Kaspersky Fraud Prevention 2019

Fraud report based on Kaspersky Fraud Prevention data.

kaspersky BRING ON THE FUTURE

More information at kfp.kaspersky.com

Table of contents

Cyberfraud in 2019

In our fast-moving digital world, regulators are trying to address the multi-faceted challenge of protecting consumers, whilst fostering innovation and economic development. The ever-increasing amounts of data flowing across ever-blurring geographical boundaries make it increasingly difficult to catch up with criminals and develop regulations able to cope with new technologies and new crimes.

This introduction is written by Neira Jones*:

More than 20 years in financial services and technology made Neira believe in change through innovation and partnerships.

She is regularly invited to advise organizations of all sizes on payments, FinTech, RegTech, cybercrime, information security, regulations (e.g. PSD2, GDPR, AML), and digital innovation.

She always strives to demystify the hype surrounding current issues and also enjoys her work as an expert witness for matters related to payments security.

She likes engaging on social media and regularly addresses global audiences as a keynote speaker or chairperson, as well as being a regular press commentator.

She is a Non-Executive Director for Nasdaq-listed cybersecurity firm Cyber1 and also chairs the Advisory Board for mobile innovator Ensygnia.

She is a partner for the international Global Cyber Alliance and ambassador for the Emerging Payments Association.

As the socio-economic landscape evolves, with the emergence of the gig economy, the increase in remote and mobile working, the adoption of "everything-as-a-service" and cloud computing, the concept of "identity management" now has to include what people own, share, and use. "Things" are becoming part of our lives and must therefore be identified and managed accordingly. "Things" are now part of the "Context" in which we interact, and as enterprises increasingly adopt intelligent devices and other endpoints (such as BYOD 13, electronic tags, sensors, process and distributed control), the attack surface grows accordingly.

The lack of interoperability and standards, combined with the disparity among industries and jurisdictions, only serves to increase complexity. And whilst a focus on technology is legitimate, we must not lose sight of the human element: social engineering is still the dominant cause of data breaches, which reminds us of the fact that a good cybersecurity strategy should always include the three elements of "People, Process, and Technology".

Undoubtedly, our current landscape not only presents an ever-growing attack surface, but also a complex regulatory maze. This complexity has generated the need for more and more automation, which itself has engendered an increased focus on technologies which deliver such automation (e.g. AI, machine learning, behavioral analytics), and the birth of a new buzzword: RegTech, meaning Regulatory Technology, or the application of technology to enhance regulatory processes.

But let's not be fooled: whilst automation has become a necessary component of any cybersecurity strategy, it alone does not make a sensible or even viable strategy. Of course, in an ideal world, technology would be able to spot and stop crime without human intervention. Unfortunately, one thing gets in the way: Real Life.

Technology is only ever as good as its designers, and the data available to derive insights is neither perfect nor completely accurate. Furthermore, technology can also be used against itself, as evidenced by the emergence of methods such as "Adversarial Machine Learning" where malicious attacks can be designed to subvert defensive technologies in order to appear legitimate or inoffensive.

So let's not get swept up by the hype. Any technology solution claiming absolute protection should be treated with caution. Whilst technologies such as AI or behavioral biometrics have a legitimate place where a specific risk can be mitigated by their use, a good cybersecurity strategy will always come down to common sense: any technology, on its own, will not do the job.

* Full article available at: https://kfp.kaspersky.com/wp-content/uploads/2019/05/It-aint-what-you-do-NJ-WEB.pdf

As always, the basics will need to be covered first, and the risks specific to the organization will need to be managed, just like any other risk. Technologies will need to be deployed, and they will not necessarily be sexy (e.g. endpoint protection, malware detection, access management, etc.). And the appropriate processes will need to be put in place to make those technologies effective (e.g. incident response, software life-cycle management, supply chain governance, patching, encryption, etc.).

And of course the human element will need to be addressed, both internally and at the consumer level (e.g. training, education, end-user policies, acceptable use, etc.). Deploying a layered approach, where automation is used and where the processes lend themselves to it, will free staff to concentrate on complex cases or reviews and value-adding activities. Again, everything has its place, in the right context.

Laws governing the security of financial organizations: everything you wanted to know about compliance

Europe

Two years have passed since the second Payment Services Directive (PSD2) went into effect on January 13, 2018. This has led to many questions. For instance, how and when is strict client authentication applied? And, if you provide third parties with access to bank accounts through an API or other interfaces, would this disrupt the long-standing ecosystem—or benefit it?

The situation was complicated even more by the enactment of the General Data Protection Regulation (GDPR) on May 25, 2018, and by the strengthening of strict rules to combat money laundering throughout the world. One of the positive market trends is the emergence of new services that utilize the advantages of Open Banking. Apps used for banking licenses have become very popular, especially in Europe, and all kinds of organizations have submitted applications to register as third-party providers in this, suddenly more open, payment ecosystem.

What happened in 2018 is a strange yet widespread change to corporate culture. This is because the new crop of digital technologies over the past several years helped companies realize that their enormous goodwill would dominate their vision statement, and the appropriate technologies were used to create this goodwill, unencumbered by obsolete infrastructure. This did not happen overnight. For example, reputable companies like Intuit, Trustly, Sofort, Yodlee and Mint relied on what is known as "screen scraping" for years. This is fraught with risk, because cybercrime continues to evolve along with the evolution of technology. Fraud and theft of personal data have become a constant problem of modern times.

In our opinion, implementation of such measures is completely logical from a security standpoint. When using a direct access model, the owner of a banking account must share their bank account data with a third party, so that data can be obtained from bank account information for service provision, such as a tax statement. It is understandable that banks are unhappy with this model, because they are not capable of knowing whether the customer obtains access to their user account directly or through a third party, as both scenarios use the same set of account credentials. Prior to PSD2, these third parties were not regulated. PSD2 places them under regulatory control as third-party providers (TPP) and classifies them as account information service providers (AISP) like Intuit, or as payment initiation service providers (PISP) like Sofort.

PSD2 is aimed at improving the security of the ecosystem by using differentiated authentication of various parties when accessing payment accounts.

PSD2 went into full effect on September 14, 2019, but the European Banking Authority allowed an extension of the deadlines for strict customer authentication (SCA) due to delays in implementation.

SCA is based on the use of two or more factors classified as follows:
- something only the user knows,
- something only the user has,
- something only the user is.

These factors must be single-use factors, non-duplicated (except inertial), and securely stored. This is required, so that if one factor is compromised, it does not threaten the security of the others. It is also developed in a way that protects the confidentiality of the authentication data.

In addition, for higher-risk remote transactions, such as online payments in which the user initiates a transfer of funds through their banking app or payment using a card on the vendor's website, the generated authentication code must correspond to the amount of the payment transaction and the recipient.

The regulation essentially prescribes a set of risk assessment rules for each transaction. If the risk is low and an exception is applied, SCA will not be required. This means that simplified payment methods, for instance, with one mouse click, are still possible, but participants of the ecosystem must have the capability to effectively use the data[1].

[1] https://kfp.kaspersky.com/wp-content/uploads/2019/05/PSD2-Open-Banking_SCREEN.pdf

Our recommendations:

- **Monitor the ID of the device** used by the customer for accessing the automated system to check if it matches the IDs of devices of other customers of the lending organization, including those customers whose accounts were closed as part of money laundering countermeasures.
- **Implement mechanisms for checking** whether transactions are involved in money laundering of illegally obtained funds that are not always directly associated with theft from bank accounts. For financial transactions, one element whose identifying information must be known is the IP address from which the customer obtains access to the remote banking system.
- **Conduct a preliminary scan of the device** to check for malware. If malicious code is detected, prevent it from being propagated further and mitigate its effects.
- **Implement mechanisms for detecting** fraudulent payments, with the capability to upload FIDOs obtained from FinCERT.
- **Notify the Bank of Russia** about any identified and potentially upcoming incidents, fraudulent accounts, and devices associated with any violation of the requirements regarding information security when transferring funds through the payment system of the Bank of Russia, including information about unauthorized transfers of funds.
- **Analyze instances** where individuals acting on behalf of a customer (agents) receive encryption keys and authentication information for remote banking system access, and identify instances where those agents acted in the interests of other customers, including customers whose accounts were closed as part of money laundering countermeasures.

Russia

Most fraudulent transactions are associated with withdrawal of stolen funds, tax evasion, laundering of criminal money to finance terrorism and other illegal activity.

The consequences of these activities negatively affect the business of financial organizations, causing direct reputational and financial damage to companies and their customers, and attracting the attention of regulatory agencies.

Failure to adhere to established regulations will result in penalties and restrictions on provision of transactional services, such as accepting deposits from individuals and issuing loans to companies.

If there are suspicions that a transaction is being conducted without the consent of the customer, it is extremely important for the bank to obtain information about this immediately. Even if a PIN code is entered incorrectly or an electronic signature is used, there is still a risk that a transaction is being conducted by a criminal. Kaspersky Fraud Prevention automatically analyzes the characteristics and parameters of the device, environment, location, time of the transaction, behavior of the customer and other parameters, and identifies signs that are not typical of the customer.

Based on rules and machine learning, the antifraud system generates ready-made incidents for associated devices that are involved in cross-organizational or international money laundering schemes.

The global database of IP addresses maintained by Kaspersky determines any connection between a specific address and the fraudulent activity. If such activity occurred, the address is marked as suspicious and the appropriate information is relayed to bank monitoring systems.

The presence of malicious code or a banking Trojan on a user's device is a high risk in terms of customer session assessment, because this type of malware can be used to spoof the actions of an authorized user, intercept security codes from text messages and push notifications, spoof money orders, etc. Kaspersky Fraud Prevention includes patented state-of-the art technologies that are able to recognize various types of malware targeting financial systems, phishing, and fake applications, and provides secure connections and data integrity.

If malicious code is detected, Kaspersky Fraud Prevention sends information about it to banking systems in real time through an API or displays web consoles.

Kaspersky Fraud Prevention is capable of detecting fraudulent activity in web banking applications, mobile banking apps and remote banking systems including compromised accounts, account takeovers and devices being used for money laundering. The solution provides the capability to upload black lists of fraudulent device IDs, IP addresses and SIM card numbers received from other resources including FinCERT.

These days, there is talk of collecting more detailed information about users' devices when working with remote banking systems. An advanced device fingerprint by Kaspersky Fraud Prevention contains more than 100 unique parameters for web applications and approximately 140 for mobile devices, which ensure the completeness of the collected information. None of this data is considered to be personal data according to the Russian classification.[2]

[2] Excerpts from the main regulatory documents
(Main documents: 115-FZ; 161-FZ, 167-FZ, 375-P; 382-P; GOST R 57580.1-2017)

General statistics based on Kaspersky Fraud Prevention data

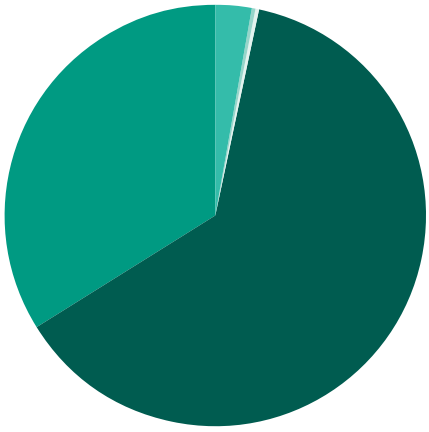
The Kaspersky Fraud Prevention report is based on incidents associated with cybercrime and on data detected by Kaspersky Fraud Prevention in 2019 after thorough analysis of consumer behavior and fraud trends. In this report, we discuss the main threats encountered by companies and cyberfraud trends with a focus on cybersecurity issues of the banking sector and e-commerce, and demonstrate our main conclusions.

Kaspersky Fraud Prevention processes traffic in real time according to the following parameters:

Metric name	Number of unique units per day
Device (browser)	50 M
User	29 M
Online session	332 M
Processed event	6 Bn

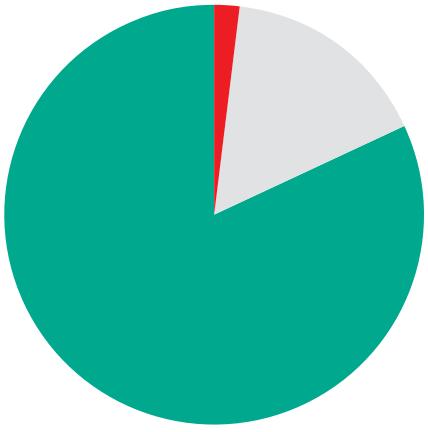
Risk-Based Authentication – an authentication method based on the assessment of various properties and parameters of an online session of a user and a device.

Incidents generated by Kaspersky Fraud Prevention



- Infected device **63%**
- Account takeover **34%**
- Money laundering **3%**
- Automation tools **0.39%**
- New account fraud **0.14%**

Risk-Based Authentication verdicts



- Red (high risk of fraud) **1.95%**
- Gray (not enough information, moderate risk of fraud) **16.21%**
- Green (legitimate user) **82%**

Session events analysis with Kaspersky Fraud Prevention

Device and Environment Analysis

Leverages the global presence of Kaspersky to identify "good" devices and use this knowledge for user authentication. Based on global device reputation, IP-address, location parameters and more any attribute marked as involved in fraudulent activity is also proactively detected and shown as suspicious or related to fraud.

Behavioral Analysis

Looks at the user's activity during the login and session, analysing the typical navigation and time patterns, how the user acts in the personal account, what he clicks and more. This data allows profiles of normal behavior to be built and any abnormal or suspicious activity during the login and the whole session to be detected.

Behavioral Biometrics

Analyses your unique customer's interaction with their device, like mouse movements, clicks, touches, swipe speed and more to detect whether a device is being used by a legitimate user or not. This technology can also be used to detect bots and remote administration tools.

Malware Detection

Is checking if the customer's device is infected with malware covering both web and mobile channels. The technology is using several sophisticated approaches including non-signature detection and agentless availability.

*Gathered data is anonymized and is not attributed to any specific person.

Cyberfraud trends in 2019

The general trends in digital fraud remained unchanged in 2019. Scammers continued to steal funds by hijacking user accounts, were still taking advantage of loyalty programs by finding loopholes in special offers and sales, and using digital service channels to launder money.

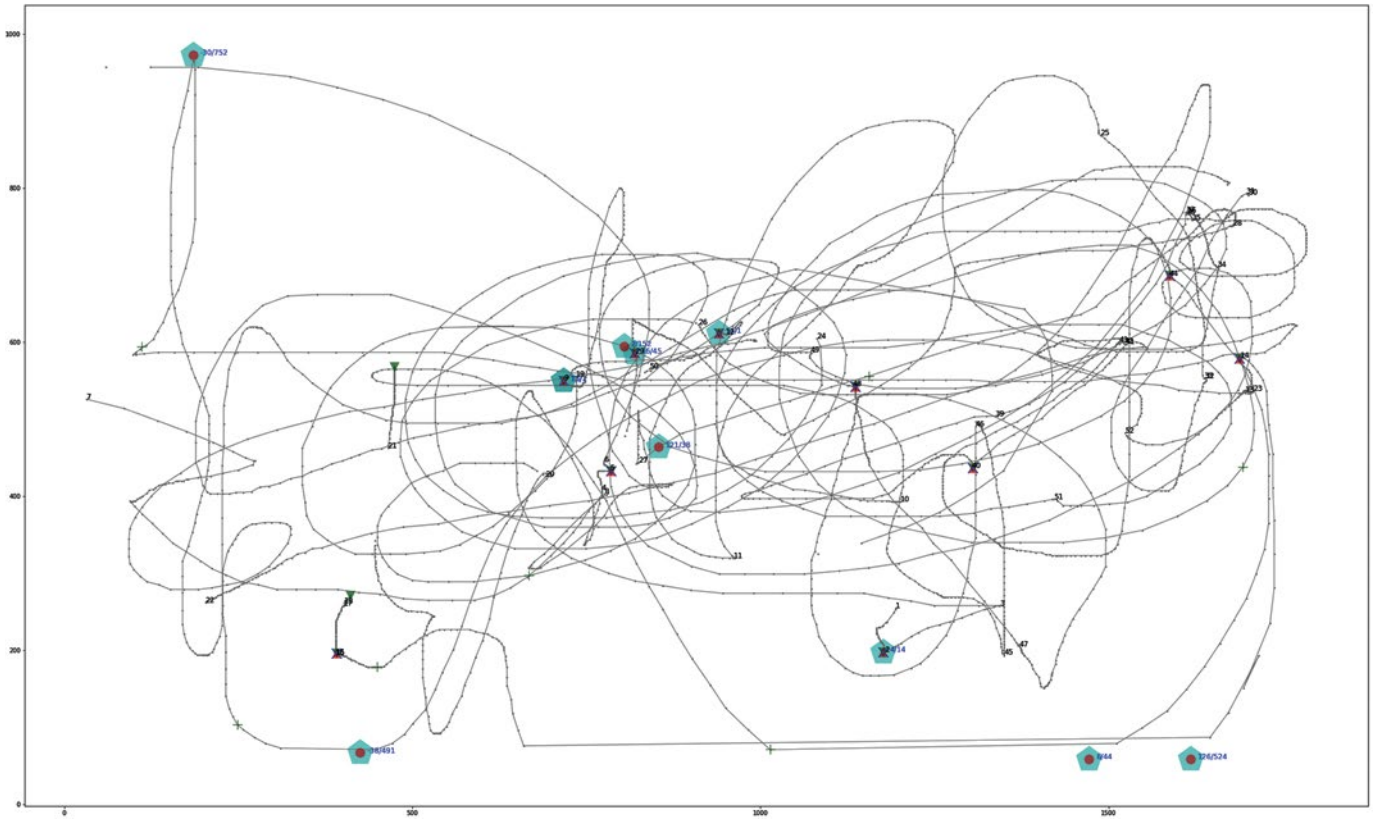
However, new trends emerged, too. This concerns, among other things, the toolkit and methods that scammers were quick to adopt. Here we'll tell you about the 'innovations' we encountered while combating digital fraud in 2019.

The Age of Humanized Bots

Cybercriminals have begun to fine-tune the behavior of bots to make them completely indistinguishable from humans. Whereas previously, computer programs were prescribed to go from point A to point B, the latest bots deviate from a straight line, shake the mouse, and demonstrate a cursor movement speed that is characteristically human. These bots can be used to buy up a large amount of tickets to sport tournaments, or to make money off of online store loyalty programs. With the emergence of human-like bots, experts are forced to find new ways to protect against the fraudulent schemes that use these bots.

The simple bots that were previously used by criminals for various fraudulent schemes and were easily caught by cybersecurity programs have now become virtually indistinguishable from humans in their digital behavior. An example of a human session is presented in the fig. 1.

1



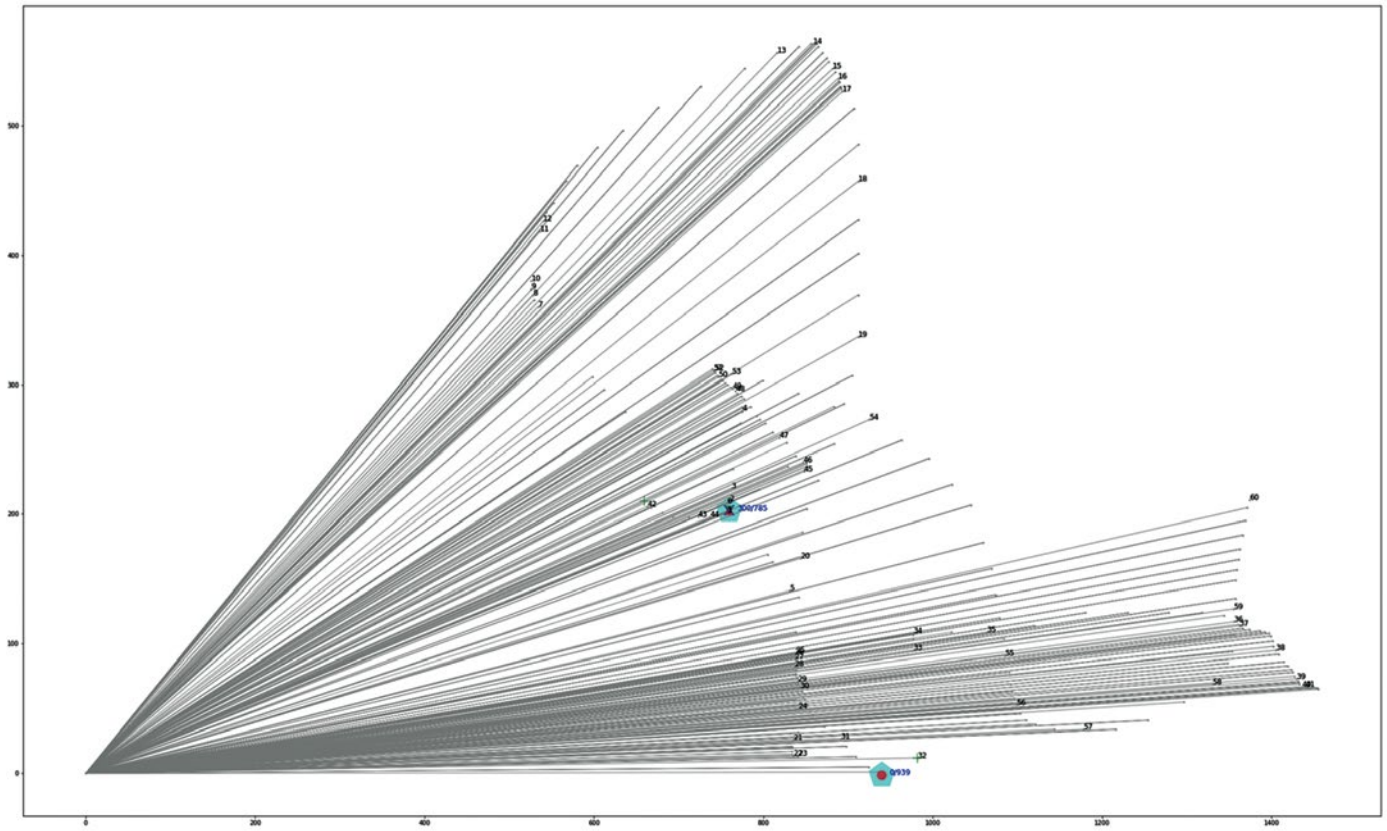
The bots that we observed five years ago, when passive biometrics had just emerged, were much more primitive than today's bots. Earlier bots simply moved from point A to point B.

Simple bot executing a predefined scenario of actions: A-> B-> C returns to its original location with the coordinates x = 0 and y = 0 between steps, just like the carriage return of a typewriter.

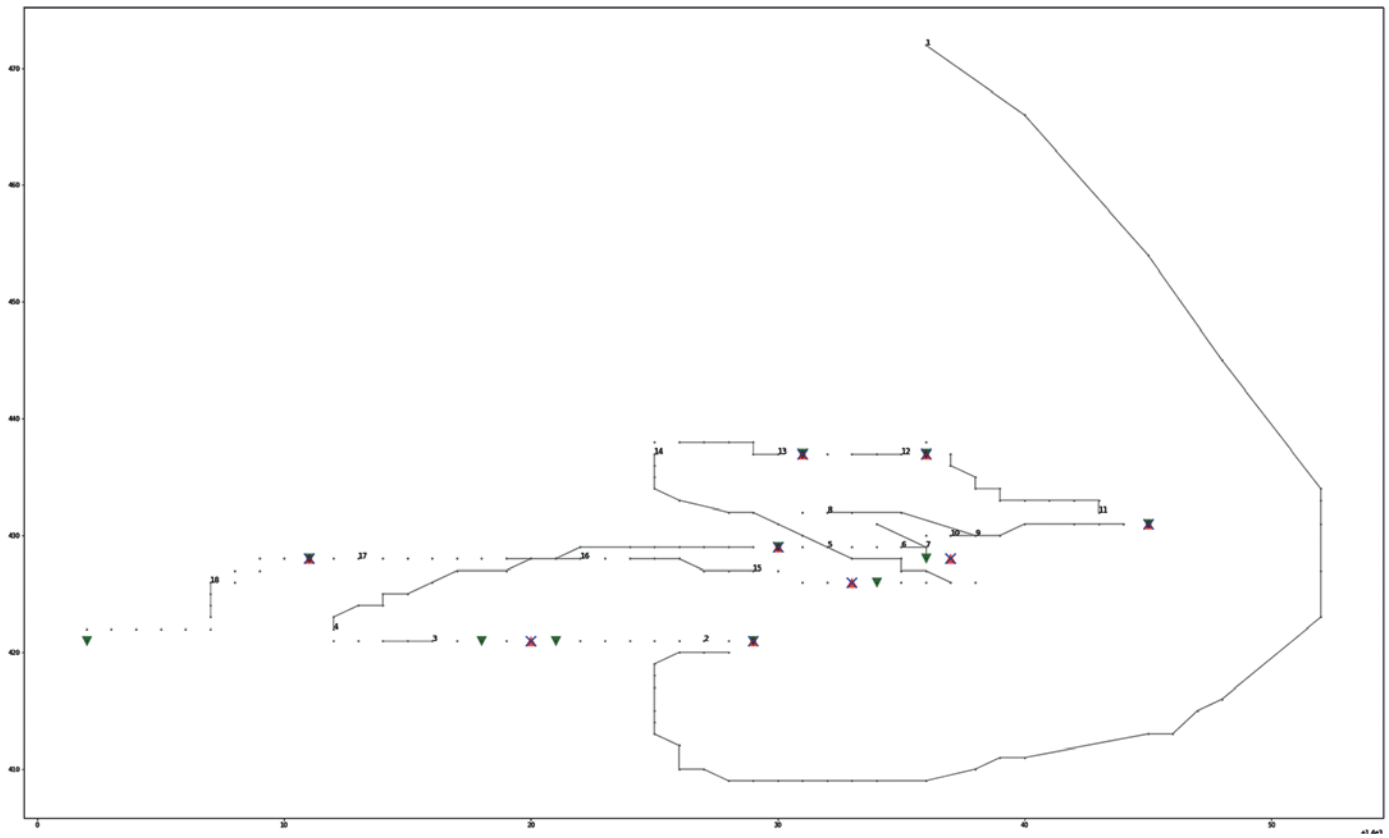
The results of this bot's activities are presented in fig. 2.

An example of a more advanced scenario is provided in fig. 3. In this case, the bot executes a predefined scenario without returning to its original location.

2



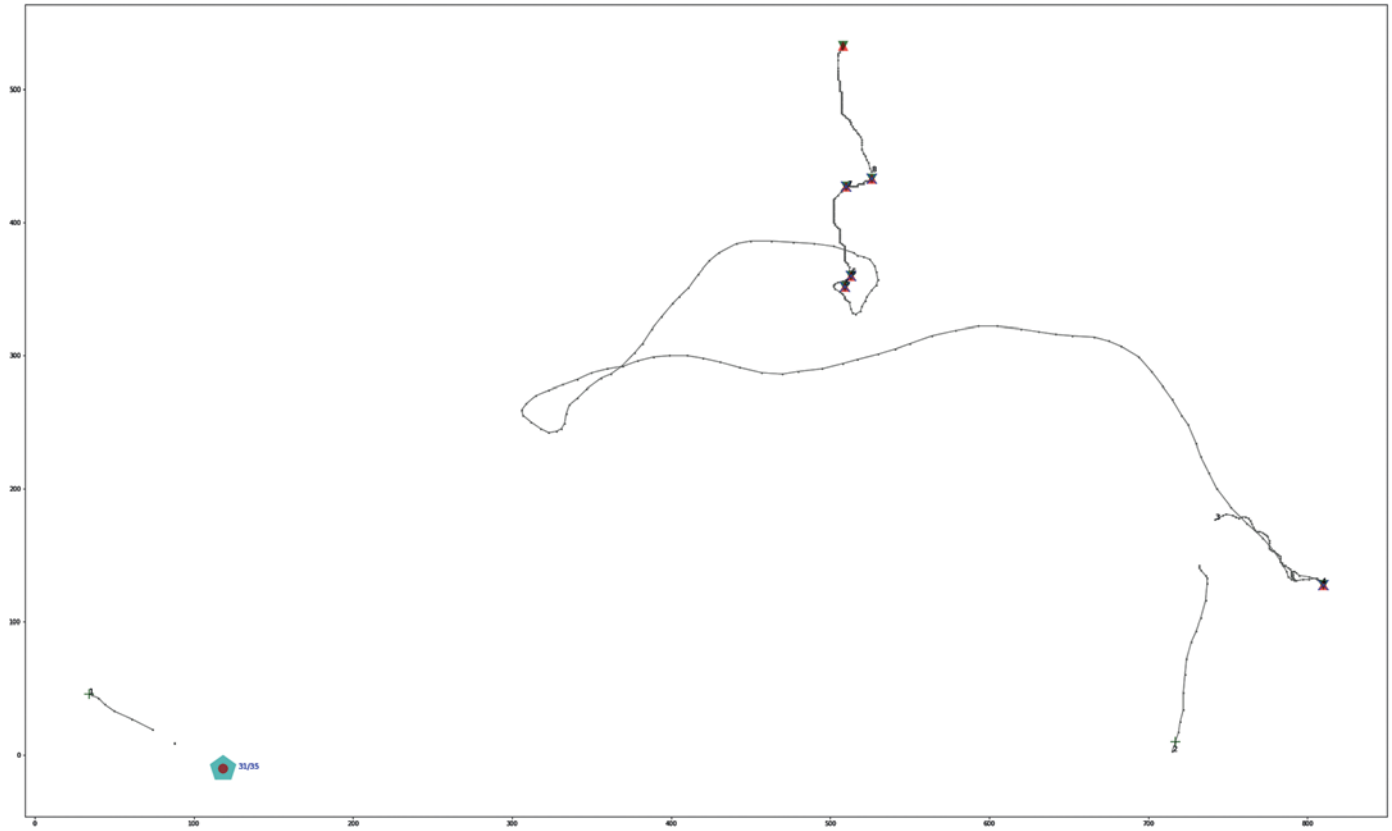
3



You can now utilize a large number of settings, such as gravitational pull on the cursor. In addition to the speed of movement, you can also specify the degree of deviation from a straight line, and slower movement at certain points. This means that criminals now have the capability to fine-tune the behavior of bots, which we all know can be used to help users as well as hurt them.

Fig. 4 depicts typical mouse behavior during a bot session, and fig. 5 shows typical behavior during a real user session.

4



5

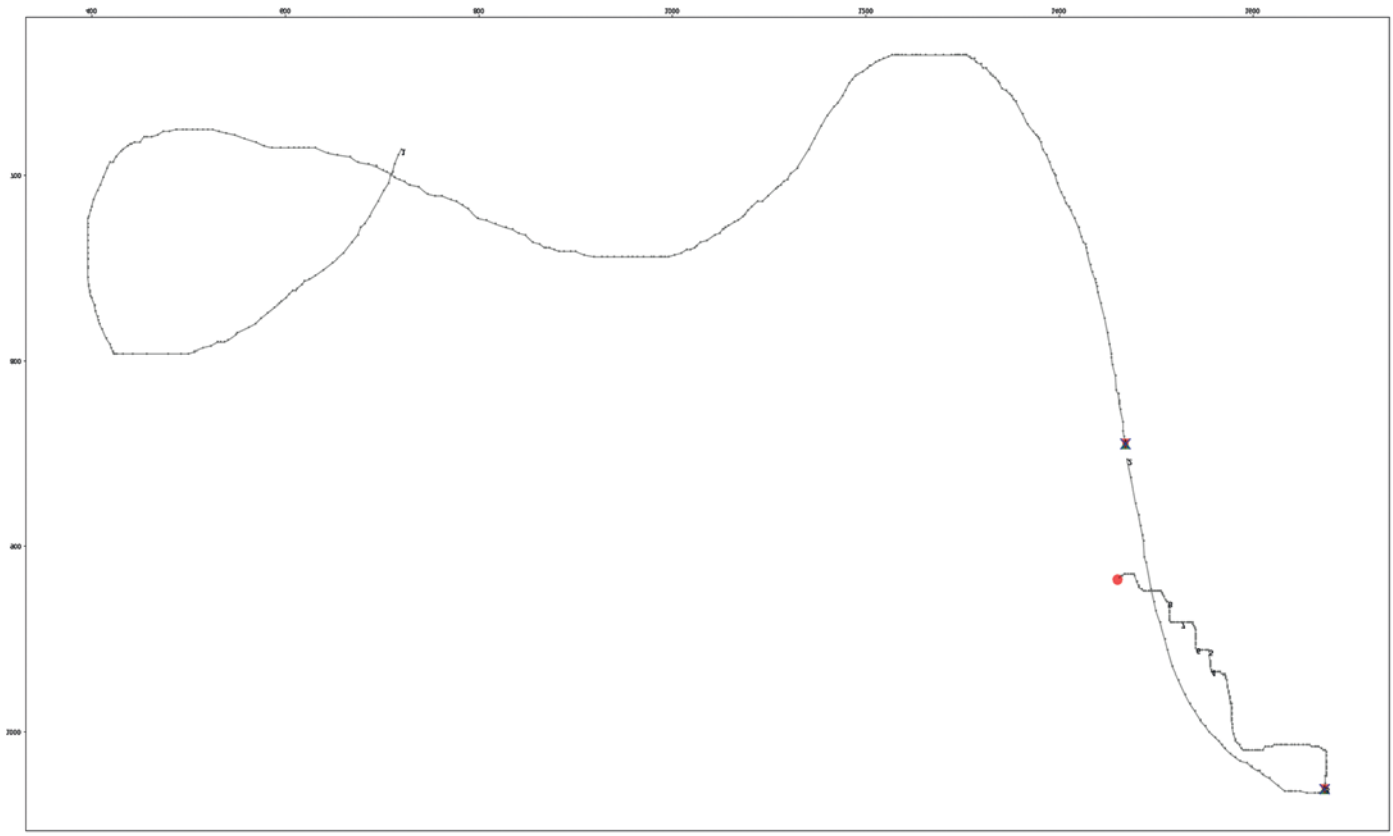
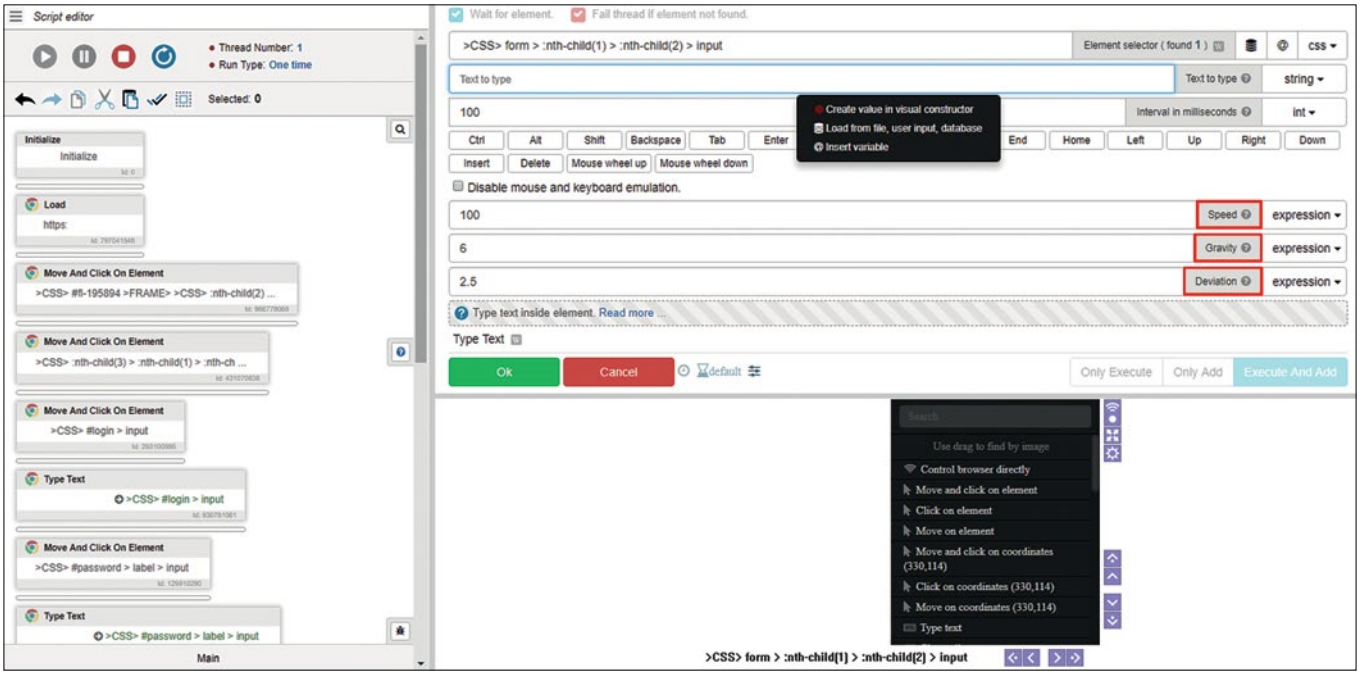


Fig. 6 represents an interface for configuring a fourth-generation bot. The Speed, Gravity and Deviation settings, used for imitating the behavior of a regular user, are framed in red.

6



The Good, the Bad and the Ugly

Many companies are attempting to use passive biometrics data for testing their applications and gadgets to predict consumer demand.

An example of such a technology would be a robot that is capable of modeling behavior of potential target customers for the business to provide better service in the future. Another type of a bot is a robotic finger that emulates human behavior with the device. It's not hard to imagine how criminals can use these tools for their goals.

Criminals have already begun taking advantage of this capability. While information security experts previously found it easy to identify bots by their instant movements and optimized trajectories, improved programs take into account the trembling of hands, the bouncing tilt of a phone and slower movement within certain segments of the computer screen.

You can use this type of human-like bot to buy up tickets to the Olympics or World Cup in order to scalp them later, obtain and use other people's miles for free air travel, or simply make a lot of money through loyalty programs offered by various online stores.

If a loyalty program accrues one thousand points for a user who brings a friend to the online store, a million bots can turn this loyalty program into an enrichment scheme. <...>

Experts provide their own protection algorithm to counteract human-like bots.

"It is impossible to imagine that a hacker could synthetically create millions of unique programs," explains Maksim Fedyushkin. "A hacker can create a hundred such devices, but it cannot create millions. For this reason, we are examining the behavior of not only an individual bot, but also a large number of users."

However, all the surveyed experts believe that optimum protection must be based on tracking and other indicators, particularly the unique attributes of the device, IP address and navigation.

The trend described above accompanies the advent of the fourth generation of bots. The first generation of bots operated on the basis of scraping tools, such as ScreamingFrog and DeepCrawl. They typically originate in data centers and use proxy IP addresses. They are easy to detect, because they cannot maintain cookies, they fail JavaScript challenges, and you can easily blacklist their associated IP addresses and UAs.

These problems were resolved by the second generation of bots, which were capable of maintaining cookies and executing JavaScript challenges. They operate through "headless" browsers (such as PhantomJS or SimpleBrowser). These bots can be identified through their browser and device characteristics. They can be blocked on the basis of their fingerprints.

Third generation bots use browsers for their activities. They are capable of emulating primitive mouse movements and keystrokes, but they cannot simulate the randomness of human interaction with a device.

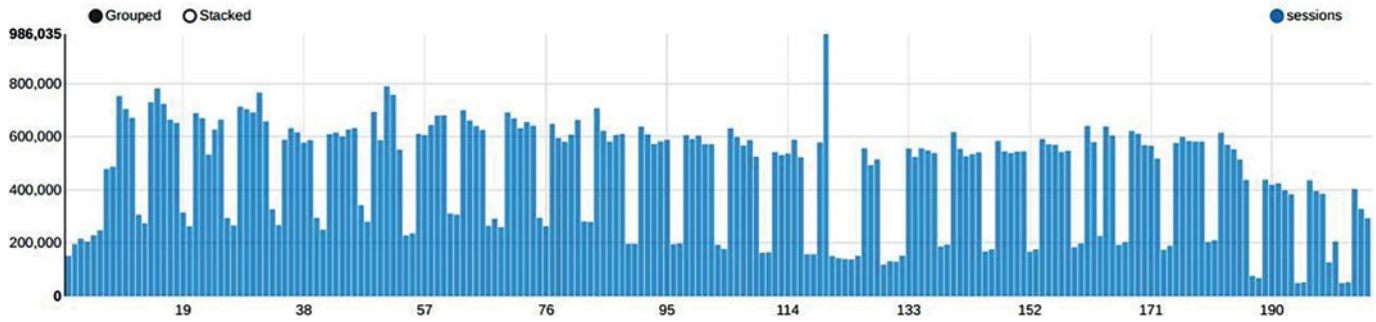
One of the ways to detect fourth-generation bots is to analyze traffic for anomalies. Identified anomalies may indicate possible attacks, such as an account takeover attempt.

Unsupervised UEBA as a method of traffic analysis to detect anomalies.

How do standard systems "see" traffic? (Fig. 7) Drawing on information obtained from sessions, users and devices, companies:

- Assess visitor traffic,
- Assess conversion,
- Assess the return on promotions and bargain sales,
- Analyze the target audience and plan to launch new programs.

7



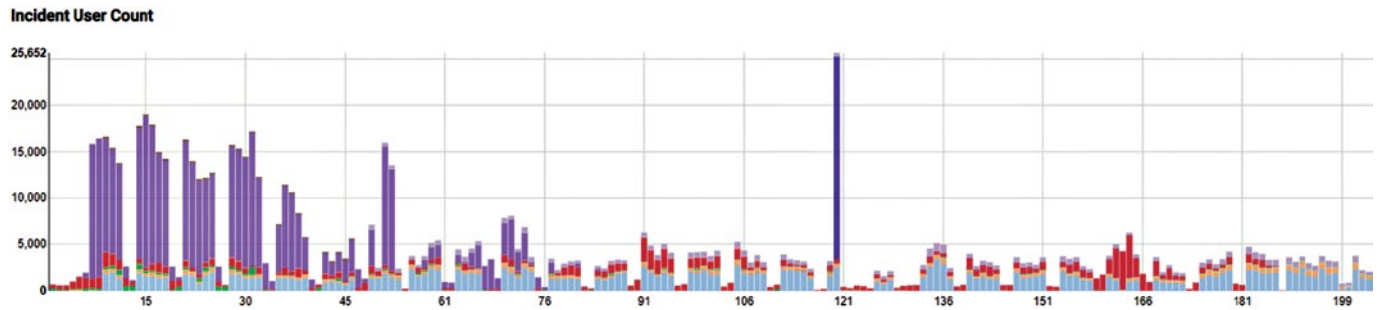
But is traffic representative of the real situation? Can we know with precision that these were real users and loyal customers?

Fig. 8 shows an analysis of this traffic for detection of synthetic behavior.

Inorganic traffic is highlighted—inorganic refers to traffic that does not originate with real users, loyal customers, or the target audience, but with scammers trying to make money off of loyalty programs.

This analysis can be conducted by examining the behavior of entities through unsupervised machine learning.

8



[3] https://kas.pr/kf4a

Future bots are expected to rely increasingly on artificial intelligence. This means that the future arms race of cybersecurity will focus on detection algorithms based on artificial intelligence—specifically, machine learning technology.

Currently, the fourth generation of bots can be effectively detected by using the approach of Kaspersky Fraud Prevention, which relies on continuous analysis of session anomalies and events, and on analysis of behavioral patterns linked to environmental and device data.

The following information can be used for analysis:

- IP address, external and local
- Screen information (resolution, window sizes)
- Firmware version
- Operating system version
- Extensions added to the browser
- Time zone
- Device ID
- Battery information
- Audio system information
- GPU information
- TCP/IP packet analysis data
- SSL/TLS traffic passive analysis data
- Cookie files
- Passive biometrics
- Navigation analysis
- Other information

Digital prints

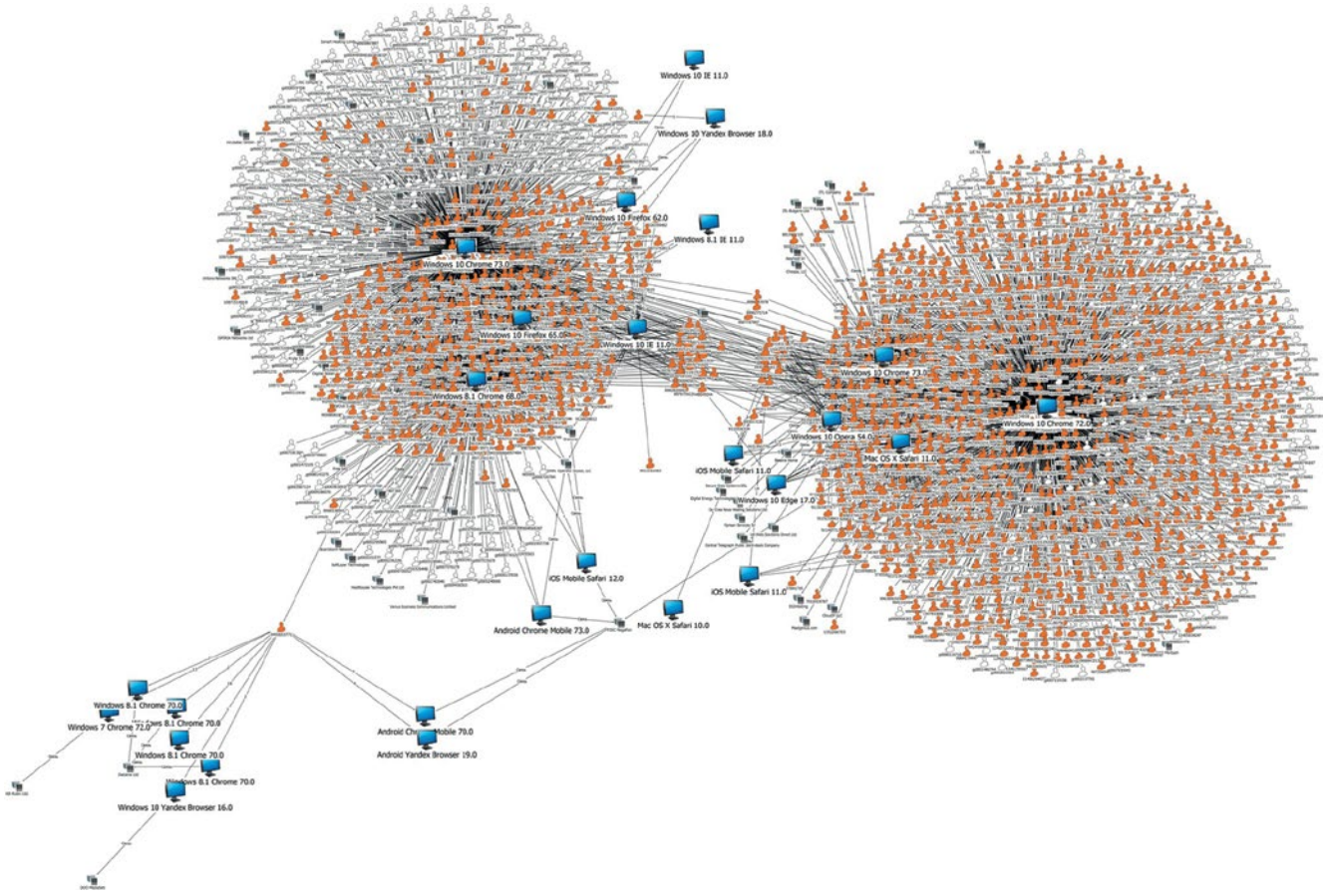
State-of-the-art antifraud systems counteract Internet fraud by maximizing the use of information about specific users and their devices. The system's goal is to identify a compromised account. To distinguish a criminal from a bona fide shopper, the system also checks the digital fingerprint of the user's device and the user's behavior. As long as no critical anomalies are identified in the resulting information, the system will not raise an alarm.

More than a hundred attributes of one device may be collected and processed for the purpose of identifying anomalies and fraud associated with a user account that is used for logging in to an online store or payment system.

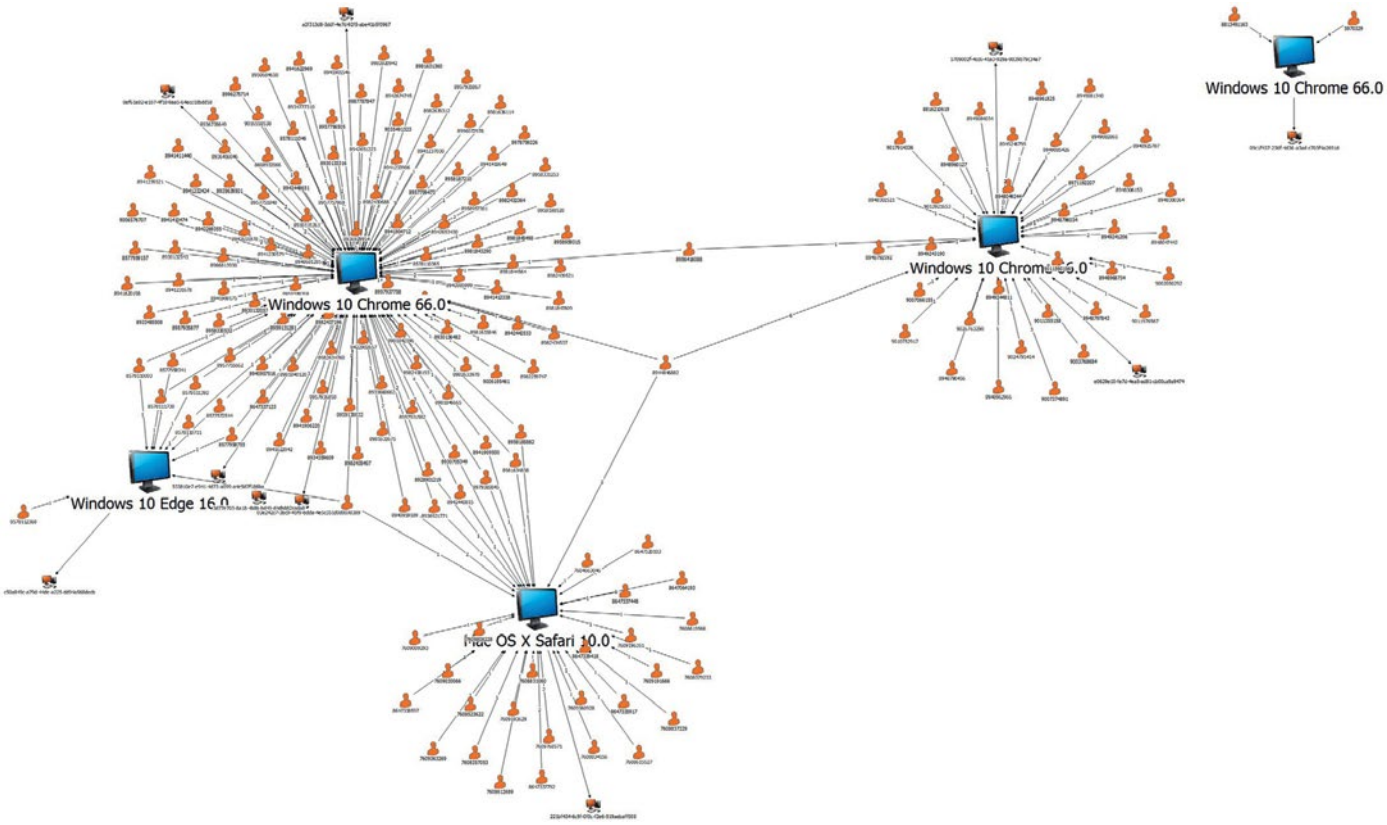
In various types of business, the use of a digital twin can lead to an increase in successful fraud cases. If a user session hijacked by a criminal appears legitimate and the user actions, such as attempting to pay for goods with a credit card, are not subject to additional verifications, the criminal will be able to steal money freely.

In the case of electronic commerce, markets providing digital twins and "configurations shops" can help criminals earn more on loyalty programs by allowing them to more easily conceal the results of their criminal activities. Fig. 9 shows a cluster identified by an antifraud system when the fraudsters were not using digital twins. Fig. 10 depicts the results of using software that provides digital twins.

9



10



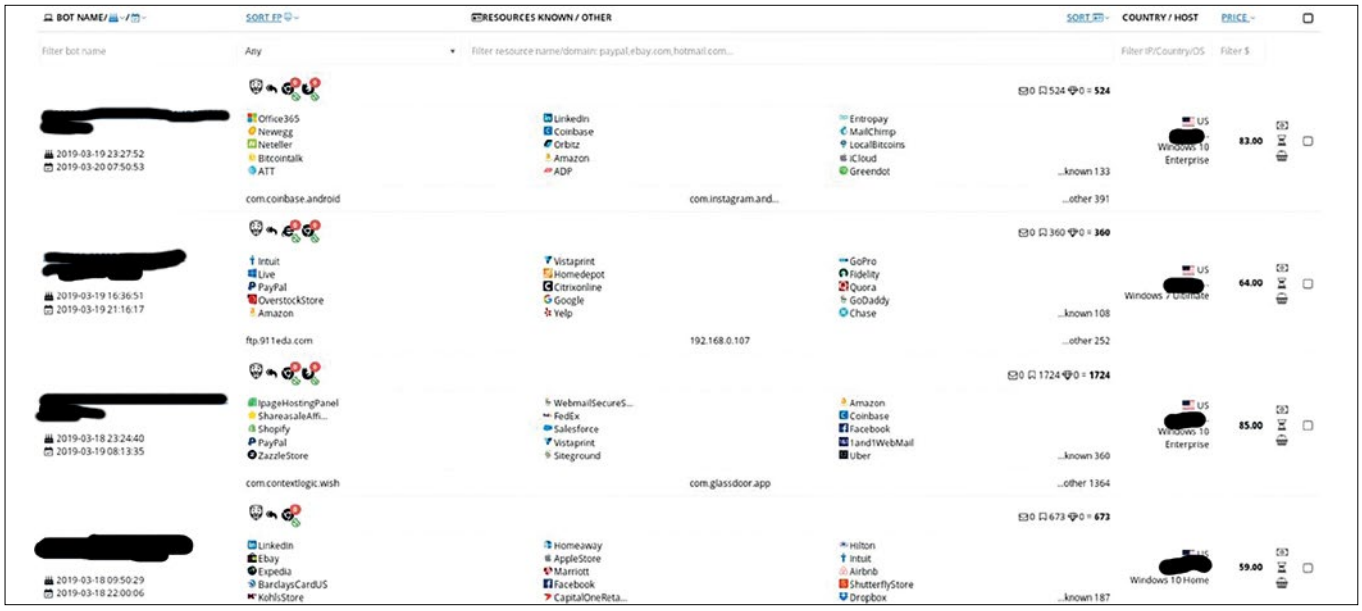
As can be seen from the above examples, the use of digital twins can help reduce the anomaly cluster.

Software that delivers digital prints

One of the most disturbing aspects of this is that one instance of a digital twin simplifies access to multiple online resources simultaneously (see the fig. 11 showing the Genesis market).

One example of a store that provides digital twins is known as Genesis.

11



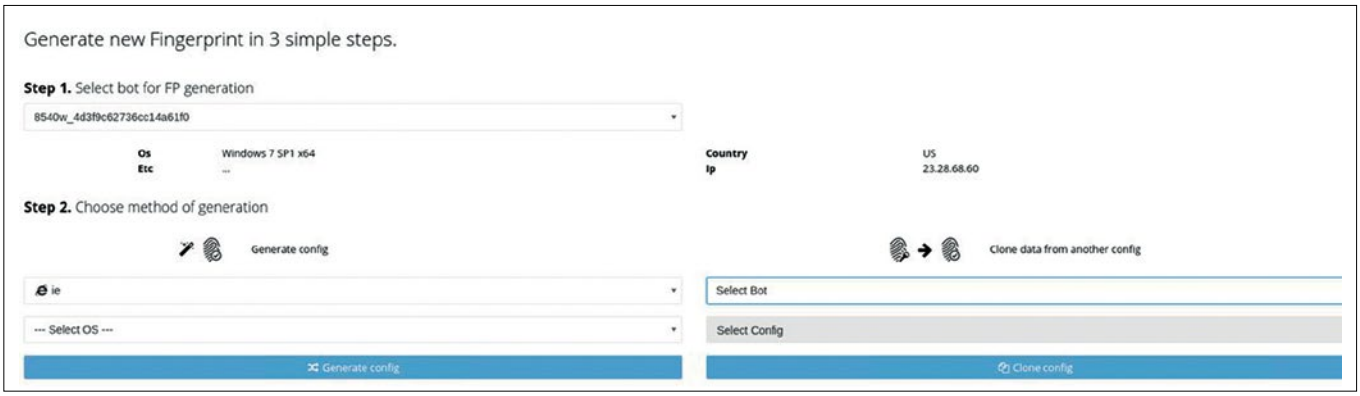
Genesis is a private online store that can be accessed only by invitation for the purpose of buying stolen digital profiles. It currently offers more than 60 thousand so-called bots for sale. A bot may include a digital fingerprint of a device (browser), user names and passwords on various websites, cookie files, and bank card details.

Experts are saying that the Genesis market, which first emerged in November of 2017, continues to serve as the key supplier of stolen digital fingerprint data. The website sells access to individual bots, meaning individual malware-infected endpoints rather than massive botnets. The company made its debut by announcing that it can get around the antifraud protection measures employed by 283 major banks and payment systems. The prices of a digital fingerprint can reach up to 200 dollars depending on the contents of the digital fingerprint data.

For convenience, they created a browser plug-in called Genesis Application, which can be used by a criminal to reconstruct the online "personality" of the data owner after purchasing a digital fingerprint.

In addition to supplying stolen digital fingerprints of real users, the Genesis service provides the capability to create new, unique fingerprints. To do so, it employs its own algorithms and plug-in to generate random digital profiles that can be used to enter the details from a stolen bank card at an online store, for example. A unique browser fingerprint will be configured in such a way that it does not appear suspicious to security systems. These types of unique fingerprints also let you circumvent session fraud monitoring solutions for the purpose of creating synthetic user accounts. Creation of a unique digital fingerprint is illustrated in the fig. 12.

12

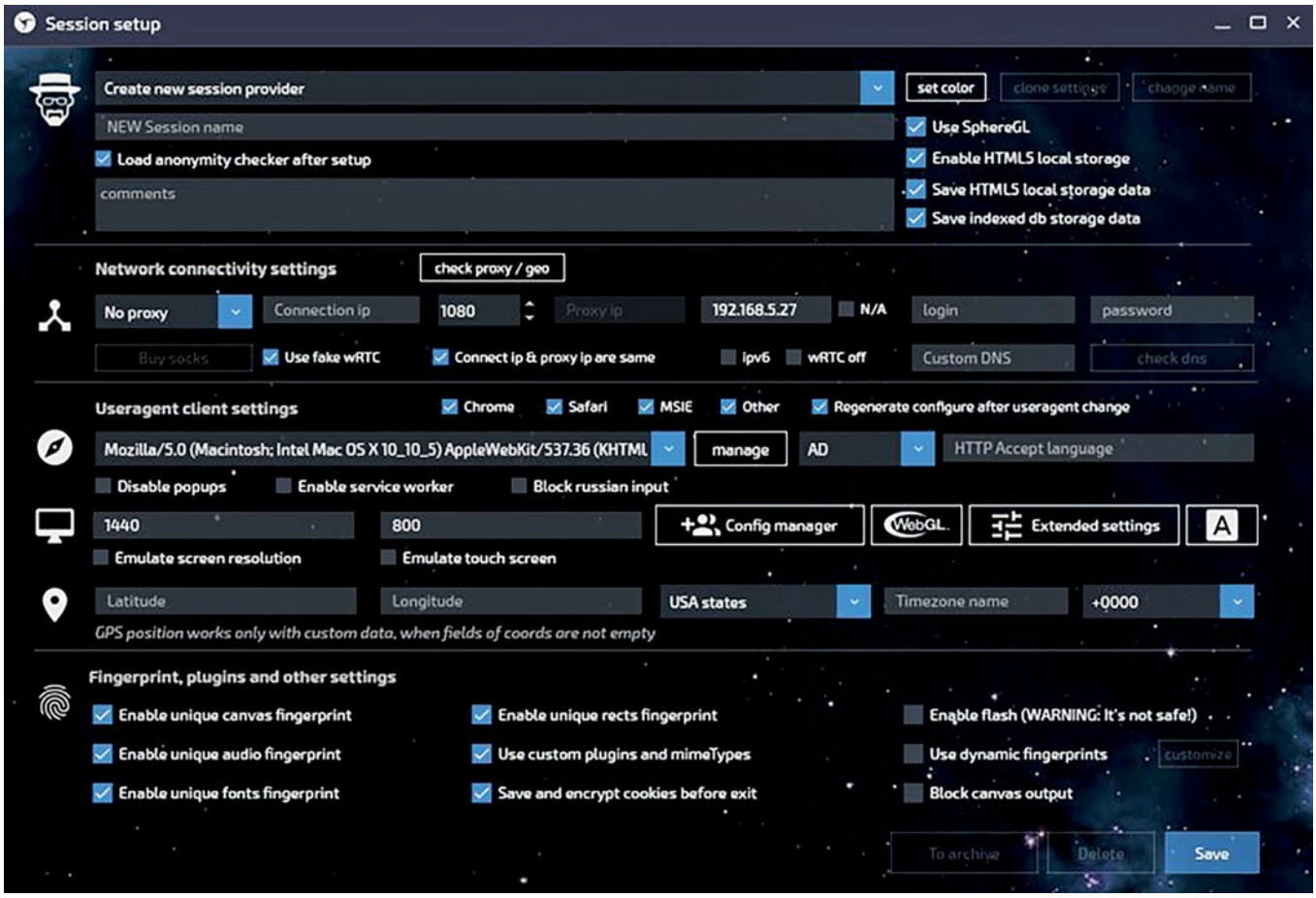


The Tenebris Linken Sphere browser is another tool that criminals use to circumvent security solutions. Its developers position the browser as a work tool for those seeking to remain anonymous, but it is really used for carding. In contrast to the Genesis plug-in, Sphere does not provide stolen digital fingerprints corresponding that match user accounts. It is a fully featured browser with extended capabilities for the creation of new digital fingerprints, automatic verification of proxy servers and other capabilities.

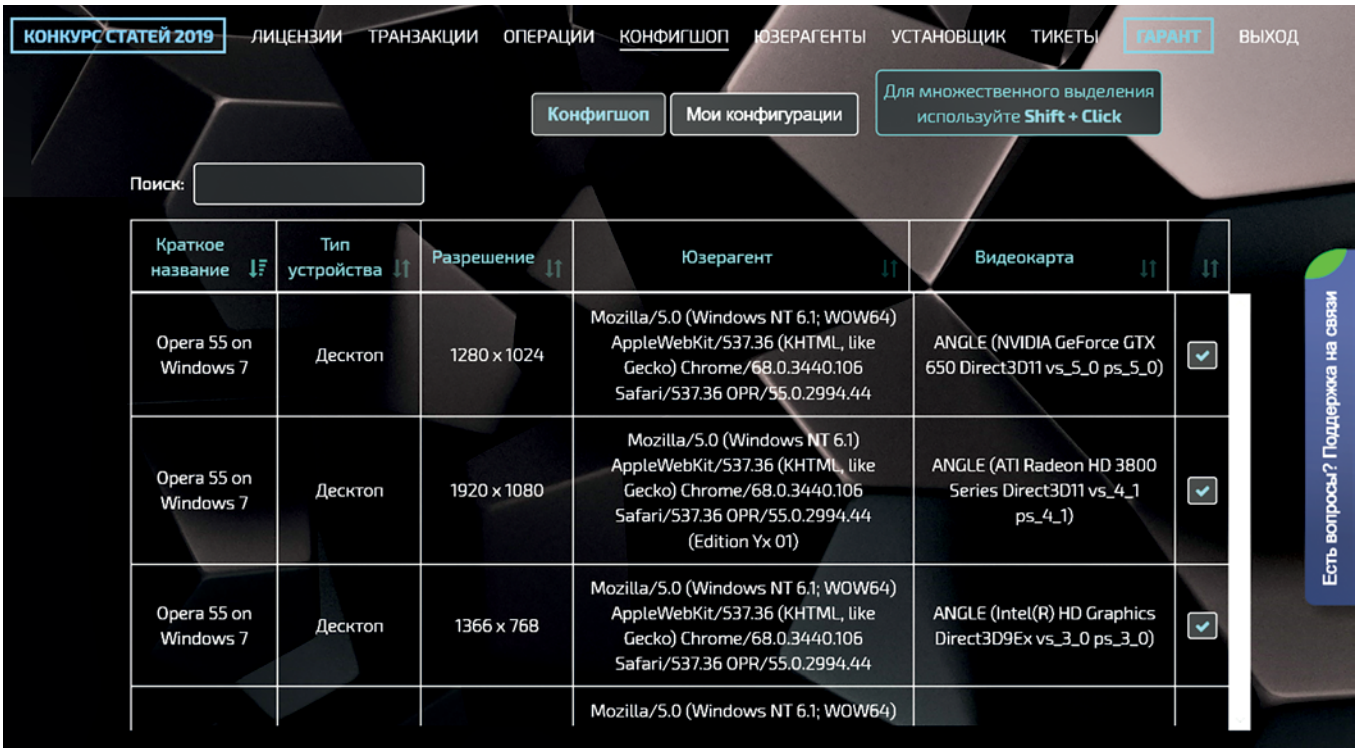
In contrast to Genesis, Sphere is a subscription-based product. A monthly subscription costs 100 US dollars, with the price increasing to 500 dollars if you also want access to a ready-to-use set of unique digital fingerprints.[4]

Configuration files online shop Linken Sphere (fig. 13 and 14)

13



14

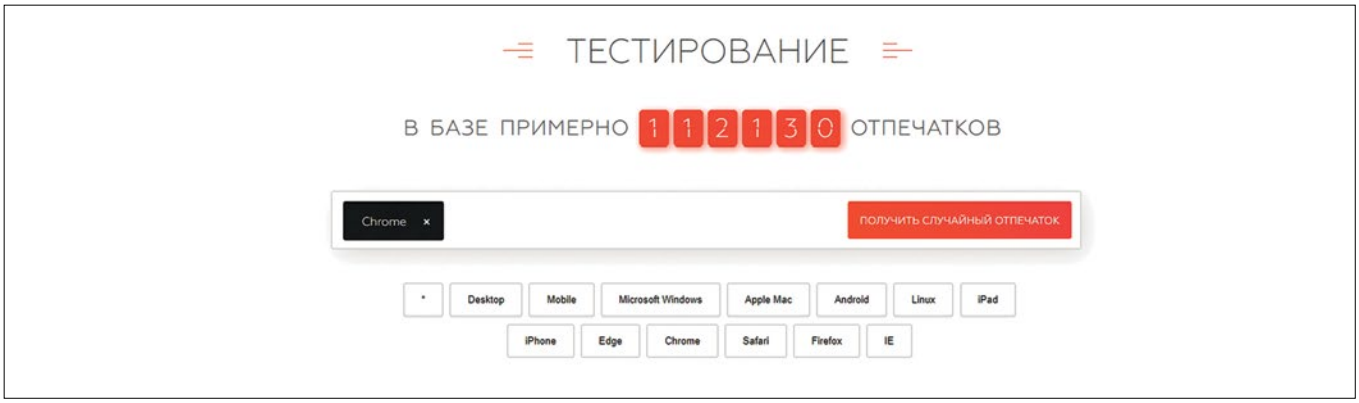


Another resource that provides digital fingerprints is FingerprintSwitcher (Fig. 15). It works in a similar way to Linken Sphere and Genesis in terms of creating a unique digital fingerprint. Its goal is the same: creating synthetic user accounts.

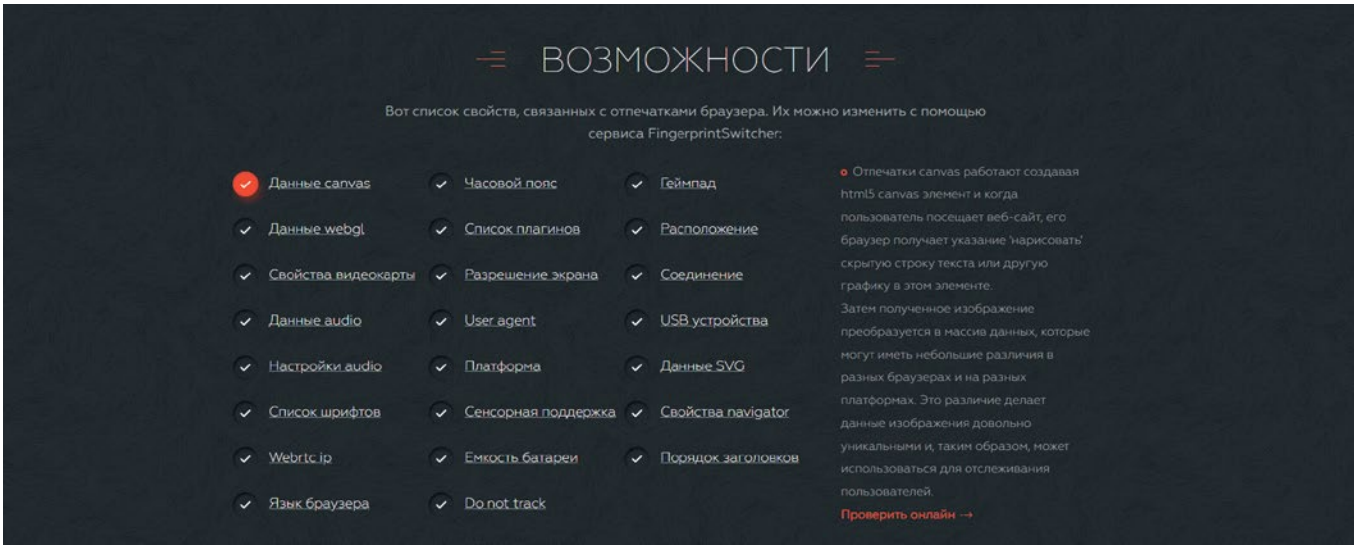
The creators of FingerprintSwitcher recommend that you verify the application of a new digital fingerprint by using the Fake Vision tool, from the providers of the Tenebris browser. The developers of FingerprintSwitcher also offer a tool called FingerprintDetector, which lets you check whether an online resource is protected by session antifraud solutions prior to launching an attack. Fig. 16 demonstrates how a random fingerprint can be obtained in FingerprintSwitcher, and Fig. 17 shows the list of properties that can be changed to modify the browser fingerprint in FingerprintDetector.

15

16



17



Summary*

Provider	Genesis	Tenebris	Bas
Solution	Genesis Application	Linken Sphere	Fingerprintswitcher
Market	USA	USA, EU	RU
Degree of completion	Complete, stable	Complete, unstable	Complete
Deliverable	Browser plug-in	Browser with the capability to configure sessions	Additional module for the hacking tool
Features	Provision of stolen fingerprints Fingerprint generator	Provision of stolen fingerprints Fingerprint generator	Provision of stolen fingerprints
Target	ATO, ML, NAF	ML, NAF	ML, NAF
Number of impressions	60 000	300	50 000
Positioning	–	Anonymization	Automation
Price	$60+ (some are $200+)	$500 for 6 months $3 for a real-world impression	$40 for 3 months

ATO: account takeover, hacking a user account

ML: money laundering

NAF: new account fraud, creating synthetic accounts for fraudulent purposes

However, 2019 can be described as a year when criminals took the next step in perfecting their tools.

Social engineering

Digital hijacking of a mobile device

One of the most popular fraud schemes in 2019 was the use of malicious apps with remote access tools. When a criminal is able to successfully execute this scheme, users willingly install the malware on their phones believing that a bank employee has called them to help cut their card servicing expenses or to warn them of an attempt to hack their account. Then, the criminal can use an Interactive Voice Response (IVR) system and ask the user to spell the user name and password to their account, and other personal data—many banks use a code-word system for user authentication by telephone. After this, the customer is prompted to install an app on their phone, which will enable the criminal to obtain remote access to the device.

After the user has installed the app on their mobile device, the cybercriminal receives access to all the capabilities of the user account. For example, they can transfer and withdraw money, change user account details, steal personal data that could be sold online for a profit, submit loan applications and many others.

* https://kas.pr/u22d

We also conducted research on the major apps used by criminals in 2019. As you can see from the table, criminals prefer such applications as AnyDesk, Team Viewer, AirDroid and AhMyth for remote management of users' devices running Android 7.1–10.0. Cases in which the user's screen can be viewed and remotely controlled are highlighted in green. Cases in which the screen can be mirrored (viewed) are highlighted in yellow. Situations in which the screen can neither be viewed nor managed are highlighted in red. The likelihood of a criminal obtaining remote access to a device is extremely high when considering that the AnyDesk & Team Viewer apps provide the capability to view the user's screen on all devices that the research covered. We analyzed the results of our research and determined that in 48% of cases, the criminal easily obtains access to the user's screen.

Brand	Model	Android OS	AnyDesk	Team Viewer
Xiaomi	Redmi 5	7,1		
Xiaomi	MIX	9,0		
Xiaomi	Redmi Go	8,1		
Xiaomi	MI9	9,0		
Xiaomi	Redmi 4	7,1		
Xiaomi	Redmi Note 5	7,1		
Xiaomi	Redmi Note 5	8,0		
Xiaomi	MIX 2S	10,0		
Xiaomi	Redmi Note 3 Pro	10,0		
Sony	XPERIA XA Dual	9,0		
Samsung	S9	9,0		
Samsung	Note 9	8,1		
Samsung	Note 9	9,0		
Samsung	Galaxy S7 Edge	10,0		
Samsung	S8	9,0		
OnePlus	7 Pro	10,0		
OnePlus	6	9,0		
LG	Nexus 5X	7,1		
LG	Nexus 5X	8,0		
Huawey	Honor X	9,0		
Google	Pixel	9,0		
Elephone	M2	8,1		
Elephone	M2	9,0		
Doogee	X9 mini	9,0		

Kaspersky Fraud Prevention identified more than 3,000 user sessions per month using remote administration tools on the network of a major bank. By employing behavior analysis and behavioral biometrics, Kaspersky Fraud Prevention can detect these types of suspicious user activities and quickly warn banks and other e-commerce and services platforms.

Gaining trust with the help of IVR (interactive voice response)

Another method that seems harmless but is, in fact, readily exploited by scammers is the creation of an IVR menu to obtain the second authentication factor. Attackers carefully select vocabulary and use a robot voice to make the request for the second factor sound as convincing as possible and avoid raising suspicions. Users often perceive interaction with a robot as safer than human interaction. Prerecorded voice messages ask the victim to enter a code received in a text message or push notification. As soon as the victim tone-dials the code, the information is transmitted to the scammers' servers, and they immediately transfer the funds to the accounts they control, as the second factor is time-sensitive.

IP/SIP caller ID spoofing

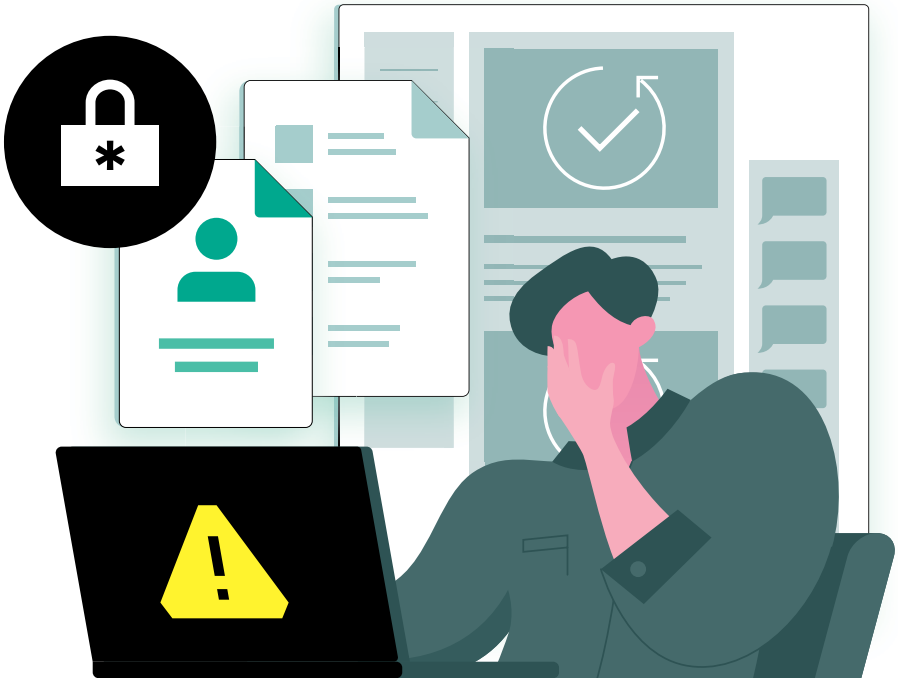
Statistically, almost every tenth Russian resident (9%) has lost a large sum of money to phone fraud.*

In addition to RAT and IVR, scammers have mastered spoofing of incoming caller numbers. They often replace only part of their numbers with digits from banks' phone numbers or display vanity numbers. Unfortunately, banking institutions have accustomed their clients to the fact that they may get calls from various numbers and callers may introduce themselves as financial agency employees. For example, these calls may come from merchant acquiring or soft collection. The practice plays into fraudsters' hands as it results in financial institutions' clients failing to perceive calls from unfamiliar numbers as suspicious or posing a threat.

* This data was obtained from a study conducted by OMI for Kaspersky in June 2019. The survey covered 1,000 Russians.

Undercover social engineering: "The rescuer" and "The Investor" scenarios

Fraudsters mainly used one of two cover stories to gain the trust of their victims in 2019: the 'rescuer' and the 'investor'.



Scenario 1 – "The rescuer"

Criminals who act as "security experts" to act out a "rescue" scenario are known as "Rescuers". They pose as security officers and call bank customers to notify them of "suspicious" debits or payments, and offer their assistance.

Rescuers offer help to a client by asking them to verify their identity by means of a code sent in a text message or a push notification. This is done under the pretext of validating the client, blocking a suspicious transaction or transferring funds to a "secure" account.

If there is a lack of trust shown for the rescuer, the fraudsters try using interactive voice response or remote connection to the device to obtain the second factor and access the victim's funds. An experienced attacker will have several readily available tools and scenarios for influencing victims, which significantly increases the likelihood of a successful attack.

Scenario 2 – "The investor"

Another popular cover story used in 2019 was that of the investor. Fraudsters pose as employees of an investment company or investment consultants from the bank. They call clients, offering the chance to make a quick buck by investing in cryptocurrency or corporate equity directly from their accounts, without having to go to a branch office. As a prerequisite for providing the "investment service", the investor asks the potential victim for the code received in a text message or push notification. The toolkit used is the same: IVR, RAT, SIP. The only difference is the source of the client database. The investor scenario is used if the potential victim has previously shown an interest in boosting their savings.

Going passwordless, or password-free realities

Aside from the fact that a password system was in use back in Ancient Rome, it has been established that 1961 was the year when CTSS (the open operating system known as the Compatible Time-Sharing System) from MIT started using the Login command for the password prompt. When entering the word "password", the system also deactivated the display of printed characters to preserve the privacy of the password being entered.

Currently, a user name and password combination is used on most digital platforms: when signing on to a computer, banking app, personal dashboard or other service.

According to a survey conducted by LogMeIn, a company specializing in password management, 59% of surveyed users use the same password for multiple user accounts*. It was also determined that users stick with the same password for a long time, or at least until the system or IT department requires them to change the password for security purposes.

In terms of security, a password is an extremely unsafe authentication method that should not be used as your only means of data protection, because it can be stolen, guessed or obtained by other means. Many companies resort to methods such as two-factor authentication, physical tokens for verification, biometrics data, facial scans and fingerprints.

While the use of passwords was previously considered logical and reasonable, today's world, with its rapidly growing number of online services, makes the use of passwords impractical, because it can be challenging to remember all of one's passwords. This is why services are striving to secure user data through the use of two-factor authentication.

Based on Kaspersky Fraud Prevention data and analysis of 400+ million sessions and 20+ million unique accounts, approximately 10% of users enter a password more than three times.

Most people use password manager software or browser autofill functions. The MacBook Pro uses active biometrics instead of a password for signing in to a user account. Even though all the authentication methods listed above provide an alternative to password security, the main problem is that the data necessary for signing in to a system is stored with the user one way or another, whether it is the user's fingerprint, token or saved password. The human element always carries the risk of an error. This is precisely why password management and memory is the doctor's true prescription against loss of personal data in today's eternally growing digital world.

Recently, Google teamed up with FIDO Alliance to declare support for the Android FIDO2 standard. The FIDO Alliance's mission is to develop and promote authentication standards that help reduce the world's excessive dependence on passwords. This means that most devices running Android 7 or later will support passwordless login methods. The Android platform previously supported FIDO login options such as mobile device fingerprint scanning. FIDO2 will make it possible to use these methods in Chrome web browsers instead of the traditional manual entry of a user name and password.

In keeping up with this trend, Kaspersky Fraud Prevention offers passwordless authentication methods that employ a PIN code or scans of biometric data from the device. The Kaspersky Fraud Prevention console lets you synchronize a trusted mobile device with a user account, which then allows you to sign in by using the biometric readers of the mobile device, such as fingerprints and facial scans, instead of entering a password. The security of this type of authentication hinges on a risk analysis for both devices (phone and computer) from which you log in to the console.

* https://www.lastpass.com/psychology-of-passwords.

[5] https://kas.pr/h6w7
[6] https://kas.pr/x45z

Mobile threats to financial institutions

A total of **69,777** installation packages for mobile banking Trojans were detected in 2019 – half as many as the year before.

Despite this, the share of banking Trojans among all mobile threats identified in 2019 grew slightly, which can be attributed to a decrease in the activity of virus writers specializing in other families and types of malware.

As before, the key propagation vectors for the threats aimed at personal data are:

- malicious mobile applications with user interfaces that mimic original banking apps and posted on Google Play;
- social engineering;
- phishing links in instant messaging apps and on the internet;
- Trojans that send themselves or other Trojans to the contacts found on an infected device.

TOP-10 largest mobile banking Trojan families by share of users attacked in 2019

Family	%
Trojan-Banker.AndroidOS Asacub	44,4
Trojan-Banker.AndroidOS Svpeng	22,4
Trojan-Banker.AndroidOS Agent	19,06
Trojan-Banker.AndroidOS Faketoken	12,02
Trojan-Banker.AndroidOS Hqwar	3,75
Trojan-Banker.AndroidOS Anubis	2,72
Trojan-Banker.AndroidOS Marcher	2,07
Trojan-Banker.AndroidOS Rotexy	1,46
Trojan-Banker.AndroidOS Gugi	1,34
Trojan-Banker.AndroidOS Regon	1,01

The year 2019 saw the first-ever example of highly automated mobile financial malware. This Trojan was named Trojan-Banker.AndroidOS.Gustuff.a. The cyberattacks it carries out involve the stealing of money by tampering with a mobile banking application. What makes this particular Trojan dangerous is that it transfers funds on its own by interfacing with the banking app.

Trojan-Banker.AndroidOS.Gustuff.a attack phases

1. Once in the system, the Trojan prompts the victim to open a legitimate banking application by displaying fake push notifications from the bank.

2. After the victim has launched and unlocked the authentic banking app, the Trojan gains full control over it.

3. In the final phase of the attack, the malware presses buttons and fills in entry forms required to transfer the funds. Amazing as it may seem, the Trojan intruder performs all these actions completely autonomously.

It is worth mentioning that these activities were made possible exclusively by the Accessibility services in Android, created by the operating system's developers to help users with disabilities. Accessibility services enable an application to actively interact with another application's interface.

Criminal gangs specializing in attacking the banking sector

FIN7

In 2018, Europol and the U.S. Department of Justice announced the arrest of the leader of the cybercrime groups known as FIN7 and Carbanak/CobaltGoblin. Although some people thought the arrest would have an impact on the activities of the groups, this has not been the case.

In fact, the number of groups operating under the aegis of CobaltGoblin and FIN7 has increased. There are several interconnected groups using very similar toolsets and the same infrastructure to conduct their cyberattacks.

The first operation in this area was the now well-known FIN7, which specializes in attacks on various companies to obtain access to their financial data or PoS infrastructure. It relies on the Griffon JScript and Cobalt/Meterpreter backdoors, or on PowerShell Empire in later attacks.

CobaltGoblin / Carbanak / EmpireMonkey. It uses the same toolset and methods, and a similar infrastructure, but it is designed only for financial institutions and their associated providers of software and services.

The last one is a recently detected group known as CopyPaste, which targets financial organizations and companies in one African country. This suggests that the group is associated with cybermercenary or a research center. The links between CopyPaste and FIN7 are still very weak. The operators in this cluster of activity might have been influenced by publications containing open source code and may actually have no connection to FIN7.

All these groups take full advantage of non-patented systems in corporate environments and continue to use effective series of phishing attacks in combination with well-known Microsoft Office exploits created by the operating environment. So far, the groups have still not used any zero-day exploits. Phishing documents used by FIN7/Cobalt may seem very basic, but when combined with the groups' extensive social engineering and targeted actions, they proved to be quite successful.

FIN7 went dormant in the middle of 2019, but it returned at the end of the year with new attacks and new tools. We suspect that the hibernation was caused by their infrastructure being shut down after their bulletproof hosting company in Eastern Europe was closed.

In contrast to FIN7, the activities of Cobalt Goblin Group continued steadily throughout the year, which once again proves that these groups operate independently even though they are linked. Their toolsets and TTP (tactics, techniques and procedures) are very similar, but they operate on their own. We only occasionally detect matches in their infrastructure. At the same time, the intensity of attacks is a little lower than it was in 2018. The tactics of Cobalt Goblin are unchanged. They still use documents containing exploits that first download a small installer, then, the Cobalt beacon. The group's main targets are also the same as before: small banks in various countries. It is possible that the lower number of attacks that we detected was due to diversification. Certain indicators suggest that the group may also be involved in JS sniffing (MageCarting) to obtain payment card data directly from websites.

JS sniffing was extremely popular all year, and we detected that thousands of e-commerce websites were infected with these scripts. The implemented scenarios work in various ways, and criminals utilize highly diverse infrastructures. This means that this type of fraud is used by at least a dozen cybercriminal groups.

A group known as Silence aggressively expanded its operations in various countries over the course of 2019. We detected attacks in regions where they were never seen before. For example, we registered attacks in Southeast Asia and Latin America. This means that they either expanded their operations on their own, or began to collaborate with other regional cybercriminal groups. However, when we examine the evolution of their main backdoor, we find that their technologies have remained nearly unchanged over the past two years.

Cases of fraud detected by Kaspersky Fraud Prevention

One of the most widespread cases of social engineering detected by Kaspersky Fraud Prevention in Latin America is the reissue of SIM cards.

SIM card fraud

This type of fraud is possible because the physical presence of the user is not required for receiving a SIM card, and there are kiosks that can be used to get a card reissued with ease. This way, criminals have the capability for large-scale interception of the second authentication factor of bank customers. Once they have access to the online service, they can transfer funds from the user's personal account to their own.

We detected that some processes used by mobile carriers are not robust and leave customers exposed to SIM card spoofing attacks. For example, confirmation of your identity on certain markets may involve the carrier asking for certain basic information such as your full name, birth date, amount of your last account refill, your last five dialed numbers, etc. Criminals may find some of that information on social networks or by using applications like TrueCaller to obtain the name of a caller based on the phone number. They can also use social engineering to attempt to guess the refill amount based on what is most popular on the local market. What about the last five calls? One method used by criminals is to employ several "missed calls" or to send text messages to the victim's phone number as bait for the victim to call them back.

Sometimes the real target is the telecom provider instead of the customer. This happens when carrier employees working in small-town offices are unable to identify a fake or counterfeit document, especially in branches located in kiosks or shopping centers, which enables a criminal to easily activate a new SIM card. Insiders within companies are also a big problem. Some cybercriminals recruit corrupt employees by paying them between 10 and 15 dollars per activated SIM card. The worst of attacks occur when a criminal sends a phishing email for the purpose of stealing account credentials for the carrier's system. Ironically, most of these systems do not use two-factor authentication. Sometimes, the goal of these emails is to install malicious software within the carrier's network. All a criminal needs is one authorization document, even from a branch in a small town, to obtain access to the carrier's system.

This scheme has become so popular that many criminals have begun to offer it as a service on fraud message boards and web portals. The price of reissuing a SIM card depends on the provider and the status of the person who orders this service. Below are the results of research conducted on one of these message boards, including the average price of a hacked SIM card. The price of one hacked SIM card does not exceed $40 on the average, and opens up access to many other online services that the customer can utilize. Considering that most criminals look for easy prey, this is a relatively simple and profitable scheme.

Provider A	Provider B	Provider C	Provider D	Provider E
$10	$15	$20	$25	$40

Kaspersky Fraud Prevention is able to detect cases of reissued SIM cards in the user accounts of remote banking services in advance by using machine learning technologies or by analyzing the device and environment, clustering devices and IP addresses for a specific user, and employing device fingerprint technology.

Top 10 countries with the highest percentage of users attacked by financial malware. China and Belarus are in the lead (**2.3%**), followed by Venezuela (**2.2%**) and South Korea (**2.1%**).

Country*	%**
China	2,30
Belarus	2,30
Venezuela	2,20
South Korea	2,10
Serbia	1,80
Greece	1,70
Cameroon	1,60
Indonesia	1,50
Pakistan	1,50
Russia	1,40

* The rating does not include countries where there are only small numbers of users of Kaspersky security products (less than 10,000).
** Percentage of unique users who experience attacks from the total users of Kaspersky security solutions within the specific country.

Exploitation of urban infrastructure

Public Internet access was previously only found in airports, hotels, and major coffeehouse chains. Nowadays, people can connect to public Wi-Fi networks in city parks, buses and even in the subway. This is advantageous for criminals because of readily available IP addresses.

It is also important to mention services that offer one-time virtual numbers. Users can pay about two cents for a number they can use to receive a verification text message.

This is an extremely popular tool for criminals, because they can avoid disclosing their own phone numbers to connect to a public Wi-Fi access point (*onlinesim.ru).

Kaspersky Fraud Prevention detected a case in which a criminal exploited the city infrastructure—in this case, the Wi-Fi network in the metro—to conceal their actions. However, the Kaspersky Fraud Prevention analyzer was able to detect the suspicious activity within the device and the IP address range. On the average, approximately 150 users per day logged in from the device and they all took similar actions: they logged in to an online store and left products in their checkout basket, thereby obtaining a promo code as a result.

18

The table below shows the number of unique users and their sessions per day associated with the specified anomaly:

Date	User Count	Session Count	ISP
2019-06-09	35	38	Metropolitan branch of OJSC MegaFon AS25159 31.173.80.0/21
2019-06-12	165	166	Metropolitan branch of OJSC MegaFon AS25159 31.173.80.0/22
2019-06-13	325	329	Metropolitan branch of OJSC MegaFon AS25159 31.173.80.0/23
2019-06-14	113	113	Metropolitan branch of OJSC MegaFon AS25159 31.173.80.0/24

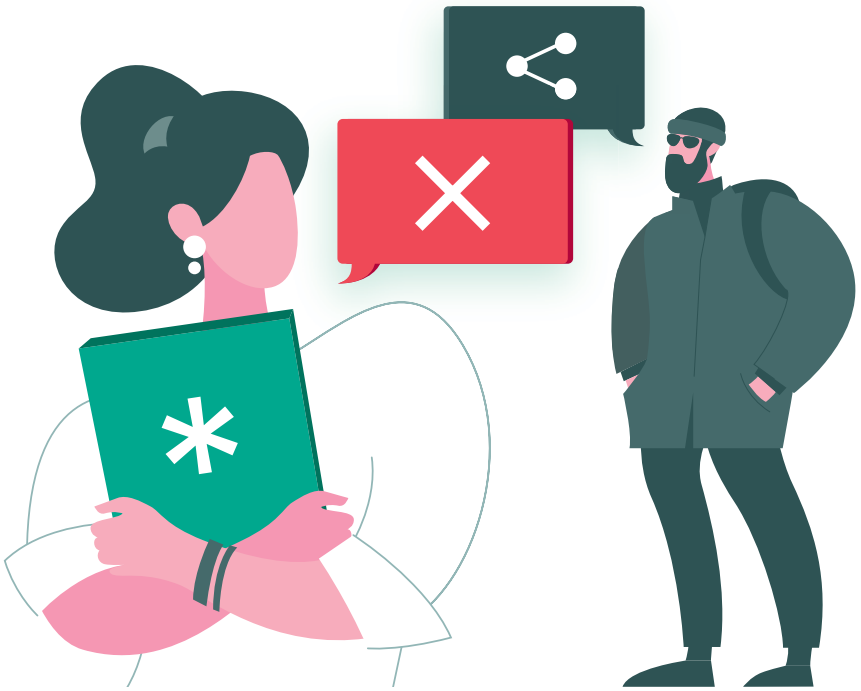
Loyalty programs and bonus points: a boon for cybercriminals

In 2019, a group of analysts for Kaspersky Fraud Prevention detected a substantial increase in the amount of fraud relating to loyalty programs and bonus points, which was especially focused on the resale of goods on other websites, and on cyberfraud schemes employing social engineering methods.

"Welcome fraud"

One of the most striking cases of cross-organizational cyberfraud exposed this year was the discovery of a network of 3,029 fraudulent accounts. The main goal of the criminals was to receive bonus points by creating a large number of accounts on an online portal. The criminals bought codes for replenishing their accounts in a gaming store and then sold them online on social networks and marketplaces. We noticed that all of the criminals performed their operations manually, and our research detected 14 devices showing mass login attempts (10 to 65 unique users). During our research, user accounts and devices were combined for the purpose of analyzing user activity, and we detected an enormous cluster of 11,256 unique users.

Another fraud technique is related to the abuse of welcome bonuses in loyalty programs. The scheme is straightforward: scammers register accounts with a marketplace en masse, receive their welcome bonus points and get goods at a reduced price. One such abuser bought up nappies and candy, subsequently selling them on classified ad websites at a profit. The accounts were later abandoned, their average lifespan being just one or two days.

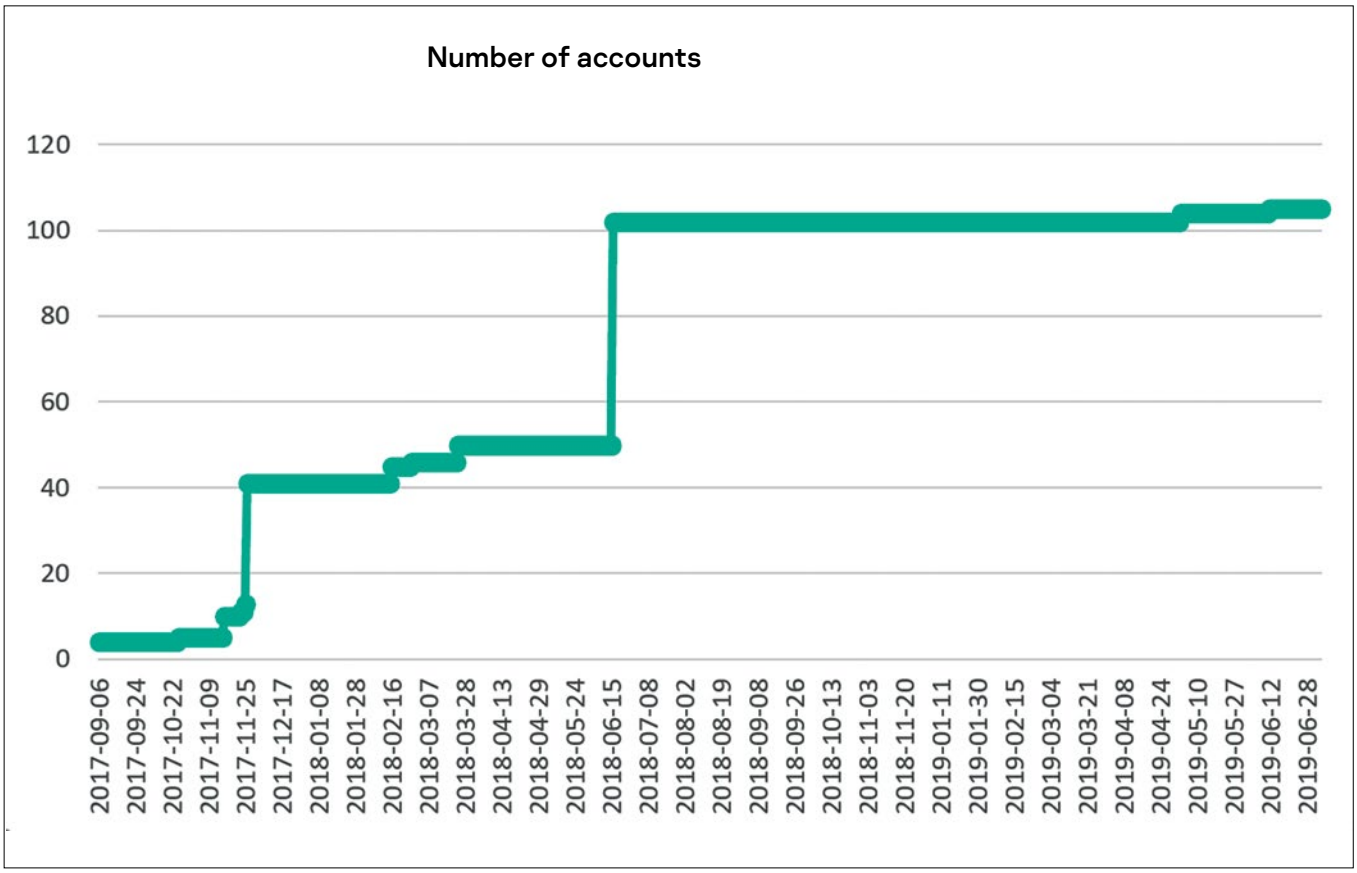


Manual fraud

In a major e-commerce store, Kaspersky Fraud Prevention detected an increase in the number of users operating from the same device. First, there were only four user accounts registered from the device, and then more and more new accounts brought that number to 14 and eventually, to more than 100.

Fig. 19 shows an evolution chart for a period of eighteen months.

19

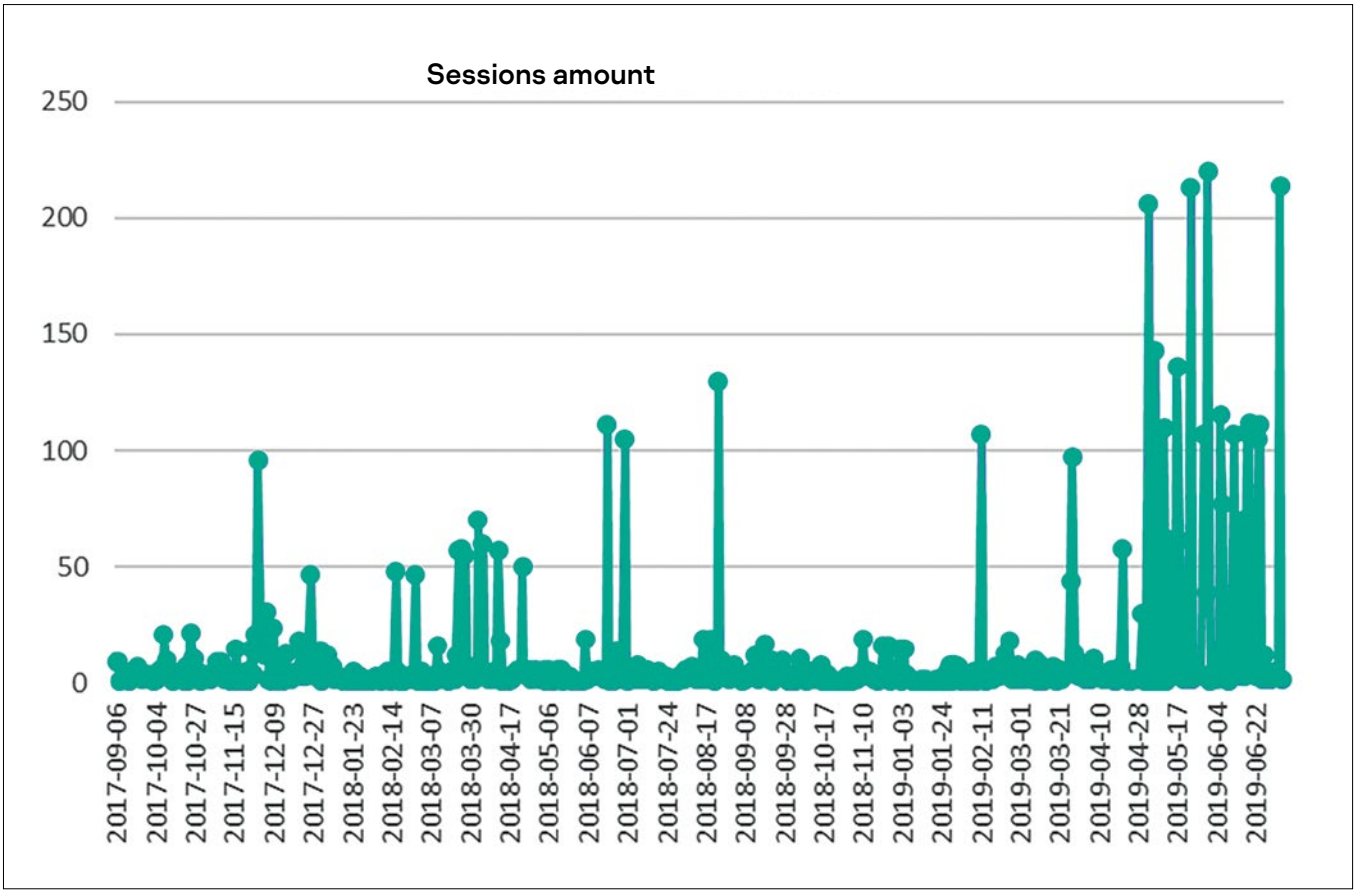


The identified group of accounts had similar marketplace activity patterns. Two accounts were mainly utilized for monitoring special offers and sales. This can be seen from user session activity indicators for this set of accounts – see Fig. 20.

The movement models during a session were extremely similar for all users. The end goal of the cybercriminals was to exploit the advantages of the bonus system. For example, a cybercriminal filled his checkout basket with goods that he was supposedly interested in buying but never actually purchased, and just waited for a discount promo code to appear in his mailbox. It turned out that the criminals were planning to redistribute the products and advertising codes online to gain income.

In the context of online commerce, we must also mention our analysis of sessions for abnormal occurrences that may not always indicate fraud at first glance. This data is useful not only from an online service security standpoint, but also in terms of business performance. Information about the behavior of users and about anomalous activity helps increase the performance bargain sales, promotions and loyalty programs.

20



Credential Stuffing

Credential stuffing is a type of cyberattack where the attacker uses stolen credentials for gaining access to user accounts via a series of automatic login attempts on a website.*

Regular account checks are becoming usual for digital service channels. In 2019, Kaspersky Fraud Prevention regularly detected attacks that took advantage of stolen account credentials. The scope of a typical account check is not that large, several thousand per attack, but in some cases tens of thousands of accounts were checked.

The attackers pursue several goals: validating accounts for subsequent resale; harvesting further information about the account owner, such as a phone number, address, etc., to enrich their database; inflicting financial damage through increased costs for second factor authentication text messages; and finally, causing denial of service through a large number of requests coming from a botnet.

Companies that face threats like this should use tried-and-true DDoS safeguards, and reset passwords for compromised accounts, as well as use risk-based authentication to prevent this type of attack and preserve funds.

* https://kas.pr/xq8d

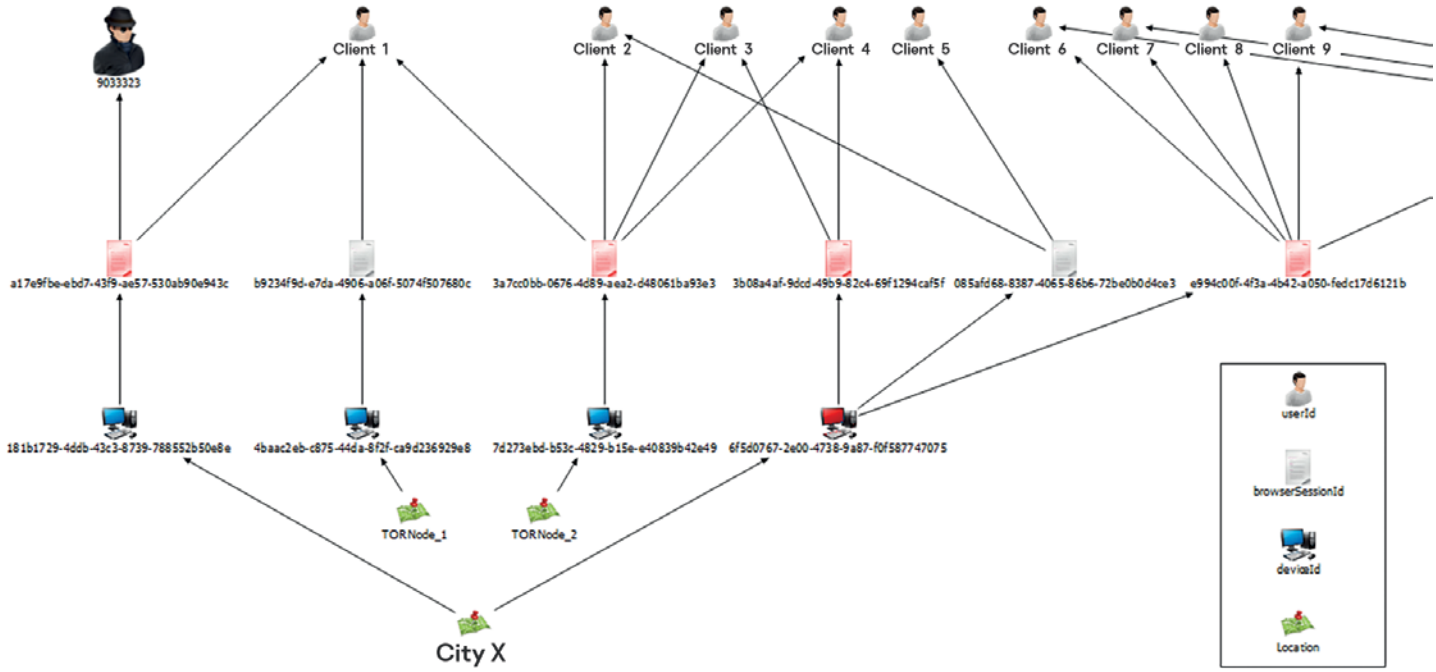
Money laundering and fraud in the financial sector

Money laundering is yet another urgent problem associated with the provision of financial services as well as cryptocurrency and exchanges. For complicated money laundering schemes that normally include the placement of illegally obtained funds, layered distribution and integration or withdrawal of funds, criminals use automation tools, proxy servers, remote administration tools, and TOR browsers to cover up their tracks and remain anonymous. Our team has come to the conclusion that the growth in money laundering attempts in 2019 is related to the complications of account takeovers and the availability of cyberfraud tools on the Internet, along with the number of personal user data leaks by companies and the distribution of that data on the Internet. Money laundering attempts increased by **181.5%** in 2019.

Fig. 21 contains only part of a chart that illustrates the core algorithm of the fraudulent scheme's 'launch' phase:

- Detected drop accounts are colored black. What is important here is separating the attacker's account from the victim's. The drop account or presumed attacker can be identified by using session antifraud solutions or by analyzing transactions initiated by the account.
- Once a drop account has been identified, the capabilities and technology offered by the session antifraud solution must be put to use. Key elements that helped to identify interlinked drop net users by using session antifraud data are colored red in the chart.

21

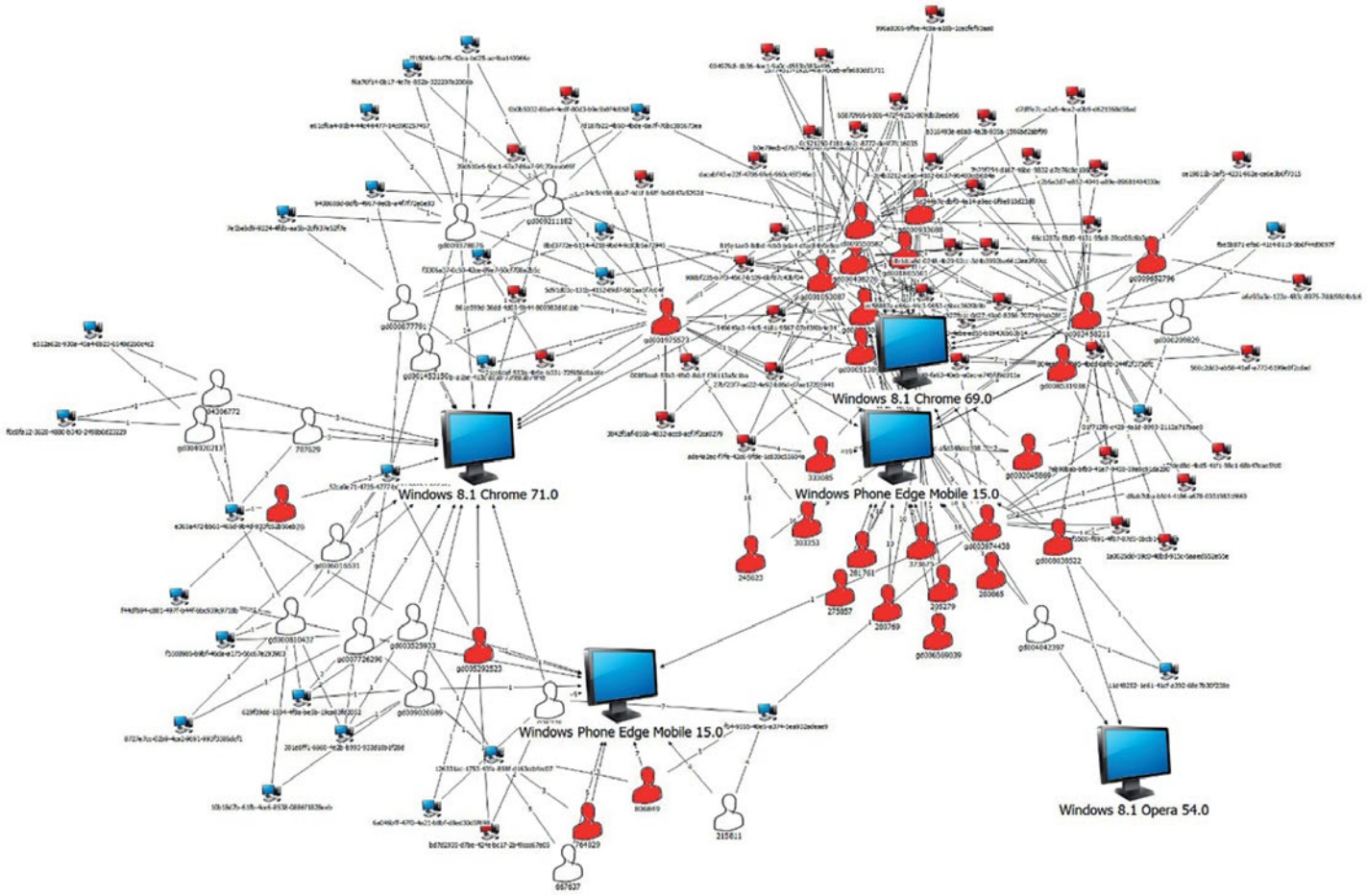


Why fighting fraud is necessary?

It is now perfectly clear that monitoring user activity and identifying correlations between devices and consumers is essential if fraudulent activities are to be prevented, the integrity of bonus points preserved and loyalty programs kept secure.

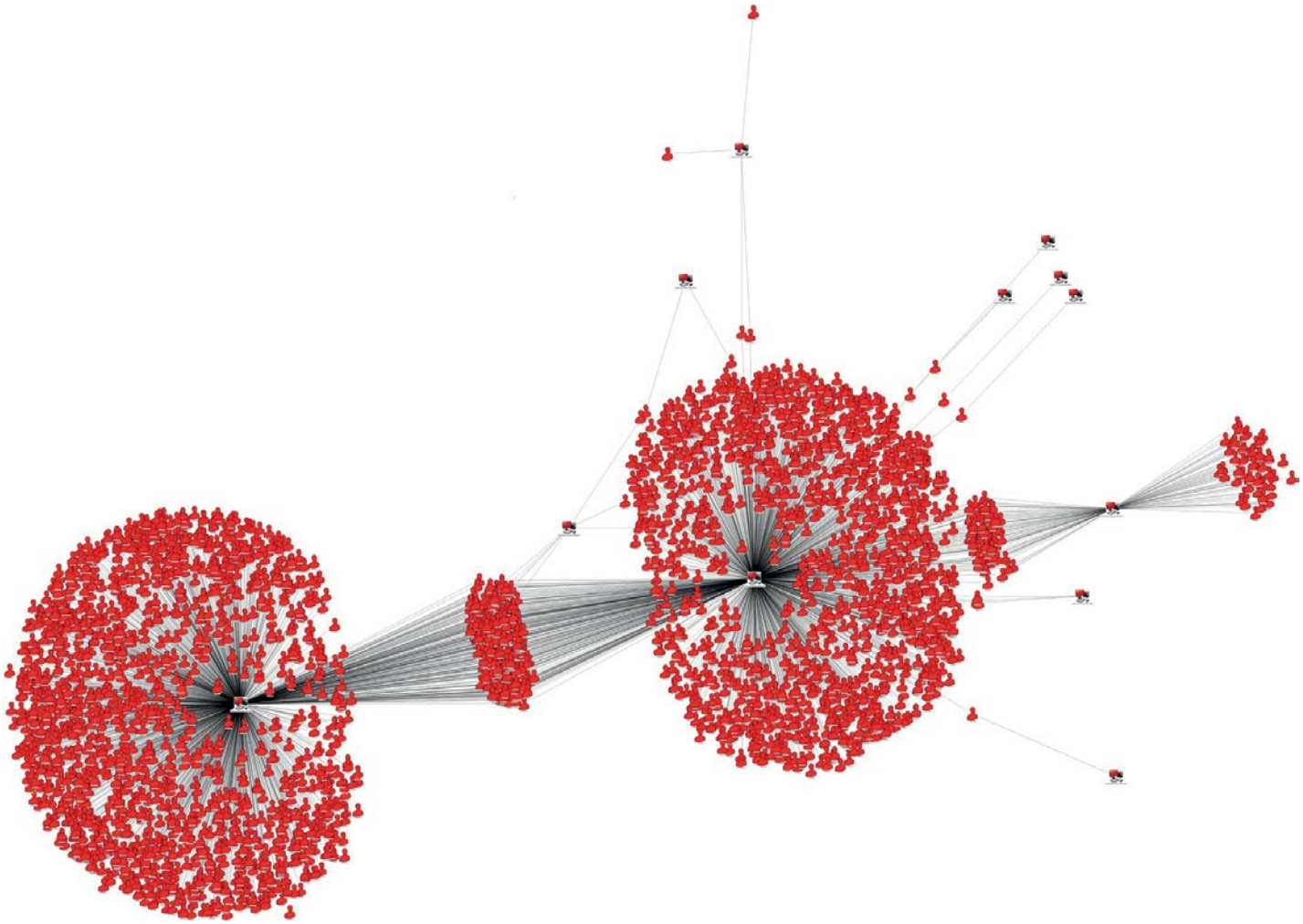
But just how important is it to undertake fraud prevention measures? We will look at cases where the customer has the Kaspersky Fraud Prevention solution installed and the results of its operation are used for countering fraud. To do this, we can look at the typical fraud cluster for this client – see fig. 22. No more than 10 fraudulent accounts can be seen for the anomaly cluster.

22



As a second example, we can use a case where the client is not using a session antifraud solution – see fig. 23. As can be seen from the diagram, the fraud clusters are much bigger in size. A network of three devices contains 2,650 users, whereas a network of 10 devices can support up to 65,000 users. The cybercriminal network, detected by the Kaspersky Fraud Prevention session antifraud solution (see fig. 22), was created in 2018 and underwent large-scale expansion that resulted in thousands of synthetic user accounts.

23



A forecast for 2020 based on cyberfraud trends

Fraud as a service

Fraud-as-a-service will further evolve both vertically (an increase in the number of identical service providers) and horizontally (a growing variety of services); markets for digital fingerprints will grow; software (anonymizers and bots) used by attackers will become more advanced; social engineering will remain the main fraud tool, utilizing caller ID spoofing, IVR, and RAT. In e-commerce, fraudsters will continue to look for design errors in loyalty programs with the aim of identifying weak spots that allow them to get rich. E-government will continue to be affected by identity and personal data theft, and illegitimate requests for services.

Resale of access to a bank account

Over the course of 2019, we witnessed cases in which groups specializing in targeted attacks on financial institutions appeared in their victims' networks only after intrusions by other groups specializing in the sale of RDP/VNC access, such as FXMSP and TA505. These observations are also confirmed by underground message boards and chat monitoring.

In 2020, we expect increased activity from groups that specialize in the sale of network access in Africa, Asia and Eastern Europe. Their main targets are small banks and financial organizations that were recently acquired by major players and are in the process of reconfiguring their cybersecurity systems to the standards of their parent companies.

Ransomware attacks banks

This forecast logically follows from the previous one. As was already mentioned above, small financial institutions frequently fall prey to opportunistic cybercriminals. If these cybercriminals are not able to resell access, or even if it becomes less likely that they will be able to withdraw money, extortion is the most logical way to monetize such access. Banks are the type of organizations that are more likely to pay ransom than tolerate data leaks, so we expect that the number of targeted extortion attacks will continue to grow in 2020.

Another vector of extortion attacks on small and medium-sized financial institutions will be the "pay for installation" scheme. Traditional botnets are gradually morphing into the more popular delivery mechanisms used against these financial institutions.

The year 2020: the return of custom tools

Anti-virus products that are able to effectively detect open-source tools used for manual testing purposes, and the implementation of the latest cybersecurity technologies will force cybercriminals in 2020 to return to custom tools, and to invest in new Trojans and exploits.

Global expansion of mobile banking Trojans: a result of data leaks

Our research and monitoring of underground message boards suggest that the source code of certain popular mobile banking Trojans are now publicly accessible. Considering the popularity of these types of Trojans, we expect a replay of the source code for the ZeuS and SpyEye Trojans leaking. The number of attempts to attack users will grow exponentially, and the coverage of attacks will expand to nearly every country in the world.

Investment applications on the rise: new target for criminals

Mobile investment apps are becoming more and more popular among users throughout the world. This trend will not go unnoticed by cybercriminals in 2020. Considering the popularity of certain FinTech companies and stock exchanges, for real money as well as for virtual money, cybercriminals will understand that not all of these companies are ready to combat large-scale cyberattacks. This is because some apps still lack even the most basic protection for customers' accounts, nor do they provide two-factor authentication for identity confirmation or assigned certificates for protecting interoperation between apps. The governments of some countries are deregulating this area, and new players are emerging every day and becoming popular very fast. We have actually seen attempts by cybercriminals to replace the interfaces of these apps with their own malicious versions.

Magecarting 3.0: even more cybercriminal groups and attacks on cloud services

Over the past couple of years, JS skimming has gained enormous popularity among criminals. Unfortunately, cybercriminals now have vast opportunities for attacks, including vulnerable e-commerce websites and extremely cheap JS skimming tools that can be purchased on various message boards for as little as 200 dollars. Currently, we can distinguish a minimum of ten different perpetrators of these types of attacks. We believe that their number will increase over the course of next year. The most dangerous attacks will be launched against organizations that provide services such as e-commerce, which will cause thousands of companies to be compromised.

Political instability leading to the spread of cybercrime in specific regions

Certain countries are experiencing political and social upheaval, which is causing massive numbers of people to seek refugee status in other countries. These waves of immigrants include very diverse groups of people including cybercriminals. This will lead to a spread of otherwise geographically localized attacks in countries that were previously unaffected.

A new attack vector may emerge with the implementation of banking regulatory rules in the European Union. The Payment Services Directive (PSD2) imposes regulatory requirements on companies that provide payment services. The new norms are also affecting FinTech companies, which traditionally were not associated with the banking community.

The security of online payments and mobile payments is the key focus of the laws. On the other hand, banks will have to deal with a requirement to open their infrastructure and data to third-parties wanting to provide services to their customers. These conditions make it very likely that cybercriminals will attempt to exploit these mechanisms by devising new fraudulent schemes.[7]

[7] https://kas.pr/h227

GBD-4136/Q1'20 V1_RU