1.0 Summary

Findings and observations:
This sample is essentially a launcher for an encrypted payload. This overall malware package establishes C2 via IRC and allows for a robust level of control on infected machines. This malware also indicates that it can be used for typical botnet operations (e.g., scanning for new victims, exploiting targets, etc.)

Recommendations:
When this sample was run as a regular (unprivileged) user, it appeared unable to fully execute however it still did appear to establish C2. Keeping regular users in appropriate (non-admin) levels of access appears to impede this sample's operations. Specifically, running as a regular user should prevent the sample from achieving persistence which would result in the sample being removed from the host upon reboot.

C2, for the time being, is located at her.d0kbilo.com (currently resolving to 37.59.118.41) on port 4466. Restricting access to this domain, IP address and port would impede or eliminate the C2 function.

Conclusion:
A skillfully executed bot client that uses multiple anti-analysis techniques to hamper the analyst.

1.1 Identification

File Name: `fcc038bc5b7297dffa9a78424c71674f (assigned by honeypot) / malexe001.exe`
File Type: Windows executable
Malware name(s): BEAR
Current detection:42/53
Malware type: Bot client / launcher
Size: 74,752 bytes
Packer: None
Encryption/encoding: Rijndael / AES (possibly 256-bit), base64
Origin: Dionaea honeypot running in New York City (also obtained about a week later in a German honeypot)
Compile time: 04JUN2016 11:23:46Z

Hashes:

```
MD5:fcc038bc5b7297dffa9a78424c71674f
SHA1:ba71062e5266b3e70e3e15b2d963ec7d5e375933
SHA256:f6fb4bde73ca1fff1fc90cff03f5c8255467b8b3d7f54330f39ecc3fa48f0e51
ssdeep:
1536:W/sLo8xocXN5U3FjAXScUC30SWEk4JgTqkKk6YqwFYtitK2TZ:WEL9okN5U3FjtQ0SWyJgT5D6wK2
```

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): ntdll, kernel32
Exports: None
Other: Requires Internet connection in order to access C2 via IRC on port 4466

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.

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.

2.3 Persistence
When running as a regular user, persistence isn't achieved. When running with administrator privileges, the malware executes a series of process replacements (between 4 and 16 were observed) of various executables before finally setting the last one to autorun. Upon reboot, the final two steps are executed (the autorun executes, which causes the final process to be replaced per the final two steps of the previous procedure).

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.

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 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.

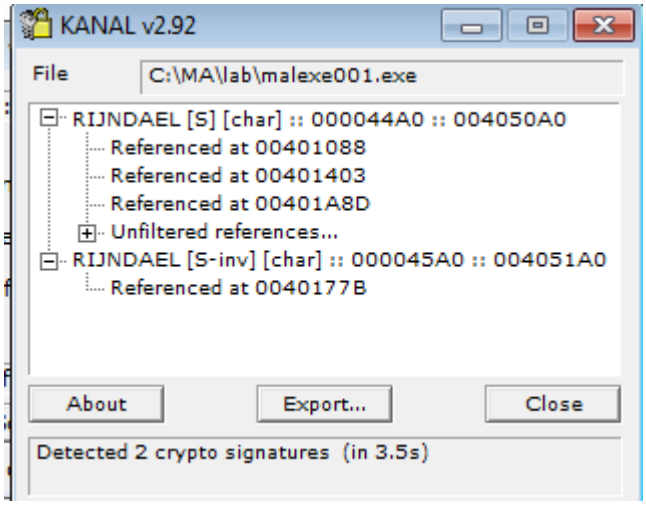
The malware appears as a process with the same name as the file. The child process is created with the same name, but then random windows processes are created and replaced with the malware payload. When running in admin mode, any one of a number of processes can be replaced such as winamp.exe, algs.exe, logon.exe, winlogon.exe, spoolsvc.exe, spoolsv.exe, lssas.exe, iexplore.exe, and possibly others that were not yet observed. In several runs of this sample, the number of processes created and

replaced by the malware ranged from 4 to 16 different processes. 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.

IRC traffic can be observed to her.d0kbilo.com on port 4466. This domain always resolves to 37.59.118.41 at this time.

3.0 Raw Notes




```
# Hosts
#
# 5 entries.

37.59.118.41    her.d0kbilo.com
```

pFile	Data	Description	Value
00004400	000056C8	Hint/Name RVA	007D ExitProcess
00004404	000056D6	Hint/Name RVA	0296 Sleep
00004408	000056DE	Hint/Name RVA	013E GetProcAddress
0000440C	000056F0	Hint/Name RVA	0126 GetModuleHandleA
00004410	00005704	Hint/Name RVA	0124 GetModuleFileNameA
00004414	0000571A	Hint/Name RVA	016D GetTickCount
00004418	00005738	Hint/Name RVA	0199 HeapAlloc
0000441C	00005744	Hint/Name RVA	019F HeapFree
00004420	00005750	Hint/Name RVA	0150 GetStartupInfoA
00004424	00005762	Hint/Name RVA	00CA GetCommandLineA
00004428	00005774	Hint/Name RVA	0174 GetVersion
0000442C	00005782	Hint/Name RVA	019D HeapDestroy
00004430	00005790	Hint/Name RVA	019B HeapCreate
00004434	0000579E	Hint/Name RVA	02BF VirtualFree
00004438	000057AC	Hint/Name RVA	02BB VirtualAlloc
0000443C	000057BC	Hint/Name RVA	01A2 HeapReAlloc
00004440	000057CA	Hint/Name RVA	029E TerminateProcess
00004444	000057DE	Hint/Name RVA	00F7 GetCurrentProcess
00004448	000057F2	Hint/Name RVA	02AD UnhandledExceptionFilter
0000444C	0000580E	Hint/Name RVA	00B2 FreeEnvironmentStringsA
00004450	00005828	Hint/Name RVA	00B3 FreeEnvironmentStringsW
00004454	00005842	Hint/Name RVA	02D2 WideCharToMultiByte
00004458	00005858	Hint/Name RVA	0106 GetEnvironmentStrings
0000445C	00005870	Hint/Name RVA	0108 GetEnvironmentStringsW
00004460	0000588A	Hint/Name RVA	026D SetHandleCount
00004464	0000589C	Hint/Name RVA	0152 GetStdHandle
00004468	000058AC	Hint/Name RVA	0115 GetFileType
0000446C	000058BA	Hint/Name RVA	022F RtlUnwind
00004470	000058C6	Hint/Name RVA	02DF WriteFile
00004474	000058D2	Hint/Name RVA	00BF GetCPInfo
00004478	000058DE	Hint/Name RVA	00B9 GetACP
0000447C	000058E8	Hint/Name RVA	0131 GetOEMCP
00004480	000058F4	Hint/Name RVA	01C2 LoadLibraryA
00004484	00005904	Hint/Name RVA	01E4 MultiByteToWideChar
00004488	0000591A	Hint/Name RVA	01BF LCMapStringA
0000448C	0000592A	Hint/Name RVA	01C0 LCMapStringW
00004490	0000593A	Hint/Name RVA	0153 GetStringTypeA
00004494	0000594C	Hint/Name RVA	0156 GetStringTypeW
00004498	00000000	End of Imports	KERNEL32.dll

Notable strings found in the initial instance of the malware memory:

```
!This program cannot be run in DOS mode.
BcH
Rich ||[
.text
`.rdata
@.data
runtime error
TLOSS error
SING error
```

```
DOMAIN error
- unable to initialize heap
- not enough space for lowio initialization
- not enough space for stdio initialization
- pure virtual function call
- not enough space for _onexit/atexit table
- unable to open console device
- unexpected heap error
- unexpected multithread lock error
- not enough space for thread data
abnormal program termination
- not enough space for environment
- not enough space for arguments
- floating point not loaded
Microsoft Visual C++ Runtime Library
Runtime Error!
Program:
<program name unknown>
GetLastActivePopup
GetActiveWindow
MessageBoxA
user32.dll
ExitProcess
Sleep
GetProcAddress
GetModuleHandleA
GetModuleFileNameA
GetTickCount
KERNEL32.dll
HeapAlloc
HeapFree
GetStartupInfoA
GetCommandLineA
GetVersion
HeapDestroy
HeapCreate
VirtualFree
VirtualAlloc
HeapReAlloc
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
FreeEnvironmentStringsA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
SetHandleCount
GetStdHandle
GetFileType
RtlUnwind
WriteFile
GetCPInfo
GetACP
GetOEMCP
LoadLibraryA
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
!This program cannot be run in DOS mode.
Rich
.text
.rdata
@.data
strlen
ceil
_ftol
_rotl
memcpy
_rotr
memmove
memset
clock
```

memcmp
strcmp
strcpy
atoi
free
malloc
sprintf
strcat
strncpy
ftell
fwrite
fclose
fopen
sscanf
strstr
_snprintf
strncmp
realloc
exit
_except_handler3
_beginthreadex
vsprintf
_vsnprintf
MSVCRT.dll
WS2_32.dll
Sleep
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
WORKGROUPlQPxf2ISQgEV1bGK
\browser
\..\..\AOHLMXY
tVersionExA
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
_itoa
_strnicmp
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
D CKFDENECFDEFFCFGEFFCCACACACACACA
EKEDFEEIEDCACACACACACACACACACAAA
SMBr
PC NETWORK PROGRAM 1.0
LANMAN1.0
Windows for Workgroups 3.1a
LM1.2X002
LANMAN2.1
NT LM 0.12
SMBs
9NTLMSSP
WORKGROUPlQPxf2ISQgEV1bGKWindows 2000 2195
Windows 2000 5.0
NTLMSSP
Windows 2000 2195
Windows 2000 5.0
WORKGROUP
Windows 2000 2195
Windows 2000 5.0
FUnMLEvdNzjntXznAvcOSDvcUlULLFJmCPCmjgeXpbDCIAtjDTRPAxyXItXCfDxvjRXtWSyACqcPrzWHeaUKfrohnEuSyZUzPzbe
PITH
IFJUOUTEPUWKXMWXUGHMIEKCYENBAQPLZEDNOOBGMW
bMZCTWLHYWI
D CKFDENECFDEFFCFGEFFCCACACACACACA
EKEDFEEIEDCACACACACACACACACACAAA
NT LM 0.12
pysmb
Samba *
Windows 5.1
Windows 5.0
Windows 2000 LAN Manager*
NT LAN Manager *.*
Service Pack 2
Service Pack 1
Windows Server 2003 *.*
Scanned
:%s in
sec.
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
open
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
.exe
QUIT :restarting
QUIT :exitting
debug
- 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
%u.%u.%u.%u
GetModuleInformation
GetModuleFileNameExA
EnumProcessModules
EnumProcesses
psapi.dll
system
SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\Li
st
%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
.bat
Windows DLL Loader
QUIT :%s uninstalled.
%s.%s.%s.%s
USA
System information - OS: Windows
). CPU: %s
MHz. Ram:
MB free. IPv6:
. Uptime:
day%s
hour%s
minute%s. Computername:
. User:
ProcessorNameString
HARDWARE\DESCRIPTION\System\CentralProcessor\0
Yes
no SP
Sysinfo thread
Network information - Host:
. Name:
. Type:
. IPv6:
. Firewalled:
. Latency:
, %u. IRC Uptime:
day%s
hour%s
minute%s.
Good
Avarage
Bad
LAN
Modem
Unknown
Netinfo thread
%sTotal drives:
, Total space:
MB free.
MB free
unknown
ramdisk
cd-rom
remote

fixed
removable
Drive information -
Driveinfo thread
thread
btg
debug
- 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.
off
Exe download server:
none
Exe download server:
f128enc+fab decrypted:
f128enc+fab encrypted: =
%c%s%c%c%u%c%u%s%c%c%c
UNK
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
NICK
USERHOST %s
JOIN %s %s
MODE %s +xi
MODE %s +smntu
JOIN
ERROR
VERSION %s
eggdrop v1.6.16
VERSION link v%d.%03d%s (Win32)
PING
PING
VERSION
VERSION
SEND
DCC
PRIVMSG
MODE
PONG
PONG %s
PING
link!link@link
ndEvery1
#balengor
debug
- eip has left the endless loop for some reason...
entry
main
loop
PING :%08X
%08x%x%08x%3x%08x%08x
C:\MA\lab\malexe001.exe
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Notable strings found in the second (child) instance of the .exe:

```
WORKGROUPlQPxf2ISQgEV1bGK
\browser
\..\..\AOHLMXY
!This program cannot be run in DOS mode.
Rich
.text
.rdata
@.data
strlen
ceil
_ftol
_rotl
memcpy
_rotr
memmove
memset
clock
memcmp
strcmp
strcpy
atoi
free
malloc
sprintf
strcat
strncpy
ftell
fwrite
fclose
fopen
sscanf
strstr
_snprintf
strncmp
realloc
exit
_except_handler3
_beginthreadex
vsprintf
_vsnprintf
MSVCRT.dll
WS2_32.dll
Sleep
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
_itoa
_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
SMBs
NTLMSSP
Windows 2000 2195
Windows 2000 5.0
SMBs
WORKGROUP
Windows 2000 2195
Windows 2000 5.0
FUnMLEvdNzjntXznAvcOSDvcUlULLFJmCPCmjgeXpbDCIAtjDTRPAxyXItXCfDxvjRXtWSyACqcPrzWHeaUKfrohnEuSyZUzPzbe
PITH
IFJUOUTEPUWKXMWXUGHMIEKCYENBAQPLZEDNOOBGMW
bMZCTWLHYWI
D CKFDENECFDEFFCFGEFFCCACACACACACA
EKEDFEEIEDCACACACACACACACACACAAA
NT LM 0.12
pysmb
Samba *
Windows 5.1
Windows 5.0
Windows 2000 LAN Manager*
NT LAN Manager *.*
Service Pack 2
Service Pack 1
Windows Server 2003 *.*
Scanned
:%s in
sec.

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
open
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
.exe
QUIT :restarting
QUIT :exitting
debug
- 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
%u.%u.%u.%u
GetModuleInformation
GetModuleFileNameExA
EnumProcessModules
EnumProcesses
psapi.dll
system
SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\Li
%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
.bat
Windows DLL Loader
QUIT :%s uninstalled.
%s.%s.%s.%s
USA
System information - OS: Windows
). CPU: %s
MHz. Ram:
MB free. IPv6:
. Uptime:
day%s
hour%s
minute%s. Computername:
. User:
ProcessorNameString
HARDWARE\DESCRIPTION\System\CentralProcessor\0
Yes
no SP
Sysinfo thread
Network information - Host:
. Name:
. Type:
. IPv6:
. Firewalled:
. Latency:
, %u. IRC Uptime:
day%s
hour%s
minute%s.
Good

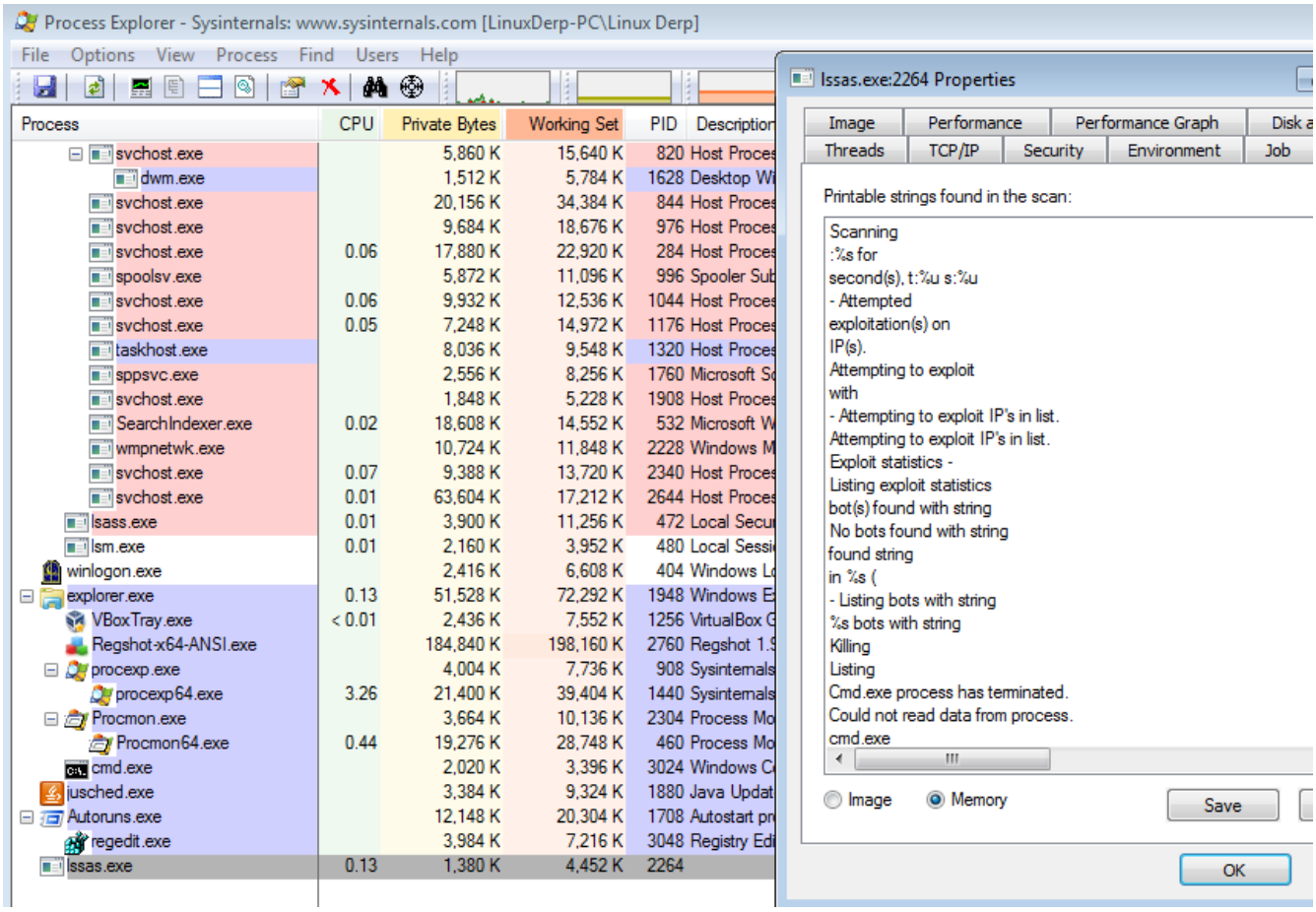
Avarage
Bad
LAN
Modem
Unknown
Netinfo thread
%sTotal drives:
, Total space:
MB free.
MB free
unknown
ramdisk
cd-rom
remote
fixed
removable
Drive information -
Driveinfo thread
thread
btg
debug
- btg tried executing an unreadable address. (%08X)
- No threads running.
- Listing
threads:
QUIT :changing server
link v
%s [Win32]
Uptime - System:
day%s
hour%s
minute%s. IRC:
day%s
hour%s
minute%s
Debug mode is %s.
off
Exe download server:
none
Exe download server:
f128enc+fab decrypted:
f128enc+fab encrypted: =
%c%s%c%c%u%c%u%s%c%c%c
UNK
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
NICK
USERHOST %s
JOIN %s %s
MODE %s +xi
MODE %s +smntu
JOIN
ERROR
VERSION %s
eggdrop v1.6.16
VERSION link v%d.%03d%s (Win32)
PING
PING
VERSION
VERSION
SEND
DCC
PRIVMSG
MODE
PONG
PONG %s
PING

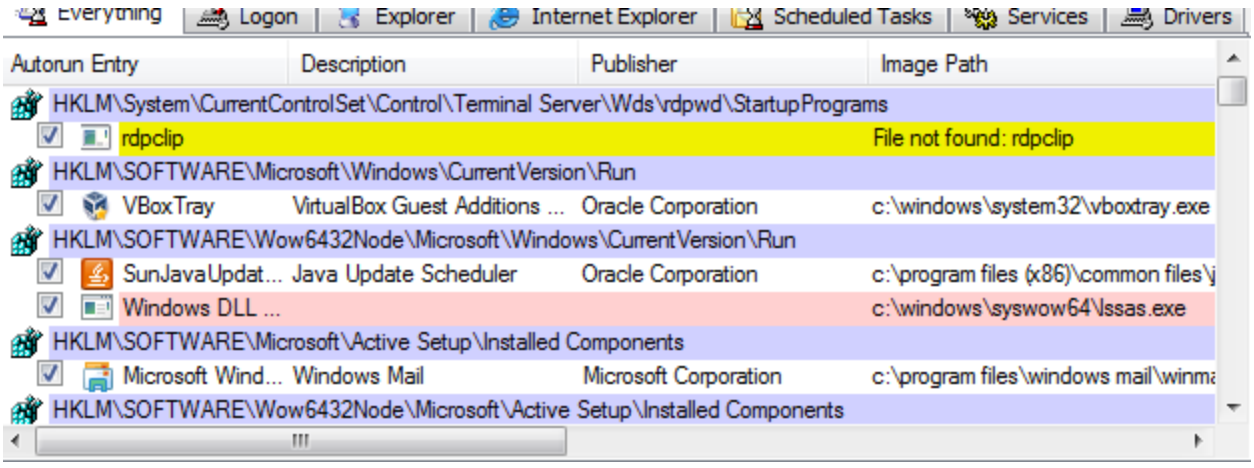
link!link@link
ndEvery1
#balengor
debug
- eip has left the endless loop for some reason...
entry
main
loop
PING :%08X
%08x%x%08x%3x%08x%08x
malexe001.exe [this is the name of the executable that I assigned to it for analysis]

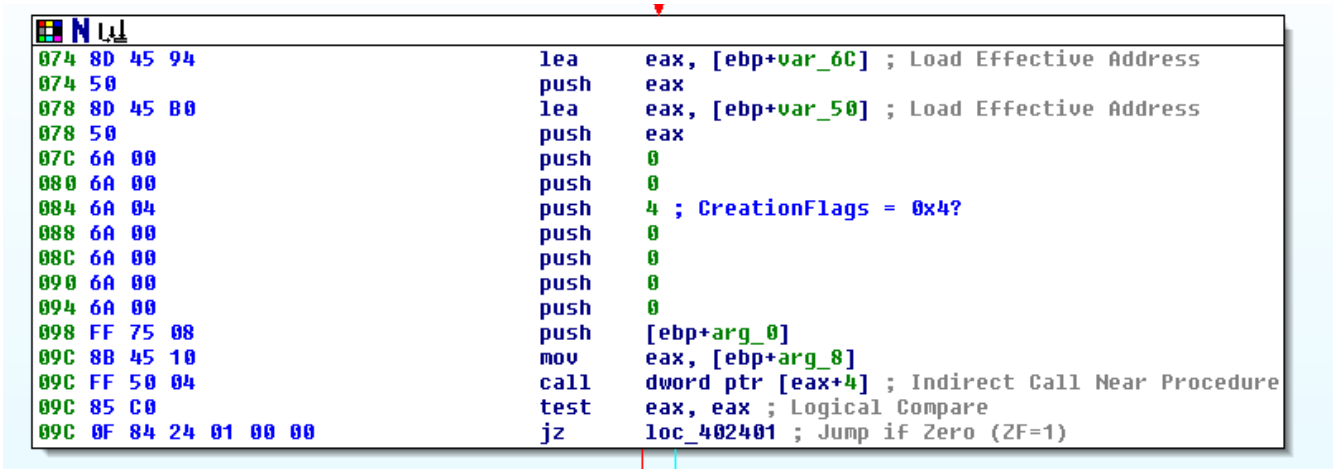
Observed the following function names get generated within the sample while debugging:
CreateProcessA
NtUnmapViewOfSection
VirtualAllocEx
WriteProcessMemory
GetThreadContext
SetThreadContext
ResumeThread
ReadProcessMemory
VirtualAlloc
VirtualFree

Dropped batch file:
@echo off
:deleteagain
del /A:H /F malexe001.exe
del /F malexe001.exe
if exist malexe001.exe goto deleteagain
del wcsqmpbh.bat

Persistence registry change:
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Windows DLL Loader:
"C:\Windows\system32\iexplore.exe"


Process Explorer - Sysinternals: www.sysinternals.com [LinuxDerp-PC\Linux Derp]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description
svchost.exe 5,860 K 15,640 K 820 Host Proces
dwm.exe 1,512 K 5,784 K 1628 Desktop Wi
svchost.exe 20,156 K 34,384 K 844 Host Proces
svchost.exe 9,684 K 18,676 K 976 Host Proces
svchost.exe 0.06 17,880 K 22,920 K 284 Host Proces
spoolsv.exe 5,872 K 11,096 K 996 Spooler Sub
svchost.exe 0.06 9,932 K 12,536 K 1044 Host Proces
svchost.exe 0.05 7,248 K 14,972 K 1176 Host Proces
taskhost.exe 8,036 K 9,548 K 1320 Host Proces
sppsvc.exe 2,556 K 8,256 K 1760 Microsoft Sc
svchost.exe 1,848 K 5,228 K 1908 Host Proces
SearchIndexer.exe 0.02 18,608 K 14,552 K 532 Microsoft W
wmpnetwk.exe 10,724 K 11,848 K 2228 Windows M
svchost.exe 0.07 9,388 K 13,720 K 2340 Host Proces
svchost.exe 0.01 63,604 K 17,212 K 2644 Host Proces
lsass.exe 0.01 3,900 K 11,256 K 472 Local Secur
lsm.exe 0.01 2,160 K 3,952 K 480 Local Sessi
winlogon.exe 2,416 K 6,608 K 404 Windows Lo
explorer.exe 0.13 51,528 K 72,292 K 1948 Windows E
VBoxTray.exe < 0.01 2,436 K 7,552 K 1256 VirtualBox G
Regshot-x64-ANSI.exe 184,840 K 198,160 K 2760 Regshot 1.9
procexp.exe 4,004 K 7,736 K 908 Sysinternals
procexp64.exe 3.26 21,400 K 39,404 K 1440 Sysinternals
Procmon.exe 3,664 K 10,136 K 2304 Process Mo
Procmon64.exe 0.44 19,276 K 28,748 K 460 Process Mo
cmd.exe 2,020 K 3,396 K 3024 Windows C
jusched.exe 3,384 K 9,324 K 1880 Java Updat
Autoruns.exe 12,148 K 20,304 K 1708 Autostart pr
regedit.exe 3,984 K 7,216 K 3048 Registry Edi
lssas.exe 0.13 1,380 K 4,452 K 2264
lssas.exe:2264 Properties
Image Performance Performance Graph Disk a
Threads TCP/IP Security Environment Job
Printable strings found in the scan:
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
Image Memory Save
OK


Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers
Autorun Entry Description Publisher Image Path
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms
rdpclip File not found: rdpclip
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
VBoxTray VirtualBox Guest Additions ... Oracle Corporation c:\windows\system32\vboxtray.exe
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
SunJavaUpdat... Java Update Scheduler Oracle Corporation c:\program files (x86)\common files\j
Windows DLL ... c:\windows\syswow64\lssas.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
Microsoft Wind... Windows Mail Microsoft Corporation c:\program files\windows mail\winma
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components



```
074 8D 45 94                        lea     eax, [ebp+var_6C] ; Load Effective Address
074 50                              push    eax
078 8D 45 B0                        lea     eax, [ebp+var_50] ; Load Effective Address
078 50                              push    eax
07C 6A 00                           push    0
080 6A 00                           push    0
084 6A 04                           push    4 ; CreationFlags = 0x4?
088 6A 00                           push    0
08C 6A 00                           push    0
090 6A 00                           push    0
094 6A 00                           push    0
098 FF 75 08                        push    [ebp+arg_0]
09C 8B 45 10                        mov     eax, [ebp+arg_8]
09C FF 50 04                        call    dword ptr [eax+4] ; Indirect Call Near Procedure
09C 85 C0                           test    eax, eax ; Logical Compare
09C 0F 84 24 01 00 00               jz      loc_402401 ; Jump if Zero (ZF=1)
```