



Reporte sobre virus Agobot.F

Anexo del Comunicado VITI

TI020-TYR-310304

Hemos encontrado actividad de un virus el cual permite que la computadora comprometida pueda ser usada para efectuar ataque de DoS (Negación de Servicio). A continuación presentamos un reporte preparado por el área de seguridad de DDT de la VITI:

Agobot.F (Backdoor.Agobot.3.f, W32.HLLW.Gaobot, Gaobot, Win32/Gaobot)

Gusano que se propaga principalmente por medio de 3 vulnerabilidades de los sistemas Windows: RPC/DCOM (<http://www.microsoft.com/technet/security/bulletin/MS03-039.asp>), RPC/Locator (<http://www.microsoft.com/technet/security/bulletin/MS03-001.asp>), y WebDAV (<http://www.microsoft.com/technet/security/bulletin/MS03-007.asp>). Para propagarse en redes locales, el gusano tiene otra rutina que trata de conectarse a los equipos en la red local con el usuario Administrador (traducido a varios idiomas) y una serie de passwords triviales. El gusano se copia en el folder de sistema y se asegura que siempre sea cargado al iniciar el equipo por medio de dos llaves en el Registro del Sistema. Después de que se inicia, el gusano se conecta a un servidor de IRC predeterminado por el puerto 9900, entra a un canal y espera instrucciones. Desde ahí, el gusano puede ser controlado para poder cargar y correr aplicaciones en el sistema infectado, buscar equipos vulnerables para infectar e infectarlos, llevar acabo ataques de DDoS, usar el equipo infectado como proxy TCP y robar llaves de CD de juegos.

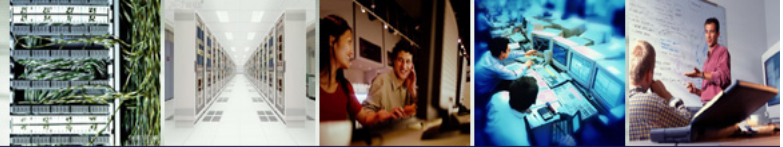
Debido a que la computadora puede ser controlada podemos encontrar cambios en el comportamiento del ataque de DoS o incluso que el atacante cambie el puerto por donde controla a ala maquina (actualmente el default es el 9900 pero no hemos encontrado actividad por ese puerto, así que filtrarlo puede no ayudar mucho). Sin embargo para el DoS actual hemos encontrado que genera DoS con puertos destino 135, 137, 1025, 2745, 3127, 6129 y 80, además de que las direcciones destino pueden (y la mayoría de las veces) no existir.

A continuación les damos un procedimiento para ejecutarse en sus equipos de redes que les puede ayudar a identificar maquinas con virus.

Procedimiento para identificar máquinas con virus

Routers/6500/4006

La actividad con el DoS actual se puede verificar con estadísticas de Netflow. Esta funcionalidad solo esta disponible en enrutadores (2620, 3640, 3725, 7200, etc), en Catalyst 6500 y Catalyst 4006 con procesadora II, para otros equipos mas adelante se da un procedimiento. A continuación se muestra el procedimiento para estos equipos.



Se requiere habilitar netflow en las interfaces de entrada (configuración) (todas las vlans de la LAN):

```
int vlan 455
ip route-cache flow
```

Posteriormente se verifica las maquinas con actividad con algunos de estos comandos:

```
6500>sh ip cac flo | inc 0401
6500>sh ip cac flo | inc 0AB9
6500>sh ip cac flo | inc 0C37
6500>sh ip cac flo | inc 17F1
```

Ejemplo de salida:

```
core1#sh ip cac flo | inc AB9
VI27 10.16.196.239 Null 10.16.237.74 06 114C 0AB9 1
VI29 10.17.117.185 VI33 10.17.151.27 06 0C87 0AB9 1
VI27 10.16.200.233 Null 10.16.165.140 06 0EA7 0AB9 1
VI35 10.17.151.77 VI23 10.17.32.46 06 070C 0AB9 1
VI39 10.16.198.226 Null 10.16.224.27 06 0656 0AB9 1
VI39 10.16.194.200 VI7 141.223.191.154 06 1158 0AB9 1
VI39 10.16.203.234 Null 10.16.106.40 06 0568 0AB9 1
VI39 10.16.194.200 VI7 141.223.105.32 06 081B 0AB9 1
VI35 10.17.151.189 VI23 10.17.55.162 06 0F18 0AB9 1
```

A menos que la maquina haga un spoofing de su IP, la mac-address se obtiene:

```
6500>sh ip arp 0009.6be1.0a89
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.16.198.226 0 0009.6be1.0a89 ARPA Vlan455
```

4507/4006/3550

Este es un ejemplo para equipo que no soportan netflow como los 4006/4507 con procesadora III y los 3550s. Es necesario poner listas de acceso que "logueen" las mac-address de las maquinas con virus. Se recomienda eliminar las listas después de algunos días para evitar el exceso de generación de log.

```
access-list 150 deny tcp any any eq 2745 log-input
access-list 150 deny tcp any any eq 3127 log-input
access-list 150 deny tcp any any eq 6129 log-input
access-list 150 deny tcp any any eq 1025 log-input
access-list 150 permit tcp any any
access-list 150 permit ip any any
```



Un ejemplo de actividad 2 minutos de poner la lista

```
deny tcp any any eq 2745 log-input (284327 matches)
deny tcp any any eq 3127 log-input (254591 matches)
deny tcp any any eq 6129 log-input (249143 matches)
deny tcp any any eq 1025 log-input (267579 matches)
permit tcp any any (1664039 matches)
permit ip any any (25692 matches)
```

Para checar las mac-address:

```
4500>sh log
```

Log Buffer (4096 bytes):

```
14:05:12: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.16.199.138(3682) (GigabitEthernet4/4
0001.0332.d708) -> 10.16.130.95(1025), 1 packet
Mar 31 14:05:13: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.16.203.236(1042)
(GigabitEthernet5/4 0009.6ba1.d6df) -> 10.88.35.195(3127), 1 packet
Mar 31 14:05:14: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.16.203.236(3408)
(GigabitEthernet5/4 0009.6ba1.d6df) -> 10.16.112.159(6129), 1 packet
Mar 31 14:05:15: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.16.202.238(4404)
(GigabitEthernet6/5 0009.6ba1.e2f2) -> 129.69.129.17(1025), 1 packet
Mar 31 14:05:16: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.16.203.236(4892)
(GigabitEthernet5/4 0009.6ba1.d6df) -> 10.16.60.185(6129), 1 packet
```

Búsqueda de MAC-Address

Para equipo con IOS:

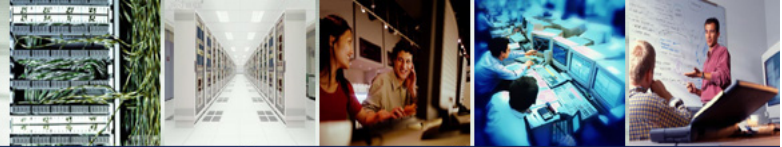
```
4500>sh mac-address-table address 0009.6ba1.d6df
Unicast Entries
vlan mac address type protocols port
-----+-----+-----+-----+-----
457 0009.6ba1.d6df dynamic ip GigabitEthernet5/4
```

Para equipo con CatOS:

```
C6500> sh cam 00-0b-cd-fd-ad-cb
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry
```

```
VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
-----
136 00-0b-cd-fd-ad-cb 5/7 [ALL]
```

Si el puerto donde se encuentra la mac address conoce mas de una mac-address, entonces el puerto interconecta a otro switch, un hub o un AP. Si es switch es necesario repetir este procedimiento hasta encontrar un puerto con solo una mac-address o que conecte a un AP inalámbrico.



Aun no se encuentra (muchas mac-address):

```
4500>sh mac-address-table interface gigabitEthernet 5/4
```

```
Unicast Entries
```

```
vlan mac address type protocols port
```

```
-----+-----+-----+-----+-----  
1 000c.ce14.34b1 dynamic other GigabitEthernet5/4  
457 0001.0388.dea4 dynamic ip GigabitEthernet5/4  
457 0009.6ba1.af8c dynamic ip GigabitEthernet5/4  
457 0009.6ba1.d6da dynamic ip GigabitEthernet5/4  
457 0009.6ba1.d6df dynamic ip GigabitEthernet5/4  
457 0009.6ba1.fde0 dynamic ip GigabitEthernet5/4
```

Hay un switch:

```
4500>sh cdp n g 5/4
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
```

```
Device ID Local Intrfce Holdtme Capability Platform Port ID  
0A603B-B-sw Gig 5/4 159 S I WS-C3550-4Gig 0/1
```

Aquí está:

```
0A603B-B-sw3550-01>sh mac-address-table address 0009.6ba1.d6df
```

```
Mac Address Table
```

```
-----
```

```
Vlan Mac Address Type Ports
```

```
-----
```

```
457 0009.6ba1.d6df STATIC Fa0/29
```

```
Total Mac Addresses for this criterion: 1
```

```
0A603B-B-sw3550-01>sh mac-address-table int fas 0/29
```

```
Mac Address Table
```

```
-----
```

```
Vlan Mac Address Type Ports
```

```
-----
```

```
457 0009.6ba1.d6df STATIC Fa0/29
```

```
Total Mac Addresses for this criterion: 1
```