Expiro Malware Is Back and Even Harder to Remove

mcafee.com/blogs/other-blogs/mcafee-labs/expiro-infects-encrypts-files-to-complicate-repair/

October 31, 2017

Xiaobing Lin

Oct 31, 2017

5 MIN READ

File infector malware adds malicious code to current files. This makes removal tricky because deleting infections results in the loss of legitimate files. Although file infectors were more popular in the 1990s and early 2000s, they still pose a significant threat. The complex disinfection process is usually leveraged by malware authors to ensure systems stay infected for a long period. This may explain why complex file infectors such as W32/VirRansom, W32/Sality, W32/Xpaj, and Expiro are still active today.

The Expiro virus is has been around for more than a decade, and the authors continue to update it with more features. Expiro is unique in that it infiltrates executable files on both 32- and 64-bit Windows systems by appending its viral code to the host. It can be used to install malicious browser extensions, lower browser security settings, and steal account credentials.

Recently we discovered a new variant of Expiro with a significant change in its infection routine. In previous variants, Expiro modified and stole code at the entry point and appended the viral payload only at the end of the original file, typical of an appender virus.

The new variant, however, changes the size of the base relocation table and encrypts the addresses inside, causing traditional appender virus repair routines to corrupt files unless they correctly restore the original base relocation table. By adding the encryption, Expiro increases the complexity of analysis and requires a customized repair routine, which makes it hard to combat.

The following screenshots demonstrate this point: The base relocation table of a file infected by the old variant of Expiro is unaffected and the contents are untouched.

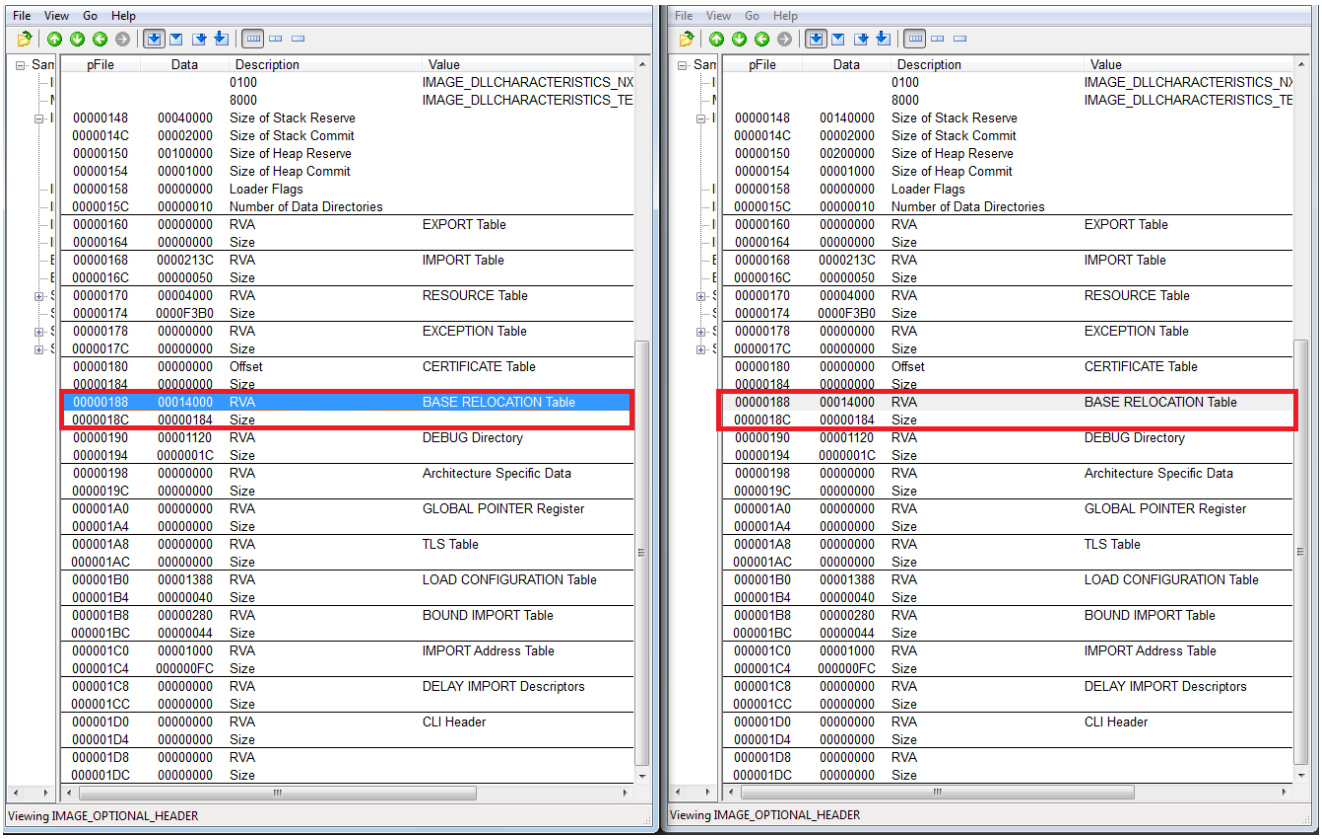

Figure 1: The relocation table remains intact when infected by the old Expiro variant.

Figure 2: The relocation table contents are not modified by the old Expiro variant.

The new variant reduces the size of the base relocation table and encrypts portions of it (outlined in red).

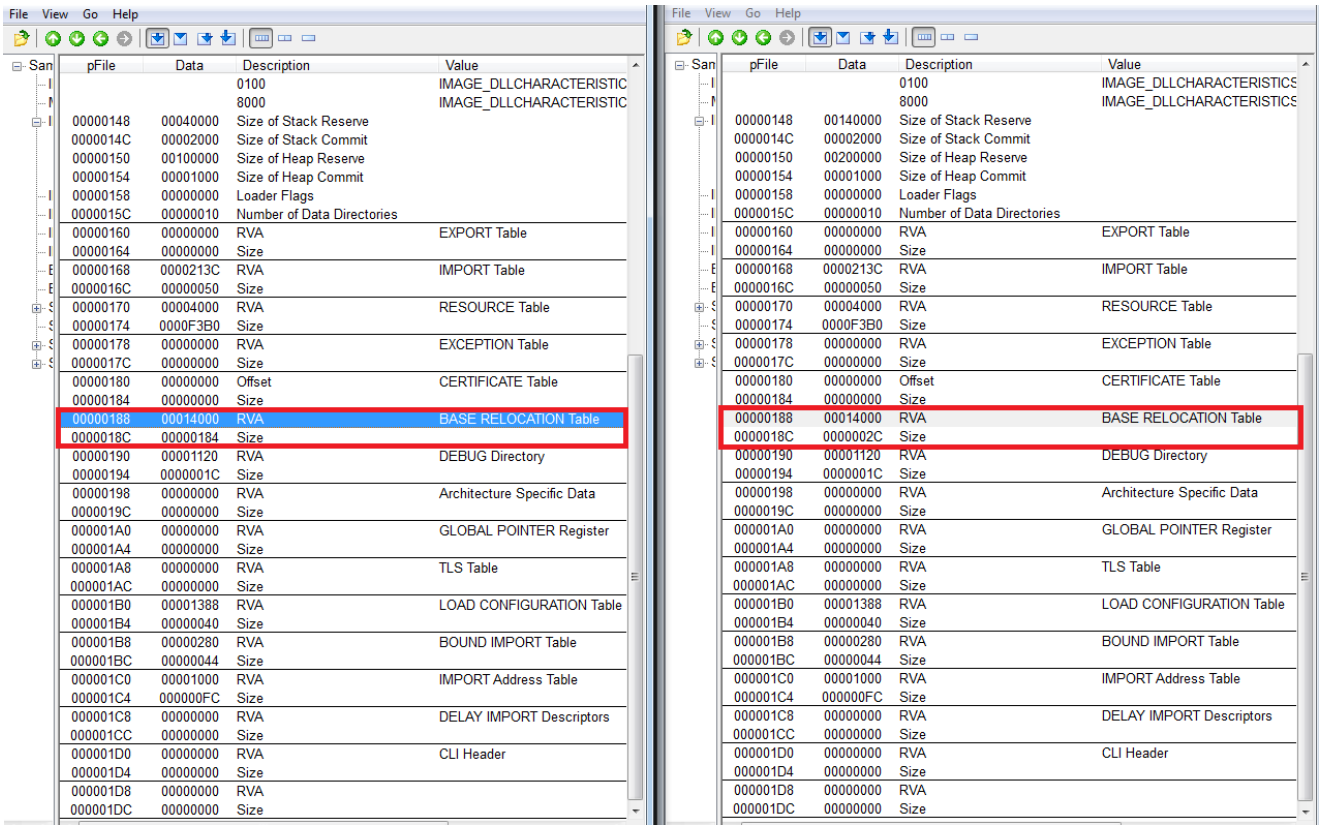

Figure 3: The latest Expiro variant reduces the size of the relocation table.

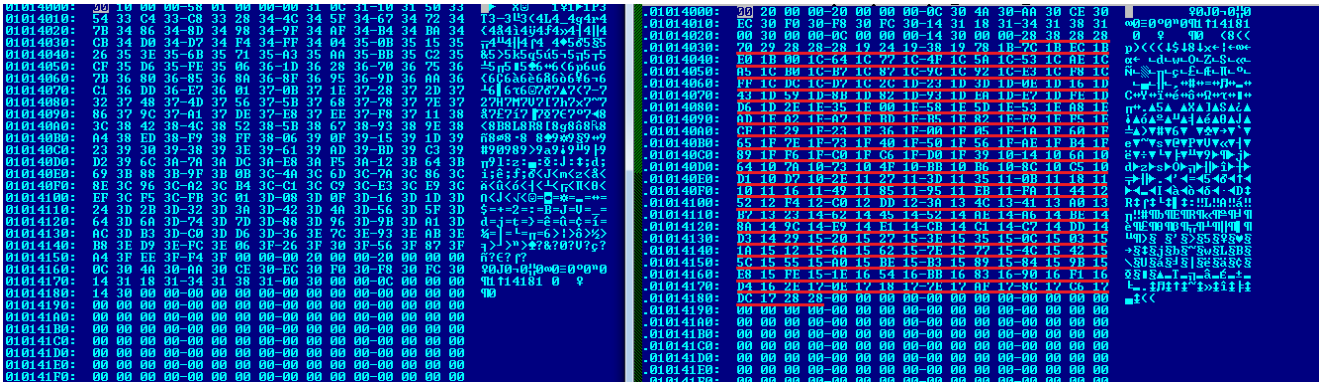

Figure 4: The relocation table encrypted by the latest Expiro variant.

To fix relocations prior to the execution of the original file's code, the Expiro virus first executes its own malicious payload. It then decrypts the relocation table and dynamically reloads all addresses to make sure the original file can run correctly.

Decryption involves a simple XOR operation with a key hardcoded within the sample.

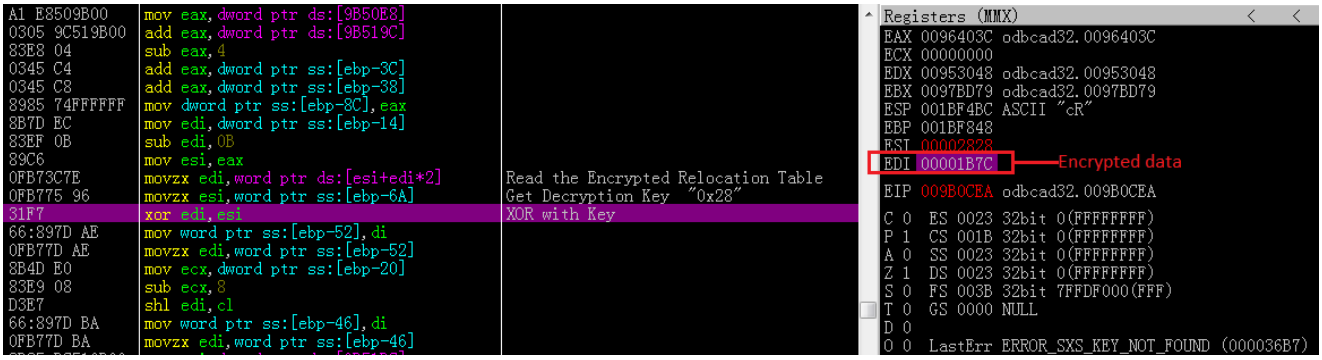

Figure 5: Relocation table being decrypted using a hardcoded XOR key.

After the decryption, the rest of original base relocation table is recovered.

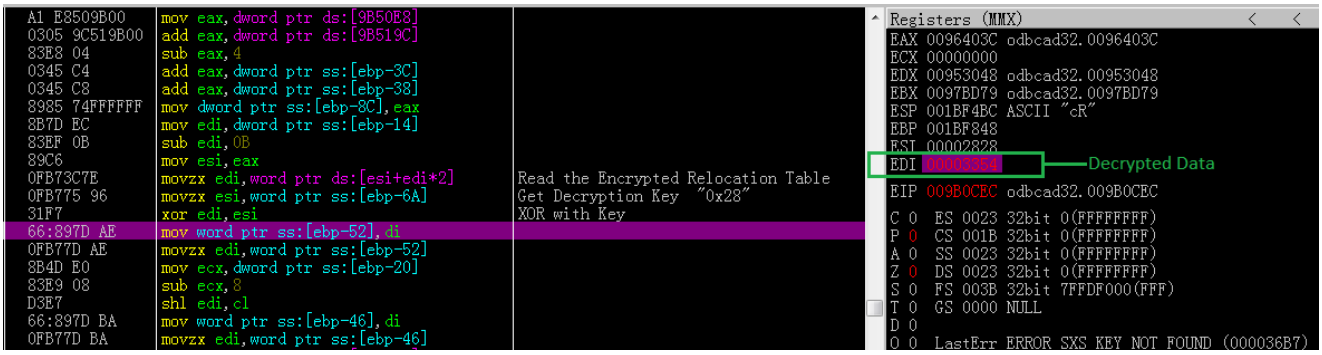

Figure 6: The EDI register now contains decrypted relocation data.

In recovery step 2, Expiro computes the address that contains the relocation address using the formula Relocation_Address = NewImageBase + Offset + VirtualAddress.

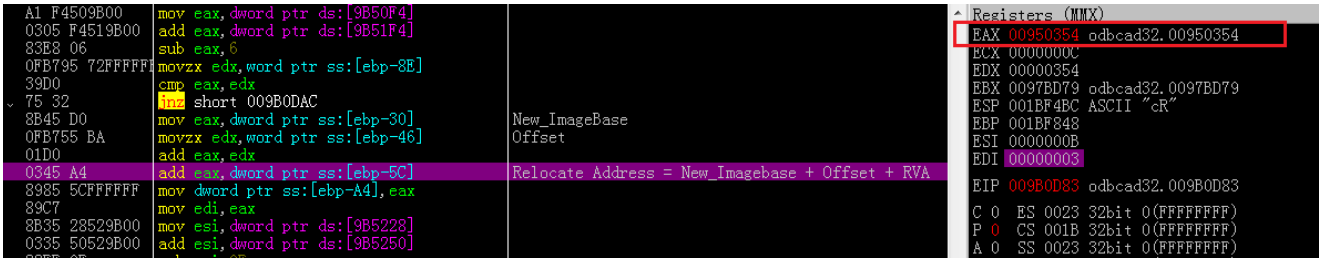

Figure 7: Calculation of the address to be relocated in Expiro's code.

As we see in the following screenshot, the formula leads to Relocation_Address = 0x950000 + 0x354 + 0x1000, so the address in 0x951354 should be relocated (stored in eax).

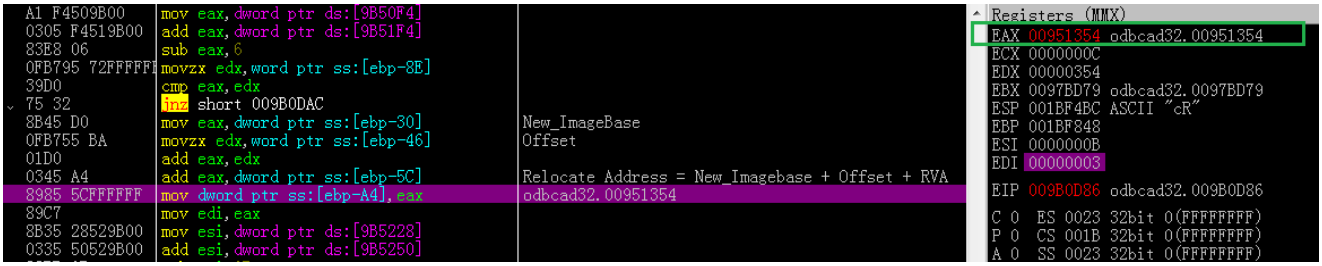

Figure 8: Relocation address being calculated.

In recovery step 3, Expiro computes the relocation value using the formula Relocation_Value = OldValue + (NewImageBase – OldImagebase).

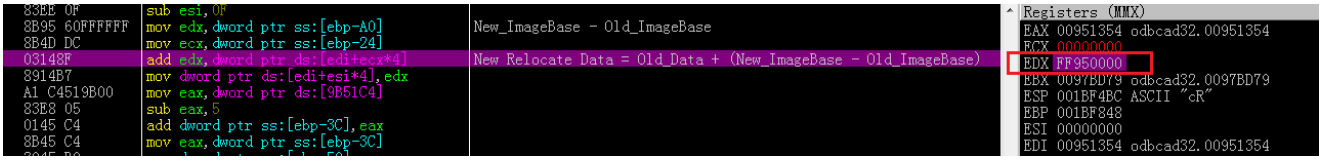

Figure 9: Relocation value being computed by Expiro.

In this case, the formula is Relocation _Value = 0x01001354 + (0x00950000 – 0x01000000), so the relocation value is 0x00951354.

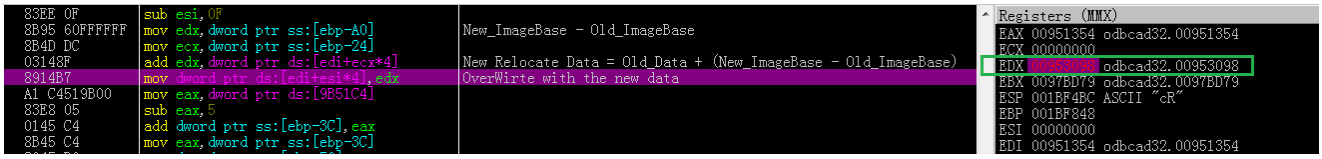

Figure 10: Expiro performing relocations on its own.

Using this technique, we can decrypt and repair the entire relocation table of the files infected by Expiro. This also helps us to calculate and replace the relocation table size in an executable's optional header with the correct values. These changes ensure the infected files can run properly after removing the malicious payload.

McAfee products detect Expiro as W32/Expiro.gen.rd and W64/Expiro.d and repair infected files from DAT Version 8665. Users can find additional information at this McAfee Labs Threat Advisory.

SHA-256 hash

f15b8fc3ca117ab38e3074adc6208666b2189259e447db8202ef85b9bbfc4537

Xiaobing Lin

More from McAfee Labs

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 05, 2022 | 4 MIN READ

Instagram Credentials Stealer: Disguised as Mod App

Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

May 03, 2022 | 4 MIN READ

Instagram Credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

May 03, 2022 | 6 MIN READ

Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ

Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ

Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ

Emotet’s Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ

HANCITOR DOC drops via CLIPBOARD

Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

‘Tis the Season for Scams

‘Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ

The Newest Malicious Actor: “Squirrelwaffle” Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ

Social Network Account Stealers Hidden in Android Gaming Hacking Tool

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ

Malicious PowerPoint Documents on the Rise

Authored by Anuradha M McAfee Labs have observed a new phishing campaign that utilizes macro capabilities available...

Sep 21, 2021 | 6 MIN READ