KASPERSKY lab

APT

Advanced threats

Targeted Attack

Abnormal Behavior

Internal threats

OLTRE IL RANSOMWARE, SCOPRI TUTTE LE CRESCENTI E NUOVE MINACCE ALLA CYBERSECURITY

Gianfranco Vinucci
Head of Pre-Sales
Kaspersky Lab Italia

FACTS ABOUT US

Essentials

Founded in **1997** and led by Eugene Kaspersky

Present on **5** continents in **200** countries and territories

Provides **innovative** IT security solutions for business and consumers

Numbers

>20 million product activations per year

~3,300 highly qualified specialists

619 million USD — global unaudited revenue in 2015*
+13% — YOY growth in local currencies

Achievements

One of the four biggest endpoint security vendors**

"Leader" according to the **Gartner Magic Quadrant*****

Our solutions are the **most tested and most awarded** in independent tests and reviews****

> 400,000,000 users worldwide are protected by our technologies

* According to International Financial Reporting Standards (IFRS)
** Worldwide Endpoint Security Market Shares, 2014: Success of Midsize Vendors (IDC # US40546915, December 2015)
*** Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Eric Ouellet, 01 February 2016
****kaspersky.com/top3

TRENDS AND THREATS

We understand global **IT trends** and the **threats** they bring

Privacy & data protection challenge

Consumerization & mobility

Increasing online commerce

Internet of Things

Cloud & virtualization

Critical infrastructure at risk

Big data

Fragmentation of the Internet

Merger of cybercrime and APTs

Malware for ATMs

Supply chain attacks

Decreasing cost of APTs

Targeted attacks

Commercialization of APTs

Hacktivism

Internet of Things

Mobile threats

Online banking at risk

Massive data leaks

Targeting hotel networks

Cyber-mercenaries

“Wipers” & cyber-sabotage

Ransomware programs

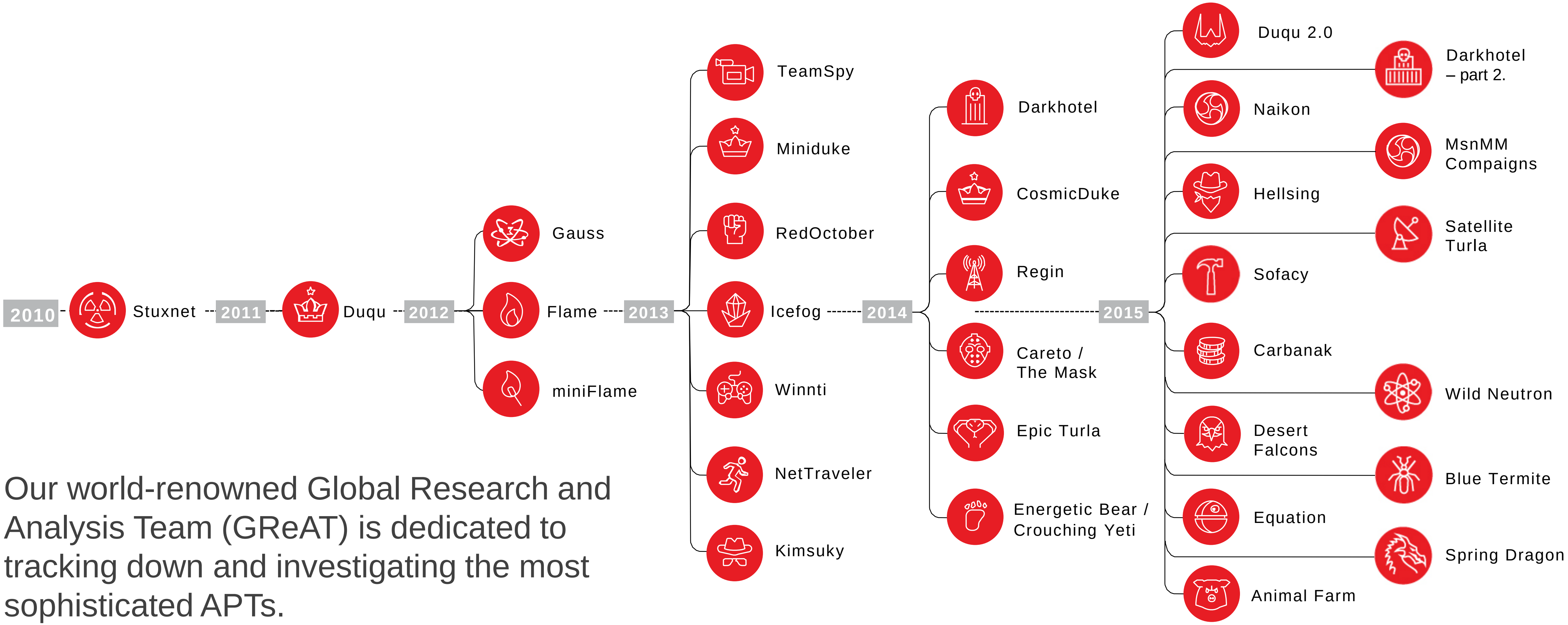
Financial phishing attacks

Attacks on PoS terminals

Threats to Smart Cities

TRANSFORMING EXPERTISE INTO PROTECTION

At Kaspersky Lab we have a proven track record in identifying the most advanced threats and implementing protection against them in our solutions. Such intelligence is the key building block of our new solution to detect targeted attacks.



2010 Stuxnet

2011 Duqu

2012 Gauss, Flame, miniFlame

2013 TeamSpy, Miniduke, RedOctober, Icefog, Winnti, NetTraveler, Kimsuky

2014 Darkhotel, CosmicDuke, Regin, Careto / The Mask, Epic Turla, Energetic Bear / Crouching Yeti

2015 Duqu 2.0, Darkhotel – part 2., Naikon, MsnMM Compaigns, Hellsing, Satellite Turla, Sofacy, Carbanak, Wild Neutron, Desert Falcons, Blue Termite, Equation, Spring Dragon, Animal Farm

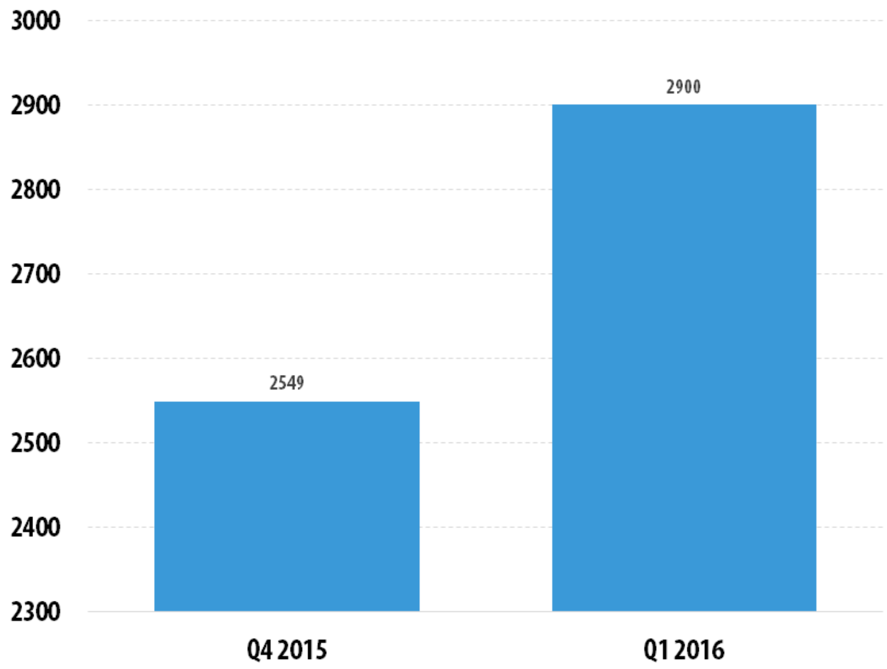
- Our world-renowned Global Research and Analysis Team (GReAT) is dedicated to tracking down and investigating the most sophisticated APTs.

MALWARE INCIDENTS

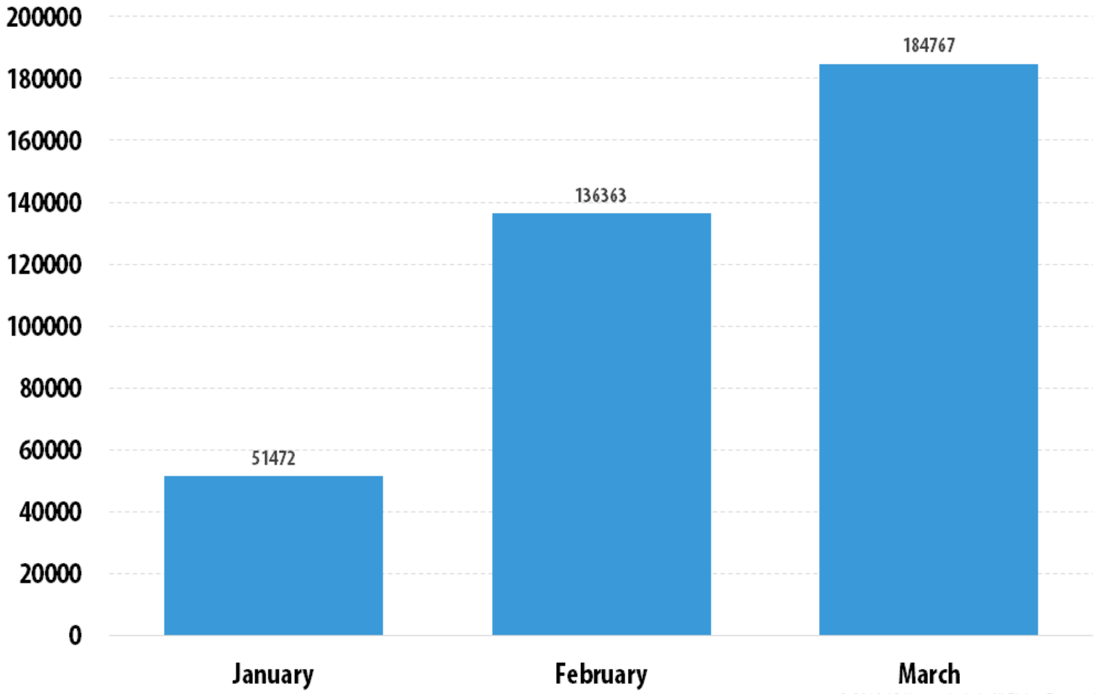
RANSOMWARE

- The overall number of encryptor modifications in our Virus Collection to date is at least 15,000. Nine new encryptor families and 2,900 new modifications were detected in Q1.

- In Q1 2016, 372,602 unique users were attacked by encryptors, which is 30% more than in the previous quarter. Approximately 17% of those attacked were in the corporate sector.



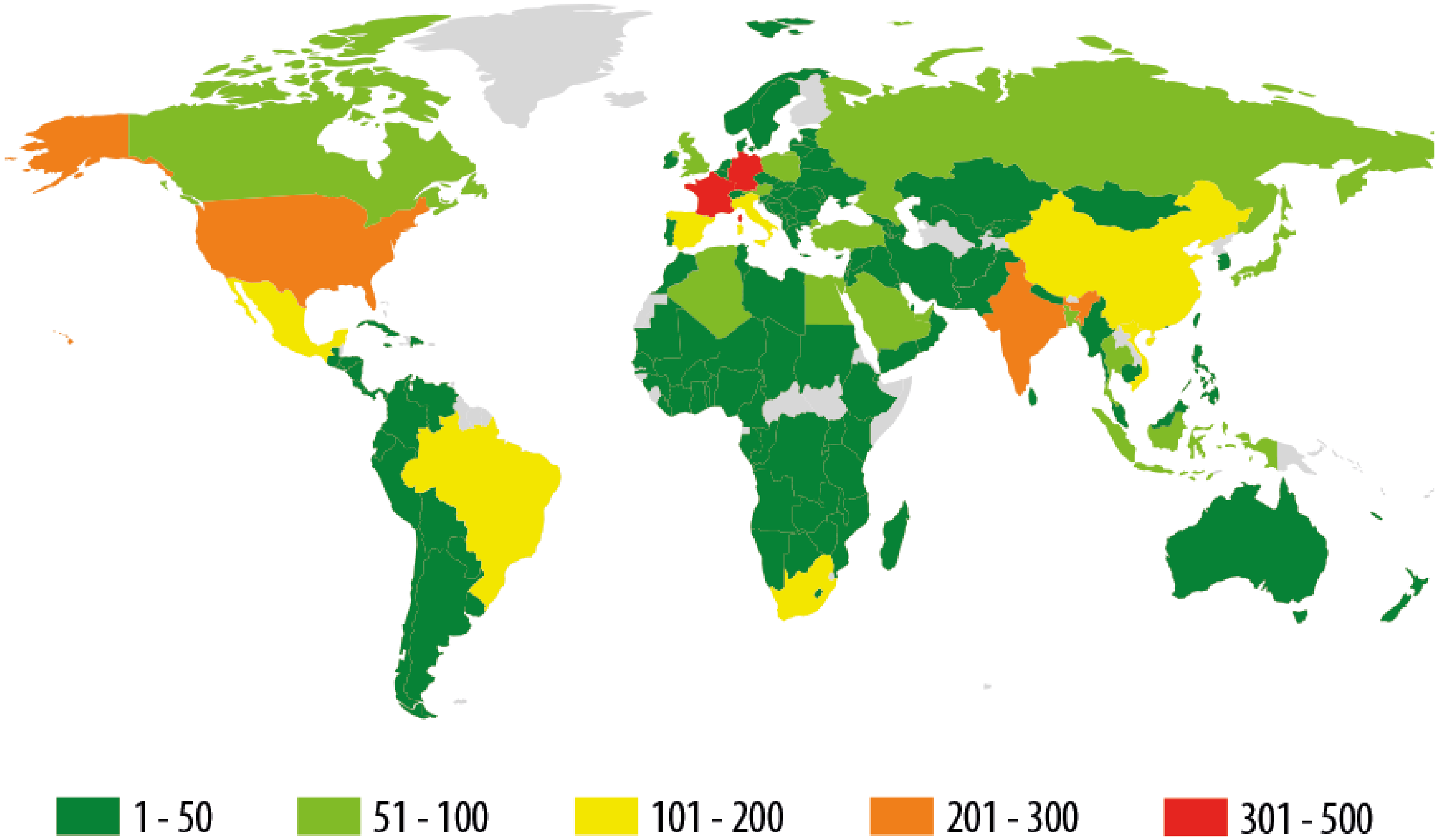
Number of ransomware samples in our collection



Number of users attacked by ransomware

RANSOMWARE – LOCKY

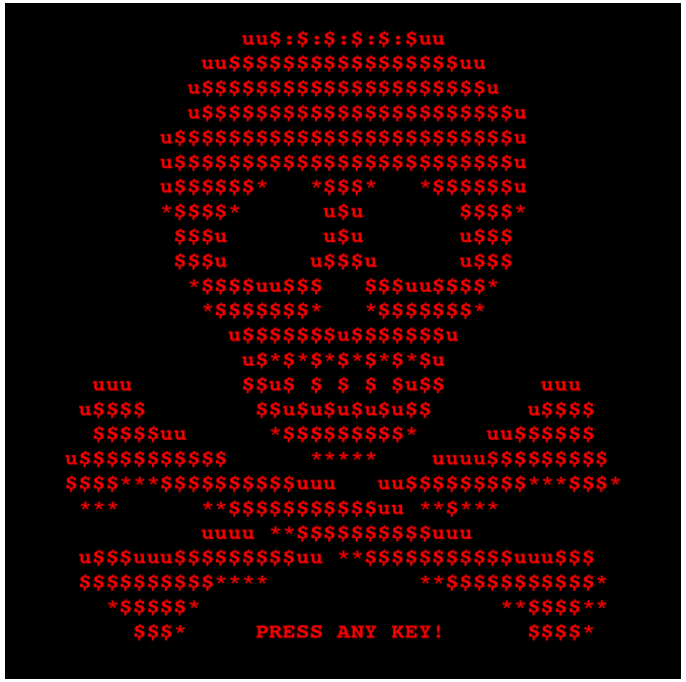
- The biggest crypto epidemic of Q1 2016 was caused by the ransomware Trojan Locky.
- Kaspersky Lab products have recorded attempts to infect users in 114 countries around the world.



RANSOMWARE – PETYA

- The most significant technical innovation in ransomware was **full disk encryption** rather than file encryption. This trick was used by the Petya Trojan.

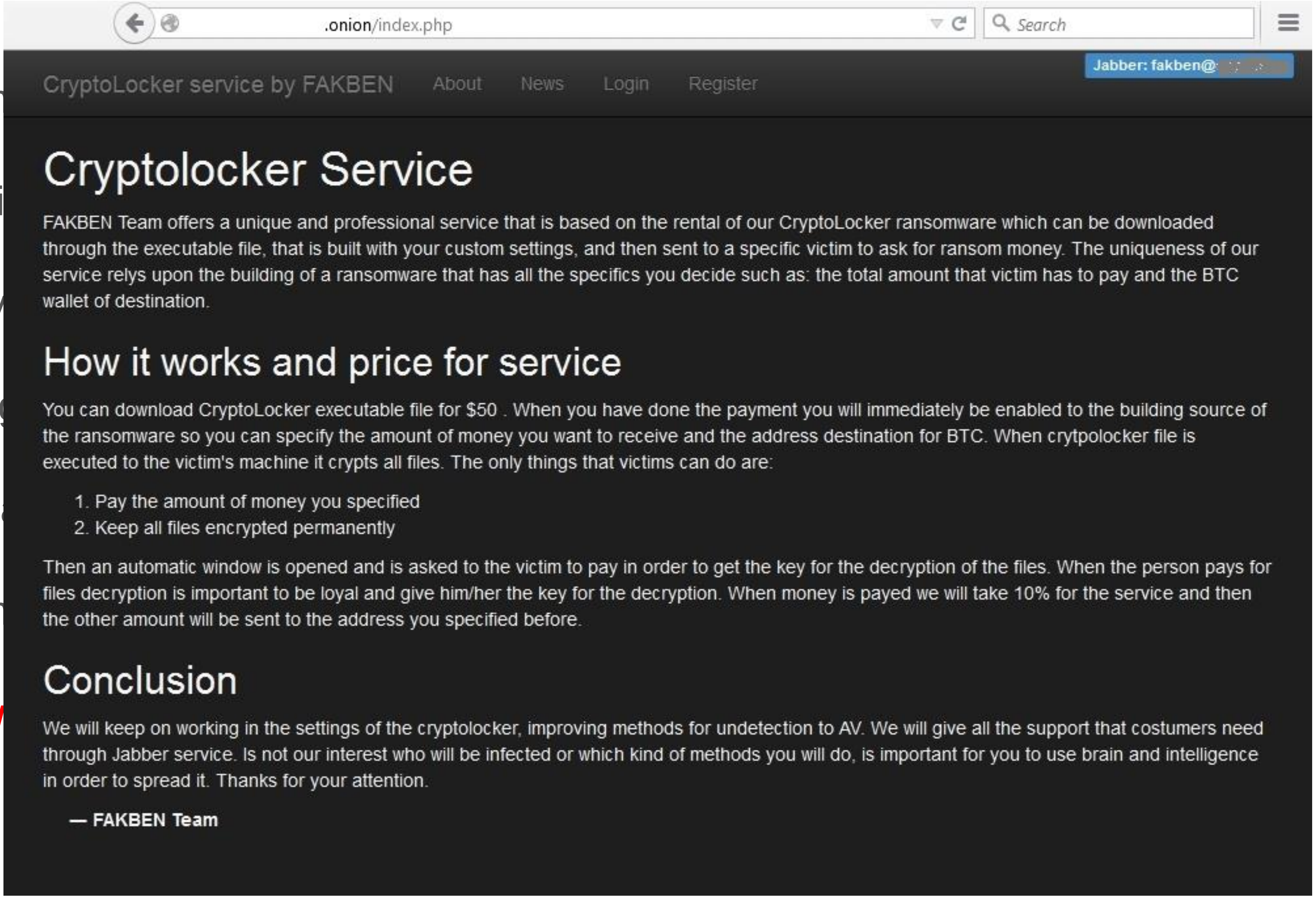
- After encrypting the main file table, Petya shows its true face – a skull and crossbones composed of ASCII characters. Then the typical encryptor routine begins: the Trojan demands a ransom from the victim, 0.9 Bitcoin (about $380) in this case.



```
             uu$:$:$:$:$:$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$u$u$u$u$u$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$      *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

RANSOMWARE - FACTS

- Ransom
- Script-ki
- Used by
- New tar
- Never p
- Ransom
- **Cryptow**



Cryptolocker Service

FAKBEN Team offers a unique and professional service that is based on the rental of our CryptoLocker ransomware which can be downloaded through the executable file, that is built with your custom settings, and then sent to a specific victim to ask for ransom money. The uniqueness of our service relys upon the building of a ransomware that has all the specifics you decide such as: the total amount that victim has to pay and the BTC wallet of destination.

How it works and price for service

You can download CryptoLocker executable file for $50 . When you have done the payment you will immediately be enabled to the building source of the ransomware so you can specify the amount of money you want to receive and the address destination for BTC. When crytpolocker file is executed to the victim's machine it crypts all files. The only things that victims can do are:

1. Pay the amount of money you specified
2. Keep all files encrypted permanently

Then an automatic window is opened and is asked to the victim to pay in order to get the key for the decryption of the files. When the person pays for files decryption is important to be loyal and give him/her the key for the decryption. When money is payed we will take 10% for the service and then the other amount will be sent to the address you specified before.

Conclusion

We will keep on working in the settings of the cryptolocker, improving methods for undetection to AV. We will give all the support that costumers need through Jabber service. Is not our interest who will be infected or which kind of methods you will do, is important for you to use brain and intelligence in order to spread it. Thanks for your attention.

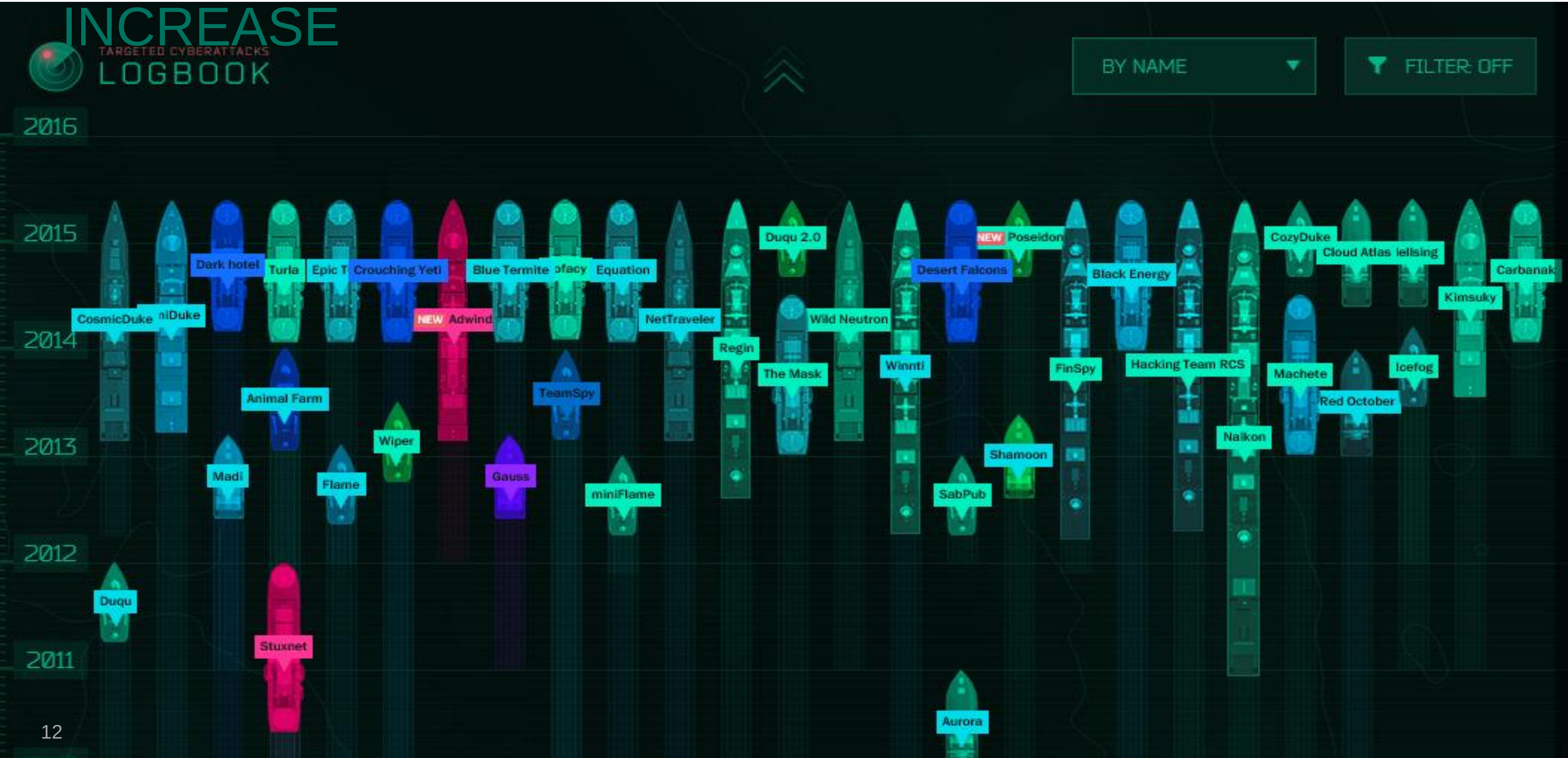
— **FAKBEN Team**

RANSOMWARE – HOW TO PROTECT

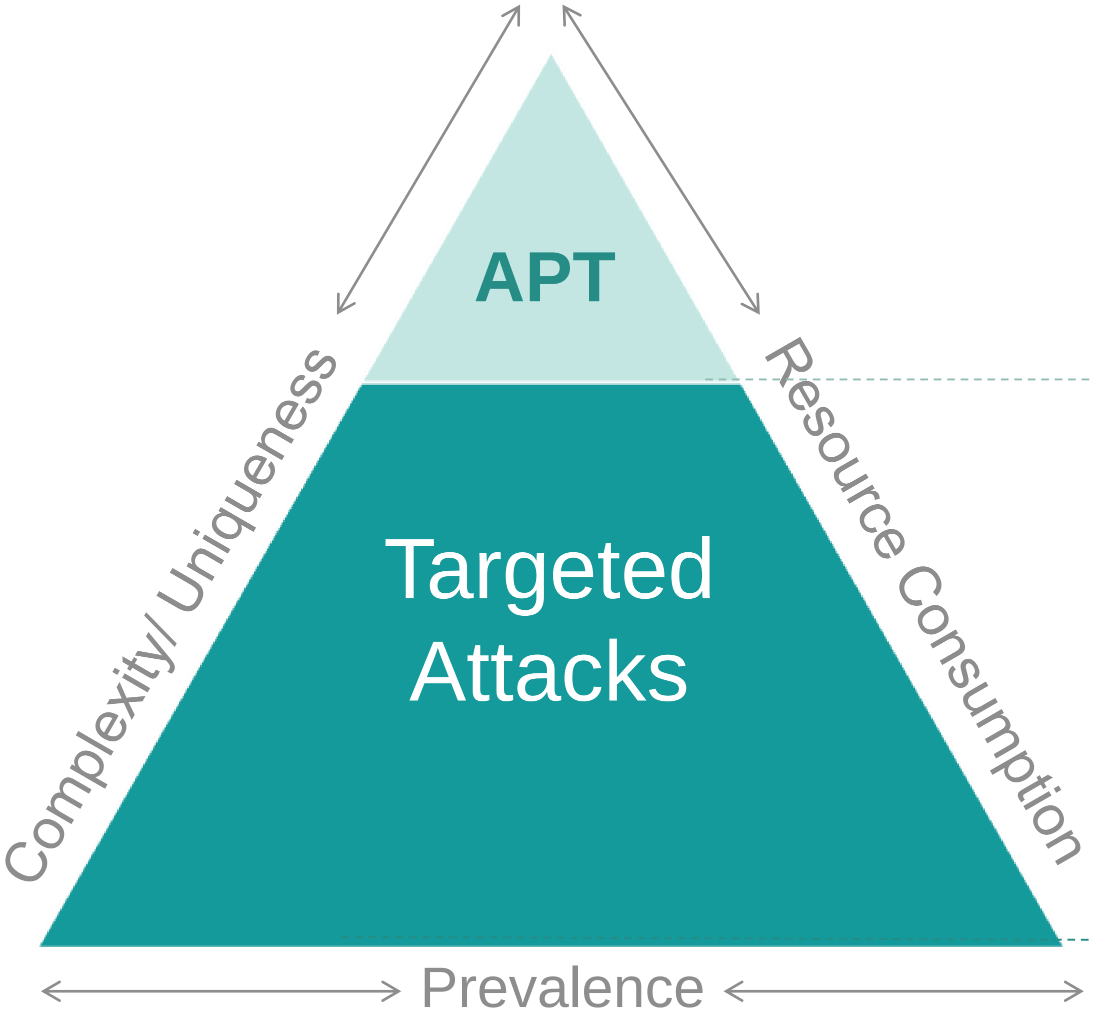
- Educate your users
- Multi-layered security solutions
  - Kaspersky System Watcher & Privilege Control
  - Kaspersky Anti-cryptor
  - Kaspersky Automatic Exploit Prevention (AEP)
  - Vulnerability Assessment and Patch Management
- Regularly backup data
- Protect all devices

TARGETED ATTACKS

TARGETED ATTACKS AND APTS SEE A STRONG INCREASE



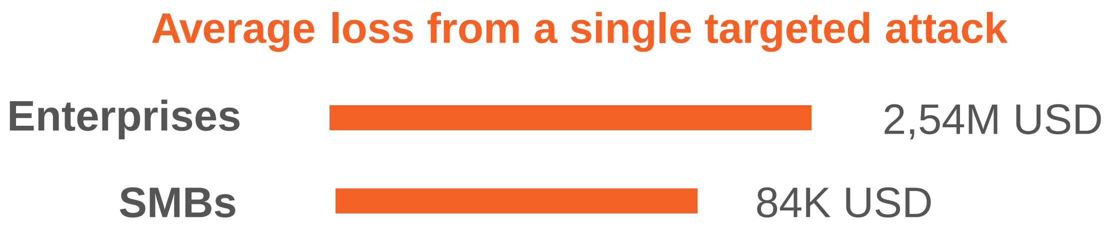
APTS AND TARGETED ATTACKS: WHAT’S THE DIFFERENCE?



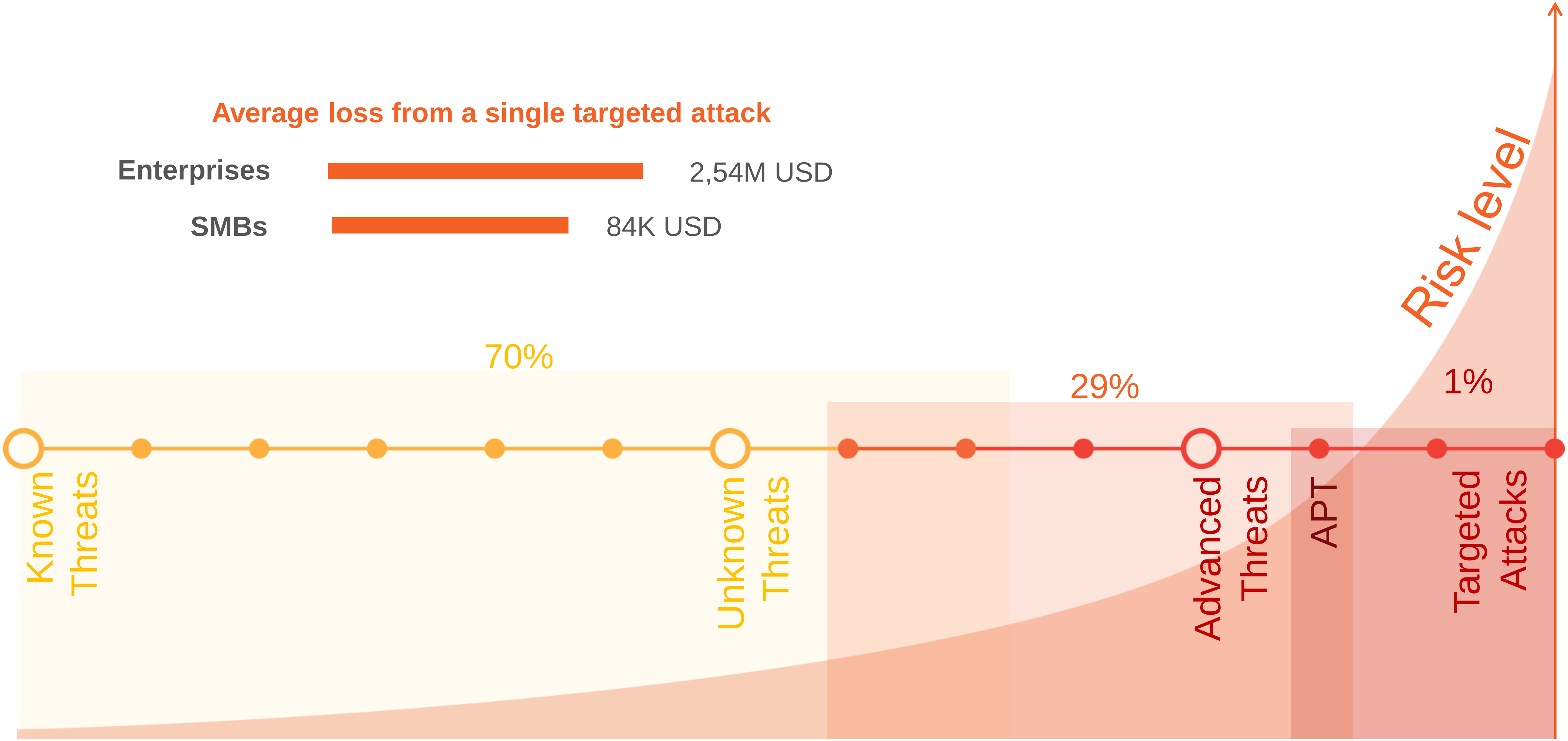
Scary, but expensive and exclusive

Much more common, but no less damaging

1% BRINGS HIGH RISK AND HIGH LOSSES



Average loss from a single targeted attack



* Based on Corporate IT Security Risks Survey, 2015, conducted by Kaspersky Lab and B2B International. Indicates an average loss from a single targeted attack, including direct losses and additional spend required to recover from an attack.

KASPERSKY lab

TARGETED ATTACKS – BLACK ENERGY

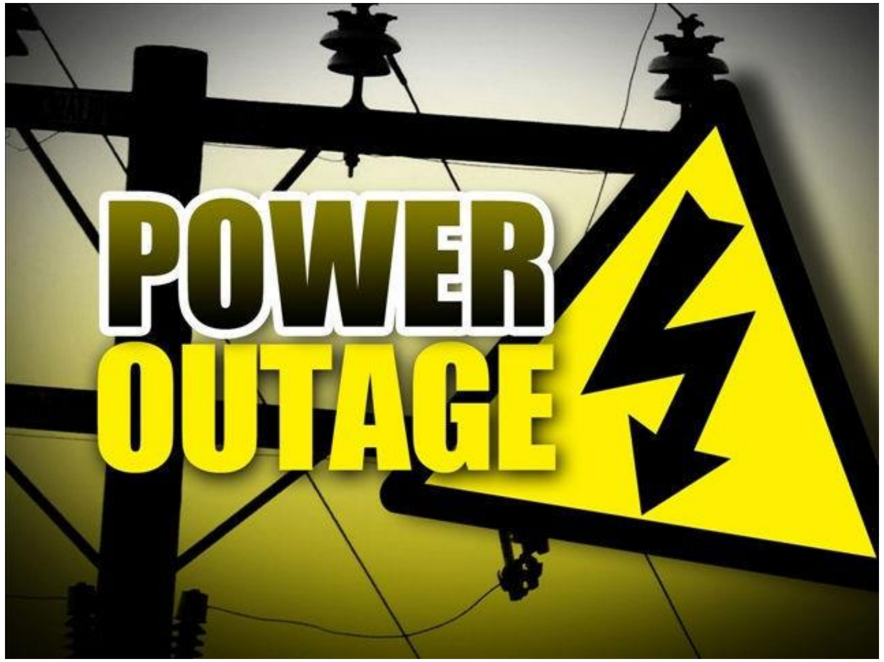
The BlackEnergy cyberattack on the Ukrainian energy sector was the most high-profile incident.

The attack was unique because of the damage it caused

- the hackers managed to disable the power distribution system in Western Ukraine

- launch the Wiper program on the targeted systems

- carry out a telephone DDoS on the technical support services of the affected companies.



Poseidon's Targeted Attacks Malware Boutique

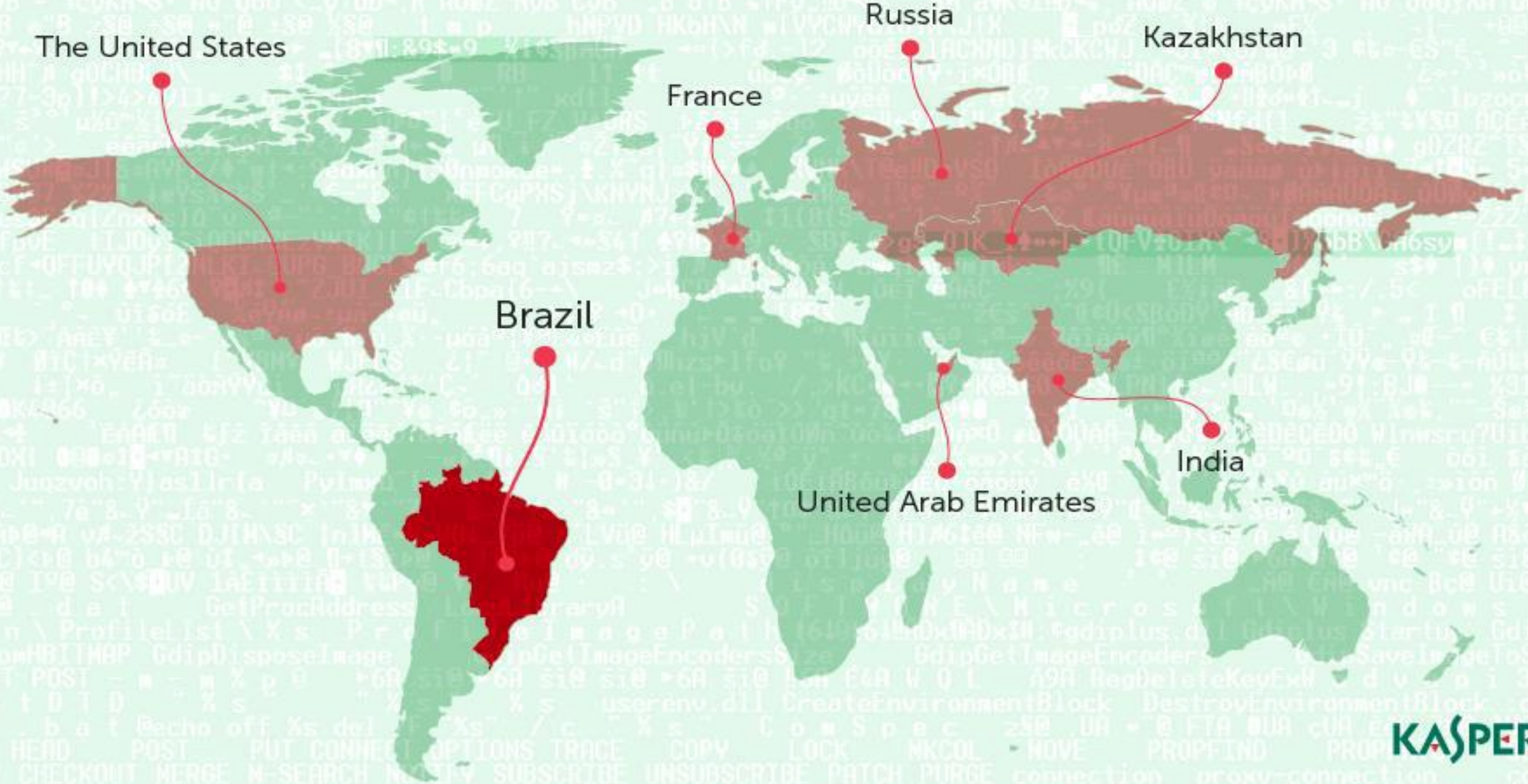
The targets of the Poseidon cyberespionage group

- Energy and utilities
- Financial institutions
- Governmental
- Public relations and media
- Manufacturing
- Natural resources
- Services

English and Portuguese.

The first ever Brazilian Portuguese speaking targeted attack campaign

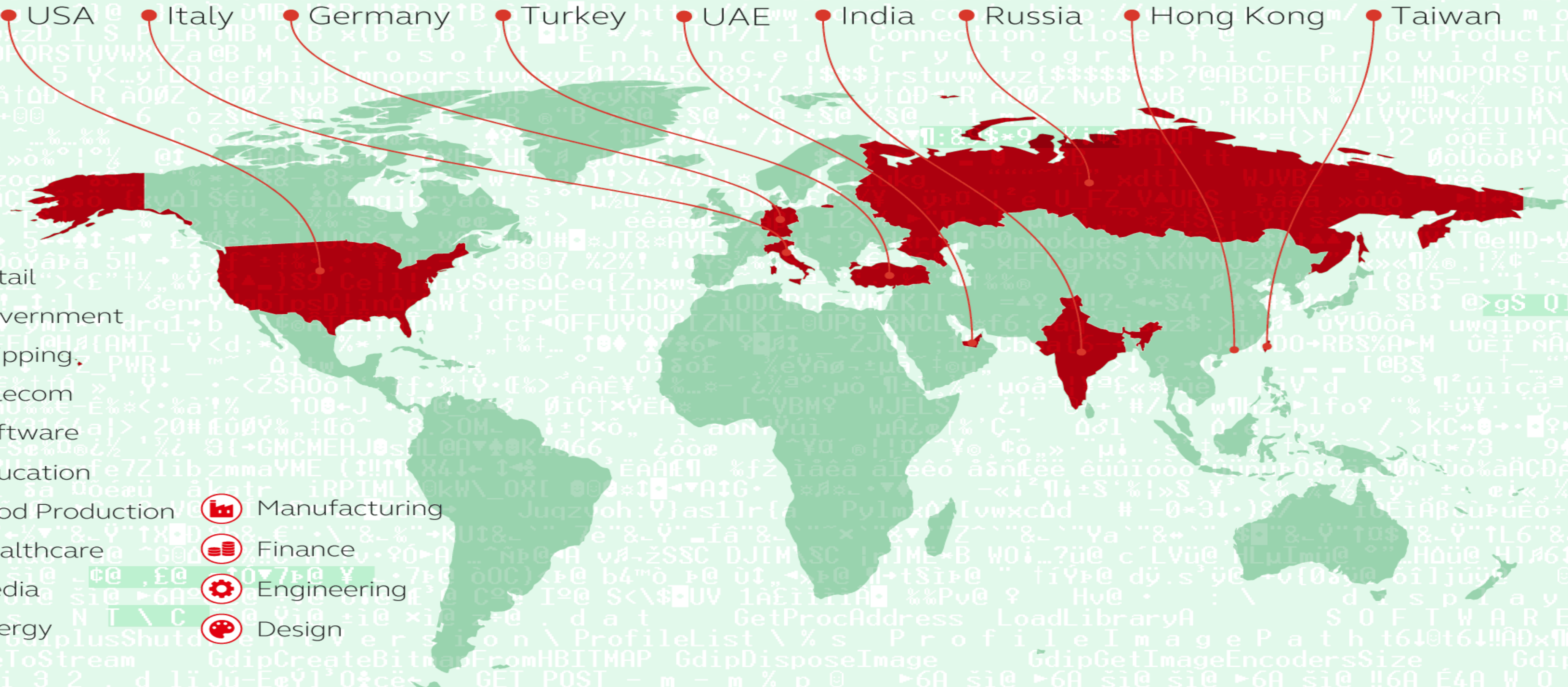
Evolving their toolkit since at least 2005, active at this time



Targets of Adwind Malware-as-a-Service Platform

During their investigation, Kaspersky Lab researchers were able to analyze nearly 200 examples of spear-phishing attacks organized by unknown criminals to spread the Adwind malware.

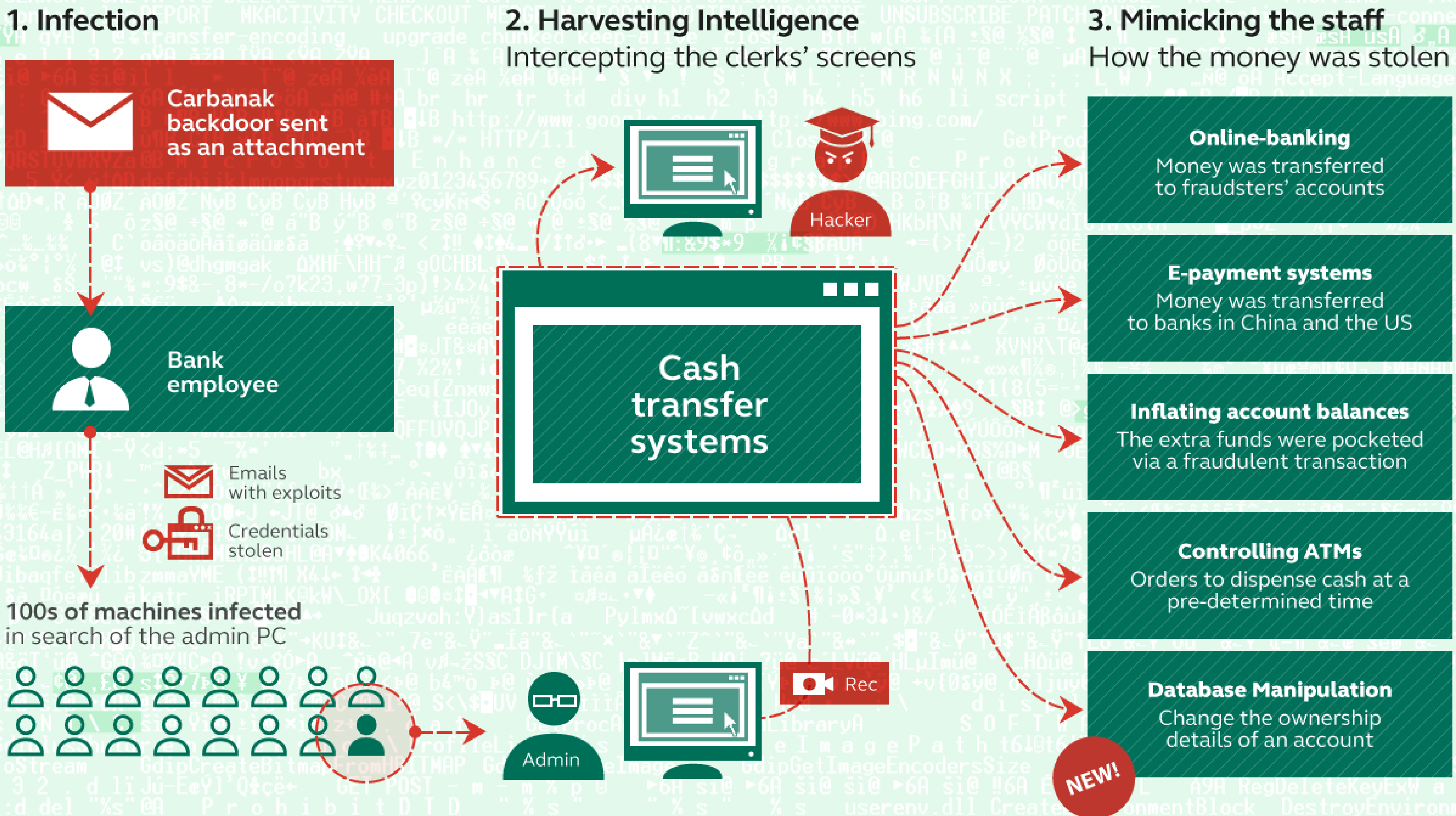
Based on information from Kaspersky Security Network, between August 2015 and January 2016 more than **68,000** users encountered Adwind RAT malware samples as a result of those 200 attacks.



- Retail
- Government
- Shipping
- Telecom
- Software
- Education
- Food Production
- Healthcare
- Media
- Energy
- Manufacturing
- Finance
- Engineering
- Design

* Top 10 most frequently attacked countries during August 2015 to January 2016

How the Carbanak cybergang targets financial organizations



1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected
in search of the admin PC

Admin

2. Harvesting Intelligence

Intercepting the clerks' screens

Hacker

Cash transfer systems

Rec

3. Mimicking the staff

How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

Inflating account balances
The extra funds were pocketed via a fraudulent transaction

Controlling ATMs
Orders to dispense cash at a pre-determined time

Database Manipulation
Change the ownership details of an account

NEW!

ENTERPRISE SECURITY TRENDS: EXTERNAL FACTORS

Most advanced threats using basic vulnerabilities and human factor

Availability and lowering prices leading to Cybercrime-as-a-Service

Attacks on third-party: SMBs can become a part of an attack chain

ENTERPRISE SECURITY TRENDS: INTERNAL FACTORS

Growing IT sophistication results in visibility gap and lack of operational information

An average targeted attack stays undetected for more than 214 days

Perimeter security is overestimated

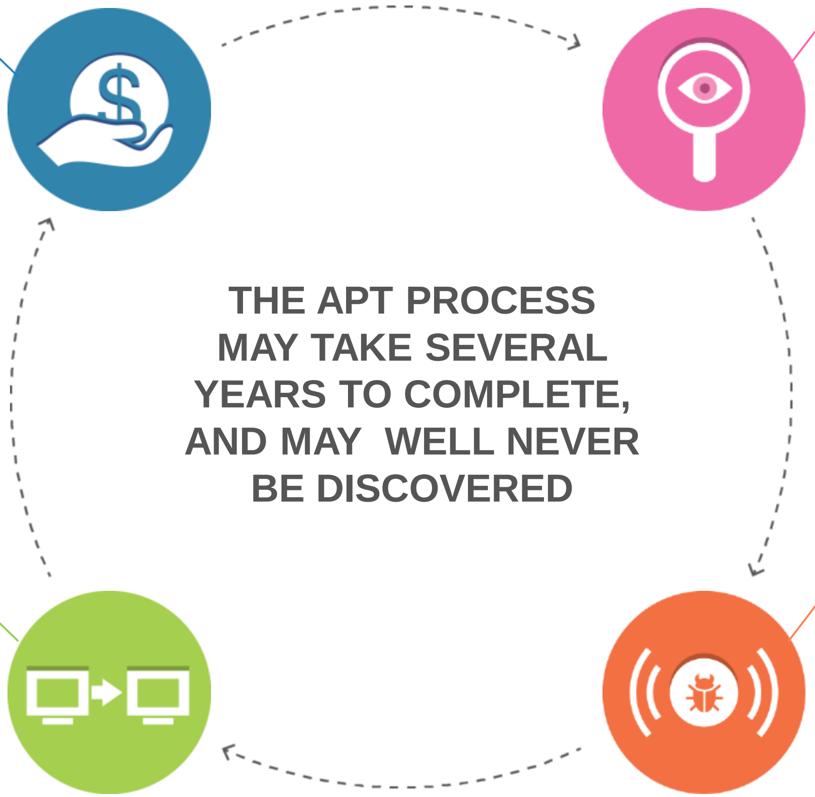
TARGETED ATTACK IS NOT A ‘ONE-OFF’ OFFENSIVE: IT’S AN ONGOING PROCESS

EXFILTRATE

- Stay dormant
- Extract data
- Cover Tracks
- Leave quietly

PREPARE

- Research target
- Create strategy
- Build a toolset



THE APT PROCESS MAY TAKE SEVERAL YEARS TO COMPLETE, AND MAY WELL NEVER BE DISCOVERED

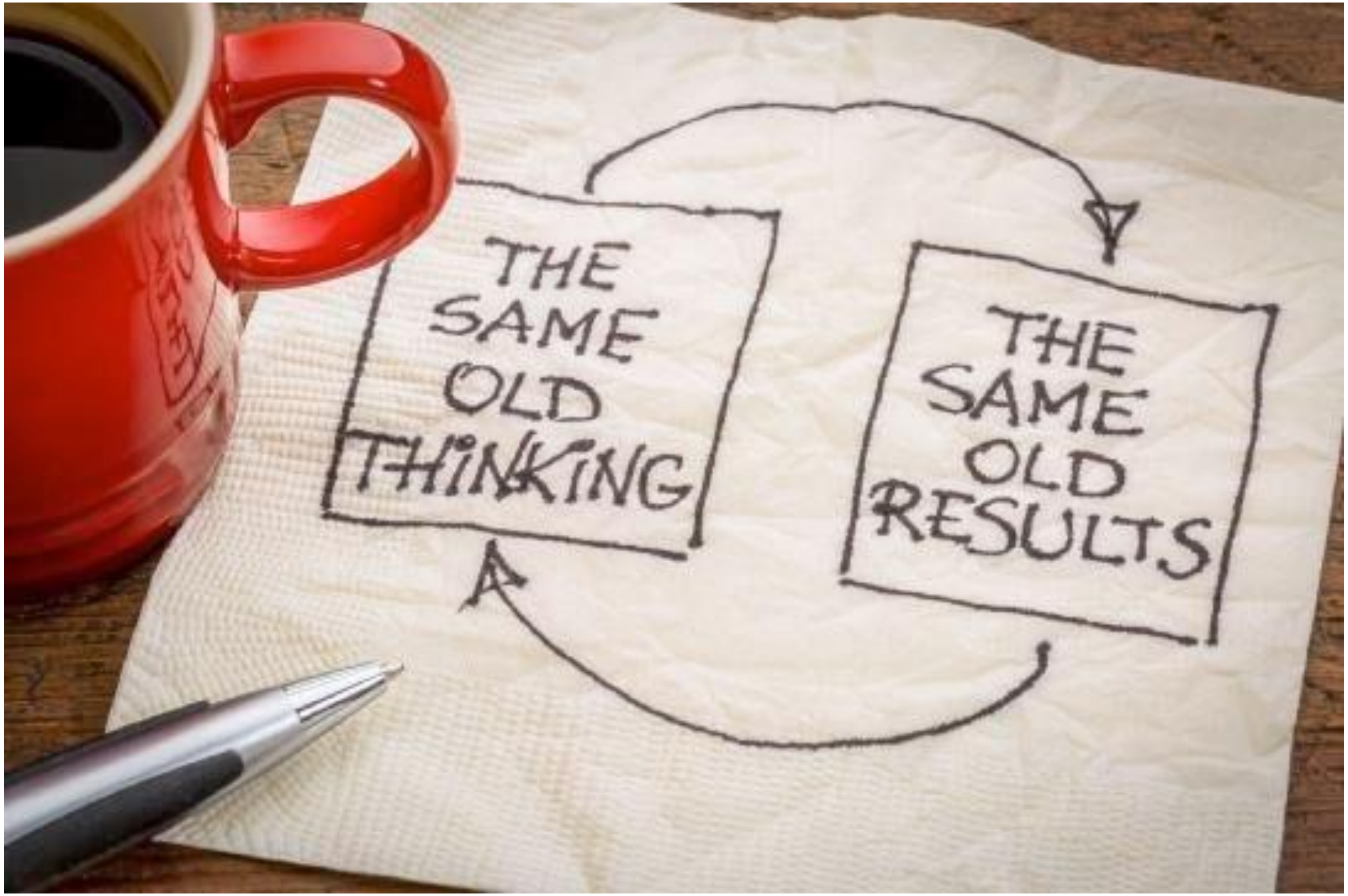
EXPAND ACCESS

- Obtain credentials
- Raise privileges
- Establish links
- Move laterally
- Take control

INFECT

- Leverage weaknesses
- Penetrate the perimeter

HOW TO **NOT** ADDRESS THE ISSUE OF TARGETED ATTACKS



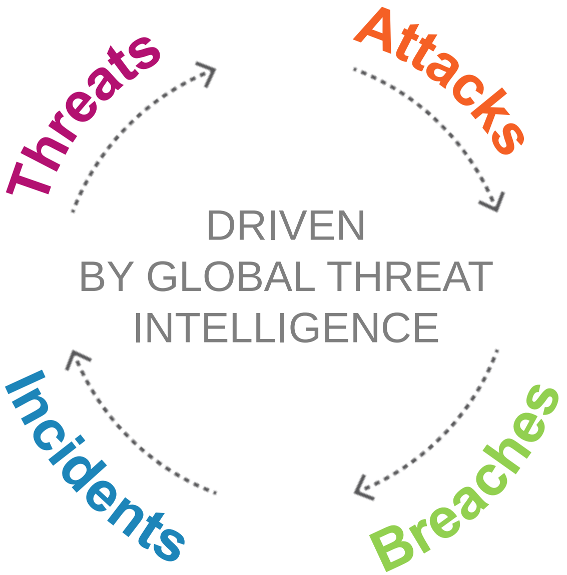
HOW TO ADDRESS THE ISSUE OF TARGETED ATTACKS

SMART PREDICT

- Analyze the potential security gaps
- Adjust countermeasures accordingly
- (if not already done) create a dedicated SOC

PREVENT MULTI-LAYERED

- Mitigate the risks
- Raise the threat awareness
- Implement the right approaches to mitigate potential risk with existing solutions



Threats

Attacks

Breaches

Incidents

DRIVEN
BY GLOBAL THREAT
INTELLIGENCE

EFFECTIVE RESPOND

- Analyze the incident
- Take immediate steps to mitigate the consequences

DETECT VIGILANT

- Discover of the incident
- Track its immediate source
- Understand its nature

BUILDING AN ADAPTIVE ENTERPRISE SECURITY STRATEGY

PREDICT

KNOW YOURSELF:

- Penetration testing service
- Security assessment service
- **Targeted Attack Discovery Service**

PREVENT

TRAIN:

- Cybersecurity training

PROTECT:

- Kaspersky Lab Enterprise security solutions

EDUCATE:

- Cyber-safety Games
- Threat simulation

DETECT

EXPERTISE:

- **Targeted Attack Investigation Training**

THREATS LANDSCAPE:

- APT reporting
- Botnet tracking
- Threat data feeds

SOLUTION:

- **Kaspersky Anti Targeted Attack Platform**

RESPOND

REACTION:

- **Incident response service**

INVESTIGATE:

- Malware analysis service
- Digital forensics services

KASPERSKY lab

TARGETED ATTACK DEMO

APT

Advanced th

Kaspersky Anti Targeted Attack Platform

Abnormal Behavior

Stage I

Attack

GRAZIE

Gianfranco Vinucci

Head of Pre-Sales

Kaspersky Lab Italia