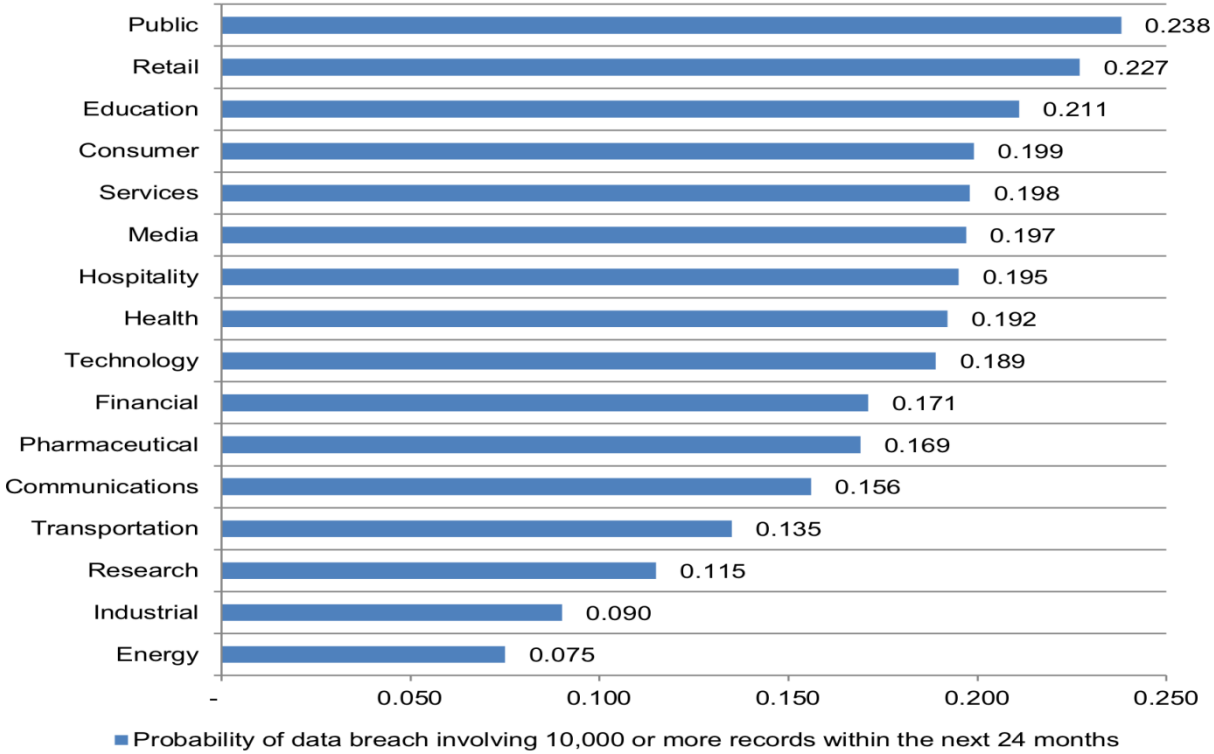
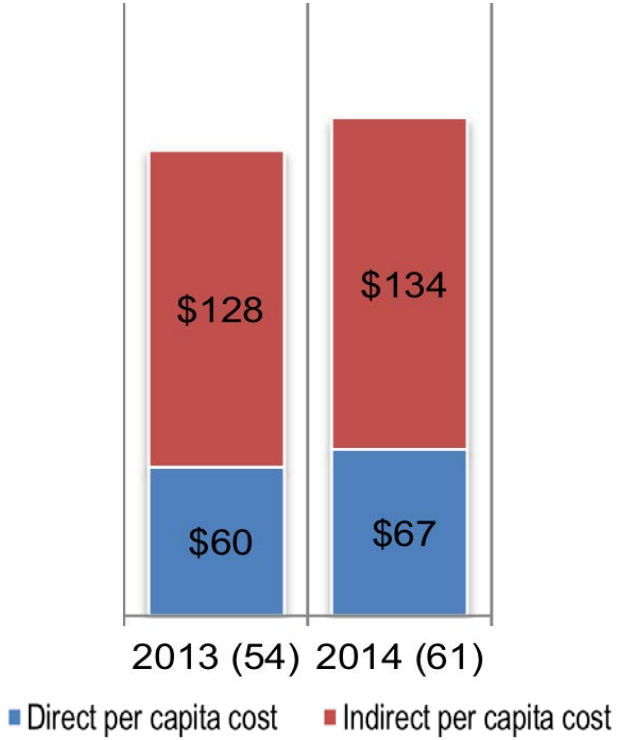
EMERGING THREATS & STRATEGIES FOR DEFENSE

Stephen Coty – Chief Security Evangelist

ALERT LOGIC

Industry Analysis – 2014 Data Breaches - Ponemon





Ponemon 2014 Data Breach Report

ALERT LOGIC

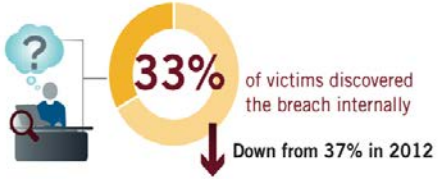
Industry Analysis – 2014 Data Breaches - Mandiant

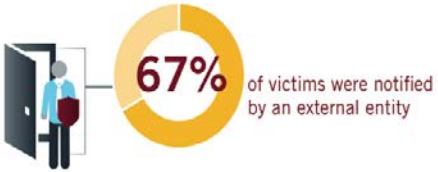
Across the Cyber Threat Landscape

	NUISANCE	DATA THEFT	CYBER CRIME	HACKTIVISM	NETWORK ATTACK
Objective	Access & Propagation	Economic, Political Advantage	Financial Gain	Defamation, Press & Policy	Escalation, Destruction
Example	Botnets & Spam	Intellectual Property Theft	Credit Card Theft	Website Defacements	Destroy Critical Infrastructure
Targeted	✗	✓	✓	✓	✓
Character	Automated	Persistent	Opportunistic	Conspicuous	Conflict Driven

	IRAN-BASED	CHINA-BASED
Industries Targeted	2 Energy, state government agencies	33 Most industry sectors
Victim Selection	Limited based on vulnerabilities	Varied and independent of vulnerabilities
Available Tools	Publicly available	Specially created, customized, publicly available
Date of Initial Mandiant Observation	2012	At least 2006
Detected by Victim	75%	33%
Average Time Spent in a Victim Organization	28 days	243 days
Re-Compromise After the Initial Security Incident	Not witnessed	40% of cases

How Compromises Are Detected





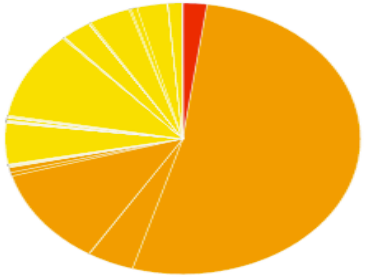
Time from Earliest Evidence of Compromise to Discovery of Compromise

Phishing Email Trends

ALERT LOGIC

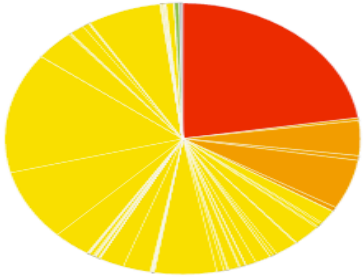
Global Analysis

All Attackers



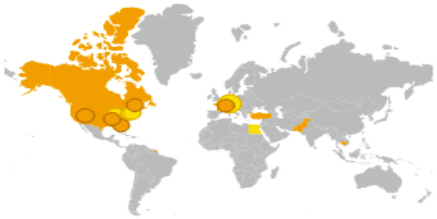
Attacker	Last 60 Days
Cyber Caliphate	
Anonymous	
Chinese hackers	
Estado Islámico	
Islamic State in Ir	
Pakistan	
Syrian hackers	
3xp1r3 Cyber Arr	
al-Assad	
Algerian hackers	
Asia	
Australia	
Bangladesh Grey	
Bharatiya Janata	

All Methods



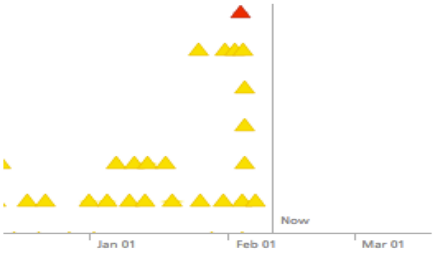
Method	Last 60 Days
d0x	
CVE-2014-3153	
Man In the Midd	
Remote Code Exe	
Trojan	
Watering hole at	
AndroidOS.in	
APT	
Backdoor	
BackDoor.Asniffe	
Backdoor.Botex	
Banking Trojan	
Bedep	
Blackhole	

All Targets



Target	Last 60 Days
Anthem	
Anthony Noto	
Delta Air Lines	
European Parliar	
Forbes	
Forbes.com	
HSBC Holdings P	
JavaScript	
Newsweek	
Papa John's Pizz	
Seth Rollins	
Standard Charte	
Washington Post	
#forbes.com	

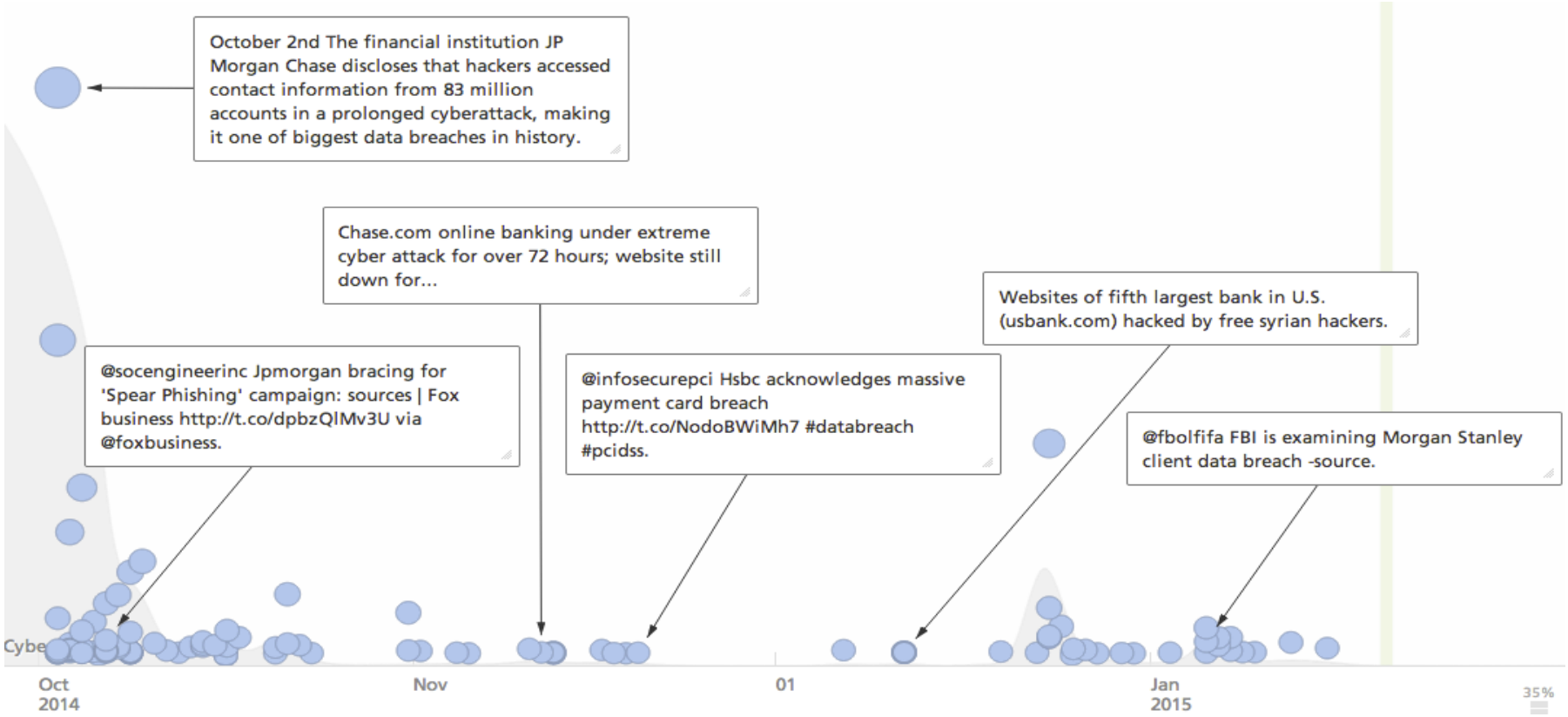
All Operations



Operation	Last 60 Days
OpISIS	
OpAntiISIS	
OpDownfall	
Operation Titsto	
OpFunKill	
OpGabon	
OpGCHQ	
OpICantBreathe	
OpIzzah	
OpLeakageJp	
OpLJ	
OpNSA	
OpESR	
#TheWeekOfHor	

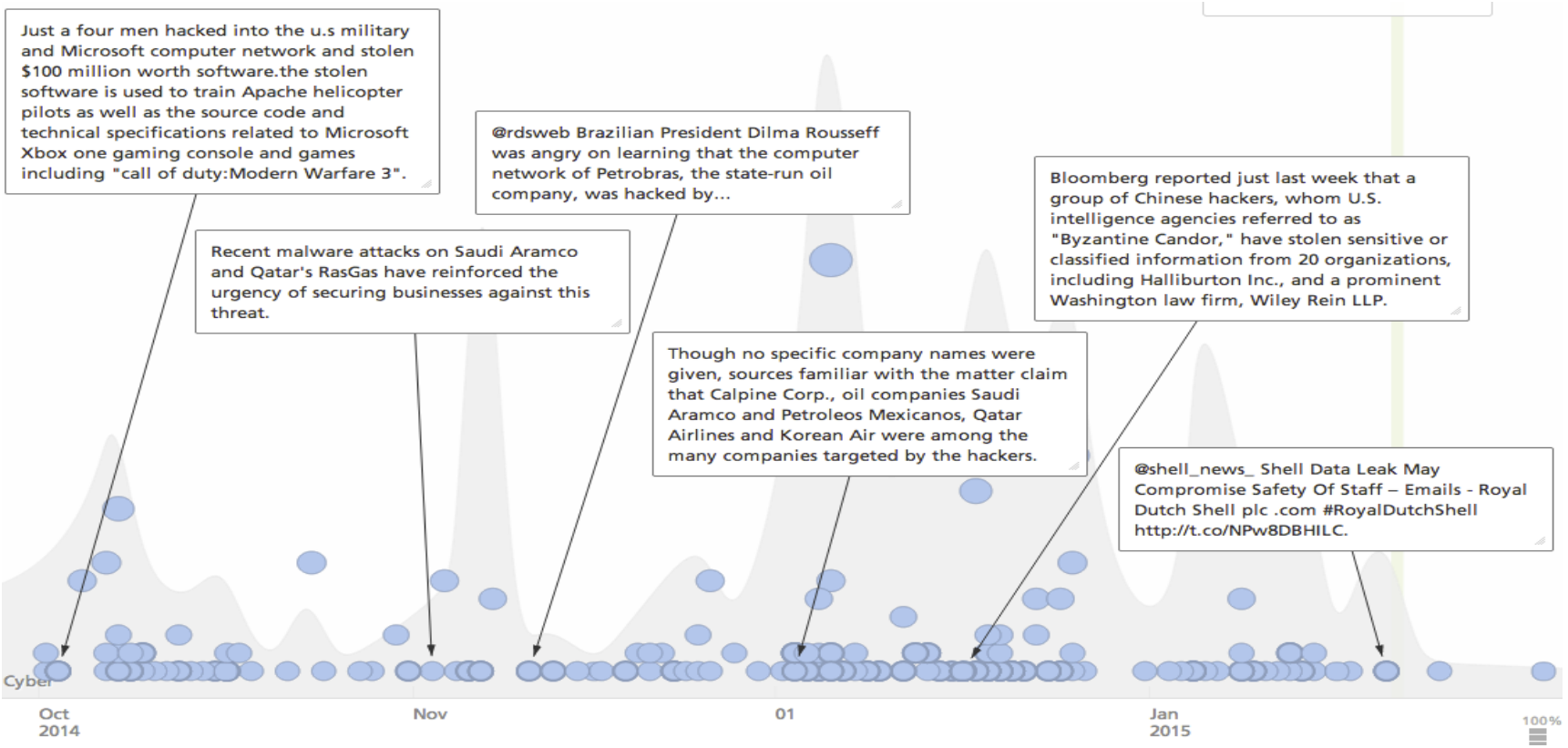
ALERT LOGIC

Industry Analysis - Financial



ALERT LOGIC

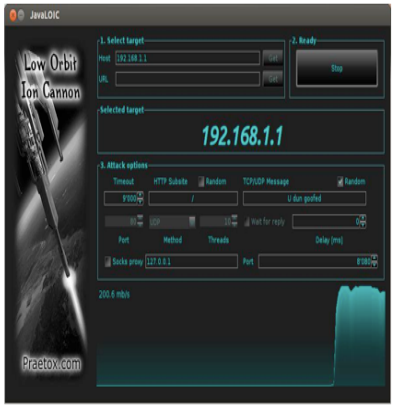
Industry Analysis - Energy



ALERT LOGIC

Where is Hacktivism Today

http://sourceforge.net/projects/javaloic/

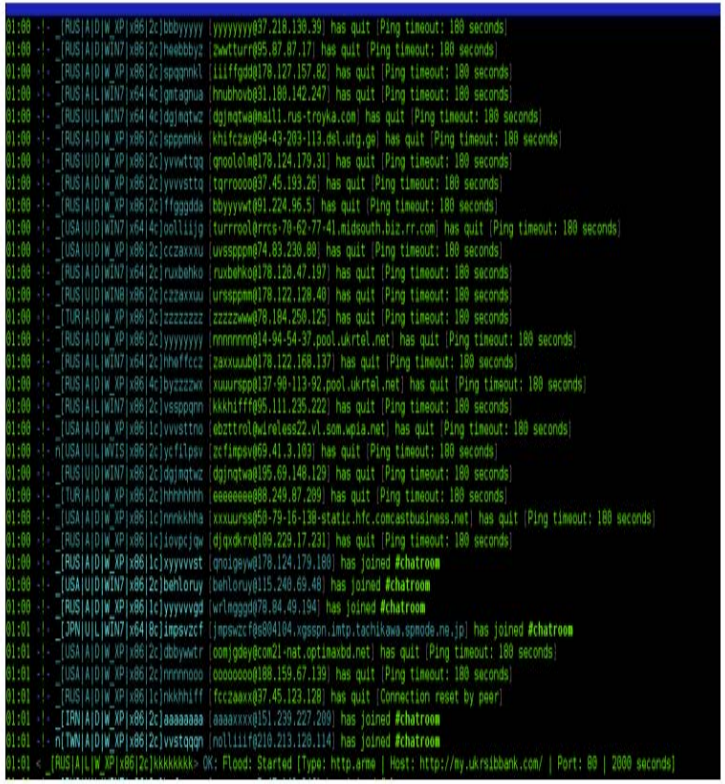


https://play.google.com/store/apps/details?id=genius.mohammad.loic&hl=

Sample of LOIC downloaded in Source Forge running on .Net

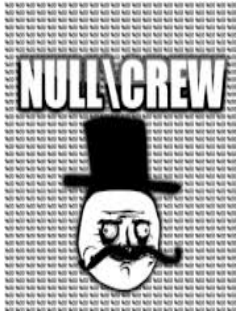
harvi@localhost: file LOIC.exe

LOIC.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows



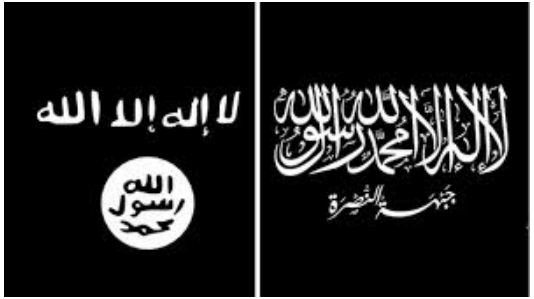
ALERT LOGIC

Different Cells



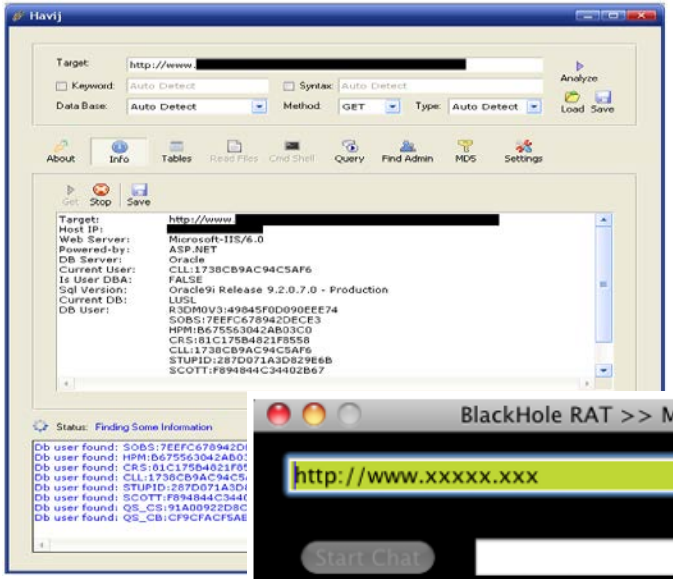
ALERT LOGIC

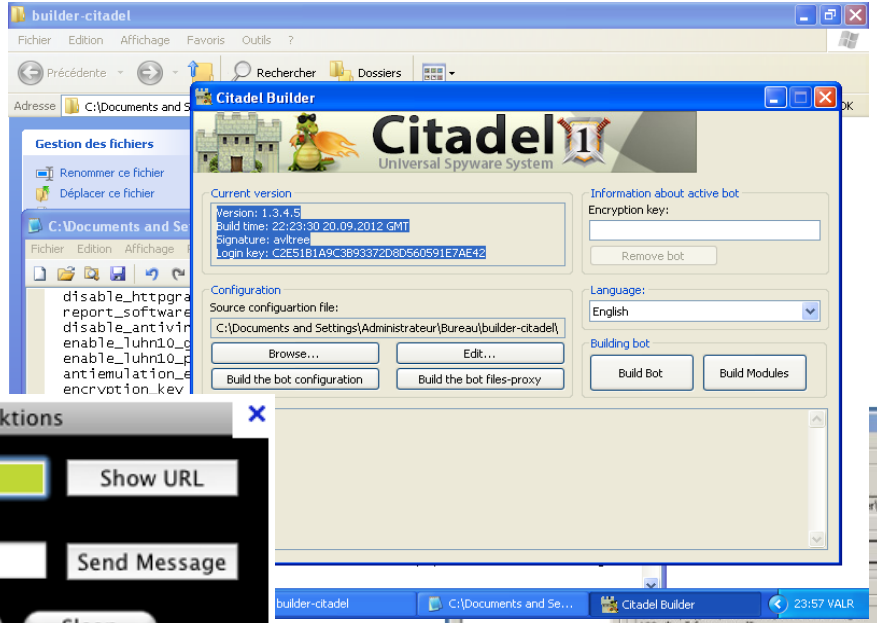
New Groups Emerging

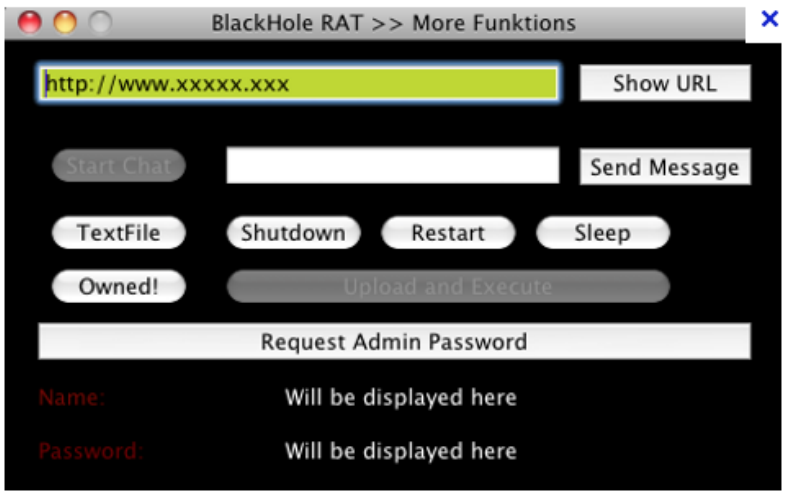


ALERT LOGIC

Tools of the Trade

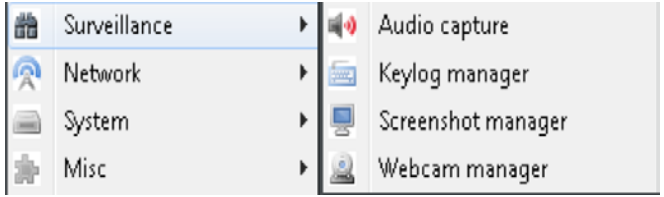


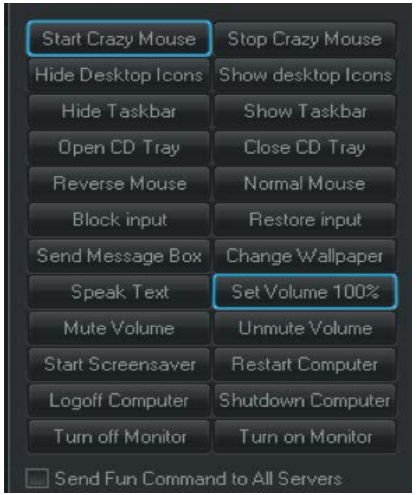


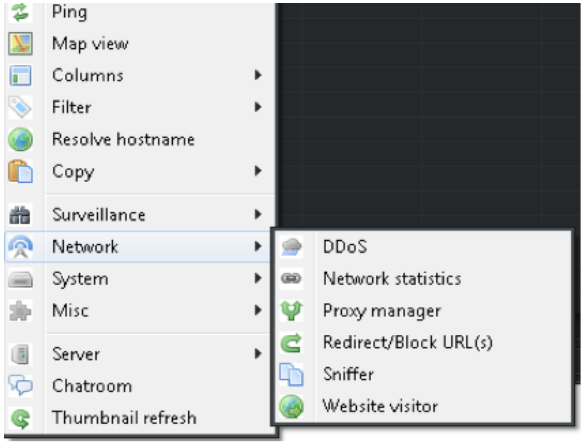


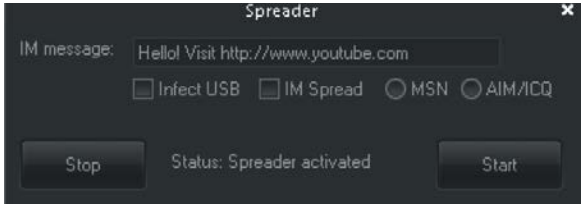
ALERT LOGIC

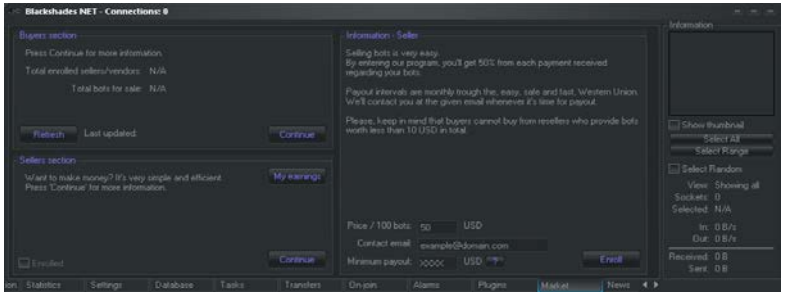
Black Shades RAT





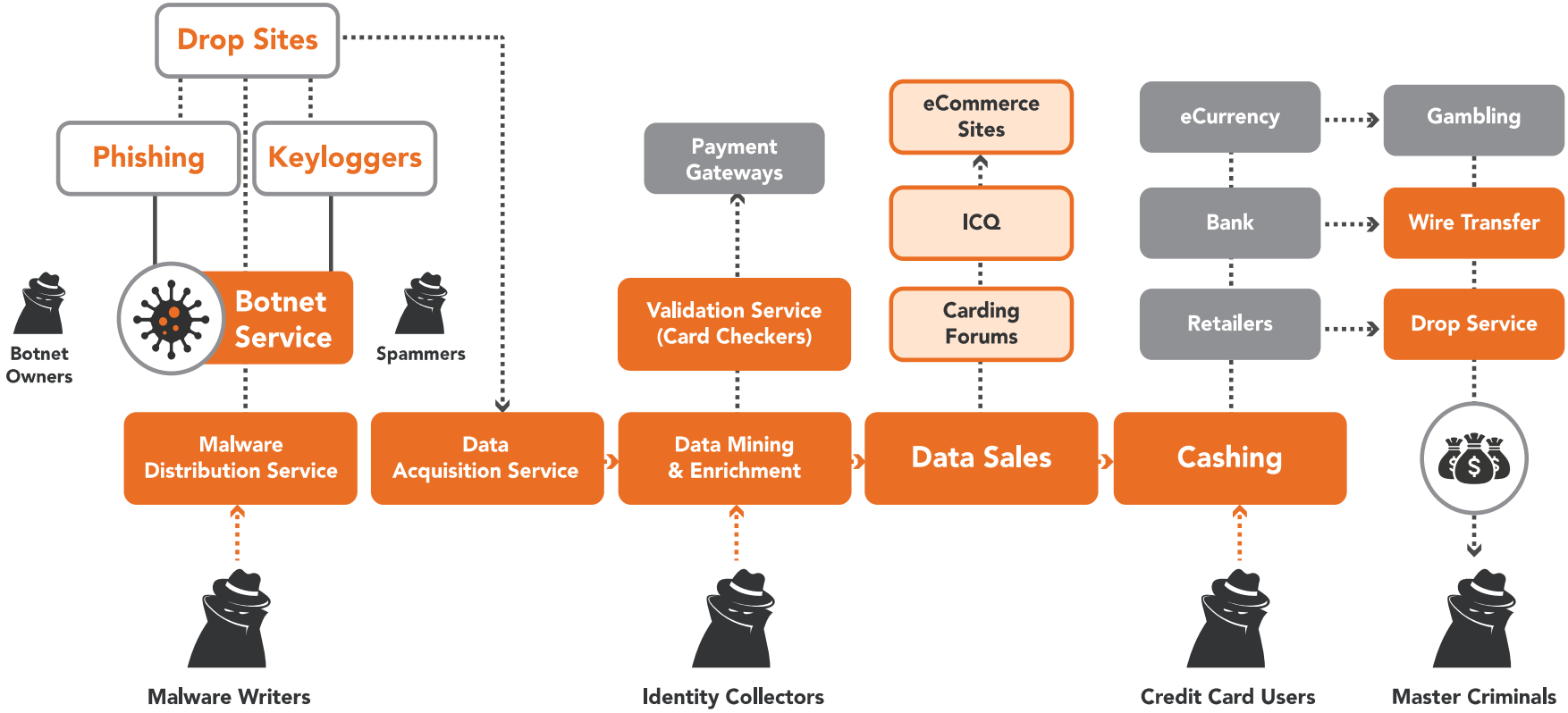






ALERT LOGIC

Underground Economy

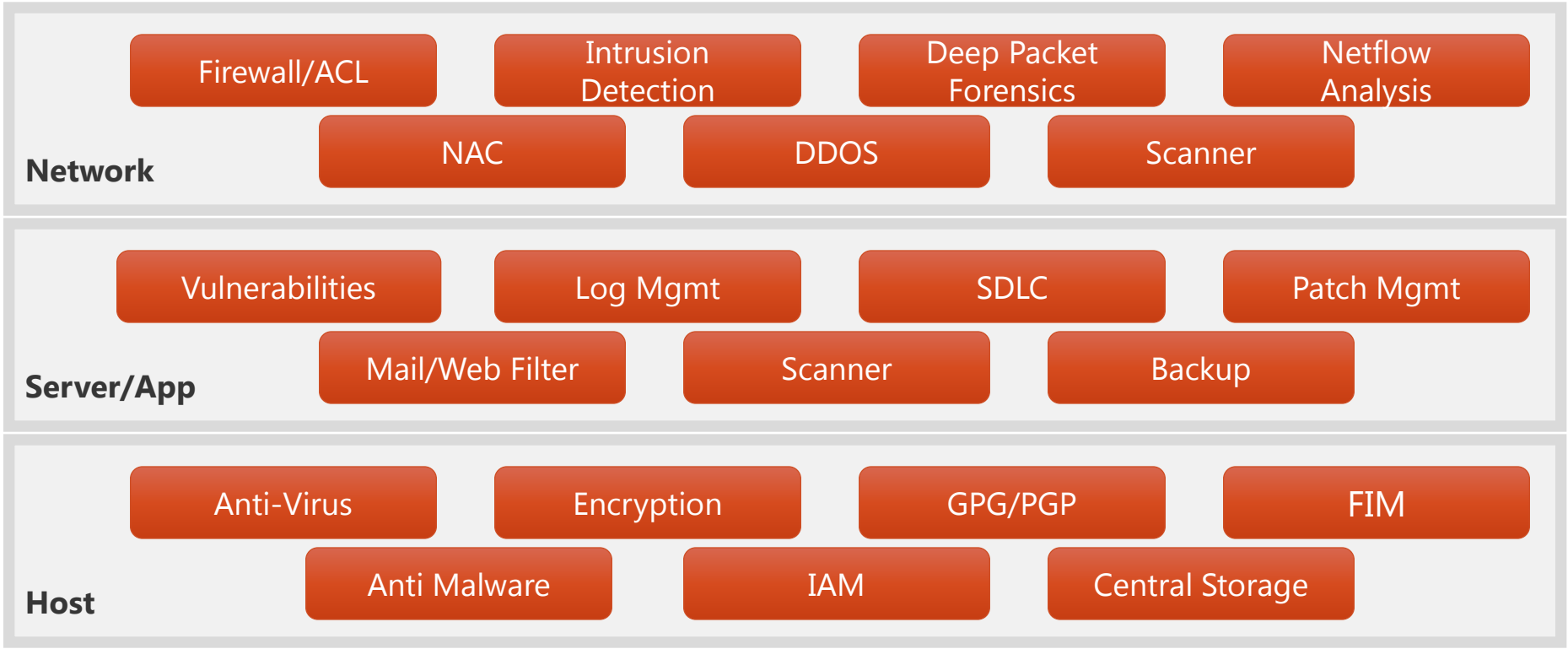


ALERT LOGIC

HOW DO WE DEFEND AGAINST THESE ATTACKS

ALERT LOGIC

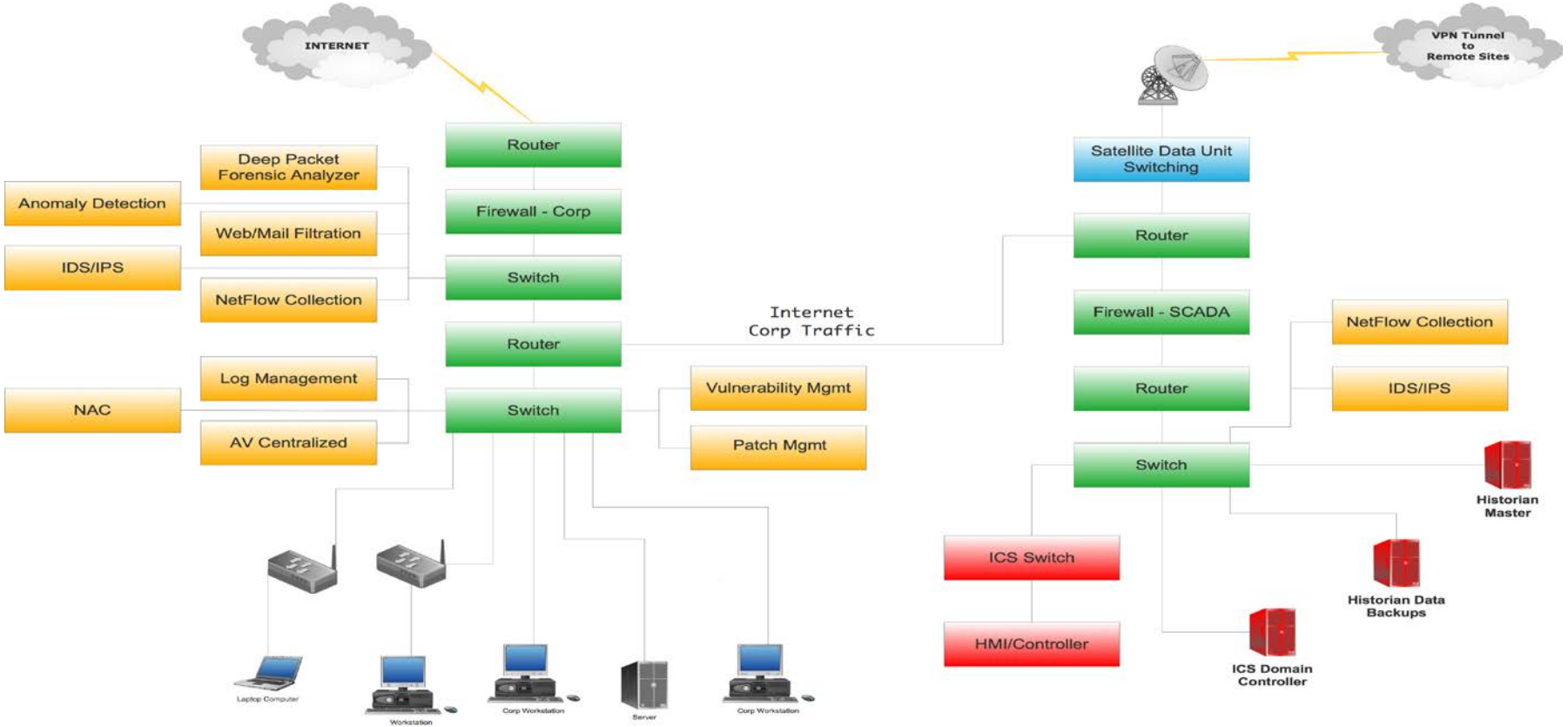
Security Architecture



http://aws.amazon.com/security/security-resources/

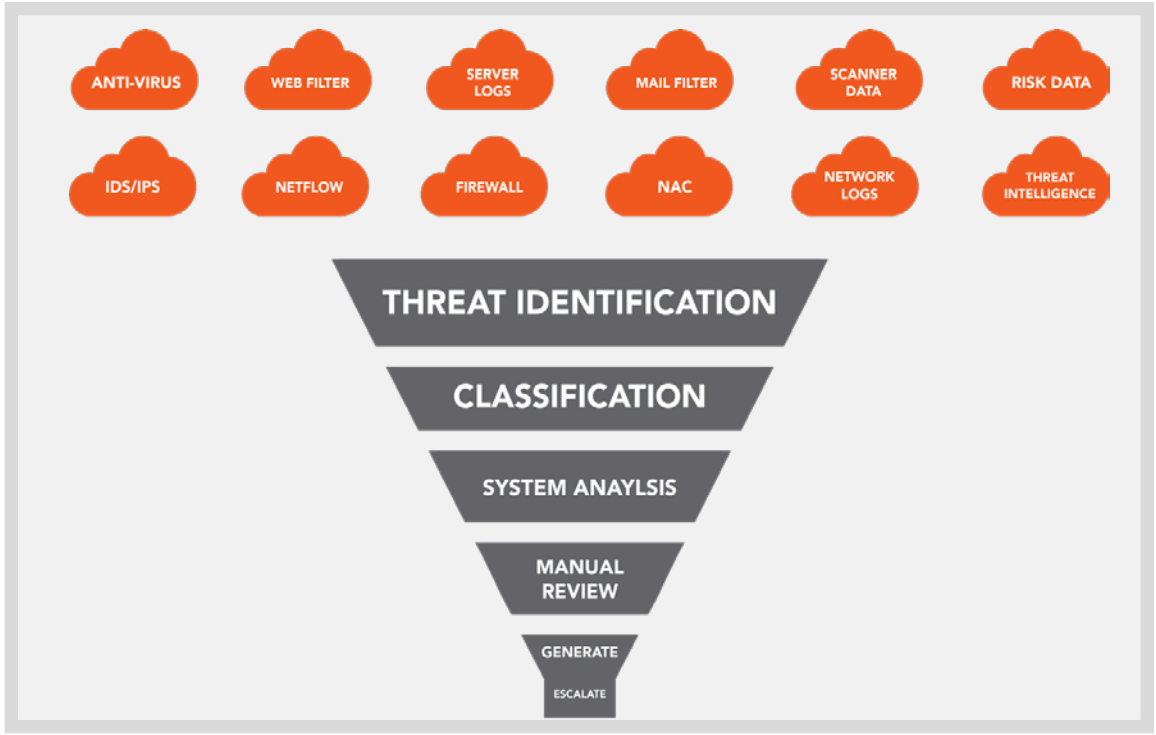
ALERT LOGIC

Deployment



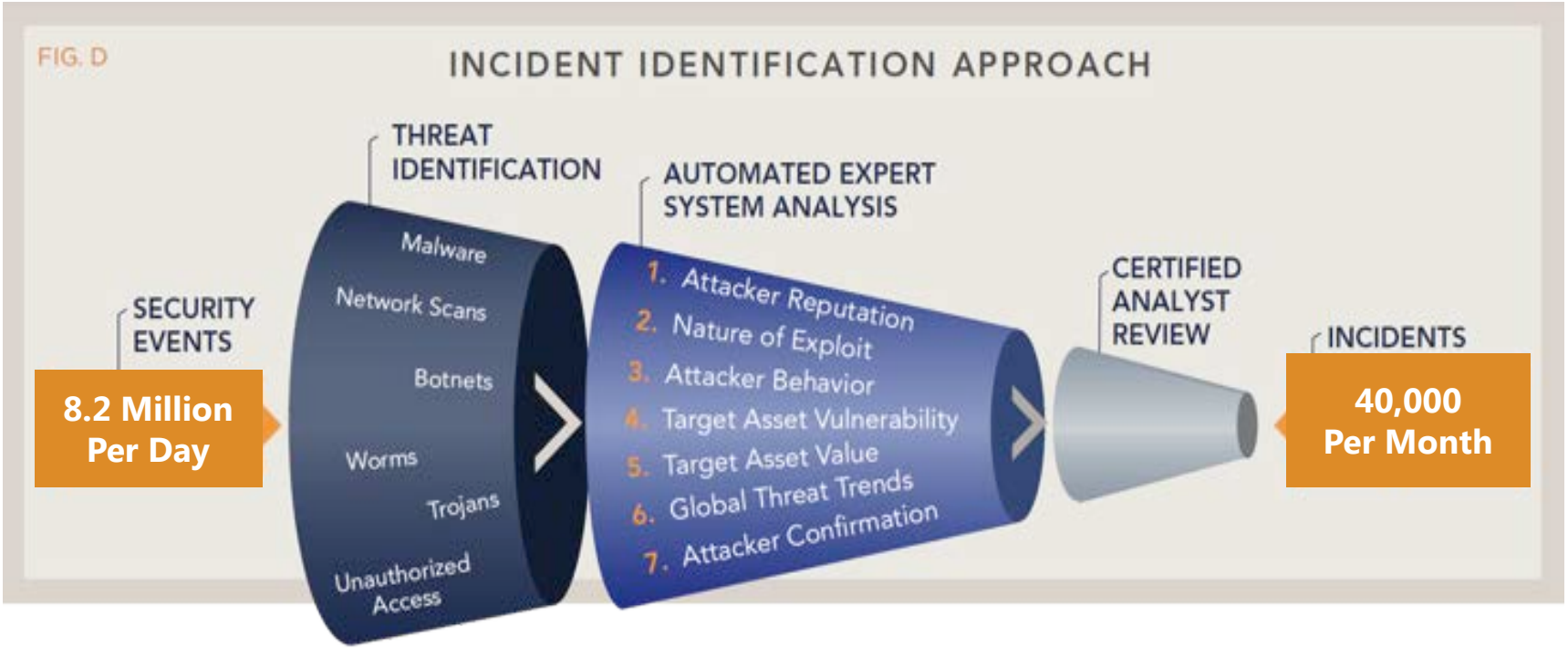
ALERT LOGIC

Data Correlation is the Key



ALERT LOGIC

NGX SIEM Operations



ALERT LOGIC

Enterprise Cyber Security Teams

Monitor and Maintain non-managed hardware deployment uptime

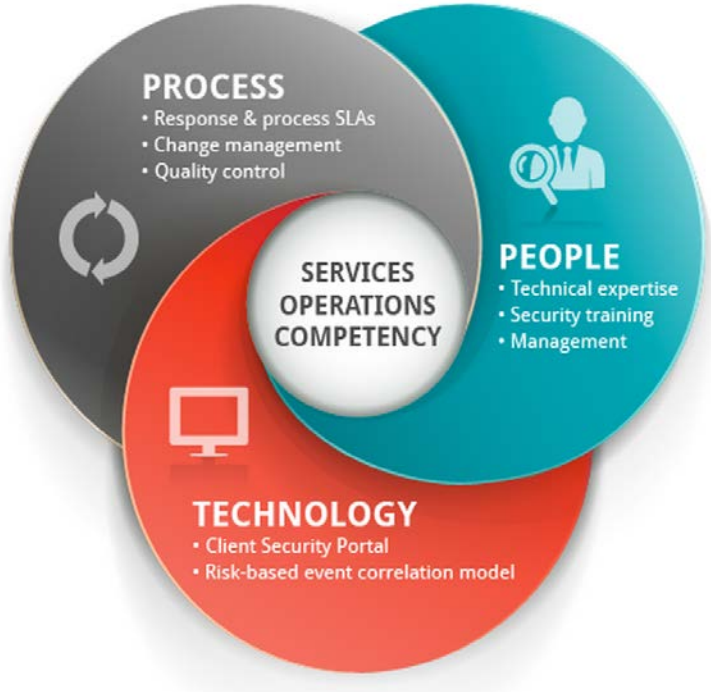
Collect and Maintain content for all non-managed devices

Operational Implementation of all security infrastructure

Cyber Security Awareness Program

Network and Application Penetration Testing and Audit Team

Incident Response Team



24x7 Security Operations Center

Monitor intrusion detection and vulnerability scan activity

Respond to incidents and provide ongoing tuning services as new threats appear

Provide guidance on remediation when incidents are identified

Detect Zero-Day and APT attacks

Proactively monitor web application firewall

Analyze incidents and escalate according to custom requirements

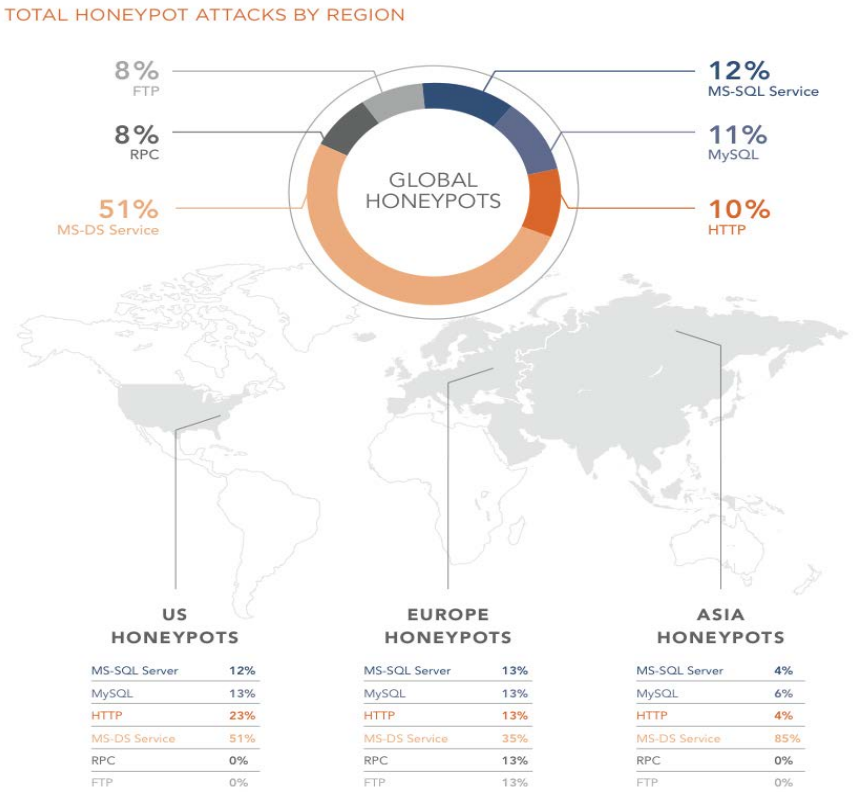
Identify and implement required policy changes

ALERT LOGIC

ALERT LOGIC

Honeypot Findings

- Highest volume of attacks occurred in Europe
- Attacks against Microsoft DS accounted for over 51% of the overall attack vectors
- Database services have been a consistent target
- 14% of the malware loaded on the Honeypots was considered undetectable by AV
- Underscores the importance of a defense in depth strategy for the need to secure your enterprise and cloud infrastructure

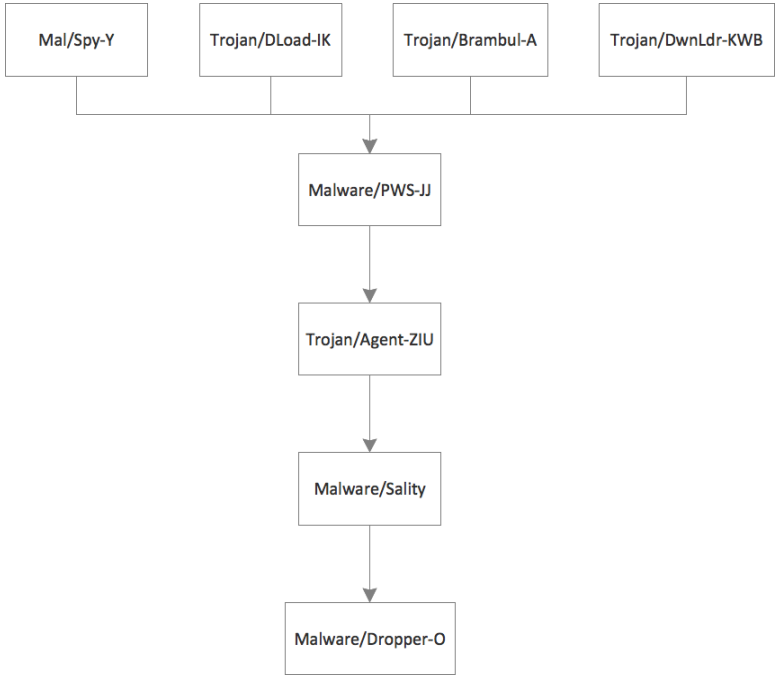


ALERT LOGIC

Samples of Malware detected

If an attacker were using the collected malware to launch an attack against an individual or an enterprise it would be theoretically run in this order.

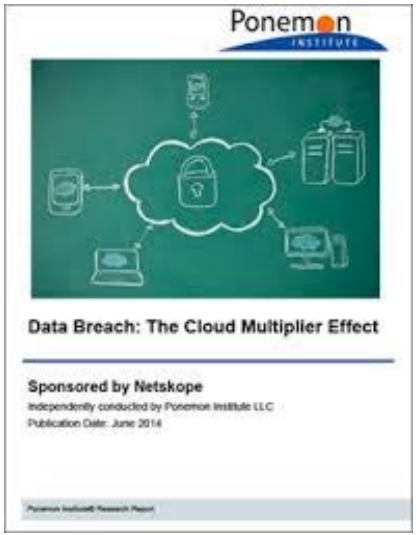
1. Ping Sweep
2. Port Reconnaissance
3. Exploit a Vulnerability
4. Check for Shares or Networked Drives
5. Load Malware
6. Load Worm
7. Load Remote Access Trojan for full Control



Partnering with other Researchers

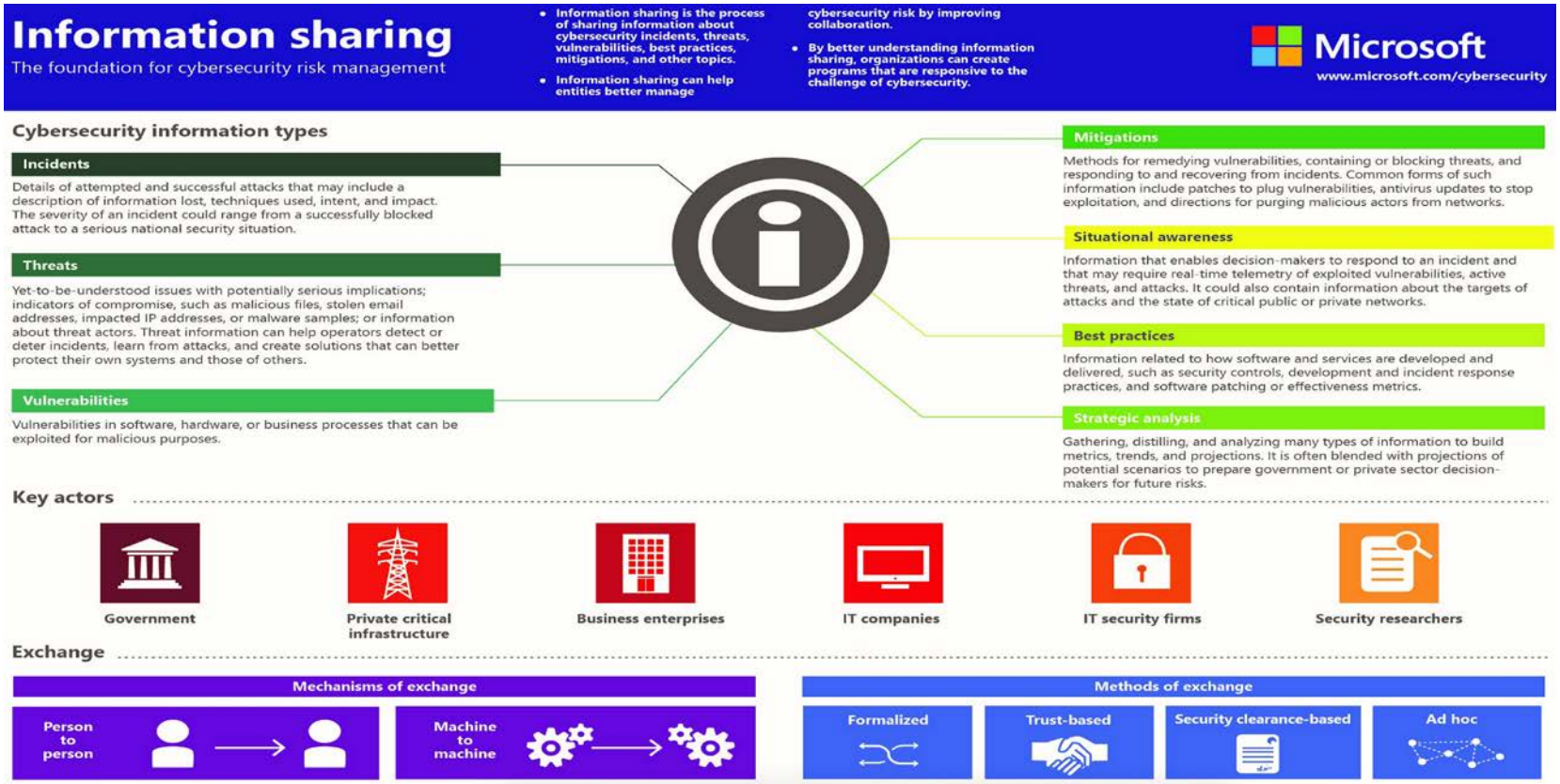
ICS-CSR

Industrial Control System - Cyber Security Research



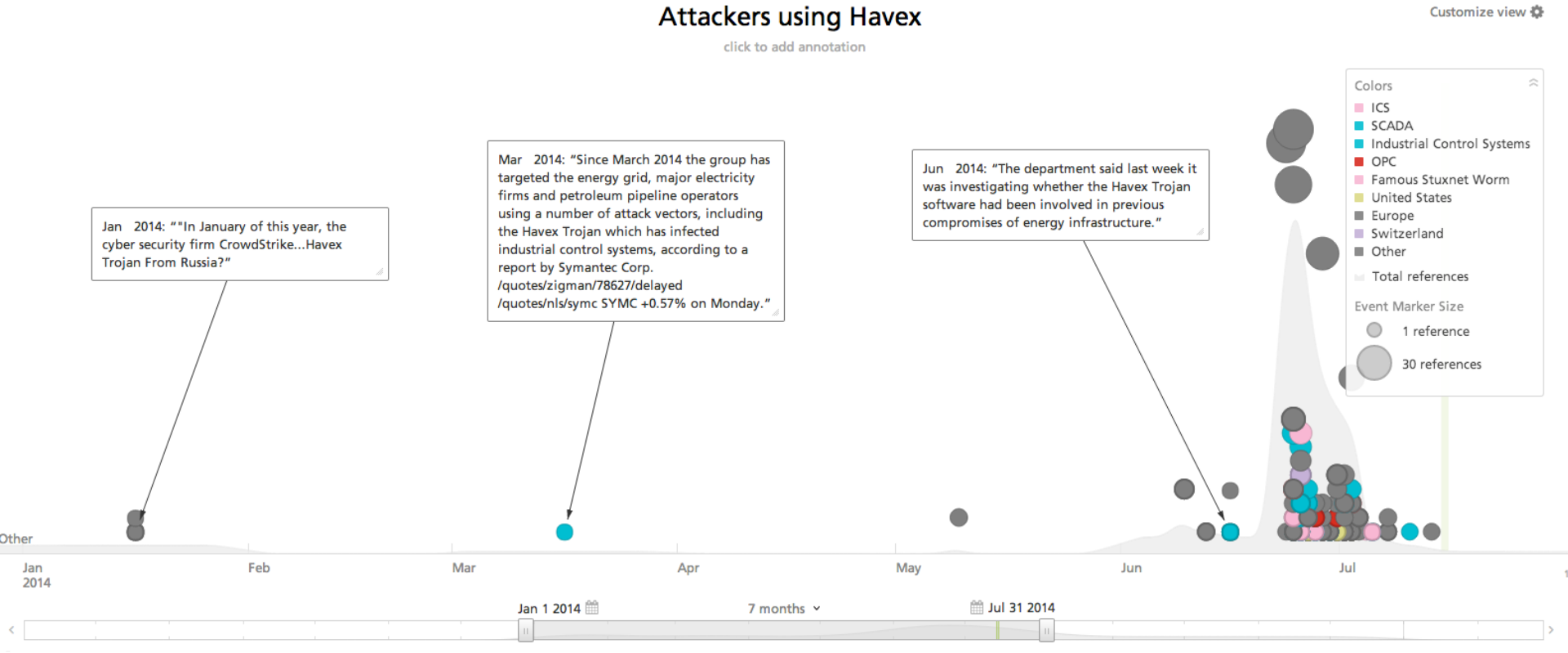
ALERT LOGIC

Information Sharing Model



ALERT LOGIC

Open/Closed Source Intelligence



ALERT LOGIC

Monitoring the Social Media Accounts

Following IRC and Forums

Athena IRC Bot

An IRC (Internet Relay Chat) bot that could steal file information, flood your network(DDOS) or any target sites with your zombie bots. The amount of Athena IRC bot is around **$100** pre-configured Bot per customer's request. **$10** for rebuild and another **$15** IRC setup via TeamViewer, join.me and PuTTY. In addition to that the bin settings has a capability or has a tool that could convert the encrypting the actual IP. The ability to download binaries (hosted elsewhere)and take over a target client to gain access/privileges.

The following PCAP sample triggered our IDS system to one of our customers.

JOIN #chatroom .
.MODE #**chatroom**
+nTtCVs..

NICK n[USA|U|D|W

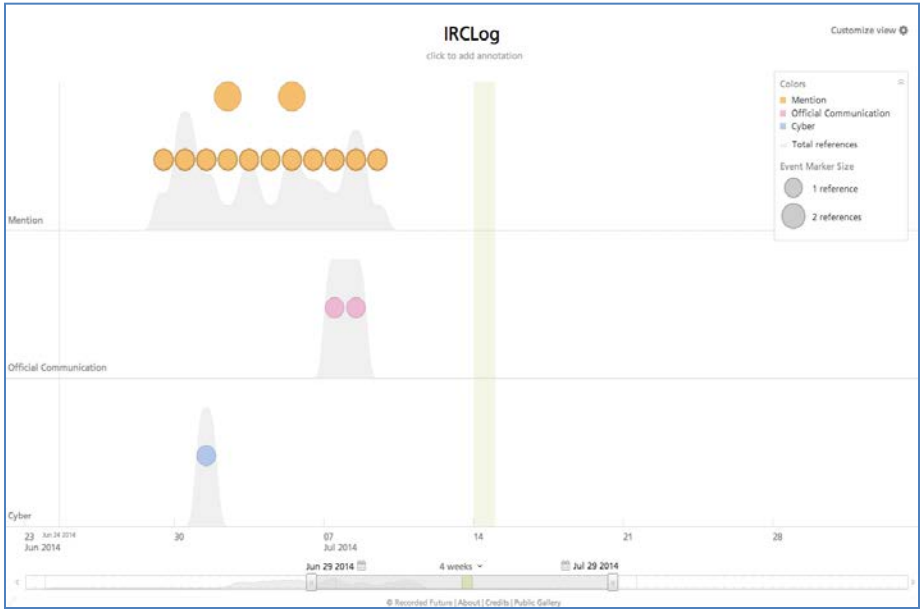
IN7|x86|2c]czzww
xuu..

n[USA|U|D|WIN7|
x86|2c]czzwwxuu!
rrrommmj@brama.g
oogle.com JOI
N :#chatroom..:
irc.private-life.biz 353 **n[USA|U|**
D|WIN7|x86|2c]cz
zwwxuu @ #chatro
om :n[USA|

oljgayvw@brama.g
oogle.com JOI
N :#chatroom..:i
rc.private-life.
biz 353 _

What was identified:

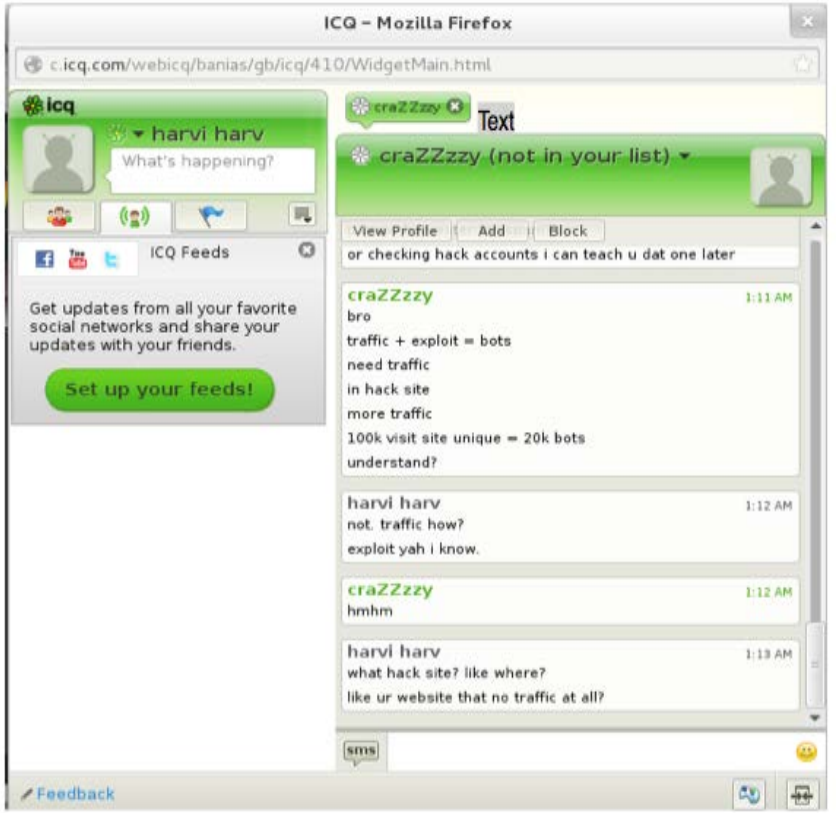
- JOIN (command use to join a channel)
- #chatroom (exisiting chatroom)
- n[USA|U|D|WIN7|x86|2c]czzwwxuu!rrrommmj@brama.google.com (a possible target /brute-forcing its way to the machine)



ALERT LOGIC

Tracking and Predicting the Next Move

- He is a guy from a European country/ (**Russia**)
- His handle or nick is **madd3**
- Using **ICQ 416417** as a tool of communication (illegal transaction)
- A simple **/whois** command to the nick provided us with good information
- 85.17.139.13 (Leaseweb)
- ircname : **John Smith**
- channels : **#chatroom**
- server : **irc.private-life.biz** [Life Server]
- Check this out user has another room. **#attackroom4**
- We can confirm that **Athena version 2.3.5** is being use to attack other sites.
- **2,300 infected Users**
- Cracked Software is available in forums
- As of today **1 BTC to $618.00 or £361.66**



ALERT LOGIC

Forums to Follow – Exploit.in

Stay Informed of the Latest Vulnerabilities

- Websites to follow
  - http://www.securityfocus.com
  - http://www.exploit-db.com
  - http://seclists.org/fulldisclosure/
  - http://www.securitybloggersnetwork.com/

To Follow our Research

- Twitter:
  - @AlertLogic
  - @StephenCoty
- Blog:
  - https://www.alertlogic.com/resources/blog
- Newsletter:
  - https://www.alertlogic.com/weekly-threat-report/
- Cloud Security Report
  - https://www.alertlogic.com/resources/cloud-security-report/
- Zero Day Magazine
  - http://www.alertlogic.com/zerodaymagazine/

ALERT LOGIC

Thank you.