Settings

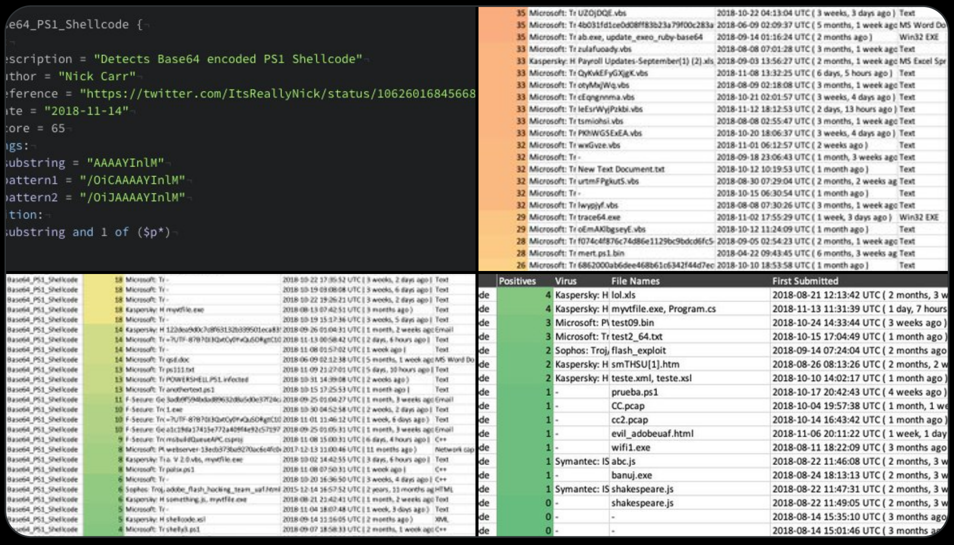
Post

Florian Roth
@cyb3rops

Great YARA rule by @ItsReallyNick for Base64 encoded PS shellcode pushed to our public signature-base repo

Rule
github.com/Neo23x0/signat...

VT Retrohunt & Munin results
docs.google.com/spreadsheets/d...



```
e64_PS1_Shellcode {

escription = "Detects Base64 encoded PS1 Shellcode"
thor = "Nick Carr"
eference = "https://twitter.com/ItsReallyNick/status/10626016845668
te = "2018-11-14"
ore = 65
gs:
substring = "AAAAYInlM"
pattern1 = "/OiCAAAAYInlM"
pattern2 = "/OiJAAAAYInlM"
tion:
substring and 1 of ($p*)
```

35	Microsoft: Tr	UZOjDQE.vbs	2018-10-22 04:13:04 UTC (3 weeks, 3 days ago)	Text
35	Microsoft: Tr	4b031fd1ce0d08ff83b23a79f00c283a	2018-06-09 02:09:37 UTC (5 months, 1 week ago	MS Word Do
35	Microsoft: Tr	ab.exe, update_exeo_ruby-base64	2018-09-14 01:16:24 UTC (2 months ago)	Win32 EXE
33	Microsoft: Tr	zulafuoady.vbs	2018-08-08 07:01:28 UTC (3 months, 1 week ago	Text
33	Kaspersky: H	Payroll Updates-September(1) (2).xls	2018-09-03 13:56:27 UTC (2 months, 1 week ago	MS Excel Spr
33	Microsoft: Tr	QyKvkEFyGXjgK.vbs	2018-11-08 13:32:25 UTC (6 days, 5 hours ago)	Text
33	Microsoft: Tr	otyMxjWq.vbs	2018-08-09 02:18:08 UTC (3 months, 1 week ago	Text
33	Microsoft: Tr	cEqngnnma.vbs	2018-10-21 02:01:57 UTC (3 weeks, 4 days ago)	Text
33	Microsoft: Tr	leEsrWyjPzkbi.vbs	2018-11-12 18:12:53 UTC (2 days, 13 hours ago)	Text
33	Microsoft: Tr	tsmiohsi.vbs	2018-08-08 02:55:47 UTC (3 months, 1 week ago	Text
33	Microsoft: Tr	PKhWGSExEA.vbs	2018-10-20 18:06:37 UTC (3 weeks, 4 days ago)	Text
32	Microsoft: Tr	wxGvze.vbs	2018-11-01 06:12:57 UTC (2 weeks ago)	Text
32	Microsoft: Tr	-	2018-09-18 23:06:43 UTC (1 month, 3 weeks ago	Text
32	Microsoft: Tr	New Text Document.txt	2018-10-12 10:19:53 UTC (1 month ago)	Text
32	Microsoft: Tr	urtmFPgkutS.vbs	2018-08-30 07:29:04 UTC (2 months, 2 weeks ag	Text
32	Microsoft: Tr	-	2018-10-15 06:30:54 UTC (1 month ago)	Text
32	Microsoft: Tr	lwypjyf.vbs	2018-08-08 07:30:26 UTC (3 months, 1 week ago	Text
29	Microsoft: Tr	trace64.exe	2018-11-02 17:55:29 UTC (1 week, 3 days ago)	Win32 EXE
29	Microsoft: Tr	oEmAKlbgseyE.vbs	2018-10-12 11:24:09 UTC (1 month ago)	Text
28	Microsoft: Tr	f074c4f876c74d86e1129bc9bdcd6fc5	2018-09-05 02:54:23 UTC (2 months, 1 week ago	Text
28	Microsoft: Tr	mert.ps1.bin	2018-04-22 09:43:45 UTC (6 months, 3 weeks ag	Text
26	Microsoft: Tr	6862000ab6dee468b61c6342f44d7ec	2018-10-10 18:53:58 UTC (1 month ago)	Text

Base64_PS1_Shellcode	18	Microsoft: Tr	-	2018-10-22 17:35:52 UTC (3 weeks, 2 days ago)	Text
Base64_PS1_Shellcode	18	Microsoft: Tr	-	2018-10-19 03:08:08 UTC (3 weeks, 6 days ago)	Text
Base64_PS1_Shellcode	18	Microsoft: Tr	-	2018-10-22 19:26:21 UTC (3 weeks, 2 days ago)	Text
Base64_PS1_Shellcode	18	Kaspersky: H	myvtfile.exe	2018-08-13 07:42:51 UTC (3 months ago)	Text
Base64_PS1_Shellcode	18	Microsoft: Tr	-	2018-10-19 15:17:36 UTC (3 weeks, 5 days ago)	Text
Base64_PS1_Shellcode	14	Kaspersky: H	122dea9d0c7d8f63132b339501eca83!	2018-09-26 01:04:31 UTC (1 month, 2 weeks ago	Email
Base64_PS1_Shellcode	14	Microsoft: Tr	=?UTF-8?B?0i3QatCy0YvQuSD0KgtC10	2018-11-13 00:58:42 UTC (2 days, 6 hours ago)	Text
Base64_PS1_Shellcode	14	Microsoft: Tr	-	2018-11-08 01:57:02 UTC (1 week ago)	Text
Base64_PS1_Shellcode	14	Microsoft: Tr	qsd.doc	2018-06-09 02:12:38 UTC (5 months, 1 week ago	MS Word Do
Base64_PS1_Shellcode	13	Microsoft: Tr	ps111.txt	2018-11-09 21:27:01 UTC (5 days, 10 hours ago)	Text
Base64_PS1_Shellcode	13	Microsoft: Tr	POWERSHELL.PS1.infected	2018-10-31 14:39:08 UTC (2 weeks ago)	Text
Base64_PS1_Shellcode	13	Microsoft: Tr	anothertext.ps1	2018-10-15 17:25:53 UTC (1 month ago)	Text
Base64_PS1_Shellcode	11	F-Secure: Ge	3adb9f594bdad89632d8a5d0e37f24c	2018-09-25 01:04:27 UTC (1 month, 3 weeks ago	Email
Base64_PS1_Shellcode	10	F-Secure: Tr	1.exe	2018-10-30 04:52:58 UTC (2 weeks, 2 days ago)	Text
Base64_PS1_Shellcode	10	F-Secure: Tr	=?UTF-8?B?0i3QatCy0YvQuSD0KgtC10	2018-11-01 11:46:12 UTC (1 week, 6 days ago)	Text
Base64_PS1_Shellcode	10	F-Secure: Ge	a1c19da17415e772a40f4e92c57197	2018-09-25 01:05:31 UTC (1 month, 3 weeks ago	Email
Base64_PS1_Shellcode	9	F-Secure: Tr	msbuildQueueAPC.csproj	2018-11-08 15:00:31 UTC (6 days, 4 hours ago)	C++
Base64_PS1_Shellcode	8	Microsoft: Pl	webserver-13ecb373ba9270ac6c4fc0	2017-12-13 11:00:46 UTC (11 months ago)	Network cap
Base64_PS1_Shellcode	8	Kaspersky: Tr	a. V 2.0.vbs, myvtfile.exe	2018-10-02 14:42:55 UTC (3 days, 6 hours ago)	Text
Base64_PS1_Shellcode	8	Microsoft: Tr	palsx.ps1	2018-11-08 07:50:31 UTC (1 week ago)	C++
Base64_PS1_Shellcode	6	Microsoft: Tr	-	2018-10-20 16:36:50 UTC (3 weeks, 4 days ago)	C++
Base64_PS1_Shellcode	6	Sophos: Troj	adobe_flash_hacking_team_uaf.html	2015-12-14 16:57:52 UTC (2 years, 11 months ag	HTML
Base64_PS1_Shellcode	6	Kaspersky: H	something.js, myvtfile.exe	2018-08-21 21:42:41 UTC (1 month, 2 weeks ago	Text
Base64_PS1_Shellcode	5	Microsoft: Tr	-	2018-11-04 18:07:48 UTC (1 week, 3 days ago)	Text
Base64_PS1_Shellcode	5	Kaspersky: H	shellcode.xsl	2018-09-14 11:16:05 UTC (2 months ago)	XML
Base64_PS1_Shellcode	4	Microsoft: Tr	shellys.ps1	2018-09-07 18:58:33 UTC (2 months, 1 week ago	C++

	Positives	Virus	File Names	First Submitted
de	4	Kaspersky: H	lol.xls	2018-08-21 12:13:42 UTC (2 months, 3 w
de	4	Kaspersky: H	myvtfile.exe, Program.cs	2018-11-13 11:31:39 UTC (1 day, 7 hours
de	3	Microsoft: P\	test09.bin	2018-10-24 14:33:44 UTC (3 weeks ago)
de	3	Microsoft: Tr	test2_64.txt	2018-10-15 17:04:49 UTC (1 month ago)
de	2	Sophos: Troj,	flash_exploit	2018-09-14 07:24:04 UTC (2 months ago
de	2	Kaspersky: H	smTHSU[1].htm	2018-08-26 08:13:26 UTC (2 months, 2 w
de	2	Kaspersky: H	teste.xml, teste.xsl	2018-10-10 14:02:17 UTC (1 month ago)
de	1	-	prueba.ps1	2018-10-17 20:42:43 UTC (4 weeks ago)
de	1	-	CC.pcap	2018-10-04 19:57:38 UTC (1 month, 1 we
de	1	-	cc2.pcap	2018-10-14 16:43:42 UTC (1 month ago)
de	1	-	evil_adobeuaf.html	2018-11-06 20:11:22 UTC (1 week, 1 day
de	1	-	wifi1.exe	2018-08-11 18:22:09 UTC (3 months ago
de	1	Symantec: IS	abc.js	2018-08-22 11:46:08 UTC (2 months, 3 w
de	1	-	banuj.exe	2018-08-24 18:13:13 UTC (2 months, 3 w
de	1	Symantec: IS	shakespeare.js	2018-08-22 11:47:31 UTC (2 months, 3 w
de	0	-	shakespeare.js	2018-08-22 11:49:05 UTC (2 months, 3 w
de	0	-	-	2018-08-14 15:35:10 UTC (3 months ago
de	0	-	-	2018-08-14 15:01:46 UTC (3 months a

3:14 PM · Nov 15, 2018

58 Reposts **3** Quotes **143** Likes **13** Bookmarks

13

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