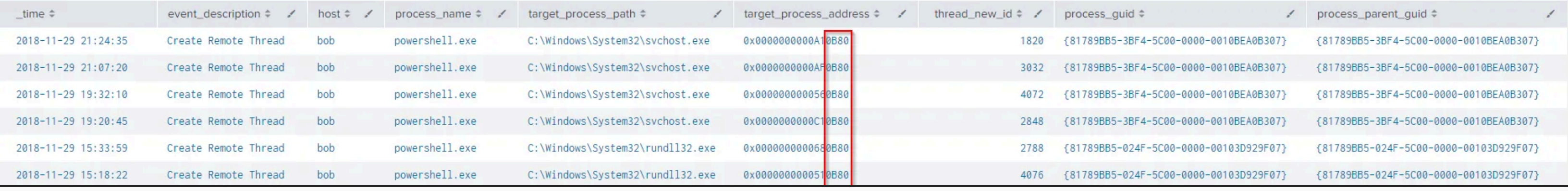
Cobalt Strike Remote Threads detection

Olaf Hartong · Follow

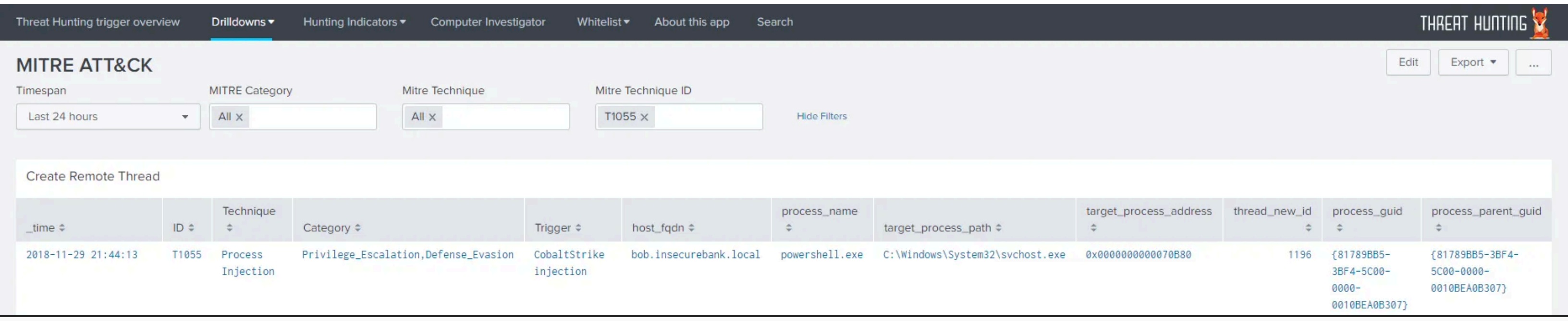
at the “Create Remote Thread” events and soon I noticed something interesting.

Every process injected bij Cobalt Strike is injected into a memory address which is starting from the same last 4 bytes on every thread.



_time	event_description	host	process_name	target_process_path	target_process_address	thread_new_id	process_guid	process_parent_guid
2018-11-29 21:24:35	Create Remote Thread	bob	powershell.exe	C:\Windows\System32\svchost.exe	0x0000000000A10B80	1820	{81789BB5-3BF4-5C00-0000-0010BEA0B307}	{81789BB5-3BF4-5C00-0000-0010BEA0B307}
2018-11-29 21:07:20	Create Remote Thread	bob	powershell.exe	C:\Windows\System32\svchost.exe	0x0000000000AF0B80	3032	{81789BB5-3BF4-5C00-0000-0010BEA0B307}	{81789BB5-3BF4-5C00-0000-0010BEA0B307}
2018-11-29 19:32:10	Create Remote Thread	bob	powershell.exe	C:\Windows\System32\svchost.exe	0x0000000000560B80	4072	{81789BB5-3BF4-5C00-0000-0010BEA0B307}	{81789BB5-3BF4-5C00-0000-0010BEA0B307}
2018-11-29 19:20:45	Create Remote Thread	bob	powershell.exe	C:\Windows\System32\svchost.exe	0x0000000000C10B80	2848	{81789BB5-3BF4-5C00-0000-0010BEA0B307}	{81789BB5-3BF4-5C00-0000-0010BEA0B307}
2018-11-29 15:33:59	Create Remote Thread	bob	powershell.exe	C:\Windows\System32\rundll32.exe	0x0000000000680B80	2788	{81789BB5-024F-5C00-0000-00103D929F07}	{81789BB5-024F-5C00-0000-00103D929F07}
2018-11-29 15:18:22	Create Remote Thread	bob	powershell.exe	C:\Windows\System32\rundll32.exe	0x0000000000510B80	4076	{81789BB5-024F-5C00-0000-00103D929F07}	{81789BB5-024F-5C00-0000-00103D929F07}

I’ve incorporated it into my ThreatHunting app, which will be released at BlackHat EU next week on Dec 5th. A detection of the event will look like this:

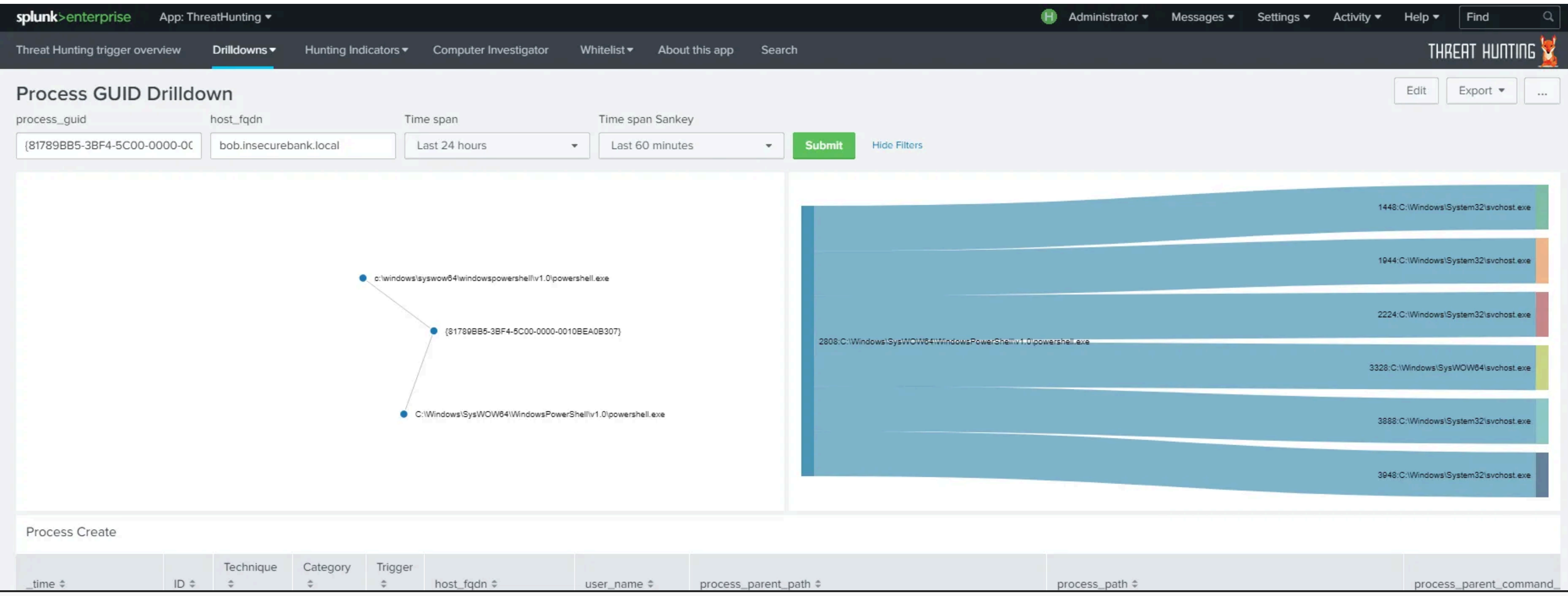


MITRE ATT&CK

Timespan: Last 24 hours
MITRE Category: All ×
Mitre Technique: All ×
Mitre Technique ID: T1055 ×

Create Remote Thread

_time	ID	Technique	Category	Trigger	host_fqdn	process_name	target_process_path	target_process_address	thread_new_id	process_guid	process_parent_guid
2018-11-29 21:44:13	T1055	Process Injection	Privilege_Escalation,Defense_Evasion	CobaltStrike injection	bob.insecurebank.local	powershell.exe	C:\Windows\System32\svchost.exe	0x0000000000070B80	1196	{81789BB5-3BF4-5C00-0000-0010BEA0B307}	{81789BB5-3BF4-5C00-0000-0010BEA0B307}


splunk>enterprise
App: ThreatHunting ▾
Administrator ▾
Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Threat Hunting trigger overview
Drilldowns ▾
Hunting Indicators ▾
Computer Investigator
Whitelist ▾
About this app
Search
THREAT HUNTING
Edit
Export ▾
...
Submit
Hide Filters
c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
{81789BB5-3BF4-5C00-0000-0010BEA0B307}
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
2808:C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
1448:C:\Windows\System32\svchost.exe
1944:C:\Windows\System32\svchost.exe
2224:C:\Windows\System32\svchost.exe
3328:C:\Windows\SysWOW64\svchost.exe
3888:C:\Windows\System32\svchost.exe
3948:C:\Windows\System32\svchost.exe

Process GUID Drilldown

process_guid: {81789BB5-3BF4-5C00-0000-0C
host_fqdn: bob.insecurebank.local
Time span: Last 24 hours
Time span Sankey: Last 60 minutes

Process Create

_time	ID	Technique	Category	Trigger	host_fqdn	user_name	process_parent_path	process_path	process_parent_command_

them.

Evasion

It seems there is a way to change this default behavior by using the following code in a malleable profile;

```
{ stage
    transform-x86 { # transform the x86 rDLL stage
    prepend "\x90\x90\x90\x90\x90\x90\x90\x90\x90"; # prepend 9
```

Detection strategy

Doing this will bypass detection of the rule mentioned above, this obviously can be changed or widened. This probably will introduce some more false positives. I believe going for the “0B80" still remains a valid detection, most red teams/adversaries won’t know about this thus won’t change the default.

On top of this baseline injection behavior in your environment, this is not that common that you get swamped by data anyway. Create an alert on

Written by Olaf Hartong

Follow

2K Followers

FalconForce | Data Dweller | Microsoft MVP