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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability</strong></td>
<td>&gt; A security flaw in a software program</td>
</tr>
<tr>
<td><strong>Exploit</strong></td>
<td>&gt; 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</td>
</tr>
</tbody>
</table>
| **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

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 81 36 80 BF 32 94 81 EE FC 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 DCE RPC 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


Ahead 113 days
How does Heartbleed work?

*Source:* http://xkcd.com/1354
Malware Detection and Communication Cut-off
How can a hacker control your device?

- Virus
- SQL Injection
- Internet
- DDoS
- Phishing
- Trojan
- Worm

13 © Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. HP Com.
Why Does Security Intelligence Matter?
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:

- 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 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
DV Labs 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

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

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
- DV Labs validated

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

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. HP Confidential.
Stop All Communications with Bad IP and Domain

**HP TippingPoint Reputation Feeds**

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

**Access Switch**

**HP TippingPoint**

**BLOCK OUTBOUND TRAFFIC**

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

**BLOCK INBOUND TRAFFIC**

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

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

**Botnet CnC**
5,000 - 6,000 sites worldwide

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

**Compromised Hosts**
Millions worldwide

**Phishing Sites**
50,000+ new phishing sites discovered monthly

**© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. HP Confidential.**
# ThreatDV stops Botnet-- Real Case

**HP TippingPoint Reputation Feed**

Czech Republic

<table>
<thead>
<tr>
<th>事件</th>
<th>源IP</th>
<th>目的IP</th>
<th>目的Port</th>
<th>目的區域</th>
<th>次數</th>
<th>時間</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.80.219.344</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:59:31</td>
</tr>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.44.138.91</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:58:35</td>
</tr>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.80.219.344</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:58:25</td>
</tr>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.44.138.91</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:57:21</td>
</tr>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.80.219.344</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:57:11</td>
</tr>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.44.138.91</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:56:19</td>
</tr>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.80.219.344</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:55:59</td>
</tr>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.44.138.91</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:55:09</td>
</tr>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.80.219.344</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:54:49</td>
</tr>
<tr>
<td>Rep-60 31 170.179.179</td>
<td>10.44.138.91</td>
<td>31.170.179.179</td>
<td>80</td>
<td>CZ</td>
<td>1</td>
<td>2013/04/03 00:53:55</td>
</tr>
</tbody>
</table>

Multiple inside devices communicate with a malicious IP in midnight.
DDoS
Real Case Study 1 (Stuff up the link of a manufacture)

**ICMP Fragmented Packet**

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.

(Compare with history behavior)
Trend analysis helps detecting abnormal traffic in real time

Drill Down ➔ We can see all attack sources

(Inside IP- Botnet)  (Destination- Victim)  (Huge Amount)
Real Case Study 2 (Brute force attack)

(17:39, Brute Force AD event burst)

(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

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

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

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

<table>
<thead>
<tr>
<th>NO</th>
<th>Event Name</th>
<th>Source IP</th>
<th>Src Country</th>
<th>Destination IP</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NXDomain-Black-List sip/tcp/sip.linkyes.com.tw</td>
<td>10.7.107</td>
<td>TW</td>
<td>192.201</td>
<td>46.99K</td>
</tr>
<tr>
<td>2</td>
<td>NXDomain-Black-List ssl</td>
<td>10.0.41</td>
<td>TW</td>
<td>192.201</td>
<td>46.8K</td>
</tr>
<tr>
<td>3</td>
<td>NXDomain-Black-List ssl</td>
<td>10.0.7.66</td>
<td>TW</td>
<td>192.201</td>
<td>43.67K</td>
</tr>
<tr>
<td>4</td>
<td>NXDomain-Black-List <a href="mailto:bcmibsqa1@broadcom.com">bcmibsqa1@broadcom.com</a></td>
<td>10.0.199</td>
<td>TW</td>
<td>192.201</td>
<td>43.28K</td>
</tr>
<tr>
<td>5</td>
<td>NXDomain-Black-List <a href="mailto:bcmibsqa1@broadcom.com">bcmibsqa1@broadcom.com</a></td>
<td>10.0.92.43</td>
<td>TW</td>
<td>192.201</td>
<td>42.39K</td>
</tr>
<tr>
<td>6</td>
<td>NXDomain-Black-List ssl</td>
<td>10.0.113</td>
<td>TW</td>
<td>192.201</td>
<td>42.13K</td>
</tr>
<tr>
<td>7</td>
<td>NXDomain-Black-List <a href="mailto:bcmibsqa1@broadcom.com">bcmibsqa1@broadcom.com</a></td>
<td>10.0.21.151</td>
<td>TW</td>
<td>192.201</td>
<td>41.81K</td>
</tr>
<tr>
<td>8</td>
<td>NXDomain-Black-List samsungvueventlog.vlingo.com</td>
<td>10.0.26.183</td>
<td>TW</td>
<td>192.201</td>
<td>41.13K</td>
</tr>
<tr>
<td>9</td>
<td>NXDomain-Black-List lipin.ctrp.cnc.cgoslbn.net</td>
<td>10.0.192.191</td>
<td>TW</td>
<td>192.201</td>
<td>32.26K</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>NO</th>
<th>Event Name</th>
<th>Source IP</th>
<th>Src Country</th>
<th>Destination IP</th>
<th>Dest Country</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13019: DNS: DNS ANY Response</td>
<td>21.38</td>
<td>TW</td>
<td>92.201</td>
<td>TW</td>
<td>773.46K</td>
</tr>
<tr>
<td>2</td>
<td>13019: DNS: DNS ANY Response</td>
<td>94.123.247.2</td>
<td>TR</td>
<td>92.190</td>
<td>TW</td>
<td>397.11K</td>
</tr>
<tr>
<td>3</td>
<td>13019: DNS: DNS ANY Response</td>
<td>245.116</td>
<td>TW</td>
<td>92.201</td>
<td>TW</td>
<td>353.73K</td>
</tr>
<tr>
<td>4</td>
<td>13019: DNS: DNS ANY Response</td>
<td>72.200.121.163</td>
<td>US</td>
<td>92.201</td>
<td>TW</td>
<td>299.8K</td>
</tr>
<tr>
<td>5</td>
<td>13019: DNS: DNS ANY Response</td>
<td>4.203</td>
<td>TW</td>
<td>92.201</td>
<td>TW</td>
<td>181.84K</td>
</tr>
<tr>
<td>6</td>
<td>13019: DNS: DNS ANY Response</td>
<td>83.161</td>
<td>TW</td>
<td>92.201</td>
<td>TW</td>
<td>169.3K</td>
</tr>
<tr>
<td>7</td>
<td>13019: DNS: DNS ANY Response</td>
<td>31.1244</td>
<td>TW</td>
<td>92.201</td>
<td>TW</td>
<td>155K</td>
</tr>
<tr>
<td>8</td>
<td>13019: DNS: DNS ANY Response</td>
<td>244.111</td>
<td>TW</td>
<td>92.201</td>
<td>TW</td>
<td>141.08K</td>
</tr>
<tr>
<td>9</td>
<td>13019: DNS: DNS ANY Response</td>
<td>4.181</td>
<td>TW</td>
<td>92.201</td>
<td>TW</td>
<td>134.99K</td>
</tr>
<tr>
<td>10</td>
<td>13019: DNS: DNS ANY Response</td>
<td>87.210.50.215</td>
<td>NL</td>
<td>92.192</td>
<td>TW</td>
<td>134.23K</td>
</tr>
</tbody>
</table>
DDoS防禦案例 (不當流覽網頁) - 即時分析得知,立即消弭

<table>
<thead>
<tr>
<th>事件</th>
<th>異常發生時間</th>
<th>異常次數</th>
<th>一一小時平均次數</th>
<th>異常率 (%)</th>
<th>峰值異常次數</th>
</tr>
</thead>
<tbody>
<tr>
<td>11349: HTTP: Default Page Request (ONLY enable when under DoS attack)</td>
<td>2013/02/19 02:54:00</td>
<td>9214</td>
<td>1521</td>
<td>605</td>
<td></td>
</tr>
</tbody>
</table>

2/19 02:54 異常突增

遭惡意流覽的網站IP

惡意流覽來源

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

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?

瞬間發出巨量SSH登入請求

2/12 07:45 異常突增
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 prevalence only continues to grow

**Mobile devices are everywhere**
Today the average person carries **2.9 devices**

**Mobile apps**
More than **160 billion apps** will be downloaded globally in 2017, up from **80 billion in 2013**

**Mobile commerce**
Projected growth from **$241 billion in 2011** to **$1 trillion in 2015**

---

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 exploit able

- 96% of attacks not particularly difficult to execute\(^2\).

\(^1\) IBM Analytics
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

Access private info
HP 2013 Cyber Risk Report

Mobile – Top Issues

- Mobile apps security: 46% of mobile iOS and Android applications use encryption improperly.
- Security issues were a result of insecure client-side operation: 52%
- Insecure server-side application code or code quality issues – unstable application behavior: 48%
- Unnecessary permissions: 74%
HP 2013 Cyber Risk Report

Mobile – Top 4 client side issues

**Top client-side issues in native mobile applications**

- Encryption: 46%
- Permissions: 24%
- Storage: 26%
- WebView: 24%
HP 2013 Cyber Risk Report

Mobile – Top 4 issues

Top Four Mobile Security Issues Breakdown

- Insecure certificate verification, 8%
- Unencrypted storage, 51%
- Insecure SSL configuration, 41%
- Excessive permissions, 74%
- Unrestricted cross-domain communication, 26%
- Insecure logging and hard codes information, 37.93%
- Insecure storage location, 41.38%
- Insecure database access, 28.69%
- Insecure native access via HTML injection, 20%
- Untrusted content, 80%
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

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Hit Count</th>
<th>Private SourceIP</th>
<th>Public SourceIP</th>
<th>Username</th>
<th>Source MAC</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012/5/7 21:36</td>
<td>1400: SMB Windows Logon Failure</td>
<td>152</td>
<td>192.168.1.222</td>
<td>210.100.38.101</td>
<td>Robin Shih</td>
<td>00-50-56-C0-00-01</td>
<td>AP-1</td>
</tr>
<tr>
<td>2012/5/7 21:44</td>
<td>9991: HTTPS: Google Gmail Access</td>
<td>2</td>
<td>2192.168.1.33</td>
<td>210.100.38.101</td>
<td>Sandy Chen</td>
<td>00-50-56-DF-11-1A</td>
<td>AP-1</td>
</tr>
<tr>
<td>2012/5/7 21:45</td>
<td>BitTorrent: Peer-to-Peer Communications</td>
<td>1</td>
<td>192.168.2.166</td>
<td>210.100.38.102</td>
<td>Ken Yip</td>
<td>00-50-56-62-13-2F</td>
<td>AP-2</td>
</tr>
<tr>
<td>2012/5/7 21:52</td>
<td>69270: BitTorrent: Peer-to-Peer Communications</td>
<td>69</td>
<td>192.168.1.33</td>
<td>210.100.38.101</td>
<td>Sandy Chen</td>
<td>00-50-56-DF-11-1A</td>
<td>AP-1</td>
</tr>
<tr>
<td>2012/5/7 21:59</td>
<td>192.168.1.45</td>
<td>1</td>
<td>192.168.1.45</td>
<td>210.100.38.101</td>
<td>Richard Chou</td>
<td>00-50-56-00-14-B4</td>
<td>AP-1</td>
</tr>
<tr>
<td>2012/5/7 22:17</td>
<td>6545: MS-RPC: Microsoft Server Service Buffer Overflow</td>
<td>1192.168.2.88</td>
<td>210.100.38.102</td>
<td>Peter White</td>
<td>00-50-56-77-11-54</td>
<td>AP-2</td>
<td></td>
</tr>
<tr>
<td>2012/5/7 22:22</td>
<td>192.168.1.77</td>
<td>1</td>
<td>192.168.1.77</td>
<td>210.100.38.101</td>
<td>Jeremy Lin</td>
<td>00-50-56-DD-30-6A</td>
<td>AP-1</td>
</tr>
<tr>
<td>2012/5/7 22:25</td>
<td>5670: HTTP: SQL Injection (SELECT)</td>
<td>17</td>
<td>192.168.2.88</td>
<td>210.100.38.102</td>
<td>Peter White</td>
<td>00-50-56-77-11-54</td>
<td>AP-2</td>
</tr>
</tbody>
</table>
Thank you