阻斷式服務攻擊的演進與應對之道

麟瑞科技
RING LINE CORPORATION

陳宏儒
Brandon_chen@ringline.com.tw

何謂 DoS DDoS?阻斷服務攻擊 分散式阻斷服務攻擊

- 亦稱洪水攻擊 流量轟炸
  - 唯一目的在於使網際網路上標的伺服器其網路資源及系統資源耗盡，使這個連上網路的主機暫時中斷或停止服務，使它無法對正常用戶提供服務。
- 目標類型
  - 大型商業網站(拍賣)，遊戲公司，任何收益來源為網站服務的企業、政府單位或學校
- 造成的傷害
  - 實際收入減少
  - 企業形象的受損，客戶信心降低
  - 遭駭客的勒索，惡性循環

2012全球資訊安全

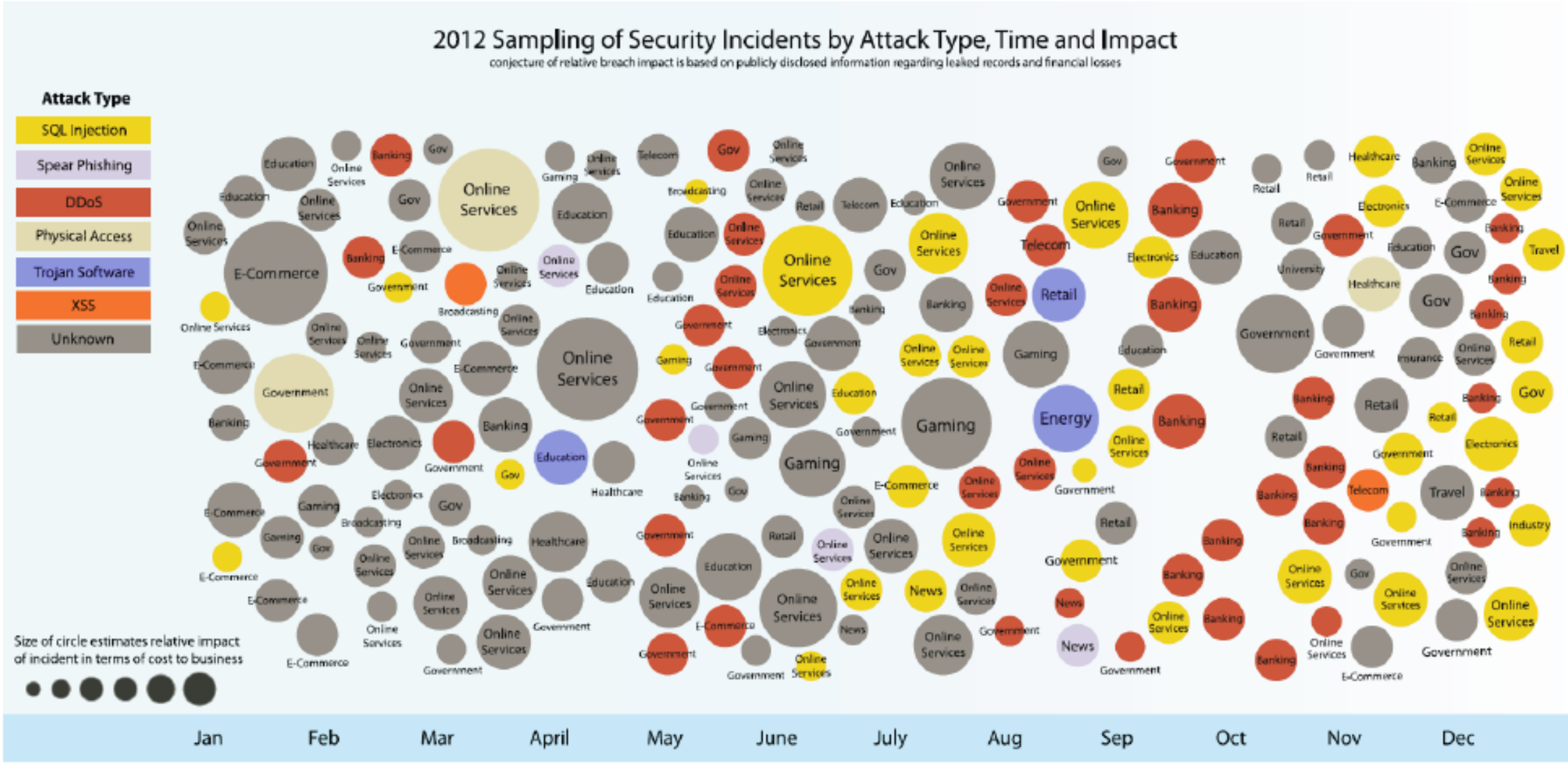


Figure 3: 2012 Sampling of Security Incidents by Attack Type, Time and Impact

2013全球資訊安全事件統計

Attack Type

- SQL Injection
- Spear Phishing
- DDos
- Physical Access
- Malware
- XSS
- Watering Hole
- Unknown

圓圈的大小表示對業務影響的大小

世界上即時DDoS攻擊!

http://www.digitalattackmap.com

您的資料中心已經做好抵禦DDoS的準備了嗎?

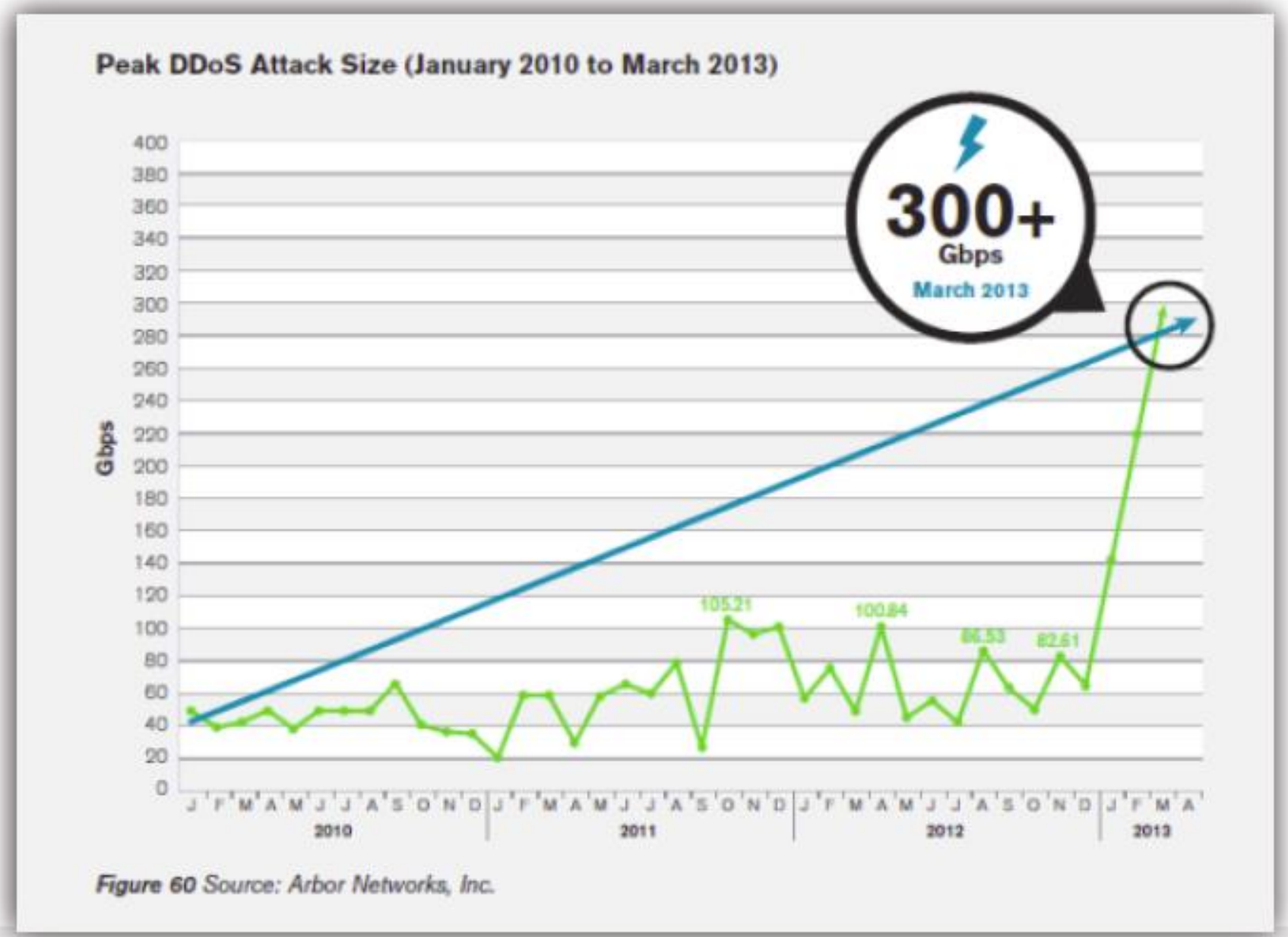
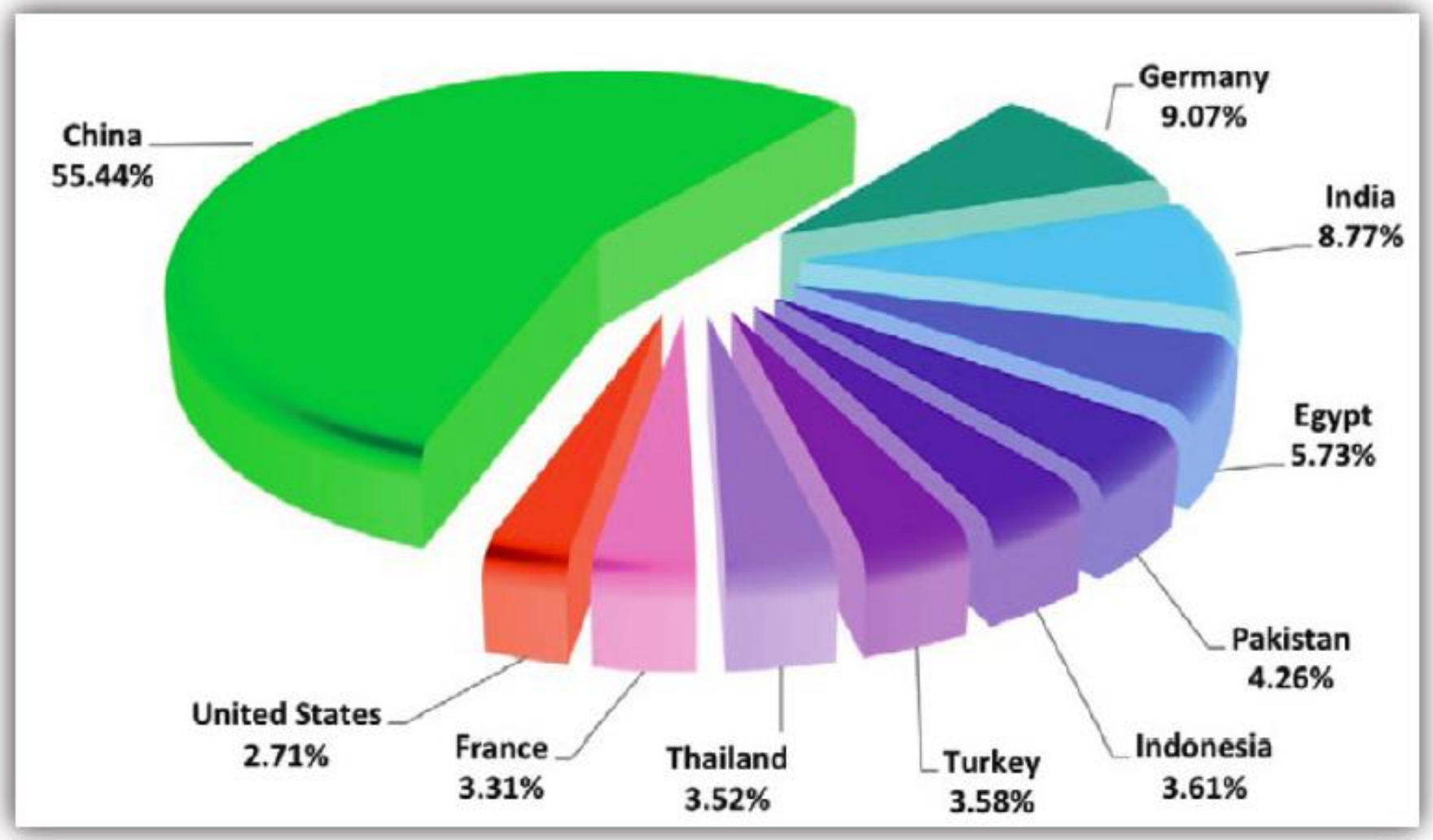


Figure 60 Source: Arbor Networks, Inc.

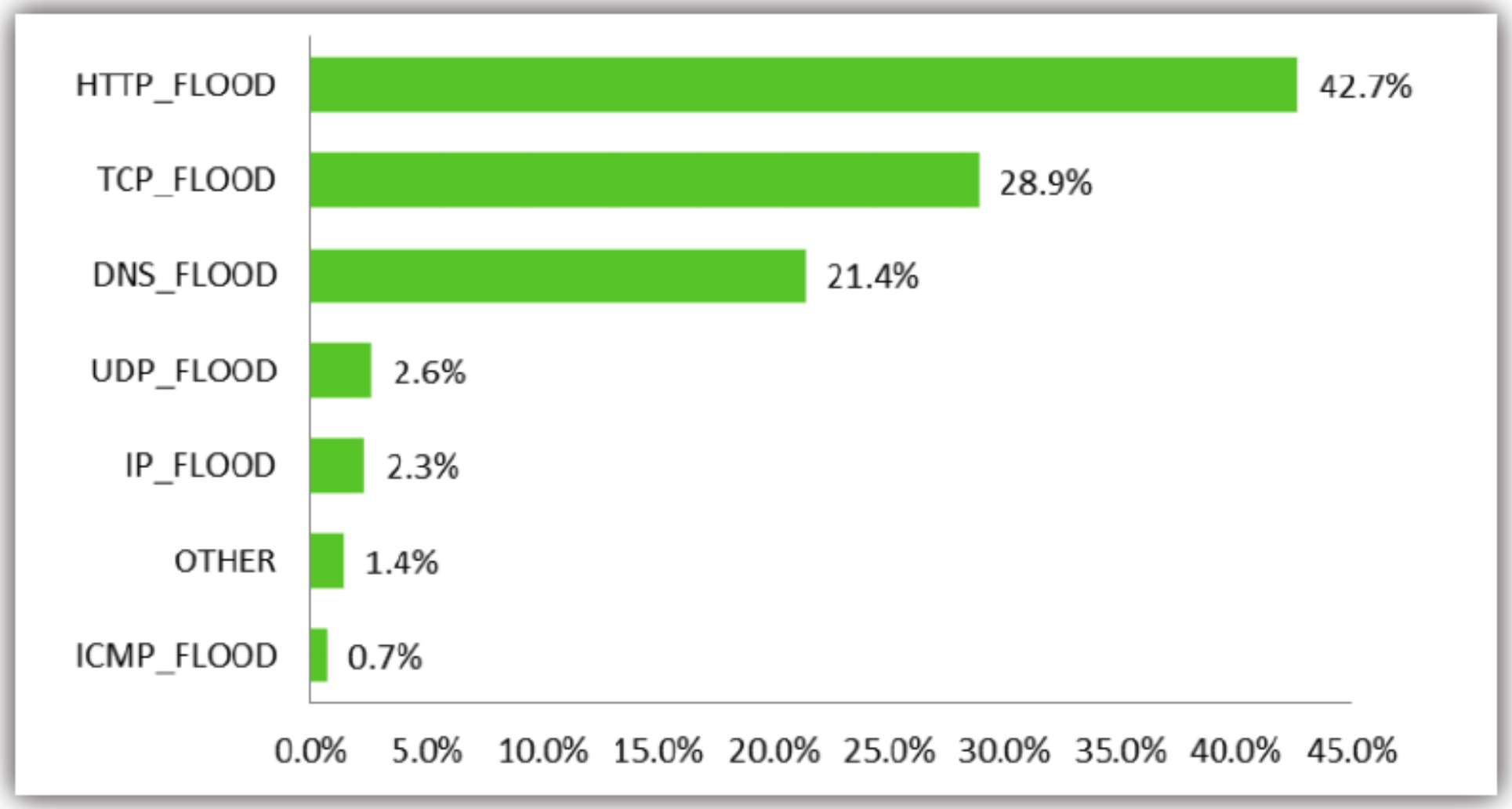
流量越來越巨大
種類越來越多樣

+300 GIGABITS/SECOND !

DDoS 攻擊源地址統計—前十名國家列表



DDoS 攻擊種類統計

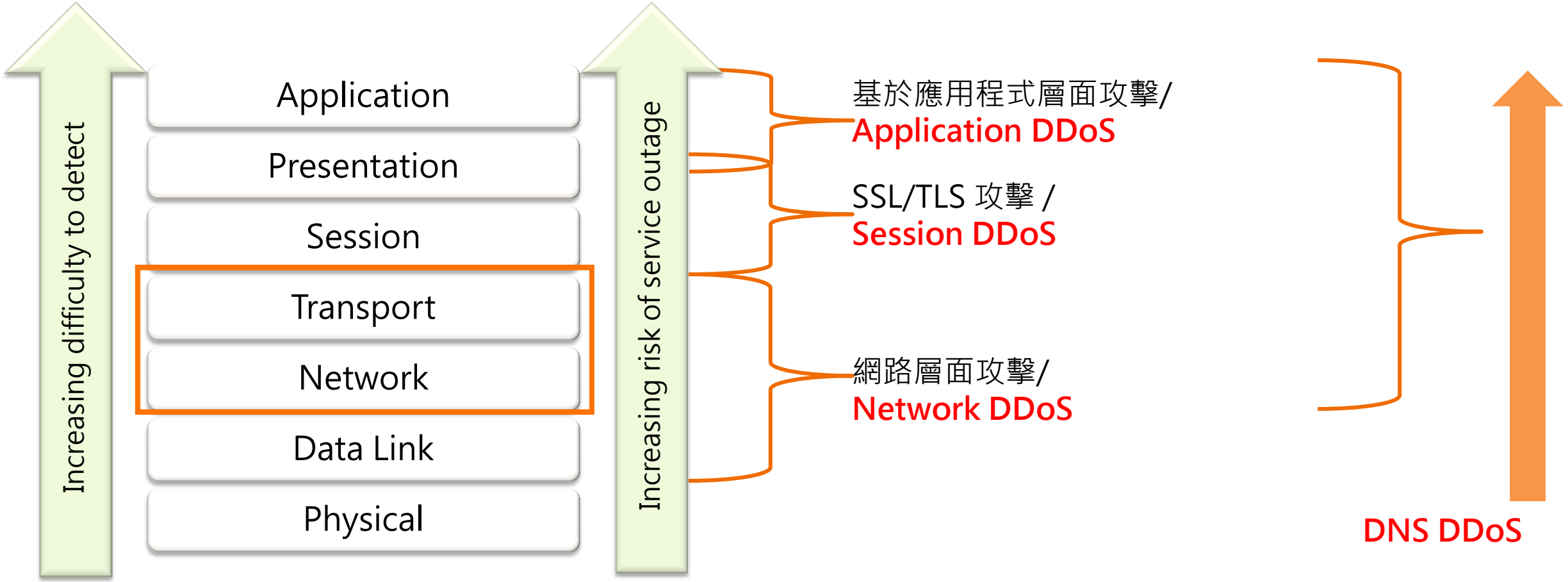

HTTP_FLOOD
42.7%
TCP_FLOOD
28.9%
DNS_FLOOD
21.4%
UDP_FLOOD
2.6%
IP_FLOOD
2.3%
OTHER
1.4%
ICMP_FLOOD
0.7%
0.0%
5.0%
10.0%
15.0%
20.0%
25.0%
30.0%
35.0%
40.0%
45.0%

DDoS attacks攻擊的主要種類

網路層DDoS攻擊

應用層DDoS攻擊

DDoS 攻擊特性 攻擊包含OSI各層面及複雜度



網路層DDoS攻擊

- UDP Flood
  - 最早期的DDOS攻擊，UDP的特性，“fire-and-forget”，用量達到DOS目的
- IP Fragment Flood(Tears Drop淚滴攻擊)
  - 每個資料要傳送前，該封包都會經過切割，每個小切割都會記錄位移的資訊，以便重組，但此攻擊模式就是捏造位移資訊，造成重組時發生問題，造成錯誤
- ping of death（死亡之Ping）
  - 是產生超過IP協定能容忍的封包數，若系統沒有檢查機制，就會當機。

網路層DDoS攻擊

- 協定分析攻擊（SYN flood，SYN洪水）
  - 最早期的TCP DDOS攻擊，不完整的Hand shacking，吃光connection table、系統記憶體和處理器資源耗盡
- LAND attack
  - 這種攻擊方式與SYN floods類似，不過在LAND attack攻擊包中的原位址和目標位址都是攻擊物件的IP。這種攻擊會導致被攻擊的機器無窮迴圈，最終耗盡資源而當機。
- 殭屍網路攻擊
  - 是產生超過IP協定能容忍的封包數，若系統沒有檢查機制，就會當機。
  - 現今最具發展的類型，與APT攻擊相互形成網路最大威脅的Circle

Session DDoS攻擊

- SSL Flood
  - 利用SSL機制，在建立安全連線交談(Handshake)期間的快速資源消耗特性，所設計的攻擊工具，建立一個安全SSL連線時，伺服器需要耗用15倍於用戶端的處理能力。

著名攻擊tool

THC SSL DoS 利用換Key的Server端高loading此種不對稱特性，灌爆伺服器以致無法在Internet提供服務。

L7 應用層 DDoS

- **Slowloris SlowPost**
  - 這類攻擊的特性是並沒有違反HTTP的連線規則，只是把這些連線大幅度的低速化，因此容易被資安監控設備忽略。
- **SlowHeader**
  - 放大HTTP request Header內文，甚至多個Header，低速傳送
- **PS:**低速化，他舉例，本來10秒可以完成的連線，被拉長到1,000分鐘；本來一秒鐘送一個字，變成100秒送一個字。其目的就是要佔住Session。

DNS DDoS

- **DNS反射(reflection)攻擊**
  - 也就是利用公開的DNS解析器(resolvers)，攻擊者假裝從目標對數萬台的DNS解析器發出請求，而這些DNS解析器會向目標回應，因此帶來大量的網路流量。
- **DNS Flood**
  - 基本洪水攻擊：這種攻擊會送出許多DNS請求到DNS伺服器上，企圖耗盡這些伺服器的網域名稱解析器，以及快取資料庫資源。
- **遞迴式洪水攻擊（Reflective DNS Flood）**
  - 攻擊者會對DNS伺服器，送出並不存在DNS快取資料的網域名稱解析請求，增加DNS伺服器與網路頻寬的負擔。
- **垃圾洪水攻擊（Garbage Flood）**
  - 這種攻擊會利用53埠，對DNS伺服器發出大量封包，進而塞暴伺服器對外的網路連線，並且讓DNS名稱解析器疲於奔命，也就無法服務正常查詢請求。

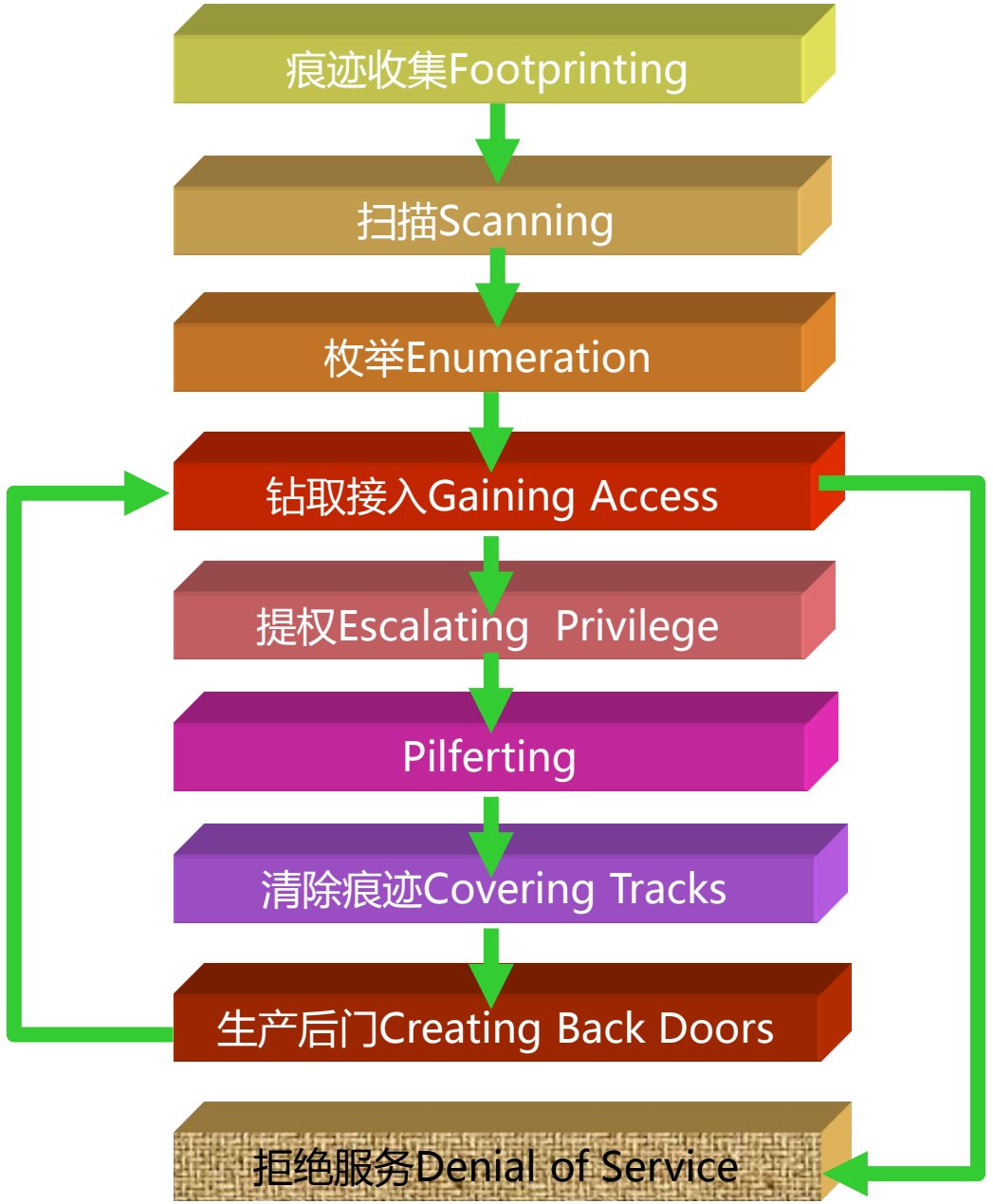
DDoS演進

攻擊趨勢演化	
年度	主要攻擊趨勢
2009 以前	巨流量攻擊 (Volumetric Attack)
2010-2011	L7 應用程式層 (Application Layer Attack)
2011-2012	混合式多向攻擊 (Multi-Vector Attack/Blended Attack)
2013	針對防禦機制的穿透式攻擊

DDoS演進 變形體 2014Jun

- Drive
  - 受到控制的殭屍電腦會自動偵測防禦機制封包回應，同時針對防禦機制回應正確封包，從而得到認證並穿透防禦機制。加上擬真度較高的網路服務請求封包，防禦機制變得不再可信，防禦DDoS攻擊的難度大大提高
  - 仍然處於起步階段，而更新、更精緻的攻擊變體仍會持續出現.....

Hacking Methodology



whois, nslookup

Nmap, fping

dumpACL, showmount
legion, rpcinfo

Tcpdump, Lophtcrack
NAT

Johntheripper, getadmin
Rhosts, userdata

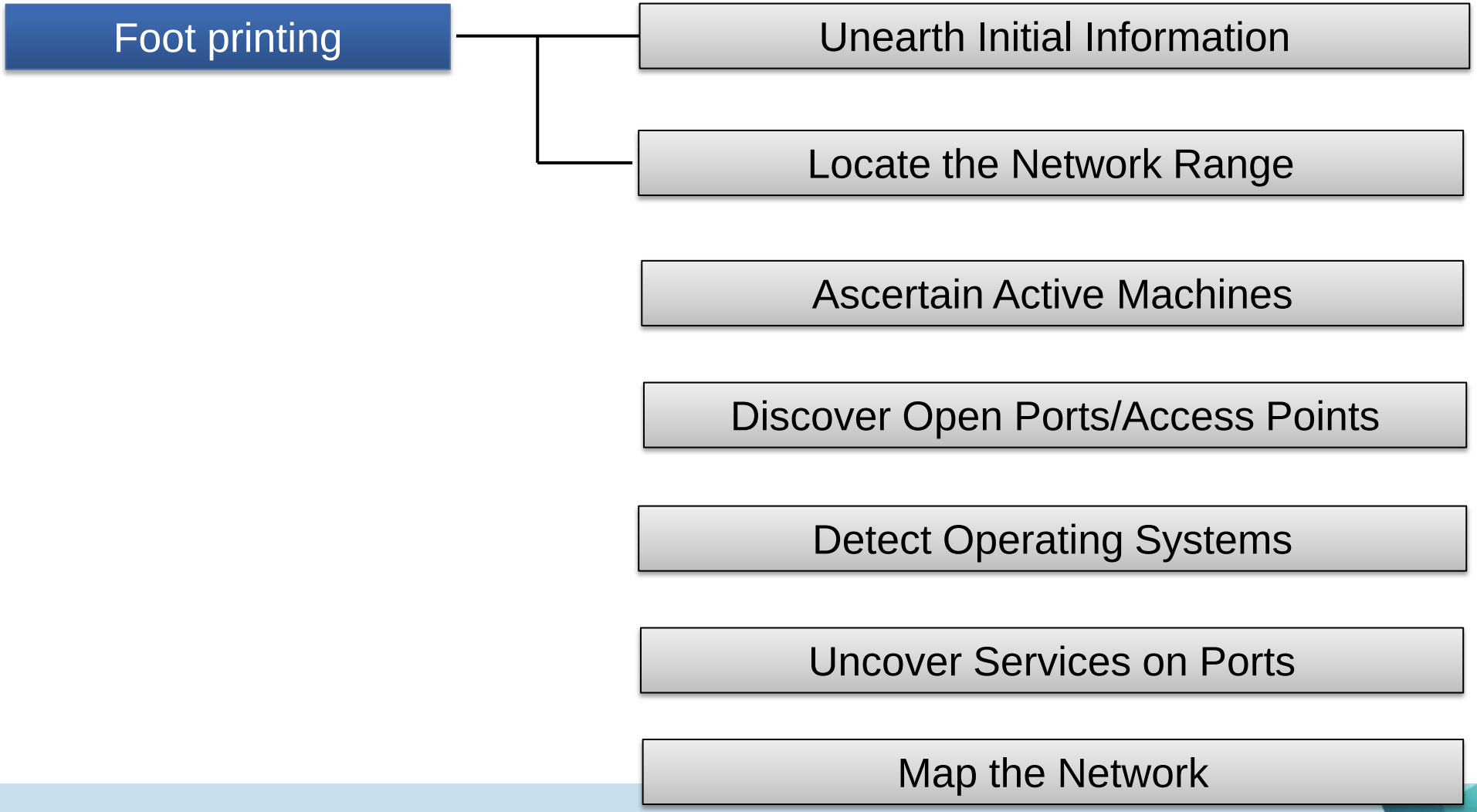
Config files, registry

zap, rootkits

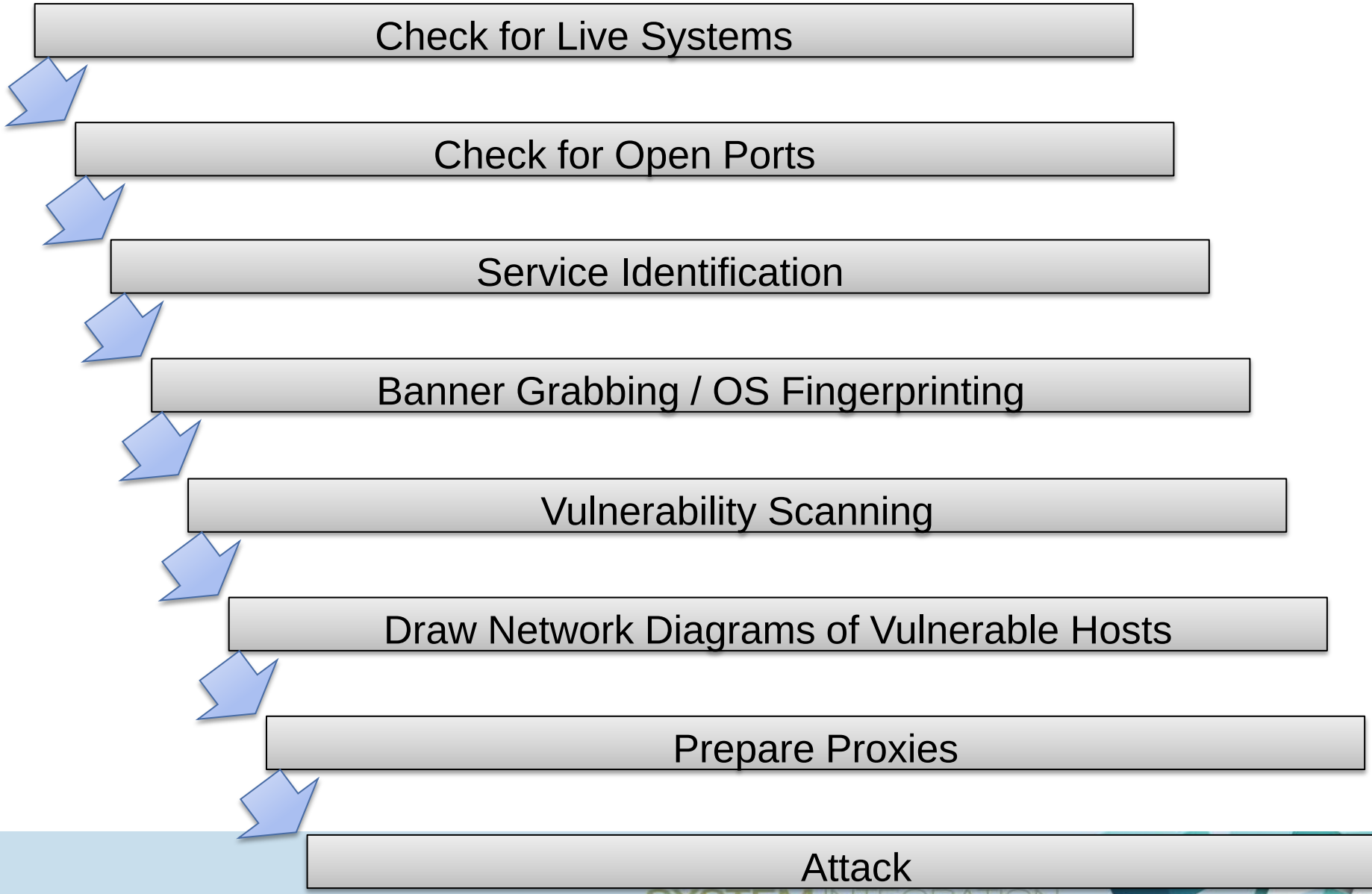
Cron,at, startup folder
netcat, keystroke logger
remote desktop

Synk4, ping of death
tfn/stacheldraht

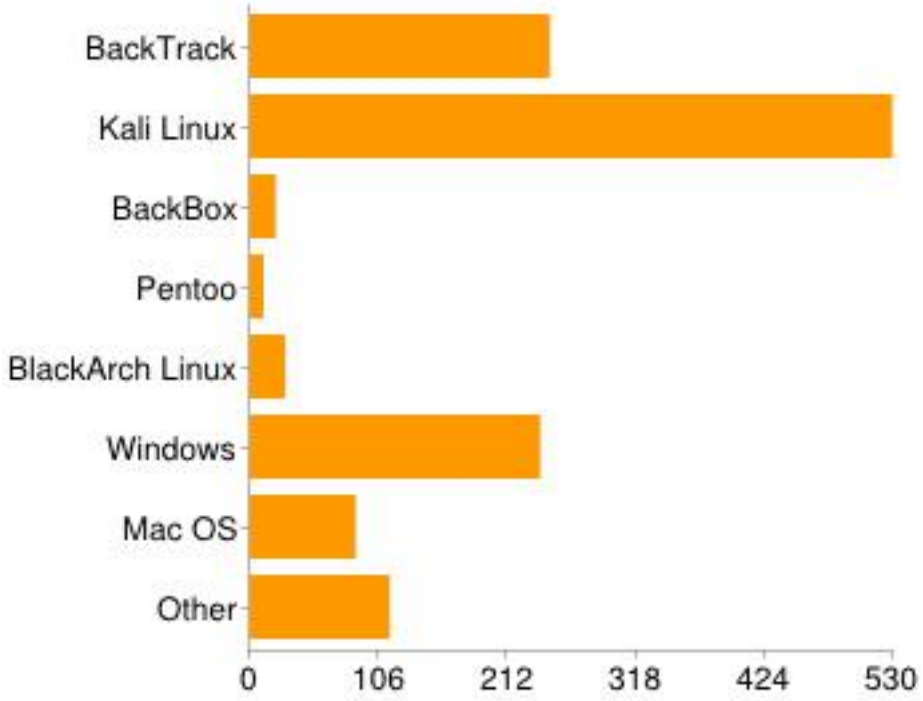
Information-Gathering Methodology



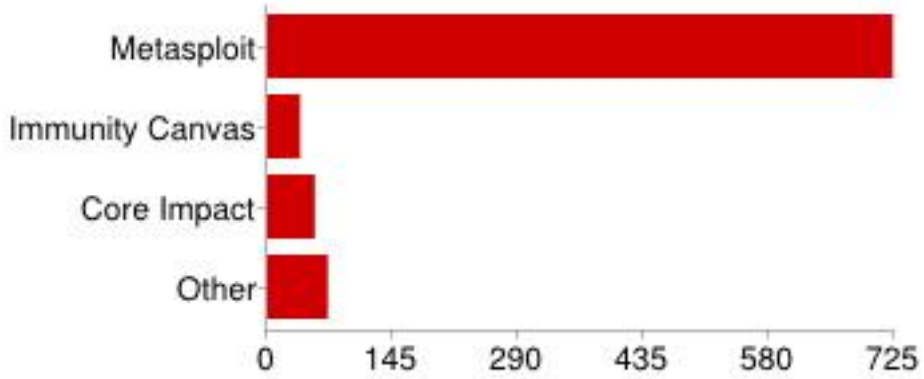
Scanning Methodology



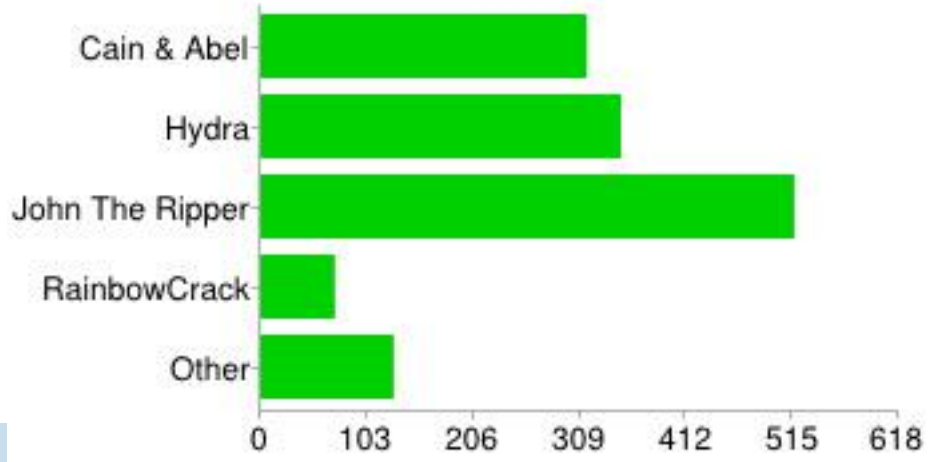
渗透测试时使用的操作系统



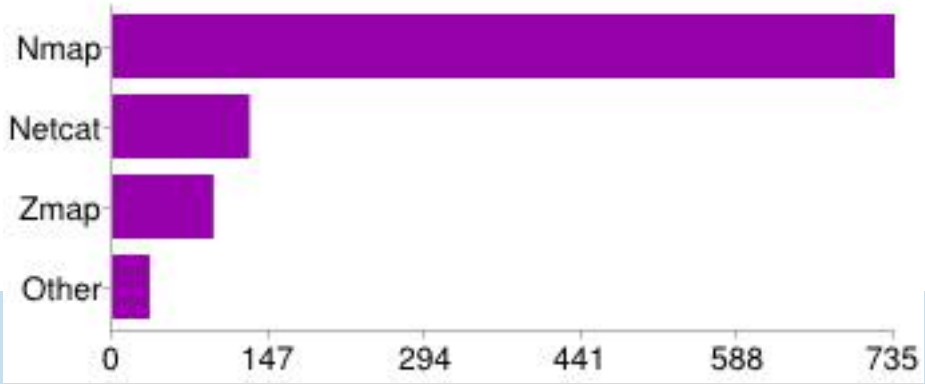
最常使用的渗透测试框架



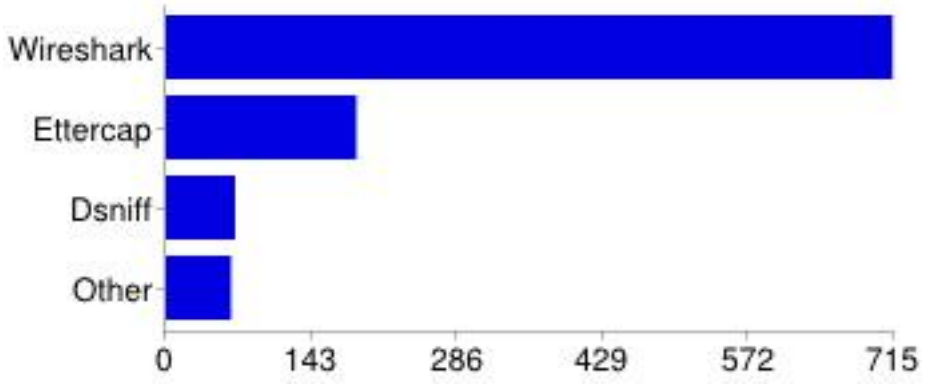
最常使用的密码/网络破解工具



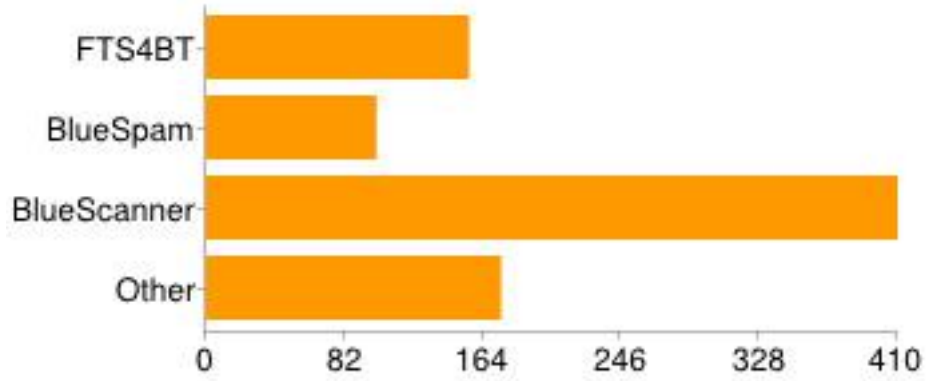
最受欢迎的网络扫描工具



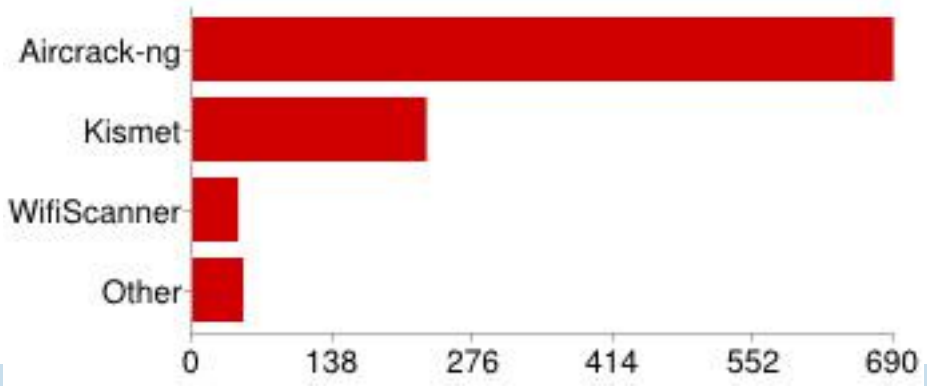
最受欢迎的嗅探工具



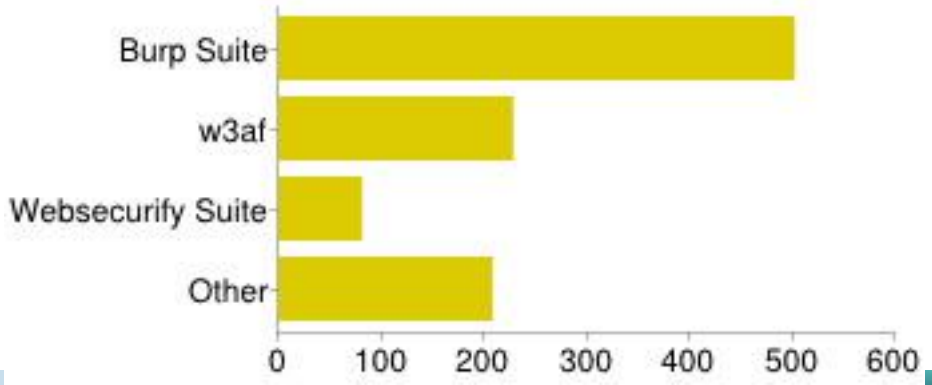
最受欢迎的蓝牙测试工具



最受欢迎的无线测试工具



最受欢迎的Web应用/网站专业扫描工具



DDoS攻擊工具隨手可得

No.	DDOS Tool	Protocol	DDOS Attack Type – FLOOD
1.	Tribe Flood network (TFN)	ICMP, TCP, UDP	ICMP Flood, smurf, UDP Flood, SYN flood
2.	TFN2K	ICMP, TCP, UDP	ICMP Flood, smurf, UDP Flood, SYN flood. Mixed attack, ARGA3 attack
3.	Tirinity v3	TCP, UDP	UDP flood, SYN flood, RST flood, randomflag flood, fragment flood, ACK flood, Establish flood, Null flood
4.	Hping	ICMP/UDP/SYN	flood
5.	Scapy	UDP, TCP	UDP flood, ICMP flood, TCP flood
6.	Phpdos	TCP	http flood
7.	Twbooter	udp	UDP flood
8.	gray pigeon	any	Flood to any protocol
9.	dark comet	tcp, udp	SYN flood, UDP flood, HTTP flood
10.	mp-ddoser	udp, tcp	SYN flood, UDP flood, HTTP flood
11.	fg power ddoser	udp	UDP flood
12.	silent ddoser	udp, tcp	SYN flood, UDP flood, HTTP flood
13.	alevolent ddoser	udp	UDP flood
14.	Ruskill	TCP, icmp	ICMP flood, HTTP flood
15.	DirtJumper (September)	TCP, ICMP	ICMP flood, Get & PUT flood
16.	Unnamed	TCP	VOIP flood
17.	Unnamed	TCP	IP fragmentation flood

Timeout or Session 狀態改變濫用之非對稱攻擊

No.	DDOS Tool	Protocol	DDOS Attack Type – Timeout, State change
1.	HOIC	TCP	SLOW GET, SLOW POST
2.	THC SSL DoS	TCP	SSL renegotiation
3.	Dedal	tcp	SLOW GET
4.	Simple Slowloris	TCP	Slowloris – incomplete header
5.	Unnamed	TCP	SlowRead
6.	Darkshell	udp, tcp, icmp	SYN, HTTP idle timeout congestions
7.	RUDY	TCP	Slow Post, Long Form Field Submission
8.	Tor Hammer	TCP	Slow Post
9.	Slowhttptest	TCP	Slowloris, Slow Post, Slow Read

現實案例 2014 Feb.

歐洲遭遇史上最大DDoS攻擊，尖峰攻擊流量達400Gbps

去年遭受阻斷式服務攻擊的Spamhaus也是CloudFlare的客戶，當時攻擊的尖峰流量為300Gbps，差點癱瘓歐洲網路。這次攻擊流量約400Gbps以上，且影響最大的地區在歐洲。不過媒體引用一家法國代管業者表示，攻擊峰值為350Gbps。

文/ 陳曉莉 | 2014-02-12 發表

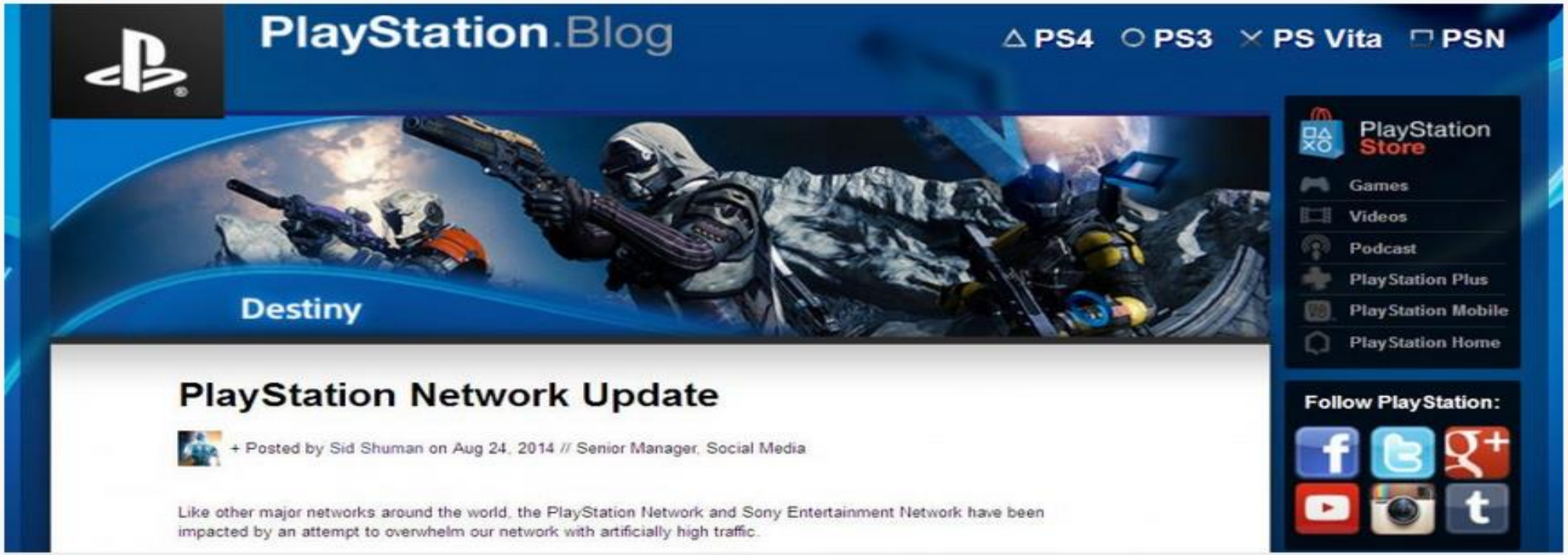
讚 7,084 按讚加入iThome粉絲團 讚 分享 10 g+1 17

現實案例 2014 Aug.

Sony PlayStation Network 遭DDoS攻擊掛點

Sony　周日證實，旗下Sony Entertainment Network 與 PlayStation Network 遊戲服務受到巨大的人為流量攻擊所影響，導致網路一度無法運作，但駭客並無存取任何個人資料。目前網站已恢復運作。

文/ 陳曉莉 | 2014-08-25 發表



Sony 發表聲明指出，人為的龐大流量影響使用者存取SEN及PSN的網路與服務。

現實案例 2014 Aug.

Blizzard's BattleNet battered by DDoS attacks

24 Aug 2014 by Peter Parrish

22 914 1 0

It's not a great evening to be trying to play Blizzard titles, as BattleNet games like *Diablo 3* and *World of Warcraft* are the latest to succumb to DDoS (Denial of Service) barrages. Several major games have been affected over the past few days, **including** *League of Legends* and *Guild Wars 2*.

The *World of Warcraft* forums acknowledge and awareness of current **connection issues**, and says Blizzard is working to resolve them "as soon as possible." Likewise, there's a lengthy thread (one of **several**) over at the *Diablo 3* forums **discussing** the status of the servers.

現實案例 2014 Jun.

香港公投網站DDoS攻擊內幕大公開，連Google、亞馬遜都擋不住

一開始投票，PopVote線上投票網站
Amazon或Google網路服務支援都擋
票過程。

Matthew Prince表示，後來，PopVote網站為了方便更多人投票，宣布投票時間由原訂6月20日起3天，延長為10天，截至29日結束，這段期間接連發生了多起大規模DDoS攻擊，從投票當天起就遭受攻擊，一直持續到投票結果出爐後的1小時才停止。其攻擊手法之複雜，Matthew Prince甚至稱之為一種Kitchen Sink Attack（用盡一切可能手段的攻擊），包括出現了大量DNS反射及NTP反射攻擊封包，對PopVote進行癱瘓攻擊，DNS反射攻擊流量每秒超過100Gb，而NTP反射攻擊流量甚至更高達每秒300Gb，當中也有許多攻擊流量來自臺灣被操控的殭屍電腦，另外還出現了以攻擊網路第四層為主的SYN Flood洪水攻擊，駭客利用殭屍電腦發送大量偽造的TCP連接請求，SYN封包傳送每秒鐘高達1億次，就連CloudFlare服務器也因此而無法承受住。

此外，駭客也發動了網路第七層應用層攻擊，包括如HTTP洪水攻擊、HTTPS加密服務攻擊等，還出現了新興的DNS Flood洪水攻擊，這也是許多網路目前最害怕的DDoS攻擊。PopVote網站遭遇到了每秒高達2億5千萬次的有效DNS請求，甚至未經放大，DNS請求就有高達每秒128 Gb的網路流量，棘手的程度，Matthew Prince甚至以Scary（可怕)來形容它。

DDOS 緩解

- 雲端智慧IP信譽資料庫 BAD IP
- 門檻值設定
- 行為分析
- Web Container timeout設定
- Set cookie
- HTTP redirect
- CAPCHA
- 站台程式改寫
- 軟體工具 - URLscan

F5 Advantage

DDoS MITIGATION

Increasing difficulty of attack detection

OSI stack	Physical (1)	Data Link (2)	Network (3)	Transport (4)	Session (5)	Presentation (6)	Application (7)	OSI stack

F5 mitigation technologies

Network attacks

SYN Flood, Connection Flood, UDP Flood, Push and ACK Floods, Teardrop, ICMP Floods, Ping Floods and Smurf Attacks

BIG-IP AFM
SynCheck, default-deny posture, high-capacity connection table, full-proxy traffic visibility, rate-limiting, strict TCP forwarding.

Packet Velocity Accelerator (PVA) is a purpose-built, customized hardware solution that increases scale by an order of magnitude above software-only solutions.

Session attacks

DNS UDP Floods, DNS Query Floods, DNS NXDOMAIN Floods, SSL Floods, SSL Renegotiation

BIG-IP LTM and GTM
High-scale performance, DNS Express, SSL termination, iRules, SSL renegotiation validation

Application attacks

OWASP Top 10 (SQL Injection, XSS, CSRF, etc.), Slowloris, Slow Post, HashDos, GET Floods

BIG-IP ASM
Positive and negative policy reinforcement, iRules, full proxy for HTTP, server performance anomaly detection

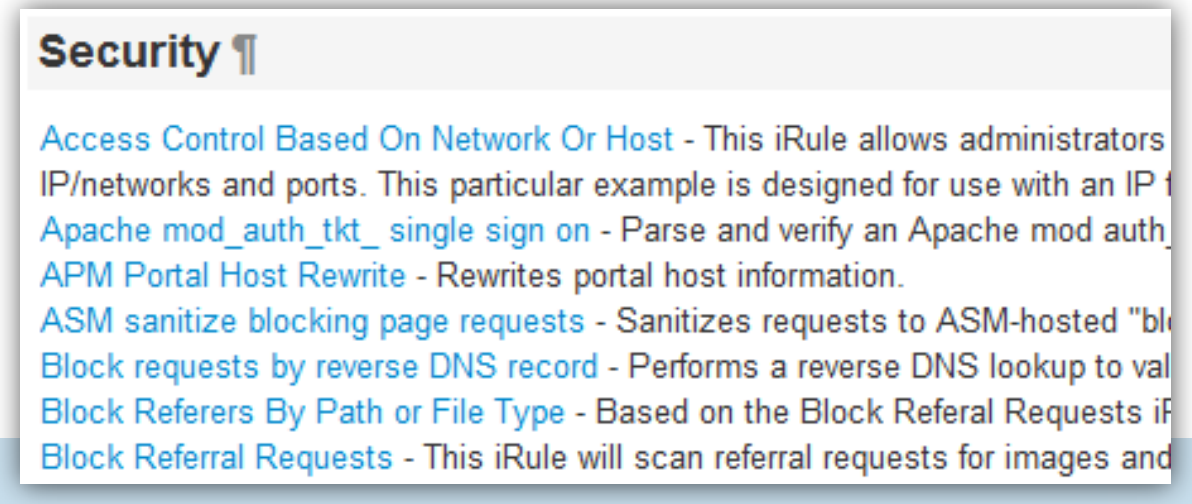
F5 Mitigation Technologies

- Protect against DDoS at all layers
- Withstand the largest attacks
- Gain visibility and detection of SSL encrypted attacks

對應關係矩陣

OSI 层级	攻击内容	LTM	LTM+ iRule	IP Intel	DNS	ASM
Network Based (2-4层)	IP Fragment					
	Tear Drop					
	SYN Flood (Dirt Jumper)					
	TCP (connection) Flood e.g. SYN-ACK, ACK & PUSH-ACK, RST or FIN and Fragmented ACK					
	Christmas Tree					
	Fake Session					
	LAND					
	Redirect Traffic Attack					
	ICMP Flood, Ping Floods and SMURF Attacks					
	Ping of Death ICMP					
DNS based (4层)	UDP Flood					
	UDP Fragment					
	DNS Flood (Distributed and DNS Blacklisting) e.g. DNS UDP Flood, DNS Query Flood and DNS NXDOMAIN Flood		IP Blacklist (Datagrp)		DNS Express + DNS iRule	
SSL/TLS based (5–6层)	SSL Floods, Malformed SSL (e.g. empty SSL HELLO)					
	SSL THC attack (Extending from SSL Renegotiation vulnerability)			IPintel iRule		
Application based (6–7层)	Slowloris (Nuclear DDoSer, Slowhttptest)					
	Keep-Dead					
	Slow POST (R-U-Dead-Yet, Tor Hammer, Nuclear DDoSer, Slowhttptest)					
	HashDoS					
	Apache Killer (Slowhttptest)					
	HTTP GET Flood, Recursive GET Flood (Web Scraping), Dirt Jumper (HTTP Flood)			IP intel iRule		
	#RefRef (exploit SQLi - OWASP Top 10 vulnerability as entry)					
	XML “Bomb” (DTD attack), XML External Entity DoS					

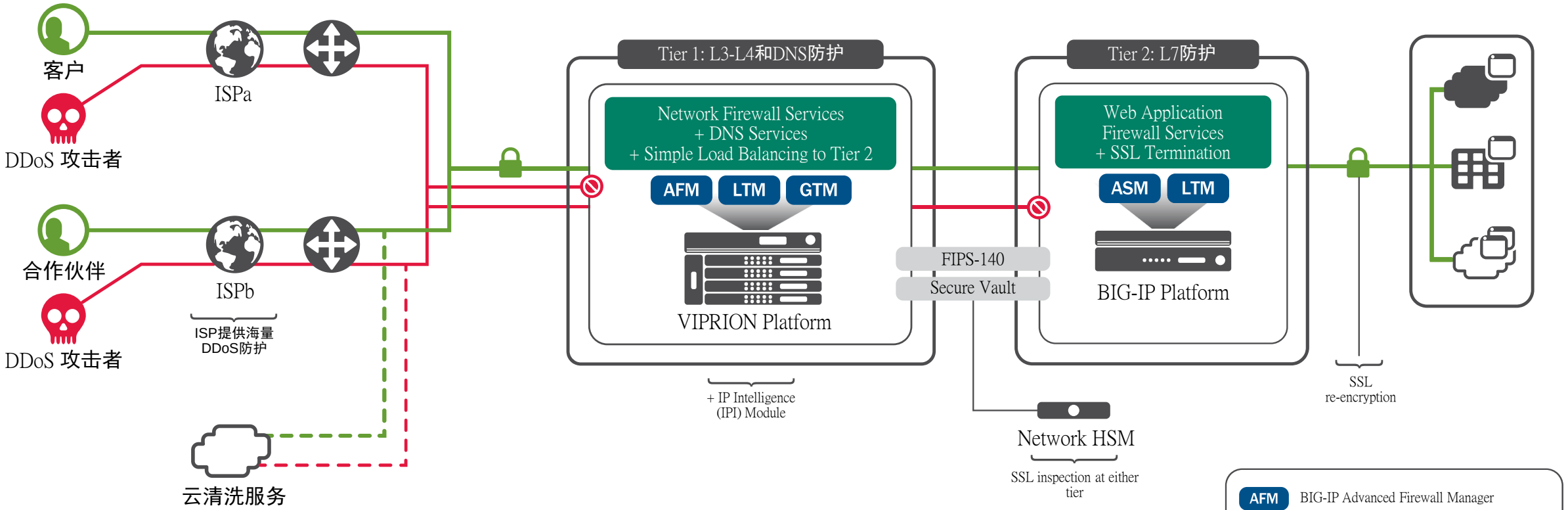
Fire Point of F5 Security



Emergency Response by iRules

1. DDoS
2. DNS
3. Access Control
4. SSL
5. Cookie
6. URL/URI
7. Client Certificate
8. CAPTCHA
9. Session
10. Slow Post
11. SQL Injection
12. Phishing

大型金融機構數據中心佈署



Accident 2

Korea National Intelligence Service(NIS) Cyber Attack 2013-06-26

etnews.com 전자신문 **Korea IT News**

NEWS | INTERNET | COMMUNICATION | COMPUTING | POLICY | ELECTRONICS | DEVICE &

Search

DMB,LCD,Samsung

GO

The Electronic Times Online Advertisement info

전자신문

전문가 번역 Pro Translation Service Go

Refund Help 환불문의

Internet

Home > Internet > Article

EMAIL PRINT KOREAN TEXT

[June 25 Cyber Terror] Blue House Urgently Responds

2013/06/26 By Kwon Sang-hee

At about 9:30 a.m. on the 25th, the Blue House website was hacked by a group presumed to be from North Korea, and its pages were painted with phrases including 'Great Leader Jeong-Eun Kim' all over the their upper sides.

Phrases posted on the Blue House webpages included "Hale to General Jeong-Eun Kim, the Unification President!," "The attack will continue until our demand is met. Wait for us. Greet us," "We Are Anonymous. We Are Legion. We Do Not Forgive. We Do Not Forget. Expect Us," and "#Anonymous Korea, aiming at democracy and unification," together with a picture of President Park in a meeting.

The Blue House immediately closed down its website after confirming that it had been hacked and started the restoration of website and the investigation to identify the suspects.

A Blue House person stated that the website had been restored at

```
when HTTP_REQUEST {
        set userhost [HTTP::host]
        if { [HTTP::cookie exists f5korealab] } {
                if { [HTTP::cookie value f5korealab] equals "mall" } {
                        pool Mall_Pool
                } else { HTTP::redirect "http://$userhost" }
        } else {
                set location "[HTTP::host][HTTP::uri]"
                set message1 "123"
                HTTP::respond 200 content "
                <html><head></head><body>
                <script type=₩"text/javascript₩">
                                                                        functi
on sleep(ms) {

   var dt = new Date();

   dt.setTime(dt.getTime() + ms);

   while (new Date().getTime() < dt.getTime());
                                                                        }
                                                                        functi
on redirect() {

            var today = new Date();

            today.setDate(today.getDate() + 1);
                document.cookie = ₩"f5korealab=mall; path=/₩;
expires=₩" + today.toGMTString() + ₩"; domain=$userhost₩"
                window.location=₩"http://$location₩";
```


Thanks you for your attention!