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...

```diff
@@ -7,7 +7,7 @@ id = "fb6939a2-1b54-428c-92a2-3a831585af2a"
 license = "Elastic License v2"
 name = "Connection to Dynamic DNS Provider by a Signed Binary Proxy"
 os_list = ["windows"]
-version = "1.0.6"
+version = "1.0.7"

 query = '''
 sequence by process.entity_id with maxspan=5m
@@ -55,12 +55,14 @@ sequence by process.entity_id with maxspan=5m
   ]
 '''

-optional_actions = []
 [[actions]]
 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_…

```
@@ -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  55
    56  + [[optional_actions]]
    57  + action = "rollback"
    58  +
57  59   [[threat]]
58  60   framework = "MITRE ATT&CK"
59  61   [[threat.technique]]
```

10

behavior/rules/command_and_control_connection_to_webservi…

```diff
@@ -7,7 +7,7 @@ id = "c567240c-445b-4000-9612-b5531e21e050"
 license = "Elastic License v2"
 name = "Connection to WebService by a Signed Binary Proxy"
 os_list = ["windows"]
-version = "1.0.6"
+version = "1.0.7"

 query = '''
 sequence by process.entity_id with maxspan=5m
@@ -69,7 +69,6 @@ sequence by process.entity_id with maxspan=5m
         "discord.com",
         "apis.azureedge.net",
         "cdn.sql.gg",
-        "api.*",
         "?.top4top.io",
         "top4top.io",
         "www.uplooder.net",
@@ -80,17 +79,20 @@ sequence by process.entity_id with maxspan=5m
         "meacz.gq",
         "rwrd.org",
         "*.publicvm.com",
-        "*.blogspot.com"
+        "*.blogspot.com",
+        "api.mylnikov.org"
     )
   ]
 '''

-optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 1

+[[optional_actions]]
+action = "rollback"
```

```
+
  [[threat]]
  framework = "MITRE ATT&CK"
  [[threat.technique]]
```

31

behavior/rules/command_and_control_connection_to_webservi…

```diff
@@ -7,15 +7,34 @@ id = "2c3efa34-fecd-4b3b-bdb6-30d547f2a1a4"
 license = "Elastic License v2"
 name = "Connection to WebService by an Unsigned Binary"
 os_list = ["windows"]
- version = "1.0.7"
+ version = "1.0.8"

 query = '''
 sequence by process.entity_id with maxspan=1m
  /* execution of an unsigned PE file followed by dns lookup to commonly abused trusted webservices */

-   [process where event.action == "start" and user.id : "S-1-5-21-*" and
+   [process where event.action == "start" and not user.id : "S-1-5-18" and
     not process.code_signature.trusted == true and
-    process.executable : ("?:\\Users\\*", "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*")]
+    (process.Ext.relative_file_creation_time <= 300 or process.Ext.relative_file_name_modify_time <= 300) and
+    process.executable : ("?:\\Users\\*", "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*") and
+    not process.args : ("--type=utility", "--squirrel-firstrun", "--utility-sub-type=*") and
+    process.executable : ("?:\\Users\\*", "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*") and
+    not (process.name : "Clash for Windows.exe" and process.args : "--utility-sub-type=network.mojom.NetworkService") and
+    not (process.name : "clash-win64.exe" and process.parent.args : "--app-user-model-
```

```
id=com.*.clashwin") and
+   not process.hash.sha256 :
+ ("1cef2a7e7fe2a60e7f1d603162e60969469488cae99d04d13c4450cb90934b0f",
+ "ec4d11bd8216b894cb02f4e9cc3974a87901e928b4cdd2cac6d6eb22b3fa25eb",
+ "5c3725fb6ef2e8044b6ffbaa3f62f1afa1f47dd69ab557b611af8d80362f99d3",
+ "cc73c1aecb17ad6ce7c74bd258704994e43dea732212326a5b205be65b3b4b61",
+ "e5f6f15243393cb03022a3f1d22e0175acbf54cc5386cf9820185cf43cc90342",
+ "83d17dc95a7eba329fb29899b43d4b89b1dc898774e31ba58de883ce4e44e833",
+ "f2e7ef9667f84a2b2f66e9116b06b6fbc3fd5af6695a50366e862692459b7a59",
+ "21b49f2824f1357684983cfacfc0d58a95a2b41cd7bbaff544d9de8e790be1b6",
+ "d71babf67e0e26991a34ea7d9cb78dc44dc0357bc20e4c15c61ba49cae99fcaa",
+ "074b780a2a22d3d8af78afdfa042083488447fd5e63e7fa6e9c6abb08227e81d",
+ "578b95a62ecf3e1a3ea77d8329e87ba72a1b3516d0e5adb8d3f3d1eb44a7941e",
+ "a9b47f62e98f2561cf382d3d59e1d1b502b4cae96ab3e420122c3b28cc5b7da6",
+ "14a4ae91ebf302026a8ba24f4548a82c683cfb5fa4494c76e39d6d3089cdbbc1")]
  [dns where
    dns.question.name :
    (
```

```diff
@@ -69,12 +88,14 @@ sequence by process.entity_id with maxspan=1m
  ]
 '''

- optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 1

+ [[optional_actions]]
+ action = "rollback"
+
 [[threat]]
 framework = "MITRE ATT&CK"
 [[threat.technique]]
@@ -99,4 +120,4 @@ name = "Command and Control"
 reference = "https://attack.mitre.org/tactics/TA0011/"

 [internal]
- min_endpoint_version = "7.15.0"
+ min_endpoint_version = "8.4.0"
```

6

behavior/rules/command_and_control_execution_of_a_file_wr…

```diff
@@ -8,7 +8,7 @@ id = "ccbc4a79-3bae-4623-aaef-e28a96bf538b"
 license = "Elastic License v2"
 name = "Execution of a File Written by a Signed Binary Proxy"
 os_list = ["windows"]
- version = "1.0.6"
+ version = "1.0.7"

 query = '''
 sequence with maxspan=5m
@@ -21,12 +21,14 @@ sequence with maxspan=5m
   ] by process.executable
 '''

- optional_actions = []
```

```
  [[actions]]
  action = "kill_process"
  field = "process.entity_id"
  state = 1

+ [[optional_actions]]
+ action = "rollback"
+
  [[threat]]
  framework = "MITRE ATT&CK"
  [[threat.technique]]
```

58

behavior/rules/command_and_control_ingress_tool_transfer_…

```
@@ -0,0 +1,58 @@
+ [rule]
+ description = """
+ Identifies downloads of remote content using Windows CURL executable. This tactic may be indicative of malicious
+ activity where malware is downloading second stage payloads using built-in Windows programs.
+ """
+ id = "336ada1c-69f8-46e8-bdd2-790c85429696"
+ license = "Elastic License v2"
+ name = "Ingress Tool Transfer via CURL"
+ os_list = ["windows"]
+ version = "1.0.3"
+
+ query = '''
+ process where event.action == "start" and
+
+  /* renamed curl or curl running from normal users writable fodlers are very noisy */
+  process.executable : ("?:\\Windows\\System32\\curl.exe", "?:\\Windows\\SysWOW64\\curl.exe") and
+
+  process.args : ("-o", "--output") and
+    (
+     (process.parent.name : ("powershell.exe", "mshta.exe", "wscript.exe", "cscript.exe", "rundll32.exe", "regsvr32.exe") and
```

```
+      process.parent.args_count >= 2) or
+
+      (process.parent.name : "cmd.exe" and process.parent.command_line : "*curl*") or
+
+      descendant of [process where process.name : ("winword.exe", "excel.exe", "powerpnt.exe")] or
+
+      process.parent.executable : ("?:\\Users\\Public\\*", "?:\\Users\\*\\AppData\\*", "?:\\ProgramData\\*")
+    ) and
+
+   /* lot of legit curl execution via custom bat scripts or interactively via cmd or powershell */
+   not (process.parent.name : "cmd.exe" and process.parent.args : "*.bat*") and
+   not (process.parent.name : ("cmd.exe", "powershell.exe") and process.parent.args_count == 1) and
+
+   /* avoid breaking privileged install */
+   not user.id : "S-1-5-18"
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1105"
+ name = "Ingress Tool Transfer"
+ reference = "https://attack.mitre.org/techniques/T1105/"
+
+
+ [threat.tactic]
+ 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_netwire_rat_registry_m…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
 name = "NetWire RAT Registry Modification"
 os_list = ["windows"]
 reference = ["https://attack.mitre.org/software/S0198/", "https://any.run/malware-trends/netwire"]
- version = "1.0.6"
+ version = "1.0.7"

 query = '''
 registry where
@@ -17,12 +17,14 @@ registry where
       "HKEY_USERS\\S-1-5-21-*\\SOFTWARE\\NetWire\\Install Date")
 '''

- optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 0

+ [[optional_actions]]
+ action = "rollback"
+
 [[threat]]
 framework = "MITRE ATT&CK"
 [[threat.technique]]
```

4

...es/command_and_control_payload_downloaded_by_process_r…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
 name = "Payload Downloaded by Process Running in Suspicious Directory"
```

```
os_list = ["macos"]
reference = ["https://attack.mitre.org/software/S0482/", "https://objective-see.com/blog/blog_0x69.html"]
- version = "1.0.6"
+ version = "1.0.7"

query = '''
sequence by process.entity_id with maxspan=5s
@@ -22,7 +22,7 @@ sequence by process.entity_id with maxspan=5s
        )
    ] and
    process.name == "curl" and
-    not process.args : "https://omahaproxy.appspot.com/history"
+    not process.args : ("https://omahaproxy.appspot.com/history", "https://console.jumpcloud.com/api/systems/*", "https://zoom.us/client/*")
  ]
  [network where event.action == "connection_attempted"]
'''
```

2

behavior/rules/command_and_control_potential_plugx_regist…

```
@@ -13,7 +13,7 @@ reference = [
"https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/",
"https://malpedia.caad.fkie.fraunhofer.de/details/win.plugx",
]
- version = "1.0.4"
+ version = "1.0.5"

query = '''
registry where
```

40

behavior/rules/command_and_control_potential_wizardupdate…

```
@@ -0,0 +1,40 @@
+ [rule]
+ description = """
+ Identifies the execution traces of the WizardUpdate malware. WizardUpdate is a macOS trojan that attempts to infiltrate
+ macOS machines to steal data and it is associated with other types of malicious payloads, increasing the chances of
+ multiple infections on a device.
+ """
+ id = "eb78fa0f-5e8a-4c15-a099-e904c4a226e6"
+ license = "Elastic License v2"
+ name = "Potential WizardUpdate Malware Infection"
+ os_list = ["macos"]
+ reference = [
+ "https://malpedia.caad.fkie.fraunhofer.de/details/osx.xcsset",
+ "https://www.microsoft.com/security/blog/2022/02/02/the-evolution-of-a-mac-trojan-updateagents-progression/",
+ ]
+ version = "1.0.2"
+
+ query = '''
+ process where event.action == "exec" and
+  (
+    (process.name : "sh" and process.command_line : "*=$(curl *eval*$*") or
+    (process.name : "curl" and process.command_line : "*_intermediate_agent_*machine_id*")
+  )
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
```

```
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+
+ [threat.tactic]
+ id = "TA0011"
+ name = "Command and Control"
+ reference = "https://attack.mitre.org/tactics/TA0011/"
+
+ [internal]
+ min_endpoint_version = "7.15.0"
```

43

behavior/rules/command_and_control_potential_xcsset_malwa…

```
@@ -0,0 +1,43 @@
+ [rule]
+ description = """
+ Identifies the execution traces of the XCSSET malware. XCSSET is a macOS trojan that primarily spreads via Xcode
+ projects and maliciously modifies applications. Infected users are also vulnerable to having their credentials,
+ accounts, and other vital data stolen.
+ """
+ id = "875b71bb-ef09-46b2-9c12-a95112461e85"
+ license = "Elastic License v2"
+ name = "Potential XCSSET Malware Infection"
+ os_list = ["macos"]
+ reference = ["https://malpedia.caad.fkie.fraunhofer.de/details/osx.xcsset"]
+ version = "1.0.2"
+
+ query = '''
+ process where event.action == "exec" and
+  (
+   (process.name : "curl" and process.parent.name : "bash" and
+    process.args : ("https://*/sys/log.php", "https://*/sys/prepod.php", "https://*/sys/bin/Pods")) or
+
```

```
+   (process.name : "osacompile" and process.args : "/Users/*/Library/Group Containers/*" and process.parent.name : "bash") or
+
+   (process.name : "plutil" and process.args : "LSUIElement" and process.args : "/Users/*/Library/Group Containers/*" and process.parent.name : "bash") or
+
+   (process.name : "zip" and process.args : "-r" and process.args : "/Users/*/Library/Group Containers/*")
+  )
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+
+ [threat.tactic]
+ 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…

```
@@ -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
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.

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

© 2024 GitHub, Inc.