ACCDFISA File Crypter Malware Analysis

April 09, 2014

Andrew Kerr
me@andrewjkerr.com

Practical #3 | CIS4930

Table of Contents

Executive Summary

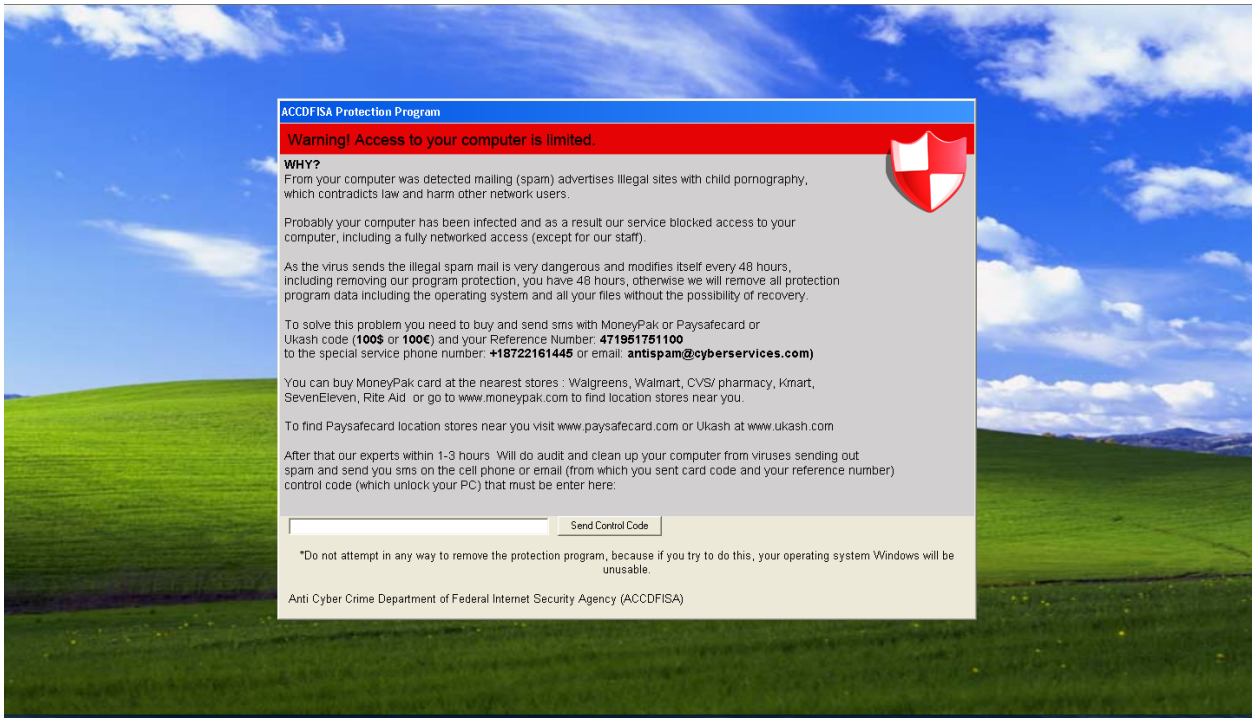
sys100s.exe is scareware that “scares” users into thinking that the “Anti Cyber Crime Department of Federal Internet Security Agency (ACCDFISA)” has quarantined their computer because of spam mail being sent from their computer.

When the malware is first executed, a link named “how to decrypt aes files” appears on the desktop as the malware starts to “encrypt” all of the user’s files with “aes encryption” (which are actually just password protected rar files.) When the user clicks on the link, the following window appears asking for a control code and a password:

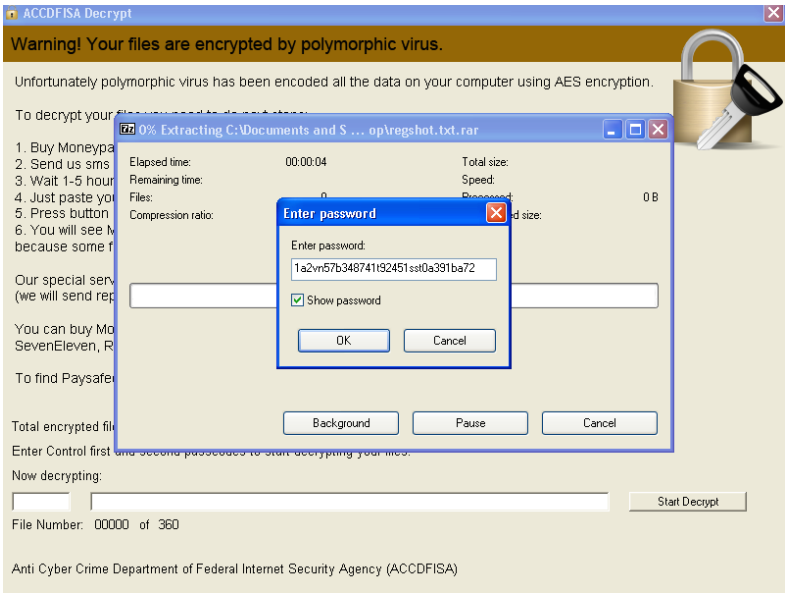
When the correct control and password (9385ee7e as the control code and 974324234213461230984324616230984324662137961292 4 as the password) is entered, the files are “decrypted”, but the login warning (to be discussed) does not disappear.

During the encryption phase, the malware is also disabling SafeBoot and adds it’s infected svchost.exe to the login registry key. There are also several files that are added that are discussed later.

After reboot, a new desktop is created by svchost.exe and a user must enter a security code. Digging through the strings (and trying a few of them), we find that the control code is 7534919801679213. When entered, the login process continues and we are allowed to access the desktop.

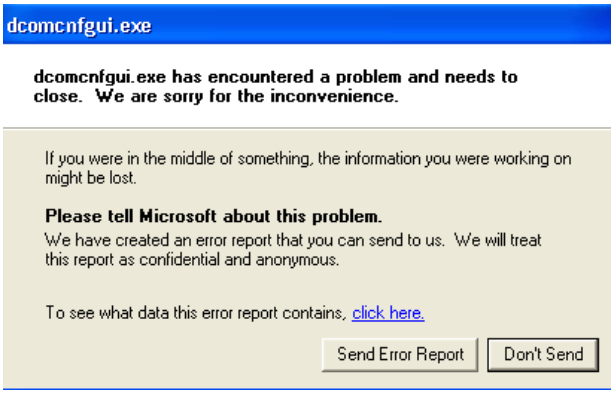


In order to access our “aes encrypted” files, rename the file from “filename.aes” to “filename.rar” and extract with 7zip. When prompted for a password, enter 1a2vn57b348741t92451sst0a391ba72 to extract your data!

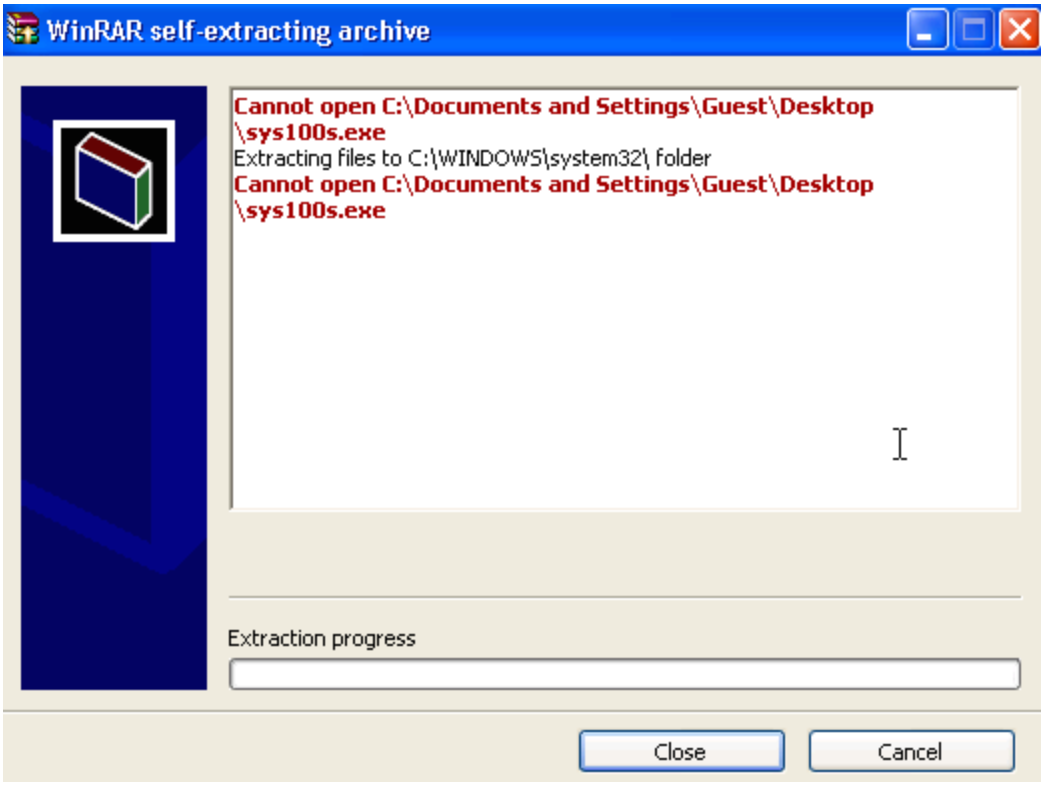


Interesting Points

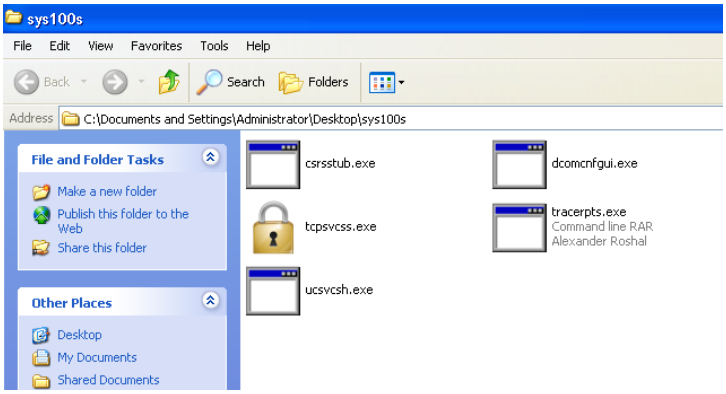
- I called the number that was listed, but it was not the ACCDFISA, but someone supposedly named Roy. Sorry Roy.
- Another interesting point is that dcomcnfgui.exe actually crashed a few times during my analysis before (and after reboot):



- The malware will not actually run on a non-administrator account since it cannot gain access to C:\WINDOWS\system32:



- You can extract some of the executables from sys100s.exe by changing the file type from .exe to .rar and extracting with 7zip:



Basic Static Analysis

1. There are several MD5 hashes that are associated with this program:
   WinRAR Executable (Actual ACCDFISA Malware):

sys100s.exe	d06f3948aec51684a26a75dbe9dcd581

   C:\ProgramData\local\

aescrypter.exe	53894890dc01bbcace449f6590a1597b
svchost.exe	6f36e46b83a61a5e251460ad825f425e
vpkswnhisp.dll	f2ae40ae7bcf6e72dc05a8bc4de8d534
dslsrunpk.dll	a84af952c36f3eec4fa7a13498dc979d
undxkpwvlk.dll	c81faf1d32a581b49975a158e3c5c268

   C:\WINDOWS\system32\

csrsstub.exe	6f36e46b83a61a5e251460ad825f425e
dcomcnfgui.exe	17fa49e023cb95cdfe365abc0d7290d0
tcpsvcss.exe	9225773aa6641d29ac88ca5eb6baeccf
tracerpts.exe	53894890dc01bbcace449f6590a1597b
ucsvcsh.exe	625ba9cf557dbb1ffac001e2a0300d32
wcmtstcsys.sss	MD5 depends on system

   C:\decrypt

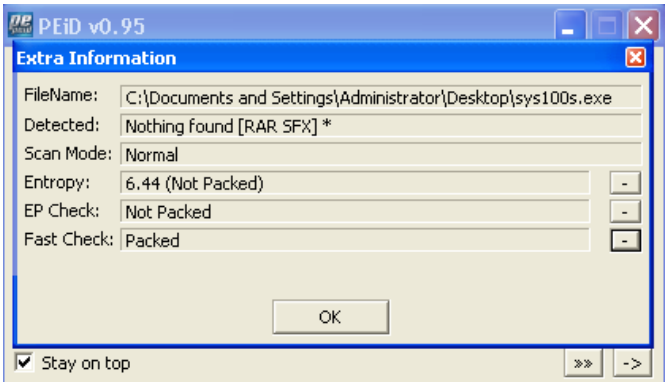
decrypt.exe	9225773aa6641d29ac88ca5eb6baeccf

   C:\

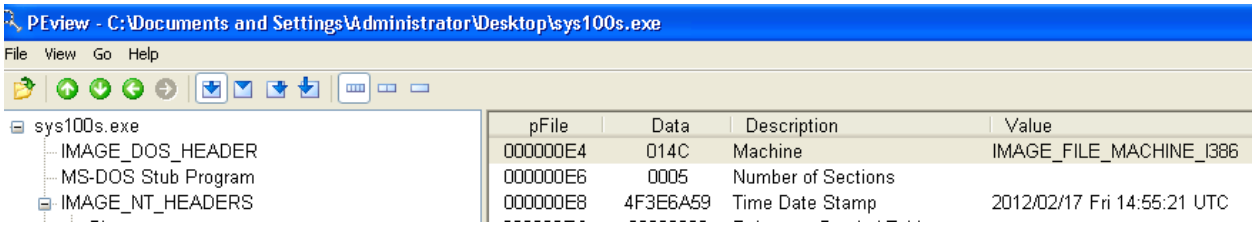
how to decrypt aes files.lnk	893dfb95584b06b28cb0335a60cc4211

   Note: When sys100s.exe is executed, the rest of the files are generated by/extracted from the malware.

2. Using PEiD, we can determine sys100s.exe is not packed.



3. Using PEviewer, we can use the IMAGE_FILE_HEADER to determine that sys100s.exe was compiled on February 17, 2012 at 14:55:21 UTC.



4. Using Dependency Walker, we can determine that the extracted executables from sys100s.exe contain the following “interesting” inports:
    a. csrsstub.exe
        i. The desktop functions in USER32.DLL. It appears that this executable has the capability to create and destroy different desktops.
        ii. The ability to modify processes including CriticalSections
        iii. RevokeDragDrop which could possibly go along with (i)
        iv. GUI functions
    b. dcomcnfgui.exe
        i. The ability to modify processes including CriticalSections
        ii. The ability to modify files
        iii. The ability to modify services
        iv. The ability to execute shell commands
    c. tcpsvcss.exe
        i. The ability to interact with thread local storage
        ii. Mainly GUI functions
        iii. The ability to execute execute shell commands
        iv. RevokeDragDrop again
    d. tracerpts.exe
        i. Lots of functions to do with files!
            1. Later identified as the command line version of WinRAR
    e. ucsvcsh.exe
        i. The ability to modify services
        ii. The ability to execute shell commands
        iii. The ability to set environment variables

5. After extracting the files from sys100s.exe, we can identify the following “interesting” strings:
    a. csrsstub.exe
        i. contains libpng and inflate programs
        ii. decrypt\decrypt.exe which is possibly an executable the malware creates
        iii. “Anti Cyber Crime Department of Federal Internet Security Agency (ACCDFISA)” which obviously does not exist

iv. two different codes:
    1. 8723739246527340998423465238490834247827346923509842 22
    2. 7534919801679213 (confirmed to be an unlock code)
v. WinSta0 which is a function that creates another “desktop”

b. dcomcnfgui.exe
    i. “how to decrypt aes files.lnk”
    ii. “1a2vn57b348741t92451sst0a391ba72” which can be confirmed as the password for all of the “encrypted” .rar files
    iii. “reg delete HKLM\System\CurrentControlSet\Control\SafeBoot /f” which implies that this malware disables SafeBoot
    iv. “\ProgramData\local\svchost.exe” which is an executable most likely created by the malware (same with “ProgramData\local\undxkpwvlk.dll”, “ProgramData\local\dslsrunpk.dll”, and others)
    v. “system32\wcmtstcsys.sss”, “system32\csrsstub.exe”, “system32\tcpsvcss.exe”, and others are most likely files created in system32
    vi. “REG ADD "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchost" /t REG_SZ /d "” which most likely starts the malware at login

c. tcpsvcss.exe
    i. Again looks like it contains the libpng and inflate programs
    ii. Contains two more code looking strings:
        1. 9743242342134612309843246162309843246621379612924
        2. 9385ee7e

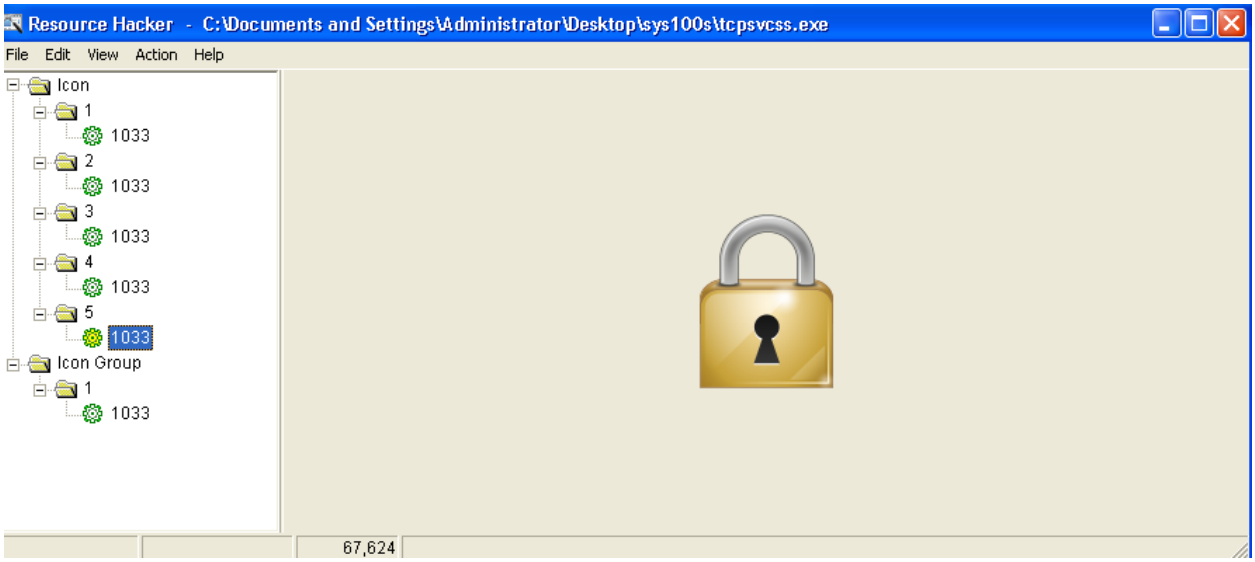
d. tracerpts.exe
    i. Strings point to a command line version of WinRAR (ex: RAR %s Copyright (c) 1993-%d Alexander Roshal %d %s %d)

e. ucsvcsh.exe
    i. “netsh.exe Interface ip Set address "” most likely sets the IP address to “172.248.0.1” which is found later in the strings
    ii. Also contains strings pointing to files being created in the ProgramData\local directory

6. Using PEviewer, we can determine that sys100s.exe contains the following sections:
    a. .text
    b. .rdata
    c. .data
    d. .CRT
    e. .rsrc

   None of the sections contain any interesting information.

7. Using Resource Hacker, we can determine that the only executables from the executables extracted from sys100s.exe that contain any resources are:
    a. tcpsvcss.exe: the icon for the executable (a lock)



    b. tracerpts.exe: the strings as well as the version information

Basic Dynamic Analysis

1. When sys100s.exe is executed, a few command prompts flash across the screen that seem to be running “ping.exe”. After those complete, uscsvcsh.exe and dcomcnfgui.exe are executed. dcomcnfgui.exe then calls aescrypter.exe to “encrypt” all of the user’s files. During this process, sys100s.exe deletes a lot of registry keys related to SafeBoot as well as adds a key that launches the infect svchost.exe on login.

2. The malware creates the following files:
   C:\ProgramData\local\
   a. aescrypter.exe - encrypts the files
   b. svchost.exe - creates the new desktop on login and prompts user for control code
   c. vpkswnhisp.dll
   d. dslsrunpk.dll
   e. undxkpwvlk.dll
      Note: not entirely sure of purpose of .dll files.

   C:\WINDOWS\system32\
   f. csrsstub.exe - same as svchost.exe (same MD5)
   g. dcomcnfgui.exe - calls the aescrypter.exe when sys100s.exe is executed
   h. tcpsvcss.exe - the file decryption screen
   i. tracerpts.exe - command line WINRAR
   j. ucsvcsh.exe - changes IP address of the system
   k. wcmtstcsys.sss - contains a list of files that the malware “encrypts”

   C:\decrypt
   l. decrypt.exe - the file decryption screen (same as tcpsvcss.exe)

   C:\
   m. how to decrypt aes files.lnk - links to decrypt.exe

3. Using RegShot, we can determine sys100s.exe adds the infected svchost.exe to the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run registry key so it runs on boot. There are also a lot of keys that are deleted that disable SafeBoot - especially HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot.

4. Using fakedns, inetsim, and Wireshark, I was unable to determine any attempted network connections.

Further Static and Dynamic Analysis

1. Using some of the codes found in the Strings, we can determine that the malware has the following “unlock” codes:
    a. 7534919801679213 will get past the window that is presented on boot and will allow access to the desktop
    b. When all of the “aes encrypted” files are changed to RAR files, 1a2vn57b348741t92451sst0a391ba72 can be used to unrar them.
    c. The decrypter will take 9385ee7e as the control code and 9743242342134612309843246162309843246621379612924 as the password.
2. Using IDA and OllyDBG, we can say that:
    a. sub_4057D6 extracts the executables from sys100s.exe and places them in the correct directory.
    b. The arguments for sub_4057D6 are:
        i. int - always “0”
        ii. LPCWSTR lpFileName - the name of the file to be extracted
        iii. DWORD dwShareMode - one of the arguments to be passed in the CreateFile function call that this subroutine makes
    c. sub_4057D6 is called 6 times at the following locations:
        i. loc_0040DDB7 (once)
        ii. loc_0040540C (5 times)

    Note: I obtained these locations from looking at the stack, but OllyDBG says that there are more local calls at loc_004051C7, loc_0040545E, and loc_004058A3
    d. All of the other interesting functions have been discussed - especially the function that creates the new desktop for the infected svchost.exe to run on.

Indicators

Since there are not any network based indicators, the MD5 hashes that were provided in the Basic Static Analysis are the best host based indicators that a machine has been infected. Also, any users reporting that the “Anti Cyber Crime Department of Federal Internet Security Agency” has blocked them from accessing their system due to their computer mailing out spam is another host based indicator.

The MD5 hash for sys100s.exe would be good to add to an IPS. The wording of the warning screen at login (specifically “your computer has been infected”) as well as the fact that the program seems to *attempt* to run silently (poorly hiding the command prompts) would lead one to believe that it is a malware downloaded by a downloader and not by the user.