RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: TTA-F02

Malware Actors and Espionage: a Shift in the Criminal Value Chain

Eward Driehuis

Product Director

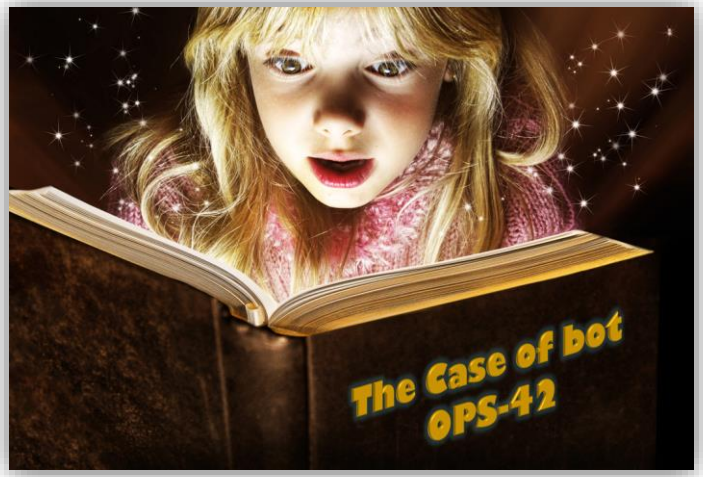
Fox-IT

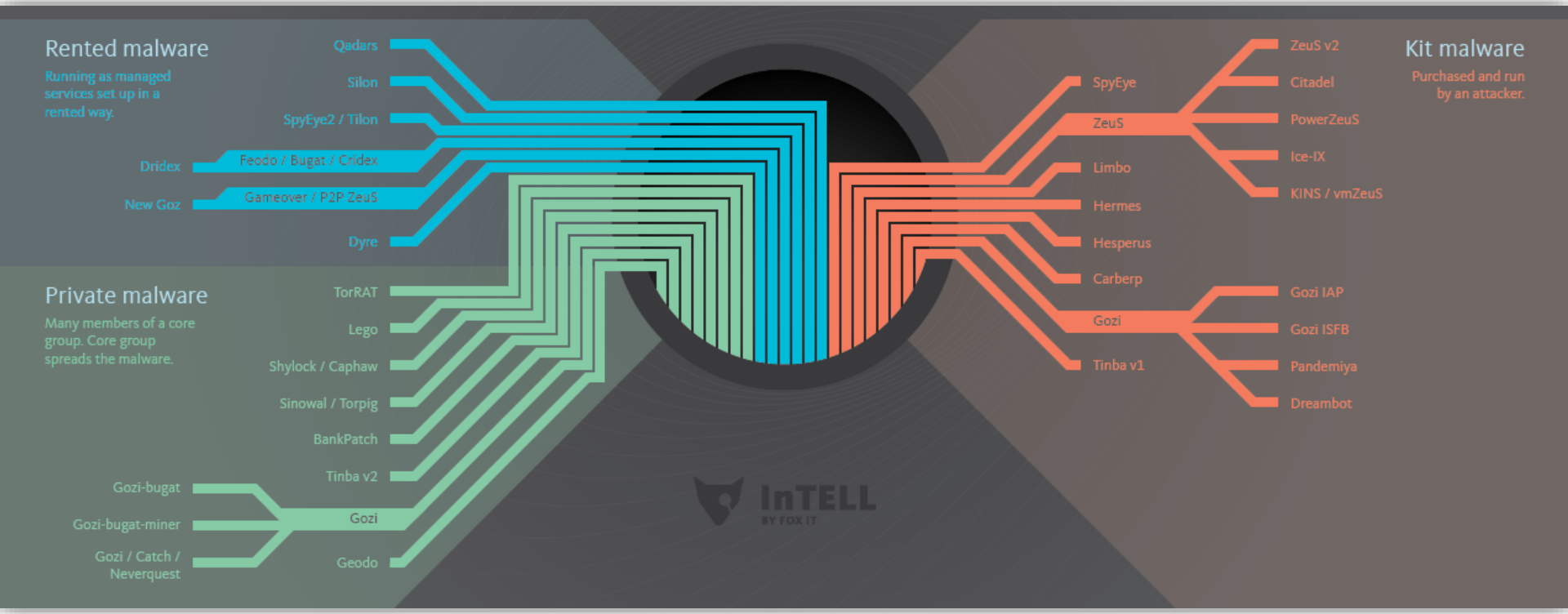
@brakendelama

Today's countries under attack

The case of bot OPS-42

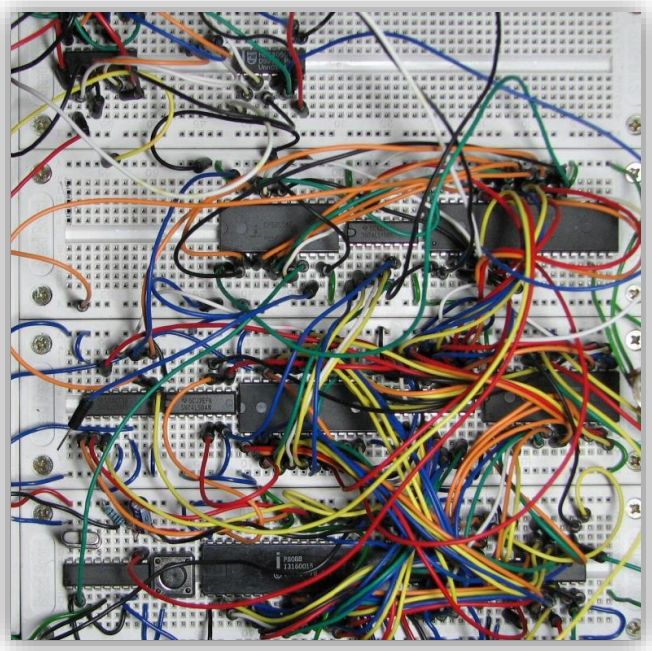
- Regular botnet research
- OPS-42
- Kept apart from others
- Espionage tooling uploaded
- Warned the victim through ISP





10 years of financial malware

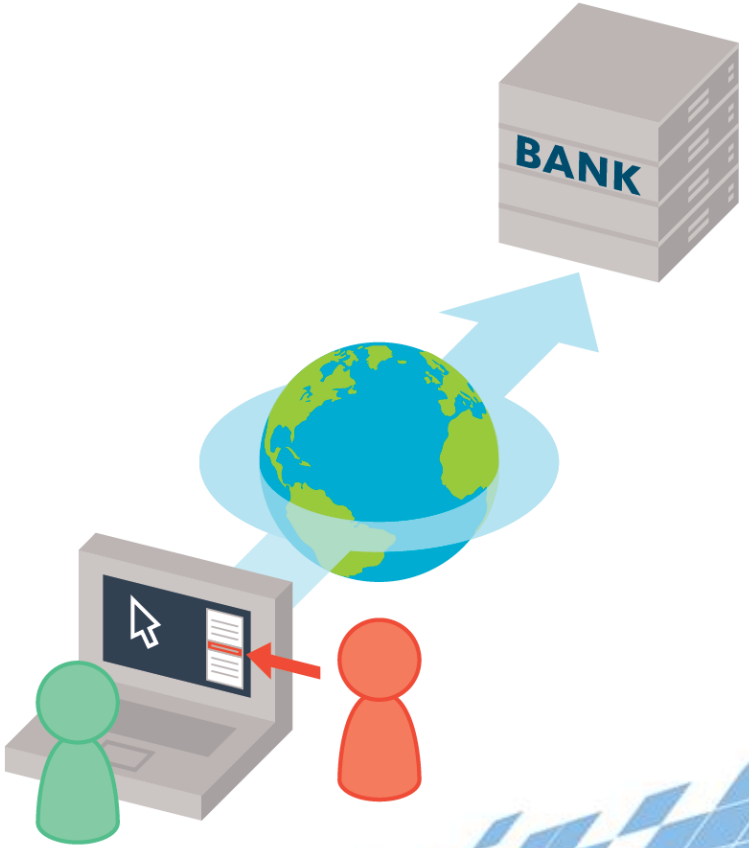
The pre-history of financial malware - 2004



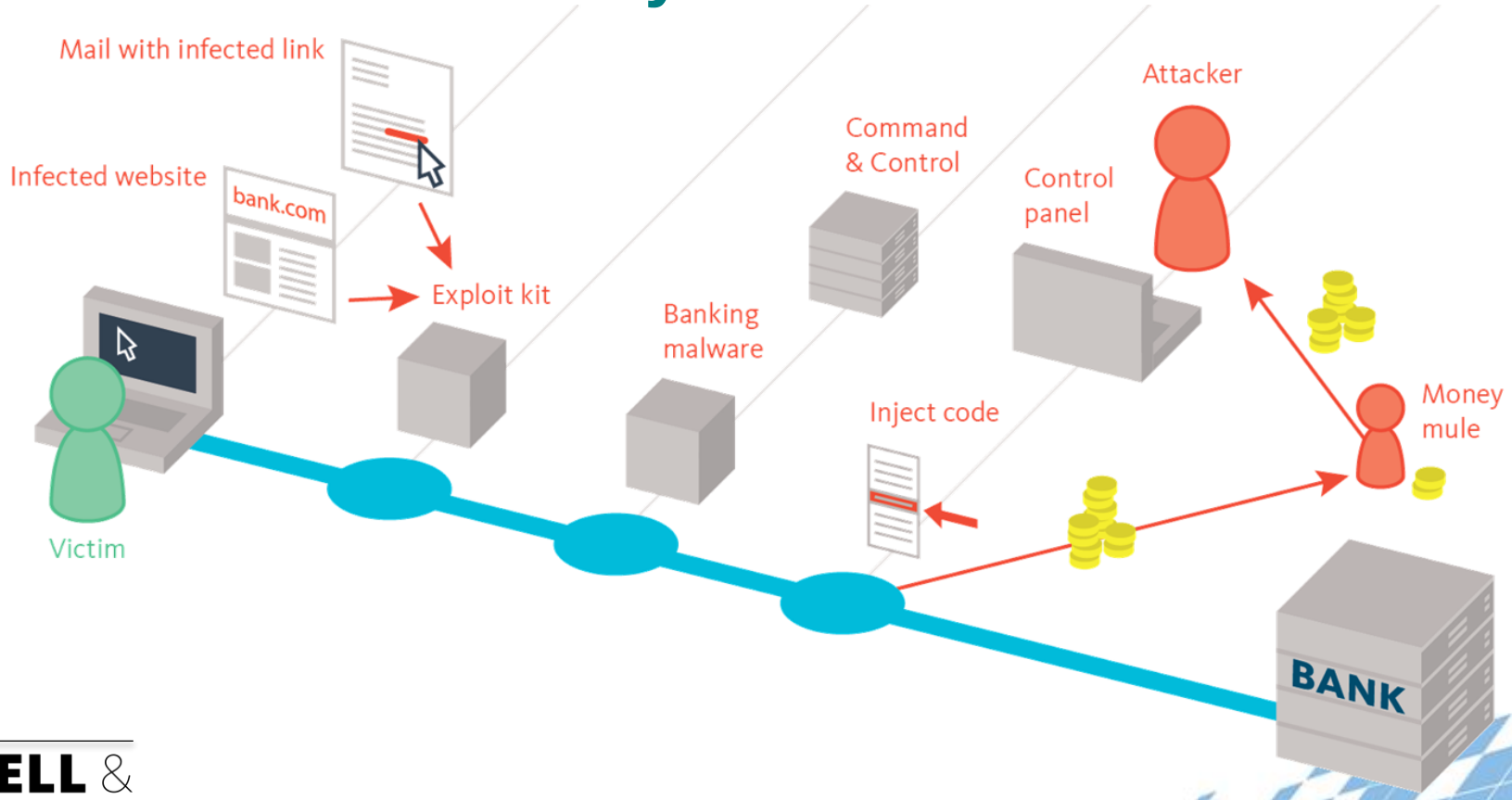
- Where it all started
- Bankpatch
- Haxdoor
- A-311 Death
- Limbo / Nethell
- Lots of tweaking required

Cybercrime kits - 2006

- **ZeuS** appears in 2006
- Aimed at finance
- Man in the browser
- Anyone can run an attack
- Introducing **Slavik**
- Very popular



The start of an ecosystem



The start of a battle - 2009

- Gunning for ZeuS market share
- First versions were terrible, but cheap
- Author is Gribodemon
- Adopts ZeuS config style

Carberp - 2009

- ZeuS and SpyEye were not the only game in town anymore
- Attacks in Europe
- Broke an important rule
- Key members arrested in 2012

Intrigue in the underground - 2010

What seemed to happen

- ZeuS is at version 2.0.8.9
- Suddenly **Slavik** announces he is quitting and

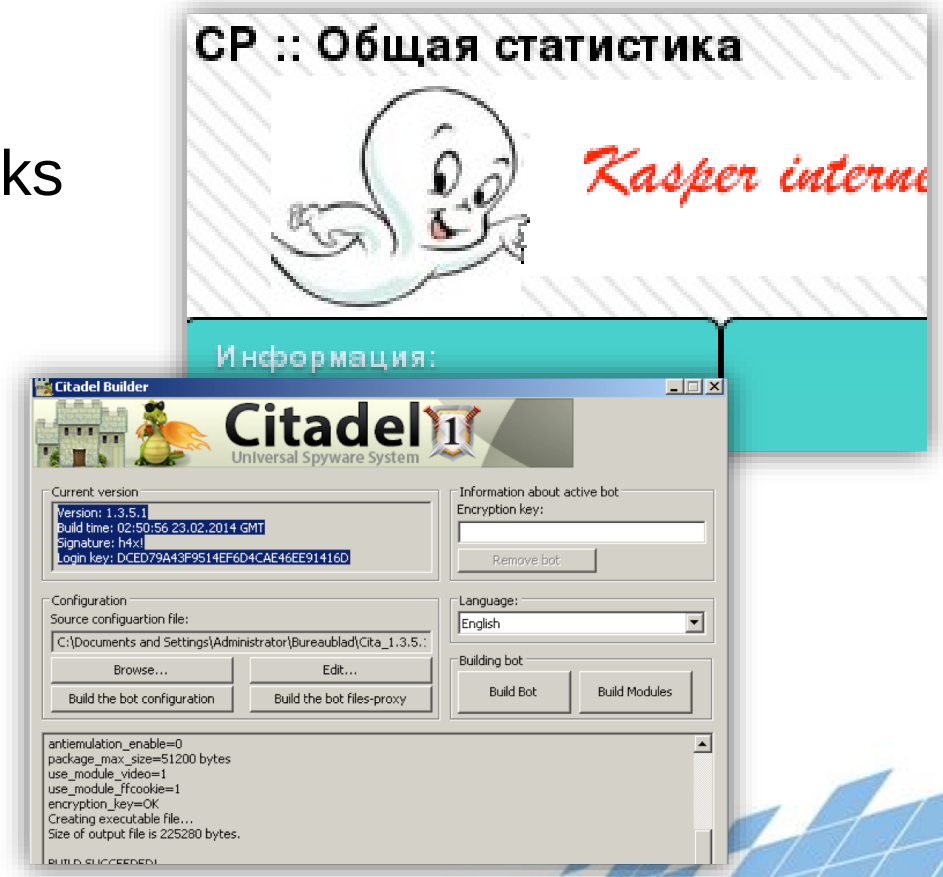
  *handing over support and development to **Gribodemon**, author of SpyEye!*

What *really* happened

- Slavik was part of a gang using ZeuS to go after high value accounts – **JabberZeuS**
- More profitable than selling ZeuS
- Wants to get rid of kit business
- Starts work on next versions which becomes **P2PZeuS**

The Big Leak - 2011

- Early 2011 ZeuS 2.0.8.9 leaks
- Lots of new families appear
- ICE-IX
- Citadel
- KINS
- Cost of malware goes down



The end of SpyEye - 2012

- **Gribodemon** never releases a SpyZeuS
- Instead he too starts working on a managed version of SpyEye, **SpyEye2**
- But he is arrested in 2012 while on holiday in Costa Rica and extradited to the US

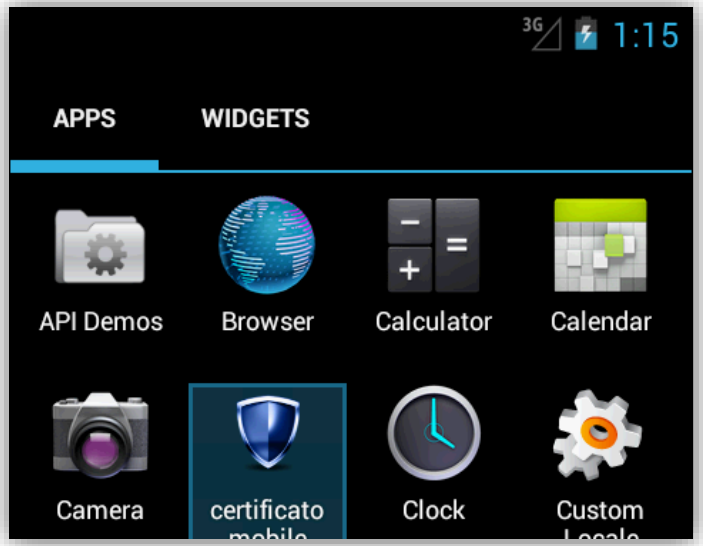
Slavik branches out

- P2P ZeuS investigation
- 500,000 private keys found
- Cryptolocker
- Ransomware

Others branch out

Selling bots to spies

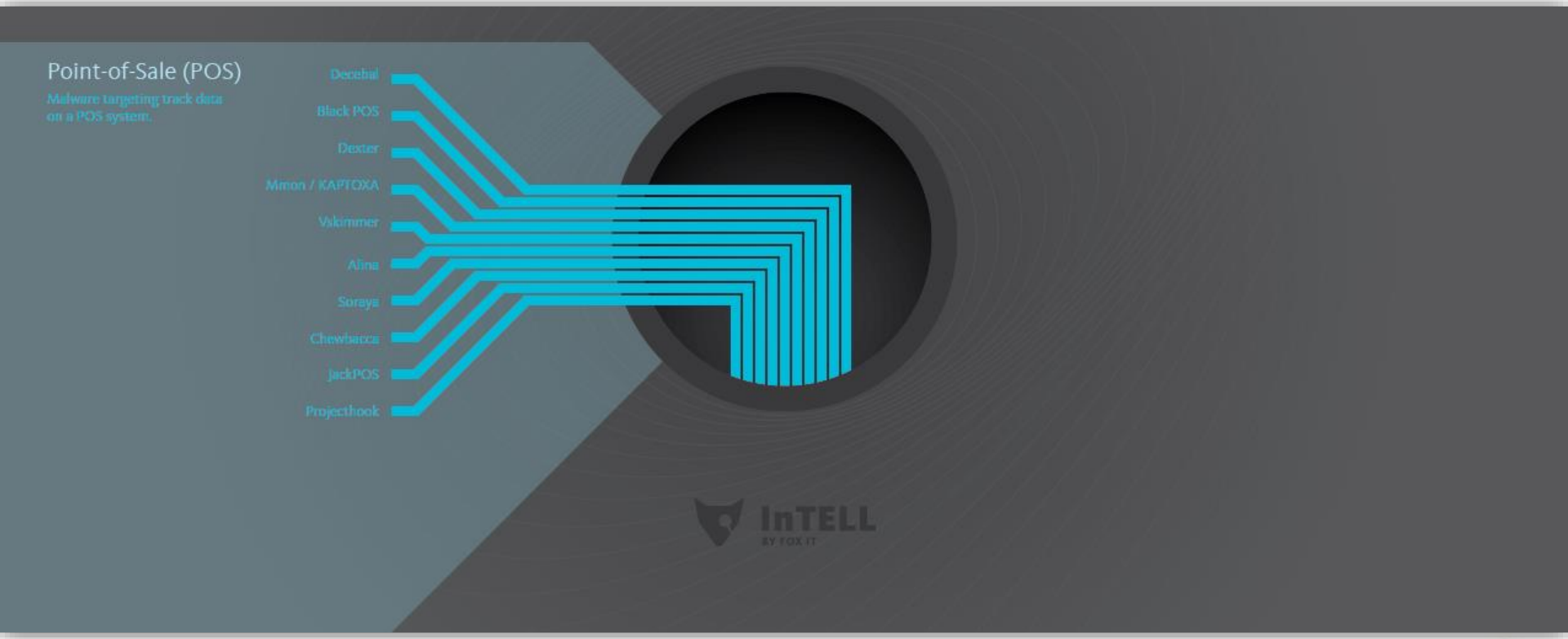
Scaling through mobile



And find innovative ways…

Litecoin mining

POS malware



Today's POS malware ecosystem

A pivoting moment

- From 2011 – 2014, P2PZeuS very popular
- Commercial banking
- Active worldwide
- In 2014 FBI takes down botnet
- Slavik's identity known

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

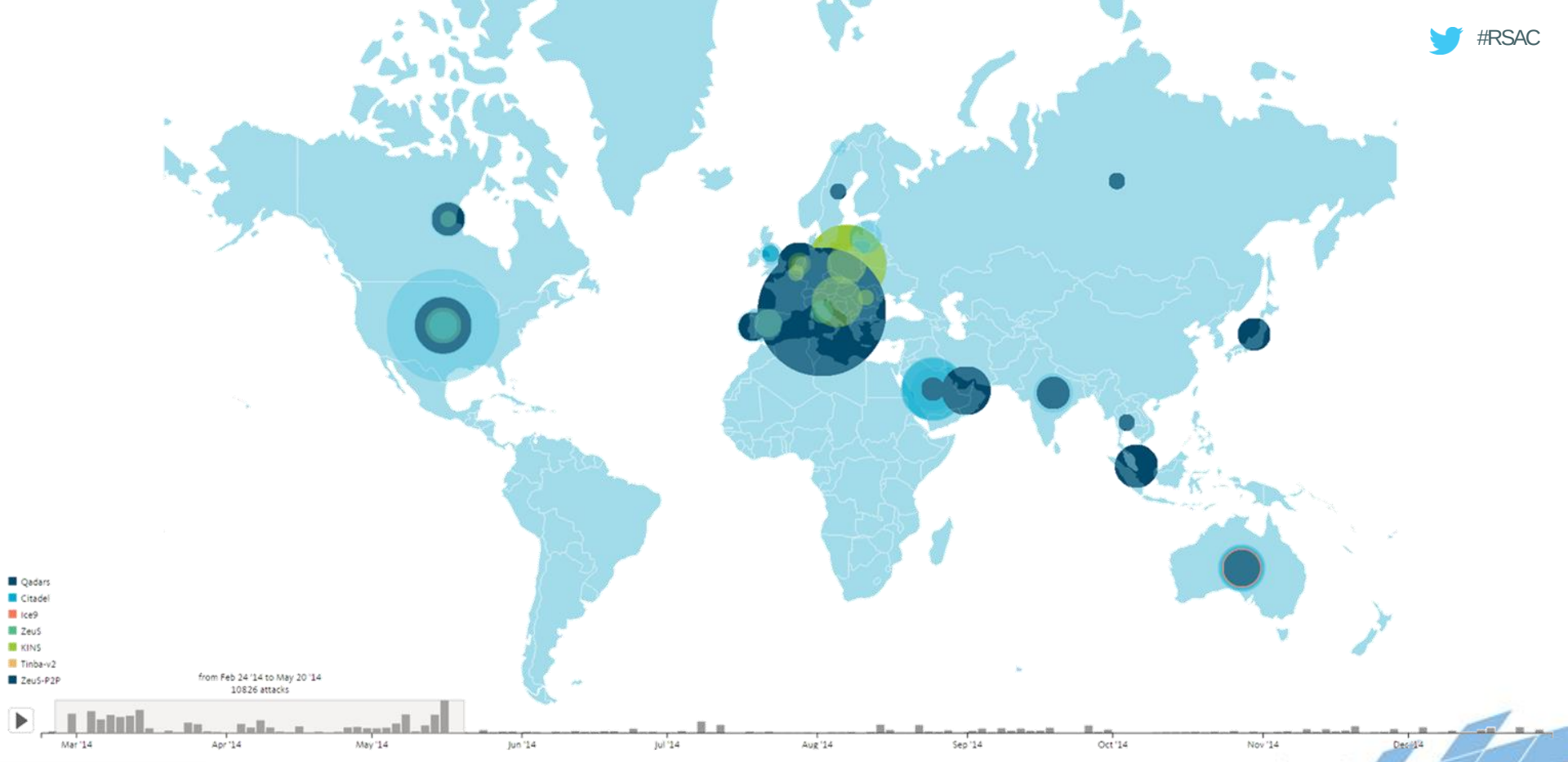
EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

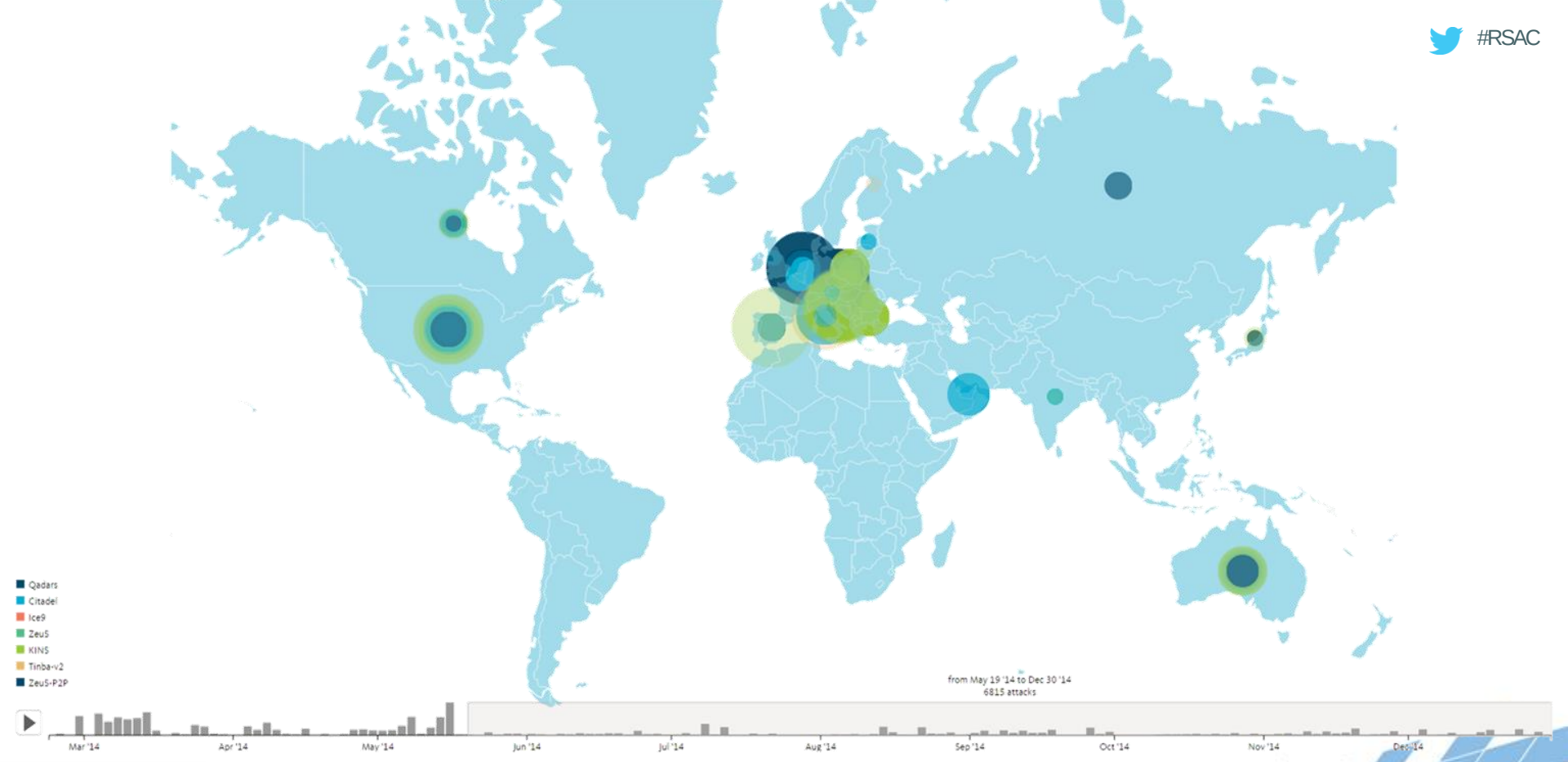
Date(s) of Birth Used: October 28, 1983
Height: Approximately 5'9"
Weight: Approximately 180 pounds
NCIC: W890989955
Occupation: Bogachev works in the Information Technology field.
Hair: Brown (usually shaves his head)
Eyes: Brown
Sex: Male
Race: White

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

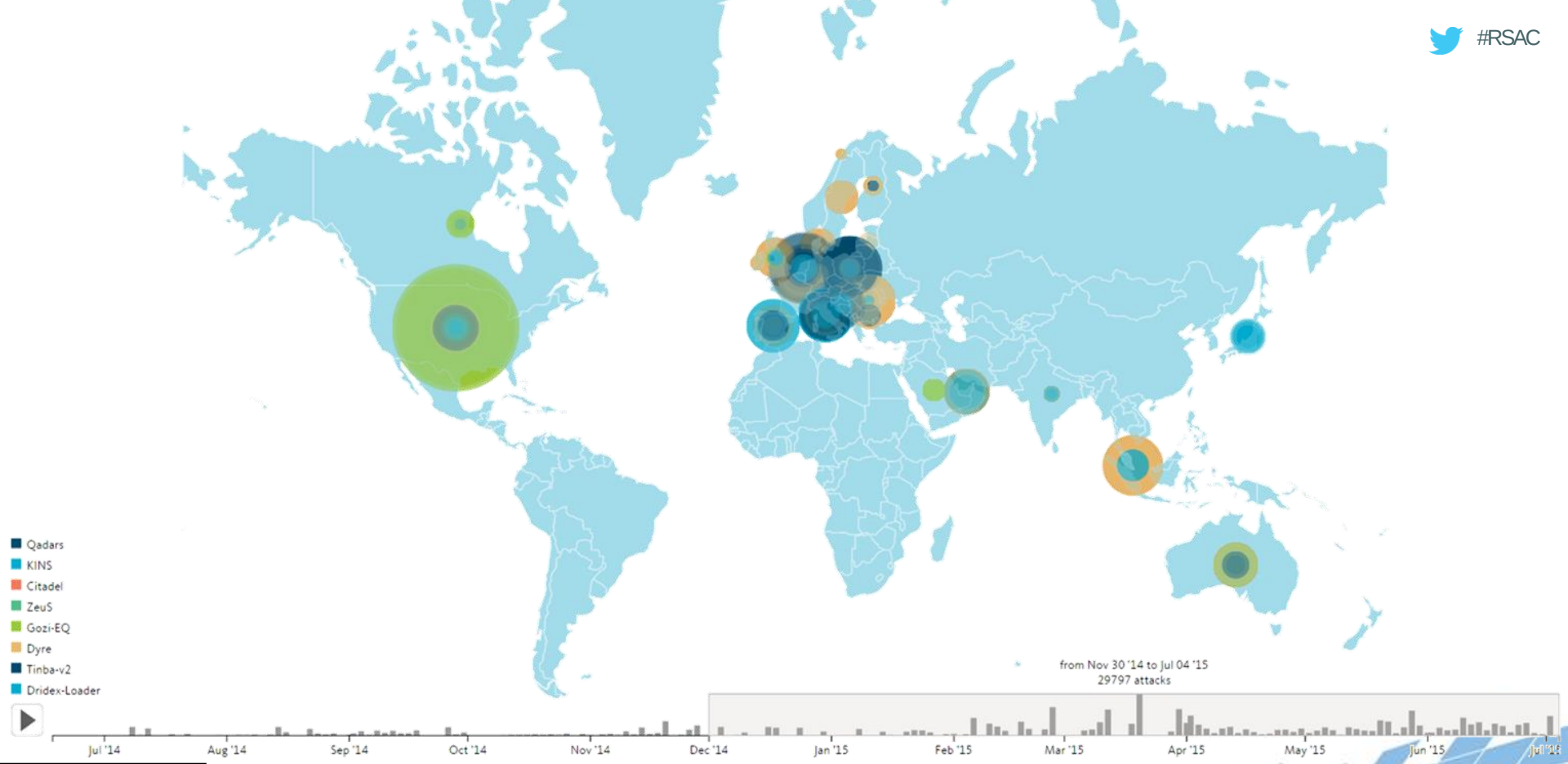


Slavik's last months: Jan-May 2014

InTELL & DetACT BY FOX IT



A period of quiet: H2 2014



A new storm: H1 2015

InTELL & DetACT BY FOX IT

A game of whack-a-mole?

Carberp

Returned as Anunak

Gribodemon

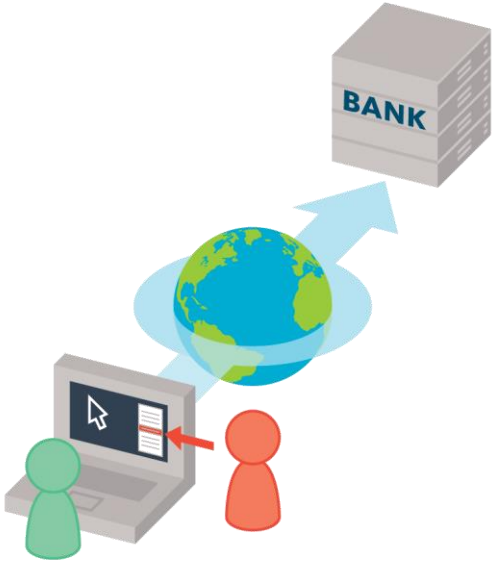
Was a scapegoat

Slavik

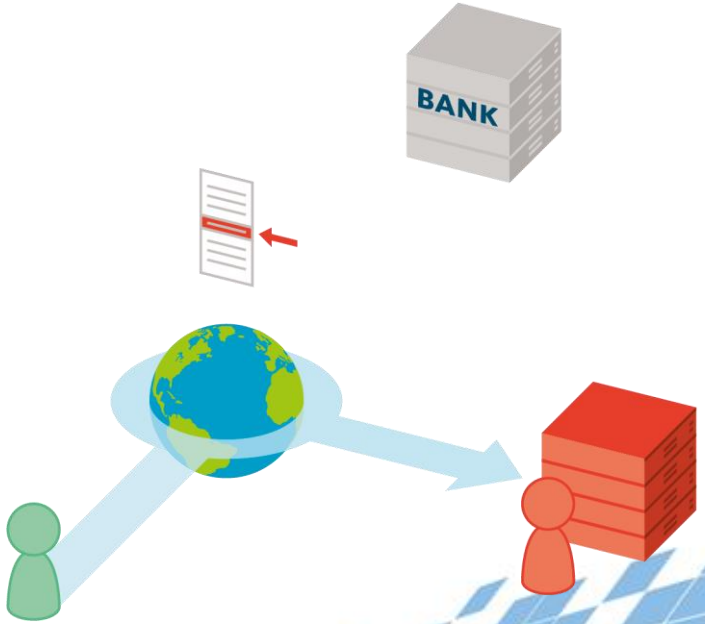
Customers took over

A shift in the criminal value chain

Past: fully automated attacks



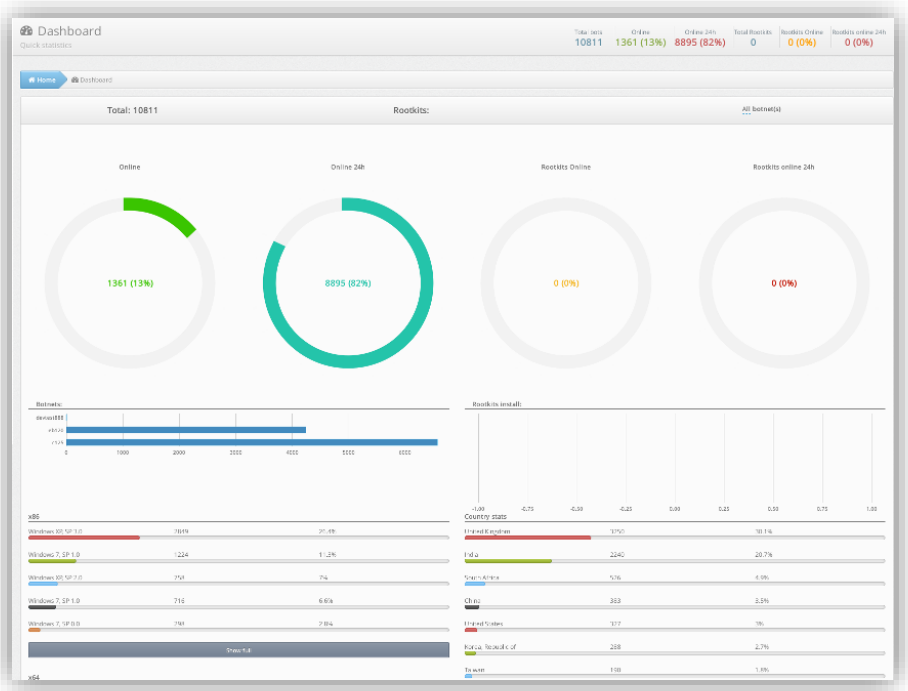
Present: semi automated



Today

- Other groups focus on retail – POS
- Copycat ransomware
- **Dyre** and **Dridex**
- **Anunak** – retail and Russian banks

Dridex

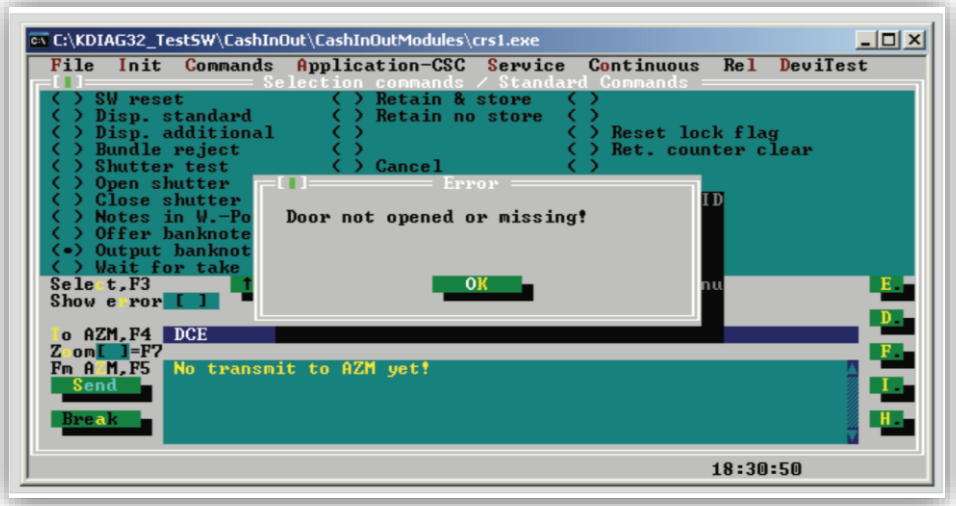


- Based on Feodo
- Main4 group P2PZeuS
- Initial focus on UK
- *Az Trade & tokengrabber*

Dyre

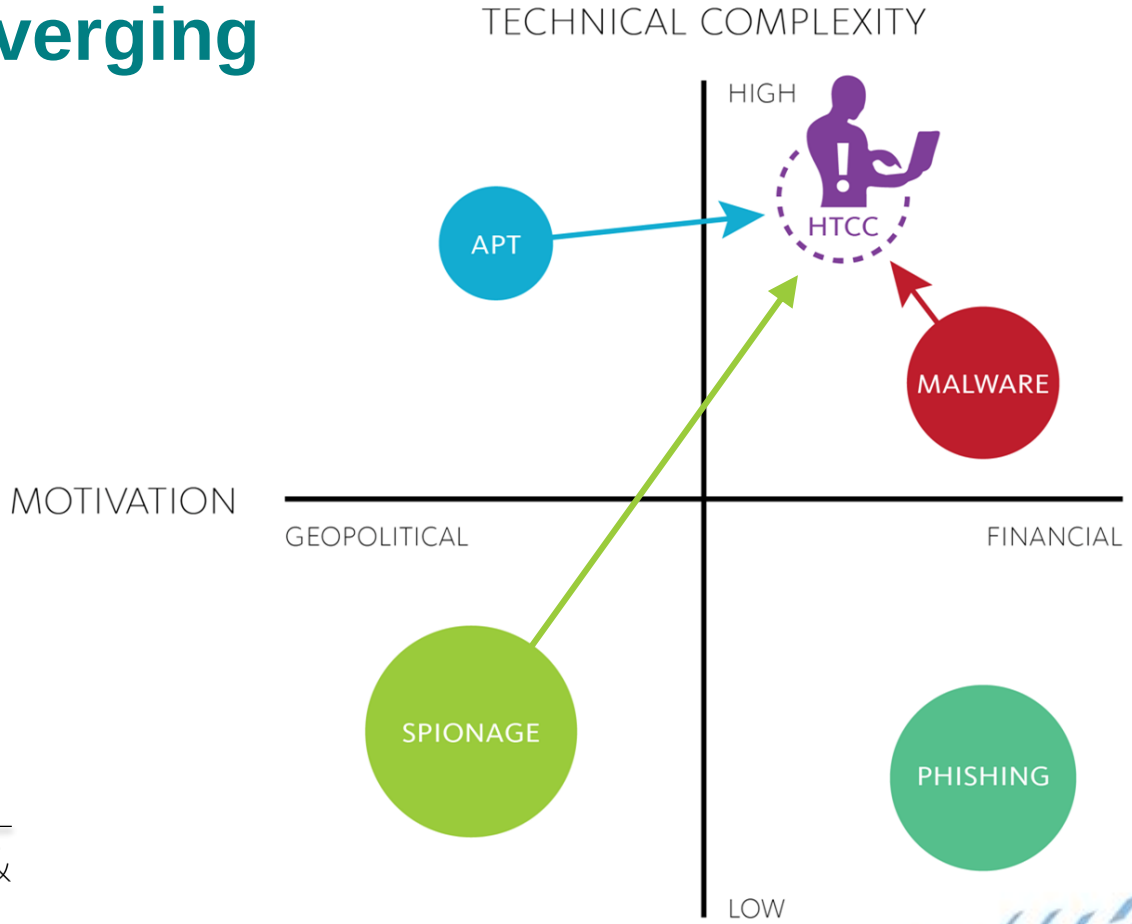
- New malware
- Uses *tokengrabber*
- Hybrid attack with webfake
- Server Side Injects

Anunak / Carbanak



- Remnants of Carberp
- Using custom malware
- Targeting (Russian) banks
- And Western retailers
- ATM networks, channel attacks
- Espionage
- Gave many quite a scare…

Attack types are converging



But not all of them…

- Criminals are more pragmatic than we can predict
- They scale & branch out
- To espionage, ransomware, litecoin mining, mobile & POS
- Attack methods converge: espionage, financial & APT

- But: threats evolve, they don't appear out of nowhere
- Global context & attribution helps you understand (is not about malware anymore)
- Build on your intelligence position in ways you can afford