1.0 Summary

Findings and observations:
Robust bot software that offers lots of features to the author or other controller. We saw that there was a detailed system inventory function; ability to (at a minimum) inventory local networks; update the C2 server; update the software; provide troubleshooting info to the author(s) in the event of errors; anti-analysis techniques; remote shell access; remote execution; various methods of hiding the malware and its traffic/activities; presumed encoding features to provide information back to C2 in the form of account names, etc.; and features that allow the bot controller to recon remote systems and also attack those systems. We also found many things in this sample and the previous sample (the launcher) to obfuscate the bot code such as encryption (AES) and other encoding (MD5, base64, xor).

Recommendations:
Same recommendations as noted in the analysis of the launcher. One might also consider blocking port 69 for TFTP unless this is actively in use, as this was shown to be one source of downloading updates for this malware.

Conclusion:
Really cool and fascinating bot to work on. Lots of features and functionality for the authors. We saw that not only does it provide some useful features such as the ability to scan and exploit other machines, remote shell access, but also housekeeping functions such as error tracking and reporting and an update feature as well. This was a great sample to work on.

1.1 Identification

File Name: payload.exe [analyst assigned]
File Type: 32-bit Windows executable
Malware name(s): BEAR.payload
Current detection: 42/53
Malware type: Bot client
Size: 56,892 bytes
Packer: None
Encryption/encoding: base64, MD5
Origin: Dionaea honeypot running in New York City (also obtained about a week later in a German honeypot)
Compile time: 24DEC2009 13:25:55Z

Hashes:

```
MD5:d4851b410d158cf650d3f772e270f305
SHA1:4ee5121b05820e8f04b6560f422180660df29b2d
SHA256:267674ddf67827afa282763e57313fc636f170fbffaf104e69ee4db49d1567d5
ssdeep:1536:daWAQE3GZ8CAu9ax2MaO7tJoQuQQTKZc9q3RXFuEUk:JAQE2UHaO2QQTv4XF9Uk
```

Test environment details: Win 7 Home Premium SP1 running in VirtualBox 5.0.18_Ubuntu r106667 on Ubuntu 16.04. Hardware is an Acer Aspire 5742 (Intel i3).

1.2 Dependencies

OS: Windows 4.0 and higher
Imports (DLLs): msvcrt.dll, kernel32.dll, ws2_32.dll, user32.dll, advapi32.dll, shell32.dll (in header).
From code: netapi32.dll, mpr.dll, psapi.dll
Exports: None

Other: Requires access to port 4466 via IRC for C2, and ports 80/21/69 for the various ways that it can connect to receive updates (HTTP/FTP/TFTP respectively)

2.0 Characteristics

2.1 Behavior

This sample gathers information about the host and then establishes communication with a C2 channel over IRC. The malware then idles in this C2 channel, periodically testing connectivity, while it waits for instructions. There also appears to be functionality for transferring files/data, so it's possible that this sample also exfiltrates data as well. This sample engages in anti-analysis behavior and other design features that complicate analysis. This sample does not appear to engage in privilege escalation, both in terms of observed code and behavior. There are many features that the C2 can engage such as remote shell, remote execution, IP address scanning and exploitation, and updates to the C2 server address.

2.2 Infection

The malware executes upon user action (either running from the command prompt or from Explorer or the equivalent). The malware spawns a child process shortly after. This child process is subject to replacement and this overall process iterates many times. The PHP found at 37.59.118.41 downloads and starts the malware as a service.

2.3 Persistence

When running with administrator privileges, the malware executes a series of process replacements of various Windows executables before finally setting the last one to autorun. Unlike the previous analysis of BEAR.launcher, the payload only spawned a single copy of each replaced process (unlike the two processes replaced in BEAR.launcher).

2.4 Movement

Not observed during cursory examination when a machine with a running instance of the sample was connected to a LAN. There was usual intra-LAN traffic observed, but nothing appeared malicious. Network recon functionality was observed, however.

2.5 Data Exfiltration

None explicitly observed, but the C2 available through the IRC channel appears to allow for this to take place. It is possible that there was no hostile operator around to trigger any of these features in the running instance.

2.6 C^2

C2 appears to be managed from an IRC server at her.d0kbilo.com:4466 in the channel #Balengor. IRC commands are passed in plaintext however communication between the bot and the C2 entity appear encrypted. There is a user associated with this channel on that server, e.TK, which appears to be the user that the malware interfaces with after check-in. This user was also observed when entering the channel from an IRC client.

2.7 Signatures

This executable drops a randomly named batch file into the same directory where the executable and each interim replaced process was run. This batch file contains commands to delete the executable and then the batch file afterwards. This file will remain (and its execution will fail) if the user is not running in admin mode.

The malware appears as a process with the same name as the file, with the final process named spooIsv.exe. The child process is created with the same name, but then random windows processes are created and replaced with the malware payload. When running in admin mode, any one of a number of processes can be replaced such as winamp.exe, algs.exe, logon.exe, winlogon.exe, spoolsvc.exe, spoolsv.exe, lssas.exe, iexplore.exe, and possibly others that were not yet observed. It's assumed that this is both to help hide the running malware process and to interfere with debugging and analysis.

Referring to the above process, the malware will add a registry value to ensure that the final replaced process in the above series is run at startup. This value is always located at:

```
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Windows DLL Loader:
"C:\Windows\system32\spooIsv.exe"
```

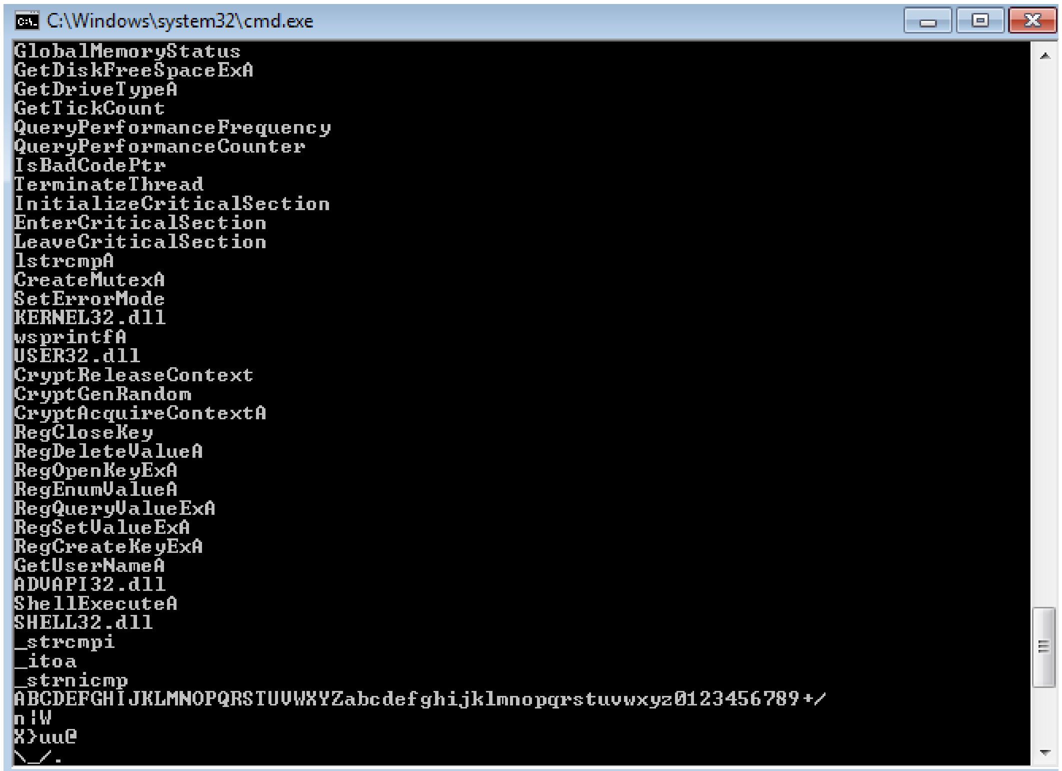
The following key can be observed on the host as well, in order to enable access through the firewall for the sample:

```
HKLM\SYSTEM\ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\Au
thorizedApplications\List\C:\Windows\system32\spooIsv.exe:
"C:\Windows\system32\spooIsv.exe:*:Enabled:Windows DLL Loader"
```

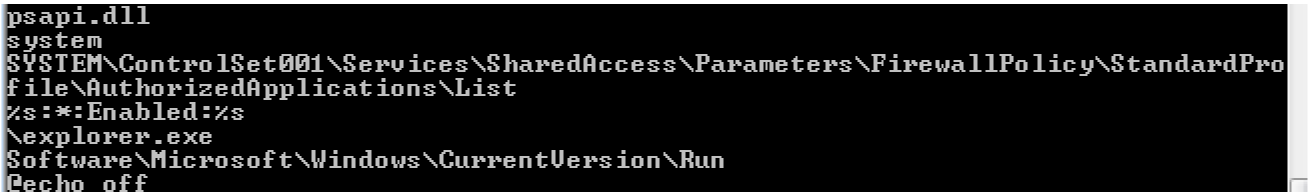
A mutex was created: dc3d5c2012d372867 88b94a5d50d7a3cf0

IRC traffic can be observed to her.d0kbilo.com on port 4466. This domain always resolves to 37.59.118.41 at this time. The malware contains code to generate an HTTP header (HTTP 1.0) so this could also be observed as indicating malware traffic if this is not a normal header for the host system.

3.0 Raw Notes



```
GlobalMemoryStatus
GetDiskFreeSpaceExA
GetDriveTypeA
GetTickCount
QueryPerformanceFrequency
QueryPerformanceCounter
IsBadCodePtr
TerminateThread
InitializeCriticalSection
EnterCriticalSection
LeaveCriticalSection
lstrcmpA
CreateMutexA
SetErrorMode
KERNEL32.dll
wsprintfA
USER32.dll
CryptReleaseContext
CryptGenRandom
CryptAcquireContextA
RegCloseKey
RegDeleteValueA
RegOpenKeyExA
RegEnumValueA
RegQueryValueExA
RegSetValueExA
RegCreateKeyExA
GetUserNameA
ADVAPI32.dll
ShellExecuteA
SHELL32.dll
_strcmpi
_itoa
_strnicmp
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
n¦W
X}uu@
\_/.
```



```
psapi.dll
system
SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardPro
file\AuthorizedApplications\List
%s:*:Enabled:%s
\explorer.exe
Software\Microsoft\Windows\CurrentVersion\Run
@echo off
```

```
!This program cannot be run in DOS mode.
.rdata
@.data
DSVWj@
HtxHuuj
YY_tDh
PVVVSVV
YY_^[]
SVhWC@
<0|C<9
PSSj(j
t<Ht(Ht
QQSVW3
QSUVWhT
PSQhP|@
YYPjZjA
j[j]Pj[
YY_^][
YYPjZjA
j[j]Pj[
strlen
memcpy
memmove
memset
memcmp
strcmp
strcpy
malloc
sprintf
strcat
strncpy
fwrite
fclose
sscanf
strstr
_snprintf
strncmp
realloc
_except_handler3
_beginthreadex
vsprintf
_vsnprintf
MSVCRT.dll
WS2_32.dll
DeleteFileA
SetFileAttributesA
CloseHandle
TerminateProcess
ReadProcessMemory
OpenProcess
GetModuleFileNameA
GetModuleHandleA
GetCurrentProcessId
ReadFile
GetExitCodeProcess
PeekNamedPipe
CreateProcessA
```

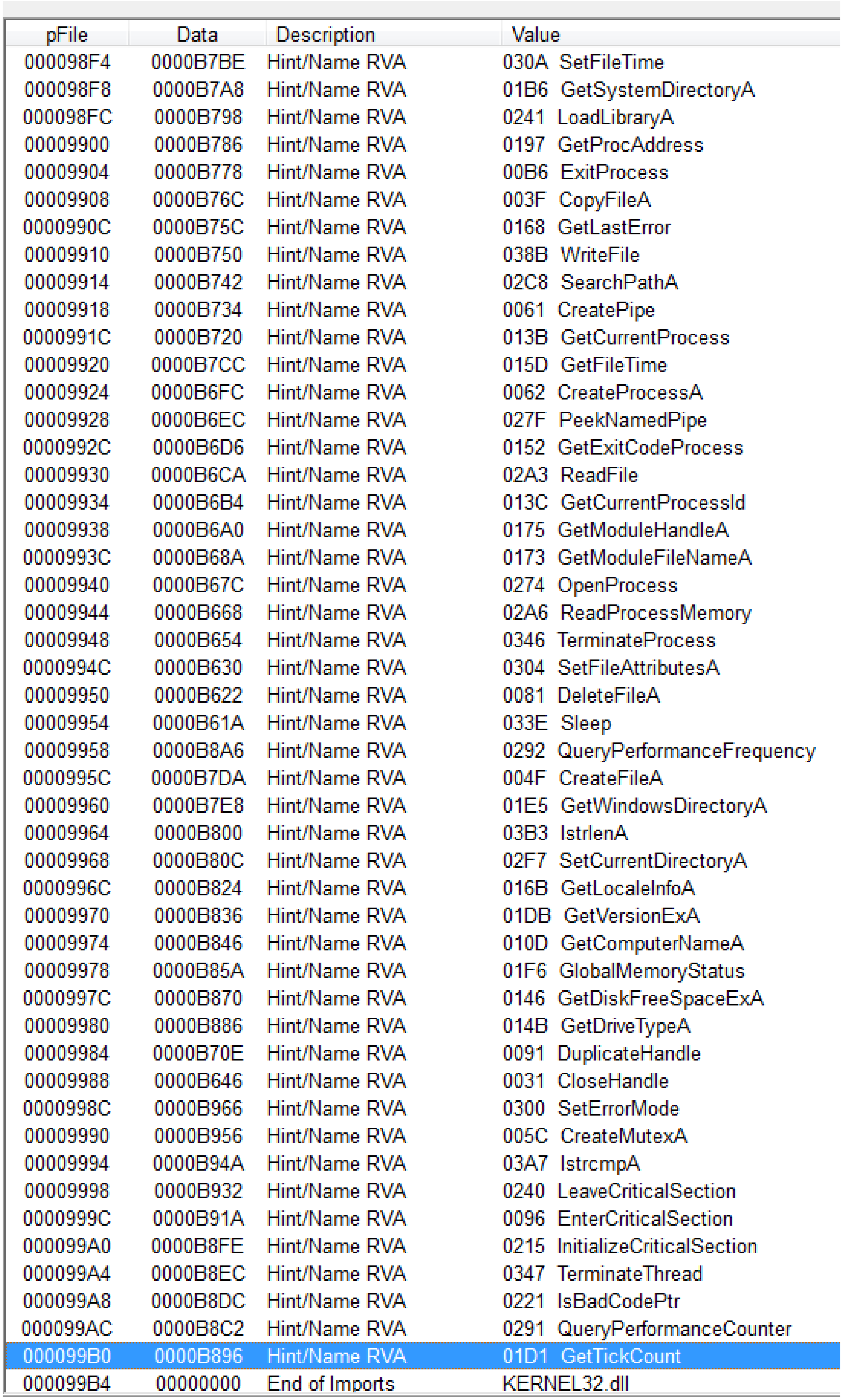
```
DuplicateHandle
GetCurrentProcess
CreatePipe
SearchPathA
WriteFile
GetLastError
CopyFileA
ExitProcess
GetProcAddress
LoadLibraryA
GetSystemDirectoryA
SetFileTime
GetFileTime
CreateFileA
GetWindowsDirectoryA
lstrlenA
SetCurrentDirectoryA
GetLocaleInfoA
GetVersionExA
GetComputerNameA
GlobalMemoryStatus
GetDiskFreeSpaceExA
GetDriveTypeA
GetTickCount
QueryPerformanceFrequency
QueryPerformanceCounter
IsBadCodePtr
TerminateThread
InitializeCriticalSection
EnterCriticalSection
LeaveCriticalSection
lstrcmpA
CreateMutexA
SetErrorMode
KERNEL32.dll
wsprintfA
USER32.dll
CryptReleaseContext
CryptGenRandom
CryptAcquireContextA
RegCloseKey
RegDeleteValueA
RegOpenKeyExA
RegEnumValueA
RegQueryValueExA
RegSetValueExA
RegCreateKeyExA
GetUserNameA
ADVAPI32.dll
ShellExecuteA
SHELL32.dll
_strcmpi
_strnicmp
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
D CKFDENECFDEFFCFGEFFCCACACACACACA
EKEDFEEIEDCACACACACACACACACACAAA
PC NETWORK PROGRAM 1.0
LANMAN1.0
Windows for Workgroups 3.1a
LM1.2X002
LANMAN2.1
NT LM 0.12
9NTLMSSP
WORKGROUPlQPxf2ISQgEV1bGKWindows 2000 2195
Windows 2000 5.0
NTLMSSP
```

```
Windows 2000 2195
Windows 2000 5.0
WORKGROUP
Windows 2000 2195
Windows 2000 5.0
FUnMLEvdNzjntXznAvcOSDvcUlULLFJmCPCmjgeXpbDCIAtjDTRPAxyXItXCfDxvjRXtWSyACqcPrzWHeaUKfrohnEuS
yZUzPzbe
IFJUOUTEPUWKXMWXUGHMIEKCYENBAQPLZEDNOOBGMW
bMZCTWLHYWI
\SRVSVC
D CKFDENECFDEFFCFGEFFCCACACACACACA
EKEDFEEIEDCACACACACACACACACACAAA
NT LM 0.12
Samba *
Windows 5.1
Windows 5.0
Windows 2000 LAN Manager*
NT LAN Manager *.*
*Service Pack 2*
*Service Pack 1*
Windows Server 2003 *.*
hws2_T
Scanned
:%s in
open IP(s) found
:%s is open
- Scanning
:%s for
second(s)
Scanning
:%s for
second(s)
Scanning
:%s for
second(s), t:%u s:%u
- Attempted
exploitation(s) on
IP(s).
Attempting to exploit
with
- Attempting to exploit IP's in list.
Attempting to exploit IP's in list.
Exploit statistics -
Listing exploit statistics
bot(s) found with string
No bots found with string
found string
in %s (
- Listing bots with string
%s bots with string
Killing
Listing
Cmd.exe process has terminated.
Could not read data from process.
cmd.exe
Error while executing command.
Remote cmd thread
Received
from
sec with
KB/sec
- Receiving
from
Receiving
from
Content-Length: %u
```

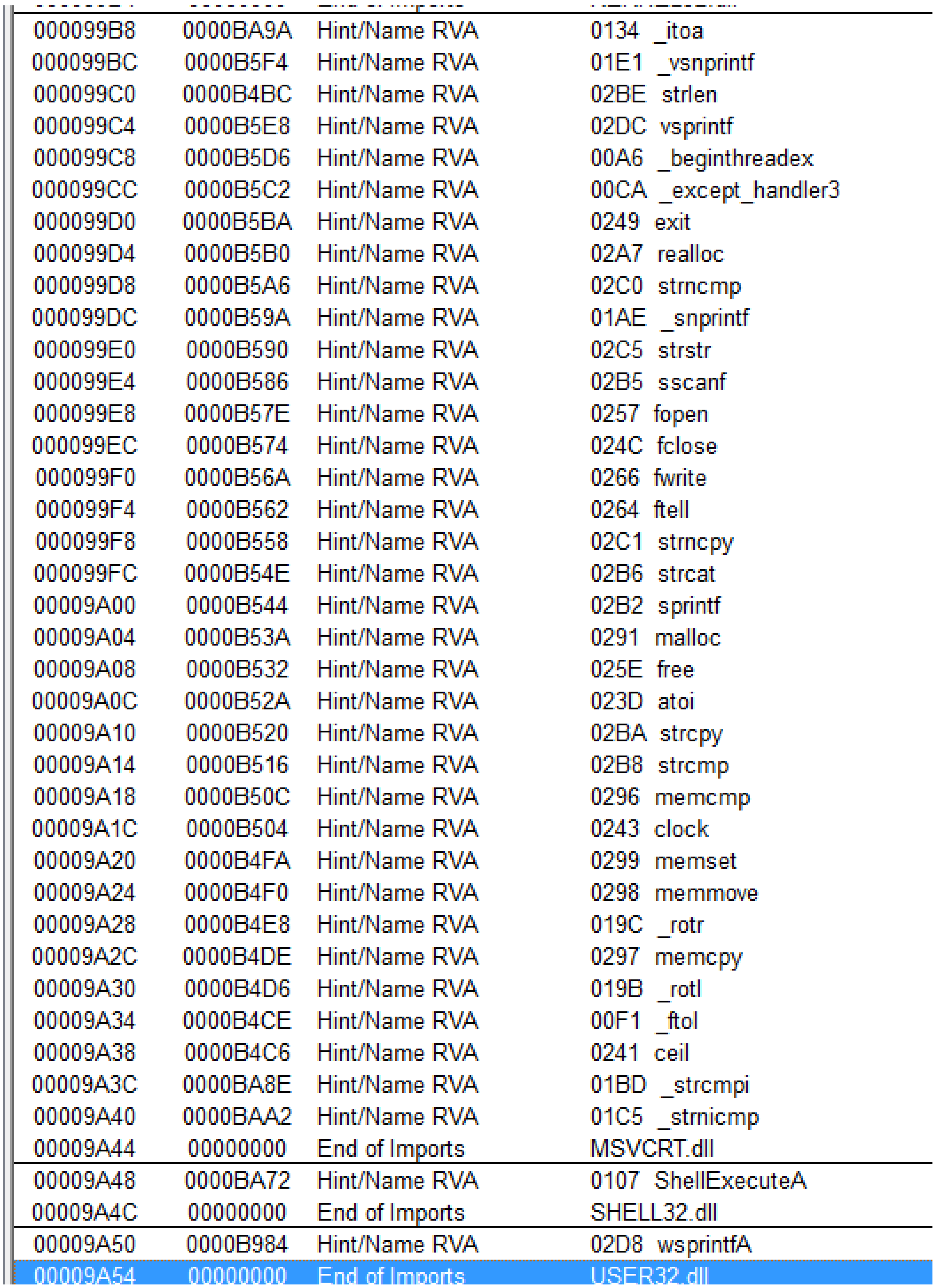
```
Content-Length:
GET /%s HTTP/1.0
Host: %s
- Unsupported protocol specified.
- Error while downloading
- Unable to start
- Successfully downloaded
with
KB/sec%s.
, executing
, updating
- No file to download specified.
tftp://
anonymous
ftp://
http://
- Cannot read source file
- Cannot write to destination file
file://
- Downloading
Downloading
QUIT :restarting
QUIT :exitting
- Module "%s" reported a crash in "%s": N=%u EAX=%08X EBX=%08X ECX=%08X EDX=%08X ESI=%08X
EDI=%08X EBP=%08X ESP=%08X EIP=%08X EFLAGS=%08X. Code: %08X (%s). %s...
Continuing
Restarting
EXCEPTION_FLT
EXCEPTION_INT_DIVIDE_BY_ZERO
EXCEPTION_STACK_OVERFLOW
EXCEPTION_NONCONTINUABLE_EXCEPTION
EXCEPTION_BREAKPOINT
EXCEPTION_ACCESS_VIOLATION
EXCEPTION_ILLEGAL_INSTRUCTION
EXCEPTION_OTHER
InternetGetConnectedStateExA
wininet.dll
freeaddrinfo
getnameinfo
getaddrinfo
ws2_32.dll
WNetCancelConnection2W
WNetCancelConnection2A
WNetAddConnection2W
WNetAddConnection2A
mpr.dll
NetAddAlternateComputerName
NetScheduleJobAdd
NetApiBufferFree
NetRemoteTOD
NetShareEnum
NetUserEnum
NetUseDel
NetUseAdd
NetUseGetInfo
netapi32.dll
InitializeCriticalSectionAndSpinCount
kernel32.dll
192.168.
%u.%u.%u.%u
GetModuleInformation
GetModuleFileNameExA
EnumProcessModules
EnumProcesses
psapi.dll
system
```

```
SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
%s:*:Enabled:%s
\explorer.exe
Software\Microsoft\Windows\CurrentVersion\Run
@echo off
:deleteagain
del /A:H /F %s
del /F %s
if exist %s goto deleteagain
del %s
Windows DLL Loader
QUIT :%s uninstalled.
%s.%s.%s.%s
System information - OS: Windows
(%s, v
). CPU: %s
MHz. Ram:
MB free. IPv6:
. Uptime:
day%s
hour%s
minute%s. Computername:
. User:
ProcessorNameString
HARDWARE\DESCRIPTION\System\CentralProcessor\0
Sysinfo thread
Network information - Host:
. Name:
. Type:
. IPv6:
. Firewalled:
. Latency:
, %u. IRC Uptime:
day%s
hour%s
minute%s.
Avarage
Unknown
Netinfo thread
%sTotal drives:
, Total space:
MB free.
MB free
unknown
ramdisk
cd-rom
remote
removable
Drive information -
Driveinfo thread
thread
- btg tried executing an unreadable address. (%08X)
- No threads running.
- Listing
threads:
QUIT :changing server
link v
%s [Win32]
Uptime - System:
day%s
hour%s
minute%s. IRC:
day%s
hour%s
minute%s
```

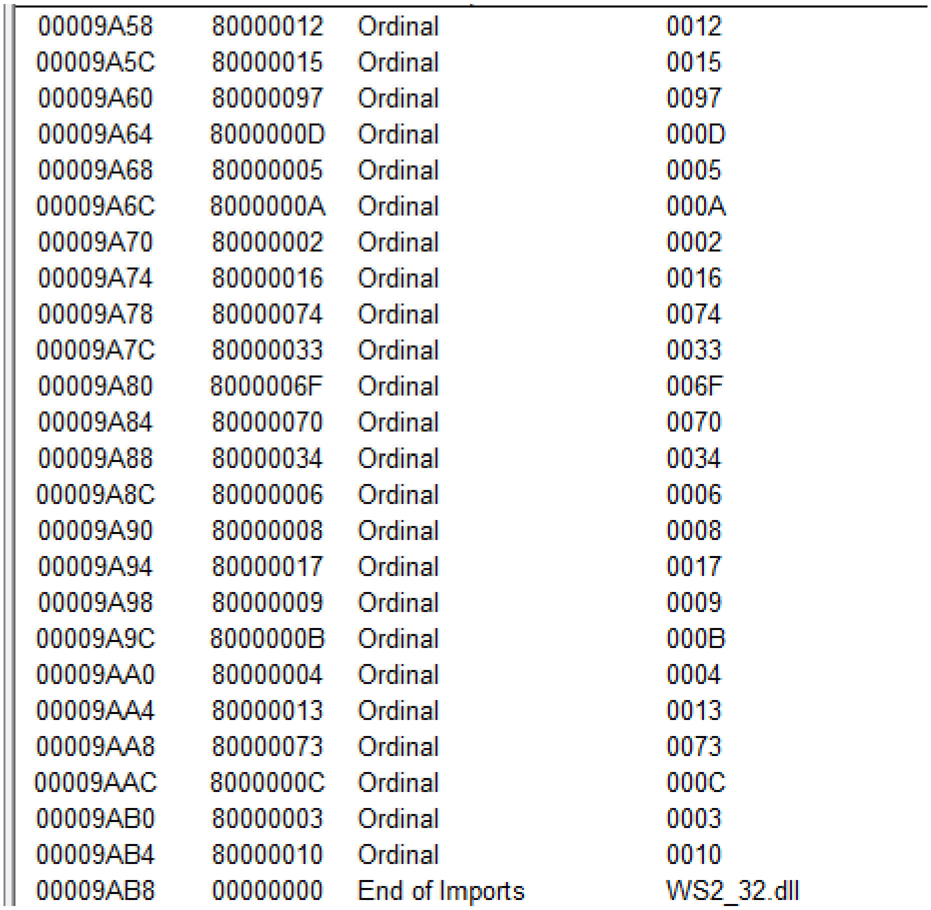
```
Debug mode is %s.
Exe download server:
Exe download server:
f128enc+fab decrypted:
f128enc+fab encrypted: =
%c%s%c%c%u%c%u%s%c%c%c
NICK %s
USER %s %s %s :%s
PASS %s
NOTICE %s :
PRIVMSG %s :
message
NOTICE %s :
PRIVMSG %s :
NOTICE
link!link@link PRIVMSG %s :%s
USERHOST %s
JOIN %s %s
MODE %s +xi
MODE %s +smntu
VERSION %s
eggdrop v1.6.16
VERSION link v%d.%03d%s (Win32)
VERSION
VERSION
PRIVMSG
PONG %s
link!link@link
ndEvery1
#balengor
- eip has left the endless loop for some reason...
PING :%08X
%08x%x%08x%3x%08x%08x
C:\MA\lab\malexe001.exe
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
WORKGROUPlQPxf2ISQgEV1bGK
\browser
\..\..\AOHLMXY
```



pFile	Data	Description	Value
000098F4	0000B7BE	Hint/Name RVA	030A SetFileTime
000098F8	0000B7A8	Hint/Name RVA	01B6 GetSystemDirectoryA
000098FC	0000B798	Hint/Name RVA	0241 LoadLibraryA
00009900	0000B786	Hint/Name RVA	0197 GetProcAddress
00009904	0000B778	Hint/Name RVA	00B6 ExitProcess
00009908	0000B76C	Hint/Name RVA	003F CopyFileA
0000990C	0000B75C	Hint/Name RVA	0168 GetLastError
00009910	0000B750	Hint/Name RVA	038B WriteFile
00009914	0000B742	Hint/Name RVA	02C8 SearchPathA
00009918	0000B734	Hint/Name RVA	0061 CreatePipe
0000991C	0000B720	Hint/Name RVA	013B GetCurrentProcess
00009920	0000B7CC	Hint/Name RVA	015D GetFileTime
00009924	0000B6FC	Hint/Name RVA	0062 CreateProcessA
00009928	0000B6EC	Hint/Name RVA	027F PeekNamedPipe
0000992C	0000B6D6	Hint/Name RVA	0152 GetExitCodeProcess
00009930	0000B6CA	Hint/Name RVA	02A3 ReadFile
00009934	0000B6B4	Hint/Name RVA	013C GetCurrentProcessId
00009938	0000B6A0	Hint/Name RVA	0175 GetModuleHandleA
0000993C	0000B68A	Hint/Name RVA	0173 GetModuleFileNameA
00009940	0000B67C	Hint/Name RVA	0274 OpenProcess
00009944	0000B668	Hint/Name RVA	02A6 ReadProcessMemory
00009948	0000B654	Hint/Name RVA	0346 TerminateProcess
0000994C	0000B630	Hint/Name RVA	0304 SetFileAttributesA
00009950	0000B622	Hint/Name RVA	0081 DeleteFileA
00009954	0000B61A	Hint/Name RVA	033E Sleep
00009958	0000B8A6	Hint/Name RVA	0292 QueryPerformanceFrequency
0000995C	0000B7DA	Hint/Name RVA	004F CreateFileA
00009960	0000B7E8	Hint/Name RVA	01E5 GetWindowsDirectoryA
00009964	0000B800	Hint/Name RVA	03B3 lstrlenA
00009968	0000B80C	Hint/Name RVA	02F7 SetCurrentDirectoryA
0000996C	0000B824	Hint/Name RVA	016B GetLocaleInfoA
00009970	0000B836	Hint/Name RVA	01DB GetVersionExA
00009974	0000B846	Hint/Name RVA	010D GetComputerNameA
00009978	0000B85A	Hint/Name RVA	01F6 GlobalMemoryStatus
0000997C	0000B870	Hint/Name RVA	0146 GetDiskFreeSpaceExA
00009980	0000B886	Hint/Name RVA	014B GetDriveTypeA
00009984	0000B70E	Hint/Name RVA	0091 DuplicateHandle
00009988	0000B646	Hint/Name RVA	0031 CloseHandle
0000998C	0000B966	Hint/Name RVA	0300 SetErrorMode
00009990	0000B956	Hint/Name RVA	005C CreateMutexA
00009994	0000B94A	Hint/Name RVA	03A7 lstrcmpA
00009998	0000B932	Hint/Name RVA	0240 LeaveCriticalSection
0000999C	0000B91A	Hint/Name RVA	0096 EnterCriticalSection
000099A0	0000B8FE	Hint/Name RVA	0215 InitializeCriticalSection
000099A4	0000B8EC	Hint/Name RVA	0347 TerminateThread
000099A8	0000B8DC	Hint/Name RVA	0221 IsBadCodePtr
000099AC	0000B8C2	Hint/Name RVA	0291 QueryPerformanceCounter
000099B0	0000B896	Hint/Name RVA	01D1 GetTickCount
000099B4	00000000	End of Imports	KERNEL32.dll



```
000099B8   0000BA9A   Hint/Name RVA   0134  _itoa
000099BC   0000B5F4   Hint/Name RVA   01E1  _vsnprintf
000099C0   0000B4BC   Hint/Name RVA   02BE  strlen
000099C4   0000B5E8   Hint/Name RVA   02DC  vsprintf
000099C8   0000B5D6   Hint/Name RVA   00A6  _beginthreadex
000099CC   0000B5C2   Hint/Name RVA   00CA  _except_handler3
000099D0   0000B5BA   Hint/Name RVA   0249  exit
000099D4   0000B5B0   Hint/Name RVA   02A7  realloc
000099D8   0000B5A6   Hint/Name RVA   02C0  strncmp
000099DC   0000B59A   Hint/Name RVA   01AE  _snprintf
000099E0   0000B590   Hint/Name RVA   02C5  strstr
000099E4   0000B586   Hint/Name RVA   02B5  sscanf
000099E8   0000B57E   Hint/Name RVA   0257  fopen
000099EC   0000B574   Hint/Name RVA   024C  fclose
000099F0   0000B56A   Hint/Name RVA   0266  fwrite
000099F4   0000B562   Hint/Name RVA   0264  ftell
000099F8   0000B558   Hint/Name RVA   02C1  strncpy
000099FC   0000B54E   Hint/Name RVA   02B6  strcat
00009A00   0000B544   Hint/Name RVA   02B2  sprintf
00009A04   0000B53A   Hint/Name RVA   0291  malloc
00009A08   0000B532   Hint/Name RVA   025E  free
00009A0C   0000B52A   Hint/Name RVA   023D  atoi
00009A10   0000B520   Hint/Name RVA   02BA  strcpy
00009A14   0000B516   Hint/Name RVA   02B8  strcmp
00009A18   0000B50C   Hint/Name RVA   0296  memcmp
00009A1C   0000B504   Hint/Name RVA   0243  clock
00009A20   0000B4FA   Hint/Name RVA   0299  memset
00009A24   0000B4F0   Hint/Name RVA   0298  memmove
00009A28   0000B4E8   Hint/Name RVA   019C  _rotr
00009A2C   0000B4DE   Hint/Name RVA   0297  memcpy
00009A30   0000B4D6   Hint/Name RVA   019B  _rotl
00009A34   0000B4CE   Hint/Name RVA   00F1  _ftol
00009A38   0000B4C6   Hint/Name RVA   0241  ceil
00009A3C   0000BA8E   Hint/Name RVA   01BD  _strcmpi
00009A40   0000BAA2   Hint/Name RVA   01C5  _strnicmp
00009A44   00000000   End of Imports  MSVCRT.dll
00009A48   0000BA72   Hint/Name RVA   0107  ShellExecuteA
00009A4C   00000000   End of Imports  SHELL32.dll
00009A50   0000B984   Hint/Name RVA   02D8  wsprintfA
00009A54   00000000   End of Imports  USER32.dll
```



```
00009A58    80000012    Ordinal                   0012
00009A5C    80000015    Ordinal                   0015
00009A60    80000097    Ordinal                   0097
00009A64    8000000D    Ordinal                   000D
00009A68    80000005    Ordinal                   0005
00009A6C    8000000A    Ordinal                   000A
00009A70    80000002    Ordinal                   0002
00009A74    80000016    Ordinal                   0016
00009A78    80000074    Ordinal                   0074
00009A7C    80000033    Ordinal                   0033
00009A80    8000006F    Ordinal                   006F
00009A84    80000070    Ordinal                   0070
00009A88    80000034    Ordinal                   0034
00009A8C    80000006    Ordinal                   0006
00009A90    80000008    Ordinal                   0008
00009A94    80000017    Ordinal                   0017
00009A98    80000009    Ordinal                   0009
00009A9C    8000000B    Ordinal                   000B
00009AA0    80000004    Ordinal                   0004
00009AA4    80000013    Ordinal                   0013
00009AA8    80000073    Ordinal                   0073
00009AAC    8000000C    Ordinal                   000C
00009AB0    80000003    Ordinal                   0003
00009AB4    80000010    Ordinal                   0010
00009AB8    00000000    End of Imports            WS2_32.dll
```