McAfee Labs Threat Advisory

Dridex

June 15, 2015

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.snssecure.mcafee.com/content/signup_login.

Summary

Dridex is "banker" malware that can steal user credentials for online accounts; it is derived from the Cridex family. This malware is downloaded by malicious document with an embedded macro and arrives via a spam or phish email. After the "document" is opened, it downloads the second-stage payload, which downloads and executes the final payload that infects the host machine. For more info about W97/Downloader (aka W97M/Bartallex), see PD25689 (https://kc.mcafee.com/corporate/index?page=content&id=PD25689).

McAfee detects this threat under the following detection name[s]:

- Downloader-FASH!
- Packed-EF!
- PWS-FCCA!
- Downloader-FARL!
- Drixed-FAI
- Drixed-FAF
- Drixed-FAG
- Drixed-FAH

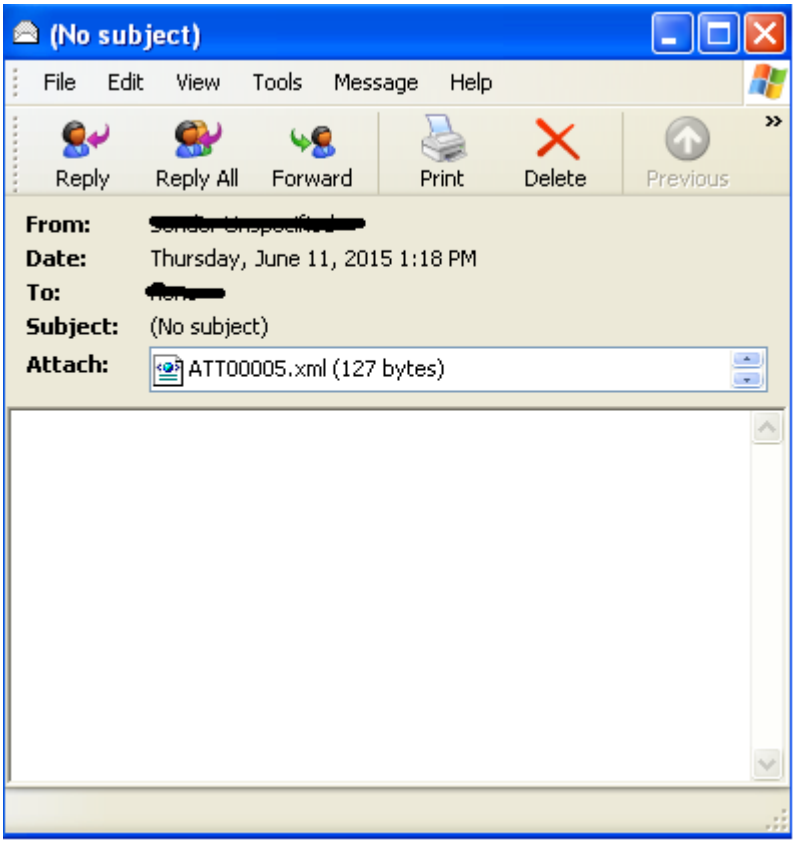
Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

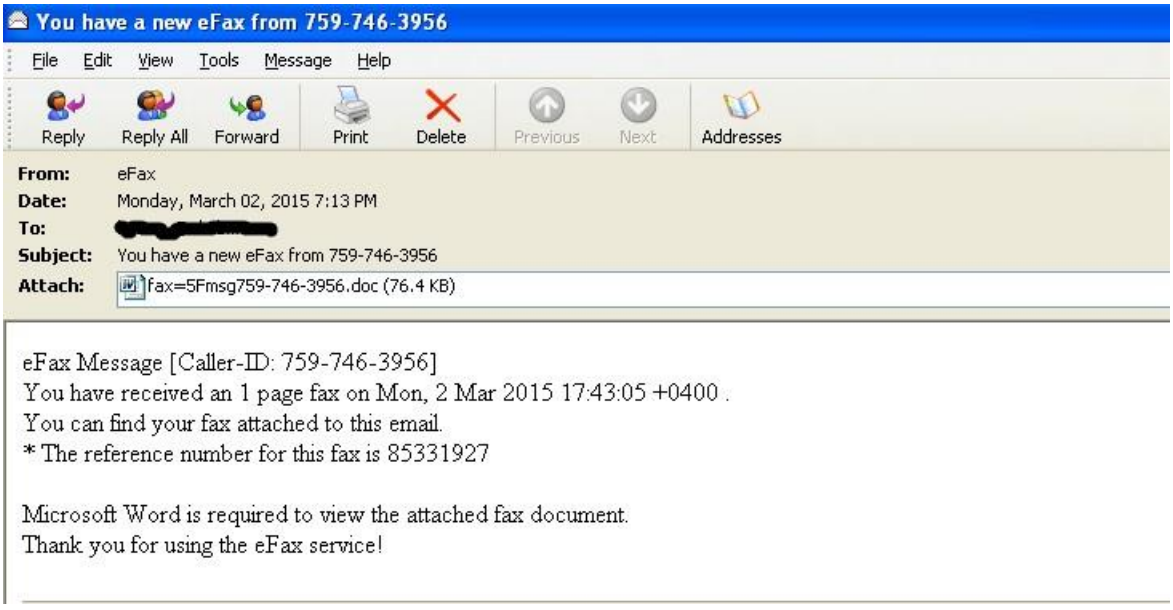
Infection and Propagation Vectors

This malware is download by via an embedded macro in a malicious document that arrives via spam or phish. After the "document" is opened, it downloads the second-stage payload, which downloads and executes the final payload that infects the host machine. The attached document can arrive in one of the variants:

- The first variant arrives as an XML document (.XML or .DOC) containing an embedded Office object encrypted with base64. The object is decrypted and executed when the XML file is opened. The embedded ActiveMime object contains an encrypted OLE document that is decrypted and executed just after the Office object is opened by the XML file. The OLE file then executes a malicious embedded macro that contains code similar to what we see in the following image. This code executes PowerShell and downloads the Dridex Loader.
- The second variant comes as a Word or Excel file (.DOC or .XLS) that contains an Office Active Object which executes the malicious code in the OLE file as native OLE code. Thus, even if the user has not enabled the execution of macros, the malware can execute by running the malicious code directly from the OLE file. To deceive the user, the malware presents a document file with an Active Object embedded.

The following are snapshots of phishing mails that contain malicious attachments.





Mitigation

Mitigating the threat at multiple levels such as file, registry, URL, and IP address can be achieved at various layers of McAfee security products. Browse the product guidelines available here (click Knowledge Center, and select Product Documentation from the Support Content list) to mitigate the threats based on the behavior described below in the Characteristics and Symptoms section.

Refer the following KB articles to configure Access Protection rules in VirusScan Enterprise:

- How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Dridex usually copies itself into the Administrator's Application Data folder using edge or edg with the random numeric numbers at the end, like the following examples:

Win XP:

C:\edge or edg[random.hex].exe

WIN7:

C:\Users\Administrator\Appdata\local\edge or edg[random.hex].exe

Users can configure and test Access Protection Rules to restrict the creation of new files and folders when there are no other legitimate uses.

Select **New files being created** and add the following file location in **File or folder name to block:**

- [OS installed drive]\edge or edg[random.hex].exe
- [OS installed drive]\[username]\Appdata\local\edge or edg[random.hex].exe

[random. hex] can be replaced with an asterisk ''. For example, you can either input edge*.exe or edge123.exe.*

Basic rules on handling emails:

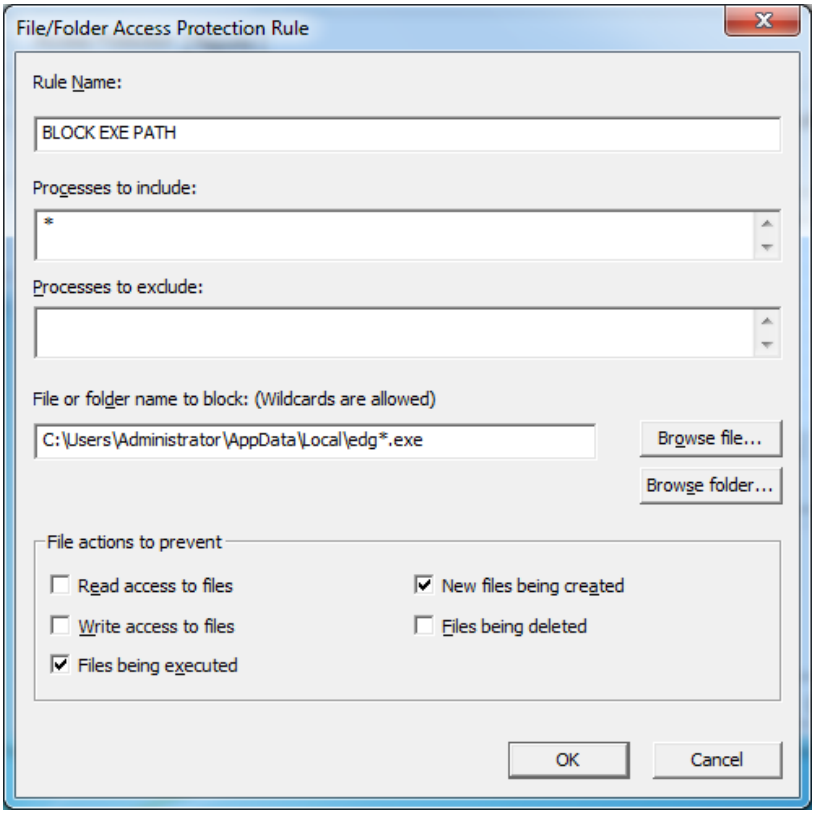
Email from unknown senders should be treated with caution. If an email looks strange, do the following: ignore it, delete it, and never open attachments or click on URLs.

Opening file attachments, especially from unknown senders, harbors risks. Attachments should first be scanned with an antivirus program and, if necessary, deleted without being opened.

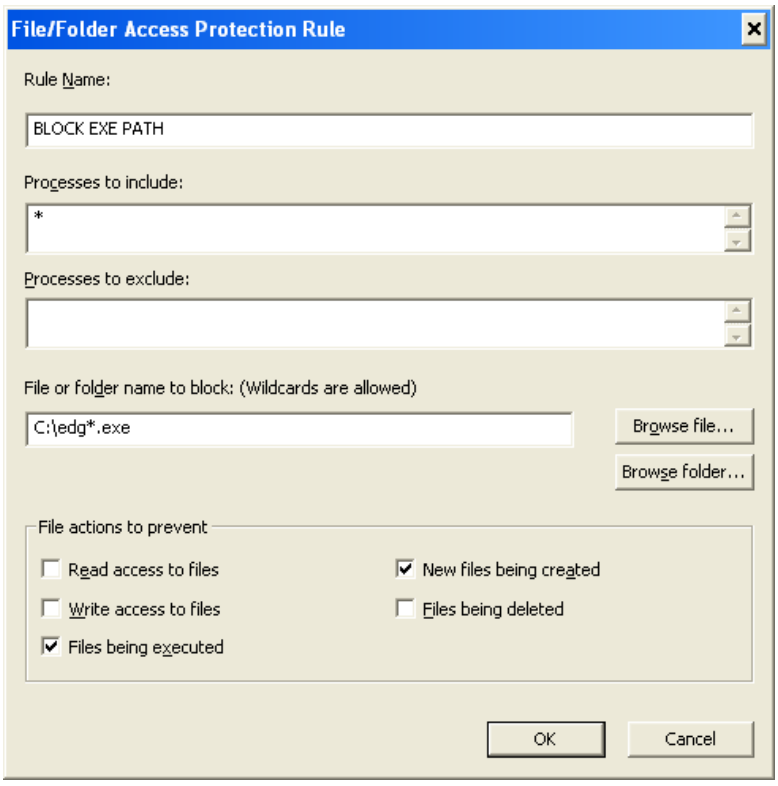
Never click links in emails without checking the URL. Many email programs permit the actual target of the link to be seen by hovering the mouse over the visible link without actually clicking on it (called the mouse-over function).

File/Folder Access Protection Rule for EXE file:

WIN7:

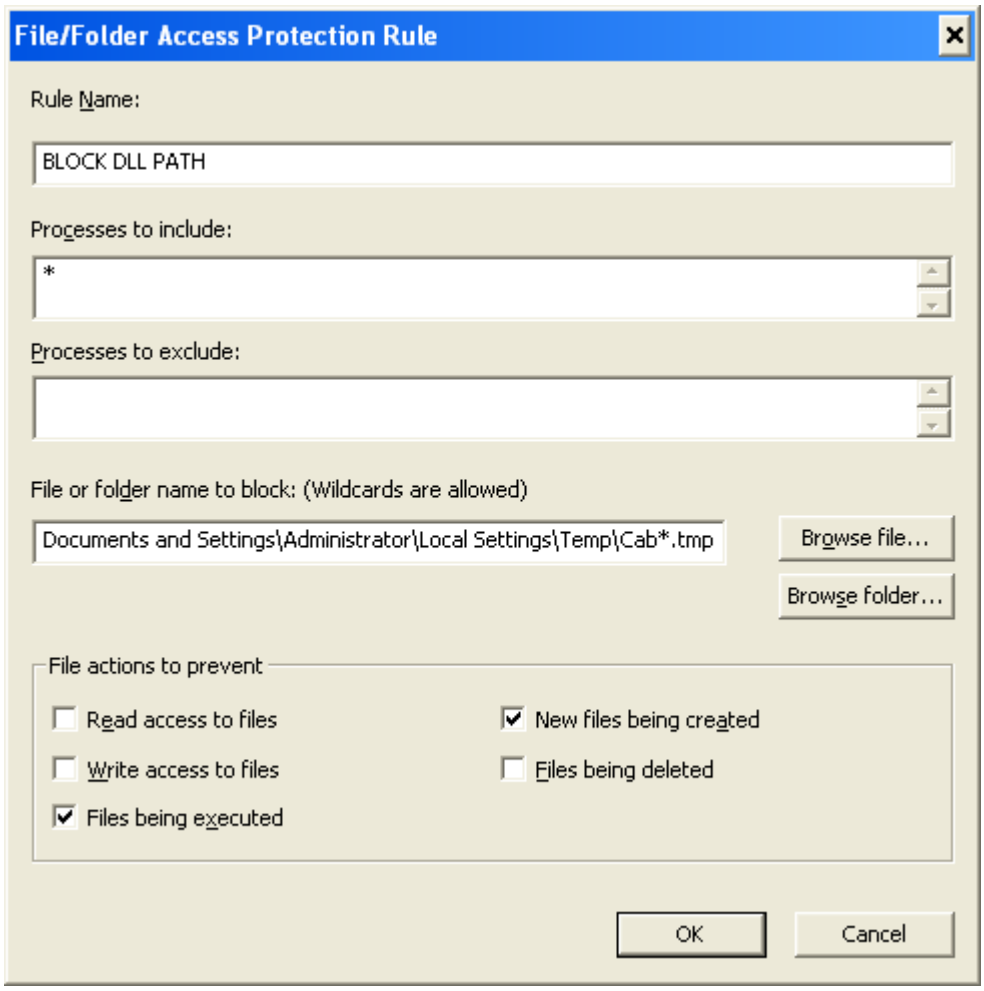


WINDOWS XP:

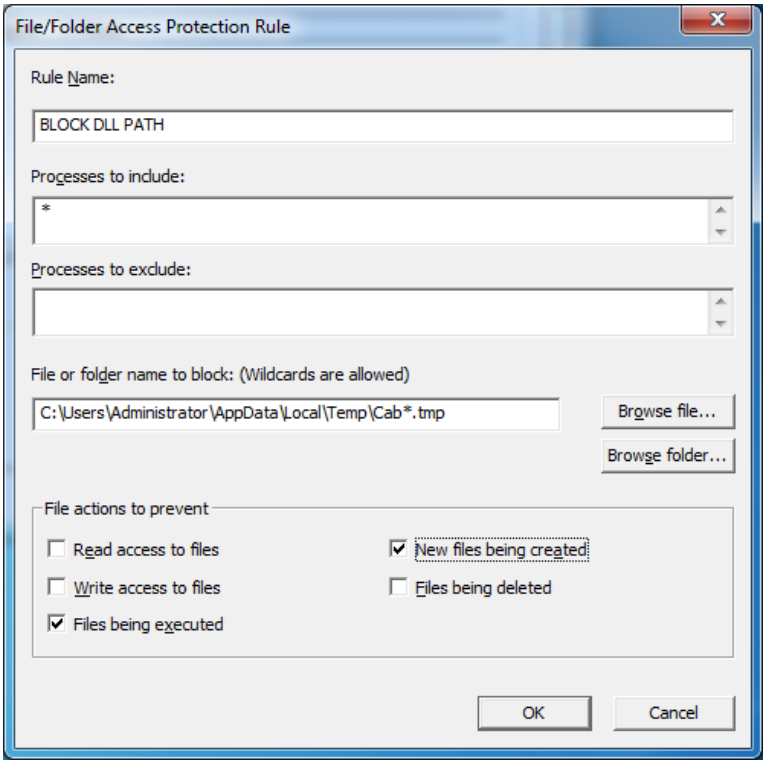


File/Folder Access Protection Rules for Dropped DLL file:

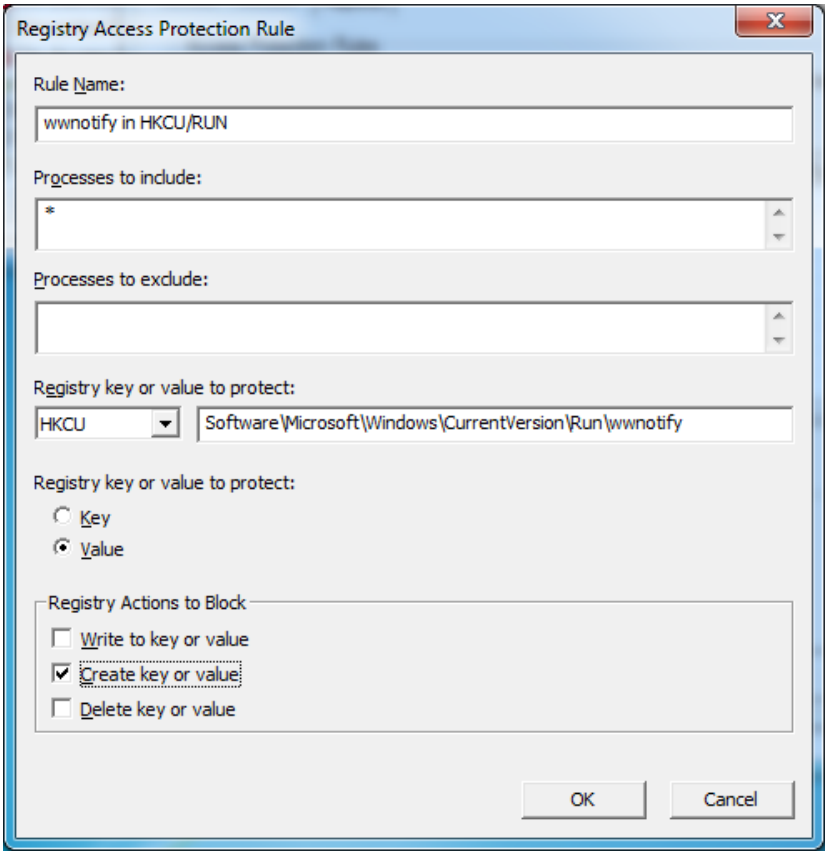
WINDOWS XP:



WIN 7:



Registry Access Protection Rule for Dropped DLL file:



Intel Security also recommends that you select and test the Create key or Value option for the above registry path.

Host Intrusion Prevention
To blacklist applications using a Host Intrusion Prevention custom signature, refer to KB71329.
To create an application blocking rules policies to prevent the binary from running, refer to KB71794.
To create an application blocking rules policies that prevents a specific executable from hooking any other executable, refer to KB71794.
To block attacks from a specific IP address through McAfee Nitrosecurity IPS, refer to KB74650.

*** Disclaimer: Use of *.* in an access protection rule would prevent all types of files from running and being accessed from that specific location. If specifying a process path under “Processes to Include”, the use of wildcards for Folder Names may lead to unexpected behavior. Users are requested to make this rule as specific as possible.

Characteristics and Symptoms

Description

This malware usually arrives as an attached document within a phish or spam email. After the “document” is opened, it downloads its payload. The attached document can arrive in one of the variants:

- The first variant comes as an XML document (.XML or .DOC) containing an embedded Office object encrypted with base 64. The object is decrypted and executed when the XML file is opened. The embedded ActiveMime object contains an encrypted OLE document that is decrypted and executed just after the Office object is opened by the XML file. The OLE file then executes a malicious embedded macro that contains code similar to what we see in the following image. This code executes PowerShell and downloads the Dridex Loader.
- The second variant comes as a Word or Excel file (.DOC or .XLS) that contains an Office Active Object which executes the malicious code in the OLE file as native OLE code. Thus, even if the user has not enabled the execution of macros, the malware can execute by running the malicious code directly from the OLE file. To deceive the user, the malware presents a document file with an Active Object embedded.

In recent scenarios, we have seen the macro downloading from a pastebin URL:
hxxp://pastebin.com/download.php?i=1YzPHtum

In the above URL, the < i=1YzPHtum > script will connect to the server < hxxp://212.76.130.99/bt/bt/get5.php>. After connection it will download Dridex payload.

Detailed Analysis:

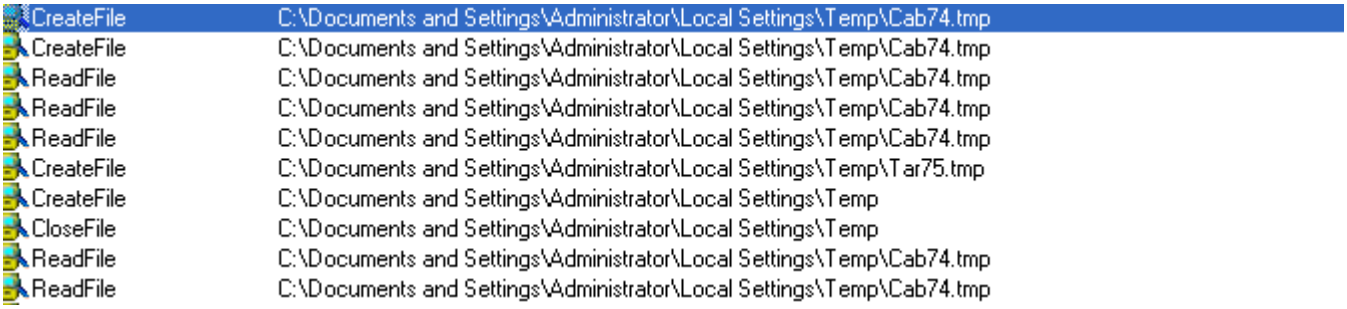
Upon execution, it copies itself into one of the following folders, depending on which operating system the malware is running:

- Windows XP: < **C:** >
- Windows 7: < **C:\Users\Administrator\Appdata\local** >

It uses edge or edg with the random numeric numbers at the end, such as the following example:

- **C:\edge74.exe**
- **C:\Users\Administrator\Appdata\local\edge74.exe**

After execution it contacts the server and downloads the DLL file into the system. The naming of file is similar to cab/tar[random.hex].tmp. Downloaded DLL file could be 32-bit or 64-bit version depending on the operating system of the infected client.



The downloaded DLL runs with the command rundll32<dllname> NotifierInit. The DLL then deletes the original exe and injects to the explorer.exe process. The injected thread then deletes the DLL itself. The following activities done by injected thread:

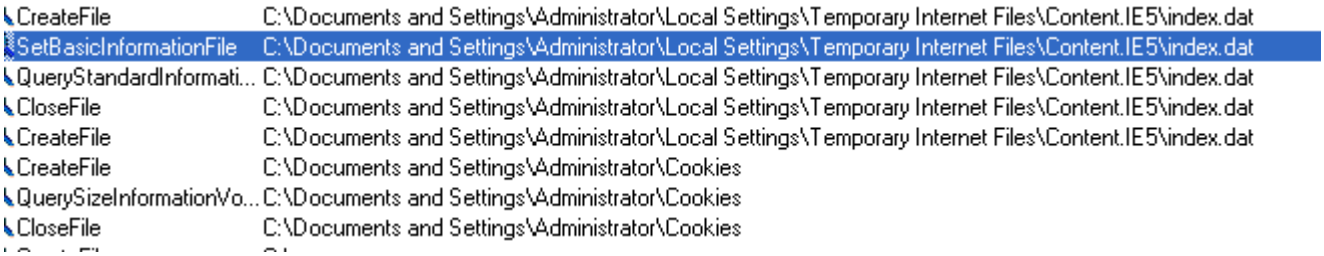
- Connects to the server and drops the payload to the system.
- Downloads the DLL again before the system shutdowns.

Before the system shutdown, the malware runs in the legitimate process memory. It drops the DLL and creates the registry entry so that malware can run again after the system restarts. After the system restarts, the DLL and registry entry are removed again:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "wwnotify"="rundll32.exe C:\\Document and Settings\\Administrator\Local Settings\Temp\cab[random hex].tmp NotifierInit"

Grabbing Browser Information

The malware grabs browser information such as Internet Explorer (IE), and so on. Internet Explorer save its browsing information in the Index.dat file. If the IE version is greater than 9, it stores in the WebCacheV24.dat or WebCacheV01.dat files. The malware will grab/steal information from the following files:



This malware also tries to access the Windows INetCache file. INetCache stores addresses of sites as you visit them.

Network Activity:

Connects to the following URL:

- download.windowsupdate.com
- 70.96.0.19
- 50.63.174.16
- 79.143.191.147

Remedies:

- Do not open any documents that come as an attachment from an unknown sender.
- If it comes from a known sender, scan all document attachments with the latest updated McAfee AV signatures before opening the document.
- Do not enable macros when any unknown document is prompted while opening.

Indicators of Compromise (IOC)

The following indicators can be used to identify Dridex infected machines in an automated way:

- Files Dropped in Administrator Application Data Folder:
    - C:\Documents and Settings\Administrator\Application Data\Local Settings\edge or edg[random.hex].exe
    - C:\Documents and Settings\Administrator\Application Data\Local Settings\Temp\cab[random.hex].tmp

Creates Run Key in the Registry:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "wwnotify"="rundll32.exe C:\\Document and Settings\\Administrator\Local Settings\Temp\cab[random hex].tmp NotifierInit"

Restart Mechanism

The following registry entry would enable the Trojan to execute every time when Windows starts.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "wwnotify"="rundll32.exe C:\\Document and Settings\\Administrator\Local Settings\Temp\cab[random hex].tmp NotifierInit"

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

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.