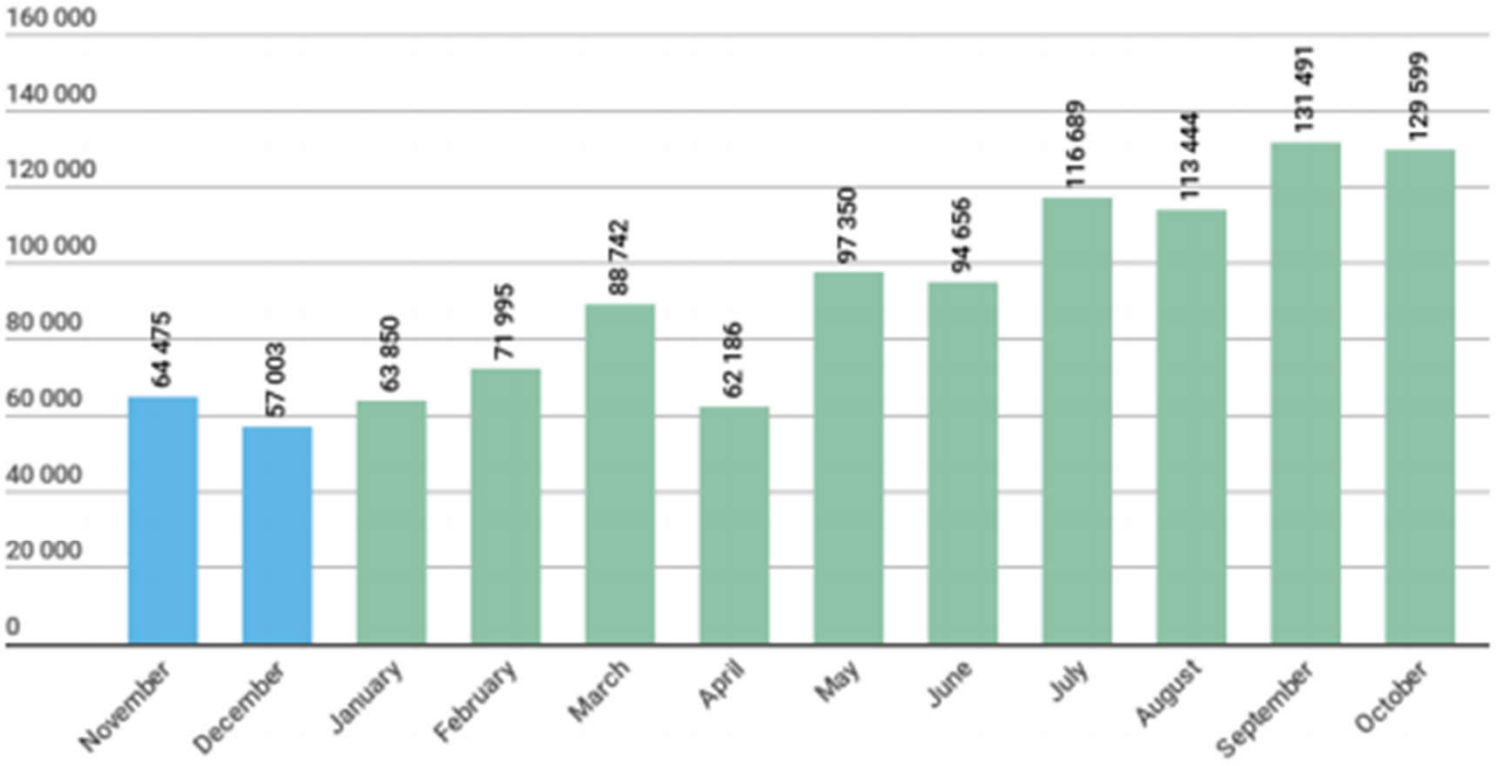
IT security (Financial threats)

Kaspersky Lab's look at the latest trends

YARNYKH ANDREY
Head of GR & Strategic Projects
Kaspersky Lab, Russia
Andrey.Yarnikh@kaspersky.com

In 2018, Kaspersky Lab solutions blocked attempts to launch one or more malicious programs designed to steal money from bank accounts on the computers of **830 135** users.



Number of unique users attacked by banking malware, November 2017 – October 2018

KASPERSKY lab

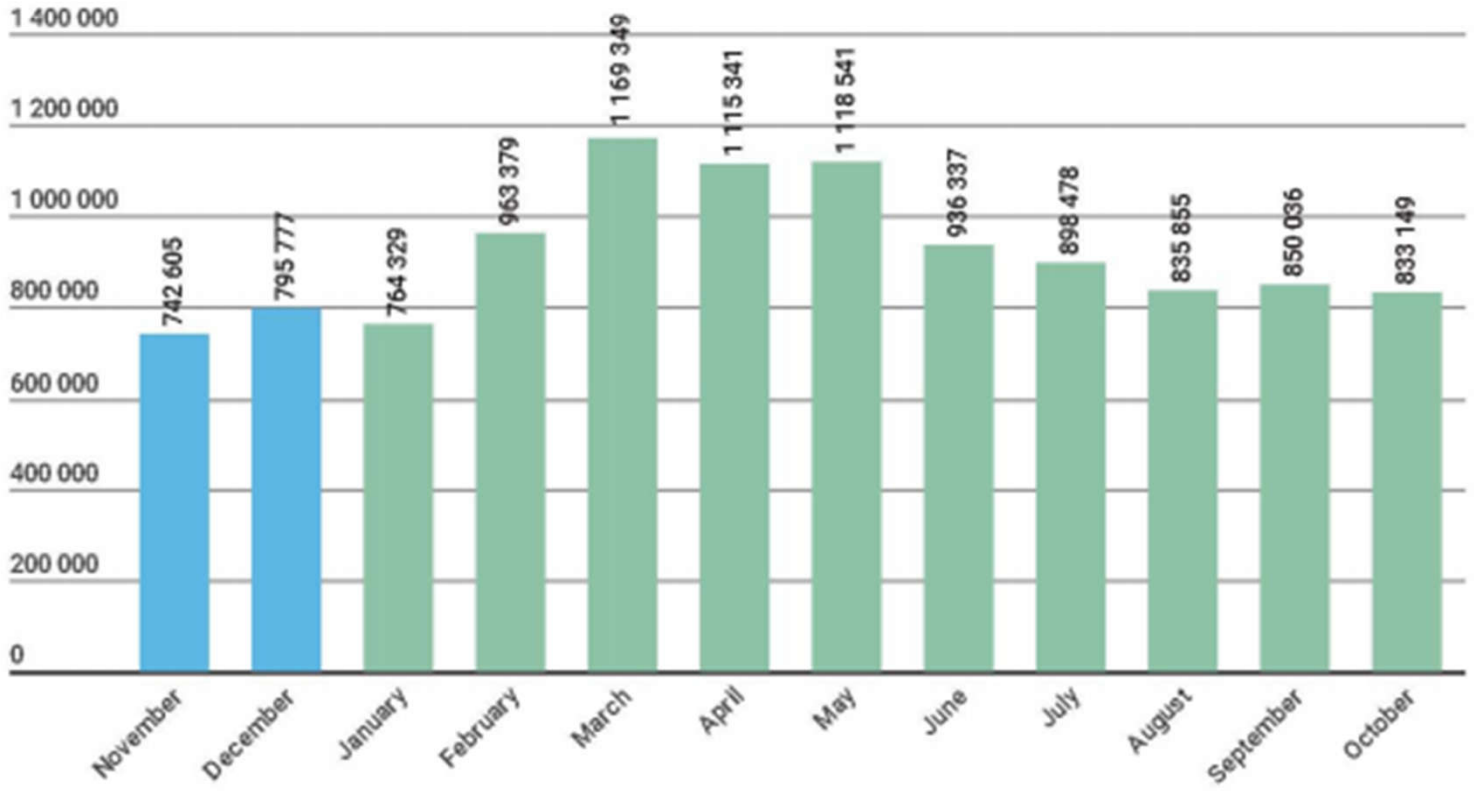
The table below shows the 10 malware families most commonly used in 2018 to attack banking users.

	Name	%*
1	Trojan.Win32. Zbot	26.3
2	Trojan.Win32. Nymaim	19.8
3	Backdoor.Win32. SpyEye	14.7
4	Backdoor.Win32. Caphaw	5.2
5	Trojan-Banker.Win32.RTM	5.2
6	Backdoor.Win32. Emotet	4.9
7	Trojan.Win32. Neurevt	3.9
8	Trojan-Banker.Win32.Tinba	1.9
9	Trojan.Win32. Gozi	1.8
10	Trojan-Banker.Win32.Trickster	1.5

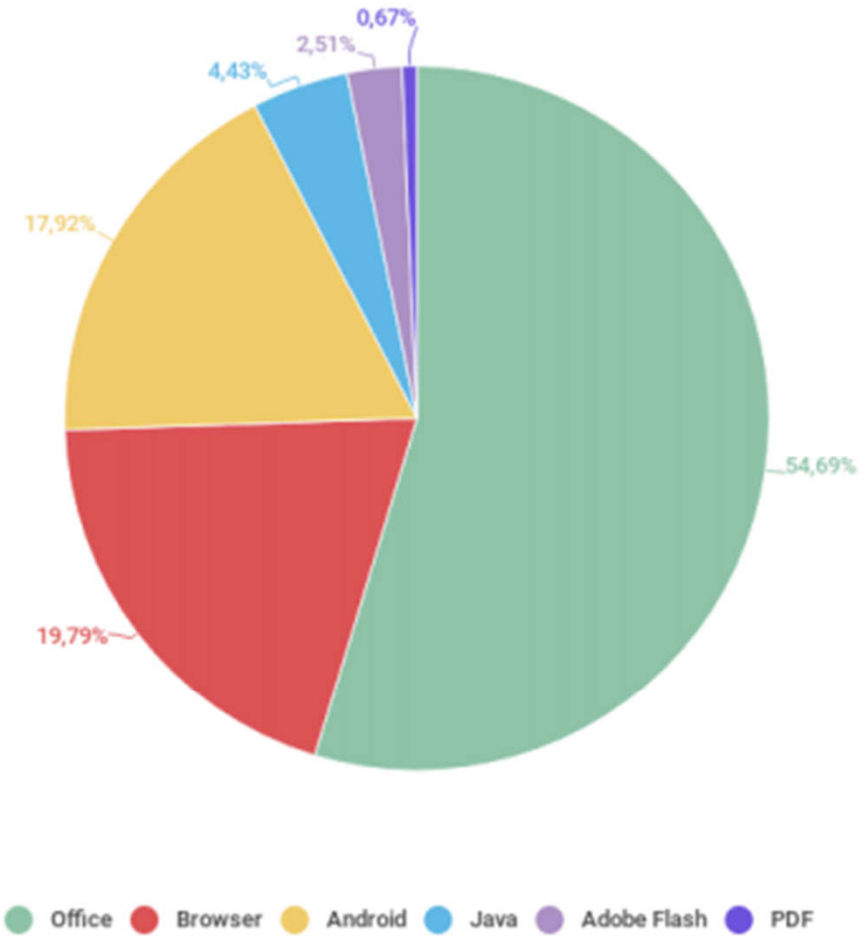
** Unique users attacked by the given malware as a percentage of all users that were attacked by banking threats.*

The number of users attacked by miners

During the reporting period, **5 638 828** unique KSN users were attacked by miners. In the total volume of detections, the share of miners was 8.50%; for Risktool it was 16.88%.



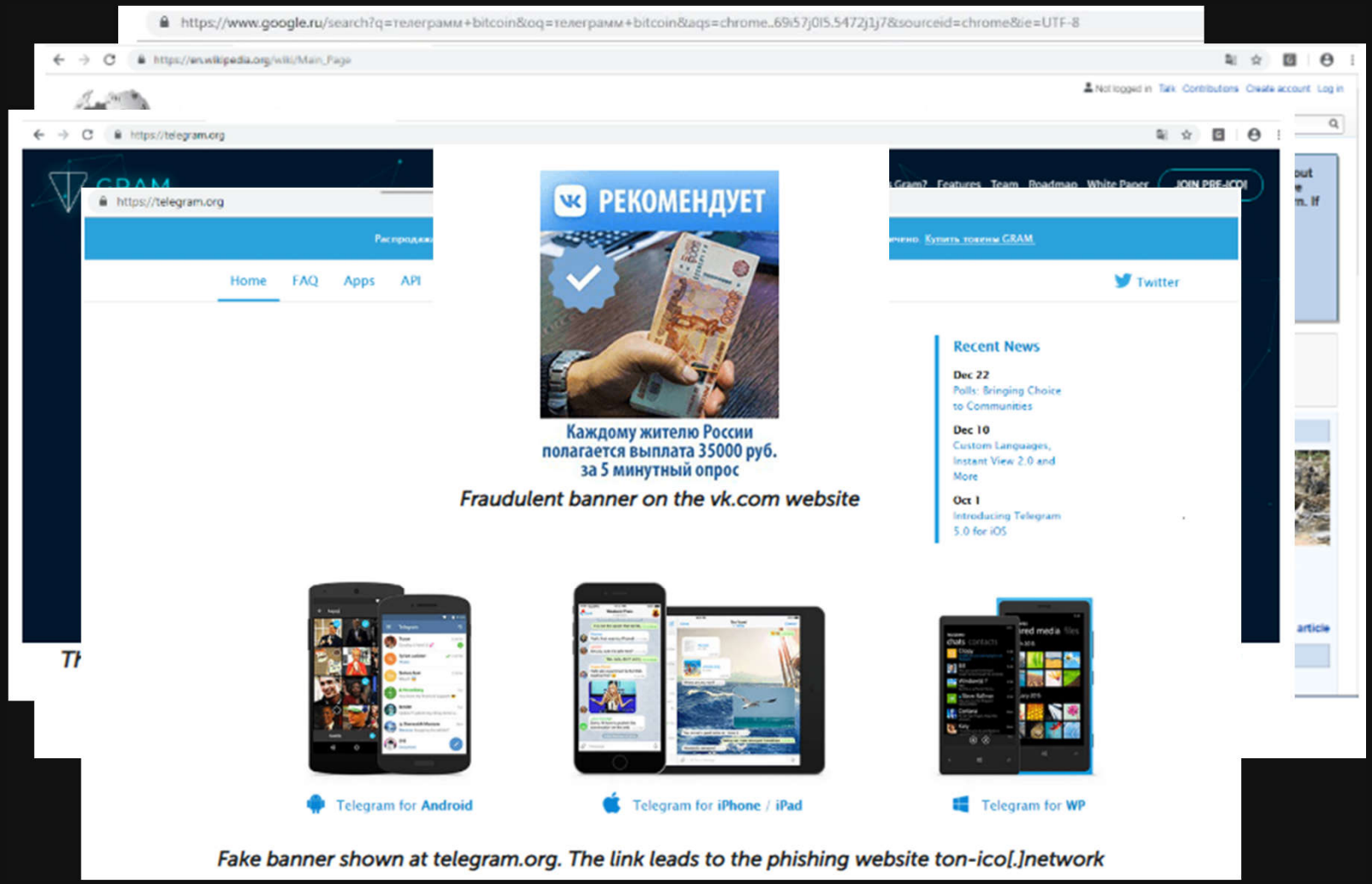
KASPERSKY lab



Distribution of exploits used in cyberattacks, by type of application attacked, November 2017 – October 2018

increase in the share of Microsoft Office exploits in our statistics,from 17.63% to an incredible 55%. The reason for this growth was the massspam mailings that spread documents with exploits for vulnerabilities CVE-2017-11882 and CVE-2018-0802

Razy in search of cryptocurrency

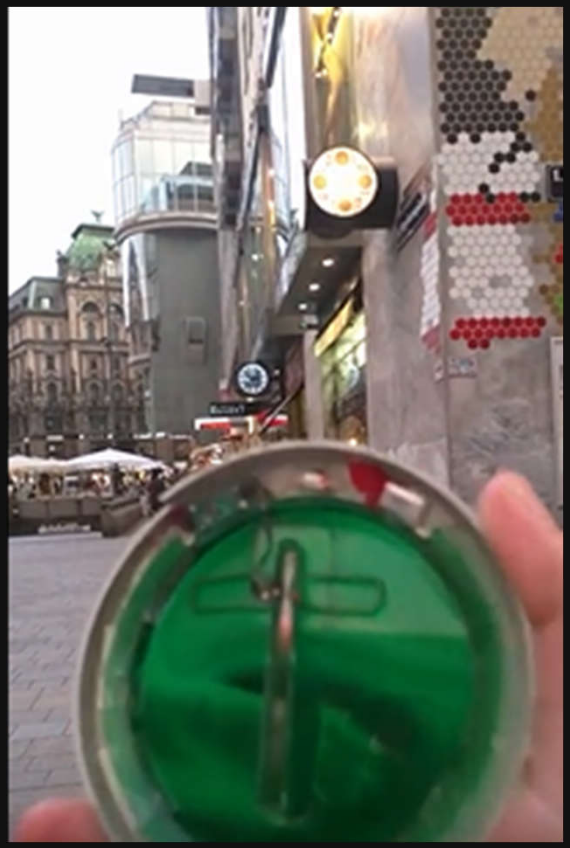


Fraudulent banner on the vk.com website

Fake banner shown at telegram.org. The link leads to the phishing website ton-ico[.]network

- Searching for addresses of cryptocurrency wallets on websites and replacing them with the threat actor's wallet addresses
- Spoofing images of QR codes pointing to wallets
- Modifying the web pages of cryptocurrency exchanges
- Spoofing Google and Yandex search results

Finding an ATM Skimmer in Vienna



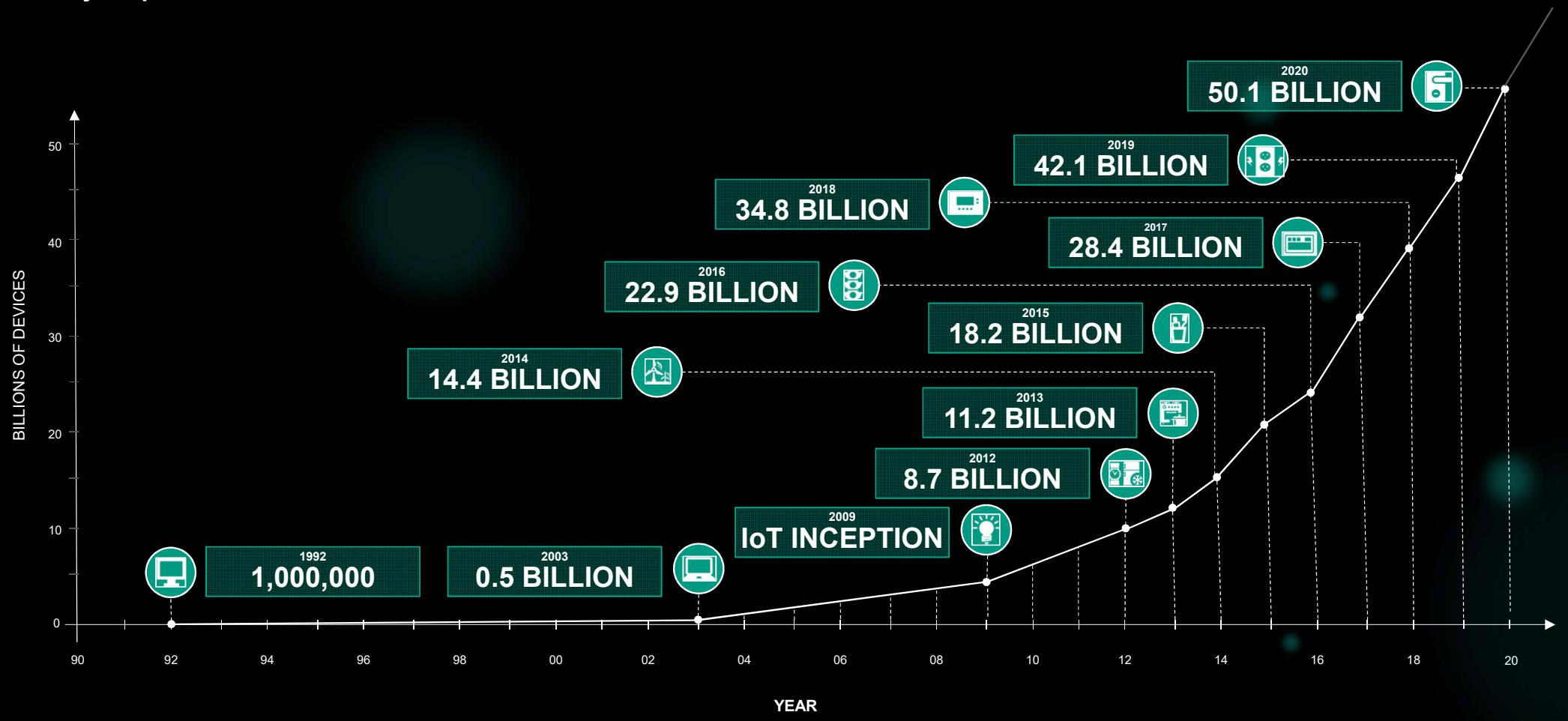
ATTACKS ON SWIFT

Targets

Financial institutions | **Casino** | **Software developers for investment companies** | **Cryptocurrency exchange**

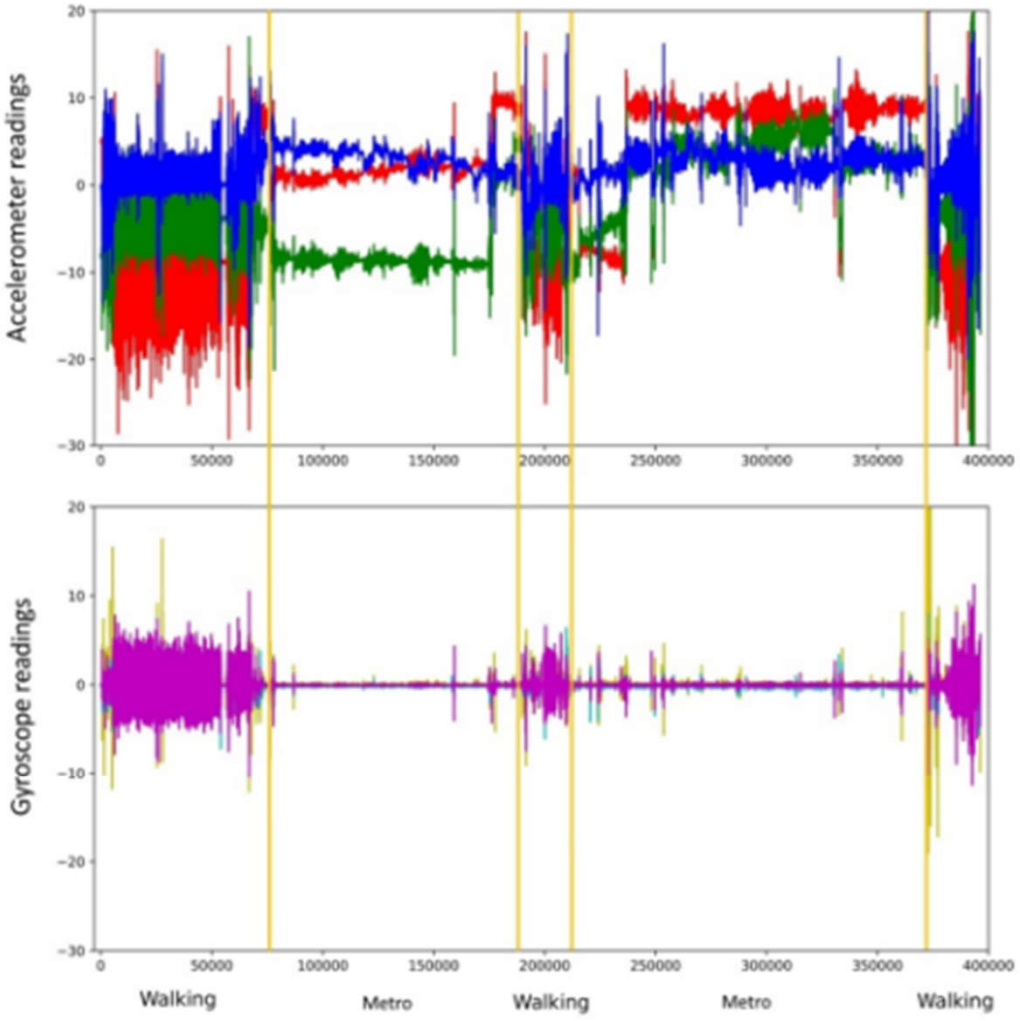
Internet Of Threats

What if your perimeter includes connected smart devices?



KASPERSKY lab

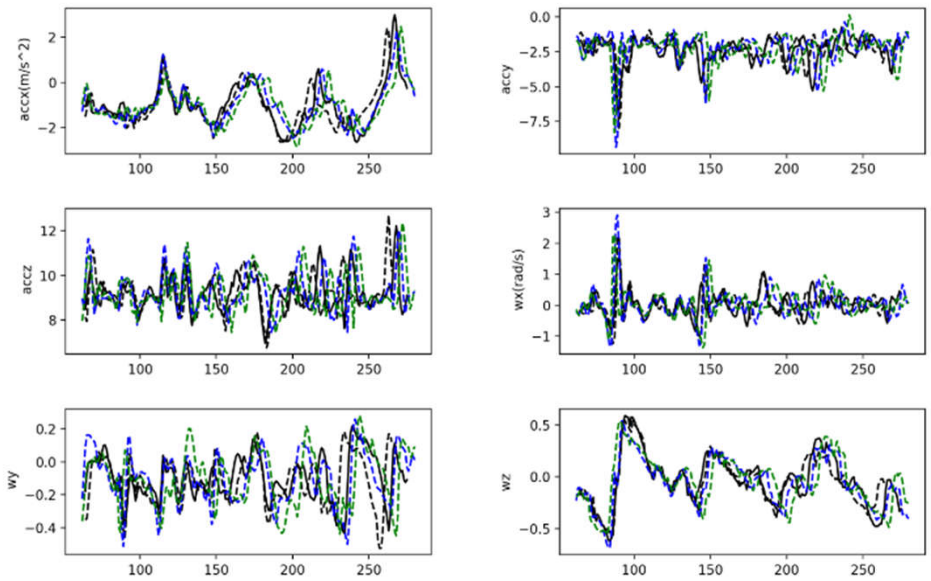
For the purpose of our study, we wrote a fairly simple app based on Google's reference code and carried out some neat experiments with the Huawei Watch (first generation), Kingwear KW88, and PYiALCY X200 smartwatches based on the Android Wear 2.5 and Android 5.1 for Smartwatch operating systems. These watches were chosen for their availability and the simplicity of writing apps for them (we assume that exploiting the embedded gyroscope and accelerometer in iOS would follow a similar path).



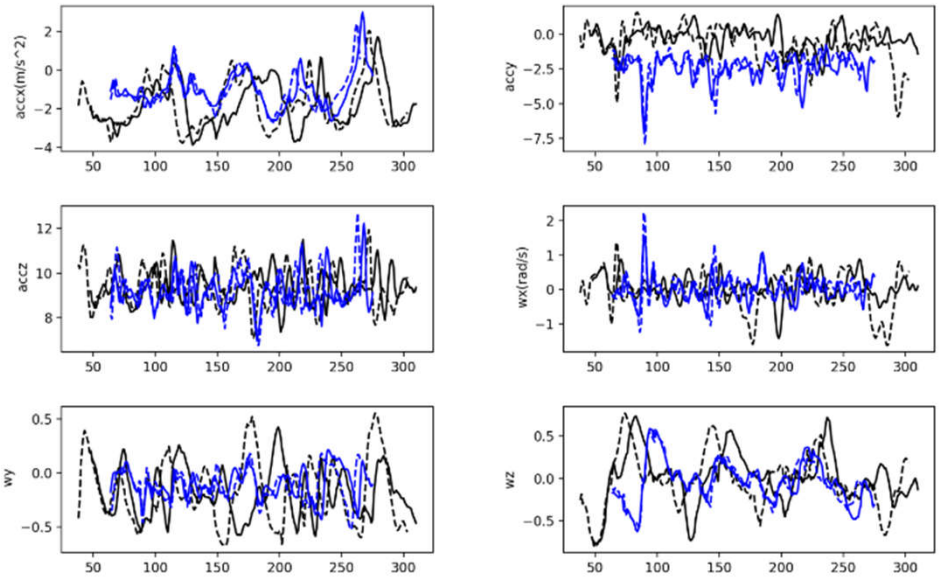
Accelerometer and gyroscope readings with decoding of areas

These are three periods of walking (12, 3, and 5 minutes) interspersed with subway journeys (20 and 24 minutes). The short walking interval has some particular characteristics, since it involved changing from one subway line to another

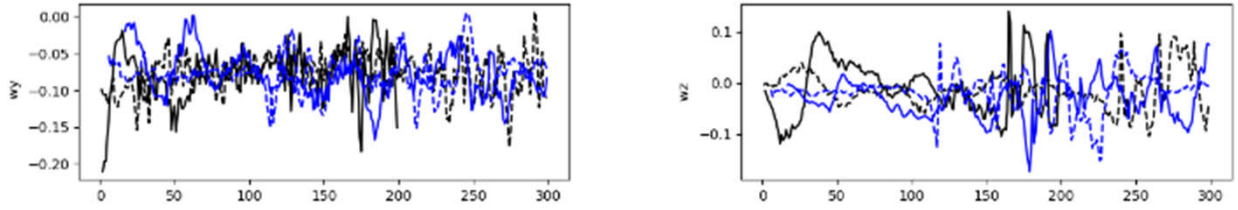
https://securelist.com/trojan-watch/85376/



Signal along the accelerometer and gyroscope axes for four attempts by one person to enter one password on a desktop computer



Signals along the accelerometer and gyroscope axes for attempts to enter the same password by different people on a desktop computer



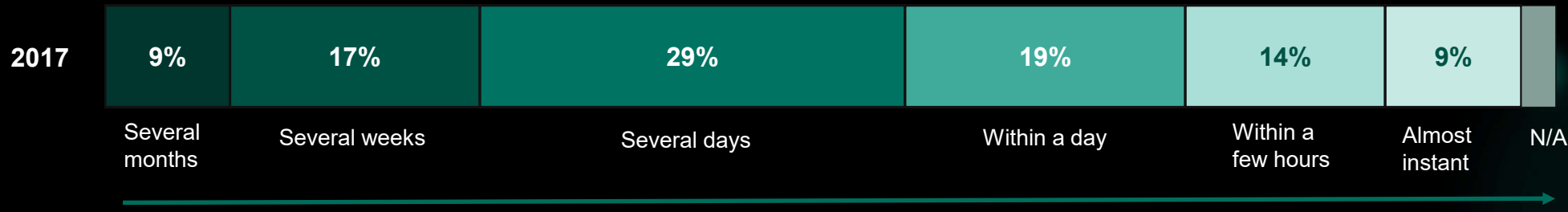
Attempts to enter a smartphone unlock code by two different people

Targeted Attacks: How To Combat Them?

- Incident detection time is critical
- Prevention strategies won't keep you safe
- Delays are expensive

CREATE AN INTERNAL ENDPOINT DETECTION AND RESPONSE STRATEGY

TIME UNTIL COMPANIES DETECT AN ATTACK



KASPERSKY lab

Сделать IoT безопасным по умолчанию

KasperskyOS®

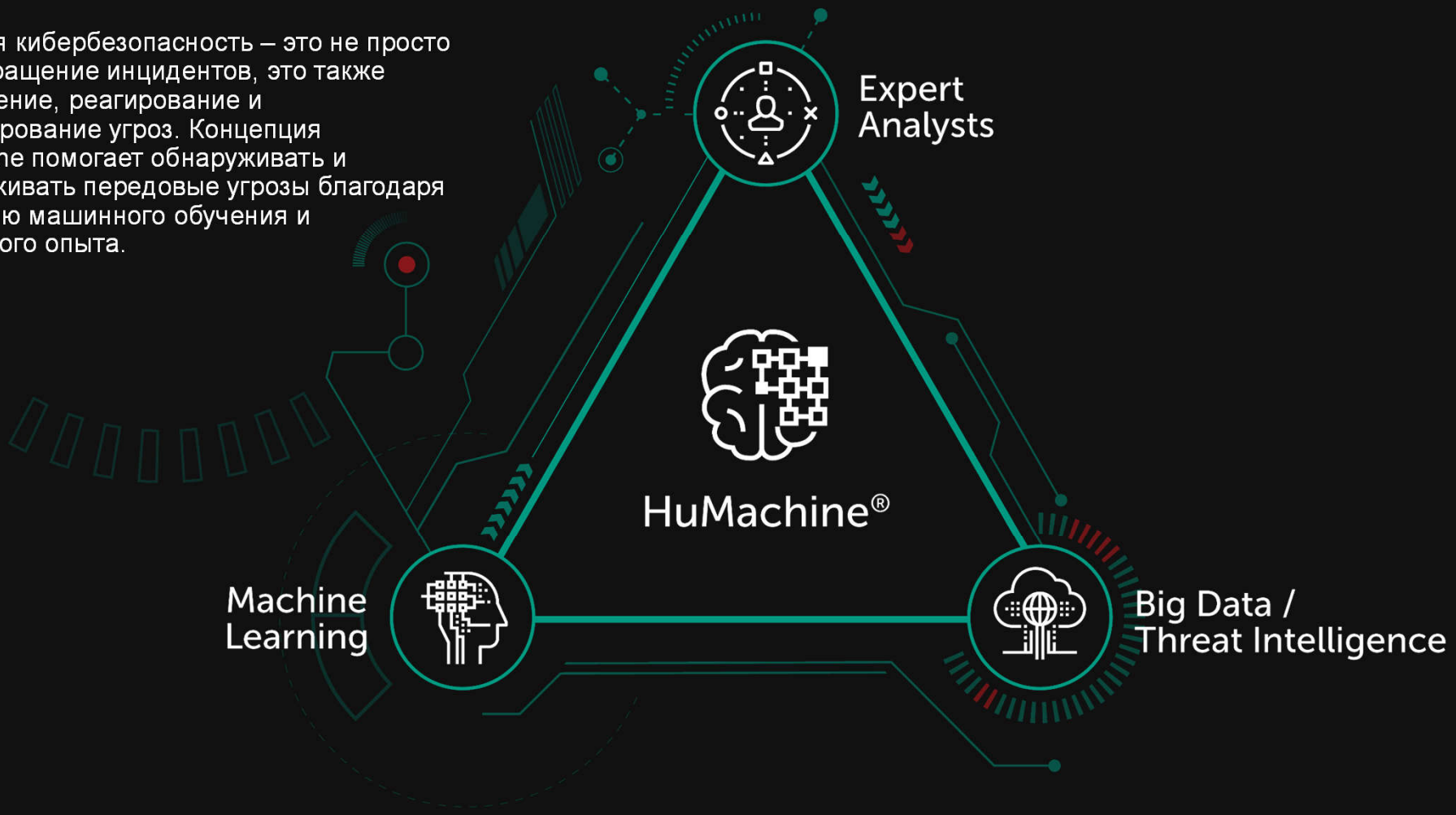
Значительно снижает возможность недокументированной функциональности

Адаптируется под потребности разработчика

Делает разработку ПО для IoT устройств изначально безопасной

Истинная кибербезопасность

Истинная кибербезопасность – это не просто предотвращение инцидентов, это также обнаружение, реагирование и прогнозирование угроз. Концепция HuMachine помогает обнаруживать и обезвреживать передовые угрозы благодаря сочетанию машинного обучения и экспертного опыта.




Let’s Talk!
KASPERSKY lab