money from corporate accounts in Russia. The major theft techniques involve gaining remote control or automated transfers through 1C accounting systems.
- Group-IB experts noted a change in attackers' tactics in the second half of 2017. Spreading Trojans was no longer done through traditional malicious campaigns or hacking popular sites, but by creating new resources tailored to accountants and company executives who use online banking, payment systems, or cryptocurrency wallets as part of their work.
- Over the last year, Group-IB experts have noted fewer epidemics in Russia involving smartphones infected with Android Trojans, despite several years of rapid growth. The number of thefts committed daily using Android Trojans in Russia has decreased almost threefold, and the average amount stolen has decreased from $164 to $104.
- Security experts did not detect new large botnets except a malware called «Banks in your hand». The Trojan was disguised as a financial application, acting as an «aggregator» of mobile banking systems used by the country's leading banks.
- Over the past year, web phishing has grown both in Russia and worldwide. The number of hacker groups that create phishing websites imitating Russian brands has gone up from 15 to 26. In Russia, the number of successful phishing attacks per day has reached 1,274 (compared to 950 previously). The damage from web phishing was estimated at $3,7 million, which is 6% more than in the previous year.
- Phishing that targets card-to-card transfers has become extremely popular. In some cases, scammers masquerade as specific banks, but phishing that is not related to bank brands also exists.

Attacks on bank clients — worldwide

- The situation on the international market is drastically different: six new PC Trojans were discovered during the analysed period (IcedID, BackSwap, DanaBot, MnuBot, Osiris, and Xbot) and source codes for five more have been shared or sold. That being said, the Trojans Shifu, Qadars, Sphinx, Tinba, and Emotet are no longer deployed. The latter is still used, but only as a loader rather than a full-fledged banking Trojan. This could be due to the work of law enforcement agencies, which have dealt a heavy blow by arresting the authors of the banking Trojans Neverquest and GozNym, as well as one of the most popular loaders — Andromeda.
- In 2017, the source codes of the banking Trojans TinyNuke and AlphaLeon (aka Thantaos, Mercury Bot) were published, but were not used thereafter.
- Groups that employ the Trojans Dridex, Trickbot, and Gozi still present the most significant banking threat. BackSwap is the most noteworthy of the new Trojans. At first it only targeted banks in Poland, but then began to attack Spanish banks as well. BackSwap is interesting because it combines several new web injection techniques that are used to automatically replace payment details.
- The new Android Trojans sold on hacker forums are primarily designed fo the use outside of Russia: Easy, Exobot 2.0, Asacub, CryEye, Cannabis, fmif, AndyBot, Loki v2, Nero banker, and Sagawa. The only exception is Asacub.
- Trojans that were active in the previous period are no longer used, probably due to poor support from their authors. These Trojans include Xbot, Abrvall, Vasya, UfoBot, and Reich.
- Usually, banking Trojans for Android are spread via SMS/MMS messages. However, in early 2018, the Exobot 2.0 Trojan was distributed through applications that had previously been downloaded from the official Google Play store.
- On average, 686,000 sets of card details and 1.1 million dumps are uploaded to such stores every month. Our records indicate that dumps account for 62% of total sets of card data sold, which means that POS threats are the main method of compromising plastic cards. Card details are sold much cheaper in card shops: their total value amounted to $95,6 million, accounting for only 17% of the overall market value, compared to 19,9 million dumps, which cost as much as $567,8 million.
- On the global scale, in contrast to the previous period, most phishers targeted cloud storages rather than the financial sector. The United States are still the top country as regards hosting phishing sites (80%); France and Germany are second and third, respectively, in this ranking. Among all phishing resources, 73% can be divided into the following categories: cloud storages (28%), financial platforms (26%), and online services (19%).

Threats to cryptocurrencies and blockchain projects

- In 2017 and 2018, hackers' interest in cryptocurrency exchanges ramped up. A total of 13 exchanges were robbed, amounting to a total loss of $877 million. That being said, 60% of the total amount was stolen from Coincheck, a Japanese cryptocurrency exchange. At least five attacks have been linked to North Korean hackers from the state-sponsored Lazarus group. Targeted phishing remains the major attack vector for corporate networks.
- ICO projects are highly vulnerable too: hackers cause serious damage to ICOs by attacking founders, community members and platforms themselves. Spear phishing remains the major vector of attack: approximately 56% of all money siphoned off from ICO were stolen through phishing attacks. A big phishing group is capable of stealing roughly $1 million a month.
- A relatively new method of fraud on the ICO market was stealing a White Paper on an ICO project and presenting an identical idea under a new brand name.
- In 2018, security researchers discovered a targeted attack used to manipulate the exchange rate of a cryptocurrency. Preparations for this attack took two months.
- Cryptojacking (hidden mining) became most widespread in 2017 and 2018. After the launch of Coinhive, a hidden mining software, seven more similar software programs were brought out (Crypto-Loot, JSEcoin, Minr, CoinImp, and ProjectPoi).
- Given the necessary preparations, hackers can gain control over 51% of the network mining power and capture control of cryptocurrency. In 2017, no successful "51% attacks" were detected, but they are now becoming more and more often. In H1 2018, five successful attacks were registered with direct financial losses ranging from $0,55 million to $18 million.

2. FORECASTS

Hardware and BIOS/UEFI vulnerabilities

- Exploits and malware leveraging hardware and UEFI/BIOS vulnerabilities will remain the prerogative of state-sponsored hackers.
- The number of UEFI infections will go up, not least because of side-channel attacks growth. These attacks are to be expected primarily in public sector due to legacy PCs and, consequently, UEFI.
- Attackers may specifically target motherboard vendors and computer hardware suppliers working with government bodies.
- Real side-channel attacks may lead to massive data leaks from cloud services undermining general trust in cloud computing — should high-profile incidents occur.

Sabotage and espionage

- Phishing will remain the main technique for critical infrastructure infiltration, but as some hacker groups evolve, new and hard to discover techniques may surface. This year the focus may shift to vulnerable network equipment connecting the network to the Internet.
- Sabotage-oriented hacker groups will continue to focus on the energy sector. However, every critical infrastructure may be a target, and so the focus must be on system compromise assessment and attack readiness.
- Organizations wishing to protect their information should consider protecting not only corporate infrastructure, but also key personnel's home networks and personal devices.
- Self-propagating ransomware will be the tool of choice in attacks on air-gapped networks.
- APT groups are increasingly becoming a target of intense research. As a countermeasure, some hacker groups may imitate other groups' unique features to throw researchers off track and cause incorrect attribution.
- APT groups are increasingly becoming a target of intense research. As a countermeasure, some hacker groups may imitate other groups' idio-syncratic characteristics to throw researchers off track and mask their true intentions and goals.

Targeted attacks on banks

- Another cybercriminal group, Silence, is experienced enough to conduct targeted attacks on Russian banks. These skills will be successful against ATMs and card payment infrastructure in countries outside Russia & the CIS.
- These days, sandboxes are more widely deployed to analyze malicious emails, prompting some hacker groups (e.g., MoneyTaker) to reconsider their initial-breach technique, abandoning spear-phishing in favor of exploiting vulnerabilities in internet-banking applications, or identifying vulnerabilities in network infrastructure.
- After their leaders' arrest, the remaining members of the Cobalt and Fin7 hacker groups might organize new teams, and this may lead to an increase in the number of active groups, training their new members.
- Currently, all financially-motivated APT groups that focus efforts on targeted attacks on the financial sector are Russian-speaking (except Lazarus which is known as a state-sponsored group, but still conduct attacks aimed to steal money). We expect similar groups to appear in Asian/Latin American hacker communities, first attacking regional banks.
- The Lazarus group will continue to attack banks and steal funds via SWIFT. They will likely experiment with attacks on card processing, primarily focusing on Asia and the Pacific.
- In addition to stealing funds, BlackEnergy and Lazarus will conduct sabotage attacks, which may potentially cost much more than the unauthorized money transfers.

Attacks on bank clients

- We still believe that a more aggressive use of self-propagating Trojans will increase the efficiency of

attacks using PC banking Trojans and POS Trojans.

- Free Wi-Fi networks set up on vulnerable routers may become a major vector for propagation in POS-equipped restaurants and retail stores.
- We expect attacks in Russia to start targeting business mobile banking apps soon. Contextual ads may become a major vector for malware propagation here.
- Losses from phishing in Russia are expected to increase. Home routers redirecting users to phishing websites will be used to improve the efficiency of these attacks.
- The Toplel and RTM botnets owners may shift their focus from attacks aimed at stealing money from businesses to targeted attacks on banks in Russia and the CIS.
- The Cutlet Maker malware may become a major threat for all ATMs as its source code has been made public. The program does not require tampering with the bank's network.
- Other malware, such as BackSwap and IcedID, has the potential to evolve into a substantial threat for banks on par with Dridex, Trickbot and Gozi.
- Android banking Trojans will continue to take over the global market, pushing banking Trojans for PC out of the market.

Threats to cryptocurrencies and blockchain projects

- We expect that the Silence, MoneyTaker, and Cobalt groups will stage multiple attacks on cryptocurrency exchanges.
- The 51% Attacks and manipulation with exchange rates will be focused only on new and relatively unknown cryptocurrencies.
- ICO projects attacks will remain a threat for every project potentially able to attract investors.
- Cryptojacking has passed the peak of its popularity. We expect to see less unauthorized mining in the coming year, whether through specialized Trojans or through cryptojacking.
- The world's largest mining pools may become the target not only for financially-motivated cybercriminals, but also for state-sponsored hackers. If successful, they may take over 51% of the network's mining hash rate and obtain control over the cryptocurrency and its transactions.
- Phishing and malware are the most tangible threats for private cryptoinvestors.

3. HARDWARE AND BIOS/UEFI VULNERABILITIES

Last year, cyber security experts were focused on the epidemic of WannaCry, NotPetya, and BadRabbit ransomware, but in 2018, the most significant issue were side-channel attacks and new vulnerabilities that were found in CPUs of different vendors and cannot be patched completely.

Another critical but less sensational issue is a firmware vulnerability in UEFI and BIOS with reports on them becoming more widely available.

Vulnerabilities in both CPUs and firmware open new prospects for attackers and in several years they may seriously affect the cyber security market. This is the reason why we have put the information about these trends first.

99,95%

the success rate of the SpectrePrime attacks

HARDWARE VULNERABILITIES

Meltdown and Spectre

Since the middle of 2017, closed security research has been conducted into hardware vulnerabilities that impact most CPUs by Intel and AMD as well as chips, which use ARM processor cores. In January 2018, information on these vulnerabilities known as Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 and CVE-2017-5715) was publicly disclosed. Information on Meltdown and Spectre has received enormous resonance, due to the danger they present. This fact, in its turn, led to more research connected to speculative execution, new vulnerabilities, and exploits.

Meltdown allows the attackers to read not only the kernel memory, but the entire physical memory of the target machines and, consequently, all the secrets stored in the software and OS. Experts believe that the greatest danger of this vulnerability is its almost complete independence from the operating system. In addition, Meltdown leaves no traces in the system, which makes it more difficult to find the malicious code that exploited this vulnerability.

Spectre breaks the isolation between different applications, allowing the malware to trick any process into leaking the content of its own memory. The first Spectre attack option offered used JavaScript to gain access to the browser memory, where attackers could get hold of other websites' data or, for example, saved passwords.

Spectre attacks can be used to leak data from the kernel or application memory and from hypervisor to the guest systems.

There were 4 published variants of microarchitectural bugs connected to speculative execution:

Variant 1. Bounds Check Bypass
CVE-2017-5753

Variant 2. Branch Target Injection
CVE-2017-5715

Variant 3. Rogue Data Cache Load
CVE-2017-5754

- **Variant 3a.** Rogue System Register Read
  CVE-2018-3640
- **Variant 4.** Speculative Store Bypass
  CVE-2018-3639

MeltdownPrime and SpectrePrime

In February, a team of security researchers from NVIDIA and Princeton University published a paper, in which they described new types of attack affecting almost all modern CPUs. The principle of these attacks is similar, but the innovation is that they focus on multi-core chips and use the revocation mechanism of cache lines in modern cache memory coherence protocols during data transfer between cores. As in the case of Meltdown and Spectre, a successful attack allows you to gain access to important information closed to third party apps, such as passwords. SpectrePrime code proposed by researchers as a proof of concept, leads to the success of 99.95% of the attacks on an Intel processor (the success rate of the Spectre attacks reaches is 97.9%).

The hardware issue is in Translation Lookaside Buffers (TLBs), which are present in all modern processors and make them all vulnerable to Meltdown and Spectre. A TLB reduces the time taken to access RAM because it eliminates the translation of memory addresses.

TLBleed

In July, another vulnerability involving TLBs surfaced, which was called TLBleed. This vulnerability allows the processes that use the same physical core but different logical cores to gain access to each other's data. It was demonstrated that cryptographic keys and other important data can be extracted from another running program with a minimum success rate of 98%. Despite the fact that the vulnerability was not identified with CVE, OpenBSD developers decided not to support the Hyper-Threading in Intel processors. TLBleed differs from Spectre and Meltdown, which exploit speculative execution. In this case, the breach is connected to weak spots in Hyper-Threading technology and the way processors cache data.

Rowhammer

Rowhammer was revealed in 2015, when Google researchers published a report on the exploit. They rated Rowhammer as one of the most potentially dangerous attack scenarios for PCs and laptops. Rowhammer attacks are possible due to the high density of memory cells in modern devices and can be triggered by repeated raw activation that can cause bit flips in adjacent rows. As a result, the attacker can gain kernel privileges on a PC or laptop and root access on a mobile device.

In March 2016, researchers in the VUSec research group at Vrije Universiteit in Amsterdam successfully conducted an attack on Android. The attack on the mobile platform via DRAM was called Drammer. It is the first root exploit for Android that does not rely on a software vulnerability but exploits the Flip Feng Shui technique. The attack was conducted on 27 different Android devices with ARM architecture (32-bit and 64-bit) including Samsung Galaxy, LG Nexus, Motorola Moto G, and HTC Desire. Researchers found that 18 devices from the test sample are vulnerable to Drammer.

In October 2017, a group of scientists from Adelaide, Pennsylvania, Maryland and Graz University of Technology published a research study in which they described a way of bypassing protection from Rowhammer, targeted at DRAM. According to the research, the scientists found a way to launch an attack, despite the security measures. To do this, the attackers only need to focus their efforts on one row of cells instead of attacking several rows. Tests show that with this approach the Rowhammer attack takes 44 to 138 hours.

In May 2018, a team of researchers from Vrije Universiteit Amsterdam presented a new way of exploiting the Rowhammer vulnerability using graphics processing units (GPUs) and WebGL to attack the device memory. The new method was called GLitch. It is a combination of a side-channel attack and a traditional Rowhammer attack. The researchers used the side-channel to determine the physical memory layout, and then they used the Rowhammer attack to flip bits and inject malicious commands into the RAM. To perform the side-channel attack, the researchers leveraged browsers and their support for the WebGL standard.

The specialists successfully tested the GLitch technique on an Android device with Chrome and Firefox browsers. They were able to compromise the device in just two minutes. To exploit the attack technique, all they had to do was upload the malicious JavaScript code to the target device. The researchers said they only tested their proof-of-concept code on a Google Nexus 5 smartphone, but the exploit code should work on all devices that use a Qualcomm Snapdragon 800 and 801 system-on-chip.

BIOS/UEFI VULNERABILITIES

BIOS and now UEFI vulnerabilities have been known about for a long time. The exploitation of the attack is not easy, and detecting an infection is even harder, so security experts of some corporate networks do not care much about this problem. However, the situation is changing rapidly, and side-channel attacks on hardware vulnerabilities may become a new driver to speed up the development of BIOS/UEFI threats.

The ability to survive both reinstallation of OS and changing a hard drive makes research in this field a priority for attackers.

On the next page you will find a graph that shows a significant growth of research activities connected to the search of vulnerabilities in BIOS/UEFI since 2015. At the same time, the number of threats that are used in real targeted attacks has also grown.

We know that BIOS/UEFI backdoors are used for real targeted attacks only from leaks:

2014 Edward Snowden leaked that NSA was exploiting the DEITYBOUNCE backdoor installed on Dell PowerEdge servers via motherboard BIOS and RAID controllers.

July 2015 Analysis of a leaked toolkit of the Italian company Hacking Team revealed a UEFI BIOS rootkit that checked and installed the main backdoor into an OS.

March 2017 Documents were published on Wikileaks on several CIA projects that the special agency used to infect Apple products (Mac, iPhone) with firmware-level malware, which worked even after OS reinstallation.

August 2017 BANANABALLOT, a BIOS implant was found among the Shadow Brokers-leaked Equation Group tools.

Data from these leaks encourages researchers to pay more attention to firmware security and publish results of their research in open access.

August 2016 Dmytro Oleksiuk wrote and published the source code of PEIbackdoor. This backdoor is applicable to UIFI-compatible firmware. It allows execution of arbitrary C code during the Pre EFI Init (PEI) phase.

October 2016 Dmytro Oleksiuk wrote and published the source code of the SMM backdoor for UEFI-compatible firmware.

July 2017 During the BlackHat conference, Alex Matrosov talked about 6 new vulnerabilities he discovered in the motherboard firmware of several manufacturers. He discovered privilege escalation on ASUS Vivo Mini (CVE-2017-11315), Lenovo ThinkCentre systems (CVE-2017-3753), and MSI Cubi2 (CVE-2017-11312 and CVE-2017-11316), as well as a way to bypass the security of Intel Boot Guard on Gigabyte BRIX, which was caused by two vulnerabilities identified as CVE-2017-11313 and CVE-2017-11314.

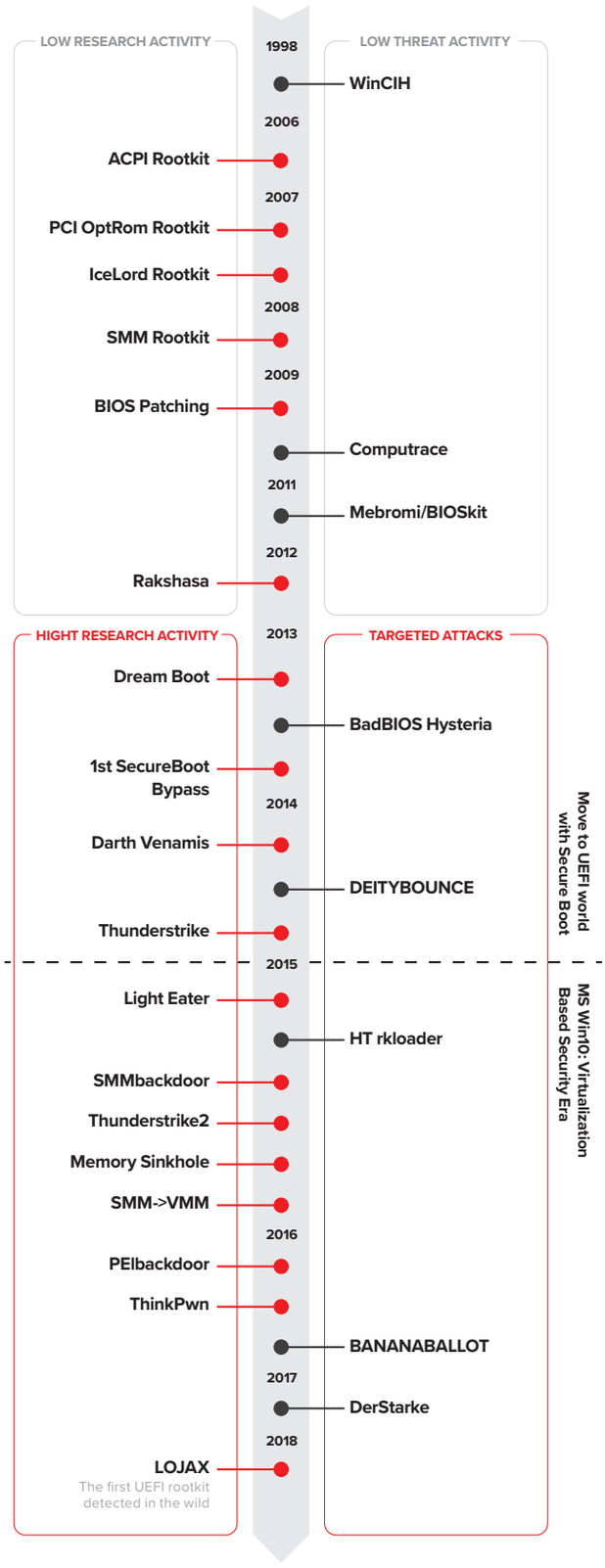
October 2017 Alexander Ermolov, a security researcher at Embedi, bypassed the security of Intel Boot Guard on a Gigabyte GA-H170-D3H motherboard. Ermolov notified AMI of his findings and was told that the issue had already been addressed and that OEMs had been alerted of the matter. The latest AMI BIOS codebase available to customers (OEMs) is no longer vulnerable. However, the researched decided to test the patch and discovered that things had gone from bad to worse.

May 2018 Malicious instances of legitimate LoJack software modified by hackers were discovered. The original software, Computrace LoJack, is used to protect their assets should they be stolen. It allows attackers to turn off the restart function of the stolen computer, turning it into a brick. LoJack, as well as the UEFI rootkit, continues to operate in the OS is reinstalled or the hard drive is changed. Researchers said that modified instances of LoJack contained small changes in the code that made it communicate with the C&C server of the attackers instead of the legitimate central server of LoJack. Researchers analyzed the addresses of the C&C servers and connected the attacks to APT28 (aka Fancy Bear, Sofacy, Pawn Storm, Sednit, and Strontium), however they could not ascertain how malicious instances of LoJack had been installed on the computers.

The leaks above imply that physical access is required to install the UEFI backdoor, but there are also scenarios for remote installation. For this purpose, the attack is divided into 4 stages:

- **Stage 1:** Exploit vulnerability in OS application to drop installer. The installer must escalate privileges to System level.
- **Stage 2:** Bypass code signing policy of the kernel application and install kernel-mode payload.
- **Stage 3:** Execute SMM exploit, escalate privileges for SMM, and execute malicious payload.
- **Stage 4:** Bypass Flash write protection and install rootkit into firmware.

Due to the last two stages, conducting such an attack seems incredibly complicated (it is), but with recent vulnerabilities and exploits it can be done:



Threat	Description
SMI Handlers	Memory corruption vulnerabilities can lead to arbitrary SMM code execution.
S3BootScript (VU #976132)	Arbitrary modification of platform firmware. Allows attacker to arbitrarily read/write to the SMRAM region.
ThinkPwn (LEN-8324)	Arbitrary SMM code execution exploit for multiple BIOS vendors. Allows attacker to disable flash write protection and modify platform firmware.
Aptiocalypsis (INTEL-SA-00057)	Arbitrary SMM code execution exploit for AMI Aptio-based firmware. Allows attacker to disable flash write protection and modify platform firmware.

Despite the fact that the vulnerabilities are from 2015 to 2016, they are still relevant. In corporate networks, UEFI is usually not updated. Moreover, some vendors do not issue updates at all. The situation worsens because of the way some motherboard manufacturers protect motherboards by default for different BIOS/UEFI.

For example, some vendors do not turn the following on by default:

- SMM_BWP — SMM BIOS Write Protect
- PRx — SPI Write Protection
- BLE — BIOS Lock Bit

Vendor Name	BLE	SMM_BWP	PRx	Authenticated Update
ASUS	+	+	-	-
MSI	-	-	-	-
Gigabyte	+	+	-	-
Dell	+	+	-+	+
Lenovo	+	+	RP	+
HP	+	+	RP/WP	+
Intel	+	+	-	+
Apple	-	-	WP	+

4. SABOTAGE AND ESPIONAGE

As we projected in our report last year, the threat landscape for critical infrastructures is growing more complex, provoked by the activity of government-related hacker groups. The centre of innovation in targeted attacks has shifted to pro-government groups. Earlier, pro-government hackers were monitoring targeted attacks, developments and tactics of financially motivated cyber criminals, whereas now these criminals are closely following pro-government attackers who are more advanced than them.

The landscape of APT threats is unique and constantly changing in every region of the world. Known groups drop out of sight, change attack tactics, and of range targets. Previously unknown groups appear. As a rule, by the time new players are discovered, they have been active for several years but went unnoticed for various reasons. Therefore, lack of data on attacks in a specific country or economic sector is likely a sign that the groups are unknown rather than non-existent.

Below you will find data on the most active APT groups in various regions as well as noteworthy tactics of state-sponsored groups.

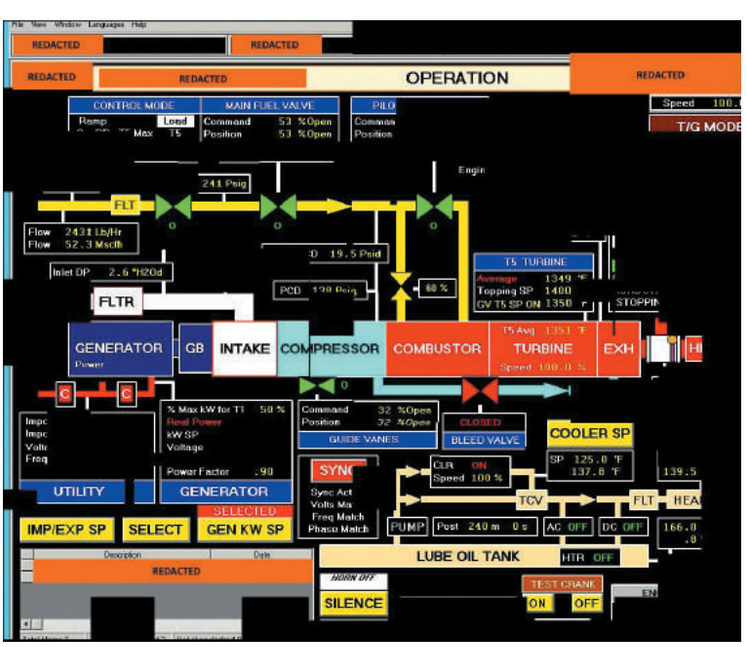
AMERICAS	EUROPE	ASIA-PACIFIC	MIDDLE EAST & AFRICA	RUSSIA
APT28 — Russia	Lazarus — North Korea	DarkHotel — North Korea	OilRig — Iran	Equation — USA
Turla — Russia	APT28 — Russia	Lazarus — North Korea	APT37 — North Korea	APT10 — China
Lazarus — North Korea	APT15 — China	Thrip — China	Slingshot — USA	APT17 — China
APT15 — China	Tick — China	APT32 — Vietnam	Newscaster	PlugX — China
Thrip — China	BlackEnergy — Russia	Andariel — North Korea	Team — Iran	Prikormka — Ukraine
Charming Kitten — Iran	Dragonfly — Russia	Mustang Panda — China	APT34 — Iran	APT28 — Russia
Mustang Panda — China	TEMP.Periscope — China	APT37 — North Korea	APT33 — Iran	BlackEnergy — Russia
Dragonfly — Russia	Gorgon Group — Pakistan	Slingshot — USA		PowerPool
Gorgon Group — Pakistan	Orangeworm	Kimsuky — North Korea		
TEMP.Periscope — China	PowerPool	Tick — China		
Newscaster		BlackEnergy — Russia		
Team — Iran		Charming Kitten — Iran		
Orangeworm		APT28 — Russia		
		MuddyWater — Iran		
		Sidewinder — India		
		Chafer — Iran		
		TEMP.Periscope — China		
		APT17 — China		
		Orangeworm		
		Rancor		

Based on attack attribution performed by security companies and law enforcement.

TARGETED ATTACKS ON CRITICAL INFRASTRUCTURE

One of the most advanced threats for critical infrastructure facilities has been Industroyer (or CRASHOVERRIDE) that disabled the Ukrainian power grid facilities in December 2016. In 2017 this tool was described in detail by ESET and it was linked to a group named Black Energy. The key feature of Industroyer is the ability to control remote terminal units (RTU) responsible for the connection and disconnection of the physical grid. Such elements are used not only in power grids but also in water supply, gas supply, and other industrial systems.

At the end of 2017 and beginning of 2018, Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) conducted a joint study and issued alerts indicating attacks on energy, nuclear, commercial, water supply, aviation and other critically important manufacturing sectors, coming from Russia (because the BlackEnergy group was linked to that country). The alerts confirmed that the attackers had successfully gained access to the SCADA control system and demonstrated one of the screenshots made by the attackers.



At the same time, an incident at one of the critical infrastructure facilities helped to reveal information on another tool called TRITON — a framework that helps to interact with Triconex Safety Instrumented System (SIS, a safety system for manufacturing processes) by Schneider Electric.

The attacker gained remote access to the workstation of an SIS operator and deployed TRITON to reprogram SIS controllers. During the incident, SIS controllers entered the safe mode that automatically turns off the manufacturing process, which forced the victim company to start an investigation. The analysis revealed that SIS controllers initiated a safe shut down when the application code failed to pass the control between back-up processors, which prompted a diagnostic error message.

TRITON helps manage SIS Triconex controllers, i.e. stop them, read the data in the memory, reprogram, and add malware functionalities. The malicious code co-runs on the controller with the legitimate one to make sure the controller remains in operation. If a failure occurs due to controller reprogramming, TRITON will try to restore its operation. If the controller has been unable to recover within a certain time window, the malicious code will replace itself with invalid data to cover up its traces.

Possessing such capabilities, the attacker may halt the operation of a manufacturing facility in one of the following ways:

- Reprogram the safety controller (SIS) so that it would think one of the processes has switched to its critical state, which would result in its suspension.
- Reprogram the controller to make it ignore truly critical process states and wait until a critical state occurs naturally.
- Reprogram the controller to make it ignore truly critical process states and provoke occurrence of such states by manipulating other production systems.

CASE: OLYMPIC DESTROYER

In February 2018, an attack by a malware dubbed Olympic Destroyer took down the official website of the Pyeongchang Olympics and Wi-Fi at the stadium, and caused interruption of a live broadcast during the opening ceremony. A number of researchers linked this attack to a group called Sofacy, also known as Fancy Bear and APT28.

The software performed the following steps to take the system down:

1. After the launch, it extracted two modules to collect logins and passwords.
2. The first module collected logins and passwords stored in the web browser.
3. The second module collected logins and passwords from the LSASS process as it was performed by a well known utility Mimikatz.
4. Using the extracted logins and passwords and an exploit called EternalRomance from the Shadow Brokers leaks, the software started propagating across the network.
5. After infecting the computers, the software continued with disabling them in the following way:
    a. Deleted shadow copies by calling up a standard utility vssadmin.exe;
    b. Deleted back-up copies by calling up a standard utility wbadmin.exe;
    c. Turned off system recovery by calling up a standard utility bcdedit.exe;
    d. Deleted system logs using a standard utility wevtutil.exe;
    e. Turned off all system services;
    f. Listed connected network folders and replaced the files with zeros.

MASS ATTACKS WITHOUT CLEAR TARGET

BadRabbit

Following WannaCry and NotPetya, on October 24, 2017 there was a new mass attack by a ransomware called BadRabbit. Group-IB was the first to confirm the connection between BadRabbit and the epidemic of the virus dubbed NotPetya that had attacked energy, telecommunication, and financial companies in Ukraine in June 2017. We discovered that the code of BadRabbit had been compiled from NotPetya's source code. There are hash functions, a network propagation method, and a log deletion approach that are unique. The module extraction logics and the modules themselves confirm this connection.

BadRabbit was a mass attack, although the number of victims was much lower than in the case with NotPetya. In Ukraine, BadRabbit attacked several strategic facilities (airport, underground, public authorities) and in Russia, offices of federal mass media. The malware also attempted to penetrate the banking infrastructure but it failed.

Unlike NotPetya, BadRabbit propagated by means of "drive-by download," not "watering hole attack." To spread the virus, the attackers used a number of popular internet resources in Ukraine and Russia. The research confirmed that the access to the websites was gained via a targeted attack — at least in one case when legitimate resources were compromised, the website developer's computer was hacked to further compromise the website.

The group made changes to its tool and tried to pretend to be a regular criminal group. Previously, NotPetya contained one wallet for ransom transfers, which lead to an assumption that the authors had intentions of decoding the files and the key goal was sabotage, whereas now a unique key is automatically generated for each computer and a separate wallet is assigned to each key. Moreover, the BadRabbit attack used a domain name earlier used by regular cyber criminals in their attacks for phishing and traffic collection purposes.

But this mass attack was only a distracting factor. The objects actually intended for destruction had been compromised prior to the attack.

VPNFilter

Another mass attack that hackers have been working on but have not launched yet is a threat dubbed VPNFilter that became known in May 2018. This malware had infected about 500 thousand routers of Linksys, MikroTik, NETGEAR, and TP-link, as well as NAS by QNAP in 54 different countries.

Unlike the vast majority of malware for routers, VPNFilter is capable of surviving after a reboot. The infection process consists of three stages and there is an individual module for each stage. The first module is simply responsible for adhering to the device even after it has been rebooted. The second module disables the device. The third module is responsible for downloading additional plug-ins that can intercept the victim's traffic and detect SCADA systems.

Even after the FBI reported they had regained control over the management server, scanning and search for new vulnerable routers continued.

SABOTAGE-ORIENTED ATTACKS ON BANKS

Banks are also considered to be part of critical infrastructure, which is why the availability of tools and experience in disrupting bank systems are priorities for attackers. Such tools are actively used by two groups in particular: BlackEnergy and Lazarus.

ONI Ransomware

From March to August 2017, hackers conducted attacks on Japanese banks and other organisations. This campaign resulted in the infection of corporate networks with the ONI ransomware. The steps of these long and complex attacks were as follows:

1. Spear-phishing emails with malicious attachment 領収証.doc (Receipt.Doc) were sent..
2. Ammyy Admin was launched on victim's PC.
3. Reconnaissance was completed, and credentials were stolen from the victim's PC.
4. Lateral movement and takeover of Domain Controller

(DC). At this stage, attackers also used the EternalBlue exploit. It should be noted that the attackers did not use a self-distribution mechanism.

5. Log wipes and ONI ransomware were spread using Group Policy Object (GPO).

Group-IB specialists assume that the attacks in Japan were conducted by BlackEnergy group. The following point to this:

- At the end of 2016 and in January and February 2017, targeted attacks on financial institutions in Ukraine were detected. Scammers spread the TELEBOT backdoor, which was controlled via Telegram Bot API. During the final stage of the attack, the hackers used the eraser KillDisk. The software deletes important system files so that the system cannot be booted and rewrites files of various types. This means that the attackers deleted signs of their presence, as was the case during the attacks against Japanese banks.
- The attacks on Japanese banks began in March 2017 at the latest, which is very soon after the attacks in Ukraine. During the attacks in both Japan and Ukraine, attackers did not use a self-distribution mechanism.
- During the attacks in Ukraine in February 2017 and later during the NotPetya and Bad Rabbit attacks, the hackers used ransomware that modifies MBR.
- ONI ransomware is based on the source codes of the DiskCryptor utility and this code was used in both NotPetya and Bad Rabbit ransomware.
- Ammyy Admin used in the Japan attacks is a utility developed by a Russian company.
- There are elements of Russian language in ONI's source code.

Lazarus attacks

The Lazarus group has repeatedly been observed conducting attacks for sabotage purposes in South Korea. In 2018, they gained access to the local networks of Banco de Chile and Bancomext and withdrew money through SWIFT. At the final stage, they used a new version of the program to overwrite the Master Boot Record (MBR) and disable the bank's network. According to media publications, the attack at Banco de Chile affected about 9,000 computers and more than 500 servers.

ATTACKS ON ROUTERS AND OTHER DEVICES

In 2018, a malware called Slingshot was found after remaining undetected for six years. It is not known exactly how Slingshot infected the first targets. However, we know that malware creators injected malicious code into the router of a Latvian company called MikroTik.

In May 2018, new malware was found called VPNFilter. Experts note its resemblance to BlackEnergy. The Trojan infected at least half a million routers of Linksys, MikroTik, NETGEAR, and TP-link, as well as NAS by QNAP and other devices (a total of 71 models) in 54 countries.

The Orangeworm group was only discovered in 2018, although they have been attacking healthcare organizations in the U.S., Europe, and Asia were since 2015. In the course of the attack, hackers infect machines with software for operating and managing hi-tech image processing devices (e.g. X-ray units, MRI units), as well as software to assist patients filling out Procedure Agreement forms.

TRENDS IN SABOTAGE AND ESPIONAGE-ORIENTED ATTACKS

Evasion and counter-forensics

An important tactic to make infection difficult to detect is covering up the interaction of infected devices with a C&C server. Traditionally, encryption is used for that purpose. However, to complicate matters even more, some groups use other interesting techniques:

- APT15 uses RoyalCli and BS2005 Trojans that communicate with C&C via Internet Explorer using COM interface of IWebBrowser2. Due to the nature of the IE injection method, several C&C commands are cached to the disk by the IE process.

- The Rokrat Trojan used by APT37 interacts with C&C server and receives commands from its operators via Twitter.

- Since October 2017, cybercriminals from Rancor added PLAINTEE, which they developed, to the armory. Its distinguishing feature is the custom version of the UDP protocol that is used to connect to the attackers' C&C server.

- Hackers from Turla used comments in Britney Spears' Instagram account to obtain relevant C&C server address. To do this, the malware read comment, calculated hash, and, after finding the comment with hash sum that equals 183, extracted the server's address as a short link.

Publicly available tools

Many APT groups do not innovate but use well known techniques and vulnerabilities. Most of them use previously created tools and existing code in new tools, which makes correlation with older attacks easier. However, there are exceptions: when APT groups use general-purpose tools, it complicates attribution.

- APT28 started using Koadic Trojan, which is an open-source RAT that is promoted as a penetration testing tool.

- Such groups as Turla, Lazarus, OilRig, Charming Kitten, Newscaster Team, APT32, and MuddyWater have started using Metasploit more often. It is a popular framework for penetration testing. The groups APT10, APT17, APT32, and TEMP.Periscope started using another popular framework called Cobalt Strike.

- OilRig groups started using Invoke-Obfuscation, which is an open-source tool available via Github repository.

- For attacks targeted at government agencies, Gorgon Group uses phishing emails with Microsoft Word documents that exploit the CVE-2017-0199 vulnerability. In the course of the attack, hackers upload a widely distributed Trojan — NanoCoreRAT, QuasarRAT, or NJRAT — to the victim's computer.

Zero-day vulnerabilities

Efficient espionage is not possible without zero-day exploits, which is why APT groups spend a lot of resources to develop and buy them.

- In the beginning of June, 2018, experts detected a new wave of attacks exploiting CVE-2018-5002: a zero-day vulnerability. Breach in Adobe Flash Player 29.0.0.171 connected to stack buffer overflow allows the attackers to launch arbitrary code on the victim's machine. It was discovered that this vulnerability was actively used in targeted attacks on the Middle East with Qatar as the main target. It is presently not known which APT group was behind the attacks.

- Recently founded group PowerPool started using the CVE-2018-8440 vulnerability in a malicious campaign. The vulnerability touches on Microsoft Windows 7 to 10, to be exact, the Advanced Local Procedure Call (ALPC) interface in the Windows Task Scheduler. It provides Local Privilege Escalation that allows the attacker to escalate privilege to System. Hackers took the exploit's Proof-of-Concept source code from a GitHub repository and partially modified it.

Among the most active exploiters of zero-day vulnerabilities are groups that are believed to be connected with North Korea.

- DarkHotel used such zero-day vulnerabilities as CVE-2018-8174 and CVE-2018-8373:
  - CVE-2018-8174 is a use-after-free (UAF) vulnerability that is connected to VBScript implementation in Internet Explorer and Microsoft Office. Initially, this zero-day vulnerability was called a “double kill.” It uses the technique of “damaging” two memory objects and changing the type of one object to Array to make reading and writing address space possible. Another object’s type is changed to Integer to obtain the address of the arbitrary object.
  - CVE-2018-8373 also touches on the VBScript engine in the last version of Windows. Attackers exploited UAF-type vulnerability located in vbscript.dll library that was left unpatched in the last VBScript engine.
- In 2018, researchers discovered a new cyberespionage campaign by Andariel, which involved at least nine breaches in ActiveX platform, including zero-day vulnerability. Researchers assumed that the latter was associated with Samsung’s desktop application — Samsung SDS Acube — which is quite popular among South Korean companies.
- Attackers from APT37 started using zero-day vulnerability in Adobe Flash Player (identified as CVE-2018-4878) in the middle of November 2017. South Korean CERT reported the vulnerability at the end of January 2018. The vulnerability was closed only in February, 2018. The vulnerability that allowed the attacker to launch arbitrary code remotely only touched on the current version of the product, 28.0.0.137, and earlier versions.

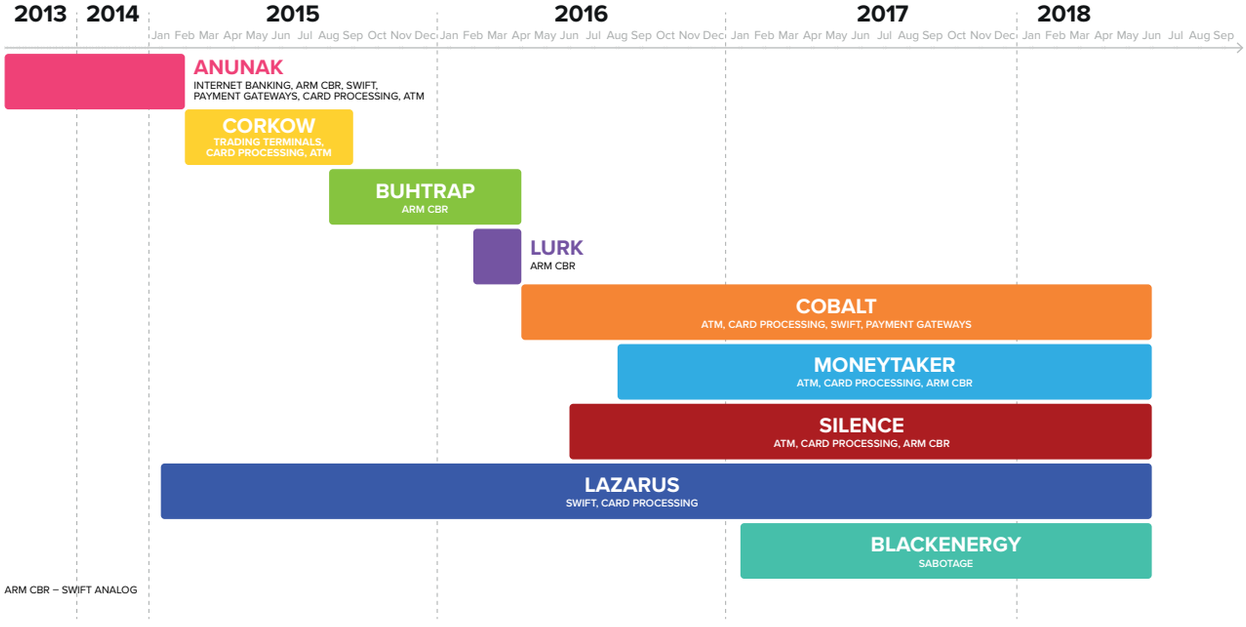
APT groups invest heavily in development and acquisition of zero-day exploits

5. THEFTS

TARGETED ATTACKS ON BANKS

Group-IB has identified four criminal APT groups that pose a real threat to the financial sector. They are able not only to penetrate a bank's network and access isolated financial systems, but also to withdraw money via SWIFT, AWS CBR, card processing systems, and ATMs. These groups include Cobalt, MoneyTaker, and Silence (all three led by Russian-speaking hackers), as well as the North Korean group Lazarus. These groups are leaders in developing new tools and techniques and set trends in advanced attacks on banks. Group-IB was the first to issue reports on all these groups.

Each of these groups has a long history. The diagram below shows the beginning and end of their activities involving attempted bank robberies. Groups that focused on sabotage and espionage have not been included.



SWIFT AND LOCAL INTERBANK PAYMENT SYSTEMS

Group-IB experts have observed that the number of targeted attacks against banks which has resulted in illicit SWIFT payments has has tripled over the reviewed period. In the previous period, three such attacks were tracked — in Hong Kong, Ukraine, and Turkey. In this period, however, 9 successful attacks have already taken place in Nepal, Taiwan, Russia, Mexico, India, Bulgaria, and Chile.

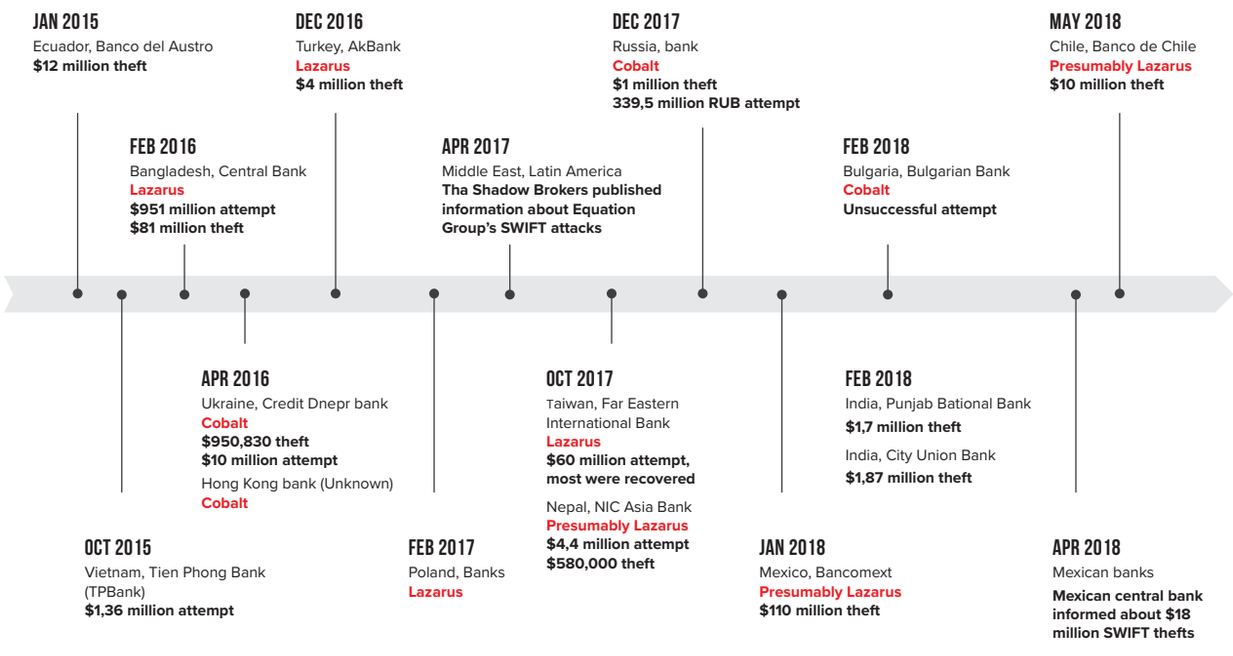
Only two criminal groups pose a threat to the SWIFT interbank transfer system: Lazarus and Cobalt. At the end of 2017, the latter conducted the first successful attack on a bank using SWIFT in the history of Russia's financial sector. The first successful attack carried out by Lazarus was tracked in February 2016, when the group attempted to steal almost $1 billion from the Central Bank of Bangladesh. Just two months later, the Cobalt group conducted two successful attacks on banks in Hong Kong and Ukraine.

When committing thefts through SWIFT, Cobalt and Lazarus carefully prepared the cash-out scheme and stole funds from two banks simultaneously, probably to reduce the costs associated with cash withdrawal. The good news is that in the case of SWIFT, most unauthorised transfers can be stopped in time.

An analysis of the bank attacks and respective threat actors behind them shows that the Lazarus group focus on the Asia-Pacific region, while the Cobalt group primarily targets Eastern Europe.

SWIFT attacks in Russia and Bulgaria were carried out without any special tools. Cobalt used only its standard toolbox. Having accessed the bank's network and obtained the logins of legitimate users, the hackers performed several transactions, most of which were successfully blocked.

Although Lazarus actively attempted to steal money through SWIFT over the past year, the group was significantly more successful in attacking cryptocurrency exchanges (see the relevant section of the report for more details). That being said, we have not identified any evidence confirming the group's interest in other local interbank transfer systems.



Attacks on AWS CBR

In 2016, the most attractive target in Russian banks for hackers was AWS CBR — the Russian equivalent of SWIFT. In 2017 and 2018, the Cobalt and Silence groups ignored AWS CBR, even in cases where they managed to get access to it. Their attention is now drawn to more reliable theft schemes, i.e. through ATMs and card processing systems. That being said, Cobalt is also interested in local systems of interbank transfers abroad. Having accessed the network of a foreign bank, they tried to withdraw more than 20 million euros through the local interbank transfer system, but the attempt was unsuccessful.

Withdrawing money through AWS CBR (Automated Work Station Client of the Russian Central Bank) is a tactic used by MoneyTaker only. In November 2017, the group managed to withdraw $104,000, while in summer 2018, they successfully stole $865,000 from Russia's PIR Bank.

In July 2018, a user with the nickname Bobby.Axelrod published, on an underground forum, the source code and instructions to the Pegasus spyware used to generate automated attacks on AWS CBR, with automated replacement of payment credentials. This spyware was used by the Buhtrap group in 2016 and all the files in the archives relate to that period. It worth noting that automated replacement of payment credentials using the spyware does not work in new versions of AWS CBR, but the archives provide valuable resources on automating other stages of attacks on banks.

CARD PROCESSING

Attacks on card processing systems remain one of the main theft methods and are actively used by Cobalt, MoneyTaker, and Silence. Focusing attacks on ATMs and card processing systems has reduced the average amount of damage caused by one attack. However, it helps hackers conduct such attacks more securely for money mules, who cash out the stolen money: the attackers are in one country, their victim (the bank) is in another, and the cashing out takes place in a third country.

Cobalt is the 'champion' when it comes to these types of attacks. In 2017, they set a "personal best" in attempting to steal over 25 million euros from a bank in Central Europe. In other regions, the financial loss has usually been much lower.

Attacks on card processing systems became more popular in 2016. In September 2016, Cobalt gained access to the networks of a bank in Kazakhstan and began preparations for a new type of theft — through the card processing system. It took around two months to prepare the attack and in November they successfully stole close to $600,000. The theft timeline was subsequently streamlined for attacks on card processing systems. Following this, card processing systems have become a major target in banks worldwide.

Around the same time, the MoneyTaker group began to carry out attacks on card processing systems. The very first attack that Group-IB attributes to MoneyTaker was conducted in the spring of 2016, when funds were stolen from a US bank by gaining access to First Data's STAR card processing system. The same bank was robbed again in January 2017, but this fact became known only seven months after the public release of our report on this group. In 2017, MoneyTaker hacked into nine more banks in the USA.

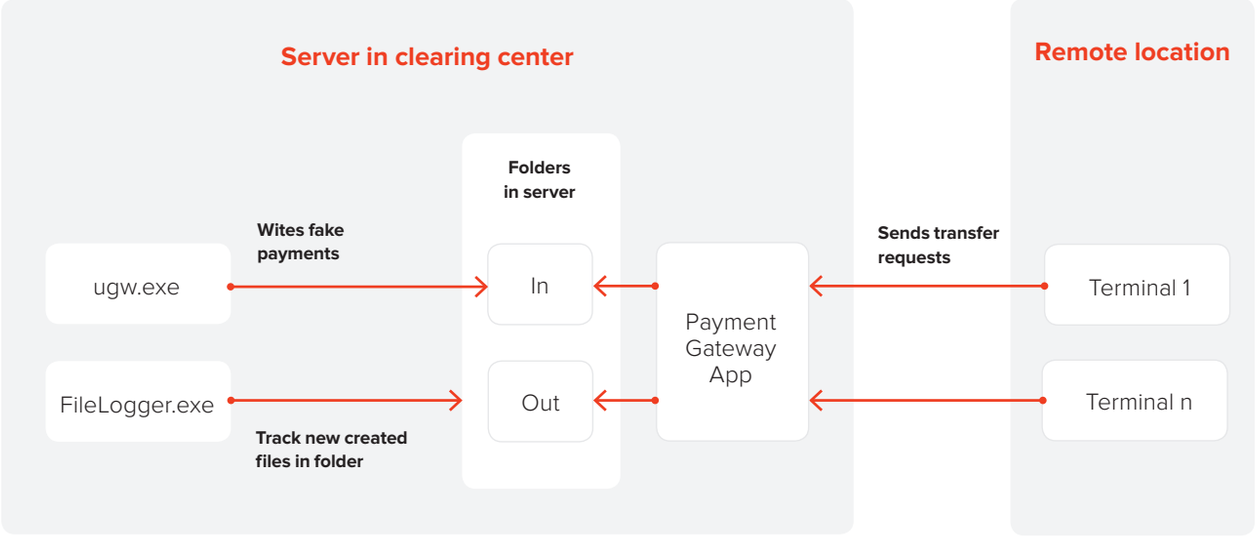
In February 2018, members of Silence conducted a successful attack on a bank and stole money via the card processing system; they managed to withdraw $522,000 from cards via a partner bank's ATMs.

No specialised software is required to successfully steal money through card processing systems. This means that the method can be used by any criminal group that has experience hacking into banking networks.

PAYMENT GATEWAYS

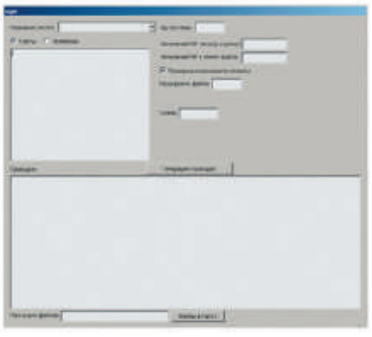
In the designated period, only Cobalt conducted attacks on payment gateways. In 2017, they used this method to steal money from two companies, however, no attempts were made in 2018. They were helped in one of their attacks by members of the group Anunak, which had not conducted at attack of this kind since 2014. Despite the arrest of the gang's leader in Spain in spring 2018, Cobalt continues to be one of the most active and aggressive groups, steadily attacking financial organizations in Russia and abroad 2-3 times a month.

The gateway normally processes two directories, In and Out, containing files with data in the format that is consistent with the transactions obtained from payment terminals. Payment files in the In directory are accepted for execution and money is transferred according to the data specified in a file.



To examine the data format, the attackers used the FileLogger.exe program which allowed them to monitor changes to a specified directory (creation of new files) and record the contents of new files into a specified text file. The directory and file are specified at program launch as input arguments.

Such gateways are usually used to transfer small amounts, therefore to steal a large sum of money the hackers had to create a number of small transactions. To perform automated transactions, the attackers created a unique program ugw.exe.

Интерфейс ugw	Содержимое файла «ugw.ini»
	[Config] typeData=0 numchek=4919 numfilename=114320 dur=0 bad=0 ext=dnr outfolder=D:\host\Gateway\In

At launch, the program requests a file with the name “terminals.txt“ containing fake terminal identifiers, to be used for fraudulent transfer requests. Following this, recipients’ accounts (telephone and card numbers) and transfer amounts are specified.

As a result, fake payment files are generated purporting to be obtained from legitimate terminals, and immediately placed in the In directory of a payment gateway. This technique enabled the attackers to transfer more than $2 million.

Learn more about Cobalt operations in our report

group-ib.com/reports

ATMS

Attacks targeting ATM networks were conducted by Cobalt and Silence. In May 2018, MoneyTaker also started attacking ATMs.

Cobalt

In 2016, the Cobalt group conducted a series of successful attacks on banks and their ATM networks in Russia and abroad. However, from autumn 2016, all their efforts were focused on different types of thefts. After a long break, in December 2017, they resumed attacks on ATMs in Russia.

The group used the same ATMSpitter malware that was previously used during attacks in Taiwan, Europe, and Russia. No major changes were made to the code. The malicious program allows the hacker to use Extensions for Financial Services (XFS) API in order to connect to an ATM dispenser and send commands to deplete cash cassettes.

The arguments transmitted at launch are the following:

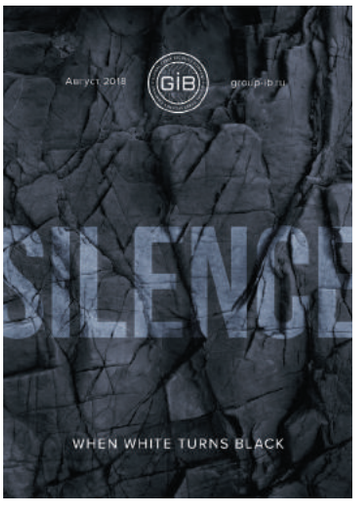
Argument	Description
ServiceLogicalName	A service name used as an argument for the WFSOpen function (for example, “Cash Dispenser Module”).
Cassettes Count	The total number of cassettes on the device. The value should be set in the interval from 1 to 15.
Cassette Number	The number of the cassette, which should dispense cash. The value should be set in the interval from 1 to 15.
Banknotes Count	The amount of banknotes to be dispensed from the cassette. The value should be set in the interval from 1 to 60.
Dispenses Count	The number of times cash dispenses should be repeated. The value should be set in the interval from 1 to 60.

Silence

To control the ATM dispenser, Silence uses a unique software called Atmosphere. Over time the Trojan has significantly evolved to address the needs of the criminals. For example, the developers have changed the logic of injection into processes and added the flexible injector, which has expanded the list of targeted ATMs.

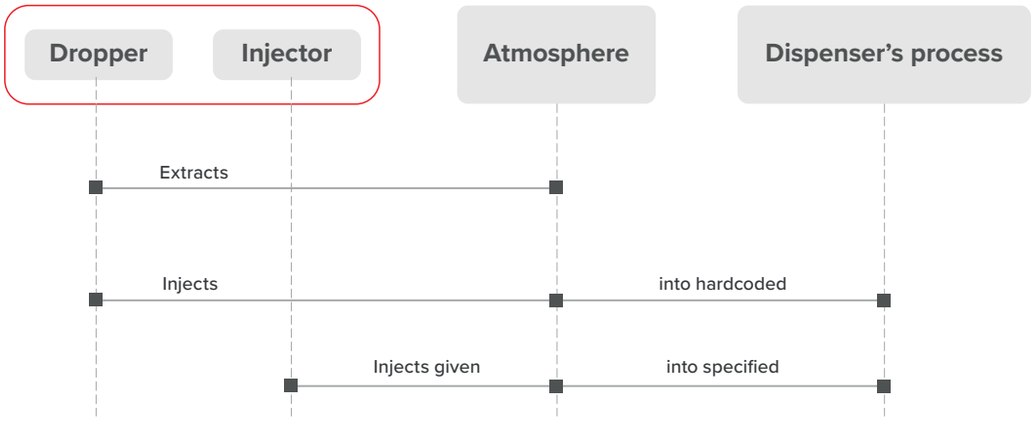
They have also removed the redundant features that interrupted the operation or were not used by the criminals. For example, the last version of the software didn't process commands from the PIN pad and the generated log got smaller. In the initial stages, the software was recompiled a lot, which resulted in several unsuccessful cashout attempts.

The hackers remotely install Atmosphere.Dropper on the ATM. The software contains a .DLL library, which is the main body of the Atmosphere Trojan. After the body is extracted, the dropper injects the library into the fwmain32.exe process. This enables the threat actor to remotely control the dispenser. In the first versions, there was a way to control the dispenser using the PIN pad, but later these features were deleted.



Learn more about Silence tactics in our report

group-ib.com/reports



Command	Description
“B”	Get information on the content of ATM cassettes. In addition, the string «cash units info received» is added into the log.
“A”	Get information on the content of ATM cassettes without logging.
“Q”	Get information on the content of ATM cassettes.
“D”	One-time withdrawal of notes of the specific face value from the ATM.
“H”	Suspend all threads in process except its own. Then use functions GetThreadContext + SetThreadContext to redirect their execution to its own function.
"M", "R", "S", "P", "T", "L"	Record the output of the last command into the C:\intel\<chrs>.007 file. This command is also executed after any other by default.

The program receives commands via files with the specific extension. The software reads commands, executes them, and then, as the author intended, it should overwrite the file with gibberish and delete it to hamper the work for forensics experts. However, the software logic contains an error, which results in the nonsensical text being written at the end of the file instead of over everything.

As part of incident response activities in one of the banks, Group-IB forensic specialists discovered about 11 samples of Atmosphere software, compiled at different times with slight changes. In one of the directories containing the Trojan we also discovered scripts for the command interpreter and a separate injector, which accepted a path to the DLL library as an argument, and an identifier of the process where it should inject the library. However, the scripts passed the target process name instead of the process identifier, which resulted in an unsuccessful attempt to take control over the dispenser.

MoneyTaker

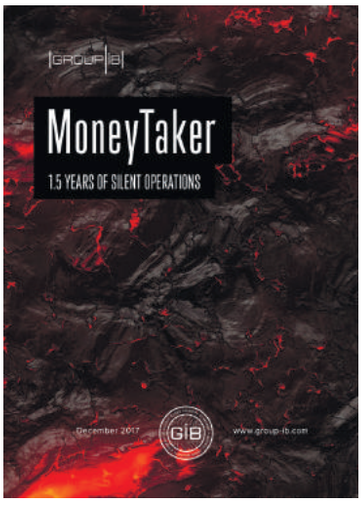
In May 2018 unknown cybercriminals conducted attacks against ATMs in Russia. To control dispenser they used unique program xfs_test.exe. Attacks were conducted against ATMs of various manufacturers.

It is known that after network penetration threat actors used PowerSploit scripts pack and tool for remote control Radmin. For the initial movement in the network, the Metasploit framework was used because there were traces of Meterpreter launching via sc.exe utility on infected machines.

Header of file contains information about path to debugging information:

M:\Work\atm\xfs_test\Release\xfs_test.pdb

This file is a program, which allows to communicate with ATM's dispenser via XFS API and to send command to empty cassettes. Sample functions in accordance with the argument sent at startup:



Learn more about MoneyTaker attacks in our report

group-ib.com/reports

Argument	Description
info	Create file «atm_info.log» and record in it all information about content of cassettes.
test	Check the possibility of cashing out from available cassettes several times, create file «atm_info.log» and record in it information about sum of cash that may be cashed out.
disp	Conduct cashing out from available cassettes several times (with 30s interval), create file «atm_info.log» and record in it information about cashed out banknotes.

ATTACKS ON BANK CLIENTS

PC TROJANS

World

The global landscape of threats from banking Trojans has changed dramatically. Six new banking Trojans for PCs have emerged: IcedID, BackSwap, DanaBot, MnuBot, Osiris, and Xbot. The same number of Trojans emerged in the last year. However, the new banking Trojans are mainly used locally.

The Osiris and Xbot Trojans were originally offered for sale on Russian-speaking hacker forums and have not yet been widely disseminated.

That said, Shifu, Qadars, Sphinx, Tinba and Emotet Trojans are no longer available. The latter is still used, but only as a loader, rather than a full-fledged banking Trojan. This could be due to the activity of law enforcement agencies, which have hit a market hard by arresting the developers of the Neverquest, GozNym banking Trojans, and also one of the most popular loaders — Andromeda.

In 2017, the source codes of the banking Trojans TinyNuke and AlphaLeon (aka Thantaos, Mercury Bot) were published. However, they were not employed later.

Zeus-based banking Trojans (ZeusVM, Atmos, Panda) are still in use, but much less and without any significant upgrades. It can be said that they are becoming obsolete.

The groups using the Dridex, Trickbot and Gozi Trojans still pose the most serious threats for banks.

Russia

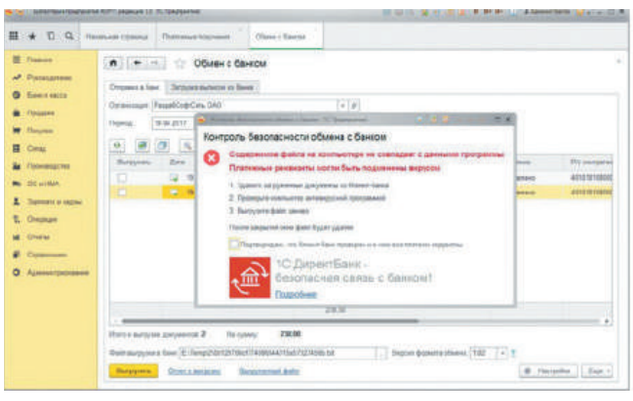
In Russia, the trend aimed at reducing threats from baning Trojans for PCs has been continuing since 2012. Within the reporting period, the damage decreased by another 12% to $8,3 mln. As in the last year, there have been no new banking Trojans for PC. In addition, there are no longer any groups left in Russia that would conduct thefts from individuals in Russia using banking Trojans for PCs.

At present, only three criminal groups — Buhtrap2, RTM, Toplel — steal money from the accounts of legal entities in Russia. However, none of them uses the «man-in-the-browser» (MitB) attack.

Buhtrap2

The Buhtrap botnet has been sold and used by other criminals since 2016. The Drive-by download method remained the main form of distribution in the first half of 2017: criminals hacked legitimate financial websites (e.g. www.glavbukh.ru), that run JavaScript, and then exploited the vulnerability in the browser.

As a result of the attack, the PowerShell script, which loads and activates the Buhtrap loader, was enabled. In the second half of 2017, the attackers changed their tactics: they started distributing Trojans not through traditional mailing and hacked popular websites, but through new thematic resources where the attackers placed code that downloaded Trojans.



As a result of the attack, the PowerShell script, which loads and activates the Buhtrap loader, was enabled. In the second half of 2017, the attackers changed their tactics: the vector for the distribution of Trojans was no longer the traditional malicious campaigns or hacked popular sites, but the creation of new thematic resources, where the criminals placed code that was designed to download the Trojans.

The owners of this botnet used automatic transfers through 1C accounting systems extensively.

After 1C developers ensured the protection against this type of attack, by adding the verification of payment details replacement, the hackers changed their code. The new Buhtrap can bypass the protection of “1C: Enterprise“ “Bank exchange security control“ by hiding the displayed alert.

RTM

The RTM banking Trojan began operating in 2016. That year, we observed that the loader from the leaked Buhtrap source code was used for distributing the RTM Trojan. This connection often confuses information security experts when it comes to attribution.

As with Buhtrap2, the main methods of stealing are a remote control or automated transfers through 1C accounting systems. However, we observed no attacks that would bypass the “1C: Enterprise” protection from automated replacement of banking details, as with Buhtrap.

Toplel

The Toplel hacker group was discovered by Group-IB experts in February 2015.

This group has been active since at least August 2014 and has been using domain names registered in the .SU zone.

At the time, the attackers used the RDPdoor Trojan (aka xTerm) to conduct attacks. This program grants remote access to the computer, which allows the attacker to make transactions from the user’s work station when it is connected to a token with an electronic signature, which is required to confirm the transaction. The program was distributed predominantly through e-mails with malicious attachments.

The criminals mainly focused on clients of banks in Russia and Ukraine. The modules of the RDPdoor Trojan targeted the following Internet banking systems: Ibank, bifit, Promsvyaz, Alfabank, Diasoft, Sberbank, Komita, Tiny, Fobos, ClntW32, cbsmain, BCClient, Tival, cbs, Severgazbank, Ibc, Interbank, RS.

Aside from the RDPdoor Trojan, criminals used a modified version of the Pony malware, which is able to collect logins and passwords on systems not related to Internet banking.

CASE: BACKSWAP

New methods of automatic payment details replacement

BackSwap is one the most interesting of the new Trojans. It originally only targeted banks in Poland, but then began to attack Spanish banks as well. BackSwap is interesting because it combines several new web injection techniques that are used to automatically replace payment details.

The injected code replaces the original transaction recipient, and to cause less suspicion, it shows the victim a fake input field with the intended recipient.

Developer Console

In the old versions, BackSwap injected a malicious script into the clipboard and simulated a keystroke combination to access the developer console (CTRL + SHIFT + J in Google Chrome, CTRL + SHIFT + K in Mozilla Firefox). Then it inserted the contents of the clipboard (CTRL + V) and “pressed“ ENTER to execute the contents of the console. To close the console, it repeated the keystroke combination. Meanwhile, the browser window becomes invisible — an ordinary user will most likely think that the browser has just frozen for a few seconds.

JavaScript in the address bar

In the new versions of the Trojan, the scheme was improved. Instead of interacting with the developer console, a malicious script is executed directly from the address bar through a special JavaScript protocol—a rarely used function supported by most browsers. The program simulates pressing CTRL + L to select the address bar, DELETE — to clear the field, «inserts» characters into JavaScript via calling SendMessageA in a loop, and then inserts a malicious script using the CTRL + V combination. The script is executed after pressing ENTER. At the end of the process, the address line is cleared to remove the traces.

Bookmarklet

The Trojan creates a bookmark in the browser, but instead of the URL, JavaScript software is added, which allows the attackers to perform auto-replacement of payment details when visiting bank websites. Bookmarklets do not usually return values and are simply executed by the browser, having access to the page opened in it. That said, they can do the same as the script placed directly on the page can.

Landscape of PC banking Trojans

	MnuBot New	BackSwap New	IcedID New	Osiris New	Xbot New	DanaBot New	Quakbot (Qbot)	Gozi (ISFB, Ursnif)	Trickbot	TinyNuke (aka NukeBot)	Gootkit	Dridex	Ramnit	ZeusVM (KINS)	Atmos	Zeus	Retefe	Corebot	UrlZone Banker	Panda Banker	Total
Australia						●		●	●		●	●		●	●	●					8
Austria																	●				1
Argentina									●											●	2
Belgium									●				●	●		●					4
Bulgaria								●							●						2
Brazil	●																				1
United Kingdom			●								●	●	●	●	●	●	●				8
Germany									●				●	●	●	●					5
Spain		●					●		●					●	●	●					6
Italy								●						●	●	●			●		5
Canada			●				●		●				●	●				●		●	7
Colombia																				●	1
Korea								●													1
Netherlands							●														1
Norway									●												1
Peru									●												1
Poland		●																	●		2
USA			●				●	●	●			●	●	●	●	●			●	●	11
Turkey															●	●					2
France									●	●		●	●		●				●		6
Switzerland																	●				1
Sweden																	●				1
Ecuador																				●	1
South Africa														●	●						2
Japan								●									●		●	●	4

ANDROID TROJANS

After several years of growth, the Android Trojans market in Russia has leveled off, but it continues to gain momentum on the world stage. The five most common theft schemes described in the 2016 report remained the same:

- Theft via SMS banking
- Card to card transfers
- Online bank transfers
- Compromise access to mobile banking
- Fake mobile banking

Landscape of Android banking Trojans

TROJANS TARGETING SMS BANKNG (RUSSIA ONLY)	TROJANS USING WEB FAKES IN RUSSIA	TROJANS USING WEB FAKES GLOBALLY
Agent.SX	Limebot (Lipton)	Easy
Flexnet	Asucub	Exobot 2.0
Granzy	Agent.BID	CryEye
Agent.BID	TarkBot	Cannabis
	Bans in your hand	Fmif
		AndyBot
		Loki v2
		Nero banker
		Sagawa
		Agent.cj
		Maza-in
		Loki v2
		Alien-bot
		Rello
		Red Alert v2

World

The new Android Trojans sold on hacker forums are focused primarily on use outside of Russia: Easy, Exobot 2.0, Asacub, CryEye, Cannabis, fmif, AndyBot, Loki v2, Nero banker, Sagawa. The only exception is Asacub.

After the publication of the source code for the Maza-in Trojan, many of its clones emerged and they are still in use. In July 2017, another author of the banking Trojan for Android Loki Bot also made source code available for the public.

The Agent.cj Trojan is used locally and targets users of Turkish banks.

Typically, Android banking Trojans propagate using SMS/MMS messages. However, in early 2018, the Exobot 2.0 Trojan was distributed via applications that had previously been downloaded from the official Google Play market. In May 2018, after its author sold the project, the source code of ExoBot 2.0 was leaked online.

A hacker nicknamed GanjaMan is a very active Russian-speaking developer of Android banking Trojans. He developed the well-known Gmbot (aka Mazar), Skunk, and VBV Grabber. These Trojans are no longer in use, and their author is banned on major underground forums. However, before being blocked, he managed to sell the source code for his new Trojan Cannabis.

Trojans that were active in the last period are no longer used, probably because of the poor support from the developers. These Trojans include Xbot, Abrvall, Vasya, UfoBot and Reich.

CASE: BANKS IN YOUR HAND

Distribution of Android Trojan via Google Play

The criminals created a new large botnet using a malware disguised as a financial application — “Banks in your hand“, acting as an “aggregator“ of mobile banking systems of the country’s leading banks. Customers could link all their cards to the app, see their card balance with an SMS detailing all transactions, transfer money from card to card, and pay for online services and purchases in online stores. The software was distributed through spam emails, on forums and through Google Play.

In May 2018, one of the participants in this scheme was detained. The criminal transferred money to bank accounts in amounts of $180 to $450 per transfer by entering the SMS confirmation code of the operation intercepted from the victim’s phone.

In Russia

The activity of Android Trojans fell sharply following the arrest of the owners of the largest Android botnets — Cron and Tiny.z — in Russia in 2017. In addition, the owner of another large botnet Honli stopped using this Trojan.

As a result, the number of daily thefts dropped almost threefold. It is also worth mentioning the decrease in the average number of thefts using Android Trojans. Last year, the average theft amount was $150; this year, the figure dropped to $100.

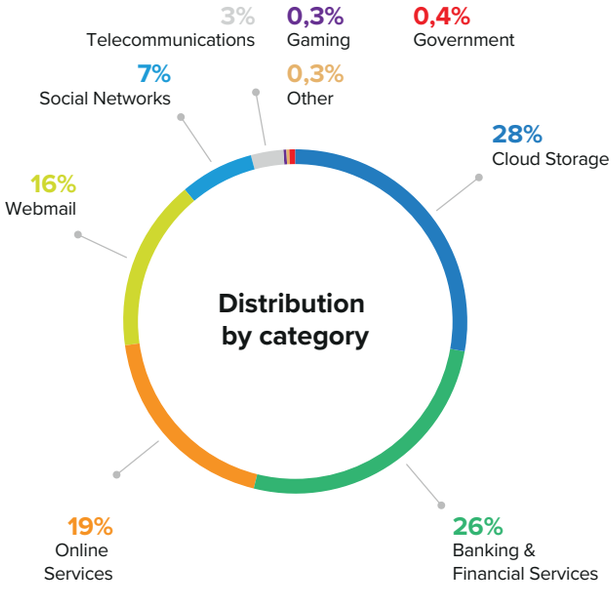
Asacub, which is a private Trojan, was the most active botnet in the last year. However, in August 2017, someone posted an offer to sell the fork of this malware, although the topic was closed in September. The second most active botnet Agent.BID has been idle for a long time, and its owners only resumed activities at the beginning of 2018.

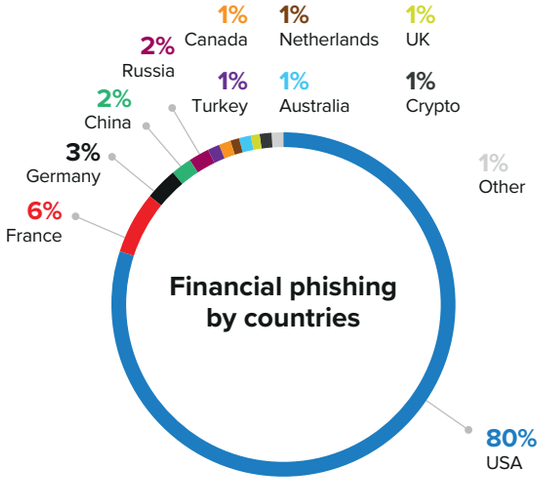
WEB PHISHING ATTACKS

World

Over the last period, GIB Threat Intelligence has identified and analysed 2,6 million unique phishing URLs on 727 thousand domains, which is nine per cent more than last year. Most phishing-hosting websites (46%) were located in the .com first-level domain, while .org, .mx and .net each held only three per cent of such websites. As it always has been, most of phishing webpages (63%) was hosted in the US. The majority of phishing resources are hosted on legal websites that have been hacked.

The leading phishing groups focused on cloud storages and not on the financial. Dropbox suddenly became the most popular among the phishers, even though we previously observed Google services to be of highest interest for the attackers. Currently, 73% of all phishing resources are made up of three categories: cloud storage (28%), financial sector (26%), and online services (19%).





The financial phishing is, predictably, mainly targeting US-based companies. The corresponding share of financial phishing webpages is 80%. France ranks second, Germany third. Various cryptocurrency projects each have 1%.

Phishers specializing in massive cyber attacks use so-called phishing kits — fully fledged phishing websites containing a configuration file that defines the site's algorithms and specifies the recipient for the compromised data. Over the last period, the GIB Threat Intelligence system has collected over 18,000 unique phishing kits and analysed their configuration files. The overwhelming majority of such tools send the compromised data to an email address. In 84% of cases phishers create a Gmail account to gather stolen data, while the Russian services Yandex and Mail.ru were only used in 4% of cases.

Phishing kit

– fully fledged phishing websites containing a configuration file that defines the site's algorithms and specifies the recipient for the compromised data

In Russia

Web phishing is the only data theft method that exhibited growth in Russia this year. The number of groups creating phishing websites that masquerade as Russian brands has grown from 15 to 26. In Russia, the phishing for data pertaining to banks and payment systems is automated and performed in real time, thus allowing the attackers to bypass SMS confirmation of transactions. The simplicity of fraudulent schemes and a wide range of tools attract new players to the phishing market.

Using web phishing, criminals have managed to steal $3,7 million (251 million rubles) this years, which is 6% more than in the previous period. On average, approximately $15 (1000 rubles) are stolen in each phishing attack. The number of successful attacks per day increased slightly to 1274, while the average number of victims per collective even decreased from 63 to 42. The main driver curbing the growth of the number of attacks is the phishing sites are actively identified and shut down, in part thanks to rapid data exchange between banks and the Bank of Russia's Financial Sector Computer Emergency Response Team (FinCERT).

Redirecting users from compromised websites and getting the phishing website to appear in search results remain the main methods to attract users to phishing pages. Russian phishers, unlike those operating in most other countries, usually register a dedicated domain name for most of the phishing websites. Phishing targeting card-to-card transfers has gained momentum; in some cases, the attackers brand phishing pages to look like a particular legitimate bank's website, however "generic" — unbranded — phishing is also occures.

CARDING

The carders can be categorized into two major segments: those selling card details (card number, expiration date, holder's name, address, CVV) and those selling the so-called "dumps" (unauthorized copy of all the information contained in the magnetic stripe of an active card). Card details collected using phishing websites, PC and Android banking, ATMs, as well as by hacking e-commerce websites. Dumps are obtained by using skimming devices and also through Trojans infecting workstations connected to POS terminals.

The large part of compromised card data is sold in specialized cardshops. GIB Threat Intelligence continuously detects and analyses data uploaded to cardshops. On average, 686 thousand sets of card details and 1,1 million dumps are uploaded to such shops monthly. Our records indicate that dumps account for 62% of total sets of card data sold, which means that POS threats represent the major method of compromising credit cards.

Aside from quantitative indicators, we also detect the price of each dump, which allows us to measure the carding market as a whole. Card details are sold much cheaper in cardshops: its total value amounted to only $95,6 million, accounting for only 17% of the overall market value, compared to 19,9 million dumps which cost as much as $567,8 million.

Carding market overview

H2 2017 — H1 2018, Group-IB

	Card details	Dumps	Total
Total amount	10 218 489	16 927 777	27 146 266
Market size	$95 590 424	$567 791 443	$663 381 867
Min price	$0.75	$0.5	
Max price	$99.99	$295	
Average price	$9.35	$33.54	
Median price	$8	$25	

POS threats

Credit card dumps are mainly obtained by infecting computers connected to POS terminals with POS Trojans. The operating principle of POS trjoans remains unchanged: they retrieve card data from RAM as the card is being read by a POS terminal.

Attackers can be categorized in two groups:

- Those who carry out random mass attacks aimed at installing a POS trojan wherever possible.
- Specialized in targeted attacks on POS terminal vendors or large chain organizations, so that network access makes it possible to infect a great number of devices at once.

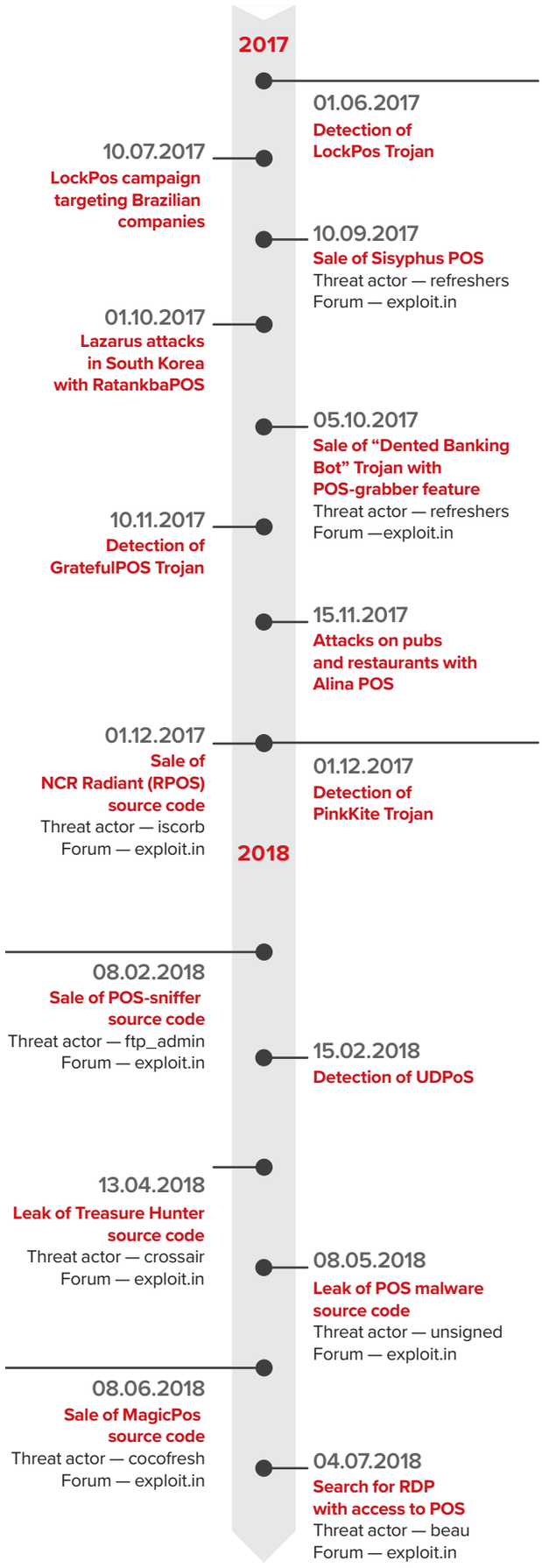
The carding industry suffered a hard blow in early 2018 when the U.S. Department of Justice announced the arrest of three Ukrainian citizens who were members of FIN7 (aka Navigator) hacking group. According to the federal indictments, Dmytro Fedorov (Hotdima), Fedir Hladyr (Das or AronaXus) and Andrii Kolpakov (Santisimo) were detained in January and March 2018. According to the Ministry of Justice statement, since 2015, FIN7 has attacked over a hundred U.S. companies and organizations and hacked thousands of systems. It is reported that the hackers stole over 15 million customer credit records from over 6,500 POS terminals in the U.S. alone.

However, POS threats are a dynamic market. Group-IB experts detect new Trojans coming out every year and source codes proven in real attacks sold and published.

POS Trojans source codes sales and publication

05 October 2017 The sale of source code for Dented banking bot was published for sale on an underground forum. This trojan collects banking card TRACK1 and TRACK2. The bot was set to be sold to three clients for $3,000 paid in bitcoin.

08 February 2018 User ftp_admin decided to sell the source code for his POS Sniffer trojan for $5,000. The trojan has been designed as system drivers for Windows x32 and has been on sale since March 2016.



08 June 2018 User cocofresh created a topic to sell MagicPos trojan with admin panel. The price was set at $350.

08 May 2018 User Unsigned char published a link to download the source code for a POS trojan to retrieve Track1 and Track2.

06 April 2018 User crossair published an archive containing source code for Treasure Hunter on an underground forum. This trojan malware has been known since as early as 2014. Trhutt34C.rar archive contains two files: adminPanel.rar and cSources.rar — the source code for the admin panel and Treasure Hunter malware itself.

New POS Trojans

June 2017 An attack campaign against Brazilian companies was registered. The attackers were using LockPos, which has been linked to FlokiBot group.

September 2017 User Refreshers published a topic to sell a new POS trojan, SisyphusPOS.

October 2017 Proofpoint experts found that Lazarus group is using a new POS trojan, RatankbaPOS, for their attacks in South Korea.

November 2017 RSA experts identified a new POS trojan, GratefulPOS. Its code comprises fragments of multiple malware families: FrameworkPOS, TRINITY, BlackPOS and BrickPOS. Similarly to FrameworkPOS, the new malware retrieves card data from terminal RAM and sends it to the control server in the form of encrypted DNS requests

December 2017 Kroll Cyber Security researchers identified another POS trojan, PinkKite. PinkKite takes up only 6 kB and contains RAM scraping and data validation modules. In this campaign, a separate RDP session was required to send the card data manually to one of the three PinkKite data exchange centres.

February 2018 Forcepoint researchers found a trojan, UDPoS, impersonating LogMeIn, a legitimate remote access system, that sent credit card data via DNS requests.

ATM threats

Some hacking groups are unable to compromise a bank's network and infect its ATM network. However, they are capable of infecting individual ATMs through physical access. In the past reporting period, there were two active threats in the banking sector: Cutlet and Ploutus-D.

The general scheme of a jackpotting attack involves three types of criminals:

- organizer / client
- software developer
- drops.

The organizer is the leader of the attack. Most often, this is also the person who has commissioned the ATM software development.

Their goal is financial gain at minimum risk. To start the attack, a full set of tools is required, and there are two ways to obtain them: order it from developers or purchase from other criminals. Once the tools are in place, the organizer finds a drop team of at least two people, who are to ensure physical access to an ATM's internal systems. A special key generator ensures that the drops do not trick the organizer and become independent. Once the malware is installed on the ATM, an activation key is required to continue. The key generator is held by the organizer.

To break into the ATM, criminals drill, burn or cut holes of approximately 5 cm in diameter in the ATM keyboard to gain direct access to the ATM wiring.

Once they have physical access, the criminals disconnect the cash dispenser from the USB hub or COM port (depending on the ATM type) and install a blocking device that imitates dispenser operation. Then they connect a low-energy microcomputer to the USB /COM port of the cash dispenser.

The drops use the phones to communicate with the organizer and get activation keys.

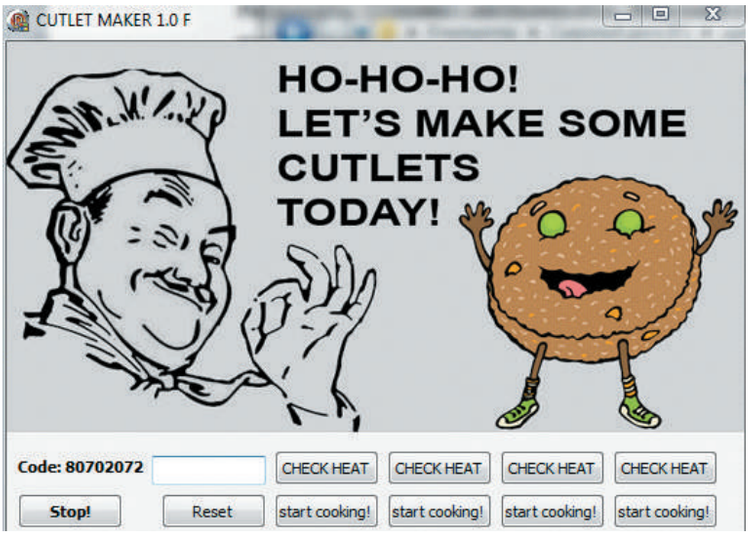
On average, the whole operation takes up approximately 8 minutes. Once the cash has been dispensed, criminals disguise the hole with a sticker.

Cutlet

In mid-2017, a new toolkit for the attacks on ATMs with a new malware called Cutlet came out. The toolkit contained very detailed user guidelines and recommendations on how to avoid problems. Later, Cutlet got its own Android app, which allowed criminals to use a smartphone instead of a laptop.

The Cutlet toolkit is still very popular, and you can buy it on various forums.

06 Dec 2017 User ‘cutlet master’ published an offer to sell the full Cutlet Maker software set at crdclub.ws. The price was stated at $1,000.



The toolkit contained three elements:

- Stimulator22, designed to estimate the current status of ATM cash cassettes
- c0decalc, designed to generate an activation key to run Cutlet Maker
- Cutlet Maker 1.0 F, designed to withdraw cash from an ATM.

15 Dec 2017 User 'md5' published a sales offer of the full Cutlet Maker toolkit at ifud.ws. The price was originally stated at $800, but went down to $500 on December 23. It is worth noting that the very first cutlet toolkit was sold for $5,000.

17 Jan 2018 User 'she0' offered to sell the full Cutlet Maker toolkit at moneymaker.hk. The price was stated at $760 (50000 rubles).

20 Dec 2017 A free download of the toolkit was announced on exploit.in, the most popular Russian-language underground forum. User 'Onions' offered to share the software with the first three long-time forum users who would ask for it.

20 Dec 2017 User 'vulns' published a link to download Cutlet at migalki.pw. The archive contained two files: cm17F (Cutlet Maker 1.7 F), Stimulator22.

28 May 2018 User 'sl111' announced the sale of Cutlet v2, a new ATM trojan malware. The announcement was published at exploit.in. Cutlet v2 was designed for Wincor ATMs. According to the forum post, Cutlet v2 had the same functionality as Cutlet Maker. The new version didn't require password generation, for which c0decalc.exe had been previously used. The author of the post, claiming to be the original developer of the malware, was selling the trojan along with its source code. The trojan is in C/C++. The price for Cutlet v2 has been stated at $5,000. The kit includes the trojan malware, source code, software documentation, and user manual.

Ploutus-D

On January 25, 2018, Diebold Nixdorf published a report titled Potential Jackpotting US, which states that the U.S. government has warned the company that possible jackpotting attacks on ATMs manufactured by the company have been registered. Earlier, in October 2017, a similar attack was detected in Mexico. Media sources have also reported possible attacks on NCR Corp ATMs.

The criminals presumably used Ploutus-D malware.

Ploutus-D is a new modification of Ploutus, malware designed to withdraw cash from ATMs. It was first detected in Mexico in 2013. At the time, it was distributed on CD-ROM. First mentions of Ploutus-D on underground forums date back to the beginning of 2017. However, there is not a single positive review of the software's implementation or verification. In addition, all sales topics were started by vendors having bad reputation. So far, no active sales at underground forums were spotted.

Ploutus is not unique: there are several similar attack schemes throughout the world. Most often, the minor differences between them are due to the specific ATM type popular in the area of the attack.

6. THREATS TO BLOCKCHAIN AND CRYPTOCURRENCY PROJECTS

Trojans for stealing private keys, mass phishing attacks, miners, tools for password cracking, website defacement, domain hijacking, and various cryptocurrency-related fraud have already become part of everyday life. However, threat landscape for the cryptocurrency market is ever-changing: this year has witnessed entirely new schemes for cryptocurrency theft and cryptocurrency exchanges hacks, as well as new modifications of schemes typical for financial sector.

ATTACKS ON BLOCKCHAIN PROJECTS

In 2018, attacks on blockchain projects fell into the following categories:

Blockchain attack

These are attacks using specific aspects of the blockchain technology itself, e.g. the so called “51% attack“ or double spend attack.

Credentials reuse

Hackers obtain old users’ passwords from various services and test if it works for the user’s cryptocurrency wallet.

Domain hijacking

These are cases of domain registration data alteration. For example, hackers can alter A records and redirect a website’s traffic to a malicious server to collect data (user login and password) or transfer money.

Insider work

Someone of the project team uses their access to data systems for cryptocurrency theft.

Malware

These are cases where specially developed malware is used to steal confidential information. Malware is not only used to steal private keys or user passwords, but also to gain access to workstations of systems administrators and to create backdoors into the cryptocurrency exchange infrastructure.

Phishing

An identical copy of a website in a different domain or fake emails or messages purporting to be from project tram may be used to steal confidential information or upload malware to the victim’s PC.

Source code vulnerability exploitation

Hackers may use logical errors or other company software vulnerabilities.

CRYPTOCURRENCY RATE MANIPULATION

Cryptocurrency market manipulation schemes are numerous. For example, Pump&Dump (P&D) schemes, where traders come together to form a group of up to several thousand members on Telegram or Discord. They pick a cryptocurrency without value or prospects (the so called 'shitcoins') and start simultaneously buying it, thus attempting to achieve an artificial rate increase. This is the 'pump' phase, followed by the 'dump' phase, when all participants of the scheme begin selling.

Most fraud schemes and tools used to steal cryptocurrency are similar to those used by the carding industry, personal data theft, etc. In 2016, we published a report on a bank hack carried out by Corkow group. By using its broker accounts, they influenced ruble exchange rate. A similar fraud scheme involving cryptocurrency was carried out by unidentified hackers in early 2018. The attack took over two months to prepare.

The attackers used the following tactics:

1. In January 2018, an unidentified hacking group registered a phishing domain corresponding to that of Binance, China's largest cryptocurrency exchange.
2. Links to the phishing website were sent to traders from the targeted exchange in order to obtain their user login and password data.
3. Having collected user login and password data, the attackers were able to create API keys to automate interaction with the exchange.
4. For two minutes on March 7, 2018, the attackers used the previously generated API keys of the compromised traders to place purchase bids for a little known cryptocurrency called Viacoin.
5. As a result, in 30 minutes, Viacoin rate went up by 143%, from $2.80 to $6.79, according to coinmarketcap.com.
6. After the dramatic increase in Viacoin rate, the attackers began selling it for Bitcoin from 31 accounts created in advance.
7. After the trading was over, withdrawal requests were sent.

However, according to posts on Bitcointalk, many user transactions were terminated and tokens were returned to users. Therefore, at present, it is impossible to assess total damage and trace the transactions within one cryptocurrency exchange.

ICO ATTACKS

In 2018, the ICO projects were fewer in number; however, they were better prepared for cyber attacks. The amounts of funds invested in the projects went significantly up, attracting criminal attention. In 2017, over $400 million was stolen from ICO projects. In H1 of 2018 alone, ICO projects raised almost $14 billion, which is twice as much as in the whole of 2017 ($5,5 billion).

In 2018, hackers attacked ICOs conducting private funding rounds. For instance, cybercriminals targeted TON project, founded by Pavel Durov, suffered a phishing attack resulting in fraudsters leaving with $35,000 in Ethereum.

The worst generally happens on the first day of token sales: a set of DDoS attacks simultaneous with an influx of users, the eruption of Telegram and Slack messages, mailing list spamming.

Phishing

Approximately 56% of total funds stolen from ICO were lost as a result of phishing attacks. On the rise of 'the cryptocurrency fever', everyone is striving to purchase tokens, often sold at a significant discount, as fast as possible and fails to pay attention to minor detail such as fake domain names.

A phishing attack on ICO does not require either thorough preparation or high professional competence on the part of the attackers.

The attack scheme has remained unaltered from 2016

- Attackers watch for new ICO projects.
- They create a phishing website with a domain name similar to the legitimate one. The main difference is a request to enter a private key or transfer cryptocurrency to a fraudster's wallet or smart contract.

- A DDoS attack on the legitimate website is launched to prevent access and encourage investors to move on to the phishing website.
- At the same time as the DDoS attack, spam messages containing a link to the phishing website are sent out.
- In addition, fraudsters purchase contextual ads in search engines, create an influx of messages in chat apps, and use every possible way to increase traffic to the phishing site, so that it appears at the top of the search results.

If an ICO project website is vulnerable, the tactics are slightly different. Instead of creating a phishing website, hackers replace the link to the wallet or smart contact with their own shortly before the start of the ICO.

Phishing attacks against ICO projects are not always aimed at stealing money. This year, there were several cases of investor database theft. This information can be later re-sold at underground hacker forum or used for blackmail.

Project theft

ICO projects are known for their full transparency and openness. Most of the developments and source codes are in open access. First and foremost, the team publishes their White Paper. The general fraud scheme is quite simple:

- Fraudsters look for a new and not yet popular project with a detailed and thorough description.
- The project description is copied in full and translated into several languages.
- Fraudsterd build a website to feature a new brand an a new team using the stolen description.
- To attract investor attention, the new project brand is actively advertised through context ads, discussion posts on specialized forum.

TARGETED ATTACKS ON CRYPTOCURRENCY EXCHANGES

In the last report, we mentioned that hackers capable of organising a professional targeted attack and stealing millions of dollars had turned they attention to cryptocurrency exchanges. In 2016 they attacked Bitfinex, Shapeshit, Gatecoin, and Bitcurex.

In 2017 and 2018, hackers' interest in cryptocurrency exchanges ramped up. A total of 13 cryptocurrency exchanges were hacked in 2017 and in the first three quarters of 2018. At least five attacks have been linked to North Korean hackers from the state-sponsored group Lazarus.

In total in 2017 and three quarters of 2018, cryptocurrency exchanges suffered a total loss of $877 million in cryptocurrency due to targeted attacks. 60% of the total amount was stolen from the Japanese exchange Coincheck.

Spear phishing remains the major vector of attack on corporate networks. For instance, fraudsters deliver malware under the cover of CV and other spam : they send an email containing a fake CV with the subject line "Engineering Manager for Crypto Currency job" or the file "Investment Proposal.doc" in attachment, that has a malware embedded in the document. If the malicious files are opened, a program called RAT developed and regularly upgraded by the Lazarus hacker group is installed on the victim's computer. After that, the the hackers browse the local network to find work stations and servers working with private cryptocurrency wallets.

Date*	Target	Country	Criminal group	Stolen in cryptocurrency	Stolen in USD
Feb 2017	Bithumb	South Korea	Unknown	-	$7 mln
Apr 2017	YouBit	South Korea	Unknown	-	$5,6 mln
Apr 2017	Yapizon (YouBit)	South Korea	Lazarus	3,816 BTC	$5,3 mln
Aug 2017	Ether Delta	-	Unknown	-	$266 k
Aug 2017	OKEx	Hong Kong	Unknown	-	$3 mln
Sep 2017	Coinis	South Korea	Lazarus	-	-
Dec 2017	YouBit	South Korea	Lazarus	17% of assets	-
Jan 2018	Coincheck	Japan	Lazarus	523,000,000 NEM	$534 mln
Feb 2018	Bitgrail	Italy	Uknown	17,000,000 NANO	$170 mln
Jun 2018	Bithumb	South Korea	Lazarus	-	$32 mln
Jun 2018	Coinrail	South Korea	Uknown	11 types of cryptocurrency	$37 mln
Jun 2018	Bancor	–	Uknown	-	$23 mln
Sep 2018	Zaif	Japan	Uknown	-	$60 mln
				Total	**$877 mln**

* The data provided in the table was revised on Oct. 22, 2018.

CRYPTOJACKING (HIDDEN MINING)

Cryptojacking is a relatively new type of fraud that developed most in 2017-2018. Specialized malware makes it possible to use computing devices to mine cryptocurrency, unknown to their owners. Hidden mining software is spread over thousands of computers forming a botnet.

The amount of cryptocurrency obtained through mining depends directly on the botnet's total processing power. Therefore, the computing power of corporate networks is of much greater interest to criminals than personal computers. For example, EternalBlue Exploit (CVE-2017-0144) may be used for mass malware distribution. A similar vulnerability was used to distribute WannaCry ransomware in May 2017 and Petya in June 2017. With the help of Smominru Trojan distributed through EternalBlue Exploit, botnet operators mined approximately 8,900 Monero ($2,8-3,6 million). The botnet mined roughly 24 Monero daily, which, at the time, was equivalent to $8,500.

Coinhive, launched in September 2017, was one of the first successful attempts of browser mining software development, followed by Crypto-Loot, JSEcoin, Minr, CoinImp, ProjectPoi (PPoi), AFMiner, Papoto. These projects provided an API that allowed website owners to use the computing power of website users' devices to mine cryptocurrency. This model immediately caught the attention of many hackers with knowledge of processing illegal web traffic.

Websites can be compromised in order to install mining malware in a number of ways:

Websites hacking

Websites can be hacked many ways: password cracking, CMS or other software vulnerability, password collection by malware or phishing websites. As mining is carried out on the user's device and only while the hacked website is open, the success of the fraud depends not on the number of sites hacked, but on the size of their audience. Therefore, just as was with Drive-by download trojan distribution, websites with larger audiences are being hacked intentionally.

Browser extensions

In 2017, the Google Chrome extension Active Poster was launched. According to estimates, hidden mining involved over a hundred thousand users. After several complaints to the support service, the extension was removed. Similar extensions were found in Mozilla Firefox.

Third party services

Many websites use third-party JavaScript libraries. These are generally advertising networks, analytical, or tracking services. Scripts for such solutions may contain mining functionality on purpose or as a result of compromise, as it happened with Coinhive scripts on YouTube.

Man-in-the-Middle attack

User traffic is redirected via intermediary nodes that often have access to content. For example, fraudsters can intercept unprotected traffic at public Wi-Fi access points and install cryptojacking scripts. Attacks of this kind have already been carried out against a Starbucks network in Argentina.

Botnets of home routers, such as Mirai or similar, are indispensable for this kind of attack. Once a home router is infected, it becomes possible to manipulate traffic of all its users. In one of the latest attacks, the attacker was able to find a zero-day vulnerability in a MikroTik router and use it to infect approximately 200,000 devices, forcing them to install Coinhive mining script into the viewed websites.

51% ATTACK

This attack, for which control over 51% of the network mining power is required, can be either carried out by one miner with a large number of computers or a group of miners forming a mining pool. Control over 51% of the network power itself is not necessarily an attack — unless there has been intentional use of this advantage.

An attacker controlling 51% of the network power can

- freeze the system,
- stop transaction verification,
- suspend mining,
- prevent other miners from verifying transactions,
- double spending.

Double spending is currently believed to be the greatest system threat. Attackers can create a hidden alternative blockchain and use it to verify their own transactions. It is possible to double spend even without controlling this much network power. However, control over 51% is an absolute guarantee that the fraudster's block is recognized as correct.

51% attacks have been known for some time. For example, in 2016, Krypton and Shift Projects suffered such an attack. During the same year, the Chinese entrepreneur Chandler Guo announced his intention to carry out a 51% attack on Ethereum Classic in cooperation with other miners.

While no successful attacks of these type were carried out in 2017, in 2018, the cryptocurrency industry witnessed as many as five successful 51% attacks:

- **April 4** The Verge network suffered a 51% attack made possible due to a bug in the code. The attack lasted approximately three hours, and, according to some estimates, the attacker was capable of obtaining over $1 million worth of cryptocurrency.

- **May 18** Edward Iskra, Director of Communications for Bitcoin Gold, warned about an attack and made it known that a miner captured at least 51% of the network's hashrate. From May 16, over 388 000 coins were transferred to the attacker's BTG address. The fraudster was capable of stealing over $18 million in total.

- **May 22** The mining pool SuprNova informed that the Verge blockchain was under 51% attack and all correct block were being rejected. According to them, the problem affected for all pools and every miner, as the fraudster was controlling all blocks. Earlier, the project representatives made it known that a DDoS attack on pools was possible and that block verification could be delayed.

- **June 3** ZenCash blockchain suffered a 51% attack resulting in the unknown criminals stealing over $550,000 in ZEN cryptocurrency. They were able to reorganize 38 blocks, while the attack itself lasted less than four hours. According to Crypto51 website dedicated to assessing losses resulting from 51% attacks, it cost the criminals $30,000 to prepare and carry out the attack.

- **June 6** The network of a new Litecoin Cash (LCC) cryptocurrency, a fork of a more well-known Litcoin (LTC), also experienced a 51% attack.

RESTRICTIONS

Group-IB hereby informs that:

- This report has been prepared by Group-IB specialists without funding from third parties.
- Assessment of the hi-tech crime market was made on the basis of proprietary internal methods developed by Group-IB.
- Technical details of cyber threats are described in this report are published only for use by information security staff with a view to prevent similar incidents in the future and to minimize the possible damage.
- Technical details of threats and attacks published in this report do not in any way support or provide advocacy of fraud and/or other illegal activities in hi-tech or other areas.
- All references to companies and trade marks in this report are made on the basis of approvals from such companies and/or on the basis of information already published in mass media.
- Information published in this report can be used by interested parties at their own discretion as long as the reference to Group-IB is given.

ABOUT GROUP-IB

15 YEARS of hands-on experience

55 000+ hours of incident response

1 000+ investigations worldide

Group-IB — is a leading provider of high-fidelity threat intelligence, best-in-class anti-APT and anti-fraud solutions.

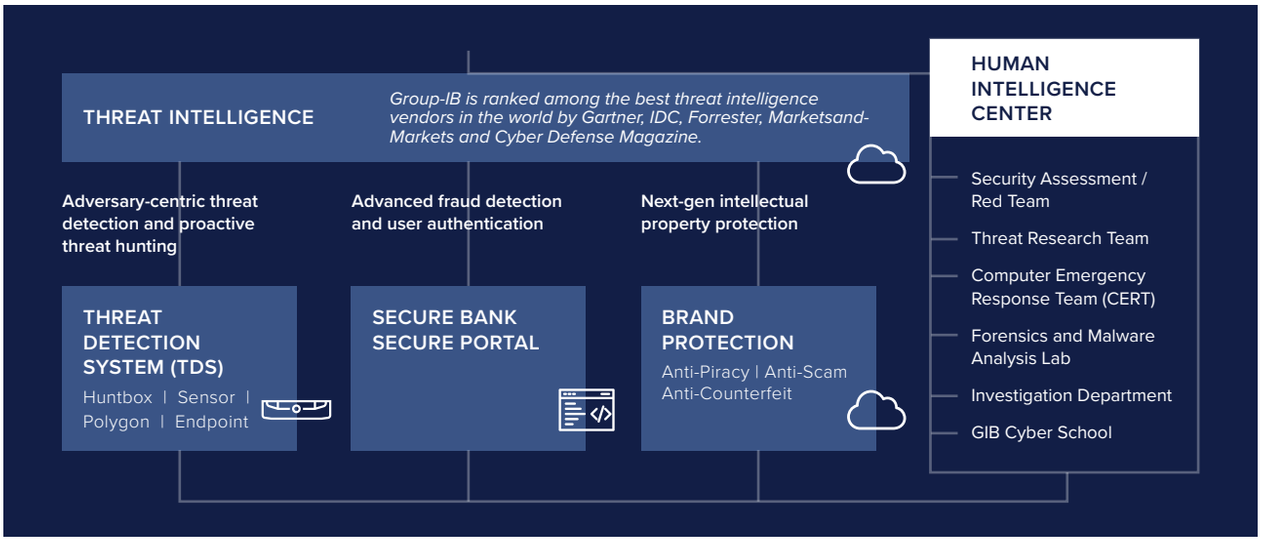
- Interpol and Europol partner
- Cyber security service provider approved by SWIFT and recommended by OSCE

Technologies with detective DNA

We leverage a comprehensive stack of proprietary technologies aimed at automated tracking of malicious activitiies, extraction and analysis of threat data, mapping of adversaries' infrastructure and enrichment of their profiles.

Best-of-breed human intelligence

A team of world-class specialists involved in response and investigation of the most advanced cyber attacks throughout the world relentlessly reinforces our technologies with insights 'from the battlefield'.



Adversary-centric approach

With over 15 years of threat research and analysis, we possess unparalleled expertise and state-of-the-art tools for pattern recognition in adversaries' TTPs.

Not only we accurately detect targeted attacks but also help our clients understand adversaries' modus operandi and keep track of changes in their tactics and infrastructure.

We have provided professional development training to Europol, INTERPOL, law enforcement agencies, corporate security teams and scholars in the UK, Germany, the Netherlands, Belgium, France, Thailand, Bahrain and Lebanon.


GLOBAL CYBER SECURITY COMPANY
GIB
GLOBAL CYBER SECURITY COMPANY

Learn more about Group-IB

group-ib.com

Get in touch

+7 (495) 984 33 64

info@group-ib.com

Follow us

twitter.com/GroupIB_GIB

youtube.com/GroupIB

facebook.com/GroupIB

instagram.com/Group_IB