McAfee Labs Threat Advisory

Dridex

November 14, 2017

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.secure.mcafee.com/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 a 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 information about W97/Downloader (also known as W97M/Bartallex), see PD25689 (https://kc.mcafee.com/corporate/index?page=content&id=PD25689).

McAfee detects this threat under the following detection names:

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

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

Infection and Propagation Vectors

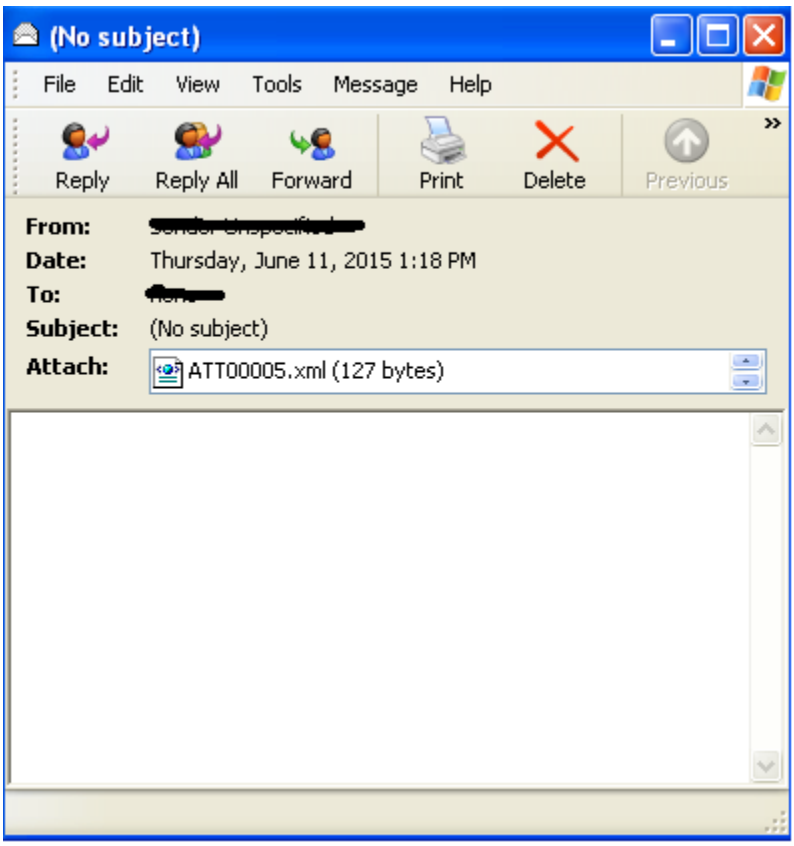
This malware can be downloaded by an embedded macro in a malicious document, or in the latest variants by JavaScript files that arrive via spam or phishing emails. After the "document" or JavaScript is opened, it can directly download and execute the Dridex payload, or it can download a second-stage payload, which downloads and executes the final payload that infects the host machine.

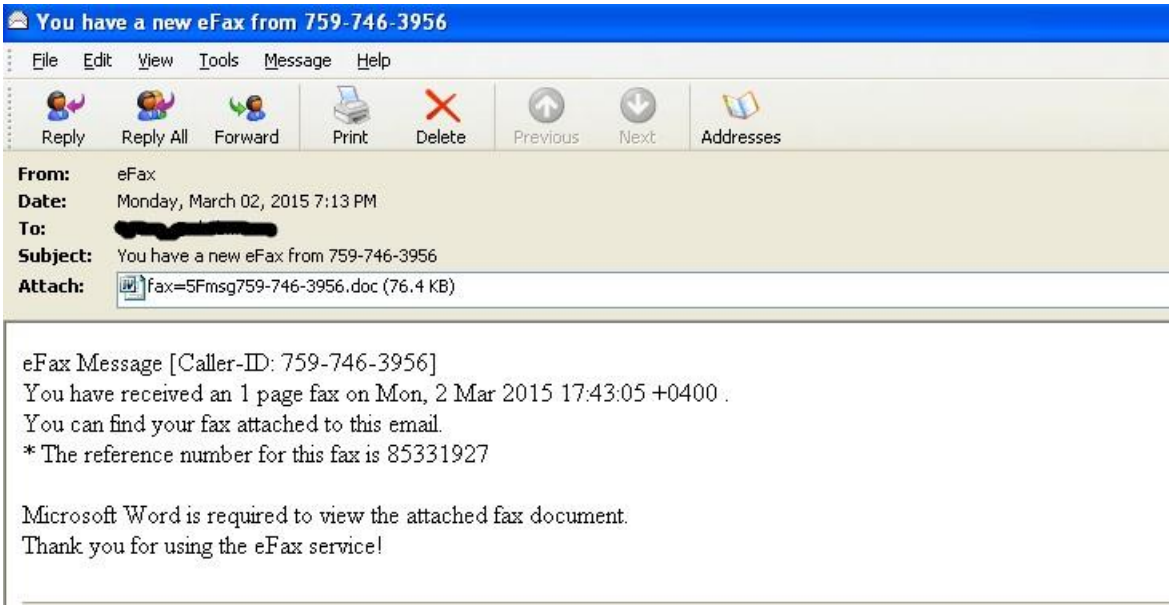
The attached document/JavaScript can arrive by one of the methods, included but not limited to, the following:

- It can arrive 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. The code in this macro executes PowerShell and downloads the Dridex Loader.

- It can arrive 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.
- It can arrive as spam email attachments as JavaScript, zip, or any other compressed file format that contains the malicious JavaScript file. There are also some variants that are being distributed as phishing emails with a link that, when clicked, download the malicious JavaScript file. All the previous mentioned attachments will download and execute Dridex when they are executed.

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





Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL can be achieved at various layers of McAfee products. Browse the product guidelines available here to mitigate the threats based on the behavior described in the Characteristics and Symptoms section.

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

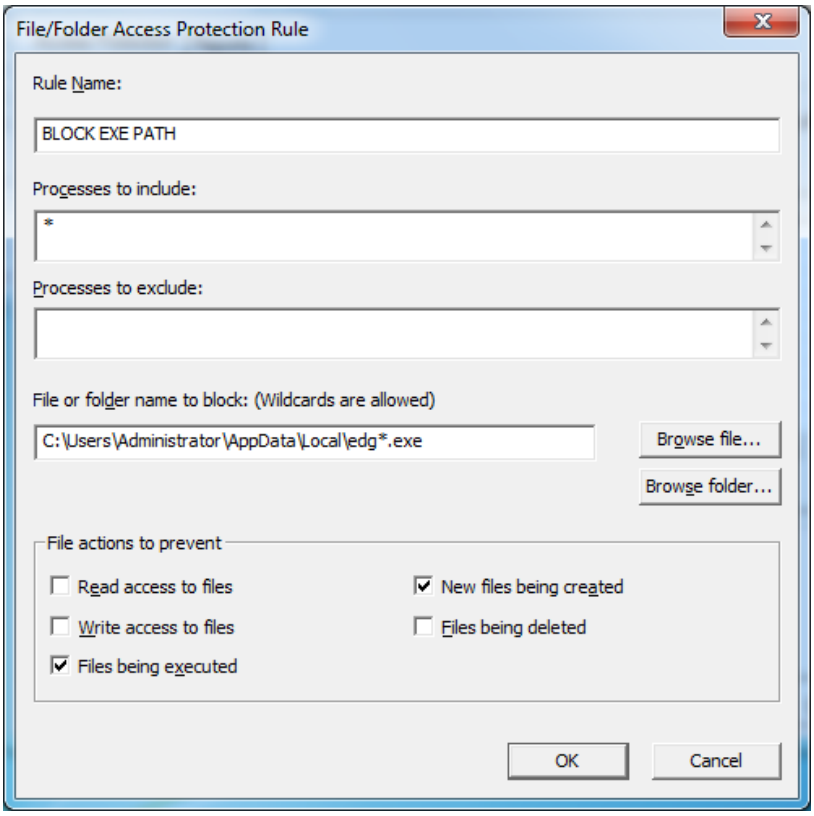
Treat email from unknown senders with caution. If an email looks strange, ignore it, delete it, and never open attachments or click on URLs.

Opening file attachments, especially from unknown senders, harbors risks. Scan attachments with an antivirus program before opening, and if necessary, delete them without being opened.

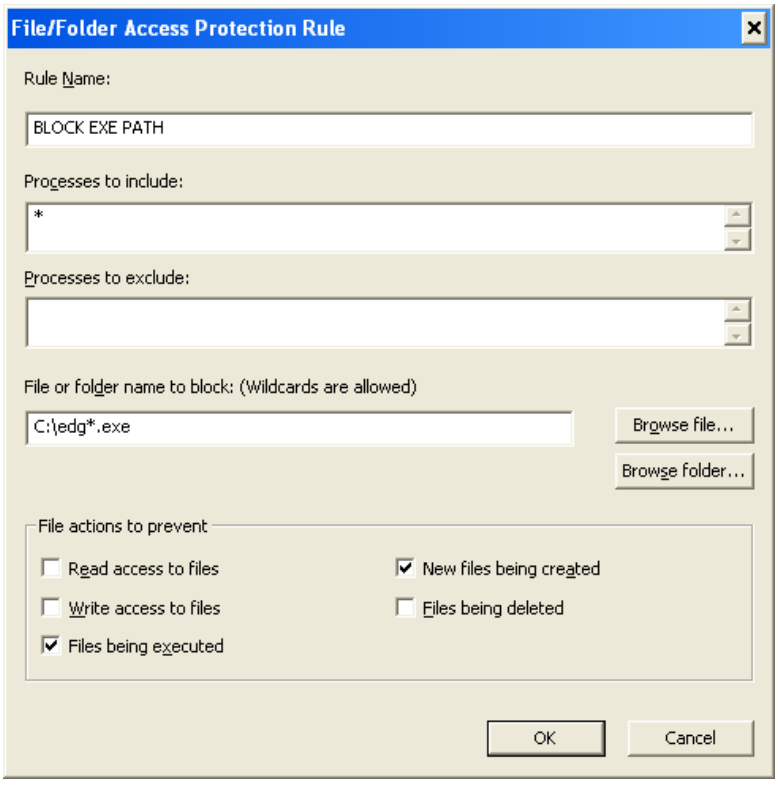
Never click links in emails without checking the URL. Many email programs allow you to view the target link by hovering the mouse over the visible link without clicking on it (called the mouse-over function).

File/Folder Access Protection Rule for EXE file:

WIN7:

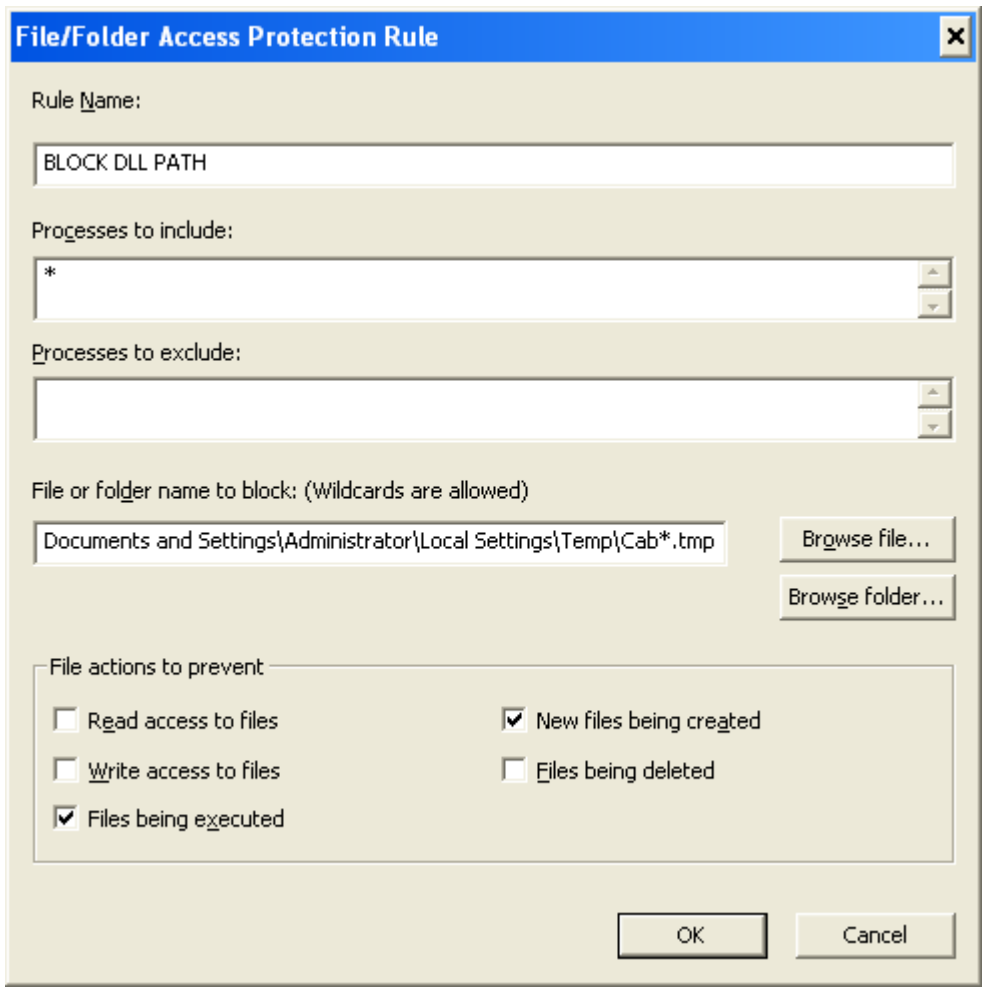


WINDOWS XP:

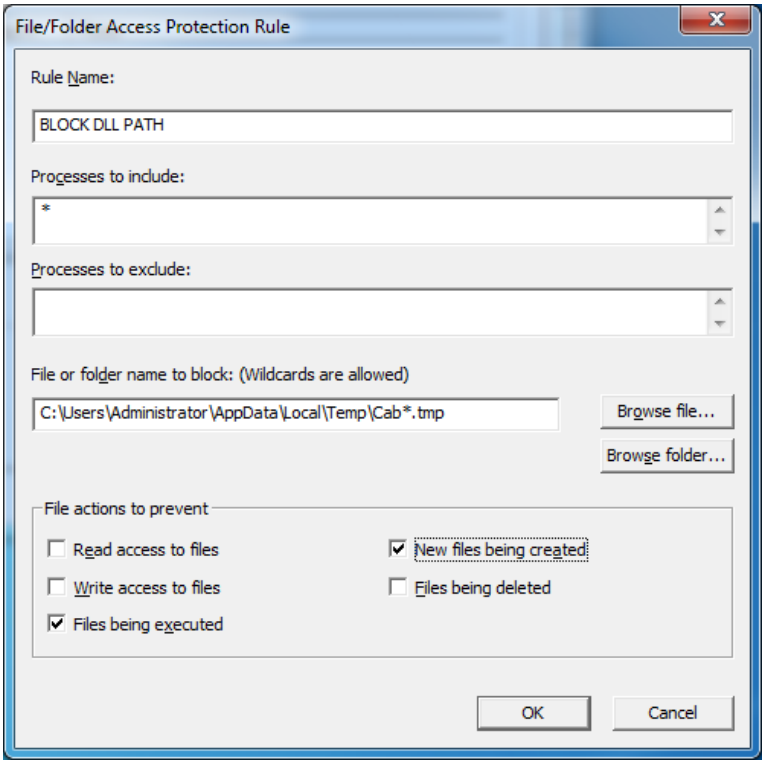


File/Folder Access Protection Rules for Dropped DLL file:

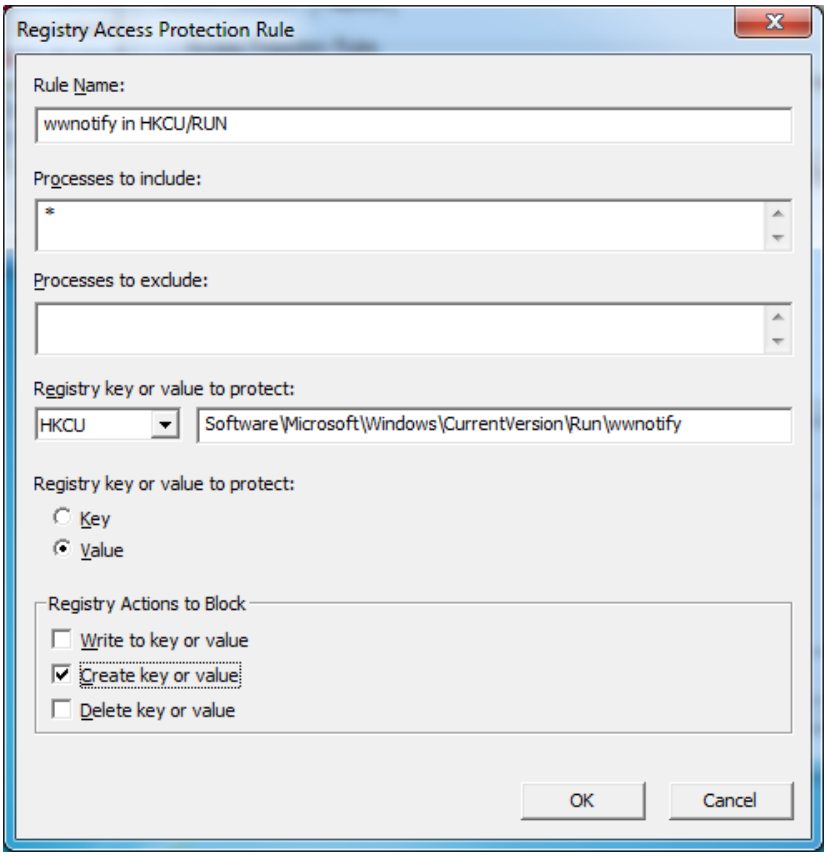
WINDOWS XP:



WIN 7:



Registry Access Protection Rule for Dropped DLL file:



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

McAfee Endpoint Security

Mitigation methods for assorted malware is available in the following product guide. Any specific mitigation steps if necessary would be described later in this advisory.
http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/ens_1000_help_0-00_en-us.pdf

ePolicy Orchestrator

- To block the access to USB drives through the ePO DLP policy, refer to this tutorial.

Endpoint Security 10.x

- Refer to article KB86577 to create an Endpoint Security Threat Prevention user-defined Access Protection Rule for a file or folder registry.

VirusScan Enterprise

- Refer to article KB53346 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable regedit.
- Refer to article KB53355 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable Task Manager.
- Refer to article KB53356 to use Access Protection policies in VirusScan Enterprise to prevent malware from changing folder options.

Host IPS

- To blacklist applications using a Host Intrusion Prevention custom signature refer KB71329.
- To create an application blocking rules policies to prevent the binary from running refer KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable refer KB71794.

McAfee Ransomware Interceptor

- To download and install McAfee Ransomware Interceptor, McAfee Free Tools

Other

- To disable the Autorun feature on Windows remotely using Windows Group Policies, refer to this article from Microsoft.

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 following 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. This code in the macro 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:

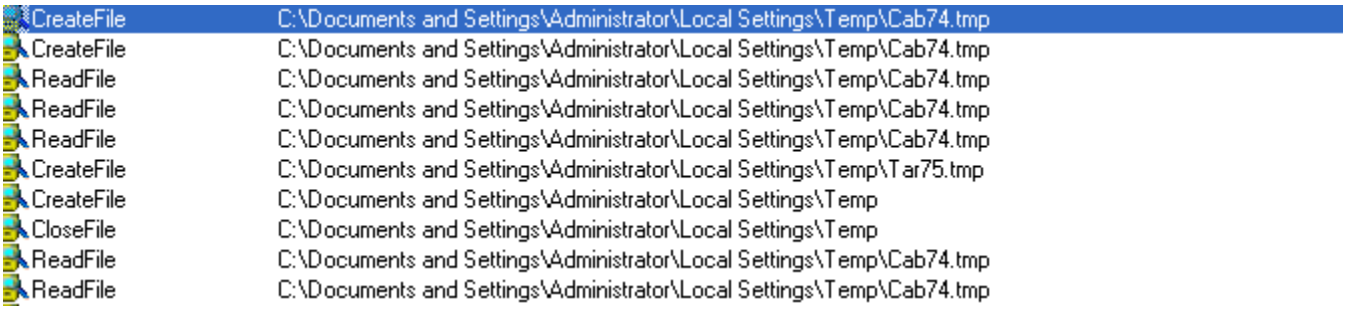
Upon execution, it copies itself into one of the following folders, depending on which operating system the malware is running:

- 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 the file is similar to cab/tar[random.hex].tmp. The downloaded DLL file could be a 32-bit or 64-bit version, depending on the operating system of the infected client.



CreateFile	C:\Documents and Settings\Administrator\Local Settings\Temp\Cab74.tmp
CreateFile	C:\Documents and Settings\Administrator\Local Settings\Temp\Cab74.tmp
ReadFile	C:\Documents and Settings\Administrator\Local Settings\Temp\Cab74.tmp
ReadFile	C:\Documents and Settings\Administrator\Local Settings\Temp\Cab74.tmp
ReadFile	C:\Documents and Settings\Administrator\Local Settings\Temp\Cab74.tmp
CreateFile	C:\Documents and Settings\Administrator\Local Settings\Temp\Tar75.tmp
CreateFile	C:\Documents and Settings\Administrator\Local Settings\Temp
CloseFile	C:\Documents and Settings\Administrator\Local Settings\Temp
ReadFile	C:\Documents and Settings\Administrator\Local Settings\Temp\Cab74.tmp
ReadFile	C:\Documents and Settings\Administrator\Local Settings\Temp\Cab74.tmp

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 are done by the injected thread:

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

Before the system shutdown, the malware runs in the legitimate process memory. It drops the DLL and creates the registry entry so the 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"

New Variants utilizing different Shellcode Injection techniques:

The latest variants of the malware are utilizing different techniques to inject Dridex Shellcode in foreign processes, which is then called to execute the final payload.

Some of the techniques utilized by Dridex recently are “Process Hollowing” and “AtomBombing” which essentially utilizes the memory process of legitimate system executables to inject and run the malicious code. These techniques help the malware to deceive the user by pretending to be a legitimate instance of a system executable running on the system. Therefore, it will be able to continue executing its malicious activities.

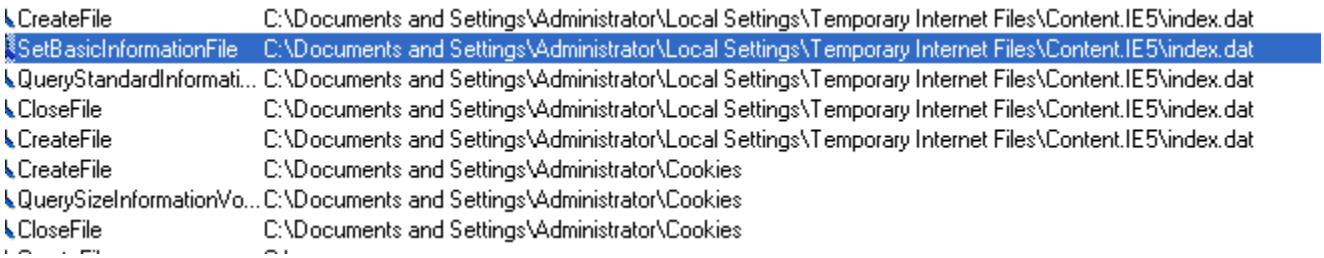
In the last version analyzed, we found the following additional activity after the Shellcode is executed:

Dridex runs two legitimate system executables to gather information from the compromised system. The information is copied to a temp file stored in XML format, which is later encrypted and exfiltrated to the C&Cs:

- Whoami.exe /all – Displays the current user name, groups belonged to along with the security identifiers (SID).
- Net.exe view – display a list of resources being shared on a computer.

Grabbing Browser Information:

The malware grabs browser information such as Internet Explorer (IE), and so on. IE saves 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 URLs:

- download.windowsupdate.com
- 70.96.0.19
- 50.63.174.16
- 79.143.191.147
- 173.203.123.102
- 162.243.137.50
- 87.106.219.40

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.

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.