One Day @

RMLLSEC 2017 - Xavier Mertens (@xme)

<profile>
<name>**Xavier Mertens**</name>
<aka>**Xme**</aka>
<jobs>
<day>**Freelancer**</day>
<night>**Blogger, ISC Handler, Hacker**</night>
</jobs>
<![CDATA[
www.truesec.be
blog.rootshell.be
isc.sans.edu
www.brucon.org
]]>
</profile>

Building a Poor Man's "F1r3Ey3" Mail Scanner

RMLLSEC16 - Xavier Mertens

$HOME Sweet $HOME

RMLL - Beauvais - July 2015 - Xavier Mertens

What Will You Investigate Today?

RMLL 2013 - Xavier Mertens - Brussels

Malware Analysis Free Toolbox

RMLL - Montpellier - July 2014 - Xavier Mertens

Once upon a time…

The ISC was created in 2001 following the successful detection, analysis, and widespread warning of the Li0n worm.

Linux.Lion.Worm

Risk Level 1: Very Low

Summary | Technical Details | Removal

Printer Friendly Page

Discovered: March 23, 2001
Updated: February 13, 2007 11:51:28 AM
Type: Worm
Systems Affected: Linux

Linux.Lion is a dangerous Linux worm that infects computers running Linux. This worm is similar to Linux.Ramen and does not execute on systems running Microsoft Windows.

Antivirus Protection Dates

- **Initial Rapid Release version** March 23, 2001
- **Latest Rapid Release version** March 23, 2017 revision 037
- **Initial Daily Certified version** March 23, 2001
- **Latest Daily Certified version** March 23, 2017 revision 041
- **Initial Weekly Certified release date** March 23, 2001

Click here for a more detailed description of Rapid Release and Daily Certified virus definitions.

Writeup By: Ralph Gutierrez

Summary | Technical Details | Removal

Once upon a time…

The Li0n worm event demonstrated what the **community** acting **together** can do to respond to broad-based malicious attacks. Most importantly, it demonstrated the value of **sharing** intrusion detection logs in **real time**.

Some Numbers…

31 handlers(*)

50 countries

500.000 IP addresses

(*) 32 for a few days :-)

Handlers

The ISC relies on an all-volunteer effort to detect problems, analyze the threat, and disseminate both technical as well as procedural information to the general public.

Who are the Handlers?

Must have some knowledge about the “Internet”
(protocols, apps, security)

Must be able to write freely (no control!)

Dedicate some spare time

Did you turn it off and on again?

Shifts

- 24 hours
- Follow up new threats in the Internet
- Reply to users emails / reports
- Write a diary
- Follow the forums
- Investigate reported incidents

US Centric

<warning> Warning for French people </warning>

SANS is an organization based in US,
100% English content
Only 5 handlers in Europe(*)

(*) 3 in Belgium, 1 in Switzerland, 1 in Croatia

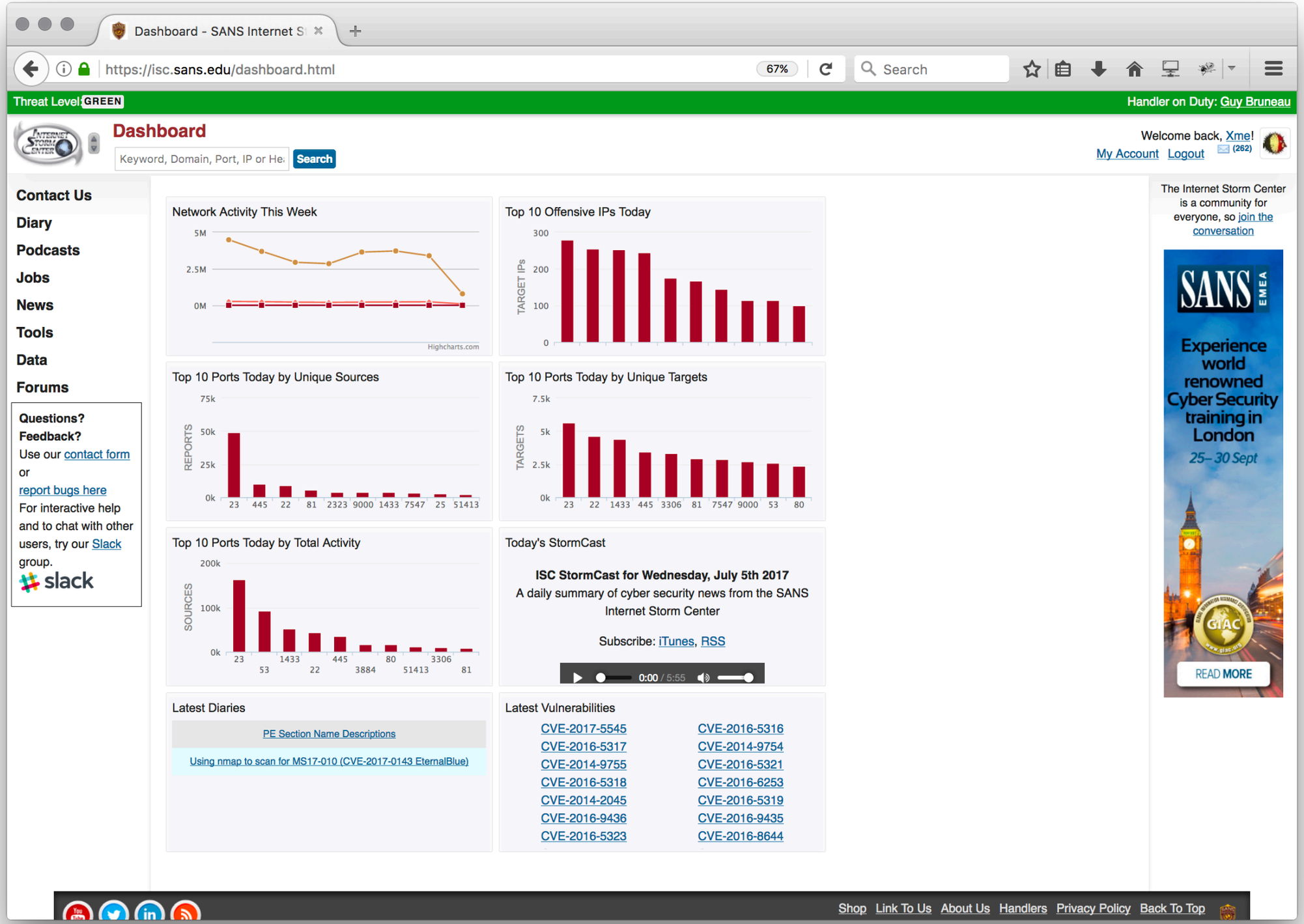
Food

The ISC needs food.
Everybody is welcome to participate
We need you

Services


Podcast
REST-API
Top-ports
Daily-Diary
SSH-Scans
Block-List
404-Project
InfoCON

Your Dashboard



InfoCon

Normal status

Significant new threat

Major Internet disruption

Loss of connectivity across a large part of the Internet

Last change: 12/05/2017 (WannaCry)

Daily Diary

Blog post that covers something about internet security from highly technical (reverse) to business (compliance)

Obfuscating without XOR

Malicious files are generated and spread over the wild Internet daily (read: "hourly"). The goal of the attackers is to use files that are:

- not know by signature-based solutions
- not easy to read for the human eye

That's why many obfuscation techniques exist to lure automated tools and security analysts. In most cases, it's just a question of time to decode the obfuscated data. A classic technique is to use the XOR cypher[1]. This is definitively not a new technique (see a previous diary[2] from 2012) but it still heavily used. And many tools can automate the search for XOR'd string. Viper, the binary analysis and management framework, is a good example. It can scan for XOR'd strings easily:

```
viper tmpnYaBJs > xor -a
[*] Searching for the following strings:
- This Program
- GetSystemDirectory
- CreateFile
- IsBadReadPtr
- IsBadWritePtrGetProcAddress
- LoadLibrary
- WinExec
- CreateFileShellExecute
- CloseHandle
- UrlDownloadToFile
- GetTempPath
```


Xme

284 POSTS

ISC HANDLER

Podcast

Daily 5 mins recap of the threat landscape

Perfect when you commute to work

(https://isc.sans.edu/dailypodcast.xml)

404Project

Because what does not exist may have a great value!
Example: scanning for DB files

- Full request URL & parameters ($_SERVER['REQUEST_URI'])
- Client IP address ($_SERVER['REMOTE_ADDR'])
- Client User-Agent ($_SERVER['HTTP_USER_AGENT'])

404Project

404 Submissions for 2017-07-03

2017-07-03: 67 Reports 50 Urls Submit

#	Time	URL	User Agent	Source
2	17:39:34	/monitoring-	Mozilla/4.0 (compatible; MSIE 6.0; MS Web Services Client Protocol 4.0.30319.17929)	41.96.34.151
2	14:28:35	/Configss.php?check=1	Mozilla/5.0 (Windows NT 6.1; rv:34.0) Gecko/20100101 Firefox/34.0	185.129.148.181
2	07:24:01	/?author=3	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)	91.200.12.73
1	06:09:39	/data/conn/config.php	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)	27.18.28.125
1	17:20:28	/apple-app-site-association	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	66.249.66.64
1	05:58:43	/plus/mytag_js.php?aid=8080	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)	27.18.28.125
1	15:46:51	/typo3	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0	80.241.220.215
1	02:46:59	/admin/config.php	curl/7.15.5 (x86_64-redhat-linux-gnu) libcurl/7.15.5 OpenSSL/0.9.8b zlib/1.2.3 libidn/0.6.5	181.143.8.34
1	13:25:55	/phpMyAdmin	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)	139.199.219.178
1	07:28:24	/stuff/malwares/htserver.exe	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.7 (KHTML, like Gecko) Chrome/16.0.912.63 Safari/535.7	208.80.194.30
1	18:37:48	/stuff/malwares/htserver.exe	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.23) Gecko/20110920 Firefox/3.6.23	208.80.194.32
1	06:04:42	/plus/90000.php	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)	27.18.28.125
1	16:28:13	/apple-app-site-association	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	66.249.76.46

DShield

- Firewall logs collector and aggregator
- Multiple clients
- Develop your own client (Ex: OSSEC)
- API via HTTPS or SMTP
- Anonymization
- Aggregation

DShield

Account Summary

Update Information

e-mail address:	
User ID:	
Last Report:	Firewall reports: 2017-07-03 21:40:07 ssh/kippo reports: 2017-06-26 06:45:17 404 logs: 2017-07-03 21:45:07
Today's Reports (Firewall+ssh):	73562 Lines (Firewall: 73562 SSH:)
Current server time:	Mon, 03 Jul 2017 21:56:10 +0000 (day # 736878)

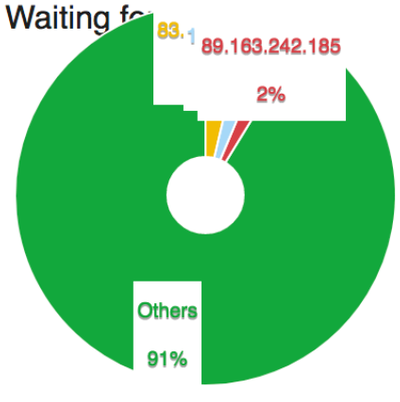
Top of page

Graph

Show reports on 2017-01-27

By Source IPs | By Target IPs | By Target Ports

Waiting fo



Top of page

SSH-Scan

Enter A Password Search

Top 10 Passwords Attempted Today

Password	Attempts	Percent
admin	8,012	4.79%
system\x00	5,235	3.13%
sh\x00	5,188	3.10%
support	5,160	3.08%
123456	3,461	2.07%
password	2,959	1.77%
1234	2,779	1.66%
12345	2,660	1.59%
root	2,530	1.51%
default	2,033	1.21%

View More

Top 10 Passwords Attempted This Month

Password	Attempts	Percent
admin	1,333,701	2.69%
ROOT	916,883	1.85%
123456	699,091	1.41%
password	606,287	1.22%
ubnt	579,743	1.17%
12345	393,209	0.79%
1234	354,090	0.71%
support	296,151	0.60%
admin123	289,308	0.58%
passw0rd	283,616	0.57%

View More

https://github.com/jkakavas/kippo-pyshield

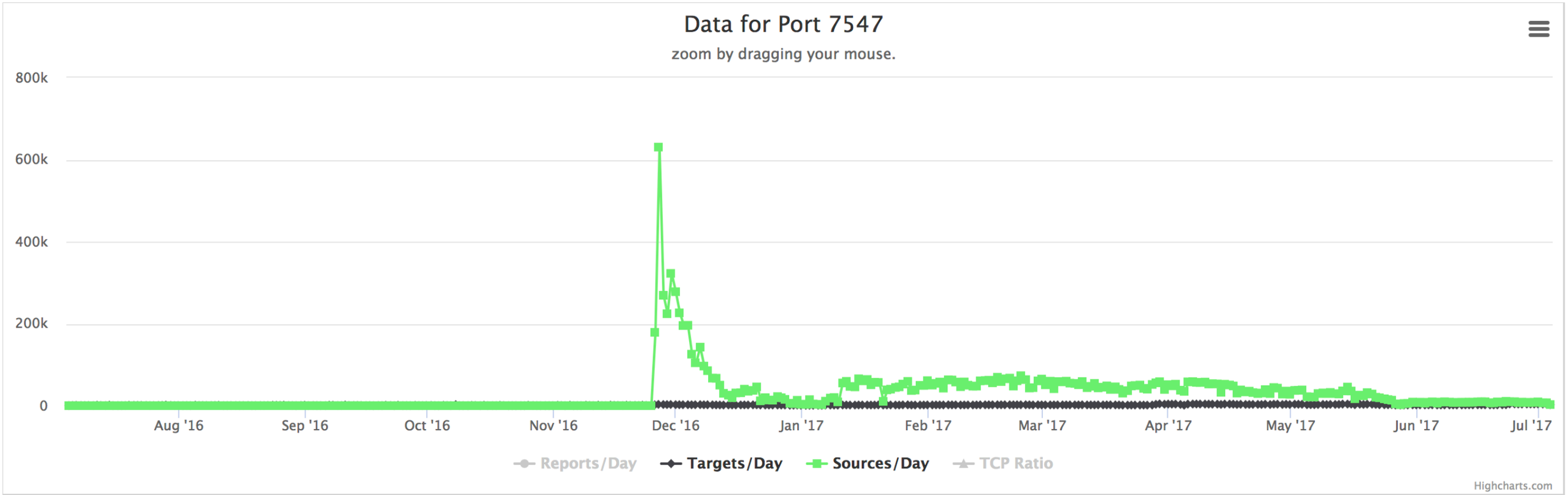
DShield on Pi

https://github.com/DShield-ISC/dshield

Top-Ports

Port	Service	Name	Trend	Protocol Ratio Change
631	ipp	IPP (Internet Printing Protocol)	447	0
5006	wsm-server	wsm server	414	59
4443	pharos	Pharos	412	1
10005	OpwinTRojan	[trojan] OpwinTRojan	412	22
636	ldaps	ldap protocol over TLS SSL (was sldap)	398	0
30005	BackdoorJZ	[trojan] Backdoor JZ	395	24
990	ftps	ftp protocol control over TLS SSL	389	0
50000	SubSARI	[trojan] SubSARI	382	6
87	priv-term-l	any private terminal link ttylink	378	0
54321	BackOrifice2000	[trojan] Back Orifice 2000	365	26

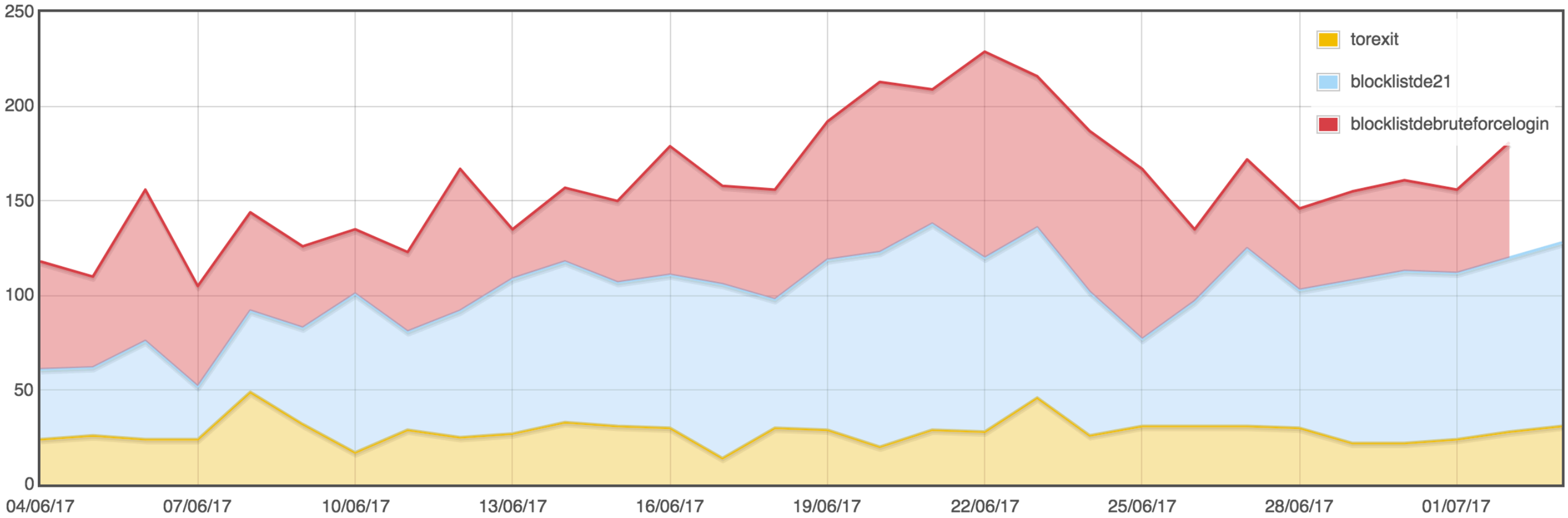
Ports Activity



Block list

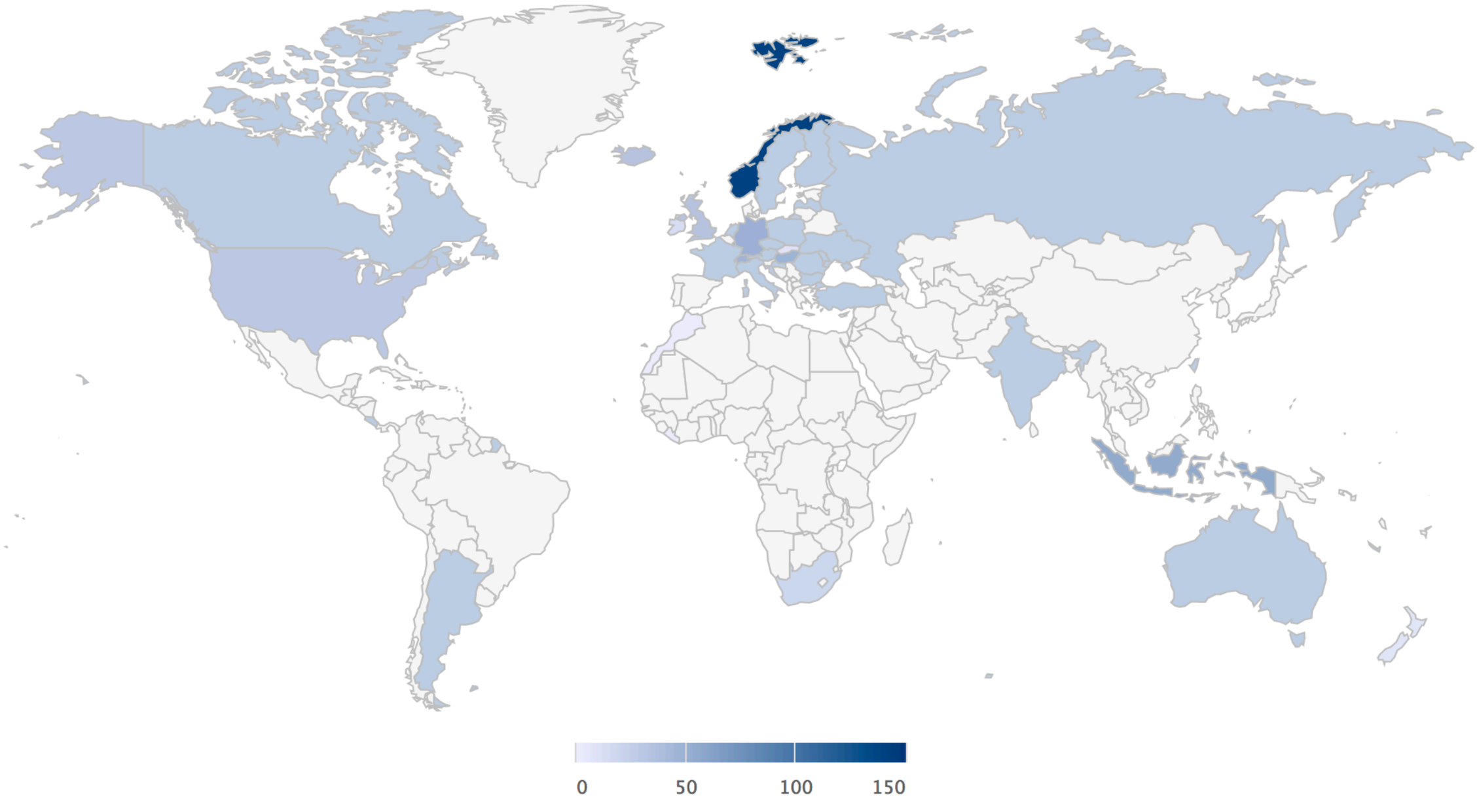
```
#
#   DShield.org Recommended Block List
#    (c) 2017 DShield.org
#   some rights reserved. Details http://creativecommons.org/licenses/by-nc-sa/2.5/
#   use on your own risk. No warranties implied.
#   primary URL: http://feeds.dshield.org/block.txt
#     PGP Sign.: http://feeds.dshield.org/block.txt.asc
#
#   comments: info@dshield.org
#    updated: Tue Jul  4 07:15:05 2017 UTC
#
#    This list summarizes the top 20 attacking class C (/24) subnets
#   over the last three days. The number of 'attacks' indicates the
#   number of targets reporting scans from this subnet.
#
#
#    Columns (tab delimited):
#
#    (1) start of netblock
#    (2) end of netblock
#    (3) subnet (/24 for class C)
#    (4) number of targets scanned
#    (5) name of Network
#    (6) Country
#    (7) contact email address
#
#    If a range is assigned to multiple users, the first one is listed.
#
Start   End     Netmask Attacks Name    Country email
91.211.2.0      91.211.2.255    24      4111    THREE-W-INFRA-AS ,      NL      abuse@3winfra.com
31.207.47.0     31.207.47.255   24      3507    HOSTKEY-AS ,    NL      abuse@hostkey.nl
185.35.62.0     185.35.62.255   24      3449    KS-ASN1 This ASN is used for Internet security research. Internet-scale port scanning activi
would you have any question.,   CH      abuse@nagra.com
80.82.77.0      80.82.77.255    24      3145    QUASINETWORKS , NL      abuse@quasinetworks.com
5.188.11.0      5.188.11.255    24      2921    PIN-AS ,        RU      abuse@pinspb.ru
5.188.10.0      5.188.10.255    24      2891    PIN-AS ,        RU      abuse@pinspb.ru
104.193.252.0   104.193.252.255 24      2684    HOSTING-SOLUTIONS - Hosting Solution Ltd.,      US      abuse@king-servers.com
45.55.11.0      45.55.11.255    24      2603    DIGITALOCEAN-ASN - Digital Ocean, Inc., US      abuse@digitalocean.com
45.55.6.0       45.55.6.255     24      2425    DIGITALOCEAN-ASN - Digital Ocean, Inc., US      abuse@digitalocean.com
71.6.216.0      71.6.216.255    24      2255    CARINET - CariNet, Inc.,        US      complaints@cari.net
216.158.238.0   216.158.238.255 24      2109    NJIIX-AS-1 - NEW JERSEY INTERNATIONAL INTERNET EXCHANGE LLC,    US      gregg@njiix.net
222.47.26.0     222.47.26.255   24      2069    CTTNET China TieTong Telecommunications Corporation,    CN      ipas@cnnic.cn
141.212.122.0   141.212.122.255 24      1939    UMICH-AS-5 - University of Michigan,    US      abuse@umich.edu
71.6.146.0      71.6.146.255    24      1736    CARINET - CariNet, Inc.,        US      complaints@cari.net
77.72.82.0      77.72.82.255    24      1716    NETUP-AS ,      RU      aospan@netup.ru
5.101.40.0      5.101.40.255    24      1672    NO_N    ZZ      no email on file
64.125.239.0    64.125.239.255  24      1671    ZAYO-6461 - Zayo Bandwidth Inc, US      abuse@zayo.com
191.96.249.0    191.96.249.255  24      1600    Digital Energy Technologies Chile SpA,  CL      noc@AS61440.NET
94.102.49.0     94.102.49.255   24      1593    QUASINETWORKS , NL      abuse@quasinetworks.com
204.42.253.0    204.42.253.255  24      1502    NTT-COMMUNICATIONS-2914 - NTT America, Inc.,    US      abuse@ntt.net
```

Threat Feeds



Threat Feeds

Threat Feed Map



Threat Feeds

THREAT FEEDS

BOTS

- bebloh C&C server
- Cryptowall C&C server
- Dyreza Servers
- Hesperbot C&C server
- matsnu C&C server
- Palevo C&C IP
- qakbot C&C server
- ramnit C&C server
- Ransomdomains
- Ransomips
- Spyeye C&C server
- Symmi C&C server
- TinyBanker C&C server
- Upatr Servers
- WebIron Bots
- Zeus C&C server
- Zeus C&C server

MALWARE

- Malwaredomainlist
- Malwaredomains
- Threatexpert

OTHERS

- CI Army List
- Emergingthreats
- Forum Spammers
- Malc0de Blacklist
- TLD Name Servers
- **Tor Exit Node** ✓

PORT SCANNERS

- Port 110 Scanner
- Port 143 Scanner
- **Port 21 Scanner** ✓
- Port 22 Scanner
- Port 25 Scanner
- Port 443 Scanner
- Port 80 Scanner
- Port 993 Scanner
- Apache Web Server Scanner
- Asterisk VoIP Scanner
- Suspect Bots/Infected
- **Bruteforce** ✓
- courier imap attacker
- courier pop3 attacker
- OpenBL FTP Scanners
- OpenBL HTTP Scanners
- OpenBL MAIL Scanners
- OpenBL SMTP Scanners
- OpenBL SSH Scanners

RESEARCH

- Blindferret
- Erratasec Masscan
- Rapid7Sonar
- Shadowserver
- ShodanHQ
- UMichigan scans.io

REST API

https://isc.sans.edu/api/

REST API

```
https://isc.sans.edu/api/infocon

<?xml version="1.0" encoding="UTF-8"?>
<infocon>
 <status>green</status>
</infocon>
```

```
https://isc.sans.edu/api/handler

<?xml version="1.0" encoding="UTF-8"?>
<handler>
 <name>Xavier Mertens<name>
</handler>
```

REST API

```
https://isc.sans.edu/api/ip/70.91.145.10

<?xml version="1.0" encoding="UTF-8"?>
<ip>
 <number>1.85.2.119</number>
 <count>9843</count>
 <attacks>34</attacks>
 <maxdate>2015-11-12</maxdate>
 <mindate>2015-10-08</mindate>
 <updated>2015-11-12 14:03:22</updated>
 <comment/>
 <asabusecontact>anti-spam@ns.chinanet.cn.net</asabusecontact>
 <as>4134</as>
 <asname>CHINANET-BACKBONE No.31,Jin-rong Street</asname>
 <ascountry>CN</ascountry>
 <assize>108902447</assize>
 <network>1.80.0.0/13</network>
 <threatfeeds>
  <blocklistde110>
   <lastseen>2015-11-11</lastseen>
   <firstseen>2015-09-22</firstseen>
  </blocklistde110>
  <blocklistde143>
   <lastseen>2015-11-11</lastseen>
   <firstseen>2015-09-22</firstseen>
  </blocklistde143>
  <blocklistde25>
```

Contact

We are not able to respond to you unless you provide an e-mail address!

Your E-Mail Address:

Name:

Subject:

Note about attached files: Please attach any files "as found". If necessary, zip or tar multiple files into one. But try not to encrypt or obfuscate the files, as this may hinder analysis.

Attach a File: Choose file **No file chosen**

Is it ok to forward your submission to our malware analysis group?
Yes ○ No ◉

May we mention your observation in our diary?
Yes ○ No ◉

May we mention your first name in our diary?
Yes ○ No ◉

Submit

Note: All information submitted via this form will be sent to all ISC handlers. The information will be kept confidential within this group. We will only publish your information with your consent.

Contact

Example of API Usage

Based on OSSEC, let's check all IP addresses against the DShield database.

Example of API Usage

```
<command>
    <name>isc-ipreputation</name>
    <executable>isc-ipreputation.py</executable>
    <expect>srcip</expect>
    <timeout_allowed>no</timeout_allowed>
</command>
```

```
<active-response>
    <!-- Collect IP reputation data from
ISC API
      -->
    <command>isc-ipreputation</command>
    <location>server</location>
    <level>6</level>
</active-response>
```

```
$ tail -f /var/log/ipreputation.log
[2015-05-27 23:30:07,769] DEBUG No data found, fetching from ISC
[2015-05-27 23:30:07,770] DEBUG Using proxy: 192.168.254.8:3128
[2015-05-27 23:30:07,772] DEBUG Using user-agent: isc-ipreputation/1.0 (blog.rootshell.be)
[2015-05-27 23:30:09,760] DEBUG No data found, fetching from ISC
[2015-05-27 23:30:09,761] DEBUG Using proxy: 192.168.254.8:3128
[2015-05-27 23:30:09,762] DEBUG Using user-agent: isc-ipreputation/1.0 (blog.rootshell.be)
[2015-05-27 23:30:10,138] DEBUG Saving 178.119.0.173
[2015-05-27 23:30:10,145] INFO IP=178.119.0.173, AS=6848("TELENET-AS Telenet N.V.,BE"),
Network=178.116.0.0/14, Country=BE, Count=148, AttackedIP=97, Trend=0, FirstSeen=2015-04-21,
LastSeen=2015-05-27, Updated=2015-05-27 18:37:15
```

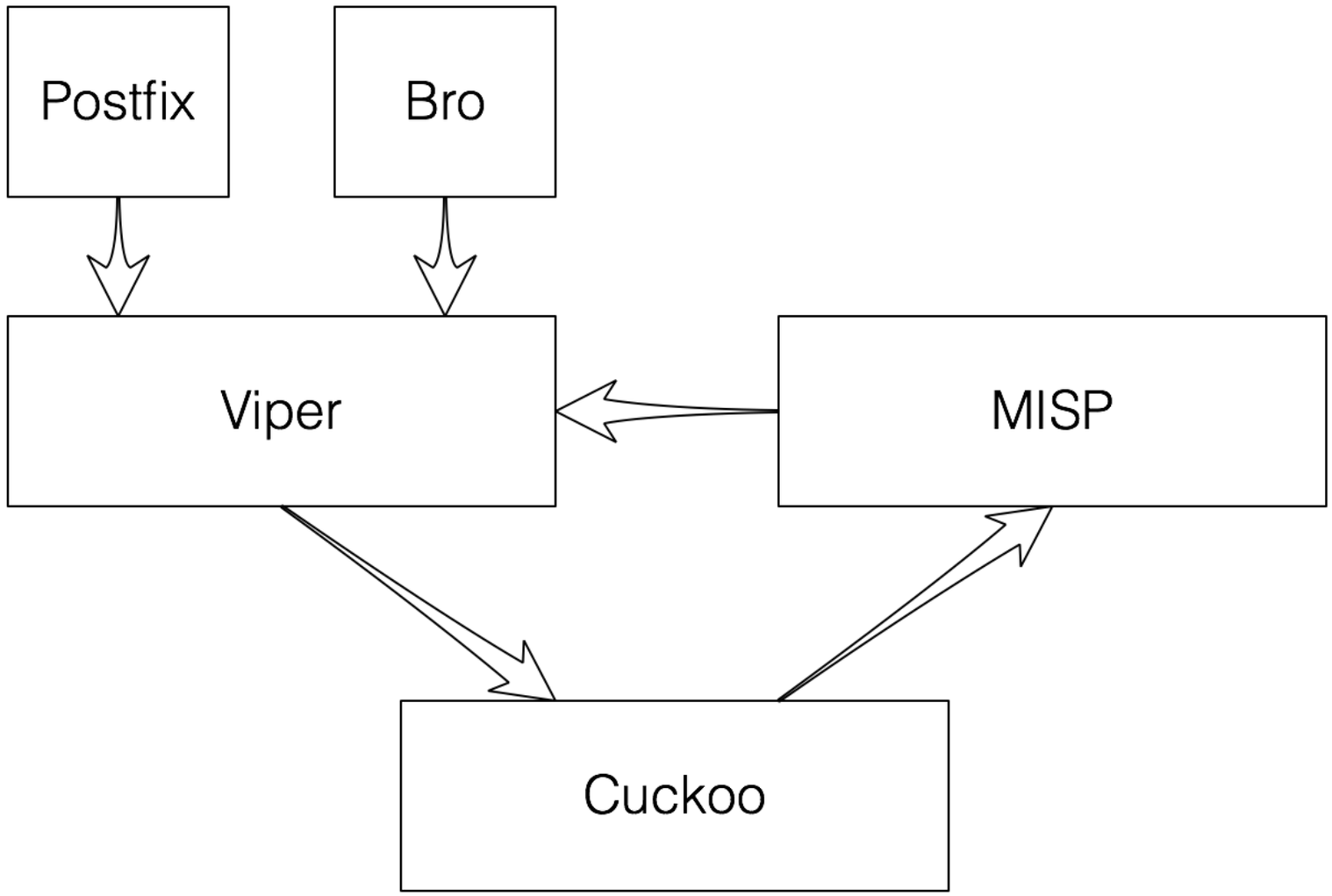
https://blog.rootshell.be/2015/06/02/playing-with-ip-reputation-with-dshield-ossec/

Feeding DShield with OSSEC

```
$ ./ossec2dshield.pl --log=/ossec/logs/firewall/firewall.log
                      --statefile=/ossec/logs/firewall/firewall.log.state
                      --userid=12345
                      --from=user@domain.com
                      --mta=localhost
                      --ports="!80,!443"
```

https://blog.rootshell.be/2011/07/15/feeding-dshield-with-ossec-logs/

Hunting for Samples



Hunting for Malicious Files

- MISP
- OSSEC
- mof.py (“MISP OSSEC Feeder”)

Hunting for Malicious Files

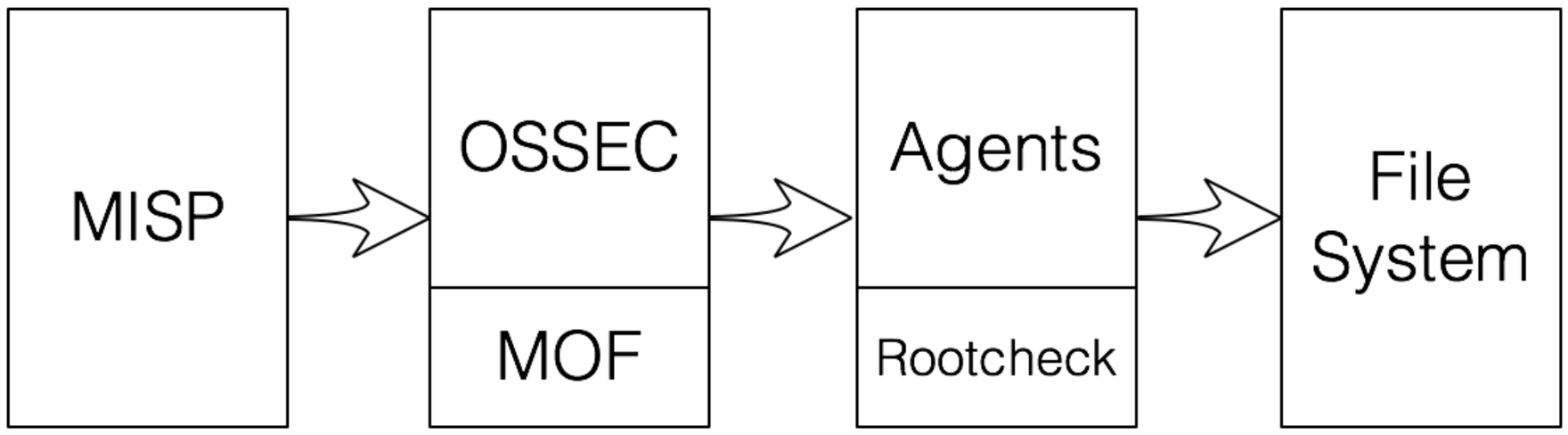
```
#
# OSSEC RootCheck IOC generated by MOF (MISP OSSEC Feeder)
# https://github.com/xme/
#
# Generated on: Mon Jul 11 22:06:56 2016
# MISP url: https://misp.home.rootshell.be/
# Wayback time: 30d
#

[MISP_2073] [any] [Packrat: Seven Years of a South American Threat Actor]
r:HKLM\SOFTWARE\Microsoft\Active;
r:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\Policies;
r:HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\msconfig;

[MISP_2200] [any] [Click-Fraud Ramdo Malware Family Continues to Plague Users]
r:HKCU\SOFTWARE\Adobe\Acrobat Reader\14.0\Globals\LastLoggedOnProvider;
r:HKCU\SOFTWARE\Adobe\Acrobat Reader\14.0\Globals\IconUnderline;
r:HKCU\SOFTWARE\Adobe\Acrobat Reader\14.0\Globals\HangDetect;
r:HKCU\SOFTWARE\Adobe\Acrobat Reader\14.0\Globals\LastProgress;
r:HKCU\SOFTWARE\Adobe\Acrobat Reader\14.0\Globals\ShowTabletKeyboard;
r:HKCU\Software\Microsoft\Windows\CurrentVersion\Run\BluetoothManage;

[MISP_2210] [any] [Jigsaw Ransomware Decrypted: Will delete your files until you pay the Ransom]
f:%USERPROFILE%\AppData\Roaming\Frfx\;
f:%USERPROFILE%\AppData\Roaming\Frfx\firefox.exe;
f:%USERPROFILE%\AppData\Local\Drpbx\;
f:%USERPROFILE%\AppData\Local\Drpbx\drpbx.exe;
f:%USERPROFILE%\AppData\Roaming\System32Work\;
f:%USERPROFILE%\AppData\Roaming\System32Work\Address.txt;
f:%USERPROFILE%\AppData\Roaming\System32Work\dr;
f:%USERPROFILE%\AppData\Roaming\System32Work\EncryptedFileList.txt;
```

Hunting for Malicious Files



Thank You!

Questions? Shoot or…

Looking for French support?

>> xmertens@isc.sans.edu

>> @xme