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

main

protectionsmachine committed on Oct 14, 2022

1 parent 00071f2 commit 7460867

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"
```

```diff
  field = "process.entity_id"
  state = 0

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

6

...r/rules/command_and_control_connection_to_dynamic_dns_…

```diff
@@ -7,7 +7,7 @@ id = "75b80e66-90d0-4ab6-9e6b-976f7d690906"
  license = "Elastic License v2"
  name = "Connection to Dynamic DNS Provider by an Unsigned Binary"
  os_list = ["windows"]
- version = "1.0.7"
+ version = "1.0.8"

  query = '''
  sequence by process.entity_id with maxspan=1m
@@ -48,12 +48,14 @@ sequence by process.entity_id with maxspan=1m
      not dns.question.name : "checkip.dyndns.org"]
  '''

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

+ [[optional_actions]]
+ action = "rollback"
+
  [[threat]]
  framework = "MITRE ATT&CK"
  [[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…

```
@@ -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 :
      (
        @@ -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 = []
```

```diff
 [[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_…

```diff
@@ -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/"
```

```
      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]]
```

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...

4 🟩🟩🟥⬜

…es/command_and_control_payload_downloaded_by_process_r…

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

- command_and_contr... ⊡
- command_and_contr... ⊡
- command_and_contr... ⊡
- command_and_contr... ⊞
- command_and_contr... ⊡
- command_and_contr... ⊡
- command_and_contr... ⊡
- command_and_contr... ⊞
- command_and_contr... ⊞
- command_and_contr... ⊡
- command_and_contr... ⊡
- command_and_contr... ⊡
- credential_access_acc... ⊡
- credential_access_cre... ⊡
- credential_access_du... ⊡
- credential_access_lsa_... ⊡

```
  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"
  name = "Remcos RAT Registry or File Modification"
  os_list = ["windows"]
  reference = ["https://attack.mitre.org/software/S0332/", "https://any.run/malware-trends/remcos"]
- version = "1.0.6"
+ version = "1.0.7"

```

```
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]]
```

2 🟩🟥⬜⬜⬜

behavior/rules/command_and_control_shlayer_malware_infect…

```
              @@ -14,7 +14,7 @@ reference = [
14    14          "https://redcanary.com/threat-detection-report/threats/shlayer/",
15    15          "https://securelist.com/shlayer-for-macos/95724/",
16    16      ]
17          - version = "1.0.6"
      17    + version = "1.0.7"
18    18
19    19      query = '''
20    20      process where event.action == "exec" and process.name == "curl" and process.args : "-f0L"
```

6 🟩🟩🟩🟥⬜

behavior/rules/command_and_control_suspicious_netsupport_…

```
              @@ -8,7 +8,7 @@ license = "Elastic License v2"
 8     8      name = "Suspicious NetSupport Execution"
```

```diff
  os_list = ["windows"]
  reference = ["https://www.netsupportsoftware.com/"]
- version = "1.0.5"
+ version = "1.0.6"

  query = '''
  sequence by process.entity_id with maxspan=1m
@@ -19,12 +19,14 @@ sequence by process.entity_id with maxspan=1m
   [dns where not dns.question.name : "*.netsupportsoftware.com"]
  '''

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

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

6 🟩🟩🟩🟥⬜

behavior/rules/credential_access_access_to_windows_passwo…

```diff
@@ -10,20 +10,22 @@ os_list = ["windows"]
  reference = [
      "https://docs.microsoft.com/en-us/uwp/api/windows.security.credentials.passwordvault.retrieve?view=winrt-22000",
  ]
- version = "1.0.4"
+ version = "1.0.5"

  query = '''
  process where event.action == "start" and
   process.pe.original_file_name == "PowerShell.EXE" and
```

```
 process.command_line : ("*Credentials.PasswordVault*", "*RetrievePassword*", "*Credentials*RetrieveAll*")
'''

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

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

12 🟩🟩🟩🟥⬜

behavior/rules/credential_access_credential_access_via_kn…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
name = "Credential Access via Known Utilities"
os_list = ["windows"]
reference = ["https://lolbas-project.github.io/"]
- version = "1.0.12"
+ version = "1.0.13"

query = '''
process where event.action == "start" and
@@ -32,7 +32,8 @@ process where event.action == "start" and
  (process.name : "createdump.exe" and process.args : "-u") or
  (process.pe.original_file_name == "FX_VER_INTERNALNAME_STR" and process.args : "-u" and process.args : "-f" and process.args_count >= 3) or
  /* taskmgr via GUI - Create dump file - excluding Explorer to avoid breaking legit use of taskmgr */
-  (process.pe.original_file_name == "Taskmgr.exe" and process.args == "/4" and not
              process.parent.executable : "?:\\Windows\\explorer.exe") or
      35   +    (process.pe.original_file_name == "Taskmgr.exe" and process.args == "/4" and
      36   +     not process.parent.executable : ("?:\\Windows\\explorer.exe", "?:\\Program Files (x86)\\AutoElevate\\AEUACAgent.exe")) or
36    37        /* Avast Home Security signed binary */
37    38        (process.pe.original_file_name == "avDump.exe" and process.args : "-dump_file")
38    39        ) and not
              @@ -46,15 +47,18 @@ process where event.action == "start" and
46    47               process.command_line : "*davclnt.dll,DavSetCookie*http*MiniDump*" and
47    48               process.parent.executable : "?:\\WINDOWS\\system32\\svchost.exe" and process.parent.args : "WebClient") and
48    49        not (process.pe.original_file_name == "reg.exe" and process.args : "?:\\ProgramData\\Bitdefender\\ForensicArtefacts\\System\\Config\\*" and
49         -         process.parent.name : "cmd.exe")
      50   +         process.parent.name : "cmd.exe") and
      51   +    not (process.executable : "C:\\Program Files (x86)\\Dental Intel\\PMSSyncService\\procdump.exe" and process.args : "office.exe")
50    52      '''
51    53
52         -  optional_actions = []
53    54      [[actions]]
54    55      action = "kill_process"
55    56      field = "process.entity_id"
56    57      state = 0
57    58
      59   +  [[optional_actions]]
      60   +  action = "rollback"
      61   +
58    62      [[threat]]
59    63      framework = "MITRE ATT&CK"
60    64      [[threat.technique]]
```

2 🟩🟥⬜⬜⬜

behavior/rules/credential_access_dumping_account_hashes_v…

```
@@ -12,7 +12,7 @@ reference = [
  "https://apple.stackexchange.com/questions/186893/os-x-10-9-where-are-password-hashes-stored",
      "https://www.unix.com/man-page/osx/8/mkpassdb/",
  ]
- version = "1.0.6"
+ version = "1.0.7"

  query = '''
  process where event.type == "start" and
```

6 🟩🟩🟩🟥⬜

behavior/rules/credential_access_lsa_dump_via_silentproce…

```
@@ -10,18 +10,20 @@ os_list = ["windows"]
  reference = [
      "https://www.deepinstinct.com/2021/02/16/lsass-memory-dumps-are-stealthier-than-ever-before-part-2/",
  ]
- version = "1.0.9"
+ version = "1.0.10"

  query = '''
  registry where registry.path : "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SilentProcessExit\\lsass*"
  '''

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

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

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

2 🟩🟥

behavior/rules/credential_access_potential_access_to_kerb…

```
@@ -12,7 +12,7 @@ reference = [
  "https://github.com/EmpireProject/EmPyre/blob/master/lib/modules/collection/osx/kerberosdump.py",
  "https://opensource.apple.com/source/Heimdal/Heimdal-323.12/kuser/kcc-commands.in.auto.html",
  ]
- version = "1.0.5"
+ version = "1.0.6"

  query = '''
  process where event.type == "start" and
```

6 🟩🟩🟩🟥

behavior/rules/credential_access_potential_credential_acc…

```
@@ -9,7 +9,7 @@ license = "Elastic License v2"
  name = "Potential Credential Access via Mimikatz"
  os_list = ["windows"]
  reference = ["https://adsecurity.org/?page_id=1821", "https://github.com/gentilkiwi/mimikatz"]
- version = "1.0.5"
+ version = "1.0.6"

  query = '''
  process where event.action == "start" and
@@ -30,12 +30,14 @@ process where event.action == "start" and
    )
  '''

```

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

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

2

behavior/rules/credential_access_potential_credential_acc…

```diff
@@ -11,7 +11,7 @@ reference = [
      "https://github.com/GhostPack/Rubeus",
  "https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_rubeus.yml",
  ]
- version = "1.0.6"
+ version = "1.0.7"

  query = '''
  process where event.action == "start" and
```

6

...r/rules/credential_access_potential_credential_access_…

```diff
@@ -9,7 +9,7 @@ license = "Elastic License v2"
  name = "Potential Credential Access via Windows Credential History"
  os_list = ["windows"]
  reference = ["http://www.harmj0y.net/blog/redteaming/operational-guidance-for-offensive-user-dpapi-abuse/"]
- version = "1.0.5"
+ version = "1.0.6"

```

```
14  14      query = '''
15  15      file where event.action == "open" and
            @@ -25,11 +25,13 @@ file where event.action == "open" and
25  25                  "?:\\Windows\\System32\\Robocopy.exe",
26  26                  "?:\\Windows\\ccmcache\\*.exe",
27  27                  "?:\\Windows\\CCM\\*.exe",
    28    +             "?:\\Windows\\explorer.exe",
28  29                  "?:\\ProgramData\\Microsoft\\Windows Defender\\*.exe",
29  30                  "?:\\Windows\\explorer.exe",
30  31                  "?:\\Windows\\System32\\WerFault.exe",
31  32                  "?:\\Windows\\SysWOW64\\WerFault.exe",
32        -             "?:\\Windows\\System32\\dllhost.exe")
    33    +             "?:\\Windows\\System32\\dllhost.exe",
    34    +             "?:\\Windows\\System32\\sdclt.exe")
33  35      '''
34  36
35  37      optional_actions = []
```

2 🟩🟥⬜⬜⬜

behavior/rules/credential_access_potential_credentials_ph…

```
            @@ -11,7 +11,7 @@ reference = [
11  11      "https://github.com/EmpireProject/EmPyre/blob/master/lib/modules/collection/osx/prompt.py",
12  12          "https://ss64.com/osx/osascript.html",
13  13      ]
14        - version = "1.0.6"
    14    + version = "1.0.7"
15  15
16  16      query = '''
17  17      process where event.action == "exec" and
```

10 🟩🟩🟩🟩🟥

behavior/rules/credential_access_potential_discovery_of_d…

```
            @@ -8,7 +8,7 @@ license = "Elastic License v2"
8   8       name = "Potential Discovery of DPAPI Master Keys"
9   9       os_list = ["windows"]
```

```diff
 reference = ["http://www.harmj0y.net/blog/redteaming/operational-guidance-for-offensive-user-dpapi-abuse/"]
-version = "1.0.8"
+version = "1.0.9"
 
 query = '''
 file where event.action == "open" and
@@ -42,7 +42,13 @@ file where event.action == "open" and
             "?:\\ProgramData\\Microsoft\\Windows Defender Advanced Threat Protection\\*.exe",
             "?:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\*.exe",
             "?:\\ProgramData\\Microsoft\\Windows Defender Advanced Threat Protection\\Platform\\*.exe",
-            "?:\\Program Files\\Windows Defender Advanced Threat Protection\\*.exe") and
+            "?:\\Program Files\\Windows Defender Advanced Threat Protection\\*.exe",
+            "?:\\Windows\\System32\\igfxtray.exe",
+            "?:\\$WINDOWS.~BT\\Sources\\SetupCore.exe",
+            "?:\\Windows\\System32\\MRT.exe",
+            "?:\\Windows\\twain_32\\Brimc16a\\Common\\TwDsUiLaunch.exe",
+            "?:\\Windows\\Microsoft.NET\\Framework64\\*\\csc.exe",
+            "?:\\Users\\*\\AppData\\Local\\JetBrains\\Toolbox\\apps\\datagrip\\ch-0\\203.5981.102\\bin\\datagrip64.exe") and
  /* MSSQL service account */
  not (process.name : "sqlservr.exe" and file.path : "?:\\Users\\svc_*")
 '''
```

8 🟩🟩🟩🟥

...vior/rules/credential_access_potential_discovery_of_wi…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
  name = "Potential Discovery of Windows Credential Manager Store"
  os_list = ["windows"]
  reference = ["http://www.harmj0y.net/blog/redteaming/operational-guidance-for-offensive-user-dpapi-abuse/"]
- version = "1.0.7"
+ version = "1.0.8"

  query = '''
  file where event.action == "open" and
@@ -38,7 +38,11 @@ file where event.action == "open" and
              "?:\\Windows\\System32\\wbem\\WmiPrvSE.exe",
              "?:\\Windows\\System32\\dllhost.exe",
              "?:\\Windows\\explorer.exe",
-             "?:\\Windows\\System32\\MRT.exe")
+             "?:\\Windows\\System32\\MRT.exe",
+             "?:\\Users\\*\\AppData\\Local\\Microsoft\\OneDrive\\OneDrive.exe",
+             "?:\\Windows\\Microsoft.NET\\Framework\\*\\csc.exe",
+             "?:\\Windows\\System32\\SearchProtocolHost.exe",
+             "?:\\Users\\*\\AppData\\Local\\ESET\\ESETOnlineScanner\\ESETOnlineScanner.exe")
  '''

  optional_actions = []
```

2 🟩🟥□□□

behavior/rules/credential_access_security_account_manager…

```
@@ -11,7 +11,7 @@ reference = [
      "https://adsecurity.org/?page_id=1821",
      "https://github.com/gentilkiwi/mimikatz/wiki/module-~-lsadump",
13   13     ]
14        - version = "1.0.9"
     14   + version = "1.0.10"
15   15
16   16     query = '''
17   17     file where event.action == "open" and
```

4

behavior/rules/credential_access_security_account_manager…

```
@@ -11,10 +11,10 @@ reference = [
11   11         "https://adsecurity.org/?page_id=1821",
12   12     "https://github.com/gentilkiwi/mimikatz/wiki/module-~-lsadump",
13   13     ]
14        - version = "1.0.7"
     14   + version = "1.0.8"
15   15
16   16     query = '''
17        - sequence by process.entity_id with maxspan=5m
     17   + sequence by process.entity_id
18   18       [process where event.action == "start" and
19   19         not process.executable : ("?:\\Program Files\\*.exe", "?:\\Program Files (x86)\\*.exe") and
20   20         not (process.name : "cscript.exe" and process.command_line : "*Tanium*collectAdInfo.vbs*" and
```

2

behavior/rules/credential_access_sensitive_file_access_cl…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
8    8      name = "Sensitive File Access - Cloud Credentials"
9    9      os_list = ["windows"]
10   10     reference = ["https://github.com/GhostPack/Seatbelt"]
11        - version = "1.0.6"
     11   + version = "1.0.7"
12   12
```

```
query = '''
sequence by process.entity_id with maxspan=5m
```

2 🟩🟥⬜⬜⬜

...vior/rules/credential_access_sensitive_file_access_rem…

```
@@ -11,7 +11,7 @@ reference = [
    "http://www.harmj0y.net/blog/redteaming/operational-guidance-for-offensive-user-dpapi-abuse/",
    "https://smsagent.blog/2017/01/26/decrypting-remote-desktop-connection-manager-passwords-with-powershell/",
]
- version = "1.0.7"
+ version = "1.0.8"

query = '''
file where event.type == "access" and
```

19 🟩🟩🟩🟥⬜

behavior/rules/credential_access_sensitive_file_access_ss…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
name = "Sensitive File Access - SSH Saved Keys"
os_list = ["windows"]
reference = ["https://github.com/GhostPack/Seatbelt", "https://github.com/AlessandroZ/LaZagne"]
- version = "1.0.8"
+ version = "1.0.10"

query = '''
any where event.category in ("registry", "file") and
@@ -20,26 +20,35 @@ any where event.category in ("registry", "file") and
      ("?:\\Program Files\\*",
           "?:\\Program Files (x86)\\*",
           "?:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\*\\MsMpEng.exe",
-           "?:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\*\\MpCopyAccelerator.exe",
+           "?:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\*\\MpCopyAccelerator.exe",
+           "?:\\ProgramData\\Microsoft\\Windows Defender Advanced Threat Protection\\Platform\\*\\MsSense.exe",
            "?:\\Windows\\System32\\OpenSSH\\*.exe",
            "?:\\Windows\\System32\\smartscreen.exe",
            "?:\\WINDOWS\\system32\\reg.exe",
            "?:\\Windows\\regedit.exe",
            "?:\\Windows\\System32\\notepad.exe",
-           "?:\\Windows\\System32\\Robocopy.exe", 
+           "?:\\Windows\\System32\\Robocopy.exe",
            "?:\\Windows\\System32\\cmd.exe",
            "?:\\Windows\\explorer.exe",
            "?:\\Windows\\System32\\svchost.exe",
            "?:\\$WINDOWS.~BT\\Sources\\setuphost.exe",
            "?:\\Users\\*\\AppData\\Local\\Programs\\Git\\mingw64\\bin\\git.exe",
            "?:\\Users\\*\\AppData\\Local\\DBeaver\\dbeaver.exe",
-           "?:\\Windows\\System32\\SearchProtocolHost.exe") and
+           "?:\\Users\\*\\Tools\\dbeaver\\dbeaver.exe",
+           "?:\\Windows\\System32\\SearchProtocolHost.exe",
+           "?:\\Users\\*\\AppData\\Local\\Microsoft\\OneDrive\\OneDrive.exe",
+           "?:\\ProgramData\\GalacticScan\\GalacticScan.exe",
+           "?:\\Users\\*\\AppData\\Local\\Programs\\GalacticScan\\GalacticScan_Warpspeed.exe",
+           "?:\\Users\\*\\AppData\\Local\\Postman\\app-*\\Postman.exe",
```

```diff
+ "?:\\Users\\*\\OneDrive\\*\\Wintriage\\Tools\\ADSecurizame.exe",
+ "?:\\Users\\*\\AppData\\Local\\JetBrains\\Toolbox\\apps\\Gateway\\*\\bin\\gateway64.exe",
+ "?:\\Users\\*\\AppData\\Local\\Google\\Chrome\\Application\\chrome.exe") and

    /* many of the following exclusions are not signed nor have an original file name  */
    not process.name : ("pscp.exe", "psftp.exe", "_ssh.exe", "plink.exe", "PuTTYNG.exe", "putty*.exe", "busybox.exe",
                        "ssh.exe", "WinSCP.exe", "bash.exe", "MoTTY.exe", "eclipse.exe", "code.exe", "datagrip*.exe",
                        "MobaXterm_Personal*.exe", "RoyalTS_PuTTY*.exe", "MAP.EXE", "rssputty.exe", "phpstorm64.exe",
-                       "Fork.exe", "fzsftp.exe")
+                       "Fork.exe", "fzsftp.exe", "OneDrive.exe")
  '''

  optional_actions = []
```

2

behavior/rules/credential_access_sensitive_file_access_sy…

```diff
@@ -8,7 +8,7 @@ license = "Elastic License v2"
  name = "Sensitive File Access - System Admin Utilities"
  os_list = ["windows"]
  reference = ["https://github.com/GhostPack/Seatbelt", "https://github.com/AlessandroZ/LaZagne"]
- version = "1.0.7"
+ version = "1.0.8"

  query = '''
  sequence by process.entity_id with maxspan=5m
```

2 🟩🟥⬜⬜⬜

behavior/rules/credential_access_sensitive_file_access_un…

```diff
@@ -11,7 +11,7 @@ reference = [
     "https://steflan-security.com/windows-privilege-escalation-credential-harvesting/",
     "https://github.com/pha5matis/Pentesting-Guide/blob/master/privilege_escalation_windows.md",
 ]
-version = "1.0.7"
+version = "1.0.8"
 
 query = '''
 sequence by process.entity_id with maxspan=1m
```

2 🟩🟥⬜⬜⬜

behavior/rules/credential_access_suspicious_access_to_act…

```diff
@@ -10,7 +10,7 @@ os_list = ["windows"]
 reference = [
     "https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration",
 ]
-version = "1.0.8"
+version = "1.0.9"
 
 query = '''
 file where event.action == "open" and process.pid != 4 and
```

7 🟩🟩🟩🟥⬜

behavior/rules/credential_access_suspicious_access_to_lsa…

```diff
@@ -12,7 +12,7 @@ reference = [
     "https://www.ired.team/offensive-security/credential-access-and-credential-dumping/dumping-lsa-secrets",
                "https://github.com/gtworek/PSBits/tree/master/LSASecretDumper",
  ]
- version = "1.0.7"
+ version = "1.0.9"

  query = '''
  registry where
@@ -25,7 +25,10 @@ registry where
                                   "?:\\Program Files\\Citrix\\PvsVm\\Service\\PvsVmAgent.exe",
                                   "?:\\Windows\\Provisioning\\Autopilot\\DiagonsticAnalysis.pif",
                                   "?:\\Program Files\\RepairTech\\LiveAgent\\SyncroLive.Agent.Runner.exe",
-                                  "?:\\Program Files\\Common Files\\Adobe\\Creative Cloud Libraries\\CCLibrary.exe") and
+                                  "?:\\Program Files\\Common Files\\Adobe\\Creative Cloud Libraries\\CCLibrary.exe",
+                                  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrowserNet\\SecuredBrowserDotNetLauncher.exe",
+                                  "?:\\Windows\\regedit.exe",
+                                  "?:\\Program Files\\Dell\\Dell Data Protection\\Encryption\\EmsService.exe") and
   not (process.executable : "?:\\Windows\\System32\\dsregcmd.exe" and registry.path : "HKLM\\SECURITY\\Policy\\Secrets\\DSREGCMD\\MutexName") and
   not (process.executable : "?:\\Windows\\LTSvc\\LTSVC.exe" and registry.path : "HKLM\\SECURITY\\Cache\\NL$1") and
   not (process.executable : ("?:\\Program Files (x86)\\*.exe", "?:\\Program Files\\*.exe") and
```

2 🟩🟥⬜⬜⬜

behavior/rules/credential_access_suspicious_access_to_web…

```diff
@@ -7,7 +7,7 @@ id = "03758167-3eed-465f-9174-b284d599036d"
 license = "Elastic License v2"
 name = "Suspicious Access to Web Browser Credential Stores"
 os_list = ["windows"]
- version = "1.0.10"
+ version = "1.0.11"
 
 query = '''
 sequence by process.entity_id with maxspan=1m
```

5 🟩🟩🟩🟥🟥

behavior/rules/credential_access_suspicious_access_to_win…

```diff
@@ -9,7 +9,7 @@ license = "Elastic License v2"
 name = "Suspicious Access to Windows Vault Files"
 os_list = ["windows"]
 reference = ["http://www.harmj0y.net/blog/redteaming/operational-guidance-for-offensive-user-dpapi-abuse/"]
- version = "1.0.5"
+ version = "1.0.6"
 
 query = '''
 file where event.action == "open" and
@@ -28,7 +28,8 @@ file where event.action == "open" and
            "?:\\Windows\\CCM\\*.exe",
            "?:\\ProgramData\\Microsoft\\Windows Defender\\*.exe",
            "?:\\Windows\\System32\\dllhost.exe",
-           "?:\\Users\\*\\AppData\\Local\\ESET\\ESETOnlineScanner\\ESETOnlineScanner.exe")
+           "?:\\Users\\*\\AppData\\Local\\ESET\\ESETOnlineScanner\\ESETOnlineScanner.exe",
     32  +             "?:\\Windows\\Explorer.exe")
32   33    '''
33   34
34   35    optional_actions = []
```

6 🟩🟩🟩🟥

behavior/rules/credential_access_suspicious_credential_fi…

```
           @@ -13,7 +13,7 @@ reference = [
13   13        "https://research.ifcr.dk/certipy-2-0-bloodhound-new-escalations-shadow-credentials-golden-certificates-and-more-34d1c26f0dc6",
14   14        "https://posts.specterops.io/certified-pre-owned-d95910965cd2",
15   15    ]
16       - version = "1.0.4"
     16  + version = "1.0.5"
17   17
18   18    query = '''
19   19    sequence by process.entity_id with maxspan=1m
           @@ -35,12 +35,14 @@ sequence by process.entity_id with maxspan=1m
35   35       not (process.name : "powershell.exe" and file.path : "?:\\Windows\\ServiceProfiles\\LocalService\\AppData\\*")]
36   36    '''
37   37
38       - optional_actions = []
39   38    [[actions]]
40   39    action = "kill_process"
41   40    field = "process.entity_id"
42   41    state = 1
43   42
     43  + [[optional_actions]]
     44  + action = "rollback"
     45  +
44   46    [[threat]]
45   47    framework = "MITRE ATT&CK"
46   48    [[threat.technique]]
```

2 🟩🟥⬜⬜⬜

behavior/rules/credential_access_system_bootkey_registry_…

```diff
@@ -11,7 +11,7 @@ reference = [
     "http://moyix.blogspot.com/2008/02/syskey-and-sam.html",
     "https://github.com/gentilkiwi/mimikatz/wiki/module-~-lsadump",
 ]
- version = "1.0.6"
+ version = "1.0.7"

 query = '''
 sequence by process.entity_id with maxspan=1m
```

6 🟩🟩🟩🟥⬜

behavior/rules/credential_access_unusual_kerberos_client_…

```diff
@@ -7,7 +7,7 @@ id = "b5c91c3e-9d2d-4df6-afb7-c9d236b5ebe2"
 license = "Elastic License v2"
 name = "Unusual Kerberos Client Process"
 os_list = ["windows"]
- version = "1.0.4"
+ version = "1.0.5"

 query = '''
 sequence by process.entity_id with maxspan=1m
@@ -23,12 +23,14 @@ sequence by process.entity_id with maxspan=1m
   not process.executable : "?:\\Program Files (x86)\\GFI\\LanGuard 12 Agent\\lnsscomm.exe"]
 '''

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

```

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

2 🟩🟥⬜⬜⬜

behavior/rules/credential_access_web_browser_credential_a…

```
@@ -7,7 +7,7 @@ id = "9ed4ee4a-bc91-4d38-b6dd-11467b774460"
  license = "Elastic License v2"
  name = "Web Browser Credential Access via Unsigned Process"
  os_list = ["windows"]
- version = "1.0.8"
+ version = "1.0.9"

  query = '''
  sequence by user.name with maxspan=2m
```

2 🟩🟥⬜⬜⬜

behavior/rules/credential_access_web_browser_credential_a…

```
@@ -7,7 +7,7 @@ id = "f488cd1b-2407-4ec8-8705-7adf99ccbd33"
  license = "Elastic License v2"
  name = "Web Browser Credential Access via Unusual Process"
  os_list = ["windows"]
- version = "1.0.6"
+ version = "1.0.7"

  query = '''
  file where event.type == "access" and
```

2 🟩🟥⬜⬜⬜

behavior/rules/credential_access_web_browsers_password_ac…

```
@@ -14,7 +14,7 @@ reference = [
    "https://ss64.com/osx/security.html",
    "https://www.intezer.com/blog/research/operation-electrorat-attacker-creates-fake-companies-to-drain-your-crypto-wallets/",
]
- version = "1.0.5"
+ version = "1.0.6"

query = '''
process where event.action == "exec" and
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_attempt_to_disable_windows…

```
@@ -4,7 +4,7 @@ id = "32ab2977-2932-4172-9117-36e382591818"
license = "Elastic License v2"
name = "Attempt to Disable Windows Defender Services"
os_list = ["windows"]
- version = "1.0.4"
+ version = "1.0.5"

query = '''
process where event.action == "start" and
@@ -17,12 +17,14 @@ process where event.action == "start" and
    process.parent.name : ("rundll32.exe", "regsvr32.exe", "wscript.exe", "cscript.exe", "powershell.exe", "mshta.exe"))
'''

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

```
  state = 0

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

11 🟩🟩🟥🟥⬜

behavior/rules/defense_evasion_binary_masquerading_via_un…

```
@@ -8,7 +8,7 @@ id = "35dedf0c-8db6-4d70-b2dc-a133b808211f"
  license = "Elastic License v2"
  name = "Binary Masquerading via Untrusted Path"
  os_list = ["windows"]
- version = "1.0.12"
+ version = "1.0.13"

  query = '''
  process where event.action == "start" and
@@ -49,11 +49,9 @@ process where event.action == "start" and
      "qprocess.exe",
      "quser.exe",
      "qwinsta.exe",
-     "reg.exe",
      "regasm.exe",
      "regsvcs.exe",
      "regsvr32.exe",
-     "runas.exe",
      "rundll32.exe",
      "schtasks.exe",
      "sdclt.exe",
@@ -62,13 +60,11 @@ process where event.action == "start" and
      "svchost.exe",
      "taskhost.exe",
      "taskhostw.exe",
-     "tasklist.exe",
      "userinit.exe",
      "vaultcmd.exe",
 68   65          "vssadmin.exe",
 69   66          "wininit.exe",
 70   67          "winlogon.exe",
 71        -      "whoami.exe",
 72   68          "wmic.exe",
 73   69          "wevtutil.exe",
 74   70          "wscript.exe",
              @@ -85,6 +81,7 @@ process where event.action == "start" and
 85   81          "?:\\Windows\\Microsoft.NET\\*.exe",
 86   82          "?:\\Program Files (x86)\\*.exe",
 87   83          "?:\\Program Files\\*.exe",
      84   +      "?:\\Windows\\WinSxS\\*.exe",
 88   85
 89   86          /* Issue # 295 */
 90   87
              "?:\\Users\\*\\AppData\\Local\\Programs\\Git\\usr\\bin\\hostname.exe",
              @@ -152,12 +149,14 @@ process where event.action == "start" and
152  149        not (process.parent.executable :
              "?:\\apps\\sage300\\Programs\\runtime\\a4wcontainerXP.exe" and process.name : "regsvr32.exe")
153  150      '''
154  151
155        -  optional_actions = []
156  152      [[actions]]
157  153      action = "kill_process"
158  154      field = "process.entity_id"
159  155      state = 0
160  156
     157   +  [[optional_actions]]
     158   +  action = "rollback"
     159   +
161  160      [[threat]]
162  161      framework = "MITRE ATT&CK"
163  162      [[threat.technique]]
```

14 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_binary_proxy_execution_via…

```
              @@ -16,7 +16,7 @@ reference = [
```

```diff
     "https://lolbas-project.github.io/lolbas/Libraries/Url/",
     "https://lolbas-project.github.io/lolbas/Libraries/Desk/",
 ]
- version = "1.0.8"
+ version = "1.0.9"

 query = '''
 sequence with maxspan=1m
@@ -32,15 +32,19 @@ sequence with maxspan=1m
                "*url.dll*FileProtocolHandler*.exe*",
                "*shell32.dll*ShellExec_RunDLL*",
                "*advpack*LaunchINFSection*",
-               "*desk*InstallScreenSaver*") and
+               "*desk*InstallScreenSaver*",
+               "*shell32*WaitForExplorerRestart*") and
    /* Issue #265 */
    not (process.command_line : "*url.dll*FileProtocolHandler*" and
         process.command_line : ("*http://*", "*zoommtg://*", "*://*&*&*")) and

    /* Legit LaunchApplication instances via msdt */
    not (process.command_line : "*pcwutl.dll,LaunchApplication*" and
         process.parent.name :  "msdt.exe" and
-        process.working_directory : "?:\\Windows\\system32\\")] by process.entity_id
+        process.working_directory : "?:\\Windows\\system32\\") and
+
+   not (process.command_line : "*shell32*WaitForExplorerRestart*" and process.args : "?:\\Windows\\*explorer.exe")
+   ] by process.entity_id
   [process where event.action == "start" and
    not process.executable : ("?:\\Program Files\\*.exe", "?:\\Program Files (x86)\\*.exe") and
    not (process.name : "wscript.exe" and process.args : "Cathexis Archive Viewer.vbs") and
@@ -49,12 +53,14 @@ sequence with maxspan=1m
    ] by process.parent.entity_id
 '''
```

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

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

13 🟩🟥🟥🟥⬜

behavior/rules/defense_evasion_control_panel_process_with…

```
@@ -7,12 +7,11 @@ id = "a4862afb-1292-4f65-a15f-8d6a8019b5e2"
  license = "Elastic License v2"
  name = "Control Panel Process with Unusual Arguments"
  os_list = ["windows"]
- version = "1.0.6"
+ version = "1.0.8"

  query = '''
  process where event.action == "start" and
   process.executable : ("?:\\Windows\\SysWOW64\\control.exe", "?:\\Windows\\System32\\control.exe") and
-  (
    process.command_line :
            ("*.jpg*",
             "*.png*",
@@ -26,14 +25,8 @@ process where event.action == "start" and
             "*..\\..\\*",
             "*/AppData/Local/*",
             "*:\\Users\\Public\\*",
-            "*\\AppData\\Local\\*") or
-
-   (process.args_count == 1 and
```

```diff
32      -    not process.parent.executable : ("?:\\Windows\\Explorer.exe", "?:\\Windows\\System32\\Sihost.exe") and
33      -    process.parent.executable != null)
34      -
35      -   ) and
36      -
     28 +            "*\\AppData\\Local\\*") and
     29 +
37   30   /* excluding FPs where /name arg is used to specify a control by name */
38   31   not (process.args : "/name" and process.args_count >= 2) and
39   32   /* excluding system IL to minimize risk of killing system critical execution */
```

9 🟩🟩🟩🟥

behavior/rules/defense_evasion_crashdump_disabled_via_reg…

```diff
@@ -11,20 +11,23 @@ reference = [
11   11      "https://elastic.github.io/security-research/intelligence/2022/03/01.hermeticwiper-targets-ukraine/article/",
12   12      "https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/memory-dump-file-options",
13   13  ]
14      - version = "1.0.6"
     14 + version = "1.0.7"
15   15
16   16  query = '''
17   17  registry where registry.value : "CrashDumpEnabled" and registry.data.strings : "0" and
18   18   not (user.id in ("S-1-5-18", "S-1-5-19", "S-1-5-20") and
19      -      process.executable : ("?:\\Windows\\System32\\svchost.exe", "?:\\Windows\\System32\\msiexec.exe"))
     19 +      process.executable : ("?:\\Windows\\System32\\svchost.exe", "?:\\Windows\\System32\\msiexec.exe")) and
     20 +  not process.executable : "?:\\Windows\\System32\\SystemPropertiesAdvanced.exe"
```

```
  '''

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

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

50 ▇▇▇▇▇

behavior/rules/defense_evasion_dll_control_panel_items_re…

```
@@ -0,0 +1,50 @@
+ [rule]
+ description = """
+ Identifies the modification of DLL Control Panel Items registry. Adversaries may load a malicious DLL when Control Panel
+ is executed via setting the CPLs subkey to the DLL path.
+ """
+ id = "340bdcad-187f-4ccb-b84e-34ee70844d78"
+ license = "Elastic License v2"
+ name = "DLL Control Panel Items Registry Modification"
+ os_list = ["windows"]
+ reference = ["https://docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/hh127454(v=vs.85)"]
+ version = "1.0.2"
+
+ query = '''
+ registry where
+  registry.path :
+       ("HKEY_USERS\\S-1-5-*\\Software\\Microsoft\\Windows\\CurrentVersion\\Control Panel\\CPLs\\*",
+ "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Control Panel\\CPLs\\*") and
+   process.executable != null and registry.data.strings != null and not registry.data.type : "REG_DWORD" and
+   not (process.executable :
+ ("?:\\Windows\\System32\\svchost.exe",
+ "?:\\Windows\\System32\\DriverStore\\FileRepository\\*.exe",
+ "?:\\Windows\\System32\\msiexec.exe") and user.id : ("S-1-5-18", "S-1-5-19", "S-1-5-20"))
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1218"
+ name = "System Binary Proxy Execution"
+ reference = "https://attack.mitre.org/techniques/T1218/"
+ [[threat.technique.subtechnique]]
+ id = "T1218.002"
+ name = "Control Panel"
+ reference = "https://attack.mitre.org/techniques/T1218/002/"
+
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.15.0"
```

90 🟩🟩🟩🟩🟩

behavior/rules/defense_evasion_evasion_via_double_file_ex…

```
@@ -0,0 +1,90 @@
+ [rule]
+ description = """
+ Adversaries may abuse a double extension or unicode right-to-left override (RTLO or RLO) character (U+202E) in the
+ filename as a means of masquerading the true file type. A file name may include a secondary file type extension that may
+ cause only the first extension to be displayed which maximize user execution likelihood.
+ """
+ id = "ccfca0c7-c975-4735-82bd-954ffbafd00b"
+ license = "Elastic License v2"
+ name = "Evasion via Double File Extension"
+ os_list = ["windows"]
+ reference = ["https://www.pcmag.com/encyclopedia/term/double-extension"]
+ version = "1.0.3"
+
+ query = '''
+ process where event.action == "start" and
+  (
+   /* double extension in process.name */
+   process.name regex~ """.+(\.|\,|\_|\-)(pdf|doc|docx|xls|xlsx|png|jpg|html|txt|zip|rar|ppt|pptx|rtf|htm|GIF)\.(scr|exe|com|pif)""" or
+
+   /* fake extension via Unicode Right-To-Left-Override technique */
+   process.name : "*\u{202E}*"
+  ) and
+
+  /* False Positives */
+  not process.hash.sha256 :
+ ("1211cb4a560586d4ffb4b1bfd268a8146318af09587a9d5e33703575d5178e77",
+ "582ae3540ba32e7100fe20c0b01d14d1d85167cdb7ee512f596544d7351a2d5e",
+ "b59ac9390d9026ec3b552ebd6f3438c05aab2880d5e17616c13c5d42b6b34c65",
+ "a781c337575da892e6c1b2ac26a6272085a127c554dfd68729deb146eca6b837",
+ "96234bb98b3266e49ef74ac7accd4644b709355057d5a34b2966e9fa56aadcf3",
+ "38473e19af02cb5e6f386f41238da862df72bbc1d7a1e94d838c4b93d6f56e72",
+ "5d62d79f6555d7a7edaf3b175312b326df779f9ae8c893e2182e4159f44c9d34",
+ "8d0434610280c8f94a0e9c29e4c33b97804fab4ab6fc29531ba76acebd2f5518",
+ "7e59dec861a2a9ad68bd2758407c256dedb233cab225683db677ab2d2fbec258",
+ "fbd43f9a3567a19427894e61052d1b46f70b7474357ef50de9dc8749fc950509",
+ "96234bb98b3266e49ef74ac7accd4644b709355057d5a34b2966e9fa56aadcf3") and
+  not (process.executable : ("?:\\Program Files\\*.exe", "?:\\Program Files (x86)\\*.exe") and process.code_signature.trusted == true) and
+  not (process.code_signature.subject_name : ("AVANQUEST SOFTWARE S.A.S", "Jernej Simončič") and process.code_signature.trusted == true)
+ '''
+
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[optional_actions]]
+ action = "rollback"
```

```
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1204"
+ name = "User Execution"
+ reference = "https://attack.mitre.org/techniques/T1204/"
+ [[threat.technique.subtechnique]]
+ id = "T1204.002"
+ name = "Malicious File"
+ reference = "https://attack.mitre.org/techniques/T1204/002/"
+
+
+
+ [threat.tactic]
+ id = "TA0002"
+ name = "Execution"
+ reference = "https://attack.mitre.org/tactics/TA0002/"
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1036"
+ name = "Masquerading"
+ reference = "https://attack.mitre.org/techniques/T1036/"
+ [[threat.technique.subtechnique]]
+ id = "T1036.002"
+ name = "Right-to-Left Override"
+ reference = "https://attack.mitre.org/techniques/T1036/002/"
+
+ [[threat.technique.subtechnique]]
+ id = "T1036.007"
+ name = "Double File Extension"
+ reference = "https://attack.mitre.org/techniques/T1036/007/"
+
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.15.0"
```

62 🟩🟩🟩🟩🟩

behavior/rules/defense_evasion_execution_of_a_file_droppe…

```
...   ...   @@ -0,0 +1,62 @@
+ [rule]
+ description = """
+ Identifies when the OpenSSL utility create a file followed by it's execution. Malware authors may attempt to evade
+ detection and trick users into executing malicious code by encoding and encrypting their payload and placing it in a
+ disk image file. This behavior is consistent with adware or malware families such as Bundlore and Shlayer.
+ """
+ id = "d2017990-b448-4617-8d4a-55aa45abe354"
+ license = "Elastic License v2"
+ name = "Execution of a File Dropped by OpenSSL"
+ os_list = ["macos"]
+ reference = ["https://attack.mitre.org/software/S0482/", "https://attack.mitre.org/software/S0402/"]
+ version = "1.0.2"
+
+ query = '''
+ sequence with maxspan=1m
+ [file where event.action != "deletion" and process.name == "openssl"] by file.path
+ [process where event.action == "exec"] by process.executable
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 1
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1204"
+ name = "User Execution"
+ reference = "https://attack.mitre.org/techniques/T1204/"
+ [[threat.technique.subtechnique]]
+ id = "T1204.002"
+ name = "Malicious File"
+ reference = "https://attack.mitre.org/techniques/T1204/002/"
+
+
+
+ [threat.tactic]
+ id = "TA0002"
+ name = "Execution"
+ reference = "https://attack.mitre.org/tactics/TA0002/"
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1027"
+ name = "Obfuscated Files or Information"
+ reference = "https://attack.mitre.org/techniques/T1027/"
+
+ [[threat.technique]]
+ id = "T1140"
+ name = "Deobfuscate/Decode Files or Information"
+ reference = "https://attack.mitre.org/techniques/T1140/"
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.15.0"
```

6

behavior/rules/defense_evasion_execution_via_internet_exp…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
  name = "Execution via Internet Explorer Exporter"
  os_list = ["windows"]
  reference = ["https://lolbas-project.github.io/lolbas/Binaries/Extexport/"]
- version = "1.0.8"
+ version = "1.0.9"

  query = '''
  sequence by user.id with maxspan=5m
@@ -20,12 +20,14 @@ sequence by user.id with maxspan=5m
                                  "?:\\Program Files\\Internet Explorer\\ExtExport.exe")]
  '''

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

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

9

behavior/rules/defense_evasion_execution_via_renamed_sign…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
  name = "Execution via Renamed Signed Binary Proxy"
  os_list = ["windows"]
  reference = ["https://lolbas-project.github.io"]
- version = "1.0.9"
+ version = "1.0.10"
```

```diff
 
 query = '''
 process where event.action == "start" and
@@ -55,16 +55,17 @@ process where event.action == "start" and
           "\\Device\\HarddiskVolume*\\Program Files (x86)\\*.exe",
          "\\Device\\HarddiskVolume*\\Program Files\\*.exe"
        ) and
-  not (process.pe.original_file_name in ("RegAsm.exe", "REGSVR32.EXE") and process.executable : "?:\\Windows\\Installer\\MSI*.tmp" and
-       process.parent.executable : "?:\\WINDOWS\\system32\\msiexec.exe")
+  not (process.executable : "?:\\Windows\\Installer\\MSI*.tmp" and process.parent.name : "msiexec.exe")
 '''
 
- optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 0
 
+ [[optional_actions]]
+ action = "rollback"
+
 [[threat]]
 framework = "MITRE ATT&CK"
 [[threat.technique]]
```

11 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_indirect_command_execution…

```diff
@@ -8,21 +8,26 @@ license = "Elastic License v2"
 name = "Indirect Command Execution via Console Window Host"
 os_list = ["windows"]
 reference = ["https://lolbas-project.github.io/lolbas/Binaries/Conhost/"]
```

```
- version = "1.0.1"
+ version = "1.0.2"

  query = '''
  process where event.action == "start" and
    process.parent.name : "conhost.exe" and process.parent.args_count >= 2 and
    process.parent.command_line : "*conhost* *.exe*" and
-   not process.command_line : ("?:\\windows\\system32\\cmd.exe", "?:\\windows\\SysWOW64\\cmd.exe", "cmd.exe")
+   not process.command_line :
+             ("?:\\windows\\system32\\cmd.exe",
+              "?:\\windows\\SysWOW64\\cmd.exe", "cmd.exe",
+ "?:\\windows\\system32\\windowspowershell\\*\\powershell.exe")
  '''

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

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

43

behavior/rules/defense_evasion_indirect_command_execution…

```
@@ -0,0 +1,43 @@
+ [rule]
+ description = """
+ Identifies the use of native Windows tool, forfiles to execute a file. Adversaries may abuse utilities that allow for
+ command execution to bypass security restrictions that limit the use of command-line interpreters.
+ """
+ id = "78afa378-d1c4-4b83-a261-ce1c90f1cbf9"
+ license = "Elastic License v2"
+ name = "Indirect Command Execution via ForFiles"
+ os_list = ["windows"]
+ reference = ["https://lolbas-project.github.io/lolbas/Binaries/Forfiles/"]
+ version = "1.0.3"
+
+ query = '''
+ process where event.action == "start" and
+   process.parent.name : "forfiles.exe" and process.parent.args : "/c" and
+   process.parent.args : "/p" and process.parent.args : "/m" and
+
+   not process.executable : "?:\\Windows\\System32\\conhost.exe" and
+   not user.id in ("S-1-5-18", "S-1-5-19", "S-1-5-20") and
+   not (process.name : "cmd.exe" and process.args: ("del", "xcopy", "cmd /c del @PATH", "move"))
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1202"
+ name = "Indirect Command Execution"
+ reference = "https://attack.mitre.org/techniques/T1202/"
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference =
  "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.15.0"
```

2 🟩🟥

behavior/rules/defense_evasion_macos_monterey_reflective_…

```
@@ -11,7 +11,7 @@ reference = [
      "https://slyd0g.medium.com/understanding-and-defending-against-reflective-code-loading-on-macos-e2e83211e48f",
      "https://github.com/slyd0g/SwiftInMemoryLoading",
  ]
- version = "1.0.4"
+ version = "1.0.5"

  query = '''
  file where event.type != "deletion" and
```

6 🟩🟩🟩🟥

behavior/rules/defense_evasion_managed_.net_code_executio…

```
@@ -7,7 +7,7 @@ id = "cd886776-8790-4724-9484-3f0008b87da7"
  license = "Elastic License v2"
  name = "Managed .NET Code Execution via PowerShell"
  os_list = ["windows"]
- version = "1.0.4"
+ version = "1.0.5"

  query = '''
  process where event.type == "start" and
@@ -22,7 +22,9 @@ process where event.type == "start" and
     "*set *set *set *", "*;iex*", "*IEX (*", "*FromBase64String*")

     ) and
```

```
-   not process.parent.args : ("?:\\Program Files (x86)\\*", "?:\\Program Files\\*")
+   not process.parent.args : ("?:\\Program Files (x86)\\*", "?:\\Program Files\\*", "visualstudio20??-workload-vctools;") and
+   not process.args : "@?:\\Windows\\TEMP\\*.cmdline" and
+   not (process.parent.args : "-ExecutionPolicy" and process.parent.command_line : "*.vscode\\extensions*")
  '''

  optional_actions = []
```

6 🟩🟩🟩🟥⬜

...ior/rules/defense_evasion_managed_.net_code_execution_…

```
@@ -12,7 +12,7 @@ reference = [
      "https://github.com/med0x2e/GadgetToJScript",
      "https://github.com/mdsecactivebreach/SharpShooter",
  ]
- version = "1.0.5"
+ version = "1.0.6"

  query = '''
  sequence by process.entity_id with maxspan=2m
@@ -38,12 +38,14 @@ sequence by process.entity_id with maxspan=2m
                 "msxsl.exe.log")]
  '''

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

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

```
48    50      framework = "MITRE ATT&CK"
49    51      [[threat.technique]]
```

2 🟩🟥⬜⬜⬜

behavior/rules/defense_evasion_modification_of_safari_set…

```
              @@ -8,7 +8,7 @@ license = "Elastic License v2"
 8     8      name = "Modification of Safari Settings via
              Defaults Command"
 9     9      os_list = ["macos"]
10    10      reference =
              ["https://objectivebythesea.com/v2/talks/OBTS_v2_Zo
              har.pdf"]
11          - version = "1.0.6"
      11    + version = "1.0.7"
12    12
13    13      query = '''
14    14      process where event.type == "start" and
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_msbuild_with_unusual_argum…

```
              @@ -8,7 +8,7 @@ license = "Elastic License v2"
 8     8      name = "MSBuild with Unusual Arguments"
 9     9      os_list = ["windows"]
10    10      reference = ["https://lolbas-
              project.github.io/lolbas/Binaries/Msbuild/"]
11          - version = "1.0.6"
      11    + version = "1.0.7"
12    12
13    13      query = '''
14    14      process where event.action == "start" and
              @@ -32,12 +32,14 @@ process where event.action ==
              "start" and
32    32                                 "msaccess.exe"))
33    33      '''
34    34
35          - optional_actions = []
36    35      [[actions]]
37    36      action = "kill_process"
38    37      field = "process.entity_id"
```

```
39   38     state = 0
40   39
     40   + [[optional_actions]]
     41   + action = "rollback"
     42   +
41   43     [[threat]]
42   44     framework = "MITRE ATT&CK"
43   45     [[threat.technique]]
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_network_connection_via_pro…

```
          @@ -8,7 +8,7 @@ id = "95601d8b-b969-4189-9744-090140ae29e6"
8    8      license = "Elastic License v2"
9    9      name = "Network Connection via Process with Unusual Arguments"
10   10     os_list = ["windows"]
11        - version = "1.0.9"
     11   + version = "1.0.10"
12   12
13   13     query = '''
14   14     sequence by process.entity_id with maxspan=5m
          @@ -52,12 +52,14 @@ sequence by process.entity_id with maxspan=5m
52   52       [network where event.action == "connection_attempted"]
53   53     '''
54   54
55        - optional_actions = []
56   55     [[actions]]
57   56     action = "kill_process"
58   57     field = "process.entity_id"
59   58     state = 0
60   59
     60   + [[optional_actions]]
     61   + action = "rollback"
     62   +
61   63     [[threat]]
62   64     framework = "MITRE ATT&CK"
63   65     [[threat.technique]]
```

7

behavior/rules/defense_evasion_ntdll_loaded_from_an_unusu…

```
@@ -7,7 +7,7 @@ id = "3205274e-7eb0-4765-a712-5783361091ae"
  license = "Elastic License v2"
  name = "NTDLL Loaded from an Unusual Path"
  os_list = ["windows"]
- version = "1.0.4"
+ version = "1.0.5"

  query = '''
  library where dll.pe.original_file_name : "ntdll.dll" and
@@ -16,17 +16,20 @@ library where dll.pe.original_file_name : "ntdll.dll" and
                  "?:\\Windows\\System32\\ntdll.dll",
                  "?:\\Windows\\WinSxS\\amd64_microsoft-windows-ntdll_*\\ntdll.dll",
                  "?:\\Windows\\WinSxS\\wow64_microsoft-windows-ntdll_*\\ntdll.dll",
+                 "?:\\Windows\\WinSxS\\Temp\\InFlight\\*\\amd64_microsoft-windows-ntdll_*\\ntdll.dll",
                  /* vsmbSharePrefix */
                  "\\Device\\vmsmb\\VSMB-{*}\\os\\windows\\*\\ntdll.dll",
                  "?:\\Windows\\WinSxS\\Temp\\PendingDeletes\\$$DeleteMe*")
  '''

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

+ [[optional_actions]]
+ action = "rollback"
+
30    33      [[threat]]
31    34      framework = "MITRE ATT&CK"
32    35      [[threat.technique]]
```

2 🟩🟥

behavior/rules/defense_evasion_operating_system_security_…

```
              @@ -8,7 +8,7 @@ license = "Elastic License v2"
 8     8      name = "Operating System Security Updates Disabled"
 9     9      os_list = ["macos"]
10    10      reference =
              ["https://blog.checkpoint.com/2017/07/13/osxdok-
              refuses-go-away-money/"]
11          - version = "1.0.5"
      11    + version = "1.0.6"
12    12
13    13      query = '''
14    14      process where event.type == "start" and
```

2 🟩🟥

behavior/rules/defense_evasion_parent_process_pid_spoofin…

```
              @@ -8,7 +8,7 @@ license = "Elastic License v2"
 8     8      name = "Parent Process PID Spoofing"
 9     9      os_list = ["windows"]
10    10      reference =
              ["https://blog.didierstevens.com/2017/03/20/"]
11          - version = "1.0.9"
      11    + version = "1.0.10"
12    12
13    13      query = '''
14    14      sequence with maxspan=5m
```

76 🟩🟩🟩🟩🟩

behavior/rules/defense_evasion_payload_decoded_and_decryp…

```
...   ...     @@ -0,0 +1,76 @@
       1    + [rule]
       2    + description = """
```

```
+ Identifies when a built-in utility is used to decode and decrypt a payload after a macOS disk image (DMG) is executed.
+ Malware authors may attempt to evade detection and trick users into executing malicious code by encoding and encrypting
+ their payload and placing it in a disk image file. This behavior is consistent with adware or malware families such as
+ Bundlore and Shlayer.
+ """
+ id = "5dce3865-838f-4773-9781-87226af1fc12"
+ license = "Elastic License v2"
+ name = "Payload Decoded and Decrypted via Built-In Utilities"
+ os_list = ["macos"]
+ reference = ["https://attack.mitre.org/software/S0482/", "https://attack.mitre.org/software/S0402/"]
+ version = "1.0.7"
+
+ query = '''
+ process where event.action == "exec" and process.name == "openssl" and
+  process.args : "/Volumes/*" and process.args : "enc" and
+     // openssl base64-decoding data
+     process.args : "-base64" and
+     // openssl decrypting input data
+     process.args : "-d"
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1059"
+ name = "Command and Scripting Interpreter"
+ reference = "https://attack.mitre.org/techniques/T1059/"
+ [[threat.technique.subtechnique]]
+ id = "T1059.004"
+ name = "Unix Shell"
+ reference = "https://attack.mitre.org/techniques/T1059/004/"
+
+
+ [[threat.technique]]
+ id = "T1204"
+ name = "User Execution"
+ reference = "https://attack.mitre.org/techniques/T1204/"
+ [[threat.technique.subtechnique]]
+ id = "T1204.002"
+ name = "Malicious File"
+ reference = "https://attack.mitre.org/techniques/T1204/002/"
+
+
+
+ [threat.tactic]
+ id = "TA0002"
+ name = "Execution"
+ reference = "https://attack.mitre.org/tactics/TA0002/"
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1027"
+ name = "Obfuscated Files or Information"
+ reference = "https://attack.mitre.org/techniques/T1027/"
+
+ [[threat.technique]]
+ id = "T1140"
+ name = "Deobfuscate/Decode Files or Information"
+ reference = "https://attack.mitre.org/techniques/T1140/"
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
```

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

4 🟩🟩🟥🟥⬜

behavior/rules/defense_evasion_potential_binary_masquerad…

```
@@ -7,13 +7,13 @@ id = "4154c8ce-c718-4641-80db-a6a52276f1a4"
  license = "Elastic License v2"
  name = "Potential Binary Masquerading via Invalid Code Signature"
  os_list = ["macos"]
- version = "1.0.4"
+ version = "1.0.5"

  query = '''
  process where event.action == "exec" and
   process.name :"com.apple.*" and
   (process.code_signature.trusted == false or process.code_signature.exists == false) and
-  not (process.code_signature.subject_name : "Software Signing" and
+  not (process.code_signature.subject_name : ("Software Signing", "com.apple.WebKit.Networking", "com.apple.WebKit.WebContent") and
        process.name :
                    ("com.apple.WebKit.WebContent.Development",
                     "com.apple.WebKit.GPU.Development",
```

2 🟩🟥⬜⬜⬜

...r/rules/defense_evasion_potential_defense_evasion_via_…

```
@@ -5,7 +5,7 @@ license = "Elastic License v2"
  name = "Potential Defense Evasion via Filter Manager Control Program"
  os_list = ["windows"]
  reference = ["https://lolbas-project.github.io/lolbas/Binaries/FltMC/"]
- version = "1.0.6"
+ version = "1.0.7"

```

```
query = '''
process where event.action == "start" and
```

62

behavior/rules/defense_evasion_potential_evasion_via_over…

```
@@ -0,0 +1,62 @@
+ [rule]
+ description = """
+ Adversaries may use binary padding to add junk data and change the on-disk representation of malware. This can be done
+ without affecting the functionality or behavior of a binary, but can increase the size of the binary beyond what some
+ security tools are capable of handling due to file size limitations
+ """
+ id = "65a402ff-904b-4d14-b7aa-fa0c5ae575f8"
+ license = "Elastic License v2"
+ name = "Potential Evasion via Oversized Image Load"
+ os_list = ["windows"]
+ reference = ["https://attack.mitre.org/techniques/T1027/001/"]
+ version = "1.0.2"
+
+ query = '''
+ sequence with maxspan=1m
+  [file where event.action != "deletion" and
+    /* over 100MB in size */
+    file.size >= 100000000 and file.Ext.header_bytes : "4d5a*" and not file.extension : "exe" and
+    not user.id : "S-1-5-18"] by file.path
+  [library where
+     (
+      process.name : ("rundll32.exe", "regsvr32.exe", "svchost.exe") or
+      process.executable :
+                  ("?:\\Users\\Public\\*",
+                   "?:\\ProgramData\\*",
+                   "?:\\Windows\\Temp\\*",
+ "?:\\Users\\*\\AppData\\Local\\Temp\\Temp?_*",
+ "?:\\Users\\*\\AppData\\Local\\Temp\\7z*",
+ "?:\\Users\\*\\AppData\\Local\\Temp\\Rar*",
+ "?:\\Users\\*\\AppData\\Local\\Temp\\BNZ.*")
+      )
+     and not dll.code_signature.trusted == true and
+     not dll.code_signature.status : "errorExpired" and
+     not user.id : "S-1-5-18"] by dll.path
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 1
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1027"
+ name = "Obfuscated Files or Information"
+ reference = "https://attack.mitre.org/techniques/T1027/"
+ [[threat.technique.subtechnique]]
+ id = "T1027.001"
+ name = "Binary Padding"
+ reference = "https://attack.mitre.org/techniques/T1027/001/"
+
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.16.0"
```

72 🟩🟩🟩🟩🟩

behavior/rules/defense_evasion_potential_initial_access_v…

```
@@ -0,0 +1,72 @@
+[rule]
+description = """
+Identifies attempts to create a DLL file to a known desktop application dependencies folder such as Slack, Teams or
+OneDrive and by an unusual process. This may indicate an attempt to load a malicious module via DLL search order
+hijacking.
+"""
+id = "ddc4fa22-4675-44c0-a813-e786e638d7e0"
+license = "Elastic License v2"
+name = "Potential Initial Access via DLL Search Order Hijacking"
+os_list = ["windows"]
+reference = ["https://posts.specterops.io/automating-dll-hijack-discovery-81c4295904b0"]
+version = "1.0.2"
+
+query = '''
+file where event.action != "deletion" and
+ file.extension : "dll" and
+ file.path :
+         ("?:\\Users\\*\\AppData\\*\\Microsoft\\OneDrive\\*.dll",
+          "?:\\Users\\*\\AppData\\*\\Microsoft OneDrive\\*.dll",
+          "?:\\Users\\*\\AppData\\*\\Microsoft\\Teams\\*.dll",
+          "?:\\Users\\*\\AppData\\Local\\slack\\app-*\\*.dll",
+          "?:\\Users\\*\\AppData\\Local\\Programs\\Microsoft VS Code\\*") and
+ process.name : ("winword.exe", "excel.exe", "powerpnt.exe", "MSACCESS.EXE", "MSPUB.EXE", "fltldr.exe", "cmd.exe",
+                  "certutil.exe", "mshta.exe", "cscript.exe", "wscript.exe", "curl.exe", "powershell.exe", "pwsh.exe") and
+  not (process.name : "cmd.exe" and file.path :"?:\\Users\\*\\AppData\\*\\Microsoft\\OneDrive\\*\\api-ms-win-core-*.dll")
+ '''
+
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[optional_actions]]
+ action = "rollback"
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1566"
+ name = "Phishing"
+ reference = "https://attack.mitre.org/techniques/T1566/"
+ [[threat.technique.subtechnique]]
+ id = "T1566.001"
+ name = "Spearphishing Attachment"
+ reference = "https://attack.mitre.org/techniques/T1566/001/"
+
+
+
+ [threat.tactic]
+ id = "TA0001"
+ name = "Initial Access"
+ reference = "https://attack.mitre.org/tactics/TA0001/"
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1574"
+ name = "Hijack Execution Flow"
+ reference = "https://attack.mitre.org/techniques/T1574/"
+ [[threat.technique.subtechnique]]
+ id = "T1574.001"
+ name = "DLL Search Order Hijacking"
+ reference = "https://attack.mitre.org/techniques/T1574/001/"
```

```
+
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.15.0"
```

12 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_potential_masquerading_as_…

```
@@ -7,14 +7,16 @@ id = "5b00c9ba-9546-47cc-8f9f-1c1a3e95f65c"
  license = "Elastic License v2"
  name = "Potential Masquerading as SVCHOST"
  os_list = ["windows"]
- version = "1.0.7"
+ version = "1.0.9"

  query = '''
  process where event.action == "start" and
    process.name : "svchost.exe" and
    process.parent.executable != null and
    not process.parent.executable : (
      "?:\\Windows\\System32\\services.exe",
+     "\\Device\\HarddiskVolume?\\Windows\\System32\\services.exe",
+     "\\Device\\HarddiskVolume??\\Windows\\System32\\services.exe",
      "?:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\*\\MsMpEng.exe",
      "?:\\Program Files\\Microsoft Security Client\\MsMpEng.exe",
      "?:\\Program Files*\\Windows Defender\\MsMpEng.exe",
@@ -24,6 +26,7 @@ process where event.action == "start" and
      "?:\\Program Files*\\Unity Client\\Unity.exe",
      "?:\\Windows\\System32\\wermgr.exe",
      "?:\\Windows\\System32\\svchost.exe",
+     "?:\\WINDOWS\\SysWOW64\\svchost.exe",
27   30        "\\Device\\VhdHardDisk*\\Windows\\System32\\services.exe",
28   31
29   32             "\\Device\\HarddiskVolume?\\Windows\\System32\\services.exe",
@@ -43,16 +46,17 @@ process where event.action == "start" and
43   46           process.Ext.token.integrity_level_name == "system") and
44   47      not (process.pe.original_file_name == "AsDVDLock.exe" and
45   48           process.executable : "?:\\Program Files (x86)\\ASUS\\ASUS Manager\\USB Lock\\svchost.exe") and
46      -   not (process.parent.executable : "?:\\Windows\\System32\\svchost.exe" and
47      -        process.parent.args : "ClipboardSvcGroup" and process.executable : "?:\\Windows\\System32\\svchost.exe")
     49 +   not (process.parent.executable : "?:\\Windows\\System32\\svchost.exe" and process.executable : "?:\\Windows\\System32\\svchost.exe")
48   50    '''
49   51
50      - optional_actions = []
51   52    [[actions]]
52   53    action = "kill_process"
53   54    field = "process.entity_id"
54   55    state = 0
55   56
     57 + [[optional_actions]]
     58 + action = "rollback"
     59 +
56   60    [[threat]]
57   61    framework = "MITRE ATT&CK"
58   62    [[threat.technique]]
```

5 🟩🟩🟩🟥🟥

behavior/rules/defense_evasion_potential_parent_process_p…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
```

```diff
 name = "Potential Parent Process PID Spoofing via MalSecLogon"
 os_list = ["windows"]
 reference = ["https://splintercod3.blogspot.com/p/the-hidden-side-of-seclogon-part-2.html"]
- version = "1.0.9"
+ version = "1.0.11"

 query = '''
 sequence with maxspan=1m
@@ -56,7 +56,8 @@ sequence with maxspan=1m
     not process.executable : ("?:\\Windows\\System32\\SpecopsClient\\SecuredBrowserNet\\*.exe", "?:\\Windows\\System32\\DriverStore\\FileRepository\\*\\SamsungSystemSupportOSD.exe") and
     not (process.executable : "?:\\Windows\\SysWOW64\\OneDriveSetup.exe" and process.parent.executable : "?:\\Windows\\SysWOW64\\OneDriveSetup.exe") and

-     not process.parent.executable : "?:\\Windows\\System32\\SpecopsClient\\SecuredBrowserNet\\SecuredBrowserDotNetLauncher.exe"
+     not process.parent.executable : "?:\\Windows\\System32\\SpecopsClient\\SecuredBrowserNet\\SecuredBrowserDotNetLauncher.exe" and
+     not process.executable : "?:\\Windows\\System32\\DriverStore\\FileRepository\\*.exe"
     ] by process.parent.Ext.real.entity_id
 '''

```

2 🟩🟥□□□

...ior/rules/defense_evasion_potential_privacy_control_by…

```diff
@@ -11,7 +11,7 @@ os_list = ["macos"]
 reference = [
     "https://blog.trendmicro.com/trendlabs-security-intelligence/xcsset-mac-malware-infects-
 xcode-projects-performs-uxss-attack-on-safari-other-browsers-leverages-zero-day-exploits/",
 ]
- version = "1.0.5"
+ version = "1.0.6"

 query = '''
 process where event.type == "start" and
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_potential_self_deletion_of…

```diff
@@ -9,7 +9,7 @@ license = "Elastic License v2"
 name = "Potential Self Deletion of a Running Executable"
 os_list = ["windows"]
 reference = ["https://github.com/LloydLabs/delete-self-poc"]
- version = "1.0.6"
+ version = "1.0.7"

 query = '''
 sequence by process.entity_id with maxspan=1m
@@ -20,12 +20,14 @@ sequence by process.entity_id with maxspan=1m
      file.name : "*:*" and not file.Ext.original.name : "*:*"  and file.size == 0] by file.Ext.original.name
 '''

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

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

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_process_executable_image_t…

```diff
@@ -13,13 +13,15 @@ license = "Elastic License v2"
 name = "Process Executable Image Tampering Attempt"
 os_list = ["windows"]
 reference = ["https://www.elastic.co/blog/process-ghosting-a-new-executable-image-tampering-attack"]
-version = "1.0.8"
+version = "1.0.9"
 
 query = '''
 process where event.action == "start" and
   process.Ext.defense_evasions : "Process Tampering: Image is locked for access" and
   not (process.code_signature.subject_name in ("Arcserve (USA) LLC", "CA") and process.code_signature.trusted == true and
-       process.executable : "?:\\Program Files\\CA\\*.exe")
+       process.executable : "?:\\Program Files\\CA\\*.exe") and
+  not (process.executable : "?:\\Windows\\System32\\esentutl.exe" and process.args : "/K" and
+       process.parent.executable : "?:\\Program Files\\CA\\SharedComponents\\ARCserve Backup\\UniAgent\\caagstart.exe")
 '''
 
 optional_actions = []
```

7 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_protected_process_light_by…

```diff
@@ -11,7 +11,7 @@ license = "Elastic License v2"
 name = "Protected Process Light Bypass via DLL Tampering"
 os_list = ["windows"]
 reference = ["https://googleprojectzero.blogspot.com/2018/08/windows-exploitation-tricks-exploiting.html"]
```

```
- version = "1.0.9"
+ version = "1.0.10"

  query = '''
  sequence by process.entity_id with maxspan=3s
@@ -35,7 +35,10 @@ sequence by process.entity_id with maxspan=3s
    not process.executable : "?:\\Program Files (x86)\\Common Files\\BattlEye\\BEService.exe" and
    /* potential services child processes */
    not (process.executable : "?:\\Windows\\System32\\services.exe" and dll.name : "*.exe") and
-   not dll.path : "?:\\Windows\\WinSxS\\Temp\\PendingDeletes\\$$DeleteMe*"]
+   not dll.path : "?:\\Windows\\WinSxS\\Temp\\PendingDeletes\\$$DeleteMe*" and
+   not (dll.path : "?:\\Program Files\\BackupClient\\DeviceLock\\DLDrvUserMode64.dll" and
+        dll.hash.sha256 : "ab813df167f8b6afe13f67231328f28fa3b0efeed8460f8b5e8a4228a8cded4e")
+   ]
  '''

  optional_actions = []
```

58 🟩🟩🟩🟩🟩

behavior/rules/defense_evasion_quarantine_attribute_delet…

```
@@ -0,0 +1,58 @@
+ [rule]
+ description = """
+ Identifies a potential Gatekeeper bypass from an unsigned or untrusted binary. In macOS, when applications or programs
+ are downloaded from the internet, there is a quarantine flag set on the file. This attribute is read by Apple's
+ Gatekeeper defense program at execution time. An adversary may disable this attribute to evade defenses.
+ """
+ id = "6e47b750-72c4-4af9-ad7b-0fc846df64d3"
+ license = "Elastic License v2"
+ name = "Quarantine Attribute Deleted via Untrusted Binary"
+ os_list = ["macos"]
+ version = "1.0.2"
+
+ query = '''
+ sequence with maxspan=1m
+  [process where event.action == "exec" and
+   (process.code_signature.trusted == false or process.code_signature.exists == false)] by process.entity_id
+  [process where event.action == "exec" and
+   process.args : "xattr" and
+   process.name : ("bash", "sh", "zsh", "xattr") and
+   (
+     (process.args : "com.apple.quarantine" and process.args : ("-d", "-w", "-?d", "-?w")) or
+     (process.args : "-c" and process.command_line :
+       (
+         "/bin/bash -c xattr -c *",
+         "/bin/zsh -c xattr -c *",
+         "/bin/sh -c xattr -c *"
+       )
+     )
+   )
+   ] by process.parent.entity_id
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1553"
+ name = "Subvert Trust Controls"
```

```
        44  + reference =
              "https://attack.mitre.org/techniques/T1553/"
        45  + [[threat.technique.subtechnique]]
        46  + id = "T1553.001"
        47  + name = "Gatekeeper Bypass"
        48  + reference =
              "https://attack.mitre.org/techniques/T1553/001/"
        49  +
        50  +
        51  +
        52  + [threat.tactic]
        53  + id = "TA0005"
        54  + name = "Defense Evasion"
        55  + reference =
              "https://attack.mitre.org/tactics/TA0005/"
        56  +
        57  + [internal]
        58  + min_endpoint_version = "8.1.0"
```

2 🟩🟥⬜⬜⬜

...es/defense_evasion_reading_or_modifying_downloaded_fil…

```
              @@ -9,7 +9,7 @@ license = "Elastic License v2"
   9     9      name = "Reading or Modifying Downloaded Files
                Database via SQLite Utility"
  10    10      os_list = ["macos"]
  11    11      reference = ["https://redcanary.com/blog/clipping-
                silver-sparrows-wings/"]
  12          - version = "1.0.6"
        12    + version = "1.0.7"
  13    13
  14    14      query = '''
  15    15      sequence with maxspan=30s
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_regsvr32_scriptlet_executi…

```
              @@ -7,7 +7,7 @@ id = "0524c24c-e45e-4220-b21a-
              abdba0c46c4d"
   7     7      license = "Elastic License v2"
   8     8      name = "Regsvr32 Scriptlet Execution"
   9     9      os_list = ["windows"]
  10          - version = "1.0.8"
```

```
+ version = "1.0.9"

  query = '''
  process where event.action == "start" and
@@ -35,12 +35,14 @@ process where event.action == "start" and
        not process.command_line : "*scrobj.dll*")
  '''

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

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

17 ■■■■□

behavior/rules/defense_evasion_regsvr32_with_unusual_argu…

```
@@ -7,7 +7,7 @@ id = "5db08297-bf72-49f4-b426-f405c2b01326"
  license = "Elastic License v2"
  name = "Regsvr32 with Unusual Arguments"
  os_list = ["windows"]
- version = "1.0.10"
+ version = "1.0.11"

  query = '''
  process where event.action == "start" and process.name : "regsvr32.exe" and
@@ -50,15 +50,26 @@ process where event.action == "start" and process.name : "regsvr32.exe" and
                "*BarTender Suite\\Codejock.DockingPane.x64.v15.3.1.ocx*") and
   not process.parent.executable : "?:\\Eaglesoft\\Shared Files\\OcxReg.exe" and
```

```diff
  not process.args : ("?:\\windows\\system32\\ChartFX.ClientServer.Data.dll", "?:\\Windows\\SysWOW64\\ChartFX.ClientServer.Data.dll") and
-  not (process.args : "?:\\Users\\*\\AppData\\Local\\Microsoft\\TeamsMeetingAddin\\*\\Microsoft.Teams.AddinLoader.dll" and process.args : "/i:user")
+  not (process.args : "?:\\Users\\*\\AppData\\Local\\Microsoft\\TeamsMeetingAddin\\*\\Microsoft.Teams.AddinLoader.dll" and process.args : "/i:user") and
+  not (process.args : "..\\*.dll" and process.working_directory : "?:\\Program Files\\LANDesk\\ManagementSuite\\Install Only Files\\") and
+  not (process.args : "..\\*.dll" and
+       descendant of
+        [process where event.action == "start" and
+         process.executable : ("?:\\Program Files\\LANDesk\\ManagementSuite\\Install Only Files\\LaunchApp.exe",
+                                "?:\\Program Files (x86)\\LANDesk\\ManagementSuite\\Install Only Files\\LaunchApp.exe")]) and
+  not (process.parent.name : "msiexec.exe" and process.parent.args : "-Embedding") and
+  not process.parent.executable : "C:\\Program Files\\LANDesk\\ManagementSuite\\Install Only Files\\LaunchApp.exe" and
+  not (process.executable : "?:\\Users\\*\\AppData\\Local\\Temp\\SSM*.tmp\\REGSVR32.EXE" and process.args : "?:\\WINDOWS\\system32\\*.dll")
 '''

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

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

```
     72  +
62   73    [[threat]]
63   74    framework = "MITRE ATT&CK"
64   75    [[threat.technique]]
```

6 🟩🟩🟩🟥

behavior/rules/defense_evasion_remote_file_execution_via_…

```
           @@ -11,7 +11,7 @@ reference = [
11   11        "https://lolbas-project.github.io/lolbas/Binaries/Msiexec/",
12   12        "https://www.guardicore.com/labs/purple-fox-rootkit-now-propagates-as-a-worm/",
13   13    ]
14       - version = "1.0.8"
     14  + version = "1.0.9"
15   15
16   16    query = '''
17   17    process where event.action == "start" and process.args_count <= 5 and
           @@ -26,12 +26,14 @@ process where event.action == "start" and process.args_count <= 5 and
26   26      not process.Ext.token.integrity_level_name == "system"
27   27    '''
28   28
29       - optional_actions = []
30   29    [[actions]]
31   30    action = "kill_process"
32   31    field = "process.entity_id"
33   32    state = 0
34   33
     34  + [[optional_actions]]
     35  + action = "rollback"
     36  +
35   37    [[threat]]
36   38    framework = "MITRE ATT&CK"
37   39    [[threat.technique]]
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_remote_msi_package_install…

```diff
@@ -11,7 +11,7 @@ reference = [
     "https://lolbas-project.github.io/lolbas/Binaries/Msiexec/",
     "https://www.guardicore.com/labs/purple-fox-rootkit-now-propagates-as-a-worm/",
 ]
-version = "1.0.6"
+version = "1.0.7"
 
 query = '''
 sequence with maxspan=1m
@@ -22,12 +22,14 @@ sequence with maxspan=1m
     not (process.executable : ("?:\\Program Files (x86)\\*.exe", "?:\\Program Files\\*.exe") and process.code_signature.trusted == true)] by process.parent.entity_id
 '''
 
-optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 1
 
+[[optional_actions]]
+action = "rollback"
+
 [[threat]]
 framework = "MITRE ATT&CK"
 [[threat.technique]]
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_renamed_autoit_scripts_int…

```diff
@@ -7,19 +7,21 @@ id = "99f2327e-871f-4b8a-ae75-d1c4697aefe4"
 license = "Elastic License v2"
 name = "Renamed AutoIt Scripts Interpreter"
```

```diff
  os_list = ["windows"]
- version = "1.0.6"
+ version = "1.0.7"

  query = '''
  process where event.action == "start" and
    process.pe.original_file_name : "AutoIt*.exe" and not process.name : "AutoIt*.exe"
  '''

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

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

6

behavior/rules/defense_evasion_renamed_third_party_admini…

```diff
@@ -4,7 +4,7 @@ id = "b707de5c-8e4d-4d2c-be22-b09a7e82b73f"
  license = "Elastic License v2"
  name = "Renamed Third Party Administrator Tools"
  os_list = ["windows"]
- version = "1.0.9"
+ version = "1.0.10"

  query = '''
  process where event.action == "start" and
@@ -21,12 +21,14 @@ process where event.action == "start" and
           "?:\\Program Files\\*.exe")
  '''

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

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

9

behavior/rules/defense_evasion_renamed_windows_automaton_…

```
@@ -9,7 +9,7 @@ license = "Elastic License v2"
  name = "Renamed Windows Automaton Script Interpreter"
  os_list = ["windows"]
  reference = ["https://blog.morphisec.com/explosive-new-mirrorblast-campaign-targets-financial-companies"]
- version = "1.0.6"
+ version = "1.0.7"

  query = '''
  process where event.action == "start" and
@@ -47,15 +47,18 @@ process where event.action == "start" and
     not (process.pe.original_file_name == "KIX32.EXE" and process.parent.command_line : "*\\netlogon\\*") and
     not (process.pe.original_file_name == "KIX32.EXE" and process.executable : ("C:\\kworking\\Bin\\RMMKSE.EXE", "C:\\kworking\\Bin\\RMMSSE.EXE")) and
     not (process.pe.original_file_name == "AutoHotkey.exe" and process.executable : "C:\\TCPU73\\Programm\\ClockTC\\ClockTC.exe" and
-         process.parent.executable : "C:\\TCPU73\\TOTALCMD.EXE")
+         process.parent.executable : "C:\\TCPU73\\TOTALCMD.EXE") and
+    not process.executable : "?:\\Program Files\\AutoHotkey\\SciTE\\InternalAHK.exe"
  '''

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

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

2 🟩🟥⬜⬜⬜

behavior/rules/defense_evasion_rundll32_regsvr32_loads_a_…

```
@@ -11,7 +11,7 @@ reference = [
      "https://blog.menasec.net/2021/05/hunting-for-suspicious-usage-of.html",
      "https://www.elastic.co/blog/hunting-for-persistence-using-elastic-security-part-2",
  ]
- version = "1.0.7"
+ version = "1.0.8"

  query = '''
  sequence with maxspan=5m
```

38 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_rundll32_with_unusual_argu…

```
@@ -7,7 +7,7 @@ id = "cfaf983e-1129-464c-b0aa-270f42e20d3d"
  license = "Elastic License v2"
  name = "RunDLL32 with Unusual Arguments"
  os_list = ["windows"]
- version = "1.0.10"
```

```
     10  + version = "1.0.11"
11   11
12   12    query = '''
13   13    process where event.action == "start" and process.name : "rundll32.exe" and
          @@ -42,7 +42,10 @@ process where event.action == "start" and process.name : "rundll32.exe" and
42   42                   "*\\M?-*.dll,_run@*",
43   43                   "*%TEMP%\\*.cpl*",
44   44                   "*\\Users\\*\\Downloads\\*.cpl*",
45       -                "*\\appdata\\roaming\\microsoft\\templates\\*,*") or
     45  +                "*\\appdata\\roaming\\microsoft\\templates\\*,*",
     46  +
     47  +                /* DLL exec by ordinal */
     48  +                "* #*", "*,#*") or
46   49          process.command_line like "*rUNdlL32.eXe*" or
47   50
48   51          /* fake Control_RunDLL export */
          @@ -56,7 +59,8 @@ process where event.action == "start" and process.name : "rundll32.exe" and
56   59
57   60          /* suspicious parent powershell args */
58   61          (process.parent.name : "powershell.exe" and
59       -         process.parent.args : ("-enc", "IEX", "*wp-content*", "*wp-admin*", "*wp-includes*", "*$*$*$*$*$*", "*^*^*^*^*^*^*^*^*^*", "*.replace*"))
     62  +         process.parent.args : ("-enc", "IEX", "*wp-content*", "*wp-admin*", "*wp-includes*", "*$*$*$*$*$*", "*^*^*^*^*^*^*^*^*^*", "*.replace*") and
     63  +         not (process.args : "UpdatePerUserSystemParameters" and process.args : "USER32.DLL"))
60   64          )
61   65
62   66        /* False Positives */
          @@ -65,38 +69,54 @@ process where event.action == "start" and process.name : "rundll32.exe" and
65   69      process.command_line :
66   70                 ("*JOBID=*",
              "*davclnt.dll,DavSetCookie*",
-             "*PhotoViewer.dll*ImageView_Fu*",
+             "*PhotoViewer*ImageView_Fu*",
              "*url.dll,FileProtocolHandler*",
              "*zzzzInvokeManagedCustomActionOutOfProc*",
              "*,DeferredDelete*",
              "*:\\WINDOWS\\system32\\spool\\*",
              "*:\\Program Files (x86)\\*",
              "*:\\Program Files\\*",
              /* Issue #282 - FP */
-             "*cryptext.dll,CryptExtAddPFX*",
+             "*cryptext*CryptExt*",
              "*dfshim.dll*ShOpenVerbShortcut*",
              "*\\Documents\\DocuShare\\*",

              /* Issue #371 */
              "*ndfapi.dll,NdfRunDllDiagnoseWithAnswerFile*",
              "*FirewallControlPanel.dll,ShowNotificationDialog*",
              "*--type=renderer*--log-file=*",
-             "*--lang=*--log-file=*") and not
+             "*--lang=*--log-file=*",
+
+             "*shell32*OpenAs_RunDLL*",
+             "*dfshim*ShOpenVerbExtension*",
+             "*printui*PrintUIEntry*",
+             "*mshtml*PrintHTML*",
+             "*shell32*#44*",
+             "*shell32.dll*ShellExec_RunDLL*#*",
+             "*EDGEHTML*#*"
+             ) and not
+
     (process.command_line : "*.tmp*" and
-     process.parent.executable : ("?:\\Windows\\System32\\msiexec.exe", "?:\\Windows\\System32\\msiexec.exe") and
+     process.parent.executable : ("?:\\Windows\\System32\\msiexec.exe", "?:\\Windows\\SysWOW64\\msiexec.exe") and
      process.parent.args : "-Embedding") and
    not process.args : "?:\\ProgramData\\Parallels\\RASLogs\\tmp*.tmp,Stop
```

```diff
 Memshell" and
   not (process.args : "?:\\Users\\Public\\IBM\\ClientSolutions\\Start_Programs\\Windows_*\\acsnative.dll*" and
        process.parent.executable : "?:\\Users\\Public\\IBM\\ClientSolutions\\Start_Programs\\Windows_*\\acslaunch_*.exe") and
-  not process.parent.executable : ("?:\\Program Files\\Common Files\\BullGuardInstall\\BullGuard*.exe", "?:\\Program Files (x86)\\Intuit\\QuickBooks 20??\\QBW??.EXE")
+  not process.parent.executable :
+                ("?:\\Program Files\\Common Files\\BullGuardInstall\\BullGuard*.exe",
+                 "?:\\Program Files (x86)\\Intuit\\QuickBooks 20??\\QBW??.EXE",
+                 "?:\\Program Files\\Intuit\\QuickBooks 2022\\QBW.EXE") and
+  not (user.name : "user" and process.args : "file.dll,#*")
 '''
 
-optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 0
 
+[[optional_actions]]
+action = "rollback"
+
 [[threat]]
 framework = "MITRE ATT&CK"
 [[threat.technique]]
```

2 🟩🟥

behavior/rules/defense_evasion_script_execution_via_macos…

```diff
@@ -12,7 +12,7 @@ reference = [
     "https://kyle-bailey.medium.com/detecting-macos-gatekeeper-bypass-cve-2021-30657-cc986a9bc751",
     "https://objective-see.com/blog/blog_0x64.html",
 ]
- version = "1.0.9"
+ version = "1.0.10"
 
 query = '''
 sequence with maxspan=5m
```

12 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_script_execution_via_micro…

```diff
@@ -7,7 +7,7 @@ id = "f0630213-c4c4-4898-9514-746395eb9962"
 license = "Elastic License v2"
 name = "Script Execution via Microsoft HTML Application"
 os_list = ["windows"]
- version = "1.0.10"
+ version = "1.0.11"
 
 query = '''
 process where event.action == "start" and
@@ -52,15 +52,21 @@ process where event.action == "start" and
      /* Execution of HTA file from mounted ISO files */
      (process.pe.original_file_name : "mshta.exe" and
       process.parent.name : ("explorer.exe", "cmd.exe", "powershell.exe") and process.working_directory : "?:\\")
-    )
+    ) and
+
+  /* FPs */
+  not (process.parent.executable : "C:\\Windows\\SysWOW64\\runonce.exe" and
+       process.args : "\"& 'C:\\System.sav\\util\\HpseuHostLauncher.ps1'\"\", 0 : window.close)")
 '''
 
```

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

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

6 🟩🟩🟩🟥

behavior/rules/defense_evasion_script_execution_via_msxsl…

```
@@ -8,20 +8,22 @@ license = "Elastic License v2"
  name = "Script Execution via MSXSL"
  os_list = ["windows"]
  reference = ["https://lolbas-project.github.io/lolbas/OtherMSBinaries/Msxsl/"]
- version = "1.0.8"
+ version = "1.0.9"

  query = '''
  sequence by process.entity_id with maxspan=1m
   [process where event.action == "start" and process.pe.original_file_name == "msxsl.exe"]
   [library where dll.name : ("scrobj.dll", "jscript.dll", "vbscript.dll", "jscript9.dll")]
  '''

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

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

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_scriptlet_execution_via_cm…

```
@@ -8,20 +8,22 @@ license = "Elastic License v2"
  name = "Scriptlet Execution via CMSTP"
  os_list = ["windows"]
  reference = ["https://lolbas-project.github.io/lolbas/Binaries/Cmstp/"]
- version = "1.0.8"
+ version = "1.0.9"

  query = '''
  sequence by process.entity_id with maxspan=1m
   [process where event.action == "start" and process.pe.original_file_name == "CMSTP.EXE"]
   [library where dll.name : "scrobj.dll"]
  '''

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

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

2 🟩🟥⬜⬜⬜

behavior/rules/defense_evasion_scriptlet_execution_via_ru…

```
@@ -11,7 +11,7 @@ reference = [
      "https://lolbas-project.github.io/lolbas/Libraries/Ieadvpack/",
      "https://lolbas-project.github.io/lolbas/Libraries/Advpack/",
  ]
```

```
- version = "1.0.8"
+ version = "1.0.9"

  query = '''
  sequence by process.entity_id with maxspan=1m
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_scriptlet_proxy_execution_…

```
  @@ -8,7 +8,7 @@ license = "Elastic License v2"
  name = "Scriptlet Proxy Execution via PubPrn"
  os_list = ["windows"]
  reference = ["https://lolbas-project.github.io/lolbas/Scripts/Pubprn/"]
- version = "1.0.8"
+ version = "1.0.9"

  query = '''
  process where event.action == "start" and
  @@ -17,12 +17,14 @@ process where event.action == "start" and
   process.command_line : ("*localhost*script:http*", "*127.0.0.*script:http*")
  '''

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

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

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_shadow_copy_service_disabl…

```
@@ -7,20 +7,22 @@ id = "b2409cd4-3b23-4b2d-82e4-bbb25594999a"
  license = "Elastic License v2"
  name = "Shadow Copy Service Disabled via Registry Modification"
  os_list = ["windows"]
- version = "1.0.4"
+ version = "1.0.5"

  query = '''
  registry where
   registry.path : "HKLM\\SYSTEM\\ControlSet*\\Services\\VSS\\Start" and registry.data.strings : "4" and
   not process.executable : "?:\\Windows\\System32\\services.exe" and process.executable : "?*"
  '''

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

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

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_solarmarker_backdoor_regis…

```
@@ -12,7 +12,7 @@ reference = [
      "https://www.ired.team/offensive-security/persistence/hijacking-default-file-extension",
      "https://www.binarydefense.com/mars-deimos-solarmarker-jupyter-infostealer-part-1/",
  ]
- version = "1.0.5"
```

```
     15  + version = "1.0.6"
16   16
17   17    query = '''
18   18    sequence by process.entity_id with maxspan=1m
           @@ -25,12 +25,14 @@ sequence by process.entity_id with maxspan=1m
25   25      registry.data.strings : "*PowerShell*" and
           length(registry.data.strings) >= 200]
26   26    '''
27   27
28       - optional_actions = []
29   28    [[actions]]
30   29    action = "kill_process"
31   30    field = "process.parent.entity_id"
32   31    state = 0
33   32
     33  + [[optional_actions]]
     34  + action = "rollback"
     35  +
34   36    [[threat]]
35   37    framework = "MITRE ATT&CK"
36   38    [[threat.technique]]
```

5

behavior/rules/defense_evasion_suspicious_bitsadmin_activ…

```
           @@ -9,7 +9,7 @@ license = "Elastic License v2"
 9    9    name = "Suspicious Bitsadmin Activity"
10   10    os_list = ["windows"]
11   11    reference = ["https://www.elastic.co/blog/hunting-for-persistence-using-elastic-security-part-2"]
12       - version = "1.0.8"
     12  + version = "1.0.9"
13   13
14   14    query = '''
15   15    process where event.action == "start" and
           @@ -79,7 +79,8 @@ process where event.action == "start" and
79   79          "powershell.exe",
80   80          "pwsh.exe",
81   81          "cmd.exe"
82       -     )])
     82  +     )]) and
```

```
+    not (process.args : "https://dl.duosecurity.com/*" and process.parent.args : "?:\\ProgramData\\NinjaRMMAgent\\scripting\\*")
 '''

 optional_actions = []
```

66

behavior/rules/defense_evasion_suspicious_control_panel_d…

```
@@ -0,0 +1,66 @@
+[rule]
+description = """
+Identifies DLL load of an unsigned or untrusted Control Panel Item by the Explorer process. Adversaries may load a
+malicious DLL when Control Panel is executed via setting the CPLs subkey to the payload path.
+"""
+id = "1dbf6ac3-540a-4214-8173-9aa93232da38"
+license = "Elastic License v2"
+name = "Suspicious Control Panel DLL Loaded by Explorer"
+os_list = ["windows"]
+reference = ["https://docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/hh127454(v=vs.85)"]
+version = "1.0.3"
+
+query = '''
+sequence  with maxspan = 5s
+
+ [library where process.name : "explorer.exe" and
+  (dll.code_signature.trusted == false or dll.code_signature.exists == false) and
+  not dll.path :
+          ("?:\\Program Files\\*",
+           "?:\\Program Files (x86)\\*",
+           "?:\\Windows\\System32\\*",
+           "?:\\Windows\\SysWOW64\\*",
+           "?:\\Windows\\assembly\\*")] by process.entity_id
+
+  [process where event.action == "start" and process.parent.name : "explorer.exe" and
+
+   /* CLSID_ControlPanelProcessExplorerHost */
+   process.parent.args : "/factory,{5BD95610-9434-43C2-886C-57852CC8A120}" and
+
+   /* false positives */
+   not (process.name : "rundll32.exe" and
+        process.args :
+             ("printui.dll,PrintUIEntryDPIAware",
+ "?:\\WINDOWS\\system32\\spool\\DRIVERS\\*PrintJobStatus",
+              "fdprint,InvokeTask")) and
+   not (process.name : "mmc.exe" and process.args : "?:\\windows\\system32\\devmgmt.msc") and
+   not process.executable : ("?:\\windows\\system32\\DevicePairingWizard.exe", "?:\\Windows\\System32\\spool\\drivers\\x64\\3\\E_YARNYWE.EXE")
+   ] by process.parent.entity_id
+ '''
+
+ optional_actions = []
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 1
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1218"
+ name = "System Binary Proxy Execution"
+ reference = "https://attack.mitre.org/techniques/T1218/"
+ [[threat.technique.subtechnique]]
+ id = "T1218.002"
+ name = "Control Panel"
+ reference = "https://attack.mitre.org/techniques/T1218/002/"
+
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.16.0"
```

2 🟩🟥

behavior/rules/defense_evasion_suspicious_execution_from_…

```
@@ -7,7 +7,7 @@ id = "42d2bbfb-a2fb-4327-b701-89ead6044ca1"
  license = "Elastic License v2"
  name = "Suspicious Execution from a Mounted Device"
  os_list = ["windows"]
- version = "1.0.10"
+ version = "1.0.11"

  query = '''
  sequence with maxspan=1m
```

6 🟩🟩🟩🟥

behavior/rules/defense_evasion_suspicious_execution_via_m…

```
@@ -11,7 +11,7 @@ reference = [
      "https://lolbas-project.github.io/lolbas/Binaries/Msiexec/",
      "https://www.guardicore.com/labs/purple-fox-rootkit-now-propagates-as-a-worm/",
  ]
- version = "1.0.4"
+ version = "1.0.5"

  query = '''
  process where event.action == "start" and
@@ -41,7 +41,9 @@ process where event.action == "start" and
    not (process.parent.executable : "?:\\Users\\*\\AppData\\Local\\Temp\\*" and process.parent.args_count >= 2 and
         process.args : "?:\\Users\\*\\AppData\\Local\\Temp\\*\\*.msi") and

-   not process.args : ("?:\\Program Files (x86)\\*", "?:\\Program Files\\*")
+   not process.args : ("?:\\Program Files (x86)\\*", "?:\\Program Files\\*") and
+
+   not (process.parent.name : "msiexec.exe" and process.parent.args : "-Embedding")
  '''

  optional_actions = []
```

2 🟩🟥⬜⬜⬜

behavior/rules/defense_evasion_suspicious_imageload_from_…

```
@@ -7,7 +7,7 @@ id = "779b9502-7912-4773-95a1-51cd702a71c8"
  license = "Elastic License v2"
  name = "Suspicious ImageLoad from an ISO Mounted Device"
  os_list = ["windows"]
- version = "1.0.6"
+ version = "1.0.7"

  query = '''
  sequence by process.entity_id with maxspan=1m
```

46 🟩🟩🟩🟩🟩

...ior/rules/defense_evasion_suspicious_imageload_via_odb…

```
@@ -0,0 +1,46 @@
+ [rule]
+ description = """
+ Identifies abuse of the ODBC Driver Configuration Program to load an arbitrary DLL. This behavior is used as a defense
+ evasion technique to blend-in malicious activity with legitimate Windows software.
+ """
+ id = "1faebe83-38d7-4390-b6bd-9c6b851e47c4"
+ license = "Elastic License v2"
+ name = "Suspicious ImageLoad via ODBC Driver Configuration Program"
+ os_list = ["windows"]
+ reference = ["https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/"]
+ version = "1.0.2"
+
+ query = '''
+ process where event.action == "start" and
+   (process.pe.original_file_name == "odbcconf.exe" or process.name : "odbcconf.exe") and
+    process.args : ("-a", "-f", "/a", "/f")
+ '''
+
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[optional_actions]]
+ action = "rollback"
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1218"
+ name = "System Binary Proxy Execution"
+ reference = "https://attack.mitre.org/techniques/T1218/"
+ [[threat.technique.subtechnique]]
+ id = "T1218.008"
+ name = "Odbcconf"
+ reference = "https://attack.mitre.org/techniques/T1218/008/"
+
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.15.0"
```

40

behavior/rules/defense_evasion_suspicious_imageload_via_w…

```
@@ -0,0 +1,40 @@
+ [rule]
+ description = """
+ Identifies abuse of the Microsoft CertOC utility to load an arbitrary DLL. This behavior is used as a defense evasion
+ technique to blend-in malicious activity with legitimate Windows software.
+ """
+ id = "6fcbf73f-4413-4689-be33-61b0d6bd0ffc"
+ license = "Elastic License v2"
+ name = "Suspicious ImageLoad via Windows CertOC"
+ os_list = ["windows"]
+ reference = ["https://lolbas-project.github.io/lolbas/Binaries/Certoc/"]
+ version = "1.0.2"
+
+ query = '''
+ process where event.action == "start" and
+   (process.pe.original_file_name == "CertOC.exe" or process.name : "certoc.exe") and process.args : "-LoadDLL"
+ '''
+
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[optional_actions]]
+ action = "rollback"
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1218"
+ name = "System Binary Proxy Execution"
+ reference = "https://attack.mitre.org/techniques/T1218/"
```

```
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.15.0"
```

6 🟩🟩🟩🟥⬜

...ior/rules/defense_evasion_suspicious_imageload_via_win…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
  name = "Suspicious ImageLoad via Windows Update Auto Update Client"
  os_list = ["windows"]
  reference = ["https://dtm.uk/wuauclt/"]
- version = "1.0.6"
+ version = "1.0.7"

  query = '''
  sequence by process.entity_id with maxspan=1m
@@ -27,12 +27,14 @@ sequence by process.entity_id with maxspan=1m
  "?:\\ProgramData\\Symantec\\Symantec Endpoint Protection\\*.dll"))]
  '''

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

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

2 🟩🟥⬜⬜⬜

behavior/rules/defense_evasion_suspicious_ntdll_image_loa…

```diff
@@ -7,7 +7,7 @@ id = "5eb3c0b3-8d11-439d-b26d-d7623c5b3723"
  license = "Elastic License v2"
  name = "Suspicious NTDLL Image Load"
  os_list = ["windows"]
- version = "1.0.4"
+ version = "1.0.5"

  query = '''
  sequence by process.entity_id with maxspan=1m
```

23 🟩🟩🟥🟥⬜

behavior/rules/defense_evasion_suspicious_parent_child_re…

```diff
@@ -7,7 +7,7 @@ id = "18a26e3e-e535-4d23-8ffa-a3cdba56d16e"
  license = "Elastic License v2"
  name = "Suspicious Parent-Child Relationship"
  os_list = ["windows"]
- version = "1.0.5"
+ version = "1.0.7"

  query = '''
  process where event.action == "start" and
@@ -21,18 +21,16 @@ process where event.action == "start" and
      */
    (process.name : "autochk.exe" and not process.parent.name : "smss.exe") or

-   (process.name : ("consent.exe", "RuntimeBroker.exe", "TiWorker.exe") and not process.parent.name : ("svchost.exe", "RuntimeBroker.exe") and
+   (process.name : ("consent.exe", "RuntimeBroker.exe") and not process.parent.name : ("svchost.exe", "RuntimeBroker.exe") and
     not process.parent.executable : "?:\\Program Files\\ThreatLocker\\threatlockerconsent.exe") or
-   (process.name : "SearchIndexer.exe" and not process.parent.name : "services.exe") or
-   (process.name : "dllhost.exe" and not process.parent.name : ("services.exe", "svchost.exe") and
-     not process.parent.executable : ("?:\\Program Files (x86)\\*", "?:\\Program Files\\*")) or
-   (process.name : "smss.exe" and not process.parent.name : ("System", "smss.exe")) or
+   (process.name : "SearchIndexer.exe" and not process.parent.name : ("services.exe", "SearchIndexer.exe")) or
+   (process.name : "smss.exe" and not process.parent.name : ("System", "smss.exe", "sihost.exe")) or
    (process.name : "wininit.exe" and not process.parent.name : "smss.exe") or
-   (process.name : ("lsass.exe", "LsaIso.exe") and not process.parent.name : "wininit.exe") or
+   (process.name : ("lsass.exe", "LsaIso.exe") and not process.parent.name : ("wininit.exe", "lsass.exe")) or
    (process.name : "services.exe" and not process.parent.name : "wininit.exe") or
    (process.name : "spoolsv.exe" and not process.parent.name : ("services.exe", "spoolsv.exe")) or
    (process.name : "taskhost.exe" and not process.parent.name : ("services.exe", "svchost.exe")) or
-   (process.name : "taskhostw.exe" and not process.parent.name : ("services.exe", "svchost.exe")) or
+   (process.name : "taskhostw.exe" and not process.parent.name : ("services.exe", "svchost.exe", "taskhostw.exe")) or
    (process.name : ("wmiprvse.exe", "wsmprovhost.exe", "winrshost.exe") and not process.parent.name : "svchost.exe") or
    (process.name : "sihost.exe" and not process.parent.name : ("svchost.exe", "sihost.exe")) or
    (process.name : ("winlogon.exe", "csrss.exe", "SearchProtocolHost.exe", "fontdrvhost.exe", "userinit.exe", "dwm.exe", "LogonUI.exe", "taskhostw.exe") and
@@ -54,15 +52,20 @@ process where event.action == "start" and
                    "?:\\Program Files (x86)\\Adobe\\Acrobat DC\\Acrobat\\*\\AcroCEF.exe",
                    "?:\\Program Files (x86)\\Adobe\\Acrobat Reader DC\\Reader\\AcroCEF\\RdrCEF.exe",
                    "?:\\Program Files\\Adobe\\Acrobat Reader DC\\Reader\\AcroCEF\\RdrCEF.exe") and
-   not (process.name : "dwm.exe" and process.code_signature.subject_name == "Teramind Inc." and process.code_signature.trusted == true)
+   not (process.name : "dwm.exe" and process.code_signature.subject_name == "Teramind Inc." and process.code_signature.trusted == true) and
+   not (process.name : "SearchProtocolHost.exe" and process.parent.name : "rundll32.exe" and process.parent.args : "AppXDeploymentExtensions.OneCore.dll,ShellRefresh") and
+   not (process.parent.executable : "?:\\Windows\\System32\\smss.exe" and process.parent.args : "-SpecialSession") and
+   not (process.parent.executable : "?:\\Program Files\\Sandboxie\\SandboxieDcomLaunch.exe" and process.name : "RuntimeBroker.exe")
'''

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

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

```
[[threat.technique]]
```

52 🟩🟩🟩🟩🟩

behavior/rules/defense_evasion_suspicious_troubleshooting…

```
@@ -0,0 +1,52 @@
+ [rule]
+ description = """
+ Identifies the execution of the Microsoft Diagnostic Wizard to open a diagcab file from a suspicious path and with an
+ unusual parent process. This may indicate an attempt to execute malicious Troubleshooting Pack Cabinet files.
+ """
+ id = "d18721f0-dce0-4bbc-a56a-06ea511b025e"
+ license = "Elastic License v2"
+ name = "Suspicious Troubleshooting Pack Cabinet Execution"
+ os_list = ["windows"]
+ reference = ["https://irsl.medium.com/the-trouble-with-microsofts-troubleshooters-6e32fc80b8bd"]
+ version = "1.0.3"
+
+ query = '''
+ process where event.action == "start" and
+  (process.name : "msdt.exe" or process.pe.original_file_name == "msdt.exe") and process.args : "/cab" and
+
+  process.parent.name : ("firefox.exe", "chrome.exe", "msedge.exe", "explorer.exe", "brave.exe", "whale.exe", "browser.exe",
+    "dragon.exe", "vivaldi.exe", "opera.exe", "iexplore", "firefox.exe", "waterfox.exe", "iexplore.exe", "winrar.exe",
+    "winrar.exe", "7zFM.exe", "outlook.exe", "winword.exe", "excel.exe") and
+
+  process.args : ("?:\\Users\\*\\Downloads\\*",
+                  "\\\\*",
+                  "?:\\Users\\*\\Content.Outlook\\*",
+                  "?:\\Users\\Public\\*",
+                  "?:\\Users\\*\\AppData\\*",
+                  "http*",
+                  "ftp://*")
+ '''
+
+ [[actions]]
+ action = "kill_process"
+ field = "process.entity_id"
+ state = 0
+
+ [[optional_actions]]
+ action = "rollback"
+
+ [[threat]]
+ framework = "MITRE ATT&CK"
+ [[threat.technique]]
+ id = "T1218"
+ name = "System Binary Proxy Execution"
+ reference = "https://attack.mitre.org/techniques/T1218/"
+
+
+ [threat.tactic]
+ id = "TA0005"
+ name = "Defense Evasion"
+ reference = "https://attack.mitre.org/tactics/TA0005/"
+
+ [internal]
+ min_endpoint_version = "7.15.0"
```

6 🟩🟩🟩🟥⬜

...or/rules/defense_evasion_suspicious_windows_defender_e…

```
@@ -10,7 +10,7 @@ os_list = ["windows"]
  reference = [
      "https://docs.microsoft.com/en-us/powershell/module/defender/add-mppreference?view=windowsserver2019-ps",
  ]
- version = "1.0.5"
+ version = "1.0.6"

  query = '''
  sequence with maxspan=1m
```

```diff
@@ -34,12 +34,14 @@ sequence with maxspan=1m
    process.args : ("-ExclusionPath", "-DisableRealtimeMonitoring", "-DisableScriptScanning", "-DisableArchiveScanning")] by process.parent.entity_id
 '''
 
- optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 0
 
+ [[optional_actions]]
+ action = "rollback"
+
 [[threat]]
 framework = "MITRE ATT&CK"
 [[threat.technique]]
```

2 🟩🟥⬜⬜⬜

behavior/rules/defense_evasion_suspicious_windows_defende…

```diff
@@ -7,7 +7,7 @@ id = "56751d32-cded-41ad-a273-e6860820c4c3"
 license = "Elastic License v2"
 name = "Suspicious Windows Defender Registry Modification"
 os_list = ["windows"]
- version = "1.0.5"
+ version = "1.0.6"
 
 query = '''
 sequence by process.entity_id with maxspan=5s
```

14 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_suspicious_windows_explore…

```diff
@@ -7,7 +7,7 @@ id = "f8ec5b76-53cf-4989-b451-7d16abec7298"
 license = "Elastic License v2"
 8   8      name = "Suspicious Windows Explorer Execution"
 9   9      os_list = ["windows"]
10        - version = "1.0.4"
    10    + version = "1.0.6"
11  11
12  12      query = '''
13  13      process where event.action == "start" and
            @@ -16,13 +16,17 @@ process where event.action == "start" and
16  16         /* miners injecting into Explorer */
17  17          process.args : ("etc", "easyminer*", "ton", "Rg", "eth", "Toncoin", "mmrig", "--cinit-*", "pool.*", "--coin=*", "--cpu-*") or
18  18
    19    +     /* excute a malicious DLL by clsid */
    20    +     (process.args : "shell:::{*" and not process.args : "shell:::{52205fd8-5dfb-447d-801a-d0b52f2e83e1}") or
    21    +
19  22          /* Explorer with unusual process arg length */
20  23          (length(process.command_line) >= 200 and process.args_count == 3 and not process.args : "/select*") or
21  24
22  25         /* commonly abused lolbin as parent */
23        -    (process.parent.name : ("rundll32.exe", "regsvr32.exe", "powershell.exe", "cmd.exe", "mshta.exe") and process.parent.args_count >= 2 and
    26    +    (process.parent.name : ("rundll32.exe", "regsvr32.exe", "powershell.exe", "mshta.exe") and process.parent.args_count >= 2 and
24  27          process.args_count == 1 and
25        -     not (process.parent.name : "rundll32.exe" and process.parent.args : "?:\\Windows\\System32\\SHELL32.dll,RunAsNewUser_RunDLL")) or
    28    +     not (process.parent.name : "rundll32.exe" and
    29    +          process.parent.args : ("?:\\Windows\\System32\\SHELL32.dll,RunAsNewUser_RunDLL", "AppXDeploymentExtensions.OneCore.dll,ShellRefresh"))) or
26  30
27  31          /* unusual parent process by path */
```

```
28   32        (process.parent.executable : ("?:\\Users\\*\\AppData\\*", "?:\\Users\\Public\\*", "?:\\ProgramData\\*", "?:\\Windows\\Microsoft.NET\\*.exe") and
@@ -38,7 +42,9 @@ process where event.action == "start" and
38   42        (process.executable : "?:\\Windows\\SysWOW64\\explorer.exe" and process.parent.executable : "?:\\Windows\\explorer.exe" and process.args_count == 1) or
39   43
40   44         /* Indirect Command Execution via Explorer */
41      -      (process.name : "explorer.exe" and process.command_line : "*.exe *.exe*" and not process.args : "*/select*" and not process.command_line : "*:\\Program Files*")
     45 +      (process.name : "explorer.exe" and process.command_line : "*.exe *.exe*" and not process.args : "*/select*" and not process.command_line : "*:\\Program Files*") and
     46 +
     47 +      not process.parent.executable : "?:\\Program Files (x86)\\BleachBit\\bleachbit.exe"
42   48        )
43   49   '''
44   50
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_suspicious_windows_lua_scr…

```
@@ -7,7 +7,7 @@ id = "8f237d98-1825-4c27-a5cd-e38bde70882a"
 7    7   license = "Elastic License v2"
 8    8   name = "Suspicious Windows LUA Script Execution"
 9    9   os_list = ["windows"]
10      - version = "1.0.5"
     10 + version = "1.0.6"
11   11
12   12   query = '''
13   13   sequence by process.entity_id with maxspan=1m
@@ -17,12 +17,14 @@ sequence by process.entity_id with maxspan=1m
```

```diff
  [network where event.action == "connection_attempted"]
 '''
 
- optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 1
 
+ [[optional_actions]]
+ action = "rollback"
+
 [[threat]]
 framework = "MITRE ATT&CK"
 [[threat.technique]]
```

6

behavior/rules/defense_evasion_suspicious_wmic_xsl_script…

```diff
@@ -8,7 +8,7 @@ id = "18371ec4-ee2f-465b-8757-ee726914006c"
 license = "Elastic License v2"
 name = "Suspicious WMIC XSL Script Execution"
 os_list = ["windows"]
- version = "1.0.9"
+ version = "1.0.10"
 
 query = '''
 sequence by process.entity_id with maxspan=2m
@@ -31,12 +31,14 @@ sequence by process.entity_id with maxspan=2m
 [library where dll.name : ("jscript.dll", "vbscript.dll")]
 '''
 
- optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 0
 
+ [[optional_actions]]
```

```
     40 + action = "rollback"
     41 +
40   42   [[threat]]
41   43   framework = "MITRE ATT&CK"
42   44   [[threat.technique]]
```

20 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_unusual_dll_extension_load…

```
@@ -7,7 +7,7 @@ id = "76da5dca-ffe5-4756-85ba-3ac2e6ccf623"
 7    7   license = "Elastic License v2"
 8    8   name = "Unusual DLL Extension Loaded by Rundll32 or Regsvr32"
 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=1s
@@ -17,24 +17,32 @@ sequence by process.entity_id with maxspan=1s
17   17     not (process.name : "regsvr32.exe" and process.args : "?:\\Program Files (x86)\\DesktopCentral_Agent\\bin\\BSPHelperObject.dll")
18   18     ]
19   19    [library where process.name : ("rundll32.exe", "regsvr32.exe") and
20      -   not dll.name : ("*.dll", "*.cpl", "*.tmp", "*.exe", "*.tlb") and
     20 +   not dll.name : ("*.dll", "*.cpl", "*.tmp", "*.exe", "*.tlb", "*.scr", "*.dll.mui", "*.ime", "*.tsp", "*.rbf") and
21   21     not (dll.name : ("*.ocx", "*.ax") and process.name : "regsvr32.exe") and
22   22     not dll.code_signature.trusted == true and
23   23     not dll.path : ("?:\\Windows\\System32\\winspool.drv",
24   24                     "?:\\Windows\\SysWOW64\\winspool.drv",
25      -                   "?:\\Windows\\System32\\liunt.ime",
-                        "?:\\Windows\\SysWOW64\\liunt.ime",
+                        "?:\\Windows\\System32\\*.ime",
+                        "?:\\Windows\\SysWOW64\\*.ime",
                         "?:\\Windows\\System32\\spool\\drivers\\*",
                         "?:\\Program Files (x86)\\*",
-                        "?:\\Program Files\\*")]
+                        "?:\\Program Files\\*",
+                        "?:\\Windows\\SysWOW64\\*.bpl") and
+   not dll.hash.sha256 : ("cfd375eb124d1fba73f2d46705a43ed30e8aaadca7627bab7718f674fb82df38",
+  "4af03da6cda5d673725b671dbb3fccfc4badc0651af9065216bdcddb0fef7adf",
+  "bf03c44224a2932e4c12ce02e12059f5c37b7d7ebfbbe4f2603b324c368ba2b9",
+  "9e318b33d7ae4ece36cdcd345ff6815816f9efcaf9a9b943999c6d80ae043e91")
+   ]
  '''

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

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

6 🟩🟩🟩🟥□

behavior/rules/defense_evasion_unusual_network_connection…

```
@@ -7,7 +7,7 @@ id = "2e708541-c6e8-4ded-923f-78a6c160987e"
```

```
 7     7      license = "Elastic License v2"
 8     8      name = "Unusual Network Connection via RunDLL32"
 9     9      os_list = ["windows"]
10          - version = "1.0.9"
      10    + version = "1.0.10"
11    11
12    12      query = '''
13    13      sequence by process.entity_id with maxspan=5m
              @@ -18,12 +18,14 @@ sequence by process.entity_id
              with maxspan=5m
18    18        [network where event.action ==
              "connection_attempted" and process.name :
              "rundll32.exe"]
19    19      '''
20    20
21          - optional_actions = []
22    21      [[actions]]
23    22      action = "kill_process"
24    23      field = "process.entity_id"
25    24      state = 1
26    25
      26    + [[optional_actions]]
      27    + action = "rollback"
      28    +
27    29      [[threat]]
28    30      framework = "MITRE ATT&CK"
29    31      [[threat.technique]]
```

6 🟩🟩🟩🟥⬜

behavior/rules/defense_evasion_windows_error_manager_repo…

```
              @@ -8,7 +8,7 @@ id = "3d16f5f9-da4c-4b15-a501-
              505761b75ca6"
 8     8      license = "Elastic License v2"
 9     9      name = "Windows Error Manager/Reporting
              Masquerading"
10    10      os_list = ["windows"]
11          - version = "1.0.8"
      11    + version = "1.0.9"
12    12
13    13      query = '''
14    14      sequence by process.entity_id with maxspan=5m
```

```diff
@@ -17,12 +17,14 @@ sequence by process.entity_id with maxspan=5m
   [network where event.action == "connection_attempted" and process.name : ("wermgr.exe", "WerFault.exe")]
 '''
 
- optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 0
 
+[[optional_actions]]
+action = "rollback"
+
 [[threat]]
 framework = "MITRE ATT&CK"
 [[threat.technique]]
```

6 🟩🟩🟩🟥⬜

...rules/defense_evasion_windows_firewall_exception_list_…

```diff
@@ -10,7 +10,7 @@ os_list = ["windows"]
 reference = [
     "https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/netsh-advfirewall-firewall-control-firewall-behavior",
 ]
-version = "1.0.9"
+version = "1.0.10"
 
 query = '''
 sequence with maxspan=1m
@@ -23,12 +23,14 @@ sequence with maxspan=1m
    ] by process.parent.entity_id
 '''
 
-optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
 state = 0
```

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

2 🟩🟥⬜⬜⬜

behavior/rules/defense_evasion_windows_installer_with_sus…

```diff
@@ -8,7 +8,7 @@ license = "Elastic License v2"
 name = "Windows Installer with Suspicious Properties"
 os_list = ["windows"]
 reference = ["https://lolbas-project.github.io/lolbas/Binaries/Msiexec/"]
-version = "1.0.4"
+version = "1.0.5"
 
 query = '''
 sequence with maxspan=1m
```

9 🟩🟩🟩🟥⬜

behavior/rules/discovery_external_ip_address_discovery_vi…

```diff
@@ -7,7 +7,7 @@ id = "51894221-7657-4b56-9406-e080e19ad159"
 license = "Elastic License v2"
 name = "External IP Address Discovery via a Trusted Program"
 os_list = ["windows"]
-version = "1.0.8"
+version = "1.0.9"
 
 query = '''
 sequence by process.entity_id with maxspan=5m
@@ -62,12 +62,17 @@ sequence by process.entity_id with maxspan=5m
   ]
 '''
```

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

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

18

behavior/rules/discovery_external_ip_address_discovery_vi…

```
@@ -7,16 +7,17 @@ id = "dfe28e03-9b0b-47f5-9753-65ed2666663f"
  license = "Elastic License v2"
  name = "External IP Address Discovery via Untrusted Program"
  os_list = ["windows"]
- version = "1.0.8"
+ version = "1.0.9"

  query = '''
  sequence by process.entity_id with maxspan=1m

   /* execution of an unsigned PE file followed by dns request to public ip discovery web services */

-   [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\\*", "?:\\Windows\\Tasks\\*")]
+   process.executable : ("?:\\Users\\*", "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*", "?:\\Windows\\Tasks\\*") and
+   (process.Ext.relative_file_creation_time <= 300 or process.Ext.relative_file_name_modify_time <= 300) ]
   [dns where
    dns.question.name :
         (
@@ -53,14 +54,17 @@ sequence by process.entity_id with maxspan=1m
          "ip4.seeip.org",
          "*.geojs.io",
          "*portmap.io"
-        )]
+        )
+        ]
 '''
 
- optional_actions = []
 [[actions]]
 action = "kill_process"
 field = "process.entity_id"
- state = 1
+ state = 0
+
+ [[optional_actions]]
+ action = "rollback"
 
 [[threat]]
 framework = "MITRE ATT&CK"
@@ -76,4 +80,4 @@ name = "Discovery"
 reference = "https://attack.mitre.org/tactics/TA0007/"
 
 [internal]
- min_endpoint_version = "7.15.0"
+ min_endpoint_version = "8.4.0"
```

2 🟩🟥□□□

behavior/rules/discovery_potential_security_software_disc…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
```

```
  name = "Potential Security Software Discovery via Grep"
  os_list = ["linux", "macos"]
  reference = ["https://objective-see.com/blog/blog_0x4F.html"]
- version = "1.0.7"
+ version = "1.0.8"

  query = '''
  process where event.type == "start" and
```

2 🟩🟥⬜⬜⬜

behavior/rules/discovery_potential_virtual_machine_finger…

```
@@ -8,7 +8,7 @@ license = "Elastic License v2"
  name = "Potential Virtual Machine Fingerprinting via Grep"
  os_list = ["macos"]
  reference = ["https://objective-see.com/blog/blog_0x4F.html"]
- version = "1.0.6"
+ version = "1.0.7"

  query = '''
  process where event.type == "start" and
```

5 🟩🟩🟩🟥🟥

behavior/rules/execution_command_shell_activity_started_v…

```
@@ -4,7 +4,7 @@ id = "b8a0a3aa-0345-4035-b41d-f758a6c59a78"
  license = "Elastic License v2"
  name = "Command Shell Activity Started via RunDLL32"
  os_list = ["windows"]
- version = "1.0.6"
+ version = "1.0.7"

  query = '''
  process where event.type == "start" and
```

```diff
@@ -22,7 +22,8 @@ process where event.type == "start" and
     not (process.args : ("launchalpsdelltouchpad://Mainpage/path2?param=start", "alpsdelltouchpadsettings://Mainpage/path2?param=start") and
          process.parent.args : "?:\\WINDOWS\\System32\\main.cpl") and
     not (process.command_line : "*REG QUERY HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Cryptography*" and
-         process.parent.args : "?:\\WINDOWS\\system32\\PcaSvc.dll,PcaPatchSdbTask")
+         process.parent.args : "?:\\WINDOWS\\system32\\PcaSvc.dll,PcaPatchSdbTask") and
+    not (process.args : "launchalpsdelltouchpad://Mainpage/path2?param=start" and process.parent.args : "Vxd_launch_UI")
 '''
 
 optional_actions = []
```

## 0 comments on commit 7460867

Please sign in to comment.

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