

Cybersecurity for Latvia

Disrupting cybercrime with public/private partnerships

Jean-Christophe Le Toquin
Director, Digital Crimes Unit
Microsoft EMEA

Riga, 8 November 2012

Microsoft Digital Crimes Unit



Transforming the fight against digital crime
through ***partnerships*** and legal and
technical
breakthroughs that ***destroy*** the way
cybercriminals operate



Agenda

Yesterday's dream and its unexpected consequences

Is isolation our best protection ?

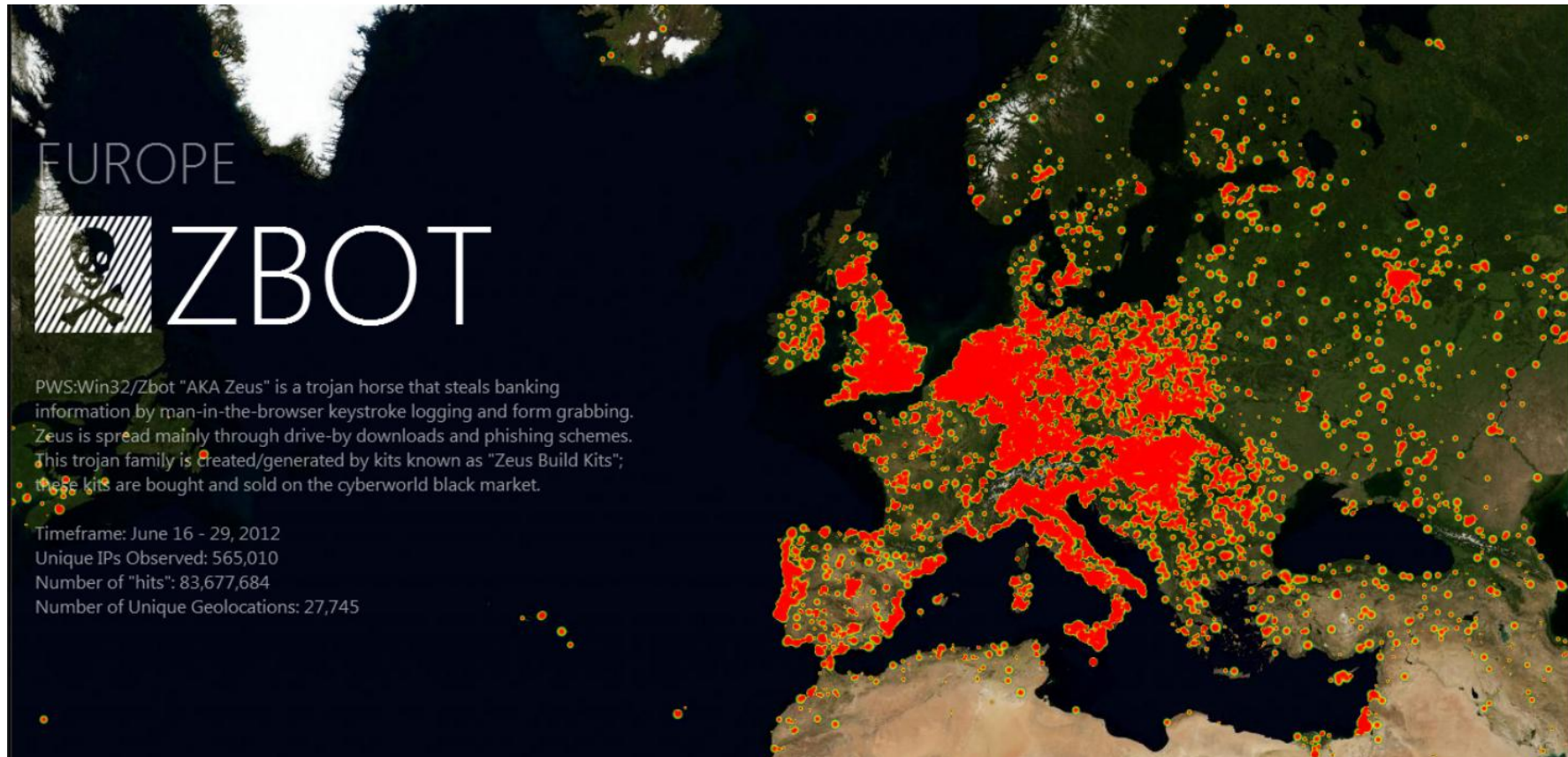
Big ambitions start with small achievements

Yesterday's dream...
and its unexpected consequences

Bill Gates' dream in 1977 :

“A computer in every home”

Our reality 35 years later



The Internet now has 340 trillion trillion addresses

CNNMoney

229 comments

By David Goldman @CNNMoneyTech June 6, 2012: 9:13 AM ET



FROM: WORLDIPv6LAUNCH.ORG

The IPv6 launch has expanded the number of Internet addresses to 340 undecillion.

Is isolation our best protection?

Isolation within companies and government



Fragmentation

Communication

Roles and
Responsibilities

Expertise

Isolation between Cybersecurity and Cybercrime



Cybercrime:
Offenses involving
ICT

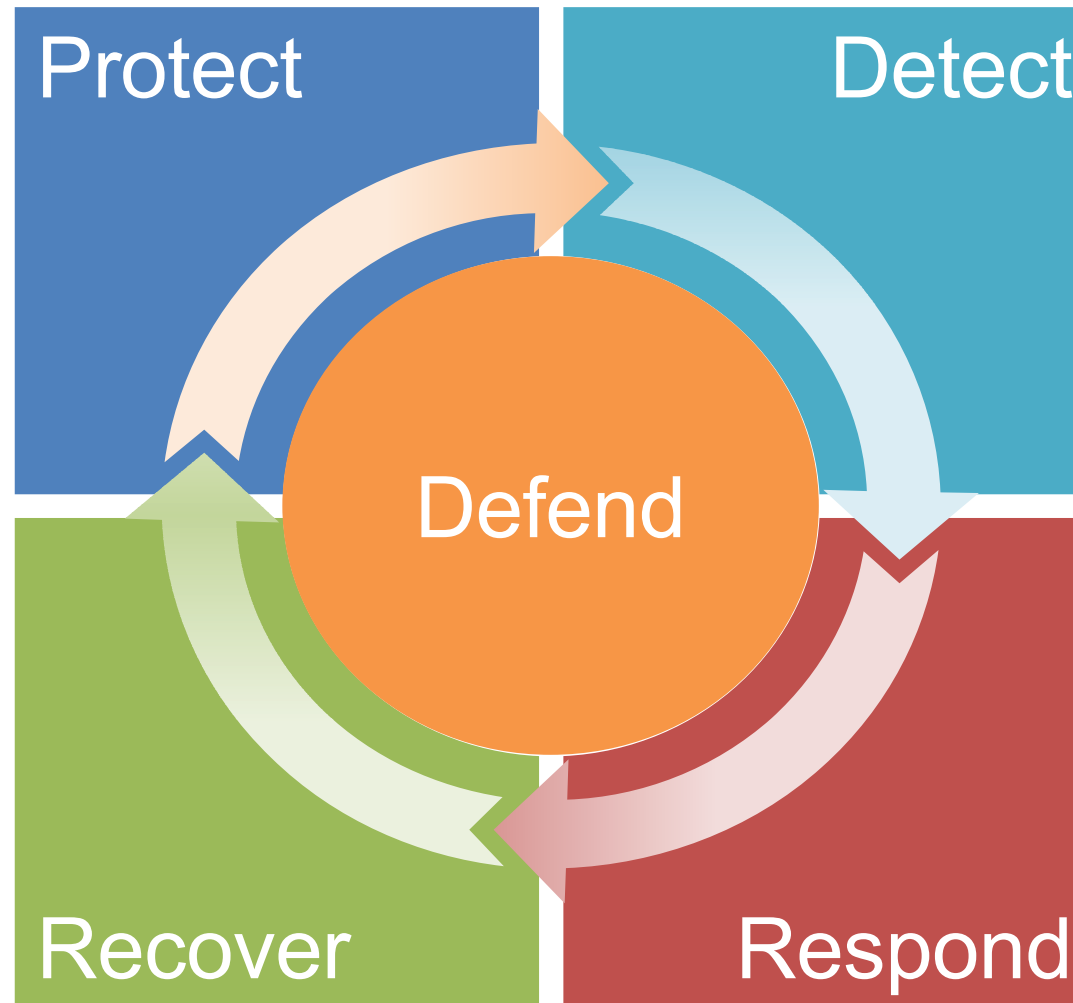
Both: offenses by
means of ITC

Cybersecurity:
non-intentional
incidents

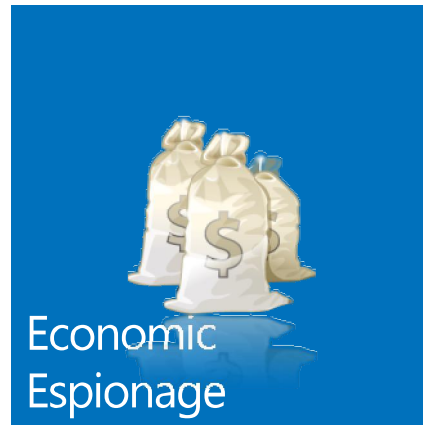
Both: intentional
incidents

Source: Council of Europe

Isolation between protection and response



Isolation among Cyber Threat Categories



A national agenda to help break silos



Cybersecurity agenda

Strategies /
Policy

ICT
Infrastructure

National
Projects and
Solutions

Relationship

Social, Economic, Political and IT Alignment

Cybersecurity agenda

Strategies /

2CENTRE
Cybercrime Centres
of Excellence Network

FOR TRAINING RESEARCH AND EDUCATION



Intrusion

Botnets

Infrastructure

ID
Theft

National
Information
Sharing Centers

Relationship

Incident
Reporting

Information
Sharing

Social, Economic



Botnet
takedowns

- Digital Crimes Community Portal
- Digital Crimes Consortium
- Threat Intelligence



ment



Big ambitions start with small
achievements...

Elements of a national dental health agenda





Since 2010, Microsoft disrupts botnets and distribute actionable data on infection to countries



4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

11-CV-00222-BOND

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,
Plaintiff,

Case No. **C11-0222** JLA

v.
JOHN DOES 1-11 CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS,
Defendants.

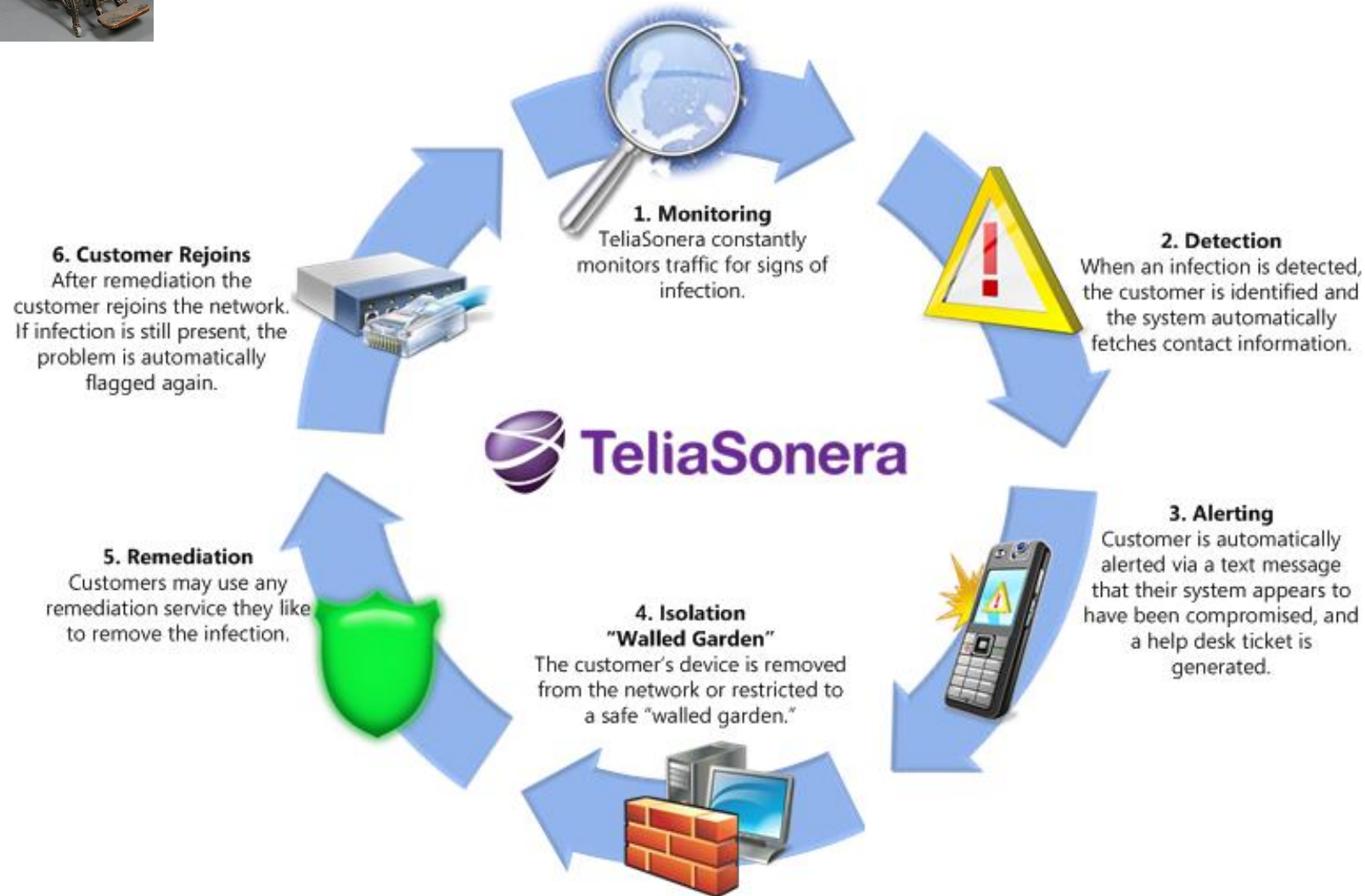
COMPLAINT
****FILED UNDER SEAL****

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges that JOHN DOES 1-11 ("Defendants") are controlling an illegal, notorious, and world-wide computer network known as the "Rastock botnet," made up of end-user computers connected to the Internet, which Defendants have infected with malicious software, and which Defendants consequently can and do direct and control for nefarious and illegal purposes through servers connected to the Internet.



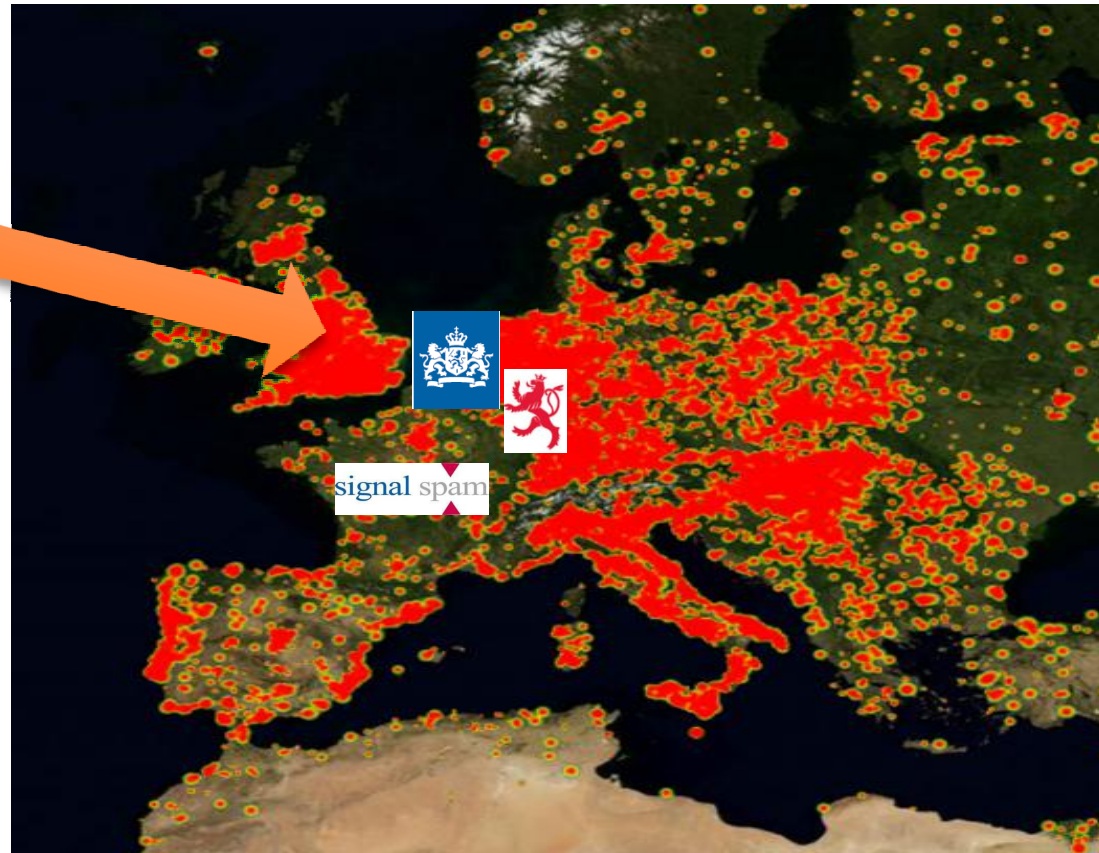


2011 : Delivery of data to ISPs to help them clean their customers





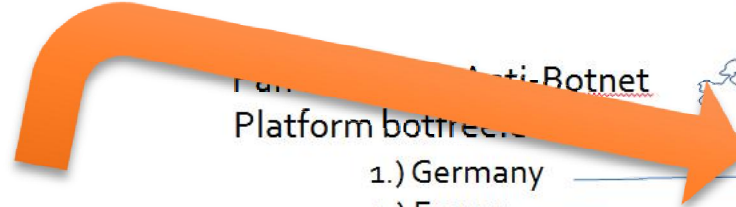
2012 : Delivery of data to national centers to help them clean their country



- Real time data
- Includes IP addresses
- Delivered through Azure Microsoft cloud



2013-2015 : support the EU botnet project for detection and prevention



Partners in the Anti-Botnet Platform botnets

- 1.) Germany
- 2.) France
- 3.) Italy
- 4.) Spain
- 5.) Portugal
- 6.) Belgium
- 7.) Romania
- 8.) Croatia



Advanced Cyber Defense Center brings together 28 partners from 14 countries to detect, analyse, notify and mitigate botnets. 30 months project starting end of 2012.

We have good news for those who believe their teeth, like their computers, do not require care and attention...



you don't
have to
~~brush~~
all your
~~teeth,~~
just the ones
you want
to keep.

Jean-Christophe Le Toquin
letoquin@microsoft.com

