

## 1.0 Summary

Findings and observations:

Mass-mailer worm. Similar to the prior sample analyzed, which I believe was derived from this new sample as this sample did not appear to have the execution issues observed previously. Sample appears to both scan new IP addresses, both for remote and local systems, probably with the intent of spreading itself. It also contains functionality around reporting system inventory and sending spam messages.

Recommendations:

- Block ports 445, 137, and 138 as this is where this sample was obtained and this sample was observed connecting to remote and local systems on these ports
- **Block port 186 as this is the port that the .rsrc payload file listens on**
- Usual recommendations against opening unsolicited mail (especially with attachments)
- Filter email associated with "[microsoft@microsoft.com](mailto:microsoft@microsoft.com)", "[information@microsoft.com](mailto:information@microsoft.com)", and "[john@barrysworld.com](mailto:john@barrysworld.com)", "[wbInfo0801@gmail.com](mailto:wbInfo0801@gmail.com)", "[wbInfo0802@gmail.com](mailto:wbInfo0802@gmail.com)"

Conclusion:

Interesting, old malware. It was good to see this worm running successfully so as to get a better opportunity to view its capabilities.

### 1.1 Identification

File Name: smb-utcm3rlu.exe

File Type: Windows executable

Malware name(s): Pepex

Current detection: 50/54 packed, 31/53 manually unpacked, 48/54 automatically unpacked

Malware type: Mass-mailer worm

Size: 33,128 bytes packed / 143,360 bytes manually unpacked / 67,072 automatically unpacked

Packer: Upack 0.39beta, Petite 2.x

Encryption/encoding: zlib detected within the .rsrc section

Origin: Dionaea honeypot running in New York City

Compile time: 2004-01-23 23:39:42

### Hashes:

Packed:

MD5: 7867de13bf22a7f3e3559044053e33e7

SHA1: 42e56d72982ac04edba2ce7fb9f4e5048766aa94

SHA256: a29d02251f54567edb1d32f7c17ce4c04d5c54e317eb3b2bea2a068da728e59a

ssdeep: 768: W0jL5WyEf531YmKtLZSI1Z0t13hHJ6kekGyQSm0Y: W0jSyEfIm0i3Z0t1RWkGyFW

Manually Unpacked:

MD5: 30891d0c95aed62d3cbf7a54239eaf17

SHA1: b3d456d0cd871b1ff5f19cd3196ebe4df064f922

SHA256: 50f3cd50216c6a4515977f46a737466bb3cc3a3cdf3add771e1e8c138dea91e4

ssdeep: 1536: oNx2Tahizzme4WPsyqFg8NIRdcBCai0jsyEfIm0i3Z0t1RWkGyF3XFuTx+WN: 8DYzzNhPJgI3iCaIH0i3Z0t1RWRNB

Automatically Unpacked:

MD5: c6829041ed0a3b1ee41b8aad7e1884b1

SHA1: 440c45dff7f43ac6478c44a1c776e643320a8a35

SHA256: 6c31f261514aa5d4b9e0098d7362dd8357a71ca9de5d3df984d4dfd80c75690c

ssdeep: 768: 8HcGaNhoWx2T7G8HEExZz+v25i6jQSGm51/GVGWsyqAgg8/8WIjL2QDMrL4: 7Nx2Tahizz1ko0VpsyqFg8NIRd

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: MS Windows NT and above

Imports (DLLs): Kernel32, User32, AdvApi32, WS2\_32  
Exports: None  
Other: N/A

## 2.0 Characteristics

### 2.1 Behavior

Sample will either work to scan for vulnerable local and remote machines to spread itself, or begin mass-mailing spam. Sample also appears to report system inventory information via email. **There is a binary within the .rsrc section that is installed and appears to have both a system inventory and C2 function.**

### 2.2 Infection

Malware appears to spread through SMB (ports 445 remotely, 137 and 138 locally). Reading online about various versions of this sample also indicates that the mass-mailing function attempts to spread the malware as email attachments.

### 2.3 Persistence

The malware attempts to install itself to run at startup as "Windows Update" under this key:  
SOFTWARE\Microsoft\Windows\CurrentVersion\Run

**The .rsrc payload file also installs itself by copying itself as %system%\system32\LSASvc.exe and then creating itself as a service that will autorun at boot:**

```
-----  
Keys added: 2  
-----  
HKLM\SYSTEM\ControlSet001\services\LSAService  
HKLM\SYSTEM\CurrentControlSet\services\LSAService  
  
-----  
Values added: 14  
-----  
HKLM\SYSTEM\ControlSet001\services\LSAService\Type: 0x00000010  
HKLM\SYSTEM\ControlSet001\services\LSAService\Start: 0x00000002  
HKLM\SYSTEM\ControlSet001\services\LSAService\ErrorControl: 0x00000001  
HKLM\SYSTEM\ControlSet001\services\LSAService\ImagePath: "C:\Windows\system32\LSASvc.exe"  
HKLM\SYSTEM\ControlSet001\services\LSAService\DisplayName: "Microsoft LSA Logon Authorization Service"  
HKLM\SYSTEM\ControlSet001\services\LSAService\WOW64: 0x00000001  
HKLM\SYSTEM\ControlSet001\services\LSAService\ObjectName: "LocalSystem"  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\Type: 0x00000010  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\Start: 0x00000002  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\ErrorControl: 0x00000001  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\ImagePath: "C:\Windows\system32\LSASvc.exe"  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\DisplayName: "Microsoft LSA Logon Authorization Service"  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\WOW64: 0x00000001  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\ObjectName: "LocalSystem"
```

### 2.4 Movement

As noted earlier, the sample tries to move via SMB on port 445 (for remote systems) and SMB on ports 137 and 138 for local networks. Material available online about this sample suggests that it also moves to other systems via email attachments as part of the mass-mailer function.

### 2.5 Data Exfiltration

It appears that this sample sends system inventory data to one of two addresses:  
[wbInfo0801@gmail.com](mailto:wbInfo0801@gmail.com) or [wbInfo0802@gmail.com](mailto:wbInfo0802@gmail.com).

## 2.6 C<sup>2</sup>

Not specifically observed, though it was seen that the .rsrc payload listens on port 186 which could be for C2 purposes.

## 2.7 Signatures

File system:

Creation of file: lsasvc.exe

Creation of service: WUpdate / Windows Genuine Update

Creation of registry value to run at boot: SOFTWARE\Microsoft\Windows\CurrentVersion\Run, "Windows Update"

Additional .rsrc payload registry changes:

```
-----  
Keys added: 2  
-----  
HKLM\SYSTEM\ControlSet001\services\LSAService  
HKLM\SYSTEM\CurrentControlSet\services\LSAService
```

```
-----  
Values added: 14  
-----  
HKLM\SYSTEM\ControlSet001\services\LSAService\Type: 0x00000010  
HKLM\SYSTEM\ControlSet001\services\LSAService\Start: 0x00000002  
HKLM\SYSTEM\ControlSet001\services\LSAService\ErrorControl: 0x00000001  
HKLM\SYSTEM\ControlSet001\services\LSAService\ImagePath: "C:\Windows\system32\LSASvc.exe"  
HKLM\SYSTEM\ControlSet001\services\LSAService\DisplayName: "Microsoft LSA Logon Authorization Service"  
HKLM\SYSTEM\ControlSet001\services\LSAService\WOW64: 0x00000001  
HKLM\SYSTEM\ControlSet001\services\LSAService\ObjectName: "LocalSystem"  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\Type: 0x00000010  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\Start: 0x00000002  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\ErrorControl: 0x00000001  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\ImagePath: "C:\Windows\system32\LSASvc.exe"  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\DisplayName: "Microsoft LSA Logon Authorization Service"  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\WOW64: 0x00000001  
HKLM\SYSTEM\CurrentControlSet\services\LSAService\ObjectName: "LocalSystem"
```

Network:

SMTP traffic for mass-mailing activity

Heavy IP address/port scanning activity (tens of thousands in a matter of minutes, ports 445, 137, 138)

Listening on port 186

## 3.0 Raw Notes

Unpacked strings:

Strings v2.51  
Copyright (C) 1999-2013 Mark Russinovich  
Sysinternals - www.sysinternals.com

```
MZP  
!This program cannot be run in DOS mode.  
.code  
.data  
.idata  
.rsrc  
ppxxxx  
(null)  
(null)  
runtime error  
TLOSS error  
SING error  
DOMAIN error  
R6028  
- unable to initialize heap  
R6027  
- not enough space for lowio initialization  
R6026  
- not enough space for stdio initialization  
R6025
```

- pure virtual function call  
R6024  
- not enough space for \_onexit/atexit table  
R6019  
- unable to open console device  
R6018  
- unexpected heap error  
R6017  
- unexpected multithread lock error  
R6016  
- not enough space for thread data  
abnormal program termination  
R6009  
- not enough space for environment  
R6008  
- not enough space for arguments  
R6002  
- floating point not loaded  
Microsoft Visual C++ Runtime Library  
Runtime Error!  
Program:  
...  
<program name unknown>  
GetLastActivePopup  
GetActiveWindow  
MessageBoxA  
user32.dll  
H:mm:ss  
dddd, MMMM dd, yyyy  
M/d/yy  
December  
November  
October  
September  
August  
July  
June  
April  
March  
February  
January  
Dec  
Nov  
Oct  
Sep  
Aug  
Jul  
Jun  
May  
Apr  
Mar  
Feb  
Jan  
Saturday  
Friday  
Thursday  
Wednesday  
Tuesday  
Monday  
Sunday  
Sat  
Fri  
Thu  
Wed  
Tue  
Mon  
Sun  
SunMonTueWedThuFriSat  
JanFebMarAprMayJunJulAugSepOctNovDec  
130  
131  
132  
133  
134  
137

139  
140  
143  
144  
210  
200  
201  
202  
203  
210  
211  
218  
219  
220  
221  
222  
147  
149  
152  
154  
158  
159  
161  
162  
167  
168  
171  
192  
194  
195  
197  
198  
199  
200  
201  
202  
203  
210  
211  
214  
216  
218  
219  
220  
221  
224

gmail-smtp-in.l.google.com  
john@barrysworld.com  
google.com  
wbInfo0801@gmail.com  
whInfo0802@gmail.com  
test1234  
pass  
!@#\$%^&\*()  
!@#\$%^&\*(  
!@#\$%^&\*  
!@#\$%^&  
!@#\$%^  
!@#\$%  
111111  
1111  
4321  
54321  
654321  
1234567  
123456  
12345  
1234  
123  
asdfgh  
asdfg  
asdf  
BUMBLE  
angel  
password

passwd  
!@#\$  
root  
admin  
db2admin  
administrator  
%d.%d.%d.%d|  
QUIT  
Subject: Hello  
From: <  
From: "Microsoft" <information@microsoft.com>  
Reply-To: "Microsoft" <microsoft@microsoft.com>  
john@barrysworld.com  
DATA  
RCPT TO:<  
MAIL FROM:<  
HELO <  
209.85.133.114  
WUpdate  
Windows Genuine Update  
Windows Update  
SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
-i  
\lsassvc.exe  
FILE  
c:\winnt\lsass.exe  
c:\windows\lsass.exe  
%s%c\$\winnt\lsass.exe  
%s%c\$\windows\lsass.exe  
Subject: %s|%s|%s  
%s\ipc\$  
%s!@#\$  
%s2  
%s123  
%s12  
%s1  
@%s@  
@%s!@  
%s!@  
%s!  
%s%s%s  
Use  
ApiBuffe  
AddConne  
CancelCo  
Api  
rEnum  
rFree  
ction2A  
nnection2A  
32.dll  
WNet  
Net  
WinXp  
Win2003  
Unkown  
WinVista  
WinNt  
Win2000  
Subject:  
SYSTEM  
%d.%d.%d.%d  
\%s  
PST  
PDT  
KERNEL32.DLL  
WideCharToMultiByte  
MultiByteToWideChar  
FreeLibrary  
GetProcAddress  
CopyFileA  
LoadResource  
FindResourceA  
GetVersion  
GetModuleFileNameA

TerminateThread  
WaitForSingleObject  
LockResource  
GetSystemDirectoryA  
CreateFileA  
WriteFile  
CloseHandle  
CreateProcessA  
lstrlenA  
GetSystemTime  
Sleep  
LoadLibraryA  
GetModuleHandleA  
GetEnvironmentStrings  
GetEnvironmentStringsW  
TerminateProcess  
FlushFileBuffers  
GetStringTypeW  
GetLastError  
CreateThread  
GetCurrentThreadId  
TlsSetValue  
ExitThread  
GetTickCount  
GetStartupInfoA  
GetCommandLineA  
ExitProcess  
TlsAlloc  
SetLastError  
TlsGetValue  
HeapFree  
HeapAlloc  
LCMapStringW  
GetCurrentProcess  
UnhandledExceptionFilter  
RtlUnwind  
FreeEnvironmentStringsA  
FreeEnvironmentStringsW  
InterlockedDecrement  
GetStringTypeA  
SetHandleCount  
GetStdHandle  
GetFileType  
DeleteCriticalSection  
HeapDestroy  
HeapCreate  
VirtualFree  
SetFilePointer  
EnterCriticalSection  
LeaveCriticalSection  
InterlockedIncrement  
InitializeCriticalSection  
VirtualAlloc  
HeapReAlloc  
GetCPInfo  
GetACP  
GetOEMCP  
SetStdHandle  
LCMapStringA  
USER32.DLL  
wsprintfA  
ADVAPI32.DLL  
RegOpenKeyExA  
RegSetValueExA  
RegCloseKey  
OpenServiceA  
DeleteService  
OpenSCManagerA  
CreateServiceA  
CloseServiceHandle  
StartServiceA  
GetUserNameA  
WS2\_32.DLL  
FILE

!This program cannot be run in DOS mode.

Rich  
S^@  
.petite  
ERROR!  
Corrupt Data!  
ExitProcess  
LoadLibraryA  
GetProcAddress  
VirtualProtect  
GlobalAlloc  
GlobalFree  
GetModuleHandleA  
MessageBoxA  
wsprintfA  
RegCloseKey  
KERNEL32.dll  
USER32.dll  
ADVAPI32.dll  
WS2\_32.dll

.rsrc payload strings:  
!This program cannot be run in DOS mode.

Rich  
.petite  
KERNEL32.dll  
USER32.dll  
ADVAPI32.dll  
WS2\_32.dll  
runtime error  
TLOSS error  
SING error  
DOMAIN error  
R6028  
- unable to initialize heap  
R6027  
- not enough space for lowio initialization  
R6026  
- not enough space for stdio initialization  
R6025  
- pure virtual function call  
R6024  
- not enough space for \_onexit/atexit table  
R6019  
- unable to open console device  
R6018  
- unexpected heap error  
R6017  
- unexpected multithread lock error  
R6016  
- not enough space for thread data  
abnormal program termination  
R6009  
- not enough space for environment  
R6008  
- not enough space for arguments  
R6002  
- floating point not loaded  
Microsoft Visual C++ Runtime Library  
Runtime Error!  
Program:  
...  
<program name unknown>  
GetLastActivePopup  
GetActiveWindow  
MessageBoxA  
user32.dll  
CloseHandle  
WaitForSingleObject  
CreateEventA  
GetLastError  
lstrcatA  
GetSystemDirectoryA  
CopyFileA  
GetModuleFileNameA  
GetModuleHandleA



CreateThread  
lstrcmpiA  
GetVersionExA  
Sleep  
GetTickCount  
lstrlenA  
GetComputerNameA  
FindClose  
FindNextFileA  
WriteFile  
FindFirstFileA  
GetTempFileNameA  
lstrcpyA  
GetTempPathA  
CreateProcessA  
DeleteFileA  
ReadFile  
SetFilePointer  
GetFileSize  
CreateFileA  
GetDriveTypeA  
wsprintfA  
StartServiceCtrlDispatcherA  
SetServiceStatus  
RegisterServiceCtrlHandlerA  
CloseServiceHandle  
StartServiceA  
CreateServiceA  
OpenSCManagerA  
RegCloseKey  
RegQueryValueExA  
RegOpenKeyExA  
ExitProcess  
TerminateProcess  
GetCurrentProcess  
GetStartupInfoA  
GetCommandLineA  
GetVersion  
UnhandledExceptionFilter  
FreeEnvironmentStringsA  
FreeEnvironmentStringsW  
WideCharToMultiByte  
GetEnvironmentStrings  
GetEnvironmentStringsW  
SetHandleCount  
GetStdHandle  
GetFileType  
HeapDestroy  
HeapCreate  
VirtualFree  
HeapFree  
RtlUnwind  
GetCPInfo  
GetACP  
GetOEMCP  
HeapAlloc  
VirtualAlloc  
HeapReAlloc  
GetProcAddress  
LoadLibraryA  
MultiByteToWideChar  
LCMapStringA  
LCMapStringW  
GetStringTypeA  
GetStringTypeW  
This file has been tampered with and  
MAY BE INFECTED BY A VIRUS!  
Unable to load function: %s (%s)  
Unable to load ordinal: %d (%s)  
LSAService  
Microsoft LSA Logon Authorization Service  
\\LSASvc.exe  
( Win32s )  
( Windows 98 )  
( Windows 95 )

ver %d.%d %s (Build %d)  
Server  
SERVERNT  
Workstation  
WINNT  
ProductType  
SYSTEM\CurrentControlSet\Control\ProductOptions  
  ( Windows2000  
  ( WindowsNT  
  ( Unknown )  
%s <%uk>  
\*%s  
C:\  
ERROR!  
Corrupt Data!  
ExitProcess  
LoadLibraryA  
GetProcAddress  
VirtualProtect  
GlobalAlloc  
GlobalFree  
GetModuleHandleA  
MessageBoxA  
wsprintfA  
RegCloseKey  
KERNEL32.dll  
USER32.dll  
ADVAPI32.dll  
WS2\_32.dll