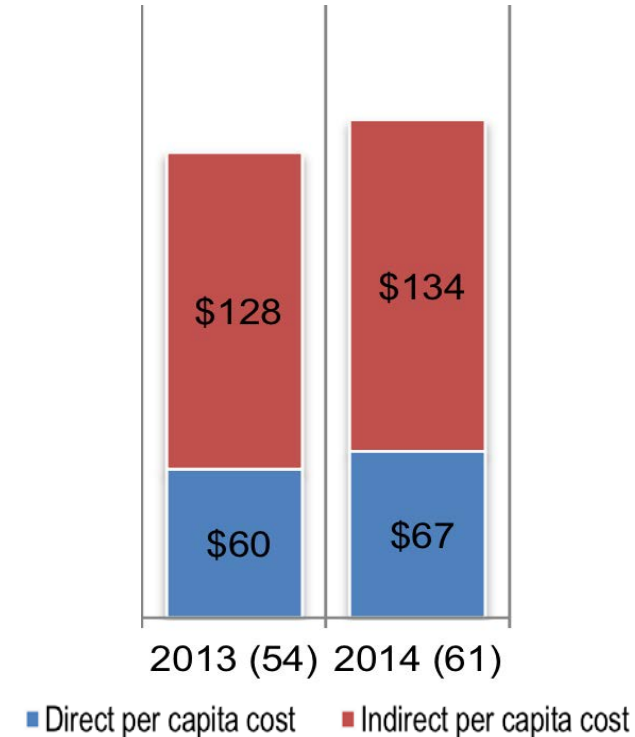
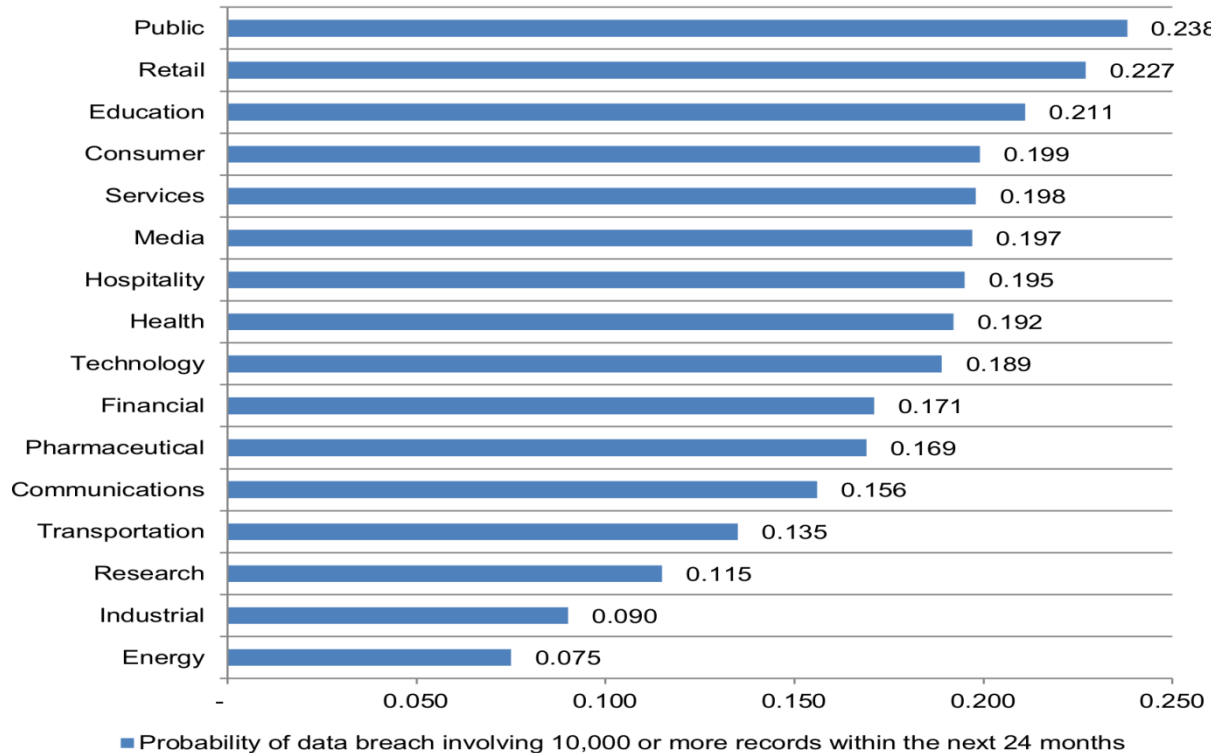


EMERGING THREATS & STRATEGIES FOR DEFENSE

Stephen Coty – Chief Security Evangelist



Industry Analysis – 2014 Data Breaches - Ponemon



Industry Analysis – 2014 Data Breaches - Mandiant

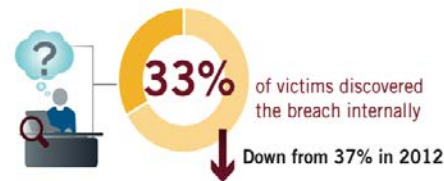
Across the Cyber Threat Landscape

	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

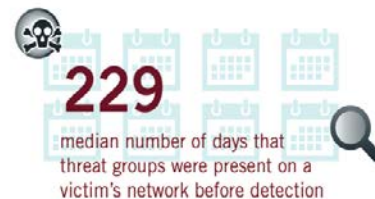
	IRAN-BASED	CHINA-BASED
Industries Targeted	2 Energy, state government agencies	33 Most industry sectors
Victim Selection	Limited based on vulnerabilities	Varied and independent of vulnerabilities
Available Tools	Publicly available	Specially created, customized, publicly available
Date of Initial Mandiant 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



↓ 14 days less than 2012

Longest Presence: 2,287 days

Phishing Email Trends

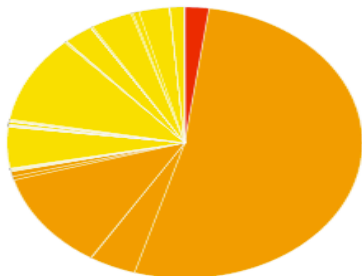


93% of phishing emails were sent on weekdays



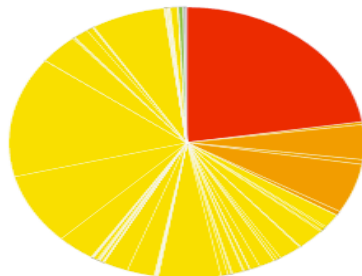
Global Analysis

All Attackers ▾



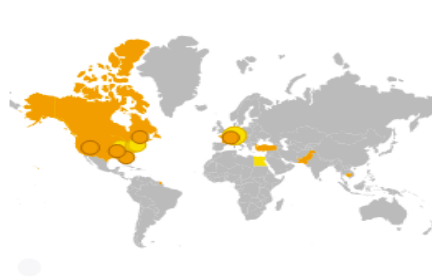
▼ Attacker	Last 60 Days
● Cyber Caliphate	
● Anonymous	
● Chinese hackers	
● Estado Islámico	
● Islamic State in Ir	
● Pakistan	
● Syrian hackers	
● 3xp1r3 Cyber Arr	
● al-Assad	
● Algerian hackers	
● Asia	
● Australia	
● Bangladesh Grey	
● Bharatiya Janata	

All Methods ▾



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

All Targets ▾



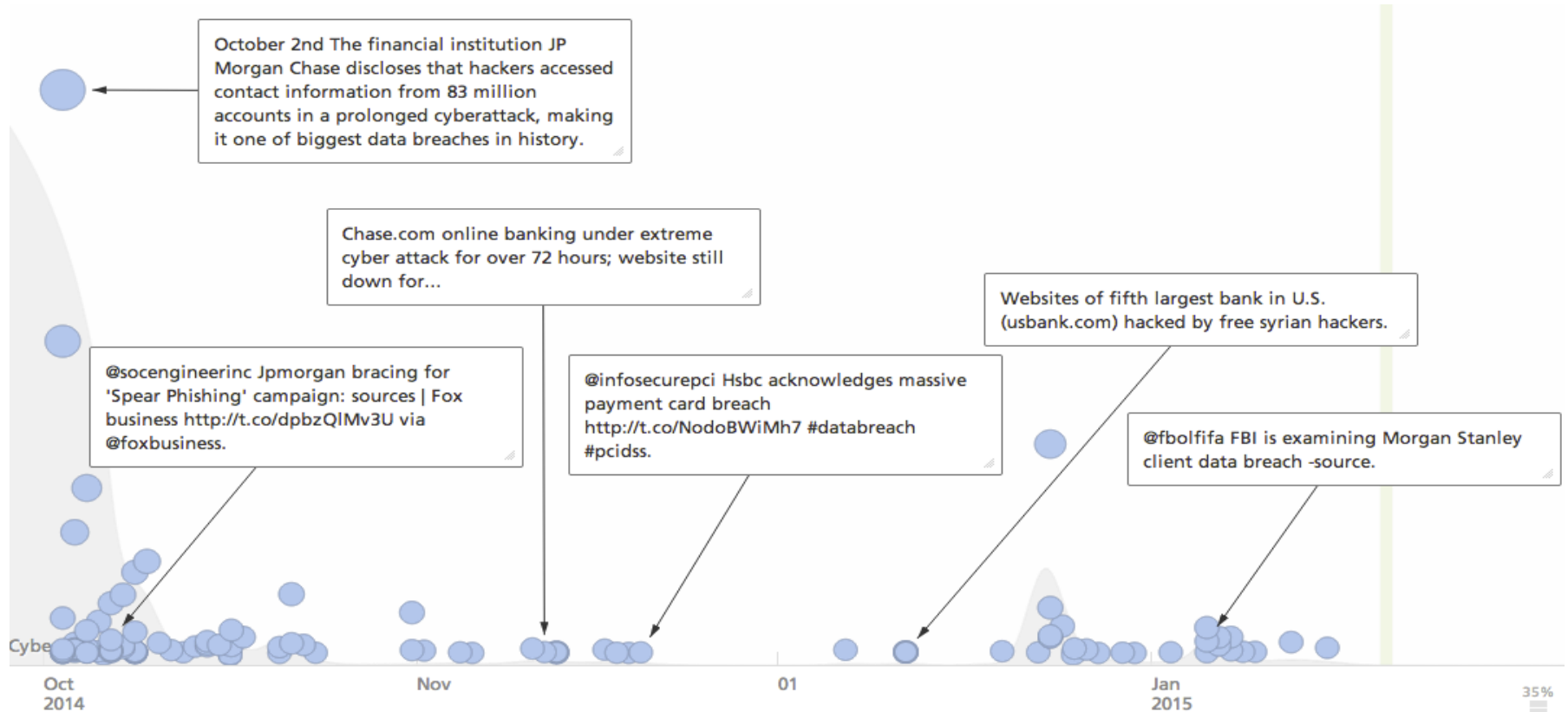
▼ Target	Last 60 Days
● Anthem	
● Anthony Noto	
● Delta Air Lines	
● European Parliar	
● Forbes	
● Forbes.com	
● HSBC Holdings P	
● JavaScript	
● Newsweek	
● Papa John's Pizzi	
● Seth Rollins	
● Standard Charter	
● Washington Post	
● #forbes.com	

All Operations ▾

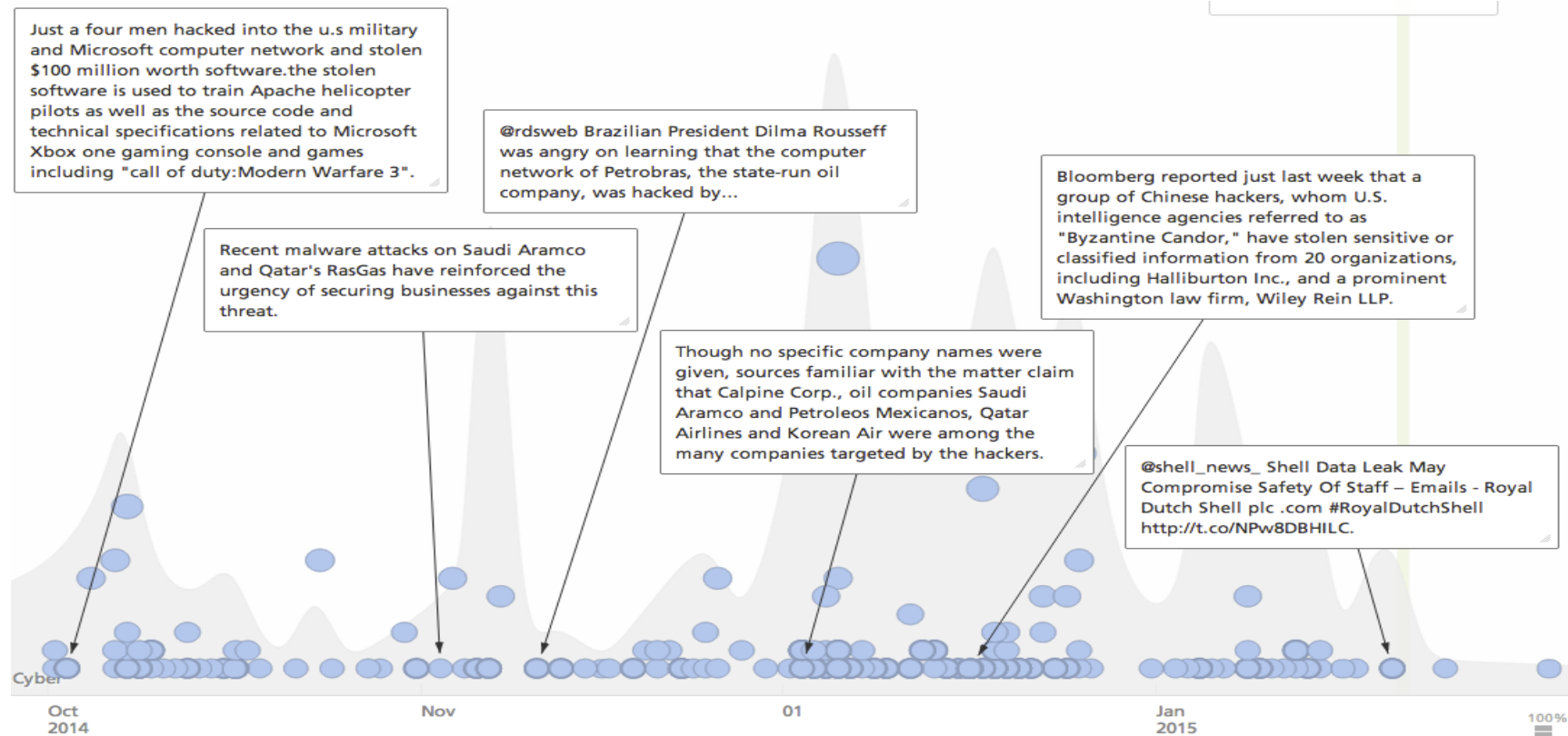


▼ Operation	Last 60 Days
● OpISIS	
● OpAntilSIS	
● OpDownfall	
● Operation Titsto	
● OpFunKill	
● OpGabon	
● OpGCHQ	
● OpICantBreathe	
● OpIzzah	
● OpLeakageJp	
● OpLJ	
● OpNSA	
● OpESR	
● #TheWeekOfHor	

Industry Analysis - Financial



Industry Analysis - Energy



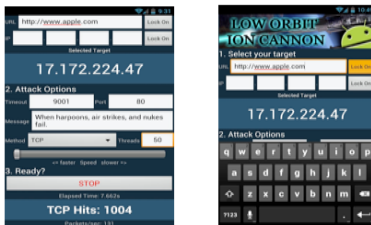
Where is Hacktivism Today



<http://sourceforge.net/projects/javaioic/>



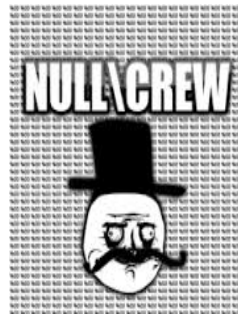
<https://play.google.com/store/apps/details?id=genius.mohammad.ioic&hl=en>



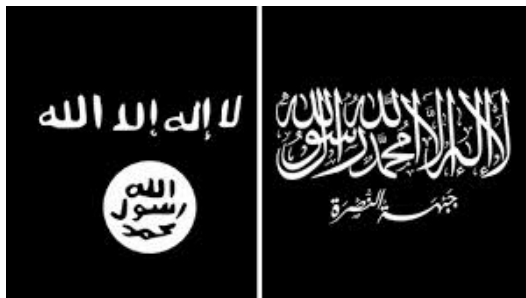
Sample of LOIC downloaded in Source Forge running on .Net
harvi@localhost: file LOIC.exe

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

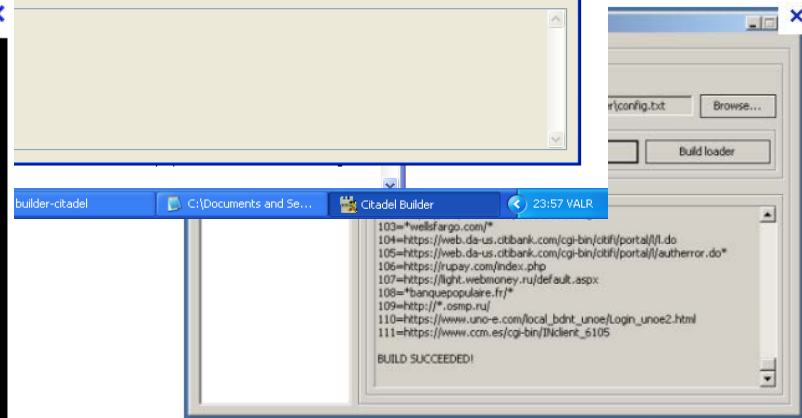
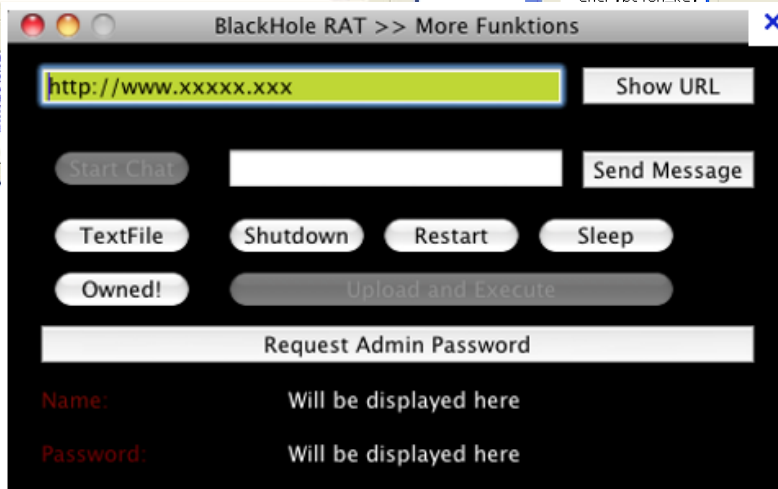
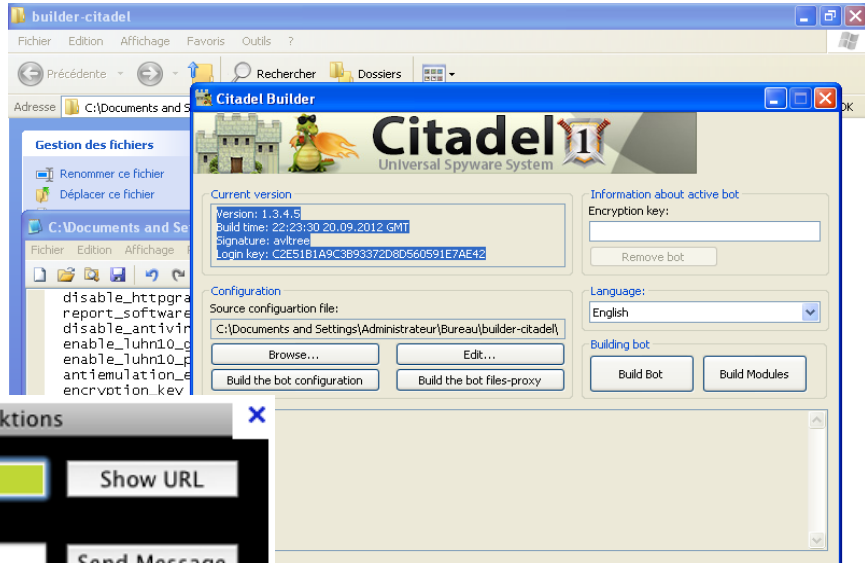
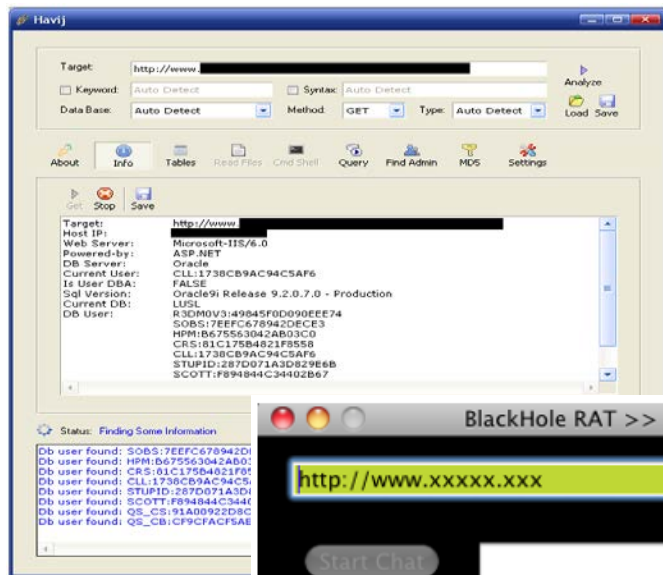
```
01:00 - [RUS]A[D]W_XP[x86]2c[bbbyyyyy] (yyyyyyyy[637.218.138.39]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]2c[heebbyz] (zawturr[65.87.171.17]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]2c[spgprkl] (lilffgdd[178.127.157.82]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[L]W_XP[x86]4c[gnatgna] (rhubovb[31.180.142.247]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]U[L]W_XP[x86]4c[dgdnqtz] (dg[netw@mail.ru-troyka.com]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]2c[spgprkl] (khifczax[94-43-203-113.61.utg.ge]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]U[D]W_XP[x86]2c[yvvtvta] (qpoololm[178.124.179.31]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]2c[yvvtvta] (tqrrooo[37.45.193.26]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]2c[yvvtvta] (tbyyyvvt[91.224.96.5]) has quit (Ping timeout: 180 seconds)
01:00 - [USA]U[D]W_XP[x86]4c[joolliij] (turrool[rrcs-70-62-77-41.midsouth.biz.rr.com]) has quit (Ping timeout: 180 seconds)
01:00 - [USA]U[D]W_XP[x86]2c[cczaxxu] (uvssppm[74.83.230.88]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]2c[rubeliko] (rubeliko[178.120.47.197]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]U[D]W_XP[x86]2c[cczaxxu] (uvssppm[178.122.120.40]) has quit (Ping timeout: 180 seconds)
01:00 - [TUR]A[D]W_XP[x86]2c[zzzzzzzz] (zzzzzzw[67.184.250.125]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]2c[jyyyyyyy] (nnnnnnn[4-94-54-37.pool.ukrtel.net]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[L]W_XP[x86]4c[hmfecf] (zaxxuuu[178.122.168.137]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]4c[byzzzzzz] (xuuurpp[137-90-113-92.pool.ukrtel.net]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[L]W_XP[x86]2c[vssppgm] (kxhiff[95.111.235.222]) has quit (Ping timeout: 180 seconds)
01:00 - [USA]A[D]W_XP[x86]1c[vvvtvtn] (ebttrol[4w.releas22.vl.som.apla.net]) has quit (Ping timeout: 180 seconds)
01:00 - n[USA]U[L]W_XP[x86]2c[jcflpsv] (zcfimps[69.41.3.103]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]U[D]W_XP[x86]2c[dgdnqtz] (dg[netw[195.69.148.129]) has quit (Ping timeout: 180 seconds)
01:00 - [TUR]A[D]W_XP[x86]2c[hhnnhhn] (eeeeeees[249.87.289]) has quit (Ping timeout: 180 seconds)
01:00 - [USA]A[D]W_XP[x86]1c[rnnkkkha] (xxuuurss[50-79-16-138-static.hfc.comcastbusiness.net]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]1c[loupcjow] (djvdkr[109.229.17.231]) has quit (Ping timeout: 180 seconds)
01:00 - [RUS]A[D]W_XP[x86]1c[yvvtvvt] (crojpay[178.124.179.168]) has joined #chatroom
01:00 - [USA]U[D]W_XP[x86]2c[benloruy] (benloruy[115.240.69.48]) has joined #chatroom
01:00 - [RUS]A[D]W_XP[x86]1c[yvvtvvt] (wrlgggg[78.84.49.194]) has joined #chatroom
01:01 - [JPN]U[L]W_XP[x86]1c[mpsvzcf] (jpswcz[fe804104.xgspn.int.tachikawa.spnec.ne.jp]) has joined #chatroom
01:01 - [USA]A[D]W_XP[x86]2c[obyywtr] (comjgdy[com2-net.optinabd.net]) has quit (Ping timeout: 180 seconds)
01:01 - [USA]A[D]W_XP[x86]2c[nnnnnnno] (ooooooo[180.159.67.139]) has quit (Ping timeout: 180 seconds)
01:01 - [RUS]A[D]W_XP[x86]1c[nkhkhiff] (fcczaax[37.45.123.128]) has quit (Connection reset by peer)
01:01 - [IRN]U[L]W_XP[x86]2c[aaaaaa] (aaaaaaa[151.239.227.289]) has joined #chatroom
01:01 - n[THW]A[D]W_XP[x86]2c[vvstppg] (noll111[6210.213.120.114]) has joined #chatroom
01:01 - [RUS]A[L]W_XP[x86]2c[hhnnhhn] OK: Flood: Started (Type: http.arm | Host: http://ny.ukrsibbank.com/ | Port: 80 | 2000 seconds)
```



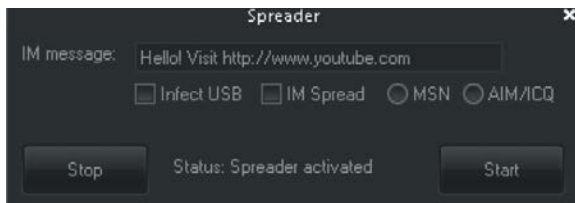
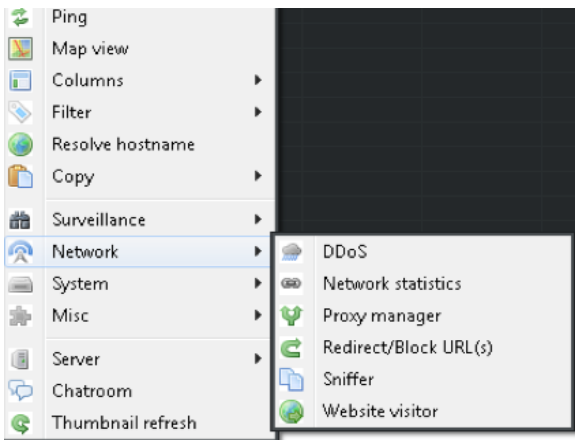
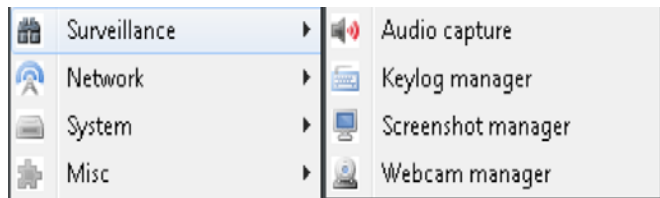
New Groups Emerging



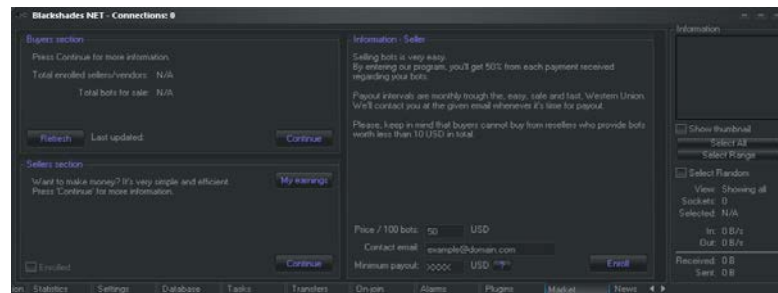
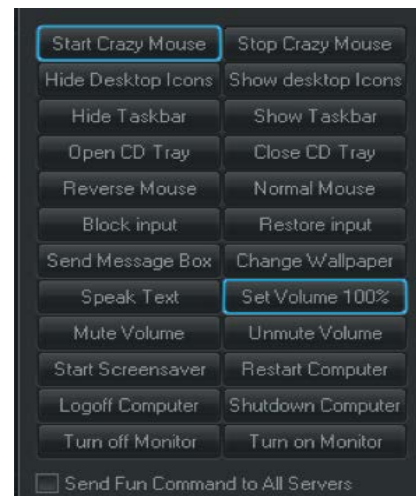
Tools of the Trade



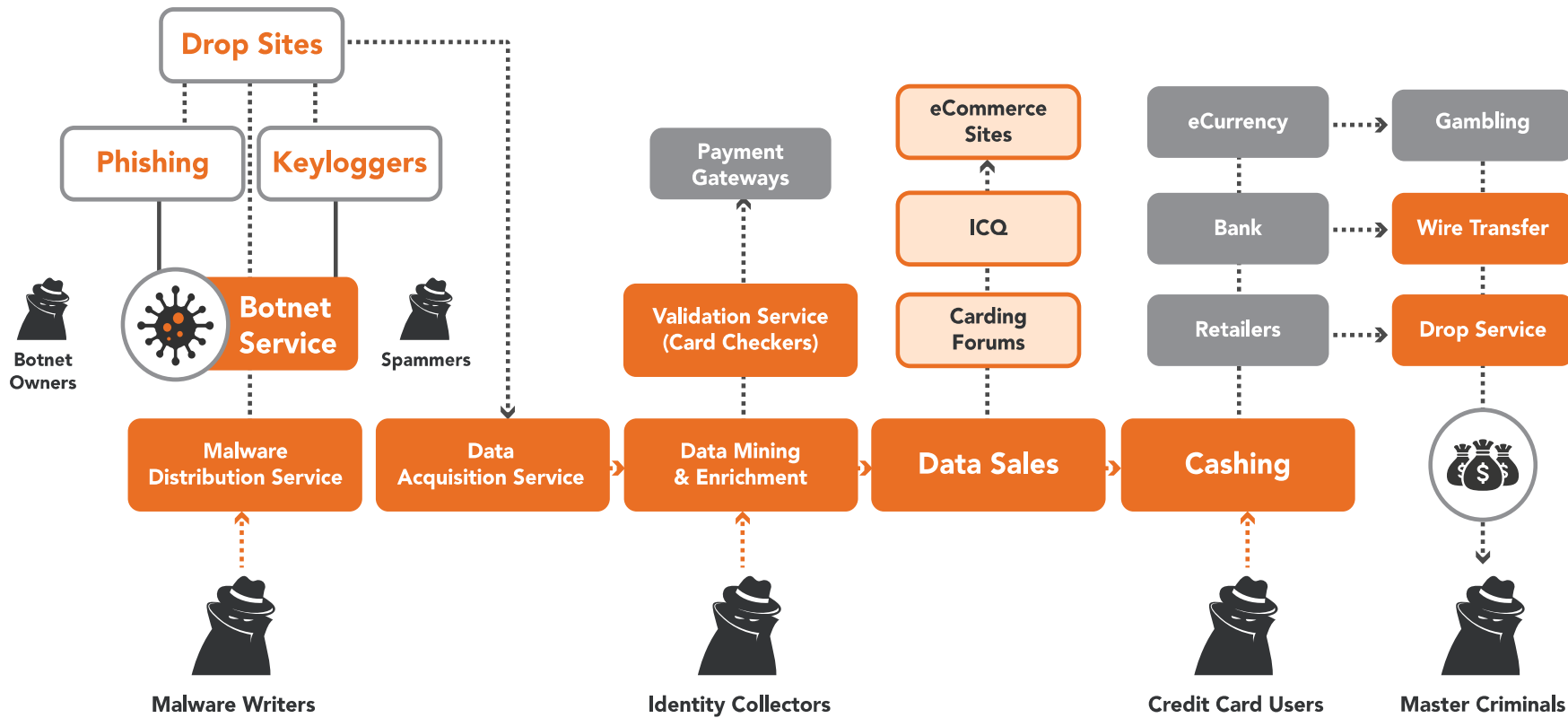
Black Shades RAT



Protocol	Source IP	Local port	Remote IP	Remote port	Size
TCP	192.168.0.4	6111	50393	1593	
TCP	192.168.0.4	6111	59215	68	
TCP	192.168.0.4	6111	59215	1556	
TCP	192.168.0.4	6111	49552	48	
TCP	192.168.0.4	6111	49552	1672	
TCP	192.168.0.4	61008	56774	42	
TCP	192.168.0.4	61008	56774	1580	
TCP	192.168.0.4	59765	4564	1464	
TCP	192.168.0.4	59765	4564	611	
TCP	192.168.0.4	59765	4564	98	
TCP	192.168.0.4	59765	4564	1464	
TCP	192.168.0.4	59765	4564	172	
TCP	192.168.0.4	59765	4564	1464	
TCP	192.168.0.4	59765	4564	130	
TCP	192.168.0.4	59765	4564	1464	
TCP	192.168.0.4	59765	4564	946	
TCP	189.112.182.234	58858	6111	20	
TCP	189.112.182.234	58858	6111		
TCP	192.168.0.4	6111	58858	1915	
TCP	192.168.0.4	6111	58858	1463	
TCP	192.168.0.4	6111	58858	260	
TCP	192.168.0.4	59765	4564	1471	
TCP	192.168.0.4	6111	60848	42	
TCP	192.168.0.4	6111	60848	1611	
8.41	4564	192.168.0.4	4564	1432	
TCP	192.168.0.4	59765	4564	1688	
TCP	192.168.0.4	59765	4564	1461	
TCP	192.168.0.4	59765	4564	1502	



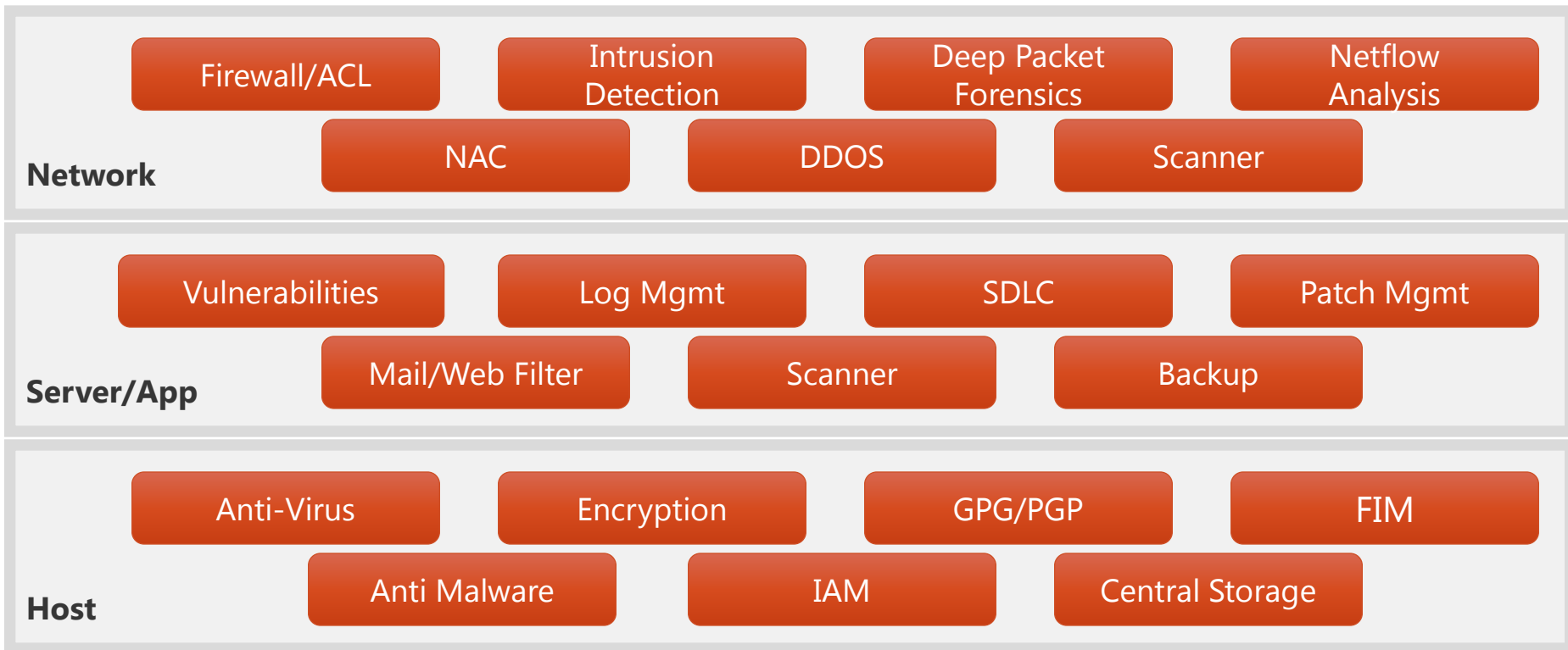
Underground Economy



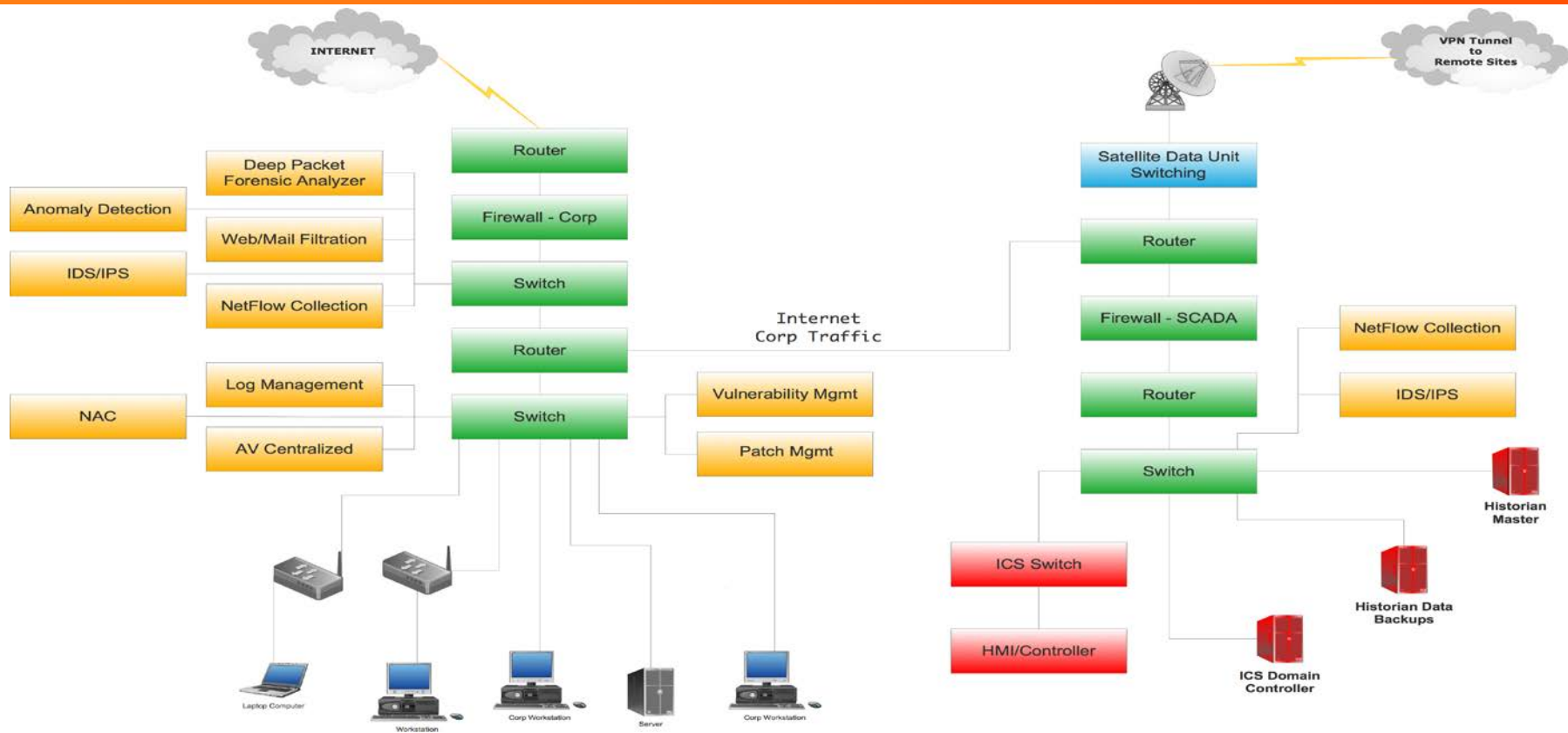
HOW DO WE DEFEND AGAINST THESE ATTACKS



Security Architecture



Deployment

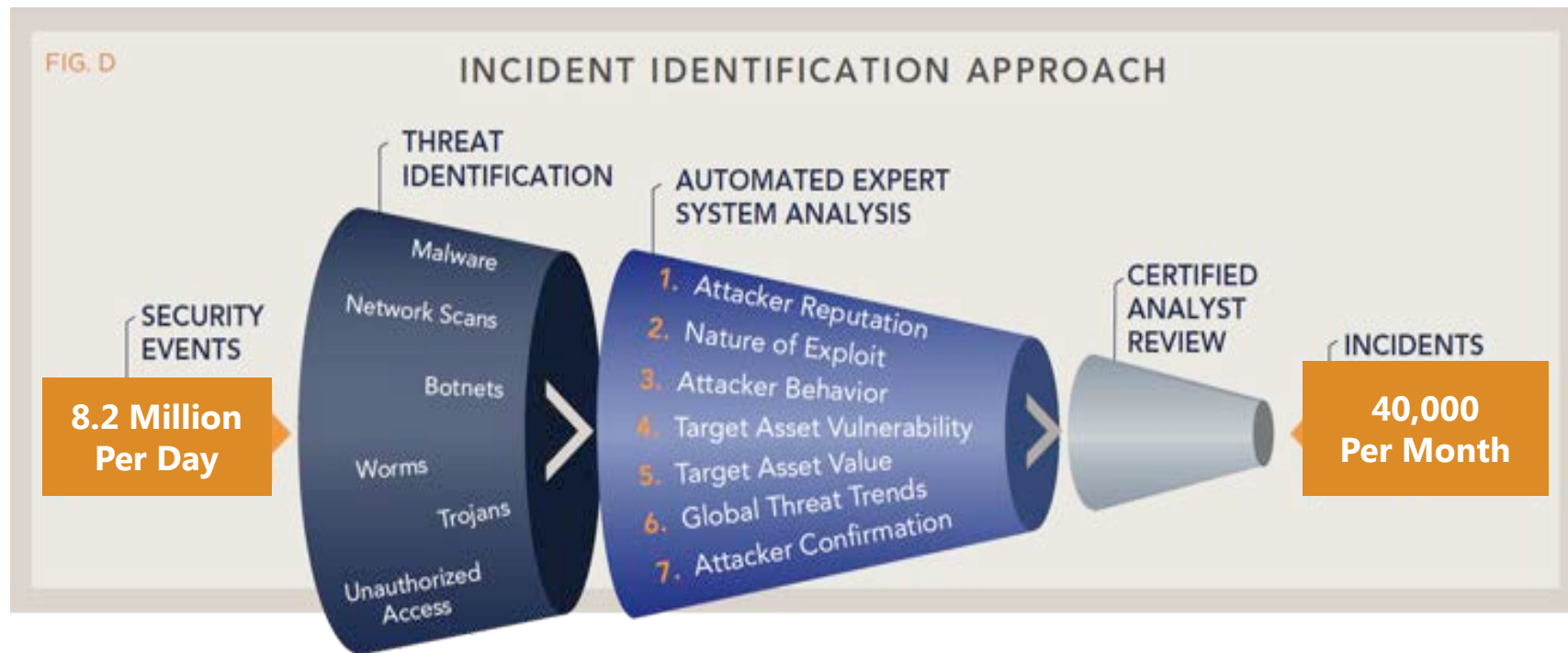


Data Correlation is the Key



SECURITY INCIDENT

NGX SIEM Operations



Enterprise Cyber Security Teams

Monitor and Maintain
non-managed hardware
deployment uptime

Collect and Maintain content for
all non-managed devices

Cyber Security
Awareness Program

Operational Implementation
of all security infrastructure

Incident Response Team

Network and Application
Penetration Testing and
Audit 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



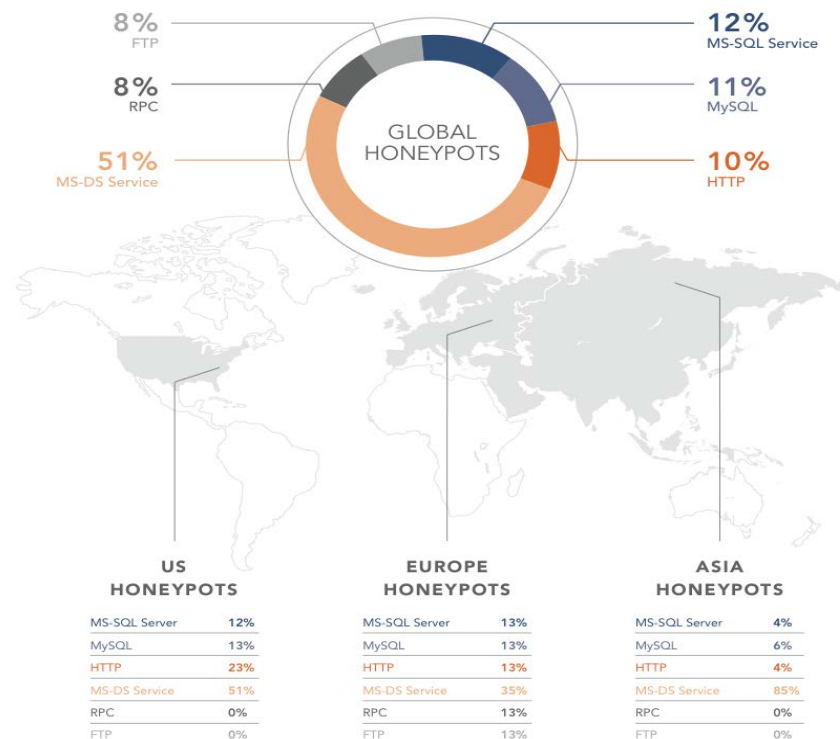
THREAT INTELLIGENCE



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

TOTAL HONEYPOT ATTACKS BY REGION



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



Information Sharing Model

Information sharing

The foundation for cybersecurity risk management

- Information sharing is the process of sharing information about cybersecurity incidents, threats, vulnerabilities, best practices, mitigations, and other topics.
- Information sharing can help entities better manage cybersecurity risk by improving collaboration.
- By better understanding information sharing, organizations can create programs that are responsive to the challenge of cybersecurity.



Cybersecurity information types

Incidents

Details of attempted and successful attacks that may include a description of information lost, techniques used, intent, and impact. The severity of an incident could range from a successfully blocked attack to a serious national security situation.

Threats

Yet-to-be-understood issues with potentially serious implications; indicators of compromise, such as malicious files, stolen email addresses, impacted IP addresses, or malware samples; or information about threat actors. Threat information can help operators detect or deter incidents, learn from attacks, and create solutions that can better protect their own systems and those of others.

Vulnerabilities

Vulnerabilities in software, hardware, or business processes that can be exploited for malicious purposes.



Mitigations

Methods for remedying vulnerabilities, containing or blocking threats, and responding to and recovering from incidents. Common forms of such information include patches to plug vulnerabilities, antivirus updates to stop exploitation, and directions for purging malicious actors from networks.

Situational awareness

Information that enables decision-makers to respond to an incident and that may require real-time telemetry of exploited vulnerabilities, active threats, and attacks. It could also contain information about the targets of attacks and the state of critical public or private networks.

Best practices

Information related to how software and services are developed and delivered, such as security controls, development and incident response practices, and software patching or effectiveness metrics.

Strategic analysis

Gathering, distilling, and analyzing many types of information to build metrics, trends, and projections. It is often blended with projections of potential scenarios to prepare government or private sector decision-makers for future risks.

Key actors



Government



Private critical infrastructure



Business enterprises



IT companies



IT security firms



Security researchers

Exchange

Mechanisms of exchange

Person to person



Machine to machine



Methods of exchange

Formalized



Trust-based



Security clearance-based



Ad hoc

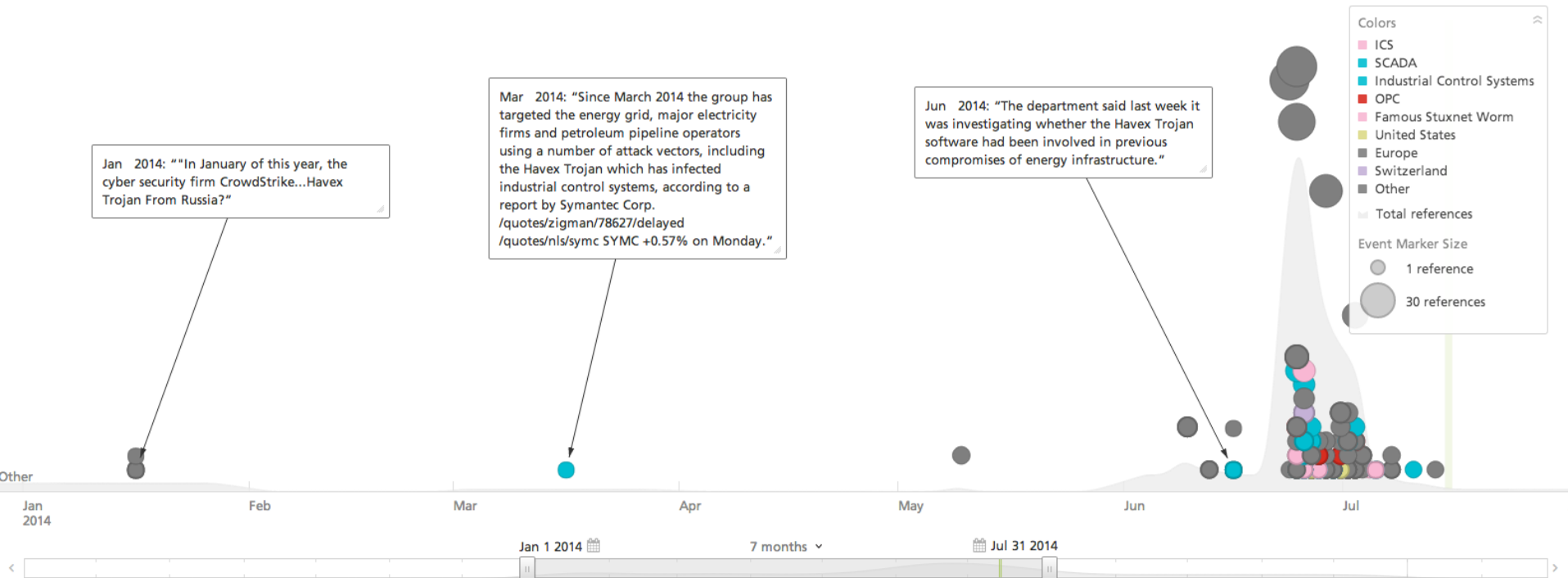


Open/Closed Source Intelligence

Attackers using Havex

click to add annotation

Customize view ⚙



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

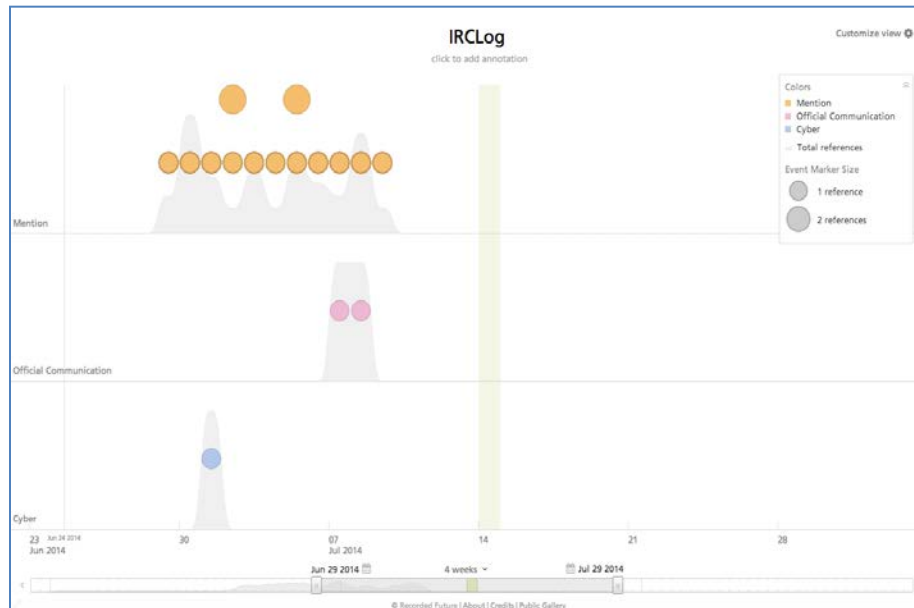
IN7|x86|2c|czzww
xuu..

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 _
```

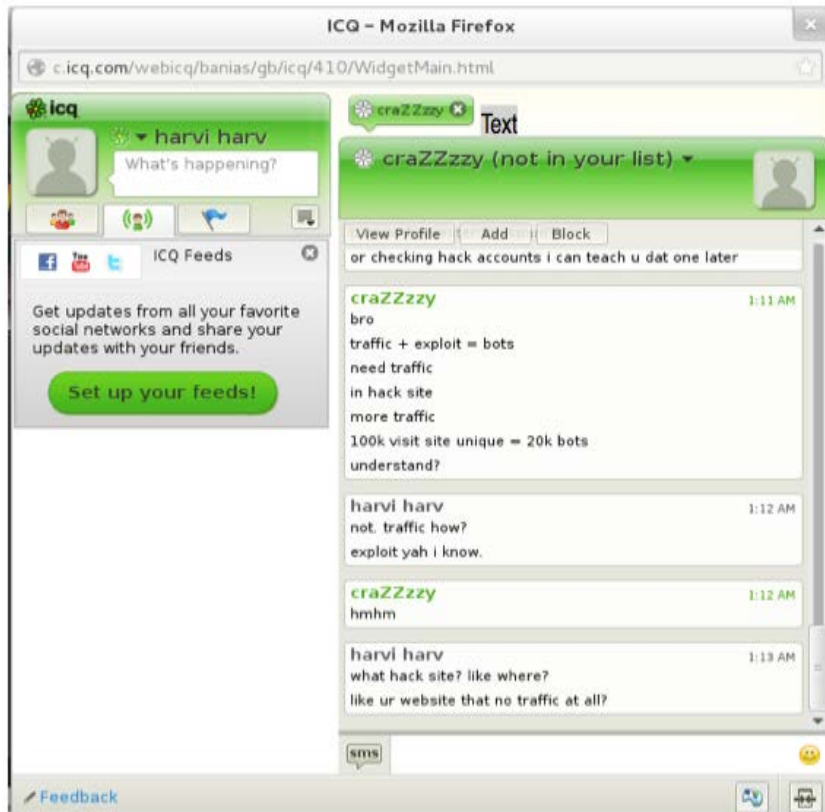
What was identified:

- 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)



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 used 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**



Forums to Follow – Exploit.in



Our mirrors: [Exploit.IN \(SSL\)](#) || [Exploit.IO](#)

Navigation

Main:

- [Home](#)
- [Contact us](#)
- [Online Tools](#)
- [Forum](#)

News:

- [News Archive](#)
- [Search News](#)
- [RSS-Feeds](#)
- [Twitter](#)

Advertising



27/10/2014 18:08: Hacker from Estonia convicted in the US for 11 years for stealing \$ 9.4 million

A US court on Friday sentenced a **hacker from Estonia Sergey Churikov to imprisonment for 11 years for breaking into RBS WorldPay**. Churikov convicted of cyber fraud and stealing \$ 9.4 million from a bank branch Royal Bank of Scotland in Atlanta in 2008. Churikov sentenced to 11 years in prison and ordered to pay \$ 8.4 million. The Government of Estonia in early May 2010 decided to give Churikova US authorities. In co-operation of the State Prosecutor's Office and the Estonian Central Criminal Police, US law enforcement May 6, 2009 were arrested members of a group of international computer fraud. As found out a consequence, Churikov in early November 2008 hacked into the database of the company-operator debit cards RBS WorldPay one of the US banks. These data Churikov gave his partner Igor Grudievu, whose task was to record dumps resulting from burglary, on cards and then cash in ATMs. Just for one day Ronald and Evelyn Choi, and Michael Evgenov removed from the accounts of different persons over 3.5 million CZK 10 000 Estonian kroons at a time in Tallinn. In the future, money from ATMs worldwide and received numerous other hired drops. The fourth key figure of the group took place on court documents as "Hacker 3". Igor chest was accused of repeated forgery of means of payment for the purpose of use, the use of counterfeit payment instruments and computer fraud. He is sentenced to 5 years imprisonment with a probation period of 5 years. Eugene and Evelyn Choi charged with computer fraud and fraudulent use of payment instruments in a large scale, Evelyn Choi was sentenced to 3 years imprisonment with a probation period of 3 years, Eugene - to 2 years imprisonment with a probation period of 2 years. In November 2008, 12 hours more than 2100 ATMs in 280 cities around the world were received US \$ 9 million. Crime seized the US, Estonia, Russia, Ukraine, Italy, Hong Kong, Japan and Canada. Withdraw money previously hired drops.

[Comment](#)

10.27.2014 6:01 p.m.: Malware Backoff increased its presence in the US by 57%

According to the company Damballa, the number of computers infected with malicious software **Backoff**, increased rapidly in North America. This malicious software used to steal information about credit cards. In Damballa observed 57% increase in activity in the period between August and September 2014. Backoff is used to scan memory and retrieval of data on credit cards. This was stated by the technical director Damballa Brian Foster (Brian Foster). Data are based on information collected from customers, businesses and Internet service providers, who use Damballa products to detect malicious activity. "We take the domain names and IP-addresses that are looking for malicious software to calculate risk. The Company monitors the number and characteristics of domain names associated with Backoff. Number of requests indicates growth of infected PC" - said Brian Foster. About 55% of the traffic, including DNS-queries, comes from North America. To preserve the privacy company is not interested in IP-addresses of most of these computers. Hadoop-cluster at

Online Tools

- [Security](#)
- [Advanced test anonymity](#)
- [test browser \(short\)](#)
- [Checking password complexity](#)
- [Password generator](#)
- [Another speed test](#)
- [download speed calculation](#)
- [converter IPv4 / IPv6](#)
- [converter UNIX / GMT time](#)
- [Jabber Valid Checker](#)

Quick jump

вирус firefox взлом форум
security flash linux ip rss
explorer windows exploit
проверка socks root apple
Google Facebook ddos
Symantec ssl ботнет Android
спам Chrome троян
добавить tag



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/>

Rescator
Samba Kaptoxa
AlinaPOS
Dexter Heartbleed
BlackPOS
Gonzales

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/>

Thank you.

