

臺灣大學計資中心網路組 北區學術資訊安全維運中心 資訊安全分析報告

Ð

資訊

DNS amplification attack 分析報告

NTU-ASOC

術資

北區 ASOC 團隊製

2013/11

1.	DNS 簡介3
2.	DNS amplification attack(放大攻擊)簡介4
3.	DNS amplification attack 分析說明8
4.	DNS amplification attack 解決方案11
	4.1 Windows DNS
	(ref:http://technet.microsoft.com/zh-tw/library/cc731367.aspx)11
	4.2 Linux DNS
	路のしの幕
	報
	VTU-ASOC

1. DNS 簡介

在早期 TCP/IP 協定的網路環境中,兩台主機間若要進行通訊,則 必須

先知道對方的 IP 位址,才能開始網路通訊,而人們對於純數字的 IP 格 式資料的記憶並不在行,DNS 服務就是為了解決這問題而生,DNS 全名為 Domain Name Service,主要的用途在於將一般人易於記憶的網址轉換成 電腦所使用的 IP 格式,而 DNS 其實沒有想像中的遙遠,當打開瀏覽器鍵入 網址連上網時,其實已經在使用 DNS 的服務了。



DNS 系統基本是採樹狀階層式(hierarchy)、類似 Windows 中的 目錄樹結構、最頂層的有數十個 root DNS servers、記錄著所有最頂層 DNS server 資料、稱為"root"或根目錄,接著下分為幾個基本的類別、如:com、 org、edu。因網際網路的蓬勃發展,在此層級,也加入國別代號,如 tw(台 灣)、hk(香港)、jp(日本)、而美國則是因為當初發展制定 Internet 規範,則 沒有國域名稱,再往下便是組織名稱,如 google、facebook、yahoo...等 等,繼組織名稱後,便是主機名稱,如 www、mail、ftp...等等,所以一個 完整的 dns 名稱就會像是: www(主機名稱).google(組織名稱).com(國別代號因美國而省略)。

2. DNS amplification attack(放大攻擊)簡介



server

發出偽造的 DNS query 封包·偽造成受害者的 IP 位

址為來源位址進行遞迴查詢(recursive query)。

Step 3: 受害的 DNS 主機向根目錄 Server 進行 domain

查

詢。 Step 4: 根目錄主機向受害 DNS 主機回傳查詢無此 domain 的 訊息,並回傳另一根伺服器可能有其 domain 資料。 Step 5: 受害 DNS 主機轉向另一根目錄 Server 進行 domain 查 韵。 Step 6: 外部根目錄 Server 回傳知道此 domain 資料的 DNS server 位址。 Step 7:受害 DNS 主機再度向此 DNS 發出查詢。 U-AS Step 8:外部 DNS 回傳受害 DNS 主機 domain 查詢資 料。 Step 9: 受害 DNS 主機向遭偽造來源的主機回傳 domain 查詢

攻擊者透過不斷重複上述步驟,向目標主機發送大量 UDP 封包,

資料。

藉此阻斷其正常服務,也由於受害 DNS 主機回傳到目標主機之封包大 小會大於殭屍電腦群所發送的封包大小,過程中流量具有放大的效果, 故稱其為 DNS 放大攻擊。

2013 年三月歐洲反垃圾郵件組織 Spamhaus 即是遭此 DDoS 攻

撃·攻擊流量高達 300Gbps·成為目前為止最嚴重的一次 DDoS 攻擊。



參考上圖可了解此種攻擊模式下的放大效果,約可從 32byte(*殭屍電腦 群發出*)放大至 3296byte(*DNS 主機回傳給受害主機*),攻擊頻寬約可被放大 100 倍左右,當殭屍電腦群發出大量的 DNS query 封包時,甚至會導致封包在 router 轉送時出現壅塞,進而產生更大規模的影響,所以 DNS 主機安全性 設定,已成為不可忽視的重要課題之一。





3. DNS amplification attack 分析說明

北區 ASOC 透過 IPS 即時監測各區網中心是否有 DNS 放大攻 擊事件,偵測基本架構可參考上圖,透過於網路骨幹中的 IPS,同時檢測 Inbound 及 Outbound 的流量,一旦有外部攻擊者發出偽造來源的惡意 DNS 封包或內部 DNS 主機發出異常 query 封包時,皆可被 IPS 偵測到, 避免 DDoS 攻擊之情事發生,在此種偵測模式下,我們可以確保轄下連線 單位內的 DNS 不被外部惡意攻擊者所利用,同時,也能確保內部不受到此 種攻擊模式危害,在大規模攻擊情事發生前,亦能提早發出告警,避免攻擊 進一步擴大而影響整體網路環境。



經過 Arcsight 收容前端 IPS 資料後,進行後續的關聯分析, 產出如上攻擊拓撲圖,可了解此種攻擊行為的模式及其關連性。其中紅色方 形代表攻擊發動者,藍色圓形表示攻擊事件類型,而白色方形代表攻擊目的 端主機,圖形的大小代表攻擊量的多寡,綜合以上資訊,可以發現 DNS 放 大攻擊模式具有多攻擊來源、單一目標、及龐大數量等特性。在此模式下, 目標主機若沒有相關防護措施,網路環境很容易被攻擊造成網路癱瘓。

lo.	Time	 Source 	Destination	Protocol	Length	Info	
	40 2013-11-0	9 23:31:17.133235		DNS	85	Standard	query
	43 2013-11-0	9 23:31:17.150343		DNS	892	Standard	query
(III			
Ŧ	2						
Ľ	sand1a.gov	: type ANY, class IN					
- f	Ariswer's	type PRETC class TN					
- 1	E sandia gov	type RRSIG, Class IN					
1	E sandia gov	type A class IN addr 12	175 81 4				
	E sandia gov	type A, Class IN, audi 15					
	Sandia gov	type TYT class IN					
	E sandia gov	type PRTC class IN					
	E sandia. gov	type DNSKEY class IN					
	E sandia. gov	type DNSKEY, class IN					
	E sandia. gov	type DNSKEY, class IN					
	E sandia. gov	type DNSKEY, class IN					
	sandia. gov	type RRSIG, class IN					
	E sandia.gov	type RRSIG, class IN					
	sandia.gov	: type RRSIG, class IN					
	sandia.gov sandia.gov s	: type SOA, class IN, mname	taurus.sandia.gov				
	sandia.gov sandia.gov s	: type RRSIG, class IN					
	sandia.gov sandia.gov s	: type DS, class IN					
	🗄 sandia.gov	: type DS, class IN					
	🗄 sandia.gov	: type DS, class IN					
	🗄 sandia.gov	: type DS, class IN					
	🗄 sandia.gov	: type NS, class IN, ns ns8.	sandia.gov				
1	🗄 sandia.gov	: type NS, class IN, ns ns2.	ca.sandia.gov				
	🗄 sandia.gov	: type NS, class IN, ns ns9.	sandia.gov				
	🗄 sandia.gov	: type NS, class IN, ns ns1.	ca.sandia.gov				

檢視 IPS 所偵測到的事件封包如上圖所示·可發現具有明確的

攻擊特徵·攻擊者偽造來源後·並針對特定 domain 發送大量 query 封包·

正常使用者不應發出如此頻繁的 DNS query · 且查詢的 Domain name 皆

U-AS

為"sandia.gov" ·明顯為異常行為的 DNS 放大攻擊。

4. DNS amplification attack 解決方案

4.1 Windows DNS (ref: http://technet.microsoft.com/zh-tw/library/cc731367.aspx)

為避免 DNS 主機被利用為攻擊的跳板,建議 DNS 設定須符 合下列兩項安全性設定:

• 設定 ACL,僅允許符合 ACL 設定的網段進行 recursive query 或關閉 recursive query



關閉 recursive query

1. 開啟 [DNS 管理員]。

2. 在主控台樹狀目錄的適當 DNS 伺服器上按一下滑 鼠右鍵,然後按一下 [內容]。

位置

DNS/適用的 DNS 伺服器

3. 按一下 [進階] 索引標籤。

4. 在 [伺服器選項]中,選取 [停用遞迴] 核取方塊,然

後按一下 [確定]。



以各 Windows 版本作業系統實作為例:

Windows 2012

1.開啟 DNS Manager



Å	DNS Manager	- 5	•	x
File Action V	/iew Help			
🗢 🔿 🔁 📅				
DNS	2 Name			
▲ WIN-V156	Configure a DNS Server			
⊳ 🛄 Fc	New Zone			
⊳ 🧰 Re	Set Aging/Scavenging for All Zones			
	Scavenge Stale Resource Records			
	Update Server Data Files			
	Lear Cache			
	View			
	Delete			
	Refresh			
	Export List 3			
	Properties			
	Help			
	·			
Opens the properti	ies dialog box for the current selection.			
4.,	選擇"介面"標籤頁。			
┎ 昶 十里 /	第右下利 ID 可以海绵			
1 4++ 3++ 1+				
3.迭挥信				
5.選擇 6.勾選兌	论許連線之介面			
5.選择種 6.勾選分	论許連線之介面 DNS Manager	_ =		x
5.迭译唱 6.勾選分	む許連線之介面 DNS Manager Tiew Help WIN-V156F3EG346 Properties ? ×		-	x
5.选择管 6.勾選外 File Action V	む許連線之介面 DNS Manager fiew Help WIN-V156F3FG346 Properties ? ×	_ []	x
5.迭评唱 6.勾選介 File Action V	む許連線之介面 DNS Manager Tiew Help WIN-V156F3FG346 Properties ? ×	_ C	3	x
5.迭评唱 6.勾選分 File Action V ◆ ● ▲ 配 DNS ▲ WIN-V156f	た許連線之介面 DNS Manager Tiew Help WIN-V156F3FG346 Properties ? × ① Debug Logging Event Logging Monitoring Interfaces Forwarders Advanced Root Hints	_ C	3	x
5.迭译译 6.勾選5 File Action V ◆ ● ▲ 配 DNS ▲ ① WIN-V1566 ▶ 圖 Global	た許連線之介面 DNS Manager fiew Help WIN-V156F3FG346 Properties ? × 1 Debug Logging Event Logging Monitoring 1 Interfaces Forwarders Advanced Root Hints F3FG346 Logs Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or	- 5	3	×
5.迭评译 6.勾選介 File Action V ◆ ● ② 証 DNS ▲ ① WIN-V156f ▷ @ Global ▷ ③ Forwar	DNS Manager Tiew Help WIN-V156F3FG346 Properties ? × Debug Logging Event Logging Monitoring Terfaces Forwarders Advanced Root Hints F3FG346 Logs d Lookup Zo a Lookup Zo	_ C	-	×
5. 迭7年目 6. 勾選分 File Action V ◆ ● ② II ◎ DNS △ ③ WIN-V1566 ▷ 圖 Global ▷ 圖 Forwar ▷ 圖 Reverse ▷ 圖 Trust P	た許連線之介面 DNS Manager Tiew Help WIN-V156F3FG346 Properties ? エ	_ C	3	×
5.迭评译 6.勾選外 File Action V ◆ ● ② ① ③ DNS ▲ ③ WIN-V156f ▷ ③ Global ▷ ③ Forwar ▷ ③ Reverse ▷ ③ Trust P ▷ ③ Condit	た許連線之介面 DNS Manager Tiew Help WIN-V156F3FG346 Properties ? エ Debug Logging Event Logging Monitoring Interfaces Forwarders Advanced Root Hints Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses. Listen on: ional Forward 5 All IP addresses	_ C		×
5.迭评译 6.勾選外 File Action V ● ● ② 証 DNS ▲ ③ WIN-V156f ▷ 圖 Global ▷ ③ Forwar ▷ ③ Reverse ▷ ③ Trust P ▷ ③ Condit	た許連線之介面 DNS Manager Tiew Help WIN-V156F3FG346 Properties ? × Debug Logging Event Logging Monitoring Interfaces Forwarders Advanced Root Hints F3FG346 Logs d Lookup Zor a Lookup Zor ioints ional Forward On Hints Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses. Listen on: ioints Only the following IP addresses:	_ E	-	×
5. 迭7 律 [6. 勾選介 File Action V ● ● ② 〒 DNS ▲ WIN-V156f ▷ 圖 Global ▷ ■ Forwar ▷ ■ Reverse ▷ ■ Trust P ▷ ■ Condit	た許連線之介面 DNS Manager New Help New Help New Help Debug Logging Event Logging Monitoring Interfaces Forwarders Advanced Root Hints F3FG346 Logs d Lookup Zot a Lookup Zot isten for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses. Listen on: ional Forward Only the following IP addresses: IP addresse: IP addresse:	_ [x
5. 迭 择 僅 6. 勾選分 File Action V ◆ ● ② ① ③ DNS ▲ ③ WIN-V1566 ▷ ③ Global ▷ ③ Forwar ▷ ③ Reverse ▷ ③ Trust P ▷ ③ Condit	む許連線之介面 DNS Manager Fiew Help Fiew Help Tew Help Debug Logging Event Logging Monitoring Interfaces Forwarders Advanced Root Hints Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses. Listen on: Listen on: Only the following IP addresses: F addresse: Dimensional Forward Debug Logging DNS Manager DNS Manager Paddresses Dimensional Forward DNS Manager DNS Manager DNS Manager DNS Manager Paddresses Dimensional Forward DNS Manager DNS Man			x
5.迭评唱 6.勾選外 File Action V ◆ ● ② ☑ DNS ▲ ③ WIN-V156f ▷ ③ Global ▷ ③ Global ▷ ③ Forwar ▷ ③ Reverse ▷ ③ Trust P ▷ ③ Condit	む許連線之介面 DNS Manager Fiew Help Fiew Help Debug Logging Event Logging Monitoring Interfaces Forwarders Advanced Root Hints Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses. Listen on: ional Forward All IP addresses Dolly the following IP addresses: IP addresse Dolly the following IP addresses: IP addresse Dolly the following IP addresses Dolly the following IP addresses Forwarders Advanced Advanced Computer Debug Logging			×
5.迭评唱 6.勾選允 File Action V ◆ ● ② 配 ③ DNS ▲ ③ WIN-V156f ▷ ③ Global ▷ ③ Global ▷ ③ Reverse ▷ ③ Trust P ▷ ③ Condit	Addresses Control Co			x
5. 迭 择 僅 6. 勾選允 File Action V ● ● ② □ ONS ● ③ Global ▷ ③ Forwar ▷ ③ Reversa ▷ ③ Trust P ▷ ③ Condit	Adtraction Adtraction DNS Manager Tiew Help Tiew Help TestFG346 Logs d Lookup Zot e Look		2	×
5. 迭 择 僅 6. 勾選分 File Action V ◆ ● ② ① ③ DNS ▲ ③ WIN-V1566 ▷ ③ Global ▷ ③ Forwar ▷ ③ Trust P ▷ ③ Trust P ▷ ③ Condit	Addresses Addresses Advanced Root Hins F3FG346 Logs d Lookup Zog isonal Forward 0 Only the following IP addresses: Isten on: 0 Only the following IP addresses: I Debug Logging Event Logging Monitoring Interfaces Forwarders Advanced Root Hints Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses. Listen on: 0 Only the following IP addresses: IP addresse: IP addresse: IP addresse: IP addresse: I for D11288:1000:1:118f:4261:a13:6cfd I fe80::118f:4261:a13:6cfd I fe9.254.108.253			×
5. 迭 择 僅 6. 勾選分 File Action V ◆ ● ② ② ③ ③ DNS △ ③ WIN-V156f ▷ ③ Global ▷ ③ Global ▷ ③ Reverse ▷ ③ Trust P ▷ ③ Condit	Addresses Addresses Tew Help Tew Help Tew Help Tew Help Tew Help Tew Help Terfaces Terfaces Terfaces Terwarders Advanced Tevent Logging Tevent Logging Tevent Logging Monitoring Interfaces Forwarders Advanced Root Hints Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses. Listen on: Terfaces Only the following IP addresses: IP addresses Distantional Forward Only the following IP addresses: IP addresses Distantion Terfaces Distantion Terfaces Distantion Dist			×
5.选择管 6.勾選外 File Action V ◆ ● ② ① ③ DNS ▲ ③ WIN-V156f ▷ ③ Global ▷ ③ Forwar ▷ ③ Reverse ▷ ③ Trust P ▷ ③ Condit	Add Debug Logging Event Logging Monitoring Tiew Help VIN-V156F3FG346 Properties 2 × Debug Logging Event Logging Monitoring Thterfaces Forwarders Advanced Root Hints Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses. Listen on: Solonity Following IP addresses: P addresses D only the following IP addresses D on			×
5.迭评唱 6.勾選允 File Action V ● ● ② 匝 ◎ DNS ▲ ③ WIN-V156f ▷ ⓓ Global ▷ ᠃ Forwar ▷ ᠃ Reversa ▷ ᠃ Trust P ▷ ○ Condit	Ad#建線之介面 Interfaces Person and a content of the provided and a content of the provided and a content of the provided and			×
5. 迭 择 僅 6. 勾選分 File Action V ◆ ● ② ② ③ DNS ④ ③ WIN-V156f ▷ ③ Global ▷ ③ Reverse ▷ ③ Trust P ▷ ③ Condit	Add Decision of the second o			×
5. 迭 择 译 6. 勾選分 File Action V ◆ ● ② ② ③ ③ DNS △ ③ WIN-V156f ▷ ③ Global ▷ ③ Forwar ▷ ③ Reverse ▷ ③ Trust P ▷ ③ Condit	DSY 建棉之介面 Interfaces Forwarders Advanced Root Hints F3FG346 Logs d Lookup Zo Lookup Zo Lookup Zo Lookup Zo Lookup Zo Lookup Zo Listen on: 1 All P addresses 2 Only the following IP addresses defined for this computer, or juints 1 Only the following IP addresses: 1 P addresse 2 Only the following IP addresses: 1 P addresse 3 Only the following IP addresses: 1 P addresse 4 Only the following IP addresses 5 Only the following IP addresses 6 Only the following IP addresses 7 Only the following IP addresses 9 Only the following IP addresses 1 Only the following IP addresses 2 Only the following IP addresses 2 Only the following IP addresses 2 Only the following IP addresses 3 Only the following IP addresses 4 Only the following IP addresses 4 Only the following IP addresses 5 Only the following			×

7.選擇" 進階" 標籤頁 8.勾選**停用遞迴**查詢選項 9.選取" **套用**"





2.選取 DNS 伺服器後,點選右鍵>內容



7.勾選"停用遞迴"

8.選擇" 套用"



2. 關閉遞迴查詢

🚾 条統管理員: 命令提示字元

C:\Users\Administrator\dnscmd 163.28.16.52 /Config /NoRecursion Ø

登錄內容 NoRecursion 已經重設成功。 命令已成功完成。

C:\Users\Administrator>_



Windows 2003

1.執行 DNS 管理員

Insmgmt 1			_ 🗆 🗙
<u>File Action Yiew W</u> indow <u>H</u> el	þ		_ -
→ 🗈 📧 🗙 😭 🕑 🔮	🖬 🗐 💮		
DNS SEAN-98F13F7314 Forward Lookup Zones Reverse Lookup Zones	Configure a DM The Domain Name System network services. DNS is the network services. This DNS server has not be zones and specifying root To configure the DNS server	NS Server (DNS) is a hierarchical naming system used for locating computers and best known for translating friendly DNS domain names to IP addresses ar even configured. Configuration includes creating forward and reverse loo : hints and forwarders. ver, on the Action menu, click Configure a DNS server.	nd
2.選擇 DNS 伺 3.選擇″內容″ ¹ dnsmgmt - [DNS\SEAN-986 ¹ Elle Action View Windd	服器,右鍵>內容 F13F7314] ow Help		-0
	1 2 🖬 🗐 🗊		
SEAN-96F INFORME SEAN-96F INFORME Second Development Rever Scavenge S Update Server Clear Cache Launch nslo All Tasks View New Window Delete Refresh Properties Help	SEAN-98F13F731 . DNS Server	 te a DNS Server System (DNS) is a hierarchical naming system used for locating comput DNS is best known for translating friendly DNS domain names to IP add s not been configured. Configuration includes creating forward and re to groot hints and forwarders. VS server, on the Action menu, click Configure a DNS server. 	ers and resses and verse lookup

4.選擇"介面"標籤頁 5.選擇只有下列IP位址 6.輸入允許連線之IP位址 7.點擊"新增" 8.選擇"**套用**"

-	Debug Loggin	9	Event Logging	1	Monitoring	
4	Interfaces	Forward	lers Advanc	ed	Root Hints	1
Si lis yı Li	elect the IP addr sten for DNS que ou can limit it to sten on:	esses that v ries on all IF selected IP a	vill serve DNS reque 9 addresses defined addresses.	sts. The s for this co	server can omputer, or	
	All IP addr <u>e</u> ss	es				
C	Only the follow	ving IP addr	esses:			
6	IP address:		7			
-	8.8.8	8.8	Add			
	163 28 16 5	4	Demous			
	103/2011010	u 	Kemove			
	1					
					8	
			1	_		
		L	ОК	Cancel	Apply	
		17.		0	///	1
		10	-ASU			
9.選擇″ 3	進階"標籤頁					
10.勾選"	停用 <u>遞迥"</u>					
	去四 //					

EAN-98F13F7314 Properties		? >
Debug Logging Interfaces Forwards Server version number:	E Logging Monito	oring t Hints
5.2 3790 (0xece)		
Server options:		
Disable recursion (also disative provided by the provided	ion	
Name checking:	Multibyte (UTF8)	-
Load zone data on startup:	From Active Directory and regis	try 💌
Enable automatic scavengi	ng of stale records	
Scavenging period:	0 days	T
	Reset to De	fault
		Apply
		B
NTU.	ASOC	

4.2 Linux DNS

為避免 DNS 主機被利用為攻擊的跳板,建議 DNS 設定須符

合下列兩項安全性設定:

- 在 BIND 版本 9.5 之前 · recursion 的功能是預設開啟的 · 故管理者必須自行關閉此功能或設定適當的存取權限 。
 - 以下為 BIND 的組態設定檔 Name.conf 的建議設定

/* 定義一個 ACL,設定能存取 DNS 服務的 IP 範圍,此例 192.168.0.0/16,可自行調整為貴單位的網段*/

 Acl "allowed-IP"{

 192.168.0.0/16;

 };

 /*僅允許符合 ACL

 Options {

 Allow-recursion {

 };

 /*提供貴單位管轄

 zone "XXX.edu.tw

 allow-query { any

/*僅允許符合 ACL 設定的網段進行 recursive query*/ Options { Allow-recursion { allowed-IP; }; }; /*提供貴單位管轄下的網域給其它 DNS 查詢*/ zone "XXX.edu.tw" in { allow-query { any; }; };

而更多詳細的設定步驟可參考:

https://kb.isc.org/category/116/0/10/Software-Prod ucts/BIND9/Documentation/

