Home Blog Research Malware & Hunting GitHub

Recent posts

Malicious document identified in the conflict Israel & Gaza themed about terrorist organizations related to Iran

Dissecting GobRAT behaviors - Linux malware

Analyzing AsyncRAT distributed in Colombia by Blind Eagle

Using Jlaive to create batch files from .NET assemblies for defense evasion

Executing SCR files using desk.cpl and InstallScreenSaver API Call

DLL Hijacking with DeviceCensus.exe on Windows 11

Executing SCR files using desk.cpl and InstallScreenSaver API Call

May 3, 2022 · 4 min read

Jose Luis Sánchez Martínez
Security Researcher

Summary

INFO

This blog was made from the following sources.

Reference 1: https://vxug.fakedoma.in/zines/29a/29a7/Articles/29A-7.030.txt

Reference 2: https://twitter.com/pabraeken/status/998627081360695297

Reference 3: https://twitter.com/VakninHai/status/1517027824984547329

Reference 4: https://lolbas-project.github.io/lolbas/Libraries/Desk/

Recently some researchers have discovered a possible execution of binaries using the Windows Desktop Settings Control Panel utility located at `C:\Windows\System32\desk.cpl` or `C:\Windows\SysWOW64\desk.cpl` for 32-bit.

This utility allows executing a binary with a `.scr` extension by calling the `InstallScreenSaver` function.

The objective of this entry is focused only on identifying the visibility and detection of the operating system.

Testing the behavior

In this case, I'm going to create a copy of `cmd.exe` called `joseliyopoc.scr` on the desktop.

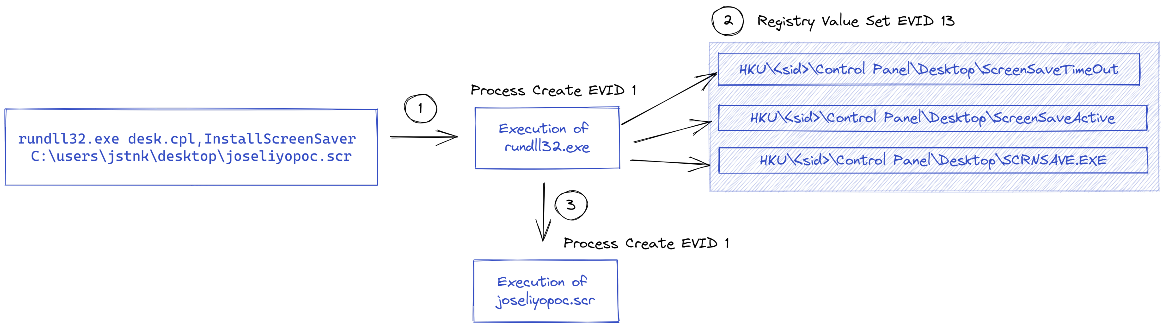
```
copy C:\windows\system32\cmd.exe C:\users\jstnk\Desktop\joseliyopoc.scr
```

After that, I run `desk.cpl` using `rundll32.exe` on a new command line passing the `InstallScreenSaver` API call and the newly created `.scr` file as parameters.

```
rundll32.exe desk.cpl,InstallScreenSaver C:\users\jstnk\desktop\joseliy
```

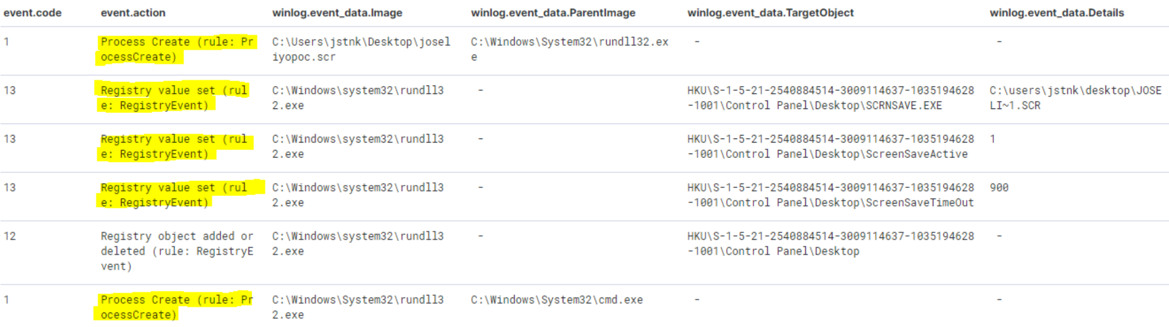
Sysmon

We can see in Sysmon how there are different events generated during the previous execution. However, focusing on those events that could be of more interest to generate detections are related to events number `1 - Process Create` and `13 - Registry Value Set`


rundll32.exe desk.cpl,InstallScreenSaver
C:\users\jstnk\desktop\joseliyopoc.scr
1
Process Create EVID 1
Execution of rundll32.exe
2
Registry Value Set EVID 13
HKU\<sid>\Control Panel\Desktop\ScreenSaveTimeOut
HKU\<sid>\Control Panel\Desktop\ScreenSaveActive
HKU\<sid>\Control Panel\Desktop\SCRNSAVE.EXE
3
Process Create EVID 1
Execution of joseliyopoc.scr

In the case of the registry key related to `HKU\<sid>\Control Panel\Desktop\SCRNSAVE.EXE`, it can be seen that the value in this case is the name of the `.scr` file. This information is really useful to generate detection mechanisms based on the entire context of this execution that we are carrying out (execution of `rundll32`, call to the `InstallScreenSaver` API, etc).

The other two values of the keys `HKU\<sid>\Control Panel\Desktop\ScreenSaveActive` and `HKU\<sid>\Control Panel\Desktop\ScreenSaveTimeOut` are also interesting, since in both cases, after multiple executions of this proof of concept, the values were the same in all cases (with this run by default).

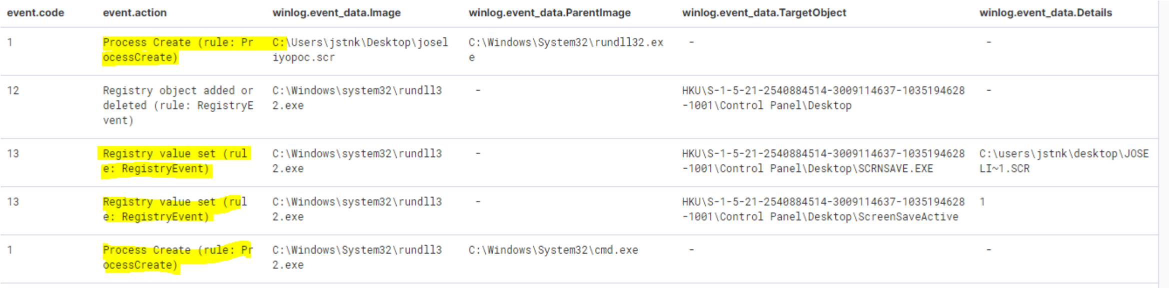


event.code	event.action	winlog.event_data.Image	winlog.event_data.ParentImage	winlog.event_data.TargetObject	winlog.event_data.Details
1	Process Create (rule: ProcessCreate)	C:\Users\jstnk\Desktop\joseliyopoc.scr	C:\Windows\System32\rundll32.exe	-	-
13	Registry value set (rule: RegistryEvent)	C:\Windows\system32\rundll32.exe	-	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\SCRNSAVE.EXE	C:\users\jstnk\desktop\JOSELI~1.SCR
13	Registry value set (rule: RegistryEvent)	C:\Windows\system32\rundll32.exe	-	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\ScreenSaveActive	1
13	Registry value set (rule: RegistryEvent)	C:\Windows\system32\rundll32.exe	-	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\ScreenSaveTimeOut	900
12	Registry object added or deleted (rule: RegistryEvent)	C:\Windows\system32\rundll32.exe	-	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop	-
1	Process Create (rule: ProcessCreate)	C:\Windows\System32\rundll32.exe	C:\Windows\System32\cmd.exe	-	-

You can get more information about these registry keys in the following links:

- ScreenSaveTimeOut: http://systemmanager.ru/win2k_regestry.en/34634.htm
- ScreenSaveActive: http://systemmanager.ru/win2k_regestry.en/93257.htm
- SCRNSAVE.EXE: https://docs.microsoft.com/sk-sk/windows/win32/devnotes/scrnsave-exe

Something interesting that is important to mention is that, in seconds, thirds, fourths, etc. executions, only two of the three registry keys seen above are modified or there is any kind of interaction with them. These keys are the ones related to `ScreenSaveActive` and `SCRNSAVE.EXE`. In both cases, the value will be the same as seen above, unless the `.scr` file we run has a different name, in which case the value of `SCRNSAVE.EXE` will be that of the new `.scr` file.

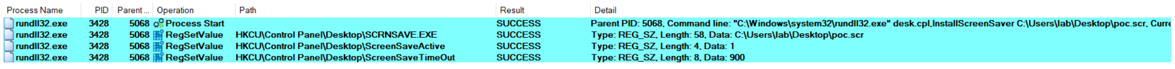


event.code	event.action	winlog.event_data.Image	winlog.event_data.ParentImage	winlog.event_data.TargetObject	winlog.event_data.Details
1	Process Create (rule: ProcessCreate)	C:\Users\jstnk\Desktop\joseliyopoc.scr	C:\Windows\System32\rundll32.exe	-	-
12	Registry object added or deleted (rule: RegistryEvent)	C:\Windows\system32\rundll32.exe	-	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop	-
13	Registry value set (rule: RegistryEvent)	C:\Windows\system32\rundll32.exe	-	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\SCRNSAVE.EXE	C:\users\jstnk\desktop\JOSELI~1.SCR
13	Registry value set (rule: RegistryEvent)	C:\Windows\system32\rundll32.exe	-	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\ScreenSaveActive	1
1	Process Create (rule: ProcessCreate)	C:\Windows\System32\rundll32.exe	C:\Windows\System32\cmd.exe	-	-

Procmon

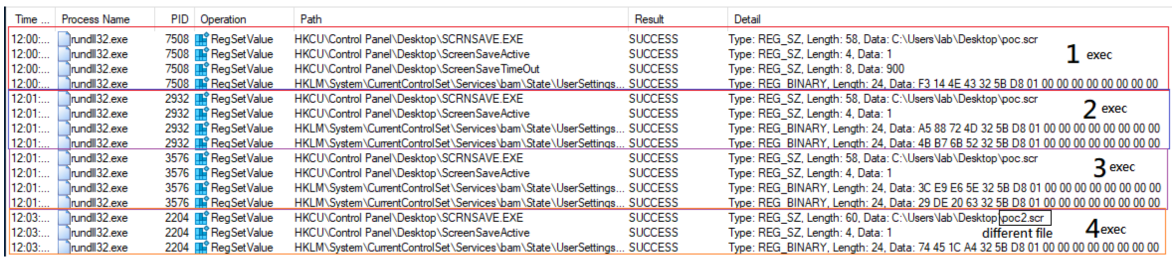
> ⓘ **INFO**
>
> In this Twitter thread you have more info about the execution I did using procmon: https://twitter.com/Joseliyo_Jstnk/status/1519769245378297856

In this case, I used a different name for the `.scr` file and a different OS version (both W10). The rest of the process was similar. The following image contains the information about the registry keys mentioned above, where it is reflected that new values are established.



Process Name	PID	Parent ...	Operation	Path	Result	Detail
rundll32.exe	3428	5068	Process Start		SUCCESS	Parent PID: 5068, Command line: "C:\Windows\system32\rundll32.exe" desk.cpl,InstallScreenSaver C:\Users\lab\Desktop\poc.scr, Curre
rundll32.exe	3428	5068	RegSetValue	HKCU\Control Panel\Desktop\SCRNSAVE.EXE	SUCCESS	Type: REG_SZ, Length: 58, Data: C:\Users\lab\Desktop\poc.scr
rundll32.exe	3428	5068	RegSetValue	HKCU\Control Panel\Desktop\ScreenSaveActive	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
rundll32.exe	3428	5068	RegSetValue	HKCU\Control Panel\Desktop\ScreenSaveTimeOut	SUCCESS	Type: REG_SZ, Length: 8, Data: 900

When performing different executions, even changing the name of the `.scr` file, it can be seen how from the second iteration, only two registry keys are modified. However, the first time we run it, all three keys are changed. The following image shows the 4 executions that I did.



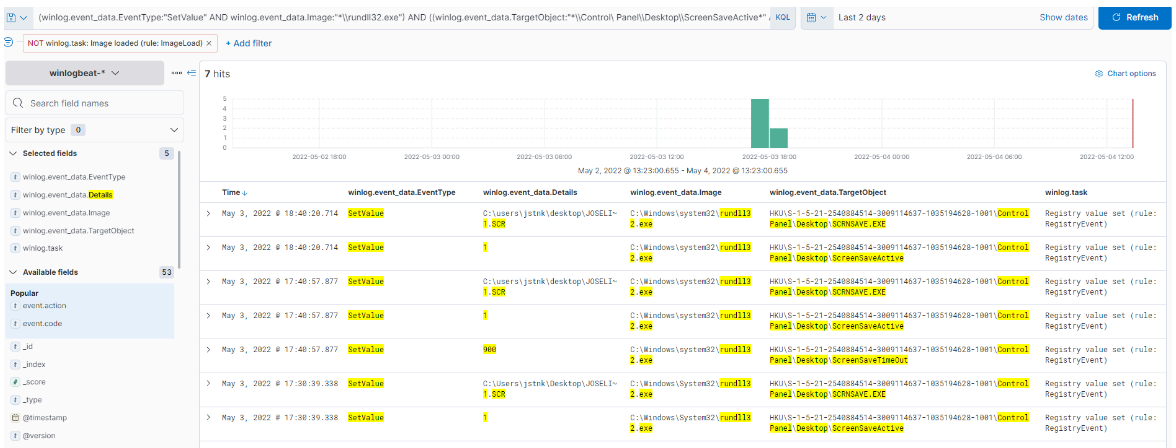
Time ...	Process Name	PID	Operation	Path	Result	Detail
12:00:...	rundll32.exe	7508	RegSetValue	HKCU\Control Panel\Desktop\SCRNSAVE.EXE	SUCCESS	Type: REG_SZ, Length: 58, Data: C:\Users\lab\Desktop\poc.scr
12:00:...	rundll32.exe	7508	RegSetValue	HKCU\Control Panel\Desktop\ScreenSaveActive	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
12:00:...	rundll32.exe	7508	RegSetValue	HKCU\Control Panel\Desktop\ScreenSaveTimeOut	SUCCESS	Type: REG_SZ, Length: 8, Data: 900
12:00:...	rundll32.exe	7508	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings...	SUCCESS	Type: REG_BINARY, Length: 24, Data: F3 14 4E 43 32 5B D8 01 00 00 00 00 00 00 00 00
12:01:...	rundll32.exe	2932	RegSetValue	HKCU\Control Panel\Desktop\SCRNSAVE.EXE	SUCCESS	Type: REG_SZ, Length: 58, Data: C:\Users\lab\Desktop\poc.scr
12:01:...	rundll32.exe	2932	RegSetValue	HKCU\Control Panel\Desktop\ScreenSaveActive	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
12:01:...	rundll32.exe	2932	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings...	SUCCESS	Type: REG_BINARY, Length: 24, Data: A5 88 72 4D 32 5B D8 01 00 00 00 00 00 00 00 00
12:01:...	rundll32.exe	2932	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings...	SUCCESS	Type: REG_BINARY, Length: 24, Data: 4B B7 6B 52 32 5B D8 01 00 00 00 00 00 00 00 00
12:01:...	rundll32.exe	3576	RegSetValue	HKCU\Control Panel\Desktop\SCRNSAVE.EXE	SUCCESS	Type: REG_SZ, Length: 58, Data: C:\Users\lab\Desktop\poc.scr
12:01:...	rundll32.exe	3576	RegSetValue	HKCU\Control Panel\Desktop\ScreenSaveActive	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
12:01:...	rundll32.exe	3576	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings...	SUCCESS	Type: REG_BINARY, Length: 24, Data: 3C E9 E6 5E 32 5B D8 01 00 00 00 00 00 00 00 00
12:01:...	rundll32.exe	3576	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings...	SUCCESS	Type: REG_BINARY, Length: 24, Data: 29 DE 20 63 32 5B D8 01 00 00 00 00 00 00 00 00
12:03:...	rundll32.exe	2204	RegSetValue	HKCU\Control Panel\Desktop\SCRNSAVE.EXE	SUCCESS	Type: REG_SZ, Length: 60, Data: C:\Users\lab\Desktop\poc2.scr
12:03:...	rundll32.exe	2204	RegSetValue	HKCU\Control Panel\Desktop\ScreenSaveActive	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
12:03:...	rundll32.exe	2204	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings...	SUCCESS	Type: REG_BINARY, Length: 24, Data: 74 45 1C A4 32 5B D8 01 00 00 00 00 00 00 00 00

Detection

The following Elastic Query can help us to detect the behavior described above, if our purpose is detect the changes of the 3 registry keys.

```
((winlog.event_data.EventType:"SetValue" AND winlog.event_data.Image:"*
```

```
((winlog.event_data.EventType:"SetValue" AND
winlog.event_data.Image:"*\\rundll32.exe") AND
((winlog.event_data.TargetObject:"*\\Control
Panel\\Desktop\\ScreenSaveActive*" AND winlog.event_data.Details:"1") OR
(winlog.event_data.TargetObject:"*\\Control
Panel\\Desktop\\ScreenSaveTimeOut*" AND winlog.event_data.Details:"900")
OR (winlog.event_data.TargetObject:"*\\Control
Panel\\Desktop\\SCRNSAVE.EXE*" AND winlog.event_data.Details:*.scr)))
```



(winlog.event_data.EventType:"SetValue" AND winlog.event_data.Image:"*\\rundll32.exe") AND ((winlog.event_data.TargetObject:"*\\Control\ Panel\\Desktop\\ScreenSaveActive*"

NOT winlog.task: Image loaded (rule: ImageLoad)

Last 2 days

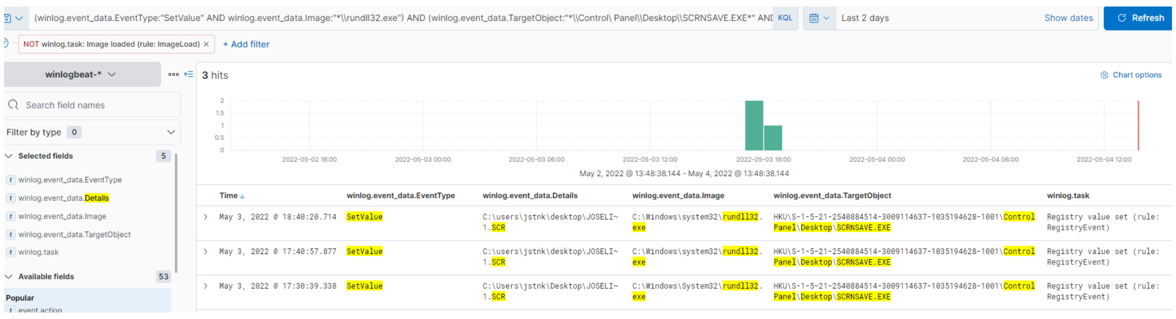
7 hits

May 2, 2022 @ 13:23:00.655 - May 4, 2022 @ 13:23:00.655

	Time ↓	winlog.event_data.EventType	winlog.event_data.Details	winlog.event_data.Image	winlog.event_data.TargetObject	winlog.task
›	May 3, 2022 @ 18:40:20.714	SetValue	C:\users\jstnk\desktop\JOSELI~1.SCR	C:\Windows\system32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\SCRNSAVE.EXE	Registry value set (rule: RegistryEvent)
›	May 3, 2022 @ 18:40:20.714	SetValue	1	C:\Windows\system32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\ScreenSaveActive	Registry value set (rule: RegistryEvent)
›	May 3, 2022 @ 17:40:57.877	SetValue	C:\users\jstnk\desktop\JOSELI~1.SCR	C:\Windows\system32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\SCRNSAVE.EXE	Registry value set (rule: RegistryEvent)
›	May 3, 2022 @ 17:40:57.877	SetValue	1	C:\Windows\system32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\ScreenSaveActive	Registry value set (rule: RegistryEvent)
›	May 3, 2022 @ 17:40:57.877	SetValue	900	C:\Windows\system32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\ScreenSaveTimeOut	Registry value set (rule: RegistryEvent)
›	May 3, 2022 @ 17:30:39.338	SetValue	C:\Users\jstnk\Desktop\JOSELI~1.SCR	C:\Windows\System32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\SCRNSAVE.EXE	Registry value set (rule: RegistryEvent)
›	May 3, 2022 @ 17:30:39.338	SetValue	1	C:\Windows\System32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\ScreenSaveActive	Registry value set (rule: RegistryEvent)

Howerver, if we want to detect only the key related to the .scr file when it is established using `rundll32.exe`, the following query can help us.

```
(winlog.event_data.EventType:"SetValue" AND winlog.event_data.Image:"*\
(winlog.event_data.EventType:"SetValue" AND
winlog.event_data.Image:"*\\rundll32.exe") AND
(winlog.event_data.TargetObject:"*\\Control
Panel\\Desktop\\SCRNSAVE.EXE*" AND winlog.event_data.Details:*.scr)
```



(winlog.event_data.EventType:"SetValue" AND winlog.event_data.Image:"*\\rundll32.exe") AND (winlog.event_data.TargetObject:"*\\Control\ Panel\\Desktop\\SCRNSAVE.EXE*" ANI

NOT winlog.task: Image loaded (rule: ImageLoad)

winlogbeat-*

3 hits

May 2, 2022 @ 13:48:38.144 - May 4, 2022 @ 13:48:38.144

	Time	winlog.event_data.EventType	winlog.event_data.Details	winlog.event_data.Image	winlog.event_data.TargetObject	winlog.task
›	May 3, 2022 @ 18:40:20.714	SetValue	C:\users\jstnk\desktop\JOSELI~1.SCR	C:\Windows\system32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\SCRNSAVE.EXE	Registry value set (rule: RegistryEvent)
›	May 3, 2022 @ 17:40:57.877	SetValue	C:\users\jstnk\desktop\JOSELI~1.SCR	C:\Windows\system32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\SCRNSAVE.EXE	Registry value set (rule: RegistryEvent)
›	May 3, 2022 @ 17:30:39.338	SetValue	C:\Users\jstnk\Desktop\JOSELI~1.SCR	C:\Windows\System32\rundll32.exe	HKU\S-1-5-21-2540884514-3009114637-1035194628-1001\Control Panel\Desktop\SCRNSAVE.EXE	Registry value set (rule: RegistryEvent)

UPDATE May 6, 2022

New query to avoid false positives related to legitimate use of screen saver. Preventing the SCRNSAVE.EXE registry key contains system32 and syswow64 paths.

```
(winlog.event_data.EventType:"SetValue" AND winlog.event_data.Image:"*\
```

```
(winlog.event_data.EventType:"SetValue" AND
winlog.event_data.Image:"*\\rundll32.exe") AND
(winlog.event_data.TargetObject:"*\\Control
Panel\\Desktop\\SCRNSAVE.EXE*" AND winlog.event_data.Details:*.scr) AND
NOT (winlog.event_data.Details:"C:\\Windows\\System32\\*" OR
winlog.event_data.Details:"C:\\Windows\\SysWOW64\\*")
```

Sigma rule

New sigma rule published on GitHub.

Sigma link: https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_set/registry_set_scr_file_executed_by_rundll32.yml

```
title: ScreenSaver Registry Key Set
id: 40b6e656-4e11-4c0c-8772-c1cc6dae34ce
description: Detects registry key established after masqueraded .scr fi
status: experimental
date: 2022/05/04
modified: 2022/05/04
author: Jose Luis Sanchez Martinez (@Joseliyo_Jstnk)
references:
    - https://twitter.com/VakninHai/status/1517027824984547329
    - https://twitter.com/pabraeken/status/998627081360695297
    - https://jstnk9.github.io/jstnk9/research/InstallScreenSaver-SCR-f
logsource:
    product: windows
    category: registry_set
detection:
    selection:
        EventType: SetValue
        Image|endswith: '\rundll32.exe'
    registry:
        TargetObject|contains: '\Control Panel\Desktop\SCRNSAVE.EXE'
        Details|endswith: '.scr'
    filter:
        Details|contains:
        - 'C:\Windows\System32\'
        - 'C:\Windows\SysWOW64\'
    condition: selection and registry and not filter
```

```
falsepositives:
    - legitimate use of screen saver
level: medium
tags:
    - attack.defense_evasion
    - attack.t1218.011
```

Contact

Twitter: https://twitter.com/Joseliyo_Jstnk

LinkedIn: https://www.linkedin.com/in/joseluissm/

Tags: threat hunting detection visibility research

Newer Post
« Using Jlaive to create batch files from .NET assemblies for defense evasion

Older Post
DLL Hijacking with DeviceCensus.exe on Windows 11 »

Docs

Home

Blog

Social Media

Twitter

LinkedIn

More

GitHub