

# HI-TECH CRIME TRENDS 2019/2020

Cyberwar

Cyberweapons

State-sponsored

2019/2020

Hacking back

Supply Chain

BGP hijacking

DNS hijacking

SWIFT

ATM Switch

SS7-threats

JS-sniffers

5G

# TABLE OF CONTENTS

## INTRODUCTION AND TOP 10 TRENDS

4-7

## KEY FINDINGS AND FORECASTS

8-17

State-sponsored threat groups, cyberweapons, and cyberwars.....	8
Key trends and forecasts by industry.....	10

## NEW PHASE IN CYBERWAR: INTERNET DESTABILIZATION ATTACKS

17-20

DNS hijacking and attacks on domain name registrars.....	18
BGP hijacking and attacks on Internet routing systems.....	19
Attacks on local systems of filtering and blocking traffic.....	20

## EVOLUTION OF STATE-SPONSORED THREAT GROUPS

21-25

Geographical scope of attacks and new groups.....	21
Supply chain attacks.....	24
Hacking back.....	25

**THREATS TO THE TELECOMMUNICATIONS SECTOR**  
**26-30**

Telecom-related targeting .....26  
 5G expansion-related challenges .....28  
 BGP hijacking and SS7 threats .....29

**THREATS TO THE ENERGY SECTOR**  
**30-31**

Energy sector-oriented groups .....31

**TARGETED ATTACKS ON THE FINANCIAL SECTOR**  
**32-42**

Evolution of threat groups and the appearance of a new player .....32  
 Theft through SWIFT .....38  
 Theft through ATM Switch .....39  
 Logical attacks on ATMs .....40  
 Theft through card processing .....41

**NON-TARGETED ATTACKS AND THREATS TO BANKING CUSTOMERS**  
**42-60**

Common carding trends .....42  
 Evolution of POS threats .....42  
 New trend: JS sniffers .....45  
 Web phishing and social engineering .....50  
 ATM Trojans .....53  
 PC Trojans .....55  
 Android Trojans .....57

**ABOUT GROUP-IB** **61**

# INTRODUCTION

## and top 10 trends

---

### END OF AN ERA OF CYBERSPACE STABILITY

Over the past decade, the number and complexity level of cyberattacks carried out by both state-sponsored hacking groups and financially motivated cybercriminals have increased significantly. People, businesses, and government institutions can no longer

be confident in neither the security of cyberspace nor the integrity and security of their data.

The Internet has become our civilization's circulatory system. Yet the freedom of communication and

the global opportunities provided by the Internet are increasingly being threatened. Data leaks and cyberattacks by unfriendly states are part of today's everyday reality.

***The freedom of communication and the global opportunities that the Internet provides are at risk***

---

For more than 16 years, Group-IB experts have been investigating cyber incidents by analyzing the tools and infrastructure used by attackers. Each new cyberattack targeting a company, political party, or critical infrastructure facility gives us the opportunity to see how attack tactics and tools evolve.

As a company, we strongly believe that public organizations and private companies that fight against cybercrime

must exchange data and publish their research. That is why 6 years ago we released the first High-Tech Crime Trends report. Every year, Group-IB's annual report highlights the changes that have occurred over the past year. It is the most comprehensive source of strategic and tactical data on current global cyberthreats. This year's study covers the period H2 2018 – H1 2019 as compared to H2 2017 – H1 2018.

[By using unique tools for monitoring the infrastructure of cybercriminals](#) and studying the findings published by other security teams worldwide, we find and confirm common patterns that form an integral picture of the evolving cyberthreat landscape. On this basis, we formulate forecasts that come true every year.

***Group-IB's report: a single comprehensive source of strategic data on cyberthreats and reliable forecasts of their development***

---

The leading and most frightening trend of 2019 was the use of cyberweapons in military operations. Conflicts between states have taken on new forms, and cyber activity plays a leading role

in this destructive dialogue. Attacks on critical infrastructure and targeted destabilization of the Internet in certain countries are breaking new ground on cyberattacks. A peaceful existence

is no longer possible while being out of touch with cybersecurity. The latter cannot be ignored by any state, corporation, or individual.

***Targeted destabilization of the Internet heralds a new era of cyberattacks***

---

Group-IB supports the initiatives of The Global Commission on the Stability of Cyberspace (GCSC), created to provide recommendations for promoting cyber stability in the world.



# TOP 10 TRENDS

## Military operations conducted using cyberweapons

### 3 military operations

were conducted in the first half of 2019 when cyberweapons were involved

In the first half of 2019, three open military operations became known: in March, a successful attack on a Venezuelan hydroelectric plant caused a massive blackout that left much of the country in the dark for several days; in May, in response to a cyberattack, Israel's military retaliated with an airstrike against a building known to be the cyber HQ for Hamas; and in June, a cyberattack was conducted on Iranian computer systems that controlled its rocket and missile launchers in response to Iran's downing of a US drone. The attack tools involved in all the above cases have not been identified, and in the latter case, a cyberattack occurred just a few days after the drone incident. This confirms the assumption that critical infrastructures of many countries have been compromised and that attackers go unnoticed until it is too late.

## Internet destabilization at the state level

### All levels

of communications infrastructure can be compromised

Newadays, the most social and economic damage can be caused by depriving people and businesses of Internet access. That being said, countries that build centralized access control to the Internet are becoming more vulnerable and may become the first targets.

In recent years, treat actors have tested attacks on various levels of the communications infrastructure. By the end of 2019, researchers had detected successful attacks on Internet routing systems and BGP hijacks, attacks on DNS root server administrators, national domain administrators and domain name registrars as well as DNS hijacks, and attacks on local systems of filtering and blocking traffic.

## 5G expansion-related challenges

### The development of 5G networks

will create new threats

Shifting to 5G networks will further deteriorate the situation in the telecommunications sector. One of the reasons is that 5G architecture paves the way for new types of attacks on operators. Another reason is that competition for a new market may lead to hacking capabilities being demonstrated against certain vendors and result in countless anonymous investigations into the vulnerabilities of some technological solutions.

## Hidden threats linked to state-sponsored groups

### 38 state-sponsored groups

were active throughout the period investigated; 7 of them are new

Although many investigations into new state-sponsored groups were published in the previous period, this sphere remains poorly understood. The activity of 38 groups was discovered; seven of them are new cyberespionage groups. This does not mean that other well-known groups ceased their activity, however. It is more likely that their campaigns remained under the radar. In the energy sector, for example, only two frameworks capable of affecting processes were detected: Industroyer and Triton (Trisis). Both were found as a result of an error on the part of their operators.

It is highly likely that there is a significant number of similar, undetected threats, which essentially is a ticking time bomb. It is also worth noting that publicly known state-sponsored groups mainly originate from developing countries. There is still no public information about such attacks orchestrated by developed countries.

## Hacking back: state-sponsored groups go against each other

### Iran, China, and Russia

were attacked and some of the data stolen were made public by groups posing as hackers

In 2019, cases where threat actors disguised as hackers or former group members released information about attack tools used by other groups became more frequent. They were most often examples of hacking back, when attackers become the victims. Today, private companies cannot legally conduct such operations. Hacking back is authorized only in the case of national security services.

## Russian-speaking groups conducting targeted attacks shift their focus to foreign banks

### Cobalt and Silence

began attacking mainly banks outside Russia

Currently, only five groups pose a real threat to the financial sector: Cobalt, Silence, MoneyTaker (Russia), Lazarus (North Korea), and SilentCards (a new group from Kenya).

In Russia, damage from targeted attacks on banks carried out by financially motivated threat groups has dwindled almost 14-fold. One of the reasons is that Russian-speaking threat actors have been shifting to banks worldwide.

## Trojans for PC and Android are gradually disappearing

### 22 trojans

for PCs and Android fell out of use and only 7 new tools appeared to replace them

The trend of Trojans for PCs disappearing from the cyberthreat landscape continues. In Russia, the "homeland" of this type of threat, hackers have stopped developing them. Brazil is becoming the main source of new PC Trojans. However, they are used locally only.

Only Trickbot has evolved significantly over the past year and can now be used in targeted attacks on banks and for espionage against government agencies, as was the case with the Trojan Zeus.

Android Trojans are disappearing slower than PC malware, but in any case the number of new ones is significantly lower than those that have disappeared. Banking fraud malware has evolved from text message interception to automatic transfer of funds through mobile banking applications; this new feature is called ATS, i.e. Automated Transfer System. The number of active Trojans will continue to decline due to the introduction of security measures and a sharp reduction in economic efficiency for attackers.

## Evolution of social engineering without the use of malware

### Remote access tools

as a relatively new social engineering vector

Amid slumping Trojans, the threat of social engineering without the use of malware is growing. Attackers continue to use fake social media accounts, phone fraud with well-prepared scripts, passport databases for reliability, etc. Relatively new methods of social engineering include controlling phones using remote access programs that victims install on their devices after being tricked into doing so by scammers.

## Growth of the carding market thanks to JS sniffers

### \$229 million

fine was imposed on British Airways for data leaks

With a drop in ROI from the use of banking Trojans for PCs and Android, attackers began to use a more effective method to make money: JS sniffers. There are already more JS sniffers than banking Trojans for PC and Android. The total number of cards compromised by JS sniffers has increased by 38%. JS sniffers will be the most rapidly evolving threat and mainly affect countries where the 3D Secure system is not widely used.

## Attacks on insurance, consulting, and construction companies

### RedCurl

a new group detected by Group-IB

In 2019, Group-IB detected attacks by a new group called RedCurl. The group's main goals are cyber espionage and financial theft. Once important documentation has been exfiltrated, the hackers install miners in the compromised company's infrastructure. The group's distinctive feature is the high quality of their phishing attacks, as part of which they tailor emails to the company they are targeting. The threat actor uses a unique custom Trojan that communicates with the C&C server via legitimate services, which makes it very difficult to detect its malicious activity in infrastructures.

## 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 based on proprietary internal methods developed by Group-IB.
- Technical details of cyber threats 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 or trademarks in this report are made with consent of such companies or trademark holders and/or on the basis of information already published in mass media.
- Information published in this report can be used by interested parties only for personal and non-profit causes as long as the reference to Group-IB and the report is given.

# KEY FINDINGS

## and forecasts

### STATE-SPONSORED THREAT GROUPS, CYBERWEAPONS, AND CYBERWARS

#### CURRENT THREATS

For the first time in history, a missile strike was carried out in response to a cyberattack. The threat actors' command center was destroyed as a result. The strike was launched by Israel, and the laws of other countries do not prohibit military action in response to cyberattacks. This sets an extremely dangerous precedent.

World leaders claim that cyberweapons can be used to disrupt adversaries' defense infrastructure. Deploying such weapons essentially equates to a military operation on another country's territory.

The blackout in Venezuela that left most of the country without electricity for days was partially caused by a cyberattack. It is believed that the attack was carried out by the opposition to destabilize the country.

State-sponsored attackers are increasingly interested in telecommunications infrastructures. Their targets are operators, domain name registrars, and organizations responsible for top-level domains and root name servers.

Some state-sponsored threat groups go against each other. Disguised as hackers, they make public the tools used by their rivals and information about them. On the one hand, this helps criminal investigators find perpetrators. On the other hand, it helps attackers better imitate the activity of other groups.

Attacks were carried out successfully on computer manufacturers, with the aim of delivering malicious code to the equipment they produce. This shows that many manufacturers are not ready to fight targeted attacks, and supply chain attacks on their customers will remain a relevant attack vector.

#### 38 groups

of state-sponsored attackers were active throughout the period investigated

#### 7 new cyberspionage groups

were discovered this year

#### Security analysts

mainly analyze groups from Russia, North Korea, Pakistan, China, Vietnam, Iran, the US, the UAE, India, Turkey, and South America

#### Information

about research into cyberattacks carried out by world powers remains unpublished

#### FORECAST: USE OF CYBERWEAPONS TO DISRUPT INTERNET STABILITY IN SOME COUNTRIES

Scenarios in which a country could be disconnected from the Internet seemed unrealistic, yet they are becoming increasingly likely. Disrupting the Web requires long-term preparation, but it is technically feasible. The increasing warmongering rhetoric and aggression could lead to demonstrations of such capabilities. Governments and businesses must ensure that their services are robust enough to withstand such situations.

Domain name registrars are part of critical infrastructures. Disrupting their work affects the World Wide Web, which is why registrars are targeted by government-sponsored threat actors. Next year, there will be a high risk of more threat actors carrying out successful attacks, including for sabotage purposes.

Certain countries are trying to build a system of centralized control over Internet access. This runs contrary to the principle of Internet robustness and

such countries are at higher risk of falling victim to attacks that disrupt the Web and cause more damage. As a result, these countries may become a place where threat actors conduct such attacks and showcase their ability to disrupt the Internet.



# GEOGRAPHICAL SCOPE OF STATE-SPONSORED GROUPS

AMERICA	EUROPE	APAC	THE MIDDLE EAST & AFRICA	RUSSIA & THE FORMER SOVIET UNION
APT28 – Russia	APT28 – Russia	DarkHotel – North Korea	OilRig – Iran	Equation Group – USA
Turla – Russia	Gorgon Group – Pakistan	APT37 – North Korea	APT37 – North Korea	PowerPool
Charming Kitten – Iran	PowerPool	Kimsuky – North Korea	Windshift	Gorgon Group – Pakistan
Gorgon Group – Pakistan	DarkHotel – North Korea	Sidewinder – India	Gaza Cybergang – Gaza	MuddyWater – Iran
APT29 – Russia	APT29 – Russia	Chafer – Iran	Bahamut – The Middle East	APT37 – North Korea
APT33 – Iran	MuddyWater – Iran	APT-C-35	MuddyWater – Iran	Winnti – China
APT-C-36 – South America	APT10 – China	BlueMushroom	APT33 – Iran	Lazarus – North Korea
Kimsuky – North Korea	APT33 – Iran	APT10 – China	Gallmaker	Whitefly
Xenotime – Russia	Gamaredon Group – Russia	APT29 – Russia	APT-C-27 – The Middle East	Gamaredon Group – Russia
Lazarus – North Korea	Gallmaker	OceanLotus – Vietnam	Lazarus – North Korea	Buhtrap – Russia
APT40 – China	Inception	OilRig – Iran	FruityArmor – UAE	APT28 – Russia
STOLEN PENCIL – North Korea	Turla – Russia	Whitefly	Emissary Panda – China	HEXANE – The Middle East
	LEAD – China	Winnti – China	APT-C-38	
	OceanLotus – Vietnam	BITTER – India	Domestic Kitten – Iran	
	Lazarus – North Korea	Turla – Russia	Chafer – Iran	
	APT40 – China	Xenotime – Russia	StrongPity – Turkey	
		Lazarus – North Korea	HEXANE – The Middle East	
		APT40 – China		
		Unidentified group, TajMahal framework		

\* new groups

# KEY TRENDS AND FORECASTS BY INDUSTRY

## Threats to the telecommunications sector

### CURRENT THREATS

A major threat to the telecommunications sector is BGP hijacking, which disrupts the accessibility of networks and many services they power. After such attacks, restoring accessibility usually takes several hours.

The expansion of 5G networks opens up new opportunities for threat actors, as does any type of next-generation technology. 5G architecture paves the way for new types of attacks on operators.

Vulnerable routers, which are rented out to legal entities and individuals, present an enormous threat to the telecom sector. Insecure settings coupled with no updates result in deteriorated services and more malicious traffic. This gives threat actors the opportunity to carry out various attacks based on operators' infrastructures.

#### 9 groups

posed a threat to the telecommunications sector during the period investigated, i.e. more than to the financial sector

#### Espionage and supply chain attacks

are the main goals of these groups, which is why their activity remains unnoticed for longer

### FORECAST: THE DEVELOPMENT OF 5G NETWORKS WILL CREATE NEW THREATS

The cybersecurity level of 5G market players will be a factor that determines their share of the market. Cybersecurity problems faced by a 5G platform provider give other providers a competitive advantage. Demonstrations of ways to exploit and disrupt the work of 5G operators will be used as a tool of unfair competition. Successful attacks could cause providers irreparable reputational damage.

Wider 5G integration will significantly increase the capabilities of ordinary cybercriminals to carry out DDoS attacks, manipulate traffic, and spread malware.

In a few years, telecom companies will struggle to detect hardware and firmware backdoors in 5G infrastructure equipment.

Many telecom operators are Managed Service Providers and provide security services to government and commercial organizations. Threat actors will attack operators to penetrate the networks they protect.



## Threats to the energy sector

### CURRENT THREATS

Compromising IT networks using traditional techniques and malware—including living off the land attacks—is the main vector for penetrating isolated segments of OT networks.

Only two frameworks capable of affecting processes, Industroyer and Triton (Trisis), were detected in recent years. Cybersecurity experts link them to Russia.

Both frameworks were detected due to a mistake on the part of their operators. It is clear that many threats remain undetected, which is a ticking time bomb.

In 2019, Lazarus attacked an energy company in India. The target is not an obvious choice for a state-sponsored threat group, which could point to the military's growing interest in this type of attack.

### 7 groups

posed a threat to the energy sector in the period investigated

### Iran and Russia

are associated with these groups

### FORECAST: IT NETWORKS AND SUPPLY CHAIN ATTACKS WILL BE THE MAIN PENETRATION VECTOR

IT networks will remain the main attack vector for threat actors. Access to these segments is crucial for espionage and collecting information about how to attack a particular energy company for sabotage purposes.

OT network compromise will be the next step once the network's IT segment is successfully breached. Detecting OT compromise is only possible in two cases: if the attack is designed for

sabotage purposes or if the malware operator makes a mistake. Attackers often try to be as covert as possible until they must carry out a mass attack.

Supply chain attacks will pose a serious problem for the energy sector from the part of various software and hardware providers. Management companies will be attacked first, then used to penetrate networks belonging to energy companies.

The most significant threat is expected to come from developed countries. Threat actors in such regions are better equipped, which is why their activity is less noticeable and less thoroughly investigated.





## Threats to the financial sector

### Targeted attacks on the financial sector

#### CURRENT THREATS

SilentCards is a new group that carries out targeted attacks on banks in Africa. Despite their poor technical skills (compared to other groups), they successfully steal money in this region.

FastCash, a new theft method, was detected in 2018, though it was first used in Asia in as early as 2016. The Lazarus group is behind all attacks of this kind.

Experts observed the following trends in attack schemes: Silence was the only threat actor that carried out attacks through ATMs; Silence and SilentCards used card processing, while Lazarus used SWIFT (two successful thefts in India and Malta amounting to \$16 million in total).

Silence stopped using mail-outs, instead buying them from other hacking groups (especially TA505).

Each Russian-speaking group carried out an attack in Russia over the period investigated. Cobalt attempted to steal from a company twice, but the theft did not cause any significant financial damage. Compared to the previous period, the average stolen sum in Russia dropped from \$1.8 million to \$480,000, with the total stolen sum amounting to \$1.5 million, i.e. 93% less than in the previous period.

#### 5 groups

posed a real threat to the financial sector during the period investigated – Cobalt, Silence, MoneyTaker, Lazarus, SilentCards

#### 3 out of 5 groups

are Russian speakers (Cobalt, Silence, and MoneyTaker); they are the only owners of Trojans that control ATM dispensers

#### 2 out of 3 groups

that are Russian speakers (Cobalt and Silence) started mainly attacking banks outside Russia

#### FORECAST: LARGER GEOGRAPHICAL SCOPE OF RUSSIAN-SPEAKING GROUPS

Russian-speaking groups (Silence, MoneyTaker, and Cobalt) are likely to continue their expansion by multiplying their attacks outside Russia. To withdraw money, they will carry out attacks on card processing systems and use Trojans for ATMs. The groups will shift their focus away from SWIFT.

Lazarus will remain the only group to steal money through SWIFT and ATM Switch. The threat actor has previously carried

out successful attacks through ATM Switch against banks that use software running on IBM AIX. Such banks will therefore be the first to catch the threat group's attention.

Infrastructure disruption to cover tracks will be the final stage of successful attacks.

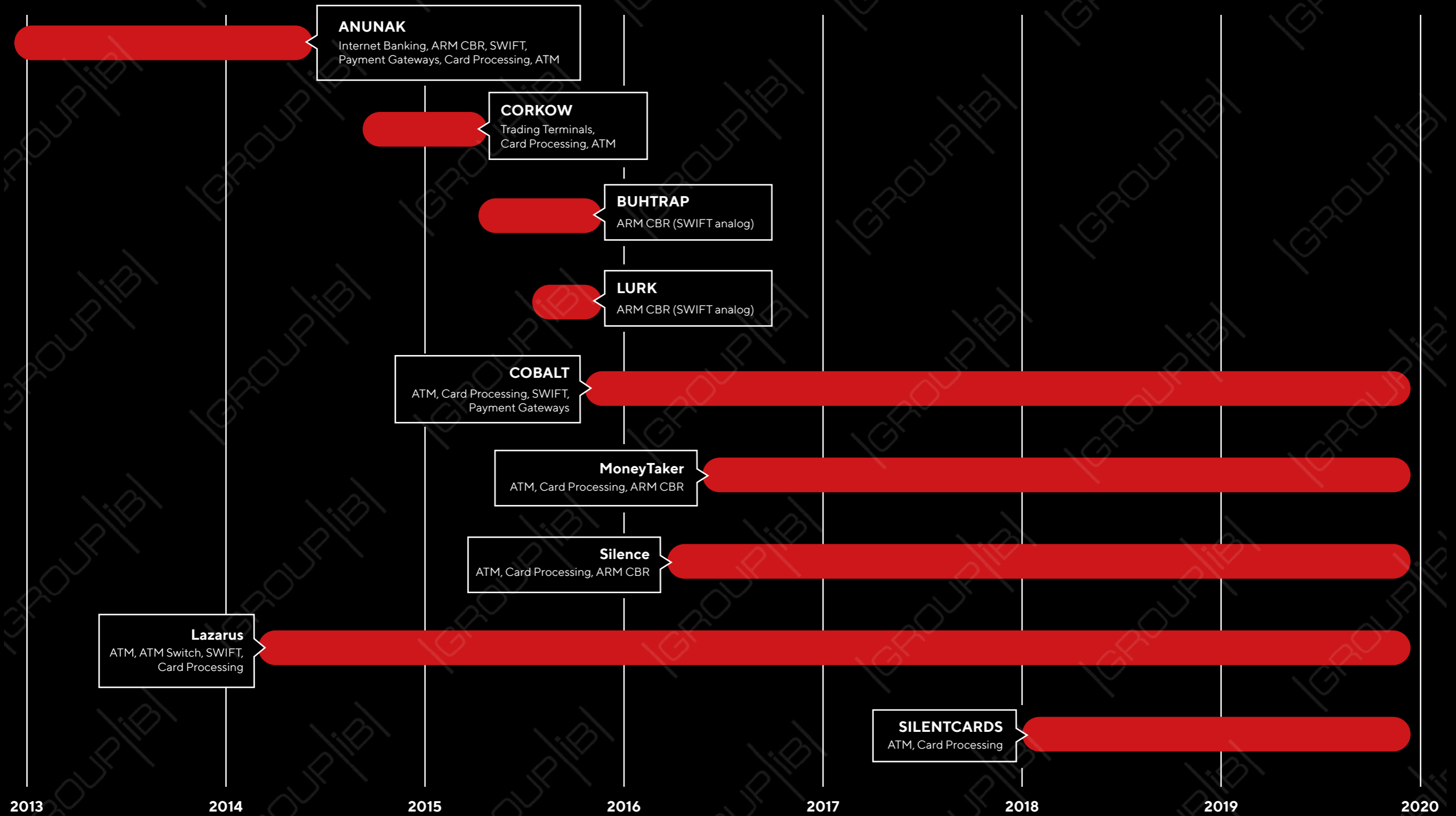
SilentCards may remain local and focus on African banks. The group is likely to expand its list of targets by attacking

other industries. Their main vector will be blackmail in ransomware attacks.

The Trickbot Trojan has markedly improved (see section Banking Trojans for PC) and can now be used in targeted attacks on banks and for espionage against government agencies, as was the case with the Trojan Zeus.



# TARGETED ATTACKS ON THE FINANCIAL SECTOR





## Non-targeted attacks and threats to banking customers

### Growth in carding activities due to the spread of JS sniffers

Dumps continue to have the largest share of the carding market, with a 46% increase in the number of dumps for sale. The sale of textual data (card number, CVV, expiration date) is also on the rise, with a 19% growth.

The largest bank card data leaks are related to compromises of US retailers. The US is far ahead and comes first, with 93% of all cards compromised.

Middle Eastern countries (Kuwait, Pakistan, the UAE, and Qatar) together account for 2.38% in this classification. It is believed that the increase in the number of compromised cards was caused by Lazarus attacks in late 2018 and early 2019.

JS sniffers became a point of growth as regards the volume of textual data. As at spring 2019, Group-IB detected 38 different JS sniffer families. At the time of publishing this report, that number has even grown. There are more JS sniffers than banking Trojans.

In terms of JS sniffer-related attacks, the US is first again, with UK banks coming second. This is mainly due to the attack on British Airways in late 2018, which resulted in more than 300,000 bank cards being compromised.

**38% growth**

in the total number of compromised cards

**\$229 million**

fine imposed on British Airways as a result of a data breach



### FORECAST: DECLINE IN PHISHING AND EXPLOSIVE GROWTH IN SOCIAL ENGINEERING

Phishing kit developers began devoting more attention to self-defense. They blacklist cybersecurity vendors' subnets and hosting providers, show phishing content only from the IP addresses of the region where their victims are located, redirect users to legitimate websites, and check anomalous user agents.

In an effort to attract customers, phishing kit developers started equipping their kits with user-friendly management systems. Now, instead of working with logs via email, customers can conveniently manage data via simple web panels.

Financial phishers began using panels for managing web injects and the autofill function. Such panels have previously been used in banking Trojans.

SMS traffic in certain countries is becoming a common tool for sharing links to phishing websites. As a result, leaks of phone number databases and access to personal mobile operator accounts, which can be used to send SMS messages, are becoming more popular.

#### **New sophisticated social engineering methods**

Considerably reduced activity of banking Trojans for PC and Android, combined with fewer phishing attacks, has made theft methods using social engineering the most widespread threat.

Social engineering comes in many forms. Schemes in which victims are prompted to reveal their logins, passwords, and bank card details and transfer money via ATMs and mobile applications are widely known. Threat actors use various channels to contact their victims, such as phone calls, messaging apps, and social media.

Moreover, new types of social engineering techniques are emerging. For instance, as part of an increasingly popular scheme, users are asked to install a remote control tool on their mobile device, thereby giving the hackers access to all applications and data thereon.

## Fewer banking Trojans for PC



Russian-speaking hackers no longer create banking Trojans for PC. Brazil has become a new source of this type of malware. So far, it is used to attack the local population only.

Owners of old botnets are not expanding their geographical scope and tend to attack banking customers in two or three countries where it is easier for them to launder stolen money.

There are two groups that still steal money in Russia using Trojans for PC: RTM and Buhtrap2. Only the former shows continued activity (and uses the Trojan RTM).

### 7 Trojans for PC

fell out of use, with no new ones created by Russian-speaking hackers during the period investigated

### Trickbot is the only Trojan to have significantly evolved over the last year:

- new module for collecting passwords from installed applications;
- ability to steal RDP, VNC, and PuTTY data as well as configuration files from SYSVOL directories on domain controllers;

- fileless attacks and use of Mimikatz;
- no module and configuration file download to disk (Windows 10);
- mail-outs from compromised computers;
- new cookie stealer.

Some experts have singled out the group Grim Spider. It uses Trickbot for network reconnaissance purposes to then load the Ryuk ransomware and demand sums exceeding \$100,000 for decrypting the victim's device.



## Autofill and fake push notifications in banking Trojans for Android

In the past, money was stolen from bank accounts mainly by displaying fake windows where bank card, login, and password details were to be entered. Transaction confirmation codes were obtained by intercepting SMS messages. The year 2019 saw the appearance of Trojans that automatically transfer money via mobile banking apps, i.e. the autofill feature.

Push notifications were thought to be a reliable method of delivering one-time codes. Now, however, Trojans use the Accessibility Service to manipulate push notifications, copy their text, and activate certain areas.

The US managed to make the authors of Android Trojans prohibit the use of their malware in the States, not just in Russia and other post-Soviet countries.

The year 2019 saw the appearance of the most advanced Android Trojans, which were developed in order to be rented out. Their price ranges from \$800 to \$2,000 per month.

Owners of banking botnets began devoting more attention to self-defense and sandbox bypassing methods.

### 15 Trojans

fell out of use; the codes of seven Trojans were adapted for modern Android OS; five new Trojans entered the market



## FORECAST: GRADUAL REPLACEMENT OF TROJANS BY JS SNIFFERS AND CHANGES TO METHODS OF SOCIAL ENGINEERING AND PHISHING DISTRIBUTION

Phishing and social engineering will remain the biggest threat to online banking customers. There may be a shift from email to text message as the main distribution channel for phishing links.

The owners of DDoS botnets built on numerous infected routers may start renting them out to hackers who engage in phishing. Phishing is usually more profitable than DDoS attacks.

Schemes involving remote support through remote access tools will shift from PCs to mobile devices. They will have one of two goals: to obtain bank card information from the customer or to request payment for fake services (e.g. security checks, removing threats from devices).

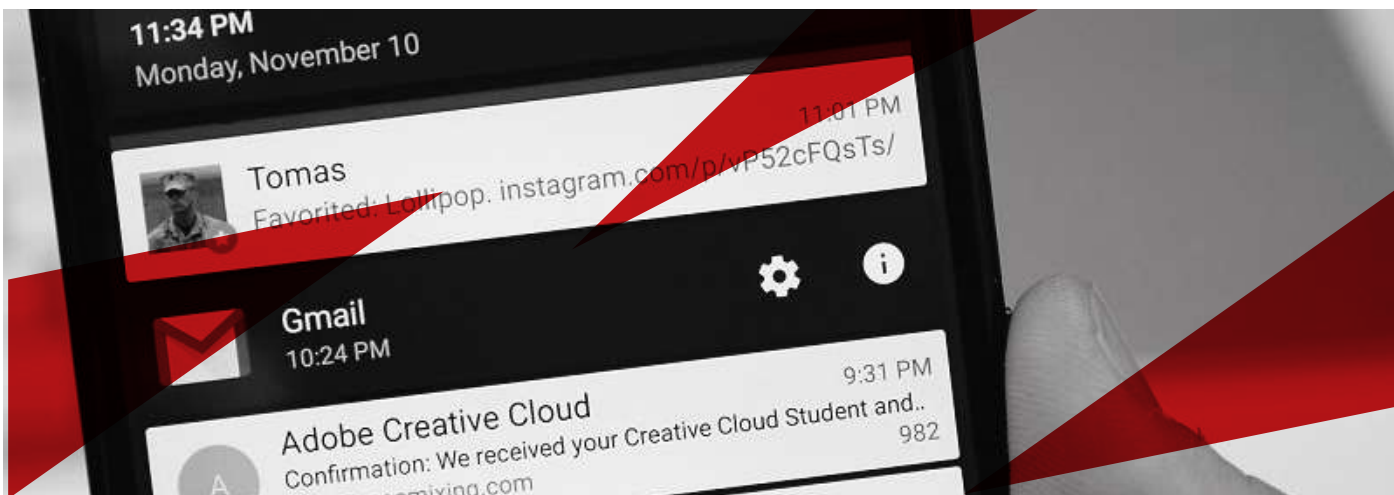
The number of active banking Trojans for PCs will decrease except in Brazil, where threats are developing locally. Moreover, their geographical scope will shrink due to the integration of security tools and markedly reduced financial benefits for attackers.

Today, malware writers develop the autofill feature for Android Trojans on their own. If a universal solution for mobile Trojans is created (as was the case with Zeus), then such attacks will become significantly more popular. However, this is unlikely to happen within a year.

JS sniffers will be the most rapidly evolving threat; they make attackers more money than banking Trojans. There are already more JS sniffers than banking

Trojans for PC and Android. That said, the threat will mainly affect countries where the 3D Secure system is not widely used.

POS Trojans will not undergo significant changes. They will continue to be used mainly in attacks on retailers in the US and, to a lesser extent, in Spanish-speaking countries.





# NEW PHASE IN CYBERWAR:

## Internet destabilization attacks

### Key cyberthreat trends by year

#### 2017

WannaCry, NotPetya, and BadRabbit ransomware epidemics

#### 2018

Side-channel attacks and new vulnerabilities in microprocessors

#### 2019

Overt military operations in cyberspace

In 2019, cybersecurity became a heavily debated topic in politics. The activities of cyber armies and the rhetoric of political leaders around cyberattacks continue to gain momentum.

**March 2019, Venezuela.** Sabotage at the Simón Bolívar Hydroelectric Plant, also known as the Guri Dam, resulted in a mass-scale blackout in Caracas and 22 of all 23 states in the country. According to TASS, a news agency, the country's Communications Minister said there had been "a cyberattack against the automated control system". The plant was shut down in response to the attack. Unlike other well-known attacks on energy companies, this is the first time that a large part of a country was left without electricity for several days.

**May 5, 2019, Palestine.** According to Israeli sources, on May 4, 2019, hackers from the militant group Hamas tried to carry out a cyberattack. Israel declined to reveal the incident details. To counter the attack, the Israel Defense Forces launched an airstrike on a building in the Gaza Strip, where the hackers headquarters is believed to have been located.

**June 2019, Iran.** On June 20, 2019, Iran's Islamic Revolutionary Guard Corps (IRGC) shot down a US drone. The US retaliated a few days later by launching a cyberattack on IRGC's missile control systems. Such an attack requires months of preparation, which suggests that the systems had been compromised prior to that.



Incident in Iran has once again confirmed the suggestion that the critical infrastructure of many countries has already been compromised, but attackers remain unnoticed until they act.

All these cases show that cyberspace is becoming a battlefield. This trend could lead to new cyberattacks on military and government systems in order to disrupt their work, cause social and economic damage, and destabilize countries.

Disruption of Internet infrastructures, which nearly all government and private organizations depend on, is becoming a dangerous attack vector. The sections below look at scenarios that have already been tested and could be used on a larger scale at government level in the next year.

# DNS HIJACKING AND ATTACKS ON DOMAIN NAME REGISTRARS

The DNS protocol underpins the World Wide Web and hackers who gain control over it can be extremely dangerous. Moreover, carrying out operations using this protocol does not require having access to DNS servers.

There are two possible scenarios when purchasing a domain name:

- either the domain registrar provides DNS server services;
- or the registrar provides a domain name only, with DNS servers being run by a different provider.

In either scenario, each customer can specify the following information in their personal account on the domain name registrar's website:

- what DNS servers will be responsible for a particular domain name;
- what IP addresses the traffic will be sent to when there is a request to access the resources related to this domain name.

This means that by compromising a particular domain name registrar, threat actors can manipulate all domains registered through that registrar. The situation is made worse by the fact that countries usually have only a few major registrars, which service both government and private organizations.

Simultaneously hacking several main registrars will paralyze website, mail, and DNS servers, as well as all services connected to them, for most

of the country. If such an attack were to be conducted in combination with sabotage activities, restoring the registrar's stability and recovering their configuration would be impossible. The resulting situation would damage all industries without exception.

In addition to individual registrars, attackers could target organizations that manage country code top-level domains. Almost every country has this type of organization. For instance, the Singapore Network Information Centre (SGNIC) Pte Ltd is responsible for Singapore's domain zone .sg.

Domain name registrars and organizations responsible for root domain services have become a new priority for threat actors. Information security experts detected several such incidents in 2019.

The attacks described above were successful and targeted individual organizations in both the government and private sectors. If threat actors become set on disrupting national infrastructures, attacks like these will have much wider consequences.

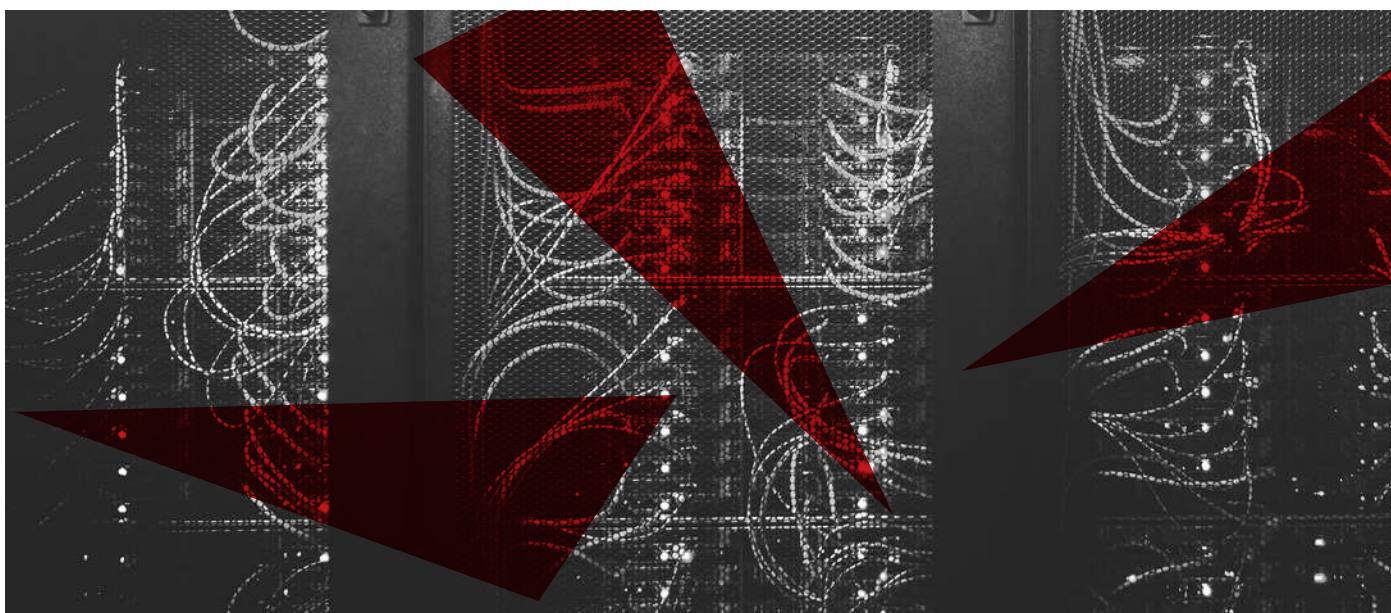
## DNS infrastructure could fall victim to a successful attack at all levels

### 12.14.2018 – 1.2.2019

Netnod, a Swedish company that was the first to manage root name servers and provide DNS services (there are only 12 organizations of this kind in the world), suffered a series of attacks between December 14, 2018 and January 2, 2019. The attackers were able to manipulate DNS records for MITM attacks targeting specific customers.<sup>[1]</sup>

### APRIL 2019

the owners of the domain names .gr and .ελ were notified that the Institute of Computer Science of the Foundation for Research and Technology (FORTH-IC), which is responsible for technical support and use of domains in these zones, fell victim to an attack. Users were asked to urgently change their passwords for authorization.<sup>[2]</sup>



<sup>[1]</sup> <https://www.netnod.se/news/statement-on-man-in-the-middle-attack-against-netnod>

<sup>[2]</sup> <https://www.zdnet.com/article/hackers-breached-greeces-top-level-domain-registrar>



# BGP HIJACKING AND ATTACKS ON INTERNET ROUTING SYSTEMS

Another fundamental routing protocol is BGP (Border Gateway Protocol). The idea behind BGP hijacking is to redirect the network traffic of certain prefixes of an autonomous system (IP address pools) through the threat actor's equipment. The most common objective of such attacks is cyberespionage.

However, network routes can also be manipulated to disrupt major telecommunications companies. There have been many major, publicly shared incidents (although they were a result of either human error or misconfiguration rather than targeted attacks).

## NOVEMBER 25, 2018

Krek Ltd, a small-scale Russian operator, made a mistake in its BGP configuration, causing 10-20% of Russian Internet users to lose access to thousands of services. The failure lasted for more than an hour and affected major companies such as Amazon, YouTube, VK (Russian social network), ivi.ru (online video streaming service), and many others.<sup>[1]</sup>

## NOVEMBER 2018

MainOne, a Nigerian Internet service provider, made a configuration mistake and changed routes in such a way that traffic to Google services was directed through China, where it was getting dropped. A total of 180 prefixes were affected. It took 74 minutes to fix the issue after it was detected. During this time, some Google users experienced access problems.<sup>[2]</sup>

## JUNE 6, 2019

the Swiss company Safe Host (AS21217) caused a leak of 70,000 routes to China Telecom (AS4134). The most heavily affected were Swisscom (AS3303) based in Switzerland, KPN (AS1136) based in the Netherlands, and Bouygues Telecom (AS5410) and Numericable-SFR (AS21502) based in France. The incident lasted for two hours.<sup>[3]</sup>

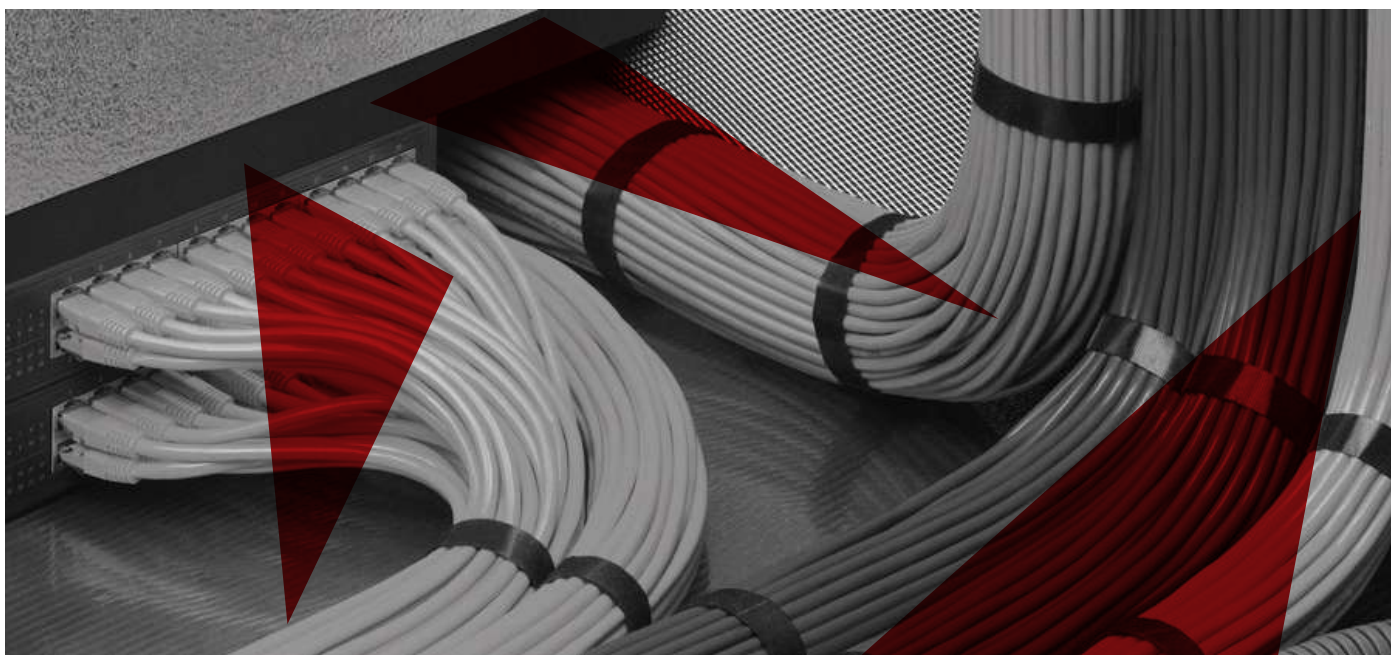
Another noteworthy example is a 2019 experiment, the aim of which was to analyze new BGP security features. It culminated in the failure of routers of Internet service providers in Asia and Australia.

## BGP ROV

The new BGP Route Origin Validation (ROV) standard is now part of the BGP protocol security package, along with BGP Resource Public Key Infrastructure (RPKI) and BGP Path Validation (BGPsec). BGP ROV allows routers to use BGP RPKI information to filter out unauthorized route advertisements and prevent BGP from being intercepted by attackers intending to redirect traffic from legitimate servers to malicious ones. Experts say the problem was that the BGP attribute they used caused a crash in the software of the routers based on FRRouting (FRR)—a set of IP protocols for Linux and Unix.

The cases described above show that manipulating traffic does not require access to the targeted company's network hardware. Access to an area border router is enough to be able to change the BGP configuration.

So far, BGP hijacking has had large-scale but short-term effects. For prolonged sabotage, threat actors will need to have both access to the network routers of several operators as well as pre-prepared scenarios for manipulating traffic. In such cases, BGP hijacking could cause significant network congestion in some countries (similar to what happens in energy company networks).



[1] <https://radar.qrator.net/blog/no-filters-shoot-your-foot>

[2] <https://blog.cloudflare.com/how-a-nigerian-isp-knocked-google-offline/>

[3] <https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/>

## ATTACKS ON LOCAL SYSTEMS OF FILTERING AND BLOCKING TRAFFIC

Some countries have implemented or are creating filtering systems that analyze and block certain user traffic. Such technological solutions facilitate attacks aimed at blocking the operation of a network in a particular country. The attacks summarized below have been tested by threat actors and may be conducted on a larger scale in the future.

### Blacklisted resources

Internet Service Providers (ISPs) block access to harmful websites (terrorist-related, malicious, linked to drug trafficking, etc.) based on blacklists. The lists consist of domains, IP addresses, and links. They are constantly updated so that malicious resource owners cannot bypass restrictions.

In cases where operators cannot deploy DPI (Deep Packet Inspection) systems, they must restrict traffic based on IP addresses. Knowing this, attackers

leverage blacklisted domains to block legitimate resources. Owners of banned websites list the IP address of a legitimate webpage in their DNS information, which leads to providers blocking the legitimate site. If a blacklisted domain name has a new legitimate IP, it will automatically be blocked by the provider.

Since 2017, attackers in Russia have used this technique to bring down Wikipedia as well as banking and government resources. In March 2019, a similar attack was carried out against the users of Yandex, a Russian search engine.

This is an easy and cheap way to conduct cyberattacks. Companies can protect themselves by introducing a whitelist of critical resources that must never be blocked. However, blacklists are distributed in a centralized manner. If an attacker gains access to the server distributing these lists, they will be able to add any subnet to it.

### Traffic decryption

Usually, transmitted content is encrypted, so some countries require users to install government-issued certificates. Once installed, the certificate helps local government agencies decrypt user traffic.

Such certificates are issued by designated centers. Banning certificates by browser and operating system would affect all users who have these certificates installed.

This happened to DarkMatter, a UAE-based cybersecurity company. Google announced plans to ban root certificates owned by DarkMatter from Chrome and Android. Mozilla also announced that its browser Firefox would not trust certificates from DarkMatter. In August 2019, Google and Mozilla blocked a Kazakh government-issued root certificate used for intercepting traffic.



<sup>[1]</sup> <https://www.netnod.se/news/statement-on-man-in-the-middle-attack-against-netnod>

# EVOLUTION

## of state-sponsored threat groups

### GEOGRAPHICAL SCOPE OF ATTACKS AND NEW GROUPS

During the reporting period, researchers analyzed attacks carried out by 38 groups and affecting the entire world. Security specialists mainly focused on groups from Russia, North Korea, Pakistan,

China, Vietnam, Iran, USA, UAE, India, Turkey, and South America.

It is important to note that there is still no public information about

attacks originating from developed countries. This again confirms that well-orchestrated attacks are difficult to detect or attribute to a specific group or country.



#### 1. ATTACKS ON AMERICA

**Russia:** APT28, Turla, APT29, Xenotime

**Pakistan:** Gorgon Group

**Iran:** APT33, Charming Kitten

**North Korea:** Kimsuky, Lazarus, STOLEN PENCIL

**China:** APT40

**South America:** APT-C-36\*

#### 2. ATTACKS ON EUROPE

**Russia:** APT28, Turla, Gamaredon Group, APT29

**Pakistan:** Gorgon Group

**Iran:** APT33, MuddyWater

**North Korea:** DarkHotel, Lazarus

**China:** APT40, LEAD, APT10

**Vietnam:** OceanLotus

**Unknown:** PowerPool, Inception, Gallmaker\*

#### 3. ATTACKS ON APAC

**North Korea:** APT37, Kimsuky, Lazarus, DarkHotel

**India:** Sidewinder, BITTER

**Iran:** Chafer, OilRig

**China:** APT10, Winnti, APT40

**Russia:** APT29, Turla, Xenotime

**Vietnam:** OceanLotus

**Unknown:** APT-C-35,

BlueMushroom\*, Whitefly\*,

Unidentified group, TajMahal framework

#### 4. ATTACKS ON MIDDLE EAST AND AFRICA

**The Middle East:** Bahamut, APT-C-27, HEXANE\*

**Turkey:** StrongPity

**Gaza:** Gaza Cybergang

**UAE:** FruityArmor

**Iran:** OilRig, MuddyWater, APT 33, Domestic Kitten, Chafer

**North Korea:** APT37, Lazarus

**China:** Emissary Panda

**Unknown:** APT-C-38, Windshift\*, Gallmaker\*

#### 5. ATTACKS ON RUSSIA AND THE FORMER SOVIET UNION

**The Middle East:** HEXANE\*

**USA:** Equation Group

**Pakistan:** Gorgon Group

**Iran:** MuddyWater

**North Korea:** APT37, Lazarus

**Russia:** Gamaredon Group, Buthtrap, APT28

**China:** Winnti

**Unknown:** PowerPool, Whitefly\*

\* new groups



Throughout the second half of 2018 and the first half of 2019, security experts identified numerous previously unknown state-sponsored groups. Many have been conducting operations for several years and have gone unnoticed for a long time. Some groups attack similar targets, which leads to competition between them and means that their actions are detected quicker.

<b>Windshift</b>	<b>Geographical scope</b> The Middle East	<b>Initial infection</b> Trusted relationship (social engineering) Spear phishing Drive-by compromise	<b>Tools</b> WindTail WindTape
------------------	--	--	--------------------------------------

The cyberespionage group WindShift has been flying under the radar for many years thanks to its distinctive feature—thorough attack preparation.

The attackers created fake user pages on social media (LinkedIn, Facebook, Twitter, Instagram, and Google Plus) and sent friendly messages to potential victims. The interactions lasted from six months to a year, during which the attackers tricked their victims into divulging valuable information.

The group mainly targets employees of government agencies and critical infrastructure facilities in the Middle East. Victims' macOS systems were attacked using crafted malicious programs: OSX.WindTail.A, OSX.WindTail.B, and OSX.WindTape.

<b>Blue Mushroom</b> (aka Sapphire Mushroom, APT-C-12)	<b>Geographical scope</b> China	<b>Initial infection</b> Spear phishing	<b>Tools</b> SinaAppEngine ps_backdoor
---	------------------------------------	--	--

The group Blue Mushroom (aka Sapphire Mushroom, APT-C-12) has been operating since 2011 but only became known in mid-2018.

Its attacks involve cloud infrastructure. For example, the group uses Amazon S3 and cloud server communication protocols to exfiltrate confidential user information.

The attackers also use the Digital Ocean cloud service as C&C and the SinaAppEngine (SAE) service to create their own C&C infrastructure.

<b>Gallmaker</b>	<b>Geographical scope</b> The Middle East Eastern Europe	<b>Initial infection</b> Spear phishing	<b>Tools</b> Metasploit
------------------	--	--	----------------------------

Gallmaker has been operating since at least December 2017 but was only discovered in 2018. To compromise systems, attackers exploit the Dynamic Data Exchange (DDE) feature in Word applications. The DDE protocol is used to exchange information between Office programs that use shared data or a shared memory.

## APT-C-36

(aka Blind Eagle)

### Geographical scope

Colombia

### Initial infection

Spear phishing

### Tools

Imminent Monitor RAT

APT-C-36 (aka Blind Eagle) is a threat actor originating from South America that became known in late 2018. Its goal is to steal trade secrets from major companies and government agencies; its main infection vector is malicious emails. To hide the sender's IP address, the threat actor uses proxy and VPN services.

## Whitefly

### Geographical scope

Southeast Asia  
Russia

### Initial infection

Spear phishing

### Tools

Mimikatz  
Trojan.Vcrodat  
Termite  
Nibatad

Security specialists first detected Whitefly in 2018 after an attack on Singapore's largest public health organization, SingHealth, which resulted in a reported 1.5 million patient records being stolen.

The group has gone unnoticed since 2017. They mainly target companies based in Singapore.

## HEXANE

(aka LYCEUM)

### Geographical scope

The Middle East  
Central Asia  
Africa

### Initial infection

Supply chain attack  
Spear phishing  
Password spraying

### Tools

DanBot  
PoshC2  
PowerShell Empire

HEXANE is a new group targeting the industrial sector. Its members have been active since mid-2018, focusing on the Middle East, Central Asia, and Africa.

## Unidentified group

### Geographical scope

Central Asia

### Initial infection

–

### Tools

TajMahal

In the fall of 2018, reports revealed a newly discovered sophisticated APT framework, TajMahal. It has been used for at least 5 years, but it remains unclear to which group the tool belongs. The framework consists of two packages named Tokyo and Yokohama and contains around 80 malicious modules. The tool is designed to conduct cyberespionage campaigns, but the list of confirmed victims only contains one: a diplomatic entity from a country in Central Asia.



# SUPPLY CHAIN ATTACKS

Last year's Group-IB Hi-Tech Crime Trends report identified BIOS/UEFI attacks as one of the most prominent trends. Experts predicted that the main targets would likely be firmware and motherboard developers based mainly in the APAC region, where large companies have their production facilities.

## Winnti attacks on hardware manufacturers and game developers

A few months after Group-IB's report was released, its prediction was confirmed by news about a malware campaign called Operation ShadowHammer.<sup>[1]</sup> To deliver malware, attackers leveraged the legitimate utility ASUS Live Update, which automatically updates components such as BIOS, UEFI, drivers, and applications.

The trojanized utility was signed with the legitimate certificate "ASUSTeK Computer Inc." and was hosted on the official ASUS server.

Similar malware delivery techniques were used to infect software belonging to three other manufacturers, whose names were not disclosed. The attacks, conducted for espionage purposes, are linked to the Chinese group Winnti.

In addition to equipment manufacturers, the same group successfully attacked the gaming industry. In total, two games and one gaming platform were infected. One of the affected gaming companies is located in Thailand.

## Plead (aka BlackTech) campaigns: Focus on Taiwan

In July 2018, cybersecurity experts discovered a new malware campaign involving the Plead backdoor, which was digitally signed using a valid D-Link Corporation code-signing certificate. At the end of April 2019, the experts identified multiple attempts to deploy the same malware in an unusual way. The Plead backdoor was created and executed by a legitimate process named AsusWSPanel.exe. The executable file was digitally signed by ASUS Cloud Corporation. Plead malware has always been most widely deployed in Taiwan.

## Unsuccessful attack on vendors of software for developers

In 2019, an attack on an international vendor of development tools for various programming languages was discovered. The attackers compromised the

company's infrastructure and accessed the Docker containers used to build the software, after which they were discovered. Allegedly, they planned to inject malicious code into legitimate programs at the assembly stage.

## Chinese group attacks through Hewlett Packard (HP) and IBM

In December 2018, Chinese attackers reportedly infiltrated the networks of Hewlett Packard Enterprise (HPE) and IBM as part of the Cloudhopper campaign. By gaining access to the networks, they were subsequently able to hack into computers belonging to HPE and IBM clients.

Cloudhopper compromised client data in 12 countries, including Brazil, Germany, India, Japan, the United Arab Emirates, Great Britain, and the United States. The clients were from industries such as finance, electronics, medical equipment, biotechnology, automotive, mining, and oil and gas.



<sup>[1]</sup> <https://securelist.com/operation-shadowhammer/89992/>

# HACKING BACK

“Hacking back” is a controversial method that helps victims of cyberattacks take a more proactive approach to deterring cyberthreats. The question of whether private companies can legally conduct such operations has been discussed for years. Today, hacking back is allowed only in the case of national security services. In 2019, there were more instances when information about tools used by attackers was made public as part of retaliatory attacks.

In March 2019, the Telegram channel Lab Dookhtegan posted tool source codes used by the Iranian group OilRig (APT34) and data about its members. The information included the identities of hacked victims as well as the names, surnames, and social media profiles of supposedly active group members, including leaders. A user with the nickname “Lab Dookhtegan” claims to be a former member of OilRig and to have worked on the group’s DNSspionage campaign.

The published hacking tools include:

- Glimpse (a new version of a PowerShell Trojan, which Palo Alto Networks named BondUpdater);
- PoisonFrog (an old version of BondUpdater);
- HyperShell (a web shell that Palo Alto Networks called TwoFace);
- HighShell (another web shell);
- Fox Panel (a phishing kit);
- Webmask (the main tool involved in the DNSspionage campaign).

Published data about 66 victims was collected in some of APT34’s backend command-and-control (C&C) servers and contained credentials from internal servers and user IP addresses. This victim list mainly includes companies and organizations in the Middle East, Africa, East Asia, and Europe.

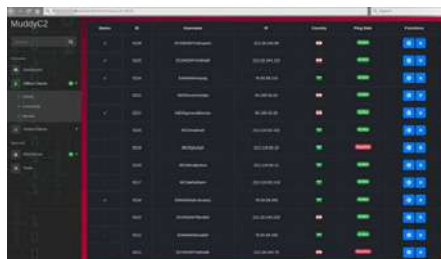
Lab Dookhtegan also leaked data about past APT34 operations, listing IP addresses and domains where the group had hosted web shells and other operational data. As of April 18, 2019, researchers were aware of 125 web shells.

In June, researchers reported an attack on a Middle East organization conducted by the group Turla in January 2018. Threat actors used OilRig (Iran) infrastructure to download a customized

variant of Mimikatz—which is unique to Turla (Russia)—to the victim’s device.

As occurred in the OilRig (APT34) case, a Telegram channel was used to leak data about another Iran-nexus group, MuddyWater. The data leaked included information about the source code of a tool written in Python and its C&C servers.

This tool is designed to generate a payload embedded in a macro. Once the macro is executed, the victim’s computer connects to the C&C server and downloads additional modules. This tool also delivers a second-stage payload, e.g. .sct, .hta, and PowerShell.



In June 2018, the United States imposed sanctions against the Russian research institute Quantum, a contractor for FSB, the Russian intelligence service. In December 2018, the group Digital Revolution published data stolen from Quantum. In July 2019, hackers breached SyTech, another FSB contractor, and shared the exfiltrated data about the company’s internal projects and screenshots of SyTech’s servers with Digital Revolution. The latter released this information online.

In August 2018, the group Intrusion Truth revealed the identities of individuals it claimed were members of the Chinese hacking group APT10. In July 2019, the same group shared details of individuals thought to be members of the China-backed group APT17.

In August 2019, FireEye released an in-depth report about the APT41 group during the BlackHat conference. APT41 seems to have several ties with APT17, which is why experts believe that these threat actors are in fact the same group (called Winnti or BARIUM).

CODE FAMILY OVERLAP AMONG DIFFERENT CHINESE ESPIONAGE GROUPS<sup>[1]</sup>

Malware	APT1	APT3	APT10	APT17	APT18	APT19	APT40	APT41
BLACKCOFFEE				●			●	●
CHINACHOP				●			●	●
COLDJAVA								●
HIGHNOON				●				●
HIGHNOON.BIN				●				●
HIGHNOON.LITE								●
HOMEUNIX	●		●	●	●			●
JUMPALL				●				●

[1] <https://content.fireeye.com/apt-41/rpt-apt41>

# TELECOMMUNICATIONS SECTOR

## *new challenges and threats*

---

### TELECOM-RELATED TARGETING

The telecom industry is a key target for state-sponsored attackers. If they manage to compromise a telecommunications company, attackers then have the opportunity to also compromise its customers for surveillance or sabotage purposes.

#### **APT10**

One of the most large-scale operations during the reporting period was an attack called Operation Soft Cell, allegedly conducted by the Chinese state-sponsored group APT10. The campaign has been active since at least 2012.

The purpose of the attack was to obtain CDR records belonging to a large telecommunications provider. The hackers were able to compromise usernames and passwords as well as billing data, detailed call records, credentials, mail servers, user location, and more.

The attack started with deploying a modified version of the China Chopper web shell on a vulnerable server. The attackers leveraged the Windows process `w3wp.exe`, which runs web applications and is responsible for requests sent to a web server.

The attackers used stolen credentials to create fraudulent domain user accounts with extensive administrator privileges. They then used these accounts or deployed the Poison Ivy RAT to maintain access to compromised resources.

#### **MuddyWater**

The state-sponsored group MuddyWater gained access to the local network of Korek Telecom, a mobile operator based in Erbil, Iraq. Compromising the operator was an intermediate stage in an attack on the oil and gas company Missan Oil Company, which is supposedly a client of Korek Telecom.

#### **APT33 (aka Elfin, Magnallium)**

In late 2018, APT33 (aka Elfin, Magnallium) resumed its attacks using a new variant of the Shamoon Trojan. The tool's first version was discovered in 2012; the second version, together with the wave of attacks during which it was used, were discovered in 2017. Shamoon-3 overwrites the master boot record (MBR), partitions, and files in the system with random data.

The updated tool's first victim was Saipem S.p.A., an Italian oil and gas industry contractor. The Shamoon wiper was also detected in attacks on oil, gas, telecommunications, and energy companies as well as government organizations in the Middle East and Southern Europe.

#### **Chafer (aka APT39)**

The goal of the group Chafer (aka APT39) is to collect personal data for further user monitoring and tracking operations in support of Iranian national interests. The collected data can also be used as a vector for further attacks.

For initial compromise, the group leverages spear-phishing emails with malicious attachments or URLs, usually resulting in a POWBAT infection. The group identifies and exploits vulnerable web servers belonging to targeted organizations in order to install web shells (e.g. ANTAK and ASPXSPY) and uses stolen legitimate credentials to compromise externally facing Outlook Web Access (OWA) resources.

#### **HEXANE**

The newly discovered group HEXANE attacks telecommunications companies in the Middle East, Central Asia, and Africa as a stepping stone in supply chain attacks. Its goal is to gain access to critical infrastructure belonging to the organizations that use the services of these telecom companies.

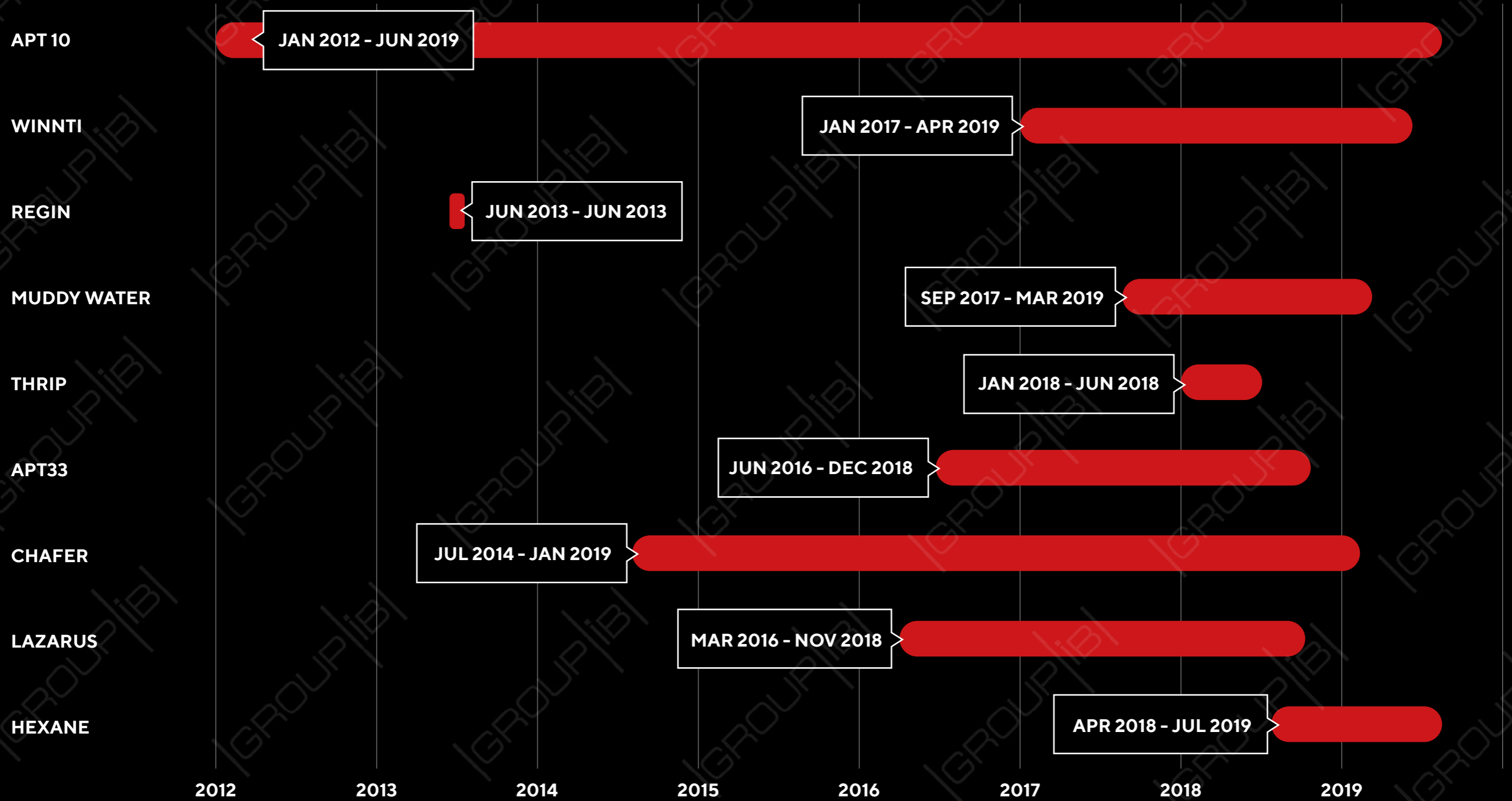
#### **Lazarus**

The group Lazarus also spies on telecommunications companies using a new backdoor called Rising Sun. The latter collects data about the infected device, such as IP address, network device information, OS name and version, system data, and username. The collected data is sent to the C&C server. This backdoor is probably spread as the first attack stage and may be followed by a download of additional malware.

#### **Thrip**

The Chinese hacker group Thrip is known for espionage and sabotage attacks. In particular, they target organizations in the satellite communications sector. The hackers use the "living off the land" technique, which involves using operating system features or legitimate network administration tools (PsExec, Mimikatz, WinSCP, and LogMeIn) to compromise victims' networks with Trojans.

# TELECOM-RELATED TARGETING





# 5G EXPANSION-RELATED CHALLENGES

The 5G standardization process is not scheduled to be completed until 2021, but the first networks have already been built. Moreover, active competition currently exists not only between technology giants, but also countries (USA and China are leading in the field of 5G).

Pioneers will set the standards and practices that will be implemented by subsequent players. This will both bring leading countries billions in revenue, create new jobs, and offer leadership opportunities in technological innovation, as was the case when the 2/3/4G networks appeared.

## 5G architectural risks

The main feature of 5G (unlike 1/2/3/4G) is that it is more of a software than a hardware platform. The equipment used in traditional mobile communication networks has been replaced with software entities operating in data centers on standard servers and virtual machines. In addition to virtual machines, software containers and the software architecture of microservices will be used to implement software functions. It is these architectural features that concern security professionals. All threats to server and software solutions are now becoming relevant for 5G network operators.

## Increased attack surface when infrastructure is compromised

Network slicing is a form of virtualization that allows multiple logical networks to run on top of a shared physical network infrastructure. This approach is used to provide various types of 5G services: web or voice traffic transfer, traffic for augmented reality applications, etc.

Access to such network slices is obtained by companies seeking to provide 5G-based services. Although the address pool is logically isolated, access to it increases the attack surface significantly, which could compromise the entire infrastructure.

APT groups could start using network slicing to conduct BIOS/UEFI-related attacks, side channel attacks, or supply chain attacks. The goals of state-sponsored hackers are likely to be espionage or sabotage in order to undermine trust in a competitor's solution.

## Investigations into 5G vulnerabilities

New challenges and security issues linked to 5G networks are worrying experts worldwide. In the past year, several studies on this topic have been published:

- In November 2018, a team of researchers from Switzerland, France, and the United Kingdom raised concerns about the 5G protocol known as Authentication and Key Agreement (AKA).
- In February 2019, a group of university researchers discovered cellular network vulnerabilities that impact both 4G and 5G LTE protocols. According to the paper, the new attack method could allow remote attackers to bypass security protections implemented in 4G and 5G, re-enabling IMSI catching devices (such as "Stingrays") to intercept phone calls and track user location.
- ToRPEDO ("TRacking via Paging mESSAGE DistributiOn) is the most dangerous attack leveraging the cellular paging protocol. It allows remote attackers to verify a victim's coarse-grained location information, inject fabricated paging messages, and mount denial-of-service attacks. ToRPEDO is effective against 4G and 5G LTE protocols.

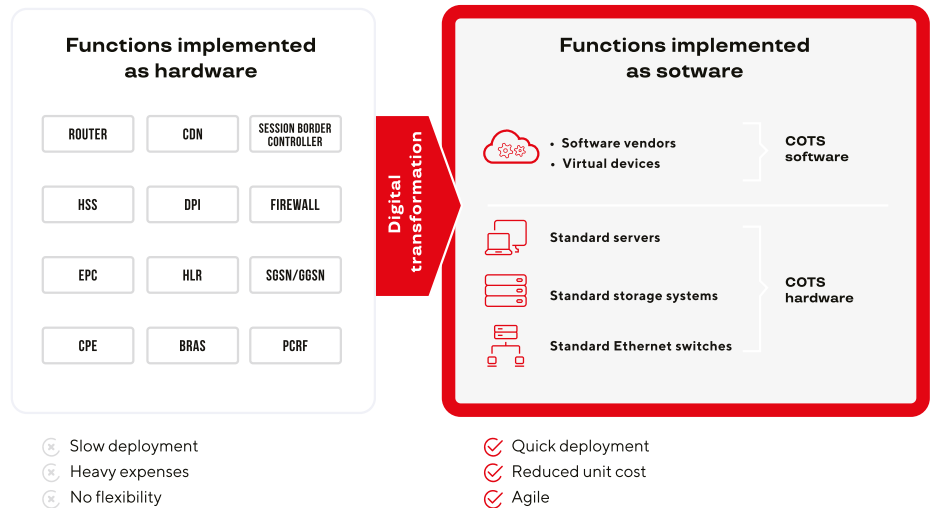
Experts tested ToRPEDO against three Canadian service providers and all US service providers.

- The PIERCER (Persistent Information Exposure by the Core Network) attack allows hackers to link the victim's IMSI to their phone number.

## New scale of traditional threats

Wider adoption of 5G will significantly increase the number of traditional attacks that providers have faced in recent years:

- DDoS attacks will become much more frequent and effective due to the large number of insecure devices and wide bandwidth.
- Proxying is another popular scam method. By turning compromised devices into proxies, hackers can use a large pool of IP addresses to attack. This helps them bypass security systems to carry out web scraping, automated fraud, and traffic cheats. Connecting IoT devices to 5G networks will significantly increase the number of insecure devices that may be used for proxying.
- The spread of malware through hacked devices is a popular practice, which will become more large-scale with the development of 5G networks.



## BGP HIJACKING AND SS7 THREATS

Exploitation of SS7 vulnerabilities for espionage and fraud purposes has long been known and continues to be used. In January 2019, UK-based Metro Bank customers fell victim to a 2FA bypass attack. Hackers exploited a vulnerability in the SS7 protocol to target bank accounts by intercepting text messages used as two-factor authentication.

Several examples of BGP hijacking were listed at the beginning of this report, but there have been many more incidents of this nature.

### Shut down of the "BGP hijack factory" – Portuguese provider Bitcanal

On June 25, 2018, independent security researcher Ronald Guilmette discovered suspicious activity associated with multiple BGP hijacks. The BGP hijacked routes were carried out by the Portuguese provider Bitcanal. When presented with the most recent evidence of hijacks, transit providers immediately disconnected Bitcanal as a customer and deprived it of international transit.

During a BGP hijack, Bitcanal announced subnets belonging to Beijing Jingdong 360 Degree E-commerce. The Portuguese provider's loss of transit also resulted in the disconnection of Routed Solutions (AS39536), presumably Bitcanal's customer or one of its affiliated companies.

### BGP/DNS hijacks targeting the payment systems WorldPay, Datawire, and Vantiv

On July 6, 2018, the provider Digital Wireless Indonesia (AS38146) announced the following prefixes for about 30 minutes:

**64.243.142.0/24 – Savvis,**  
**64.57.150.0/24 – Vantiv, LLC,**  
**64.57.154.0/24 – Vantiv, LLC,**  
**69.46.100.0/24 – Q9 Networks Inc.,**  
**216.220.36.0/24 – Q9 Networks Inc.**

On July 10, 2018, Malaysian operator Extreme Broadband (AS38182) announced the exact same five prefixes listed above for 30 minutes. An hour later, they were announced again for about 15 minutes.

On July 11, 2018, Malaysian operator Extreme Broadband (AS38182) began announcing a new set of prefixes:

**209.235.25.0/24 – Mercury Payment Systems, 63.111.40.0/24 – Mercury Payment Systems, 8.25.204.0/24 – Level 3, 12.130.236.0/24 – CERFnet**

On 12 July 2018, AS38182 began hijacking the same five routes that had been targeted twice previously.

**64.243.142.0/24 – Savvis,**  
**64.57.150.0/24 – Vantiv, LLC,**  
**64.57.154.0/24 – Vantiv, LLC,**  
**69.46.100.0/24 – Q9 Networks Inc.,**  
**216.220.36.0/24 – Q9 Networks Inc.**

This time, the hijack lasted much longer than in the previous cases: the provider announced the prefixes to intercept traffic for almost three hours.

An hour later, AS38182 began hijacking various routes for approximately 10 minutes:

**199.7.68.0/24 – UltraDNS Corporation,**  
**199.7.69.0/24 – UltraDNS Corporation,**  
**204.74.108.0/24 – UltraDNS Corp,**  
**204.74.109.0/24 – Internet Media Network, 204.74.114.0/24 – Internet Media Network, 204.74.115.0/24 – Internet Media Network, 65.118.49.0/24 – CenturyLink**

These Internet routing attacks were presumably designed to redirect traffic directed at payment processors to servers controlled by malicious actors who would then attempt to steal the data. Passive DNS observations between the July 10 and 13 showed \*.datawire.net domains resolving to 45.227.252.17 (AS58271, VSERVER-AS, Panama).

### Multiple cases of traffic misdirection by China Telecom

A joint paper from the U.S. Naval College and Tel Aviv University (Israel) claims that China Telecom, a Chinese telecommunications company, has systematically hijacked Internet traffic for years by exploiting BGP weaknesses.

One example cited by the authors is route diversions between Canadian and South Korean government websites. In 2016, internet traffic was diverted by China Telecom and routed through its PoP (point of presence) in Toronto, then forwarded to its PoP on the West Coast of the United States, followed by China and finally South Korea.

In 2017, China Telecom intercepted traffic between Scandinavia and Japan that crossed the United States and redirected it to a mail server operated by a large Thai financial company. According to the authors, after China Telecom copied the data for encryption breaking and analysis, traffic was delivered to the intended networks within a short time.

### Attack on public DNS servers in Taiwan

On May 15, 2019, researchers reported that BGP routes had been hijacked to intercept traffic going through a public DNS run by the Taiwan Network Information Center (TWNIC). On May 8, 2019, traffic was rerouted to the network belonging to the Brazilian provider Fibra Plus Telecomunicacoes LTDA (AS268869). The incident lasted three and a half minutes. On May 8, the Brazilian provider (AS268869) started advertising the prefix 101.101.101.0/24, which does not belong to it—the move was an attempt to hijack the Quad101 prefix. Quad101 is an experimental Public DNS project run by TWNIC, a ccTLD (country-code Top Level Domain) registry operator.



# ENERGY SECTOR

## state-sponsored groups

In the energy sector, threat actors usually carry out attacks for espionage purposes. Yet in some cases, critical infrastructure facilities were shut down.

<b>3 countries</b> have attack tools and experience: Iran, Russia, and North Korea	<b>Covert players</b> Stuxnet, Dugu, Flame, and the attack on Venezuela confirm that the most dangerous threats have not yet been identified	<b>The Middle East</b> is a testing ground for tools used in attacks on energy organizations from the times of Stuxnet up until now
---	---	--

## ENERGY SECTOR-ORIENTED GROUPS

### HEXANE

In 2018, a new group called HEXANE was discovered. Its members focus on industrial control systems and attack oil and gas companies in the Middle East (mainly Kuwait). The threat actors bypass security tools through trusted vendors by compromising the software and telecommunications networks belonging to their targets.

### LeafMiner

LeafMiner hackers, believed to be based in Iran, use both publicly known tools (such as Inception Framework) and self-developed programs (Trojan. Imecab and Backdoor.Sorgu according to Symantec's classification). The group's main targets are located in the Middle East.

LeafMiner uses watering hole attacks to infiltrate targeted organizations. The threat actors embed malicious links into compromised websites to establish an SMB connection and steal Windows credentials. Based on security analyst observations, LeafMiner does not disrupt ICS when gaining initial access to organizations' credentials.

### Xenotime

In 2018, the hacking group Xenotime also switched to power grids. The group became known for its malware called Triton (aka Trisis), which has been used for attacks on Schneider Electric's Triconex Safety Instrumented System (SIS) controllers.

It was later found that Xenotime had improved its malware and that its new version could be used to attack various industrial safety systems. These are separate safety mechanisms that are activated to help manage industrial processes if they approach unsafe conditions such as over-pressurization, overspeed, or over-heating.

### Lazarus

On September 23, it was reported that the hacking group Lazarus had developed a new set of tools, which were used in attacks on Indian companies between late 2018 and the spring of 2019. The threat actors successfully compromised the account belonging to a senior employee at the headquarters of a nuclear organization in the APAC region.

Although the aforementioned groups were active in the period investigated, two already known groups, BlackEnergy and Dragonfly, should not be overlooked. The hackers redeveloping their tools and techniques for new attacks could explain the lull in their activity.

### The Middle East

is a testing ground for tools used in attacks on energy organizations from the times of Stuxnet up until now

### BlackEnergy

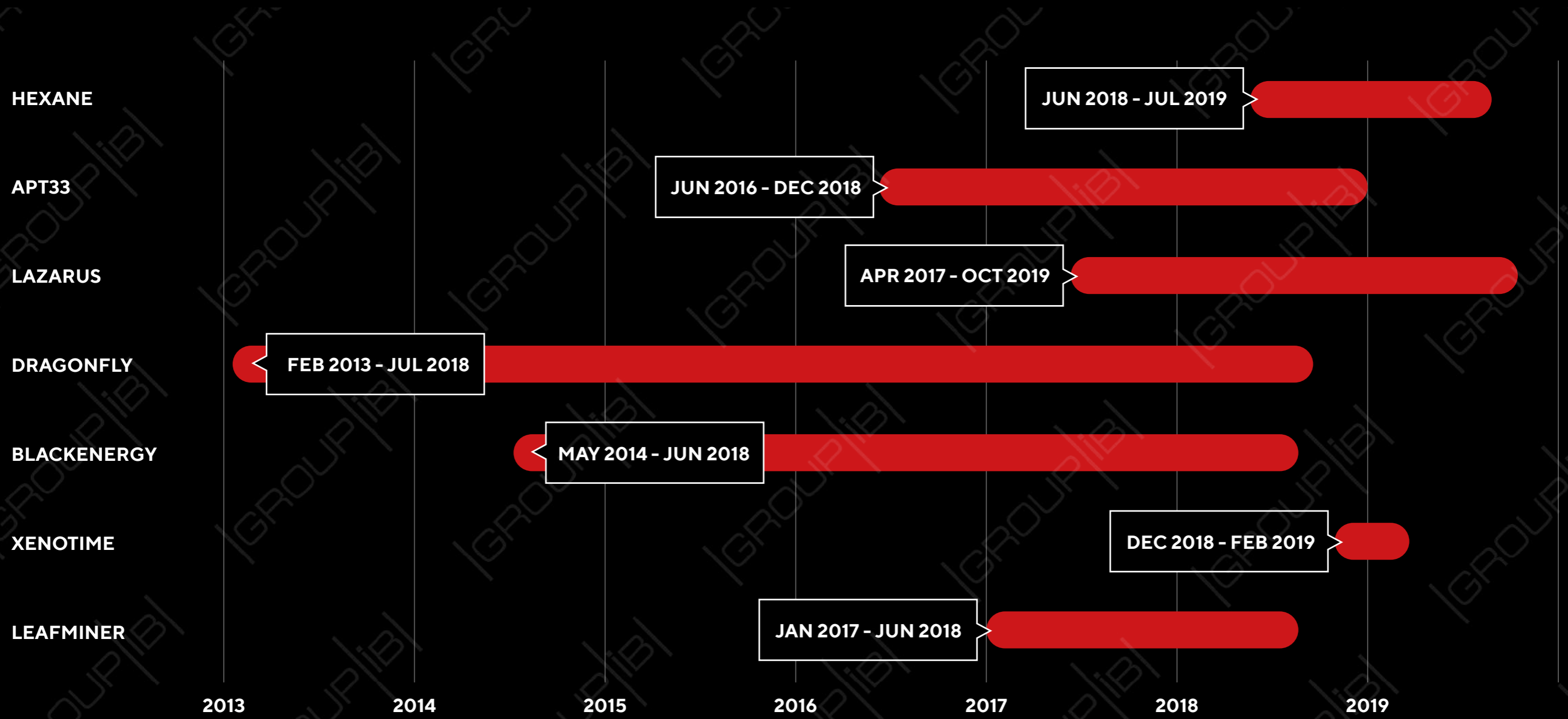
BlackEnergy is one of the most advanced energy sector-oriented groups and has caused disruptions in energy organizations more than once. The group focuses on ICS/SCADA systems worldwide. The most damaging incident occurred in late 2015, when an attack disrupted electric power supply in a region in Ukraine.

Industroyer, also known as CRASHOVERRIDE, remains the main tool used by the hackers. The tool gains control over remote terminal units (RTU) that manage switches and circuit breakers at power grid substations. The group added BadRabbit and VPNFilter to its arsenal in 2017 and 2018, respectively. The latter is designed for attacks on routers and contains a module for detecting SCADA systems.

### Dragonfly

The group Dragonfly, believed to be sponsored by Russia, focuses on collecting data from energy and industrial facilities. The threat actors use phishing emails to attack individual employees and watering hole attacks for larger-scale thefts of corporate credentials. Dragonfly's arsenal also includes tools such as Goodor, DorShel, and Karagany.

# ENERGY SECTOR-ORIENTED GROUPS





# FINANCIAL SECTOR

## targeted attacks

### EVOLUTION OF THREAT GROUPS AND THE APPEARANCE OF A NEW PLAYER

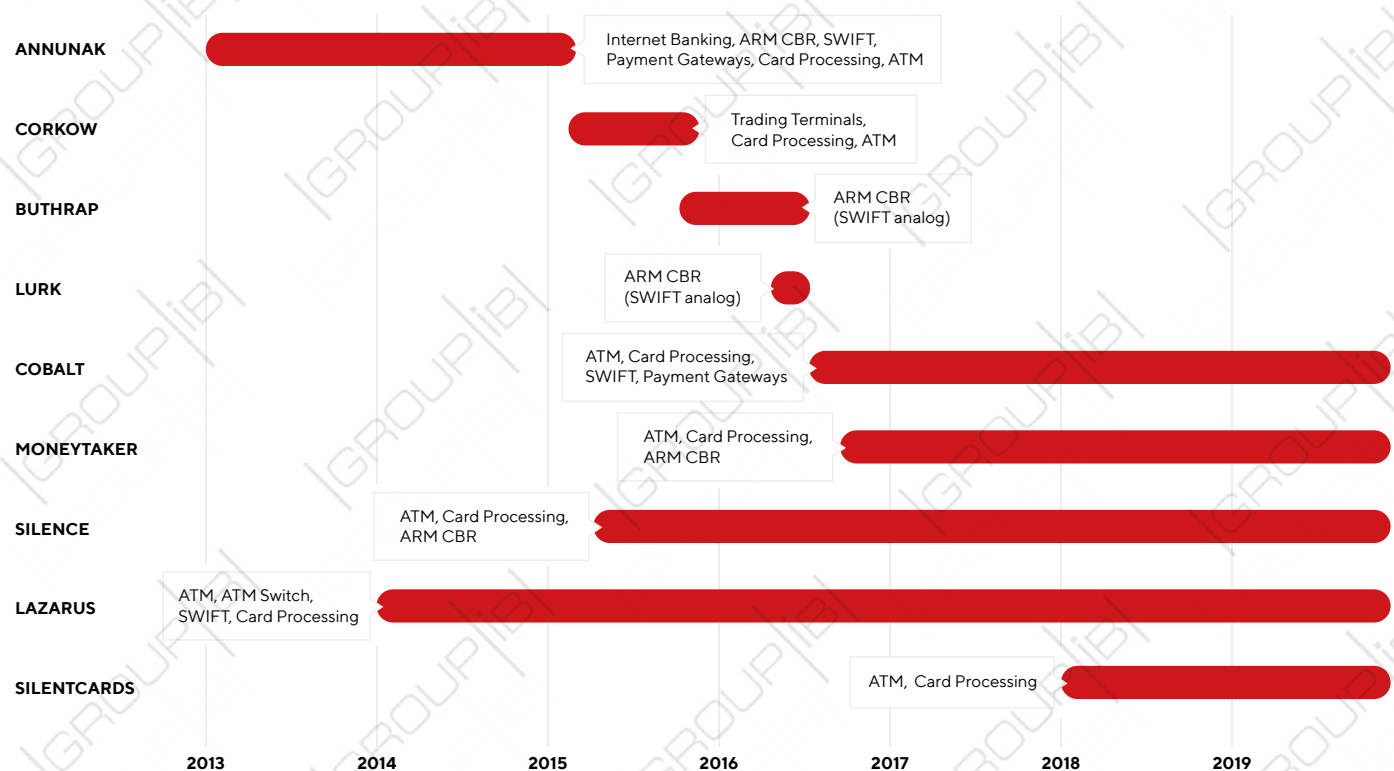
<p><b>5 groups from 3 countries</b></p> <p>conduct targeted attacks on financial organizations</p>	<p><b>3 out of 5 groups</b></p> <p>are Russian speakers and target various regions</p>	<p><b>Lazarus</b></p> <p>uses the most interesting theft and penetration methods</p>
--	--	--

There are currently only five groups that pose a genuine threat to banks worldwide: they use various attack vectors, are able to reach isolated systems, and withdraw money. Nearly every group has a rich background and some companies and media outlets occasionally give these groups new names, but in reality their number does not change. The timeline below shows these hackers' activities in the

banking industry. The timeline does not include groups that engage in sabotage or cyberespionage.

“The Big Three” among hackers are Cobalt, MoneyTaker, and Silence—all Russian speakers. The group SilentCards is from Kenya and was not noticed by security analysts until 2018. As for Lazarus, the group is believed to be sponsored by North Korea.

Before 2018, Russian-speaking groups focused on banks in Russia and other post-Soviet countries, but the trend has changed drastically over the past year. Attackers now mainly target banks and organizations outside the post-Soviet region.



## TIMELINE AND GEOGRAPHICAL SCOPE OF TARGETED ATTACKS ON BANKS FOR 2018-2019

- The names of financial organizations are mentioned only if they have been publicly shared. We deem it unethical to list the names of other victims.
- In the case of Lazarus, the attribution of some attacks may be inaccurate due to a lack of technical details about certain incidents.



## Silence

### Geographical scope

Russia  
The former Soviet Union  
APAC  
The Middle East  
Eastern Europe  
Africa  
Latin America

### Theft methods

ATM trojan (xfs-disp)  
Card processing  
ARM CBR

### Initial infection

Phishing

### Tools

Silence Trojan  
Silence Proxybot  
Atmosphere  
xfs-disp.exe  
Ivoke  
EDA – EmpireDNSAgent  
(Empire+dnscat2)  
PowerMTA  
Farse  
Cleaner  
Metasploit  
Mimikatz  
winexe  
RAdmin

[More information](#) on Silence is available in Group-IB's technical report



### Geographical scope

Silence is one of the most actively developing threat groups at large. When the group first started, it used Russia as a testing ground to prepare for worldwide expansion.

- First half of 2018: main activity and first successful attacks in Russia.
- Fall of 2018: first mass attacks in other countries, mainly in the Middle East and South-East Asia.
- February 2019: activity in Russia drastically declined. Silence shifts their focus to the financial sectors in Bulgaria, India, Bangladesh, Chile, Costa Rica and Ghana.
- Forecast for the second half of 2019 and 2020: the group may significantly expand the geographical scope of their attacks by working together with other threat actors. In particular, Group-IB's incident response operations in a number of banks revealed that Silence has already started paying another hacking group (TA505) for installing its Trojan in banks.

### Theft method

Silence's recent targets were ATMs, on which the group installed a new version of an ATM Trojan and gained remote access to the machine's dispenser.

It is worth noting that the threat actors have experience in stealing money through bank card management systems, which may have been successfully applied during the attack on the Dutch-Bangla Bank and banks in Russia before that.

### Penetration method

The group's only method of breaching a bank's security lies in carefully prepared, but not targeted, phishing emails. The preliminary stage of a Silence attack is characterized by "recon" emails without any malicious content. This helps create an up-to-date list of email addresses and find out what cybersecurity solutions the targeted organization uses. Phishing emails with a malicious payload are then sent to the updated list of email addresses.

In mid-2019, Silence purchased access to banks from TA505. Group-IB confirmed this fact while conducting an incident response operation in a Bulgarian bank. Silence will most likely abandon mail-outs and continue using the services of other threat groups.

### Tools

The main tool Silence uses is their own framework, named Silence after the group. In late 2018, the hackers revamped their loader called Ivoke, which:

- became fileless (written in PowerShell);
- learned how to bypass detection solutions more effectively;
- started to collect data on targeted systems more actively to help make decisions on whether it is worth pursuing the attack;
- had commands pointing to Russian words deleted;
- was fitted with a new feature for transferring files from the infected system to the C&C server;
- had the protocol for communicating with the C&C server changed

The group continues to use Silence.Proxy to proxy traffic. In addition, the threat actors employ other remote control tools, such as DarkVNC and a modified version of AmmyAdmin, which has been dubbed FlawedAmmy. This is a full-fledged remote access Trojan (RAT), which enables the threat actors to gain administrative control over infected devices in order to monitor user activity, profile the system, and steal credentials. Silence is not the only group that uses FlawedAmmy. In particular, hackers from TA505 have used it in recent attacks.

In the past, Silence used only its own unique Trojan called Atmosphere. In 2019, however, the group started using new malware. After successfully testing it on IT Bank (Russia), the new tool was presumably used for theft at Dutch-Bangla Bank (Bangladesh).

## Cobalt

### Geographical scope

Russia  
Kazakhstan  
Georgia  
Europe  
India  
Greece

### Theft methods

ATM trojan  
Card processing  
Payment gateways  
SWIFT  
Local Interbanking systems

### Initial infection

Phishing  
Supply chain  
Driveby

### Tools

CobInt  
JS-backdoor  
SSH-backdoor  
Cobalt Strike  
alexusMailer  
SoftPerfect Network Scanner  
Eternal Blues  
EternalPunch  
Radmin  
AmmyAdmin  
TeamViewer  
RPIVOT  
Mimikatz  
PetrWrap  
InfoStealer v. 0.2



[More information](#)  
on Cobalt is  
available in  
Group-IB's  
technical report

### Geographical scope

Cobalt's last successful theft in Russia was observed in November 2018. It was not until July 2019 that the group resumed their attempts to breach Russian banks. In the meantime, the threat actors focused on other countries. They sent out phishing emails disguised as messages from the European Banking Federation, Diebold Nixdorf, the Interkassa e-payment system, SEPA Europe, and SWIFT.

It is worth highlighting the mail-outs purporting to be from banks in Europe, Greece, India, and Kazakhstan: they were sent from the mail servers belonging to the targeted organizations, which suggests that either the banks or employee email accounts had been compromised.

Despite the mail-outs and other traces of activity, there is no publicly available information about thefts that Cobalt committed outside Russia. This indicates that there are no informatory procedures in place in the regions attacked rather than that there are no attacks.

### Penetration method

To breach infrastructures, Cobalt engages in phishing by posing as banks, financial organizations, and their partners. After successfully attacking a bank, the threat actors sometimes continue using the access they gained to send phishing emails under the victim's name and from the entity's mail servers.

In October 2018, Group-IB detected an attack carried out from the subdomains of a governmental portal in Russia, which redirected users to servers using the RIG Exploit Kit. As a result, CobaltStrike Beacon was installed on the victim's computer. It was later established that this attack resulted in a theft from a bank in a post-Soviet country.

In January 2019, Cobalt started using a new scheme to spread their malware. The group sent emails using free email services and posing as individuals who are well known in financial circles.

Another important email-related change was higher quality. Earlier texts were poorly phrased and had no decoy documents attached, but during recent attacks the emails looked much more trustworthy and the malicious attachments contained clever baits.

### Theft method

In 2018, the threat group used various theft methods: SWIFT, local interbank transfer systems, card processing, and the payment gateways of instant money transfer systems. Interestingly, only Cobalt has experience in using payment gateways for theft, which they only did in Russia.

### Tools

First, the targeted company is infected with the modular backdoor CobInt. It launches other modules that collect system information and download and launch the main tool for developing the attack further. Its main tool is still Cobalt Strike, which the group has been using since it started its activity.

Another tool that Cobalt has been using is a JS backdoor that downloads and launches PE files and executes scripts. As for Cobalt's Trojans for Windows, Linux, and ATMs, they were not used in the period investigated.



## MoneyTaker

### Geographical scope

Russia

### Theft methods

ATM trojan  
ARM CBR

### Initial infection

Phishing  
Network vulnerability  
Supply chain

### Tools

Metasploit  
ATM trojan  
MTHole.VBE  
VNC  
Mimikatz  
MBR Killer



[More information](#) on MoneyTaker is available in Group-IB's full technical report

### Geographical scope

In 2018 and 2019, MoneyTaker was observed to be active only in Russia. Initially, its activity had been detected due to their attacks in the US. At the time, the group had remained unnoticed for many years.

### Penetration method

MoneyTaker uses three main methods for penetrating networks:

1. Vulnerable network equipment.  
Once the threat actors gain access to it, they use a VPN to add their server to the bank's local network and develop the attack further using that server. This vector is very difficult to detect, which is why it took experts a long time to determine how exactly MoneyTaker penetrated networks.
2. Access to a trusted partner's networks by brute forcing the passwords of local administrators, with further attack development.
3. Phishing emails purporting to be from banks and financial regulators.

### Theft method

MoneyTaker steals money through the Russian interbank transfer system or ATMs using a self-developed ATM Trojan, which was created in 2018 and designed to remotely control ATM dispensers. The threat actors grew more cautious with the former method; they abandoned automation tools and now carry out transactions manually instead.

### Tools

Metasploit remains MoneyTaker's main tool; the group has been using it since the beginning. The threat actors also employ another popular framework called PowerSploit, as well as Radmin for remote control and a self-developed ATM Trojan for theft from ATMs.

## SilentCards

### Geographical scope

Kenya

### Theft methods

Card processing

### Initial infection

—

### Tools

Metasploit  
Battlefield  
Mimikatz  
Pylogger  
Kitho Backdoor  
MTRReverseTCP Stager

### Geographical scope

SilentCards is a new local threat group based in Kenya. So far, it has attacked targets in its own country only. The group has been involved in two known successful thefts.

### Penetration method

We do not have accurate information about the attack methods and vectors that the group uses to penetrate networks. Neither phishing emails nor malicious documents that could have been used to deliver the payload have been discovered. However, some malicious file samples were configured to work with C&C servers on the local network. Based on this data, we can assume that the hackers already have a controlled device within the organization that allows them to attack the corporate network. This could be either a corporate computer or a device brought from outside.

### Theft method

The threat actors withdraw money through card processing: they gain access to bank card management systems, change card limits, and withdraw cash from ATMs using cards they obtained in advance.

### Tools

SilentCards uses self-developed tools, Metasploit, and various PowerShell scripts to automate certain tasks during attacks. The group's own tools include:

- keylogger, which sends the results of its activity to an FTP server or email address;
- battlefield: a shell written in Python and packed in .exe using py2exe. Its capabilities include a remote command shell, creating and saving screenshots to a local disk, and downloading files from an arbitrary URL.

## Lazarus

### Geographical scope

Europe  
APAC  
Latam  
MiddleEast

### Theft methods

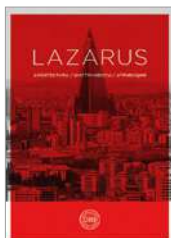
SWIFT  
Local Interbanking systems  
ATM Switch

### Initial infection

Phishing  
Network vulnerability  
Supply chain

### Tools

Ratankba  
PowerRatankba  
ClientRAT (aka FALLCHILL aka Manuscript)  
ClientTrafficForwarder (Proxy)  
AppleJeus  
PowerTask  
PowershellRAT  
Banswift/BBSwift  
FastCash  
RatankbaPOS  
Mimikatz  
Metasploit  
Cobalt Strike  
Dtrack



[More information](#) on Lazarus is available in Group-IB's full technical report

### Geographical scope

Lazarus has always been mainly focused on the Asia-Pacific region. Its attack on Polish banks in 2017 seemed more like an exception rather than the rule.

However, in October 2018, HSBC detected an attack on its Maltese office carried out by an unidentified threat actor that was named EmpireMonkey. In February 2019, €13 million was stolen from Bank of Valletta, a Maltese bank.

Group-IB attributes the attacks on Maltese banks to Lazarus, which could indicate the group's renewed interest in European companies.

### Penetration method

Lazarus uses various vectors and sophisticated tools to breach banks:

- Spear phishing, which is used for targeting a very small group of recipients.
- Watering hole: By gaining access to the websites of financial regulators, Lazarus attacks the website's visitors. The malicious code is loaded only if the visitor comes from a specific pool of IP addresses.
- Social engineering: The threat actors identify the most suitable employee on social media and offer them a job; the employee is prompted to download and install a malicious program at their workplace.

### Theft method

The main method Lazarus uses in attacks on financial organizations is SWIFT. The group has also presumably been using ATM Switch to withdraw money since 2016, with two such thefts in India in Chile reported in 2018.

### Tools

The threat actors continue to use their loader (known as Ratankba) for the first stage of attack. The loader's first PowerShell modification was released in 2017, and in 2019 security experts discovered its updated version. To attack Apple users, Lazarus created a loader that has been named AppleJeus.

In late 2018, Client\_RAT (aka FALLCHILL, Manuscript), the group's main Trojan, was also rewritten in PowerShell. Its functionality is identical to that of the previous version, but it is much more difficult to detect.

To proxy traffic, the group uses its own proxy bot called ClientTrafficForwarder, but also employs the well-known Metasploit and Cobalt Strike frameworks during attacks, which makes it more difficult to attribute the attack to a specific group.

The threat actors carry out thefts through ATM Switch using their own unique malware called Fastcash.

# THEFT THROUGH SWIFT



## CURRENT THREATS

Most thefts through SWIFT occurred in the second half of 2017 and the first half of 2018, which was followed by a lull. Over the period investigated, the attackers carried out only two successful thefts from banks in India and Malta, with the overall sum stolen amounting to \$16 million.

Only two groups, Lazarus and Cobalt, have successfully stolen money through SWIFT. As such, when the incident in Malta could not be attributed to either, some cybersecurity specialists suggested that there was a “new” group called EmpireMonkey. The second incident

attributed to this group was an attack on HSBC’s Maltese office, which was successfully halted. Group-IB believes that the group behind these attacks is Lazarus.

In as early as 2017, Lazarus tried to attack banks in Europe by using the watering hole penetration method. Apart from Poland, the threat actors compromised the websites of financial regulators in Mexico and Uruguay. Security specialists managed to locate a configuration file that specified the subnets of banks in which Lazarus was interested. The file listed the subnets

of Mexican banks, Banco de Chile, and the Turkish bank Akbank, which all fell victim to a successful theft a year later, and also the HSBC subnets that were allegedly attacked by “EmpireMonkey”.

This shows that, despite fewer thefts through SWIFT overall, this attack vector remains relevant. Moreover, new tools designed for these types of attack may emerge.

## FORECAST: THE APPEARANCE OF POWERSHELL-WRITTEN BANSWIFT/BBSWIFT

In 2016, during the well-known attack on the central bank of Bangladesh, Lazarus used a special program called Banswift/BBSwift. It allowed the hackers to track transactions, modify databases, and block the printing of SWIFT documents.

During all subsequent incidents, the group abandoned these types of automation tools and carried out theft operations manually. The attackers compromised the workstations of operators who had legitimate access to the SWIFT interface. To withdraw money, the threat actors used the MT103 Serial or MT103 Cover messages.

Over the past year, Lazarus has significantly improved its tools, mainly by redeveloping them using PowerShell. The group might use an equivalent of Banswift/BBSwift written in PowerShell in future thefts.

## THEFT THROUGH ATM SWITCH

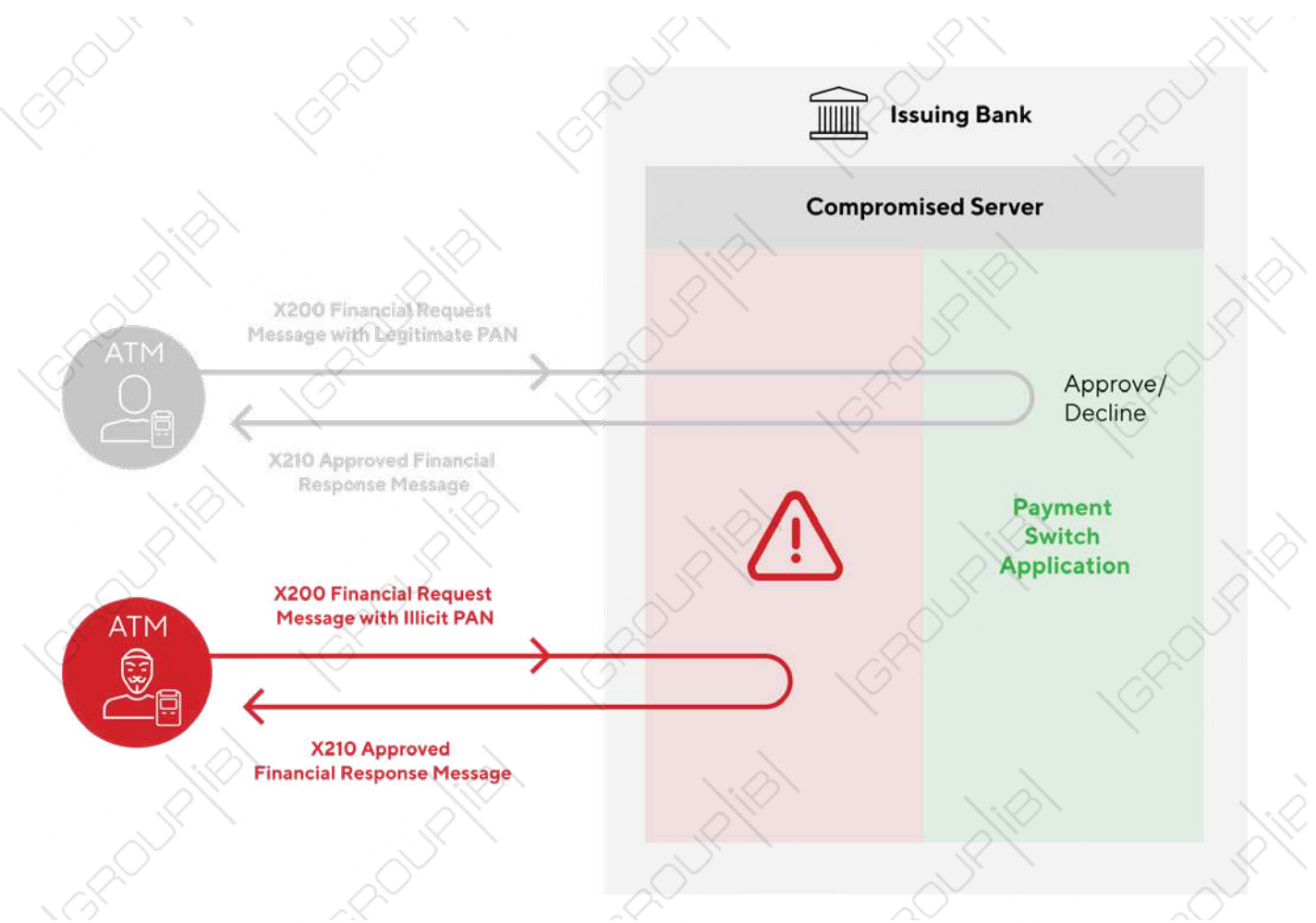
In 2018, Lazarus attacked Cosmos Bank, an Indian bank, which resulted in a two-step money withdrawal process:

- \$11 million was withdrawn from banking customer accounts with the help of third-party individuals using forged bank cards in ATMs. Nearly 15,000 such transactions were carried out in 28 countries in just seven hours. Another \$400,000 was cashed out in ATMs using fake cards in India only.
- \$2 million was transferred through SWIFT from the bank's accounts to fraudulent accounts in Hong Kong the next day.

The method used by the threat actors at the first stage of attack was named FastCash. The scheme seems simple but is difficult to implement:

- Obtain access to a bank's network.
- Find Switch application servers for handling ATM transactions—ATM Switch, which runs on the AIX operating system by IBM (similar to UNIX).
- Compromise these servers and upload a command-line utility to add the threat actor's malicious library to a running process.

Usually, requests from ATMs are received by an application server, which runs checks in the bank's systems to determine whether to approve a money withdrawal. The malicious code intercepted these requests and substituted responses to approve the money withdrawal.



### The attack described above was far from the only one:

- Some of the malicious files related to the Cosmos Bank incident were compiled in 2016.
- After the incident, a customer informed Group-IB that their bank in Asia had been attacked in the same way in as early as 2016.
- In 2017, US-CERT reported that a similar method had been used to steal money through ATMs in 30 countries. The announcement was likely related to a 2015 incident when Lazarus attacked an ATM operator in South Korea and had access to their network and ATMs until February 2017.
- In addition to Cosmos Bank, 2018 saw a similar technique being successfully used to steal money through Redbanc, a Chilean interbank network.



## LOGICAL ATTACKS ON ATMS

As mentioned earlier, three out of five active groups possess ATM Trojans, namely Cobalt, Silence, and MoneyTaker. However, over the period investigated, only Silence conducted successful attacks on ATMs.

The group had previously used their own Trojan called Atmosphere, but in February 2019 they employed a new Trojan in an attack in Russia. The malware's code indicated that it was designed for theft in dollars.

Three months later, Silence successfully robbed Dutch-Bangla Bank Limited (DBBL), a Bangladeshi bank, presumably using the new Trojan they had tested in Russia. Soon thereafter, six Ukrainians who had withdrawn the money from ATMs were arrested.

```
qmncpy(v141, "USD BUSD", 8);
v143 = 5;
v144 = 1000;
v145 = 1000;
v158 = &windowName;
strcpy(v159, "USD CUSD\n");
v161 = 1000;
v162 = 1000;
v175 = &windowName;
qmncpy(v176, "USD DUSD", 8);
v178 = 20;
v179 = 1000;
v180 = 1000;
snprintf(&v1[1], 3u, "USD");
snprintf(v123, 5u, "USD A");
snprintf(&v142[1], 3u, "USD");
snprintf(v141, 5u, "USD B");
snprintf(&v160[1], 3u, "USD");
snprintf(v159, 5u, "USD C");
snprintf(&v177[1], 3u, "USD");
snprintf(v176, 5u, "USD D");
v6 = &v84;
v7 = &v102;
v8 = &v120;
v9 = &v138;
v10 = &v156;
v11 = &v173;
v198 = '\x06\0\0';
v199 = (int *)&v6;
v3 = WFSExecute(v1, 312, &v198, 60000, &v206); // WFS_CMD_CDM_END_EXCHANGE
```



In addition to the confirmed attack on DBBL, Silence attempted to steal money from two other banks (NCC Bank and Prime Bank). The banks said that financial losses had been prevented, however.

Silence's new Trojan scans all running processes for "msxfs.dll" and injects code into the process where the .dll file is detected. The injected code

enumerates all threads in the application and freezes some of them, likely those belonging to the "msxfs.dll" module. Instead of using regular XFS API with the constants WFS\_CMD\_CDM\_DENOMINATE and WFS\_CMD\_CDM\_DISPENSE, money is withdrawn using WFS\_CMD\_CDM\_START\_EXCHANGE and WFS\_CMD\_CDM\_END\_EXCHANGE sequentially.

In May 2018, MoneyTaker successfully tested their unique Trojan for ATMs in Russia, but no other incidents followed. Unlike Silence, MoneyTaker's ATM Trojan can interact with the dispenser specifically through XFS API.

## THEFT THROUGH CARD PROCESSING

### Stages of card processing attacks:

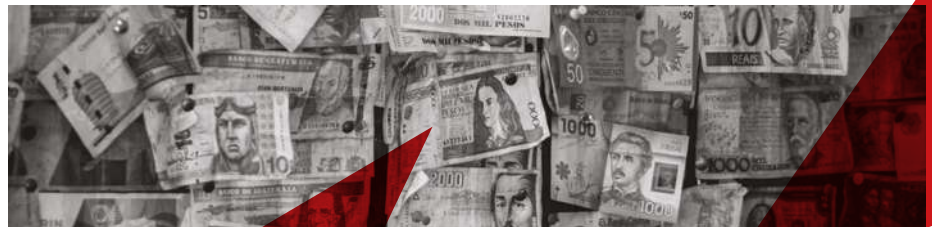
- Gain control over a bank's network.
- Check whether it is possible to connect to the card processing system.
- Issue or buy cards for the banks where access has been established.
- Train money mules who will travel to another country with these cards.
- Remove or increase the cash withdrawal limit.
- Remove overdraft limits to withdraw cash when the balance is below zero, even for debit cards.
- Withdraw money on command from various ATMs thanks to the mules.

At different stages of their evolution, Cobalt, MoneyTaker, and Silence carried out attacks on card processing systems. Only Silence continued to use this method over the period investigated, but a new group with a similar-sounding name appeared: SilentCards.

Silence conducted their first card processing attack in March 2018 and managed to steal \$549,000 from a Russian bank. Analysis of publicly available information about incidents in India related to Dutch-Bangla Bank Limited, NCC Banks, and Prime Bank revealed that the money was withdrawn from ATMs in Russia, Ukraine, and Cyprus. This scheme could only

be possible if the attackers had gained access to the card processing systems and had been in possession of several cards issued by these banks. This scheme is completely safe for the mules, who can withdraw money in a different country until the cards are blocked or until they run out of ATMs with money.

In 2018, researchers detected an incident that has been linked to the group SilentCards. The hackers gained access to a card processing system and successfully transferred 400 million Kenyan shillings by penetrating the corporate network and infiltrating the key servers responsible for money transfers.



# NON-TARGETED ATTACKS

## and threats to banking customers

In recent years, threat actors have been gradually abandoning banking Trojans, attacks on banking customers have become increasingly simpler from a technical point of view, and each direct theft has caused less damage.

However, because financial data is easy to compromise, such incidents have become significantly more frequent. In 2019, JS sniffers made carding one of the fastest-growing threats to online banking customers.

### COMMON CARDING TRENDS

In recent years, the market for collecting bank card data has continued to grow. It can be divided into two segments: textual data (card number, expiration date, cardholder name, address, CVV) and dumps (magnetic stripe data).

Dumps are collected using skimming devices and Trojans for computers

that are connected to POS terminals. To obtain textual data, hackers use phishing websites; banking Trojans for PC, Android, and ATMs; and JS sniffers (malicious code incorporated into the websites of online stores or other portals where users enter their card payment details). JS sniffers are the main discovery

this year and security experts note a clear trend of their increasing popularity.

Over the period investigated, the number of compromised cards grew from 27.1 million to 43.8 million. The average price for textual data increased from \$9 to \$14, while the average price for a dump fell from \$33 to \$22.

Year	2019			2018		
	Textual data	Dumps	Total	Textual data	Dumps	Total
Total number	12,540,190	31,213,941	43,754,131	10,218,489	16,927,777	27,146,266
Market size	\$179,159,552	\$700,520,520	\$879,680,072	\$95,590,424	\$567,791,443	\$663,381,867
Minimum price	\$0.70	\$0.50		\$0.75	\$0.50	
Maximum price	\$150	\$500		\$99.99	\$295	
Average price	\$14.29	\$22.44		\$9.35	\$33.54	
Median	\$13	\$12		\$8	\$25	

### EVOLUTION OF POS THREATS

Bank card dumps make up about 80% of the carding market. Over the period investigated, cybersecurity specialists detected 31.2 million dumps put up for sale, i.e. 46% more than last year.

The main method of compromising magnetic stripe data is infecting computers connected to POS terminals with special Trojans that collect bank card information from RAM.

In the past year, cybersecurity specialists detected four new POS Trojans, which had been actively used in attacks but remained unnoticed. The source codes of most programs known previously (Alina, MajikPos, FrameworkPOS) have long been shared on hacker forums and could be used by anyone.



#### New Trojans

- DMSniff
- Glitch
- Badhatch
- RtPOS

#### Old but still active Trojans

- FrameworkPOS
- MajikPos
- TinyPOS
- UdPOS
- Alina

A total of 17 major data leaks—14 identified and three yet unlinked to any company—occurred between March 2018 and June 2019. The descriptions of the databases found on card shops mention that much more

compromised data is available than what has been put up for sale. When evaluating this market, Group-IB experts only took into account the data that has been put up for sale; the actual volume of dumps could be even bigger. There

are 3.6 million such cards in total, which accounts for 11% of their overall number. The rest of the data is posted in small batches, which makes it more difficult to link it to major leaks.

Date	Compromised company	Database names on card shops	Number of cards	Group
March 2018	Applebees in Ohio	BOSSA, NAIFESI, HYTIRI, EXCIRA, PEGASUS, GAZZE, ZYLLA, COSMOS, TRENZO, SABBIA, WYREX, GIRLIX, FANTASI, MCUSTA, FURRI, SIMINDI, TEGRITY, GAZZAK, VELTEX, FIERCE, HISAIS, BAVATA, HAXTI, BAZO, ZERCO, TIGGI, LYZYN, MUAZA, FIREFEX, SERPENTA, SECARMA	121 987	-
March 2018	Zippy's Restaurants	-	-	-
April 2018	Saks Fifth Avenue and Lord & Taylor Stores	BIGBADABOOM-02	1 094 232	Fin7
May 2018	Chilis	ZIPPO	1 582 565	Fin7
June 2018	PDQ	-	-	-
July 2018	-	ARABIAN-NIGHTS	603 828	-
August 2018	Cheddar's Scratch Kitchen	-	567 000	-
August 2018	Burgerville	-	-	Fin7
September 2018	-	FIERYRAIN	1 225 311	-
October 2018	Taco Bueno	-	-	-
November 2018	Caribou Coffee	-	-	-
December 2018	-	BADASS-SANTA	184 927	-
January 2019	Huddle House	-	-	-
January 2019	Nerth Country (NCBP)	-	-	-
March 2019	Earl Enterprise (Buca di Beppo, Earl of Sandwich, Planet Hollywood)	DAVINCI	883 290	-
May 2019	Checkers and Rally's	-	-	-
June 2019	Cotton Patch Cafe	BLACKSPIDER, BENEDICT, INTUITION, PERMANENT, ROOTDIRECTORY, VITAMIN	113 500	-



## Difficulties in attributing major leaks

When dumps are identified, almost no technical details are available, which makes the attribution process difficult and only allows for assumptions about who might be responsible for a particular leak.

In the case of FIN7, the attackers were identified either when an attacked company named that group specifically or when company names were published in indictments as part of investigations.

When it comes to major leaks, we can only guess the possible links between

response operations to particular incidents and the publication of technical descriptions of new Trojans without company names being mentioned. For instance:

- In August 2018, it was reported that Cheddar’s Scratch Kitchen experienced a data breach. Later that month, information about a Trojan called RtPOS was first published.
- In March 2019, a response operation to the incident at Earl Enterprise (Buca di Beppo, Earl of Sandwich, Planet Hollywood) started; in the same month, information about two new POS Trojans (GlitchPOS and DMSniff) appeared.

- In June 2019, a month after the response to the Cotton Patch Cafe incident, news emerged about the Badhatch Trojan, which was linked to FIN8.

## Geographical scope of dump sources

The main targets for attackers are fast food restaurants in the US. The country comes first in terms of the number of compromised cards—close to 93% of all dumps. This year, the US is followed by Middle Eastern countries (Kuwait, Pakistan, the UAE, and Qatar), which together account for 2.38%.

Country	Number of dumps	Percentage (%)
US	29,121,383	93,30
Kuwait	359,037	1,15
Pakistan	261,901	0,76
UK	238,186	0,47
Canada	145,366	0,47
China	119,807	0,38
Brazil	95,344	0,31
UAE	87,447	0,28
Republic of Korea	64,946	0,21
Qatar	59,364	0,19
Other countries	661,178	2,12

## Possible reasons for the Middle Eastern anomaly

Thanks to proprietary infrastructure for monitoring underground forums and card shops, Group-IB sees the full picture of the carding market and detects anomalies therein. In the period investigated, there was an unusual rise in the number of compromised Pakistani bank cards, which almost no one sold before October 2018.

On October 26, a database containing 10,467 dumps was put up for sale, with 8,704 of them belonging to Pakistani banks, including BankIslami. Two days later, BankIslami announced that on October 27, attackers withdrew about \$2.6 million from the bank’s accounts.

After the news was shared, another two databases with Pakistani bank data were published:

- October 31, 2018 – 11,795 dumps;
- November 13, 2018 – 177,878 dumps.

A total of 150,632 dumps of Pakistani cards were put up for sale. This was only the first wave, however.

On January 24, a small-scale database appeared with 1,535 dumps; 96% of the cards in it had been issued by the Pakistani bank Meezan Bank Ltd. On January 30, a large database of 67,654 dumps emerged.

What distinguished this database from previous ones was that it contained PIN codes. Obtaining dumps with PIN codes usually requires hardware

skimming equipment, but the amount of data collected that way is always small. Another option is to compromise a bank that does not comply with international security requirements and stores PIN code information.

On January 16, a file called “ApplicationPDF.exe” was uploaded to VirusTotal from Pakistan. The file is a malicious program created by the threat group Lazarus, which the threat actors send to bank employees after interacting with them on social media. A similar program was used for gaining access during the attack on Redbanc, a Chilean interbank network. The file uploaded to VirusTotal was compiled on October 31, 2018 and cannot be linked to the 2018 leaks, but it can explain the incidents in 2019.

# NEW TREND: JS SNIFFERS

JS sniffers are one of the most effective methods of compromising bank cards. A sniffer is a type of malicious code that threat actors incorporate into their victims' websites to intercept data entered by users, such as bank card numbers, names, addresses, logins, and passwords. Threat actors sell the payment data they obtain or use it themselves to buy valuable goods.

RiskIQ, together with Flashpoint, were the first to analyze the activities of threat actors that use sniffers. They singled

out 12 groups and gave them a common name: MageCart. Group-IB analyzed the discovered sniffers, and—by applying proprietary analytical systems—exposed the entire infrastructure and gained access to the threat actors' source codes and tools. This approach helped detect at least 38 different sniffer families as at spring 2019. At the time of publishing this report, that number has grown.

Each sniffer family has unique characteristics and is most likely managed by different individuals. As all sniffers have similar functionalities, it is not practical for the same threat group to create two different sniffers.

## List of JS-sniffer families analyzed in this report: 15 out of 38 discovered by Group-IB team

TokenLogin	March 2016	Illum	End of 2016	MagentoName	December 2017
TokenMSN	Mid 2016	WebRank	End of 2016	ImageID	End of 2017
G-Analytics	September 2016	ReactGet	June 2017	GetBilling	Start of 2018
PreMage	November 2016	PostEval	Mid 2017	Qoogle	April 2018
FakeCDN	November 2016	CoffeMokko	September 2017	GMO	May 2018

## How sniffers work

Step 1: Gain access to a website

- Option 1 – Gain access to the administrator panel by using password-stealing malware.
- Option 2 – Search for vulnerable websites (exploits of popular CMSs; known vulnerabilities of service providers). By using exploits, threat actors load a web shell, gain access to a website, and modify its files.
- Option 3 – Purchase access to a website from another threat group.

Step 2: Acquire a JS sniffer

- Option 1 – Develop a JS sniffer.
- Option 2 – Buy or rent a ready-made solution on an underground forum.

Step 3: Install a sniffer

Installed via a control panel or web shell, a JS sniffer collects data and sends it to a host managed by the threat actor. Some sniffers use techniques that allow them to remain unnoticed during manual checks:

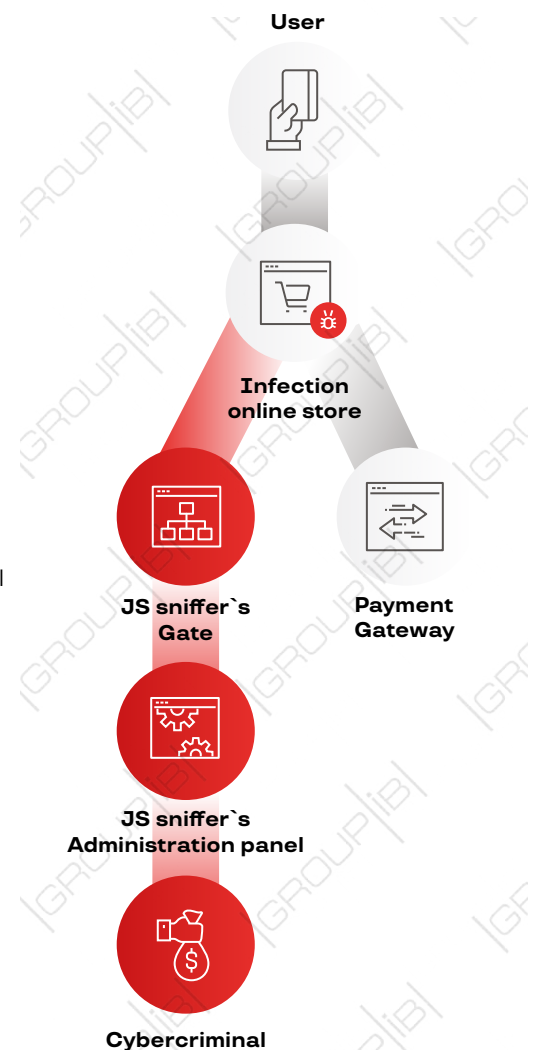
- Add it to a legitimate script library.
- Suspend JS sniffer activity when the developer console is being used (e.g. Chrome DevTools or Firefox Browser Toolbox).

Step 4: Monetization

- Option 1: Sell data to carders for \$1–\$5 per card. This is the easiest method as only the contact details of verified buyers are needed.
- Option 2: Use stolen cards to purchase easily re-sellable goods, such as gadgets, electronics, home appliances, interior items, clothes, and shoes.

Collected payment and the victim's personal data are sent to the threat actors' server (a gate). To make it more complicated to detect the threat actors' server, the JS sniffer chain uses many levels of gates located on different servers or hacked websites. In some cases, however, the admin panel is located on the same host as the gate that is used for collecting stolen data.

The threat actor's end server for tracking JS sniffer activity and exporting stolen data can be either a full-feature administrator panel or a server for hosting database administration tools. For example, administrator panel features can be performed by tools such as Adminer or phpMyAdmin.



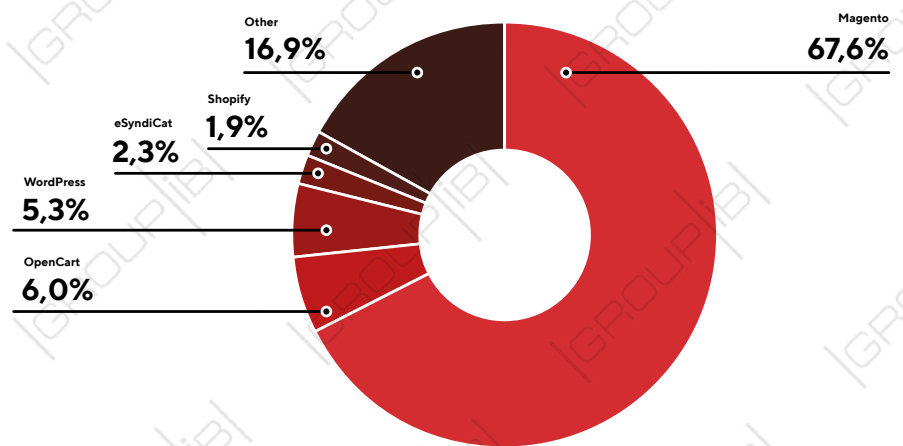
## Infection methods

Threat actors use various methods to infect websites and inject malicious code.

## Exploitation of CMS vulnerabilities

Malicious code can be injected into the code of online store websites by exploiting vulnerabilities in CMSs developed specifically for online stores—Magento, OpenCart, and others.

- Loading a web shell on a website by exploiting a vulnerability, with subsequent changes to the website files.
- Injecting the JS sniffer code by exploiting a vulnerability that allows malicious code to be added to one of the site code blocks (e.g. a footer).



## Hacking of a website's administrator panel

JS sniffers can be installed by obtaining access to a website's administrator panel with permission to edit files. The login and password can be compromised through several methods:

- stealers, i.e. programs that extract passwords saved in browsers;
- malware for intercepting entered data (including logins and passwords);
- brute force.

## Hacking of third-party services

A sniffer can infiltrate a website through hacked third-party services, whose scripts work on the target website:

- Hacking websites that provide services for online stores (customer support chats or analytics and statistics systems). By injecting malicious code into the service script code, a JS sniffer infiltrates the code of online store websites.
- Hacking the accounts of CDN services, with the ability to modify scripts loaded from CDN to target websites.

## Supply chain attacks

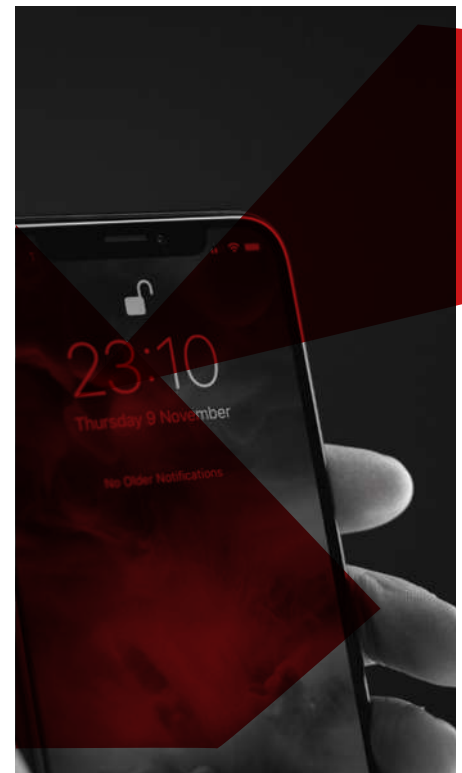
The threat group that used the WebRank JS sniffer family often carried out attacks on third-party sites that provided various services for other websites. For example, by hacking into a web analytics system,

the threat actors injected the JS sniffer code into the web analytics script. The script, which is loaded by many sites, would load a bank card JS sniffer along with itself.

This type of malware delivery can result in rival sniffer families being hacked. For instance, during one wave of infections, the operators of the WebRank sniffer gained access to the MagentoName JS sniffer code and added their malicious code to it.

Another example is the attack on Feedify, a real-time push notification service. By injecting the JS sniffer code into the code of a given file, the threat actor automatically uploaded the JS sniffer to all Feedify customers, and their sites were infected with the feedbackembad-min-1.0.js script. The sniffer was injected into the Feedify code on August 17, and was detected and removed on September 11. However, the intruders infected the website again on September 12.

Supply chain attacks have proven successful: more than 60% of the 300 sites that download the Feedify script are e-commerce and therefore targets for the WebRank JS sniffer family.



## Target payment systems

In terms of architecture, each JS sniffer has a client and a server part.

The client part of the JS sniffer is responsible for initial data collection, which can be carried out in various ways:

- On a hardcoded list of names of payment form fields for various payment systems;
- Using a list of regular expressions that define fields of interest to the JS sniffer and contain sensitive information;
- According to the list of basic HTML elements used in the payment form.

The server part is the application that the JS sniffer operator works with.

The functions performed by the server depend on how accurately the client part determines the type of data stolen. If the data is transmitted in an unprocessed form, the card number, CVV, expiration date, etc. are identified in the administrative panel.

Processing data in the administrative panel is the most convenient option as it is easier for hackers to make changes to the administrative panel code if necessary rather than to change the code of the JS sniffer injected into the online store website.

Many JS sniffer families are not universal, however, and use unique options for each payment system, which requires modifying and testing the script before each infection.

### Universal JS sniffers

• Universal JS sniffer families steal information from payment forms and do not require modifications tailored to specific websites. G-Analytics and WebRank JS sniffer families collect all the content from the hardcoded list of HTML elements, which means that

all the collected information is parsed in the administrative panels of these JS sniffers, on the server side.

- WebRank JS sniffers search for elements such as "text", "a", "button", "input", "submit", and "form" and create specific event handlers for them all.
- G-Analytics JS sniffers search for elements such as "input", "select", "textarea", and "checkbox". If the search results contain data matching the credit card number's regular expression, the JS sniffer sends this information to the attackers' server.

### JS sniffers for specific CMSs

Most JS sniffer families detected were developed to steal information from the payment forms within a specific CMS. These JS sniffers search for specific fields by the list of names hardcoded in the JS sniffer source code. The fields could contain the victim's payment information.

The following JS sniffer families search default Magento fields:

- PreMage;
- MagentoName;
- FakeCDN;
- Qoogle.

The GetBilling JS sniffer family also targets Magento websites, but it searches by name for forms, not fields. The PostEval JS sniffer family targets OpenCart websites. These JS sniffers use a hardcoded list of names that correspond to the fields in a payment form. The list of field names is used to search for the victim's payment information.

### JS sniffer as a service

Each individual JS sniffer family can represent a different service. When analyzing underground forums intended for communication between cybercriminals, experts discovered a large number of services offering a comprehensive solution, including:

- JS sniffer or utility for generating JS sniffers;
- administrative panel for data processing and tracking JS sniffer activity;
- manuals for infecting online store sites;
- ready-made exploits to infect sites;
- auxiliary utilities for vulnerability searches and mass website infections.

Analysis of some JS sniffer families showed that, in some cases, the domains used to store the JS sniffer code and collect stolen data had been registered by different users. In other cases, the code had been modified and various obfuscation methods and malicious activity concealment techniques had been used. This could indicate that a separate family of JS sniffers is used by different threat actors, i.e. it is delivered as a service.

In other cases, a given threat actor's activities were clearly observed, which could mean that it acts independently of outside developers and uses exclusively its own products. This implies that such threat actors have at least one member with web development skills and knowledge of languages such as HTML, JavaScript, and PHP.

### The cost of JS sniffers

The cost of JS sniffers ranges from \$250 to \$5,000. Some services offer the option to work in partnership: the client provides access to the store and receives 80% of the revenue, while the JS sniffer developer is responsible for providing hosting servers, technical support, and an administrative panel for the client.



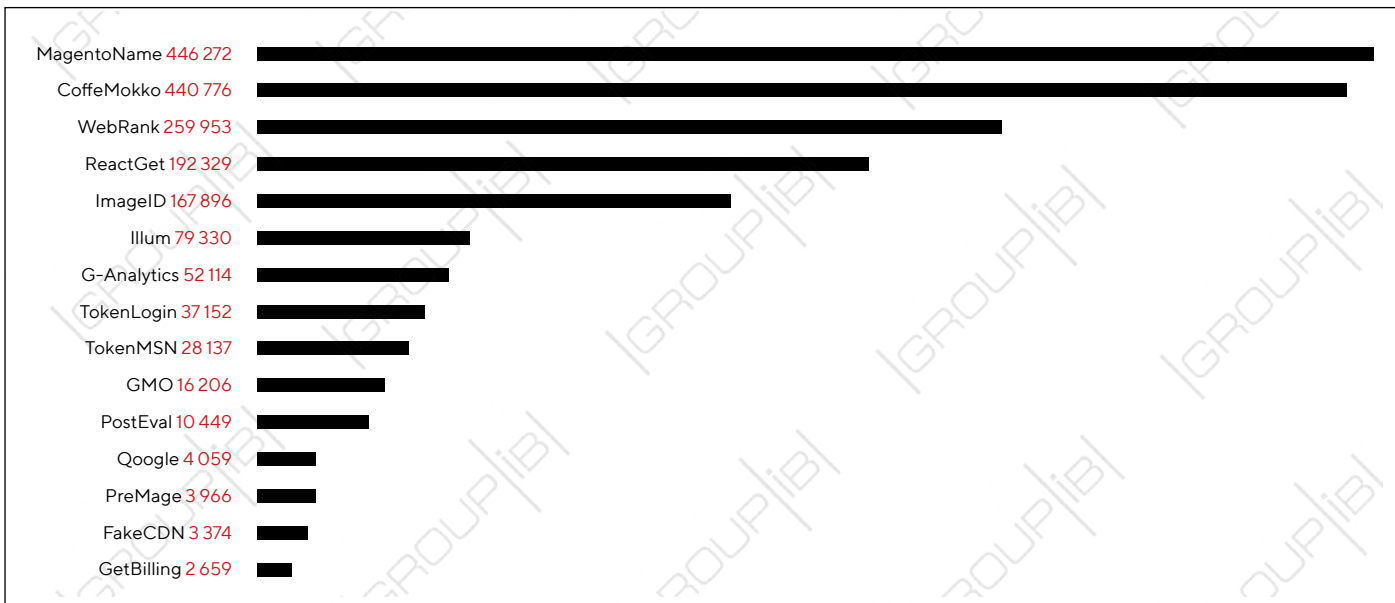
### Infection scale and victims

The JS sniffer families detected were used to infect at least 2,440 online stores that accept payment by bank card. The total daily number of visitors to all the infected websites is more than 1.5 million people.

The average number of visitors to infected websites for each JS sniffer family shows which JS sniffers are used to infect the most popular online stores. The average number of visitors to websites infected with Illum, G-Analytics, and TokenMSN is about 3,000 people per day per site, while for MagentoName it is about 500 people.

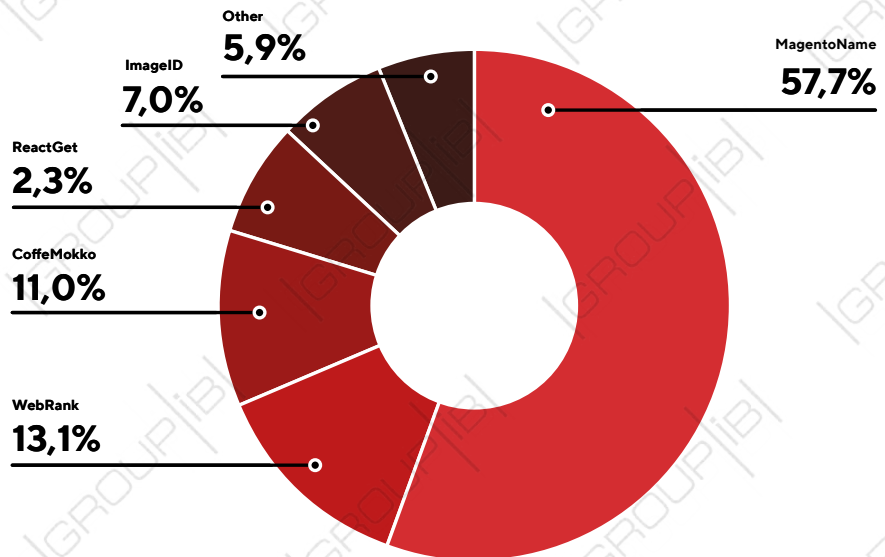
**JS sniffers that are used to conduct the most large-scale attacks**

Due to mass website infections (with the most visitors to sites infected by the families MagentoName and CoffeMokko), every day more than 440,000 people visit the websites infected with these JS sniffers. The JS sniffer family that comes third in terms of the number of websites infected is WebRank, accounting for 250,000 visitors.



Analysis of the sites showed that more than half were infected with MagentoName, whose operators use vulnerabilities to inject malicious code into the code of sites running on older versions of the CMS Magento. More than 13% of infections involve WebRank, which is used in attacks on third-party services to inject malicious code into target sites. Moreover, 11% are infected by JS sniffers belonging to the CoffeMokko family, whose operators use obfuscated scripts that search payment forms for specific fields by the list of names hardcoded in the JS sniffer source code. Such fields could contain the victim's payment information.

Based on an analysis of the list of TLDs (top-level domains) of infected online stores, it can be concluded that attackers are generally interested in infecting websites from major developed countries: the USA, the UK, Germany, etc.



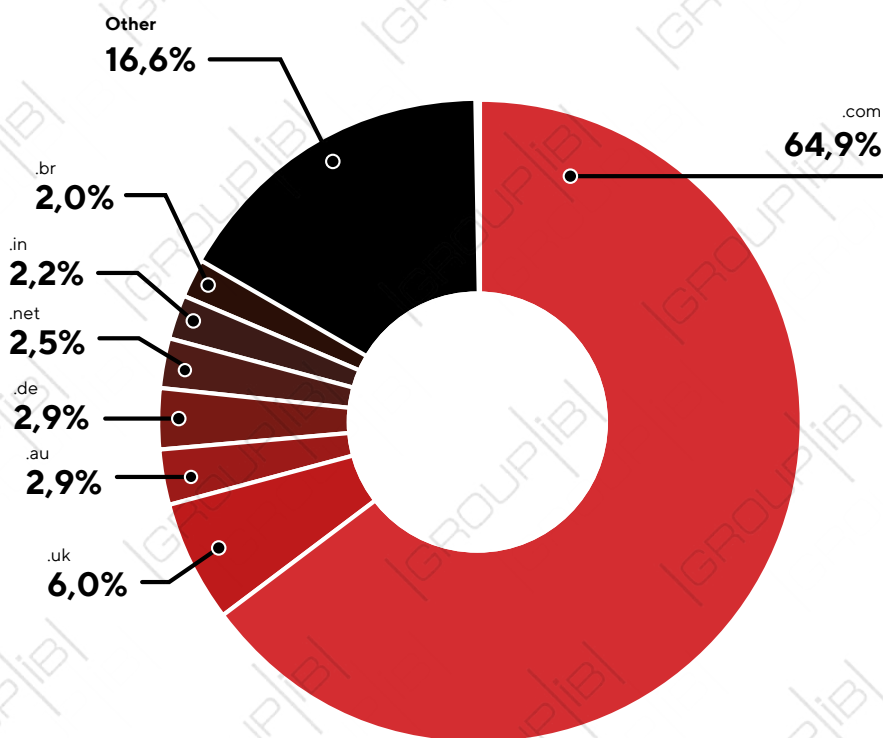
Similarly to attacks on POS terminals, attackers mainly target banking customers in the USA. UK banks rank second, mainly due to a successful attack on British Airways in late 2018 during which its resources were infected with a JS sniffer. As a result, a \$229 million fine was imposed on British Airways for data leaks relating to more than 300,000 cards.

Analysis showed that there are 11 JS sniffer families that are behind the attacks on Asian website users:

- MagentoName;
- Inter;
- addtoev Group;
- Qoogle;
- Illum;
- CoffeMokko;
- EUTag;
- WebRank;
- ImageID;
- TokenLogin;
- OnlineStatus.

The attackers mainly focused on websites of companies based in Singapore, China, and Malaysia.

Country	Number of websites
Singapore	24
China	17
Malaysia	15
Indonesia	6
Vietnam	4
Thailand	4
The Philippines	4



## WEB PHISHING AND SOCIAL ENGINEERING

Web phishing, one of the oldest and simplest types of fraud, is often used by attackers of all kinds. It is gradually replacing complex attacks involving expensive Trojans or hacking tools.

One of the reasons that web phishing attacks are so popular is because they are easy to conduct despite the fact that they are continuously changing. Having analyzed over three million links and 27,000 unique phishing kits over the past year, Group-IB experts identified the main trends in this threat's evolution.

### Anti-evasion techniques

Given that more and more companies provide services for blocking phishing websites, phishing kit developers tend to sell them with built-in anti-evasion mechanisms:

- **Blocking by subnet:** If a page request is sent from a subnets belonging to a company that provides phishing detection services, phishing content will not be shown.
- **Blocking by user agent:** Attackers analyze the user agent and try to understand if the user is real. For example, if the attack targets mobile device users, then visitors using PC browsers will not receive phishing pages. Usually, phishing scripts check the user agent field by a list of predefined keywords.

- **Blocking by region:** Attackers actively use GeoIP databases; if users are not located in the targeted region, they will not be forwarded to the phishing page.
- **Redirection to official websites:** Special checks help attackers identify suspicious users and redirect them to the attacked brand's official website or the website of another legitimate service instead of displaying phishing content.

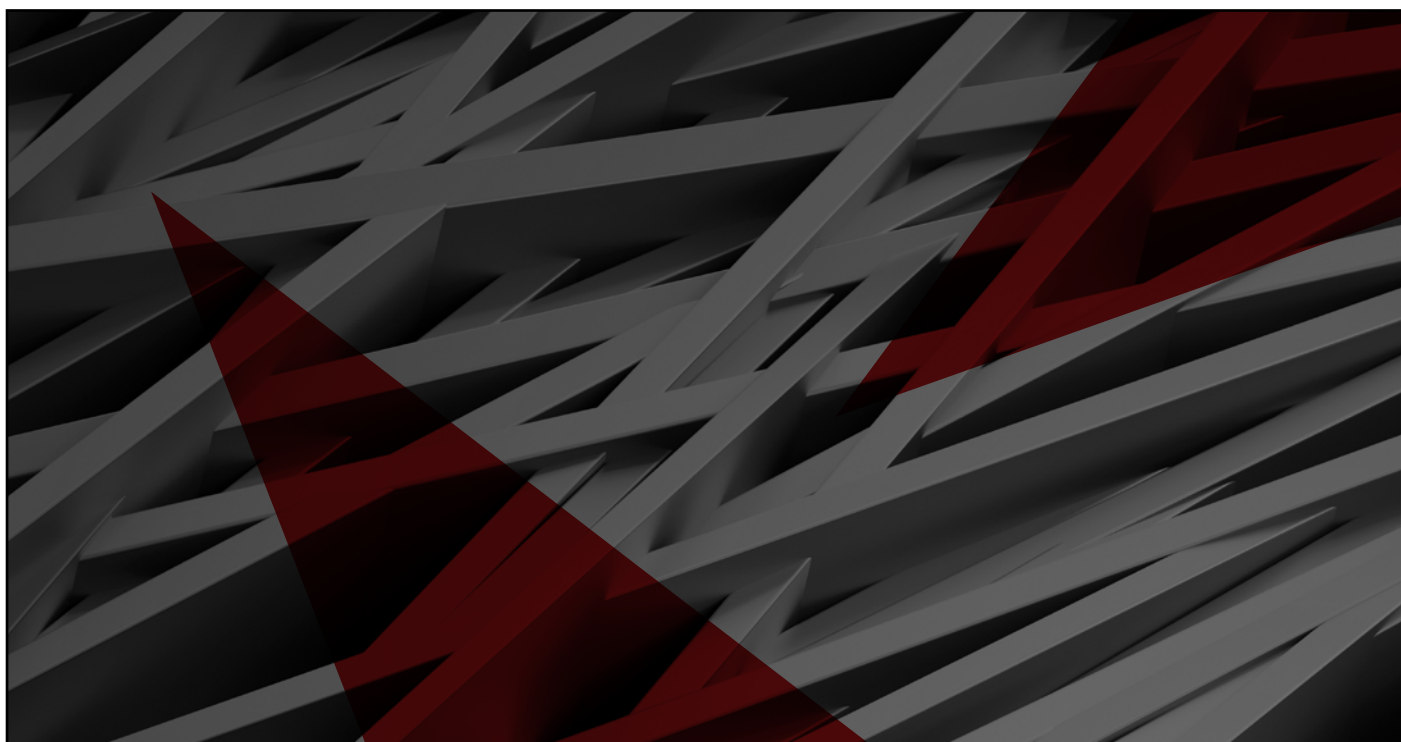
### DNS hijacking

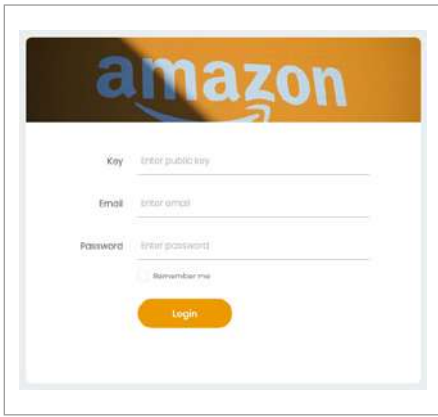
Last year's Group-IB Hi-Tech Crime Trends report predicted that DNS hijacking would actively evolve to help conduct phishing attacks even more effectively. Below is a reminder of how this method works.

1. **Access the router in one of the following ways:**
  - **Brute-force attacks:** Companies that provide routers for rent do not care much about their security level, set default passwords, and enable access to their management interfaces via the Internet.
  - **Exploitation of known vulnerabilities:** Updating home routers is not easy. The support cycle for such devices is very short, and updates are often unavailable. Even in cases where updates exist, users rarely install them.

2. **Change the device DNS settings** by writing the addresses of the hacker-controlled DNS servers into the router configuration. This means that instead of returning the IP address of the website that the user wants to visit (for example, an online banking page), the malicious DNS server returns a forged IP address. In other words, malefactors trick the browser into loading a phishing webpage instead of the website the user was looking for.

In September 2018, Qihoo 360 discovered a mass campaign. In one week, the security company identified more than 100,000 compromised routers, most of which were located in Brazil. The threat, called GhostDNS, was active at least until May 2019. The campaign mainly targeted customers of several banks in Brazil and the Netflix service.





Phishing admin panel for a fake Amazon website



Phishing admin panel for a fake Apple website

## Phishing management systems

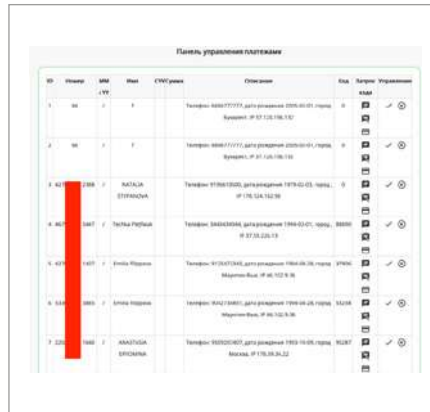
Once the victim's data is collected, phishers usually perform one of the following actions:

- Send data via email (still the most popular method).
- Save data to a local text file, which the criminal can retrieve from a remote server in various ways.
- Upload logs to a remote FTP server (rare).

Given that security systems have evolved, however, criminals must handle data in real time. Moreover, in an effort to attract customers, criminals providing phishing as a service started offering user-friendly management systems.

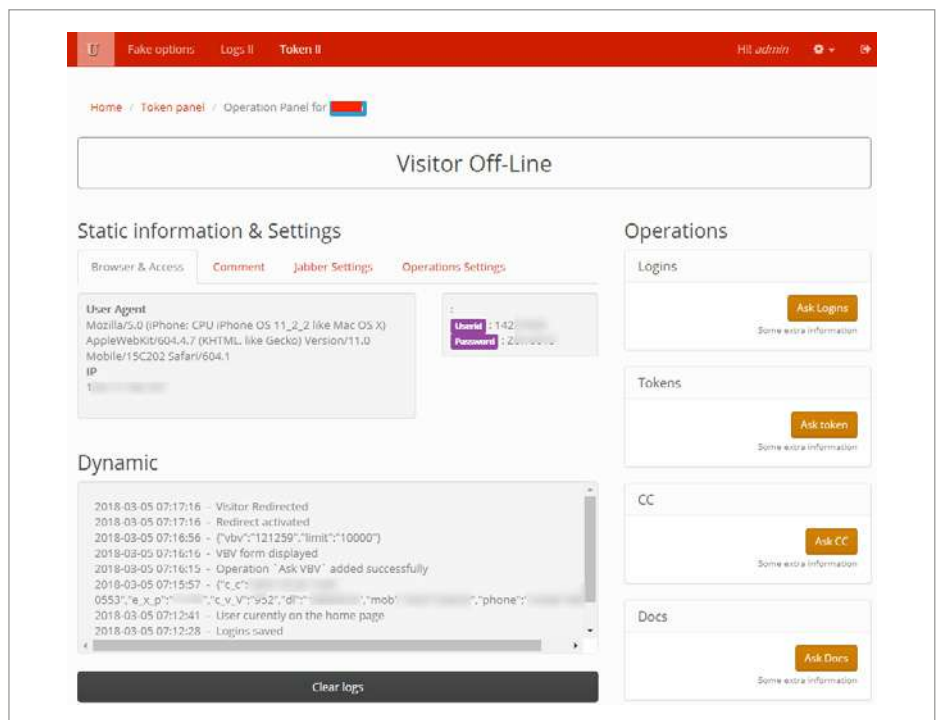


Admin panel for a banking phishing website



Admin panel targeting Russian banks

Phishers targeting banking customers have started using panels for managing web injects more actively. The panels help conduct attacks in real time, receive one-time passwords from victims, and perform additional actions to confirm financial transactions. One of the most popular panels is U-Admin.



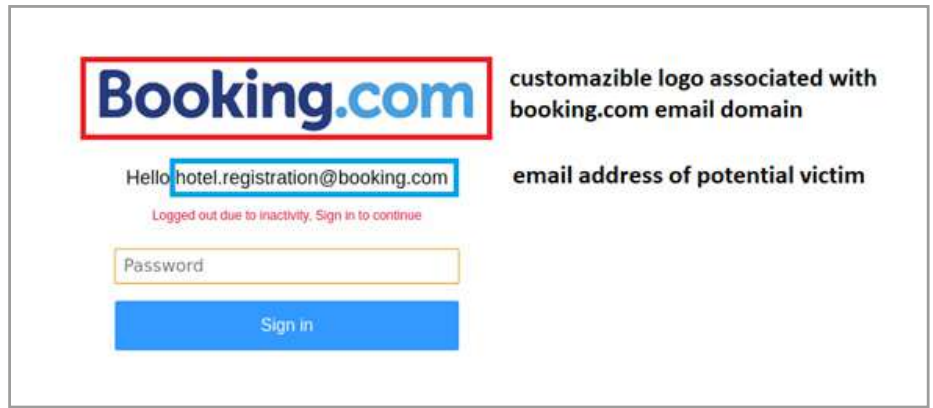
Automated phishing framework



## Automated phishing framework

An interesting example of phishing automation was a phishing campaign that targeted more than 200 banks, universities, and companies to collect email addresses and passwords. Its particularity was that the framework used was automatically tailored to each victim.

1. Links to the phishing page were sent via email.
2. If the victim clicked on the link, information about the email address from which the link was followed was marked as a parameter.
3. The phishing page scripts checked the domain in the email address and made an API request to the server to obtain data to be displayed on the phishing page.
4. By domain, the server determined whether the user was of interest and which logo should be used on the phishing page.



5. If the user was of interest, the victim was redirected to further pages after entering the login and password on the phishing page.

## Growth of social engineering attacks without the use of malware

Social engineering without using malware or phishing websites remains one of the most widespread and popular schemes. Criminals have always used phone calls, text messages, and social media to communicate with victims. As a result, the victim provides the scammer with all the necessary information or installs remote access programs on their PC that help the attacker perform fraudulent activity. A new, unprecedented scheme that appeared this year tricks victims into installing remote control tools on their mobile device instead of their PC.

A typical fraud scenario involves the following:

- The hacker calls posing as a bank employee and informs the customer that an attempt has been made to break into their online banking account or withdraw funds.
- The customer is told that the bank's security team needs help with solving a technical issue to counter the fraud.
- The victim is asked to urgently install a remote control tool on their smartphone to protect the user.
- Having obtained control of the device, the criminal withdraws funds through the mobile banking app.

During calls, criminals use various tricks, some of which are highly convincing, to win the victim's trust:

- They make calls from official bank numbers using IP telephony by replacing the phone number through special programs.
- They provide the transaction history and other information about the customer, for example where the victim lives (databases with such information are available for purchase on darknet forums).



# ATM TROJANS

The main and most dangerous threat to ATMs is logical attacks. As the final stage of targeted campaigns, logical attacks result in gaining remote control over ATMs. However, such schemes are only available to advanced attackers.

Low-skilled actors must still gain physical access to ATMs to steal money. Their main limitation is the ability to attack only one ATM at a time, so the potential damage from such threats is much lower.

Malware is downloaded to specific ATMs using CD-ROMs, USB flash drives, or Raspberry Pi devices. Such "jackpotting" attacks require the involvement of three types of criminals: organizer/customer, software developer, and money mules.

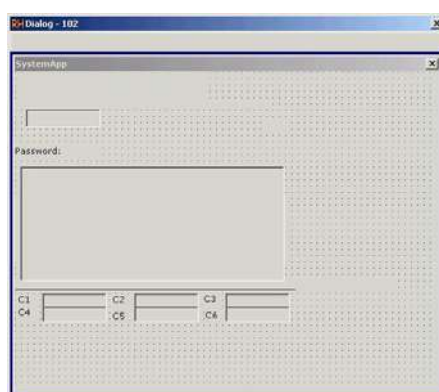
Compared to logical attacks, the landscape of such threats is much smaller. It continues to evolve actively.

## New threats

### Unnamed Trojan from Africa

In April 2019, Group-IB experts discovered an interesting sample of an ATM Trojan from Africa. The program is designed to control ATMs through the pinpad: when the correct PIN code is entered, it interacts with the dispenser directly, and when a bank card with a certain number is used, the threat actor can deplete the entire ATM.

To bypass whitelists, attackers used the cmd.dll file, which is similar to the cmd.exe command-line interpreter used in the ReactOS operating system.



### HelloWorld

In January 2019, a user with the nickname "gookee" made a post on the underground forum exploit.in about the sale of new malware. The name "HelloWorld" was mentioned in the topic about the sale of its previous, unfinished version. The following versions of the program were for sale:

- an executable file similar to "Cutlet Maker", with a keygen or without;
- an IMG image for saving it onto a flash drive;
- a CD image;
- a floppy disk image;
- an ISO image for booting via PXE (under development).

The Trojan runs on all Wincor/Diebold Nixdorf models released after 2001, which have MXFS/CSCW DLL files. The cost of the program is \$2,000 for an .EXE file or image, \$3,000 for all options, and \$10,000 for source codes.

## JavaDispCash

This Trojan was uploaded to VirusTotal first from Colombia, then from Mexico. Unlike similar tools, it infiltrates the ATM application via JAVA Attach API instead of using CNG, XFS, or JXFS. The approach to command and control is also unusual: an HTTP server is launched on the ATM, which interprets certain paths as commands.

Path	Command description
/d	Dispense banknotes
/eva	Check the transferred code on the ATM
/mgr	Show the list of all running classes in the attached Java virtual machine, allowing the threat actor to call any function with arbitrary arguments
/core	Upload a .jar file from the victim's file system
/root	Accept a POST request and forward its contents to cmd.exe for execution

## Evolution of ATM Trojans

### Cutlet Maker

Cutlet is one of the most widespread ATM Trojans available for free. The tool has been active since mid-2017. To date, multiple malware variants have been spotted on hacking forums.

In December 2018, yet another version was posted on a Russian-speaking forum. Cutlet has been used to successfully attack Europe as well as Russia, and other post-Soviet countries.

### WinPot (Cutlet V2)

In May 2018, a user with the nickname "sl111" made a post on an underground forum about the sale of an ATM Trojan for Wincor called "Cutlet Maker v2" (aka WinPot). The Trojan is sold as a bundle together with its source code. The cost of the program varies from 500 to 1,000 US dollars. Like its predecessor, the Trojan has been used to attack ATMs in Europe.

### Ploutus

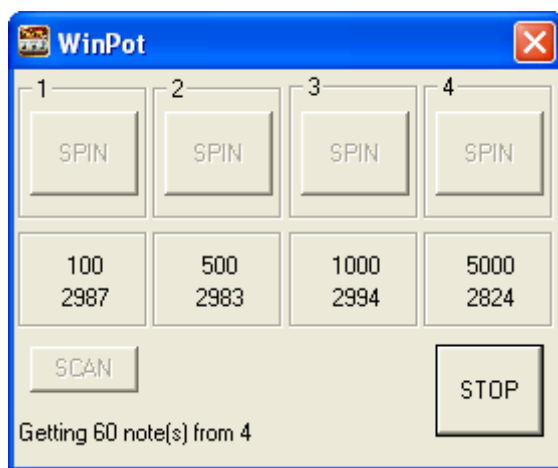
This malware was originally for sale in 2016. It had been used in Mexico for a long time; in 2018, it appeared in the USA. Despite its age, Ploutus is still active; since 2019, ads about its sale have been posted on hacker forums regularly.

### ATMii

ATMii was first discovered in April 2017. Its distinctive feature was targeting only ATMs running on Windows 7 and Windows Vista. The malware's approach was very peculiar because most ATMs used Windows XP at the time. In December 2018, ATMii was also published on a Russian-speaking hacker forum.

### Alice

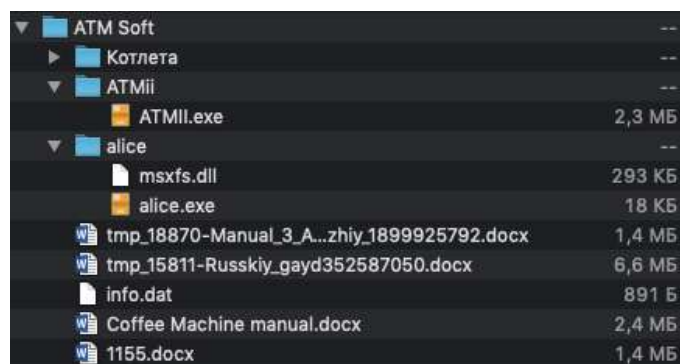
This Trojan has been known since November 2016. The tool reappeared on underground forums in December 2018, as had ATMii. Compared to the free tool Cutlet Maker, Alice is less user-friendly and has not been observed in attacks over the reporting period.



### Cutlet Maker



### WinPot (Cutlet V2)



### ATMii

### Alice

# PC TROJANS

The trend towards a decrease in the activity of banking Trojans for PCs has only intensified. Criminals have stopped developing new theft techniques involving PC Trojans. The only country where these Trojans continue to be developed is Brazil.

The target list has not changed. Owners of banking botnets mainly focus on 18 countries: Australia, Austria, Bulgaria, Brazil, the UK, Germany, Spain, Italy, Canada, the Netherlands, Norway, Poland, Russia, the USA, Ukraine, France,

Switzerland, and Japan. The most active Trojans remain local, attacking users in 2 or 3 countries.

Old	New	Disappeared
BackSwap, IcedID, Qbot, Gozi (ISFB, Ursnif), Trickbot, TinyNuke (aka NukeBot), Gootkit, Buhtrap, Dridex, Ramnit, Panda Banker, Retefe, Danabot, Osiris, Loki PWS	BANKER.THBAIAI, CamuBot	Zeus, ZeusVM, Atmos, Corebot, UriZone, Xbot, Topel

	Poland	Spain	USA	Canada	United Kingdom	The Netherlands	Germany	Bulgaria	Australia	Austria	France	post-Soviet countries	Russia	Japan	Switzerland	Norway	Ukraine	Brazil	Taiwan	Italy
BackSwap	█	█																		
IcedID			█	█	█															
Qbot		█	█	█		█														
Gozi (ISFB, Ursnif)				█					█					█						█
Trickbot		█	█	█	█	█	█	█	█	█										█
TinyNuke (aka NukeBot)	█										█									
Gootkit		█		█	█	█	█		█	█										█
RTM												█	█							
Buhtrap													█							
Dridex	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
LokiPWS	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
Ramnit			█	█	█								█	█						█
Panda Banker			█	█	█									█						
Retefe										█					█	█				
DanaBot	█		█				█		█	█							█			█
Osiris	█						█							█						
BANKER.THBAIAI																		█	█	
CamuBot																				█

global



## USA and Canada

In the USA, the threat landscape related to PC banking Trojans has not changed much: attacks have been mainly conducted using IcedID, Trickbot, and Dridex and, to a lesser extent, Qbot, Ramnit, Panda Banker, and Danabot. The situation in Canada has always been similar to that in the USA, and only the owners of one of the Gozi forks have a particular interest in banking customers in Canada. IcedID continues to use web injections. Unlike many other banking Trojans, it employs the Automatic Transfer System (ATS) to steal money from victims' bank accounts automatically.

It is worth paying particular attention to the Trickbot Trojan. Over the past year, it has been fitted with a new module for collecting passwords from installed apps and has been programmed to steal configuration files from SYSVOL directories on domain controllers. It has also started employing Mimikatz and has featured in fileless attacks and active mail-outs from compromised computers. These functionalities can be used for targeted attacks on large organizations. We believe that, in the near future, a new group may emerge that will use Trickbot for targeted attacks on banks rather than their customers.

## Europe

European banking customers are still being targeted by BackSwap, Gootkit, Danabot, Osiris, and TinyNuke tools. The simple banking Trojan Retefe poses a serious threat to northern European countries.

All these Trojans are well known except BackSwap, which is relatively new. Over the past year, the Trojan began attacking banking customers—first Polish, then Spanish. In general, Poland is the only European country in which attackers have been noticeably more interested.

## Russia and other post-Soviet countries

In Russia, the "homeland" of most banking Trojans, only one banking Trojan continues to be actively used: RTM. Its victims are mainly customers of poorly protected banks, however. The banking botnet Toplel has stopped being used and no new thefts were detected this year.

The owners of the botnet Buhtrap2 previously performed automated transfers through the Russian 1C accounting system. This scheme led to compromise being detected, however, which prevented criminals from carrying out the thefts. In February 2019, the hackers tried to revive their botnet, but the financial outcome was unsatisfactory and they stopped their activity.

## APAC

The most attractive country for attackers in this region is Australia, where Gozi, Trickbot, Gootkit, Ramnit, and Danabot are all used to attack victims. The second most popular country is Japan, where the list of active Trojans includes Gozi, Ramnit, Panda banker, and Osiris. Despite the high population and developed banking services, attackers have no interest in other countries in the region.

## Latin America

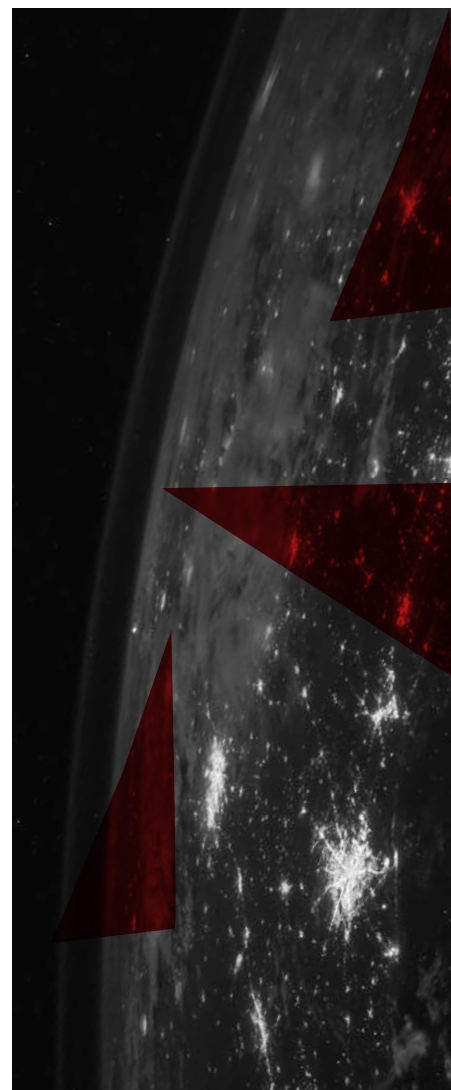
As mentioned earlier, Brazil is becoming the main source of new banking Trojans. However, they are used locally only and are most likely developed by local hackers. A distinctive feature of these Trojans is overlapping windows that emulate the operation of banking applications.

MnuBot, discovered in the first half of 2018, is notable for the fact that its component is a remote access Trojan that receives commands from the Microsoft SQL database server. A configuration file with a list of targeted banks is also received from the C&C server.

CamuBot was first used for attack purposes in August 2018. Attackers took an atypical approach to its distribution. Instead of mass campaigns, they called victims purporting to be bank employees and tricked them into visiting a phishing website to download a "security" module. Once downloaded to the victim's device, CamuBot creates a tunnel that allows attackers to direct their own traffic through the infected machine and use the victim's IP address when accessing the compromised bank account. When the installation is complete, a pop-up screen redirects the victim to a phishing website disguised as their bank's online banking portal. The victim is asked to log into their account and unknowingly sends the credentials to the attacker.

Another banking Trojan was discovered in March 2019, tracked as BANKER.THBAIAI. Below is a description of the entire toolset that scammers use to conduct attacks involving it.

1. The first module infects the computer, then loads and executes PowerShell scripts that write .LNK files to the Startup folder and force the computer to reboot. After the reboot, a fake login screen is displayed to intercept user credentials.
2. The second Trojan is launched; it attempts to open Microsoft Outlook and obtain all the email addresses stored therein. If Outlook is not installed on the computer, this step is skipped.
3. RADMIN is installed on the system.
4. The last step is the installation of a fileless banking Trojan that targets customers of the Brazilian banks Banco Bradesco, Banco do Brasil, and Sicredi.



# ANDROID TROJANS

Usually, Android banking Trojans steal money using one of the following techniques:

- money transfers through hijacked SMS messaging;
- rogue mobile banking apps;
- collection of bank card data, logins and passwords by displaying fake windows.

The first two methods have serious limitations as regards the extent of the theft. Few banks provide SMS money transfer services and the transfer limits are very low. The proliferation of fake banking mobile applications requires considerable investment and effort to advertise and promote them. As such, the use of fake windows has been the most effective method. Phishing windows are displayed on top of other apps and require the user to enter the relevant data.

When security policies were tightened in updated versions of Android and fraudulent applications could no longer display arbitrary windows, the attack scheme stopped being effective. Most Android Trojan developers were unable to adjust their malware to updates, which meant that many effective Android Trojans stopped working. Some projects were closed, others were abandoned by developers. The development of these Trojans slowed noticeably, leading to less damage from their actions.

In the past, to confirm banking operations, banks used text messages. With the widespread introduction of mobile applications, banks began to switch from text messages to PUSH notifications. Transaction confirmation codes are also delivered through PUSH notifications. Compared to text messages, PUSH notifications have

several key advantages: they are cheaper for banks and safer against Android Trojans because all Android-based banking Trojans are able to intercept text messages. This was another reason why the activity of Android banking Trojans decreased.

Nevertheless, security measures used by banks can be bypassed using the Accessibility Service, which is intended for people with disabilities. Having received permission to use the Accessibility Service, the malicious application can block other applications' windows, control the device using voice commands, listen to (rather than view) content, manage PUSH notifications, covertly unlock the device, and perform arbitrary actions, all the while keeping the screen turned off.

Old	New	Disappeared
Red Alert, Anubis, Asacub, Loki v2, TarkBot (Rotexy), Flexnet, Riltok	Gustuff, Cerberus, CometBot, Exobot Compact, BasBanke	Agent.sx, Granzy, Agent.BID, LimeBot, Sagawa, Maza-in, Alienbot, Rello, Easy, CryEye, Cannabis, Fmif, AndyBot, Nero banker, Exobot



## Gustuff: ATS feature for Android

The Gustuff Trojan is an improved version of the malware AndyBot, developed by the same author. The application's features include: sending information about the infected device to the server, reading/sending text messages, sending USSD requests, setting up the SOCKS5 proxy, following links, displaying push notifications, transferring files (including photos) to the server, displaying fake web pages, and resetting the device to factory settings. The application also uses the Accessibility Service to interact with elements of windows in other apps

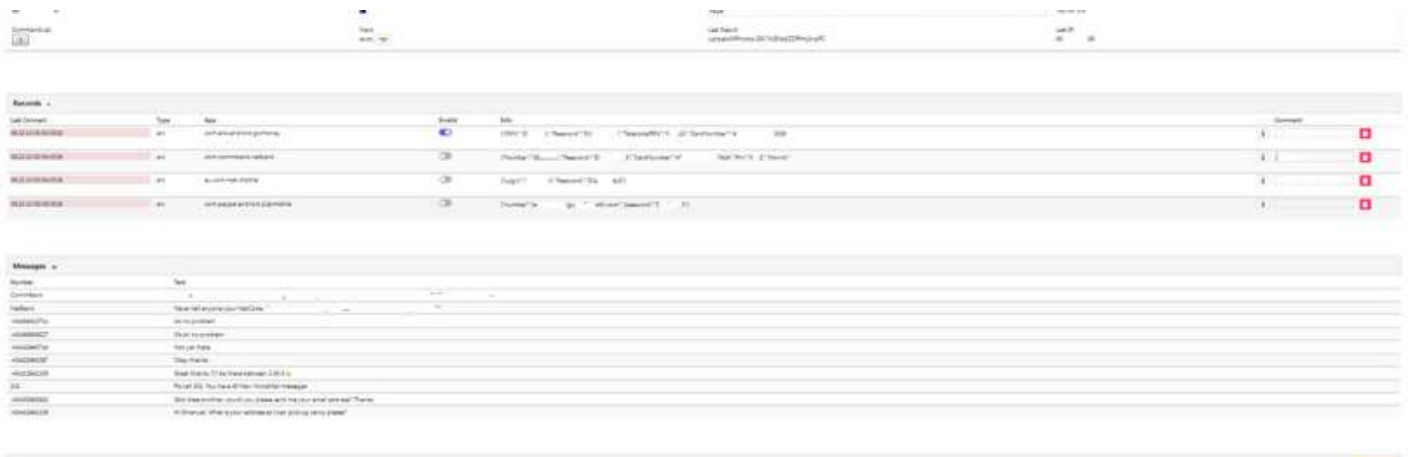
and perform actions that are crucial for hackers, such as focusing on the object, clicking on the object, and changing object text content. For example, at the server's instruction, the Trojan is able to change text field values in banking apps.

Gustuff has a unique feature that has not been seen previously in malicious programs for Android: an ATS mechanism, which works according to the following algorithm:

- The Trojan sends a PUSH notification to the user with the banking app's official icon.

- The user clicks on the PUSH notification.
- The associated legitimate app opens.
- The user logs in to the application.
- On the server's command, Gustuff automatically fills payment fields for illicit transactions.

The price for leasing the "Gustuff Bot" is \$800 per month. The author claims to take care of their own safety, which is why the bot does not operate in Russia, post-Soviet countries, or the USA.



## New adjusted Trojans without ATS

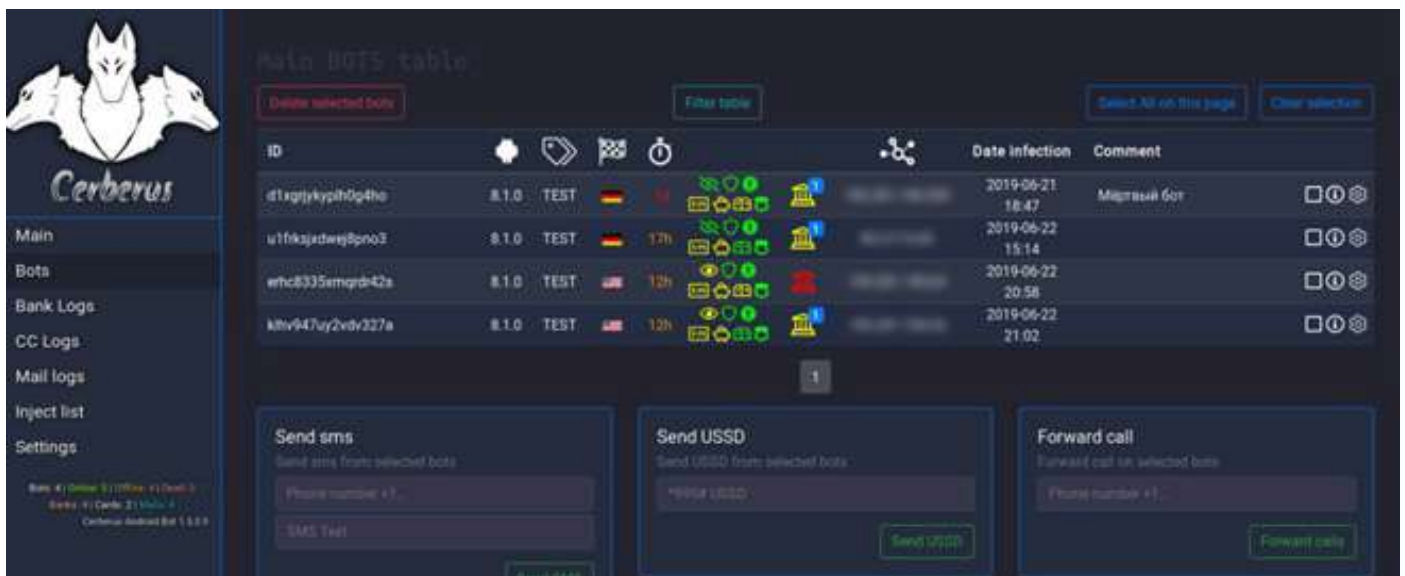
Cerberus was put up for sale in June 2019. Its features are similar to Gustuff's. It can also be used to manipulate PUSH notifications from banks. The Cerberus Trojan uses enhanced self-defense techniques:

- Disable Google Play Protect and turn it off after a time period specified in the admin panel;
- Prevent the bot from being deleted, administrator rights from being disabled, and the Accessibility Service from being turned off.

- Evasion of sandbox analysis using accelerometer data.

The author prohibits the use of the Trojan in Russia and other post-Soviet countries.

The price for leasing the Trojan is \$2,000 per month.





**CometBot** emerged on hacking forums in February 2019, when a user with the nickname "SickHavana" made a post about renting out new malware for Android.

This Trojan's features are much inferior to those of the programs described above. However, it works on the latest Android versions. The offer only included ready-made web fakes for German banks and one Spanish bank, with the possibility of a simple expansion to target banks in other regions.

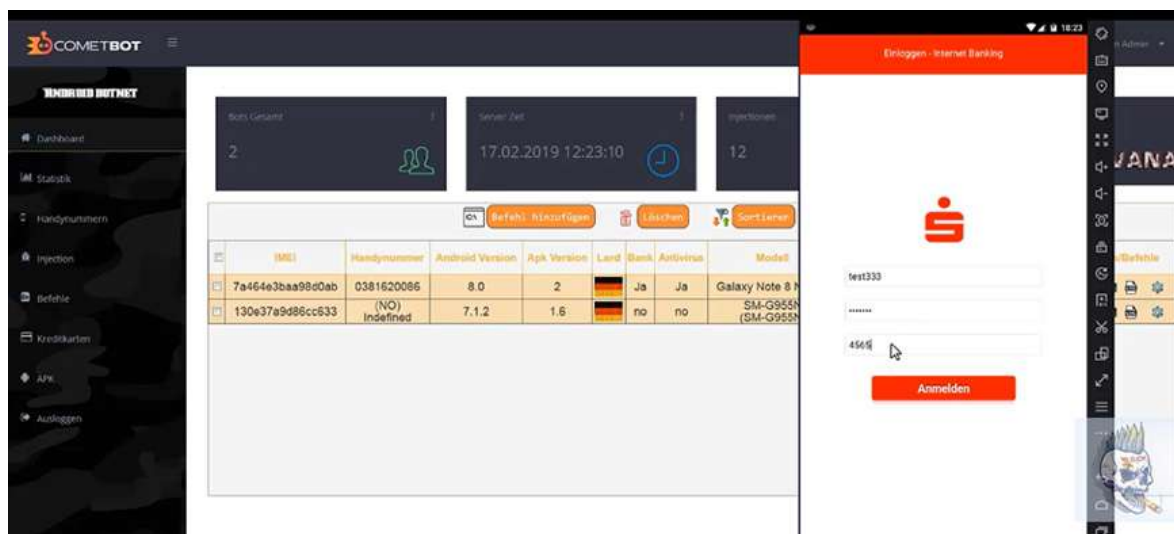
**The price for leasing the Trojan is \$850 per month.**

In March 2019, **Exobot Compact**, the third version of the infamous malware for Android called Exobot, was put up for sale. In May 2018, the source code for Exobot version 2 was made public. The new version was completely rewritten and optimized compared to the one that was publicly available. Exobot Compact runs on modern versions of Android up to Android 9.

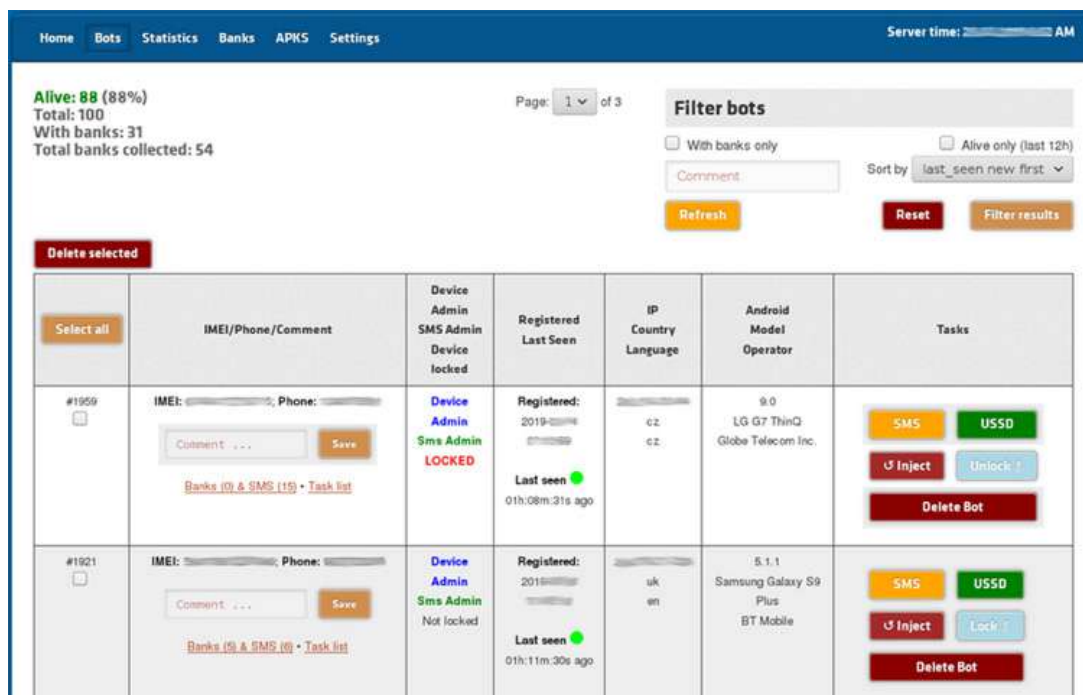
As was the case with Gustuff, the author prohibits attacks in Russia and other post-Soviet countries and the USA, although the program has fake pages for U.S. banks.

**The price for leasing the program is \$1,500 per month.**

**BasBanke** is a new Android Trojan that targets banking customers in Brazil. BasBanke's functionality is quite basic, but its owners were able to place it on Google Play. As a result, it was downloaded more than 10,000 times. This malware can perform tasks such as keystroke logging, screen recording, and text message interception.









CometBot




Exobot Compact



# ANDROID TROJANS

	Poland	Germany	Spain	Australia	Europe	The Netherlands	France	Hong-Kong	Turkey	India	USA	Russia	Ukraine	Italy	United Kingdom	Brazil	Post-Soviet countries
RedAlert  *	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
CometBot		█	█														
Exobot  **	█	█	█	█	█	█	█	█	█	█				█	█	█	
Exobot Compact (Exobot 3)  **	█	█	█	█	█	█	█	█	█	█				█	█	█	
Cerberus  ***	█	█	█	█	█	█	█	█	█	█	█			█	█	█	
Loki v2 	█	█	█	█	█	█	█	█	█	█	█		█	█	█	█	█
Gustuff (aka AndyBot)  ****				█	█												
Anubis		█	█	█	█	█	█	█	█	█	█						
Riltok							█					█	█	█	█		
Tarkbot (Rotexy)												█	█	█	█		
Flexnet												█	█	█	█		
Asacub												█	█	█	█		
Agent.BID												█	█	█	█		
BasBanke																█	

 global

\* more than 200 targets in various countries

\*\* except post-Soviet countries and the USA

\*\*\* except post-Soviet countries

\*\*\*\* he use is prohibited in the post-Soviet countries and the USA

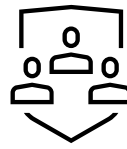
# ABOUT GROUP-IB

Group-IB is a leading provider of high-fidelity adversary tracking & threat attribution framework, best-in-class anti-APT and online fraud prevention solutions

<b>16 years</b> of hands-on experience	<b>60 000+</b> hours of incident response experience	<b>1 000+</b> cybercrime investigations worldwide	<b>360+</b> world-class cybersecurity experts
---	---	--	--

## OUR CLIENTS

Our clients include banks, financial institutions, oil and gas companies, telecoms, IT and cloud service providers, e-commerce and FMCG companies, fintech and blockchain startups. We especially enjoy working with the next generation of cybersecurity specialists who share our passion for threat hunting.



**400+**  
enterprise clients



**60**  
countries

### We have provided professional development training to:

- Europol, INTERPOL
- Law enforcement agencies
- Corporate security teams in the UK, Germany, the Netherlands, Belgium, Thailand, France, Bahrain, and Lebanon.

We hunt down real cybercriminals to prevent them from harming your business and provide evidence to put them in jail. We train security professionals around the globe to do it.

**OSCE**

Recommended by the Organization for Security and Cooperation in Europe

**INTERPOL**

Official partners

**EUROPOL**

**SWIFT**

Approved as a cybersecurity service provider

## PROACTIVE & REACTIVE SERVICES

Strengthen your cybersecurity posture with services and advice from experienced specialists with 'boots on the ground' and access to one of the most advanced threat attribution and intelligence gathering infrastructures in the world.

<p><b>SECURITY &amp; RISK ASSESSMENT</b></p> <ul style="list-style-type: none"> <li>• Penetration Testing</li> <li>• Vulnerability Assessment</li> <li>• Source Code Analysis</li> <li>• Compromise Assessment</li> <li>• Red Teaming</li> <li>• Pre-IR Assessment</li> <li>• Compliance Audit</li> </ul>	<p><b>THREAT HUNTING &amp; RESPONSE</b></p> <ul style="list-style-type: none"> <li>• 24/7 CERT-GIB</li> <li>• External and Internal Threat Hunting</li> <li>• Onsite Incident Response</li> <li>• Incident Response Retainer</li> </ul>	<p><b>DIGITAL FORENSICS &amp; INVESTIGATIONS</b></p> <ul style="list-style-type: none"> <li>• Digital Forensics</li> <li>• Investigations of hi-tech financial &amp; corporate crimes, critical infrastructure attacks</li> </ul>	<p><b>PROFESSIONAL CYBER EDUCATION</b></p> <ul style="list-style-type: none"> <li>• Digital Forensics</li> <li>• Incident Response</li> <li>• Malware Analysis</li> </ul>
---	---	---	---

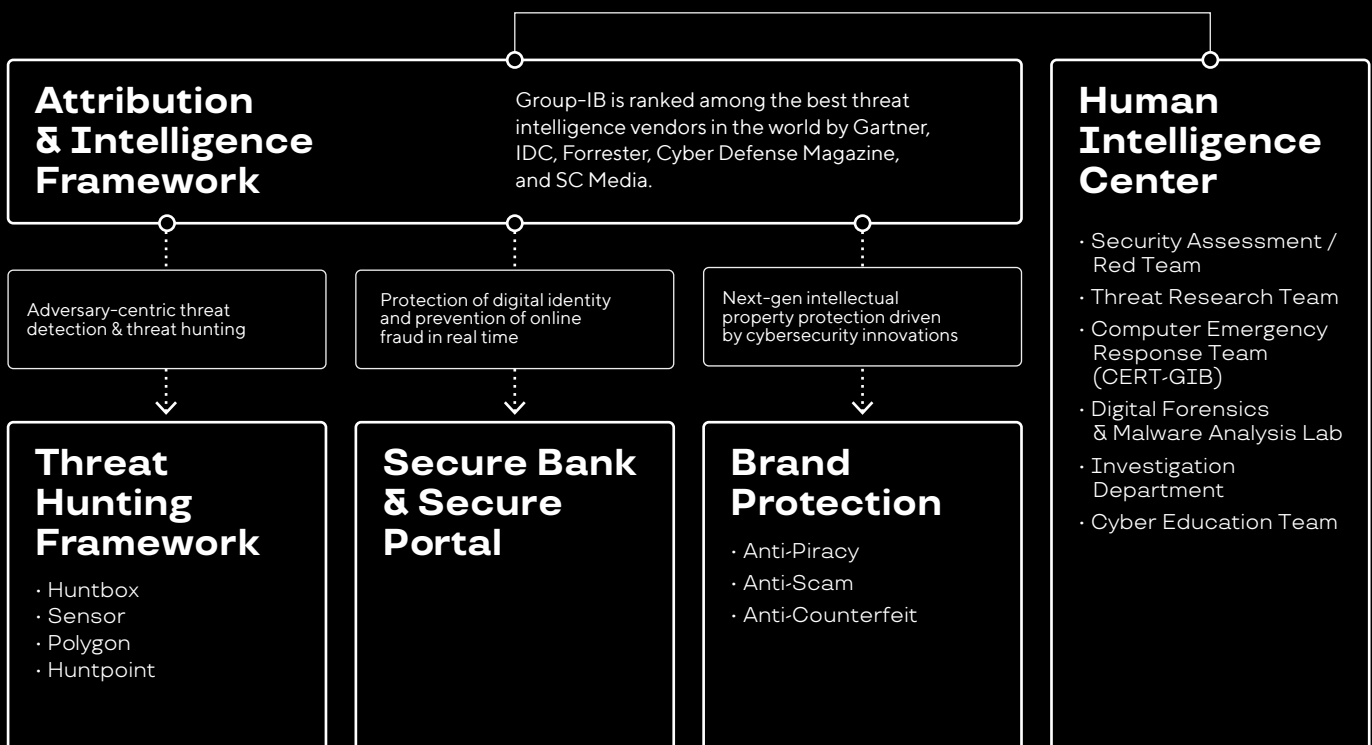
## 24/7 RESPONSE AND SUPPORT

Our certified CERT, authorized by Carnegie Mellon University, actively collaborates with other CERTs, domain registrars and hosting service providers to ensure prompt takedown of malicious hosts and fraudulent websites across the globe.

## INVESTIGATIONS AND EXPERT WITNESSING

We have successfully investigated APT & DDoS-attacks, disclosed fraud and theft, and uncovered espionage campaigns and networks of counterfeit distribution. We have sufficient technologies and knowledge at our disposal to profile and trace perpetrators, reveal their identities and secure conviction.

## Group-IB's Security Ecosystem



**PREVENTING AND  
INVESTIGATING  
CYBERCRIME  
SINCE 2003**