

Sign in

elastic / protections-artifacts

Public

Notifications

Fork

117

Star

1k

<> Code

Issues 3

Pull requests 1

Actions

Projects

Security

Insights

Commit

Updating artifacts

Browse files

Loading branch information.

protectionsmachine

 committed on Oct 14, 2022

1 parent 00071f2 commit 7460867

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

Whitesp...

Ignore whitespa...

Sp...

Unifi...

Filter changed files

behavior/rules

command_and_contr...

command_and_contr...

command_and_contr...

command_and_contr...

command_and_contr...

command_and_contr...

6

...

...ules/command_and_control_connection_to_dynamic_dns_pro...

@@ -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
64      63      + [[optional_actions]]
65      64      + action = "rollback"
66      65      +
67      66      [[threat]]
68      67      framework = "MITRE ATT&CK"
69      68      [[threat.technique]]

```



6

...r/rules/command_and_control_connection_to_dynamic_dns_...



```
@@ -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 = []
```

```
52     51     [[actions]]
53     52     action = "kill_process"
54     53     field = "process.entity_id"
55     54     state = 1
```



```
56 + [[optional_actions]]
57 + action = "rollback"
58 +
```



```
57     59     [[threat]]
58     60     framework = "MITRE ATT&CK"
59     61     [[threat.technique]]
```





95	+	
94	96	[[threat]]
95	97	framework = "MITRE ATT&CK"
96	98	[[threat.technique]]
↓		
✓ 31		
behavior/rules/command_and_control_connection_to_webservi... 		
↑	@@ -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	+	
		("1cef2a7e7fe2a60e7f1d603162e60969469488cae99d04d13
		c4450cb90934b0f",
26	+	
		"ec4d11bd8216b894cb02f4e9cc3974a87901e928b4cdd2cac6
		d6eb22b3fa25eb",
27	+	
		"5c3725fb6ef2e8044b6ffbaa3f62f1afa1f47dd69ab557b611
		af8d80362f99d3",
28	+	
		"cc73c1aecb17ad6ce7c74bd258704994e43dea732212326a5b
		205be65b3b4b61",
29	+	
		"e5f6f15243393cb03022a3f1d22e0175acbf54cc5386cf9820
		185cf43cc90342",
30	+	
		"83d17dc95a7eba329fb29899b43d4b89b1dc898774e31ba58d
		e883ce4e44e833",
31	+	
		"f2e7ef9667f84a2b2f66e9116b06b6fbc3fd5af6695a50366e
		862692459b7a59",
32	+	
		"21b49f2824f1357684983cfacfc0d58a95a2b41cd7bbaff544
		d9de8e790be1b6",
33	+	
		"d71babf67e0e26991a34ea7d9cb78dc44dc0357bc20e4c15c6
		1ba49cae99fcaa",
34	+	
		"074b780a2a22d3d8af78afdafa042083488447fd5e63e7fa6e9
		c6abb08227e81d",
35	+	
		"578b95a62ecf3e1a3ea77d8329e87ba72a1b3516d0e5adb8d3
		f3d1eb44a7941e",
36	+	
		"a9b47f62e98f2561cf382d3d59e1d1b502b4cae96ab3e42012
		2c3b28cc5b7da6",
37	+	
		"14a4ae91ebf302026a8ba24f4548a82c683cfb5fa4494c76e3
		9d6d3089cdbbc1")]
19	38	[dns where
20	39	dns.question.name :
21	40	(


	@@ -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]]
	@@ -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_wr... 



@@ -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 = []

Page 6 of 14

```
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_...

... @@ -0,0 +1,58 @@

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

```
21 +     process.parent.args_count >= 2) or
22 +
23 +     (process.parent.name : "cmd.exe" and
24 +      process.parent.command_line : "*curl*") or
25 +
26 +     descendant of [process where process.name :
27 +      ("winword.exe", "excel.exe", "powerpnt.exe")] or
28 +
29 +     process.parent.executable :
30 +      ("?:\\Users\\Public\\*",
31 +       "?:\\Users\\*\\AppData\\*", "?:\\ProgramData\\*")
32 +   ) and
33 +
34 +   /* lot of legit curl execution via custom bat
35 +    scripts or interactively via cmd or powershell */
36 +   not (process.parent.name : "cmd.exe" and
37 +        process.parent.args : "*.bat*") and
38 +   not (process.parent.name : ("cmd.exe",
39 +        "powershell.exe") and process.parent.args_count ==
40 +        1) and
41 +
42 +   /* avoid breaking privileged install */
43 +   not user.id : "S-1-5-18"
44 +   ''
45 +
46 +   optional_actions = []
47 +   [[actions]]
48 +   action = "kill_process"
49 +   field = "process.entity_id"
50 +   state = 0
51 +
52 +   [[threat]]
53 +   framework = "MITRE ATT&CK"
54 +   [[threat.technique]]
55 +   id = "T1105"
56 +   name = "Ingress Tool Transfer"
57 +   reference =
58 +     "https://attack.mitre.org/techniques/T1105/"
59 +
60 +
61 +
62 +   [[threat.tactic]]
63 +   id = "TA0011"
64 +   name = "Command and Control"
65 +   reference =
66 +     "https://attack.mitre.org/tactics/TA0011/"
```


56	+	
57	+	[internal]
58	+	min_endpoint_version = "7.15.0"
▼ ↕ 6 ■■■■		
behavior/rules/command_and_control_netwire_rat_registry_m...		
↑	@@ -8,7 +8,7 @@	license = "Elastic License v2"
8	8	name = "NetWire RAT Registry Modification"
9	9	os_list = ["windows"]
10	10	reference = ["https://attack.mitre.org/software/S0198/", "https://any.run/malware-trends/netwire"]
11	-	version = "1.0.6"
11	+	version = "1.0.7"
12	12	
13	13	query = ''
14	14	registry where
↕	@@ -17,12 +17,14 @@	registry where
17	17	"HKEY_USERS\\S-1-5-21- *\\SOFTWARE\\NetWire\\Install Date")
18	18	''
19	19	
20	-	optional_actions = []
21	20	[[actions]]
22	21	action = "kill_process"
23	22	field = "process.entity_id"
24	23	state = 0
25	24	
25	+	[[optional_actions]]
26	+	action = "rollback"
27	+	
26	28	[[threat]]
27	29	framework = "MITRE ATT&CK"
28	30	[[threat.technique]]
↓		

▼

↕

4

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

<

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_regist... 📄		
		@@ -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/w in.plugx", 15 15] 16 16 - version = "1.0.4" 16 16 + version = "1.0.5" 17 17 18 18 query = '' 19 19 registry where

▼ 40 ■■■■■

behavior/rules/command_and_control_potential_wizardupdate... 


...

... @@ -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 +
13   "https://malpedia.caad.fkie.fraunhofer.de/details/osx.xcsset",
14 +
15   "https://www.microsoft.com/security/blog/2022/02/02/
    the-evolution-of-a-mac-trojan-updateagents-
    progression/",
16 + ]
17 + version = "1.0.2"
18 +
19 + query = ''
20 + process where event.action == "exec" and
21 + (
22 +   (process.name : "sh" and process.command_line :
23     "=$(curl *eval*$(*)" or
24 +   (process.name : "curl" and process.command_line
25     : " *_intermediate_agent_*machine_id*")
26 + )
27 + ''
28 +
29 + optional_actions = []
30 + [[actions]]
31 + action = "kill_process"
32 + field = "process.entity_id"
33 + state = 0
```

```
30 +
31 + [[threat]]
32 + framework = "MITRE ATT&CK"
33 +
34 + [threat.tactic]
35 + id = "TA0011"
36 + name = "Command and Control"
37 + reference =
38 +     "https://attack.mitre.org/tactics/TA0011/"
39 +
40 + [internal]
40 + min_endpoint_version = "7.15.0"
```

▼ 43 ■■■■■■

behavior/rules/command_and_control_potential_xcsset_malwa... 

... @@ -0,0 +1,43 @@

```
1 + [rule]
2 + description = ""
3 + Identifies the execution traces of the XCSSET
4 + malware. XCSSET is a macOS trojan that primarily
5 + spreads via Xcode
6 + projects and maliciously modifies applications.
7 + Infected users are also vulnerable to having their
8 + credentials,
9 + accounts, and other vital data stolen.
10 + ""
11 + id = "875b71bb-ef09-46b2-9c12-a95112461e85"
12 + license = "Elastic License v2"
13 + name = "Potential XCSSET Malware Infection"
14 + os_list = ["macos"]
15 + reference =
16 +     ["https://malpedia.caad.fkie.fraunhofer.de/details/
17 +     osx.xcsset"]
18 + version = "1.0.2"
19 +
20 + query = ''
21 + process where event.action == "exec" and
22 + (
23 +     (process.name : "curl" and process.parent.name :
24 +     "bash" and
25 +     process.args : ("https://*/sys/log.php",
26 +     "https://*/sys/prepod.php",
27 +     "https://*/sys/bin/Pods")) or
28 +
```

```
20 + (process.name : "osacompile" and process.args :  
    + "/Users/*/Library/Group Containers/*" and  
    + process.parent.name : "bash") or  
21 +  
22 + (process.name : "plutil" and process.args :  
    + "LSUIElement" and process.args :  
    + "/Users/*/Library/Group Containers/*" and  
    + process.parent.name : "bash") or  
23 +  
24 + (process.name : "zip" and process.args : "-r" and  
    + process.args : "/Users/*/Library/Group  
    + Containers/*")  
25 + )  
26 + '''  
27 +  
28 + optional_actions = []  
29 + [[actions]]  
30 + action = "kill_process"  
31 + field = "process.entity_id"  
32 + state = 0  
33 +  
34 + [[threat]]  
35 + framework = "MITRE ATT&CK"  
36 +  
37 + [threat.tactic]  
38 + id = "TA0011"  
39 + name = "Command and Control"  
40 + reference =  
    + "https://attack.mitre.org/tactics/TA0011/"  
41 +  
42 + [internal]  
43 + min_endpoint_version = "7.15.0"
```

6

behavior/rules/command_and_control_remcos_rat_registry_or...

...	@@ -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"
	11	+ 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
)
		'''
24		- optional_actions = []
25	24	[[actions]]
26	25	action = "kill_process"
27	26	field = "process.entity_id"
28	27	state = 0
29	28	
		+ [[optional_actions]]
		+ action = "rollback"
		+
30	32	[[threat]]
31	33	framework = "MITRE ATT&CK"
32	34	[[threat.technique]]



0 comments on commit 7460867

Please [sign in](#) to comment.