
Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing


Q


Sign in


Sign up

 elastic / protections-artifacts 


Public


 Notifications


 Fork 117


 Star 1k


<> Code


 Issues 3

 Pull requests 1

 Actions


 Projects


 Security

 Insights

## Commit

Updating artifacts

 Loading branch information

 protectionsmachine committed on Oct 14, 2022

1 parent 00071f2    commit 7460867

Browse files

 Showing 279 changed files with 3,012 additions and 1,001 deletions.

Whitespace

Ignore whitespace


Split


Unified


Q


Filter changed files


behavior/rules


command\_and\_control\_con... 






command\_and\_control\_con... 


command\_and\_control\_con... 

command\_and\_control\_con... 






command\_and\_control\_exec... 


command\_and\_control\_ingr... 

6     

...ules/command\_and\_control\_connection\_to\_dynamic\_dns\_provider\_by\_a\_signed\_binary\_p... 

↑...	@@ -7,7 +7,7 @@ id = "fb6939a2-1b54-428c-92a2-3a831585af2a"
7	7 license = "Elastic License v2"
8	8 name = "Connection to Dynamic DNS Provider by a Signed Binary Proxy"
9	9 os_list = ["windows"]
10	- version = "1.0.6"
10	+ version = "1.0.7"
11	11
12	12 query = ''
13	13 sequence by process.entity_id with maxspan=5m
↓...↑	@@ -55,12 +55,14 @@ sequence by process.entity_id with maxspan=5m
55	55 ]
56	56 ''
57	57
58	- optional_actions = []
59	58 [[actions]]
60	59 action = "kill_process"
61	60 field = "process.entity_id"
62	61 state = 0
63	62
	63 + [[optional_actions]]
	64 + action = "rollback"
	65 +
64	66 [[threat]]
65	67 framework = "MITRE ATT&CK"
66	68 [[threat.technique]]
↓	

6     

...r/rules/command\_and\_control\_connection\_to\_dynamic\_dns\_provider\_by\_an\_unsigned\_bi... 

↑...	@@ -7,7 +7,7 @@ id = "75b80e66-90d0-4ab6-9e6b-976f7d690906"
7	7 license = "Elastic License v2"
8	8 name = "Connection to Dynamic DNS Provider by an Unsigned Binary"
9	9 os_list = ["windows"]
10	- version = "1.0.7"
10	+ version = "1.0.8"
11	11
12	12 query = ''
13	13 sequence by process.entity_id with maxspan=1m
↓...↑	@@ -48,12 +48,14 @@ sequence by process.entity_id with maxspan=1m
48	48 not dns.question.name : "checkip.dyndns.org"]
49	49 ''
50	50
51	- optional_actions = []

Page 1 of 8

52	51	[[actions]]
53	52	action = "kill_process"
54	53	field = "process.entity_id"
55	54	state = 1
56	55	
	56	+ [[optional_actions]]
	57	+ action = "rollback"
	58	+
57	59	[[threat]]
58	60	framework = "MITRE ATT&CK"
59	61	[[threat.technique]]
behavior/rules/command_and_control_connection_to_webservice_by_a_signed_binary_prox...		
@@ -7,7 +7,7 @@ id = "c567240c-445b-4000-9612-b5531e21e050"		
7	7	license = "Elastic License v2"
8	8	name = "Connection to WebService by a Signed Binary Proxy"
9	9	os_list = ["windows"]
10		- version = "1.0.6"
	10	+ version = "1.0.7"
11	11	
12	12	query = ''
13	13	sequence by process.entity_id with maxspan=5m
@@ -69,7 +69,6 @@ sequence by process.entity_id with maxspan=5m		
69	69	"discord.com",
70	70	"apis.azureedge.net",
71	71	"cdn.sql.gg",
72	-	"api.*",
73	72	"?.top4top.io",
74	73	"top4top.io",
75	74	"www.uploader.net",
@@ -80,17 +79,20 @@ sequence by process.entity_id with maxspan=5m		
80	79	"meacz.gq",
81	80	"rwr.org",
82	81	"*.publicvm.com",
83	-	"*.blogspot.com"
	82	+ "*.blogspot.com",
	83	+ "api.mylnikov.org"
84	84	)
85	85	]
86	86	''
87	87	
88		- optional_actions = []
89	88	[[actions]]
90	89	action = "kill_process"
91	90	field = "process.entity_id"
92	91	state = 1
93	92	
	93	+ [[optional_actions]]
	94	+ action = "rollback"
	95	+
94	96	[[threat]]
95	97	framework = "MITRE ATT&CK"
96	98	[[threat.technique]]
behavior/rules/command_and_control_connection_to_webservice_by_an_unsigned_binary.t...		
@@ -7,15 +7,34 @@ id = "2c3efa34-fecd-4b3b-bdb6-30d547f2a1a4"		
7	7	license = "Elastic License v2"
8	8	name = "Connection to WebService by an Unsigned Binary"
9	9	os_list = ["windows"]
10		- version = "1.0.7"
	10	+ version = "1.0.8"
11	11	
12	12	query = ''
13	13	sequence by process.entity_id with maxspan=1m

14	14	/* execution of an unsigned PE file followed by dns lookup to commonly abused trusted webservices */
15	15	
16	-	[process where event.action == "start" and user.id : "S-1-5-21-*" and
	16	+ [process where event.action == "start" and not user.id : "S-1-5-18" and
17	17	not process.code_signature.trusted == true and
18	-	process.executable : ("?:\\Users\\*", "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*")]
	18	+ (process.Ext.relative_file_creation_time <= 300 or
		process.Ext.relative_file_name_modify_time <= 300) and
19	+	process.executable : ("?:\\Users\\*", "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*") and
20	+	not process.args : ("--type=utility", "--squirrel-firststrun", "--utility-sub-type=*") and
21	+	process.executable : ("?:\\Users\\*", "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*") and
22	+	not (process.name : "Clash for Windows.exe" and process.args : "--utility-sub-type=network.mojom.NetworkService") and
23	+	not (process.name : "clash-win64.exe" and process.parent.args : "--app-user-model-id=com.*.clashwin") and
24	+	not process.hash.sha256 :
25	+	
		("1cef2a7e7fe2a60e7f1d603162e60969469488cae99d04d13c4450cb90934b0f",
26	+	"ec4d11bd8216b894cb02f4e9cc3974a87901e928b4cdd2cac6d6eb22b3fa25eb",
27	+	"5c3725fb6ef2e8044b6ffbaa3f62f1afa1f47dd69ab557b611af8d80362f99d3",
28	+	"cc73c1aecb17ad6ce7c74bd258704994e43dea732212326a5b205be65b3b4b61",
29	+	"e5f6f15243393cb03022a3f1d22e0175acbf54cc5386cf9820185cf43cc90342",
30	+	"83d17dc95a7eba329fb29899b43d4b89b1dc898774e31ba58de883ce4e44e833",
31	+	"f2e7ef9667f84a2b2f66e9116b06b6fbc3fd5af6695a50366e862692459b7a59",
32	+	"21b49f2824f1357684983cfacfc0d58a95a2b41cd7bbaff544d9de8e790be1b6",
33	+	"d71babf67e0e26991a34ea7d9cb78dc44dc0357bc20e4c15c61ba49cae99fcaa",
34	+	"074b780a2a22d3d8af78afdfa042083488447fd5e63e7fa6e9c6abb08227e81d",
35	+	"578b95a62ecf3e1a3ea77d8329e87ba72a1b3516d0e5adb8d3f3d1eb44a7941e",
36	+	"a9b47f62e98f2561cf382d3d59e1d1b502b4cae96ab3e420122c3b28cc5b7da6",
37	+	"14a4ae91ebf302026a8ba24f4548a82c683cfb5fa4494c76e39d6d3089cdbbc1")]
19	38	[dns where
20	39	dns.question.name :
21	40	(
<div>⬇ ↑</div>		@@ -69,12 +88,14 @@ sequence by process.entity_id with maxspan=1m
69	88	]
70	89	'''
71	90	
72	-	optional_actions = []
73	91	[[actions]]
74	92	action = "kill_process"
75	93	field = "process.entity_id"
76	94	state = 1
77	95	
	96	+ [[optional_actions]]
	97	+ action = "rollback"
	98	+
78	99	[[threat]]
79	100	framework = "MITRE ATT&CK"
80	101	[[threat.technique]]
<div>↕</div>		@@ -99,4 +120,4 @@ name = "Command and Control"
99	120	reference = "https://attack.mitre.org/tactics/TA0011/"
100	121	
101	122	[internal]
102	-	min_endpoint_version = "7.15.0"
	123	+ min_endpoint_version = "8.4.0"

▼ 6

behavior/rules/command\_and\_control\_execution\_of\_a\_file\_written\_by\_a\_signed\_binary\_p...

...		@@ -8,7 +8,7 @@ id = "ccbc4a79-3bae-4623-aaef-e28a96bf538b"
8	8	license = "Elastic License v2"
9	9	name = "Execution of a File Written by a Signed Binary Proxy"
10	10	os_list = ["windows"]
11		- version = "1.0.6"
	11	+ version = "1.0.7"
12	12	
13	13	query = ''
14	14	sequence with maxspan=5m
...		@@ -21,12 +21,14 @@ sequence with maxspan=5m
21	21	] by process.executable
22	22	''
23	23	
24		- optional_actions = []
25	24	[[actions]]
26	25	action = "kill_process"
27	26	field = "process.entity_id"
28	27	state = 1
29	28	
	29	+ [[optional_actions]]
	30	+ action = "rollback"
	31	+
30	32	[[threat]]
31	33	framework = "MITRE ATT&CK"
32	34	[[threat.technique]]
....		

▼ 58

behavior/rules/command\_and\_control\_ingress\_tool\_transfer\_via\_curl.toml

...	...	@@ -0,0 +1,58 @@
	1	+ [rule]
	2	+ description = ""
	3	+ Identifies downloads of remote content using Windows CURL executable. This tactic may be indicative of malicious
	4	+ activity where malware is downloading second stage payloads using built-in Windows programs.
	5	+ ""
	6	+ id = "336ada1c-69f8-46e8-bdd2-790c85429696"
	7	+ license = "Elastic License v2"
	8	+ name = "Ingress Tool Transfer via CURL"
	9	+ os_list = ["windows"]
	10	+ version = "1.0.3"
	11	+
	12	+ query = ''
	13	+ process where event.action == "start" and
	14	+
	15	+ /* renamed curl or curl running from normal users writable fodlers are very noisy */
	16	+ process.executable : ("?:\\Windows\\System32\\curl.exe", "?:\\Windows\\SysWOW64\\curl.exe") and
	17	+
	18	+ process.args : ("-o", "--output") and
	19	+ (
	20	+ (process.parent.name : ("powershell.exe", "mshta.exe", "wscript.exe", "cscript.exe", "rundll32.exe", "regsvr32.exe") and
	21	+ process.parent.args_count >= 2) or
	22	+
	23	+ (process.parent.name : "cmd.exe" and process.parent.command_line : "*curl*") or
	24	+
	25	+ descendant of [process where process.name : ("winword.exe", "excel.exe", "powerpnt.exe")] or
	26	+
	27	+ process.parent.executable : ("?:\\Users\\Public\\*", "?:\\Users\\*\\AppData\\*", "?:\\ProgramData\\*")
	28	+ ) and
	29	+

```
...es/command_and_control_payload_downloaded_by_process_running_in_suspicious_direc...  
@@ -8,7 +8,7 @@ license = "Elastic License v2"  
8      8      name = "Payload Downloaded by Process Running in Suspicious Directory"  
9      9      os_list = ["macos"]  
10     10     reference = ["https://attack.mitre.org/software/S0482/", "https://objective-  
see.com/blog/blog_0x69.html"]  
11     - version = "1.0.6"
```

11

+ version = "1.0.7"

12

12

13

13

query = ''

14

14

sequence by process.entity\_id with maxspan=5s

⬆️

@@ -22,7 +22,7 @@ sequence by process.entity\_id with maxspan=5s

22

22

)

23

23

] and

24

24

process.name == "curl" and

25

-

not process.args : "https://omahaproxy.appspot.com/history"

25

+

not process.args : ("https://omahaproxy.appspot.com/history",

"https://console.jumpcloud.com/api/systems/\*", "https://zoom.us/client/\*")

26

26

]

27

27

[network where event.action == "connection\_attempted"]

28

28

'''

⬇️

▼ ⬆️ 2

behavior/rules/command\_and\_control\_potential\_plugx\_registry\_modification.toml

⌂

...

⬆️

@@ -13,7 +13,7 @@ reference = [

13

13

"https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-

new-korplug-variant/",

14

14

"https://malpedia.caad.fkie.fraunhofer.de/details/win.plugx",

15

15

]

16

-

version = "1.0.4"

16

+

version = "1.0.5"

17

17

18

18

query = ''

19

19

registry where

⬇️

▼ 40

behavior/rules/command\_and\_control\_potential\_wizardupdate\_malware\_infection.toml

⌂

...

...

...

@@ -0,0 +1,40 @@

1

+

[rule]

2

+

description = ""

3

+

Identifies the execution traces of the WizardUpdate malware. WizardUpdate is a

macOS trojan that attempts to infiltrate

4

+

macOS machines to steal data and it is associated with other types of

malicious payloads, increasing the chances of

5

+

multiple infections on a device.

6

+

""

7

+

id = "eb78fa0f-5e8a-4c15-a099-e904c4a226e6"

8

+

license = "Elastic License v2"

9

+

name = "Potential WizardUpdate Malware Infection"

10

+

os\_list = ["macos"]

11

+

reference = [

12

+

"https://malpedia.caad.fkie.fraunhofer.de/details/osx.xcsset",

13

+

"https://www.microsoft.com/security/blog/2022/02/02/the-evolution-of-a-

mac-trojan-updateagents-progression/",

14

+

]

15

+

version = "1.0.2"

16

+

17

+

query = ''

18

+

process where event.action == "exec" and

19

+

(

20

+

(process.name : "sh" and process.command\_line : "=\$(curl \*eval\*\$\*)" or

21

+

(process.name : "curl" and process.command\_line :

"\*\_intermediate\_agent\_\*machine\_id\*")

22

+

)

23

+

'''

24

+

25

+

optional\_actions = []

26

+

[[actions]]

27

+

action = "kill\_process"

28

+

field = "process.entity\_id"

29

+

state = 0

30

+

31

+

[[threat]]

32

+

framework = "MITRE ATT&CK"

33

+

```
34 + [threat.tactic]
35 + id = "TA0011"
36 + name = "Command and Control"
37 + reference = "https://attack.mitre.org/tactics/TA0011/"
38 +
39 + [internal]
40 + min_endpoint_version = "7.15.0"
```

▼ 43 ■■■■■■

behavior/rules/command\_and\_control\_potential\_xcsset\_malware\_infection.toml

...	...	@@ -0,0 +1,43 @@
1	+	[rule]
2	+	description = ""
3	+	Identifies the execution traces of the XCSSET malware. XCSSET is a macOS trojan that primarily spreads via Xcode
4	+	projects and maliciously modifies applications. Infected users are also
5	+	vulnerable to having their credentials,
6	+	accounts, and other vital data stolen.
7	+	""
8	+	id = "875b71bb-ef09-46b2-9c12-a95112461e85"
9	+	license = "Elastic License v2"
10	+	name = "Potential XCSSET Malware Infection"
11	+	os_list = ["macos"]
12	+	reference = ["https://malpedia.caad.fkie.fraunhofer.de/details/osx.xcsset"]
13	+	version = "1.0.2"
14	+	
15	+	query = ''
16	+	process where event.action == "exec" and
17	+	(
18	+	(process.name : "curl" and process.parent.name : "bash" and
19	+	process.args : ("https://*/sys/log.php", "https://*/sys/prepod.php",
20	+	"https://*/sys/bin/Pods")) or
21	+	
22	+	(process.name : "osacompile" and process.args : "/Users/*/Library/Group
23	+	Containers/*" and process.parent.name : "bash") or
24	+	
25	+	(process.name : "plutil" and process.args : "LSUIElement" and process.args :
26	+	"/Users/*/Library/Group Containers/*" and process.parent.name : "bash") or
27	+	
28	+	(process.name : "zip" and process.args : "-r" and process.args :
29	+	"/Users/*/Library/Group Containers/*")
30	+	)
31	+	''
32	+	
33	+	optional_actions = []
34	+	[[actions]]
35	+	action = "kill_process"
36	+	field = "process.entity_id"
37	+	state = 0
38	+	
39	+	[[threat]]
40	+	framework = "MITRE ATT&CK"
41	+	
42	+	[threat.tactic]
43	+	id = "TA0011"
	+	name = "Command and Control"
	+	reference = "https://attack.mitre.org/tactics/TA0011/"
	+	
	+	[internal]
	+	min_endpoint_version = "7.15.0"

▼ ↕ 6 ■■■■□

behavior/rules/command\_and\_control\_remcos\_rat\_registry\_or\_file\_modification.toml

↑...	@@ -8,7 +8,7 @@	license = "Elastic License v2"
8	8	name = "Remcos RAT Registry or File Modification"
9	9	os_list = ["windows"]
10	10	reference = ["https://attack.mitre.org/software/S0332/",
		"https://any.run/malware-trends/remcos"]
11	-	version = "1.0.6"
	+	version = "1.0.7"
12	12	

13	13	query = ''
14	14	any where event.category : ("registry", "file") and
		@@ -21,12 +21,14 @@ any where event.category : ("registry", "file") and
21	21	)
22	22	'''
23	23	
24		- optional_actions = []
25	24	[[actions]]
26	25	action = "kill_process"
27	26	field = "process.entity_id"
28	27	state = 0
29	28	
	29	+ [[optional_actions]]
	30	+ action = "rollback"
	31	+
30	32	[[threat]]
31	33	framework = "MITRE ATT&CK"
32	34	[[threat.technique]]



0 comments on commit 7460867

Please [sign in](#) to comment.