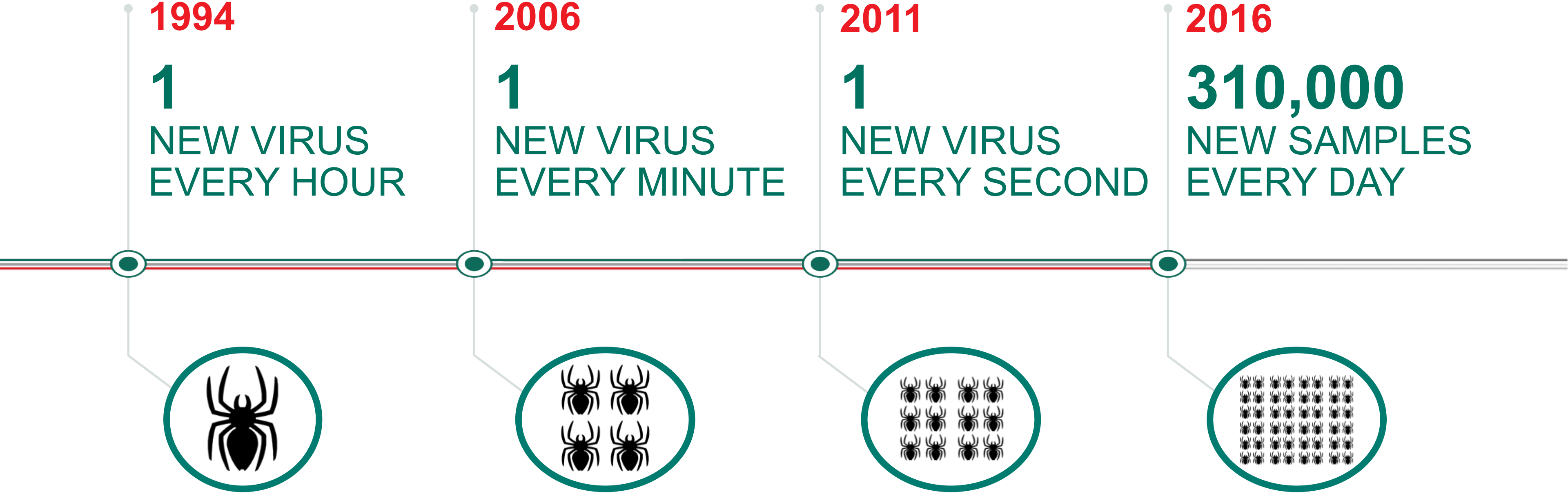
CYBER THREATS DISCOVERED BY KASPERSKY LAB

Andis Šteinmanis, Managing Director, Kaspersky Lab Baltic

MALWARE EVOLUTION

Looking Back: 20 Years of Malware Evolution

THE SCALE OF THE THREAT



1994

1

NEW VIRUS
EVERY HOUR

2006

1

NEW VIRUS
EVERY MINUTE

2011

1

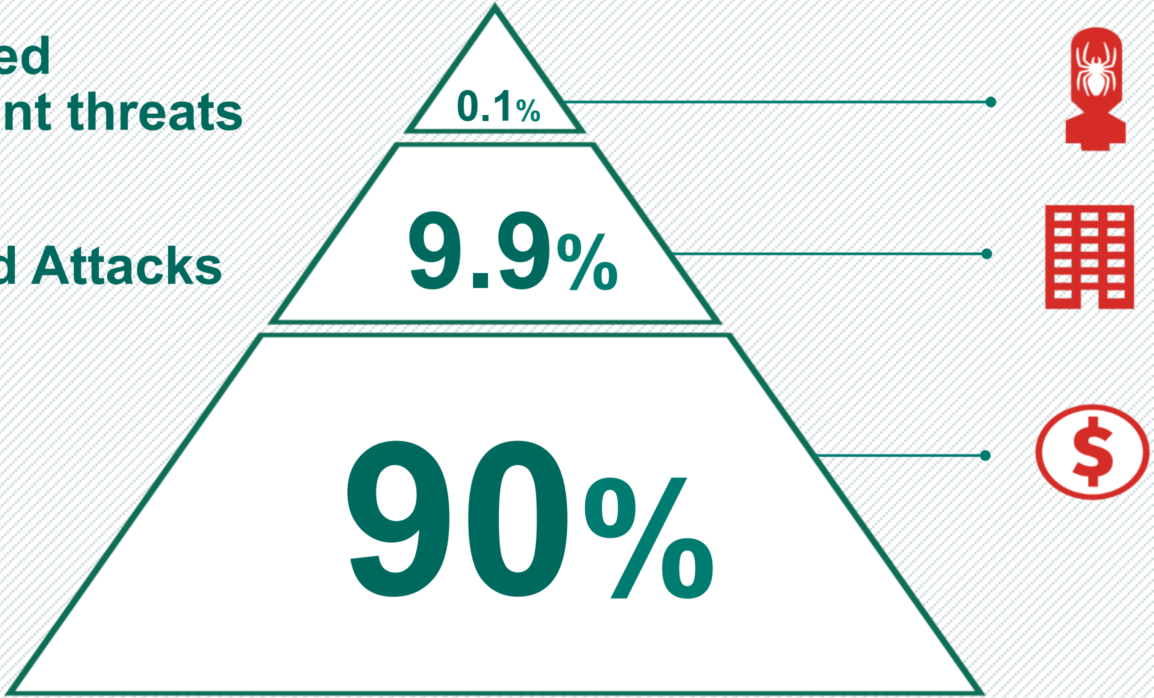
NEW VIRUS
EVERY SECOND

2016

310,000

NEW SAMPLES
EVERY DAY

THE NATURE OF THE THREAT



Advanced persistent threats

Targeted Attacks

0.1%

9.9%

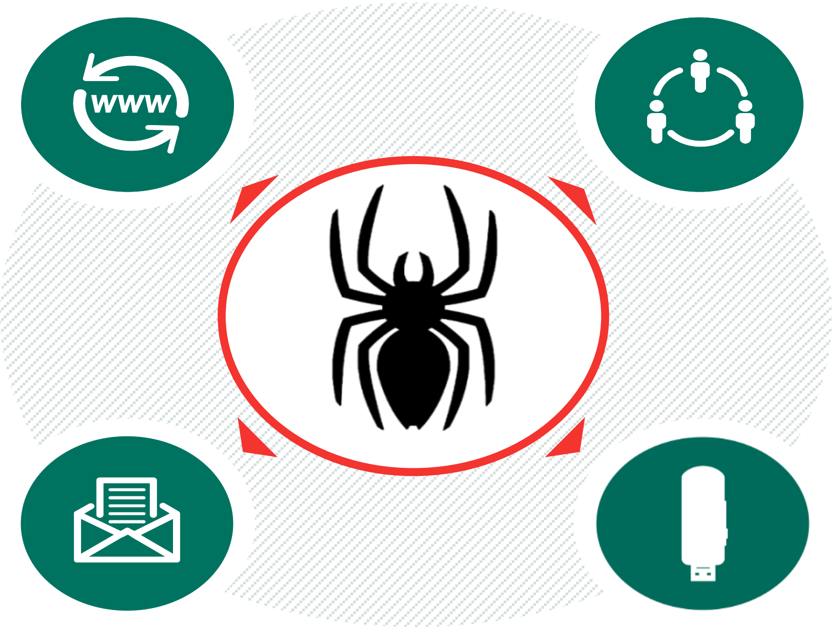
90%

Cyber-weapons

Targeted threats to organisations

Traditional cybercrime

HOW MALWARE SPREADS



Exploit kits

Social networks

Email

USB

GREAT – GLOBAL RESEARCH & ANALISYS TEAM

GREAT

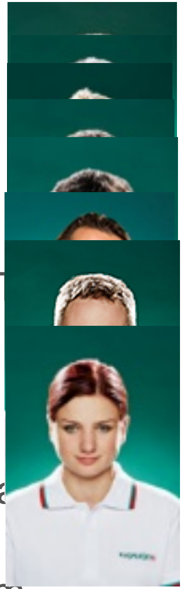
- **Costin Raiu** - Director, Global Research & Analysis Team
- Sergey Novikov – Deputy Director, Global Research & Analysis Team
- Ryan Narayne - Director, Global Research & Analysis Team, US
- Dmitry Bestuzhev - Director, Global Research & Analysis Team, Latin Amer
- Marco Preuss - Director, Global Research & Analysis Team, Europe
- Vitaly Kamluk - Director, Global Research & Analysis Team, APAC
- Alex Gostev - Chief Security Expert, Global Research & Analysis Team
- David Emm, Principal Security Researcher, Global Research & Analysis Team

GREAT

- Nicolas Brulez- Principal Security Researcher, Global Research & Analysis Team
- Vicente Diaz – Principal Security Researcher, Global Research & Analysis Team
- Kurt Baumgartner - Principal Security Researcher, Global Research & Analysis Tean
- Sergey Golovanov - Principal Security Researcher, Global Research & Analysis Tea
- Igor Soumenkov - Principal Security Researcher, Global Research & Analysis Team
- Roberto Martinez - Principal Security Researcher, Global Research & Analysis Team
- Christian Funk - Head of Global Research and Analysis Team (GReAT), DACH
- Dirk Kollberg, Senior Security Researcher, Global Research & Analysis Team

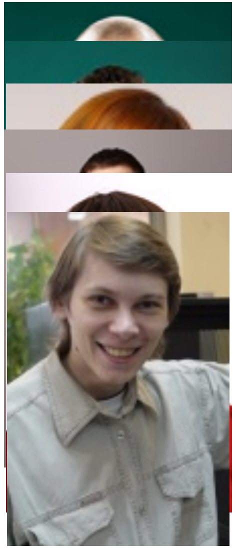
GREAT

- Fabio Assolini - Senior Security Researcher, Global Research & Analysis Team
- Juan Andrés Guerrero-Saade - Senior Security Researcher, Global Research & Analysis T
- Stefan Tanase - Senior Security Researcher, Global Research & Analysis Team
- Ghareeb Saad Muhammad - Senior Security Researcher, Global Research & Analysis Tea
- Mohammad Amin Hasbini - Senior Security Researcher, Global Research & Analysis Team
- Sergey Lozhkin - Senior Security Researcher, Global Research & Analysis Team
- Jornt van der Wiel - Senior Security Researcher, Global Research & Analysis Team
- Marta Janus , Senior Security Researcher, Global Research & Analysis Team



GREAT

- Santiago Pontiroli - Senior Security Researcher, Global Research & Analysis Team
- Stefan Ortloff - Senior Security Researcher, Global Research & Analysis Team
- Darya Loseva - Head of Content Analysis & Research
- Vyacheslav Zakorzhevsky - Head of Anti-Malware Team, Kaspersky Lab
- Mikhail Pavlyushchik - Security Expert, Anti-Malware Research, USA
- Oleg Zaitsev – Security expert

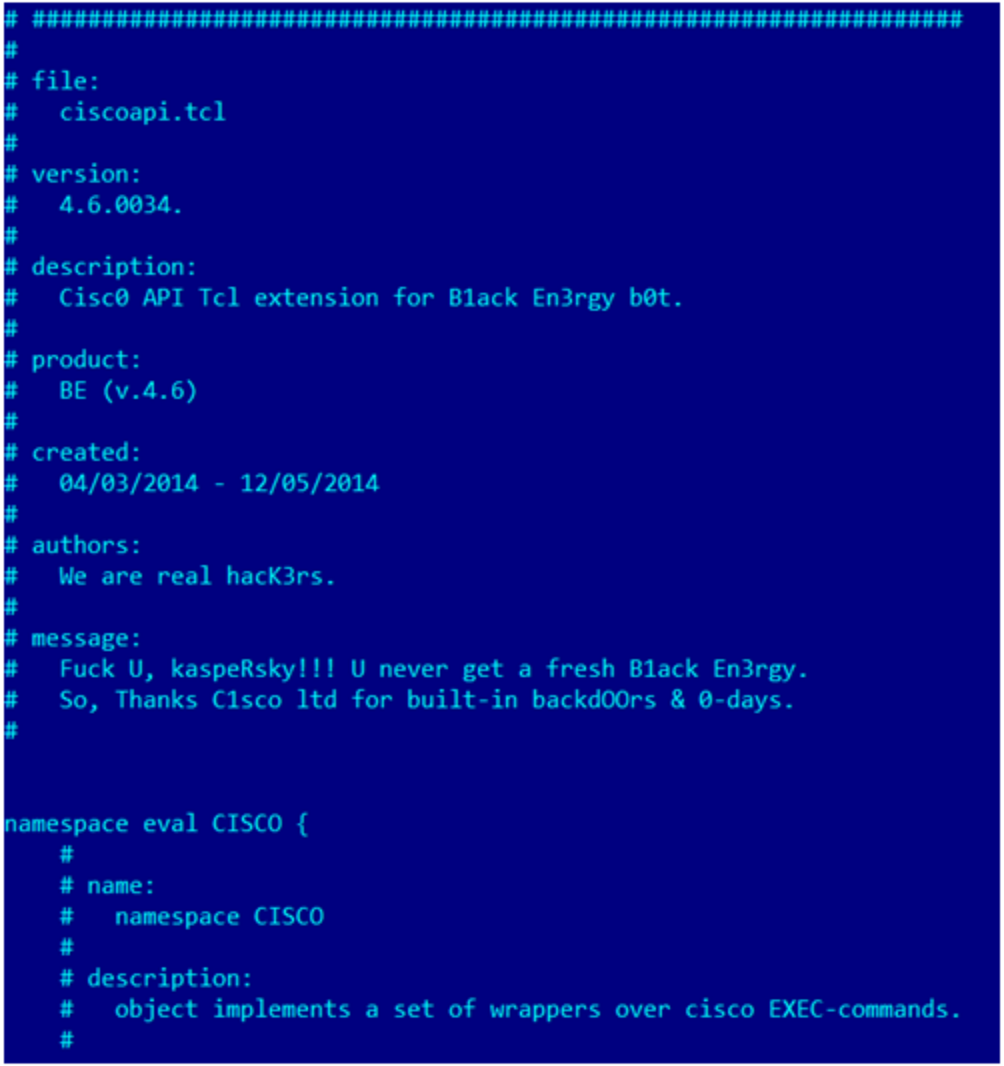


DISCOVERED IN 2015-2016

TARGETED /

The BlackEnergy cy
st high-profile
incident. Although it
it happened only
appeared in the cou
/ cybercriminals to
arrange new attacks

The attack was uniq
anaged to disable
the power distributio
am on the targeted
systems and carry o
s of the affected
companies.



```
# ####################################################################
#
# file:
#   ciscoapi.tcl
#
# version:
#   4.6.0034.
#
# description:
#   Cisc0 API Tcl extension for B1ack En3rgy b0t.
#
# product:
#   BE (v.4.6)
#
# created:
#   04/03/2014 - 12/05/2014
#
# authors:
#   We are real hacK3rs.
#
# message:
#   Fuck U, kaspeRsky!!! U never get a fresh B1ack En3rgy.
#   So, Thanks C1sco ltd for built-in backd0Ors & 0-days.
#


namespace eval CISCO {
    #
    # name:
    #   namespace CISCO
    #
    # description:
    #   object implements a set of wrappers over cisco EXEC-commands.
    #
```

TARGETED ATTACKS – POSEIDON

Poseidon – the first Portuguese-speaking targeted attack group which had set up a custom-tailored malware boutique.

Although the report was only released in 2016, the group has been operational for a long time. Malware campaigns that were most probably supported by Poseidon were detected as far back as 2005, while the first sample dates back to 2001.

Having gained access to the corporate network, the criminals move across the network and collect as much data as possible in order to escalate their privileges, create a network map and to identify the computer they need. The main target of the attack is usually the local Windows domain controller. Once they have control over it, the attackers can steal intellectual property, data, trade secrets, and other valuable information.

The information collected by Poseidon for its owners was in most cases used to blackmail victim companies into contracting the Poseidon Group as a security firm. Regardless of whether a contract was signed, Poseidon remained on the network.

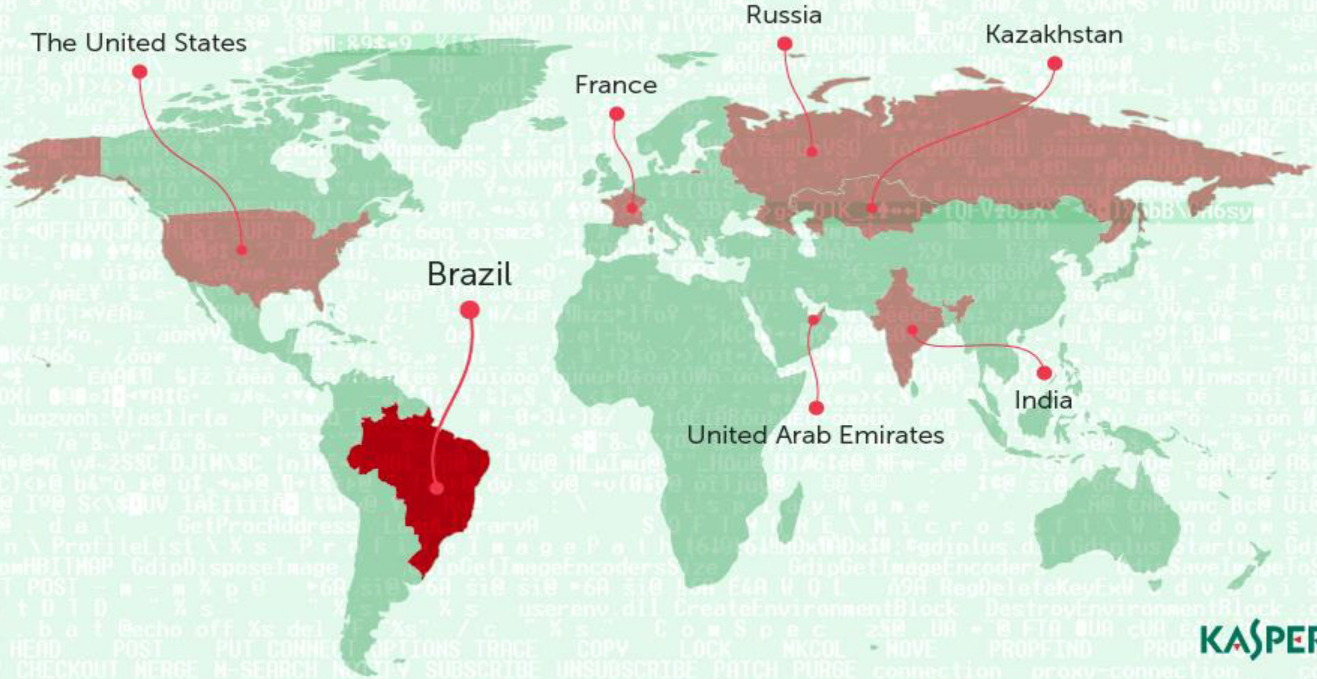
Poseidon's Targeted Attacks Malware Boutique

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

KASPERSKY lab

TARGETED ATTACKS – ADWIND MALWARE-AS-A-SERVICE

The Trojan was developed continuously over several years, with the first samples appearing in 2012. It has had different names at different times: in 2012, the creators were selling it as Frutas; in 2013 it was called Adwind; in 2014 the Trojan was known as Unrecom and AlienSpy; and in 2015 it was named JSocket.

The main users of this Trojan are those conducting advanced cyber fraud, unscrupulous competitors, as well as so-called Internet mercenaries who are paid for spying on people and organizations online. Adwind can also be used by anyone wishing to spy on their friends.

Fortunately, our investigation was not in vain – a few days after its publication, the JSocket website stopped working and the Adwind author ceased their activity. Since then, no new versions of the Trojan have appeared. Perhaps we can expect another reincarnation of the Trojan, or maybe this is the end of the story.

TARGETED ATTACKS – ADWIND MALWARE-AS-A-SERVICE

The malware's list of functions includes the ability to:

- collect keystrokes
- steal cached passwords and grab data from web forms
- take screenshots
- take pictures and record video from the webcam
- record sound from the microphone
- transfer files
- collect general system and user information
- steal keys for cryptocurrency wallets

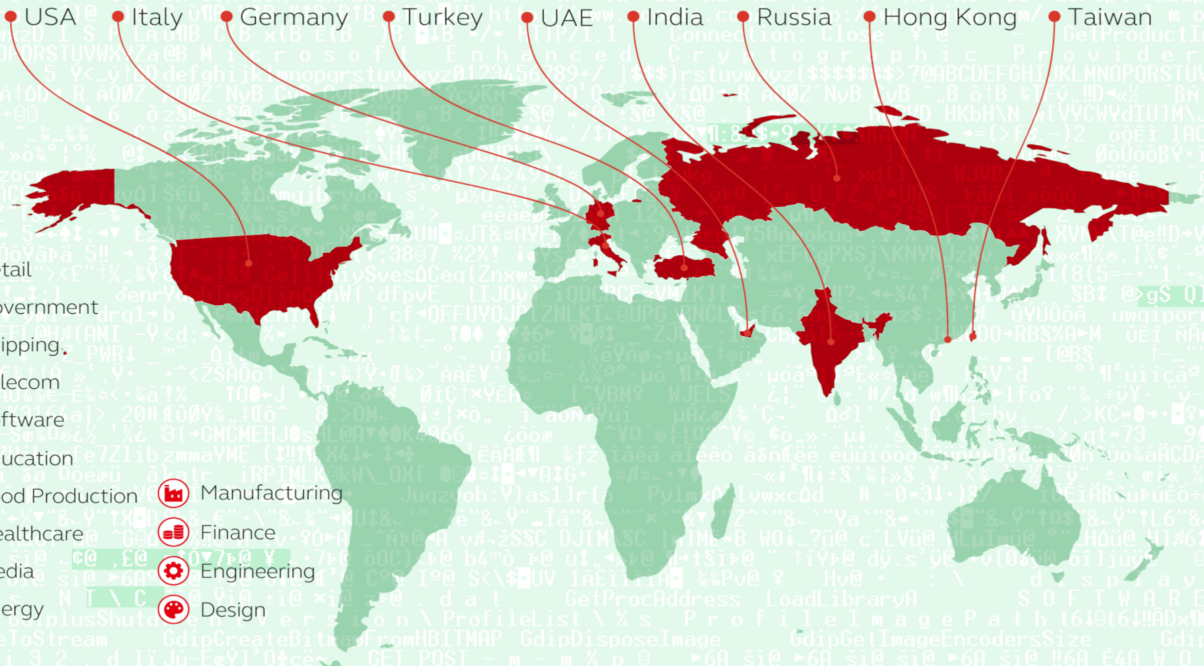
manage SMS (for Android)

steal VPN certificates

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

GREAT KASPERSKY lab

TARGETED ATTACKS – BANKING THREATS

At the Security Analyst Summit, Kaspersky Lab announced the discovery of two new gangs engaged in APT-style bank robberies – Metel and GCMAN – and the re-emergence of the Carbanak group with new targets in its sights.

In 2015, Kaspersky Lab researchers conducted incident response investigations for 29 organizations located in Russia that were infected by these three groups.

The activity of Carbanak 2.0 is of particular interest. In December 2015, Kaspersky Lab confirmed that the group was still active after discovering signs of Carbanak in a telecommunications company and a financial organization. An interesting feature of the Carbanak 2.0 group is that they have a different type of victim. The group has moved beyond banks and is now targeting the budgeting and accounting departments of any organization that interests them, using the same APT-style tools and techniques.

TARGETED ATTACKS – LURK

Lurk uses a fileless spreading mechanism – malicious code was not saved on the hard drive and ran in memory only. However, until now no detailed description of Lurk had been published.

Lurk has existed and actively evolved for over five years, but it works selectively – only on those computers where it can steal money. In the more than five years that it has been active, about 60,000 bots have been registered in the C&C, which is not a huge number.

Lurk is a versatile banker Trojan – it can steal money not only from the iBank 2 system that is used by many Russian banks but also from the unique online banking systems of some large Russian banks.

Lurk actively resists detection: its developers work hard to minimize detections of their Trojan, while targeted attacks make it difficult to get new samples quickly.

Based on the methods of internal organization used in the malware, its feature set and the frequency with which it is modified, it can be concluded that a team of professional developers and testers is working on the project.

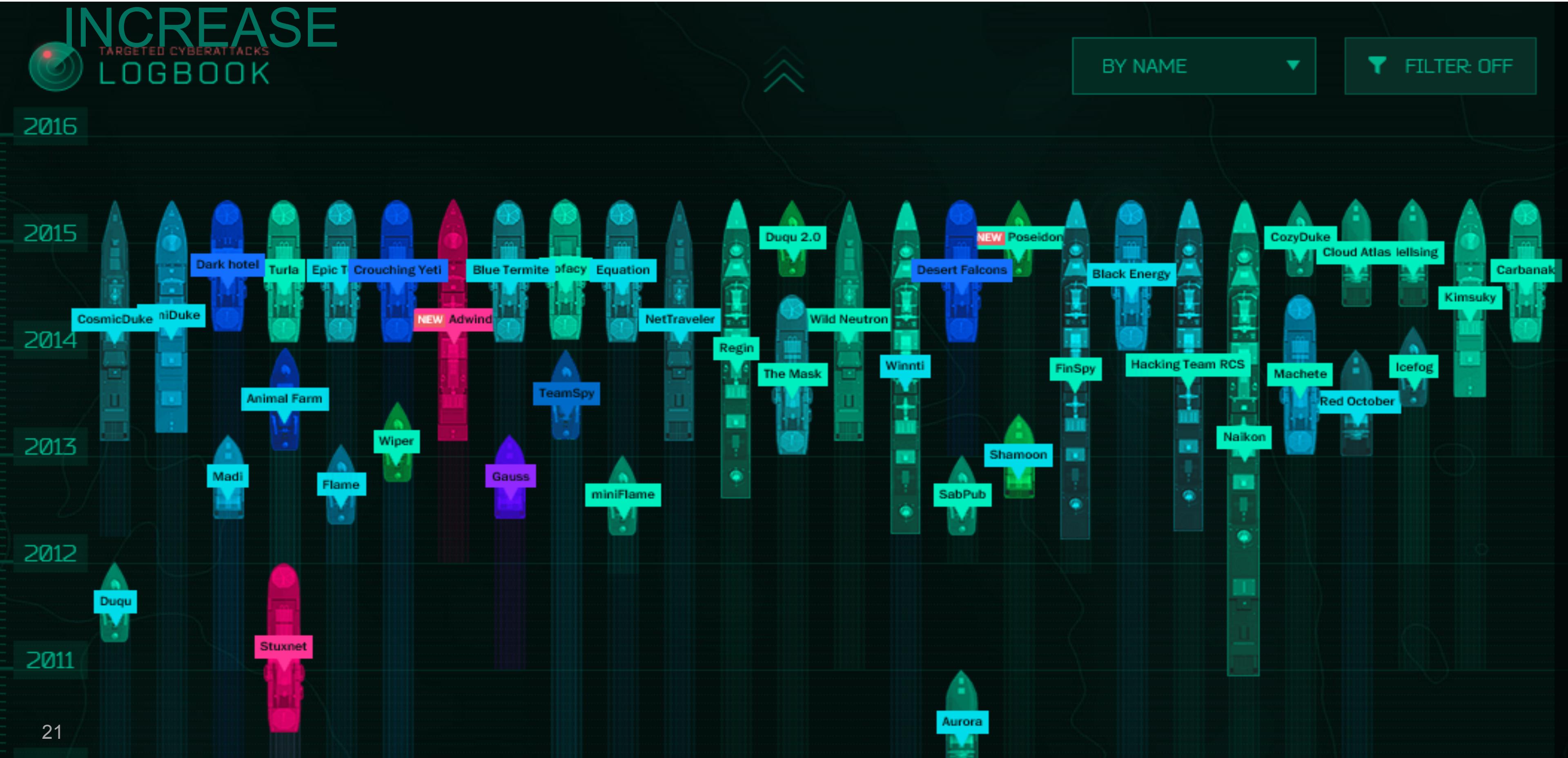
TARGETED ATTACKS – LURK

Kaspersky Lab helps crush Russian hacker cybercrimes who stole US$45 million

Russia’s largest cybercriminal arrest has happened in part thanks to the enlightened efforts of security supremos, Kaspersky Lab, with the Lurk gang of 50 people arrested.

Kaspersky Lab’s experts, and those of Sberbank (one of Russia’s largest banks,) "worked closely with Russian law enforcement agencies in an investigation into the Lurk gang that has now resulted in the arrest of 50 people".

TARGETED ATTACKS AND APTS SEE A STRONG INCREASE



XDEDIC

Who Else is Using your Servers?

A global forum where cybercriminals can buy and sell access to compromised servers for as little as $6 each.

The xDedic marketplace, which appears to be run by a Russian-speaking group, currently lists 70,624 hacked Remote Desktop Protocol (RDP) servers for sale.

Those servers are found in 173 countries

Many of the servers host or provide access to popular consumer websites and services and some have software installed for direct mail, financial accounting and Point-of-Sale (PoS) processing.

XDEDIC

An European internet service provider (ISP) alerted Kaspersky Lab to the existence of xDedic and the companies worked together to investigate how the forum operates.

The process is simple and thorough: hackers break into servers, often through brute-force attacks, and bring the credentials to xDedic. The hacked servers are then checked for their RDP configuration, memory, software, browsing history and more – all features that customers can search through before buying. After that, they are added to a growing online inventory that includes access to:

- Servers belonging to government networks, corporations and universities

- Servers tagged for having access to or hosting certain websites and services, including gaming, betting, dating, online shopping, online banking and payment, cell phone networks, ISPs and browsers

- Servers with pre-installed software that could facilitate an attack, including direct mail, financial and PoS software

Links of interest

https://cyberstat.kaspersky.com/

https://securelist.com/

https://blog.kaspersky.com/

https://apt.securelist.com/#firstPage

ANY QUESTIONS OR REQUESTS?

PLEASE WRITE TO ME:

Andis.steinmanis@kaspersky.com

Kaspersky Lab Baltic