Anonymous_DO Exposed

Esto espero sea una lession para otros.....hace exactamente 4 dias era 24 de Diciembre, un dia como cualquier otro en la vidad de los internautas, hackers, programados, pedofilos, crackers, Skids, /b/rothers, etc etc...yo tratando de calmar un poco mi infinito aburrimiento entro a la "red social"[concepto totalmente absurdo]...sin expectativa de nada fuera de lo comun...pero de pronto empezaron a caer meteoritos del cielo, la tierra se abrio y nos empezo a tragar a todos, y vi como satanas tomaba a las personas que alcanzaba y les extraia el alma....

Bueno eso querria yo que pasara..-pero de pronto a wild twitt apears-...

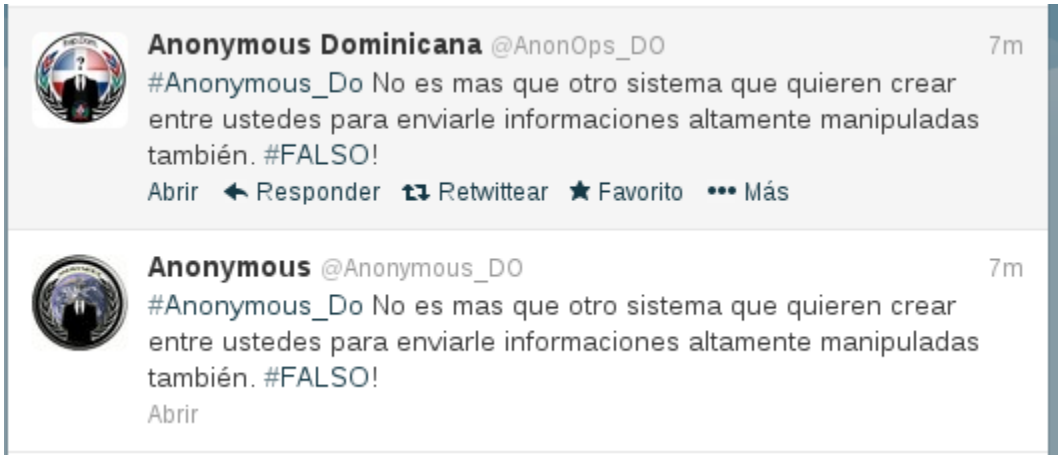
..como he tenido ya experiencias con este tipo de cosas me imaginaba lo que venia, y a sabiendas de lo que podria

tratarse decidi darle a este “hacker” una prueba...asi que fui al link..,http://www.filedropper.com/webtracket me descargue el supuesto programa [para “tumbar” paginas con “metadatos” y escanear vulnerabilidades en cualquier web....]

Desde el momento de descomprimirlo el programa me parecio sospechoso..

..que corporacion o programador serio nombraria un programa “dxwebsetup”,.quize ir mas profundo asi que puse mi Vbox a trabajar por suerte tengo una VM de Windows XP la cual uso para hacer “test” con otros programas..antes de ejecutarlo ya tenia unos programas que pertenecen a la suite de “sysinternals” listos para recolectar la informacion necesaria mientras el drama seguia en twitter...

el usuario ***Anonymous_Do*** habia sido hackeado por un tal @x3ns0ft_RD por razones que desconocia en el momento..



algunos miembros de "Anonymous Dominicana" acusaban a ***Anonymous_Do* de ser lo que en este pais se conoce como "chivato"(rata, boca floja, topo, whistle-blower, entre otras)..y la situacion continuaba..**

jeje desde que "Anonymous Dominicana" empezo a moverse siempre he dicho lo que hasta ahora sigo diciendo, la persona acargo de la cuenta ***Anonymous_Do* no sabia en nada lo que estaba haciendo o era un novato o un lammer o solo una "attention whore" buscando salir en los medios..**

seguia el drama...y las acusasiones de que [los ateriscos son estrellas por que el susodicho se considera un erudito

de la informatica]***Anonymous_Do***...quiza hasta tenga superpoderes..nadie sabe..

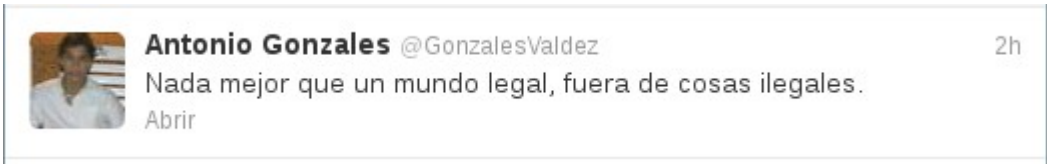
como decimos en este pais, "el tipo eh un montro" o por lo menos eso es lo que piensa el..

trato de involucrar a otros mencionando el nombre de un ex-miembro de "Anonymous_Dominicana" que resulta fue apresado junto a otros cinco..hace ya un tiempo..

a menos segun menciono otro miembro de "Anonymous Dominicana" el sujeto en cuestion logro defacear una pagina..esperemos que el server no haya sido un IIS 5.0..

..hace mucho rondaba en la red una lista de las cosas que un "hacker" nunca debia hacer..creo que este fulano ha roto con todas...

haaa..legal una palabra de dos silabas que suena tambien., pero muy pocos van de las palabras a la accion..



si mi abuela americana estuviera aqui diria -BUUUULLLLSHIIIIIT- claro que no tengo abuela americana pero naaaaah sigamos...pero que quede claro que este personaja es un genio de la informatica[un lvl-99, Godlike, un pro, un over power[OP], un CCNP+CCNSP+CCIE y CISP al

mismo tiempo] lulz! Este twitt me hiso temblar de miedo ante la presencia de una persona con tal nivel de conocimiento...:DDD

espero que se entienda el peligro mortal de tener un 'fatal error' habia..como mis corneas estaban ardiendo ante tal alarde de grandeza decidi dejar todo el drama y los twitts y dirigir mi atencion hacia el programita..

antes de ejecutar el "super escaner de vulnerabilidades" ejecuto las herramientas necesarias para obtener la mayor cantidad de info posible..

```
explorer.exe:1236    OPEN
    C:\Users\Admin\Desktop\WebTracket\setup.exe    SUCCESS
    Options: Open  Access: Read
```

luego de ya ejecutado el "programa" inyecta el explorer[explorer.exe] para que haga el trabajo sucio por el...y empieza a buscar programas y archivos del sistema..

```
explorer.exe:1236    QUERY INFORMATION
    C:\Users\Admin\Desktop\WebTracket\ativtutw.inf


explorer.exe:1236    QUERY INFORMATION

C:\Users\Admin\Desktop\WebTracket\bkoffice\i386\bosres.dll
```

podria mostrar el log completo pero se tornaria confuso

612 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\SOUNDS\SOUNDS.CC2 PATH NOT FOUND Attributes: Error
613 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\Clifford_Reading.exe NOT FOUND Attributes: Error
614 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\CS.2 NOT FOUND Attributes: Error
615 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\CS.2 NOT FOUND Attributes: Error
616 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\DATA1.CAB NOT FOUND Attributes: Error
617 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\data1.cab NOT FOUND Attributes: Error
618 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\data\SOFTBALL.EXE PATH NOT FOUND Attributes: Error
619 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\data1.cab NOT FOUND Attributes: Error
620 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\Fp-400 NOT FOUND Attributes: Error
621 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\CSS-AMGR.EXE NOT FOUND Attributes: Error
622 10:30:54 PM explorer.exe:1236 QUERY INFORMATION

C:\Users\Admin\Desktop\WebTracket\COMANDOS\VIDEO\H_Afri.avi PATH NOT FOUND Attributes: Error
623 10:30:54 PM explorer.exe:1236 QUERY INFORMATION C:\Users\Admin\Desktop\WebTracket\allied.ico NOT FOUND Attributes: Error
624 10:30:54 PM explorer.exe:1236 QUERY INFORMATION

luego de gastar espacio de memoria y buscar archivos y informacion del sistema el programa crea un arcivo ejecutable llamado svchost.exe

trata de garantizar su ejecucion luego de iniciada la pc..

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft SUCCESS "C:\Users\Admin\My Documents\MSDCSkk\svchost.exe"

el cual se guarda en la carpeta MisDocumentos..[WWOOOOOOOW QUE CREATIVO!!!![sarcasmo] el cual a mi parecer resulta ser el server de un RAT muy conocido en el 'underground' llamado DarkComet[esto no lo tengo confirmado] :'(

el server entonces procede a enviar solicitudes de coneccion a el/las IPs pertenecientes a la persona/personas que lo esta controlando...

pude logear informarcion del intercambio de paquetes usando un snifer

```
00000000  11 02 80 3C 0A 00 02 0F  00 8A 00 C6 00 00 20 46   ...<.... ...... F
00000010  45 46 43 46 46 45 46 43  4E 46 44 45 4A 45 4E 46   EFCFFEFC NFDEJENF
00000020  41 45 4D 45 46 43 41 43  41 43 41 43 41 41 41 00   AEMEFCAC ACACAAA.
00000030  20 41 42 41 43 46 50 46  50 45 4E 46 44 45 43 46    ABACFPF PENFDECF
00000040  43 45 50 46 48 46 44 45  46 46 50 46 50 41 43 41   CEPFHFDE FFPFPACA
00000050  42 00 FF 53 4D 42 25 00  00 00 00 00 00 00 00 00   B..SMB%. ........
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000070  00 00 11 00 00 2C 00 00  00 00 00 00 00 00 00 E8   .....,.. ........
00000080  03 00 00 00 00 00 00 00  00 2C 00 56 00 03 00 01   ........ .,.V....
00000090  00 01 00 02 00 3D 00 5C  4D 41 49 4C 53 4C 4F 54   .....=.\ MAILSLOT
000000A0  5C 42 52 4F 57 53 45 00  0C 00 C0 27 09 00 4E 41   \BROWSE. ...'..NA
000000B0  54 4C 4F 4F 4E 41 53 00  88 8E 10 00 00 30 03 0A   TLOONAS. .....0..
000000C0  00 10 00 80 00 30 FA 7F  54 52 55 45 2D 53 49 4D   .....0.■ TRUE-SIM
000000D0  50 4C 45 00                                       PLE.
```

y leyendolos a puro ojo pude encontrar unos paquetes interesantes..

```
00000000  2F 4E 01 00 00 01 00 00  00 00 00 00 06 72 65 61   /N...... .....rea
00000010  73 65 6E 05 6E 6F 2D 69  70 03 6F 72 67 00 00 01   sen.no-i p.org...
00000020  00 01                                             ..

00000000  2F 4E 81 80 00 01 00 01  00 00 00 00 06 72 65 61   /N...... .....rea
00000010  73 65 6E 05 6E 6F 2D 69  70 03 6F 72 67 00 00 01   sen.no-i p.org...
00000020  00 01 C0 0C 00 01 00 01  00 00 00 12 00 04 4D E4   ........ ......M.
00000030  BF B7                                             ..
```

mis ojotes no me enganaban -jojojo- asi que segui leyendo paquetes...hasta que encontre este

```
00000000  65 28 01 00 00 01 00 00  00 00 00 00 06 77 65 62   e(...... .....web
00000010  73 65 63 05 6E 6F 2D 69  70 03 6F 72 67 00 00 01   sec.no-i p.org...
00000020  00 01                                             ..

00000000  65 28 81 80 00 01 00 01  00 00 00 00 06 77 65 62   e(...... .....web
00000010  73 65 63 05 6E 6F 2D 69  70 03 6F 72 67 00 00 01   sec.no-i p.org...
00000020  00 01 C0 0C 00 01 00 01  00 00 00 21 00 04 C9 E5   ........ ...!....
00000030  CD 82                                             ..
```

este paquete fue el que me dijo donde/quien/como/cuando/por que/etc etc etc....como no soy tan tontontonto...le hise whois a las Ips que me mostraba otro programa...

|setup.exe:900 TCP true-simple.lan:1158 static-183-191-228-77.ipcom.comunitel.net:8585 ESTABLISHED|

Organisation Name.... VODAFONE ESPA?A S.A.

Organisation Address. Pontevedra
Organisation Address. SPAIN
****

tdev205-130.codetel.net.do <---a esta ultima no tuve tiempo de hacerle whois

quise ver que me decia el wireshark que tenia corriendo en la otra plataforma..end gues wat?

```
76 Standard query 0xd1b3  A reasen.no-ip.org
92 Standard query response 0xd1b3  A 77.228.191.183
```

Y nuestro amigo de espania volvia a aparecer....

196.3.81.5	DNS	87 Standard query 0xc860 PTR 183.191.228.77.in-addr.arpa
200.88.127.22	DNS	87 Standard query 0xc860 PTR 183.191.228.77.in-addr.arpa
10.0.0.121	DNS	142 Standard query response 0xc860 PTR static-183-191-228-77.ipcom.comunitel.net
196.3.81.5	DNS	87 Standard query 0x58d1 PTR 183.191.228.77.in-addr.arpa
Broadcast	ARP	60 Who has 10.0.0.1? Tell 10.0.0.10
10.0.0.121	DNS	142 Standard query response 0x58d1 PTR static-183-191-228-77.ipcom.comunitel.net
10.0.0.121	DNS	142 Standard query response 0xc860 PTR static-183-191-228-77.ipcom.comunitel.net

pense que algo no andaba bien por que el sujeto en cuestion es 'Dominicano' y vive y estudia en 'Santo Domingo' por lo tanto decidi seguir rastreando a nuestro/nuestros amiguito/amiguitos...en el momento en que intentaban usar el chatbox y mandarme mensajes graciosos como "U MAD BRO?" fue/fueron tan ineptos que abrio/abrieron/abriran/vosotros abrireis/ellos abren.....el server de otro RAT con todo y archivo .zip en mi pantalla momento que aproveche para guardar el archivo en mi USB y ver si podia sacar algo de info...

..como pude darme cuenta incluia un archivo config.xml por lo tanto me imaginaba para que era y sabia que obtendria algo de info si lo abriaaa

```
<properties>
<comment>Frutas rat v0.8</comment>
<entry key="avs">mbam.exe#mbamgui.exe#mbam
<entry key="prefijo">Warner_</entry>
<entry key="uac">false</entry>
<entry key="delay">1</entry>
<entry key="puerto2">1001</entry>
<entry key="dns">reasen.zapto.org</entry>
<entry key="keyClase">N0IAoYsM</entry>
<entry key="puerto1">1000</entry>
<entry key="jarname">Oracle</entry>
<entry key="instalar">true</entry>
<entry key="hklm">true</entry>
<entry key="password">e3a8809017dd76bd2655
<entry key="tskschedule">true</entry>
<entry key="regname">Microsoft</entry>
</properties>
```

no pude haber estado mas en lo cierto...eureka!! otra vez me encontre la direccion del No-ip que usaba lo cual me fue util ya que habia intentado poderle hacer whois a ambas direcciones..ya que trate con las que obtuve del sniffer: reasen.no-ip.org y websec.no-ip.org sin tener exito...ya que reasen.no-ip.org no respondia pero websec.no-ip.org si..

asi que decidi usar un programa que viene incluido en algunas distros[no ubuntu] para resolver los nombres de dominio a sus respectivas IP's.....

```
root@n3t_3rr0r:~# resolveip reasen.zapto.org
IP address of reasen.zapto.org is 77.228.191.183
```

y tratar con la otra ya fue facil...

```
root@n3t_3rr0r:~# resolveip websec.no-ip.org
IP address of websec.no-ip.org is 201.229.205.130
```

Espero que hayan aprendido algo chicos no vallan de aquiparalla queriendo tirarle sus sucios RATs a todo el mundo les puede salir muuuuuy caro...

Este personaje hasta publico su numero telefonico en twitter[no juzgare su inteligencia] hay otros que intentan hacer lo mismo...

por ahora

AM OUT!!