RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

How Microsoft, FS-ISAC & Agari Took Down the Citadel Cybercrime Ring

SESSION ID: HT-R03

Moderator: Patrick Peterson
Founder & CEO, Agari
@Agariinc

Panelists: Richard Boscovich
Assistant General Council
Microsoft

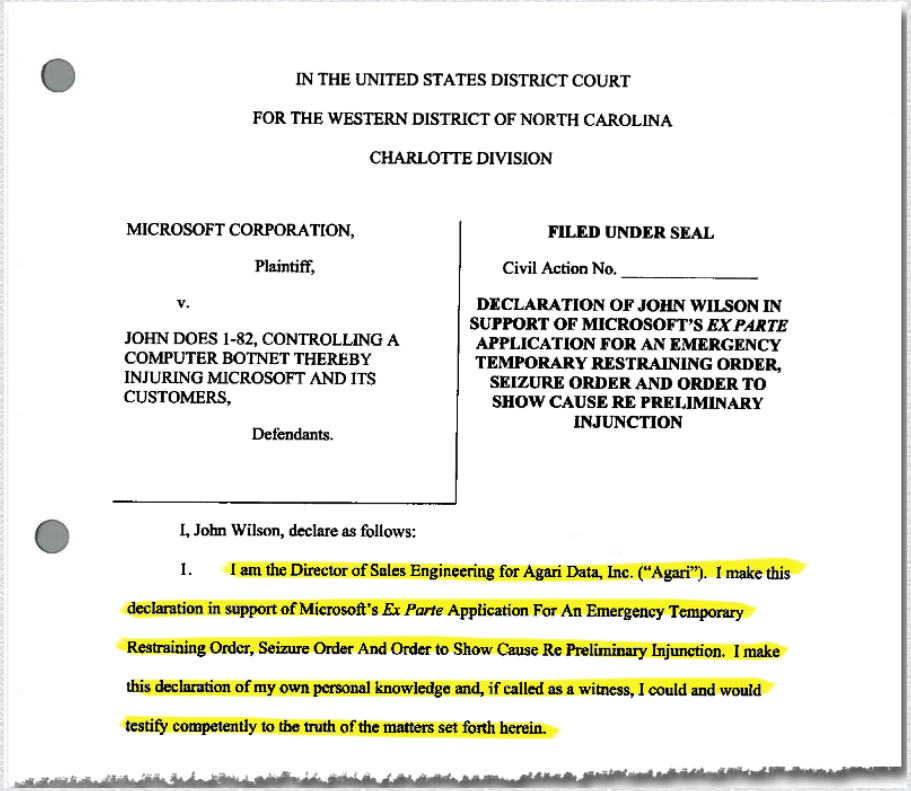
John Wilson
Director, Sales Engineering
Agari

Errol Weiss
Financial Services Information Sharing &
Analysis Center (FS-ISAC) Board Member

Citadel Botnet Takedown – Roles

- **Agari** provided intelligence on Citadel root cause - phishing email with malicious URLs using web exploits for Citadel malware installation
  - Data must be provided at Internet scale and in real-time
- Leveraged data on fraudulent email purporting to be from seven **FS-ISAC** members sent to ~1B consumer inboxes
- Submitted data on 3,762,605 emails from 4 March – 19 April 2013 to **Microsoft** Digital Crimes Unit for analysis
  - 40% phish, 60% malware (Source: Microsoft)

AGARI, FS-ISAC & Microsoft DCU Crush Citadel



IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF NORTH CAROLINA

CHARLOTTE DIVISION

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-82, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,

Defendants.

FILED UNDER SEAL

Civil Action No. _____

DECLARATION OF JOHN WILSON IN SUPPORT OF MICROSOFT'S *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, John Wilson, declare as follows:

1. I am the Director of Sales Engineering for Agari Data, Inc. ("Agari"). I make this declaration in support of Microsoft's *Ex Parte* Application For An Emergency Temporary Restraining Order, Seizure Order And Order to Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

- Agari provided a declaration in support of the TRO, Seizure Order, and Order to Show Cause

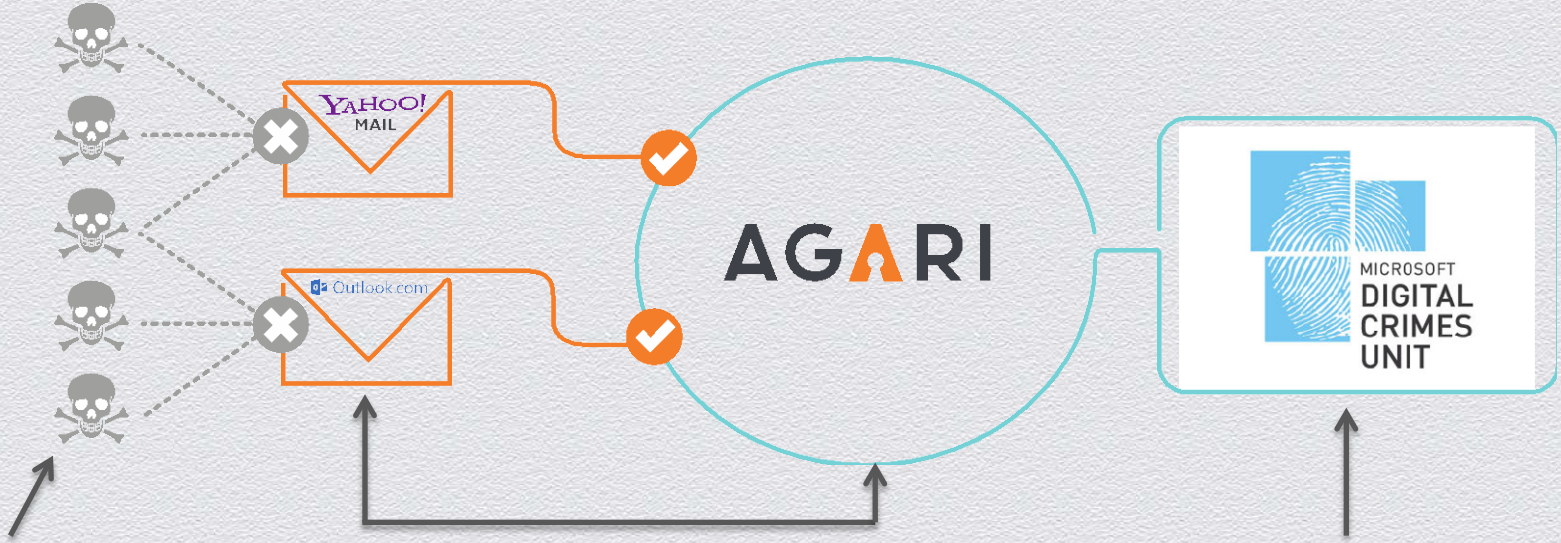
AGARI

Sample of Malicious Emails

Timestamp:	April 15,2013 20:43
From:	LinkedInServices<lybegalka@firstusa.com
Subject:	**You have a new message in your inbox**
Sending IP:	66.207.195.176
URL:	http://203.150.225.61/~mindphotobook/ enthusiastic.html?fa=288746

Timestamp:	April 15,2013 2:08
From:	ional Automated Clearing House Association risk-management@nacha.org
Subject:	**Fwd: ACH Transfer rejected**
Sending IP:	IP: 173.60.91.194
URL:	http://taurus.gaming.free.fr/riding.htm

Data Flow: From Spam to Intelligence

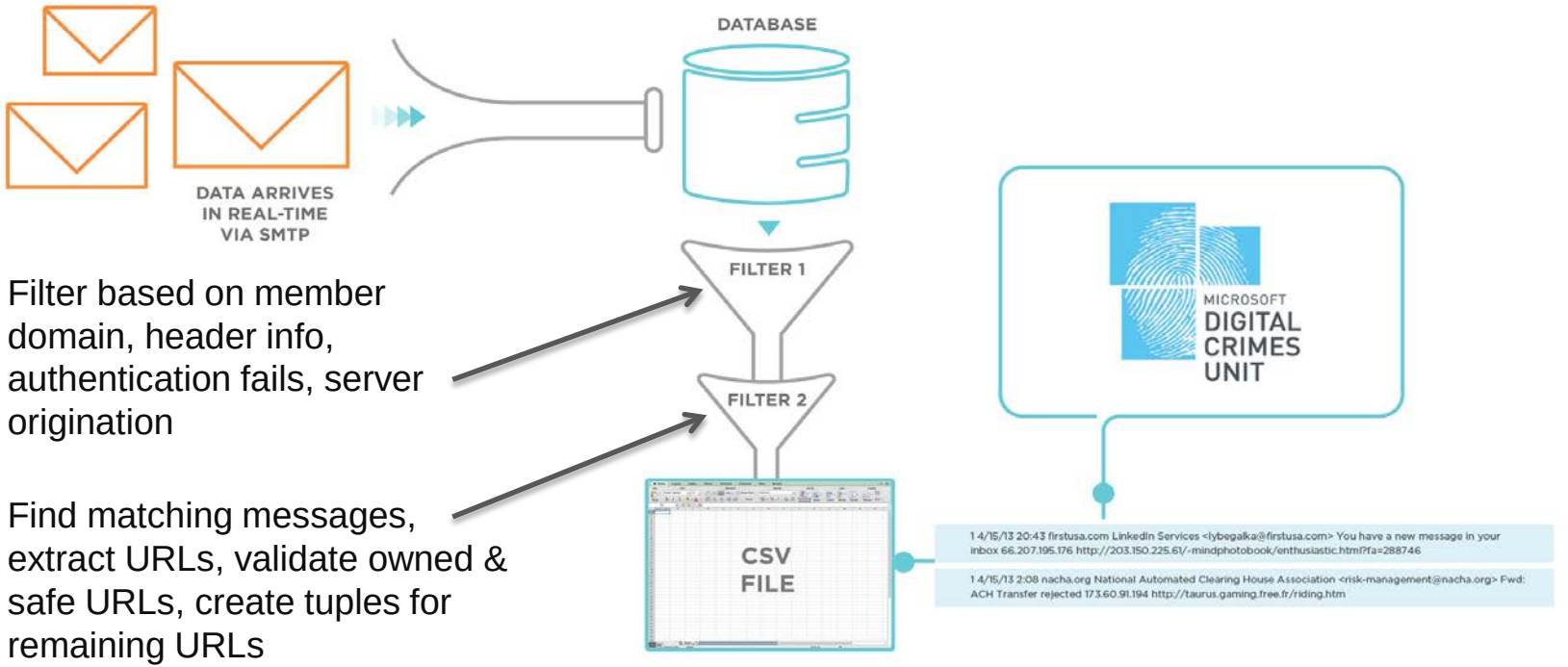


1. Criminals send spoofed messages purporting to be from FS-ISAC members.

2. Microsoft and Yahoo! send forensic copies of the spoofed messages to Agari for analysis.

3. Agari sends forensic analysis to the Microsoft DCU for further analysis and correlation with additional data.

Filtering for Relevant Intelligence

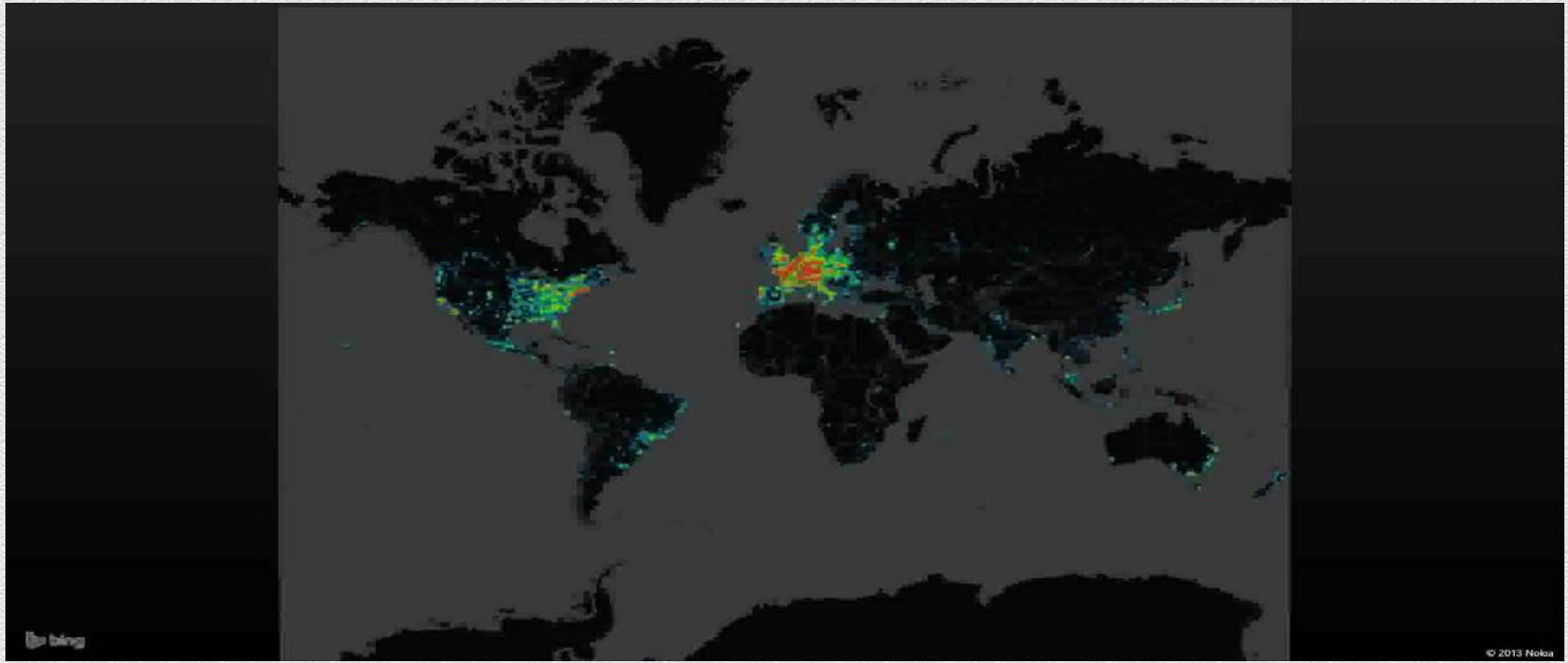


Filter based on member domain, header info, authentication fails, server origination

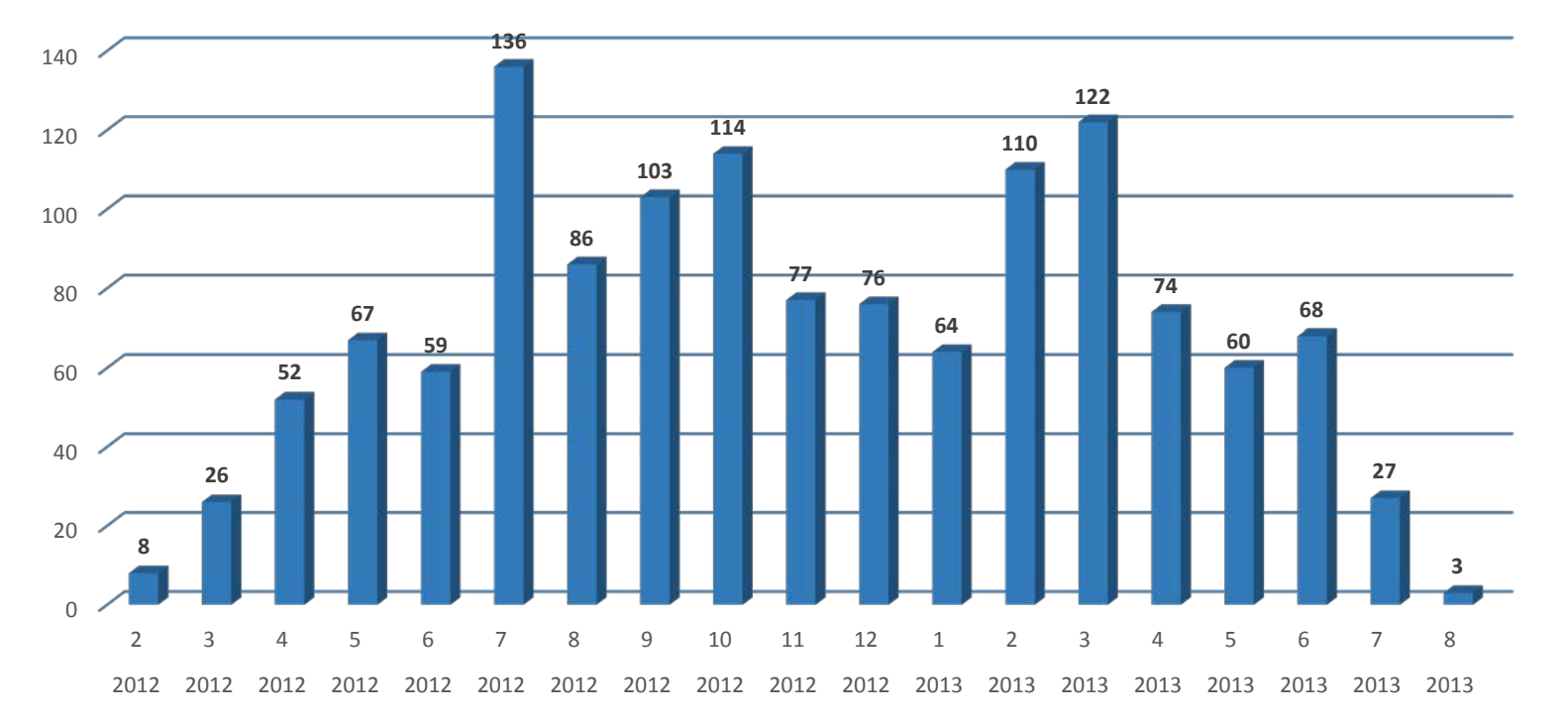
Find matching messages, extract URLs, validate owned & safe URLs, create tuples for remaining URLs

Map of a Single Day's Worth of Data

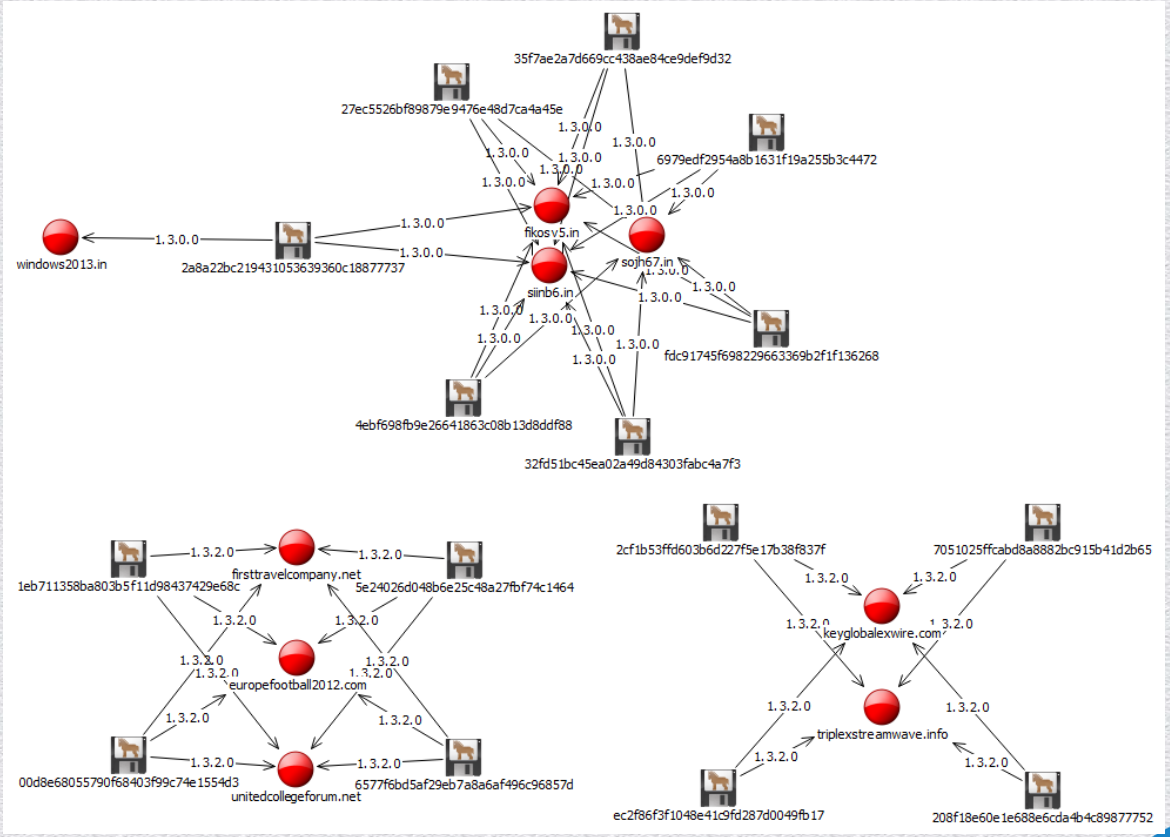
Citadel Infection



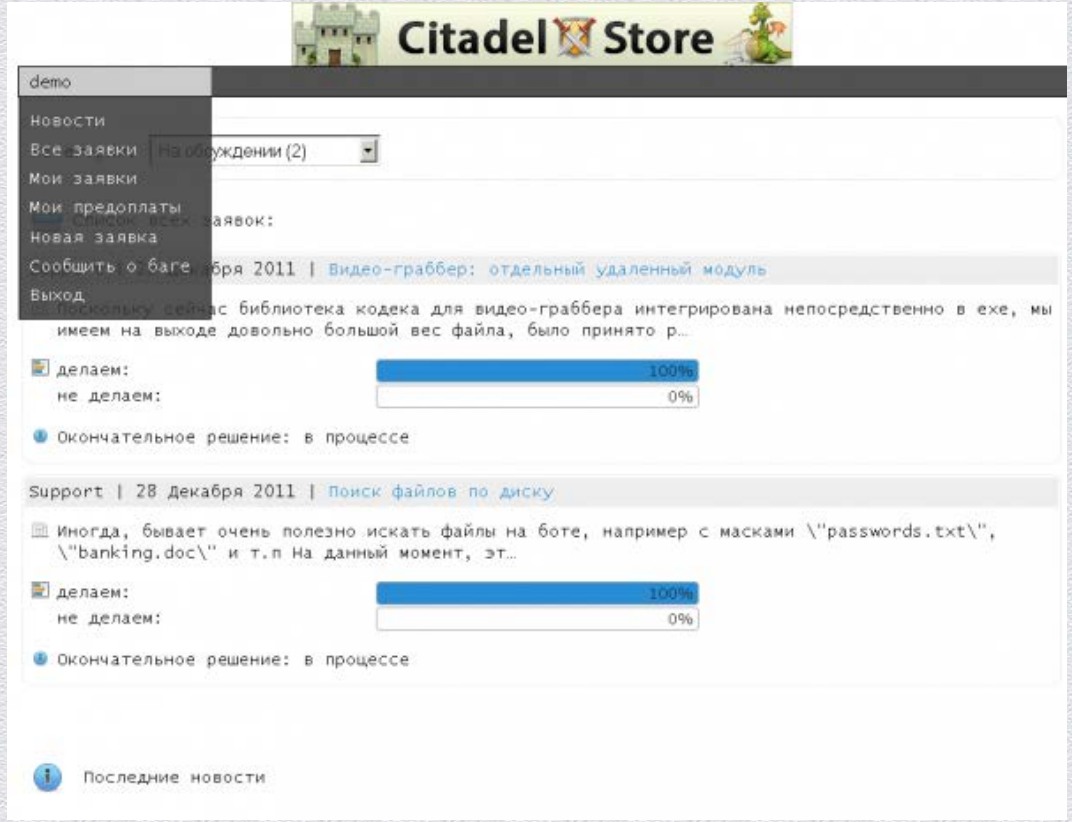
Citadel 2012 - 2013



Citadel Dependency



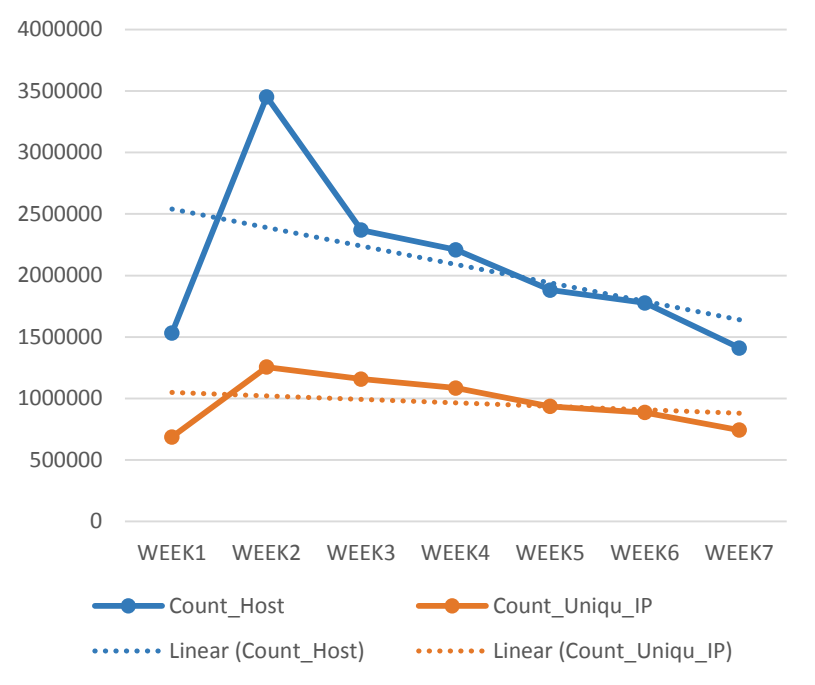
Citadel Store



Citadel Highlights

- Disrupted 82.22% of Citadel botnet
- Microsoft Sinkhole has 67% of Citadel botnet
- Coordinated takedown of 1450~ IP addresses globally
- New direction in public-private partnership

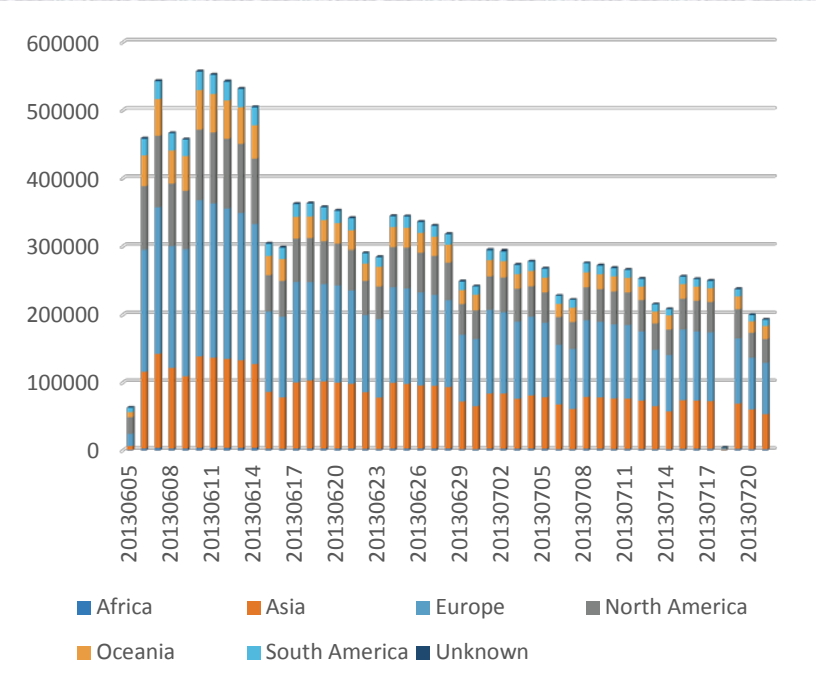
Citadel Sinkhole MIS - Volume

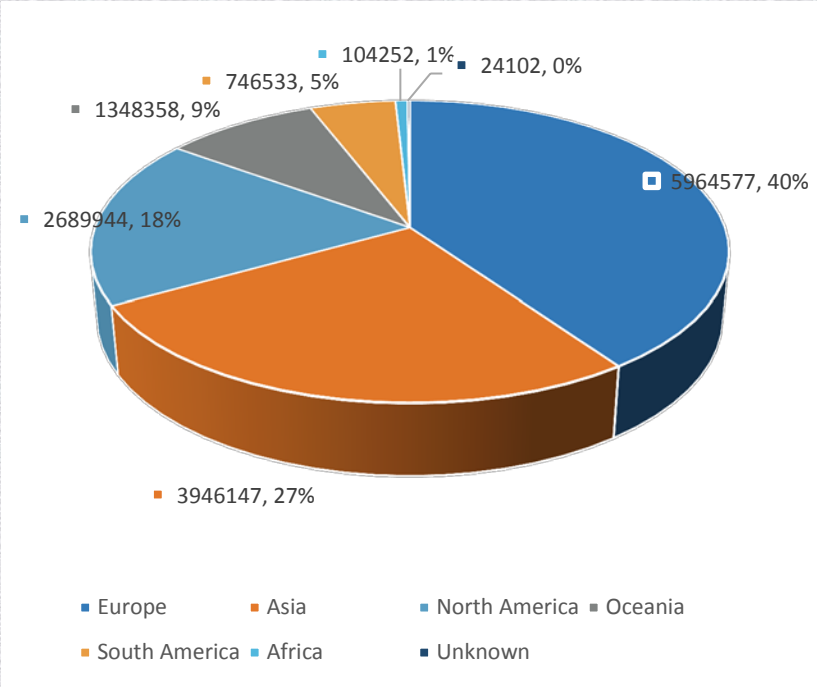


- 14,823,913 unique host
- 5,259,350 unique IP address

- 78% decrease in unique host
- 40% decrease in unique IP address

Citadel Sinkhole MIS - GeoLocation





Top 10 Victim Countries

Infection by Host

Country	Count
United States of America	1693059
Thailand	1636119
Germany	1443381
Australia	1280594
Italian	1015104
Canada	810518
Poland	718393
India	688620
France	630287
Japan	557652

Infection by IP Address

Country	Count
Germany	808824
Thailand	659863
Italy	513389
India	498255
Poland	338368
Australia	290945
United States of America	250922
Brazil	217252
United Kingdom	153363
Japan	126674

Partnerships are Key

Direct Engagement ISP / CERT	Smart Network Data Services	Threat Intelligence Vendors
Electronic Service Providers	Network Infrastructure	Third Party Software Developers

Microsoft Cyber Crime Center

AGARI

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

THANK YOU!