KASPERSKY lab

Kaspersky®
Fraud Prevention

Kaspersky Fraud Prevention

Principle fraud risks for the digital businesses

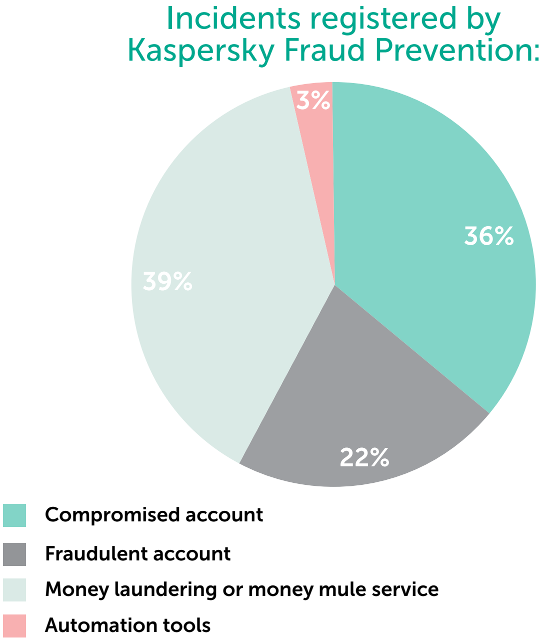
www.kaspersky.com/fraudprevention
#truecybersecurity

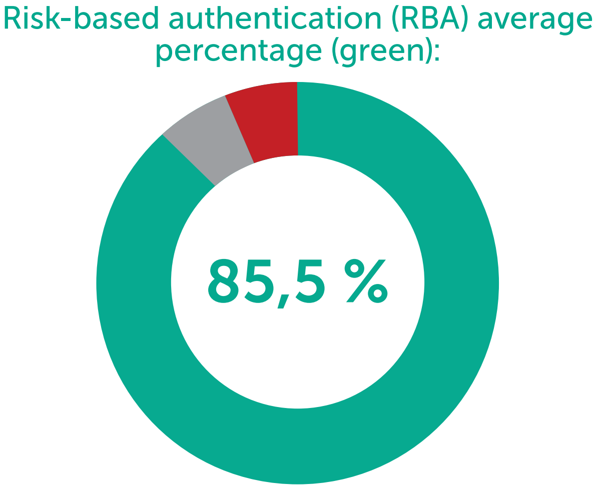
Contents

1 General statistics for Kaspersky Fraud Prevention

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

Metric	Number of unique units per day
Device (browser)	**~503k**
User	**~487k**
Online session	**~873k**
Processed event	**~34.1M**





2 Principle fraud risks for remote service accounts

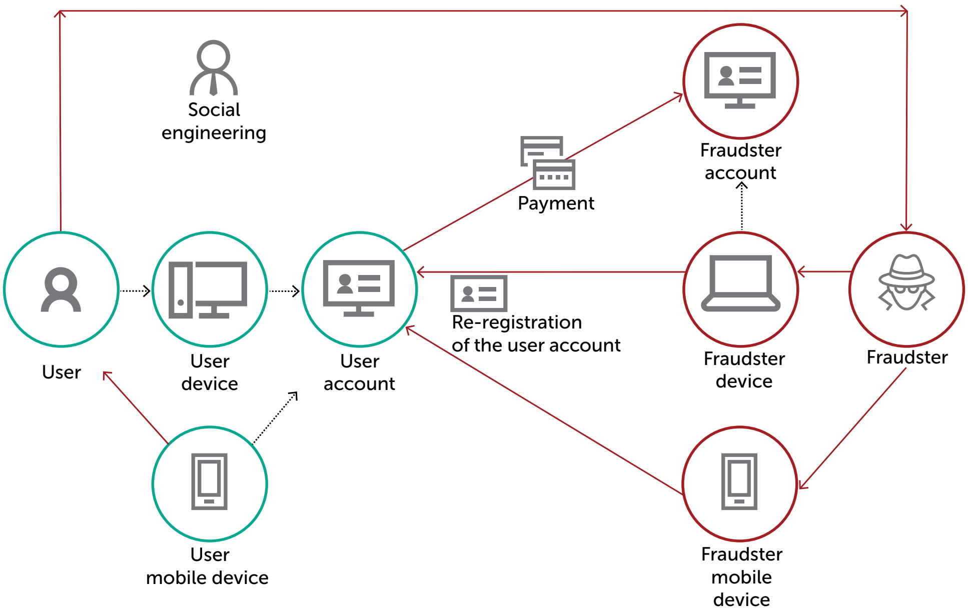
Threats to remote banking accounts

2.1.1 Compromise of remote personal banking accounts

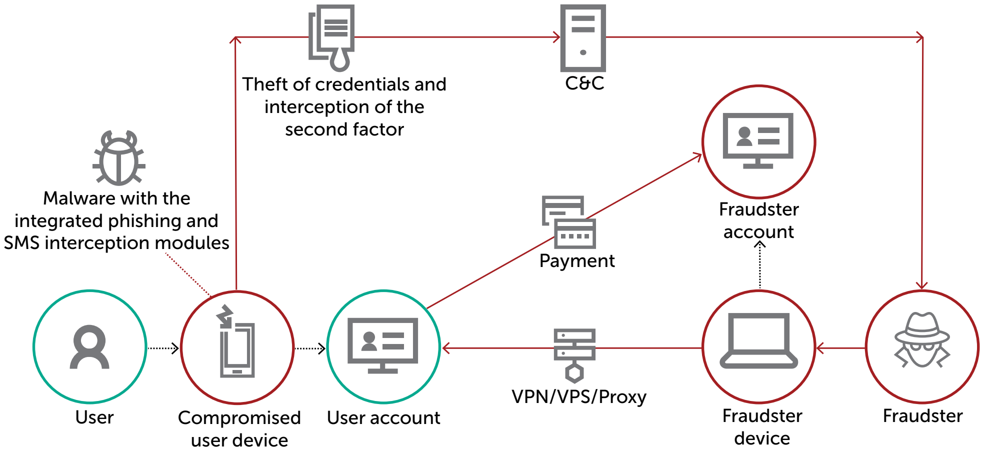
The compromising of remote personal banking accounts remains one of the biggest cyberfraud threats. The main attack scenario also remains unchanged:

- Use of standard methods such as phishing, Trojan stealers, social engineering, etc. to compromise the login-password pair to access remote banking accounts.
- Re-registration of the remote banking account, for example, using a bank card number.
- Deception, theft or interception of the second factor (SMS or push notifications) used to complete remote banking login/re-registration and subsequent operations with the account.
- Theft from the victim’s account – money transferred to the fraudsters using bank accounts, payment systems, electronic wallets, cellular operators.

The main way to steal credentials and/or the second factor notification is social engineering:



Social engineering is not the only method, however; malicious software can also be used on mobile devices to steal credentials and intercept messages containing one-time passwords (OTP):

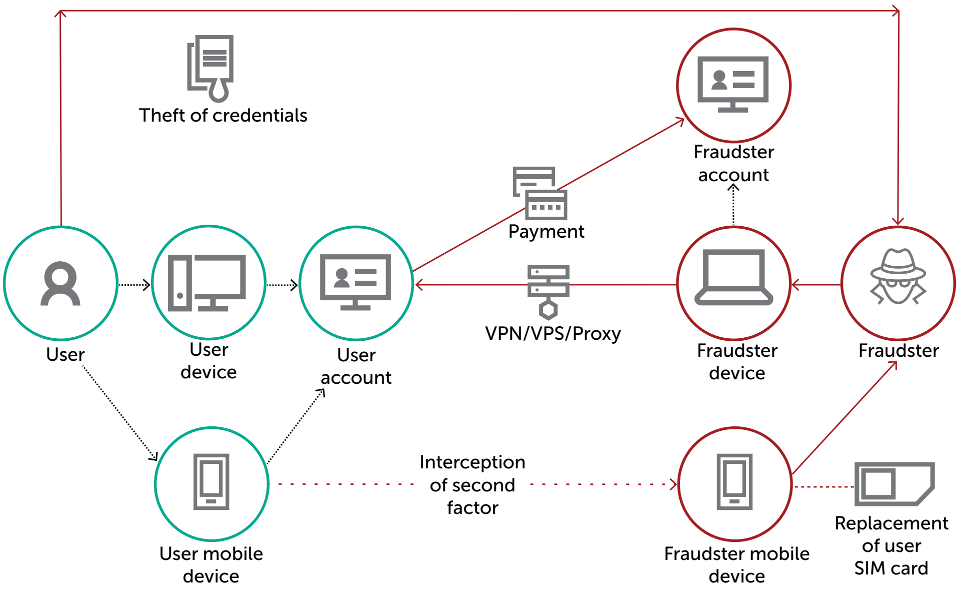

Theft of credentials and interception of the second factor
C&C
Malware with the integrated phishing and SMS interception modules
Fraudster account
Payment
User
Compromised user device
User account
VPN/VPS/Proxy
Fraudster device
Fraudster

2.1.2 Compromise of remote corporate banking accounts

New attack scenarios continue to complement existing fraudulent methods and scams.

Bypassing or intercepting the so-called second factor is a priority for the fraudsters. It is necessary to sign off a payment when transferring funds to the criminals' accounts.

Remote attacks on legal entities can be carried out using malicious software, though malware is not always necessary. In the non-malware cases, scammers resort to phishing, social engineering, etc. If a payment order can be signed without a physical token using an OTP, the password can be stolen by a cybercriminal with the help of social engineering, or some other method such as the unauthorized replacement of the user's SIM card which the OTP is sent to.

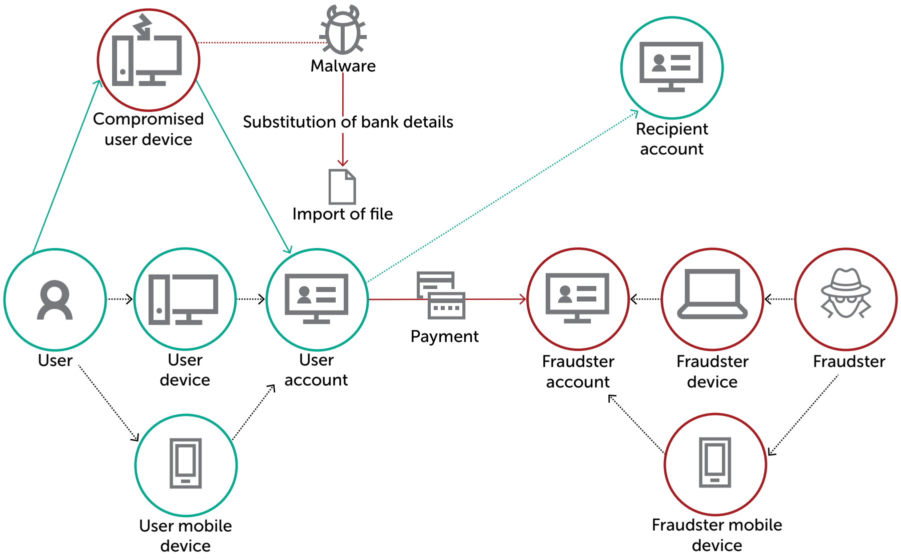


As a rule, malware is distributed via email spam. These malicious emails contain MS Office documents with exploits that download a banking Trojan when the recipient opens the attachment.

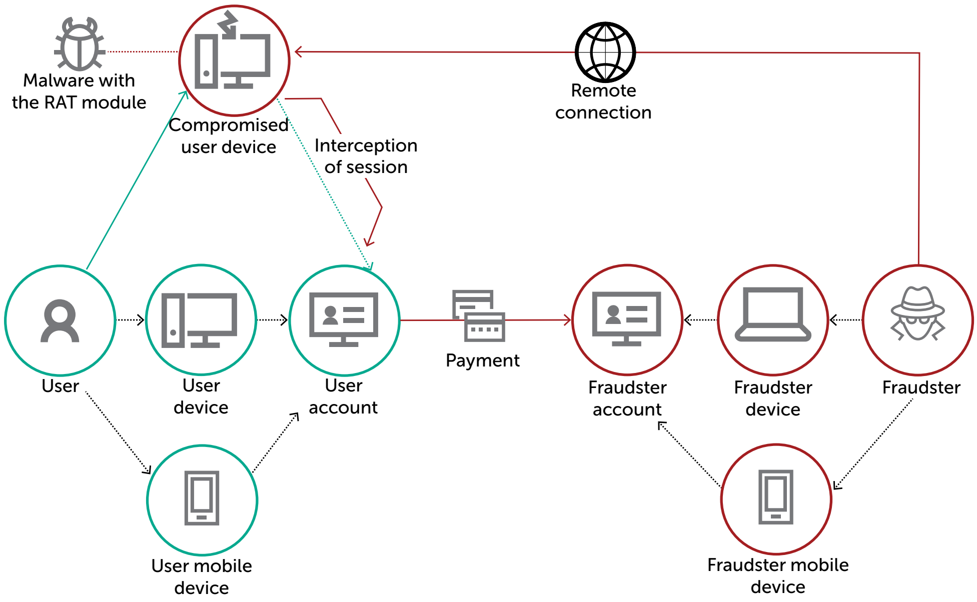
Malicious software can also be distributed via physical keys (USB). However, in this case, a fraudulent payment can only be made from the user's device with the installed key.

The main functions of malware designed to attack remote corporate banking accounts are:

- Substitution of the payment details in a file that is imported from third-party financial software by an accountant via the remote banking system. The malware changes the account of the transfer recipient on the fly, resulting in the accountant signing off the changed payment order using a physical token or a password and the money going to an account controlled by the attacker.



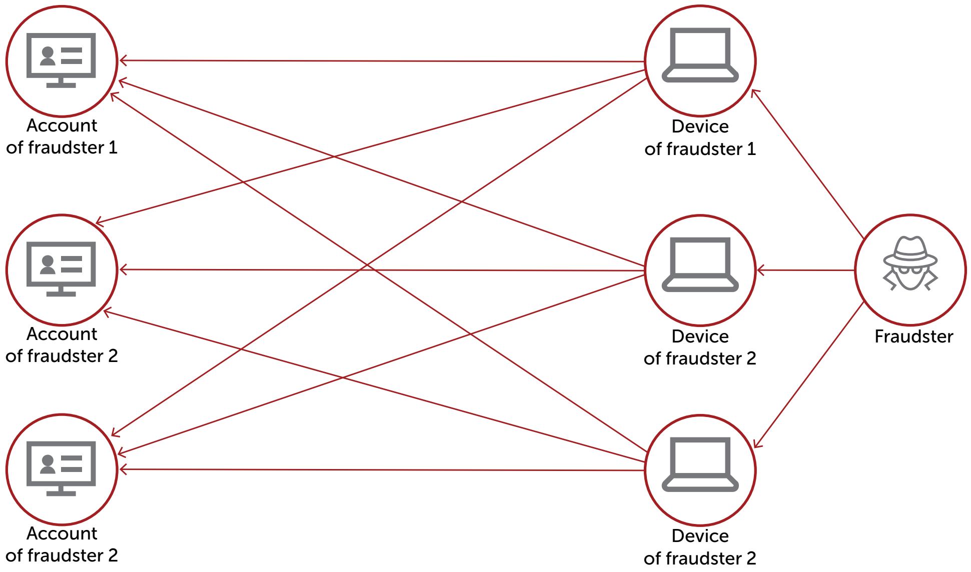
- Interception of a user's online banking session in the browser using a remote administration tool embedded in the malware. Within the framework of a remote connection, an attacker can sign any payment orders if a physical key is currently installed on the victim's PC. The malware displays a fake OS error screen to conceal the fraudulent creation of payments. Modified VNC libraries, LiteManager, AmmyAdmin or TeamViewer are usually built into the malware to enable a remote connection.



2.1.3 Use of remote corporate and personal banking accounts for money laundering

The following types of fake corporate and personal accounts are used in fraudulent activities:

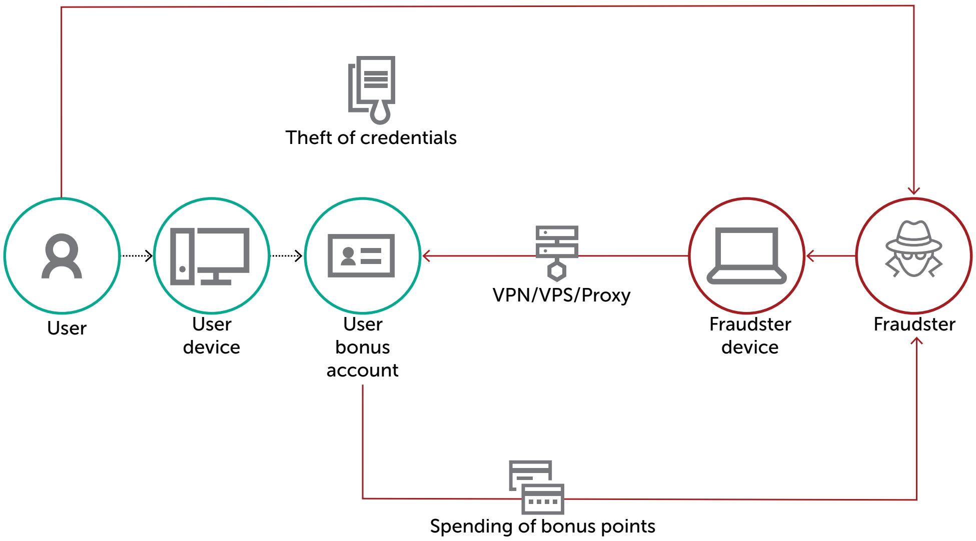
- Corporate accounts used to receive stolen funds.
- Corporate accounts involved in money laundering schemes ('commercial monetization').
- Corporate accounts used for the unauthorized transfer of funds.
- Personal accounts used as the final points in fraudulent schemes and/or money laundering schemes ('cash drops').



Threats to loyalty program accounts

2.2.1 Compromise of a loyalty program account

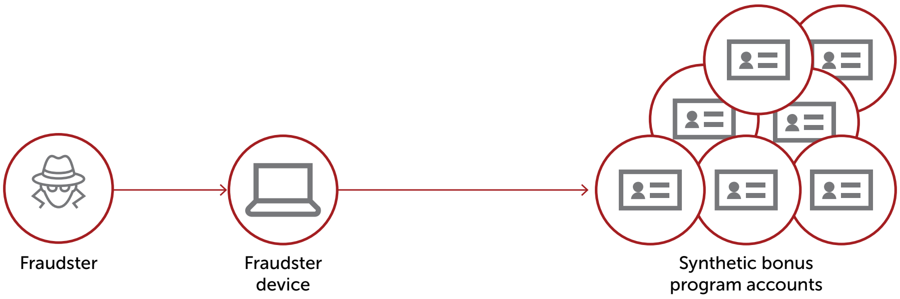
The compromise of a bonus system account usually occurs in three ways: a targeted attack on a personal account (brute force), collateral compromise via other services (email account), or with the help of Trojan stealers. The attacker then enters the personal account, preventing the owner from restoring access by changing the contact information, and subsequently manages the bonus account.



- Bonus points stolen by transferring them to other accounts (if the bonus program allows transfers).
- Bonus points spent on purchases/orders issued to other account details, addresses, etc.
- Use by the fraudster of various privileges available to the compromised account (discounts, gifts, etc.).
- Sale of a compromised account to other interested parties on internet sites with a related theme.

2.2.2 'Synthetic' loyalty program accounts

The creation of 'synthetic' (fake) accounts is relatively easy for scammers and at the same time provides lots of opportunities to commit fraud. Fraudsters can use or resell 'welcome' bonuses, promo codes or other gifts received upon registration or they can boost their chances of winning a prize in promos by participating from multiple accounts.



If a bonus program participant only uses a physical bonus card, the fraudster (armed with the bonus card data) can create a new, fake account, attach it to the card and steal the user's accumulated bonus points.

Sometimes synthetic accounts can be used with various partner programs for fraudulent schemes involving advertising traffic.

Then there is the creation of synthetic accounts by 'resellers' of goods that are bought using a 'welcome' bonus and then resold on other sites; this also comes with the added benefit of more loyalty program bonus points and, for example, cashback to the bank card used to make the purchase.

3 Examples of client incident investigations

Fraudulent re-registration of a personal online banking account

Several fraudulent groups that were compromising remote banking accounts to steal money were discovered in a large financial organization.

The attackers used compromised bank card numbers to initiate the registration of a remote banking account in an online banking system. In the first four months of 2018, 470 accounts were detected that had been compromised by these groups.

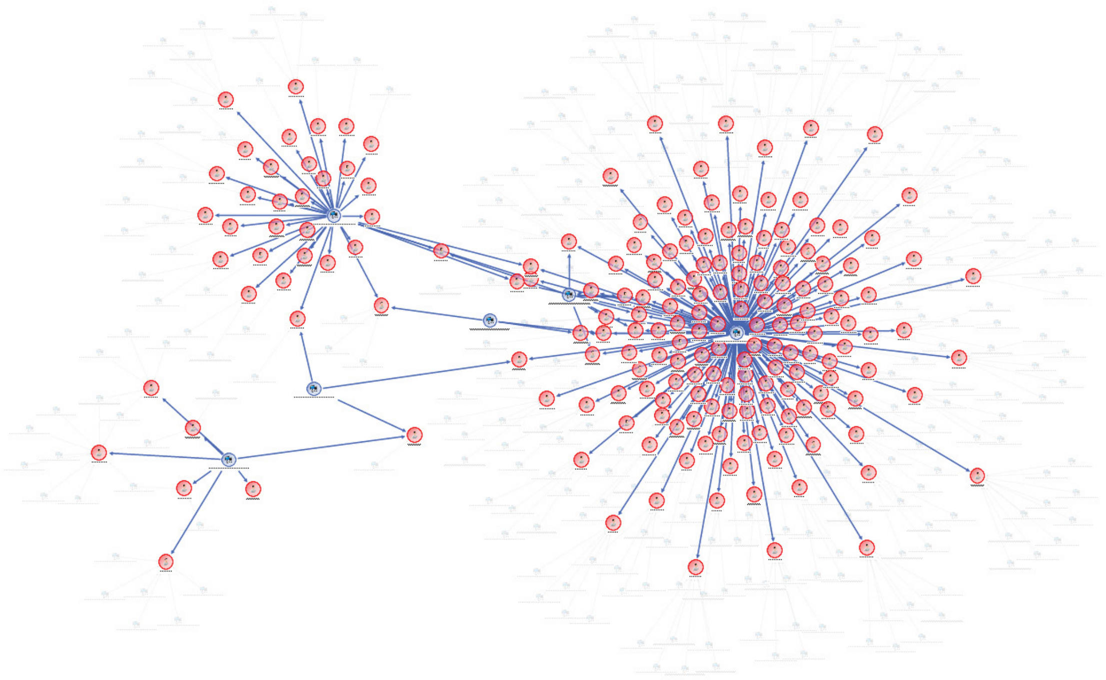
To obtain the second factor (SMS or push notification), the scammers used social engineering (calls or messages that appear to come from bank employees). After successfully registering in the online banking system, the attackers transfered money from the victim's account to the fraudsters'.

Fraudulent online sessions can be detected by the following indicators:

- Untypical user environment: new device or IP address, abnormal geolocation change.
- Sequence of suspicious account activities: re-registration on the remote banking system followed by a payment.
- Use of IP anonymization tools: proxy, VPN, VPS.
- Links to other compromised accounts via a fraudulent device.

The fraudulent devices used to access compromised remote banking accounts also allowed Kaspersky Fraud Prevention tools to discover several compromised personal accounts at two other banks.

Below is an illustration of the links between compromised accounts on the devices of one fraudulent group:



Interception of an online corporate banking session by means of remote control

In February 2018, there was an incident at a large bank involving the theft of funds from a corporate account via a remote banking portal.

The investigation revealed that an accountant's computer had been infected with a banking Trojan of the RTM group. The Trojan installed a modified library utility in the operating system for remote access to the device (VNC or TeamViewer) via which the fraudster managed to connect to the accountant's online session and make an unauthorized payment.

05.02.2018 14:36 MSK*: remote online banking session started; at some point the attacker started monitoring the session before connecting remotely.*
05.02.2018 14:54 MSK *accountant made first payment and signed it with a USB token.*
05.02.2018 15:33 MSK *accountant made second payment and signed it with a USB token.*
05.02.2018 15:33 MSK *fraudster interfered in the online session and began to arrange a payment.*
05.02.2018 15:41 MSK *fraudster made payment and signed it because the USB token had not been removed from the PC.*

Although this sort of attack is quite common, two specific features were identified in the fraudulent session:

1. Once connected to the accountant's online session, the fraudster began to arrange a payment in a new browser window to hide their activity; meanwhile, the accountant's attention was focused on the original remote banking window (the Trojan supposedly displayed a fake notification about a problem with the banking system or the computer).

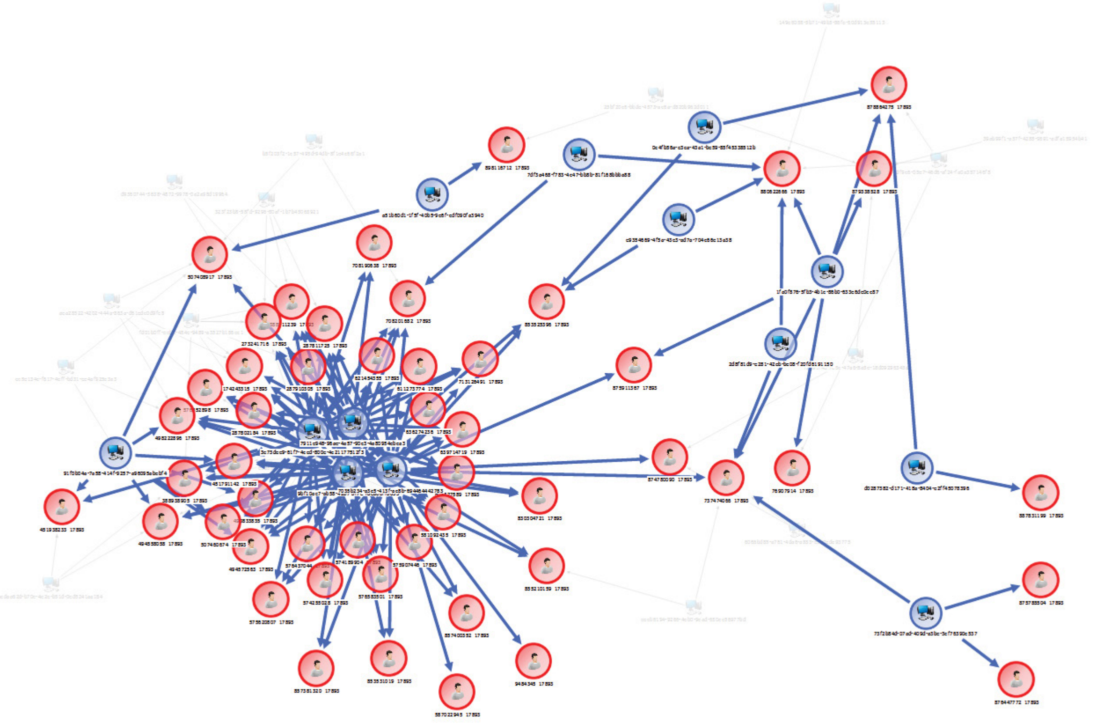
2. During the interception of the online session, the number of times the mouse cursor was outside the browser window increased significantly and abnormally, which may indicate that the remote connection program on the attacker's side was opened in windowed mode, explaining why the cursor constantly left the active area.

Personal account 'bot-clicker' used for monetization

At another financial organization, a group of 50 personal accounts involved in money laundering was revealed. The verdict was based on the use of the same devices to manage fraudulent accounts in the online banking system and the use of various VPNs and proxies to anonymize and hide the real IP address.

With the help of Kaspersky Fraud Prevention, it was also found that to manage these accounts automation tools (automation of mouse clicks, or a bot-clicker) were used to perform typical remote banking tasks such as checking the balance.

Illustration of account links via fraudulent devices:



Mass compromise of loyalty program accounts

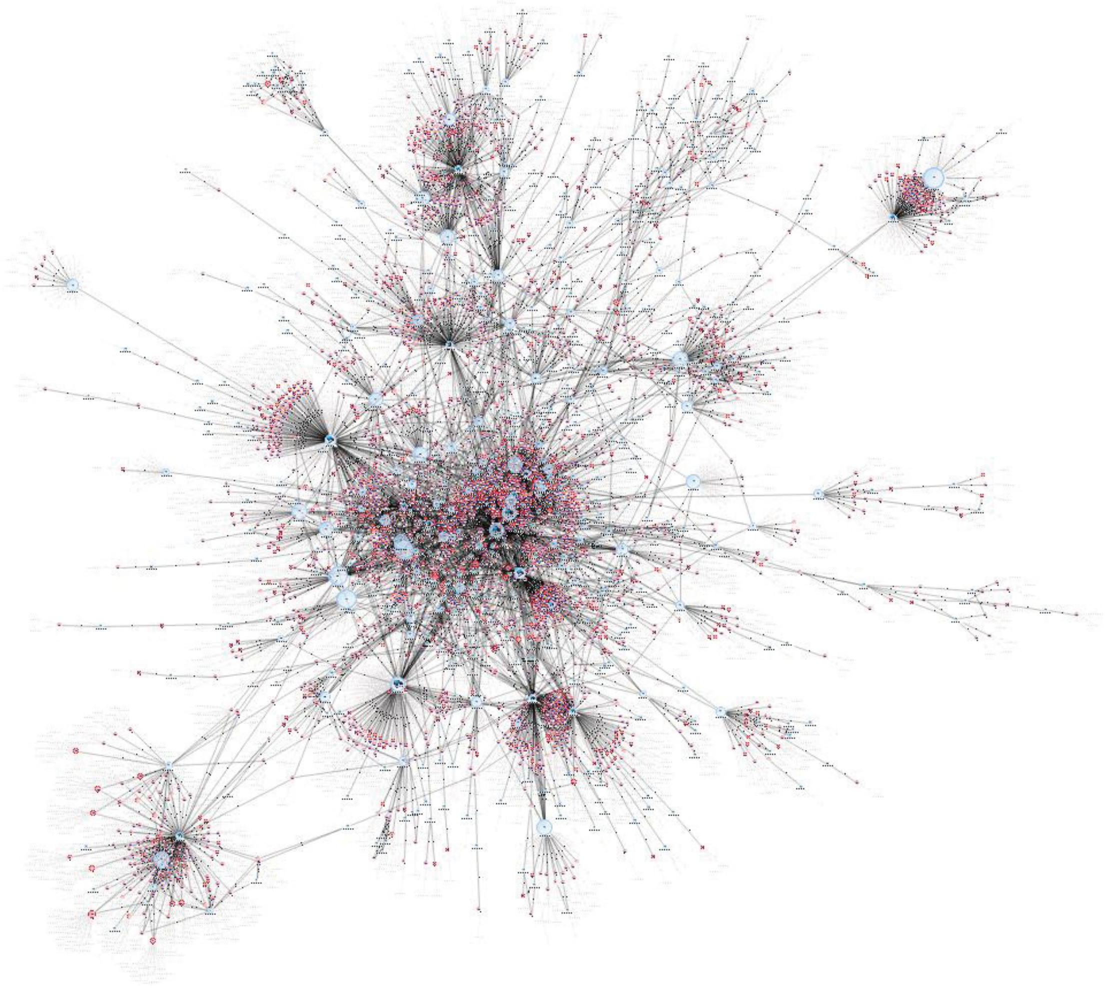
A fraudulent scheme related to the compromise of user accounts was discovered at a large internet service provider.

As a result of brute-force attacks or email accounts being compromised, the scammers managed to obtain user credentials, and hindered legitimate users from restoring access by changing contact information, specifically, by changing an email address to the address of a 'one-time email' controlled by the attackers. After that, the current tariff plan is changed to obtain a bonus by specifying the corresponding user name. The scammers then carry out transactions with the compromised accounts on internet sites with a similar theme.

Kaspersky Fraud Prevention analyzed the connections via the fraudsters' devices to identify more than 25,000 compromised user accounts involved in this fraudulent scheme. Every month the number of compromised accounts rose by approximately 5,000.

After the provider took measures to forcefully reset the passwords of the compromised accounts, repeated fraudulent logins were detected with approximately 10% of users (with the scammers recovering passwords themselves by reattaching accounts to their email addresses).

Illustration of compromised account links via the scammers' devices:

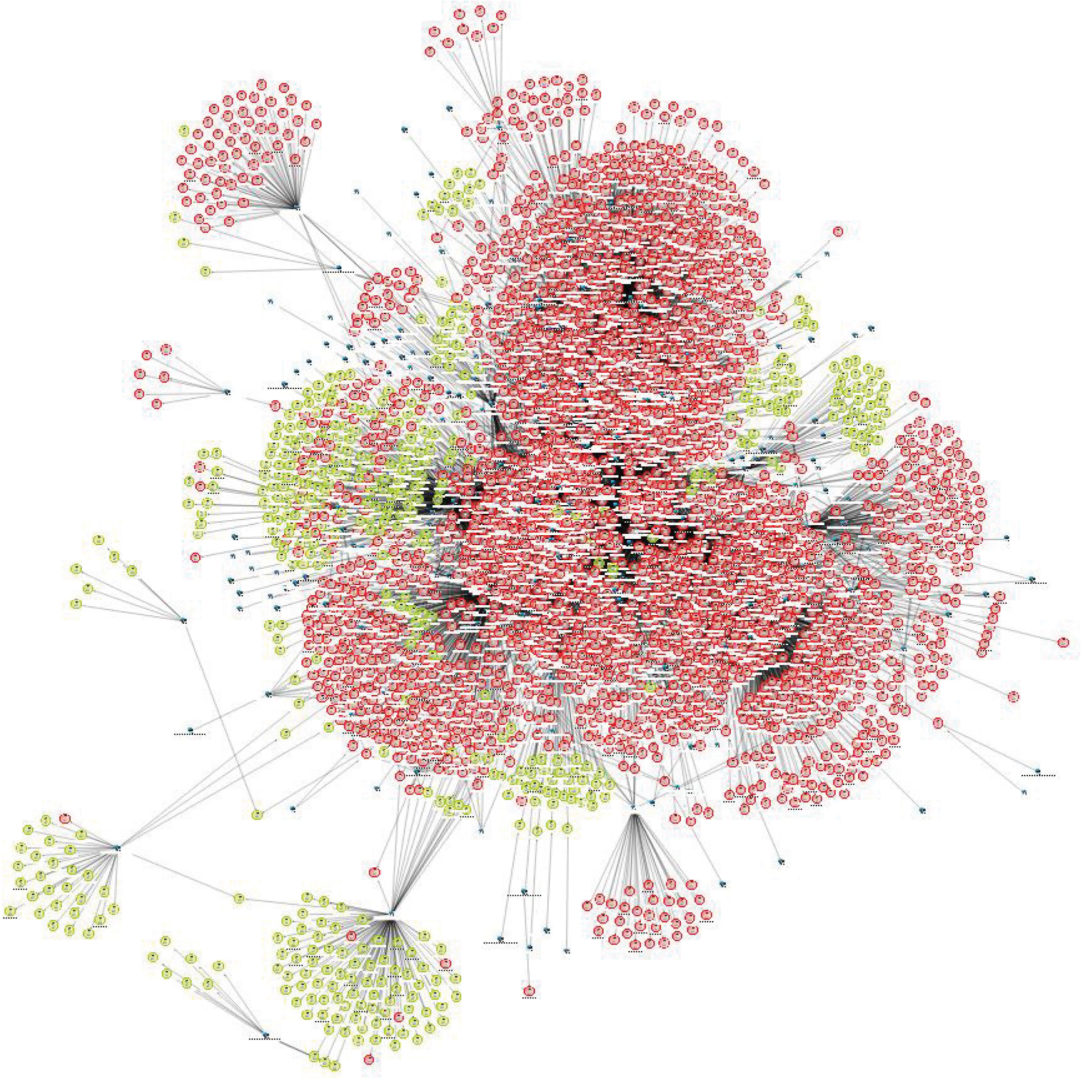


Creation of synthetic accounts to obtain promotional codes for a loyalty program

At the end of 2017, a group of almost 3,000 synthetic accounts was discovered among the accounts of a loyalty program. They were used to receive 'welcome' bonuses for registering new accounts, with a view to reselling them on related internet sites. A distinctive feature of this group was the use of a single email box to manage the entire group. This was made possible due to a feature of the Gmail service that does not take into account the dot symbol in an alias, allowing all accounts in the incident to become modified versions of the main primary address with the addition of a dot.

After Kaspersky Fraud Prevention was connected to another major marketplace bonus program it was found that the same scammer had begun creating synthetic accounts to receive welcome bonuses for this service as well, using the same devices and the same trick with the email addresses on Gmail. The attacker managed to create a total of 542 synthetic accounts in the bonus program.

Illustration of compromised account links for two different loyalty programs via the fraudster's devices:



Beat fraud and ensure seamless digital experience for your clients

True Machine Learning

Forensic Capabilities

Reduced Operational Costs

Automated Fraud Analytics

- Real-time detection and analysis of in-session events
- Identification of new account fraud, money laundering and account takeover incidents
- Global entity linking and mapping

Advanced Authentication

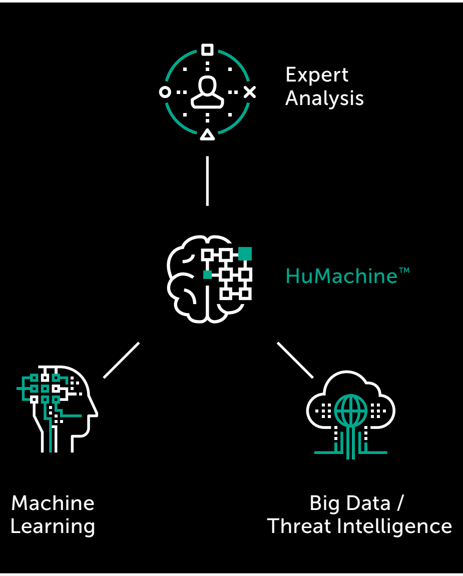
- RBA functionality
- Continuous authentication
- Reduced second factor costs

Order your demo by contacting us at kfp@kaspersky.com

Kaspersky Lab
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com/fraudprevention


Expert
Analysis
HuMachine™
Machine
Learning
Big Data /
Threat Intelligence