資安報告暨風險事件分析

2014-1120 ~2014-1127

網路安全分析內容說明

應用程式行為分析：

TOP 10 應用程式統計
TOP 10 應用程式主機流量分析
TOP 10 內網主機流量統計

入侵偵測事件分析：

TOP 10 安全威脅事件統計
TOP N 安全威脅事件類別統計
TOP 10 安全威脅內網主機統計

Botnet事件分析：

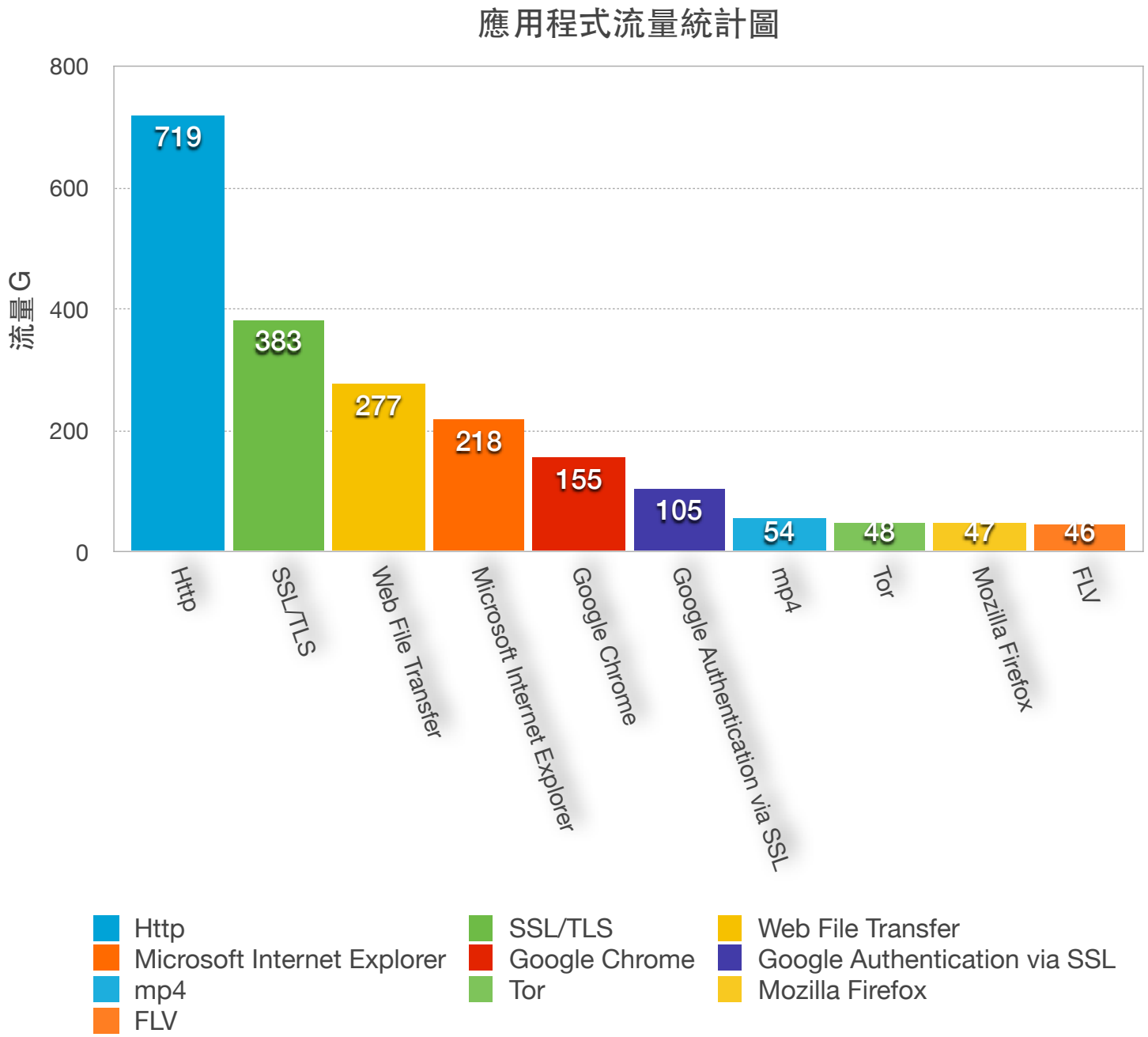
TOP 10 Botnet 內網可疑主機分析
TOP 10 Botnet C&C 活動分析
TOP 10 Botnet RBL 惡意目標分析

趨勢比較圖

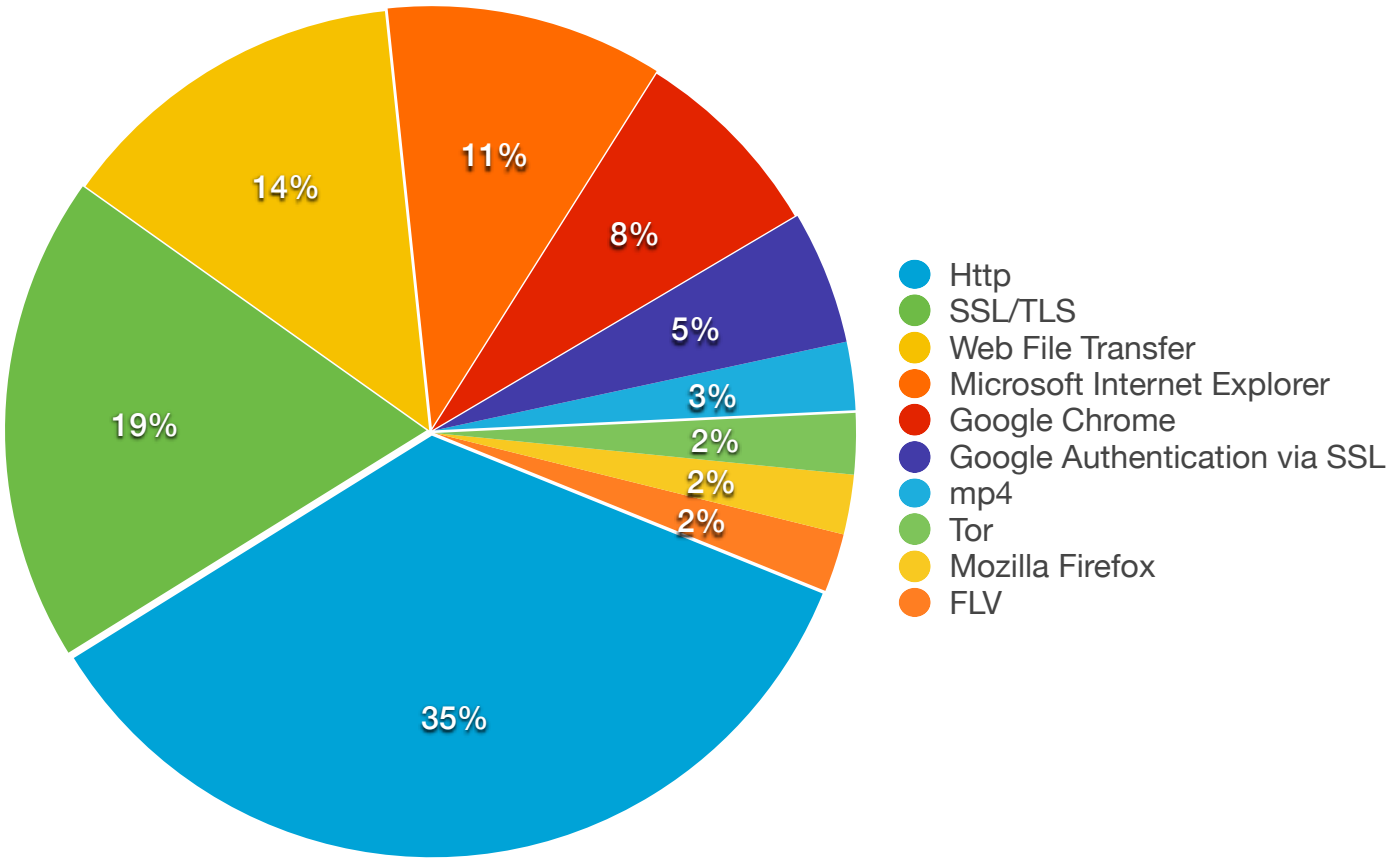
資安事件趨勢比較圖
資安事件統計
資安事件曲線圖
高危險內部主機列表

應用程式行為分析

TOP 10 應用程式統計



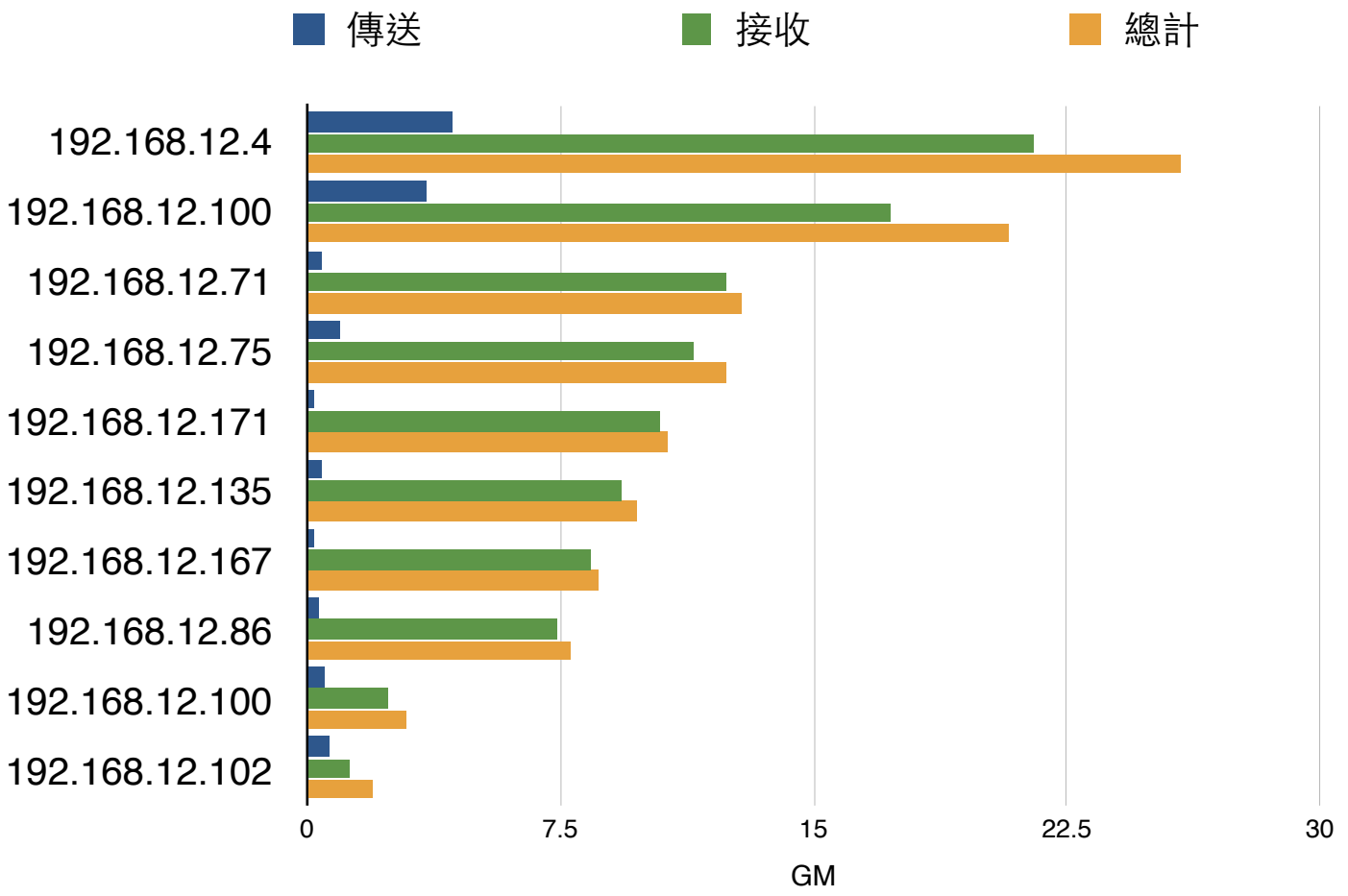
應用程式流量統計圖

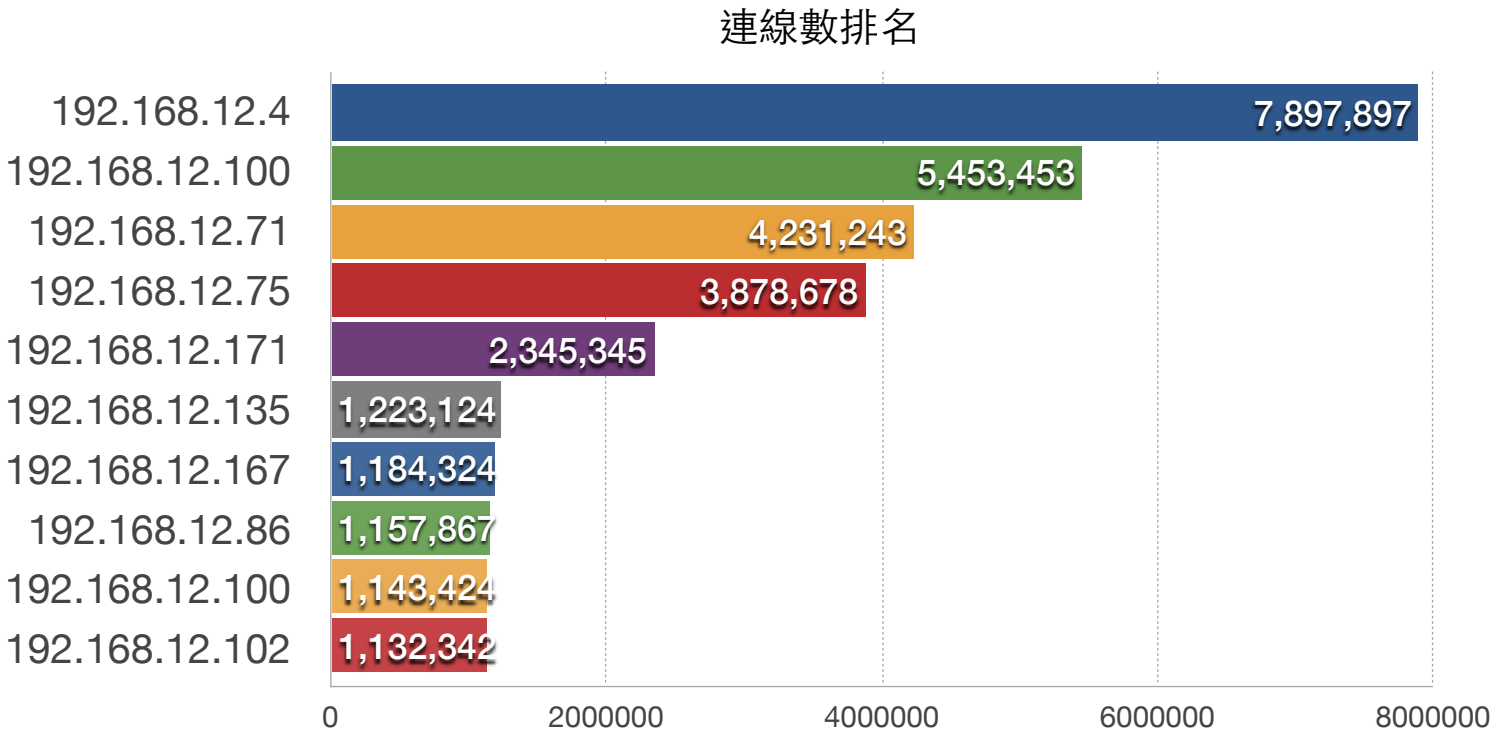


TOP 10 應用程式統計

應用程式名稱	流量
Http	719 GM
SSL/TLS	383 GM
Web File Transfer	277 GM
Microsoft Internet Explorer	218 GM
Google Chrome	155 GM
Google Authentication via SSL	105 GM
mp4	53.61 GM
Tor	48 GM
Mozilla Firefox	47 GM
FLV	46 GM

應用程式主機流量分析


傳送
接收
總計
192.168.12.4
192.168.12.100
192.168.12.71
192.168.12.75
192.168.12.171
192.168.12.135
192.168.12.167
192.168.12.86
192.168.12.100
192.168.12.102
0
7.5
15
22.5
30
GM

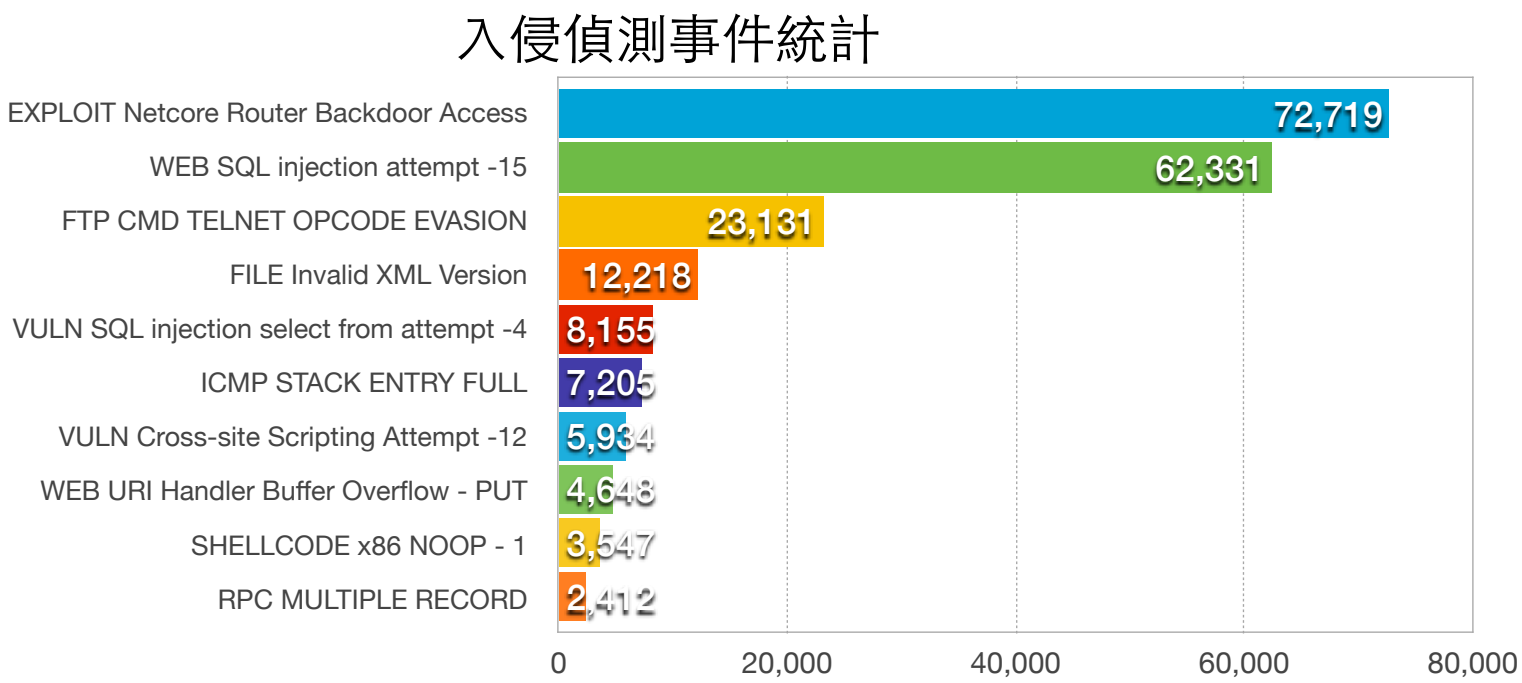

連線數排名
192.168.12.4
192.168.12.100
192.168.12.71
192.168.12.75
192.168.12.171
192.168.12.135
192.168.12.167
192.168.12.86
192.168.12.100
192.168.12.102
7,897,897
5,453,453
4,231,243
3,878,678
2,345,345
1,223,124
1,184,324
1,157,867
1,143,424
1,132,342
0
2000000
4000000
6000000
8000000

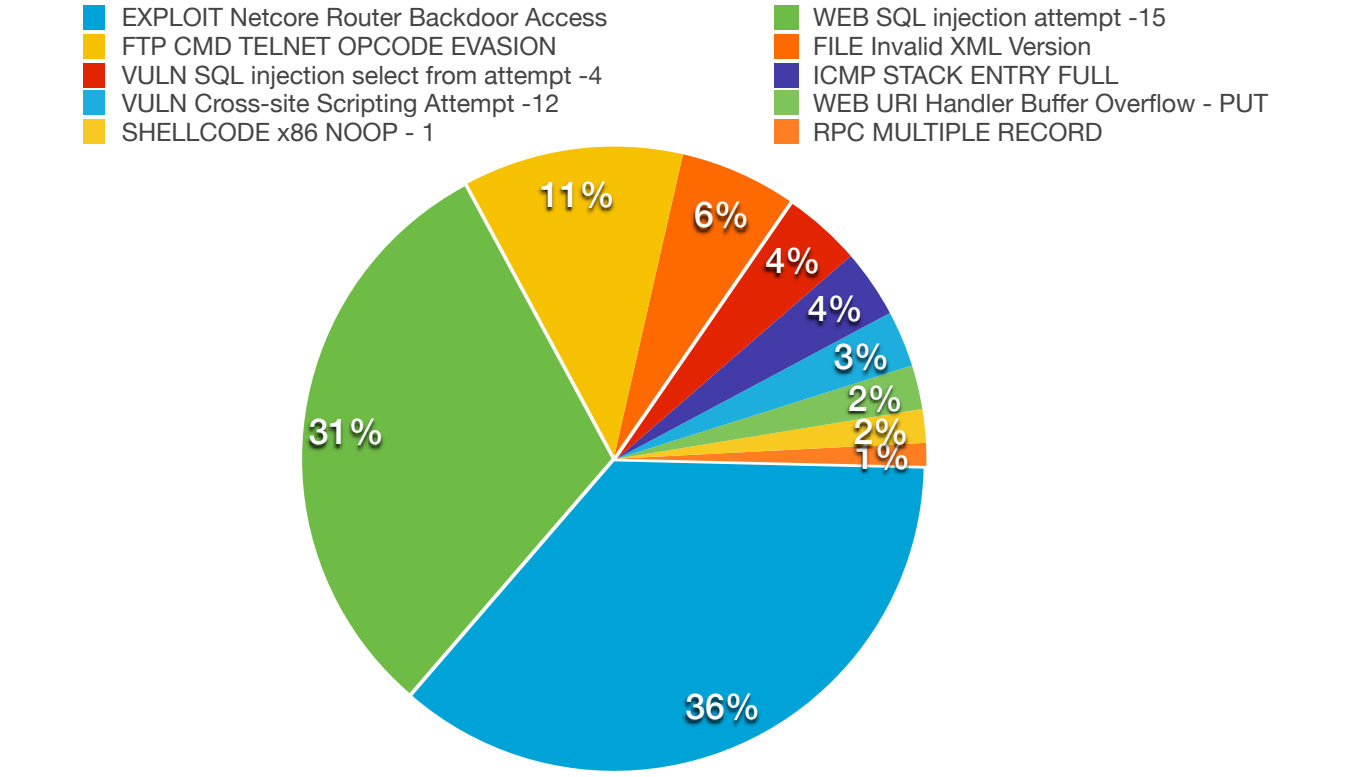
主機流量排名

排名	內網主機	傳送	接收	總計	連接數
1	192.168.12.4	4.28 GM	213.56 GM	217.8 GM	7897897
2	192.168.12.100	42.5 GM	7.24 GM	49.74 GM	3453453
3	192.168.12.71	412 MB	42.43 GM	42.84 GM	1231243
4	192.168.12.75	945 MB	33,45 GM	34.39 GM	678678
5	192.168.12.171	18 MB	23,42 GM	23.44 GM	345345
6	192.168.12.135	456 MB	18.34 GM	18.79 GM	123124
7	192.168.12.167	32 MB	13.42 GM	13.45 GM	84324
8	192.168.12.86	43 MB	12.42 GM	12.46 GM	57867
9	192.168.12.100	64 MB	2.43 GM	2.49 GM	43424
10	192.168.12.102	87 MB	234 GM	321 MB	22342

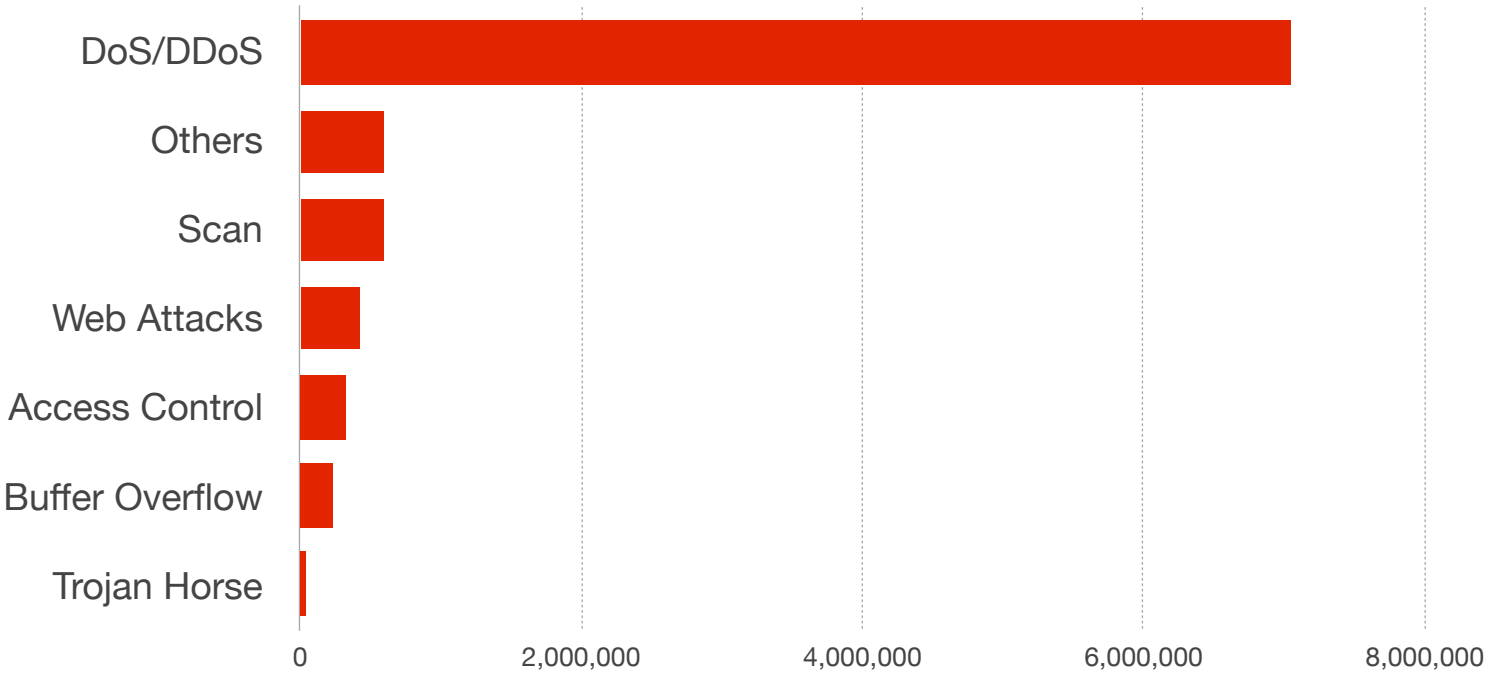
入侵偵測事件分析

TOP 10 安全威脅事件統計





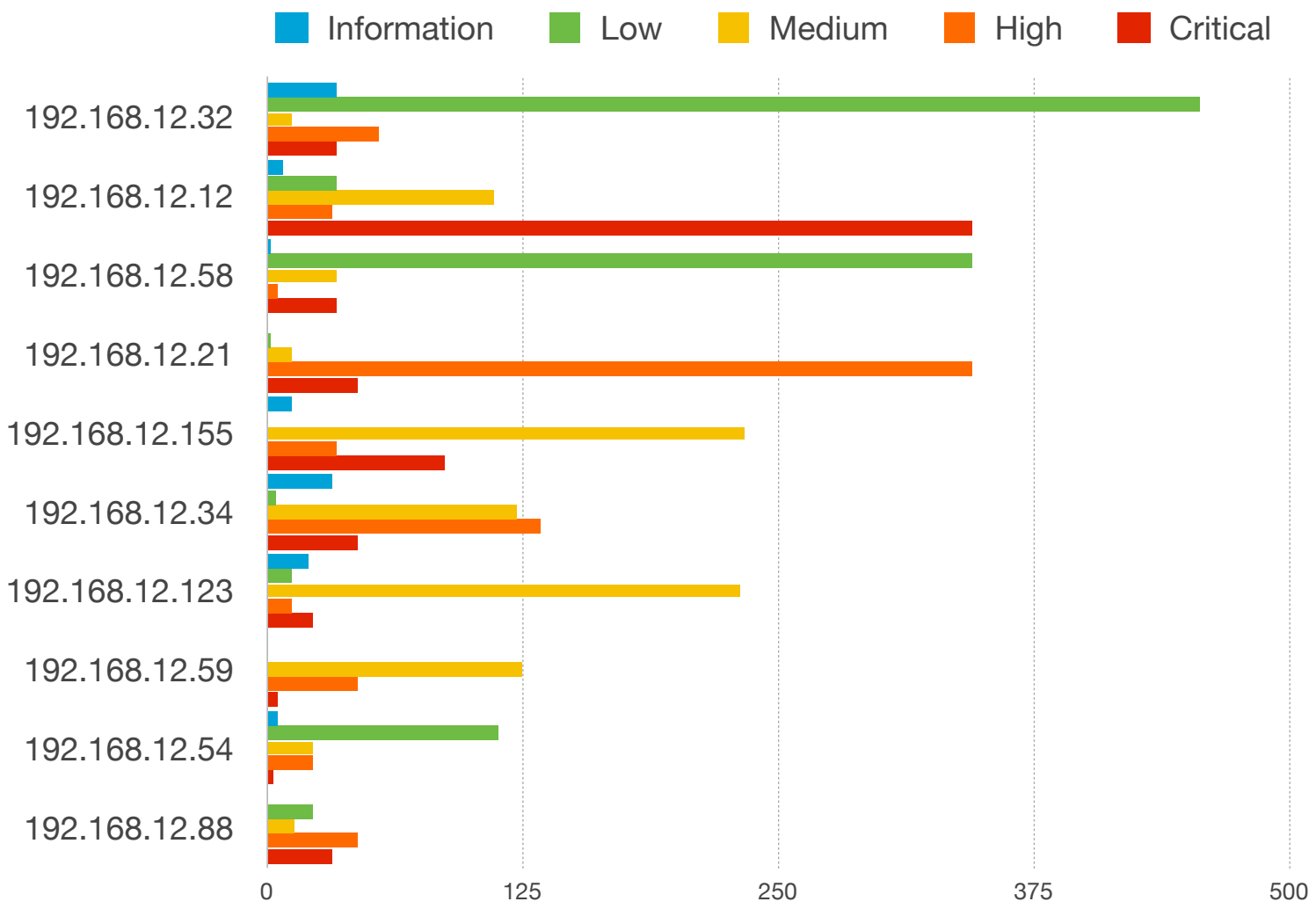
攻擊名稱	攻擊次數
EXPLOIT Netcore Router Backdoor Access	72,719
WEB SQL injection attempt -15	62,331
FTP CMD TELNET OPCODE EVASION	23,131
FILE Invalid XML Version	12,218
VULN SQL injection select from attempt -4	8,155
ICMP STACK ENTRY FULL	7,205
VULN Cross-site Scripting Attempt -12	5,934
WEB URI Handler Buffer Overflow - PUT	4,648
SHELLCODE x86 NOOP - 1	3,547
RPC MULTIPLE RECORD	2,412



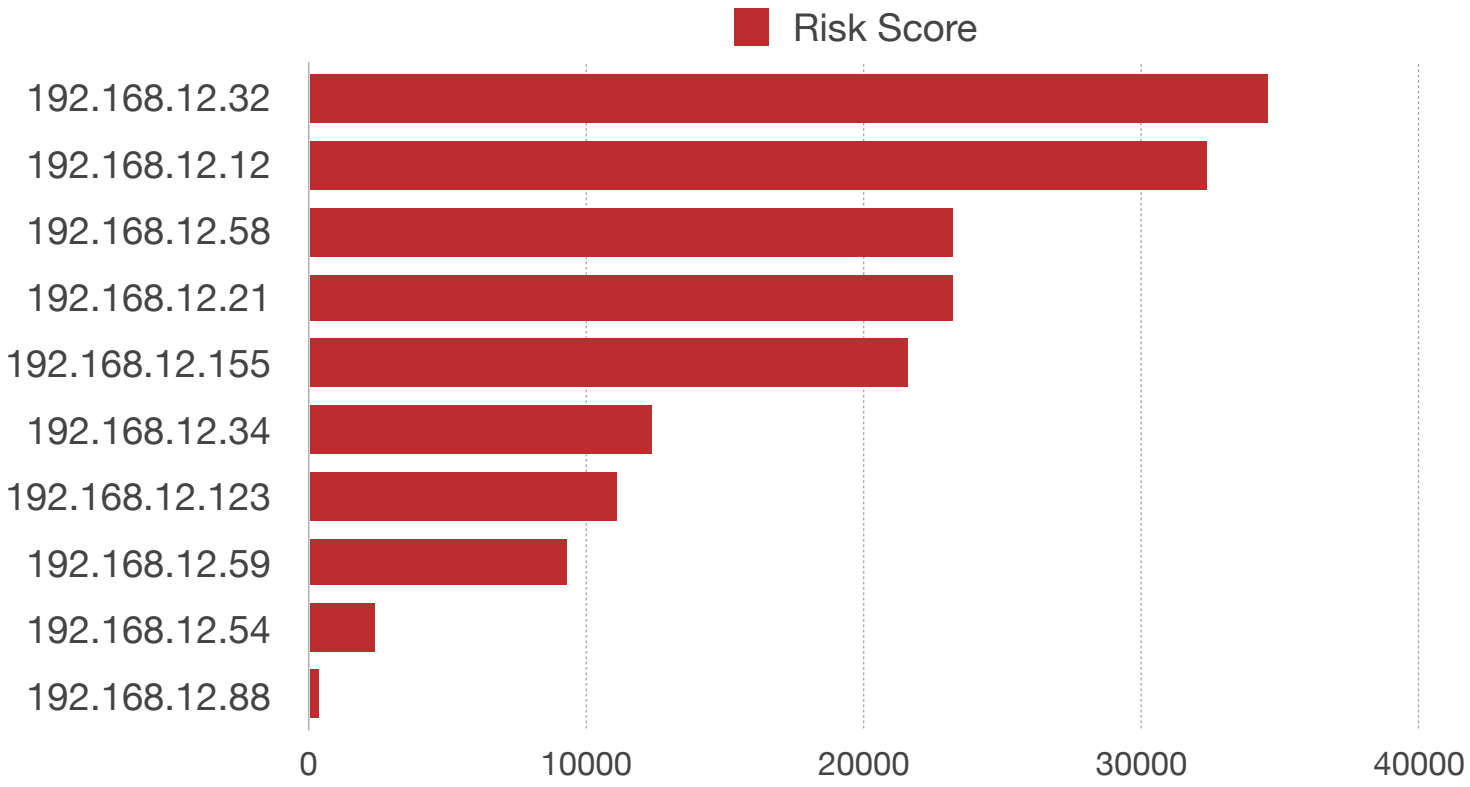
TOP N 安全威脅事件類別統計

TOP	類別	次數
1	DoS/DDoS	7,041,698
2	Others	600,585
3	Scan	587,023
4	Web Attacks	427,053
5	Access Control	327,063
6	Buffer Overflow	227,013
7	Trojan Horse	47,063

TOP 10 安全威脅內網主機統計



威脅評分

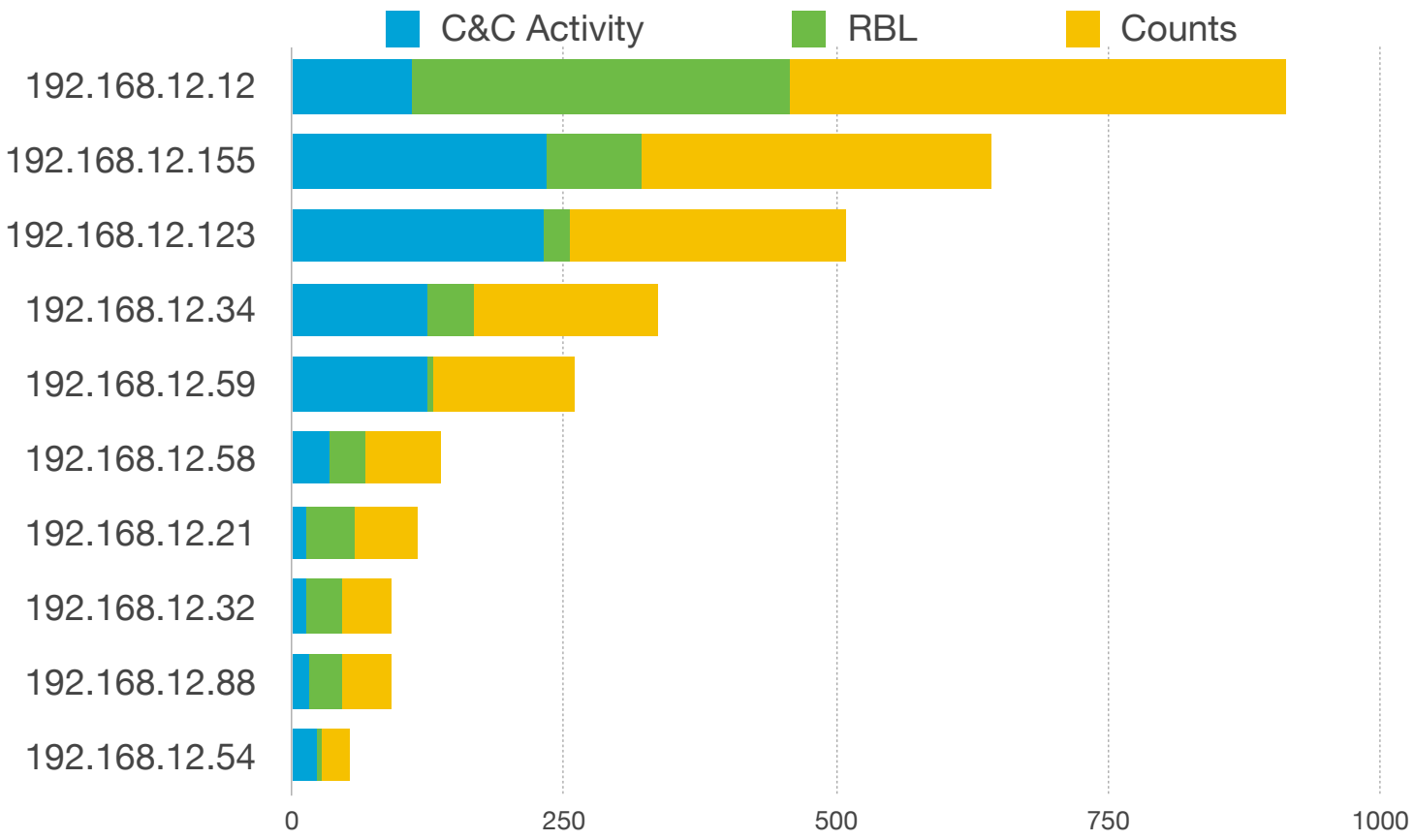


威脅總表

Host Name	Information	Low	Medium	High	Critical	Total	Risk Score
192.168.12.32	34	456	12	55	34	591	34534
192.168.12.12	8	34	111	32	345	530	32331
192.168.12.58	2	345	34	5	34	420	23223
192.168.12.21	0	2	12	345	45	404	23234
192.168.12.155	12	1	234	34	87	368	21545
192.168.12.34	32	4	123	134	45	338	12335
192.168.12.123	21	13	231	13	23	301	11134
192.168.12.59	0	1	125	45	5	176	9235
192.168.12.54	5	113	23	23	3	167	2345
192.168.12.88	0	23	14	45	32	114	342

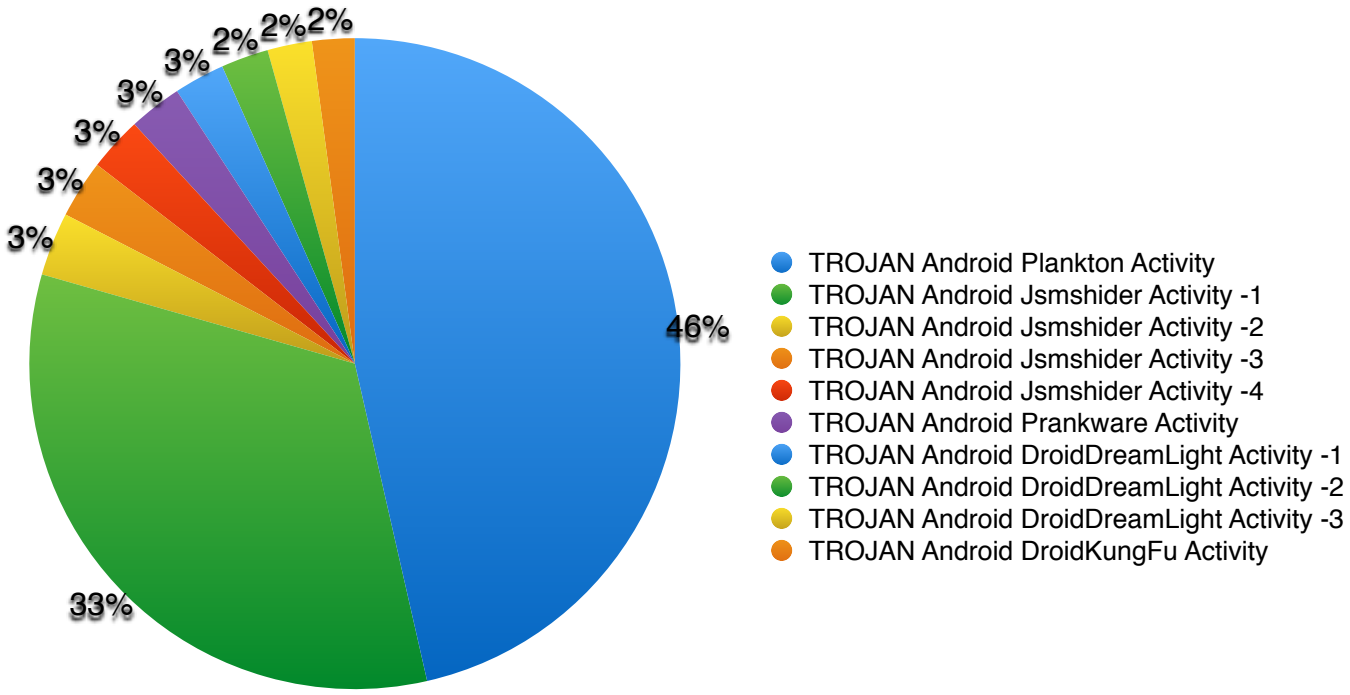
Botnet事件分析

TOP 10 Botnet 內網可疑主機分析



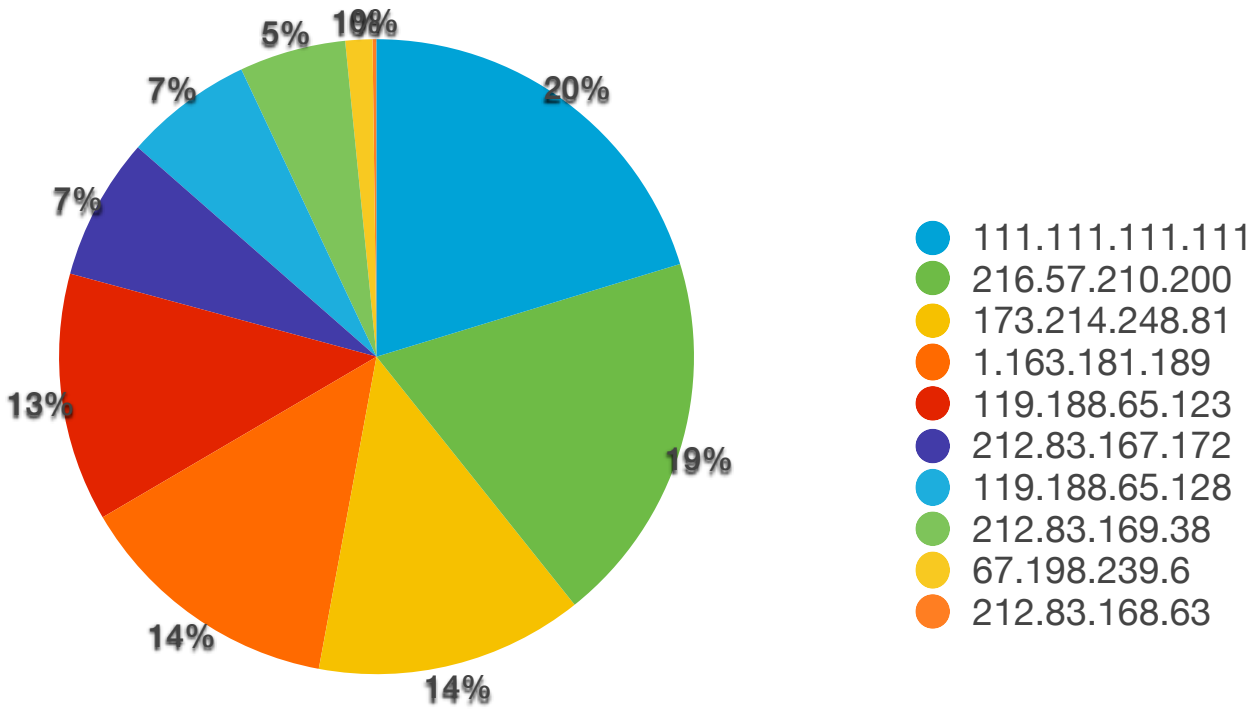
主機名稱	C&C Activity	RBL	Counts
192.168.12.12	111	345	456
192.168.12.155	234	87	321
192.168.12.123	231	23	254
192.168.12.34	123	45	168
192.168.12.59	125	5	130
192.168.12.58	34	34	68
192.168.12.21	12	45	57
192.168.12.32	12	34	46
192.168.12.88	14	32	46
192.168.12.54	23	3	26

TOP 10 Botnet C&C 活動分析



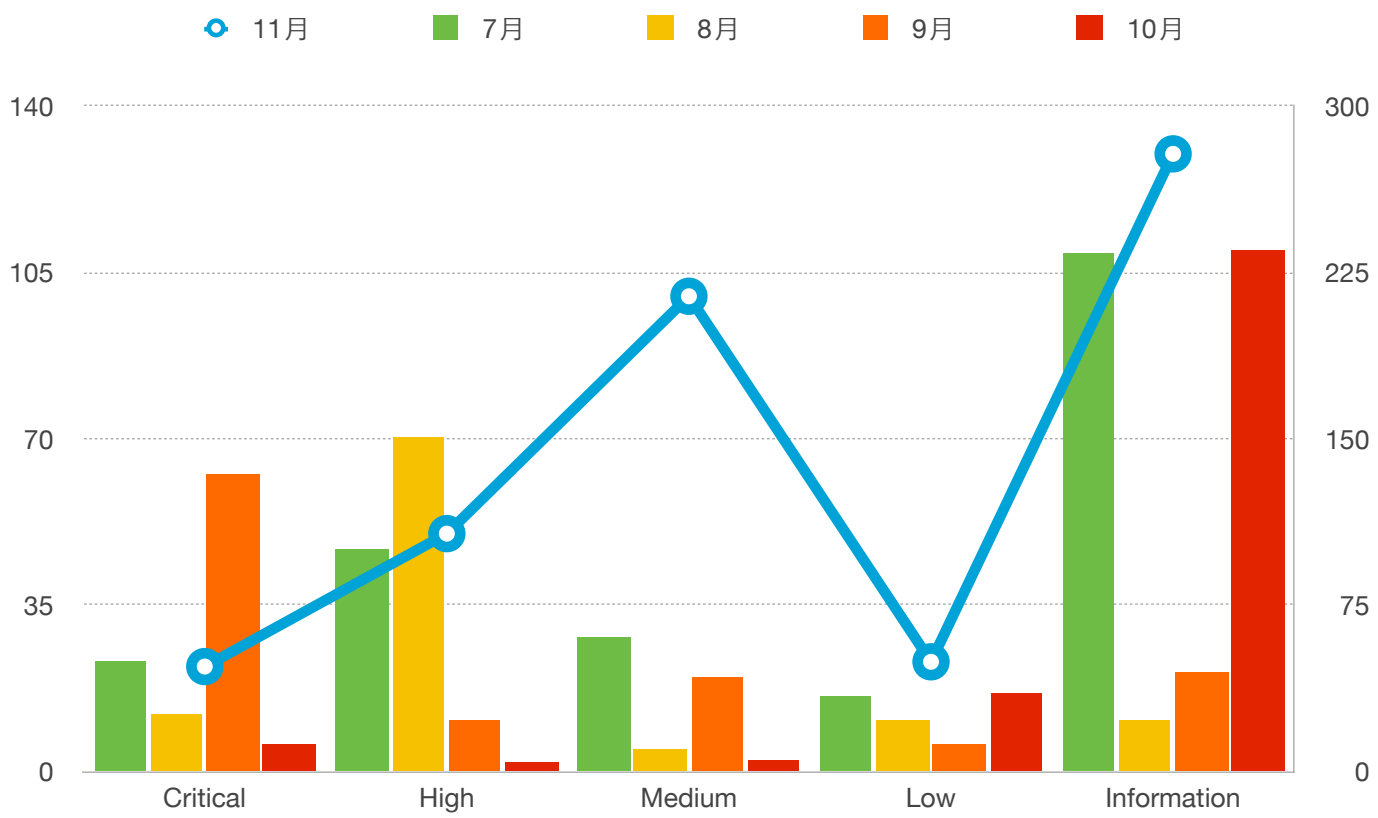
Rule ID	C & C 事件名稱	累積次數
1055166	TROJAN Android Plankton Activity	34534
1055271	TROJAN Android Jsmshider Activity -1	24534
1055272	TROJAN Android Jsmshider Activity -2	2344
1055273	TROJAN Android Jsmshider Activity -3	2145
1055274	TROJAN Android Jsmshider Activity -4	2004
1055275	TROJAN Android Prankware Activity	1965
1055276	TROJAN Android DroidDreamLight Activity -1	1876
1055277	TROJAN Android DroidDreamLight Activity -2	1754
1055278	TROJAN Android DroidDreamLight Activity -3	1643
1055279	TROJAN Android DroidKungFu Activity	1573

TOP 10 Botnet RBL 惡意目標分析



TOP	惡意位置	累積次數
1	111.111.111.111	34534
2	216.57.210.200	32331
3	173.214.248.81	23223
4	1.163.181.189	23234
5	119.188.65.123	21545
6	212.83.167.172	12335
7	119.188.65.128	11134
8	212.83.169.38	9235
9	67.198.239.6	2345
10	212.83.168.63	342

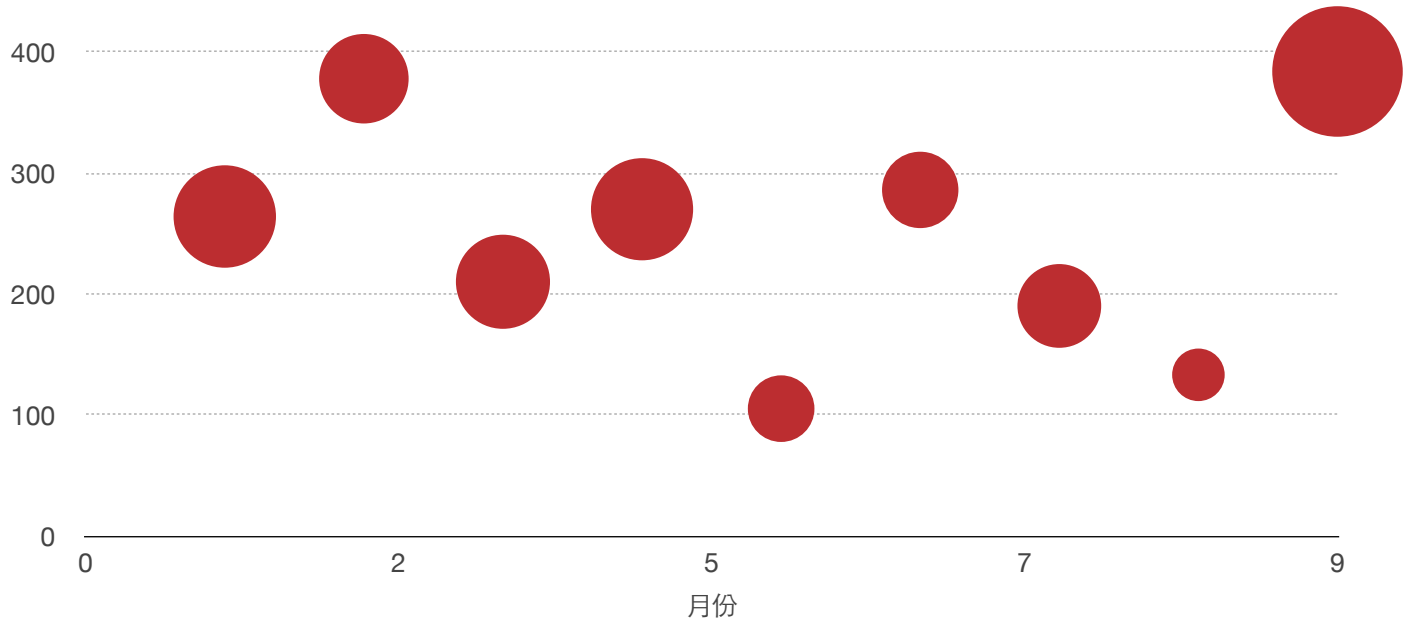
資安事件趨勢比較圖



資安事件統計

描述	11月	7月	8月	9月	10月
Critical	22	50	25	134	12
High	50	100	150	23	4
Medium	100	60	10	42	5
Low	23	34	23	12	35
Information	130	234	23	45	235

資安事件曲線圖



高危險內部主機列表