Botfox - 基於瀏覽器與社交工程之殭屍網路研究

Botnet based on Browser and Social Engineering

動機

你知道嗎？
現行的安全防護不像你想像的那般健壯 ...

實驗證實，
『它』可以繞過目前所有常見的安全防護 ...

你相信嗎？
『它』的技術含量低到只有我用『它』...

你相信嗎？
『它』的建置成本很低很低 ...

你認同嗎？
大腦本身就是一種永遠可以被利用的 0day...

自我介紹

Ant

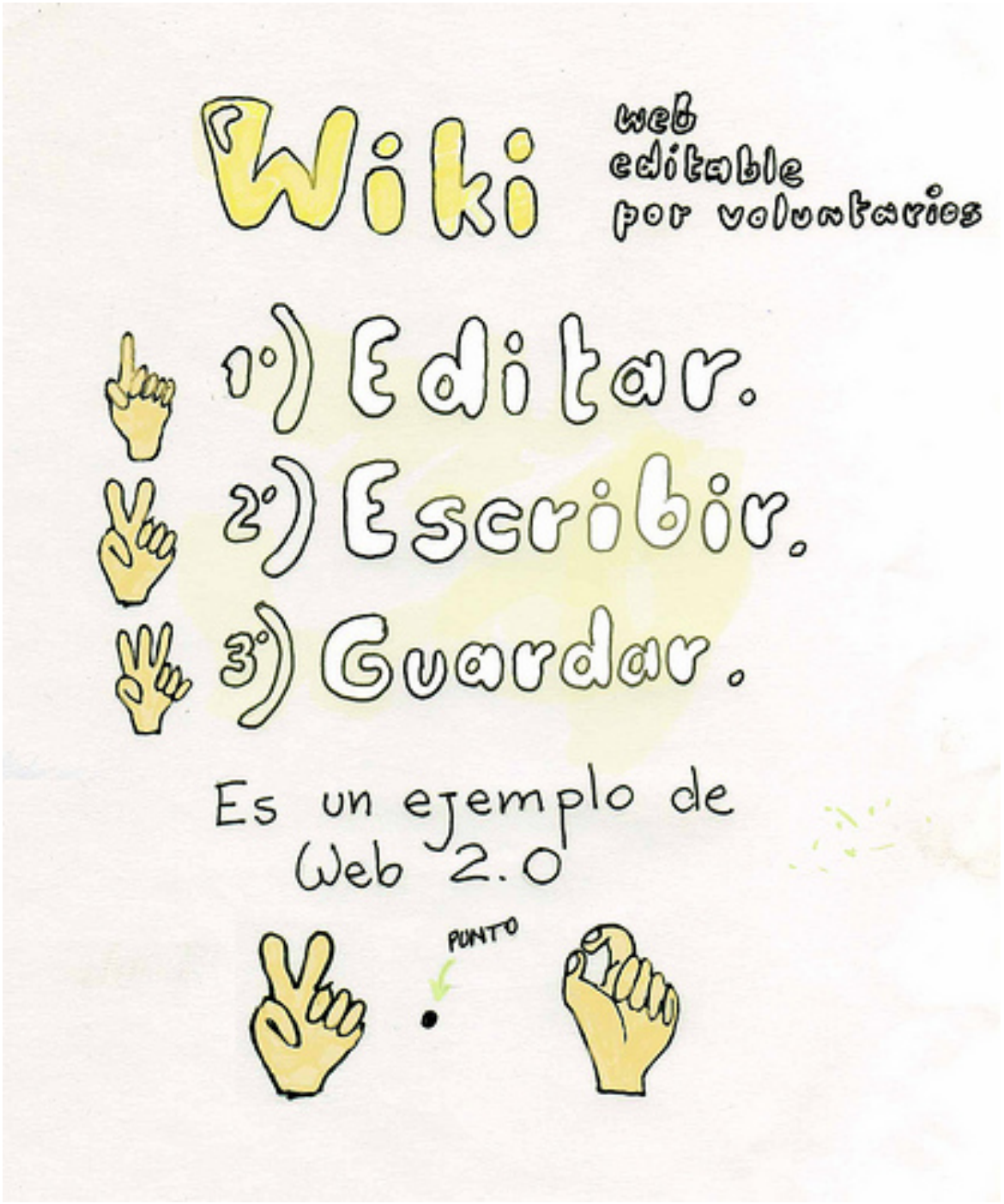
yftzeng@gmail.com


FreeBSD 官方中文文件維護者
自由軟體授權
系統管理師
Wow!USB 隨身碟防毒
經濟學
中研院
自由軟體鑄造場
台灣駭客年會講師
Wow!ScanEngine 掃毒引擎
程式設計師
Wow!ARP 防護軟體

主題

歡迎來到

Web 2.0 的時代

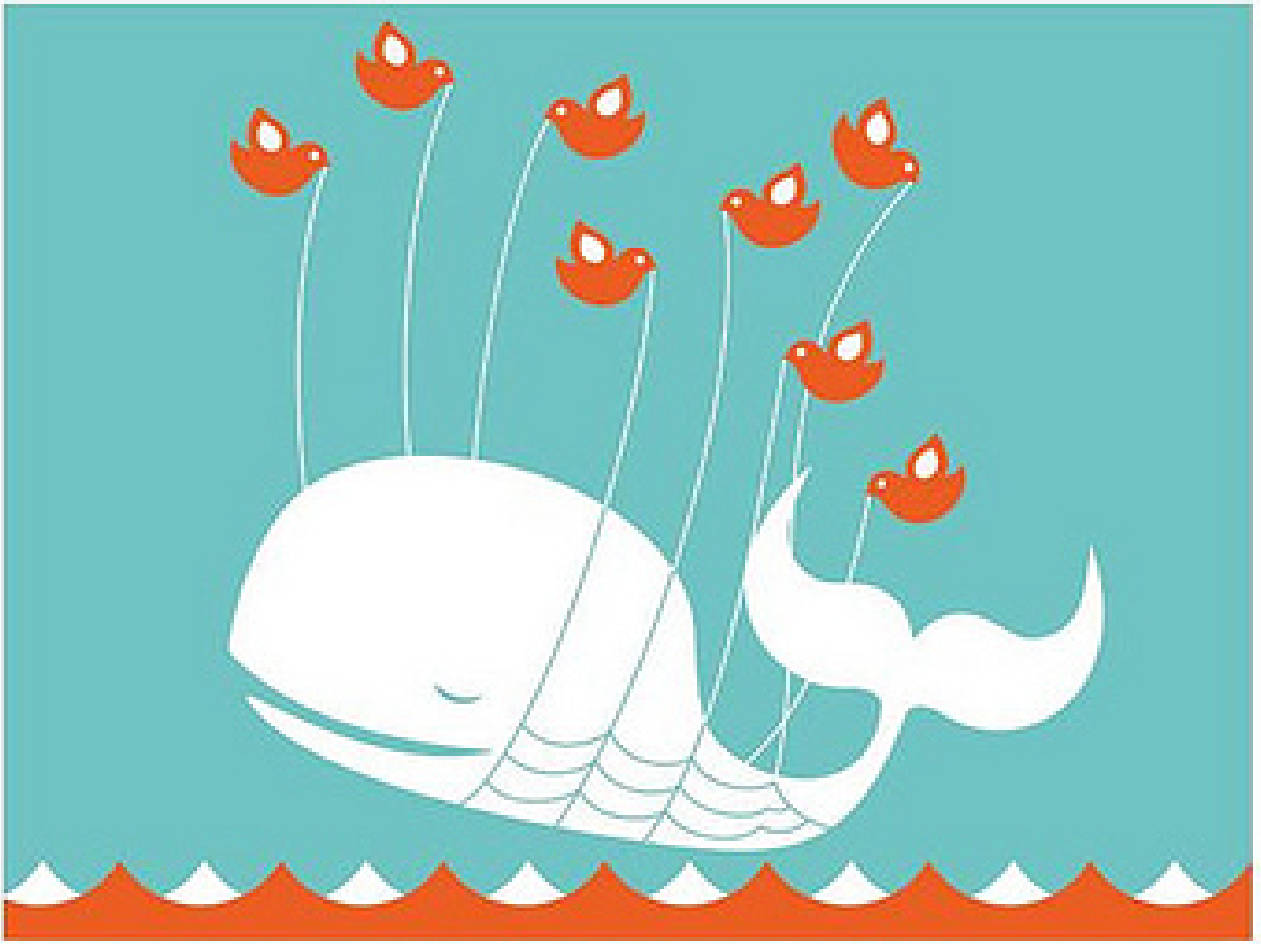


twitter

Home Public Timeline Help

Twitter is over capacity.

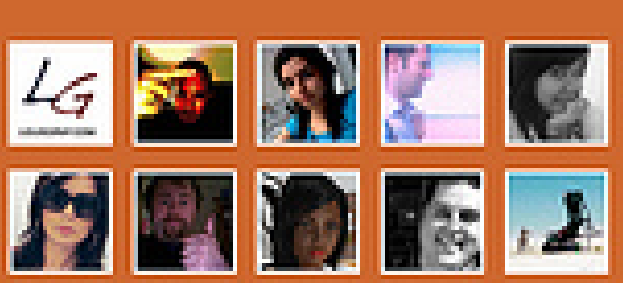
Too many tweets! We'll try to lighten the load and have things back to normal soon.



Already a member? Sign in

Plurk is a place that lets you publish and share your thoughts, emo-ness, #^@%!*%(& and loves.

See what other people are doing right now or signup.



歡迎來到

Cloud 的時代

Power · Robust · Convenience

當一切都變得不再單純 ...

混沌、複雜

Friday, April 3, 2009

TEST

S:*:DEMO:yftzeng@gmail.com:Hi
Welcome to HIT 2009

Posted by Ant at 12:18 AM 0 comments

Labels

- words (169)
- security (53)
- management (37)
- feeling (30)
- rethinking (24)

twitter

Home Profile Find People Settings Help Sign out

o_O **demohit**

Follow

<Email>:[text]:Email:ant
<Passwd>:
[password]:Passwd:ossf
<PersistentCookie>:
[checkbox]:PersistentCookie:yes
<signIn>:[submit]:sign in

less than a minute ago from web

Name HIT

0 following 16 followers

Updates 296

Favorites

Actions

block **demohit**

Following

RSS feed of demohit's updates

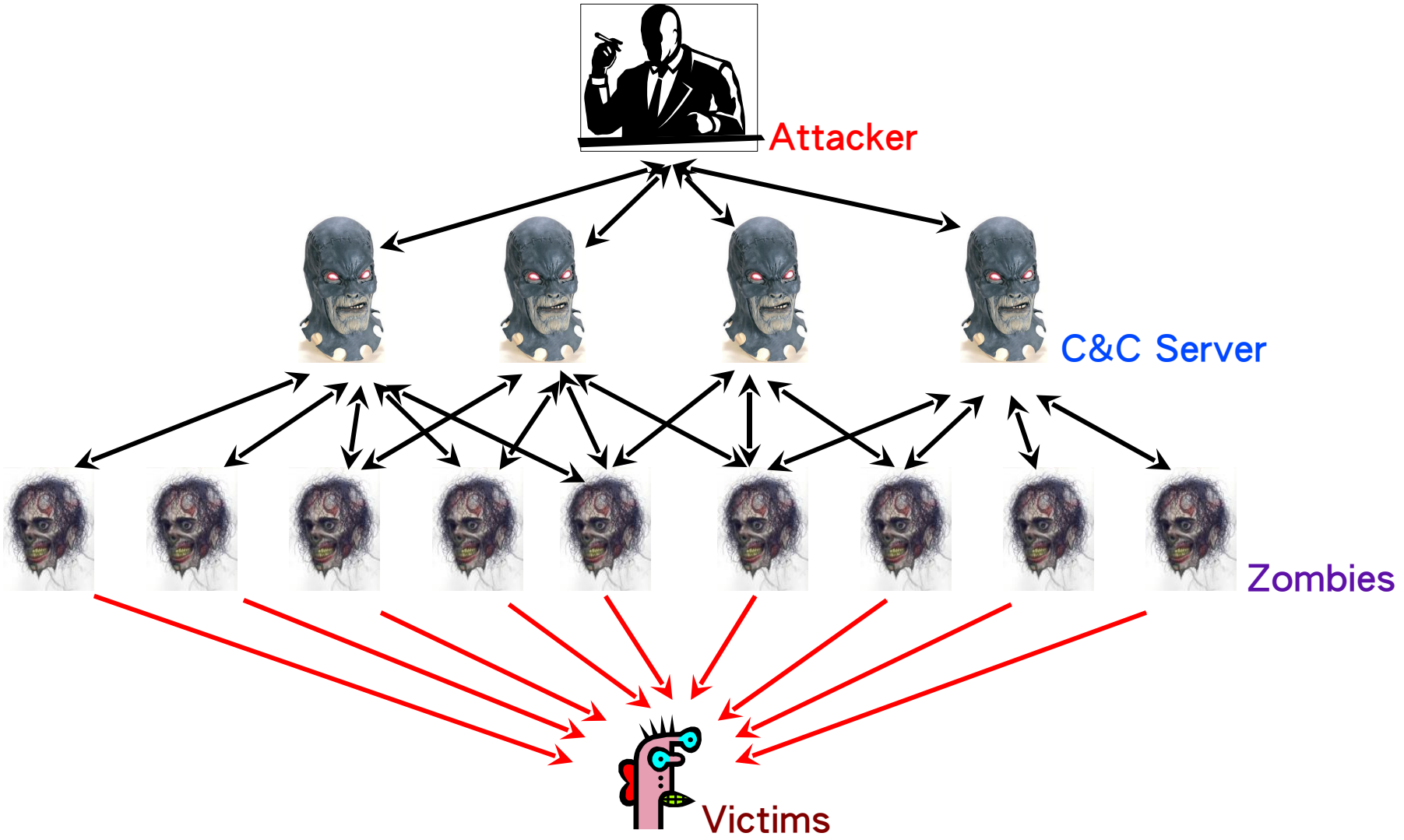
歡迎來到

~~Web 2.0 的時代~~

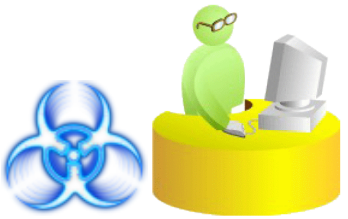
Bot 2.0 的時代

(aka. CloudBot)

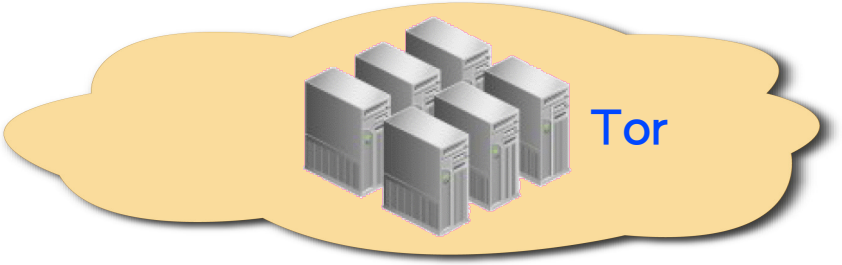
Bot 1.0


Attacker
C&C Server
Zombies
Victims

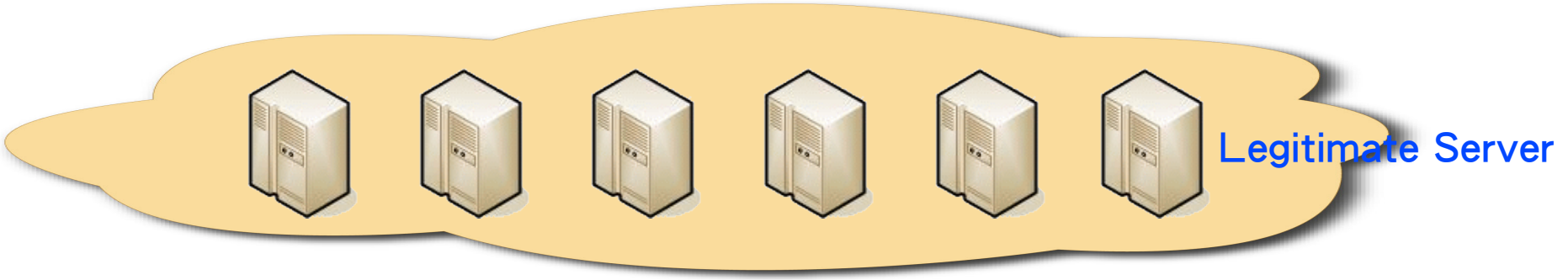
Bot 2.0
(aka CloudBot)



Attacker

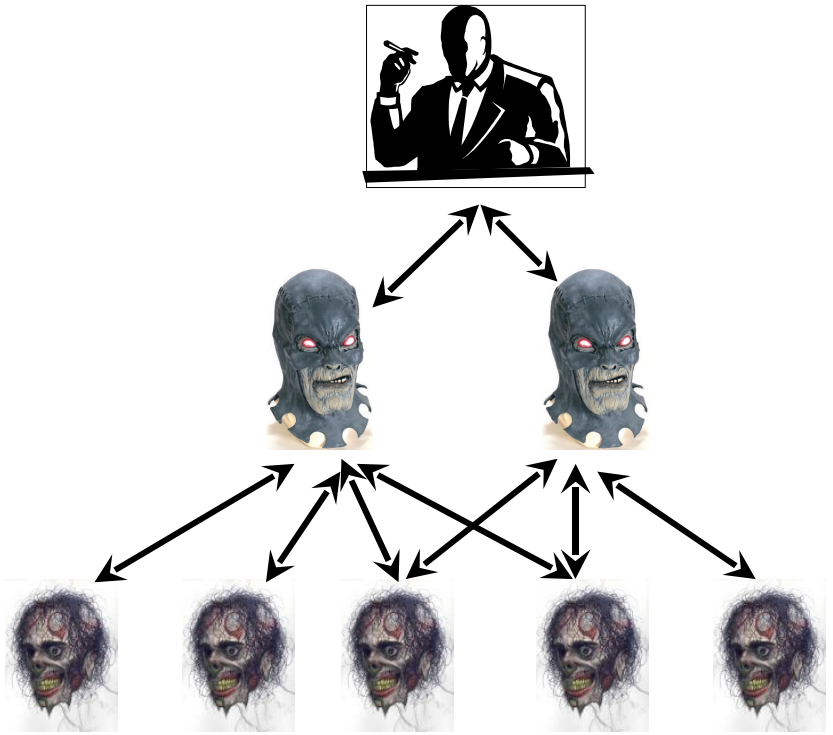


Tor

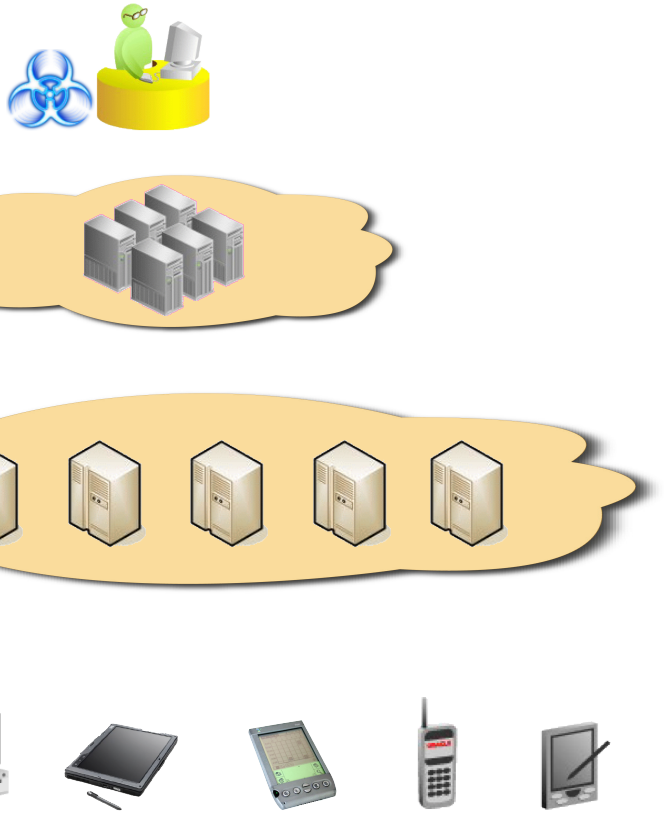


Legitimate Server

Bot 1.0



Bot 2.0



Botnet 的定義

指由 Malware 操控平台所成形成的一種 Command and Control (C&C) Topology 。透過 Botnet 架構讓 Hacker 能夠大量且自動化地操控 Bot 。

來源：

Jeremy Chiu (aka Birdman)

Workshop on Understanding Botnets of Taiwan 2009
第一屆台灣區 Botnet 偵測與防治技術研討會

殭屍網路的
演化史

演化趨勢
推斷未來模式

以 Protocol 分群

Protocol

1. IRC
2. HTTP
3. P2P
4. Instant Messenger (MSN etc.)
5. Own communication

Botnet Trends Analysis

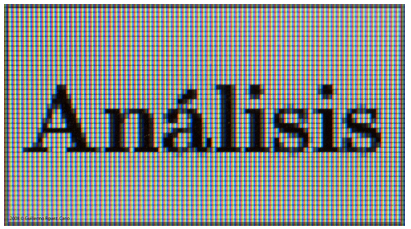
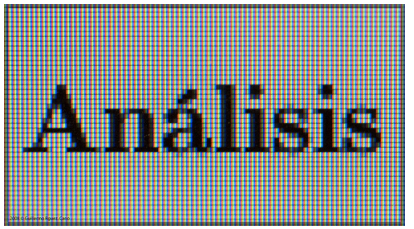


Photo:
wil.eeam@flickr.com
http://www.flickr.com/photos/wileeam/2410989725/

Botnet Trends Analysis



1. 高隱匿、難追蹤
2. 利用社交工程
3. 開始注意嵌入式設備
4. 以感染的數量換取其它的優勢

Photo:
wil.eeam@flickr.com
http://www.flickr.com/photos/wileeam/2410989725/

Router Botnet

* called 'psyb0t'
* maybe first botnet worm to target routers and DSL modems
* contain shellcode for many mipsel devices
* not targeting PCs and Servers
* user multiple strategies for exploitation, such as bruteforce user/pass
* harvests usernames and passwords through deep packet inspection
* can scan for exploitable phpMyAdmin and MySQL servers

回到主題

Botfox - 基於瀏覽器與社交工程之殭屍網路研究

Botnet based on Browser and Social Engineering

提出一個對於未來演化的可能
以及早對未來作出因應對策

Botfox *Research*

1. 基於瀏覽器
2. 基於社交工程
3. 基於純 JavaScript 語言
4. 基於 Web 2.0/Cloud

Photo:
Sparrow*@flickr.com
http://www.flickr.com/photos/90075529@N00/140896634

基於瀏覽器

1. 非常容易模擬正常行為（基於 Port 80, 443 的實現）
2. 跨平台特性（手持式裝置、手機等）
3. 最常使用的應用程式之一
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

基於社交工程

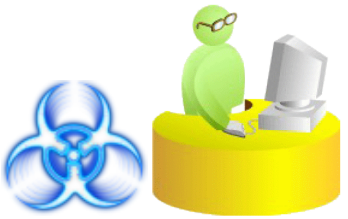
1. 人性是資訊安全最弱的一環
2. 修補大腦比修補軟體漏洞來得難
3. 即使訓練有素，仍難敵好奇心驅使

基於純 JavaScript

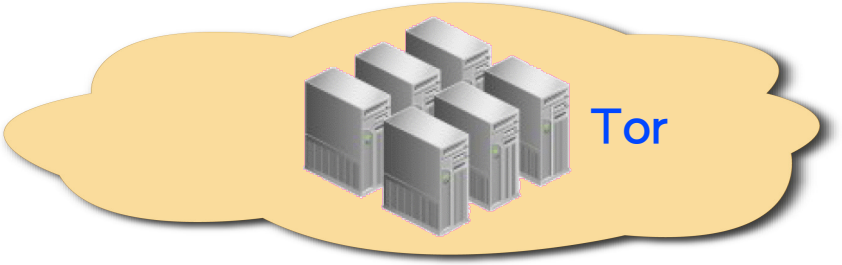
1. 網頁標準語言之一
2. 跨瀏覽器的特性
3. 防毒軟體難以分析其惡意程式
4. 不需額外開啟通訊埠(port)

基於 Web 2.0/Cloud

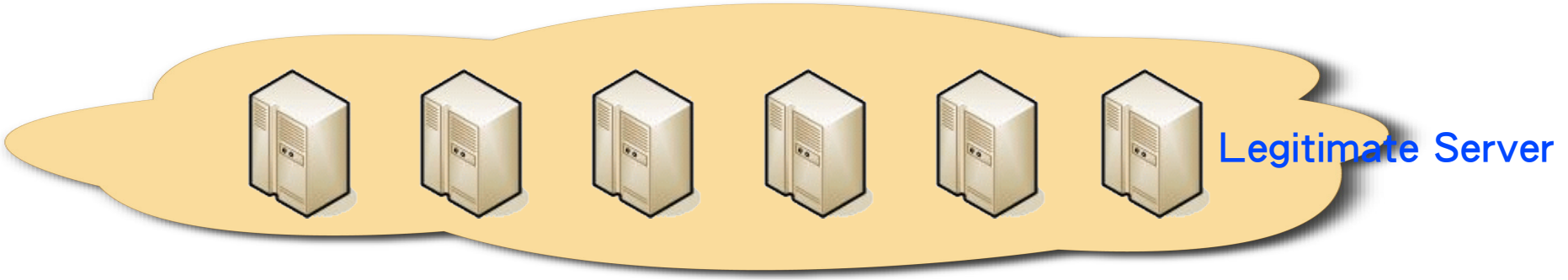
1. 運用 Web 2.0 的發文機制
2. 使用 Cloud 的效能與穩定性
3. 低成本開發，不需設計 Protocol 與建置 C&C
4. 基於合法網站為掩護



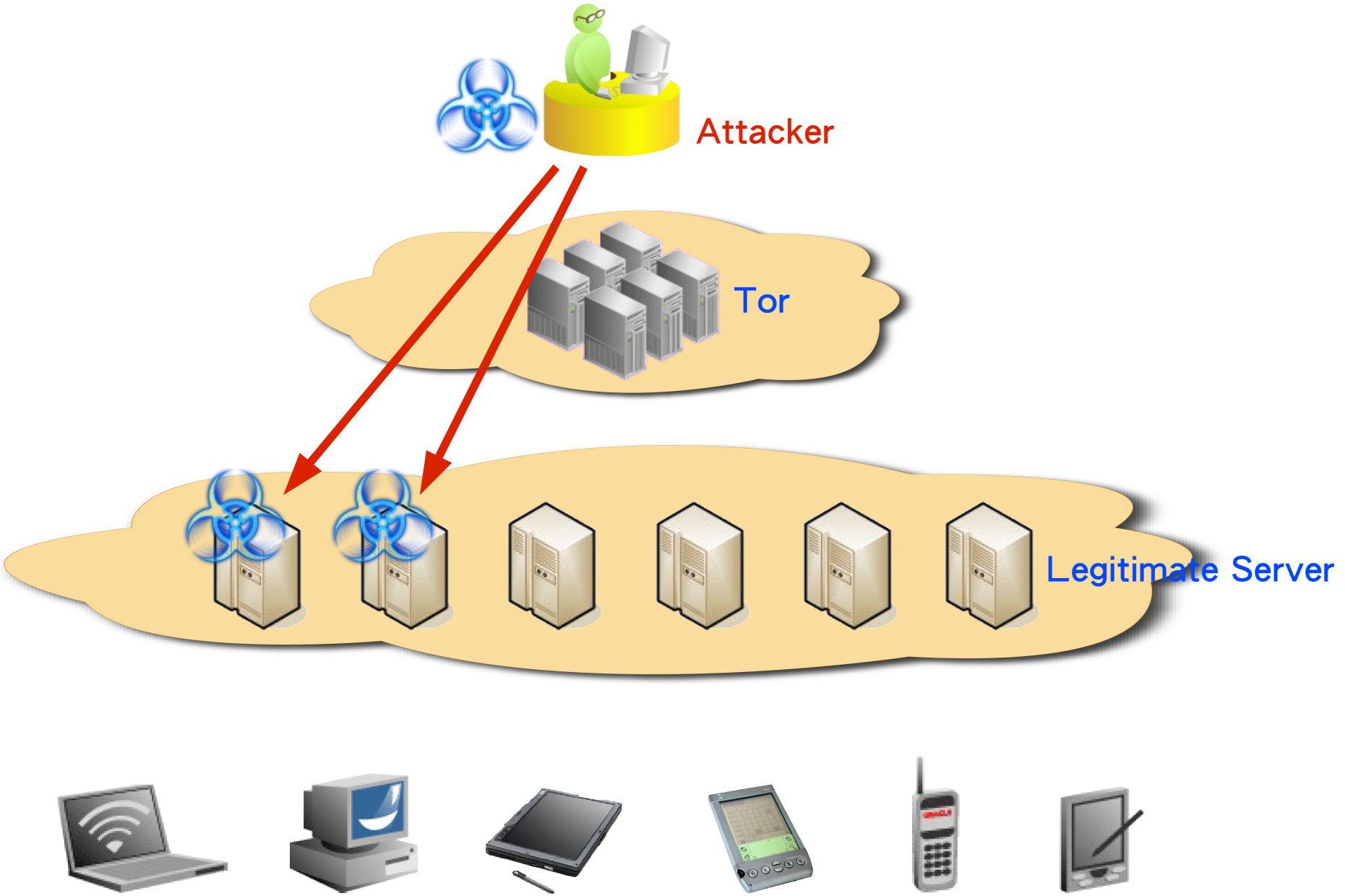
Attacker



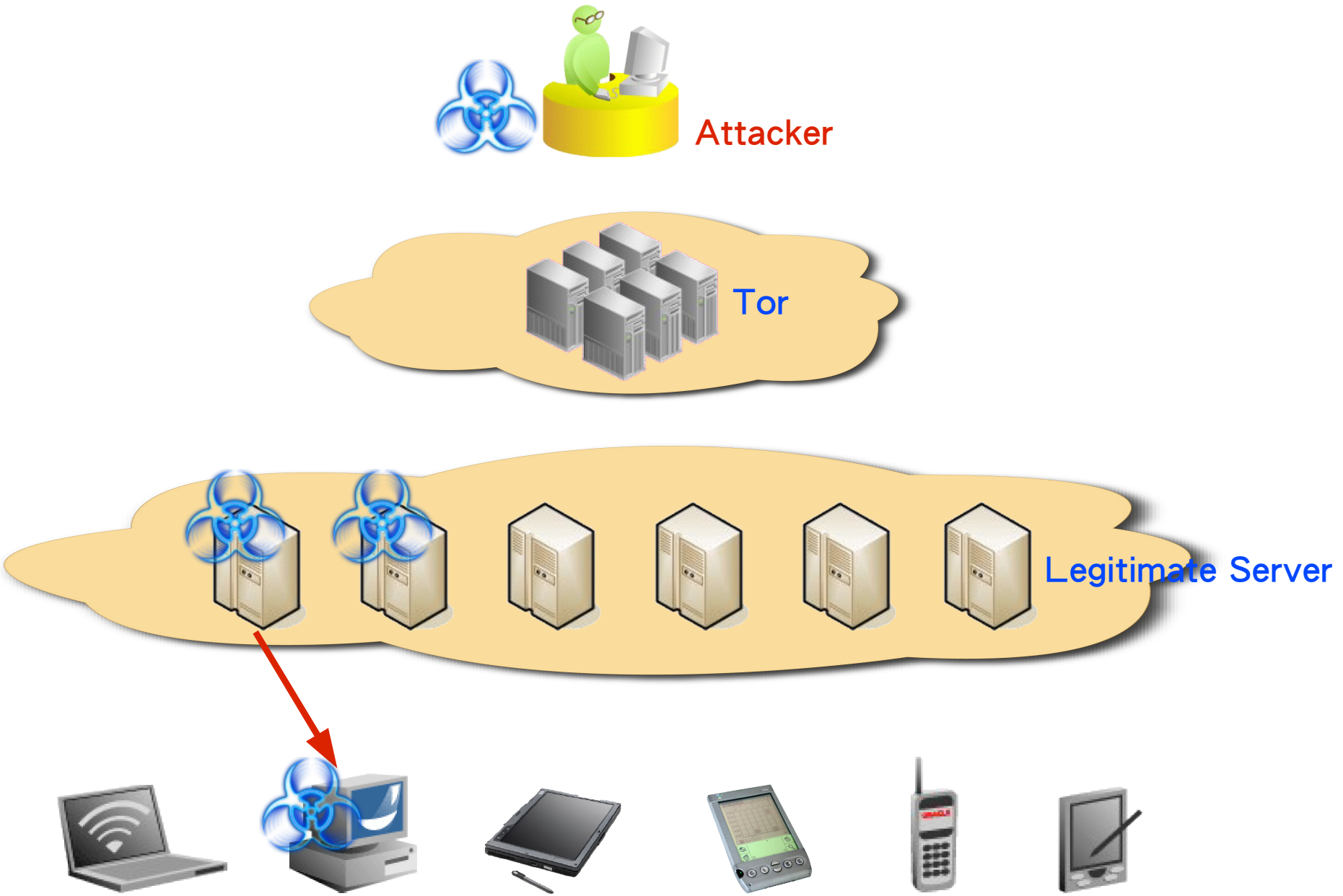
Tor



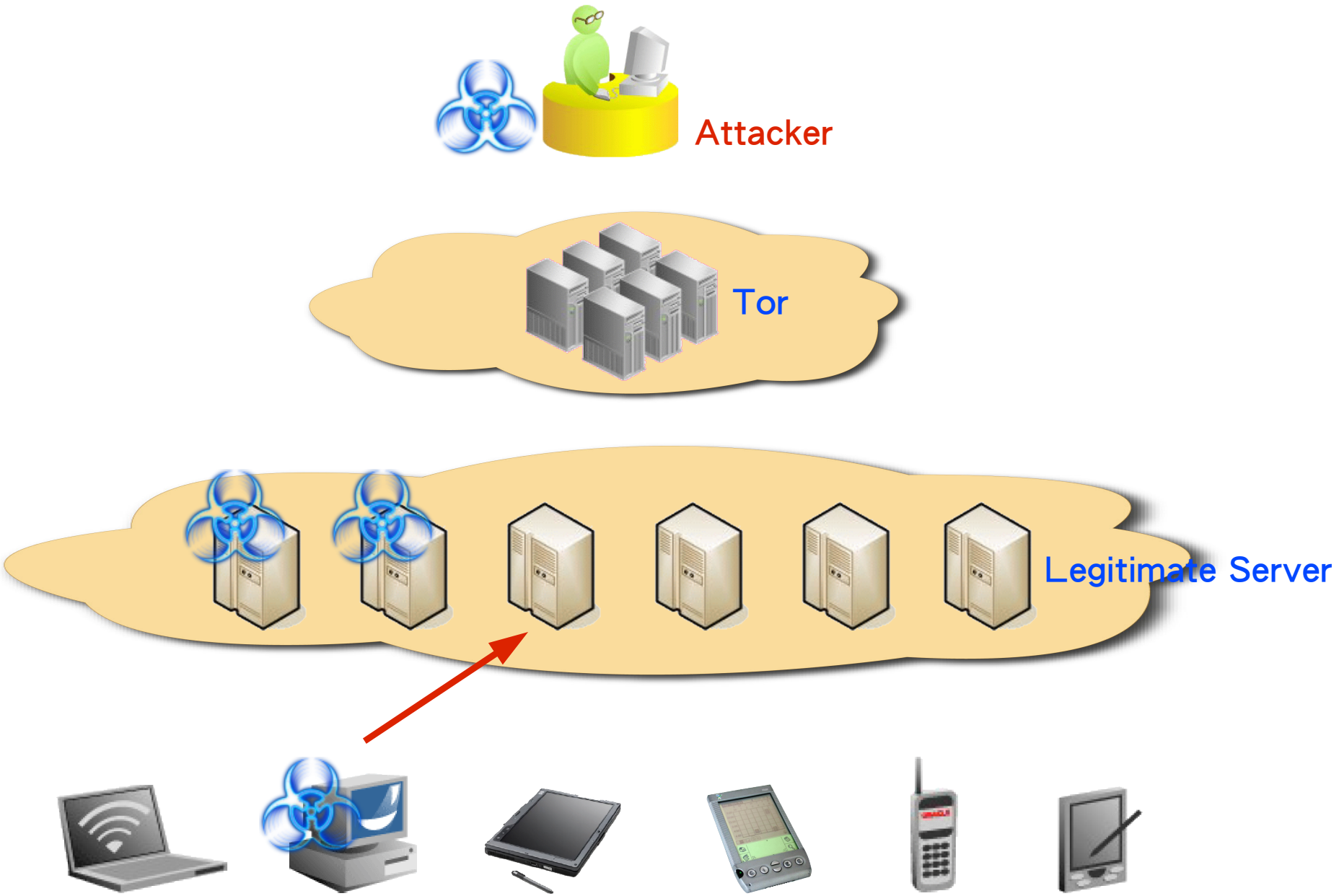
Legitimate Server

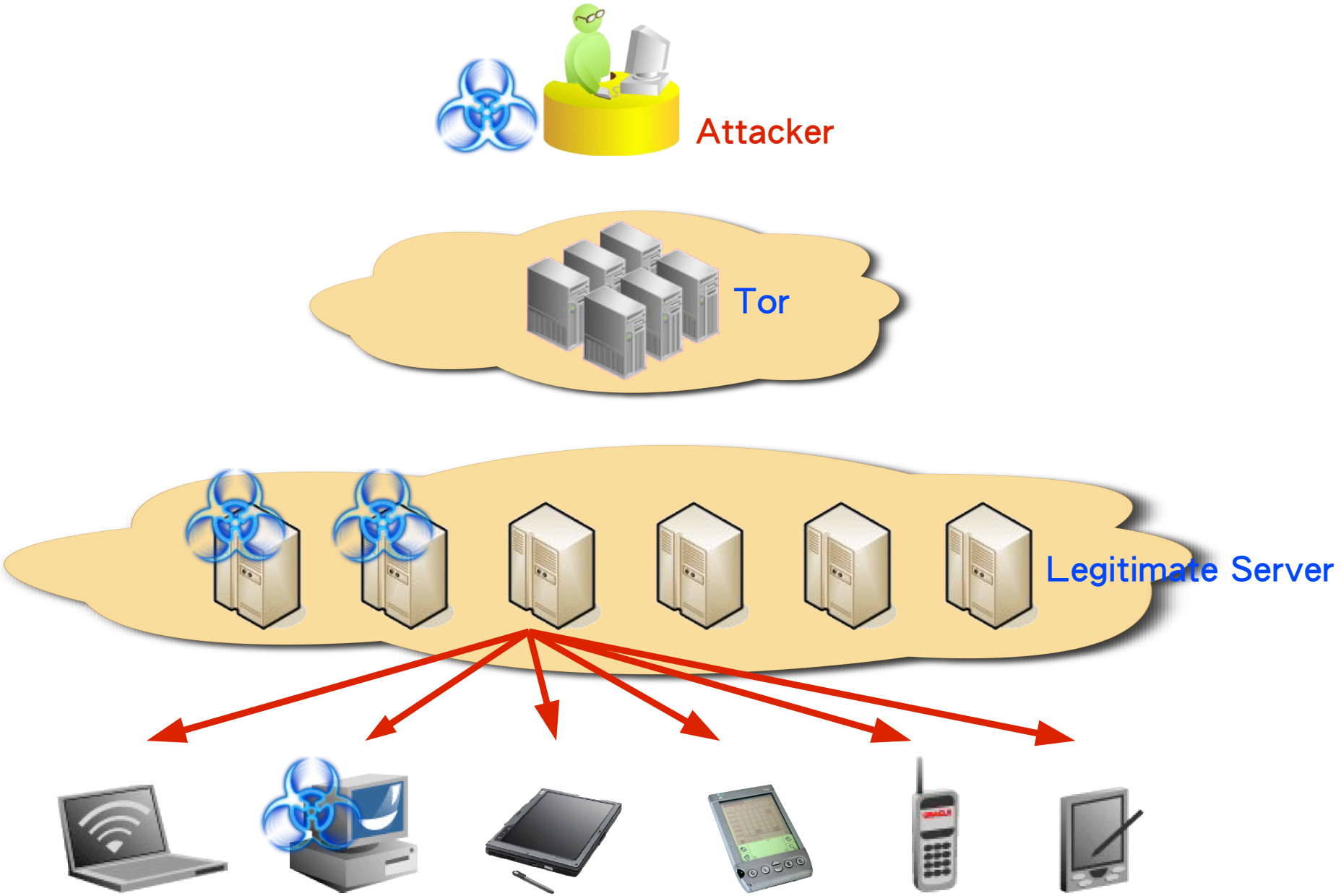

Attacker
Tor
Legitimate Server


Attacker
Tor
如釣魚般等待上餌
Legitimate Server

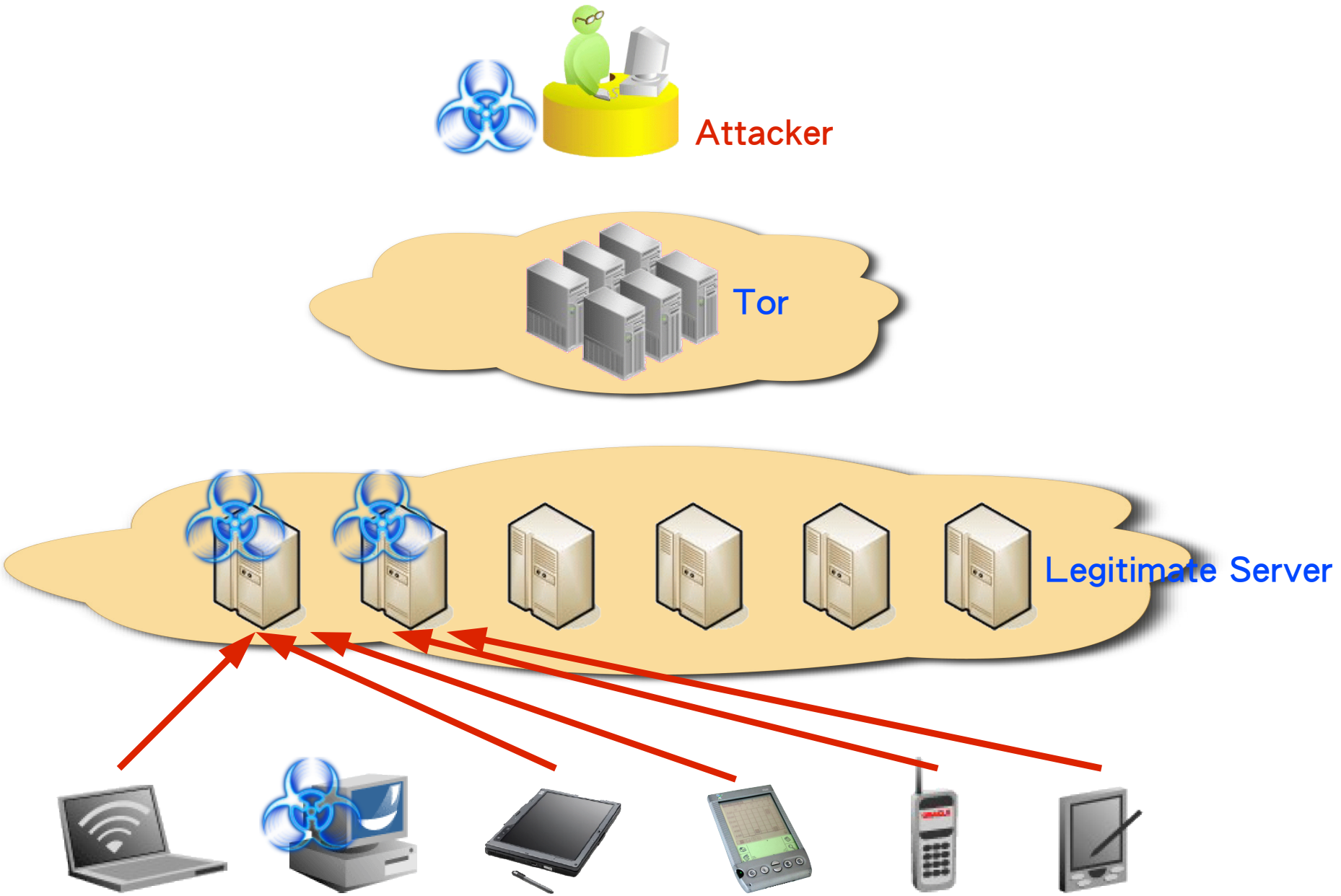

Attacker
Tor
Legitimate Server

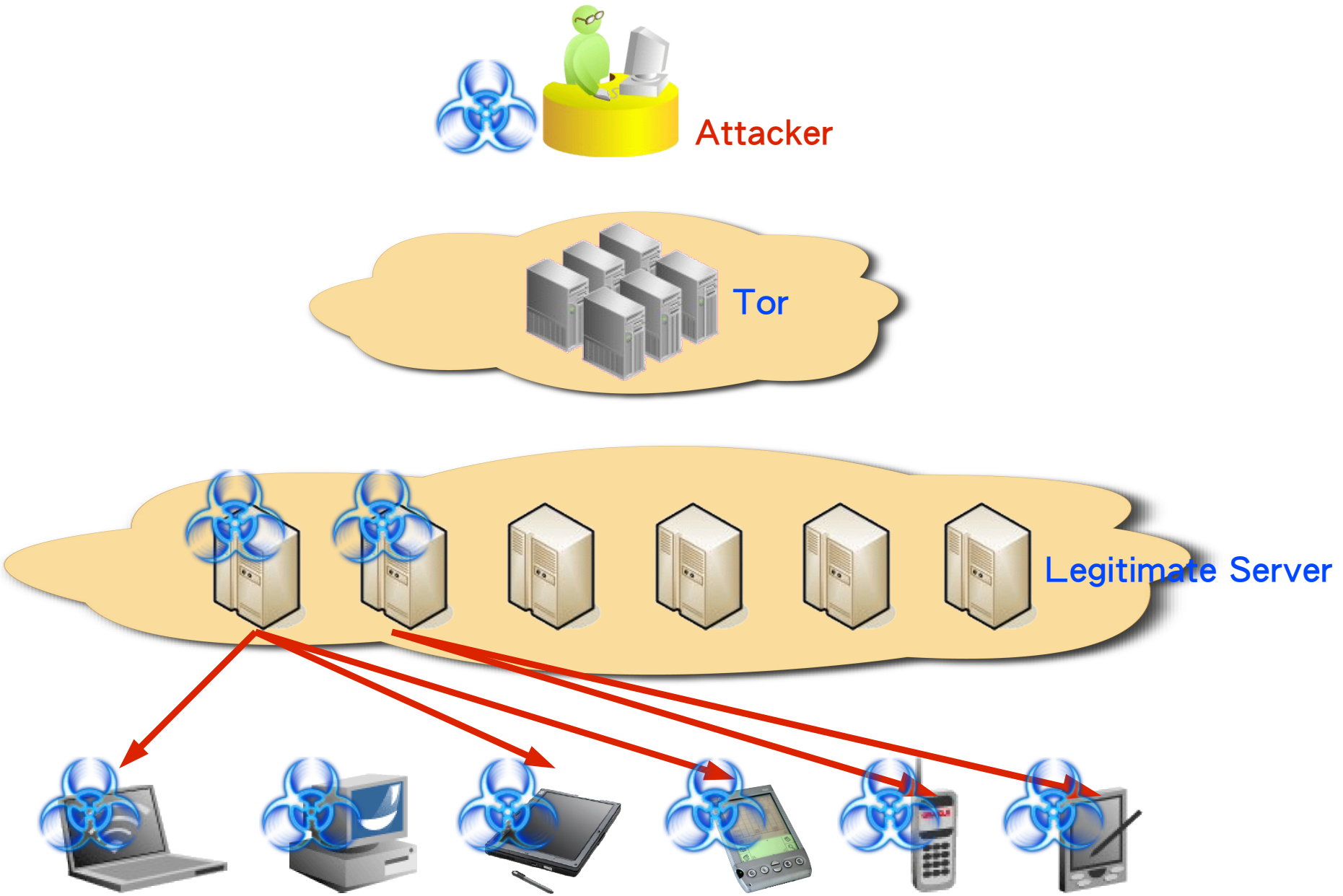

Attacker
Tor
利用受害者的名義及社交網路散佈 (如 Email)
Legitimate Server


Attacker
Tor
Legitimate Server

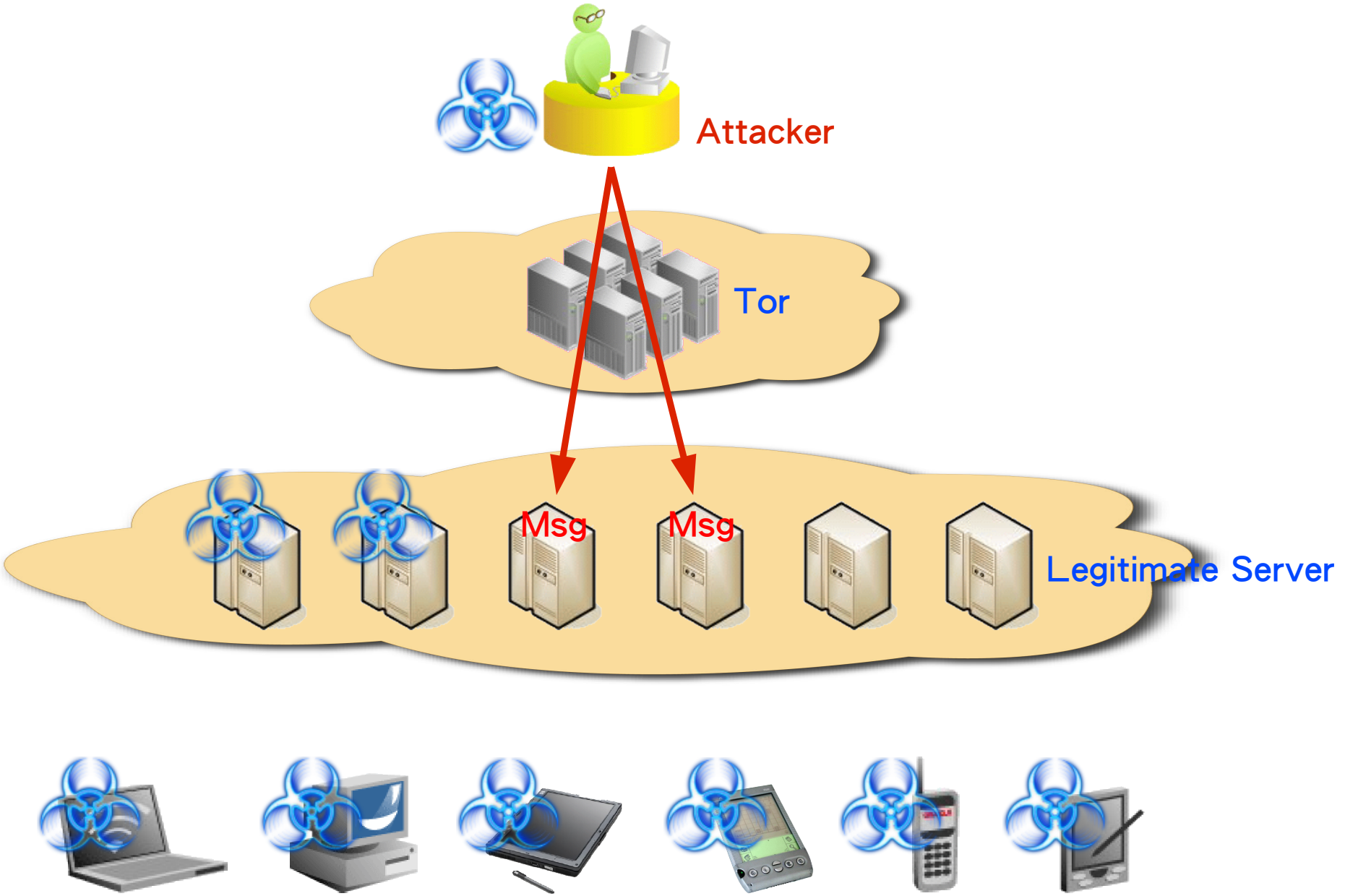

Attacker
Tor
Legitimate Server

因有別於其它 SPAM 方式，使得釣魚成功率提高


Attacker
Tor
Legitimate Server

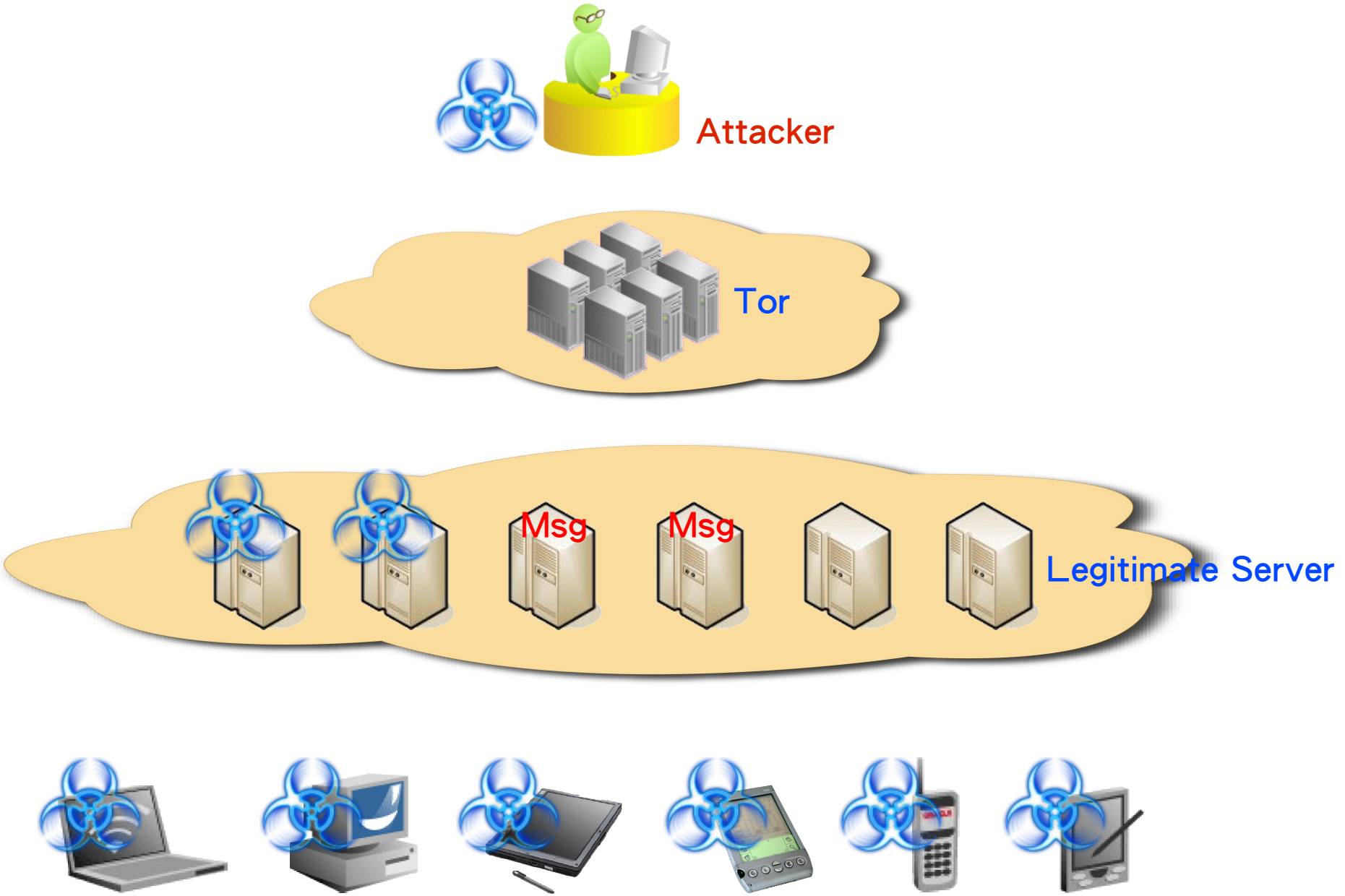

Attacker
Tor
Legitimate Server

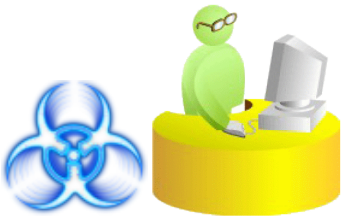

Attacker
Tor
在合法網站上的 C&C 分散佈置 (如 Blog,Twitter,Plurk)
Legitimate Server


Attacker
Tor
Msg
Msg
Legitimate Server

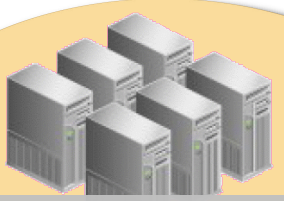

SEARCH BLOG
FLAG BLOG
FOLLOW BLOG
Next Blog»
yftzeng@gmail.com | New Post | Customize | Sign Out
混沌、複雜
Friday, April 3, 2009
TEST
D:ant.openfoundry.org
Posted by Ant at 12:18 AM
Labels
words (169)
security (53)
management (37)
feeling (30)


SEARCH BLOG
FLAG BLOG
FOLLOW BLOG
Next Blog»
yftzeng@gmail.com | New Post | Customize | Sign Out
混沌、複雜
對 ant.openfoundry.org 進行 DDoS 攻擊
TEST
D:ant.openfoundry.org
Posted by Ant at 12:18 AM
Labels
security (53)
management (37)
feeling (30)


Attacker
Tor
Msg
Msg
Legitimate Server



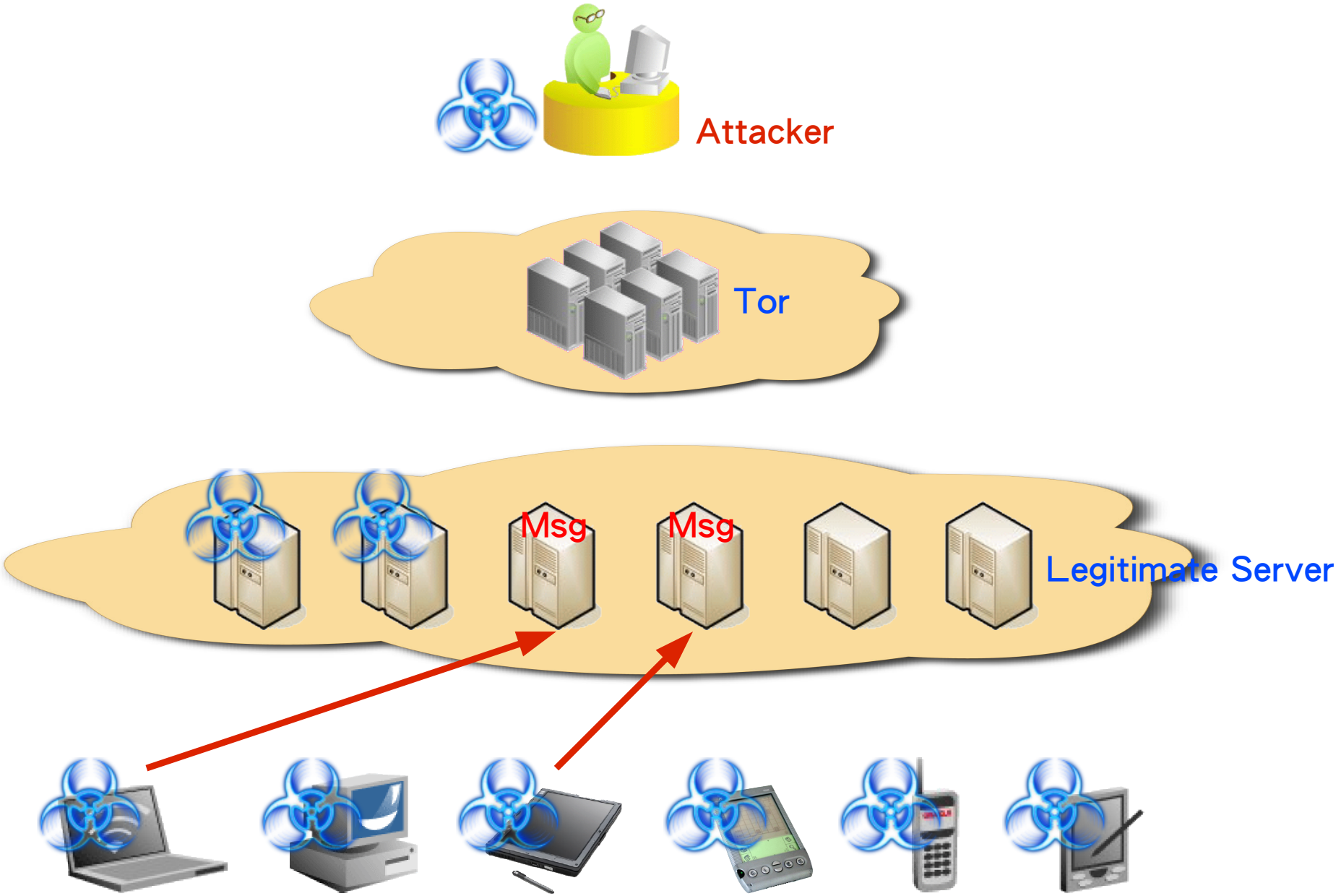
Attacker

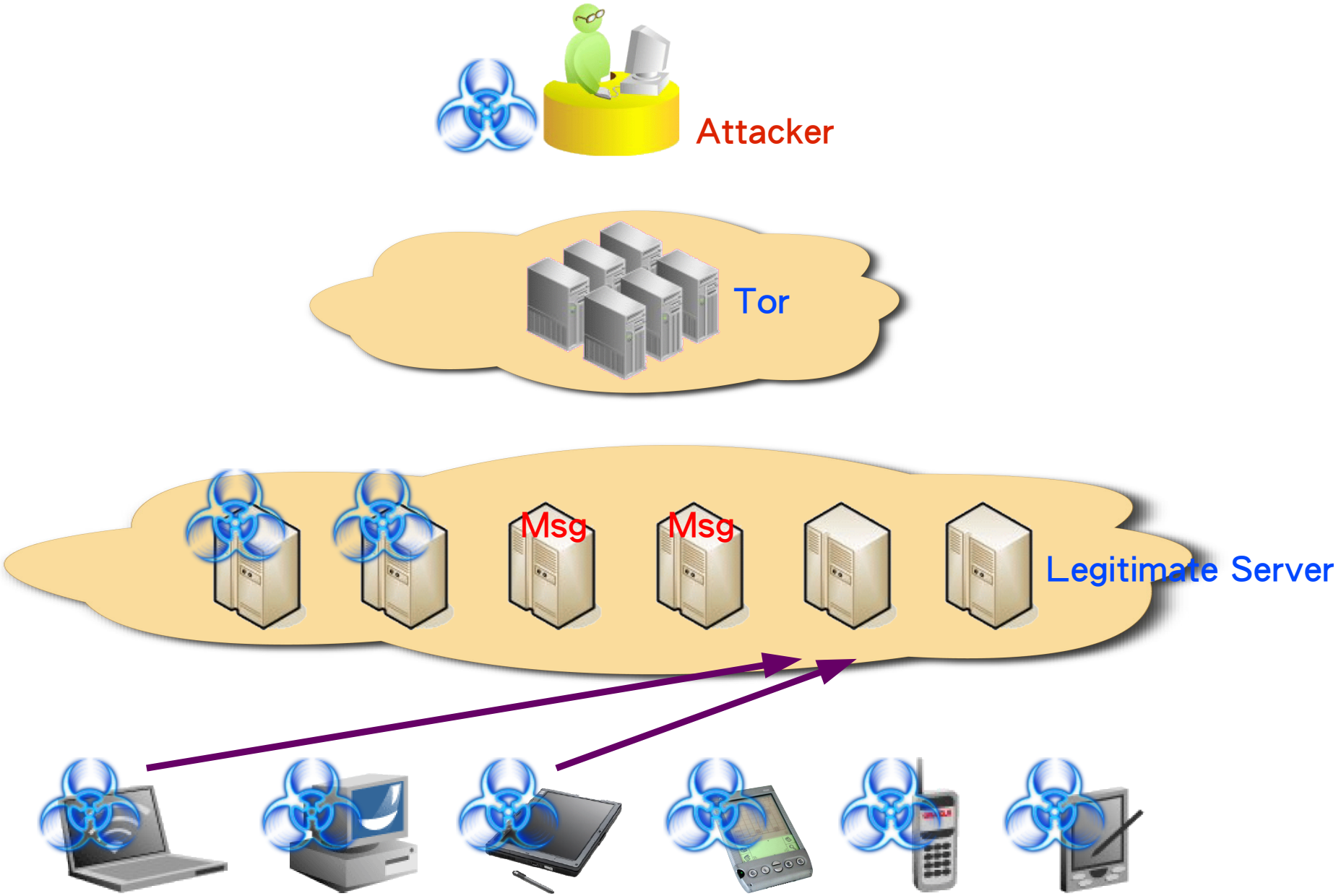


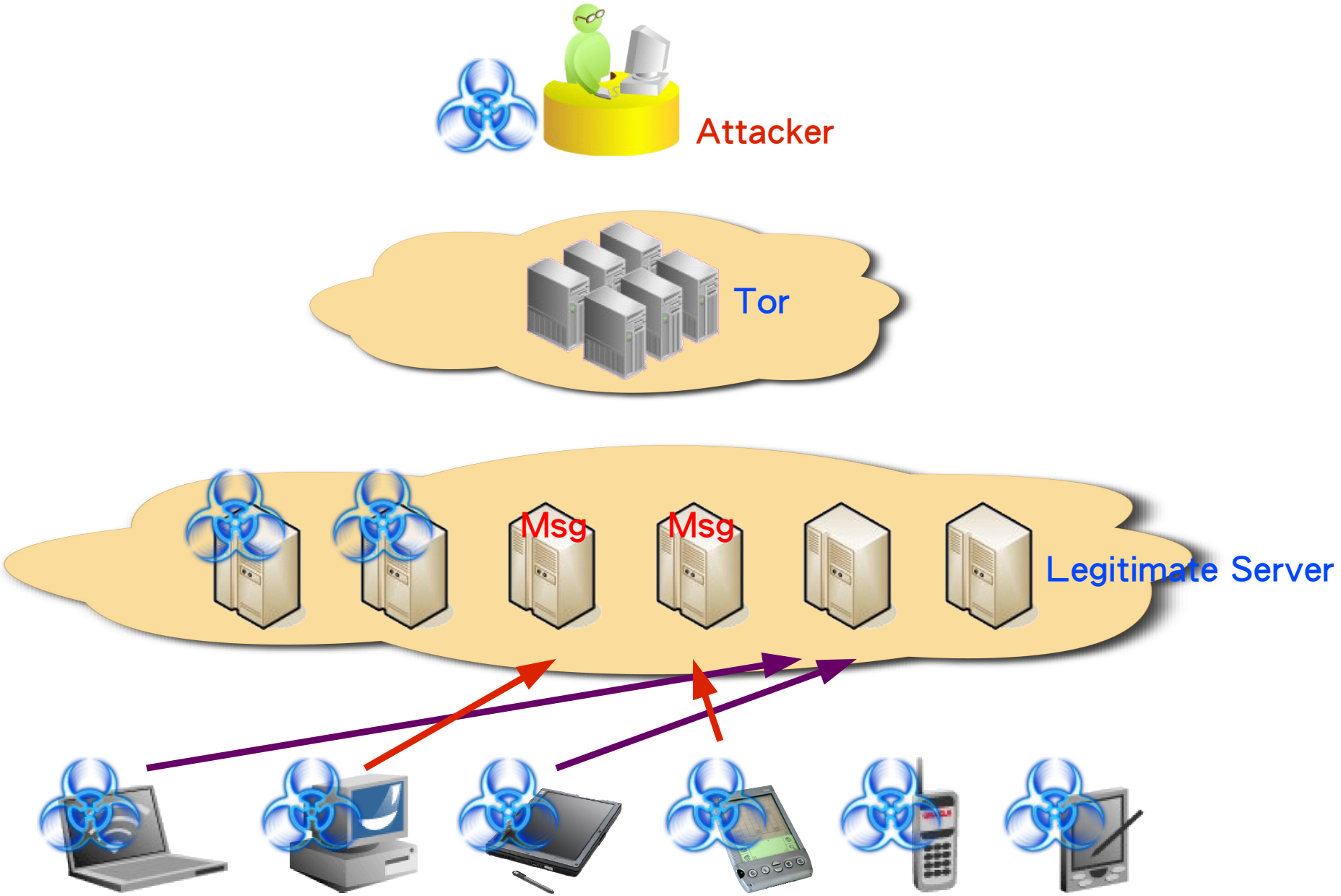
Tor

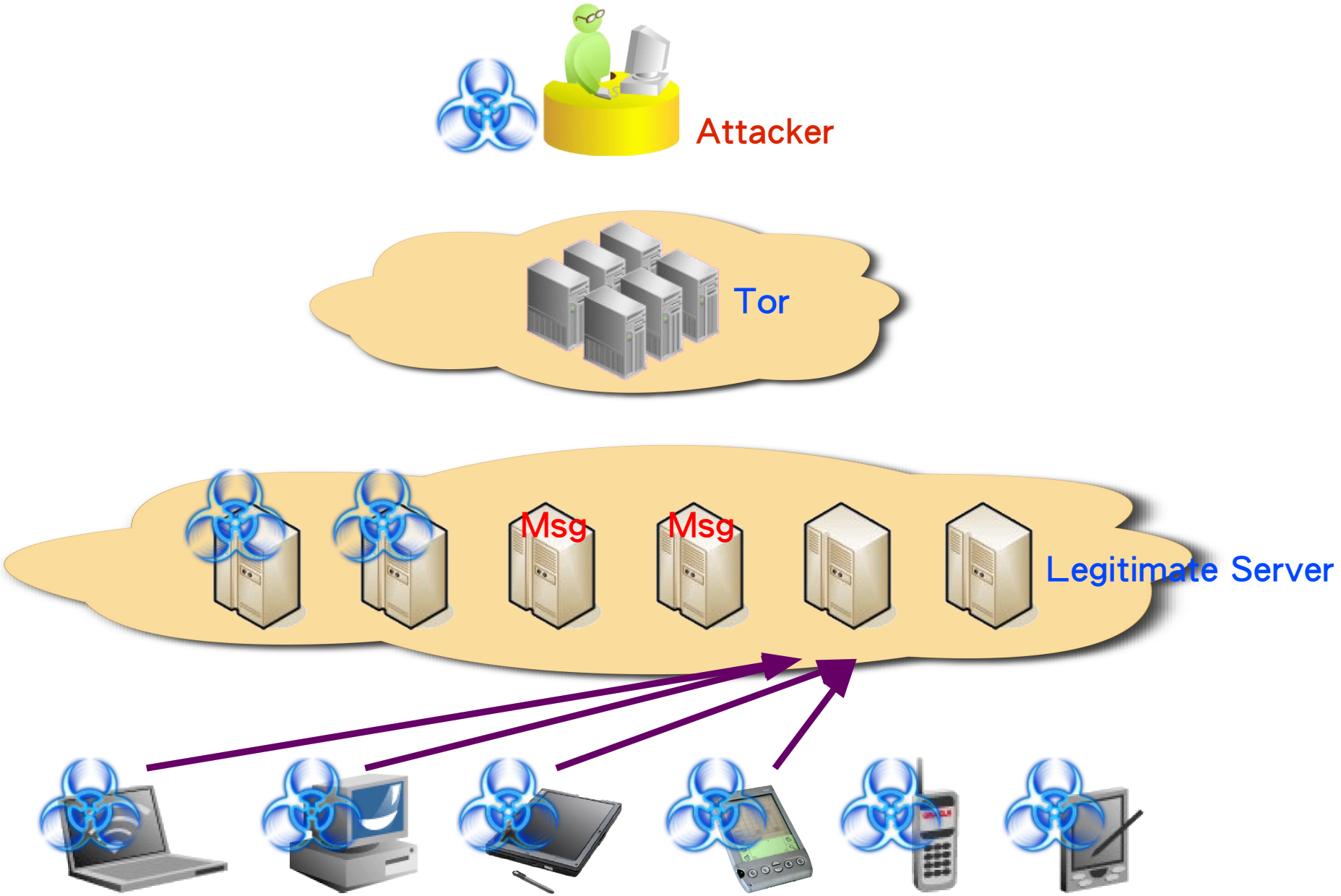
Bots 不定時向 C&C 收取訊息

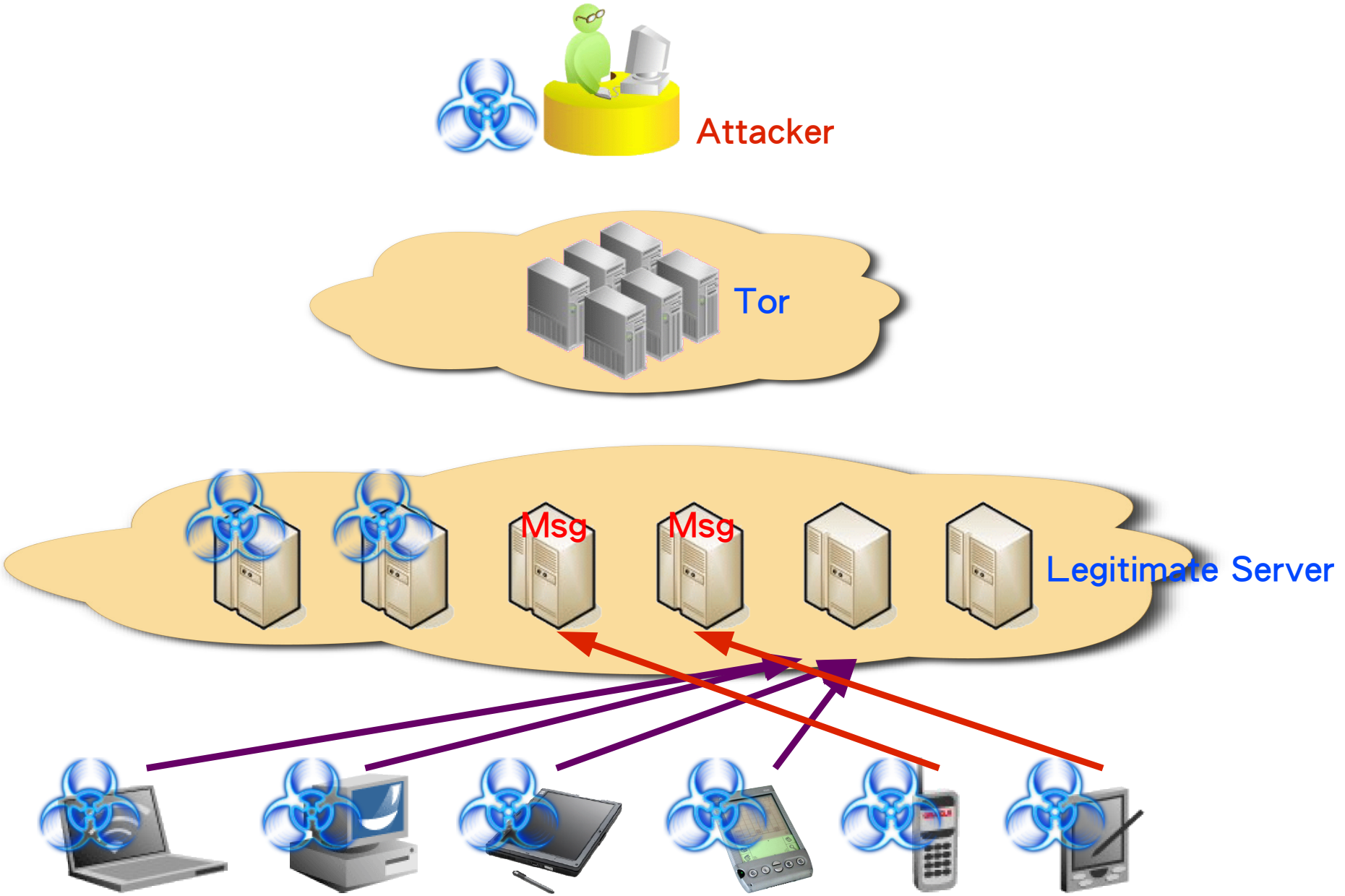
Legitimate Server

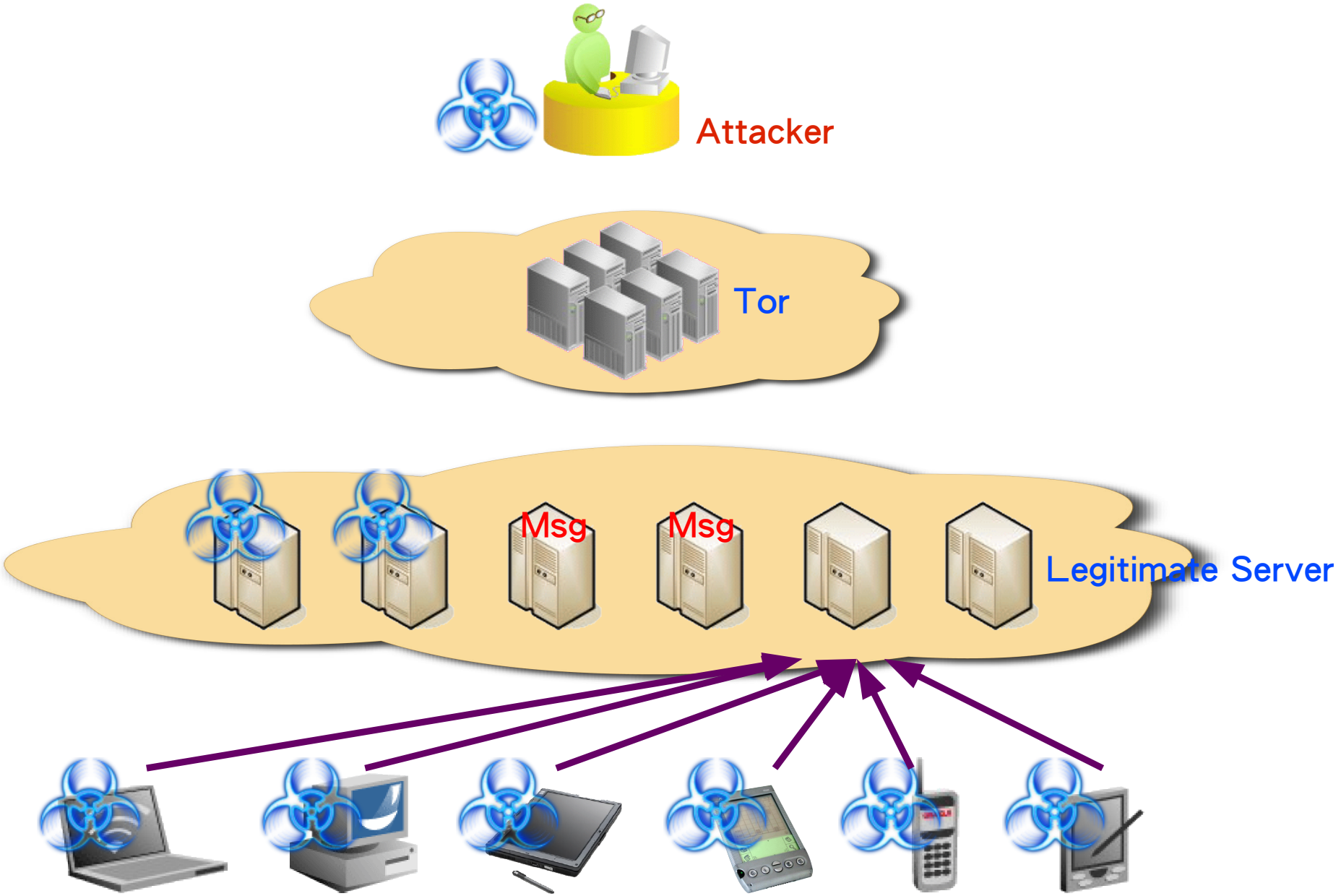

Attacker
Tor
Msg
Msg
Legitimate Server


Attacker
Tor
Msg
Msg
Legitimate Server

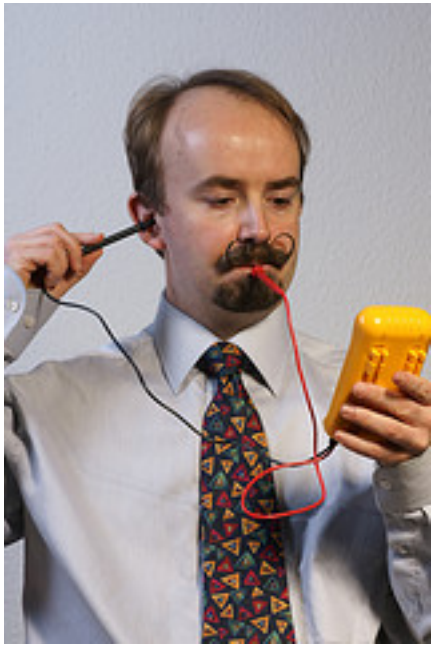

Attacker
Tor
Msg
Msg
Legitimate Server


Attacker
Tor
Msg
Msg
Legitimate Server


Attacker
Tor
Msg
Msg
Legitimate Server


Attacker
Tor
Msg
Msg
Legitimate Server

DEMO



Botnet Detection

Photo:
andreasnilsson1976@flickr.com
http://www.flickr.com/photos/andreasnilsson1976/2093950981/

Bypass Matrix

	Pass	Comments
AntiVirus	✅	Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection	✅	Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer	✅	Combine with Browser, No Process, No DLL
Network Monitor	✅	Same with normal network traffic
Honeypots	✅	Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis	✅	Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic	✅	Use legitimate DNS server, No DDNS
SPAM Signatures	✅	Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis	✅	No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis	✅	No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy	✅	No Open Proxy
VPN	✅	Normal allow HTTP/HTTPs
Content Filter	✅	Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

Bypass Matrix

	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

File **BotFox.xpi** received on **2009.07.16 05:29:57 (UTC)**
Current status: **finished**
Result: **0/41 (0.00%)**

Antivirus	Version	Last Update	Result
a-squared	4.5.0.24	2009.07.16	-
AhnLab-V3	5.0.0.2	2009.07.16	-
AntiVir	7.9.0.215	2009.07.16	-
Antiy-AVL	2.0.3.7	2009.07.16	-
Authentium	5.1.2.4	2009.07.16	-
Avast	4.8.1335.0	2009.07.16	-
AVG	8.5.0.387	2009.07.15	-
BitDefender	7.2	2009.07.16	-
CAT-QuickHeal	10.00	2009.07.16	-
ClamAV	0.94.1	2009.07.16	-
Comodo	1666	2009.07.16	-
DrWeb	5.0.0.12182	2009.07.16	-
eSafe	7.0.17.0	2009.07.15	-
eTrust-Vet	31.6.6617	2009.07.15	-
F-Prot	4.4.4.56	2009.07.16	-
F-Secure	8.0.14470.0	2009.07.16	-
Fortinet	3.120.0.0	2009.07.16	-
GData	19	2009.07.16	-
Ikarus	T3.1.1.64.0	2009.07.16	-
Jiangmin	11.0.706	2009.07.15	-
K7AntiVirus	7.10.793	2009.07.15	-
Kaspersky	7.0.0.125	2009.07.16	-
McAfee	5677	2009.07.15	-
McAfee+Artemis	5677	2009.07.15	-
McAfee-GW-Edition	6.8.5	2009.07.16	-
Microsoft	1.4803	2009.07.16	-
NOD32	4248	2009.07.16	-
Norman	6.01.09	2009.07.15	-
nProtect	2009.1.8.0	2009.07.16	-
Panda	10.0.0.14	2009.07.15	-
PCTools	4.4.2.0	2009.07.15	-
Prevx	3.0	2009.07.16	-
Rising	21.38.30.00	2009.07.16	-
Sophos	4.43.0	2009.07.16	-
Sunbelt	3.2.1858.2	2009.07.15	-
Symantec	1.4.4.12	2009.07.16	-
TheHacker	6.3.4.3.368	2009.07.15	-
TrendMicro	8.950.0.1094	2009.07.16	-
VBA32	3.12.10.8	2009.07.15	-
ViRobot	2009.7.16.1838	2009.07.16	-
VirusBuster	4.6.5.0	2009.07.15	-

AntiVirus

1. JavaScript 的特性，使得在判斷上有許多困難。
2. 無任何 API Hooks 。
3. 無任何 Registry 。
4. 無任何 DLL 。

T 牌、K 牌、S 牌、A 牌、N 牌 ... 等，
全數通過 VirusTotal 的廠商。

Bypass Matrix

	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

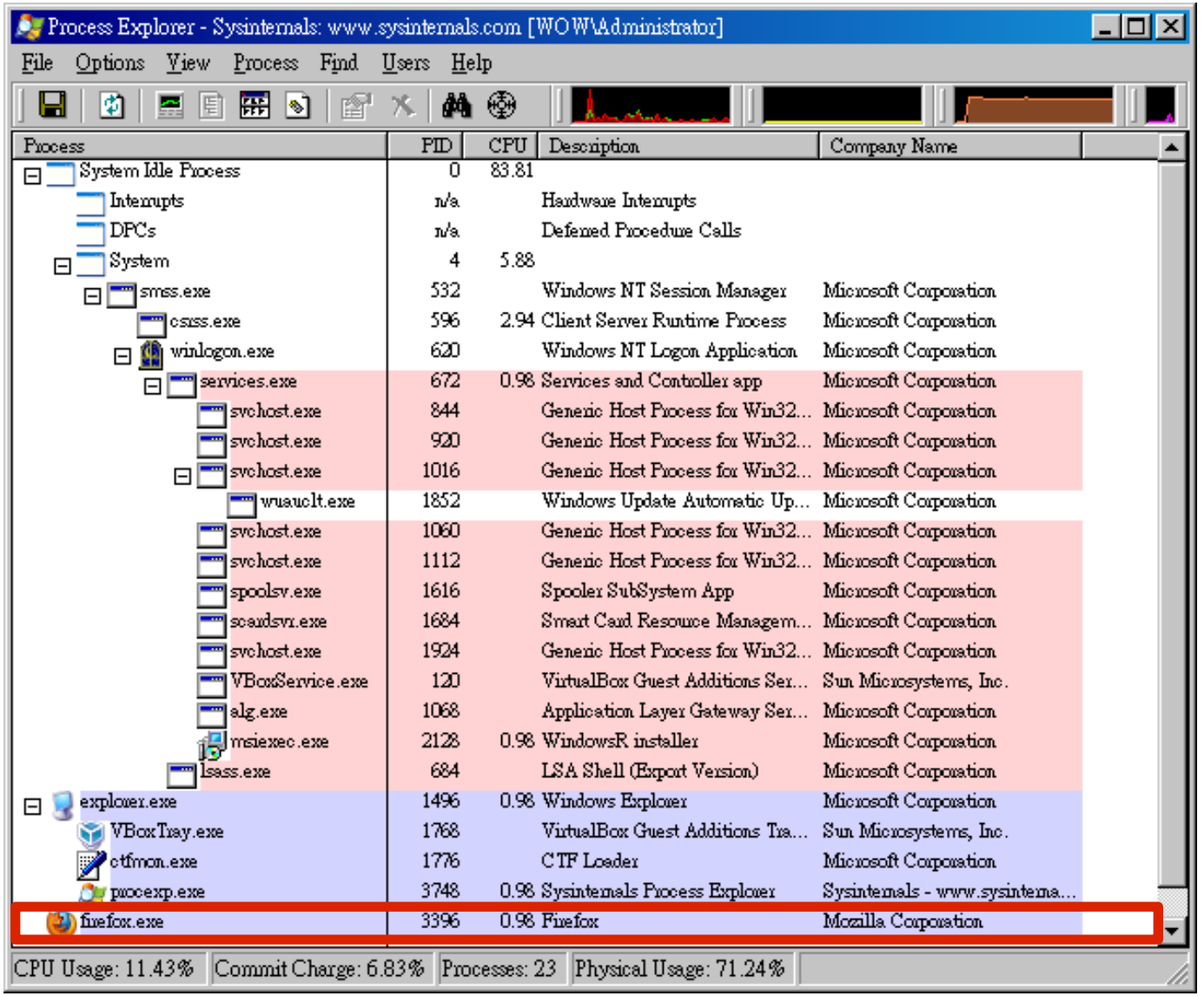
Rootkit Detection

1. JavaScript 的特性，使得在判斷上有許多困難。
2. 無任何 API Hooks 。
3. 無任何 Registry 。
4. 無任何 DLL 。

RootkitRevealer 、 RkHunter 、 GMER 、 Panda Anti-Rootkit 、 Sophos Anti-Rootkit 、 Rootkit Hook Analyzer 、 IceSword 、 Avira Rootkit Detection 、 Rootkit UnHooker 、 AVG Anti-Rootkit 、 McAfee Rootkit Detective 、 DarkSpy 、 F-Secure BlackLight 。

Bypass Matrix

	Pass	Comments
AntiVirus	✅	Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection	✅	Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer	✅	Combine with Browser, No Process, No DLL
Network Monitor	✅	Same with normal network traffic
Honeypots	✅	Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis	✅	Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic	✅	Use legitimate DNS server, No DDNS
SPAM Signatures	✅	Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis	✅	No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis	✅	No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy	✅	No Open Proxy
VPN	✅	Normal allow HTTP/HTTPs
Content Filter	✅	Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords


Process Explorer - Sysinternals: www.sysinternals.com [WOW\Administrator]
File Options View Process Find Users Help
Process PID CPU Description Company Name
System Idle Process 0 83.81
Interrupts n/a Hardware Interrupts
DPCs n/a Deferred Procedure Calls
System 4 5.88
smss.exe 532 Windows NT Session Manager Microsoft Corporation
csrss.exe 596 2.94 Client Server Runtime Process Microsoft Corporation
winlogon.exe 620 Windows NT Logon Application Microsoft Corporation
services.exe 672 0.98 Services and Controller app Microsoft Corporation
svchost.exe 844 Generic Host Process for Win32... Microsoft Corporation
svchost.exe 920 Generic Host Process for Win32... Microsoft Corporation
svchost.exe 1016 Generic Host Process for Win32... Microsoft Corporation
wuauclt.exe 1852 Windows Update Automatic Up... Microsoft Corporation
svchost.exe 1060 Generic Host Process for Win32... Microsoft Corporation
svchost.exe 1112 Generic Host Process for Win32... Microsoft Corporation
spoolsv.exe 1616 Spooler SubSystem App Microsoft Corporation
scardsvr.exe 1684 Smart Card Resource Managem... Microsoft Corporation
svchost.exe 1924 Generic Host Process for Win32... Microsoft Corporation
VBoxService.exe 120 VirtualBox Guest Additions Ser... Sun Microsystems, Inc.
alg.exe 1068 Application Layer Gateway Ser... Microsoft Corporation
msiexec.exe 2128 0.98 Windows® installer Microsoft Corporation
lsass.exe 684 LSA Shell (Export Version) Microsoft Corporation
explorer.exe 1496 0.98 Windows Explorer Microsoft Corporation
VBoxTray.exe 1768 VirtualBox Guest Additions Tra... Sun Microsystems, Inc.
ctfmon.exe 1776 CTF Loader Microsoft Corporation
procexp.exe 3748 0.98 Sysinternals Process Explorer Sysinternals - www.sysinterna...
firefox.exe 3396 0.98 Firefox Mozilla Corporation
CPU Usage: 11.43% Commit Charge: 6.83% Processes: 23 Physical Usage: 71.24%

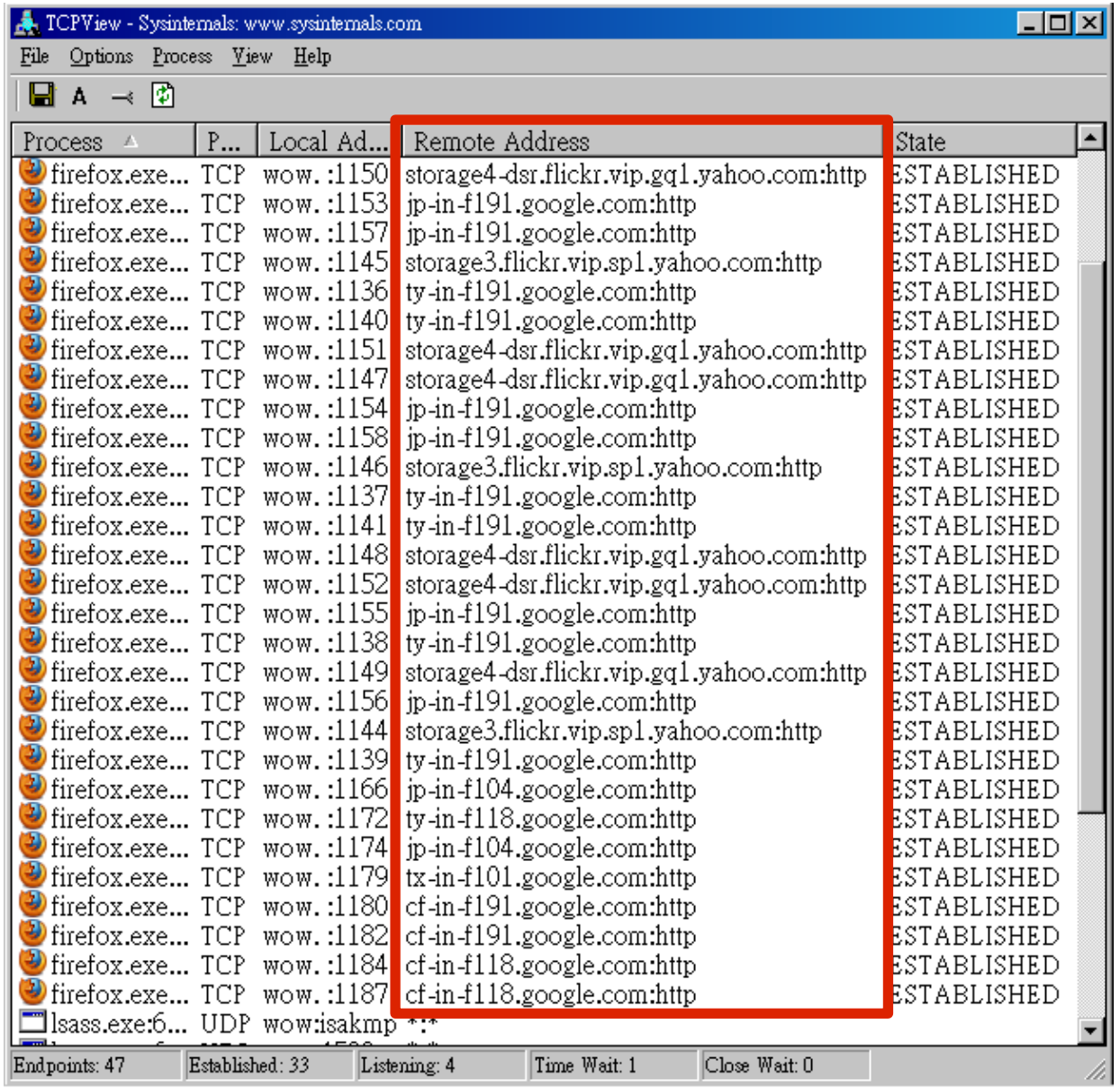
Process Explorer

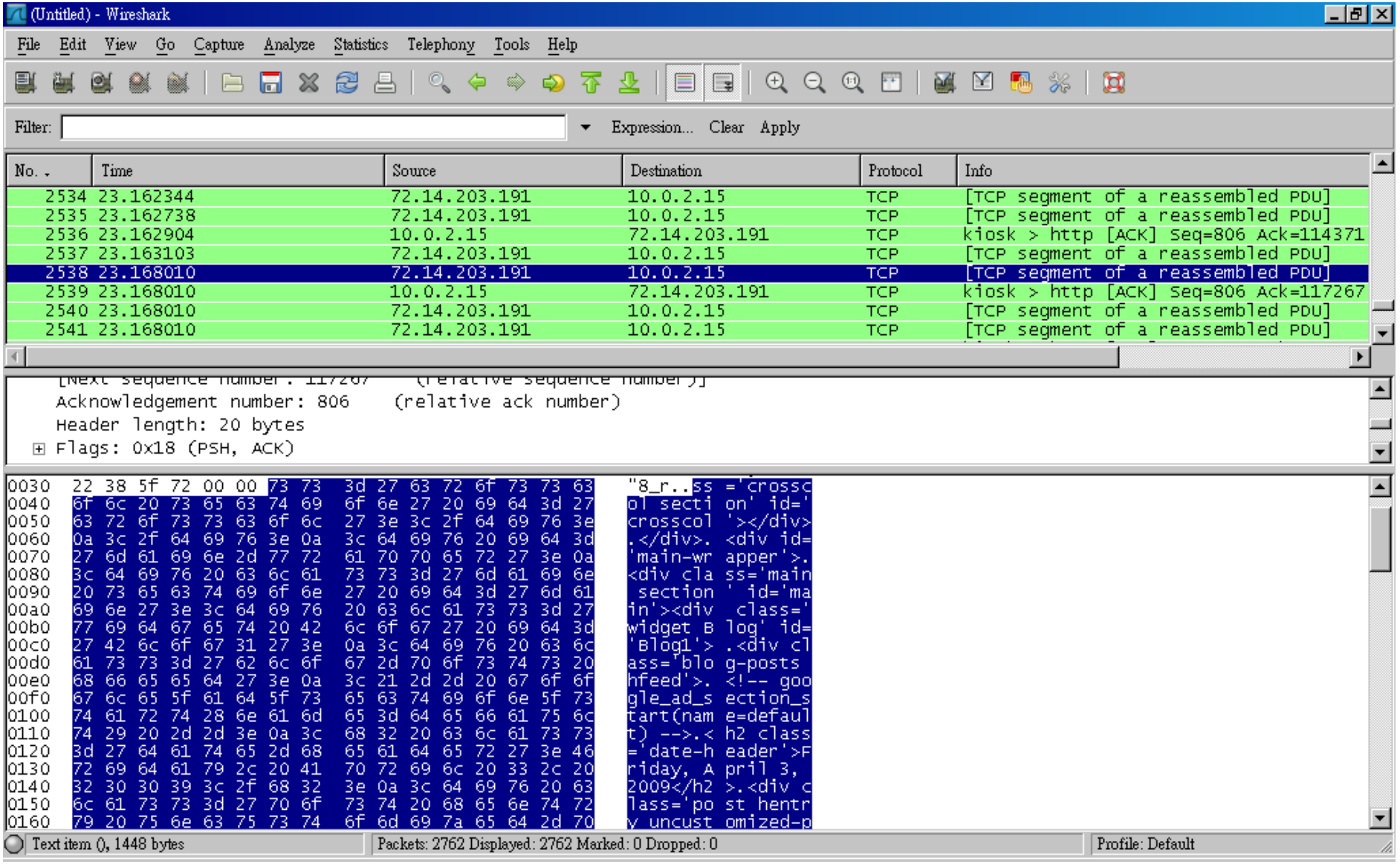
1. 基於瀏覽器。
2. 不需額外的 Process 。
3. 無任何 DLL 。

Process Explorer 、 Process Monitor 、 Combofix 、 Hijackthis 、 SREng 、 EFIX 、 Runscanner 、 Autoruns 。

Bypass Matrix

	Pass	Comments
AntiVirus	✓	Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection	✓	Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer	✓	Combine with Browser, No Process, No DLL
Network Monitor	✓	Same with normal network traffic
Honeypots	✓	Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis	✓	Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic	✓	Use legitimate DNS server, No DDNS
SPAM Signatures	✓	Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis	✓	No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis	✓	No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy	✓	No Open Proxy
VPN	✓	Normal allow HTTP/HTTPs
Content Filter	✓	Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process P... Local Ad... Remote Address State
firefox.exe... TCP wow. :1150 storage4-dsr.flickr.vip.gq1.yahoo.com:http ESTABLISHED
firefox.exe... TCP wow. :1153 jp-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1157 jp-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1145 storage3.flickr.vip.sp1.yahoo.com:http ESTABLISHED
firefox.exe... TCP wow. :1136 ty-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1140 ty-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1151 storage4-dsr.flickr.vip.gq1.yahoo.com:http ESTABLISHED
firefox.exe... TCP wow. :1147 storage4-dsr.flickr.vip.gq1.yahoo.com:http ESTABLISHED
firefox.exe... TCP wow. :1154 jp-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1158 jp-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1146 storage3.flickr.vip.sp1.yahoo.com:http ESTABLISHED
firefox.exe... TCP wow. :1137 ty-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1141 ty-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1148 storage4-dsr.flickr.vip.gq1.yahoo.com:http ESTABLISHED
firefox.exe... TCP wow. :1152 storage4-dsr.flickr.vip.gq1.yahoo.com:http ESTABLISHED
firefox.exe... TCP wow. :1155 jp-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1138 ty-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1149 storage4-dsr.flickr.vip.gq1.yahoo.com:http ESTABLISHED
firefox.exe... TCP wow. :1156 jp-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1144 storage3.flickr.vip.sp1.yahoo.com:http ESTABLISHED
firefox.exe... TCP wow. :1139 ty-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1166 jp-in-f104.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1172 ty-in-f118.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1174 jp-in-f104.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1179 tx-in-f101.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1180 cf-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1182 cf-in-f191.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1184 cf-in-f118.google.com:http ESTABLISHED
firefox.exe... TCP wow. :1187 cf-in-f118.google.com:http ESTABLISHED
lsass.exe:6... UDP wow:isakmp *:*
Endpoints: 47 Established: 33 Listening: 4 Time Wait: 1 Close Wait: 0


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
2534 23.162344 72.14.203.191 10.0.2.15 TCP [TCP segment of a reassembled PDU]
2535 23.162738 72.14.203.191 10.0.2.15 TCP [TCP segment of a reassembled PDU]
2536 23.162904 10.0.2.15 72.14.203.191 TCP kiosk > http [ACK] Seq=806 Ack=114371
2537 23.163103 72.14.203.191 10.0.2.15 TCP [TCP segment of a reassembled PDU]
2538 23.168010 72.14.203.191 10.0.2.15 TCP [TCP segment of a reassembled PDU]
2539 23.168010 10.0.2.15 72.14.203.191 TCP kiosk > http [ACK] Seq=806 Ack=117267
2540 23.168010 72.14.203.191 10.0.2.15 TCP [TCP segment of a reassembled PDU]
2541 23.168010 72.14.203.191 10.0.2.15 TCP [TCP segment of a reassembled PDU]
Acknowledgement number: 806 (relative ack number)
Header length: 20 bytes
Flags: 0x18 (PSH, ACK)
0030 22 38 5f 72 00 00 73 73 3d 27 63 72 6f 73 73 63 "8_r..ss ='crossc
0040 6f 6c 20 73 65 63 74 69 6f 6e 27 20 69 64 3d 27 ol secti on' id='
0050 63 72 6f 73 73 63 6f 6c 27 3e 3c 2f 64 69 76 3e crosscol '>
0060 0a 3c 2f 64 69 76 3e 0a 3c 64 69 76 20 69 64 3d . . <div id=
0070 27 6d 61 69 6e 2d 77 72 61 70 70 65 72 27 3e 0a 'main-wr apper'>.
0080 3c 64 69 76 20 63 6c 61 73 73 3d 27 6d 61 69 6e <div cla ss='main
0090 20 73 65 63 74 69 6f 6e 27 20 69 64 3d 27 6d 61 section ' id='ma
00a0 69 6e 27 3e 3c 64 69 76 20 63 6c 61 73 73 3d 27 in'><div class='
00b0 77 69 64 67 65 74 20 42 6c 6f 67 27 20 69 64 3d widget B log' id=
00c0 27 42 6c 6f 67 31 27 3e 0a 3c 64 69 76 20 63 6c 'Blog1'> .<div cl
00d0 61 73 73 3d 27 62 6c 6f 67 2d 70 6f 73 74 73 20 ass='blo g-posts
00e0 68 66 65 65 64 27 3e 0a 3c 21 2d 2d 20 67 6f 6f hfeed'>. <!-- goo
00f0 67 6c 65 5f 61 64 5f 73 65 63 74 69 6f 6e 5f 73 gle_ad_s ection_s
0100 74 61 72 74 28 6e 61 6d 65 3d 64 65 66 61 75 6c tart(nam e=defaul
0110 74 29 20 2d 2d 3e 0a 3c 68 32 20 63 6c 61 73 73 t) -->.< h2 class
0120 3d 27 64 61 74 65 2d 68 65 61 64 65 72 27 3e 46 ='date-h eader'>F
0130 72 69 64 61 79 2c 20 41 70 72 69 6c 20 33 2c 20 riday, A pril 3,
0140 32 30 30 39 3c 2f 68 32 3e 0a 3c 64 69 76 20 63 2009</h2 >.<div c
0150 6c 61 73 73 3d 27 70 6f 73 74 20 68 65 6e 74 72 lass='po st hentr
0160 79 20 75 6e 63 75 73 74 6f 6d 69 7a 65 64 2d 70 y uncust omized-p
Text item (), 1448 bytes
Packets: 2762 Displayed: 2762 Marked: 0 Dropped: 0
Profile: Default

Network Monitor

1. 基於瀏覽器，不需開啟 Port 。
2. 使用 HTTP/HTTPs 。
3. 使用正常 DNS 。
4. 封包 / 字串無任何惡意內容。

TCPView 、 WireShark 、 Nmap 。

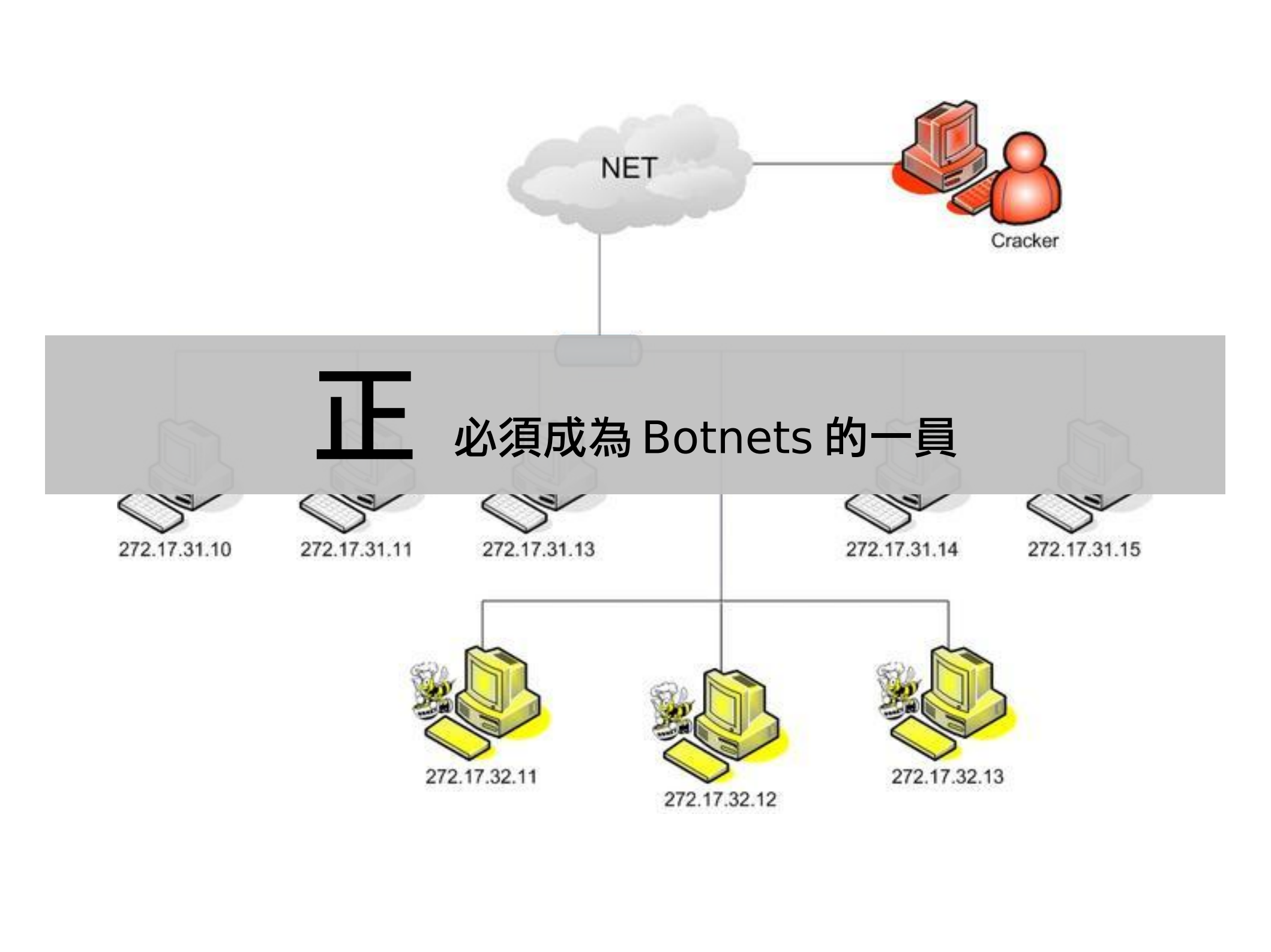
Bypass Matrix

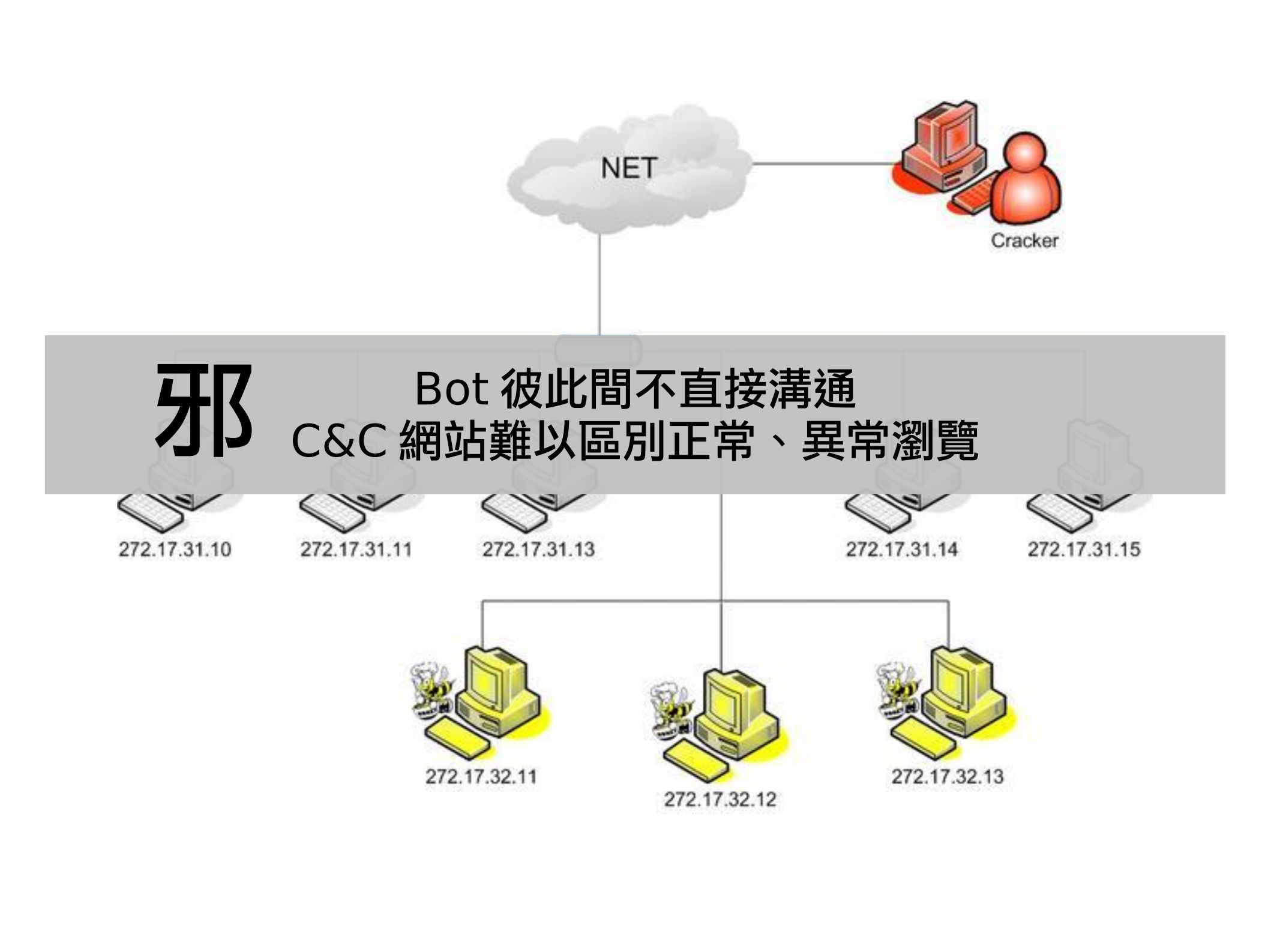
	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

Honeypots

1. 被動式 Honeypot → 使用社交工程手法。
2. 主動式 Honeypot → Bots 間不溝通，避免被名單搜集。
3. C&C 使用正常網站，難以區別正常、異常瀏覽。
4. 封包 / 字串無任何惡意內容。

Capture-HPC 、 Tinyhoneypot 、 Capture BAT 、 Google Hack Honeypot 、 Honeyd 、 Honeytrap 、 Honeywall 、 Honeyclient 。

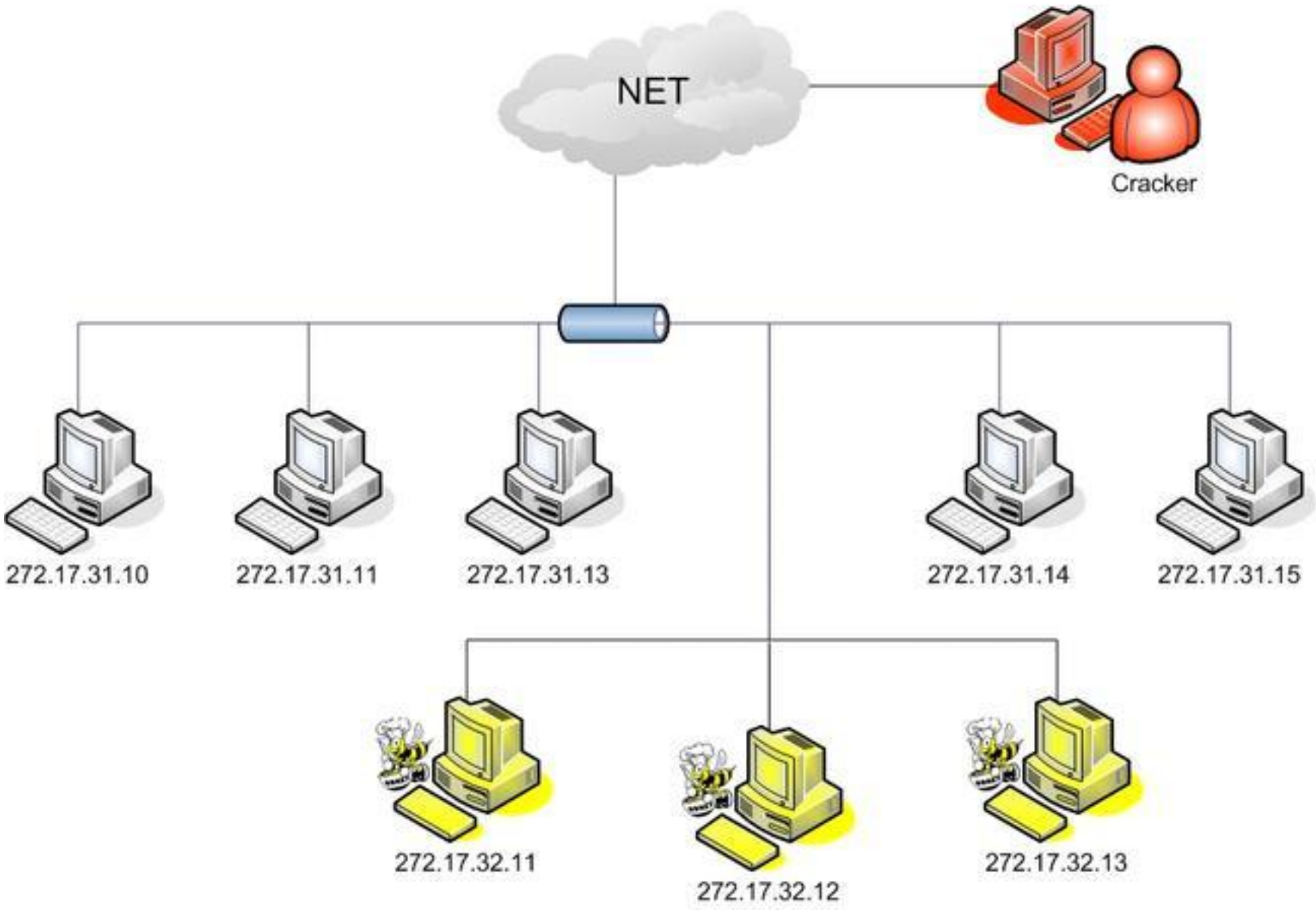

NET
Cracker
正 必須成為 Botnets 的一員
272.17.31.10
272.17.31.11
272.17.31.13
272.17.31.14
272.17.31.15
272.17.32.11
272.17.32.12
272.17.32.13



邪

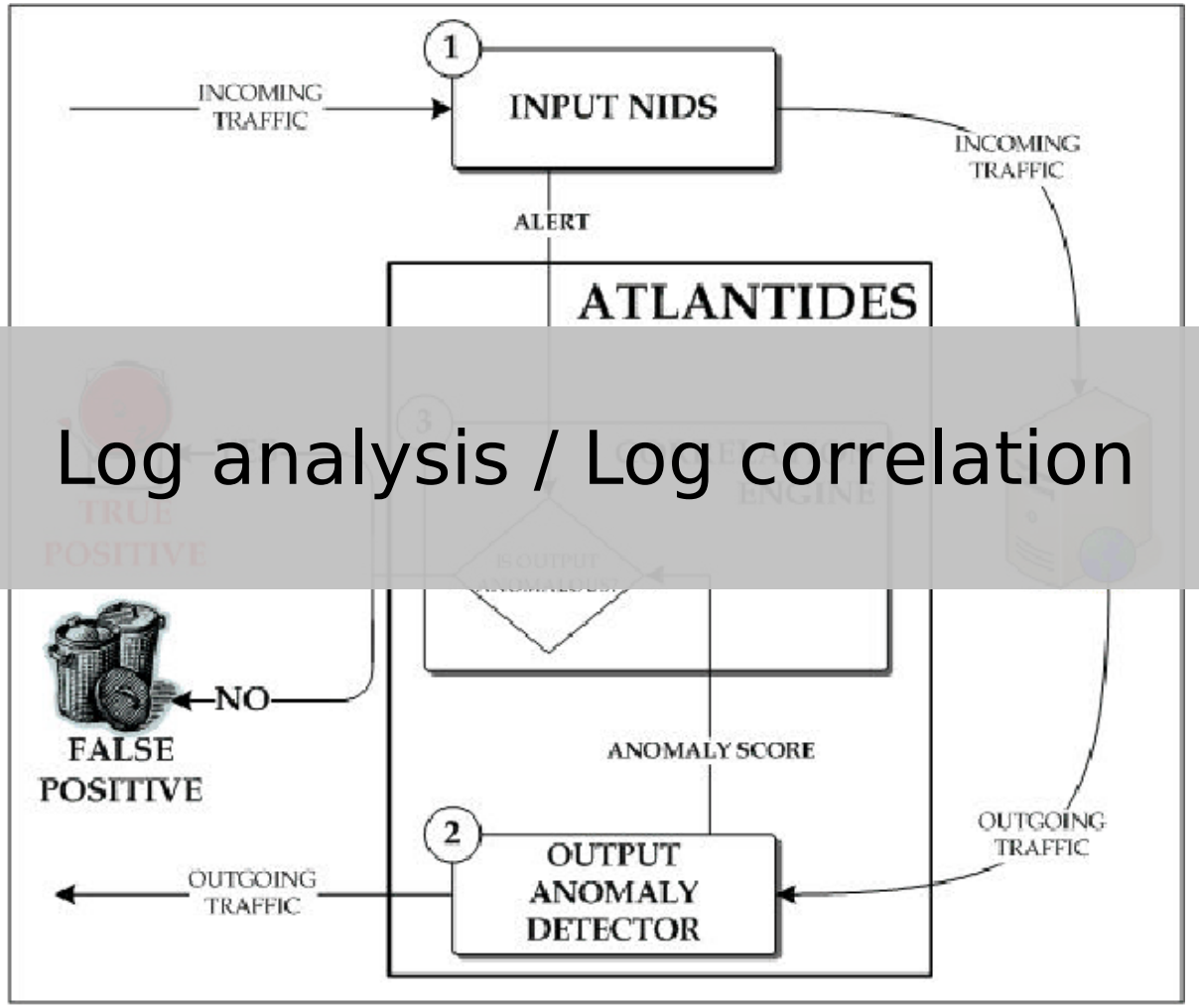
Bot 彼此間不直接溝通

C&C 網站難以區別正常、異常瀏覽

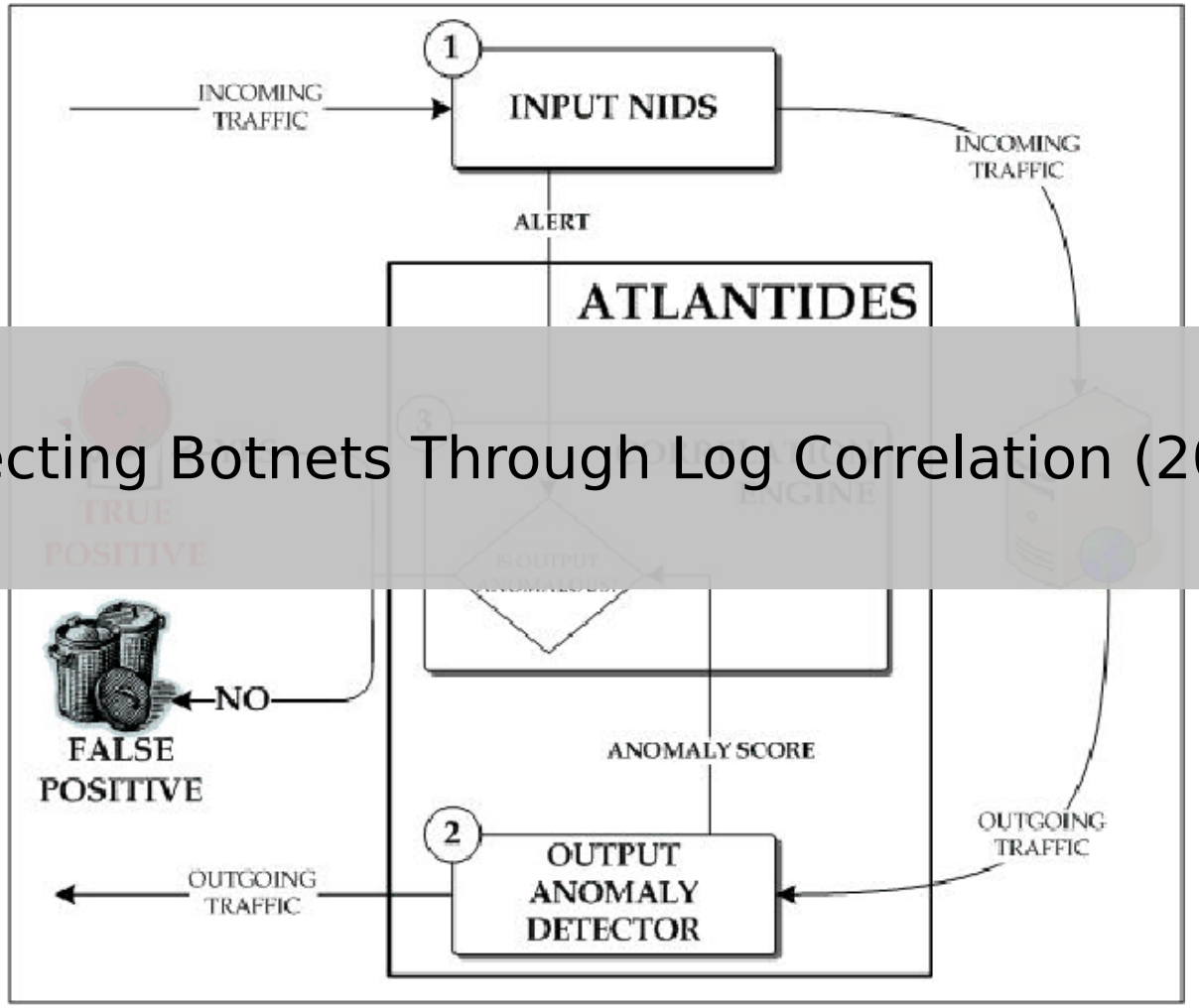

NET
Cracker
272.17.31.10
272.17.31.11
272.17.31.13
272.17.31.14
272.17.31.15
272.17.32.11
272.17.32.12
272.17.32.13

Bypass Matrix

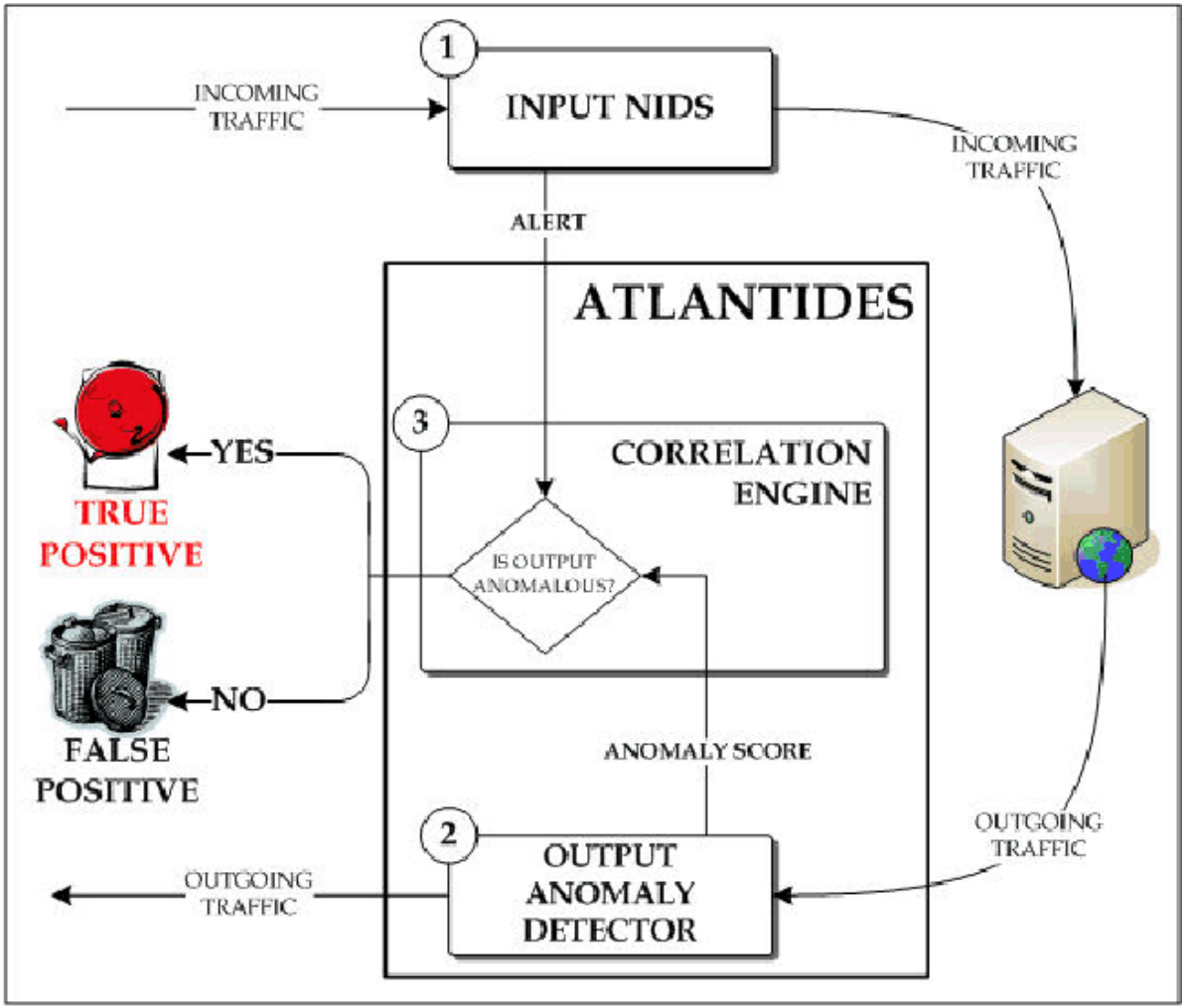
	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords



Log analysis / Log correlation



Detecting Botnets Through Log Correlation (2006)


1
INPUT NIDS
INCOMING TRAFFIC
INCOMING TRAFFIC
ALERT
ATLANTIDES
3
CORRELATION ENGINE
IS OUTPUT ANOMALOUS?
YES
TRUE POSITIVE
NO
FALSE POSITIVE
ANOMALY SCORE
2
OUTPUT ANOMALY DETECTOR
OUTGOING TRAFFIC
OUTGOING TRAFFIC

基於瀏覽器

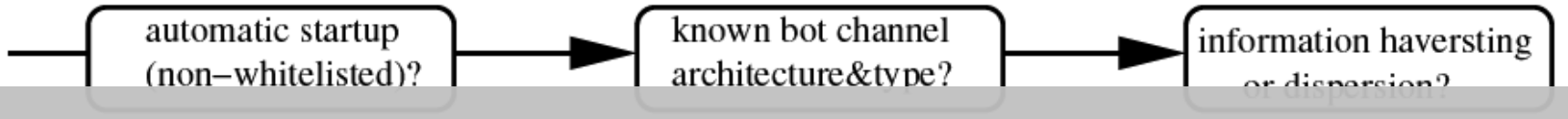
BotFox

4. 白名單的常客
5. 完全使用正常的 DNS 查詢

基於瀏覽器

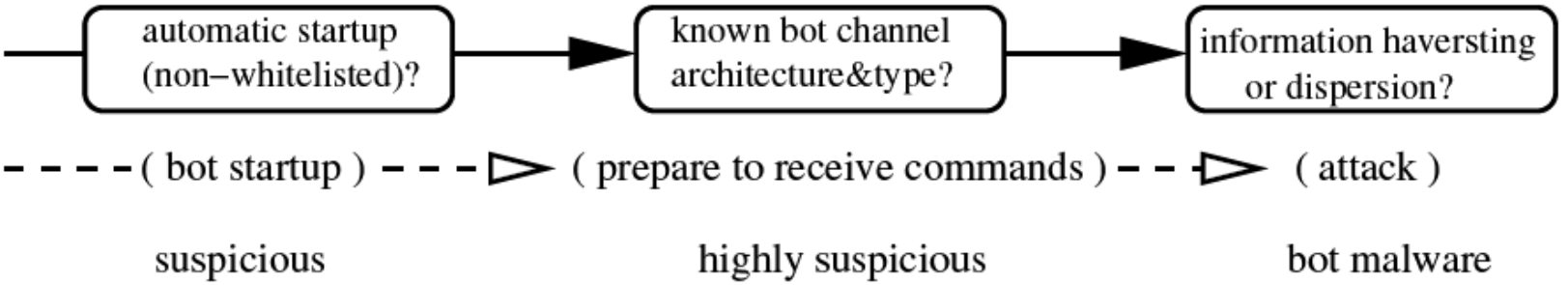
1. 非常容易模擬正常行為（基於 Port 80, 443 的實現）
2. 跨平台特性（手持式裝置、手機等）
3. 最常使用的應用程式之一
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

BotTracer



BotTracer: Execution-based Bot-like Malware Detection (2008)

BotTracer


automatic startup
(non−whitelisted)?
known bot channel
architecture&type?
information haversting
or dispersion?
(bot startup)
(prepare to receive commands)
(attack)
suspicious
highly suspicious
bot malware

基於瀏覽器

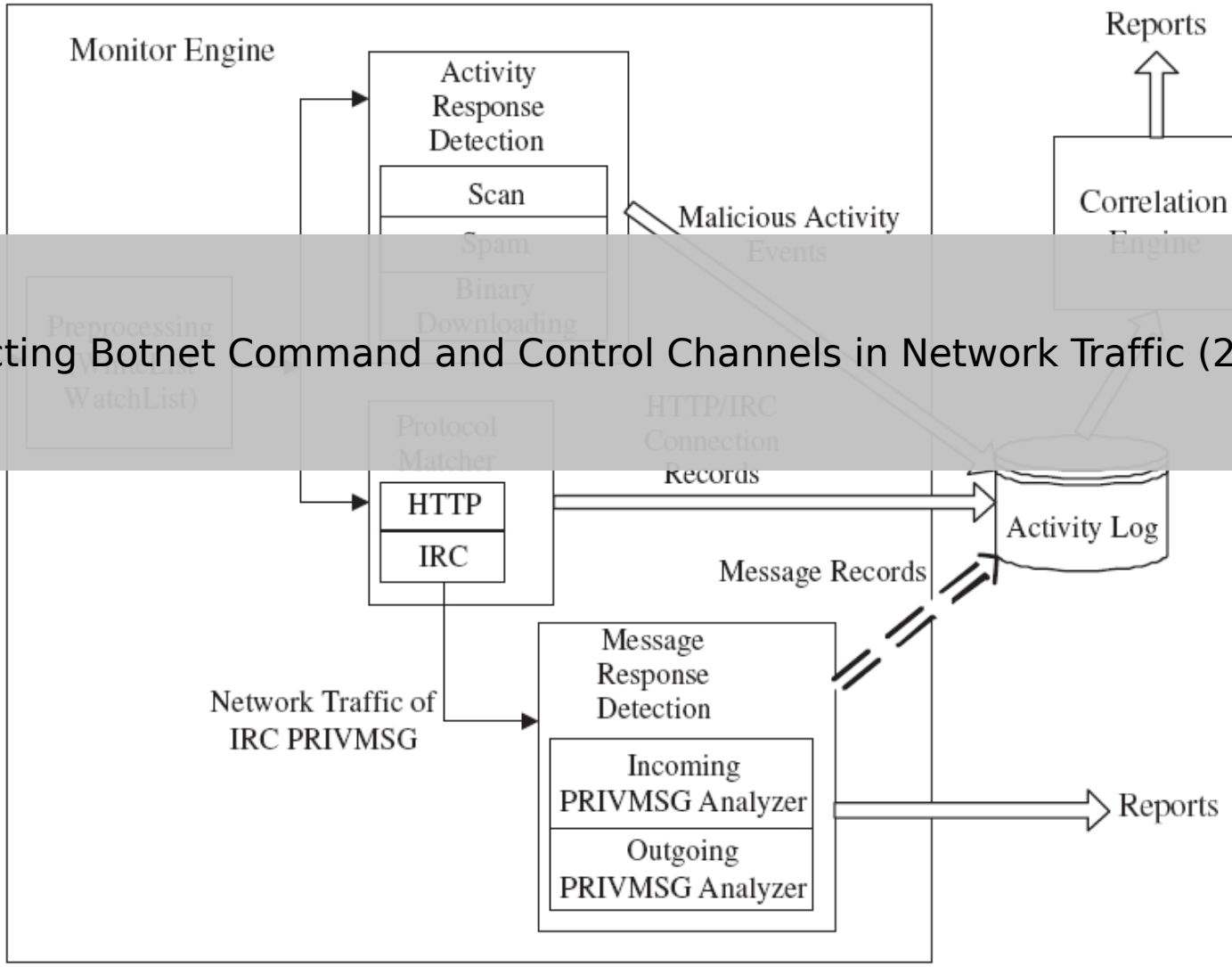
1. 非常容易模擬正常行為（基於Port 80, 443 的實現）
2. 跨平台特性（手持設備更是趨勢）
3. 最常使用的應用程式是
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

BotFox

基於瀏覽器

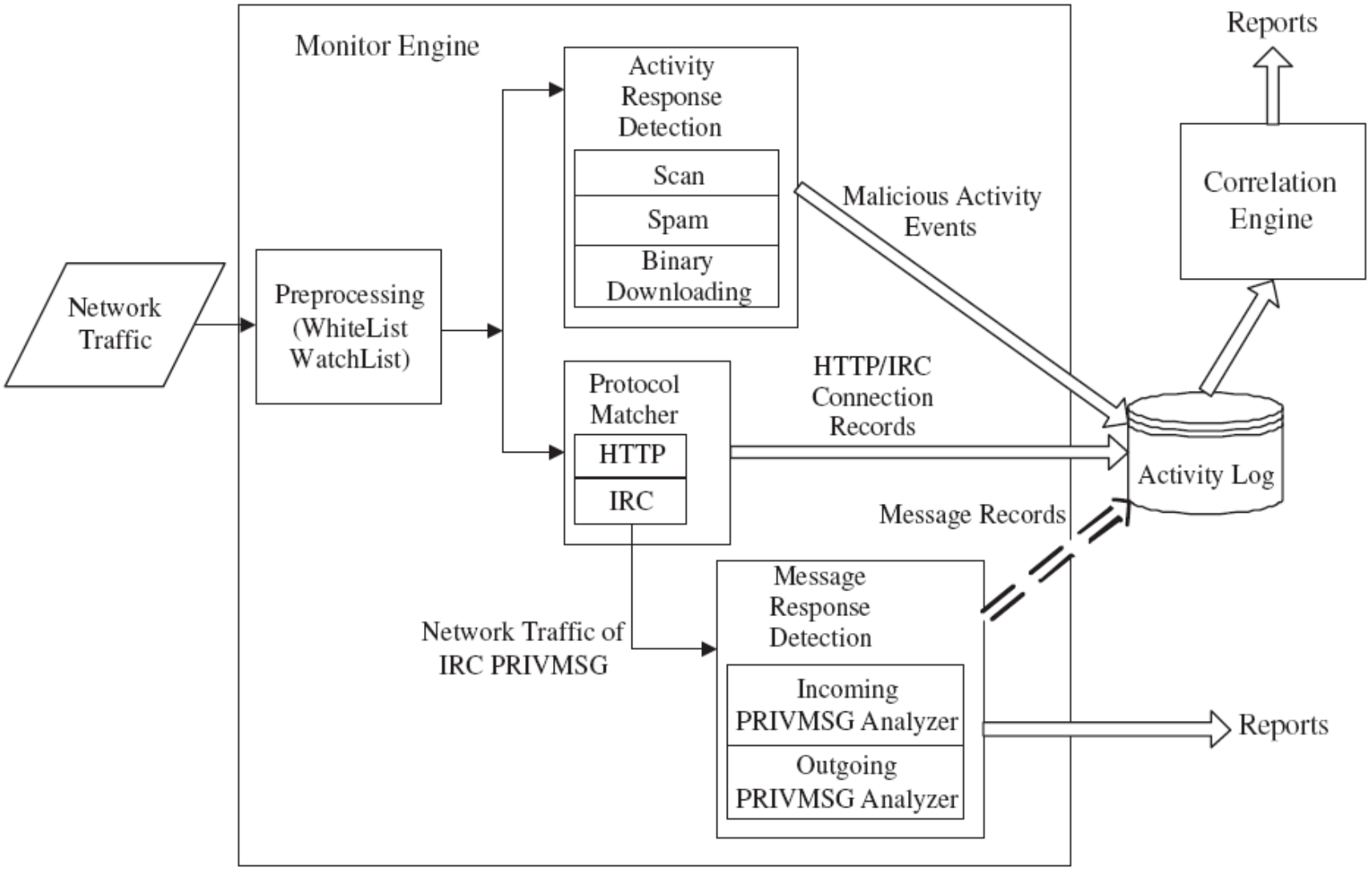
1. 非常容易模擬正常行為（基於 Port 80, 443 的實現）
2. 跨平台特性（手持式裝置、手機等）
3. 最常使用的應用程式之一
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

BotSniffer



BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic (2008)

BotSniffer


Monitor Engine
Activity
Response
Detection
Scan
Spam
Binary
Downloading
Malicious Activity
Events
Reports
Correlation
Engine
Network
Traffic
Preprocessing
(WhiteList
WatchList)
Protocol
Matcher
HTTP
IRC
HTTP/IRC
Connection
Records
Activity Log
Message Records
Message
Response
Detection
Network Traffic of
IRC PRIVMSG
Incoming
PRIVMSG Analyzer
Outgoing
PRIVMSG Analyzer
Reports

基於瀏覽器

1. 非常容易模擬正常行為（基於Port 80, 443 的實現）
2. 跨平台特性（手持設備、嵌入式系統）
3. 最常使用的應用程式是 [illegible]
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

BotFox

基於瀏覽器

1. 非常容易模擬正常行為（基於 Port 80, 443 的實現）
2. 跨平台特性（手持式裝置、手機等）
3. 最常使用的應用程式之一
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

Behavior/Log Analysis

1. 基於瀏覽器，非常容易模擬正常行為。
2. 瀏覽器常為白名單的一員。
3. 使用 HTTP/HTTPs ，封包 / 字串無任何惡意內容。
4. 使用正常 DNS 。

BotSniffer 、 BotTracer 、 Log Analyzer 。

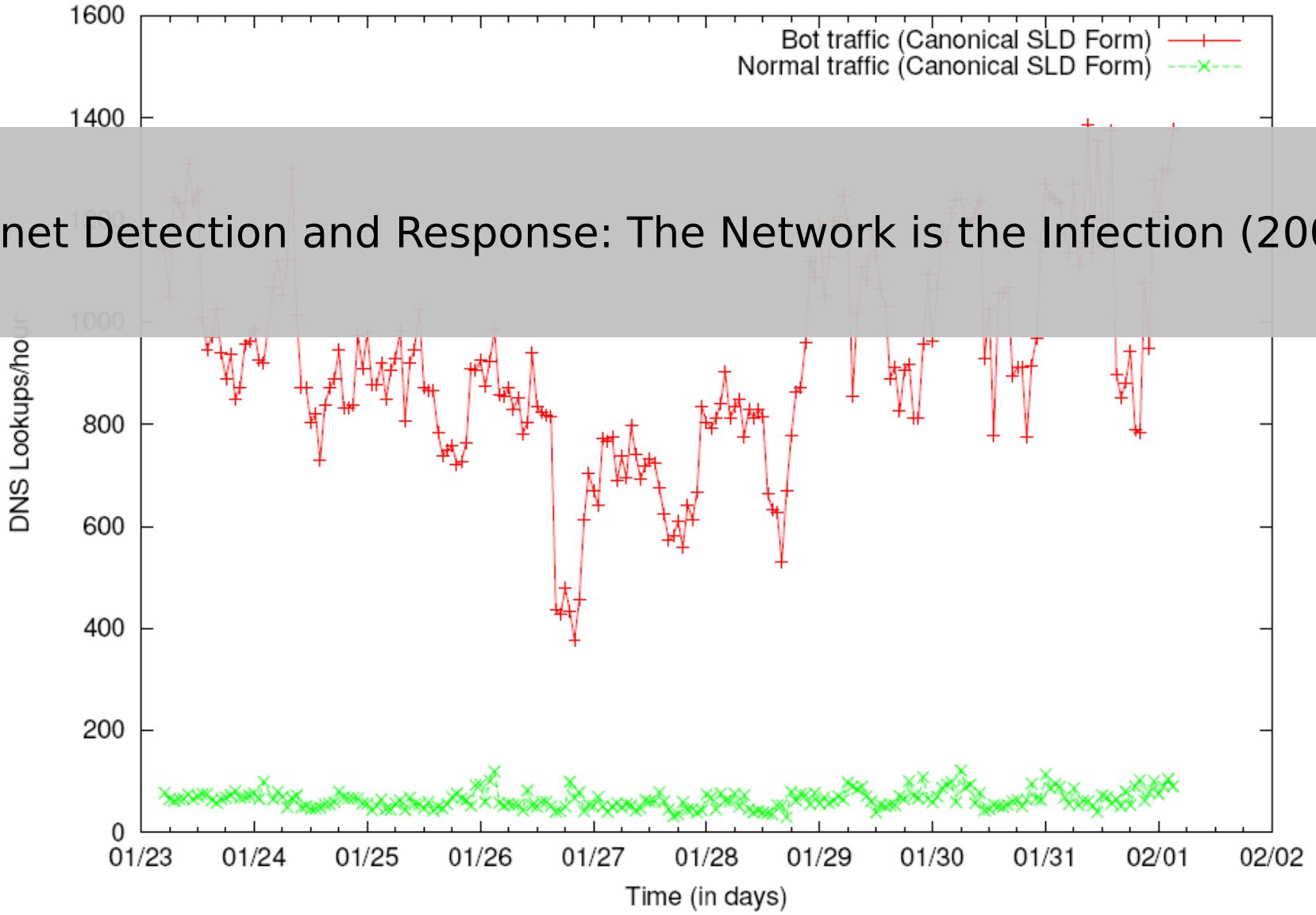
Bypass Matrix

	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

Detecting DDNS Bots

Assumption:

1. For DDNS, botnets tend use subdomains; legitimate directories use subdirectories
2. Use SLD/3LD-ratios to identify botnet traffic

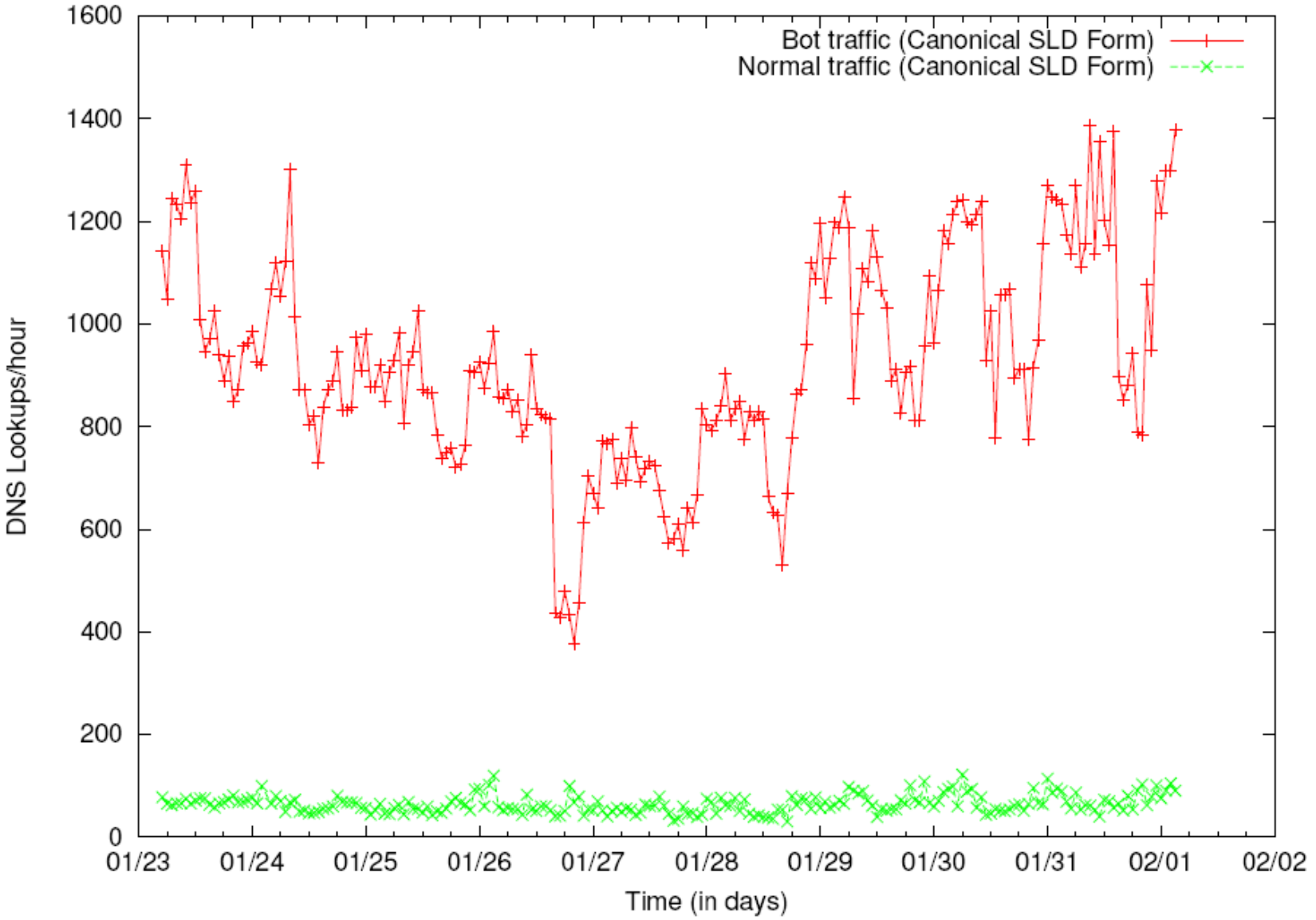


Botnet Detection and Response: The Network is the Infection (2005)

Detecting DDNS Bots

Assumption:

1. For DDNS, botnets tend use subdomains; legitimate directories use subdirectories
2. Use SLD/3LD-ratios to identify botnet traffic



Monitoring Group Activities

Differences between Botnet and Legitimate DNS

	Source IPs accessed to domain name	Activity and Appearance Patterns	DNS Type
Botnet DNS	Anonymous (Botnet members)	Group activity Randomly appeared (Specific situation)	Usually DDNS
Legitimate DNS	Anonymous (Legitimate users)	Non-group activity Randomly and continuously appered (Usually)	Usually DNS

Botnet Detection by Monitoring Group Activities in DNS Traffic (2007)

Monitoring Group Activities

Differences between Botnet and Legitimate DNS

	Source IPs accessed to domain name	Activity and Appearance Patterns	DNS Type
Botnet DNS	Fixed size Group (Botnet members)	Group activity Intermittently appeared (Specific situation)	Usually DDNS
Legitimate DNS	Anonymous (Legitimate users)	Non-group activity Randomly and continuously appered (Usually)	Usually DNS

Anomaly Detection to DNS Traffic

Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic (2008)

Assumption: Bots typically employ DDNS

Methods:

1. High DDNS query rates may be expected because botmasters frequently move C&C servers.
2. looking for abnormally recurring DDNS (NXDOMAIN). Such queries may correspond to bots trying to locate C&C servers that have been taken down.

Anomaly Detection to DNS Traffic

Assumption: Bots typically employ DDNS

Methods:

1. High DDNS query rates may be expected because botmasters frequently move C&C servers.
2. looking for abnormally recurring DDNS (NXDOMAIN). Such queries may correspond to bots trying to locate C&C servers that have been taken down.

基於瀏覽器

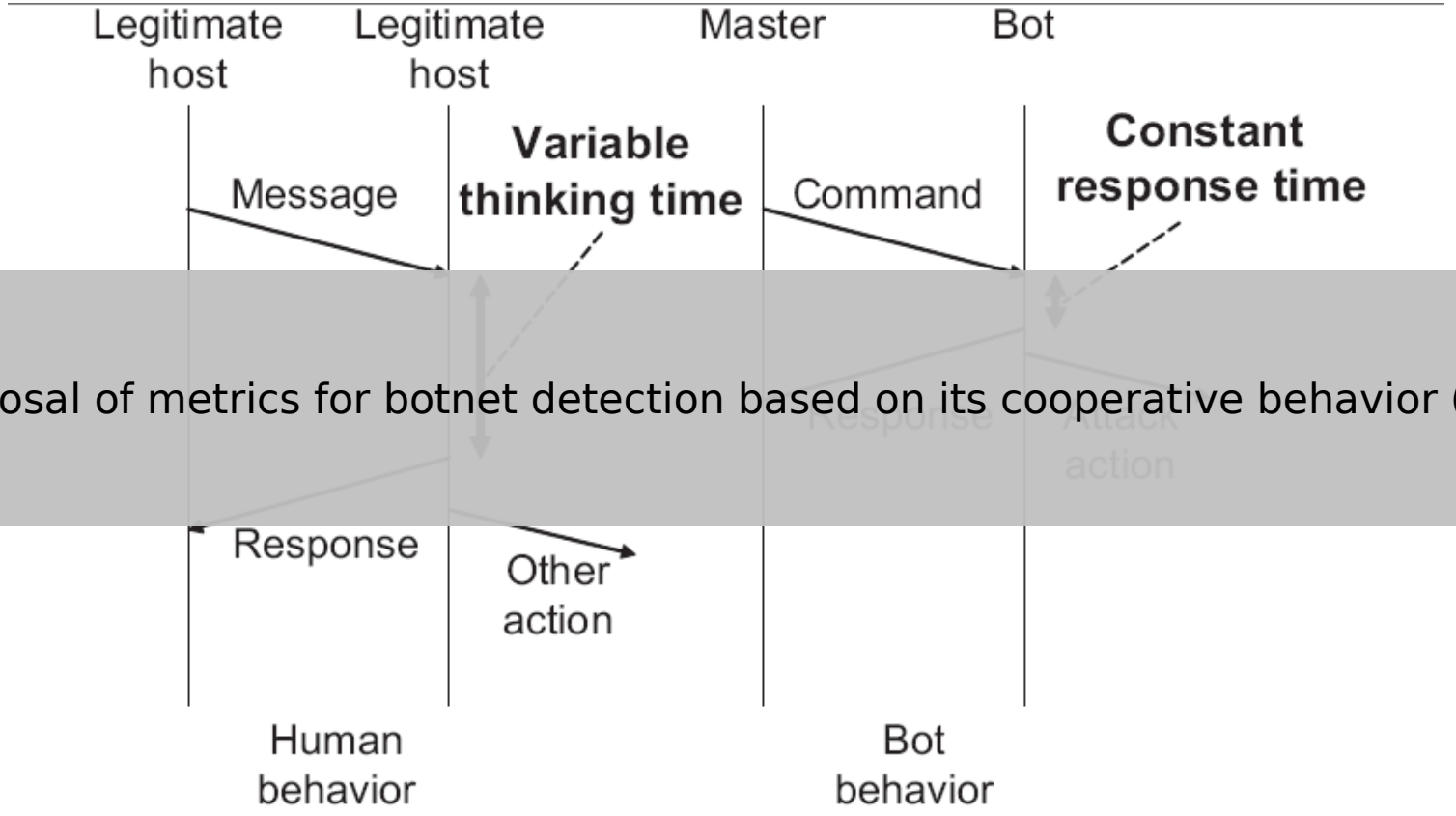
1. 非常容易模擬正常行為（基於Port 80, 443 的實現）
2. 跨平台特性（手持設備上的支持）
3. 最常使用的應用程式是
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

BotFox

基於瀏覽器

1. 非常容易模擬正常行為（基於 Port 80, 443 的實現）
2. 跨平台特性（手持式裝置、手機等）
3. 最常使用的應用程式之一
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

Cooperative behavior



A proposal of metrics for botnet detection based on its cooperative behavior (2007)

Figure 2. Comparison of response time between humans and bots

Cooperative behavior

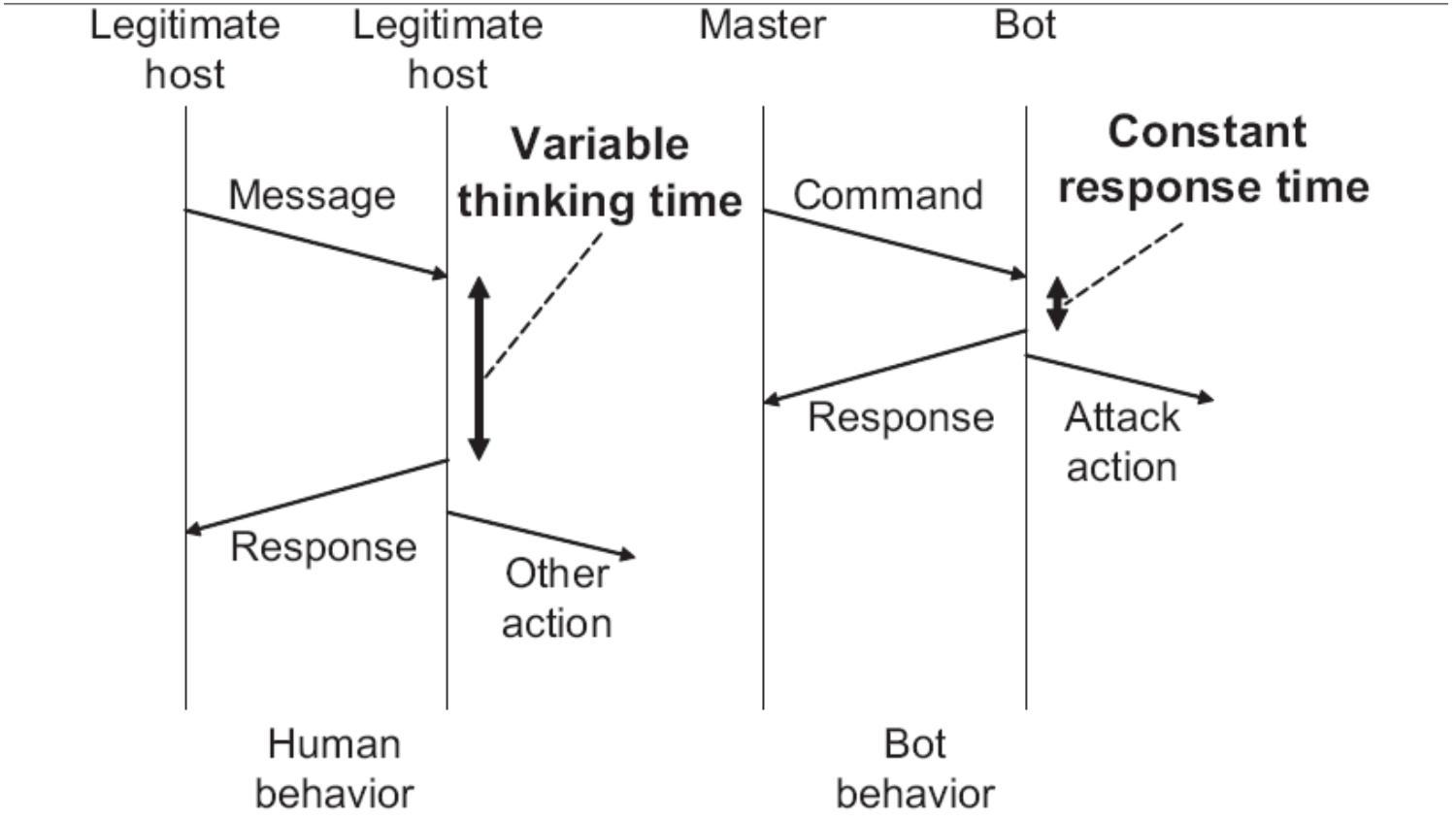


Figure 2. Comparison of response time between humans and bots

基於瀏覽器

1. 非常容易模擬正常行為（基於Port 80, 443 的實現）
2. 跨平台特性（手持設備、嵌入式系統）
3. 最常使用的應用程式是 [illegible]
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

BotFox

基於瀏覽器

1. 非常容易模擬正常行為（基於 Port 80, 443 的實現）
2. 跨平台特性（手持式裝置、手機等）
3. 最常使用的應用程式之一
4. 白名單的常客
5. 完全使用正常的 DNS 查詢

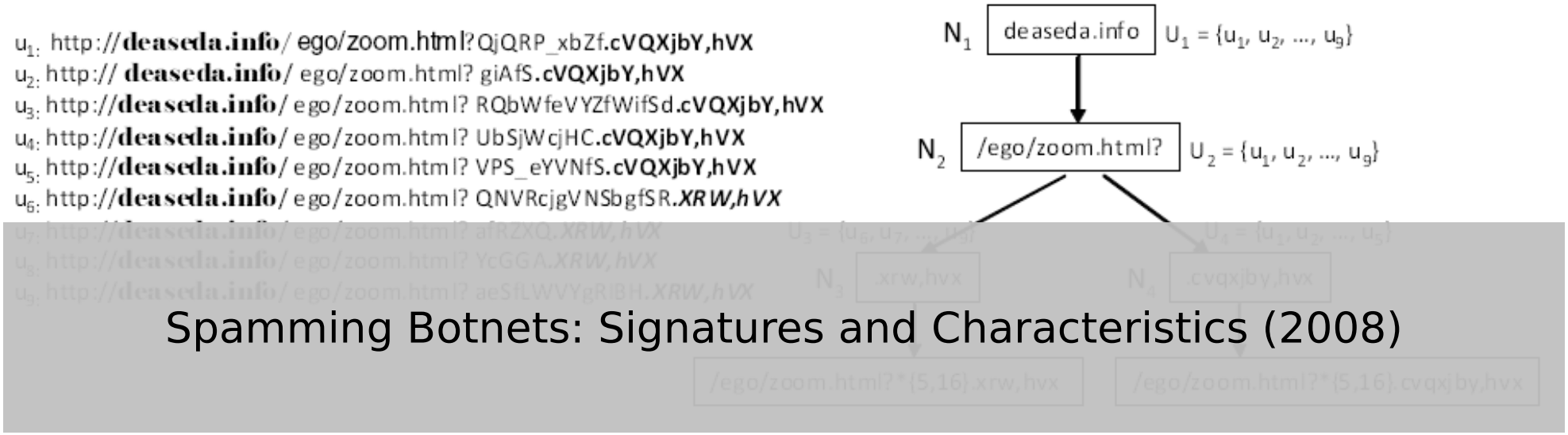
DNS Traffic

1. 基於瀏覽器，非常容易模擬正常行為。
2. 使用正常 DNS 。

Bypass Matrix

	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

Spam Signatures



Spamming Botnets: Signatures and Characteristics (2008)

Figure 5: Example input URLs and the keyword-based signature tree constructed by AutoRE.

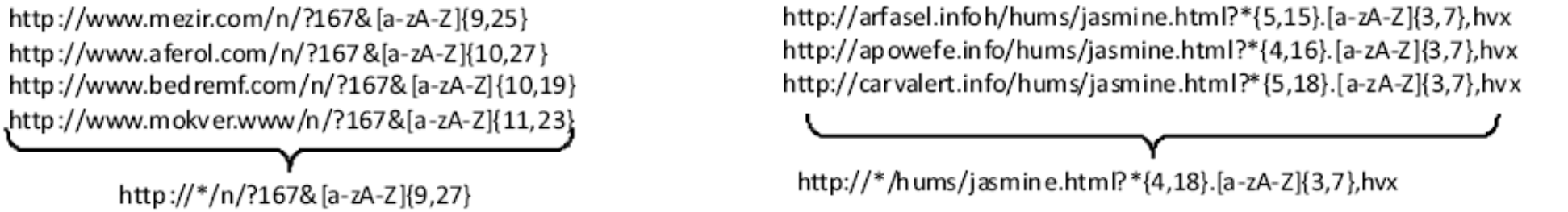


Figure 6: Generalization: Merging domain-specific regular expressions into domain-agnostic regular expressions.

Spam Signatures

u_1: http://**deaseda.info**/ego/zoom.html?QjQRP_xbZf.**cVQXjbY,hVX**
u_2: http://**deaseda.info**/ego/zoom.html?giAfS.**cVQXjbY,hVX**
u_3: http://**deaseda.info**/ego/zoom.html?RQbWfeVYZfWifSd.**cVQXjbY,hVX**
u_4: http://**deaseda.info**/ego/zoom.html?UbSjWcjHC.**cVQXjbY,hVX**
u_5: http://**deaseda.info**/ego/zoom.html?VPS_eYVNfS.**cVQXjbY,hVX**
u_6: http://**deaseda.info**/ego/zoom.html?QNVRcjgVNSbgfSR.***XRW,hVX***
u_7: http://**deaseda.info**/ego/zoom.html?afRZXQ.***XRW,hVX***
u_8: http://**deaseda.info**/ego/zoom.html?YcGGA.***XRW,hVX***
u_9: http://**deaseda.info**/ego/zoom.html?aeSfLWVYgRlBH.***XRW,hVX***

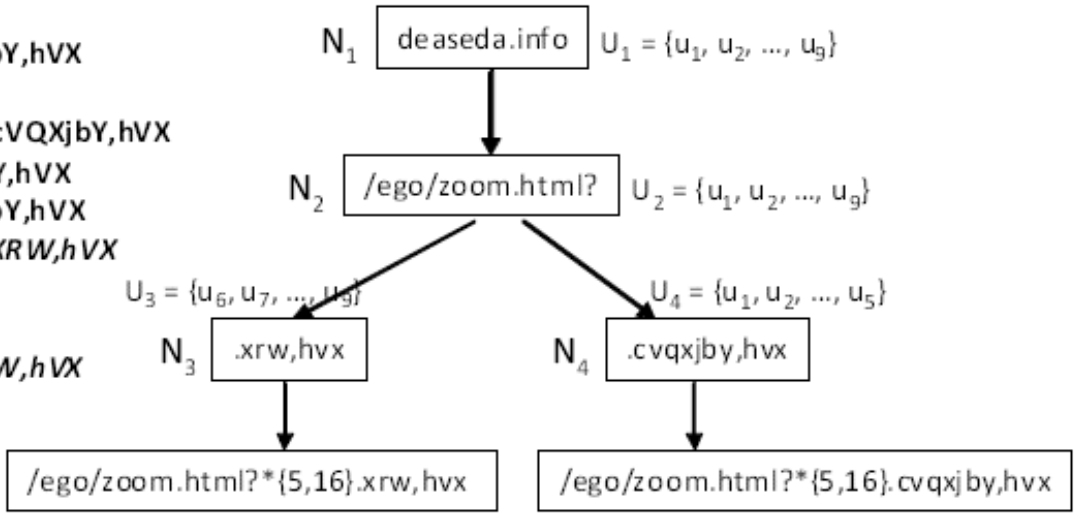


Figure 5: Example input URLs and the keyword-based signature tree constructed by AutoRE.

http://www.mezir.com/n/?167&[a-zA-Z]{9,25}
http://www.aferol.com/n/?167&[a-zA-Z]{10,27}
http://www.bedremf.com/n/?167&[a-zA-Z]{10,19}
http://www.mokver.www/n/?167&[a-zA-Z]{11,23}

http://*/n/?167&[a-zA-Z]{9,27}

http://arfasel.infoh/hums/jasmine.html?*{5,15}.[a-zA-Z]{3,7},hvx
http://apowefe.info/hums/jasmine.html?*{4,16}.[a-zA-Z]{3,7},hvx
http://carvalert.info/hums/jasmine.html?*{5,18}.[a-zA-Z]{3,7},hvx

http://*/hums/jasmine.html?*{4,18}.[a-zA-Z]{3,7},hvx

Figure 6: Generalization: Merging domain-specific regular expressions into domain-agnostic regular expressions.

SPAM Signatures

1. 使用受害者的線上郵遞系統 → 正當來源， SPAM 特徵低。
2. 使用多個線上郵遞系統，如 Gmail 、 Yahoo → 降低同源特徵。
3. 還有很多方法可以避開 SPAM 特徵。

Bypass Matrix

	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

IRC Analysis

1. 不使用 IRC protocol 。
2. 很多網路環境禁用 IRC protocol 。
3. 許多安全工具視 IRC 封包為可疑 / 惡意封包。

Bypass Matrix

	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

P2P Analysis

1. 不使用 P2P protocol 。
2. 不需與 P2P-filter 攻防戰。
3. 不需額外開 Port ，降低被偵測的機率。
4. 可運行於僅允許 HTTP/HTTPs 的網路環境。

Bypass Matrix

	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

Open Proxy

1. 不使用 Open Proxy 。
2. 不需額外開 Port ，降低被偵測的機率。

Bypass Matrix

	Pass	Comments
AntiVirus	✅	Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection	✅	Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer	✅	Combine with Browser, No Process, No DLL
Network Monitor	✅	Same with normal network traffic
Honeypots	✅	Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis	✅	Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic	✅	Use legitimate DNS server, No DDNS
SPAM Signatures	✅	Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis	✅	No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis	✅	No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy	✅	No Open Proxy
VPN	✅	Normal allow HTTP/HTTPs
Content Filter	✅	Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

VPN

1. 通常 VPN 會允許 HTTP/HTTPs 。

Bypass Matrix

	Pass	Comments
AntiVirus		Pure JavaScript, No API Hooks, No Registry, No DLL
Rootkit Detection		Pure JavaScript, No API Hooks, No Registry, No DLL
Process Explorer		Combine with Browser, No Process, No DLL
Network Monitor		Same with normal network traffic
Honeypots		Bots only connect with legitimate server (C&C), Hard to distinguish between normal and evil traffic
Behavior/Log Analysis		Borwser is in Whitelist (Basically), Same with normal network traffic
DNS Traffic		Use legitimate DNS server, No DDNS
SPAM Signatures		Use real behavior and account, and many ways to bypass SPAM detection
IRC Analysis		No Implement IRC protocol. (IRC protocol often block by corporation, even some tools judge all IRC are evil connect)
P2P Analysis		No implement P2P protocol. (No need to comfront P2P filter, No open port, Surf with HTTP/HTTPs only environment)
Open Proxy		No Open Proxy
VPN		Normal allow HTTP/HTTPs
Content Filter		Connect with legitimate server, Pure JavaScript, Contents is pure data not malware code, Hard to extract keywords

Content Filter

1. 封包 / 字串無任何惡意內容 → 防止關鍵字偵測。
2. 使用正常 DNS → 防止 DNS 黑名單。
3. JavaScript 的特性使的關鍵特徵難以擷取。

©Google

Google Chrome

Opera

Microsoft IE

更甚者

©Microsoft

©Google

地理定位技術
Geolocation

©Mozilla

©Opera software

©Apple

結論

1. 歡迎來到 Bot 2.0 (aka CloudBot) 的時代。
2. 『它』可以繞過目前所有常見的安全防護。
3. 技術量低、成本低。
4. 大腦本身就是一種永遠可以被利用的 0day（社交工程手法）。
5. 雲端運算的時代，也意謂著
   更強大、更穩健、隨開即用之跨平台惡意程式時代的來臨。

Ant

yftzeng@gmail.com