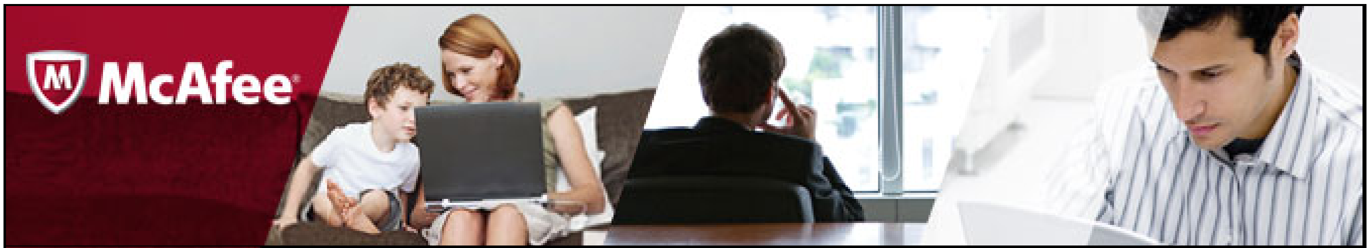


McAfee Labs Threat Advisory

W32/XDocCrypt.a

August 9, 2012

Summary

Detailed information about the worm, its propagation, and mitigation are in the following sections:

Infection and Propagation Vectors

Though we have not been able to verify the initial Infection Vector, it is assumed that dropper samples are being propagated as attachments over spam email.

Characteristics and Symptoms

Description

XDocCrypt.a belongs to a family of malware which encrypts Microsoft Office word, Excel and Executable files present in the system. It encrypts these files using RC4 encryption Algorithm. On successful encryption, the original file will be replaced with the infector followed by encrypted data; and if the original file name has ".doc"/".docx" then it will be replaced by "U+202Ecod.scr", if original filename has ".xls/.xlsx" then it will be replaced by "U+202Eslx.scr",

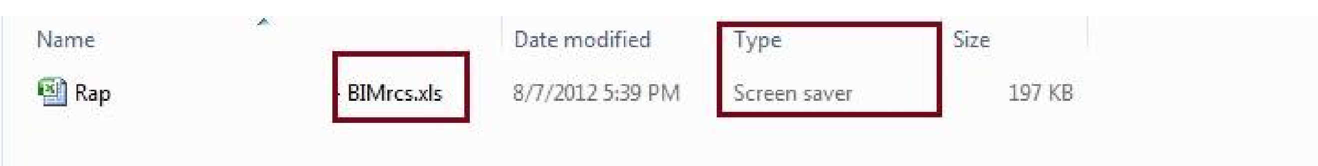
Note the presence of special character "U+202E" while renaming; this Unicode character caused the remaining of filename to be shown from right to left; while viewing in explorer.exe. This character is supported by default from Windows Vista operating systems onwards. On earlier versions (XP and below) this character is supported only if supported language packs are installed on the system.

Illustrating with an example:

Filename.xlsx would be renamed to: Filename?slx.scr

This file would be shown in Explorer as:

Filenamercs.xls (But type of the file will be shown correctly by Explorer.exe)



Command line will show the correct filename:

```
08/08/2012  08:21 PM    <DIR>          .
08/08/2012  08:21 PM    <DIR>          ..
08/07/2012  05:39 PM           200,728 Rap[redacted] - BIM▯slx.scr
               1 File(s)        200,728 bytes
               2 Dir(s)  179,376,926,720 bytes free
```

Malware copies itself into the following location:
- %APPDATA%\<random>\<random>.exe

Malware creates a shortcut file(detected as W32/XDcocCrypt.a!lnk) to launch the dropped executable file and malware adds this shortcut file under the following registry key to launch it on reboot.

HKEY_CURRENT_USER\Software\Microsoft\windows NT\Current Version\Windows
- Load = <path to shortcut file>

Infection routine is executed, if "-launcher" is passed as an argument to the executable file.

The infection routine searches for ".doc/.xls/.exe" in the file name and tries to infect it. Malware reads the original file content and encrypts it using RC4 encryption. On successful encryption, the original file will be replaced with the infector followed by "[+++scarface+++]", followed by encrypted data.

When an infected file is executed, Malware decrypts the encrypted original file and drops it to same folder with original name, adds appropriate extension (".docx" / ".doc" / ".xlsx" / ".xls" / ".exe") and will open the dropped original file. The dropped file will have hidden attributes. After some time the dropped original file will be deleted.

Infector runs in an infinite loop and gets terminated as soon as Task Manager(taskmgr.exe) is opened.

Network connections:
184.82.162.163
184.22.103.202

Mitigation
Block communications to above said IPs.
Opening Task Manager will terminate the infection routine.

Rootkit Behavior

No Rootkit behavior has been observed.

Restart Mechanism

Description
Creates a shortcut file with random name under %APPDATA%\<random>\ pointing to the dropped executable file and passes "-launcher" to it.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx