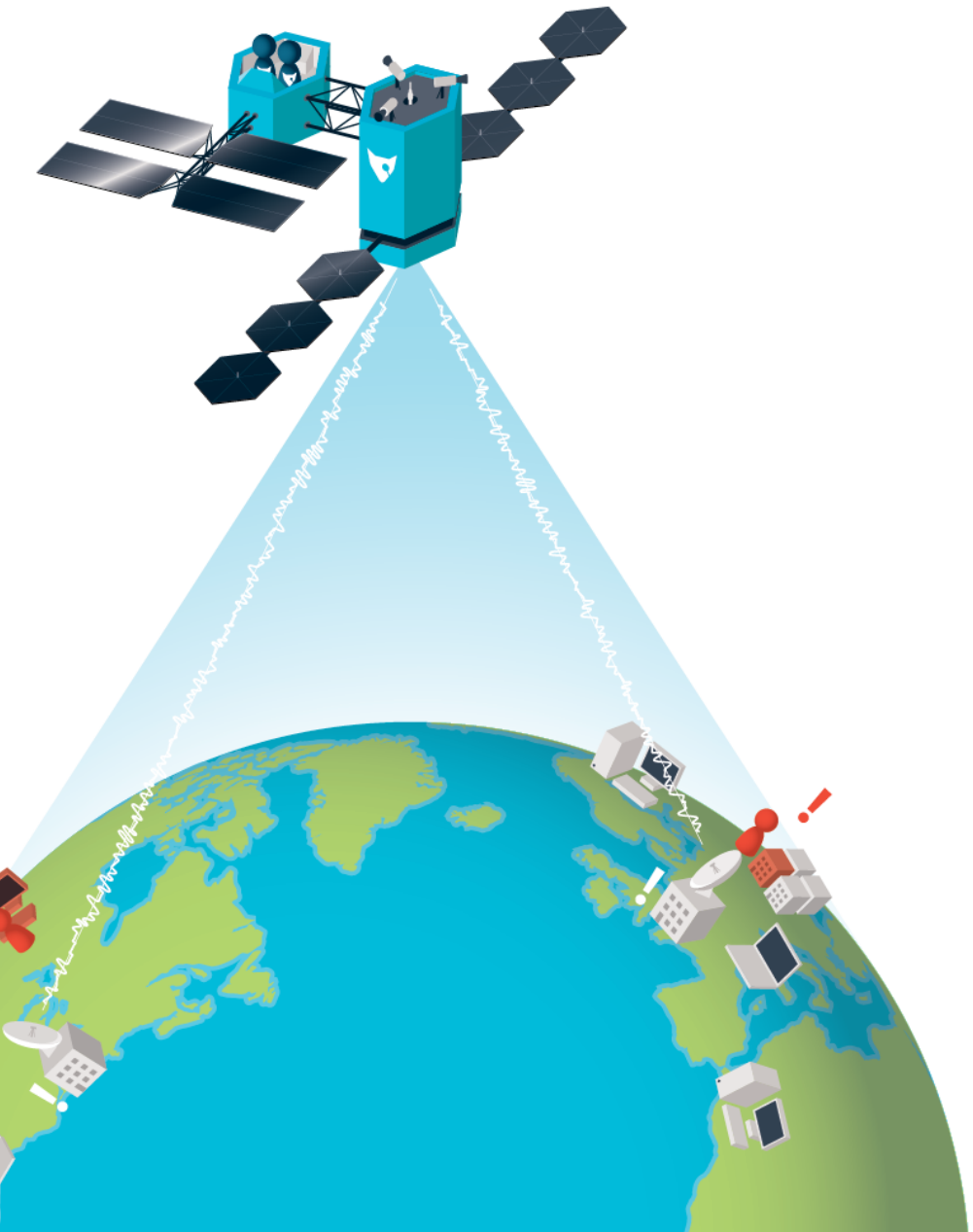


From ZeuS to Dyre

In 20 minutes

And how to use this knowledge to fight fraud

Eward Driehuis
driehuis@fox-it.com

FOX IT
FOR A MORE SECURE SOCIETY

theguardian

News | Sport | Comment | Culture | Business | Money | Life & sty

News › UK news › GCHQ

GCHQ: EU surveillance hearing is told of huge cyber-attack on Belgian firm

Belgacom boss says no company or country could have withstood cyber-attack of this size and sophistication

Ian Traynor in Brussels

Set edition preference

Home | Video | World | U.S. | Africa | Asia | Europe | Latin America | Middle East | Business | World Sport | Entertainment

Malware attack hits thousands of Yahoo users per hour

By Faith Karimi and Joe Sutton, CNN
January 6, 2014 -- Updated 1342 GMT (2142 HKT) |

SHARE THIS

Recommend 5.5k

Most Popular »

Today's five most popular sto

Mary Kay Letourneau, convic arrested in Washington state

Judge rules Chicago gun bar

Fox-IT technology leadership

BBC News | Sport | Weather | Capital | Future | Shop

NEWS TECHNOLOGY

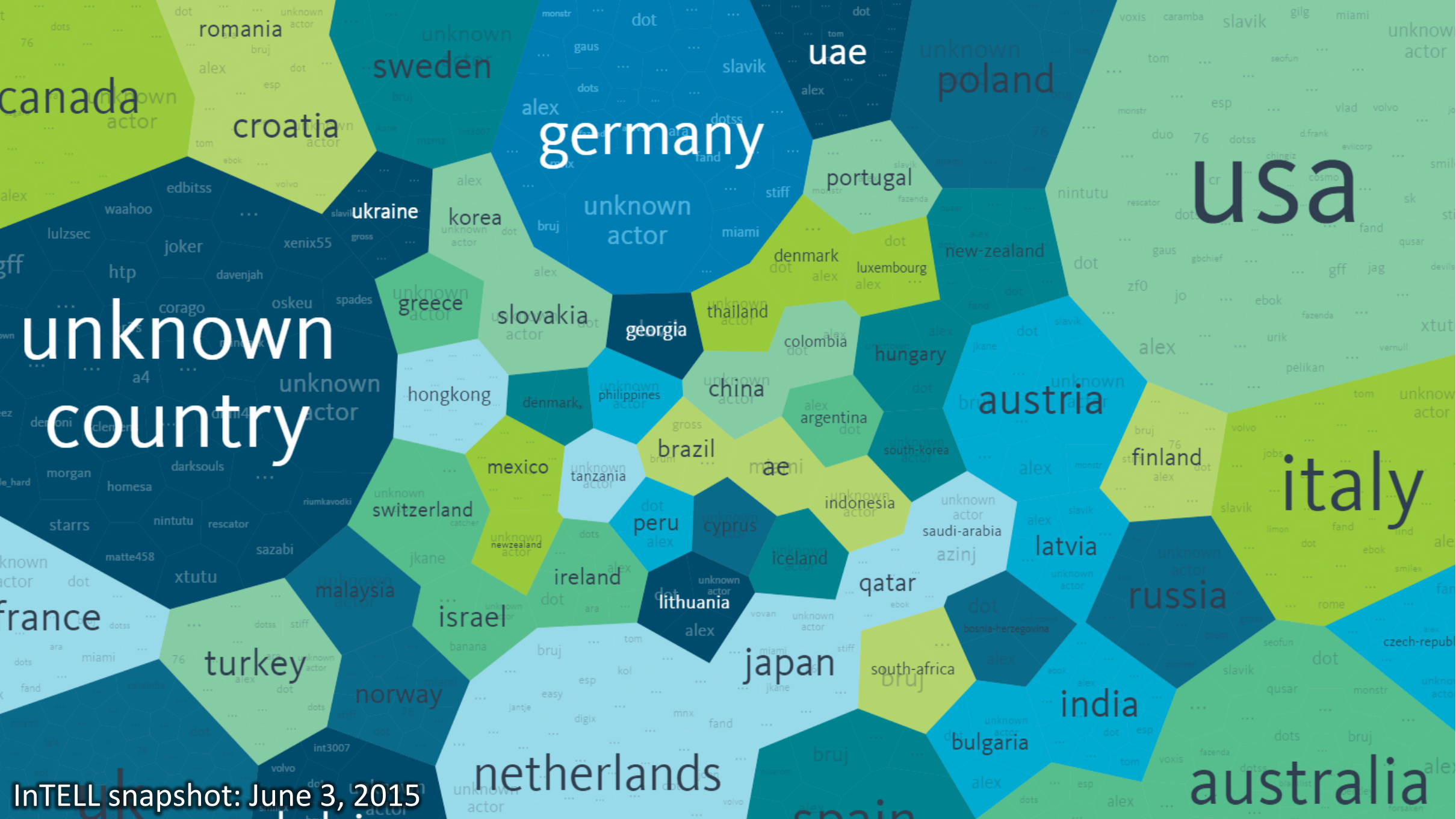
Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environm

Cryptolocker victims to get files back for free

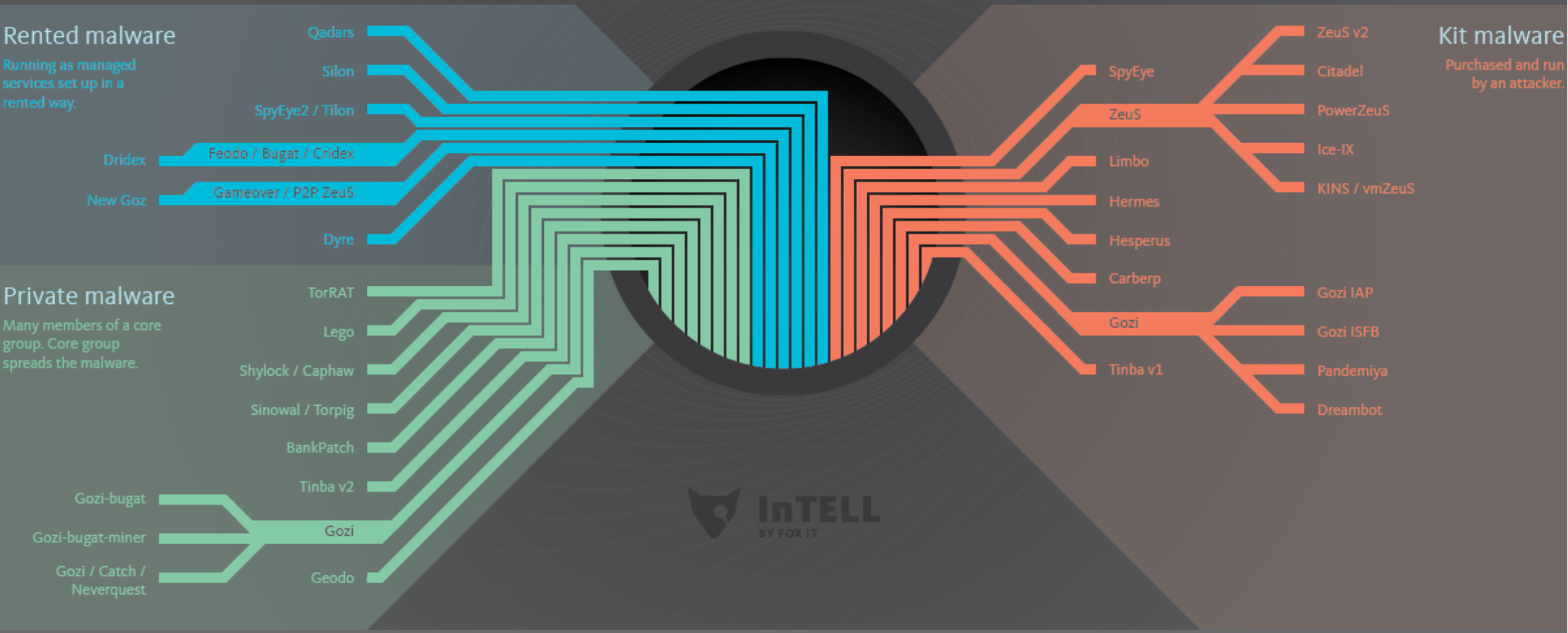
By Mark Ward
Technology correspondent, BBC News

Proven track record


InTELL snapshot: June 3, 2015

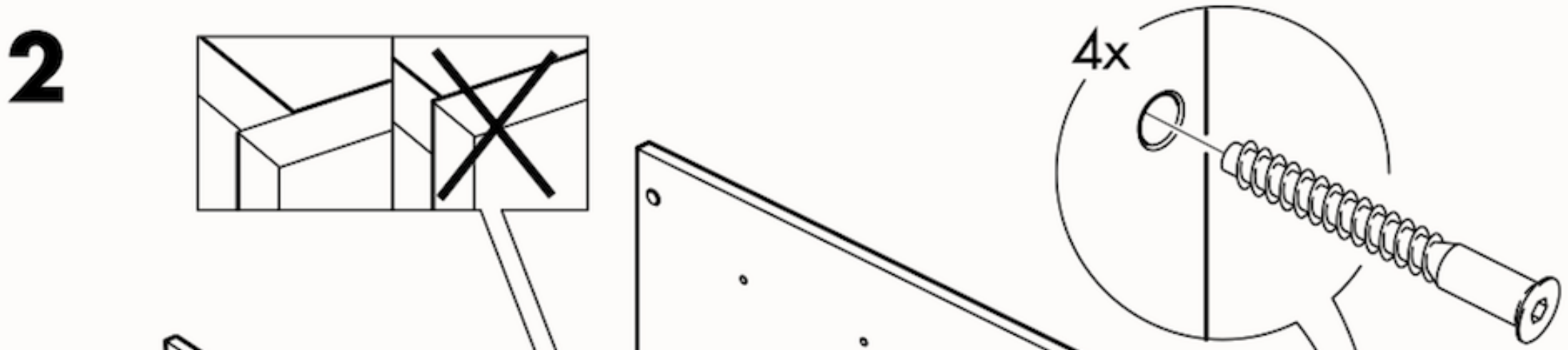

unknown country
usa
germany
canada
romania
croatia
sweden
uae
poland
ukraine
korea
portugal
denmark
luxembourg
new-zealand
greece
slovakia
georgia
thailand
colombia
hungary
hongkong
china
austria
philippines
argentina
brazil
ae
mexico
tanzania
finland
italy
switzerland
indonesia
peru
cyprus
saudi-arabia
latvia
ireland
iceland
qatar
russia
malaysia
israel
lithuania
japan
south-africa
india
turkey
norway
bulgaria
netherlands
australia
france
edbitss
waahoo
lulzsec
joker
xenix55
htp
davenjah
corago
oskeu
spades
a4
morgan
darksouls
homesa
starrs
nintutu
rescator
matte458
sazabi
xtutu
int3007
volvo
czech-republ
bosnia-herzegovina
InTELL snapshot: June 3, 2015

Financial malware families



Cybercrime ecosystem

- In 2006 **ZeuS** appears
- The original cybercrime kit
- Author goes by the name of **Slavik**
- ZeuS becomes very popular
- Ecosystem moving to managed malware in 2010
- Private groups



The life & death of P2PZeuS

From 2011 – 2014, P2PZeuS very popular

Active worldwide

In 2014 after years of investigation lead by the FBI botnet is taken down

Slavik's identity becomes 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.

U.S. DEPARTMENT OF STATE
DIPLOMACY IN ACTION

Enter keyword here Search

SECRETARY KERRY | MEDIA CENTER | TRAVEL | CAREERS | BUSINESS | YOUTH & EDUCATION

ABOUT STATE | POLICY ISSUES | COUNTRIES & REGIONS | ECONOMICS, ENERGY & ENVIRONMENT | ARMS CONTROL & INTERNATIONAL SECURITY | CIVILIAN SECURITY & DEMOCRACY | PUBLIC DIPLOMACY & PUBLIC AFFAIRS | ASSISTANCE & DEVELOPMENT

YOU ARE IN: Home > Briefings > -- By Date > 2015 > February

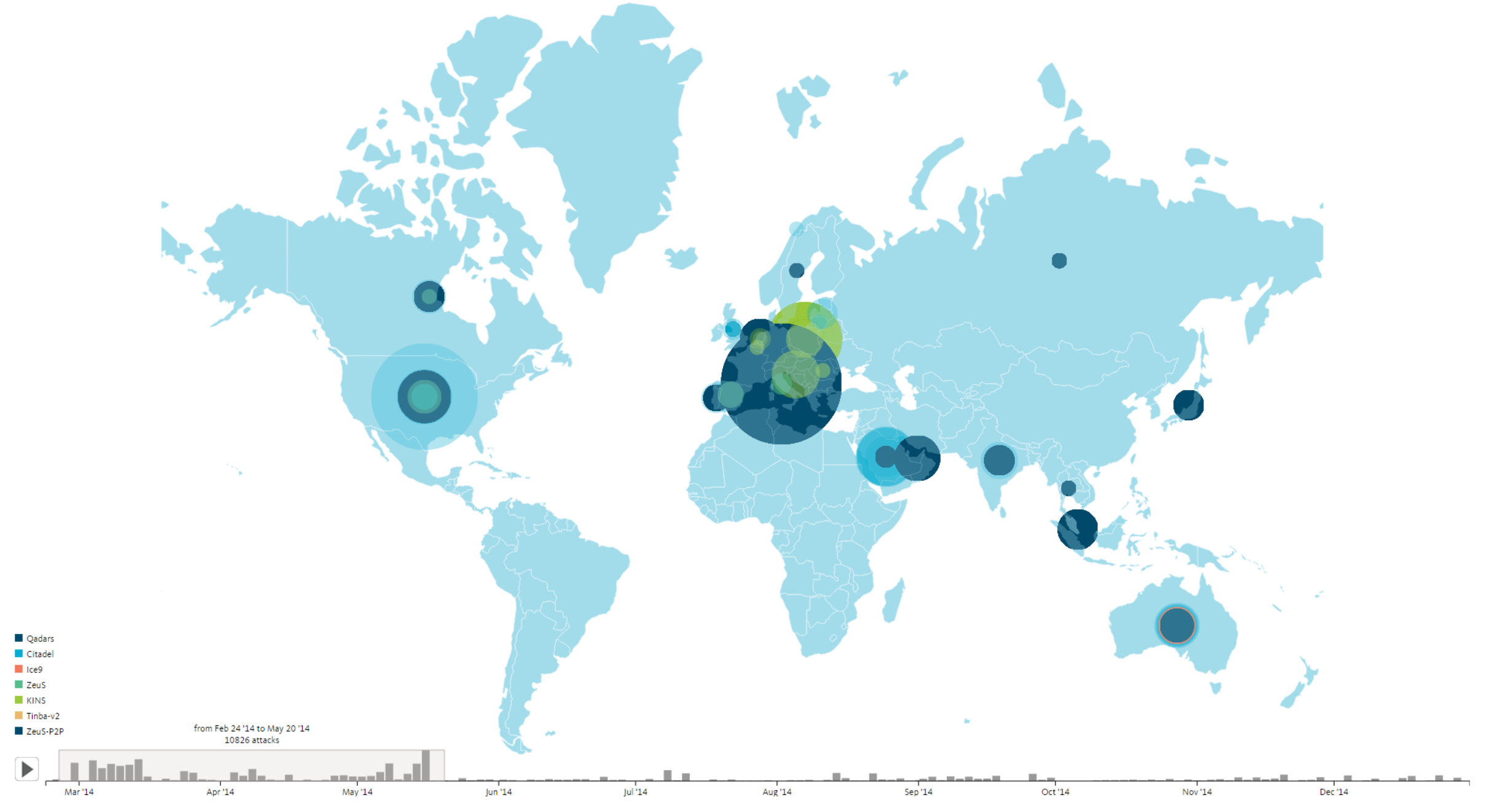
New Reward for Cyber Fugitive

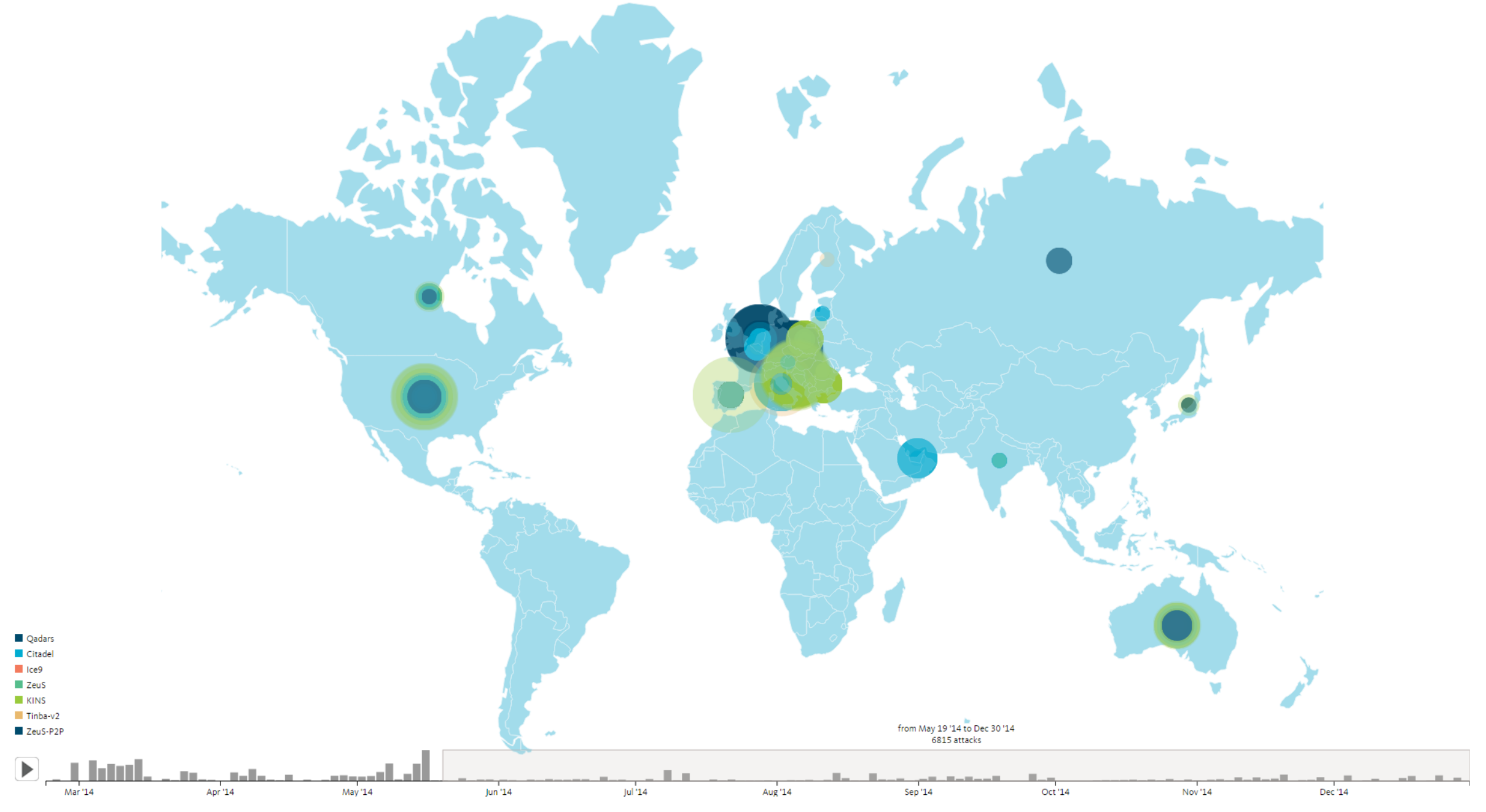
Department of Justice Assistant Attorney General for the Criminal Division Leslie Caldwell; Assistant Secretary of State for International Narcotics and Law Enforcement Affairs William Brownfield; Federal Bureau of Investigation (FBI) Assistant Director for Cyber Security Joseph Demarest; and, U.S. Attorney for the Western District of Pennsylvania David Hickton

Washington, DC
February 24, 2015

2:30 P.M. EST

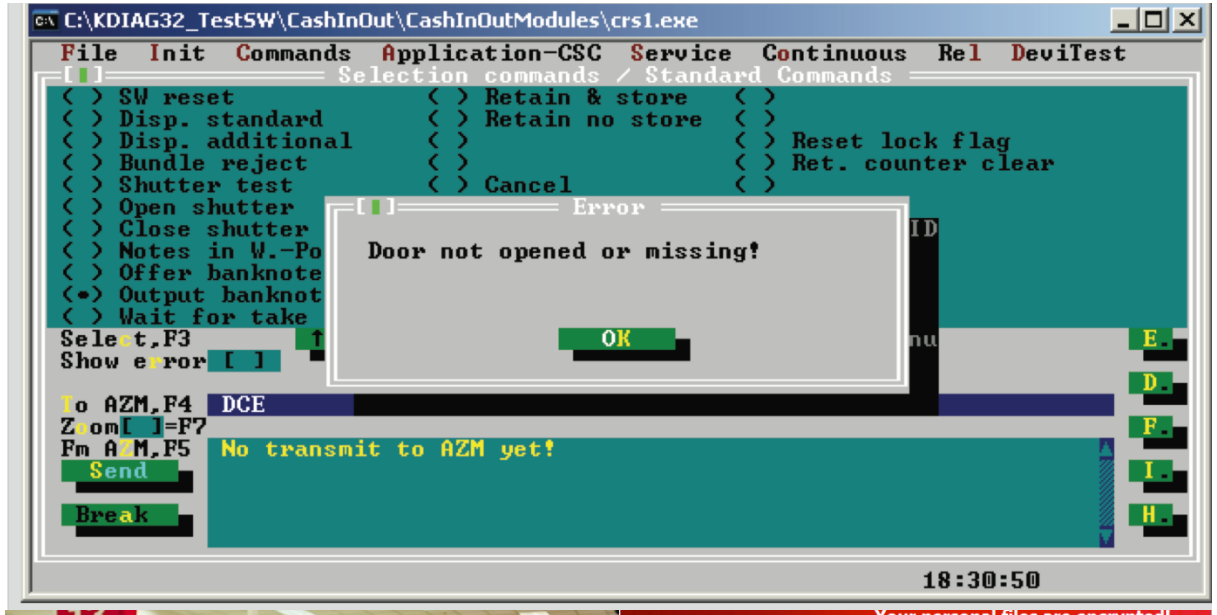
THE WASHINGTON FOREIGN PRESS CENTER, WASHINGTON,


Qadars
Citadel
Ice9
ZeuS
KINS
Tinba-v2
ZeuS-P2P
from Feb 24 '14 to May 20 '14
10826 attacks
Mar '14
Apr '14
May '14
Jun '14
Jul '14
Aug '14
Sep '14
Oct '14
Nov '14
Dec '14


Qadars
Citadel
Ice9
ZeuS
KINS
Tinba-v2
ZeuS-P2P
from May 19 '14 to Dec 30 '14
6815 attacks
Mar '14
Apr '14
May '14
Jun '14
Jul '14
Aug '14
Sep '14
Oct '14
Nov '14
Dec '14

Today

- Former P2PZeuS customers building alternative platforms: **Dyre** and **Dridex**
- Remnants of Carberp involved with **Anunak**
- Banking attacks, ATM cashouts, retail attacks and… Espionage
- But more are coming



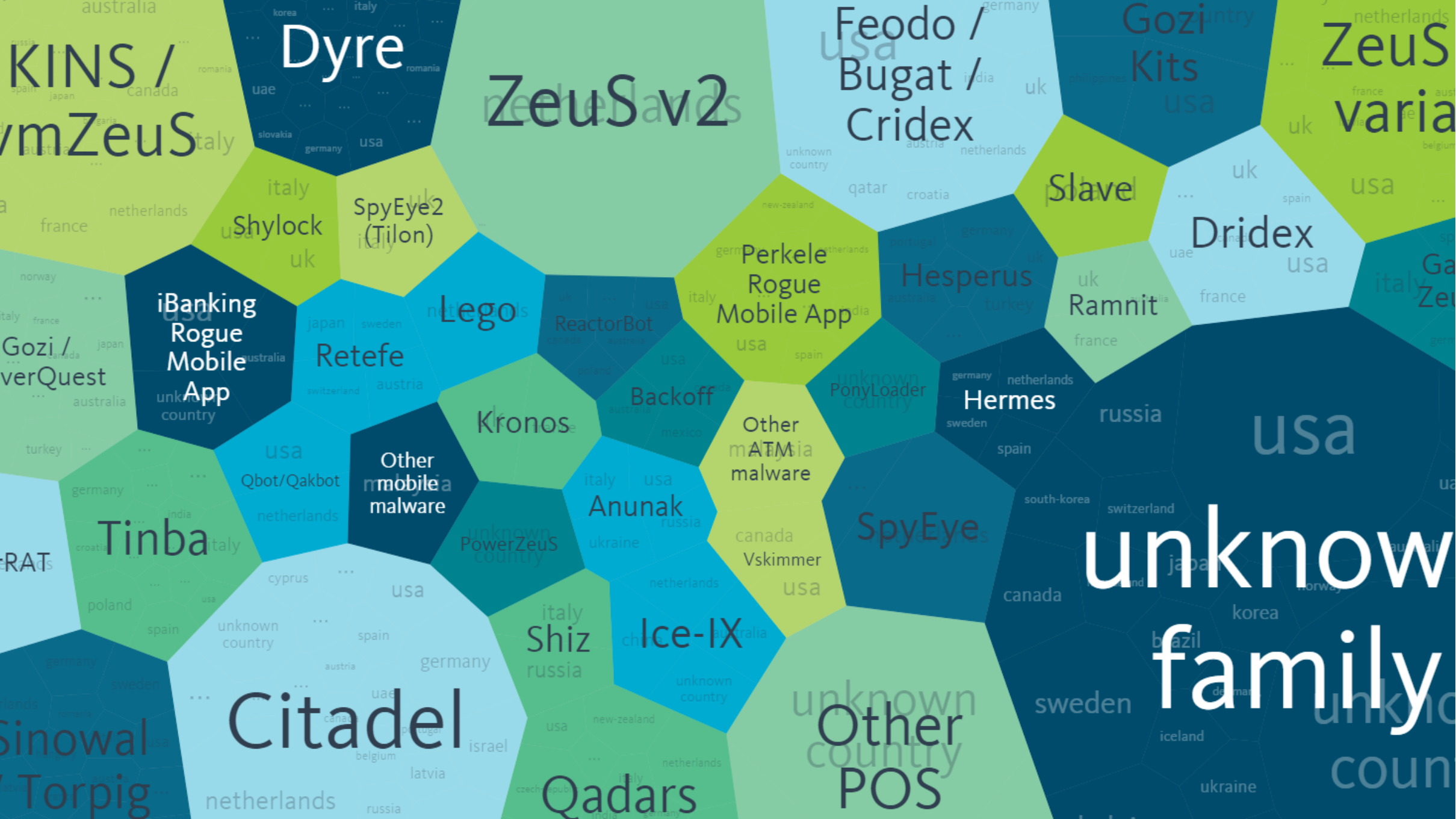
Automated vs hybrid attacks

Automated attack: inject code does everything

Hybrid attack: most steps by operator

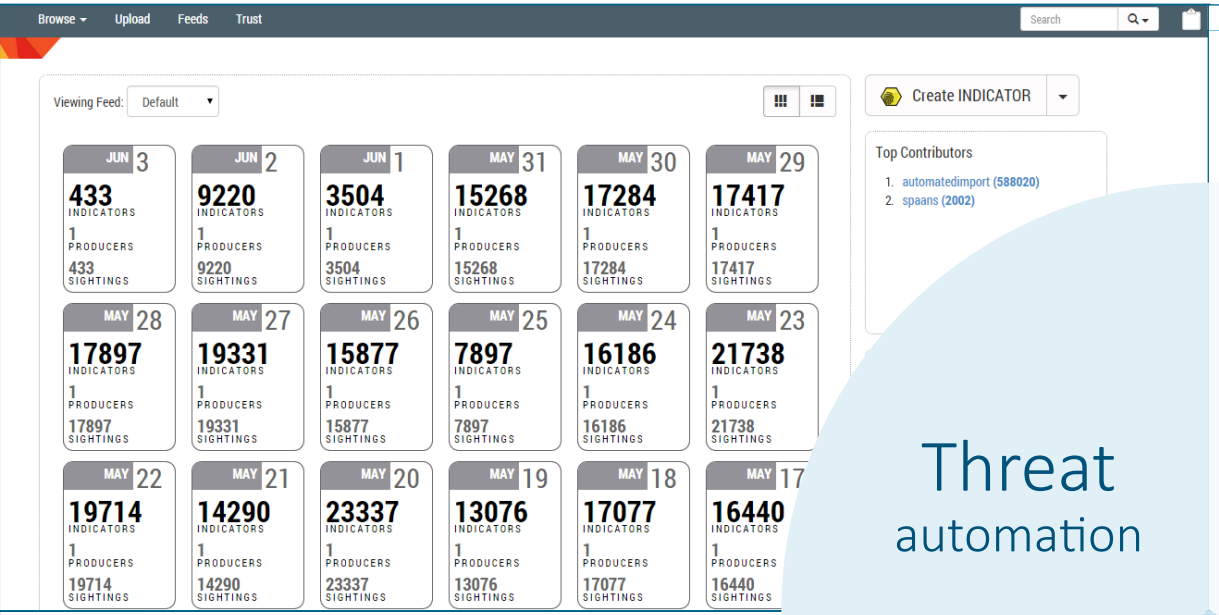
ATS: expensive setup, scales well

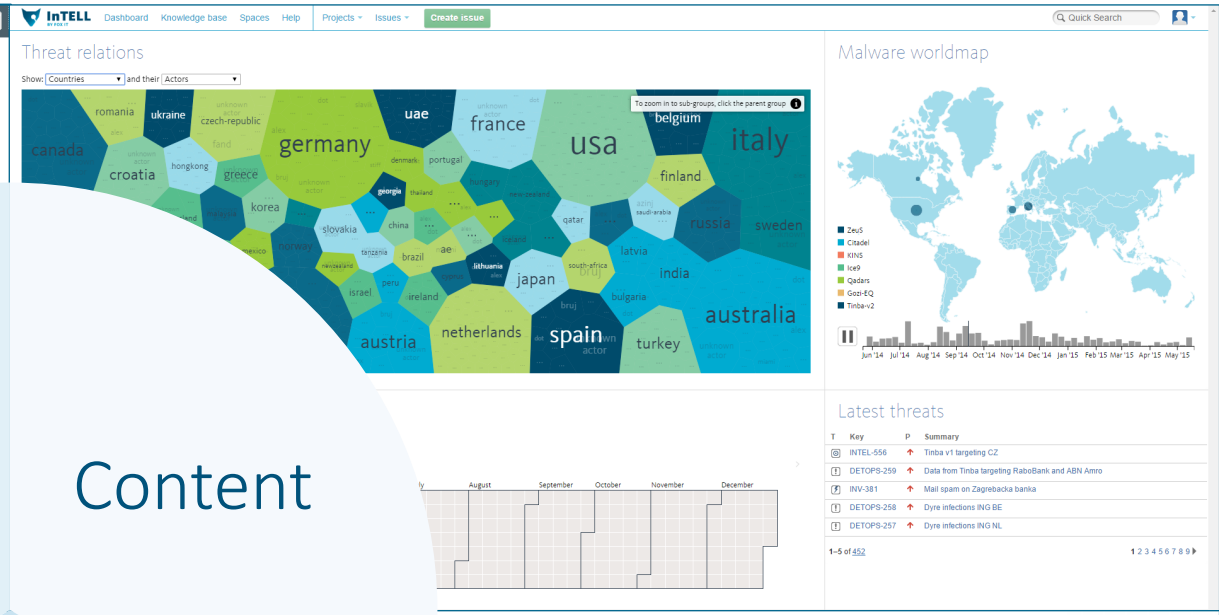
Hybrid: cheap to setup, scales less


KINS /
vmZeuS
Dyre
ZeuS v2
Feodo /
Bugat /
Cridex
Gozi
Kits
ZeuS
varia
Shylock
SpyEye2
(Tilon)
Slave
Dridex
iBanking
Rogue
Mobile
App
Lego
Perkele
Rogue
Mobile App
Hesperus
Ramnit
Gozi /
verQuest
Retefe
ReactorBot
Backoff
PonyLoader
Hermes
Kronos
Other
ATM
malware
Other
mobile
malware
Qbot/Qakbot
Anunak
SpyEye
unknow
family
Tinba
PowerZeuS
Vskimmer
Shiz
Ice-IX
Citadel
Other
POS
Qadars
Sinowal
/ Torpig
-RAT

Threats in Italy

Sharing, content & automation

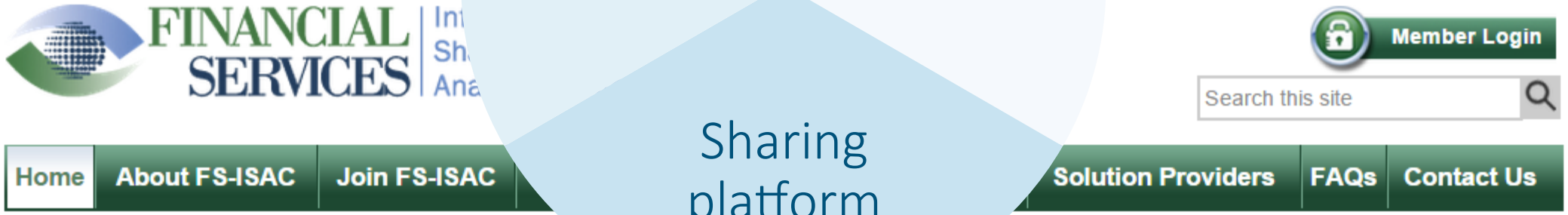




Threat automation

Content

Sharing platform



Attacks & anomalies

day - month - year

Rule group	Alert count	Alerts over time
Beneficiary blacklisti...	5	
Change detection	54	
Cookie anomalies	0	
Cookie blacklisting	17	
IP blacklisting	3	
Logon anomalies	35	
Machine blacklisting	0	
Phishing and phishin...	0	

Cases

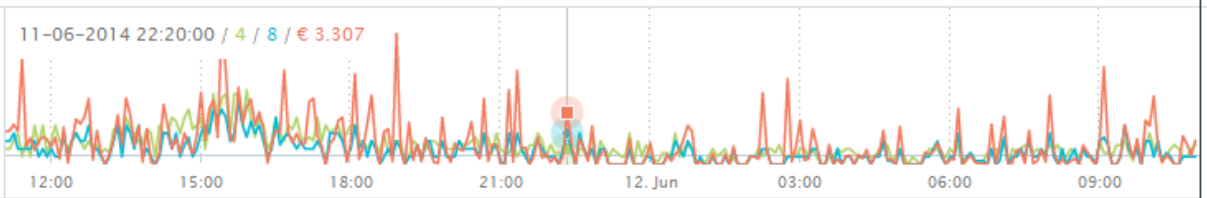
ID	External ...	Description
C6	201405...	Session changes to a different IP.
C7	201405...	Possible infection
C8	201405...	Additional post parameters found.
C9	201405...	Strange behaviour on the mobile ...
C10		r3 demo 1
C12	R3 demo...	This case is a **demo** case.
C13	IPCh 1	IP change case 1
C14	ID-4374...	

Channels (2)

day - month - year

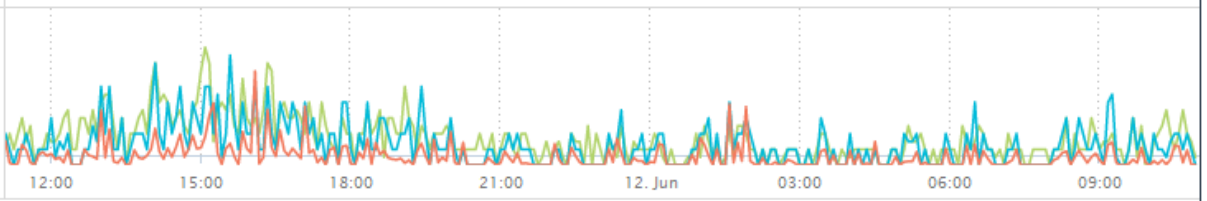
main

Sessions:	1.394
Transactions:	1.002
Transaction amount:	€ 378.026



mobile

Sessions:	979
Transactions:	772
Transaction amount:	€ 319.488



System

Current version:	3.0.6
Last deployment:	03-06-2014 15:15:13
Active users:	12

The game is not about malware anymore

Threats evolve, they don’t appear out of nowhere

Successful organizations share

In intelligence, content is key

Use it to protect your channels in real-time