McAfee Labs Threat Advisory
W32/Expiro, W64/Expiro

July 22, 2013

Summary

The W32/Expiro and W64/Expiro family of malware is a virus that parasitically infects executables by appending its viral code to the host. It could also download other malwares and steal system information.

Aliases:

- W32/Expiro.W
- Virus.Win32.Expiro
- Virus.Win32.Expiro.h
- Virus.Win32.Expiro.W
- Virus:Win32/Expiro.AL
- Malware.Xpiro
- W32.Xpiro.E
- PE_EXPIRO.RAP

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

Additionally, McAfee Labs Threat Intelligence descriptions for W32/Expiro.gen.o and W32/Expiro.dr are available in the following locations:

- http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=3391050
- http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=2187346

The minimum DAT versions are:

- W32/Expiro.gen.o: 7107 (2013-06-15)
- W32/Expiro.dr: 7062 (2013-05-01)
- W64/Expiro: Beta DAT and Stinger available.

The Threat Intelligence Library contains details of the most recent DAT with updated signatures. W64/Expiro detection in production DAT is pending release as it is going through QA. McAfee Labs will post an update to this document when the detection is released.

Infection and Propagation Vectors

W32/Expiro and W64/Expiro searches for executable files to infect in all drives including mounted shared directories and portable drives. Infected executables may then infect others if used on other systems.

Mitigation

- Disable the Autorun feature on Windows. You can do this remotely using Windows Group Policies (http://support.microsoft.com/kb/967715).
- Restrict the use of USB drives in mission-critical and server machines.
- Implement and test Access Protection Rules using VirusScan Enterprise to prevent writing of

AUTORUN.INF files.
- Enforce a strict password policy on all network shares and allow write permissions to only trusted accounts that need it.

Characteristics and Symptoms

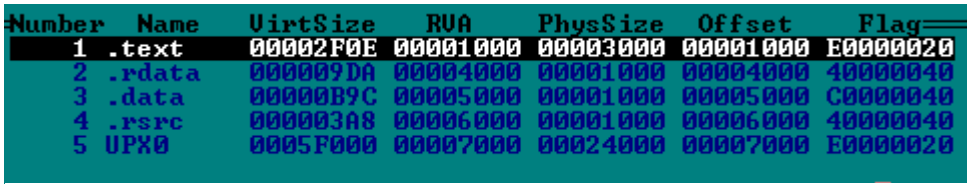
Description
W32/Expiro searches for and infects all 32-bit PE executables in the system except for those that have the following characteristics:

- With data overlay
- Not enough space in header for additional section data
- Already infected file
- DLL and driver files

W64/Expiro searches for and infects all AMD64 64-bit PE executables in the system as long as the previous characteristics are not met.

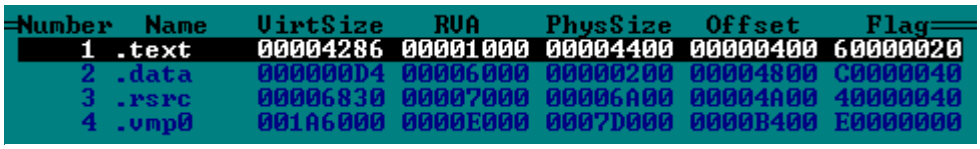
It infects by adding a new section and appending its viral code to the host. Current variants add one section with a name "UPX0" with an added section size of around 0x24000 bytes, or ".vmp0" with an added section size of 0x7C000 or 0x7D000 bytes, which increases file size by 496-500KB.

An infected executable's section data looks like this:



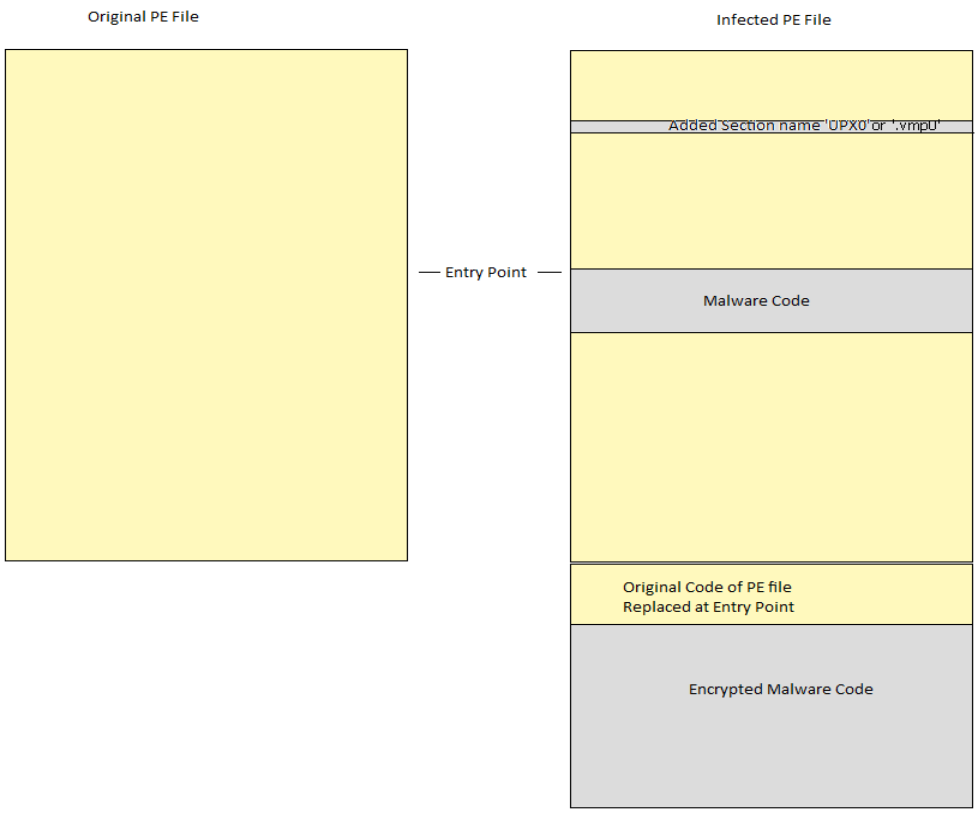
Number	Name	VirtSize	RVA	PhysSize	Offset	Flag
1	.text	00002F0E	00001000	00003000	00001000	E0000020
2	.rdata	000009DA	00004000	00001000	00004000	40000040
3	.data	00000B9C	00005000	00001000	00005000	C0000040
4	.rsrc	000003A8	00006000	00001000	00006000	40000040
5	UPX0	0005F000	00007000	00024000	00007000	E0000020

Or



Number	Name	VirtSize	RVA	PhysSize	Offset	Flag
1	.text	00004286	00001000	00004400	00000400	60000020
2	.data	000000D4	00006000	00000200	00004800	C0000040
3	.rsrc	00006830	00007000	00006A00	00004A00	40000040
4	.vmp0	001A6000	0000E000	0007D000	0000B400	E0000000

To execute its own code at execution, it replaces a block of code from the entry point of the host file. Replaced code data is moved to the new section as shown below.



Symptoms of an infected file:

- File size increase of 140 KB to 500KB
- Change of file timestamp
- PE file last section name is UPX0 or .vmp0

While running, a Mutex is created to ensure only one instance of the Virus is running at a time. The Mutex name is:

- kkq-vx_mtx{random 1-digit number}

This virus could collect the following sensitive information:

- Installed certificates
- Credentials stored by FileZilla
- Credentials stored by Windows Protected Storage
- Passwords stored by Internet Explorer, within the following registry entry:
    - HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

It logs the stolen credentials in either of the following non-malicious files:

- %UserProfile%\Local Settings\Application Data\wsr{random 2 digit number}zt32.dll
- %UserProfile%\Local Settings\Application Data\dfl{random 2 digit number}z32.dll
- %UserProfile%\Local Settings\Application Data\dfl{random 2 digit number}z32.dll
- %UserProfile%\AppData\Local\kf{random 2 digit number}lz32.dll
- C:\ProgramData\i{random 2 digit number}fidjfebb.dat
- %UserProfile%\AppData\Local\fidjfebb{random 2 digit number}.nls

It also installs a Firefox extension by adding the following files in the Firefox extension directory:

- {ec9032c7-c20a-464f-7b0e-13a3a9e97385}\components\red.js
- {ec9032c7-c20a-464f-7b0e-13a3a9e97385}\install.rdf

- {ec9032c7-c20a-464f-7b0e-13a3a9e97385}\chrome\content.jar
- {ec9032c7-c20a-464f-7b0e-13a3a9e97385}\chrome.manifest

W64/Expiro installs a Chrome extension by adding the following files in the Chrome extension directory:

- dlddmedljhmbgdhapibnagaanenmajcm\1.0_0\background.js
- dlddmedljhmbgdhapibnagaanenmajcm\1.0_0\content.js
- dlddmedljhmbgdhapibnagaanenmajcm\1.0_0\manifest.json

The Firefox extension could redirect the compromised user to the following domains:

- stopbadware.org
- gektar-promarenda.ru
- cashing.cc
- hdecub-ydyg.ry
- directconnection.ws
- mediaportal-2016.ru
- kamlashop-ultras.org
- theplan-from-iran.net
- erussia-govsvc.ru
- ijmash-gunszavod.ru
- egypt-bizneonet.biz
- hlop-v-job.ru
- pasha-mers50.ru
- entry-retails555.biz

The Chrome extension could redirect the compromised user to the following domains:

- stopbadware.org
- vwwzbgk-xqid.eu
- kepancex-za.ws
- zuwyxtiver-xockok.ru
- nanukde-uneri.com
- himoxoffo-my.ru
- cihyjuxkoxwu.ws
- dyhasfosce-lyhol.ru
- yjokipyjryro.ru
- buwarfofziku.net
- iqylazomanete.ru
- nocytywcumawke.in
- weresvarujuve.ws
- pysexynasy.com
- ramilepo-anur.net
- xyniwsursynemyc.cc
- ociptowit-be.net
- ikoleqadxavpo.net
- edybosewybopy.in
- efazenuwfutejsiq.com
- onozusca-awe.ru
- ocibaminiwono.ru
- ebyxbifoqtyfy.ws
- qyjbyphawoha.ru

W32/Expiro also connects to the following domain on port 80 to send and receive information and download other malwares:

- greatsouthoffshore.com
- angar-promarenda.ru
- kasperskygayformula.biz
- www.microavrc-usb33bit.com
- leninheadshop.ru

- fdecub-ydyg.ru
- fgefa-bugin.com
- fkegy-bikav.com
- indirs-vostok.ws
- fmyjo-boneb.com
- 64.70.19.33
- indirs-locmocz.ws
- 109.236.88.70
- international-spcsz.ru
- mkz-coffestores.cc
- angar-promarenda.ru
- kasperskygay-formula.in
- microavrc-usb33bit.com
- verified.ru
- fmyjo-boneb.com
- fpykyb-aquh.ru
- fsymi-betop.com
- fvypeb-ywav.ru
- visualillusionist.com
- indirs-vostok.ws
- fzuqib-ubyc.ru
- grewz-platker.ru

Captured POST requests:
The Expiro virus transmits a unique Hardware ID in the User-Agent header which consists of Operating System and software versions.

> POST [malicious domain] HTTP/1.1
> User-Agent: Mozilla/{majorversion}.{minorversion} (Compatible; MSIE {IE version}; NT{windows major version}.{minor version}.{build}-{eight characters}.ENU.{eight characters}-{six numbers}-{six alphanumeric characters}-{eight alphanumeric characters}; .NET CLR {major version}/{minor version})
>
> Example:
> POST greatsouthoffshore.com HTTP/1.1
> User-Agent: Mozilla/4.1 (compatible; MSIE 20; NT5.1.2600-ABCDEF01.ENU.CDEF0123-012345-ABCDEF-1438147D)
>
> POST zykabociqat.ws HTTP/1.1
> User-Agent: Mozilla/4.0 (Compatible; MSIE 28; NT6.1.7600-ABCDEF01.ENU.CDEF0123-012345-ABCDEF-15CC175E; .NET CLR 00000000/00000000)

W64/Expiro also connects to the following domains to port 80 to send and receive information and download other malware:

- ecokirejopa.in
- udujimxawivu.ru
- wicyftufenyx.ru
- zykabociqat.ws
- tarpibyde-ti.ru
- xpibob-urok.ru
- xridyb-ivar.ru
- xnukoc-ysyp.ru
- xvofib-oxyx.ru
- xgyfa-camob.com
- xguly-diwiv.com
- punanyhwerovir.net
- zewyxa-mi.net
- azipoxikyf-amopu.biz
- miqockyrkopse.biz
- jubmilazicipmu.biz
- axihsicotatmukaq.ru
- joziclohoso.net
- sitesedirimxizy.com

- jesyvihuxeno.com
- hudnalsaluh-va.biz
- folfobupikidpu.cc
- foceqjazqepyra.org
- witeqilqasybkok.org
- mipibuzycysfe.org
- ykekuqizase.org

This family uses a domain generation algorithm (DGA) that constructs URLs based on the following rules:

- Top-Level Domain Name is picked from one of the following:
  - .in, .ru, .ws, .com, .net, .biz, .org, .cc, .eu
- Second-Level Domain Name is a randomly generated name chosen from any lowercase alphabet and a hyphen (-).
- The total length of the URL varies from 13 to 20 characters.

Domains that satisfy the DGA rules are hosted at:

- 64.70.19.198
- 159.148.27.210

Additionally, some variants may attempt to connect to remote hosts via the following ports:

Remote port 53:

- 220.225.236.85
- zavrchckshopsz.ru
- pdecub-ydyg.ru
- pgefa-bugin.com
- zerrblashingz.cc
- indirs-locmocz.ws
- pkegy-bikav.com
- pmyjo-boneb.com
- ppykyb-aquh.ru
- insecto-pestarz.ru
- psymi-betop.com
- kgbrelaxxlubz.ru
- pvypeb-yxav.ru
- pvypeb-yxav.ru
- 64.70.19.33
- 202.54.6.60

Remote port 137[NetBIOS]:

- pgefa-bugin.com
- pkegy-bikav.com

Mitigation

- If possible, block access to the ports and monitor and block the above mentioned URLs.
- Add Access Protection rules to deny writing data to existing files with EXE extension, to avoid files being re-infected.

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