GROUP-IB

HI-TECH CRIME TRENDS 2021/2022

FINANCIAL SECTOR THREATS

Access Brokers
Corporansom
Financial Sector Threats
Cyberwarfare
Scams and phishing

DISCLAIMER

1. The report was written by Group-IB experts without any third-party funding.
2. The report provides information on the tactics, tools, and infrastructure of the various groups. The report's goal is to minimize the risk of the groups committing further illegal acts, suppress any such activity in a timely manner, and raise awareness among readers. The report also contains recommendations on how to protect against future attacks. The details about threats are provided solely for information security specialists so that they can familiarize themselves with them, prevent similar incidents from occurring in the future, and minimize potential damage. Any information outlined in the report is not intended to advocate fraud or other illegal activities in the field of high technologies or any other fields.
3. The report is for information purposes only and is limited in distribution. Readers are not authorized to use it for commercial purposes and any other purposes not related to education or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.
4. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use the information or other content without the right owner's prior written consent.
5. If Group-IB's copyright is violated, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the perpetrator as provided by law, including recovery of damages.

HI-TECH CRIME TRENDS 2021/2022

Big money: threats to financial sector

PART 3

A look at the cyber threat landscape: ransomware attacks, carding activity, network access sales, phishing and scams

TABLE OF CONTENTS

GROUP-IB HI-TECH CRIME TRENDS REPORT

00

The Hi-Tech Crime Trends report analyzes cyberattacks, examines how the cybercrime industry functions, and forecasts upcoming changes in the threat landscape for various sectors of the global economy. Group-IB has published the report every year since 2012, integrating valuable data and key insights that the team has gained through over 70,000 hours of experience in responding to cybersecurity incidents worldwide.

The information provided in Hi-Tech Crime Trends enables businesses, NGOs, governments, and law enforcement agencies around the world to fight cybercrime and help potential victims. Intended for IT directors, heads of cybersecurity teams, SOC analysts, incident responders, and other security professionals, the Hi-Tech Crime Trends report serves as a practical guide for strategic and tactical planning.

With the use of unique tools for tracking threat-actor infrastructures and the careful analysis of globally-distributed specialists, Group-IB experts identify and confirm patterns of cyber threats each year. This information serves as a basis for forecasts, which have proven accurate every year since the first Hi-Tech Crime Trends report was published. These forecasts help companies around the world build effective cybersecurity strategies with relevant threats in mind.

The forecasts and recommendations contained in Hi-Tech Crime Trends are aimed at reducing financial losses and infrastructure downtime. They are also designed to help organizations take preventive measures to counteract targeted attacks, espionage, and cyber-terrorism operations.

Group-IB strongly believes that the continual exchange of data, combined with lasting partnerships between private companies and international law enforcement agencies, is the most effective way to combat cybercrime. Cybersecurity awareness helps preserve and protect digital spaces and freedom of communication. It is to these ends that the Hi-Tech Crime Trends report is published.

INTRODUCTION 01

Organizations in the financial sector face a hostile threat landscape, as they are often the preferred targets of profit-seeking cybercriminals. To properly protect their networks, infrastructure, and data, security teams at financial institutions must have access to the latest intelligence on the most common attacks, how they are carried out, and which bad actors are responsible. This report provides precisely this information in order to help finance industry organizations stay one step ahead of threat actors.

In the second half of 2020 and the first half of 2021, one cyber threat stood out as the most damaging to financial sector organizations: ransomware. Group-IB experts have carefully monitored and analyzed this major issue, finding that threat actors are demanding huge ransoms, sometimes as much as $70 million, from their victims. The negative impact of ransomware attacks are unprecedented.

The staggering growth in ransomware use is closely related to another current trend: an increasing number of threat actors are selling access to compromised networks. Stolen access rights can be used both to conduct targeted attacks and to spread ransomware and other malware. During the reporting period from the second half of 2020 to the first half of 2021, **Group-IB Threat Intelligence** experts identified 95 cases of threat actors selling access to systems belonging to financial companies located in Australia, Brazil, UK, Germany, Egypt, India, Iran, Spain, Italy, Canada, China, Mexico, Nigeria, UAE, Paraguay, Portugal, Russia, Saudi Arabia, Singapore, US, Thailand, Philippines, France, Chile, and Japan. In most cases, the cybercriminals advertised access to American banks and financial institutions.

Group-IB also looked into the market for phishing and affiliate programs. Even though this type of activity has been practiced in the underground since as early as 2017, the current number of affiliate programs is at an historic peak.

Another significant threat is the distribution of fake payment pages that use legal bank transactions to transfer customers' money to accounts controlled by the threat actors.

In Russia, after a long pause, attacks on AWS CBR (Automated Work Station Client of the Russian Central Bank) have once again become a pressing issue. In early 2021, a group called **MoneyTaker** is assumed to have stolen from a Russian bank.

Among other financially motivated threat groups, the one known as **OPERA1ER** (aka DESKTOP-GROUP, Common Raven, and NXSMS), which has attacked banks, financial institutions, and telecommunications companies in Africa, Asia, and Latin America, are highlighted in this report. In the future, OPERA1ER is likely to scale up and add other regions to its list.

Group-IB experts assessed the current state of the carding market by analyzing the activities of major card shops, marketplaces where criminals sell compromised bank card data. The market has shrunk due to the largest card shop, Joker's Stash, closing down.

As always, Group-IB investigated the activity of banking Trojans for PC and Android. Most banking Trojans that were active from the second half of 2020 to the first half of 2021 were developed by Russian threat actors. Latin American malicious actors created only a small number of the banking Trojans developed in the reporting period, but the banking Trojan market in Latin America is on the rise.

Group-IB experts studied the 11 most dangerous phishing kits. Many are based on the source code of a framework called **U-Admin**.

During the reporting period, the number of JS sniffer families detected reached **98**, with **42** of them being active during this time. JS sniffers pose the most risk to online retailers. Last year, they were used to compromise more than **80,000** bank cards belonging to customers of online stores.

MAIN TRENDS 02

THE MARKET FOR ACCESS TO CORPORATE NETWORKS HAS GROWN

The market for access to corporate networks has grown significantly. Compared to the previous period, the number of initial access brokers (IABs) has increased from **18 to 47** , while the number of known sale incidents went up from **31** to **95**.

THE NUMBER OF BANK CARDS FOR SALE IS DECREASING

2021 saw a drastic decrease in the number of bank cards put up for sale. One of the key reasons for this decline is the closure of Joker's Stash, a major card shop for selling compromised bank cards that accounted for 40% of the global carding market. In addition to Joker's Stash, more than 10 smaller card shops shut down in 2021. That said, the share of bank cards put up for sale by other card shops remained the same.

THE FAKE PAYMENT PAGES MARKET IS EVOLVING

The fake payment pages market has evolved recently. In Russia alone, the financial damage caused by such attacks amounted to almost $43.4 million per year. In the reporting period, more than 40 million card transaction confirmation requests were made on phishing websites.

PHISHING AFFILIATE PROGRAMS ARE BECOMING MORE AND MORE POPULAR

Phishing and fraudulent affiliate programs are becoming more and more popular. Group-IB experts believe that there currently are more than 70 fake programs. In the reporting period, their joint profit amounted to at least $10 million.

NEW JS OBFUSCATION TECHNIQUES ARE EMERGING

JS sniffer operators have shifted to new obfuscation techniques because the methods they used before no longer allow them to keep the code hidden from antivirus tools for long enough.

JS SNIFFERS ARE BEING DELIVERED USING LEGITIMATE SERVICES

It is increasingly common for threat actors to try new ways of delivering malicious code and exfiltrating data. To do so, they use legitimate services such as Google Tag Manager, Google Apps Script, and Telegram.

BANKING TROJANS FOR PC ARE DISAPPEARING

The market for desktop banking Trojans is gradually disappearing. Latin America remains the only region where they still pose a serious risk, but, even there, only two new viruses were detected during the reporting period.

BANKING TROJANS FOR ANDROID REMAIN ACTIVE

The market for Android banking Trojans has not changed significantly. However, three new Trojans were detected: **Ghimob** (mostly active in Latin America), FluBot (in Europe), and TeaBot aka Anatsa (in Europe and Russia). The most widely used Android Trojans, **FluBot** and **TeaBot**, have become a significant threat. Their creators shape their operations based on the affiliate program model, thereby attracting many hackers from various regions, especially those who have experience in spreading Android Trojans and using them to commit theft.

HACKERS ARE USING TELEGRAM BOTS AND BUYING PHISHING FRAMEWORKS

As a rule, threat actors who use phishing frameworks do not develop them from scratch but rather buy ready-to-use products. Many popular phishing sites are based on the source code of older, well-known models such as **U-Admin** and **Kr3pto**. Threat actors have started to steal data via Telegram bots, whereas in the past, they mainly used email. It is worth noting that threat actors often attack banks (and their clients) based in the same regions that the hackers themselves live. This trend was observed in the Netherlands and Spain.

INTER: THE MOST POPULAR JS SNIFFER

Inter is one of the most popular JS sniffers sold on underground forums. Dozens of threat actors have used it to steal bank cards.

THE NUMBER OF RANSOMWARE ATTACKS ON FINANCIAL COMPANIES HAS INCREASED

Ransomware attacks on financial institutions have become more common. In the reporting period, **127** ransomware attacks were identified compared to less than **50** in the previous period.

FORECASTS

CARDING WILL BECOME LESS APPEALING FOR THREAT ACTORS

Carding will become less appealing for threat actors. Given that many card shops have been closed closed, Group-IB expects the number of bank cards put up for sale to go down with time. This will mostly affect the selling of dumps.

THE NUMBER OF PHISHING FRAMEWORKS WILL GROW

The number of phishing frameworks is expected to grow, with one of the reasons being that banks are implementing multi-factor authentication more and more often.

THE PHISHING-AS-A-SERVICE FORMAT WILL CONTINUE TO EVOLVE

The phishing-as-a-service format will continue to evolve. This will mean that even threat actors who cannot develop their own tools will be able to carry out attacks. Threat actors will offer phishing infrastructure for rent (on a weekly or monthly basis). Such offers will include a comprehensive package of services: phishing kit/framework, domain name, hosting service, security pack against bots and website blockage, and technical support. This business model is already used in the Netherlands, and it could spread to other regions in the future.

JS SNIFFERS CONTINUE TO BE THE MAIN THREAT FOR THE ONLINE RETAIL SECTOR

Threat groups who use JS sniffers are likely to become a main threat for the online retail sector, especially in the US. This will affect smaller enterprises that work with platforms such as Magento and OpenCart. The main risks will be related to security violation fees, not to reputational losses or compensating for losses incurred by clients.

EXPERIMENTS WITH JS SNIFFERS WILL CONTINUE

JS sniffer operators will continue experimenting with various methods to deliver code and transfer stolen data. They will also continue developing automated code obfuscation methods. The Inter sniffer family will remain the most widely used.

PHISHING FRAMEWORKS WILL TARGET NEW REGIONS

While in the past phishing frameworks mainly targeted European banks, in the near future this threat will become relevant for the Asia-Pacific region and North America.

TELEGRAM: THE MOST POPULAR TOOL AMONG CYBERCRIMINALS

Telegram will become the most widely used tool for obtaining compromised data from phishing websites.

MONEYTAKER WILL CONTINUE TO ATTACK IN RUSSIA

After a long break, MoneyTaker carried out a successful attack on a Russian bank. The threat actors will likely not stop there and will attack other entities.

CARDING WILL BECOME LESS APPEALING FOR THREAT ACTORS

Carding will become less appealing for threat actors. Given that many card shops were closed, Group-IB expects the number of bank cards put up for sale to go down with time. This will mostly affect the selling of dumps.

THE NUMBER OF PHISHING AND FRAUD-RELATED AFFILIATE PROGRAMS WILL GROW

Phishing and fraud-related affiliate programs are likely to become more popular. Currently, they mainly mimic delivery services and marketplaces. In the future, however, threat actors will step up the development of phishing affiliate programs targeted at the financial sector. This type of fraud could become a technologically advanced replacement of calls from fake call centers.

CRYPTOCURRENCY IS UNDER THREAT

The number of phishing attacks aimed at stealing cryptocurrency is expected to increase.

SALE OF ACCESS TO FINANCIAL ORGANIZATIONS

04

Over the past four years, one of the clearest trends on underground forums is a sharp increase in the number of offers to sell access to compromised corporate networks.

Corporate networks can be accessed using Citrix Gateway (later simply referred to as Citrix), VPN and RDP account data; control panels; web shells; reverse shells; Cobalt Strike sessions; and more. Regardless of access type, gaining initial access enables threat actors to penetrate the target company's network and obtain legitimate user or administrator rights.

The access market has a low threshold. A threat actor can gain access by using a type of malware called an information stealer, brute force, or by carrying out a targeted attack. The latter requires in-depth knowledge and skills, while the former two are available to low-skilled threat actors who cannot independently develop a profitable attack. In the case of information stealers, threat actors do not even need to think about how to deliver the malware to the target: the "results" of information stealer activity are sold on underground forums as archives containing various compromised credentials, both personal and corporate. Within that data, threat actors only need to find active accounts for corporate resources. The brute-force scenario does not require much knowledge, either: ready-made programs for brute-forcing passwords are publicly available. Attackers merely pick their victim.

The fact that tools for conducting full-fledged attacks against corporate networks are widely available means that underground actors can make money with almost no risk or effort. The market for initial selling access has been flooded with low-skilled threat actors who, despite their poor knowledge of the technical aspects involved, pose a threat to companies.

The unauthorized initial access market includes data belonging to private and state companies across various industries. This report focuses on banks and financial institutions. To learn more about the market for unauthorized access to compromised corporate resources, see the report **Uninvited guests: the sale of access to corporate networks**.

In the last year, the number of offers to sell access to banks and financial institutions increased by almost **206 percent**, from 31 (H2 2019 – H1 2020) to 95 (H2 2020 – H1 2021). The number of initial access brokers (IABs) selling access to financial institutions also more than doubled, from 18 to 47.

Uninvited guests: the sale of access to corporate networks

The total cost of access to financial sector companies offered for sale in H2 2020 — H1 2021 was $530,000. Most frequently, their victims were US-based banks and financial institutions (22 instances of access being sold).

Offer publication date (MM/DD/YYYY)	IAB's alias	Victim company's country	Access price (USD)	Victim company's revenue (USD mln)
07/01/2020	vasyldn	UK	1,500	
07/06/2020	drumrlu	Thailand		
07/13/2020	pshmm	Portugal	2,500	
07/13/2020	pshmm	Canada	2,500	
07/15/2020	drumrlu	Saudi Arabia	3,000	
07/27/2020	vasyldn	UK	5,000	
07/27/2020	vasyldn	Mexico	500	
07/29/2020	EronM	Singapore	12,000	3,000
08/04/2020	EronM	US	6,500	3,200
08/04/2020	vasyldn	UK	5,800	
08/04/2020	vasyldn	Mexico	600	
08/12/2020	bc.monster	Brazil	2,000	
08/21/2020	r41s3r	Paraguay	3,000	
08/25/2020	itrade4living	Australia	2,500	5,460
08/25/2020	Nikolay (aka Marlon_Brando aka LinuxW)	US	20,000	
08/26/2020	EronM	France	5,000	22,000
09/04/2020	davidarnold0151	Japan		
09/05/2020	r0t	Australia	10,000	
09/12/2020	pshmm	USA	1,500	6
09/13/2020	petervodz (aka johnakamai)	Canada	400	10
09/13/2020	petervodz (aka johnakamai)	Canada	800	25
09/15/2020	pshmm	UK	1,750	232
09/17/2020	drumrlu	Thailand	2,000	
09/19.2020	drumrlu	Vietnam	3,000	
09/19/2020	pshmm		2,000	17
09/21/2020	NetNet	US	700	35
09/23/2020	NetNet	US	700	35
09/25/2020	vasyldn	Mexico	5,000	
09/27/2020	Andreich_kms	France	100	1
09/27/2020	Andreich_kms	Spain	100	2
09/27/2020	Andreich_kms		100	10
09/27/2020	drumrlu	Thailand	1,000	140

Offer publication date (MM/DD/YYYY)	IAB's alias	Victim company's country	Access price (USD)	Victim company's revenue (USD mln)
10/03/2020	Zorbon	Iran	12,000	
10/08/2020	magicman1337	Russia		
10/11/2020	3073a (aka DarkGod3)	China	4,000	49
10/11/2020	magicman1337			100,000
10/12/2020	Medusa23	Nigeria	4,000	9,000
10/17/2020	bryanross		11,500	1,000
10/24/2020	iannker	US	10,000	
10/26/2020	artur11	Philippines		
10/30/2020	3073a (aka DarkGod3)	Italy	3,000	2
11/06/2020	pshmm	US	1,500	6
11/07/2020	LORD1			50,000
11/08/2020	artur11	Philippines	2,400	
11/11/2020	drumrlu	UAE	2,000	800
11/11/2020	drumrlu	Saudi Arabia	2,000	15
11/23/2020	Cipher-Strike	UAE		
12/02/2020	zanko	India	20,000	
12/02/2020	JxB1990	US	600	5
12/02/2020	pshmm	US	2,000	
12/07/2020	realname	US	4,999	
12/09/2020	Medusa23	UAE		
12/12/2020	zanko	India	4,000	49
12/13/.2020	SHERIFF		23,500	1,000
12/13/2020	SHERIFF		23,500	1,000
12/13/2020	SHERIFF		23,500	1,000
12/13/2020	SHERIFF		23,500	1,000
12/13/2020	SHERIFF		23,500	
12/13/2020	SHERIFF		23,500	
12/13/2020	SHERIFF		23,500	
12/13/2020	SHERIFF		23,500	
12/17/2020	JPDeadly	Germany		400
12/24/2020	maroder	Chile	7,000	1,000
12/25/2020	barf	US	100	1
01/04/2021	x_04X		1,500	
01/05/2021	EvilKitten	Iran	7,000	100
01/27/2021	7h0rf1nn	France	1,000	
01/29/2021	zanko	India	500	5
02/09/2021	Expl0i7	US	5,000	

Offer publication date (MM/DD/YYYY)	IAB's alias	Victim company's country	Access price (USD)	Victim company's revenue (USD mln)
02/24/2021	cc2btc		10,000	79,000
02/28/2021	barf	Iran	1,500	1,700
03/01/2021	pshmm	Canada	500	
03/02/2021	Aristokrat	Thailand		
03/08/2021	Nei	US	300	5
03/14/2021	drumrlu	US	1,000	19
03/15/2021	vasyldn	US	5,000	
03/16/2021	vasyldn	US	2,000	
03/16/2021	vasyldn	US	10,000	
03/19/2021	vasyldn	US	20,000	
03/22/2021	babam	Mexico	150	4
03/29/2021	drumrlu	India	1,500	41
04/14/2021	groupby	US	2,500	18
04/19/2021	novichok2021	Italy	100	2
04/23/2021	gospoda		5,000	
04/26/2021	babam	UAE	1,000	2,000
04/27/2021	NaMneCash	Egypt		
05/07/2021	fab1us	Egypt		2,000
05/08/2021	zanko	India	5,000	
05/08/2021	Suraj	India	3,000	3,400
05/10/2021	scredou	UAE	10,000	1,000
05/18/2021	Novelli	US	300	1
05/28/2021	vasyldn	US	50,000	1,000
05/29/2021	Alexlogin	Australia	1,000	
06/26/2021	babam	UK	5,000	
06/28/2021	T3atral	US	500	

One of the main factors driving growth for the initial access market is the steep increase in the number of ransomware attacks. IABs remove the need for ransomware operators to breach and penetrate corporate networks at the first stage of attack.

RANSOMWARE ATTACKS AGAINST FINANCIAL INSTITUTIONS

05

Group-IB Threat Intelligence experts observed a significant increase in the number of ransomware attacks against financial institutions. In the reporting period (H2 2020 - H1 2021), **127 attacks** of this type were detected, while a year ago (H2 2019 — H1 2020) the number was **less than 50.**

Group-IB identified **24 groups** who carried out attacks against organizations in the financial sector. The most prolific among them were **REvil**, **Conti**, and **Avaddon**. Most victim companies are located in the US (**66**). Canada and the UK (**12**) share second place. France (**8**) is third.

Detailed information can be found in the table below:

Attack date (MM/DD/YYYY)	Industry	Headquarters location	Ransomware group
07/13/2020	Financial Services	US	DoppelPaymer
08/08/2020	Financial Services	US	Darkside
08/18/2020	Financial Services: Accounting	US	REvil
08/18/2020	Financial Services	US	REvil
08/18/2020	Financial Services: Insurance	US	REvil
08/19/2020	Financial Services: Accounting	US	NetWalker
08/20/2020	Financial Services	US	REvil
08/20/2020	Financial Services: Accounting	Canada	REvil
08/20/2020	Financial Services	India	Clop
08/20/2020	Financial Services: Accounting	UK	REvil
08/24/2020	Financial Services	Hong Kong	REvil
08/30/2020	Financial Services	US	NetWalker
09/02/2020	Financial Services: Insurance	US	DoppelPaymer
09/14/2020	Financial Services: Insurance	US	Conti
09/25/2020	Financial Services: Insurance	US	Egregor
09/25/2020	Financial Services: Insurance	US	Conti
09/28/2020	Financial Services: Accounting	US	MAZE

Attack date (MM/DD/YYYY)	Industry	Headquarters location	Ransomware group
10/08/2020	Financial Services	Canada	NetWalker
10/14/2020	Financial Services: Accounting	Trinidad and Tobago	REvil
10/20/2020	Financial Services: Accounting	US	Conti
10/20/2020	Financial Services: Insurance	US	Egregor
10/20/2020	Financial Services: Accounting	France	Egregor
10/20/2020	Financial Services: Insurance	US	Egregor
10/20/2020	Financial Services: Insurance	US	Egregor
10/22/2020	Financial Services: Insurance	US	REvil
10/26/2020	Financial Services: Insurance	US	Darkside
11/01/2020	Financial Services	Canada	Pysa
11/06/2020	Financial Services	US	Egregor
11/14/2020	Financial Services: Banking	US	Avaddon
11/18/2020	Financial Services: Insurance	US	Egregor
11/20/2020	Financial Services: Accounting	US	Egregor
11/21/2020	Financial Services: Insurance	UK	Egregor
11/23/2020	Financial Services	Italy	Pysa
11/25/2020	Financial Services	Spain	NetWalker
11/26/2020	Financial Services	Zimbabwe	Egregor
11/27/2020	Financial Services: Accounting	Canada	NetWalker
11/28/2020	Financial Services: Accounting	UK	NetWalker
12/02/2020	Financial Services: Banking	US	Egregor
12/03/2020	Financial Services: Banking	India	Everest
12/09/2020	Financial Services: Accounting	Canada	Conti
12/11/2020	Financial Services	India	Egregor
12/11/2020	Financial Services	New Zealand	NetWalker
12/18/2020	Financial Services	US	Egregor
12/19/2020	Financial Services: Insurance	US	Conti
12/28/2020	Financial Services: Accounting	US	Ragnarok
12/30/2020	Financial Services	Belgium	Avaddon
01/08/2021	Financial Services: Insurance	Canada	DoppelPaymer
01/11/2021	Financial Services	US	Conti
01/14/2021	Financial Services	US	NetWalker
01/20/2021	Financial Services	US	Darkside
01/25/2021	Financial Services: Accounting	US	NetWalker
01/25/2021	Financial Services	Luxemburg	DoppelPaymer
01/28/2021	Financial Services	Hong Kong	RansomEXX
01/30/2021	Financial Services: Accounting	Italy	Pysa
02/01/2021	Financial Services: Insurance	Indonesia	Avaddon

Attack date (MM/DD/YYYY)	Industry	Headquarters location	Ransomware group
02/03/2021	Financial Services: Insurance	France	Avaddon
02/04/2021	Financial Services: Banking	US	Darkside
02/08/2021	Financial Services: Insurance	US	REvil
02/11/2021	Financial Services	US	Pysa
02/15/2021	Financial Services: Accounting	US	Avaddon
02/18/2021	Financial Services	US	Cuba
02/22/2021	Financial Services: Accounting	US	Everest
02/22/2021	Financial Services: Insurance	Mexico	Nefilim
02/22/2021	Financial Services	Canada	DoppelPaymer
02/26/2021	Financial Services: Banking	Nigeria	REvil
02/27/2021	Financial Services: Banking	Mexico	REvil
02/28/2021	Financial Services: Accounting	US	Lorenz
02/28/2021	Financial Services	Jamaica	Darkside
03/02/2021	Financial Services: Banking	Indonesia	Darkside
03/02/2021	Financial Services: Insurance	US	REvil
03/06/2021	Financial Services: Insurance	US	REvil
03/08/2021	Financial Services: Banking	US	Clop
03/09/2021	Financial Services: Insurance	US	REvil
03/09/2021	Financial Services: Banking	US	Ragnar Locker
03/09/2021	Financial Services: Banking	US	Ragnar Locker
03/11/2021	Financial Services: Insurance	US	Babuk v.1
03/12/2021	Financial Services: Accounting	US	DoppelPaymer
03/13/2021	Financial Services: Insurance	US	Darkside
03/14/2021	Financial Services: Accounting	US	LV v.1
03/14/2021	Financial Services: Accounting	US	LV v.2
03/16/2021	Financial Services	US	Conti
03/17/2021	Financial Services	Canada	Conti
03/20/2021	Financial Services: Insurance	US	Darkside
03/23/2021	Financial Services: Accounting	US	Clop
03/23/2021	Financial Services: Banking	US	REvil
03/23/2021	Financial Services: Banking	US	REvil
03/28/2021	Financial Services	Spain	Ragnarok
03/28/2021	Financial Services: Insurance	US	DoppelPaymer
04/04/2021	Financial Services	US	REvil
04/09/2021	Financial Services: Accounting	US	Avaddon
04/13/2021	Financial Services	US	Marketo
04/17/2021	Financial Services	US	REvil
04/18/2021	Financial Services	Germany	REvil

Attack date (MM/DD/YYYY)	Industry	Headquarters location	Ransomware group
04/19/2021	Financial Services	Spain	Avaddon
04/22/2021	Financial Services	UK	Conti
04/22/2021	Financial Services: Accounting	UK	Conti
05/01/2021	Financial Services	Canada	REvil
05/10/2021	Financial Services	Salvador	Prometheus
05/12/2021	Financial Services	France	Avaddon
05/13/2021	Financial Services	Italy	Babuk v.1
05/13/2021	Financial Services	UK	Avaddon
05/15/2021	Financial Services: Insurance	France	Avaddon
05/18/2021	Financial Services: Insurance	US	Conti
05/20/2021	Financial Services	France	Prometheus
05/20/2021	Financial Services: Accounting	UK	Conti
05/20/2021	Financial Services	UK	Conti
05/20/2021	Financial Services	UK	Avaddon
05/20/2021	Financial Services: Accounting	Cyprus	Avaddon
05/28/2021	Financial Services	Jamaica	Avaddon
05/28/2021	Financial Services: Accounting	UK	REvil
05/31/2021	Financial Services	France	Everest
06/01/2021	Financial Services	Canada	Grief
06/03/2021	Financial Services: Insurance	US	Vice Society
06/05/2021	Financial Services: Accounting	UK	Conti
06/08/2021	Financial Services: Banking	US	Avaddon
06/12/2021	Financial Services: Insurance	US	REvil
06/14/2021	Financial Services: Accounting	US	REvil
06/14/2021	Financial Services	Canada	REvil
06/15/2021	Financial Services	Brazil	Prometheus
06/16/2021	Financial Services	US	Conti
06/19/2021	Financial Services: Accounting	South Africa	REvil
06/19/2021	Financial Services: Accounting	UK	REvil
06/21/2021	Financial Services	France	Everest
06/21/2021	Financial Services	Mexico	LV v.1
06/23/2021	Financial Services: Accounting	France	Conti
06/25/2021	Financial Services: Insurance	Canada	Conti
06/25/2021	Financial Services: Insurance	US	Conti

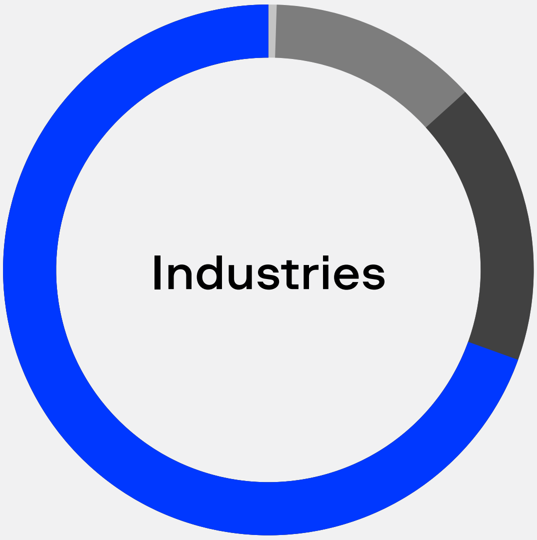
PHISHING AND SCAM AFFILIATE PROGRAMS

06

In the last few years, phishing and scam affiliate programs have become highly popular. Research conducted by Group-IB shows that there are more than 70 phishing and scam affiliate programs. Participants aim to steal money, as well as personal and payment data. In the reporting period, the threat actors who took part in such schemes pocketed at least $10 million in total. On average, the amount stolen by any single threat actor is estimated at $83. The affiliate programs involve large numbers of participants, have strict hierarchy, and use complex technical infrastructures to automate fraudulent activities. This helps scale phishing campaigns and customize them for banks, popular email services, marketplaces, logistics companies, and other organizations.

Affected brands broken down by industry

Industry	%
🟦 Marketplaces	**69.6%**
■ Delivery services	**17.2%**
■ Carpooling services	**12.8%**
□ Banking services	**0.4%**



Having honed their scheme through practice against users from Russia and other CIS (Commonwealth of Independent States) countries, affiliate programs have started their online migration to Europe, America, Asia, and the Middle East. This is exemplified by **Classiscam**, a scheme that is widely used in scam affiliate programs. Currently, affiliate program members attack users in the following countries:

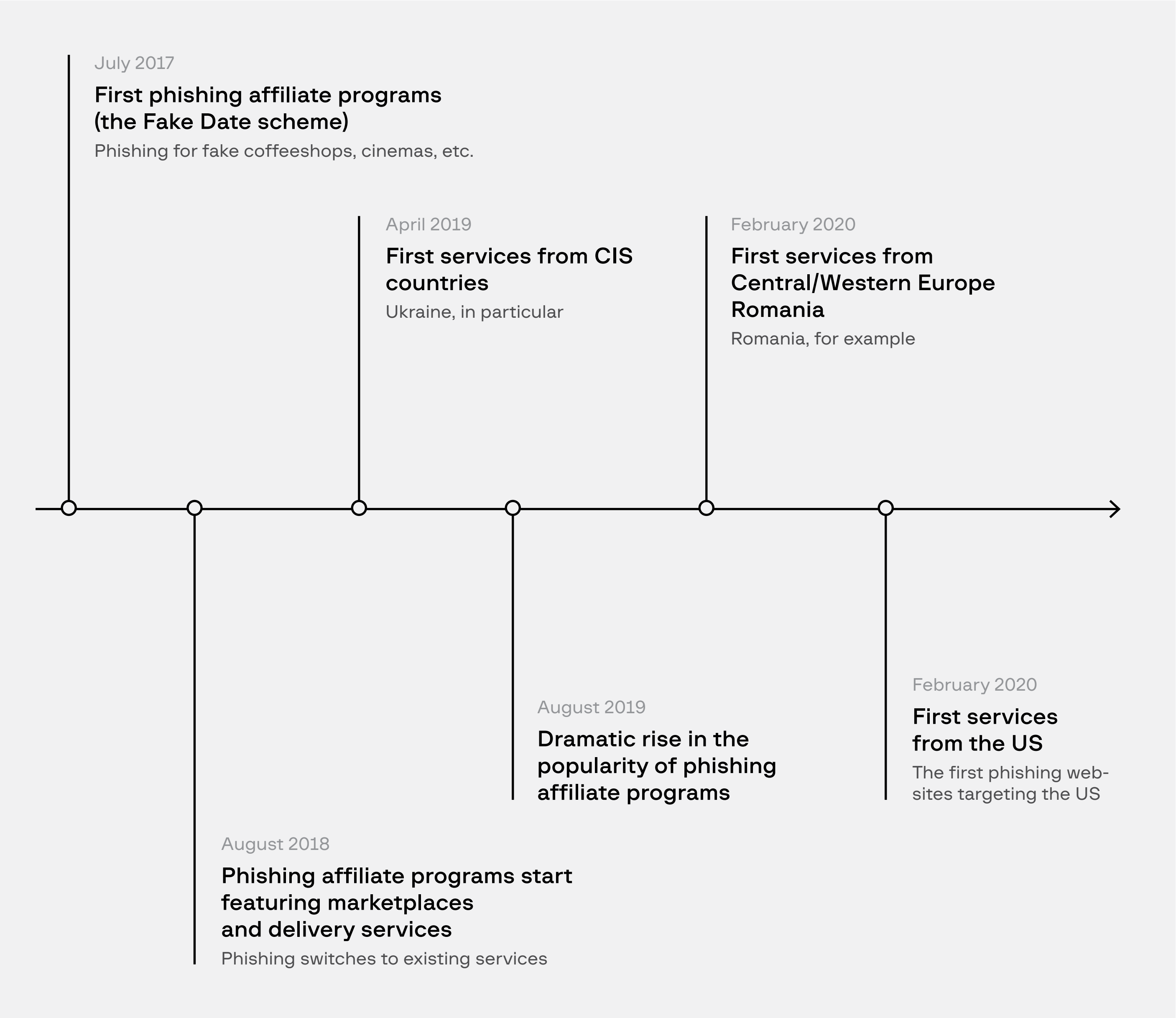
Attacks of Classiscam by country

Russia, Kazakhstan, Belarus, Romania, Poland, Ukraine, Czech Republic, Bulgaria, Uzbekistan, France, Azerbaijan, Kyrgyzstan, Moldova, Italy, Spain, Estonia, Sweden, Qatar , Other EU countries, Finland , Australia, Mexico, Philippines, Slovakia , Latvia, Lithuania, US, Georgia, Norway, Ireland, Denmark, Hungary, Cyprus, Croatia, Austria, UAE, Macedonia

31 countries

were affected by attacks of Classiscam

The first phishing affiliate programs appeared as early as 2017 and have proliferated with each year since then.


July 2017

First phishing affiliate programs (the Fake Date scheme)

Phishing for fake coffeeshops, cinemas, etc.

August 2018

Phishing affiliate programs start featuring marketplaces and delivery services

Phishing switches to existing services

April 2019

First services from CIS countries

Ukraine, in particular

August 2019

Dramatic rise in the popularity of phishing affiliate programs

February 2020

First services from Central/Western Europe Romania

Romania, for example

February 2020

First services from the US

The first phishing websites targeting the US

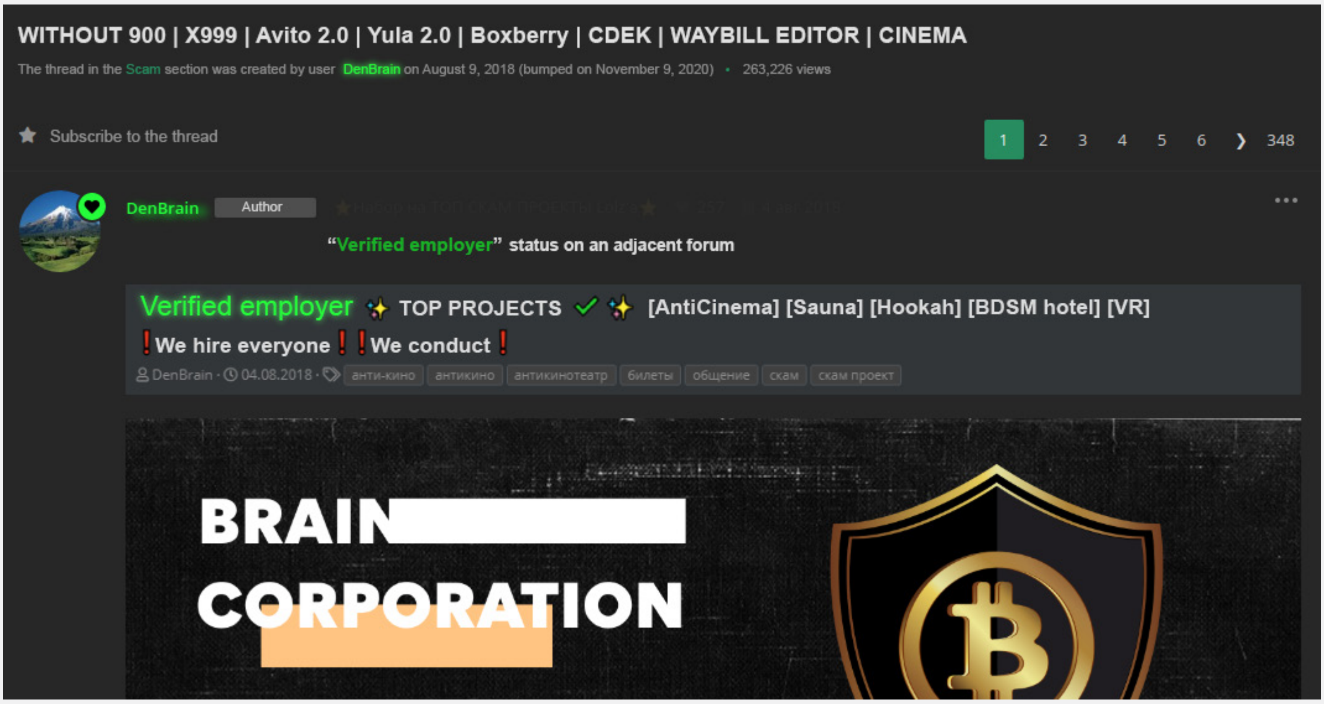
Group-IB experts point out that from 2017 to 2021, the scheme saw some considerable changes. Threat actors started using Telegram extensively. The affiliate programs began attracting a great amount of manually attracted traffic as a result of targeted steps taken with victims.

The number of attacked brands and regions increased, likely due to the following factors:

- A fear of getting caught if the same brand was imitated too often
- A limited area leads to more intense competition
- High awareness of the problem in CIS countries
- Desire to target an unoccupied niche and increase profits

Affiliate programs involve many people who can be categorized into three groups: owners, technical experts, and so-called workers.

New affiliate program members are sought on underground forums or in specific Telegram channels. For the reporting period, Group-IB experts found around **2,000 threads** on **60 underground forums** related to recruiting workers for phishing affiliate programs.



WITHOUT 900 | X999 | Avito 2.0 | Yula 2.0 | Boxberry | CDEK | WAYBILL EDITOR | CINEMA

The thread in the Scam section was created by user DenBrain on August 9, 2018 (bumped on November 9, 2020) • 263,226 views

Subscribe to the thread

1 2 3 4 5 6 ❯ 348

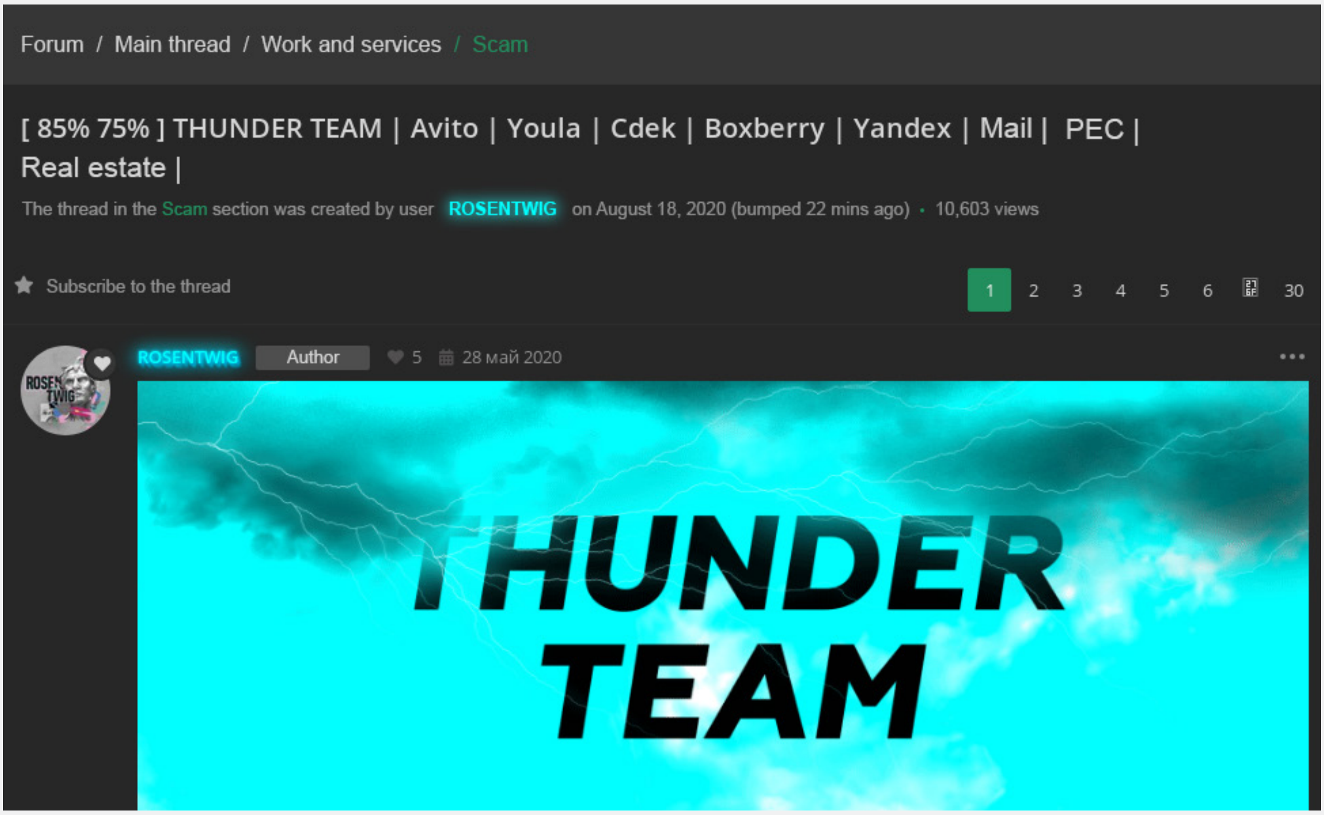
DenBrain Author

"Verified employer" status on an adjacent forum

Verified employer ✨ TOP PROJECTS ✓ ✨ [AntiCinema] [Sauna] [Hookah] [BDSM hotel] [VR]

❗We hire everyone❗❗We conduct❗

DenBrain · 04.08.2018 · анти-кино антикино антикинотеатр билеты общение скам скам проект



Forum / Main thread / Work and services / Scam

[85% 75%] THUNDER TEAM | Avito | Youla | Cdek | Boxberry | Yandex | Mail | PEC | Real estate |

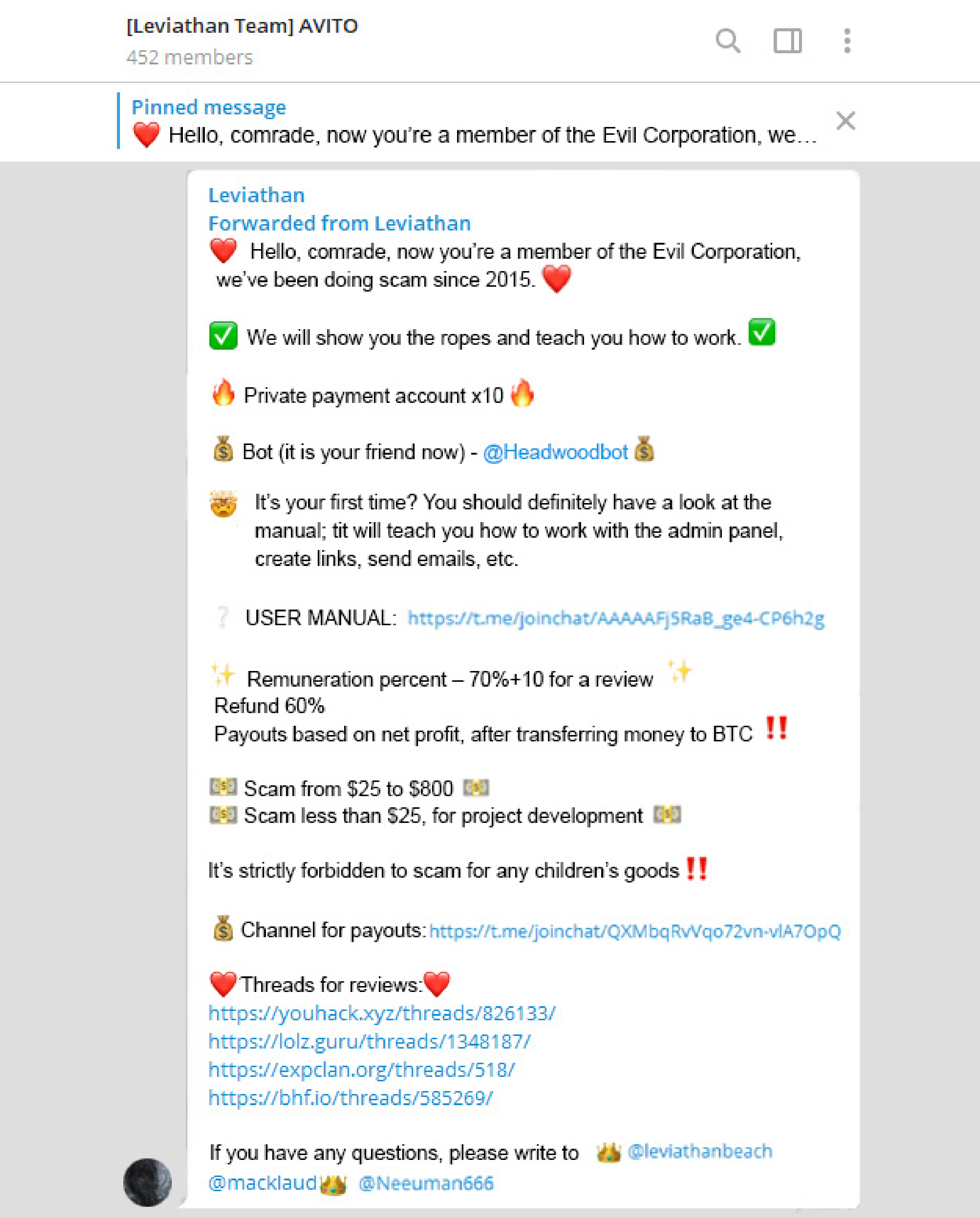
The thread in the Scam section was created by user ROSENTWIG on August 18, 2020 (bumped 22 mins ago) • 10,603 views

Subscribe to the thread

1 2 3 4 5 6 30

ROSENTWIG Author 5 28 май 2020

After becoming a member of an affiliate program, workers (low-skilled fraudsters) receive a manual with the algorithm, as well as the terms of work and access to the relevant Telegram bot. Workers are tasked with using these tools to search for new victims.



[Leviathan Team] AVITO
452 members

Pinned message
❤️ Hello, comrade, now you're a member of the Evil Corporation, we...

Leviathan
Forwarded from Leviathan

❤️ Hello, comrade, now you're a member of the Evil Corporation, we've been doing scam since 2015. ❤️

✅ We will show you the ropes and teach you how to work. ✅

🔥 Private payment account x10 🔥

💰 Bot (it is your friend now) - @Headwoodbot 💰

🤯 It's your first time? You should definitely have a look at the manual; tit will teach you how to work with the admin panel, create links, send emails, etc.

❔ USER MANUAL: https://t.me/joinchat/AAAAAFj5RaB_ge4-CP6h2g

✨ Remuneration percent – 70%+10 for a review ✨
Refund 60%
Payouts based on net profit, after transferring money to BTC ‼️

💵 Scam from $25 to $800 💵
💵 Scam less than $25, for project development 💵

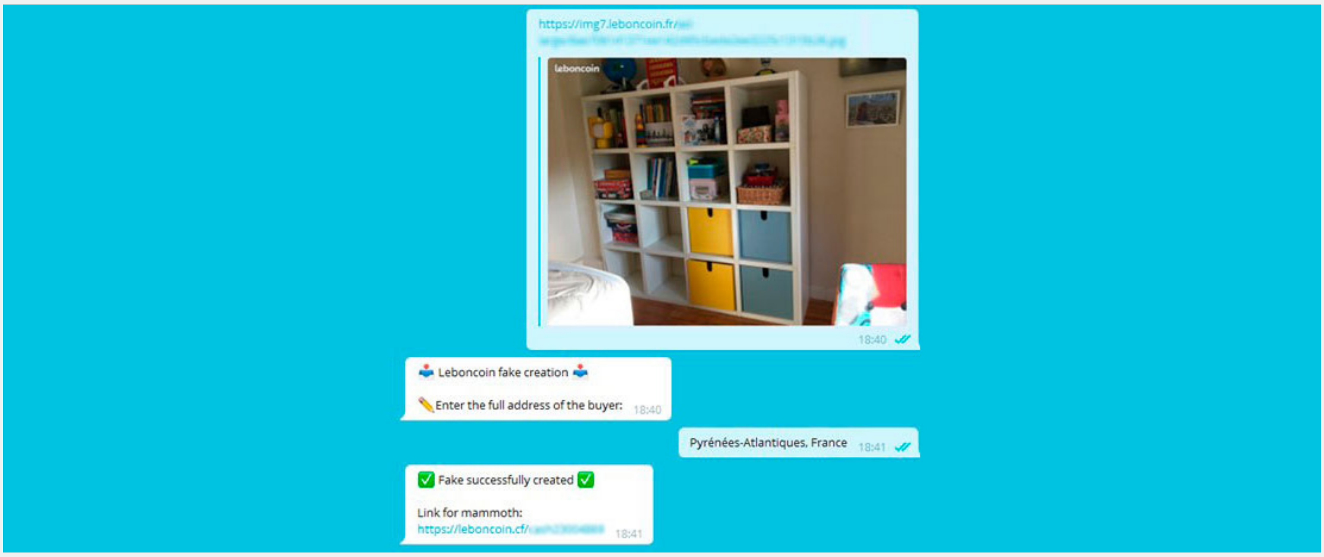
It's strictly forbidden to scam for any children's goods ‼️

💰 Channel for payouts: https://t.me/joinchat/QXMbqRvVqo72vn-vlA7OpQ

❤️Threads for reviews:❤️
https://youhack.xyz/threads/826133/
https://lolz.guru/threads/1348187/
https://expclan.org/threads/518/
https://bhf.io/threads/585269/

If you have any questions, please write to 👑 @leviathanbeach
@macklaud👑 @Neeuman666

After identifying a victim and initiating a conversation (which can be done via the chat feature on a popular marketplace), the worker lures the victim into visiting a third-party phishing website and entering their bank card details. Fraudsters try to lead their victims away from the legitimate website (the marketplace or advertisement website) because internal antifraud systems will block any phishing links shared in the chat. To avoid these controls, the scammers send messages via email. The victim receives an email with a link that leads to the phishing page, which the workers create and receive via Telegram bots.



https://img7.leboncoin.fr/[redacted]

18:40

Leboncoin fake creation

✏️Enter the full address of the buyer: 18:40

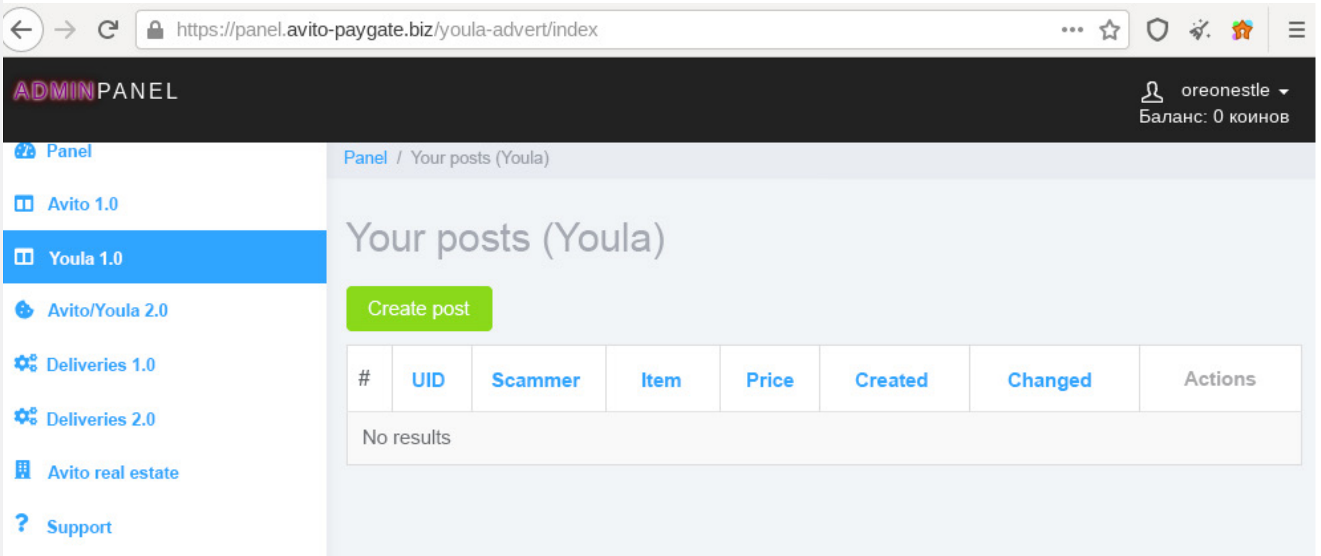
Pyrénées-Atlantiques, France 18:41

✅ Fake successfully created ✅

Link for mammoth:
https://leboncoin.cf/[redacted] 18:41

As a result of this type of scam, fraudsters steal the victim's money and bank card details.

Workers interact with the affiliate program via Telegram bots or the administrative panel.

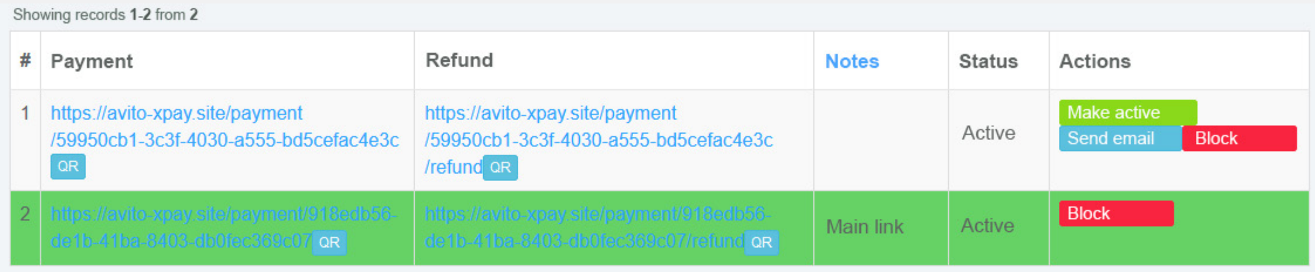


https://panel.avito-paygate.biz/youla-advert/index

Your posts (Youla)

#	UID	Scammer	Item	Price	Created	Changed	Actions
No results							

After a link is created, the panel looks like this:



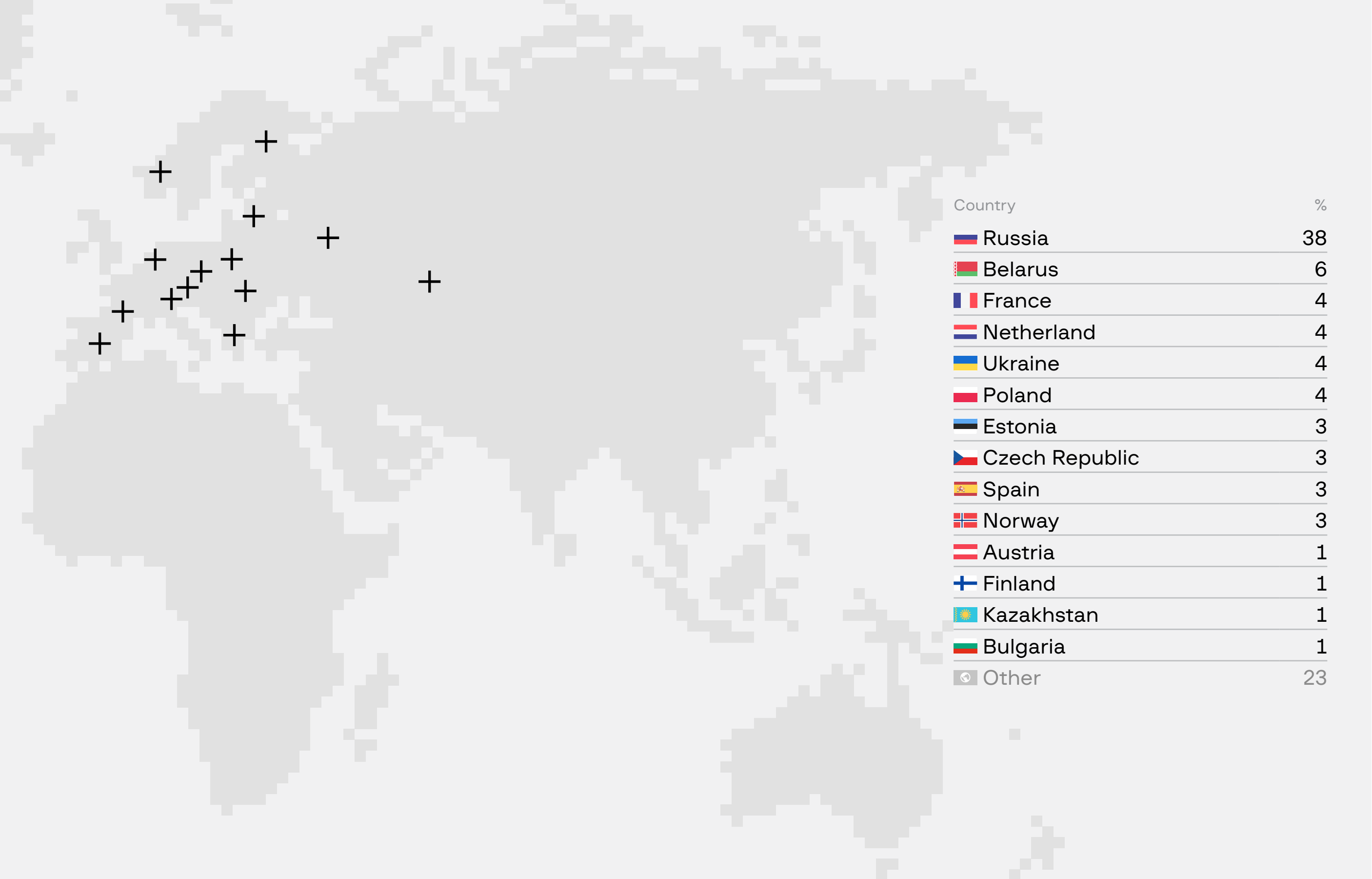
Showing records 1-2 from 2

#	Payment	Refund	Notes	Status	Actions
1	https://avito-xpay.site/payment/59950cb1-3c3f-4030-a555-bd5cefac4e3c QR	https://avito-xpay.site/payment/59950cb1-3c3f-4030-a555-bd5cefac4e3c/refund QR		Active	Make active Send email Block
2	https://avito-xpay.site/payment/918edb56-de1b-41ba-8403-db0fec369c07 QR	https://avito-xpay.site/payment/918edb56-de1b-41ba-8403-db0fec369c07/refund QR	Main link	Active	Block

The technical specialists handle tasks such as creating user manuals, phishing kits, Telegram bots, and administrative panels.

Neither owners nor technical specialists engage in the scam directly. They are responsible for ensuring that the scam affiliate program operates seamlessly. This includes organizing and maintaining the financial infrastructure designed to accept payments from victims, as well as withdrawing money via bank cards or electronic wallets that belong to money mules.

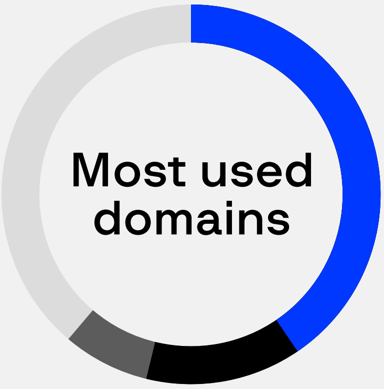
Phishing and scam affiliate programs initially focused on Russia and other CIS countries. Recently, however, Group-IB experts have identified more and more programs targeting European, Asian, Middle Eastern, and American companies. Group-IB is aware of phishing pages mimicking 71 brands from 36 countries, all created and distributed by affiliate program members.

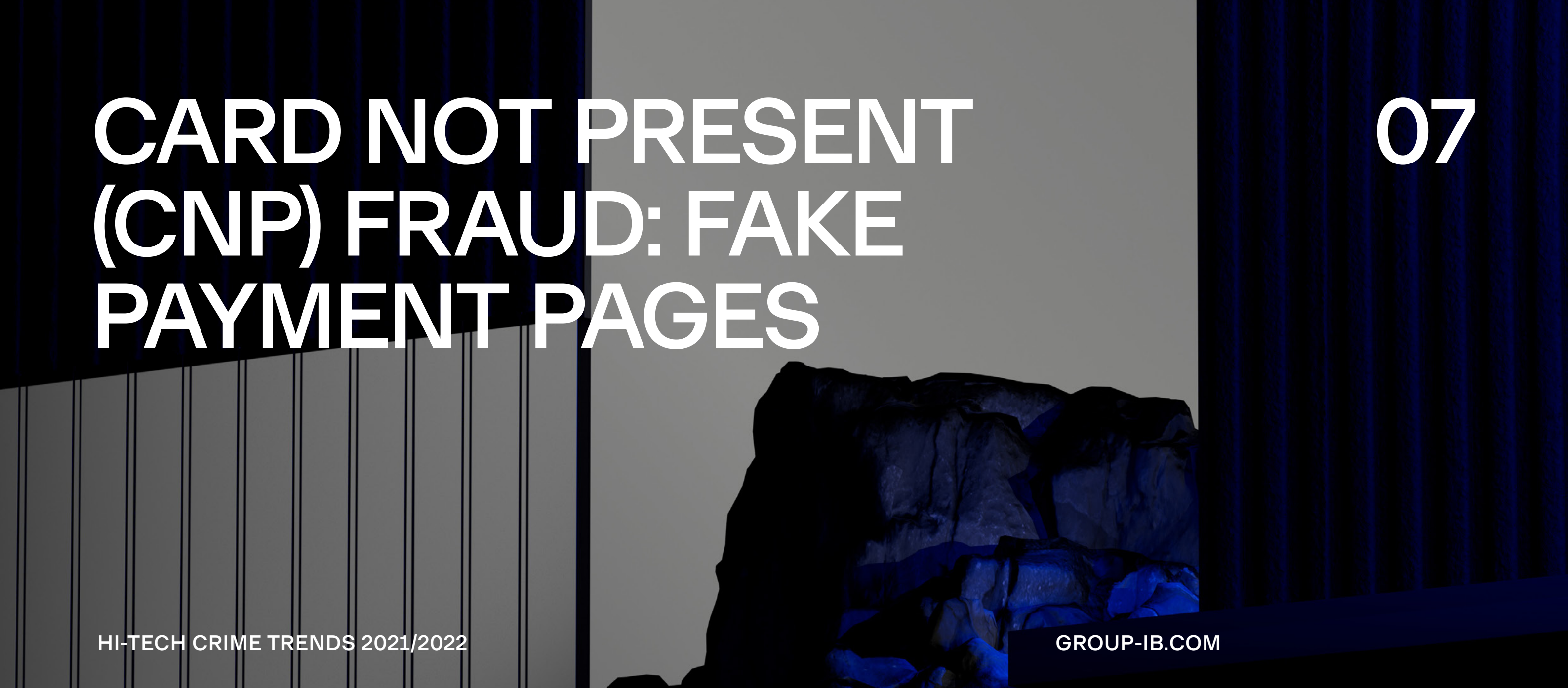


Country	%
Russia	38
Belarus	6
France	4
Netherland	4
Ukraine	4
Poland	4
Estonia	3
Czech Republic	3
Spain	3
Norway	3
Austria	1
Finland	1
Kazakhstan	1
Bulgaria	1
Other	23

Affiliate program members control more than 10,000 domain names.
Below are the most frequently used domain zones.

Domain zone	%
🟦 .ru	40.4
⬛ .online	13.3
▨ .site	7.4
.com	6.2
.su	6.0
.info	5.8
.xyz	2.8
.net	2.7
.store	2.6
.cc	1.4
Other	11.4

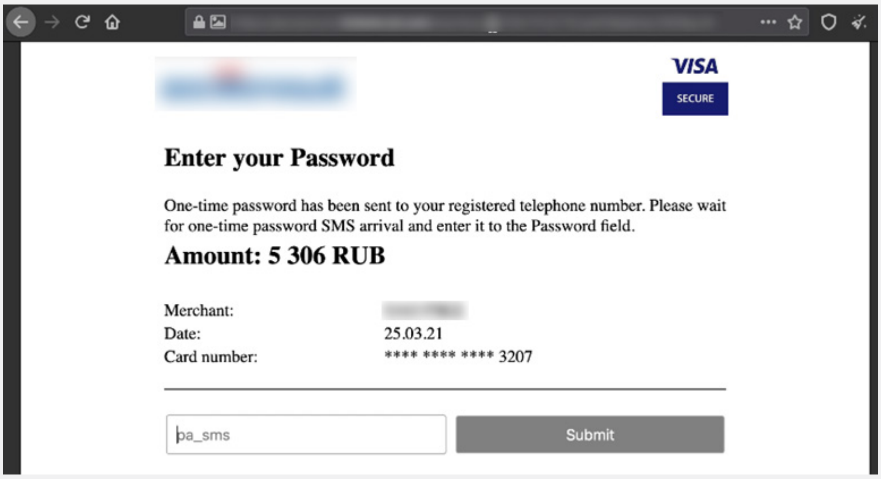




CARD NOT PRESENT (CNP) FRAUD: FAKE PAYMENT PAGES

When creating phishing websites that mimic popular services and online stores, fraudsters started using a new scheme featuring fake pages for accepting and verifying payments. Such pages are used to transfer money from a victim's account directly to the fraudster's account via a legal bank transaction. The scheme is widely used in phishing affiliate programs. The circle of victims is wide and includes the banking customer who loses money without receiving the goods they paid for, the card-issuing bank that approved the transaction, the online service or store whose website the fraudsters faked, and the payment systems whose brands are used illegally and without their knowledge. In Russia alone, the scheme caused damages amounting to some $43.4 million during the most recent reporting period. The sum is based on the average transaction size multiplied by the number of detected transactions on phishing payment pages. Group-IB experts believe that in the future the scheme will be widely used in other regions as well, causing significant financial losses.

The classic fake merchant scheme works as follows. The victim is led to the phishing store page (fake merchant) via fraudulent advertisements, spam email campaigns, or fake buy/sell ads. Then, to pay for the chosen item, the user is asked to enter their bank card details in a fake payment acceptance form, which can be located either on the website belonging to the fraudsters or on a third-party page. Next, the victim sends their card data to the server used by the fraudsters.



Enter your Password

One-time password has been sent to your registered telephone number. Please wait for one-time password SMS arrival and enter it to the Password field.

Amount: 5 306 RUB

Merchant:	[redacted]
Date:	25.03.21
Card number:	**** **** **** 3207

pa_sms

A fake payment form

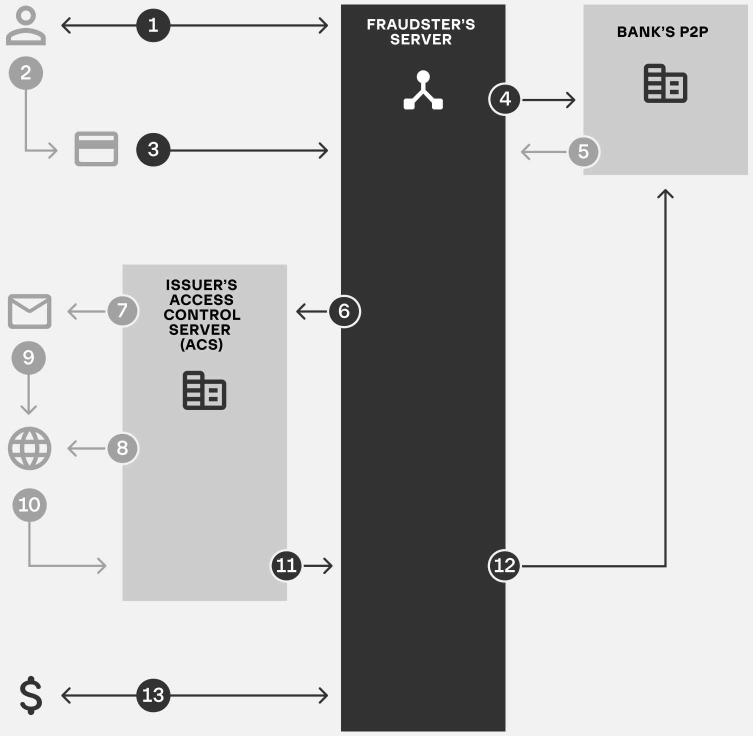
After that, to move the stolen money to their personal bank account, the threat actors create a money transfer using one of the public card-to-card payment services (P2P) provided by banks. Fraudsters specify their own card in the payment recipient information.

As is the case with any legitimate online purchase, the buyer receives an SMS code to confirm the transaction. Yet by entering the code on the 3DS page, the victim is not confirming the purchase through the online store.Instead, the victim is transferring money to the threat actor's account. To conceal any traces of third-party P2P services from users, threat actors replace the authorization URL and merchant data in the PaReq so that the victim does not come across any suspicious information on the 3DS page for entering the SMS code.

Although the widely-used 3DS technology (v. 1.0) currently protects payments from external fraudsters and foils attempts to use stolen bank card data, it does not protect against fraud from online stores.

With the first version of the 3-D Secure protocol, fraudsters can replace the PaReg of the acquiring bank's MPI. PaReq is an XML message compressed and encoded in Base64. The procedure does not include an integrity control code or signature, which allows fraudsters to change the message content as they please.

1. User visits an illegitimate/ fraudulent website
2. Enters their bank card data
3. Entered bank card data goes to the fraudster
4. Payment to the fraudster's card is created
5. Payment Authentication Request (PaReq) message
6. Request to confirm the payment from the substituted PaReq message
7. SMS with one-time code to confirm the payment
8. Redirect to the legitimate 3-D Secure page
9. One-time code is entered by the user to confirm the payment
10. Payment confirmation
11. Response about the transaction is sent
12. Payment goes to the illegitimate/ fraudulent website
13. User is returned to illegal/fraudulent site



To protect themselves from this type of fraud, some banks started checking PaReq to verify the data provided. Threat actors modified the scheme, however, by adding a fake 3-D Secure page.

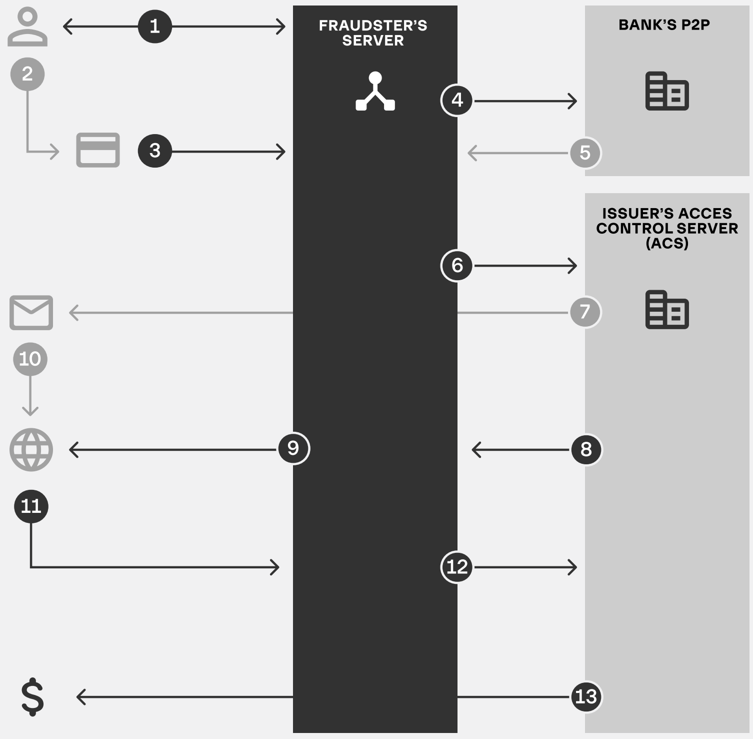
The new scheme is dangerous in the following ways:

- For the card holder, the payment process on a fraudulent website looks exactly like that of the legitimate website.
- For the issuing bank, the process looks like a typical card-to-card transfer.
- The scheme works with 3-D secure v. 2.x

As in the case of fake merchant services, users are initially directed to the fraudulent store page. When trying to pay for the goods or service, the user enters their bank card details on the fraudulent website, just as they would on typical legitimate payment forms. Next, their data is transferred to the fraudster's server, which accesses the P2P services of various banks and provides the fraudster's bank card details as the recipient. In response, the fraudster's server receives a service message from the bank's P2P service (known as a PaReq message) containing the payer's bank card details, the transfer amount and the details of the P2P service in encoded form. To prevent the victim from knowing that the bank's P2P service is used, the fraudster's server replaces authentic online store data located on the 3-D Secure page received from the bank with fake data. After that, the fraudsters redirect the buyer to the bank's 3-D Secure page containing the fake data, which the buyer sees on this page.

The victim enters their payment information to purchase the goods. To confirm the transaction, the victim receives an SMS code. They enter the code in the same field on the legitimate 3-D Secure page. Mimicking the victim, the fraudster enters the received code on the card-to-card transfer service page. The money is transferred to the fraudster's card.

1. User visits a phishing website mimicking an online store
2. Enters their bank card data
3. Entered bank card data goes to the fraudster
4. Payment to the fraudster's bank card is created
5. Payment Authentication Request (PaReq) message
6. Request to confirm the payment from the original PaReq message
7. One-time code to confirm the payment
8. Redirect to the legitimate 3-D Secure page
9. Redirect to the fake 3-D Secure page
10. One-time code entered
11. One-time code is hijacked by the fraudster
12. One-time code is entered by the user to confirm the payment
13. Payment for the online purchase goes to the fraudster



MoneyTaker

In February 2021, Group-IB's Digital Forensic Lab experts responded to an incident involving a Russian bank. The attackers had gained access to the interbank transfer system via a workstation connected to Russia's Central Bank. After examining the TTPs used by the threat actors, Group-IB experts concluded that the attack could have been conducted by a group called **MoneyTaker**. In 2016-2019, the group launched a number of attacks on workstations connected to the Russian Central Bank and on card processing systems in the UK, Hong Kong, the US, Ukraine, and Russia. After a break that lasted more than a year, MoneyTaker resumed their attacks on financial institutions.

Through incident response procedures, it was discovered that the attack began in June 2020 via a compromised company affiliated with the bank. It is assumed that the threat actors' first step was a piece of hardware installed in the affiliate network. Investigators were unable to identify the computer on which the attack started. However, Group-IB specialists found evidence that an old vulnerability, Fortigate OS fortiOS 5.6.4 (CVE-2018-13379), had been exploited.

In the first month after compromising the first device, the attackers had gained access to the bank's network. Over the next six months, they examined the network.

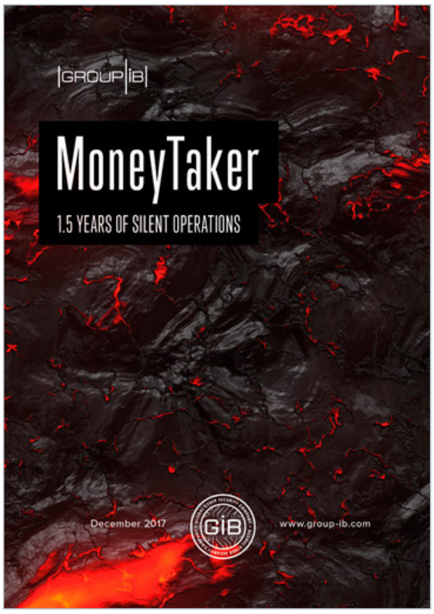
During the attack, the threat actors used Mimikatz software, built-in Windows utilities (such as WinRM and WMI), RStudio software, a remote access tool called DameWare, the Metasploit framework for remote command execution, and the utilities nbtstat, netstat, tasklist, PsExec, among others.

In January 2021, the threat actors moved to the last stage of the attack. They registered domain names similar to the bank name: the original domain name was <BANK>.ru, and the fake ones read <BANK>.org and <BANK>.com.

In February 2021, the attackers stole digital keys that they subsequently used to sign the transactions running through the Russian Central Bank's gateway. Next, they manually copied fake signed payment documents to a dedicated folder located at the workstation that communicated with Russia's Central Bank.

Finally, the attackers used malware called MBR Killer on the targeted system. Most logs were erased. After finishing the operation, the threat actors deleted the configuration of the Fortigate network firewall that isolated the network segment dedicated to the workstation which communicates with Russia's Central Bank.

MoneyTaker report



OPERA1ER

In the most recent reporting period, Group-IB experts detected attacks on banks and financial institutions located in Africa, Asia, and Latin America. While investigating the incidents, the Group-IB Threat Intelligence team found that a financially motivated threat group called OPERA1ER (aka DESKTOP-GROUP, Common Raven, and NXSMS was behind the attacks. Group-IB experts are aware of dozens of successful attacks by OPERA1ER on banks, financial institutions, and telecom companies in Africa, Asia, and Latin America. Some victims were attacked twice.

As its initial attack vector, OPERA1ER uses phishing emails with finance-related decoy documents. The phishing emails are tailored to targeted companies. OPERA1ER siphons internal documents to later use them in their phishing attacks and carefully studies their victim's infrastructure. The group's distinctive feature is that it does not develop its own malware and relies on existing tools instead. An interesting tactic of the group is deploying Metasploit directly in the attacked banks' networks, their servers in particular.

OPERA1ER's main target is an e-money platform used by its victims.

CARDING MARKET 09

The carding market can be divided into two main segments: selling card data in text format (card number, expiration date, cardholder's name, address, and CVV) and card dumps (information taken from the card's magnetic stripe).

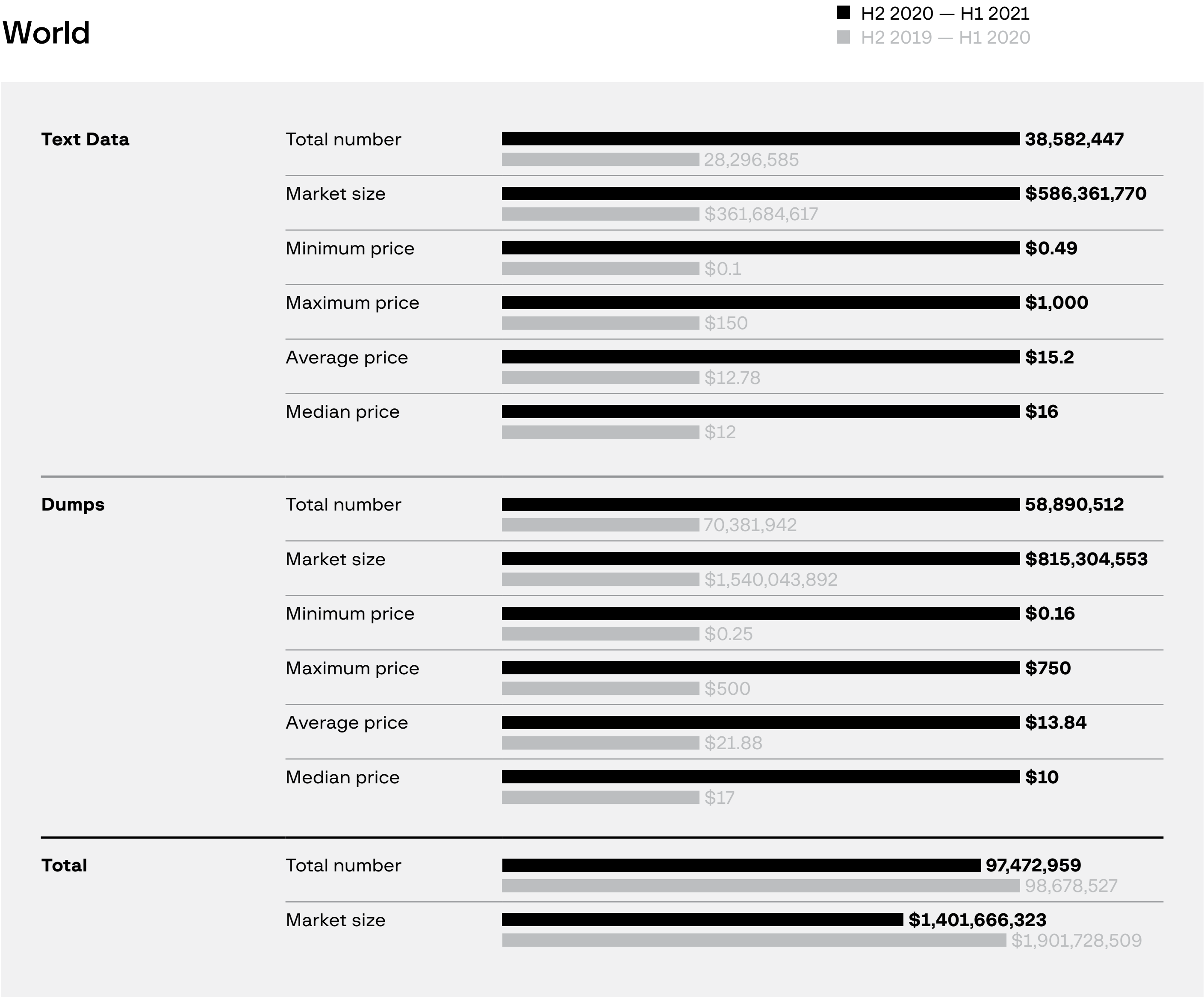
Text data is collected via phishing websites and banking Trojans for PC and Android, and ATMs. Text data can also be obtained by breaching e-commerce websites and using JS sniffers.

Card dumps are obtained with skimming devices or by using Trojans for PCs with connected POS terminals.

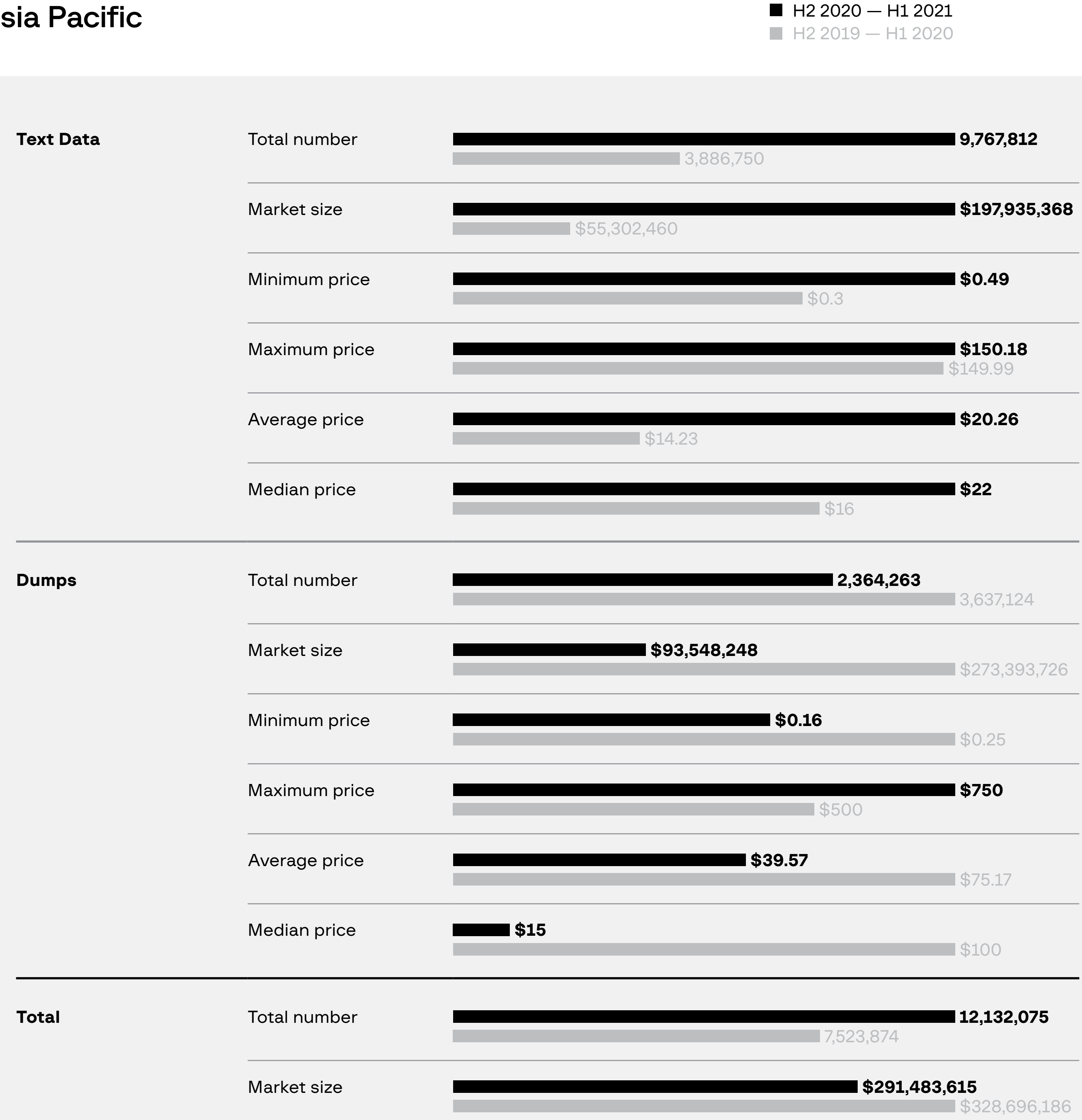
In the most recent reporting period, the total volume of the carding market fell from $1.9 billion to $1.4 billion compared to the previous year. The decrease was caused by fewer dumps put up for sale (58 million compared to 70 million) after a major card shop, Joker's Stash, closed down.

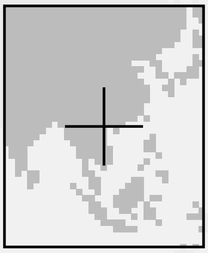
On the other hand, the number of textual card data offers increased from 28 to 38 million due to the growth of phishing resources during the pandemic, among other things.

World

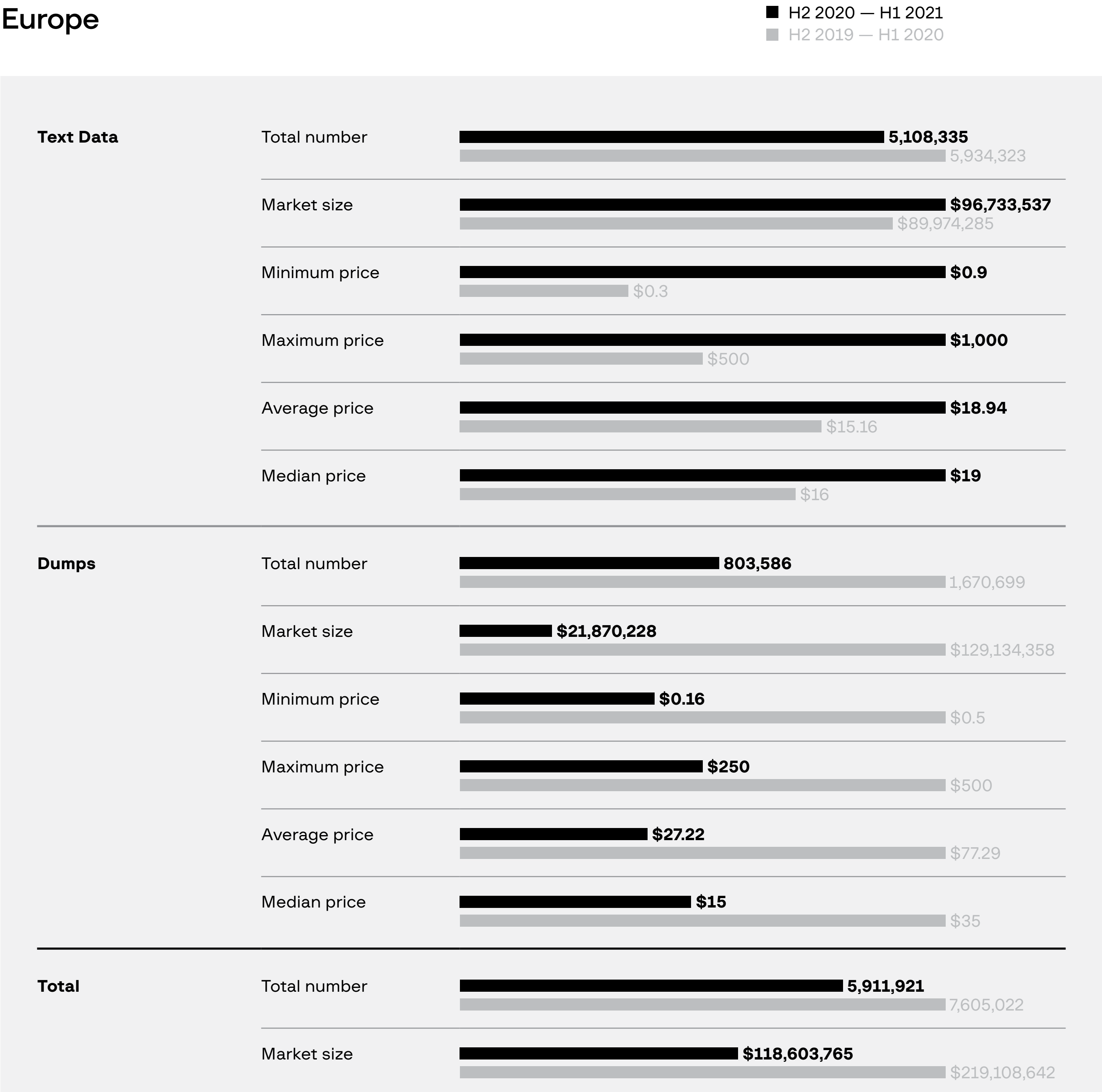


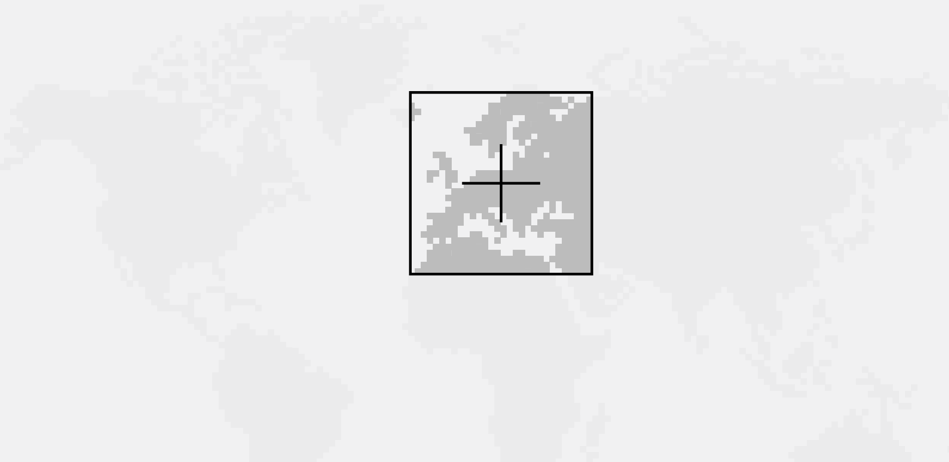
Asia Pacific



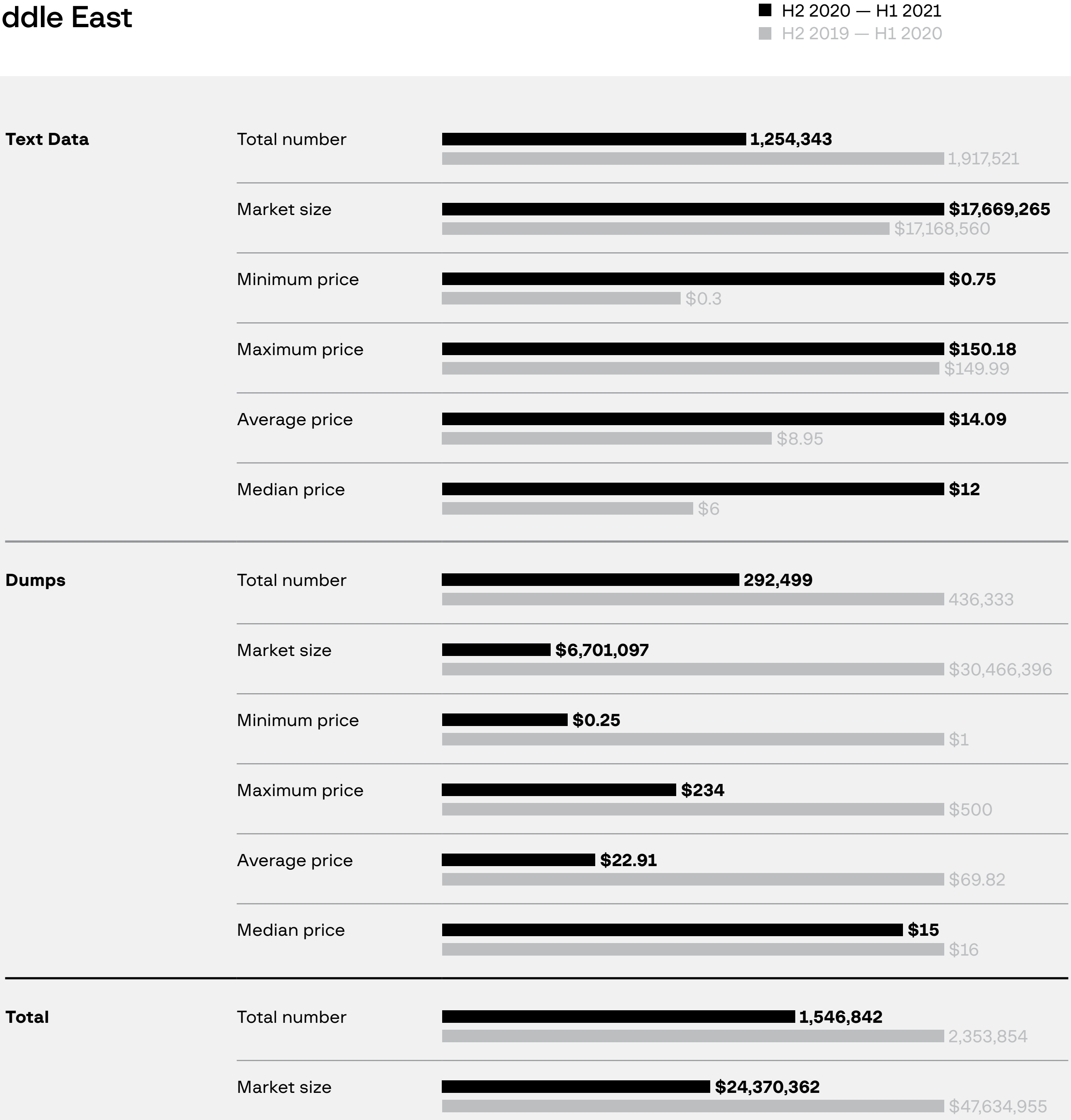


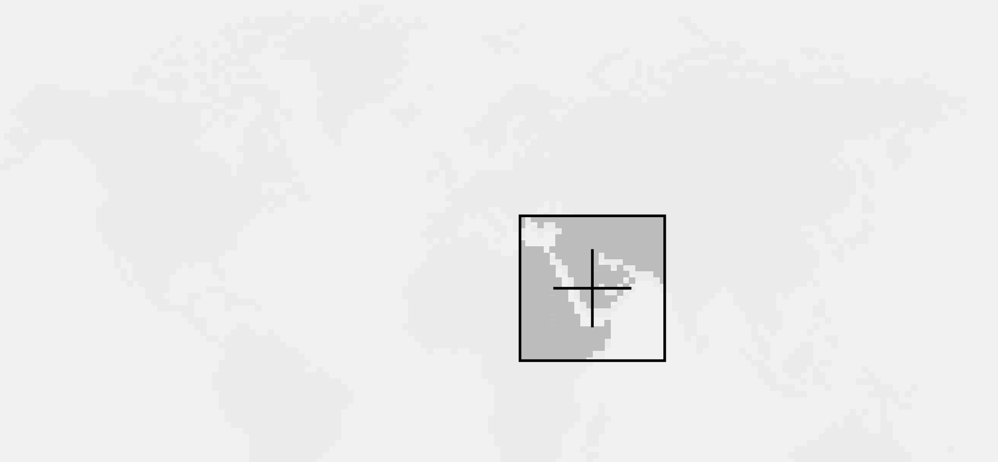
Europe


■ H2 2020 — H1 2021
■ H2 2019 — H1 2020
Text Data
Total number
5,108,335
5,934,323
Market size
$96,733,537
$89,974,285
Minimum price
$0.9
$0.3
Maximum price
$1,000
$500
Average price
$18.94
$15.16
Median price
$19
$16
Dumps
Total number
803,586
1,670,699
Market size
$21,870,228
$129,134,358
Minimum price
$0.16
$0.5
Maximum price
$250
$500
Average price
$27.22
$77.29
Median price
$15
$35
Total
Total number
5,911,921
7,605,022
Market size
$118,603,765
$219,108,642

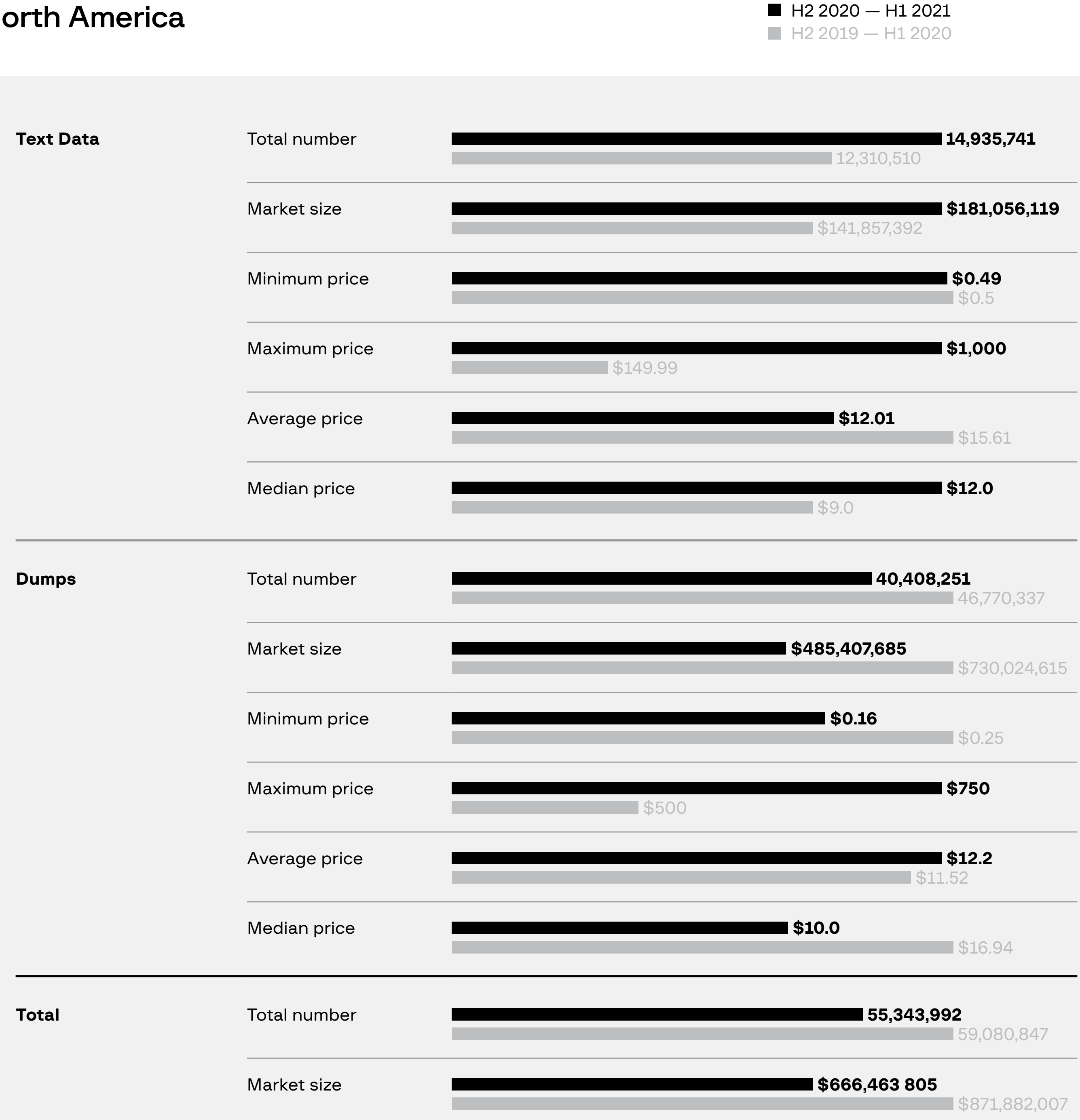


Middle East

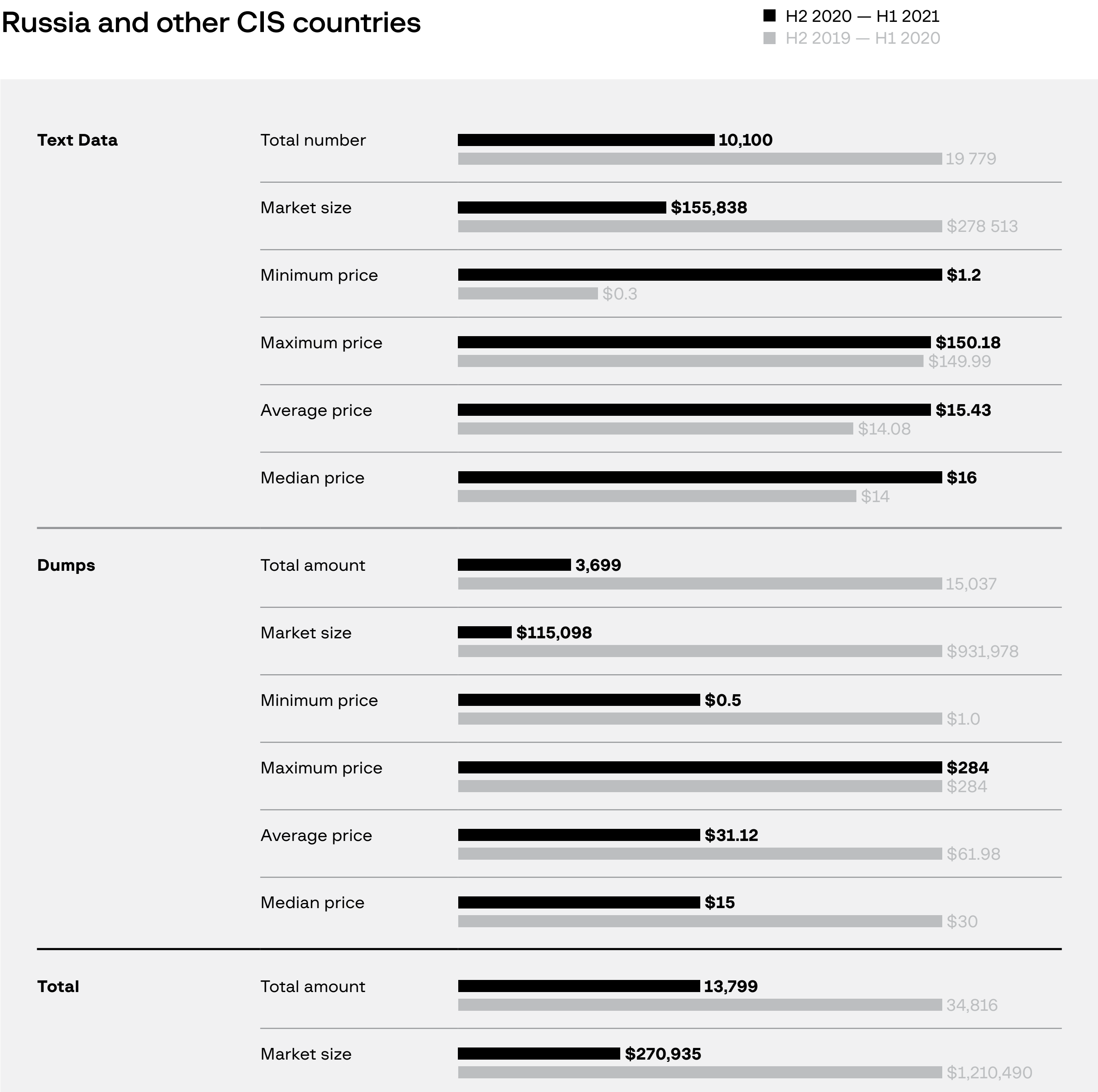

■ H2 2020 — H1 2021
■ H2 2019 — H1 2020
Text Data
Total number
1,254,343
1,917,521
Market size
$17,669,265
$17,168,560
Minimum price
$0.75
$0.3
Maximum price
$150.18
$149.99
Average price
$14.09
$8.95
Median price
$12
$6
Dumps
Total number
292,499
436,333
Market size
$6,701,097
$30,466,396
Minimum price
$0.25
$1
Maximum price
$234
$500
Average price
$22.91
$69.82
Median price
$15
$16
Total
Total number
1,546,842
2,353,854
Market size
$24,370,362
$47,634,955

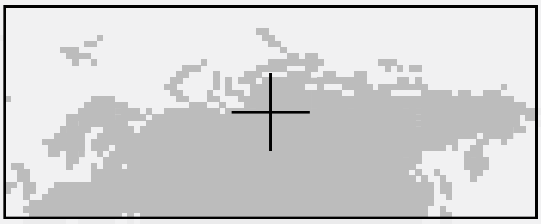


North America



Russia and other CIS countries





BANKING TROJANS FOR PC 10

During the reporting period, out of all known banking Trojans, **18 stood out as the most active**. Of those, eight were developed by fraudsters based in Latin America, while nine were created by Russian-speaking threat actors.

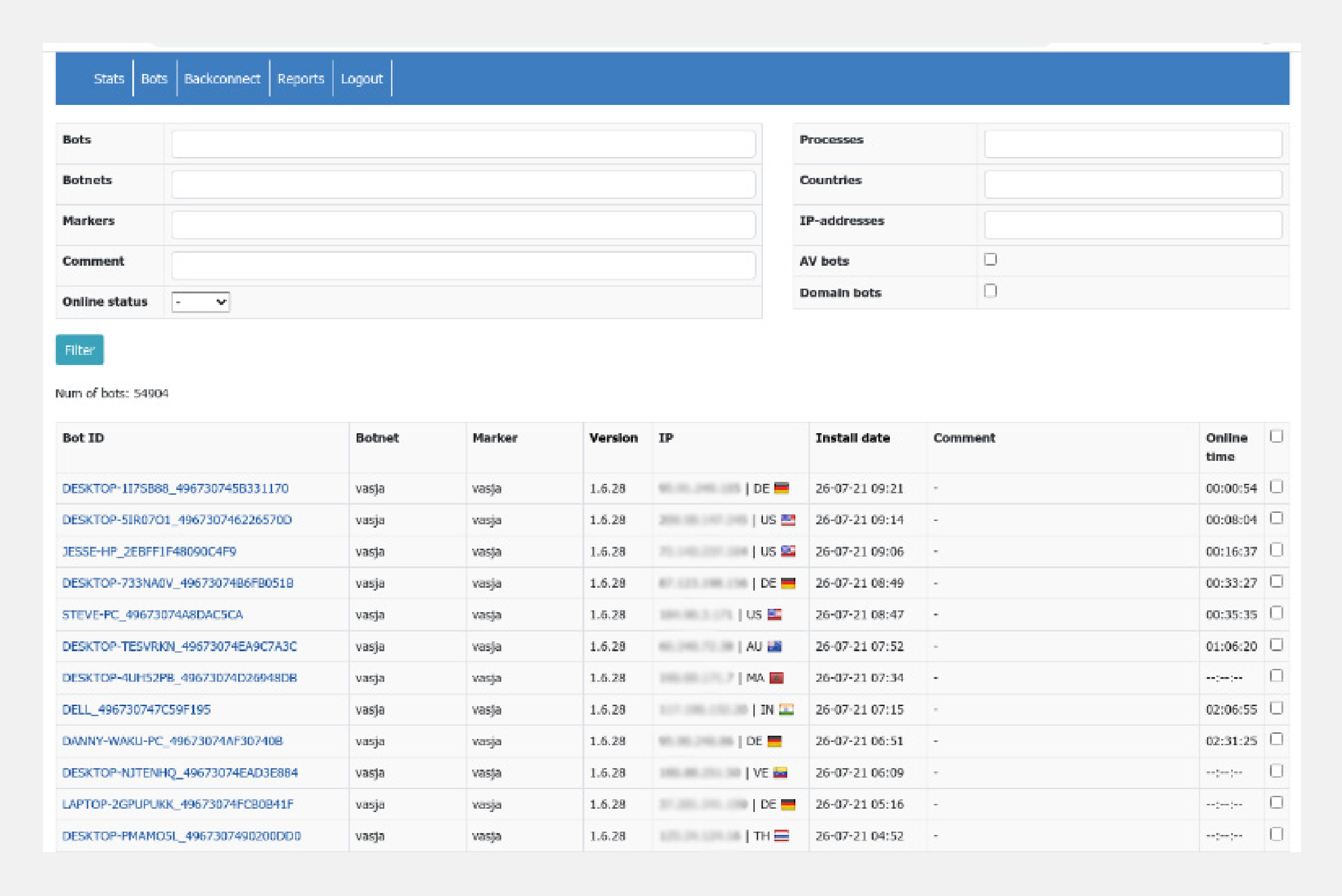
Currently active banking Trojans in different regions

Status	Trojan	Date first appeared	Developer's region	Region of attack
NEW	BBtok	Q4 2020	Latin America	Latin America
NEW	Bizarro	Q1 2021	Latin America	Latin America
ACTIVE	Grandoreiro	2017	Latin America	US and Canada, Latin America, Europe
ACTIVE	Javali	2017	Latin America	Latin America
ACTIVE	Guildma	2017	Latin America	Latin America
ACTIVE	Pazera	2015	Latin America	Latin America
ACTIVE	Metamorfo (Casbaneiro)	2018	Latin America	Latin America
ACTIVE	Janeleiro	2019	Latin America	Latin America
ACTIVE	RTM	2015	Russia	Russia
ACTIVE	zLoader	2019	Russia	US and Canada, Europe, Asia Pacific
ACTIVE	Qbot	2009	Russia	US and Canada
ACTIVE	Trickbot	2016	Russia	US and Canada, Asia Pacific
ACTIVE	IcedID	2017	Russia	US and Canada, Europe, Asia Pacific

Status	Trojan	Date first appeared	Developer's region	Region of attack
ACTIVE	Ramnit	2010	Russia	US and Canada, Europe, Asia Pacific
ACTIVE	LokiPWS	2015	Russia	US and Canada, Europe
ACTIVE	Gozi	2007	Russia	Asia Pacific
ACTIVE	Danabot	2018	Russia	Europe, Asia Pacific
ACTIVE	Backswap	2018	Unknown	Europe
LOW ACTIVITY	Retefe	2014	Россия	Europe
LOW ACTIVITY	MnuBot	2018	Latin America	Latin America
LOW ACTIVITY	CamuBot	2018	Latin America	Latin America
LOW ACTIVITY	Melcoz	2018	Latin America	Latin America

Screenshots of some malware administrative panels:

zLoader

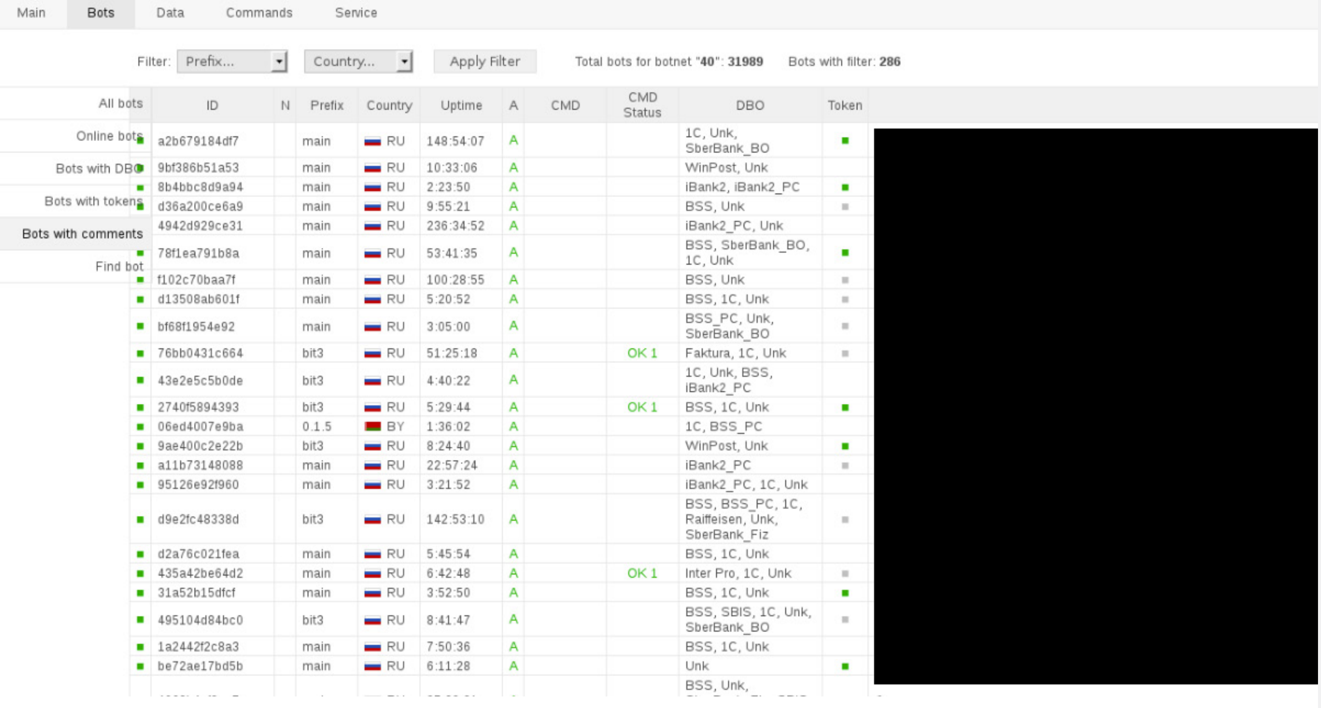


Bots		Processes	
Botnets		Countries	
Markers		IP-addresses	
Comment		AV bots	□
Online status	-	Domain bots	□

Num of bots: 54904

Bot ID	Botnet	Marker	Version	IP	Install date	Comment	Online time	□
DESKTOP-1I7SB88_496730745B331170	vasja	vasja	1.6.28	[redacted] | DE	26-07-21 09:21	-	00:00:54	□
DESKTOP-5IR07O1_4967307462265700	vasja	vasja	1.6.28	[redacted] | US	26-07-21 09:14	-	00:08:04	□
JESSE-HP_2EBFF1F48090C4F9	vasja	vasja	1.6.28	[redacted] | US	26-07-21 09:06	-	00:16:37	□
DESKTOP-733NA0V_49673074B6FB051B	vasja	vasja	1.6.28	[redacted] | DE	26-07-21 08:49	-	00:33:27	□
STEVE-PC_49673074A8DAC5CA	vasja	vasja	1.6.28	[redacted] | US	26-07-21 08:47	-	00:35:35	□
DESKTOP-TESVRKN_49673074EA9C7A3C	vasja	vasja	1.6.28	[redacted] | AU	26-07-21 07:52	-	01:06:20	□
DESKTOP-4UH52PB_49673074D26948DB	vasja	vasja	1.6.28	[redacted] | MA	26-07-21 07:34	-	--:--:--	□
DELL_496730747C59F195	vasja	vasja	1.6.28	[redacted] | IN	26-07-21 07:15	-	02:06:55	□
DANNY-WAKU-PC_49673074AF30740B	vasja	vasja	1.6.28	[redacted] | DE	26-07-21 06:51	-	02:31:25	□
DESKTOP-NJTENHQ_49673074EAD3E884	vasja	vasja	1.6.28	[redacted] | VE	26-07-21 06:09	-	--:--:--	□
LAPTOP-2GPUPUKK_49673074FCB0B41F	vasja	vasja	1.6.28	[redacted] | DE	26-07-21 05:16	-	--:--:--	□
DESKTOP-PMAMO5L_496730749020DD0	vasja	vasja	1.6.28	[redacted] | TH	26-07-21 04:52	-	--:--:--	□

RTM

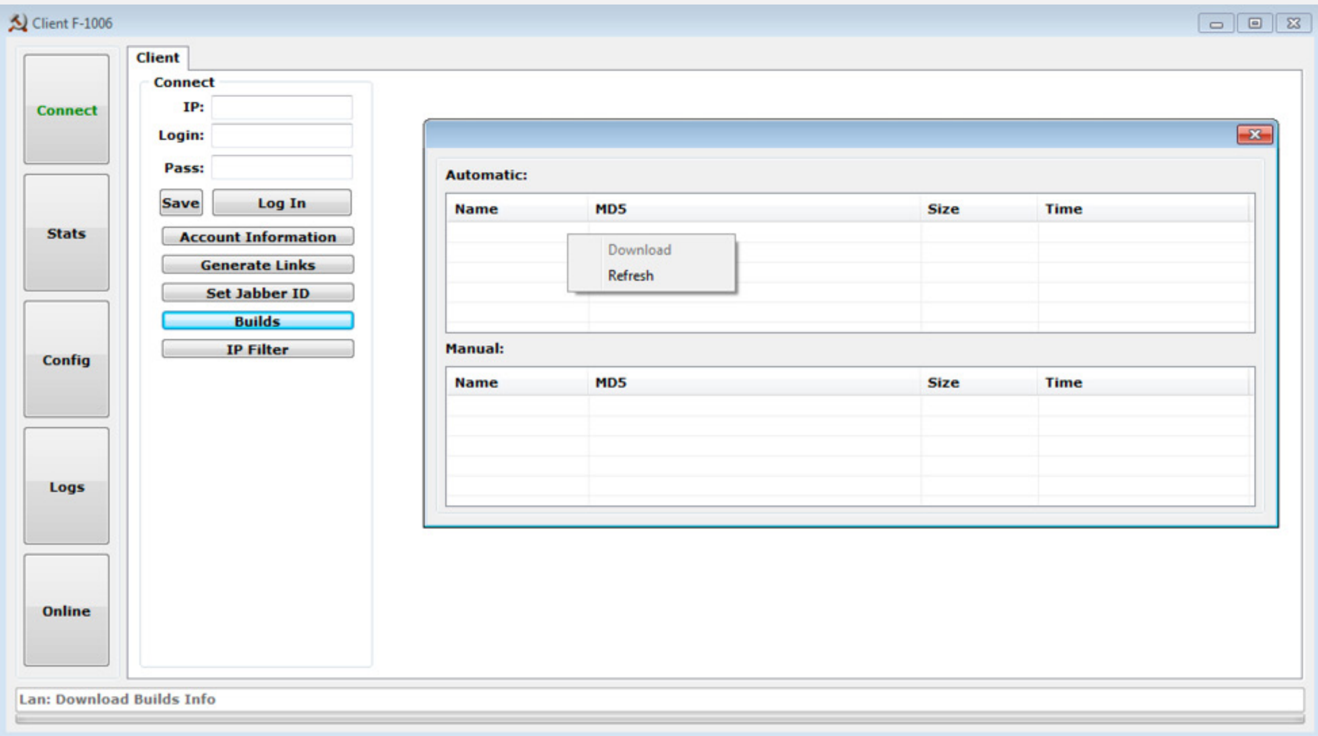


Total bots for botnet "**40**": **31989** Bots with filter: **286**

	ID	N	Prefix	Country	Uptime	A	CMD	CMD Status	DBO	Token
🟩	a2b679184df7		main	RU	148:54:07	A			1C, Unk, SberBank_BO	🟩
🟩	9bf386b51a53		main	RU	10:33:06	A			WinPost, Unk	
🟩	8b4bbc8d9a94		main	RU	2:23:50	A			iBank2, iBank2_PC	🟩
🟩	d36a200ce6a9		main	RU	9:55:21	A			BSS, Unk	■
	4942d929ce31		main	RU	236:34:52	A			iBank2_PC, Unk	
🟩	78f1ea791b8a		main	RU	53:41:35	A			BSS, SberBank_BO, 1C, Unk	🟩
🟩	f102c70baa7f		main	RU	100:28:55	A			BSS, Unk	■
🟩	d13508ab601f		main	RU	5:20:52	A			BSS, 1C, Unk	■
🟩	bf68f1954e92		main	RU	3:05:00	A			BSS_PC, Unk, SberBank_BO	■
🟩	76bb0431c664		bit3	RU	51:25:18	A		OK 1	Faktura, 1C, Unk	■
🟩	43e2e5c5b0de		bit3	RU	4:40:22	A			1C, Unk, BSS, iBank2_PC	
🟩	2740f5894393		bit3	RU	5:29:44	A		OK 1	BSS, 1C, Unk	🟩
🟩	06ed4007e9ba		0.1.5	BY	1:36:02	A			1C, BSS_PC	
🟩	9ae400c2e22b		bit3	RU	8:24:40	A			WinPost, Unk	🟩
🟩	a11b73148088		main	RU	22:57:24	A			iBank2_PC	■
🟩	95126e92f960		main	RU	3:21:52	A			iBank2_PC, 1C, Unk	
🟩	d9e2fc48338d		bit3	RU	142:53:10	A			BSS, BSS_PC, 1C, Raiffeisen, Unk, SberBank_Fiz	■
🟩	d2a76c021fea		main	RU	5:45:54	A			BSS, 1C, Unk	
🟩	435a42be64d2		main	RU	6:42:48	A		OK 1	Inter Pro, 1C, Unk	■
🟩	31a52b15dfcf		main	RU	3:52:50	A			BSS, 1C, Unk	🟩
🟩	495104d84bc0		bit3	RU	8:41:47	A			BSS, SBIS, 1C, Unk, SberBank_BO	■
🟩	1a2442f2c8a3		main	RU	7:50:36	A			BSS, 1C, Unk	
🟩	be72ae17bd5b		main	RU	6:11:28	A			Unk	🟩
									BSS, Unk,	

[redacted]

Danabot



Automatic:

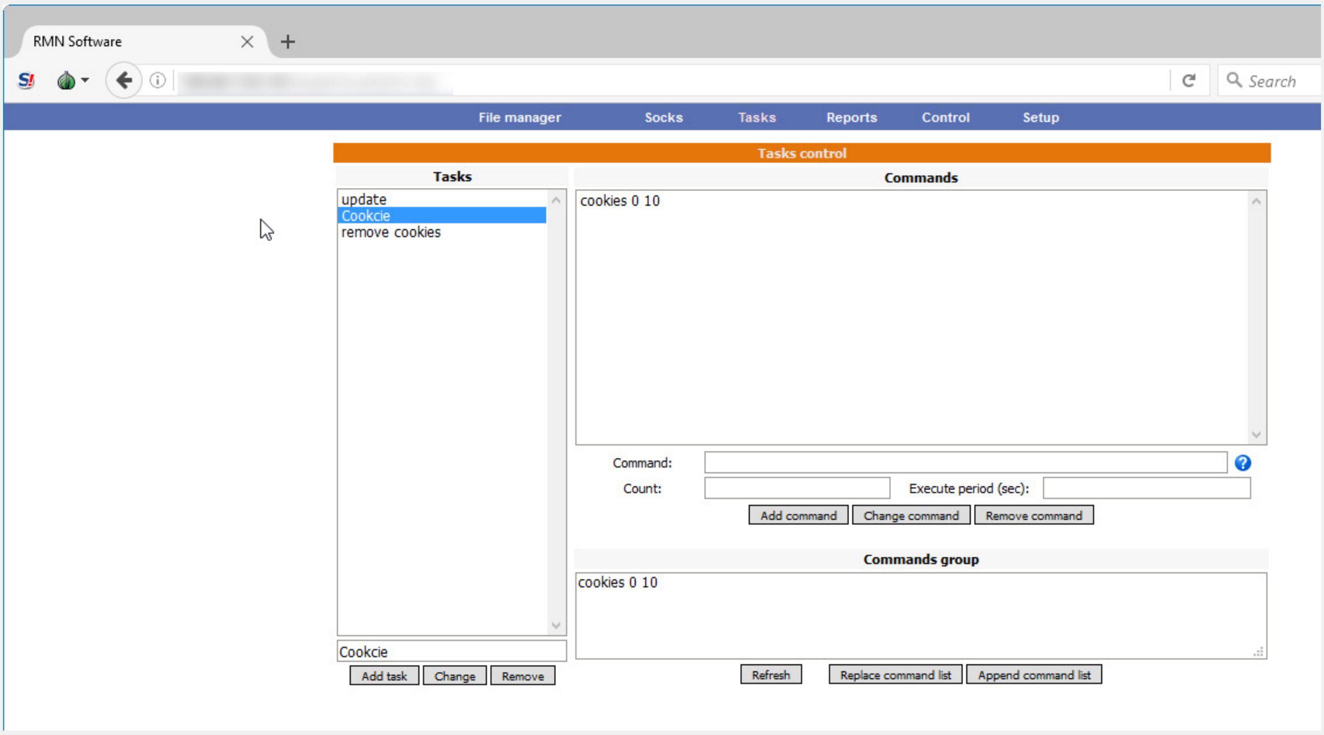
Name	MD5	Size	Time

Manual:

Name	MD5	Size	Time

Lan: Download Builds Info

Ramnit



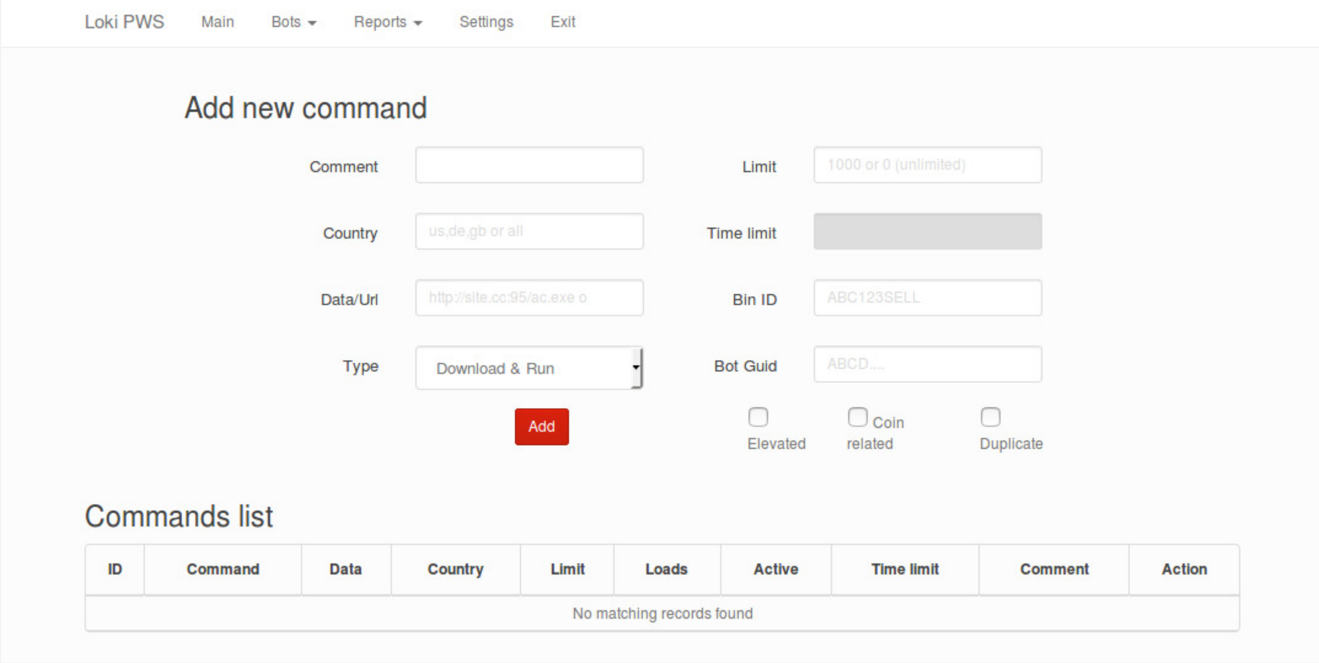
Tasks:
update
Cookcie
remove cookies

Commands:
cookies 0 10

Commands group:
cookies 0 10

Cookcie

LokiPWS



Add new command

Comment		Limit	1000 or 0 (unlimited)
Country	us,de,gb or all	Time limit	
Data/Url	http://site.cc:95/ac.exe o	Bin ID	ABC123SELL
Type	Download & Run	Bot Guid	ABCD....

Commands list

ID	Command	Data	Country	Limit	Loads	Active	Time limit	Comment	Action
No matching records found									

Last year's trend of malware distributors helping ransomware operators gain initial access to corporate networks continued in the most recent reporting period. This trend is described in Group-IB's report entitled **Ransomware Uncovered 2020-2021**.

- Qbot → ProLock, DoppelPaymer, Egregor
- Gozi → Egregor, Revil
- zLoader → Ryuk, Egregor, DarkSide
- Trickbot → Cl0p, Conti, Ryuk, RansomEXX
- IcedID → Maze, Egregor, RansomEXX, Revil, Conti
- Dridex* → DoppelPaymer, Grief

Lately, most cyberattacks have involved ransomware, while banking Trojans have not been actively developed. The only region where Trojans have evolved is Latin America.

In early June 2021, the US Department of Justice **pressed charges** against a 55-year-old Latvian national arrested in Miami who allegedly helped develop a Trojan called Trickbot. In September of this year, law enforcement officials detained another Trojan developer in South Korea. Nevertheless, the malware remains active.

The creators of a Trojan called Qbot continue to actively develop their product. They improved the network protocol and defense mechanisms,- such as security checks on the server side. They also implemented a security check that forces a compromised machine to send verification data one hour after it was registered in the botnet.

As for zLoader, Group-IB identified and analyzed two botnets with more than 350,000 bots. Most infected devices were located in Germany, Canada, the US, and Japan.

One Trojan deserves a special mention: Ramnit. No attacks on financial organizations were detected in the reporting period that would be typical of this Trojan. Instead, the Ramnit malware targeted organizations from the education, insurance, and governmental sectors. In the first quarter of 2021, there were infections by this Trojan in the UK, India, Russia, Turkey, and the US.

Ransomware Uncovered 2020-2021

* In the reporting period, Dridex was not identified as a stand-alone banking Trojan; it was only observed in use as part of ransomware distribution.

BANKING TROJANS FOR ANDROID

11

As with the market for PC Trojans, the market for Android Trojans barely changed. No offers to sell/rent new malware were identified on underground forums during the reporting period.

However, three new Trojans emerged during this time: Ghimob (active in Latin America), FluBot (active in Europe), and TeaBot (aka Anatsa, Toddler), which targets Europe and Russia.

Ghimob is believed to have been developed by the same Latin American threat group that created Guildma (Astaroth). At the moment, it is unclear who developed FluBot and TeaBot or where.

The Brazilian banking Trojans OperadorMIB and BasBanke (Coybot) stopped being active, and the same is true for Alien Bot. OperadorMIB was developed by a Brazilian threat actor whose activity peaked in the first half of 2020.

Gustuff, another Trojan that used to be very active, also disappeared.

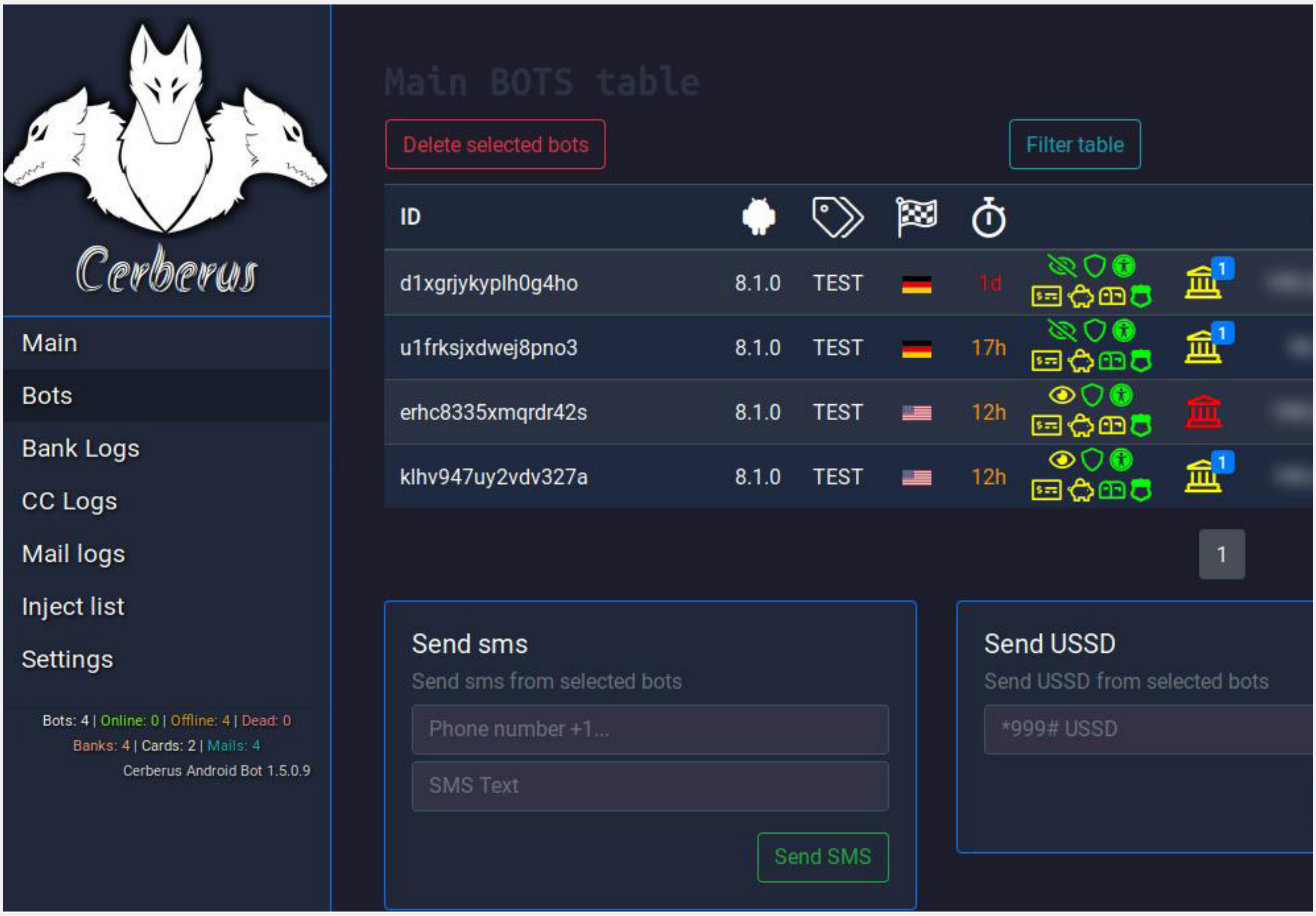
Active Android banking Trojans by region

Status	Trojans	Date first appeared	Developer’s region	Attack region
NEW	Ghimob	Q4 2020	Latin America	Latin America
NEW	TeaBot (Anatsa)	Q1 2021	Unknown	Russia, Europe
ACTIVE	EventBot	Q1 2020	Unknown	Europe
ACTIVE	Cerberus v2	Q2 2020	Russia	US and Canada, Europe, Asia Pacific
ACTIVE	Anubis	Q4 2019	Russia	US and Canada, Europe, Asia Pacific
ACTIVE	Ginp	Q3 2019	Unknown	Europe
ACTIVE	BlackRock	Q2 2020	Unknown	US and Canada, Asia Pacific

Status	Trojans	Date first appeared	Developer's region	Attack region
ACTIVE	FluBot	Q1 2021	Russia	Europe
LOW ACITIVITY	Alien Bot	Q12020	Russia	US and Canada, Europe, Asia Pacific
LOW ACITIVITY	OperadorMIB	Q12020	Latin America	Latin America
LOW ACITIVITY	BasBanke (Coybot)	2018	Latin America	Latin America
LOW ACITIVITY	Gustuff	Q4 2017	Russia	US and Canada, Asia Pacific
LOW ACITIVITY	FlexNet	2014	Russia	Russia

Below are screenshots of some malware admin panels:

Cerberus



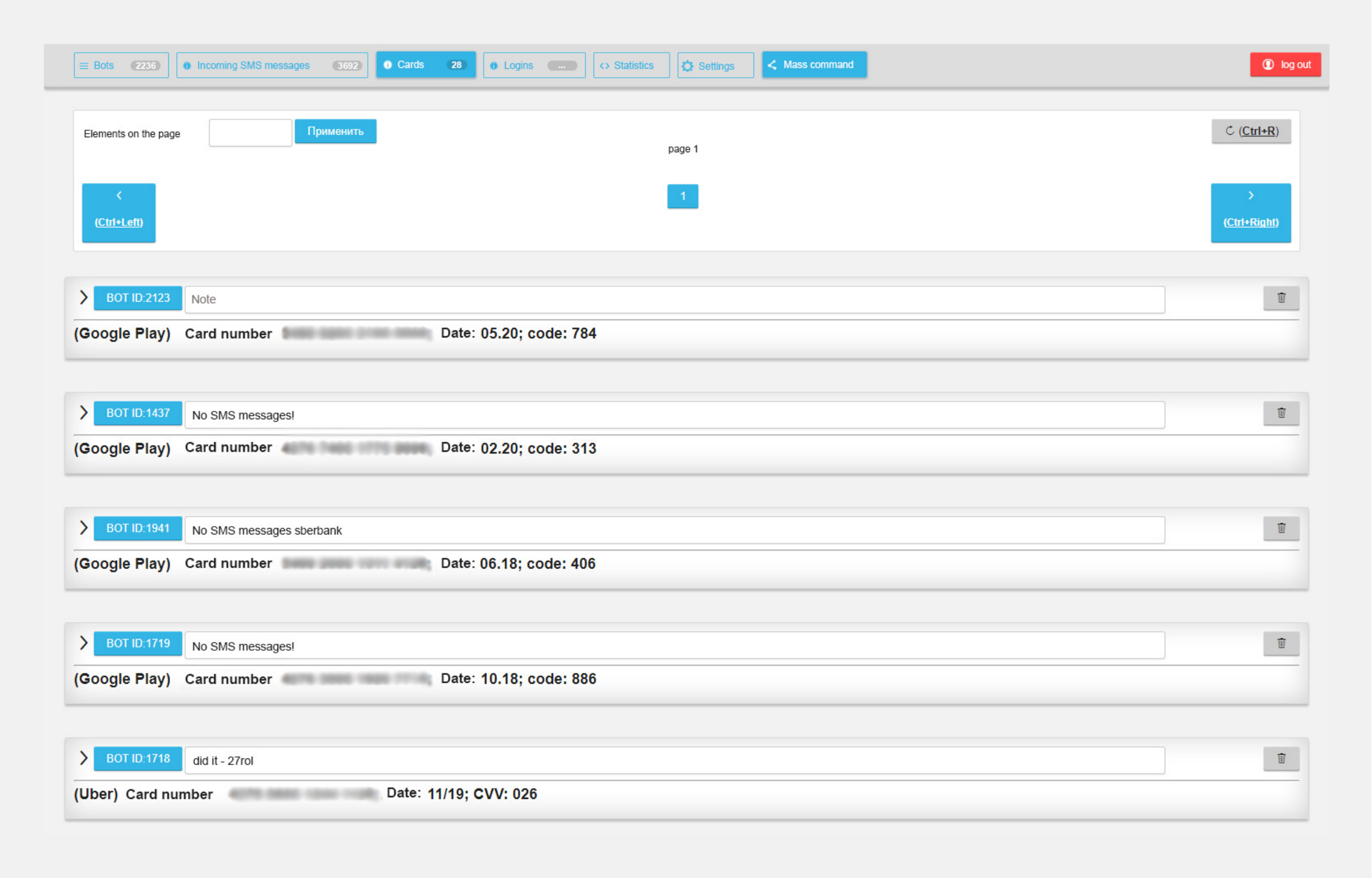
ID				
d1xgrjykyplh0g4ho	8.1.0	TEST	🇩🇪	1d
u1frksjxdwej8pno3	8.1.0	TEST	🇩🇪	17h
erhc8335xmqrdr42s	8.1.0	TEST	🇺🇸	12h
klhv947uy2vdv327a	8.1.0	TEST	🇺🇸	12h

Bots: 4 | Online: 0 | Offline: 4 | Dead: 0
Banks: 4 | Cards: 2 | Mails: 4
Cerberus Android Bot 1.5.0.9

Send sms
Send sms from selected bots
Phone number +1...
SMS Text
Send SMS

Send USSD
Send USSD from selected bots
*999# USSD

FlexNet



BOT ID:2123 Note

(Google Play) Card number [redacted] Date: 05.20; code: 784

BOT ID:1437 No SMS messages!

(Google Play) Card number [redacted] Date: 02.20; code: 313

BOT ID:1941 No SMS messages sberbank

(Google Play) Card number [redacted] Date: 06.18; code: 406

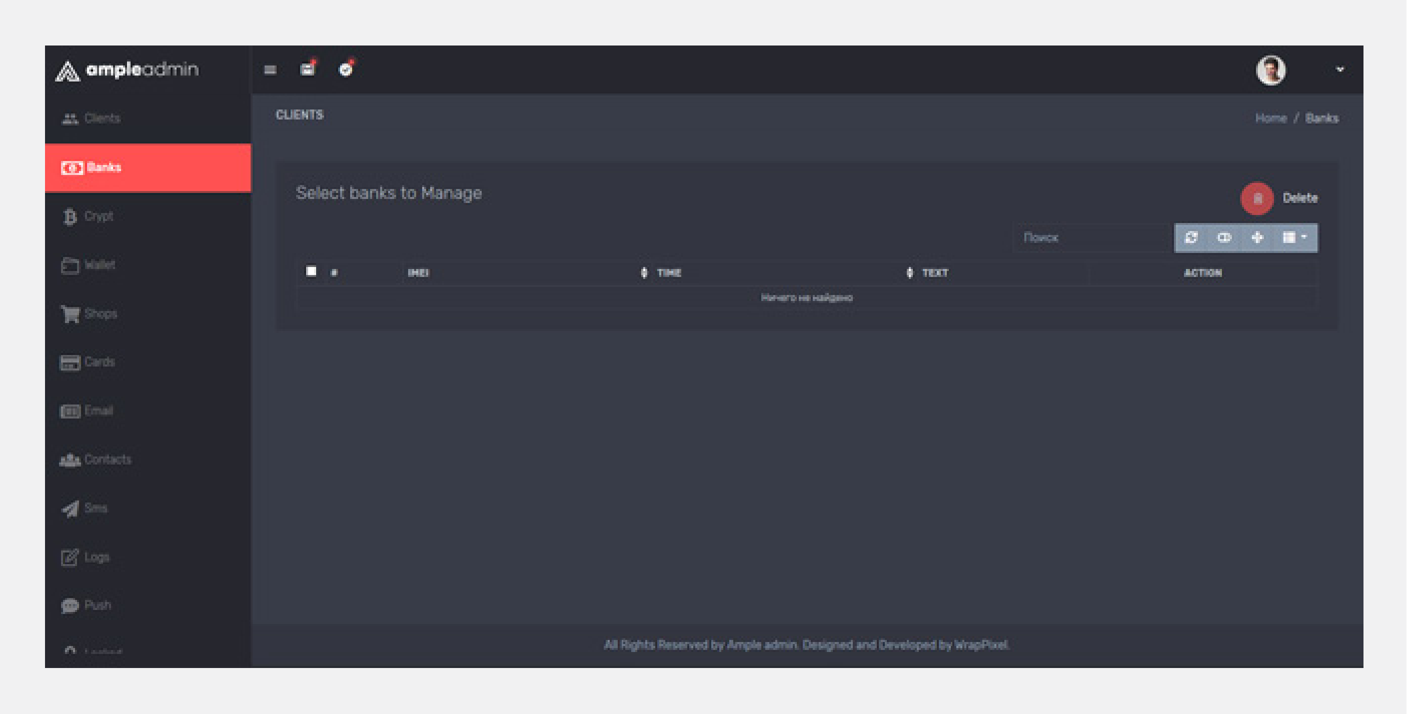
BOT ID:1719 No SMS messages!

(Google Play) Card number [redacted] Date: 10.18; code: 886

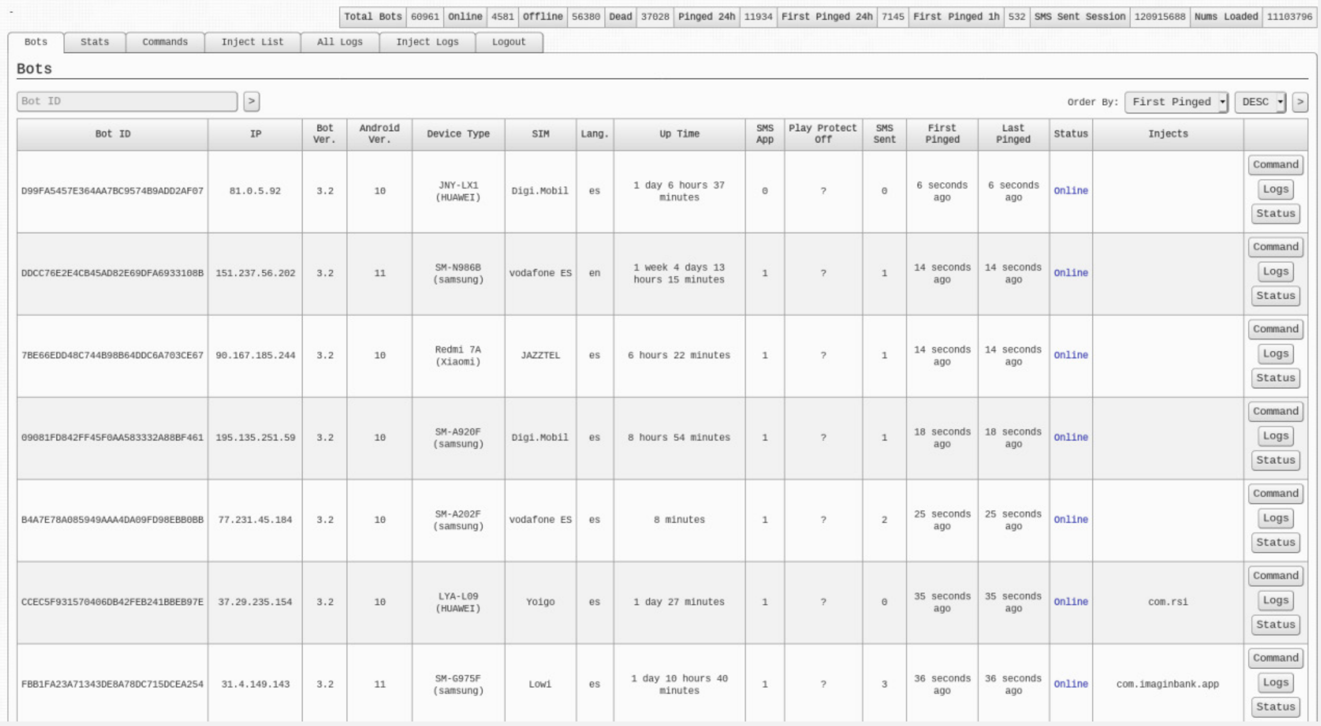
BOT ID:1718 did it - 27rol

(Uber) Card number [redacted] Date: 11/19; CVV: 026

BlackRock



FluBot



Total Bots	60961	Online	4581	Offline	56380	Dead	37028	Pinged 24h	11934	First Pinged 24h	7145	First Pinged 1h	532	SMS Sent Session	120915688	Nums Loaded	11103796

Bots | Stats | Commands | Inject List | All Logs | Inject Logs | Logout

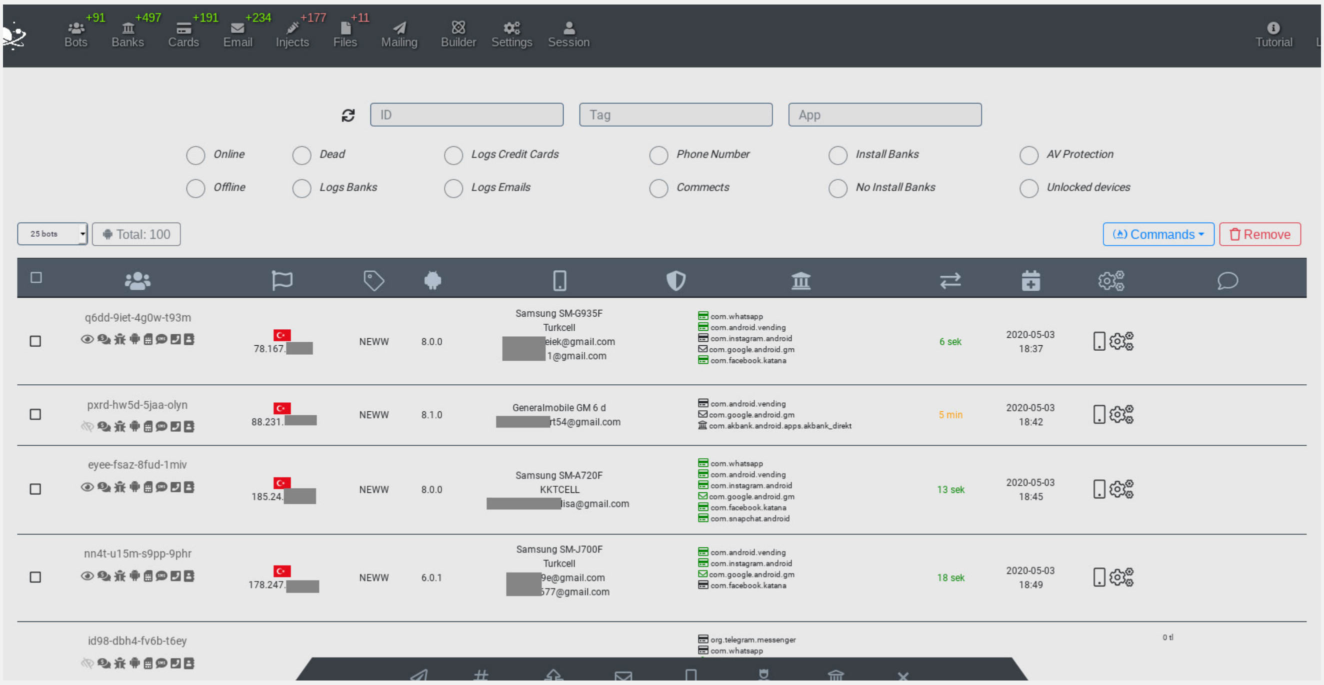
Bots

Bot ID >

Order By: First Pinged DESC >

Bot ID	IP	Bot Ver.	Android Ver.	Device Type	SIM	Lang.	Up Time	SMS App	Play Protect Off	SMS Sent	First Pinged	Last Pinged	Status	Injects	
D99FA5457E364AA7BC9574B9ADD2AF07	81.0.5.92	3.2	10	JNY-LX1 (HUAWEI)	Digi.Mobil	es	1 day 6 hours 37 minutes	0	?	0	6 seconds ago	6 seconds ago	Online		Command Logs Status
DDCC76E2E4CB45AD82E69DFA6933108B	151.237.56.202	3.2	11	SM-N986B (samsung)	vodafone ES	en	1 week 4 days 13 hours 15 minutes	1	?	1	14 seconds ago	14 seconds ago	Online		Command Logs Status
7BE66EDD48C744B98B64DDC6A703CE67	90.167.185.244	3.2	10	Redmi 7A (Xiaomi)	JAZZTEL	es	6 hours 22 minutes	1	?	1	14 seconds ago	14 seconds ago	Online		Command Logs Status
09081FD842FF45F0AA583332A88BF461	195.135.251.59	3.2	10	SM-A920F (samsung)	Digi.Mobil	es	8 hours 54 minutes	1	?	1	18 seconds ago	18 seconds ago	Online		Command Logs Status
B4A7E78A085949AAA4DA09FD98EBB0BB	77.231.45.184	3.2	10	SM-A202F (samsung)	vodafone ES	es	8 minutes	1	?	2	25 seconds ago	25 seconds ago	Online		Command Logs Status
CCEC5F931570406DB42FEB241BBEB97E	37.29.235.154	3.2	10	LYA-L09 (HUAWEI)	Yoigo	es	1 day 27 minutes	1	?	0	35 seconds ago	35 seconds ago	Online	com.rsi	Command Logs Status
FBB1FA23A71343DE8A78DC715DCEA254	31.4.149.143	3.2	11	SM-G975F (samsung)	Lowi	es	1 day 10 hours 40 minutes	1	?	3	36 seconds ago	36 seconds ago	Online	com.imaginbank.app	Command Logs Status

Alien Bot



ID | Tag | App

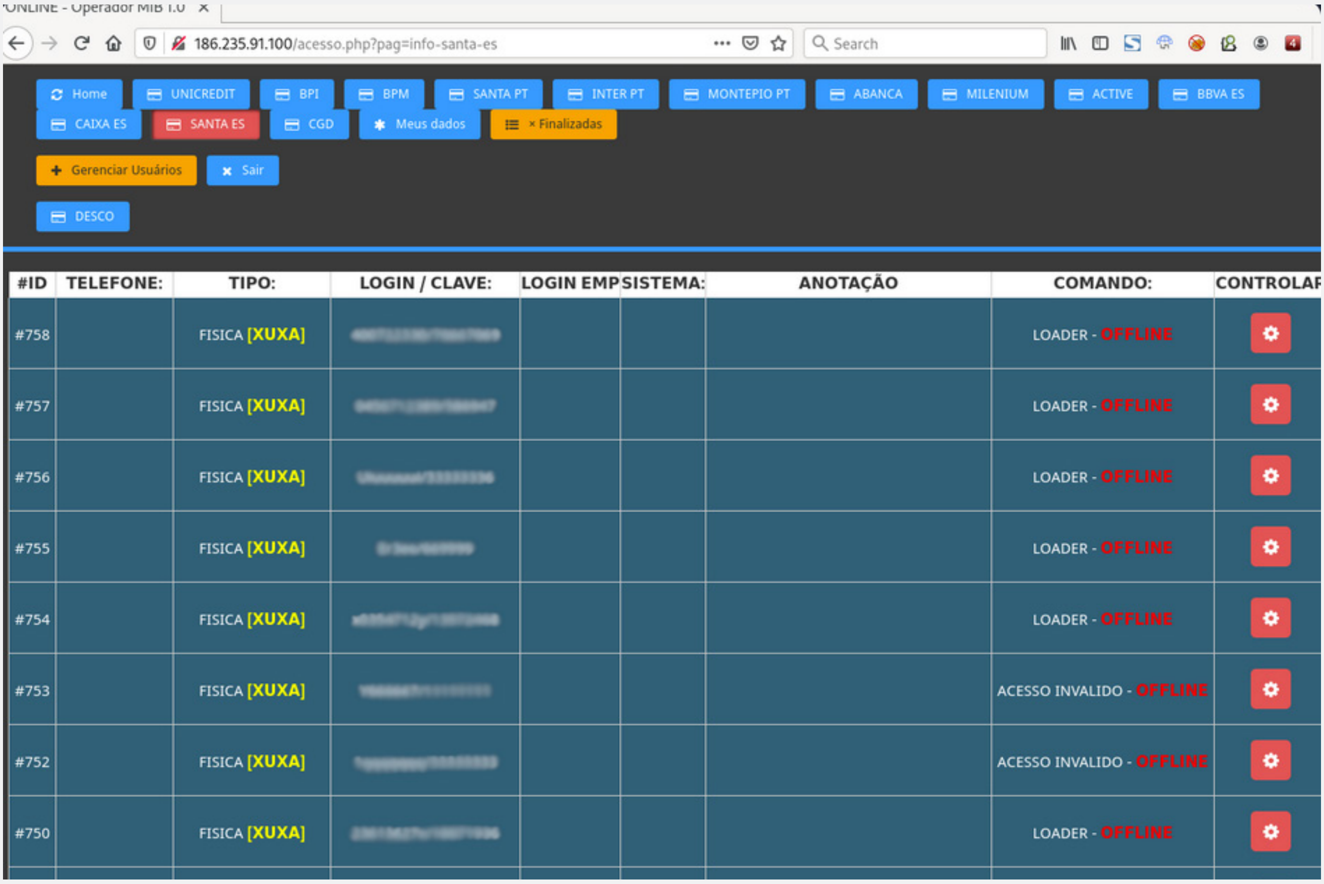
○ Online ○ Dead ○ Logs Credit Cards ○ Phone Number ○ Install Banks ○ AV Protection

○ Offline ○ Logs Banks ○ Logs Emails ○ Commects ○ No Install Banks ○ Unlocked devices

25 bots | Total: 100 | Commands | Remove

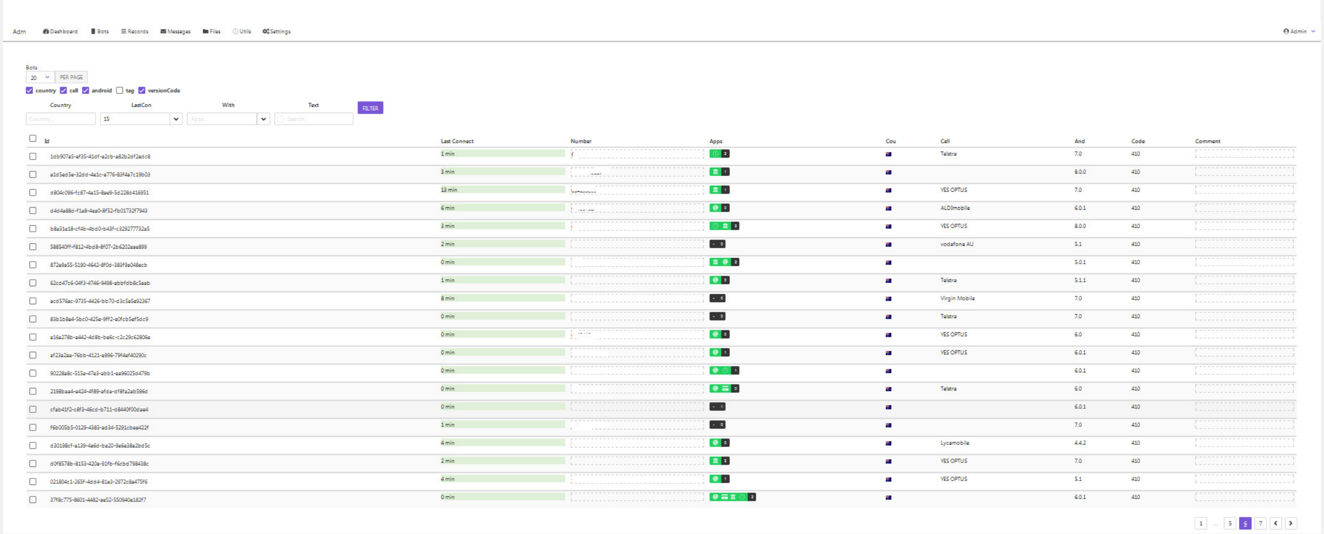
□											
□	q6dd-9iet-4g0w-t93m	78.167.[redacted]	NEWW	8.0.0	Samsung SM-G935F Turkcell [redacted]eiek@gmail.com 1@gmail.com		com.whatsapp com.android.vending com.instagram.android com.google.android.gm com.facebook.katana	6 sek	2020-05-03 18:37		
□	pxrd-hw5d-5jaa-olyn	88.231.[redacted]	NEWW	8.1.0	Generalmobile GM 6 d [redacted]rt54@gmail.com		com.android.vending com.google.android.gm com.akbank.android.apps.akbank_direkt	5 min	2020-05-03 18:42		
□	eyee-fsaz-8fud-1miv	185.24.[redacted]	NEWW	8.0.0	Samsung SM-A720F KKTCELL [redacted]lisa@gmail.com		com.whatsapp com.android.vending com.instagram.android com.google.android.gm com.facebook.katana com.snapchat.android	13 sek	2020-05-03 18:45		
□	nn4t-u15m-s9pp-9phr	178.247.[redacted]	NEWW	6.0.1	Samsung SM-J700F Turkcell [redacted]9e@gmail.com 577@gmail.com		com.android.vending com.instagram.android com.google.android.gm com.facebook.katana	18 sek	2020-05-03 18:49		
	id98-dbh4-fv6b-t6ey						org.telegram.messenger com.whatsapp			0 tl	

OperadorMIB



#ID	TELEFONE:	TIPO:	LOGIN / CLAVE:	LOGIN EMP	SISTEMA:	ANOTAÇÃO	COMANDO:	CONTROLAR
#758		FISICA [XUXA]	[redacted]				LOADER - OFFLINE	⚙
#757		FISICA [XUXA]	[redacted]				LOADER - OFFLINE	⚙
#756		FISICA [XUXA]	[redacted]				LOADER - OFFLINE	⚙
#755		FISICA [XUXA]	[redacted]				LOADER - OFFLINE	⚙
#754		FISICA [XUXA]	[redacted]				LOADER - OFFLINE	⚙
#753		FISICA [XUXA]	[redacted]				ACESSO INVALIDO - OFFLINE	⚙
#752		FISICA [XUXA]	[redacted]				ACESSO INVALIDO - OFFLINE	⚙
#750		FISICA [XUXA]	[redacted]				LOADER - OFFLINE	⚙

Gustuff



☑ country ☑ cell ☑ android □ tag ☑ versionCode

Country: Country... LastCon: 15 With: Apps... Text: Search...

□	Id	Last Connect	Number	Apps	Cou	Cell	And	Code	Comment
□	1db907a5-af35-41df-a2cb-a82b2df2adc8	1 min	[redacted]	2		Telstra	7.0	410	
□	a1d5ad5a-32dd-4a1c-a776-83f4a7c19b03	3 min	[redacted]	1			8.0.0	410	
□	d804c096-fc87-4a15-8aa9-5d228d416951	13 min	[redacted]	1		YES OPTUS	7.0	410	
□	d4d4a88d-f1a8-4aa0-8f52-fb01732f7943	6 min	[redacted]	0		ALDImobile	6.0.1	410	
□	b8a31a18-cf4b-4bd0-b43f-c329277732a5	3 min	[redacted]	3		YES OPTUS	8.0.0	410	
□	588540ff-f812-4bd8-8f07-2b6202aaa899	2 min		0		vodafone AU	5.1	410	
□	872a9a55-5190-4642-8f0d-383f9a048acb	0 min		2			5.0.1	410	
□	62cd47c6-04f3-4746-9498-abbfdb8c5aab	1 min		0		Telstra	5.1.1	410	
□	acd576ac-9735-4426-bb70-d3c5a5a92367	8 min		0		Virgin Mobile	7.0	410	
□	83b1b8a4-5bc0-425a-9ff2-a0fcb5af5dc9	0 min		0		Telstra	7.0	410	
□	a16a278b-a442-4d8b-ba6c-c2c29c62806a	0 min	[redacted]	0		YES OPTUS	6.0	410	
□	af23a2aa-76bb-4121-a996-79f4af40290c	0 min		1		YES OPTUS	6.0.1	410	
□	90228a8c-515a-47a3-abb1-aa96025d479b	0 min		1			6.0.1	410	
□	2198baa4-a424-4f89-afda-df8fa2ab596d	0 min		0		Telstra	6.0	410	
□	cfab41f2-c8f3-46cd-b711-d8440f00daa4	0 min		1			6.0.1	410	
□	f6b005b5-0129-4383-ad34-5291cbaa422f	1 min		0			7.0	410	
□	d30198cf-a139-4a6d-ba20-9a6a38a2bd5c	4 min		0		Lycamobile	4.4.2	410	
□	d0f8578b-8153-420a-91fb-f6cbd798438c	2 min		2		YES OPTUS	7.0	410	
□	021804c1-265f-4dd4-81a3-2972c8a475f6	4 min		1		YES OPTUS	5.1	410	
□	37f8c775-8601-4482-aa52-550940a182f7	0 min		2			6.0.1	410	

PHISHING FRAMEWORKS

12

Over the past year, Group-IB specialists identified nearly 10,000 phishing attacks that involved the 11 most popular phishing frameworks[1]. Phishing framework developers are often based in the same region as the banks and other organizations that they target. Another trend is that attacks involving a specific framework continue even if the developer has been arrested. For example, many threat actors have created their own versions of phishing kits based on available U-Admin panel source code, which has lived on and enabled new threat actors to launch attacks despite its original developer being behind bars.

[1] Phishing frameworks are sets of tools designed for phishing that include kits that help quickly create phishing pages and admin panels for communicating with phishing websites and collecting stolen information.

U-Admin

#1

Attacked countries

Australia, Belgium, Germany, Greece, Denmark, Ireland, Spain, Italy, Colombia, Netherlands, New Zeland, Poland, US, Canada, Singapore, Finland, France, Sweden

Creator

Kaktys1010[2]

First activity

Unknown

Phishing frameworks

1593

U-Admin Panel ↗

[2] Kaktys1010 was arrested by Ukrainian law enforcement officials in February 2021.

Contiinued

#2

Attacked countries

Australia, UK, Ireland, Lithuania, Singapore, Sweden

Creator

Contiinued

First activity

April 2021

Phishing frameworks

34[1]

Contiinued panel ↗

Core Actions

#3

Attacked countries

Australia, UK, Ireland, Spain, Colombia, New Zeland, Norway, Philippines

Creator

Unknown

First activity

April 2021

Phishing frameworks

26

Express

#4

Attacked countries

Unknown

Creator

Express[2]

First activity

Unknown

Phishing frameworks

109

Express panel ↗

[1] Since May 17, 2021, Group-IB researchers have discovered 34 Contiinued admin panels, which means that this type of panel has been discovered on 34 different domains.

[2] The developer of the Express panel was arrested on July 20, 2021 as part of a joint effort by Group-IB specialists and the Dutch national police.

Haiku

#5

Attacked countries

Belgium, Netherlands

Creator

Haiku[1]

First activity

April 2021

Phishing frameworks

420

Haiku panel ↗

Kr3pto

#6

Attacked countries

Australia, UK, Ireland

Creator

Kr3pto

First activity

Unknown

Phishing frameworks

420

Kr3pto panel ↗

Kr3pto-A2 (ATPro)

#7

Attacked countries

UK, Denmark,
Norway, Singapore

Creator

Unknown[2]

First activity

April 2021

Phishing frameworks

18

[1] Haiku was arrested on October 19, 2020 thanks to the efforts of the cybercrime team of the Hague police.

[2] Kr3pto-A2, also known as ATPro, is a phishing panel based on the code of the Kr3pto panel. It was developed by a threat actor believed to be based in the United Kingdom.

Reliable[1]

#8

Attacked countries

Belgium, Netherlands

Creator

Reliable[2]

First activity

Unknown

Phishing frameworks

17

Reliable panel ↗

Secure Key

#9

Attacked countries

UK, Australia

Creator

Unknown

First activity

March 2020

Phishing frameworks

2679

sm_o

#10

Attacked countries

US

Creator

Unknown

First activity

July 2020

Phishing frameworks

249

[1] The phishing admin panel has all the capabilities and eliminates weaknesses of another popular phishing admin panel, U-Admin

[2] The developer of Reliable was arrested on July 20, 2021 as part of a joint effort by Group-IB specialists and the Dutch national police.

SPOX

#11

Attacked countries

🇺🇸 US

Creator

Dila Belmili[1]

First activity

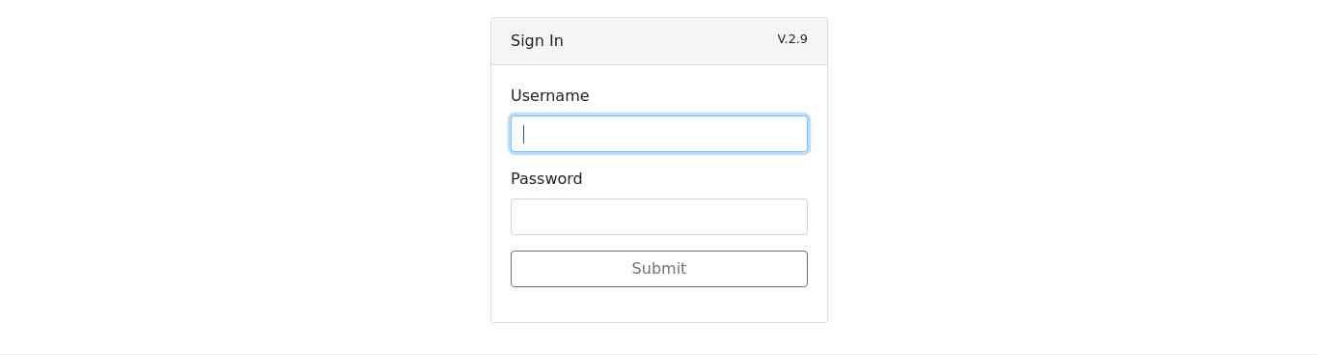
Неизвестно

Phishing frameworks

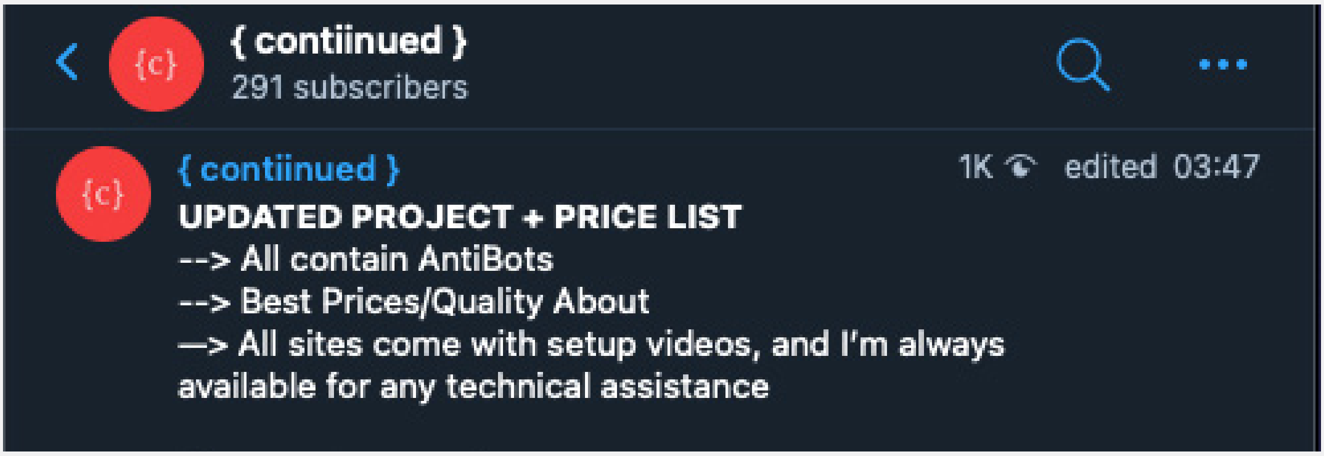
78

[1] Phishing panel developed by an Algerian threat actor called Dila Belmili.

U-Admin panel



Contiinued panel



{ contiinued }

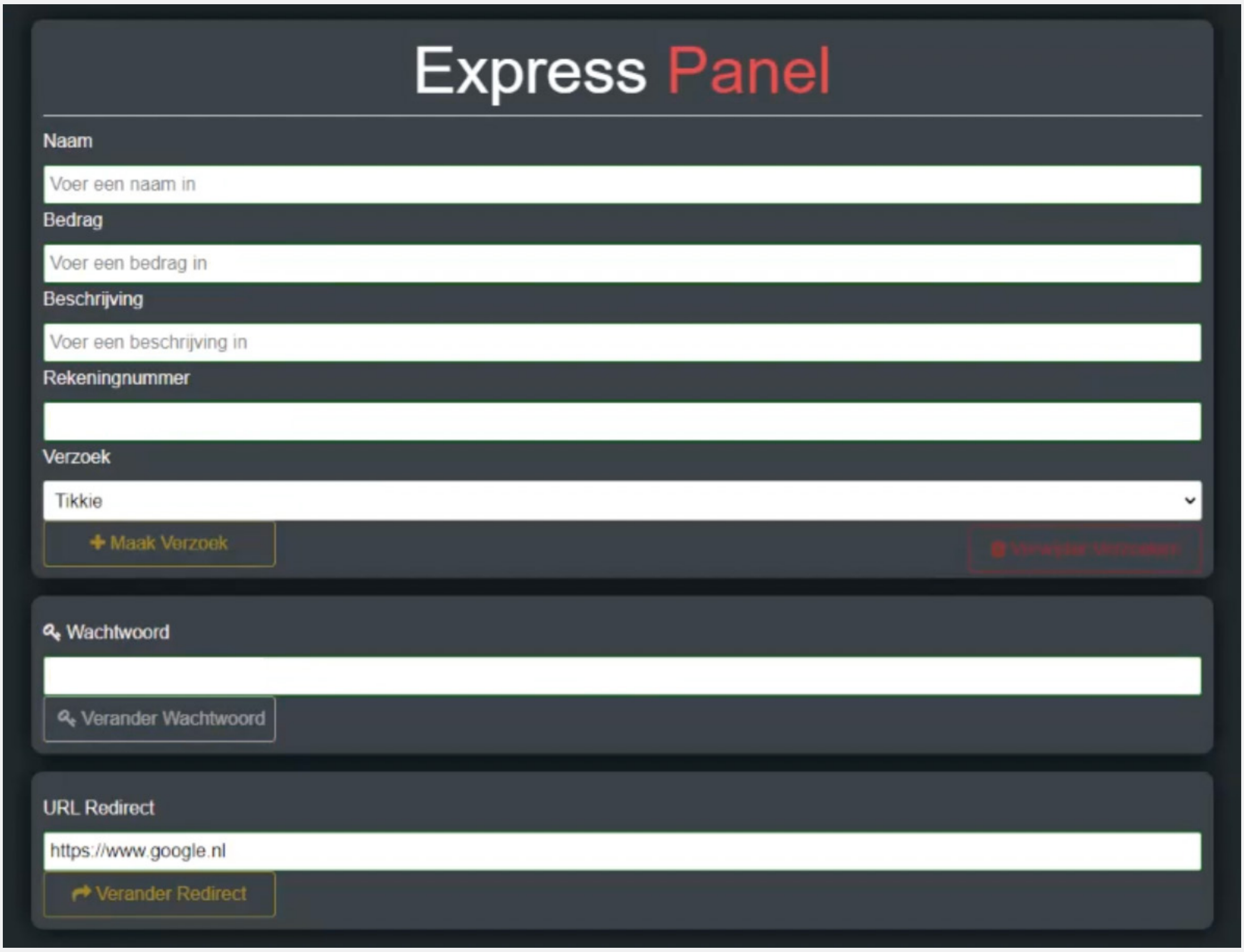
UPDATED PROJECT + PRICE LIST

--> All contain AntiBots

--> Best Prices/Quality About

—> All sites come with setup videos, and I'm always available for any technical assistance

Express panel



Express Panel

Naam

Voer een naam in

Bedrag

Voer een bedrag in

Beschrijving

Voer een beschrijving in

Rekeningnummer

Verzoek

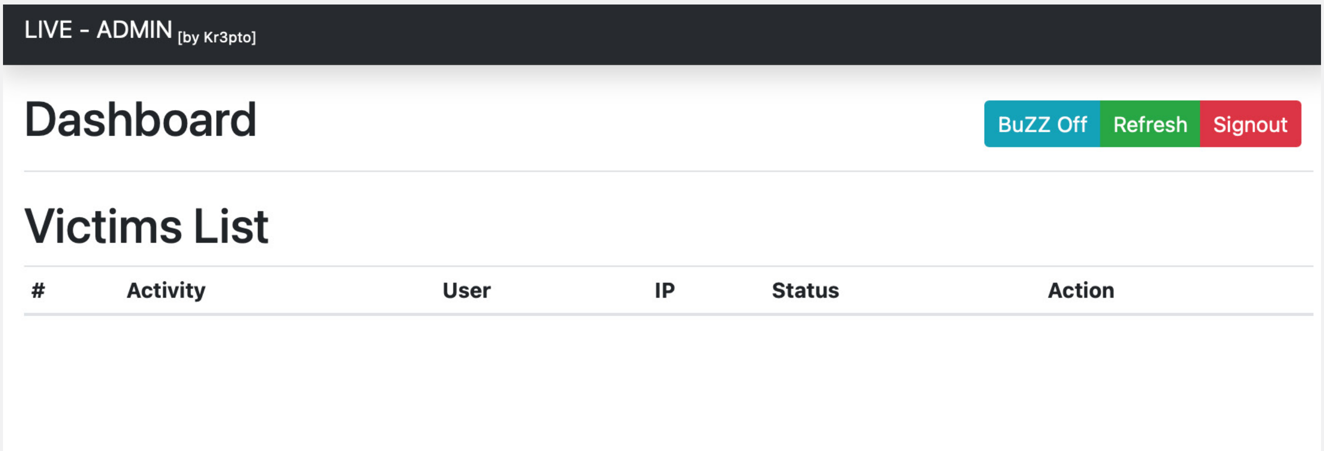
Tikkie

Wachtwoord

URL Redirect

https://www.google.nl

Kr3pto panel



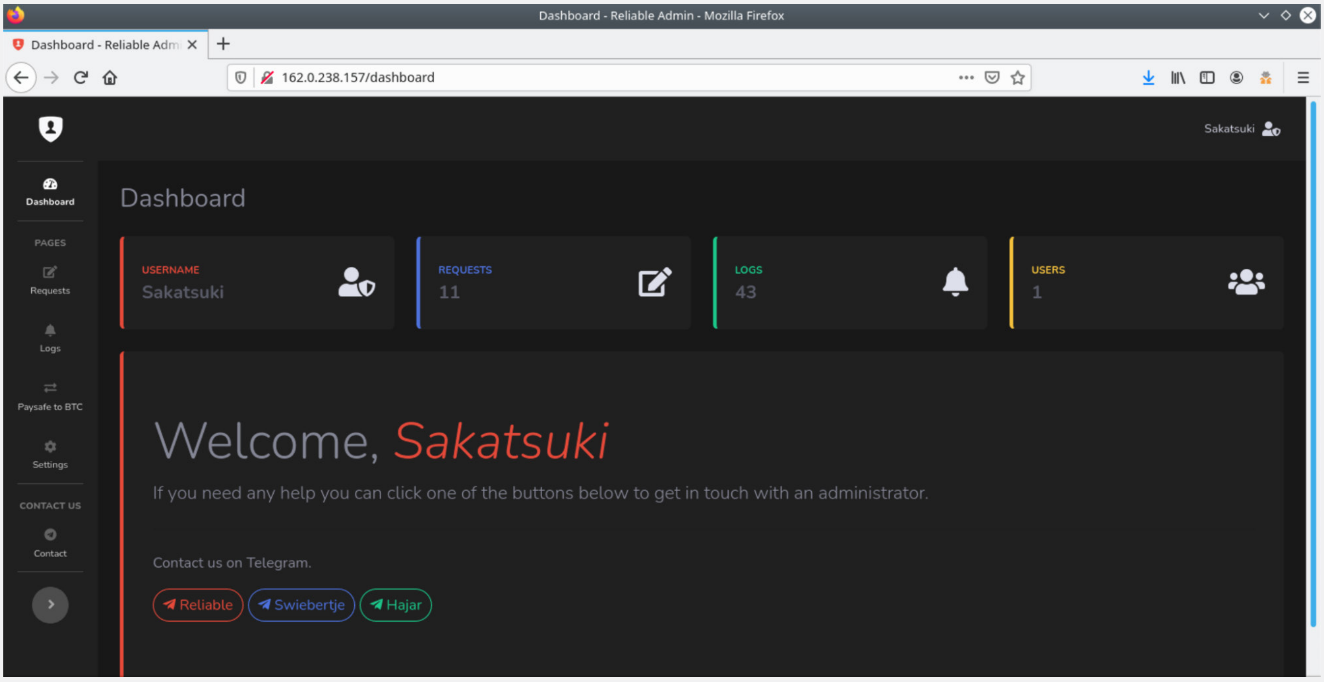
LIVE - ADMIN [by Kr3pto]

Dashboard

Victims List

#	Activity	User	IP	Status	Action

Reliable panel and examples of ads



Dashboard

USERNAME Sakatsuki

REQUESTS 11

LOGS 43

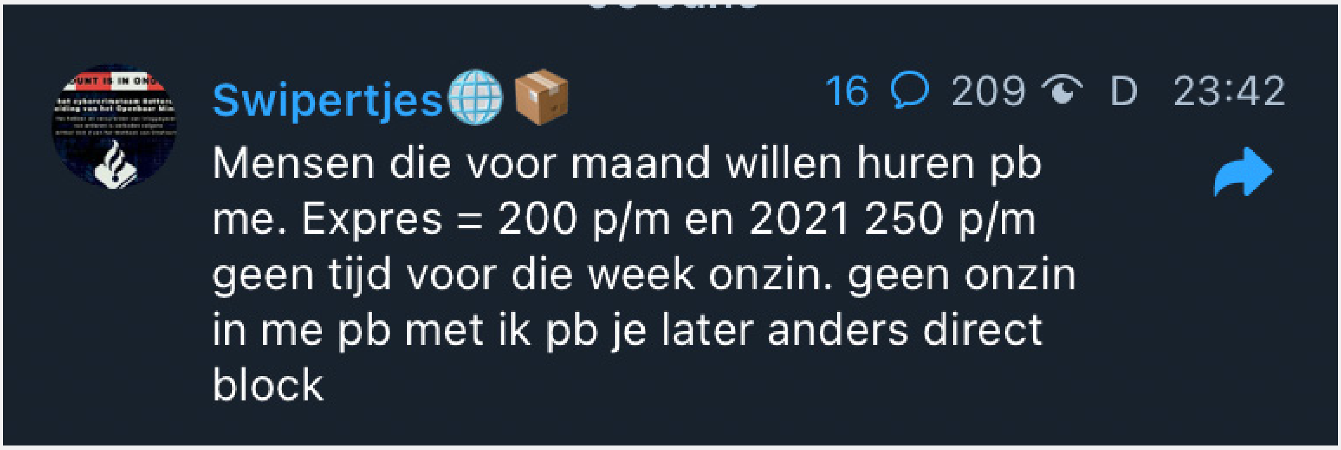
USERS 1

Welcome, *Sakatsuki*

If you need any help you can click one of the buttons below to get in touch with an administrator.

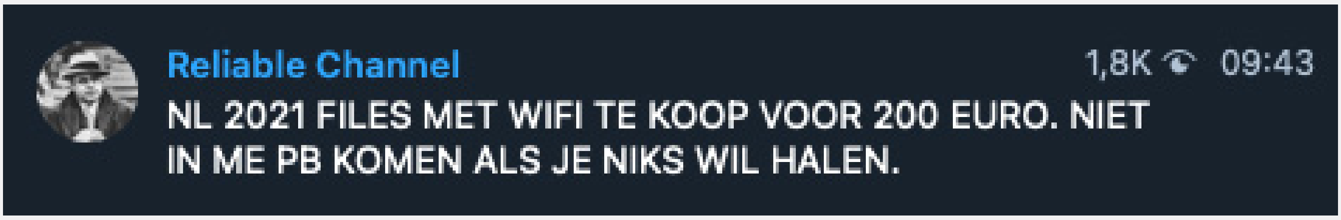
Contact us on Telegram.

Reliable Swiebertje Hajar



Swipertjes🌐📦 16 💬 209 👁 D 23:42

Mensen die voor maand willen huren pb me. Expres = 200 p/m en 2021 250 p/m geen tijd voor die week onzin. geen onzin in me pb met ik pb je later anders direct block



Reliable Channel 1,8K 👁 09:43

NL 2021 FILES MET WIFI TE KOOP VOOR 200 EURO. NIET IN ME PB KOMEN ALS JE NIKS WIL HALEN.

ACTIVITY OF JS SNIFFERS

13

During the most recent reporting period, Group-IB specialists discovered over 80,000 bank cards compromised using JavaScript sniffers. The top five banks who had the most cards compromised are all based in the US. The top 20 include Brazilian, UK, Indian, Canadian, Malaysian, and Singaporean banks. This means that, even though threat actors are interested in attacks on online stores in many countries, cards in the US are still a priority for them. Out of 98 families known to Group-IB specialists, 42 were active in the reporting period.

More than 33,000 cards were compromised using the JS sniffer called ImageID, which was developed by a threat actor with the alias poter. A threat group dubbed Improved-ImageID continues to use a modified version of poter's malware to attack online stores. In October 2020, MalwareBytes specialists **discovered** that the group had infected the website belonging to the wireless provider boom! MOBILE.

The group **CoffeMokko** is still active. According to Group-IB's data, the hackers stole more than 29,000 bank cards using JS sniffers In November 2020, Group-IB specialists noticed that nearly all of the group's infrastructure had gone offline, but attacks involving the CoffeMokko JS sniffer against e-commerce websites quickly resumed.

In March 2021, Group-IB specialists discovered a new sniffer family dubbed WorldCommerce. The hackers use compromised websites as gates for collecting stolen data. During the reporting period, nearly 300 bank cards were stolen using this sniffer. A little later, the group compromised about 6,000 more bank cards.

Several threat groups that use the JS sniffer called Inter, which was developed by a threat actor with the alias Sochi, were also active in the past year. According to Group-IB, more than 16,000 bank cards have been stolen using Inter. One of the group's victims was a video-conferencing platform called Playback Now. Malwarebytes reported about the breach in October 2020.

UltraRank: The unexpected twist of a JS-sniffer triple threat

ULTRARANK

AUGUST 2020

The unexpected twist of a JS-sniffer triple threat

NAME	UltraRank
ACTIVITY	Theft of bank card data using JavaScript sniffers
VICTIMS	691 online stores, 13 third-party suppliers
GEOGRAPHICAL SCOPE	Europe, Asia, North America, Latin America
PERIOD OF ACTIVITY	5 years

GROUP-IB

group-ib.com

In November 2020, Group-IB specialists **discovered** new attacks on e-commerce websites conducted by the group called UltraRank, which has been active since 2015. As part of its new campaign, the group hacked 12 websites belonging to online stores and infected them with the JS sniffer called SnifLite, which the group started using as early as 2018. In late January 2021, however, the card shop ValidCC, believed to have been used by the group to monetize stolen cards, closed down. A ValidCC representative known on underground forums as SPR said that the closure was due to servers being seized by law enforcement. As a result, the card shop's operators lost access to the compromised card database and the shop's backend. Since the shop closed, Group-IB specialists have not detected any new UltraRank attacks, despite the group's infrastructure still being partially active.

Some threat groups that target online stores experiment with legitimate infrastructures to host malicious code. In May 2021, Group-IB specialists **described** the activity of a group called GrelosGTM, which was discovered in April 2020. As part of its activity, the group used a legitimate service, Google Tag Manager, to deliver malicious code to infected websites. In February 2021, researcher Eric Brandel, together with Sansec specialists, found that GrelosGTM used a different platform, Google Apps Script, to deliver malicious code to online stores.

Threat actors also experiment with ways to exfiltrate bank card data stolen from users of infected online stores. A JS sniffer dubbed TelegramExfil used the Telegram bot API to send intercepted card data to the sniffer operators; this was **reported** by Malwarebytes in September 2020.

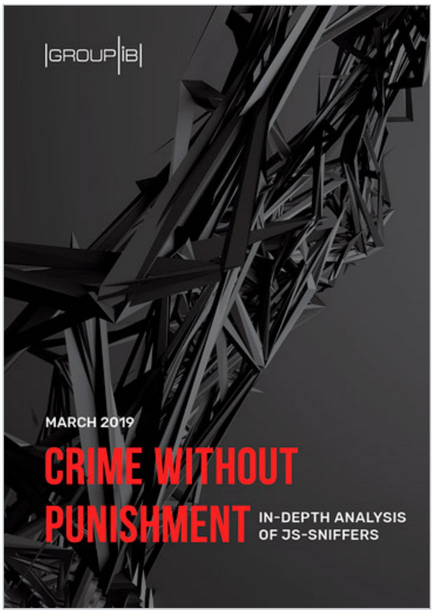
In January 2021, Group-IB specialists detected a new sniffer family called **E1RB**. The threat group that developed the sniffer used multiple unconventional approaches to obfuscate malicious code samples: with each request to the threat actors' server, a new and unique obfuscated sniffer sample was generated. Part of the obfuscation mechanism was request time, where the minute value was used to decrypt the sniffer code when the code was being executed. To obfuscate the JS code, the threat actors used an open-source obfuscator called **Hunter**.

In December 2020, Group-IB specialists published a detailed **analysis** of the activity of the threat group known as FakeSecurity, which carried out malicious campaigns targeting admins of online stores in order to infect their websites with malicious JS code and steal bank cards. During its attacks, the group used a framework for creating landing pages to spread the malware Mephistophilus, the stealers Vidar and Raccoon, as well as the stealer FakeSecurity, which was developed internally by the group and obfuscated using an algorithm called aaencode.

Attacks involving a JS sniffer called Mr.Sniffa, created by a threat actor with the alias Billar, continue. In addition, unidentified threat actors adjusted the sniffer's admin panel to distribute malware under the guise of Adobe Flash Player. In November 2020, Sucuri specialists described a campaign that involved an injector borrowed from Mr.Sniffa, but instead of stealing cards it loaded obfuscated code to show a fake update window.

At least four groups behind JS-sniffers described in the report **Crime without punishment: In-depth analysis of JS-sniffers** are still active. The group that uses PostEval continues to attack online shops. The group behind Illum also remains active. The group that used MagentoName modified the code from its arsenal and carried out one of the biggest attacks against Magento websites, which was discovered by Sansec specialists in September 2020. At the time, the group infected 2,806 websites powered by Magento version 1. The group that uses ReactGet is still active: it infects websites, maintains its infrastructure, and conducts

Crime without punishment: in-depth analysis of JS-sniffers



phishing attacks, some of which were discovered in September–December 2020 and January–March 2021.

Table with active and non-active JS-sniffers during the reporting period (H2 2020 — H1 2021)

Sniffer Name	Emerged/Detected	Active during the reporting period
Qoogle	April 2018	Yes
FareCloud	April 2020	Yes
SF_GATE	April 2020	Yes
ant_cockroach	August 2019	Yes
AnyCDN	August 2020	Yes
Inter	December 2018	Yes
docReady	December 2019	Yes
CounterApi	December 2020	Yes
ShipBill	December 2020	Yes
Shopi-DGA	December 2020	Yes
ArrCut	February 2020	Yes
EpikCDN	February 2020	Yes
OurHoney	February 2021	Yes
FakeClicky	January 2018	Yes
E1RB	January 2021	Yes
ImageId/Poter/Improved-ImageId	July 2016	Yes
FakeGraph	June 2020	Yes
Mr.Sniffa	March 2020	Yes
SunPearl	March 2020	Yes
WorldCommerce	March 2021	Yes
ReactGet	May 2017	Yes
OrderManagement	May 2021	Yes
Illum	November 2016	Yes
FakeSecurity	November 2018	Yes
OrderData	November 2019	Yes
AngryBeaver	November 2020	Yes
ClearConsole	November 2020	Yes
SadPixel	October 2019	Yes
FellSoGood	July 2020	Yes
CoffeMokko	September 2017	Yes
PostEval	September 2017	Yes
SnifLite	September 2018	Yes
occhurch	September 2020	Yes

Sniffer Name	Emerged/Detected	Active during the reporting period
TelegramExfil	September 2020	Yes
GuettaTech	October 2020	Yes
HostSSL	April 2020	Yes
JCI	October 2019	Yes
LazySale	November 2020	Yes
TrackStat	December 2019	Yes
WooAnalytics	July 2021	Yes
XStatic	November 2020	Yes
zzzerohost/Baka	March 2020	Yes
MirrorThief	April 2019	No
SJTI	April 2019	No
PokerFace	August 2019	No
OldGrelos	December 2015	No
MagentoName	December 2017	No
event_handler	December 2019	No
fouhasgfuas	December 2019	No
GetBilling	February 2018	No
Atlas	February 2019	No
MageConnectors	February 2019	No
TimedMe	January 2018	No
FabricRelay	January 2019	No
Luna	January 2019	No
MakeFrame	January 2020	No
SeoStat	January 2020	No
SpaceManager	January 2020	No
FakeLogistics	July 2015	No
EUTag	July 2018	No
addtoev	July 2019	No
simplewheel	July 2019	No
TokenMSN	June 2016	No
CheckTrack	June 2020	No
TokenLogin	March 2016	No
Analyt	May 2019	No
ATMZOW	May 2019	No
AwesomeSocket	May 2019	No
CDNAPI	May 2019	No
GMO.LI	May 2019	No
ShellSn	May 2019	No

Sniffer Name	Emerged/Detected	Active during the reporting period
FakeCDN	November 2016	No
PreMage	November 2016	No
LoadReplay	November 2017	No
503Susp	November 2018	No
Pipka	November 2019	No
cCreateSelectionDiv	March 2020	No
WebRank	October 2016	No
MatrixShop	October 2018	No
FakePixel	October 2019	No
MakeEvent	October 2020	No
G-Analytics	September 2016	No
OrgCDN	September 2018	No
FakeGAds	September 2019	No
GrelosAnalytics	July 2019	No
HellGate	May 2019	No
HotelTrack	August 2019	No
Iranimo	October 2019	No
jQueryFact	May 2019	No
Lazarus clientToken	May 2019	No
Lazarus preloader	February 2020	No
LinkCatalog	June 2017	No
LogEvil	January 2019	No
MajorMs	October 2018	No
WebPackCDN	July 2019	No
VeterinaryConcepts	September 2018	No
Voldemort	August 2018	No
XMLRAW	September 2019	No

SECURITY RECOMMENDATIONS

14

Financial organizations face a number of serious cyber threats. After studying the techniques and methods used by threat actors, Group-IB developed recommendations to help organizations in the finance industry to defend against all types of attack.

Sale of access to financial institutions

1. Configure account access blocking to protect against brute-force attacks.
2. Check public data leaks for sets of credentials and change passwords that have been found in leaks.
3. Limit remote access so that it can be gained only from trusted IP addresses or after a device that tries to gain remote access has been successfully identified. If these measures are not possible, ensure filtering by Geo IP.
4. Disable or block unused remote services.
5. Use multi-factor authentication for remote service accounts. This limits opportunities for using compromised credentials.
6. Use minimal privileges for service accounts, restricting the permissions granted to processes with potential vulnerabilities that hackers can potentially exploit.
7. Install software updates on a regular and timely basis to eliminate any identified vulnerabilities.
8. Analyze security posture and test for breach vulnerabilities to identify weaknesses and possible attack vectors.
9. Take stock of the external network perimeter, network firewall rules, and network address broadcasting (NAT) rules to minimize the likelihood of making any services public by mistake.
10. Continuously identify shadow IT[1] to manage your attack surface.

[1] Shadow IT are systems and devices used by employees without the company's IT department knowledge or approval.

11. Ban Internet access for any easily compromised devices such as video surveillance equipment, smart home devices, office equipment (printers, scanners, multifunctional printers), and storage devices and media (such as SOHO-segment NAS servers).
12. Limit network access for specific tasks (e.g., contractors should get access only to servers that they need to carry out their work, rather than a whole network segment or the entire network).
13. Add an “expires at” field to user accounts and access privileges for situations when manually revoking remote access could fail.
14. Identify signs of initial access, gaining persistence, and progress across the network. Although most techniques used by attackers are primitive and can be detected even with an untrained eye, regular proactive threat hunting helps prevent and combat sophisticated attacks.
15. Regularly scan the infrastructure for indicators of compromise to detect signs of unauthorized network access.
16. Ban users from signing up to third-party services with their corporate email address.

Ransomware attacks

1. Focus on winword.exe/excel.exe creating suspicious folders and files or starting processes such as rundll32.exe and regsvr32.exe.
2. Hunt for suspicious cscript.exe/wscript.exe executions, especially involving network activity.
3. Search for powershell.exe processes with suspicious or obfuscated command lines.
4. Analyze executables and scripts dropped into the Startup folder, added to Run keys, or run via scheduled tasks.
5. Monitor sdbinst.exe execution for suspicious command line arguments.
6. Monitor sub keys created under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.
7. Make sure your security controls detect command lines that are typical for credential dumping tools such as Mimikatz.
8. Hunt for common artifacts of network reconnaissance tools such as AdFind’s command line arguments.
9. Search for file artifacts related to executing files from uncommon locations such as C:\ProgramData, %TEMP% or %AppData%.
10. Hunt for RDP-related Windows Registry and Firewall modifications.
11. Collect and analyze RDP connection data to uncover any lateral movement attempts.
12. Hunt for wmic.exe executions with suspicious command lines.
13. Monitor bitsadmin.exe for abnormal behavior, especially related to downloads of potentially malicious files.
14. Make sure that your systems detect Cobalt Strike beacons and similar payloads typical for post-exploitation frameworks. At the very least, focus on systems that are launched with common command line arguments and from common locations.
15. Hunt for network connections from common system processes. You can also use known lists of Cobalt Strike team servers, which you can obtain from your cyber threat intelligence provider.
16. Search for new service creation events related to PsExec, SMBExec, and other dual-use or offensive security tools.

17. Hunt for executables masqueraded as common system files (e.g. svchost.exe) and that have uncommon execution parents or locations.
18. Monitor remote access software in your network for signs of unauthorized usage.
19. Search for cloud storage client installation events and cloud storage access events and check whether they are legitimate.
20. Hunt for common FTP software on endpoints to identify installations with malicious configurations.

Phishing, scam and phishing affiliate programs, fake payment pages

1. Set up a process for collecting information about fraudulent links and screenshots with links submitted by customers.
2. The links must be analyzed and blocked.
3. Analyze transactions to identify cash-out schemes.
4. Hunt for phishing websites.
5. Inform customers about fraud schemes.

Banking botnets and Trojans

1. Conduct session analysis to detect man-in-the-browser attacks.
2. Analyze sessions to detect instances of remote control over a computer during payment.
3. Analyze and identify user computer environment simulation.
4. Detect compromised logins, passwords, and bank cards.

Malware for Android

1. Using mobile apps, analyze the environment and detect suspicious apps on the device.
2. Detect instances of applications being launched with root permissions.
3. Detect overlay windows being displayed.
4. Detect SMS messages and push notifications being intercepted.

JS sniffers

1. Require that e-commerce websites adhere to strict security measures.
2. Make provisions for malware express checks on e-commerce websites, in the contracts.
3. Carry out express checks.
4. Detect the source of compromised cards by identifying locations (physical or online) where multiple compromised cards have been used.
5. Analyze the cards put up for sale on card shops to detect how and from where the card data may have been stolen.

Group-IB

A global leader in high-fidelity Threat hunting and Intelligence, best-in-class fraud prevention solutions, and high-profile cyber investigations.

Group-IB's mission: Fight Against Cybercrime

Interpol and Europol

Partner and active collaborator in global investigations

APAC TOP 10

Ranked among the Top 10 cybersecurity companies in the APAC region according to APAC CIO Outlook

Group-IB Threat Intelligence and Research Centers

- Globally distributed cybercrime monitoring infrastructure
- Digital Forensics & Malware Analysis laboratory
- Incident Response and High-Tech Crime Investigations
- CERT-GIB: 24/7 monitoring centers and Computer Emergency Response Team

- Europe
- Russia
- Middle East
- Asia-Pacific

Group-IB's technologies & innovations

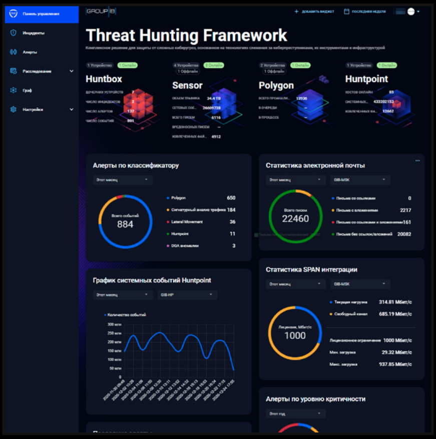
Group-IB's experience in performing successful global investigations with state-of-the-art threat intelligence and detecting cybercriminals at every stage of attack preparation has been fused into an ecosystem of highly sophisticated software and hardware solutions designed to monitor, identify, and prevent cyber threats.

Group-IB's technologies are recognized by the world's leading research agencies

IDC Gartner FORRESTER kuppingercole ANALYSTS FROST & SULLIVAN

Threat Intelligence & Attribution

System for analyzing and attributing cyberattacks, threat hunting, and protecting network infrastructure

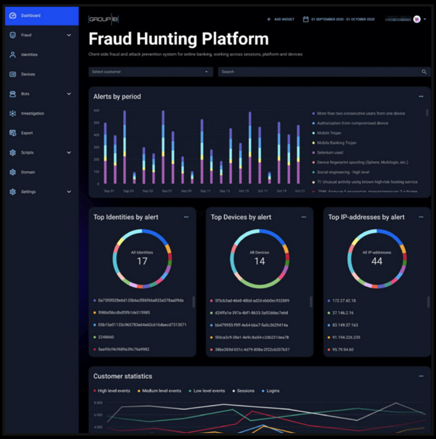


Threat Hunting Framework

Adversary-centric detection of targeted attacks and unknown threats within the infrastructure and beyond

Digital Risk Protection

AI-driven platform for digital risk identification and mitigation



Fraud Hunting Platform

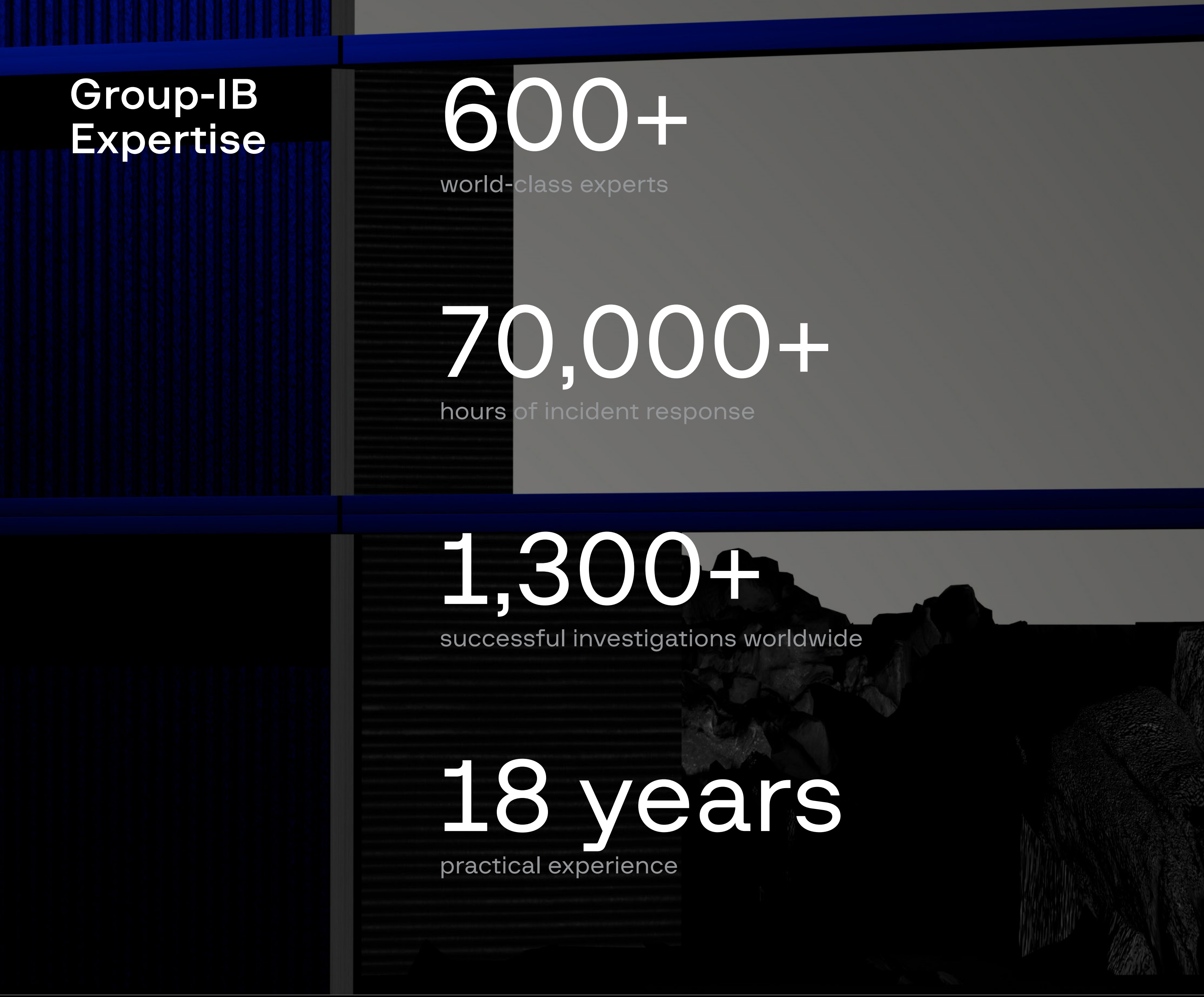
Real-time client-side digital identity protection and fraud prevention

Atmosphere: Cloud Email Protection

Patented email security technology that blocks, detonates and hunts for the most advanced email threats

AssetZero

Intelligence-driven attack surface management that continuously discovers all external-facing IT assets



Group-IB Expertise

600+
world-class experts

70,000+
hours of incident response

1,300+
successful investigations worldwide

18 years
practical experience

Intelligence-driven services

Group-IB's technological leadership and R&D capabilities are built on the company's 18 years of hands-on experience in performing successful cybercrime investigations worldwide and the 70,000 hours of cybersecurity incident response accumulated in our leading forensic laboratory and CERT-GIB.

Prevention

- Security Assessment
- Compliance Audit
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Cyber Education

Response

- Managed Incident reponse
- Managed detection and threat hunting

Investigation

- Digital Forensics
- Investigations
- Financial Forensics
- eDiscovery

PREVENTING AND RESEARCHING CYBERCRIME SINCE 2003

www.group-ib.com info@group-ib.com group-ib.com/blog +7 495 984 3364