RIPlace Evasion Technique

High Probability Ransomware Detection Bypass and EDR Evasion

NYOTRON
SECURING THE WORLD

Executive Summary

Nyotron's Research team discovered a Windows file system technique that, when used to maliciously alter files, bypasses most existing anti-ransomware methods as well as other file system/data protections. In fact, all antivirus products tested so far were completely blind to file operations using this technique, including encryption. Moreover, even Endpoint Detection and Response (EDR) products are blind to this technique and hence these operations will not be visible for future incident response and investigation purposes. This technique has been named **RIPlace**.

Video demonstration of the RIPlace technique evading Windows Defender AV/CFA can be found here.

Background

Most ransomware perform the following actions:

1. Open and read original file
2. Encrypt content in memory
3. Destruct the original file by:
    - Writing encrypted content into original file
    - OR saving encrypted file to disk, while removing the original file using Delete file (or any similar method)
    - OR saving encrypted file to disk, then replace it with the original file using Rename (Rename has an option to overwrite the target in case it exists on disk)

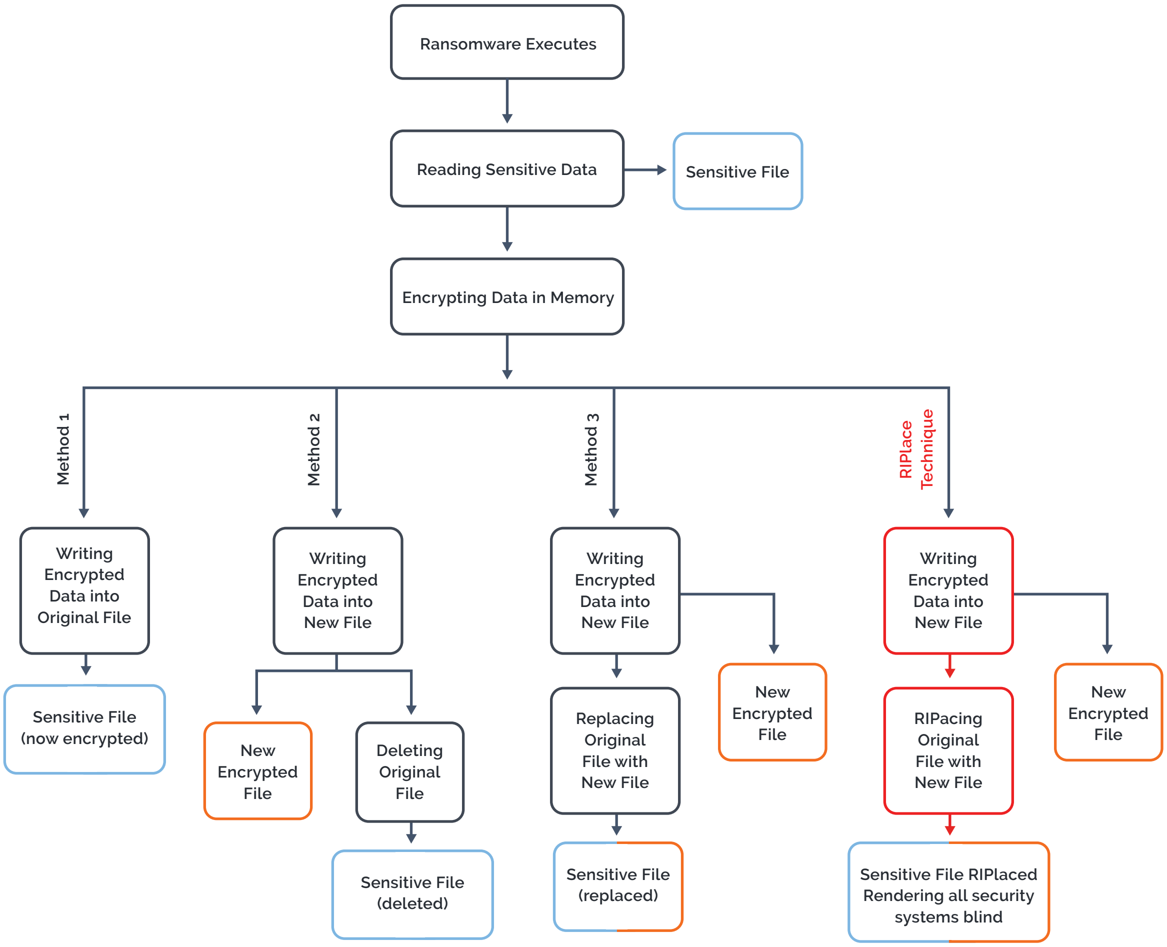
In order for a filter-driver (and hence an anti-ransomware or anti-malware product) to be effective against ransomware, these methods should be covered.

Enter RIPlace Evasion Technique

Let's now focus on the latter technique of file replacement using the Rename operation. Every time a Rename request is being called (specifically, IRP_MJ_SET_INFORMATION with FileInformationClass set to FileRenameInformation), the filter driver gets a callback, so that it could filter the request.

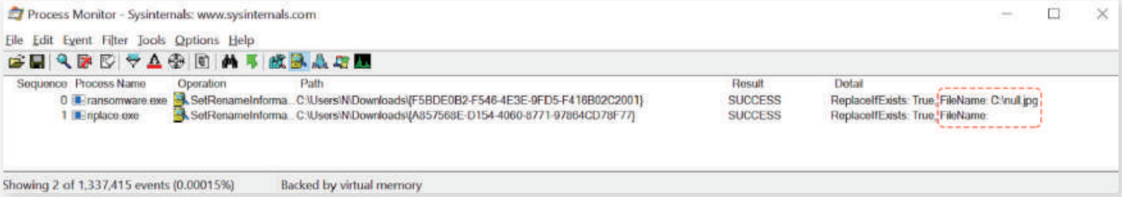
If prior to calling Rename, we call DefineDosDevice (a legacy function that creates a symlink), we can pass an arbitrary name as the device name, and the original file path, as the target to point on. This way we can get our device "XY" to refer to "C:\passwords.txt".

The RIPlace discovery is that in the callback function filter driver fails to parse the destination path when using the common routine FltGetDestinationFileNameInformation. It returns an error when passing a DosDevice path (instead of returning the path, post-processed); however, the Rename call succeeds.



Ransomware Executes
Reading Sensitive Data
Sensitive File
Encrypting Data in Memory
Method 1
Method 2
Method 3
RIPlace Technique
Writing Encrypted Data into Original File
Sensitive File (now encrypted)
Writing Encrypted Data into New File
New Encrypted File
Deleting Original File
Sensitive File (deleted)
Writing Encrypted Data into New File
New Encrypted File
Replacing Original File with New File
Sensitive File (replaced)
Writing Encrypted Data into New File
New Encrypted File
RIPacing Original File with New File
Sensitive File RIPlaced Rendering all security systems blind

When filtering such calls with Procmon, you can see an empty destination path (see sequence 1 below):


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Sequence	Process Name	Operation	Path	Result	Detail
0	ransomware.exe	SetRenameInforma...	C:\Users\N\Downloads\{F5BDE0B2-F546-4E3E-9FD5-F416B02C2001}	SUCCESS	ReplaceIfExists: True, FileName: C:\null.jpg
1	riplace.exe	SetRenameInforma...	C:\Users\N\Downloads\{A857568E-D154-4060-8771-97864CD78F77}	SUCCESS	ReplaceIfExists: True, FileName:

Showing 2 of 1,337,415 events (0.00015%)   Backed by virtual memory

Using this technique, it is possible to maliciously encrypt files and bypass antivirus/anti-ransomware products that do not properly handle IRP_MJ_SET_INFORMATION callback. We believe that malicious actors may abuse this technique in order to bypass security products that rely on FltGetDestinationFileNameInformation routine as well as avoid any recording of such activity by EDR products.

Credits

Daniel Prizmant, Guy Meoded, Freddy Ouzan, Hanan Natan.

Please reach out to **riplace@nyotron.com** for the POC or any other questions.

NYOTRON

SECURING THE WORLD

2880 Lakeside Drive Suite 237
Santa Clara, CA 95054
+1 (408) 780-0750

www.nyotron.com