ANALYSING FINANCIAL SECTOR DATA NETWORK & SECURITY.

ANA University

Vachagan Melkonyan

Karen Tadevosyan

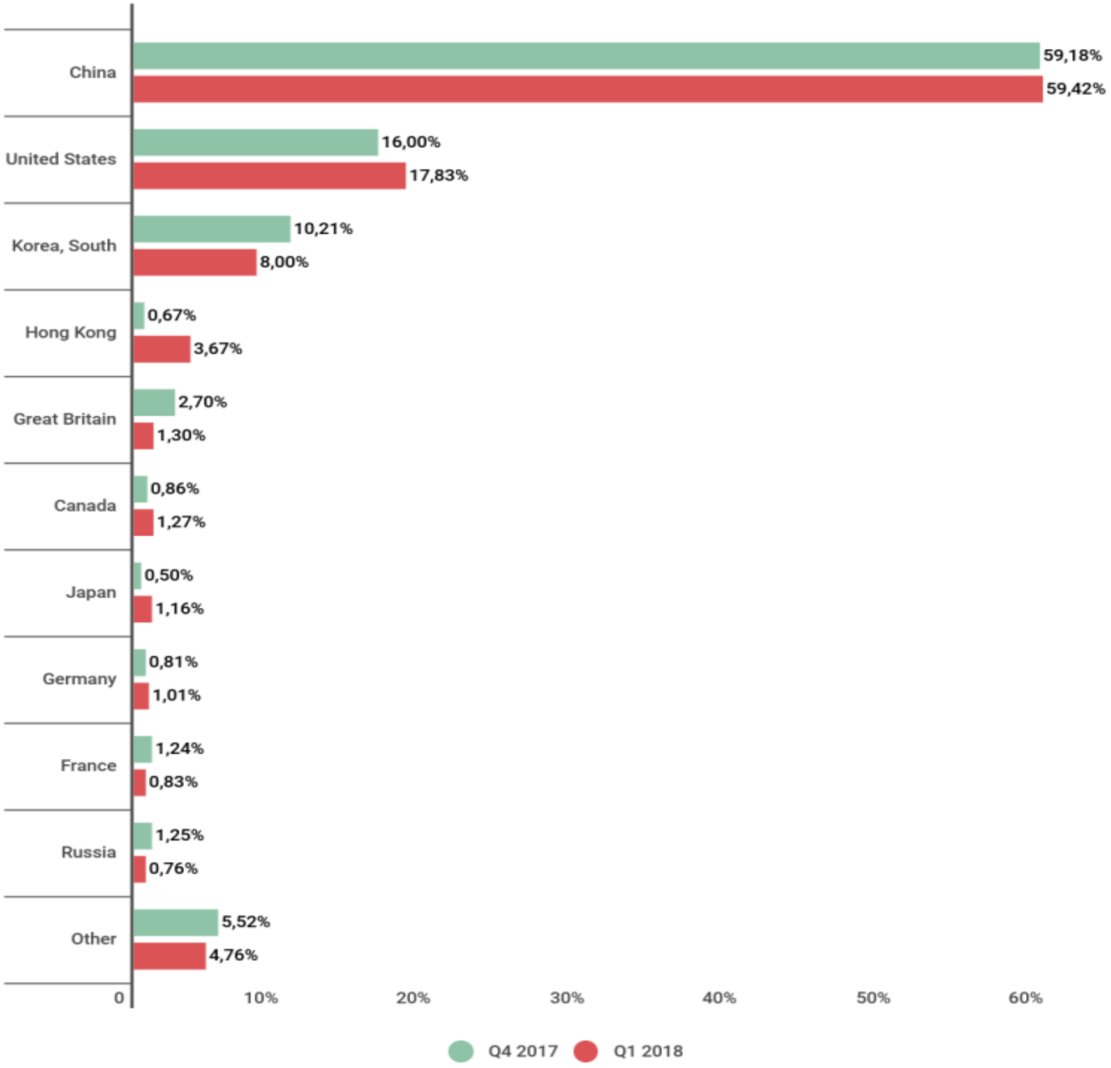
AGENDA

- Global research
- Review of Financial sector cyber security
- Review of cyber attacks at Financial sector
- IoT in Banks
- Conclusions

Global research

Overall in first quarter of 2018, DDoS botnets attacked online resources in 79 countries. The countries experiencing the largest number of attacks were once again China, the U.S. and South Korea, which all continue to lead in terms of the number of servers available to attackers as well as the number of sites and services hosted on them.

Tenth place in Q1 2018 went to Russia, whose share decreased from 1.25% to 0.76%. The Netherlands and Vietnam dropped out of the top ten, but Hong Kong (with a solid 3.67% against 0.67% in Q4 2017) and Japan (1.16%) reappeared.



Tenth place in Q1 2018 went to Russia, whose share decreased from1.25% to 0.76%. The Netherlands and Vietnam dropped out of the top ten, but Hong Kong (with a solid 3.67% against 0.67% in Q4 2017) and Japan (1.16%) reappeared.

* Based by Kaspersky DDoS Protection product statistical data

However, banking attacks are usually a multi-step process: social engineering, phishing, and the use of Trojan-Downloaders which then download the financial malware. It’s easier for the criminals to modify the Trojan-Downloader programs (which are usually smaller in size, and generally less complex) than the financial malware itself.

The most common types Cyber Attacks on Banks

□ DDoS attacks

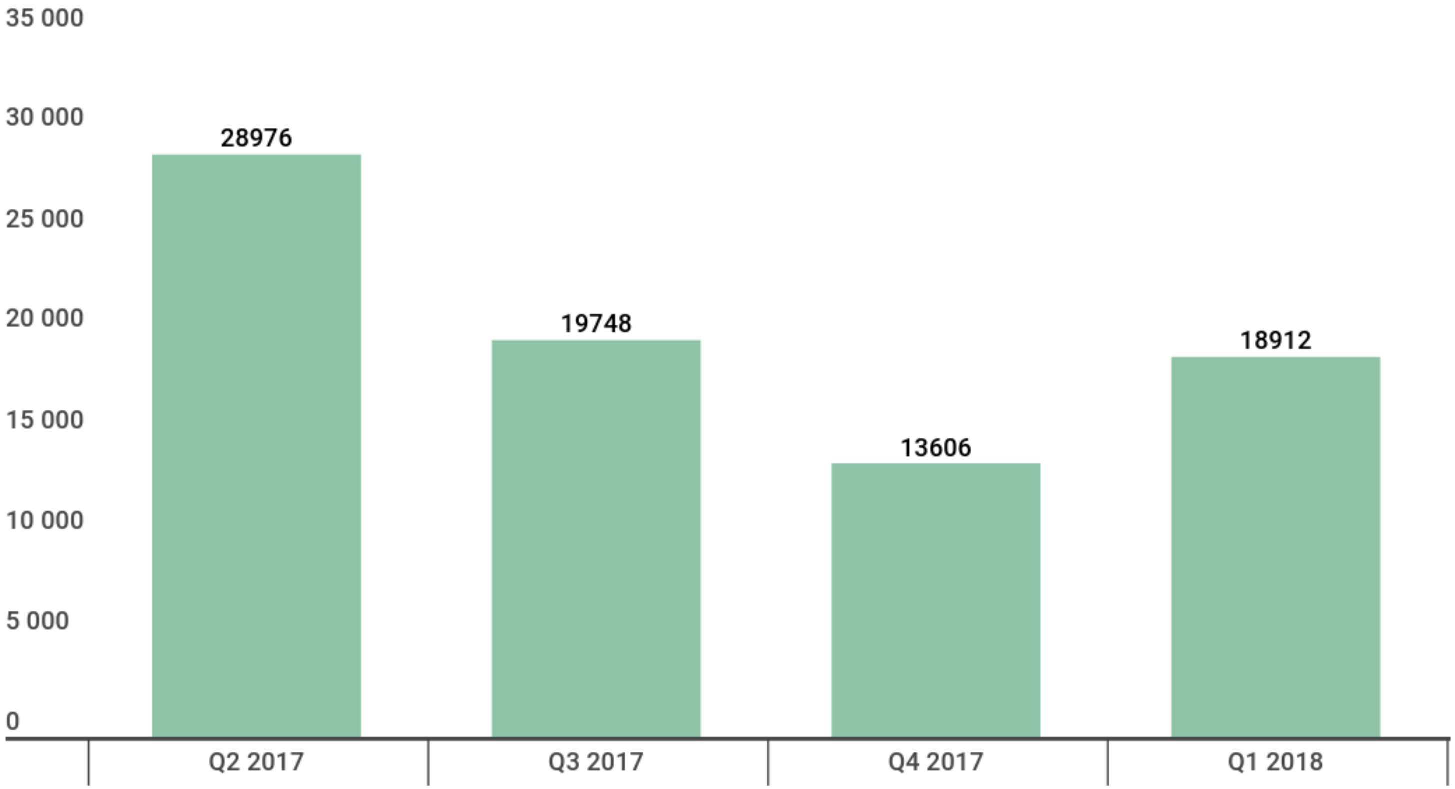
□ Phishing

□ Redirecting traffic

□ Man-in-the-Middle attack

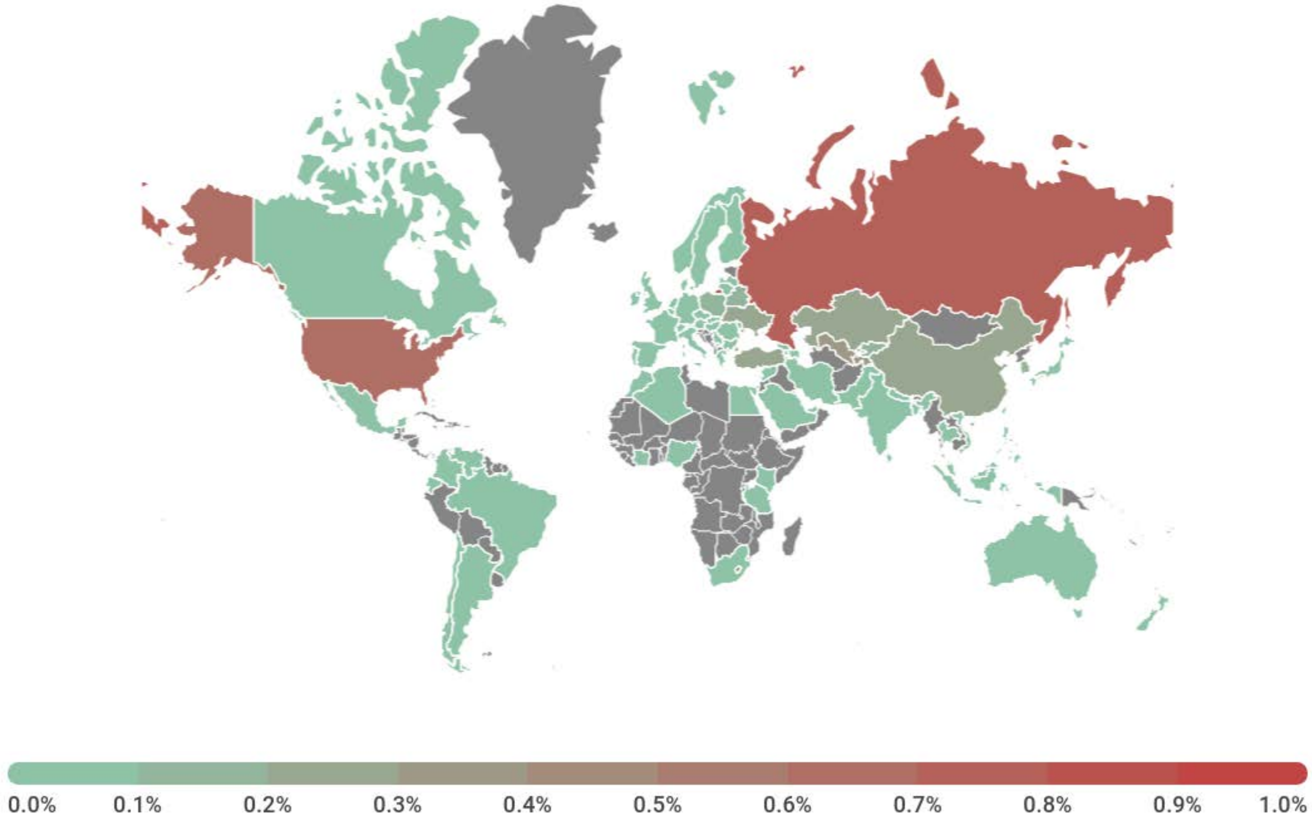
□ Other

According to KSN data, Kaspersky Lab solutions blocked 796,806,112 attacks launched from online resources located in 194 countries all over the world. (Q12018) In the reporting period, was detected 18,912 installation packages for mobile banking Trojans, which is 1.3 times more than in Q4 2017.



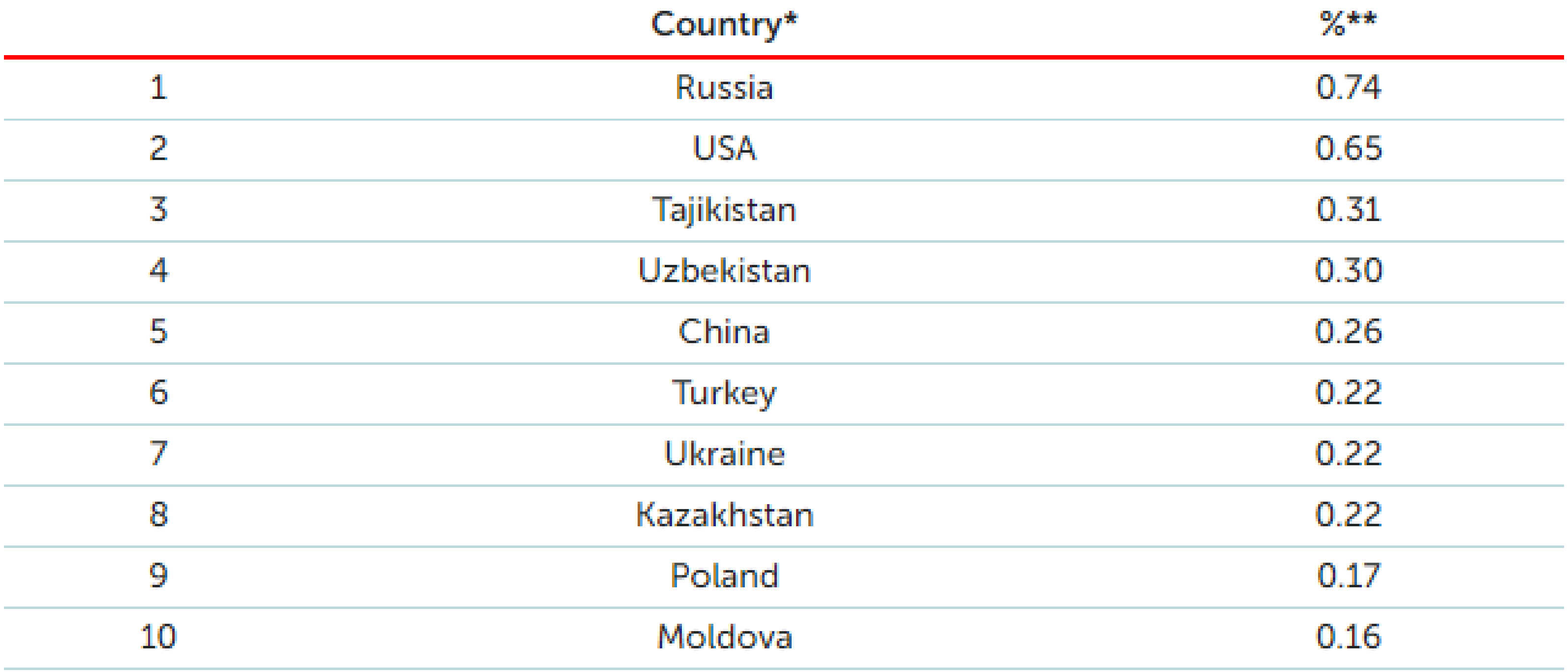
Number of installation packages for mobile banking Trojans detected by Kaspersky Lab, Q2 2017 – Q1 2018

The most popular mobile banking Trojan in Q1 was Asacub.bj (12.36%), nudging ahead of second-place Svpeng.q (9.17%). Both these Trojans use phishing windows to steal bank card and authentication data for online banking. They also steal money through SMS services, including mobile banking.



Geography of mobile banking threats in Q1 2018 (percentage of attacked users)

TOP 10 countries by share of users attacked by mobile banking Trojans

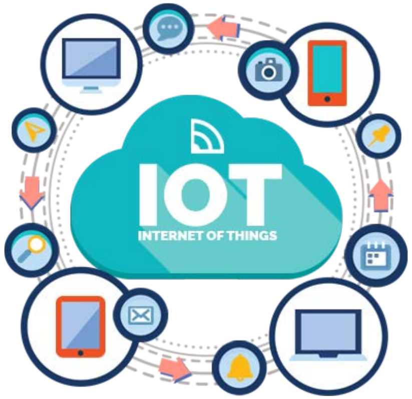


	Country*	%**
1	Russia	0.74
2	USA	0.65
3	Tajikistan	0.31
4	Uzbekistan	0.30
5	China	0.26
6	Turkey	0.22
7	Ukraine	0.22
8	Kazakhstan	0.22
9	Poland	0.17
10	Moldova	0.16

The Q1 2018 rating was much the same as the situation observed throughout 2017: Russia (0.74%) remained top. The US (0.65%) and Tajikistan (0.31%) took silver and bronze, respectively.

* Based by Kaspersky product users statistical data

IoT in Banks



One of the most important benefits of IoT in the banking sector is providing rewarding, easy-to-access services to both credit and debit card customers. Banks can analyse the usage of ATM kiosks in specific areas and increase / decrease the installation of ATMs depending on usage volumes. Along with ATMs, banks can also use IoT data in bringing on-demand services closer to customers by providing kiosks, and increase the accessibility of services to customers.

The customer data available through IoT will help banks identify their customers business needs, their value chain – like suppliers, retailers, distributers – and also gain customer insights. Customer information will also help banks provide value added services, financial assistance, and customized products to ensure a win win situation for both parties.

A survey found that 64.5% of global banking executives monitored their customers through mobile apps on smart phones, tablets and other digital devices. In addition, 31.6% of banking organizations used the IoT to monitor retail locations (e.g., bank branches), 21.1% used digital sensors to gather product performance data and 15.8% used IoT sensors in wearable's to track customer product usage.

Financial companies have prioritized customer and product monitoring in response to higher levels of online fraud, difficulty with identity verification and fears of hacked computer systems and networks. Banks are also using the IoT to monitor and collect data about their customers' financial transactions, while lenders are exploring ways to finance and track assets and value collateral based on sensor data.

More advanced IoT implementations include the ability to conduct basic banking using wearable's (smart watches or fitness bands) and voice-first devices (Amazon's Echo), the integration of invisible payments in transportation (Uber) and restaurants (Dine and Dash), and the leveraging of smart home appliances (Amazon Dash, Samsung Family Hub refrigerators).

Conclusion: Key actions ahead for Banks

□ Understand threats.

Just as the likelihood and impact of cybercrimes varies, so should the responses to them . In this effort, banks need to distinguish between financially motivated attacks and those that are non financial in nature.

□ Cooperate externally.

Banks are perceived as operating in silos, but greater external cooperation should enhance their cyber security efforts more broadly. Criminals often target weaker links in the banking Ecosystem, and it would be in the banks long-term interests to help third-party actors improve their own cyber security efforts .

□ Improve awareness.

Greater communication between the technical and business functions is necessary to improve cyber security within enterprises. By educating everyone from end users and employees to top management, banks must continue to improve educational efforts surrounding cyber security.

THANK YOU!

Questions?