1.0 Summary

Findings and observations:
Mass-mailer worm with execution issues. Design flaws reveal functionality and signatures. This sample was first observed 14+ years ago, but doesn't seem to have any obvious malicious function besides wasting resources.

Recommendations:
Detection is very high for this sample, probably due to age, so up-to-date AV probably would help mitigate this sample. Not opening suspicious files received via email or other routes also stands for this sample. Use of strong passwords (and definitely NOT the very poor examples found in this malware) is advised. Removal can be done by modifying the registry entry for persistence (if successful in the first place) and also the Isass.exe file.

Conclusion:
Interesting to see this very old piece of malware, even if it didn't fully run in the test environment.

1.1 Identification

File Name: `4d56562a6019c05c592b9681e9ca2737 (packed)`
File Type: Windows executable
Malware name(s): Pepex
Current detection: 50/54 packed, 29/54 unpacked
Malware type: Worm (mass-mailer)
Size: 12,800 bytes packed / 47,104 bytes manually unpacked / 32,768 automatically unpacked
Packer: UPX
Encryption/encoding: Occasional XOR decoding of certain strings related to persistence and SMTP commands
Origin: Dionaea honeypot running in New York City
Compile time: 2011-02-01 07:31:18

Hashes:

```
Packed:
MD5:4d56562a6019c05c592b9681e9ca2737
SHA1:5e805107360e1d5f668a01ab6722791ce4c4db33
SHA256:e441718e331af69579b2699b07c8211aa776c5634e60a570099917b2f8603a29
ssdeep:192:N81SjNvWmmubvcWfEZAvpfhxT1gcfUZIEyfvxhsjg6JhJ66AjAEodg9J:NjNvWhuATOvnpfAtixhsU6Jh
J6dAKf

Manually Unpacked:
MD5:5d0991861e652a367a7ea61f4b8b2bc7
SHA1:bd4a5a341b8ebef63763567ffcb80969e65f733b
SHA256:f421df27b7c315331e7f099b42277cf946966b0e4e54a4e437c5daee60bae2f1
ssdeep:768:7jNviuAPsbuJPfMABytIT4euP4f2TKu+hLxCtJhJ6d7Tgrc7:nsPsb6XXB98QLP

Automatically Unpacked:
MD5:e0d337ff5974a26ccc1764fab553d1d2
SHA1:ad468acebc461f2ea2da53064097747c96c20741
SHA256:62ea220bd9ce404c411a6128ed23acd4dbdc0395badd5f9a054da9e83026bc75
ssdeep:384:BosbuJCIz8EM5BiYqBDGt5u4LzqNc2r81bP8uThFgNQkweWLs0s22e:msbuJPfMABytIT4euTgNQle+2
```

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): kernel32, advapi32, mscvrt, user32, ws2_32
Exports: None
Other: N/A

2.0 Characteristics

2.1 Behavior
The file attempts to resolve certain Google domains and then start mail-mailing targets via building SMTP commands. Unclear from the debugging how the email addresses are obtained, though literature suggests that it could be harvested from the host. Persistence is attempted, and the malware also tries to create a service to run itself.

2.2 Infection
Executing the malware should cause infection, though as noted above malware functionality did not fully execute in the test environment.

2.3 Persistence
Persistence is attempted by creating a copy of itself in the %system% directory as Isass.exe, and then adding a registry key to automatically run at startup:

```
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Local Security Authority
Process: “ %1”
```

2.4 Movement
Not observed, either in execution or in code, with the caveat that fully successful execution of the malware was not achieved in the test environment.

2.5 Data Exfiltration
Not observed, either in execution or in code, with the caveat that fully successful execution of the malware was not achieved in the test environment.

2.6 C^2
Not observed, either in execution or in code, with the caveat that fully successful execution of the malware was not achieved in the test environment.

2.7 Signatures
File system:
- Sample attempts to create a copy of itself in %system% as “Isass.exe”
- “stm8.inf” is also possibly observed, either in %system% or in a temporary file folder
- Registry is modified (see persistence section above) to enable autorun at boot
- Malware attempts to create a service for itself:
servicename: wgautr
displayname: Windows Genuine Updater

Network:
- Attempts to resolve several Google domains (though it’s important to keep in mind that resolving these domains is likely not malicious, which is probably why this sample uses these):
gmail-smtp-l.google.com

alt2.gmail-smtp-l.google.com
alt1.gmail-smtp-l.google.com
alt3.gmail-smtp-l.google.com
alt4.gmail-smtp-l.google.com
- Malware will try to manually construct email / SMTP commands. Not 100% clear how these look, though look for emails that include data such as “Microsoft News Letter” and addresses such as microsoft@microsoft.com, information@microsoft.com, crist.jessica@msn.com.

3.0 Raw Notes

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

!This program cannot be run in DOS mode.
,Rich]
UPX0
UPX1
UPX2
.idata2
3.08
google.com
iphlpapi.dll
administrator
tigger
thomas
trustno1
batman
jennifer
ranger
harley
jordan
monkey
shadow
football
michael
master
baseball
letmein
mustang
696969
qwerty
dragon
12345678
test1234
asdfg
root
qwer1234
1119
1021
1012
1001
aaa111
7942
789456
4444
1234qwer
1223
1221
1213
```

happy
a34567
54321
1qaz
1226
1224
1124
q1w2e3r4
1231
1214
1028
1025
1020
!@#$%^&*()
qazwsxedc
2002
1123
1228
love
a1234
7777
qwe
asdf
a12345
9999
1010
asd123
1234567890
1230
server
1122
!@#$%^&*
manager
1024
qaz
1234567
1225
asd
13579
11111
1357
2580
1212
a123456
654321
q1w2e3
1q2w3e4r
1004
qwe123
1qaz2wsx
1q2w3e
123qwe
abc123
qwer987
a111
adminadmin
123123
aaaa1
1111
db2admin
12345
administrador
admin1234
1234
123
admin

password
123456
c:\windows\%s
c:\winnt\
Isass.exe
Subject: %s|%s|%s
%s\c$\windows\%s
%s\c$\winnt\%s
stm8.inf
~tmp
%s\ipc$
%d.%d.%d.%d
\\%s
Local Security Authority Process
%s %%1
Kernel32.dll
AdvApi32.dll
%s\%s
-%d
+%d
Win7
Win2003
Unknown
WinXp
WinNt
Win2000
WinVista
%d.%d.%d.%d|
%s%s%s
Use
nnection2A
ApiBuffe
CancelCo
Api
rEnum
Net
rFree
ction2A
AddConne
WNet
32.dll
Subject:
SYSTEM
Invalid operation
System Error!
wgautr
QUIT
From: "%s" <information@microsoft.com>
Reply-To: "%s" <microsoft@microsoft.com>
Microsoft
News Letter
DATA
RCPT TO:<
MAIL FROM:<
HELO <
173.194.65.27
173.194.67.26
173.194.73.27
173.194.68.27
74.125.133.26
alt%d.
Windows Genuine Updater
DnsQuery_A
dnsapi.dll
GetNetworkParams
GetWindowsDirectoryA

WriteFile
CreateFileA
DeleteFileA
ReadFile
GetVersion
GetSystemTime
GetLocalTime
FreeLibrary
DeleteCriticalSection
LoadLibraryA
GetModuleFileNameA
lstrcmpiA
lstrcpynA
HeapAlloc
GetProcessHeap
HeapFree
GetModuleHandleA
GetStartupInfoA
GetProcAddress
CopyFileA
lstrlenA
GetTickCount
Sleep
EnterCriticalSection
LeaveCriticalSection
WaitForSingleObject
TerminateThread
CloseHandle
MultiByteToWideChar
WideCharToMultiByte
GetTempPathA
GetTempFileNameA
InitializeCriticalSection
RegisterServiceCtrlHandlerA
StartServiceA
OpenServiceA
QueryServiceStatus
ControlService
DeleteService
CreateServiceA
StartServiceCtrlDispatcherA
GetUserNameA
RegOpenKeyExA
RegCloseKey
OpenSCManagerA
CloseServiceHandle
SetServiceStatus
_strupr
sprintf
_beginthreadex
rand
srand
_endthreadex
strncpy
__p___argv
__p___argc
_exit
_XcptFilter
exit
_acmdln
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode

__set_app_type
_except_handler3
_controlfp
_stricmp
wsprintfA
MessageBoxA
.text
`.rdata
@.data
.rsrc
goog`
le.comiphlpapi.dll
administra6
tor
tigger
Ed#monk
love
QUIT
dDATA
RCPT
TO:<MAIL FROM
<HELOp
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
USER32.dll
WS2_32.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
RegCloseKey
rand
wsprintfA
ADVAPI32.dll
RegisterServiceCtrlHandlerA
StartServiceA
OpenServiceA
QueryServiceStatus
ControlService
DeleteService
CreateServiceA
StartServiceCtrlDispatcherA
GetUserNameA
RegOpenKeyExA
RegCloseKey
OpenSCManagerA
CloseServiceHandle
SetServiceStatus
kernel32.dll
GetWindowsDirectoryA
WriteFile
CreateFileA
DeleteFileA
ReadFile
GetVersion
GetSystemTime
GetLocalTime
FreeLibrary
DeleteCriticalSection
LoadLibraryA
GetModuleFileNameA
lstrcmpi
lstrcpyn

HeapAlloc
GetProcessHeap
HeapFree
GetModuleHandleA
GetStartupInfoA
GetProcAddress
CopyFileA
lstrlen
GetTickCount
Sleep
EnterCriticalSection
LeaveCriticalSection
WaitForSingleObject
TerminateThread
CloseHandle
MultiByteToWideChar
WideCharToMultiByte
GetTempPathA
GetTempFileNameA
InitializeCriticalSection
msvcrt.dll
_strupr
sprintf
_beginthreadex
rand
srand
_endthreadex
strncpy
__p___argv
__p___argc
_exit
_XcptFilter
exit
_acmdln
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
_strcmpi
USER32.dll
wsprintfA
MessageBoxA
WS2_32.dll
WSAGetLastError
connect
ioctlsocket
socket
htons
listen
bind
gethostbyname
closesocket
accept
recv
send
inet_ntoa
WSACleanup
WSAStartup
htons
sendto
select

```
gethostname
inet_addr
```