Ex0c0 Submission

Gary Jones

Contents

Executive Summary

Goals

To use the Veil evasion framework to establish a meterpreter session on host books.artstailor.com.

Risk Ranking/Profile

Medium

Summary of Findings

It was found that the windows antivirus software dynamically identifies the python payload/handler veil-evasion meterpreter session that is sent to books.artstailor.com

Technical Report

Finding: *Descriptive Name*

Risk Rating

The risk rating is medium. Since the meterpreter session can be established for a few moments before being dynamically identified by windows defender there are a few moments where an intruder could issue commands into the system and compromise its integrity.

Vulnerability Description

By pivoting off the costumes.artstailor.com network I was able to connect to books.artstailor.com and establish a meterpreter session, if only for a few moments. This was accomplished by using the n.nomen credentials that were extracted and cracked using John the Ripper in earlier tests.

Mitigation or Resolution Strategy

A mitigation strategy would be to have n.nomen update their credentials to be in accordance with NIST Special Publication 800-63B.

Attack Narrative

In order to get to books.artstailor.com I had to go through costumes.artstailor.com. This was accomplished using two rdesktop sessions. The first session I connected to costumes.artstailor.com and utilized the administrator credentials

provided. Once the firewall was down I then connected to the costumes network and using Chisel in conjunction with proxychains issued a second rdesktop session to books.artstailor.com (see figure 1). Once connected to books.artstailor.com I was able to login as n.nomen. Back on kali I utilized veil to create a payload/handler pair and designated the LHOST to be the kali ip address (see figure 2). After this I then started the msfconfig using the resource commands created in the meterp.rc file from veil (see figure 3). After copying the distribution directory into the shared /tmp folder I was able to change directories into it on the books.artstailor.com host and run the meterp.exe executable which was found to be dynamically identified by windows security (see figures 4, 5, and 6).

Following this I then ran veil again and utilized the c sharp version of this payload and noticed a difference in behavior. While the meterpreter session was able to run for a few moments with the python executable the c sharp version of this program was identified immediately and did not have a chance to run. Therefore it was identified statically.

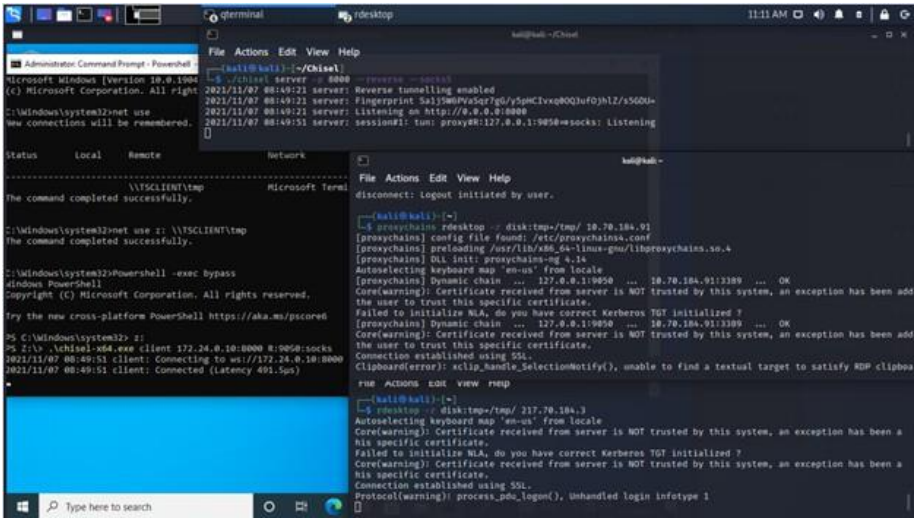

Figure 1:

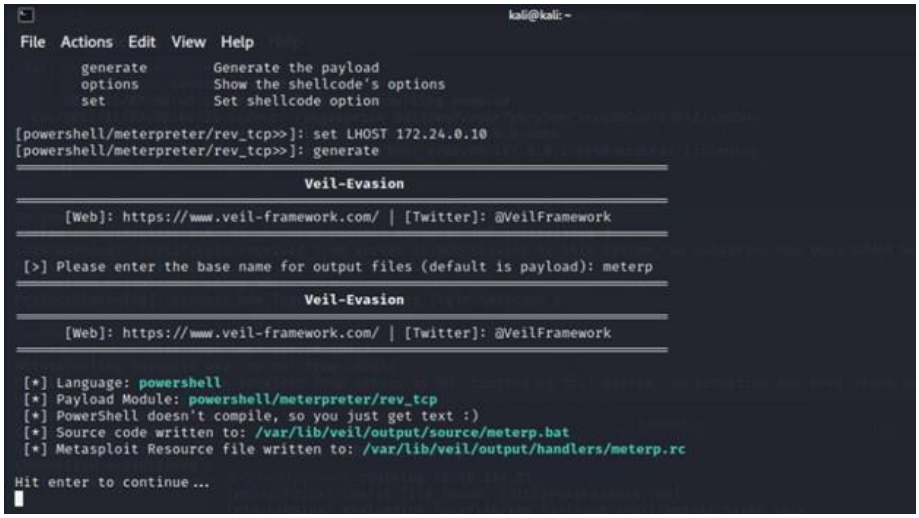

Figure 2:

Figure 3:

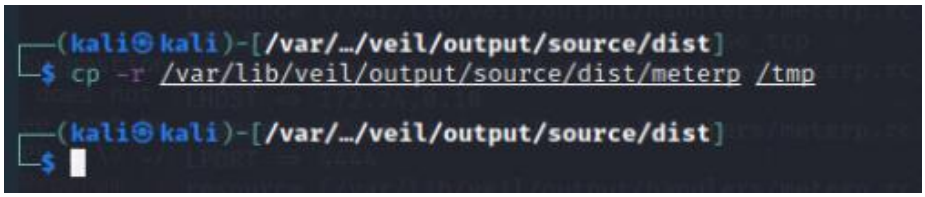

Figure 4:

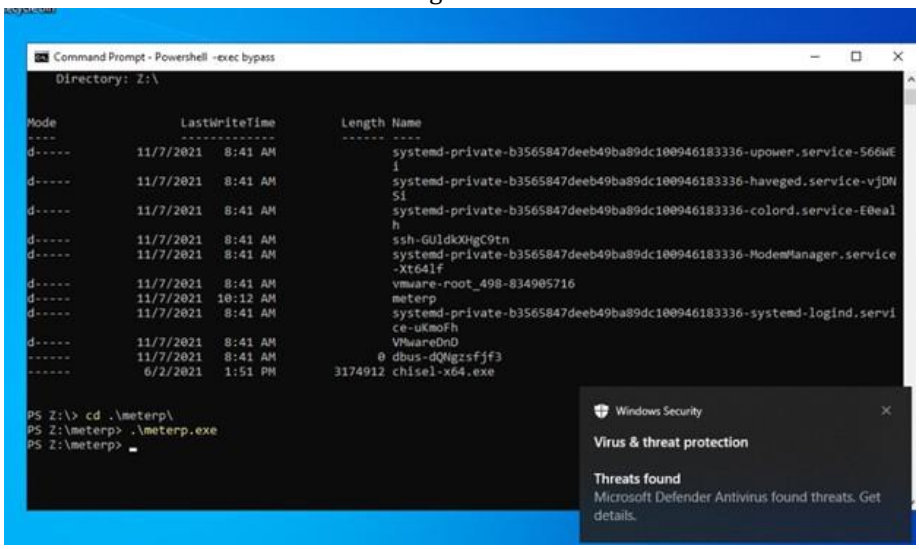

Figure 5:

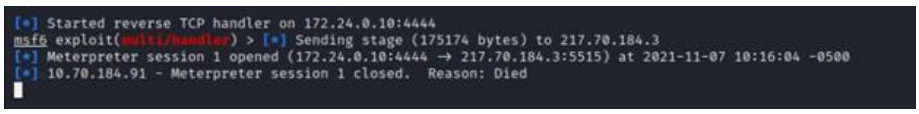

Figure 6: