

← Post

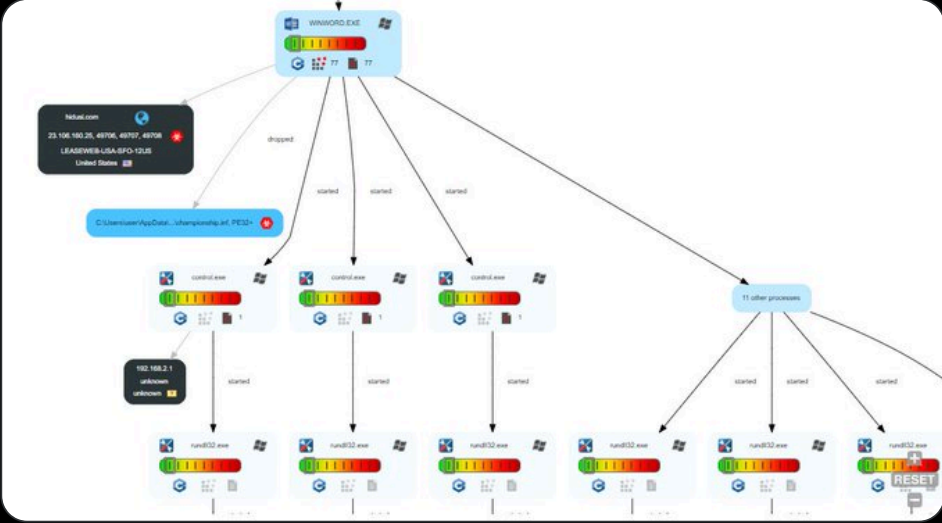
neonprimetime
@neonprimetime

sample mentioned in sigma rule from @JAMESWT_MHT

[bazaar.abuse.ch/sample/938545f...](#)

[app.any.run/tasks/36c14029...](#)

md5 1d2094ce85d66878ee079185e2761beb



Ring3API 🇪🇺🇧🇪 @ntlmrelay · Sep 8, 2021

Another #IOC-Based free #Sigma which included this behavior. @RedDrip7 nice find! this also tracked by @joe4security sandbox.

➡️ [tdm.socprime.com/tdm/info/vzmHh...](#)

+ one more #ThreatHunting rule available by tag: ➡️ [tdm.socprime.com/?tagsCustom=CV.....](#)

Show more

sources:

- [https://twitter.com/EXPMON_/status/1435389115883828296](#)
- [https://twitter.com/ShadowChasing1/status/1433252128186829861](#)
- [https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444](#)
- [https://www.joesandbox.com/analysis/476188/1/lochtal](#)

source:

category: process_creation

product: windows

action:

selection_ioc:

- image_endswith:
 - 'control.exe'
- command_line_contains_all:
 - 'championship.inf' #https://www.joesandbox.com/analysis/476188/1/
 - 'AppData'

selection_behaviour:

- image_endswith:
 - 'control.exe'
- command_line_contains_all:
 - 'cpl' #https://www.joesandbox.com/analysis/476188/1/lochtal
 - '..\\'

selection_hashes:

- hashes_contains:
 - '6c18d7d8866eac1afd3804e61bf232329a276cdc'
 - '56a8d4f7809ca732c9e28f3df945a7826315254c'
 - '53b31e513d8e23e38b7f13364504ca7429f8e1fe'

condition: selection_ioc or selection_behaviour or selection_hashes

positives:

- unknown

severity:

- high

attack.initial_access

attack.t1566.001

Standard 🔍 Content Automation Analytics ⌵ Tools ⌵

🔍 CVE-2021-40444

111 out of 132,852 Rules 4 Sigma Rules 7 Log Sources 0 Tools 0 Actors 2 Tests

Zero Day Attack Detected by EXPMON [CVE-2021-40444 Exploitation] (via cmd)

IC Prime Team	type	Rule	logsource	process_creation
				1 ⬇️ 0

Zero Day Attack Detected by EXPMON [CVE-2021-40444 Exploitation] (via dns)

IC Prime Team	type	Rule	logsource	dns
				1 ⬇️ 0

Zero Day Attack Detected by EXPMON [CVE-2021-40444 Exploitation] (via proxy)

IC Prime Team	type	Rule	logsource	proxy
				6 ⬇️ 2

2:41 PM · Sep 8, 2021

8 Reposts 1 Quote 15 Likes 1 Bookmark

🗨️ ↺️ ❤️ 📌 1 ↗️

New to X?

Sign up now to get your own personalized timeline!

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Something went wrong. Try reloading.

Retry

[Terms of Service](#) [Privacy Policy](#) [Cookie Policy](#)
[Accessibility](#) [Ads info](#) [More ...](#) © 2024 X Corp.

Don't miss what's happening

People on X are the first to know.

Log in

Sign up

Welcome to x.com!

We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.
For more details, see our Privacy Policy: <https://x.com/en/privacy>.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies