

```
60
                field = "process.entity_id"
  61
  62
         61
                state = 0
  63
         62
         63
              + [[optional_actions]]
              + action = "rollback"
         64
         65
                [[threat]]
  64
         66
  65
         67
                framework = "MITRE ATT&CK"
                [[threat.technique]]
  66
         68
     ....
 ...r/rules/command_and_control_connection_to_dynamic_dns ... 「☐
                @@ -7,7 +7,7 @@ id = "75b80e66-90d0-4ab6-9e6b-
     .
                976f7d690906"
                license = "Elastic License v2"
   7
          7
   8
                name = "Connection to Dynamic DNS Provider by an
                Unsigned Binary"
   9
          9
                os_list = ["windows"]
              - version = "1.0.7"
  10
              + version = "1.0.8"
         10
  11
         11
  12
         12
                query = '''
  13
                sequence by process.entity_id with maxspan=1m
         13
     ····
                @@ -48,12 +48,14 @@ sequence by process.entity_id
     ...
                with maxspan=1m
  48
         48
                    not dns.question.name : "checkip.dyndns.org"]
  49
         49
  50
         50
              - optional_actions = []
  51
  52
         51
                [[actions]]
                action = "kill_process"
  53
         52
  54
         53
                field = "process.entity_id"
  55
         54
                state = 1
  56
         55
         56
              + [[optional_actions]]
         57
              + action = "rollback"
         58
  57
         59
                [[threat]]
  58
         60
                framework = "MITRE ATT&CK"
  59
         61
                [[threat.technique]]
     +
```

```
behavior/rules/command_and_control_connection_to_webservi... [ ]
                 @@ -7,7 +7,7 @@ id = "c567240c-445b-4000-9612-
     <u></u>
                 b5531e21e050"
                 license = "Elastic License v2"
   7
           7
           8
                 name = "Connection to WebService by a Signed Binary
   8
                 Proxy"
   9
           9
                 os_list = ["windows"]
               - version = "1.0.6"
  10
          10
               + version = "1.0.7"
  11
          11
  12
          12
                 query = '''
  13
          13
                 sequence by process.entity_id with maxspan=5m
                 @@ -69,7 +69,6 @@ sequence by process.entity_id
     <u>†</u>
                 with maxspan=5m
  69
          69
                         "discord.com",
  70
          70
                         "apis.azureedge.net",
  71
          71
                         "cdn.sql.gg",
  72
                         "api.*",
          72
                         "?.top4top.io",
  73
  74
          73
                         "top4top.io",
  75
          74
                         "www.uplooder.net",
                 @@ -80,17 +79,20 @@ sequence by process.entity_id
     ....
                 with maxspan=5m
          79
                         "meacz.gq",
  80
                         "rwrd.org",
  81
          80
  82
          81
                         "*.publicvm.com",
                         "*.blogspot.com"
  83
                         "*.blogspot.com",
          82
                         "api.mylnikov.org"
          83
  84
          84
                     )
                   ]
  85
          85
                 1.1.1
          86
  86
  87
          87
  88
               - optional_actions = []
  89
          88
                 [[actions]]
  90
          89
                 action = "kill_process"
  91
          90
                 field = "process.entity_id"
                 state = 1
  92
          91
  93
          92
          93
               + [[optional_actions]]
          94
               + action = "rollback"
```

```
95
  94
         96
                [[threat]]
                framework = "MITRE ATT&CK"
  95
         97
  96
                [[threat.technique]]
         98
 behavior/rules/command_and_control_connection_to_webservi...
                @@ -7,15 +7,34 @@ id = "2c3efa34-fecd-4b3b-bdb6-
     †
                30d547f2a1a4"
                license = "Elastic License v2"
   7
          7
                name = "Connection to WebService by an Unsigned
   8
           8
                Binary"
                os_list = ["windows"]
   9
              - version = "1.0.7"
  10
              + version = "1.0.8"
         10
  11
         11
                query = '''
  12
         12
         13
                sequence by process.entity_id with maxspan=1m
  13
                 /* execution of an unsigned PE file followed by
  14
                dns lookup to commonly abused trusted webservices
                */
  15
         15
                  [process where event.action == "start" and
  16
                user.id : "S-1-5-21-*" and
                  [process where event.action == "start" and not
         16
                user.id: "S-1-5-18" and
                   not process.code_signature.trusted == true and
  17
         17
                   process.executable : ("?:\\Users\\*",
  18
                "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*")]
                   (process.Ext.relative_file_creation_time <= 300</pre>
         18
                or process.Ext.relative_file_name_modify_time <=
                300) and
                   process.executable : ("?:\\Users\\*",
         19
                "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*") and
                   not process.args : ("--type=utility", "--
         20
                squirrel-firstrun", "--utility-sub-type=*") and
                   process.executable : ("?:\\Users\\*",
         21
                "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*") and
                   not (process.name : "Clash for Windows.exe" and
         22
                process.args : "--utility-sub-
                type=network.mojom.NetworkService") and
                   not (process.name : "clash-win64.exe" and
         23
                process.parent.args : "--app-user-model-
```

```
id=com.*.clashwin") and
          + not process.hash.sha256 :
       25 +
              ("1cef2a7e7fe2a60e7f1d603162e60969469488cae99d04d13
              c4450cb90934b0f",
       26
              "ec4d11bd8216b894cb02f4e9cc3974a87901e928b4cdd2cac6
              d6eb22b3fa25eb",
       27 +
              "5c3725fb6ef2e8044b6ffbaa3f62f1afa1f47dd69ab557b611
              af8d80362f99d3",
       28
              "cc73c1aecb17ad6ce7c74bd258704994e43dea732212326a5b
              205be65b3b4b61",
       29
              "e5f6f15243393cb03022a3f1d22e0175acbf54cc5386cf9820
              185cf43cc90342",
       30
              "83d17dc95a7eba329fb29899b43d4b89b1dc898774e31ba58d
              e883ce4e44e833",
       31 +
              "f2e7ef9667f84a2b2f66e9116b06b6fbc3fd5af6695a50366e
              862692459b7a59",
       32 +
              "21b49f2824f1357684983cfacfc0d58a95a2b41cd7bbaff544
              d9de8e790be1b6",
       33 +
              "d71babf67e0e26991a34ea7d9cb78dc44dc0357bc20e4c15c6
              1ba49cae99fcaa",
       34 +
              "074b780a2a22d3d8af78afdfa042083488447fd5e63e7fa6e9
              c6abb08227e81d",
       35
              "578b95a62ecf3e1a3ea77d8329e87ba72a1b3516d0e5adb8d3
             f3d1eb44a7941e",
       36
              "a9b47f62e98f2561cf382d3d59e1d1b502b4cae96ab3e42012
              2c3b28cc5b7da6",
       37 +
              "14a4ae91ebf302026a8ba24f4548a82c683cfb5fa4494c76e3
              9d6d3089cdbbc1")]
19
       38
                [dns where
20
       39
                  dns.question.name :
21
       40
```

```
+
                @@ -69,12 +88,14 @@ sequence by process.entity_id
     .
                with maxspan=1m
  69
          88
                  ]
                 . . .
          89
  70
  71
          90
              - optional_actions = []
  73
          91
                 [[actions]]
                action = "kill_process"
  74
          92
                field = "process.entity_id"
  75
          93
                state = 1
  76
          94
  77
          95
          96
              + [[optional_actions]]
          97
              + action = "rollback"
          98
                [[threat]]
  78
          99
  79
                framework = "MITRE ATT&CK"
         100
  80
         101
                [[threat.technique]]
     ....
                @@ -99,4 +120,4 @@ name = "Command and Control"
  99
         120
                reference =
                 "https://attack.mitre.org/tactics/TA0011/"
 100
        121
        122
                 [internal]
 101
              - min_endpoint_version = "7.15.0"
 102
         123
              + min_endpoint_version = "8.4.0"
 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"
                os_list = ["windows"]
  10
          10
              - version = "1.0.6"
  11
              + version = "1.0.7"
          11
  12
          12
                query = '''
  13
          13
  14
          14
                sequence with maxspan=5m
     .
                @@ -21,12 +21,14 @@ sequence with maxspan=5m
  21
          21
                    ] by process.executable
                 1.1.1
          22
  22
          23
  23
  24
              - optional_actions = []
```

```
25
         24
                [[actions]]
  26
         25
               action = "kill_process"
               field = "process.entity_id"
  27
         26
  28
         27
                state = 1
  29
         28
              + [[optional_actions]]
         29
         30
              + action = "rollback"
         31 +
         32
                [[threat]]
  30
                framework = "MITRE ATT&CK"
  31
         33
  32
                [[threat.technique]]
         34
 behavior/rules/command_and_control_ingress_tool_transfer_... 💾
               @@ -0,0 +1,58 @@
        . . .
          1 + [rule]
          2 + description = """
          3 + Identifies downloads of remote content using
                Windows CURL executable. This tactic may be
                indicative of malicious
          4 + activity where malware is downloading second stage
                payloads using built-in Windows programs.
          5 + """
          6 + id = "336ada1c-69f8-46e8-bdd2-790c85429696"
          7 + license = "Elastic License v2"
          8 + name = "Ingress Tool Transfer via CURL"
          9 + os_list = ["windows"]
         10 + version = "1.0.3"
         11 +
         12 + query = '''
         + process where event.action == "start" and
         14
         15 + /* renamed curl or curl running from normal users
               writable fodlers are very noisy */
         16 + process.executable :
                ("?:\\Windows\\System32\\curl.exe",
                "?:\\Windows\\SysWOW64\\curl.exe") and
         17
             + process.args : ("-o", "--output") and
         18
         19
         20
                    (process.parent.name : ("powershell.exe",
                "mshta.exe", "wscript.exe", "cscript.exe",
                "rundll32.exe", "regsvr32.exe") and
```

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

```
56
          57
               + [internal]
               + min_endpoint_version = "7.15.0"

√ · ‡· 6 ■■■■□

behavior/rules/command_and_control_netwire_rat_registry_m... 💾
     <u></u>
                 @@ -8,7 +8,7 @@ license = "Elastic License v2"
                 name = "NetWire RAT Registry Modification"
   8
   9
           9
                 os_list = ["windows"]
  10
          10
                 reference =
                 ["https://attack.mitre.org/software/S0198/",
                 "https://any.run/malware-trends/netwire"]
               - version = "1.0.6"
  11
               + version = "1.0.7"
          11
  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
               - optional_actions = []
  20
                 [[actions]]
  21
          20
                 action = "kill_process"
  22
          21
          22
                 field = "process.entity_id"
  23
                 state = 0
  24
          23
  25
          24
               + [[optional_actions]]
          25
               + action = "rollback"
          26
          27
          28
                 [[threat]]
  26
  27
          29
                 framework = "MITRE ATT&CK"
  28
          30
                 [[threat.technique]]
                               Whitesp...
                                            Ignore whitespa...
                                                              Sp...
                                                                    Unifi...
```

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

```
Q Filter changed files

> behavior/rules
```

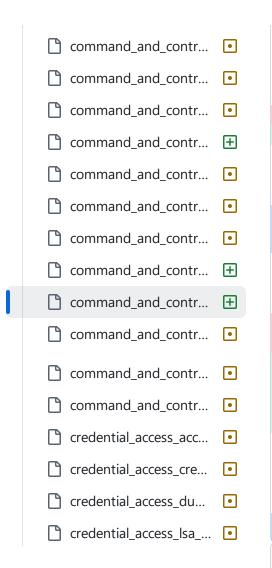
command\_and\_contr...

command\_and\_contr...

```
...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"
```



```
9
           9
                os_list = ["macos"]
  10
         10
                reference =
                ["https://attack.mitre.org/software/S0482/",
                "https://objective-see.com/blog/blog_0x69.html"]
              - version = "1.0.6"
  11
              + version = "1.0.7"
         11
  12
         12
         13
                query = '''
  13
                sequence by process.entity_id with maxspan=5s
  14
         14
                @@ -22,7 +22,7 @@ sequence by process.entity_id
     .‡.
                with maxspan=5s
         22
  22
         23
  23
                     ] and
                     process.name == "curl" and
  24
         24
  25
                     not process.args :
                "https://omahaproxy.appspot.com/history"
         25
                    not process.args :
                ("https://omahaproxy.appspot.com/history",
                "https://console.jumpcloud.com/api/systems/*",
                "https://zoom.us/client/*")
  26
         26
                  1
  27
         27
                  [network where event.action ==
                "connection_attempted"]
  28
         28
 behavior/rules/command_and_control_potential_plugx_regist... 💾
     .
                @@ -13,7 +13,7 @@ reference = [
  13
         13
                "https://www.welivesecurity.com/2022/03/23/mustang-
                panda-hodur-old-tricks-new-korplug-variant/",
  14
         14
                "https://malpedia.caad.fkie.fraunhofer.de/details/w
                in.plugx",
  15
         15
  16
              - version = "1.0.4"
         16
              + version = "1.0.5"
```

query = '''

registry where

17

19

+

17

18

19

```
behavior/rules/command_and_control_potential_wizardupdate... [ ]
               @@ -0,0 +1,40 @@
          1 + [rule]
          2 + description = """
          3 + Identifies the execution traces of the WizardUpdate
               malware. WizardUpdate is a macOS trojan that
               attempts to infiltrate
          4 + macOS machines to steal data and it is associated
               with other types of malicious payloads, increasing
               the chances of
          5 + multiple infections on a device.
          6 + """
          7 + id = "eb78fa0f-5e8a-4c15-a099-e904c4a226e6"
          8 + license = "Elastic License v2"
          9 + name = "Potential WizardUpdate Malware Infection"
         10 + os_list = ["macos"]
         11 + reference = [
         12 +
                "https://malpedia.caad.fkie.fraunhofer.de/details/o
                sx.xcsset",
         13 +
                "https://www.microsoft.com/security/blog/2022/02/02
                /the-evolution-of-a-mac-trojan-updateagents-
               progression/",
         14 + ]
         15 + version = "1.0.2"
         16 +
         17 + query = '''
             + process where event.action == "exec" and
         19
                  (process.name : "sh" and process.command_line :
         20
               "*=$(curl *eval*$*") or
                  (process.name : "curl" and process.command_line
               : "*_intermediate_agent_*machine_id*")
         22
             + )
         23 + '''
         24 +
         25 + optional_actions = []
         26 + [[actions]]
         27 + action = "kill_process"
         28 + field = "process.entity_id"
         29 + state = 0
```

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

✓ 43 ■■■■■
behavior/rules/command_and_control_potential_xcsset_malwa... 📙
               @@ -0,0 +1,43 @@
        . . .
 . . .
          1 + [rule]
          2 + description = """
          3 + Identifies the execution traces of the XCSSET
                malware. XCSSET is a macOS trojan that primarily
               spreads via Xcode
          4 + projects and maliciously modifies applications.
               Infected users are also vulnerable to having their
               credentials,
          5 + accounts, and other vital data stolen.
          6 + """
          7 + id = "875b71bb-ef09-46b2-9c12-a95112461e85"
          8 + license = "Elastic License v2"
          9 + name = "Potential XCSSET Malware Infection"
         10 + os_list = ["macos"]
         11 + reference =
                ["https://malpedia.caad.fkie.fraunhofer.de/details/
               osx.xcsset"]
         12 + version = "1.0.2"
         13 +
         14 + query = '''
         + process where event.action == "exec" and
         16
             + (process.name : "curl" and process.parent.name :
         17
               "bash" and
                  process.args : ("https://*/sys/log.php",
         18 +
                "https://*/sys/prepod.php",
                "https://*/sys/bin/Pods")) or
         19 +
```

20

```
process.parent.name : "bash") or
         21
         22
                  (process.name : "plutil" and process.args :
                "LSUIElement" and process.args :
                "/Users/*/Library/Group Containers/*" and
                process.parent.name : "bash") or
         23
         24 +
                  (process.name : "zip" and process.args : "-r" and
                process.args : "/Users/*/Library/Group
                Containers/*")
         25
             + )
         26 + '''
         27 +
         28 + optional_actions = []
         29 + [[actions]]
         30 + action = "kill_process"
         31 + field = "process.entity_id"
         32 + state = 0
         33
         34 + [[threat]]
         35
             + framework = "MITRE ATT&CK"
         36
         37 + [threat.tactic]
         38 + id = "TA0011"
         39 + name = "Command and Control"
         40
             + reference =
                "https://attack.mitre.org/tactics/TA0011/"
         41 +
         42 + [internal]
         43 + min_endpoint_version = "7.15.0"
 behavior/rules/command_and_control_remcos_rat_registry_or... 📮
    <u></u>
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
   8
          8
                name = "Remcos RAT Registry or File Modification"
   9
          9
               os_list = ["windows"]
                reference =
  10
         10
                ["https://attack.mitre.org/software/S0332/",
                "https://any.run/malware-trends/remcos"]
              - version = "1.0.6"
  11
             + version = "1.0.7"
         11
  12
         12
```

(process.name : "osacompile" and process.args :

"/Users/\*/Library/Group Containers/\*" and

```
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]]
                action = "kill_process"
  26
          25
  27
                field = "process.entity_id"
          26
  28
          27
                state = 0
  29
          28
          29
              + [[optional_actions]]
          30
              + action = "rollback"
          31
          32
                [[threat]]
  30
                framework = "MITRE ATT&CK"
  31
          33
  32
          34
                [[threat.technique]]
 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
                1
  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"
     +
```

```
behavior/rules/command_and_control_suspicious_netsupport_... 

....

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

8 8 name = "Suspicious NetSupport Execution"
```

```
9
          9
                os_list = ["windows"]
  10
         10
                reference = ["https://www.netsupportsoftware.com/"]
              - version = "1.0.5"
  11
         11
              + version = "1.0.6"
  12
         12
                query = '''
  13
         13
  14
         14
                sequence by process.entity_id with maxspan=1m
                @@ -19,12 +19,14 @@ sequence by process.entity_id
     .
                with maxspan=1m
  19
         19
                 [dns where not dns.question.name :
                "*.netsupportsoftware.com"]
  20
         20
  21
         21
              - optional_actions = []
  22
         22
                [[actions]]
  23
                action = "kill_process"
  24
         23
  25
                field = "process.entity_id"
         24
         25
                state = 0
  26
  27
         26
         27
              + [[optional_actions]]
             + action = "rollback"
         28
         29
  28
         30
                [[threat]]
  29
         31
                framework = "MITRE ATT&CK"
  30
         32
                [[threat.technique]]
     +
 behavior/rules/credential_access_access_to_windows_passwo... 📮
     .
                @@ -10,20 +10,22 @@ os_list = ["windows"]
  10
         10
                reference = [
  11
         11
                    "https://docs.microsoft.com/en-
                us/uwp/api/windows.security.credentials.passwordvau
                lt.retrieve?view=winrt-22000",
  12
         12
                ]
  13
              - version = "1.0.4"
         13
             + version = "1.0.5"
  14
         14
                query = '''
  15
         15
  16
         16
                process where event.action == "start" and
  17
         17
                 process.pe.original_file_name == "PowerShell.EXE"
                and
```

```
18
         18
                 process.command_line :
                ("*Credentials.PasswordVault*",
                "*RetrievePassword*", "*Credentials*RetrieveAll*")
  19
         19
  20
         20
  21
              - optional_actions = []
  22
         21
                [[actions]]
  23
         22
                action = "kill_process"
         23
                field = "process.entity_id"
  24
  25
                state = 0
         24
  26
         25
         26
              + [[optional_actions]]
         27
              + action = "rollback"
         28
         29
  27
                [[threat]]
  28
         30
                framework = "MITRE ATT&CK"
  29
         31
                [[threat.technique]]
     +
 behavior/rules/credential_access_credential_access_via_kn... [ ]
    <u></u>
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
   8
                name = "Credential Access via Known Utilities"
   9
          9
                os_list = ["windows"]
  10
                reference = ["https://lolbas-project.github.io/"]
         10
              - version = "1.0.12"
  11
              + version = "1.0.13"
         11
         12
  12
                query = '''
  13
         13
  14
         14
                process where event.action == "start" and
                @@ -32,7 +32,8 @@ process where event.action ==
     ....
                "start" and
  32
         32
                  (process.name : "createdump.exe" and process.args
                : "-u") or
  33
         33
                  (process.pe.original_file_name ==
                "FX_VER_INTERNALNAME_STR" and process.args : "-u"
                and process.args : "-f" and process.args_count >=
                3) or
  34
         34
                  /* taskmgr via GUI - Create dump file - excluding
                Explorer to avoid breaking legit use of taskmgr */
  35
                  (process.pe.original_file_name == "Taskmgr.exe"
                and process.args == "/4" and not
```

```
process.parent.executable :
              "?:\\Windows\\explorer.exe") or
                (process.pe.original_file_name == "Taskmgr.exe"
       35
              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
       47
                     process.command_line :
46
              "*davclnt.dll,DavSetCookie*http*MiniDump*" and
                     process.parent.executable :
47
       48
              "?:\\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\\S
              ystem\\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")
              1.1.1
50
       52
       53
51
52
            - optional_actions = []
53
       54
              [[actions]]
              action = "kill_process"
54
       55
              field = "process.entity_id"
55
       56
       57
              state = 0
56
       58
57
       59
            + [[optional_actions]]
            + action = "rollback"
       60
       61
       62
              [[threat]]
58
              framework = "MITRE ATT&CK"
59
       63
              [[threat.technique]]
60
       64
  Τ...
```

```
behavior/rules/credential_access_dumping_account_hashes_v... 📮
     .
                @@ -12,7 +12,7 @@ reference = [
         12
  12
                "https://apple.stackexchange.com/questions/186893/o
                s-x-10-9-where-are-password-hashes-stored",
         13
                    "https://www.unix.com/man-
  13
                page/osx/8/mkpassdb/",
         14
  14
              - version = "1.0.6"
  15
         15
              + version = "1.0.7"
  16
         16
                query = '''
         17
  17
                process where event.type == "start" and
  18
         18
     Τ...
```

```
√ · ‡· 6 ■■■■□

behavior/rules/credential_access_lsa_dump_via_silentproce... 📮
     .
                @@ -10,18 +10,20 @@ os_list = ["windows"]
          10
  10
                reference = [
  11
          11
                     "https://www.deepinstinct.com/2021/02/16/lsass-
                 memory-dumps-are-stealthier-than-ever-before-part-
                 2/",
  12
          12
                1
               - version = "1.0.9"
          13
              + version = "1.0.10"
  14
          14
  15
          15
                query = '''
  16
                registry where registry.path:
          16
                 "HKLM\\SOFTWARE\\Microsoft\\Windows
                NT\\CurrentVersion\\SilentProcessExit\\lsass*"
  17
          17
  18
          18
  19
              - optional_actions = []
  20
          19
                [[actions]]
  21
          20
                action = "kill_process"
  22
          21
                field = "process.entity_id"
  23
          22
                state = 0
  24
          23
          24
              + [[optional_actions]]
              + action = "rollback"
```

26

```
25
         27
                [[threat]]
                framework = "MITRE ATT&CK"
  26
         28
  27
         29
                [[threat.technique]]
 behavior/rules/credential_access_potential_access_to_kerb... 💾
     <u></u>
                @@ -12,7 +12,7 @@ reference = [
  12
         12
                "https://github.com/EmpireProject/EmPyre/blob/maste
                r/lib/modules/collection/osx/kerberosdump.py",
  13
         13
                "https://opensource.apple.com/source/Heimdal/Heimda
                1-323.12/kuser/kcc-commands.in.auto.html",
  14
         14
                1
  15
              - version = "1.0.5"
         15
              + version = "1.0.6"
  16
         16
                query = '''
  17
         17
         18
                process where event.type == "start" and
  18
     +
 behavior/rules/credential_access_potential_credential_acc... 📮
     .
                @@ -9,7 +9,7 @@ license = "Elastic License v2"
   9
                name = "Potential Credential Access via Mimikatz"
                os_list = ["windows"]
  10
         10
                reference = ["https://adsecurity.org/?
  11
         11
                page_id=1821",
                "https://github.com/gentilkiwi/mimikatz"]
              - version = "1.0.5"
  12
             + version = "1.0.6"
         12
  13
         13
                query = '''
  14
         14
  15
         15
                process where event.action == "start" and
                @@ -30,12 +30,14 @@ process where event.action ==
     ....
                "start" and
  30
         30
                  )
                1.1.1
         31
  31
```

32

32

```
33
               - optional_actions = []
  34
          33
                [[actions]]
                action = "kill_process"
  35
          34
          35
                field = "process.entity_id"
  36
  37
          36
                state = 0
  38
          37
          38
              + [[optional_actions]]
          39
              + action = "rollback"
          40
                [[threat]]
  39
          41
  40
          42
                framework = "MITRE ATT&CK"
          43
                [[threat.technique]]
  41
     ....
 behavior/rules/credential_access_potential_credential_acc... 「  
     <u></u>
                @@ -11,7 +11,7 @@ reference = [
          11
                    "https://github.com/GhostPack/Rubeus",
  11
  12
          12
                "https://github.com/SigmaHQ/sigma/blob/master/rules
                /windows/process_creation/win_hack_rubeus.yml",
          13
  13
                1
  14
              - version = "1.0.6"
              + version = "1.0.7"
          14
          15
  15
          16
                query = '''
  16
  17
          17
                process where event.action == "start" and
```

```
...r/rules/credential_access_potential_credential_access_... [ ]
     <u>+</u>
                @@ -9,7 +9,7 @@ license = "Elastic License v2"
          9
                name = "Potential Credential Access via Windows
                Credential History"
                os_list = ["windows"]
  10
         10
                reference =
  11
         11
                ["http://www.harmj0y.net/blog/redteaming/operationa
                1-guidance-for-offensive-user-dpapi-abuse/"]
              - version = "1.0.5"
  12
         12
             + version = "1.0.6"
  13
         13
```

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",
                           "?:\\Windows\\CCM\\*.exe",
  27
         27
         28
                            "?:\\Windows\\explorer.exe",
  28
         29
                            "?:\\ProgramData\\Microsoft\\Windows
                Defender\\*.exe",
  29
         30
                           "?:\\Windows\\explorer.exe",
  30
         31
                            "?:\\Windows\\System32\\WerFault.exe",
                            "?:\\Windows\\SysWOW64\\WerFault.exe",
  31
         32
                            "?:\\Windows\\System32\\dllhost.exe")
  32
                            "?:\\Windows\\System32\\dllhost.exe",
         33
                            "?:\\Windows\\System32\\sdclt.exe")
         34
                1.1.1
  33
         35
  34
         36
  35
         37
                optional_actions = []
 behavior/rules/credential_access_potential_credentials ph... [ ]
     <u></u>
                @@ -11,7 +11,7 @@ reference = [
  11
         11
                "https://github.com/EmpireProject/EmPyre/blob/maste
                r/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
     +
 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"]
```

```
10
         10
                reference =
                ["http://www.harmj0y.net/blog/redteaming/operationa
                l-guidance-for-offensive-user-dpapi-abuse/"]
  11
              - version = "1.0.8"
         11
              + version = "1.0.9"
  12
         12
  13
         13
                query = '''
  14
         14
                file where event.action == "open" and
    Τ...
                @@ -42,7 +42,13 @@ file where event.action ==
    ....
                "open" and
  42
         42
                            "?:\\ProgramData\\Microsoft\\Windows
                Defender Advanced Threat Protection\\*.exe",
                            "?:\\ProgramData\\Microsoft\\Windows
         43
  43
                Defender\\Platform\\*.exe",
         44
                            "?:\\ProgramData\\Microsoft\\Windows
  44
                Defender Advanced Threat
                Protection\\Platform\\*.exe",
                            "?:\\Program Files\\Windows Defender
  45
                Advanced Threat Protection\\*.exe") and
                            "?:\\Program Files\\Windows Defender
         45
                Advanced Threat Protection\\*.exe",
                            "?:\\Windows\\System32\\igfxtray.exe",
         46
         47
                "?:\\$WINDOWS.~BT\\Sources\\SetupCore.exe",
         48
                            "?:\\Windows\\System32\\MRT.exe",
         49
                "?:\\Windows\\twain_32\\Brimc16a\\Common\\TwDsUiLau
                nch.exe",
         50
                "?:\\Windows\\Microsoft.NET\\Framework64\\*\\csc.ex
         51
                "?:\\Users\\*\\AppData\\Local\\JetBrains\\Toolbox\\
                apps\\datagrip\\ch-
                0\\203.5981.102\\bin\\datagrip64.exe") and
                 /* MSSQL service account */
  46
         52
  47
         53
                 not (process.name : "sqlservr.exe" and file.path :
                "?:\\Users\\svc_*")
                1.1.1
  48
         54
     +
 ...vior/rules/credential_access_potential_discovery_of_wi... 📮
```

```
†
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
                name = "Potential Discovery of Windows Credential
   8
          8
                Manager Store"
   9
          9
                os_list = ["windows"]
  10
         10
                reference =
                ["http://www.harmj0y.net/blog/redteaming/operationa
                l-guidance-for-offensive-user-dpapi-abuse/"]
              - version = "1.0.7"
  11
              + version = "1.0.8"
         11
         12
  12
  13
         13
                query = '''
  14
         14
                file where event.action == "open" and
                @@ -38,7 +38,11 @@ file where event.action ==
     ....
                "open" and
  38
         38
                "?:\\Windows\\System32\\wbem\\WmiPrvSE.exe",
         39
                             "?:\\Windows\\System32\\dllhost.exe",
  39
                             "?:\\Windows\\explorer.exe",
  40
         40
  41
                             "?:\\Windows\\System32\\MRT.exe")
                             "?:\\Windows\\System32\\MRT.exe",
         41
         42
                "?:\\Users\\*\\AppData\\Local\\Microsoft\\OneDrive\
                \OneDrive.exe",
         43
                "?:\\Windows\\Microsoft.NET\\Framework\\*\\csc.exe"
         44
                "?:\\Windows\\System32\\SearchProtocolHost.exe",
         45
                "?:\\Users\\*\\AppData\\Local\\ESET\\ESETOnlineScan
                ner\\ESETOnlineScanner.exe")
  42
         46
  43
         47
  44
         48
                optional_actions = []
 behavior/rules/credential_access_security_account_manager...
     †
                @@ -11,7 +11,7 @@ reference = [
  11
         11
                    "https://adsecurity.org/?page_id=1821",
  12
         12
                "https://github.com/gentilkiwi/mimikatz/wiki/module
                -~-lsadump",
```

```
13
         13
                ]
  14
              - version = "1.0.9"
              + version = "1.0.10"
         14
         15
  15
  16
         16
                query = '''
  17
         17
                file where event.action == "open" and
     ....
 behavior/rules/credential_access_security_account_manager...
    <u></u>
                @@ -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"
              + version = "1.0.8"
         14
  15
         15
                query = '''
  16
         16
              - sequence by process.entity_id with maxspan=5m
  17
         17
              + sequence by process.entity_id
         18
                  [process where event.action == "start" and
  18
                   not process.executable : ("?:\\Program
  19
         19
                Files\\*.exe", "?:\\Program Files (x86)\\*.exe")
                   not (process.name : "cscript.exe" and
  20
         20
                process.command_line : "*Tanium*collectAdInfo.vbs*"
                and
```

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

```
13
         13
                query = '''
  14
         14
                sequence by process.entity_id with maxspan=5m
     ····
 . . .
...vior/rules/credential_access_sensitive_file_access_rem... 📮
    .
                @@ -11,7 +11,7 @@ reference = [
  11
         11
                "http://www.harmj0y.net/blog/redteaming/operational
                -guidance-for-offensive-user-dpapi-abuse/",
                    "https://smsagent.blog/2017/01/26/decrypting-
  12
         12
                remote-desktop-connection-manager-passwords-with-
                powershell/",
                1
  13
         13
              - version = "1.0.7"
  14
              + version = "1.0.8"
         14
  15
         15
                query = '''
  16
         16
         17
                file where event.type == "access" and
  17
     ....
    · 19
```

```
behavior/rules/credential_access_sensitive_file_access_ss... 📮
     .
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
                name = "Sensitive File Access - SSH Saved Keys"
   8
   9
           9
                os_list = ["windows"]
          10
                reference =
  10
                 ["https://github.com/GhostPack/Seatbelt",
                 "https://github.com/AlessandroZ/LaZagne"]
  11
              - version = "1.0.8"
              + version = "1.0.10"
          11
  12
          12
                query = '''
  13
          13
  14
                 any where event.category in ("registry", "file")
                 and
                @@ -20,26 +20,35 @@ any where event.category in
     .‡.
                 ("registry", "file") and
                       ("?:\\Program Files\\*",
  20
          20
                            "?:\\Program Files (x86)\\*",
  21
          21
  22
          22
                            "?:\\ProgramData\\Microsoft\\Windows
                Defender\\Platform\\*\\MsMpEng.exe",
```

| 23 |    | - "?:\\ProgramData\\Microsoft\\Windows              |
|----|----|---|
|    |    | Defender\\Platform\\*\\MpCopyAccelerator.exe",      |
|    | 23 | + "?:\\ProgramData\\Microsoft\\Windows              |
|    |    | Defender\\Platform\\*\\MpCopyAccelerator.exe",      |
|    | 24 | + "?:\\ProgramData\\Microsoft\\Windows              |
|    |    | Defender Advanced Threat                            |
|    |    | <pre>Protection\\Platform\\*\\MsSense.exe",</pre>   |
| 24 | 25 | "?:\\Windows\\System32\\OpenSSH\\*.exe",            |
| 25 | 26 |   |
|    |    | "?:\\Windows\\System32\\smartscreen.exe",           |
| 26 | 27 | "?:\\WINDOWS\\system32\\reg.exe",                   |
| 27 | 28 | "?:\\Windows\\regedit.exe",                         |
| 28 | 29 | "?:\\Windows\\System32\\notepad.exe",               |
| 29 |    | - "?:\\Windows\\System32\\Robocopy.exe",            |
|    | 30 | + "?:\\Windows\\System32\\Robocopy.exe",            |
| 30 | 31 | "?:\\Windows\\System32\\cmd.exe",                   |
| 31 | 32 | "?:\\Windows\\explorer.exe",                        |
| 32 | 33 | "?:\\Windows\\System32\\svchost.exe",               |
| 33 | 34 |   |
|    |    | "?:\\\$WINDOWS.~BT\\Sources\\setuphost.exe",        |
| 34 | 35 |   |
|    |    | "?:\\Users\\*\\AppData\\Local\\Programs\\Git\\mingw |
|    |    | 64\\bin\\git.exe",                                  |
| 35 | 36 |   |
|    |    | "?:\\Users\\*\\AppData\\Local\\DBeaver\\dbeaver.exe |
|    |    | ",  |
| 36 |    | -   |
|    |    | "?:\\Windows\\System32\\SearchProtocolHost.exe")    |
|    |    | and   |
|    | 37 | +   |
|    |    | "?:\\Users\\*\\Tools\\dbeaver\\dbeaver.exe",        |
|    | 38 | +   |
|    |    | "?:\\Windows\\System32\\SearchProtocolHost.exe",    |
|    | 39 | +   |
|    |    | "?:\\Users\\*\\AppData\\Local\\Microsoft\\OneDrive\ |
|    |    | \OneDrive.exe",                                     |
|    | 40 | +   |
|    |    | "?:\\ProgramData\\GalacticScan\\GalacticScan.exe",  |
|    | 41 | +   |
|    |    | "?:\\Users\\*\\AppData\\Local\\Programs\\GalacticSc |
|    |    | an\\GalacticScan_Warpspeed.exe",                    |
|    | 42 | +   |
|    |    | "?:\\Users\\*\\AppData\\Local\\Postman\\app-        |
|    |    | *\\Postman.exe",                                    |
|    |    |   |

```
43
                "?:\\Users\\*\\OneDrive\\*\\Wintriage\\Tools\\ADSec
                urizame.exe",
          44
                "?:\\Users\\*\\AppData\\Local\\JetBrains\\Toolbox\\
                apps\\Gateway\\*\\bin\\gateway64.exe",
          45
                "?:\\Users\\*\\AppData\\Local\\Google\\Chrome\\Appl
                ication\\chrome.exe") and
  37
          46
  38
          47
                  /* many of the following exclusions are not
                signed nor have an original file name */
  39
          48
                  not process.name : ("pscp.exe", "psftp.exe",
                "_ssh.exe", "plink.exe", "PuTTYNG.exe",
                "putty*.exe", "busybox.exe",
          49
                                       "ssh.exe", "WinSCP.exe",
  40
                "bash.exe", "MoTTY.exe", "eclipse.exe", "code.exe",
                "datagrip*.exe",
  41
          50
                                       "MobaXterm_Personal*.exe",
                "RoyalTS_PuTTY*.exe", "MAP.EXE", "rssputty.exe",
                "phpstorm64.exe",
                                       "Fork.exe", "fzsftp.exe")
  42
          51
                                       "Fork.exe", "fzsftp.exe",
                "OneDrive.exe")
  43
          52
  44
          53
  45
          54
                optional_actions = []
     ····
 behavior/rules/credential_access_sensitive_file_access_sy... 💾
     <u></u>
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
   8
           8
                name = "Sensitive File Access - System Admin
                Utilities"
                os_list = ["windows"]
   9
           9
  10
          10
                reference =
                ["https://github.com/GhostPack/Seatbelt",
                "https://github.com/AlessandroZ/LaZagne"]
              - version = "1.0.7"
  11
              + version = "1.0.8"
          11
  12
          12
          13
                query = '''
  13
  14
          14
                sequence by process.entity_id with maxspan=5m
```

```
....
 behavior/rules/credential_access_sensitive_file_access_un... 📮
     <u></u>
                @@ -11,7 +11,7 @@ reference = [
         11
                    "https://steflan-security.com/windows-
  11
                privilege-escalation-credential-harvesting/",
                    "https://github.com/pha5matis/Pentesting-
  12
         12
                Guide/blob/master/privilege_escalation_windows.md",
  13
         13
                1
              - version = "1.0.7"
  14
              + version = "1.0.8"
         14
  15
         15
                query = '''
  16
         16
                sequence by process.entity_id with maxspan=1m
  17
         17
     ....
```

```
behavior/rules/credential_access_suspicious_access_to_act... 📮
     <u></u>
                @@ -10,7 +10,7 @@ os_list = ["windows"]
  10
         10
                reference = [
                    "https://www.ired.team/offensive-
  11
         11
                security/credential-access-and-credential-
                dumping/ntds.dit-enumeration",
         12
  12
              - version = "1.0.8"
  13
              + version = "1.0.9"
         13
  14
         14
  15
         15
                query = '''
  16
                file where event.action == "open" and process.pid
                != 4 and
```

| 13  | 13             | "https://github.com/gtworek/PSBits/tree/master/LSAS   |
|-----|----------------|---|
|     |                | ecretDumper",   |
| 14  | 14             | ]   |
| 15  |                | - version = "1.0. <mark>7</mark> "  |
|     | 15             | + version = "1.0.9"   |
| 16  | 16             |   |
| 17  | 17             | query = '''   |
| 18  | 18             | registry where  |
| .‡. |                | @@ -25,7 +25,10 @@ registry where   |
| 25  | 25             | "?:\\Program  |
|     |                | <pre>Files\\Citrix\\PvsVm\\Service\\PvsVmAgent.exe",</pre>  |
| 26  | 26             |   |
|     |                | "?:\\Windows\\Provisioning\\Autopilot\\DiagonsticAn   |
|     |                | alysis.pif",  |
| 27  | 27             | "?:\\Program  |
|     |                | Files\\RepairTech\\LiveAgent\\SyncroLive.Agent.Runn   |
|     |                | er.exe",  |
| 28  |                | - "?:\\Program  |
|     |                | Files\\Common Files\\Adobe\\Creative Cloud  |
|     |                | Libraries\\CCLibrary.exe") and  |
|     | 28             | + "?:\\Program  |
|     |                |   |
|     |                | Files\\Common Files\\Adobe\\Creative Cloud  |
|     |                | <pre>Files\\Common Files\\Adobe\\Creative Cloud Libraries\\CCLibrary.exe",</pre>  |
|     | 29             | <pre>Libraries\\CCLibrary.exe", +</pre>   |
|     | 29             | <pre>Libraries\\CCLibrary.exe", +    "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows</pre>  |
|     |                | <pre>Libraries\\CCLibrary.exe", +</pre>   |
|     | 29             | <pre>Libraries\\CCLibrary.exe", +    "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows    erNet\\SecuredBrowserDotNetLauncher.exe", +</pre>   |
|     | 30             | <pre>Libraries\\CCLibrary.exe", +    "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows    erNet\\SecuredBrowserDotNetLauncher.exe", +    "?:\\Windows\\regedit.exe",</pre>  |
|     |                | <pre>Libraries\\CCLibrary.exe", +    "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows    erNet\\SecuredBrowserDotNetLauncher.exe", +    "?:\\Windows\\regedit.exe", +    "?:\\Program</pre>  |
|     | 30             | <pre>Libraries\\CCLibrary.exe", +    "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows    erNet\\SecuredBrowserDotNetLauncher.exe", +     "?:\\Windows\\regedit.exe", +     "?:\\Program Files\\Dell\\Dell Data</pre>   |
|     | 30             | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\SecuredBrowserDotNetLauncher.exe",  +  "?:\\Windows\\regedit.exe",  +  "?:\\Program Files\\Dell\\Dell Data Protection\\Encryption\\EmsService.exe") and   |
| 29  | 30             | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\SecuredBrowserDotNetLauncher.exe",  +  "?:\\Windows\\regedit.exe",  +  "?:\\Program Files\\Dell\\Dell Data Protection\\Encryption\\EmsService.exe") and not (process.executable :   |
| 29  | 30             | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\SecuredBrowserDotNetLauncher.exe",  +  "?:\\Windows\\regedit.exe",  +  "?:\\Program Files\\Dell\\Dell Data Protection\\Encryption\\EmsService.exe") and not (process.executable :  "?:\\Windows\\System32\\dsregcmd.exe" and  |
| 29  | 30             | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\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 :  |
| 29  | 30             | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\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\\MutexNa   |
|     | 30<br>31<br>32 | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\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\\MutexNa me") and  |
| 29  | 30             | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\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\\MutexNa me") and  not (process.executable :   |
|     | 30<br>31<br>32 | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\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\\MutexNa me") and  not (process.executable :  "?:\\Windows\\LTSvc\\LTSVC.exe" and registry.path :  |
| 30  | 30<br>31<br>32 | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\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\\MutexNa me") and not (process.executable :  "?:\\Windows\\LTSvc\\LTSVC.exe" and registry.path :  "HKLM\\SECURITY\\Cache\\NL\$1") and  |
|     | 30<br>31<br>32 | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\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\\MutexNa me") and not (process.executable:  "?:\\Windows\\LTSvc\\LTSVC.exe" and registry.path:  "HKLM\\SECURITY\\Cache\\NL\$1") and not (process.executable: ("?:\\Program Files |
| 30  | 30<br>31<br>32 | Libraries\\CCLibrary.exe",  +  "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows erNet\\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\\MutexNa me") and not (process.executable :  "?:\\Windows\\LTSvc\\LTSVC.exe" and registry.path :  "HKLM\\SECURITY\\Cache\\NL\$1") and  |

```
behavior/rules/credential_access_suspicious_access_to_web... 📮
                @@ -7,7 +7,7 @@ id = "03758167-3eed-465f-9174-
     <u></u>
                b284d599036d"
                license = "Elastic License v2"
   7
                name = "Suspicious Access to Web Browser Credential
   8
          8
                Stores"
   9
          9
                os_list = ["windows"]
              - version = "1.0.10"
  10
         10
              + version = "1.0.11"
         11
  11
                query = '''
         12
  12
         13
                sequence by process.entity_id with maxspan=1m
  13
```

```
behavior/rules/credential access suspicious access to win... 「↓
    <u>†</u>
                @@ -9,7 +9,7 @@ license = "Elastic License v2"
   9
          9
                name = "Suspicious Access to Windows Vault Files"
                os_list = ["windows"]
  10
         10
  11
         11
                reference =
                ["http://www.harmj0y.net/blog/redteaming/operationa
                1-guidance-for-offensive-user-dpapi-abuse/"]
              - version = "1.0.5"
  12
         12
             + version = "1.0.6"
  13
         13
                query = '''
  14
         14
  15
         15
                file where event.action == "open" and
                @@ -28,7 +28,8 @@ file where event.action == "open"
     .‡.
                and
  28
         28
                           "?:\\Windows\\CCM\\*.exe",
  29
         29
                           "?:\\ProgramData\\Microsoft\\Windows
                Defender\\*.exe",
  30
         30
                           "?:\\Windows\\System32\\dllhost.exe",
  31
                "?:\\Users\\*\\AppData\\Local\\ESET\\ESETOnlineScan
                ner\\ESETOnlineScanner.exe")
         31 +
                "?:\\Users\\*\\AppData\\Local\\ESET\\ESETOnlineScan
                ner\\ESETOnlineScanner.exe",
```

```
32
                            "?:\\Windows\\Explorer.exe")
                1.1.1
  32
          33
  33
          34
  34
          35
                optional_actions = []
 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
                1
              - version = "1.0.4"
  16
          16
              + version = "1.0.5"
          17
  17
          18
                query = '''
  18
  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\\AppDat
                a\\*")]
                1.1.1
  36
          36
  37
          37
               - optional_actions = []
  38
  39
          38
                [[actions]]
  40
          39
                action = "kill_process"
                field = "process.entity_id"
  41
          40
  42
          41
                state = 1
  43
          42
          43
              + [[optional_actions]]
          44
              + action = "rollback"
          45
          46
                [[threat]]
  44
                framework = "MITRE ATT&CK"
  45
          47
  46
          48
                [[threat.technique]]
     T
```

```
behavior/rules/credential_access_system_bootkey_registry_... 📮
    †
                @@ -11,7 +11,7 @@ reference = [
         11
                    "http://moyix.blogspot.com/2008/02/syskey-and-
  11
                sam.html",
         12
  12
                "https://github.com/gentilkiwi/mimikatz/wiki/module
                -~-lsadump",
         13
  13
  14
              - version = "1.0.6"
         14
              + version = "1.0.7"
         15
  15
                query = '''
  16
         16
  17
         17
                sequence by process.entity_id with maxspan=1m
     Τ...
```

```
behavior/rules/credential_access_unusual_kerberos_client_... [ ]
                @@ -7,7 +7,7 @@ id = "b5c91c3e-9d2d-4df6-afb7-
     <u></u>
                c9d236b5ebe2"
   7
           7
                license = "Elastic License v2"
   8
           8
                name = "Unusual Kerberos Client Process"
                os_list = ["windows"]
   9
           9
              - version = "1.0.4"
  10
         10
              + version = "1.0.5"
  11
         11
                query = '''
  12
         12
  13
         13
                sequence by process.entity_id with maxspan=1m
                @@ -23,12 +23,14 @@ sequence by process.entity_id
     .‡.
                with maxspan=1m
  23
         23
                  not process.executable : "?:\\Program Files
                (x86)\\GFI\\LanGuard 12 Agent\\lnsscomm.exe"]
         24
  24
  25
         25
  26
              - optional_actions = []
  27
         26
                [[actions]]
                action = "kill_process"
  28
         27
                field = "process.entity_id"
  29
         28
                state = 0
         29
  30
  31
         30
```

```
31 + [[optional_actions]]
         32 + action = "rollback"
         33 +
  32
         34
               [[threat]]
  33
         35
               framework = "MITRE ATT&CK"
  34
         36
               [[threat.technique]]
     Τ.
 behavior/rules/credential_access_web_browser_credential_a... 💾
               @@ -7,7 +7,7 @@ id = "9ed4ee4a-bc91-4d38-b6dd-
     .
               11467b774460"
               license = "Elastic License v2"
   7
          7
               name = "Web Browser Credential Access via Unsigned
   8
               Process"
               os_list = ["windows"]
   9
              - version = "1.0.8"
  10
             + version = "1.0.9"
         10
  11
         11
               query = '''
  12
         12
         13
                sequence by user.name with maxspan=2m
  13
     +
 behavior/rules/credential_access_web_browser_credential_a...
               @@ -7,7 +7,7 @@ id = "f488cd1b-2407-4ec8-8705-
    7adf99ccbd33"
               license = "Elastic License v2"
   7
          7
               name = "Web Browser Credential Access via Unusual
          8
   8
               Process"
               os_list = ["windows"]
   9
             - version = "1.0.6"
  10
             + version = "1.0.7"
         10
```

file where event.type == "access" and

11

12 13 11

12

13

query = '''

```
<u></u>
             @@ -14,7 +14,7 @@ reference = [
        14
                 "https://ss64.com/osx/security.html",
  14
        15
  15
              "https://www.intezer.com/blog/research/operation-
             electrorat-attacker-creates-fake-companies-to-
              drain-your-crypto-wallets/",
        16
  16
            - version = "1.0.5"
  17
            + version = "1.0.6"
  18
        18
             query = '''
        19
  19
  20
        20
             process where event.action == "exec" and
    Τ...
```

```
√ · ‡· 6 ■■■■□

behavior/rules/defense_evasion_attempt_to_disable_windows... [ ]
                @@ -4,7 +4,7 @@ id = "32ab2977-2932-4172-9117-
     .
                36e382591818"
   4
                license = "Elastic License v2"
   5
           5
                name = "Attempt to Disable Windows Defender
                Services"
                os_list = ["windows"]
   6
           6
   7
               - version = "1.0.4"
           7
              + version = "1.0.5"
   8
           8
   9
           9
                query = '''
  10
          10
                process where event.action == "start" and
                @@ -17,12 +17,14 @@ process where event.action ==
     .‡.
                 "start" and
  17
          17
                     process.parent.name : ("rundll32.exe",
                 "regsvr32.exe", "wscript.exe", "cscript.exe",
                 "powershell.exe", "mshta.exe"))
  18
          18
  19
          19
  20
               - optional_actions = []
  21
          20
                [[actions]]
  22
          21
                action = "kill_process"
                field = "process.entity_id"
  23
          22
```

```
24
          23
                state = 0
  25
          24
              + [[optional_actions]]
          25
          26
              + action = "rollback"
          27
  26
          28
                [[threat]]
  27
          29
                framework = "MITRE ATT&CK"
  28
          30
                 [[threat.technique]]
     Τ...
  behavior/rules/defense_evasion_binary_masquerading_via_un... 📙
                @@ -8,7 +8,7 @@ id = "35dedf0c-8db6-4d70-b2dc-
     .
                a133b808211f"
                license = "Elastic License v2"
   8
                name = "Binary Masquerading via Untrusted Path"
   9
           9
  10
          10
                os_list = ["windows"]
              - version = "1.0.12"
  11
          11
              + version = "1.0.13"
  12
          12
                query = '''
  13
          13
  14
                process where event.action == "start" and
          14
                @@ -49,11 +49,9 @@ process where event.action ==
     .
                 "start" and
  49
          49
                     "qprocess.exe",
  50
          50
                     "quser.exe",
  51
          51
                     "qwinsta.exe",
  52
                     "reg.exe",
  53
          52
                     "regasm.exe",
  54
          53
                     "regsvcs.exe",
  55
          54
                     "regsvr32.exe",
                     "runas.exe",
  56
  57
          55
                     "rundll32.exe",
  58
          56
                     "schtasks.exe",
  59
                     "sdclt.exe",
          57
                @@ -62,13 +60,11 @@ process where event.action ==
     -‡-
                 "start" and
                     "svchost.exe",
  62
          60
          61
                     "taskhost.exe",
  63
                     "taskhostw.exe",
  64
          62
                     "tasklist.exe",
  65
                     "userinit.exe",
  66
          63
  67
          64
                     "vaultcmd.exe",
```

```
68
          65
                     "vssadmin.exe",
  69
          66
                     "wininit.exe",
  70
          67
                     "winlogon.exe",
  71
                     "whoami.exe",
  72
          68
                     "wmic.exe",
                     "wevtutil.exe",
  73
          69
  74
          70
                     "wscript.exe",
                @@ -85,6 +81,7 @@ process where event.action ==
     .‡.
                 "start" and
                     "?:\\Windows\\Microsoft.NET\\*.exe",
  85
          81
          82
                     "?:\\Program Files (x86)\\*.exe",
  86
  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 ==
     <u></u>
                 "start" and
 152
        149
                   not (process.parent.executable :
                 "?:\\apps\\sage300\\Programs\\runtime\\a4wcontainer
                XP.exe" and process.name : "regsvr32.exe")
        150
                 1.1.1
 153
 154
        151
               - optional_actions = []
        152
 156
                [[actions]]
 157
        153
                action = "kill_process"
                field = "process.entity_id"
 158
         154
                state = 0
        155
 159
 160
         156
         157
              + [[optional_actions]]
        158
              + action = "rollback"
        159
 161
         160
                 [[threat]]
 162
         161
                framework = "MITRE ATT&CK"
 163
        162
                 [[threat.technique]]
     ....
 behavior/rules/defense_evasion_binary_proxy_execution_via... 📮
     †
                @@ -16,7 +16,7 @@ reference = [
```

```
16
       16
                  "https://lolbas-
              project.github.io/lolbas/Libraries/Url/",
       17
                  "https://lolbas-
17
              project.github.io/lolbas/Libraries/Desk/",
18
       18
19
            - version = "1.0.8"
       19
            + version = "1.0.9"
20
       20
       21
              query = '''
21
       22
22
              sequence with maxspan=1m
  .‡.
              @@ -32,15 +32,19 @@ sequence with maxspan=1m
32
       32
                          "*url.dll*FileProtocolHandler*.exe*",
                          "*shell32.dll*ShellExec_RunDLL*",
       33
33
                          "*advpack*LaunchINFSection*",
34
       34
                          "*desk*InstallScreenSaver*") and
35
                          "*desk*InstallScreenSaver*",
       35
       36
                         "*shell32*WaitForExplorerRestart*") and
       37
                 /* Issue #265 */
36
                 not (process.command_line :
37
       38
              "*url.dll*FileProtocolHandler*" and
38
       39
                      process.command_line : ("*http://*",
              "*zoommtg://*", "*://*&*&*")) and
39
       40
40
       41
                 /* Legit LaunchApplication instances via msdt */
41
       42
                 not (process.command line :
              "*pcwutl.dll,LaunchApplication*" and
42
       43
                      process.parent.name : "msdt.exe" and
43
                      process.working_directory :
              "?:\\Windows\\system32\\")] by process.entity_id
       44
                      process.working_directory :
              "?:\\Windows\\system32\\") and
       45
                 not (process.command line :
       46
              "*shell32*WaitForExplorerRestart*" and process.args
              : "?:\\Windows\\*explorer.exe")
       47
                 ] by process.entity_id
                [process where event.action == "start" and
44
       48
45
       49
                 not process.executable : ("?:\\Program
              Files\\*.exe", "?:\\Program Files (x86)\\*.exe")
              and
46
       50
                 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
       53
49
50
       54
```

```
51
         55
  52
              - optional_actions = []
  53
         56
                [[actions]]
  54
         57
                action = "kill_process"
  55
         58
                field = "process.entity_id"
                state = 1
  56
         59
  57
         60
         61
              + [[optional_actions]]
         62
              + action = "rollback"
         63
                [[threat]]
  58
         64
  59
         65
                framework = "MITRE ATT&CK"
  60
         66
                [[threat.technique]]
 behavior/rules/defense_evasion_control_panel_process_with... 📮
                @@ -7,12 +7,11 @@ id = "a4862afb-1292-4f65-a15f-
     .
                8d6a8019b5e2"
                license = "Elastic License v2"
          8
                name = "Control Panel Process with Unusual
   8
                Arguments"
   9
                os_list = ["windows"]
              - version = "1.0.6"
  10
         10
              + version = "1.0.8"
  11
         11
  12
         12
                query = '''
  13
         13
                process where event.action == "start" and
  14
         14
                 process.executable :
                ("?:\\Windows\\SysWOW64\\control.exe",
                "?:\\Windows\\System32\\control.exe") and
  15
         15
  16
                  process.command_line :
         16
  17
                           ("*.jpg*",
         17
  18
                           "*.png*",
                @@ -26,14 +25,8 @@ process where event.action ==
     .
                "start" and
  26
         25
                            "*..\\..\\*",
  27
         26
                            "*/AppData/Local/*",
  28
         27
                            "*:\\Users\\Public\\*",
  29
                            "*\\AppData\\Local\\*") or
  30
  31
                  (process.args_count == 1 and
```

```
32
                   not process.parent.executable :
                ("?:\\Windows\\Explorer.exe",
                "?:\\Windows\\System32\\Sihost.exe") and
                   process.parent.executable != null)
  33
  34
  35
                  ) and
  36
                            "*\\AppData\\Local\\*") and
         28
         29
                 /* excluding FPs where /name arg is used to
  37
         30
                specify a control by name */
                 not (process.args : "/name" and process.args_count
  38
         31
                >= 2) and
                 /* excluding system IL to minimize risk of killing
  39
         32
                system critical execution */
     ····
  behavior/rules/defense_evasion_crashdump_disabled_via_reg... [ ]
     <u></u>
                @@ -11,20 +11,23 @@ reference = [
         11
                    "https://elastic.github.io/security-
  11
                research/intelligence/2022/03/01.hermeticwiper-
                targets-ukraine/article/",
                    "https://docs.microsoft.com/en-
  12
         12
                us/troubleshoot/windows-server/performance/memory-
                dump-file-options",
  13
         13
              - version = "1.0.6"
  14
              + version = "1.0.7"
         14
  15
         15
                query = '''
         16
  16
  17
         17
                registry where registry.value : "CrashDumpEnabled"
                and registry.data.strings: "0" and
                 not (user.id in ("S-1-5-18", "S-1-5-19", "S-1-5-
  18
         18
                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
             + not process.executable :
                "?:\\Windows\\System32\\SystemPropertiesAdvanced.ex
```

```
1.1.1
  20
         21
  21
         22
  22
              - optional_actions = []
         23
  23
                [[actions]]
  24
         24
                action = "kill_process"
  25
         25
                field = "process.entity_id"
                state = 0
  26
         26
  27
         27
             + [[optional_actions]]
         28
         29
             + action = "rollback"
         30
  28
         31
                [[threat]]
  29
         32
                framework = "MITRE ATT&CK"
                [[threat.technique]]
  30
         33
     ....
 behavior/rules/defense_evasion_dll_control_panel_items_re... 📮
                @@ -0,0 +1,50 @@
          1 + [rule]
          2 + description = """
          3 + Identifies the modification of DLL Control Panel
                Items registry. Adversaries may load a malicious
                DLL when Control Panel
          4 + is executed via setting the CPLs subkey to the DLL
                path.
          5 + """
          6 + id = "340bdcad-187f-4ccb-b84e-34ee70844d78"
          7 + license = "Elastic License v2"
          8 + name = "DLL Control Panel Items Registry
                Modification"
          9 + os_list = ["windows"]
         10 + reference = ["https://docs.microsoft.com/en-
                us/previous-
                versions/windows/desktop/legacy/hh127454(v=vs.85)"]
         11 + version = "1.0.2"
         12 +
         13 + query = '''
         14 + registry where
         15
             + registry.path:
         16 +
                      ("HKEY_USERS\\S-1-5-
                *\\Software\\Microsoft\\Windows\\CurrentVersion\\Co
                ntrol Panel\\CPLs\\*",
```

```
17 +
      "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion
      \\Control Panel\\CPLs\\*") and
18 + process.executable != null and
      registry.data.strings != null and not
      registry.data.type : "REG_DWORD" and
19 + not (process.executable :
20
      ("?:\\Windows\\System32\\svchost.exe",
21 +
      "?:\\Windows\\System32\\DriverStore\\FileRepository
      \\*.exe",
22 +
      "?:\\Windows\\System32\\msiexec.exe") and user.id :
      ("S-1-5-18", "S-1-5-19", "S-1-5-20"))
23 + '''
24 +
25 + optional_actions = []
26 + [[actions]]
27 + action = "kill_process"
28 + field = "process.entity id"
29 + state = 0
30 +
31 + [[threat]]
32 + framework = "MITRE ATT&CK"
33 + [[threat.technique]]
34 + id = "T1218"
35 + name = "System Binary Proxy Execution"
36 + reference =
      "https://attack.mitre.org/techniques/T1218/"
37 + [[threat.technique.subtechnique]]
38 + id = "T1218.002"
39 + name = "Control Panel"
40 + reference =
      "https://attack.mitre.org/techniques/T1218/002/"
41
42 +
43 +
44 + [threat.tactic]
45 + id = "TA0005"
46 + name = "Defense Evasion"
47 + reference =
      "https://attack.mitre.org/tactics/TA0005/"
48
49
   + [internal]
```

```
50 + min_endpoint_version = "7.15.0"
 behavior/rules/defense_evasion_evasion_via_double_file_ex... 🖳
               @@ -0,0 +1,90 @@
          1 + [rule]
          2 + description = """
          3 + Adversaries may abuse a double extension or unicode
               right-to-left override (RTLO or RLO) character
               (U+202E) in the
          4 + filename as a means of masquerading the true file
               type. A file name may include a secondary file type
               extension that may
          5 + cause only the first extension to be displayed
               which maximize user execution likelihood.
          6 + """
          7 + id = "ccfca0c7-c975-4735-82bd-954ffbafd00b"
          8 + license = "Elastic License v2"
          9 + name = "Evasion via Double File Extension"
         10 + os_list = ["windows"]
         11 + reference =
               ["https://www.pcmag.com/encyclopedia/term/double-
               extension"]
         12 + version = "1.0.3"
         13 +
         14 + query = '''
         + process where event.action == "start" and
         16 + (
         17 + /* double extension in process.name */
         18 + process.name regex~ """.+(\.|\,|\_|\-)
               (pdf|doc|docx|xls|xlsx|png|jpg|html|txt|zip|rar|ppt
               |pptx|rtf|htm|GIF)\.(scr|exe|com|pif)""" or
         19 +
            + /* fake extension via Unicode Right-To-Left-
         20
               Override technique */
         21 + process.name : "*\u{202E}*"
         22 + ) and
         23
         24 + /* False Positives */
         25 + not process.hash.sha256:
         26
               ("1211cb4a560586d4ffb4b1bfd268a8146318af09587a9d5e3
               3703575d5178e77",
```

```
27 +
      "582ae3540ba32e7100fe20c0b01d14d1d85167cdb7ee512f59
      6544d7351a2d5e",
28 +
      "b59ac9390d9026ec3b552ebd6f3438c05aab2880d5e17616c1
      3c5d42b6b34c65",
29
      "a781c337575da892e6c1b2ac26a6272085a127c554dfd68729
      deb146eca6b837",
30
      "96234bb98b3266e49ef74ac7accd4644b709355057d5a34b29
      66e9fa56aadcf3",
31 +
      "38473e19af02cb5e6f386f41238da862df72bbc1d7a1e94d83
      8c4b93d6f56e72",
32 +
      "5d62d79f6555d7a7edaf3b175312b326df779f9ae8c893e218
      2e4159f44c9d34",
33
      "8d0434610280c8f94a0e9c29e4c33b97804fab4ab6fc29531b
      a76acebd2f5518",
34
      "7e59dec861a2a9ad68bd2758407c256dedb233cab225683db6
      77ab2d2fbec258",
35
      "fbd43f9a3567a19427894e61052d1b46f70b7474357ef50de9
      dc8749fc950509",
36 +
      "96234bb98b3266e49ef74ac7accd4644b709355057d5a34b29
      66e9fa56aadcf3") and
37 + not (process.executable : ("?:\\Program
      Files\\*.exe", "?:\\Program Files (x86)\\*.exe")
      and process.code_signature.trusted == true) and
38 + not (process.code_signature.subject_name :
      ("AVANQUEST SOFTWARE S.A.S", "Jernej Simončič") and
      process.code_signature.trusted == true)
39 + '''
40 +
41 + [[actions]]
42 + action = "kill process"
43 + field = "process.entity_id"
44 + state = 0
45
46 + [[optional_actions]]
47 + action = "rollback"
```

```
48 +
49 + [[threat]]
50 + framework = "MITRE ATT&CK"
51 + [[threat.technique]]
52 + id = "T1204"
53 + name = "User Execution"
54 + reference =
      "https://attack.mitre.org/techniques/T1204/"
+ [[threat.technique.subtechnique]]
56 + id = "T1204.002"
57 + name = "Malicious File"
   + reference =
58
      "https://attack.mitre.org/techniques/T1204/002/"
59
60 +
61 +
62 + [threat.tactic]
63 + id = "TA0002"
64 + name = "Execution"
65 + reference =
      "https://attack.mitre.org/tactics/TA0002/"
66 + [[threat]]
67 + framework = "MITRE ATT&CK"
68 + [[threat.technique]]
69 + id = "T1036"
70 + name = "Masquerading"
71 + reference =
      "https://attack.mitre.org/techniques/T1036/"
72 + [[threat.technique.subtechnique]]
73 + id = "T1036.002"
74 + name = "Right-to-Left Override"
75 + reference =
      "https://attack.mitre.org/techniques/T1036/002/"
76 +
77 + [[threat.technique.subtechnique]]
78 + id = "T1036.007"
79 + name = "Double File Extension"
   + reference =
80
      "https://attack.mitre.org/techniques/T1036/007/"
81 +
82 +
83 +
84 + [threat.tactic]
85 + id = "TA0005"
86 + name = "Defense Evasion"
```

```
87
             + reference =
                "https://attack.mitre.org/tactics/TA0005/"
         88 +
         89 + [internal]
         90 + min_endpoint_version = "7.15.0"
 behavior/rules/defense_evasion_execution_of_a_file_droppe... 「□
               @@ -0,0 +1,62 @@
        . . .
          1 + [rule]
          2 + description = """
          3 + Identifies when the OpenSSL utility create a file
                followed by it's execution. Malware authors may
                attempt to evade
          4 + detection and trick users into executing malicious
                code by encoding and encrypting their payload and
                placing it in a
          5 + disk image file. This behavior is consistent with
                adware or malware families such as Bundlore and
               Shlayer.
          6 + """
          7 + id = "d2017990-b448-4617-8d4a-55aa45abe354"
          8 + license = "Elastic License v2"
          9 + name = "Execution of a File Dropped by OpenSSL"
         10 + os_list = ["macos"]
         11 + reference =
                ["https://attack.mitre.org/software/S0482/",
               "https://attack.mitre.org/software/S0402/"]
         12 + version = "1.0.2"
         13 +
         14 + query = '''
             + sequence with maxspan=1m
         16 + [file where event.action != "deletion" and
               process.name == "openssl"] by file.path
             + [process where event.action == "exec"] by
               process.executable
         18 + '''
         19
         20 + optional_actions = []
         21 + [[actions]]
         22 + action = "kill process"
         23 + field = "process.entity_id"
         24 + state = 1
         25 +
```

```
26 + [[threat]]
27 + framework = "MITRE ATT&CK"
28 + [[threat.technique]]
29 + id = "T1204"
30 + name = "User Execution"
31 + reference =
      "https://attack.mitre.org/techniques/T1204/"
32 + [[threat.technique.subtechnique]]
33 + id = "T1204.002"
34 + name = "Malicious File"
35 + reference =
      "https://attack.mitre.org/techniques/T1204/002/"
36 +
37 +
38 +
39 + [threat.tactic]
40 + id = "TA0002"
41 + name = "Execution"
42 + reference =
      "https://attack.mitre.org/tactics/TA0002/"
43 + [[threat]]
44 + framework = "MITRE ATT&CK"
45 + [[threat.technique]]
46 + id = "T1027"
47 + name = "Obfuscated Files or Information"
48 + reference =
      "https://attack.mitre.org/techniques/T1027/"
49 +
50 + [[threat.technique]]
51 + id = "T1140"
52 + name = "Deobfuscate/Decode Files or Information"
53 + reference =
      "https://attack.mitre.org/techniques/T1140/"
54 +
55 +
56 + [threat.tactic]
57 + id = "TA0005"
58 + name = "Defense Evasion"
59 + reference =
      "https://attack.mitre.org/tactics/TA0005/"
60 +
61 + [internal]
62 + min_endpoint_version = "7.15.0"
```

```
behavior/rules/defense_evasion_execution_via_internet_exp... 📮
     <u>†</u>
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
                name = "Execution via Internet Explorer Exporter"
   8
           8
   9
           9
                os_list = ["windows"]
                reference = ["https://lolbas-
  10
          10
                 project.github.io/lolbas/Binaries/Extexport/"]
  11
              - version = "1.0.8"
              + version = "1.0.9"
          11
  12
          12
  13
          13
                query = '''
  14
          14
                 sequence by user.id with maxspan=5m
                @@ -20,12 +20,14 @@ sequence by user.id with
     .‡.
                maxspan=5m
  20
          20
                                             "?:\\Program
                 Files\\Internet Explorer\\ExtExport.exe")]
          21
  21
  22
          22
              - optional_actions = []
  23
  24
          23
                [[actions]]
  25
                action = "kill_process"
          24
                field = "process.entity_id"
  26
          25
  27
          26
                state = 1
  28
          27
          28
              + [[optional_actions]]
          29
              + action = "rollback"
          30
  29
          31
                 [[threat]]
          32
                framework = "MITRE ATT&CK"
  30
  31
          33
                 [[threat.technique]]
     ....
```

```
behavior/rules/defense_evasion_execution_via_renamed_sign... 🕌
     <u></u>
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
                name = "Execution via Renamed Signed Binary Proxy"
   8
          8
   9
          9
                os_list = ["windows"]
                reference = ["https://lolbas-project.github.io"]
  10
         10
              - version = "1.0.9"
  11
             + version = "1.0.10"
         11
```

```
12
         12
  13
         13
                query = '''
  14
         14
                process where event.action == "start" and
     T
                @@ -55,16 +55,17 @@ process where event.action ==
     .
                "start" and
  55
         55
                           "\\Device\\HarddiskVolume*\\Program Files
                (x86)\*.exe",
  56
         56
                           "\\Device\\HarddiskVolume*\\Program
                Files\\*.exe"
                        ) and
  57
         57
                  not (process.pe.original_file_name in
  58
                ("RegAsm.exe", "REGSVR32.EXE") and
                process.executable :
                "?:\\Windows\\Installer\\MSI*.tmp" and
  59
                       process.parent.executable :
                "?:\\WINDOWS\\system32\\msiexec.exe")
         58
             + not (process.executable :
                "?:\\Windows\\Installer\\MSI*.tmp" and
                process.parent.name : "msiexec.exe")
         59
  60
  61
         60
              - optional_actions = []
  62
                [[actions]]
  63
         61
  64
         62
                action = "kill_process"
                field = "process.entity id"
  65
         63
                state = 0
  66
         64
  67
         65
         66
              + [[optional_actions]]
              + action = "rollback"
         67
         68
  68
         69
                [[threat]]
                framework = "MITRE ATT&CK"
  69
         70
  70
         71
                [[threat.technique]]
 behavior/rules/defense_evasion_indirect_command_execution... 📮
     <u></u>
                @@ -8,21 +8,26 @@ license = "Elastic License v2"
                name = "Indirect Command Execution via Console
   8
           8
                Window Host"
   9
          9
                os_list = ["windows"]
                reference = ["https://lolbas-
  10
         10
                project.github.io/lolbas/Binaries/Conhost/"]
```

```
11
              - version = "1.0.1"
              + version = "1.0.2"
          12
  12
  13
          13
                query = '''
  14
          14
                process where event.action == "start" and
  15
          15
                  process.parent.name : "conhost.exe" and
                process.parent.args_count >= 2 and
          16
                  process.parent.command_line : "*conhost* *.exe*"
  16
                and
  17
              - not process.command_line :
                 ("?:\\windows\\system32\\cmd.exe",
                 "?:\\windows\\SysWOW64\\cmd.exe", "cmd.exe")
                  not process.command_line :
          17
                             ("?:\\windows\\system32\\cmd.exe",
          18
                              "?:\\windows\\SysWOW64\\cmd.exe",
          19
                 "cmd.exe",
          20
                 "?:\\windows\\system32\\windowspowershell\\*\\power
                 shell.exe")
                 1.1.1
  18
          21
  19
          22
              - optional_actions = []
  20
          23
                [[actions]]
  21
  22
          24
                action = "kill_process"
                field = "process.entity_id"
  23
          25
  24
                state = 0
          26
  25
          27
          28
              + [[optional_actions]]
          29
              + action = "rollback"
          30
                [[threat]]
  26
          31
                framework = "MITRE ATT&CK"
  27
          32
                 [[threat.technique]]
  28
          33
     Τ...

✓ 43 ■■■■■
                                                                   . . .
behavior/rules/defense_evasion_indirect_command_execution... 📮
                @@ -0,0 +1,43 @@
         . . .
          1 + [rule]
           2 + description = """
           3 + Identifies the use of native Windows tool, forfiles
                to execute a file. Adversaries may abuse utilities
                that allow for
```

```
4 + command execution to bypass security restrictions
      that limit the use of command-line interpreters.
 5 + """
6 + id = "78afa378-d1c4-4b83-a261-ce1c90f1cbf9"
7 + license = "Elastic License v2"
8 + name = "Indirect Command Execution via ForFiles"
9 + os_list = ["windows"]
10 + reference = ["https://lolbas-
      project.github.io/lolbas/Binaries/Forfiles/"]
11 + version = "1.0.3"
12 +
13 + query = '''
14 + process where event.action == "start" and
15 + process.parent.name : "forfiles.exe" and
     process.parent.args : "/c" and
16 + process.parent.args : "/p" and
      process.parent.args: "/m" and
17
18 + 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
20
   + not (process.name : "cmd.exe" and process.args:
      ("del", "xcopy", "cmd /c del @PATH", "move"))
21 + '''
22 +
23 + optional_actions = []
24 + [[actions]]
25 + action = "kill_process"
26 + field = "process.entity_id"
27 + state = 0
28 +
29 + [[threat]]
30 + framework = "MITRE ATT&CK"
31 + [[threat.technique]]
32 + id = "T1202"
33 + name = "Indirect Command Execution"
34 + reference =
      "https://attack.mitre.org/techniques/T1202/"
35 +
36 +
37 + [threat.tactic]
38 + id = "TA0005"
39 + name = "Defense Evasion"
```

```
40
             + reference =
                "https://attack.mitre.org/tactics/TA0005/"
         41 +
         42 + [internal]
         43 + min_endpoint_version = "7.15.0"
 behavior/rules/defense_evasion_macos_monterey_reflective_... 📮
    †
                @@ -11,7 +11,7 @@ reference = [
  11
         11
                    "https://slyd0g.medium.com/understanding-and-
                defending-against-reflective-code-loading-on-macos-
                e2e83211e48f",
  12
         12
                "https://github.com/slyd0g/SwiftInMemoryLoading",
         13
  13
              - version = "1.0.4"
  14
         14
              + version = "1.0.5"
         15
  15
         16
                query = '''
  16
                file where event.type != "deletion" and
  17
         17
     +
 behavior/rules/defense_evasion_managed_.net_code_executio... 🖳
                @@ -7,7 +7,7 @@ id = "cd886776-8790-4724-9484-"
    .
                3f0008b87da7"
                license = "Elastic License v2"
   7
          7
                name = "Managed .NET Code Execution via PowerShell"
   8
          8
   9
          9
                os_list = ["windows"]
              - version = "1.0.4"
  10
              + version = "1.0.5"
         10
         11
  11
  12
         12
                query = '''
  13
         13
                process where event.type == "start" and
                @@ -22,7 +22,9 @@ process where event.type ==
     .‡.
                "start" and
  22
         22
                   "*set *set *set *", "*;iex*", "*IEX (*",
                "*FromBase64String*")
```

) and

2324

23

24

```
25
                    not process.parent.args : ("?:\\Program Files
                 (x86)\\*", "?:\\Program Files\\*")
                    not process.parent.args : ("?:\\Program Files
          25
                 (x86)\\*", "?:\\Program Files\\*",
                 "visualstudio20??-workload-vctools;") and
          26
                    not process.args :
                 "@?:\\Windows\\TEMP\\*.cmdline" and
          27
                    not (process.parent.args : "-ExecutionPolicy"
                 and process.parent.command_line :
                 "*.vscode\\extensions*")
          28
  26
  27
          29
  28
          30
                optional_actions = []
     ....
 ...ior/rules/defense_evasion_managed_.net_code_execution_... 「  
     <u>†</u>
                @@ -12,7 +12,7 @@ reference = [
  12
          12
                     "https://github.com/med0x2e/GadgetToJScript",
  13
          13
                 "https://github.com/mdsecactivebreach/SharpShooter"
          14
                 1
  14
               - version = "1.0.5"
  15
          15
               + version = "1.0.6"
  16
          16
                 query = '''
  17
          17
  18
                 sequence by process.entity_id with maxspan=2m
          18
                 @@ -38,12 +38,14 @@ sequence by process.entity_id
     .
                 with maxspan=2m
  38
          38
                                 "msxsl.exe.log")]
                 \mathbf{r}_{-} = \mathbf{r}_{-}
  39
          39
  40
          40
  41
               - optional_actions = []
  42
          41
                 [[actions]]
  43
          42
                 action = "kill_process"
                field = "process.entity_id"
  44
          43
  45
          44
                 state = 0
  46
          45
          46
               + [[optional_actions]]
          47
               + action = "rollback"
          48
  47
          49
                 [[threat]]
```

```
48
         50
                framework = "MITRE ATT&CK"
  49
         51
                [[threat.technique]]
     ····
 behavior/rules/defense_evasion_modification_of_safari_set... 📮
     .
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
                name = "Modification of Safari Settings via
   8
                Defaults Command"
   9
          9
                os_list = ["macos"]
  10
         10
                reference =
                ["https://objectivebythesea.com/v2/talks/OBTS_v2_Zo
                har.pdf"]
              - version = "1.0.6"
  11
              + version = "1.0.7"
         11
  12
         12
                query = '''
  13
         13
  14
         14
                process where event.type == "start" and
     Τ...
```

```
behavior/rules/defense_evasion_msbuild_with_unusual_argum... 📮
     .
                 @@ -8,7 +8,7 @@ license = "Elastic License v2"
                 name = "MSBuild with Unusual Arguments"
                 os_list = ["windows"]
   9
           9
          10
                 reference = ["https://lolbas-
  10
                 project.github.io/lolbas/Binaries/Msbuild/"]
               - version = "1.0.6"
  11
              + version = "1.0.7"
          11
  12
          12
                 query = '''
  13
          13
  14
          14
                 process where event.action == "start" and
                 @@ -32,12 +32,14 @@ process where event.action ==
     .‡.
                 "start" and
  32
          32
                                             "msaccess.exe"))
                 \mathbf{r}_{-1}, \mathbf{r}_{-1}
          33
  33
  34
          34
  35
               - optional_actions = []
          35
                 [[actions]]
  36
  37
                 action = "kill_process"
          36
  38
                 field = "process.entity_id"
```

```
39
          38
                state = 0
  40
          39
              + [[optional_actions]]
          40
          41
              + action = "rollback"
          42
  41
          43
                [[threat]]
  42
          44
                framework = "MITRE ATT&CK"
  43
          45
                 [[threat.technique]]
     Τ...
 behavior/rules/defense_evasion_network_connection_via_pro... 📮
                @@ -8,7 +8,7 @@ id = "95601d8b-b969-4189-9744-
     .
                090140ae29e6"
                license = "Elastic License v2"
           8
   8
   9
           9
                name = "Network Connection via Process with Unusual
                Arguments"
  10
          10
                os_list = ["windows"]
              - version = "1.0.9"
  11
          11
              + version = "1.0.10"
  12
          12
                query = '''
          13
  13
  14
                sequence by process.entity_id with maxspan=5m
          14
     ....
                @@ -52,12 +52,14 @@ sequence by process.entity_id
     <u></u>
                with maxspan=5m
  52
          52
                   [network where event.action ==
                 "connection_attempted"]
  53
          53
  54
          54
  55
               - optional_actions = []
  56
          55
                [[actions]]
                action = "kill_process"
  57
          56
  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]]
     +
```

```
behavior/rules/defense_evasion_ntdll_loaded_from_an_unusu... 📮
                @@ -7,7 +7,7 @@ id = "3205274e-7eb0-4765-a712-
     <u></u>
                5783361091ae"
                license = "Elastic License v2"
   7
           7
           8
                name = "NTDLL Loaded from an Unusual Path"
   8
   9
           9
                os_list = ["windows"]
              - version = "1.0.4"
  10
              + version = "1.0.5"
          10
  11
          11
  12
          12
                query = '''
  13
          13
                library where dll.pe.original_file_name :
                "ntdll.dll" and
                @@ -16,17 +16,20 @@ library where
     ....
                dll.pe.original_file_name : "ntdll.dll" and
          16
  16
                "?:\\Windows\\System32\\ntdll.dll",
  17
          17
                "?:\\Windows\\WinSxS\\amd64_microsoft-windows-
                ntdll_*\\ntdll.dll",
  18
          18
                "?:\\Windows\\WinSxS\\wow64_microsoft-windows-
                ntdll_*\\ntdll.dll",
          19
                "?:\\Windows\\WinSxS\\Temp\\InFlight\\*\\amd64_micr
                osoft-windows-ntdll_*\\ntdll.dll",
  19
          20
                                  /* vsmbSharePrefix */
                                  "\\Device\\vmsmb\\VSMB-
  20
          21
                {*}\\os\\windows\\*\\ntdll.dll",
  21
          22
                "?:\\Windows\\WinSxS\\Temp\\PendingDeletes\\$$Delet
                eMe*")
                0.00
  22
          23
  23
          24
  24
              - optional_actions = []
          25
                [[actions]]
  25
  26
          26
                action = "kill_process"
                field = "process.entity_id"
  27
          27
                state = 0
  28
          28
  29
          29
              + [[optional_actions]]
          30
              + action = "rollback"
          31
          32
```

```
30
         33
               [[threat]]
  31
         34
               framework = "MITRE ATT&CK"
                [[threat.technique]]
  32
         35
    +
 behavior/rules/defense_evasion_operating_system_security_... 📮
    .
               @@ -8,7 +8,7 @@ license = "Elastic License v2"
               name = "Operating System Security Updates Disabled"
   8
   9
          9
               os_list = ["macos"]
               reference =
  10
         10
               ["https://blog.checkpoint.com/2017/07/13/osxdok-
               refuses-go-away-money/"]
              - version = "1.0.5"
  11
             + version = "1.0.6"
         11
  12
         12
               query = '''
  13
         13
  14
         14
               process where event.type == "start" and
     Τ...
 behavior/rules/defense_evasion_parent_process_pid_spoofin... 📮
    .
               @@ -8,7 +8,7 @@ license = "Elastic License v2"
               name = "Parent Process PID Spoofing"
   9
          9
               os_list = ["windows"]
         10
               reference =
  10
                ["https://blog.didierstevens.com/2017/03/20/"]
              - version = "1.0.9"
  11
             + version = "1.0.10"
         11
  12
         12
               query = '''
  13
         13
                sequence with maxspan=5m
  14
         14
     Τ.
 behavior/rules/defense_evasion_payload_decoded_and_decryp... 📮
               @@ -0,0 +1,76 @@
          1 + [rule]
          2 + description = """
```

```
3 + Identifies when a built-in utility is used to
      decode and decrypt a payload after a macOS disk
      image (DMG) is executed.
4 + Malware authors may attempt to evade detection and
      trick users into executing malicious code by
      encoding and encrypting
 5 + their payload and placing it in a disk image file.
      This behavior is consistent with adware or malware
      families such as
6 + Bundlore and Shlayer.
7 + """
8 + id = "5dce3865-838f-4773-9781-87226af1fc12"
9 + license = "Elastic License v2"
10 + name = "Payload Decoded and Decrypted via Built-In
      Utilities"
11 + os_list = ["macos"]
12 + reference =
      ["https://attack.mitre.org/software/S0482/",
      "https://attack.mitre.org/software/S0402/"]
13 + version = "1.0.7"
14 +
15 + query = '''
+ process where event.action == "exec" and
      process.name == "openssl" and
17 + process.args : "/Volumes/*" and process.args :
      "enc" and
        // openssl base64-decoding data
18
19
          process.args: "-base64" and
20 +
         // openssl decrypting input data
          process.args : "-d"
21 +
22 + '''
23 +
24 + optional_actions = []
25 + [[actions]]
26 + action = "kill_process"
27 + field = "process.entity_id"
28 + state = 0
29 +
30 + [[threat]]
31 + framework = "MITRE ATT&CK"
32 + [[threat.technique]]
33 + id = "T1059"
34 + name = "Command and Scripting Interpreter"
35 + reference =
      "https://attack.mitre.org/techniques/T1059/"
```

```
36 + [[threat.technique.subtechnique]]
37 + id = "T1059.004"
38 + name = "Unix Shell"
39 + reference =
      "https://attack.mitre.org/techniques/T1059/004/"
40 +
41 +
42 + [[threat.technique]]
43 + id = "T1204"
44 + name = "User Execution"
45 + reference =
      "https://attack.mitre.org/techniques/T1204/"
46 + [[threat.technique.subtechnique]]
47 + id = "T1204.002"
48 + name = "Malicious File"
49 + reference =
      "https://attack.mitre.org/techniques/T1204/002/"
50
51 +
52 +
53 + [threat.tactic]
54 + id = "TA0002"
55 + name = "Execution"
56 + reference =
      "https://attack.mitre.org/tactics/TA0002/"
57 + [[threat]]
58 + framework = "MITRE ATT&CK"
59 + [[threat.technique]]
60 + id = "T1027"
61 + name = "Obfuscated Files or Information"
62 + reference =
      "https://attack.mitre.org/techniques/T1027/"
63 +
64 + [[threat.technique]]
65 + id = "T1140"
66 + name = "Deobfuscate/Decode Files or Information"
67 + reference =
      "https://attack.mitre.org/techniques/T1140/"
68
69 +
70 + [threat.tactic]
71 + id = "TA0005"
72 + name = "Defense Evasion"
73 + reference =
      "https://attack.mitre.org/tactics/TA0005/"
```

```
74 +
         75 + [internal]
         76 + min_endpoint_version = "7.15.0"
 behavior/rules/defense_evasion_potential_binary_masquerad... 「  
                @@ -7,13 +7,13 @@ id = "4154c8ce-c718-4641-80db-
     .
                a6a52276f1a4"
                license = "Elastic License v2"
   7
          7
   8
                name = "Potential Binary Masquerading via Invalid
                Code Signature"
   9
          9
                os_list = ["macos"]
              - version = "1.0.4"
  10
              + version = "1.0.5"
         10
  11
         11
  12
         12
                query = '''
  13
         13
                process where event.action == "exec" and
                 process.name : "com.apple.*" and
  14
         14
  15
         15
                 (process.code signature.trusted == false or
                process.code_signature.exists == false) and
              - not (process.code_signature.subject_name :
  16
                "Software Signing" and
             + not (process.code_signature.subject_name :
                ("Software Signing", "com.apple.WebKit.Networking",
                "com.apple.WebKit.WebContent") and
  17
         17
                      process.name :
         18
  18
                ("com.apple.WebKit.WebContent.Development",
  19
         19
                            "com.apple.WebKit.GPU.Development",
     Τ...
```

```
...r/rules/defense_evasion_potential_defense_evasion_via_... 📮
    <u></u>
               @@ -5,7 +5,7 @@ license = "Elastic License v2"
   5
          5
               name = "Potential Defense Evasion via Filter
               Manager Control Program"
               os_list = ["windows"]
   6
          6
   7
          7
               reference = ["https://lolbas-
                project.github.io/lolbas/Binaries/FltMC/"]
              - version = "1.0.6"
   8
             + version = "1.0.7"
          8
```

```
10
         10
                query = '''
  11
         11
                process where event.action == "start" and
     ····
  ✓ 62 ■■■■■
                                                                 . . .
behavior/rules/defense_evasion_potential_evasion_via_over... 📮
                @@ -0,0 +1,62 @@
         . . .
          1 + [rule]
          2 + description = """
          3 + Adversaries may use binary padding to add junk data
                and change the on-disk representation of malware.
                This can be done
          4 + without affecting the functionality or behavior of
                a binary, but can increase the size of the binary
                beyond what some
          5 + security tools are capable of handling due to file
                size limitations
          6 + """
          7 + id = "65a402ff-904b-4d14-b7aa-fa0c5ae575f8"
          8 + license = "Elastic License v2"
             + name = "Potential Evasion via Oversized Image Load"
         10 + os_list = ["windows"]
         11 + reference =
                ["https://attack.mitre.org/techniques/T1027/001/"]
         12 + version = "1.0.2"
         13
         14 + query = '''
             + sequence with maxspan=1m
         15
         16 + [file where event.action != "deletion" and
                   /* over 100MB in size */
         17
                   file.size >= 100000000 and file.Ext.header_bytes
         18
                : "4d5a*" and not file.extension : "exe" and
                   not user.id: "S-1-5-18"] by file.path
         19
             + [library where
         20
         21
                    (
         22
                     process.name : ("rundll32.exe",
                "regsvr32.exe", "svchost.exe") or
                     process.executable :
         23
         24
                               ("?:\\Users\\Public\\*",
         25
                                "?:\\ProgramData\\*",
                                "?:\\Windows\\Temp\\*",
         26
         27
                "?:\\Users\\*\\AppData\\Local\\Temp\\Temp?_*",
```

```
28
      "?:\\Users\\*\\AppData\\Local\\Temp\\7z*",
29
      "?:\\Users\\*\\AppData\\Local\\Temp\\Rar*",
30
      "?:\\Users\\*\\AppData\\Local\\Temp\\BNZ.*")
31
           )
          and not dll.code_signature.trusted == true and
32
          not dll.code_signature.status : "errorExpired"
33
      and
          not user.id : "S-1-5-18"] by dll.path
34
35 + '''
36 +
37 + optional_actions = []
38 + [[actions]]
39 + action = "kill_process"
   + field = "process.entity_id"
40
41 + state = 1
42 +
43 + [[threat]]
44 + framework = "MITRE ATT&CK"
45 + [[threat.technique]]
46 + id = "T1027"
47
   + name = "Obfuscated Files or Information"
48 + reference =
      "https://attack.mitre.org/techniques/T1027/"
49 + [[threat.technique.subtechnique]]
50 + id = "T1027.001"
51 + name = "Binary Padding"
52 + reference =
      "https://attack.mitre.org/techniques/T1027/001/"
53
54 +
55 +
56 + [threat.tactic]
57 + id = "TA0005"
58 + name = "Defense Evasion"
59
   + reference =
      "https://attack.mitre.org/tactics/TA0005/"
60
61 + [internal]
  + min_endpoint_version = "7.16.0"
```

```
behavior/rules/defense_evasion_potential_initial_access_v...
```

```
@@ -0,0 +1,72 @@
1 + [rule]
2 + description = """
3 + Identifies attempts to create a DLL file to a known
      desktop application dependencies folder such as
      Slack, Teams or
4 + OneDrive and by an unusual process. This may
      indicate an attempt to load a malicious module via
      DLL search order
 5 + hijacking.
6 + """
7 + id = "ddc4fa22-4675-44c0-a813-e786e638d7e0"
8 + license = "Elastic License v2"
9 + name = "Potential Initial Access via DLL Search
      Order Hijacking"
10 + os_list = ["windows"]
11 + reference =
      ["https://posts.specterops.io/automating-dll-
      hijack-discovery-81c4295904b0"]
12 + version = "1.0.2"
13 +
14 + query = '''
15 + file where event.action != "deletion" and
16 + file.extension : "dll" and
17 + file.path:
18 +
      ("?:\\Users\\*\\AppData\\*\\Microsoft\\OneDrive\\*.
      dll",
19
               "?:\\Users\\*\\AppData\\*\\Microsoft
      OneDrive\\*.dll",
20
      "?:\\Users\\*\\AppData\\*\\Microsoft\\Teams\\*.dll"
              "?:\\Users\\*\\AppData\\Local\\slack\\app-
21
      *\\*.dll",
22 +
      "?:\\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",
24 +
      "cscript.exe", "wscript.exe", "curl.exe",
      "powershell.exe", "pwsh.exe") and
```

```
25 + not (process.name : "cmd.exe" and file.path
      :"?:\\Users\\*\\AppData\\*\\Microsoft\\OneDrive\\*\
      \api-ms-win-core-*.dll")
26 + '''
27 +
28 + [[actions]]
29 + action = "kill_process"
30 + field = "process.entity_id"
31 + state = 0
32 +
33 + [[optional_actions]]
34 + action = "rollback"
35 +
36 + [[threat]]
37 + framework = "MITRE ATT&CK"
38 + [[threat.technique]]
39 + id = "T1566"
40 + name = "Phishing"
41 + reference =
      "https://attack.mitre.org/techniques/T1566/"
42 + [[threat.technique.subtechnique]]
43 + id = "T1566.001"
44 + name = "Spearphishing Attachment"
   + reference =
      "https://attack.mitre.org/techniques/T1566/001/"
46 +
47 +
48 +
49 + [threat.tactic]
50 + id = "TA0001"
51 + name = "Initial Access"
52 + reference =
      "https://attack.mitre.org/tactics/TA0001/"
53 + [[threat]]
54 + framework = "MITRE ATT&CK"
55 + [[threat.technique]]
56 + id = "T1574"
57 + name = "Hijack Execution Flow"
58 + reference =
      "https://attack.mitre.org/techniques/T1574/"
+ [[threat.technique.subtechnique]]
60 + id = "T1574.001"
61 + name = "DLL Search Order Hijacking"
62 + reference =
      "https://attack.mitre.org/techniques/T1574/001/"
```

```
63
         64
              +
         65 +
         66 + [threat.tactic]
         67
             + id = "TA0005"
         68 + name = "Defense Evasion"
              + reference =
         69
                "https://attack.mitre.org/tactics/TA0005/"
         70
         71 + [internal]
             + min_endpoint_version = "7.15.0"
 behavior/rules/defense_evasion_potential_masquerading_as_... 📮
                @@ -7,14 +7,16 @@ id = "5b00c9ba-9546-47cc-8f9f-
     <u></u>
                1c1a3e95f65c"
   7
           7
                license = "Elastic License v2"
                name = "Potential Masquerading as SVCHOST"
   8
          8
   9
                os_list = ["windows"]
              - version = "1.0.7"
  10
              + version = "1.0.9"
         10
  11
         11
                query = '''
  12
         12
         13
  13
                process where event.action == "start" and
                  process.name : "svchost.exe" and
  14
         14
                  process.parent.executable != null and
  15
         15
  16
         16
                  not process.parent.executable : (
  17
         17
                    "?:\\Windows\\System32\\services.exe",
         18
                    "\\Device\\HarddiskVolume?
                \\Windows\\System32\\services.exe",
         19
                    "\\Device\\HarddiskVolume??
                \\Windows\\System32\\services.exe",
  18
         20
                    "?:\\ProgramData\\Microsoft\\Windows
                Defender\\Platform\\*\\MsMpEng.exe",
  19
         21
                    "?:\\Program Files\\Microsoft Security
                Client\\MsMpEng.exe",
  20
         22
                    "?:\\Program Files*\\Windows
                Defender\\MsMpEng.exe",
                @@ -24,6 +26,7 @@ process where event.action ==
     .
                "start" and
         26
                    "?:\\Program Files*\\Unity Client\\Unity.exe",
  24
  25
         27
                    "?:\\Windows\\System32\\wermgr.exe",
                    "?:\\Windows\\System32\\svchost.exe",
  26
         28
         29
                    "?:\\WINDOWS\\SysWOW64\\svchost.exe",
```

```
27
         30
                "\\Device\\VhdHardDisk*\\Windows\\System32\\service
                s.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
         47
                 not (process.pe.original_file_name ==
  44
                "AsDVDLock.exe" and
         48
                      process.executable : "?:\\Program Files
  45
                (x86)\\ASUS\\ASUS Manager\\USB Lock\\svchost.exe")
                 not (process.parent.executable :
  46
                "?:\\Windows\\System32\\svchost.exe" and
  47
                      process.parent.args : "ClipboardSvcGroup"
                and process.executable :
                "?:\\Windows\\System32\\svchost.exe")
             + not (process.parent.executable :
         49
               "?:\\Windows\\System32\\svchost.exe" and
                process.executable :
                "?:\\Windows\\System32\\svchost.exe")
  48
         50
         51
  49
  50
              - optional_actions = []
  51
         52
               [[actions]]
         53
               action = "kill_process"
  52
  53
         54
               field = "process.entity_id"
  54
         55
                state = 0
  55
         56
         57
             + [[optional_actions]]
         58
             + action = "rollback"
         59
                [[threat]]
  56
         60
  57
         61
                framework = "MITRE ATT&CK"
  58
                [[threat.technique]]
         62
     ....
 <u>†</u>
               @@ -8,7 +8,7 @@ license = "Elastic License v2"
```

```
8
          8
                name = "Potential Parent Process PID Spoofing via
                MalSecLogon"
   9
          9
                os_list = ["windows"]
  10
         10
                reference =
                ["https://splintercod3.blogspot.com/p/the-hidden-
                side-of-seclogon-part-2.html"]
              - version = "1.0.9"
  11
         11
              + version = "1.0.11"
  12
         12
         13
                query = '''
  13
  14
         14
                sequence with maxspan=1m
                @@ -56,7 +56,8 @@ sequence with maxspan=1m
     †
  56
         56
                    not process.executable :
                ("?:\\Windows\\System32\\SpecopsClient\\SecuredBrow
                serNet\\*.exe",
                "?:\\Windows\\System32\\DriverStore\\FileRepository
                \\*\\SamsungSystemSupportOSD.exe") and
  57
         57
                    not (process.executable :
                "?:\\Windows\\SysWOW64\\OneDriveSetup.exe" and
                process.parent.executable :
                "?:\\Windows\\SysWOW64\\OneDriveSetup.exe") and
  58
         58
  59
                    not process.parent.executable :
                "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows
                erNet\\SecuredBrowserDotNetLauncher.exe"
         59
                    not process.parent.executable :
                "?:\\Windows\\System32\\SpecopsClient\\SecuredBrows
                erNet\\SecuredBrowserDotNetLauncher.exe" and
                    not process.executable :
         60
                "?:\\Windows\\System32\\DriverStore\\FileRepository
                \\*.exe"
                    ] by process.parent.Ext.real.entity_id
  60
         61
         62
  61
  62
         63
     ....
 ...ior/rules/defense_evasion_potential_privacy_control_by... 📮
    †
                @@ -11,7 +11,7 @@ os_list = ["macos"]
  11
         11
                reference = [
  12
         12
                    "https://blog.trendmicro.com/trendlabs-
                security-intelligence/xcsset-mac-malware-infects-
```

```
xcode-projects-performs-uxss-attack-on-safari-
                other-browsers-leverages-zero-day-exploits/",
                1
  13
         13
  14
              - version = "1.0.5"
              + version = "1.0.6"
          14
  15
          15
                query = '''
          16
  16
  17
          17
                process where event.type == "start" and
     Τ...
 behavior/rules/defense_evasion_potential_self_deletion_of... 💾
     †
                @@ -9,7 +9,7 @@ license = "Elastic License v2"
   9
           9
                name = "Potential Self Deletion of a Running
                Executable"
          10
                os_list = ["windows"]
  10
                reference = ["https://github.com/LloydLabs/delete-
  11
                self-poc"]
              - version = "1.0.6"
  12
          12
              + version = "1.0.7"
  13
          13
                query = '''
  14
          14
  15
          15
                sequence by process.entity_id with maxspan=1m
                @@ -20,12 +20,14 @@ sequence by process.entity_id
     ....
                with maxspan=1m
  20
          20
                     file.name : "*:*" and not
                file.Ext.original.name : "*:*" and file.size == 0]
                by file.Ext.original.name
                . . .
  21
          21
  22
          22
  23
              - optional_actions = []
  24
          23
                [[actions]]
  25
          24
                action = "kill_process"
  26
          25
                field = "process.entity_id"
  27
          26
                state = 0
  28
          27
          28
              + [[optional_actions]]
          29
              + action = "rollback"
          30
  29
          31
                [[threat]]
  30
          32
                framework = "MITRE ATT&CK"
  31
          33
                [[threat.technique]]
```

```
behavior/rules/defense_evasion_process_executable_image_t... 📮
     †
                @@ -13,13 +13,15 @@ license = "Elastic License v2"
         13
                name = "Process Executable Image Tampering Attempt"
  13
  14
         14
                os_list = ["windows"]
                reference = ["https://www.elastic.co/blog/process-
  15
         15
                ghosting-a-new-executable-image-tampering-attack"]
              - version = "1.0.8"
  16
              + version = "1.0.9"
         16
  17
         17
  18
         18
                query = '''
         19
                process where event.action == "start" and
  19
                  process.Ext.defense_evasions : "Process
  20
         20
                Tampering: Image is locked for access" and
                  not (process.code_signature.subject_name in
  21
         21
                ("Arcserve (USA) LLC", "CA") and
                process.code signature.trusted == true and
                       process.executable : "?:\\Program
  22
                Files\\CA\\*.exe")
                       process.executable : "?:\\Program
         22
                Files\\CA\\*.exe") and
            + not (process.executable :
         23
                "?:\\Windows\\System32\\esentutl.exe" and
                process.args: "/K" and
                       process.parent.executable : "?:\\Program
         24 +
                Files\\CA\\SharedComponents\\ARCserve
                Backup\\UniAgent\\caagstart.exe")
         25
  23
  24
         26
  25
         27
                optional_actions = []
```

```
behavior/rules/defense_evasion_protected_process_light_by... 📮
     <u></u>
                @@ -11,7 +11,7 @@ license = "Elastic License v2"
  11
         11
                name = "Protected Process Light Bypass via DLL
                Tampering"
  12
         12
                os_list = ["windows"]
  13
         13
                reference =
                ["https://googleprojectzero.blogspot.com/2018/08/wi
                ndows-exploitation-tricks-exploiting.html"]
```

```
14
              - version = "1.0.9"
         14
              + version = "1.0.10"
         15
  15
         16
                query = '''
  16
  17
         17
                sequence by process.entity_id with maxspan=3s
                @@ -35,7 +35,10 @@ sequence by process.entity_id
     .
                with maxspan=3s
  35
         35
                  not process.executable : "?:\\Program Files
                (x86)\\Common Files\\BattlEye\\BEService.exe" and
                  /* potential services child processes */
  36
         36
  37
         37
                  not (process.executable :
                "?:\\Windows\\System32\\services.exe" and dll.name
                : "*.exe") and
              - not dll.path :
  38
                "?:\\Windows\\WinSxS\\Temp\\PendingDeletes\\$$Delet
                eMe*"]
         38
             + not dll.path:
                "?:\\Windows\\WinSxS\\Temp\\PendingDeletes\\$$Delet
                eMe*" and
             + not (dll.path : "?:\\Program
         39
                Files\\BackupClient\\DeviceLock\\DLDrvUserMode64.dl
                1" and
                       dll.hash.sha256 :
         40
                "ab813df167f8b6afe13f67231328f28fa3b0efeed8460f8b5e
                8a4228a8cded4e")
         41
                 ]
  39
         42
  40
         43
  41
         44
                optional_actions = []
     T
 ∨ 58 ■■■■■
behavior/rules/defense_evasion_quarantine_attribute_delet... 📮
                @@ -0,0 +1,58 @@
          1 + [rule]
          2 + description = """
          3 + Identifies a potential Gatekeeper bypass from an
                unsigned or untrusted binary. In macOS, when
                applications or programs
          4 + are downloaded from the internet, there is a
                quarantine flag set on the file. This attribute is
                read by Apple's
```

```
5 + Gatekeeper defense program at execution time. An
      adversary may disable this attribute to evade
      defenses.
6 + """
7 + id = "6e47b750-72c4-4af9-ad7b-0fc846df64d3"
8 + license = "Elastic License v2"
9 + name = "Quarantine Attribute Deleted via Untrusted
      Binary"
10 + os_list = ["macos"]
11 + version = "1.0.2"
12 +
   + query = '''
13
14 + sequence with maxspan=1m
   + [process where event.action == "exec" and
15
16 + (process.code_signature.trusted == false or
      process.code_signature.exists == false)] by
      process.entity_id
17
    + [process where event.action == "exec" and
        process.args: "xattr" and
18
19
        process.name : ("bash", "sh", "zsh", "xattr") and
20
   +
          (process.args : "com.apple.quarantine" and
21
      process.args : ("-d", "-w", "-?d", "-?w")) or
22
          (process.args : "-c" and process.command_line :
           (
23
24 +
              "/bin/bash -c xattr -c *",
              "/bin/zsh -c xattr -c *",
25 +
              "/bin/sh -c xattr -c *"
26
27 +
            )
          )
28
29
30 +
      ] by process.parent.entity_id
31 + '''
32 +
33 + optional_actions = []
34 + [[actions]]
35 + action = "kill_process"
36 + field = "process.entity_id"
37 + state = 0
38 +
39 + [[threat]]
40 + framework = "MITRE ATT&CK"
41 + [[threat.technique]]
42 + id = "T1553"
43 + 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"
 ...es/defense_evasion_reading_or_modifying_downloaded_fil... ☐
    <u></u>
                @@ -9,7 +9,7 @@ license = "Elastic License v2"
          9
               name = "Reading or Modifying Downloaded Files
               Database via SQLite Utility"
               os_list = ["macos"]
  10
         10
                reference = ["https://redcanary.com/blog/clipping-
  11
         11
                silver-sparrows-wings/"]
  12
              - version = "1.0.6"
             + version = "1.0.7"
         12
         13
  13
                query = '''
  14
         14
  15
         15
                sequence with maxspan=30s
     +
 behavior/rules/defense_evasion_regsvr32_scriptlet_executi... 📮
                @@ -7,7 +7,7 @@ id = "0524c24c-e45e-4220-b21a-
    †
                abdba0c46c4d"
   7
               license = "Elastic License v2"
                name = "Regsvr32 Scriptlet Execution"
   8
          8
                os_list = ["windows"]
   9
          9
              - version = "1.0.8"
  10
```

```
10
              + version = "1.0.9"
  11
          11
                query = '''
  12
          12
  13
                process where event.action == "start" and
          13
                @@ -35,12 +35,14 @@ process where event.action ==
     .
                "start" and
                      not process.command_line : "*scrobj.dll*")
  35
          35
          36
  36
  37
          37
  38
               - optional_actions = []
  39
          38
                [[actions]]
  40
          39
                action = "kill_process"
                field = "process.entity_id"
  41
          40
                state = 0
  42
          41
  43
          42
          43
              + [[optional_actions]]
          44
              + action = "rollback"
          45
                [[threat]]
  44
          46
                framework = "MITRE ATT&CK"
  45
          47
  46
          48
                [[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"
   7
   8
           8
                name = "Regsvr32 with Unusual Arguments"
                os_list = ["windows"]
  10
              - version = "1.0.10"
              + version = "1.0.11"
          10
  11
          11
                query = '''
  12
          12
  13
          13
                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
          50
  50
                Suite\\Codejock.DockingPane.x64.v15.3.1.ocx*") and
                 not process.parent.executable :
  51
          51
                "?:\\Eaglesoft\\Shared Files\\OcxReg.exe" and
```

```
52
       52
              not process.args :
              ("?:\\windows\\system32\\ChartFX.ClientServer.Data.
              dll",
              "?:\\Windows\\SysWOW64\\ChartFX.ClientServer.Data.d
              11") and
53
            - not (process.args :
              "?:\\Users\\*\\AppData\\Local\\Microsoft\\TeamsMeet
              ingAddin\\*\\Microsoft.Teams.AddinLoader.dll" and
              process.args : "/i:user")
       53 + not (process.args:
              "?:\\Users\\*\\AppData\\Local\\Microsoft\\TeamsMeet
              ingAddin\\*\\Microsoft.Teams.AddinLoader.dll" and
              process.args : "/i:user") and
       54 + not (process.args : "..\\*.dll" and
              process.working_directory : "?:\\Program
              Files\\LANDesk\\ManagementSuite\\Install Only
              Files\\") and
       55
           + not (process.args : "..\\*.dll" and
                    descendant of
       56
       57 +
                     [process where event.action == "start" and
       58
                      process.executable : ("?:\\Program
              Files\\LANDesk\\ManagementSuite\\Install Only
              Files\\LaunchApp.exe",
       59
                                            "?:\\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
       61
              Files\\LANDesk\\ManagementSuite\\Install Only
              Files\\LaunchApp.exe" and
       62 + not (process.executable :
              "?:\\Users\\*\\AppData\\Local\\Temp\\SSM*.tmp\\REGS
             VR32.EXE" and process.args :
              "?:\\WINDOWS\\system32\\*.dll")
              . . .
       63
54
55
       64
            - optional_actions = []
56
57
       65
              [[actions]]
              action = "kill process"
58
       66
              field = "process.entity_id"
59
       67
60
       68
              state = 0
61
       69
            + [[optional_actions]]
       70
           + action = "rollback"
```

```
72
  62
          73
                 [[threat]]
                framework = "MITRE ATT&CK"
  63
          74
  64
          75
                 [[threat.technique]]
 behavior/rules/defense_evasion_remote_file_execution_via_... 📮
     †
                @@ -11,7 +11,7 @@ reference = [
  11
          11
                     "https://lolbas-
                 project.github.io/lolbas/Binaries/Msiexec/",
          12
                     "https://www.guardicore.com/labs/purple-fox-
  12
                rootkit-now-propagates-as-a-worm/",
  13
          13
              - version = "1.0.8"
  14
              + version = "1.0.9"
          14
  15
          15
                query = '''
  16
          16
                process where event.action == "start" and
  17
          17
                process.args_count <= 5 and</pre>
                @@ -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"
                 1.1.1
  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
          33
  34
          34
              + [[optional_actions]]
              + action = "rollback"
          35
          36
  35
          37
                 [[threat]]
  36
          38
                 framework = "MITRE ATT&CK"
  37
          39
                 [[threat.technique]]
     ....
```

```
behavior/rules/defense_evasion_remote_msi_package_install... 「  
     .
                @@ -11,7 +11,7 @@ reference = [
         11
  11
                    "https://lolbas-
                project.github.io/lolbas/Binaries/Msiexec/",
         12
                    "https://www.guardicore.com/labs/purple-fox-
  12
                rootkit-now-propagates-as-a-worm/",
  13
         13
                1
              - version = "1.0.6"
  14
              + version = "1.0.7"
         14
  15
         15
                query = '''
         16
  16
  17
         17
                sequence with maxspan=1m
     .‡.
                @@ -22,12 +22,14 @@ sequence with maxspan=1m
  22
         22
                    not (process.executable : ("?:\\Program Files
                (x86)\*.exe", "?:\\Program Files\\*.exe") and
                process.code_signature.trusted == true)] by
                process.parent.entity_id
         23
  23
  24
         24
  25
              - optional_actions = []
  26
         25
                [[actions]]
  27
         26
                action = "kill_process"
                field = "process.entity_id"
  28
         27
                state = 1
  29
         28
         29
  30
         30
              + [[optional_actions]]
              + action = "rollback"
         31
         32
  31
         33
                [[threat]]
  32
         34
                framework = "MITRE ATT&CK"
                [[threat.technique]]
  33
         35
     +
```

```
9
          9
                os_list = ["windows"]
  10
              - version = "1.0.6"
              + version = "1.0.7"
         10
         11
  11
  12
         12
                query = '''
  13
         13
                process where event.action == "start" and
  14
                  process.pe.original_file_name : "AutoIt*.exe" and
         14
                not process.name : "AutoIt*.exe"
         15
  15
  16
         16
  17
              - optional_actions = []
                [[actions]]
  18
         17
  19
         18
                action = "kill_process"
         19
                field = "process.entity_id"
  20
                state = 0
  21
         20
  22
         21
              + [[optional_actions]]
         22
         23
              + action = "rollback"
         24
  23
         25
                [[threat]]
                framework = "MITRE ATT&CK"
  24
         26
  25
         27
                [[threat.technique]]
     ....
 behavior/rules/defense_evasion_renamed_third_party_admini... 「  
                @@ -4,7 +4,7 @@ id = "b707de5c-8e4d-4d2c-be22-
     .
                b09a7e82b73f"
                license = "Elastic License v2"
   4
                name = "Renamed Third Party Administrator Tools"
   5
           5
                os_list = ["windows"]
   6
           6
   7
              - version = "1.0.9"
              + version = "1.0.10"
   8
           8
                query = '''
   9
           9
  10
         10
                process where event.action == "start" and
                @@ -21,12 +21,14 @@ process where event.action ==
     ....
                "start" and
  21
         21
                          "?:\\Program Files\\*.exe")
                1 1 1
  22
         22
  23
         23
              - optional_actions = []
  24
                [[actions]]
  25
         24
```

```
26
          25
                action = "kill_process"
  27
          26
                field = "process.entity_id"
  28
          27
                state = 0
  29
          28
          29
              + [[optional_actions]]
              + action = "rollback"
          30
          31
  30
          32
                [[threat]]
          33
                framework = "MITRE ATT&CK"
  31
  32
          34
                [[threat.technique]]
     +
 behavior/rules/defense_evasion_renamed_windows_automaton_... 📮
     <u></u>
                @@ -9,7 +9,7 @@ license = "Elastic License v2"
          9
   9
                name = "Renamed Windows Automaton Script
                Interpreter"
                os_list = ["windows"]
  10
          10
                reference = ["https://blog.morphisec.com/explosive-
  11
          11
                new-mirrorblast-campaign-targets-financial-
                companies"]
  12
              - version = "1.0.6"
          12
              + version = "1.0.7"
          13
  13
                query = '''
  14
          14
  15
          15
                process where event.action == "start" and
     +
                @@ -47,15 +47,18 @@ process where event.action ==
     <u></u>
                "start" and
  47
          47
                   not (process.pe.original_file_name ==
                "KIX32.EXE" and process.parent.command_line :
                "*\netlogon\*") and
                    not (process.pe.original_file_name ==
  48
          48
                "KIX32.EXE" and process.executable :
                ("C:\\kworking\\Bin\\RMMKSE.EXE",
                "C:\\kworking\\Bin\\RMMSSE.EXE")) and
  49
          49
                    not (process.pe.original_file_name ==
                "AutoHotkey.exe" and process.executable :
                "C:\\TCPU73\\Programm\\ClockTC\\ClockTC.exe" and
  50
                         process.parent.executable :
                "C:\\TCPU73\\TOTALCMD.EXE")
          50
                         process.parent.executable :
                "C:\\TCPU73\\TOTALCMD.EXE") and
```

```
51
                   not process.executable : "?:\\Program
                 Files\\AutoHotkey\\SciTE\\InternalAHK.exe"
          52
  51
  52
          53
              - optional_actions = []
  54
          54
                 [[actions]]
                action = "kill_process"
  55
          55
                field = "process.entity_id"
  56
          56
                state = 0
  57
          57
  58
          58
          59
              + [[optional_actions]]
              + action = "rollback"
          60
          61
                 [[threat]]
  59
          62
                framework = "MITRE ATT&CK"
  60
          63
                 [[threat.technique]]
  61
          64
     ....
 behavior/rules/defense_evasion_rundl132_regsvr32_loads_a_... 📮
     <u>†</u>
                @@ -11,7 +11,7 @@ reference = [
          11
                     "https://blog.menasec.net/2021/05/hunting-for-
  11
                 suspicious-usage-of.html",
                     "https://www.elastic.co/blog/hunting-for-
  12
          12
                persistence-using-elastic-security-part-2",
  13
          13
              - version = "1.0.7"
  14
              + version = "1.0.8"
          14
  15
          15
                query = '''
  16
          16
  17
          17
                 sequence with maxspan=5m
     ....
    ·‡· 38 ■■■■
```

```
10
            + version = "1.0.11"
11
       11
       12
              query = '''
12
13
       13
              process where event.action == "start" and
              process.name : "rundll32.exe" and
  ....
              @@ -42,7 +42,10 @@ process where event.action ==
  <u></u>
              "start" and process.name : "rundll32.exe" and
                         "*\\M?-*.dll,_run@*",
42
       42
43
       43
                         "*%TEMP%\\*.cpl*",
                         "*\\Users\\*\\Downloads\\*.cpl*",
44
       44
45
              "*\\appdata\\roaming\\microsoft\\templates\\*,*")
       45
              "*\\appdata\\roaming\\microsoft\\templates\\*,*",
       46
                         /* DLL exec by ordinal */
       47
                         "* #*", "*,#*") or
       48
                  process.command_line like "*rUNdlL32.eXe*" or
46
       49
47
       50
                  /* fake Control_RunDLL export */
48
       51
              @@ -56,7 +59,8 @@ process where event.action ==
  .‡.
              "start" and process.name : "rundll32.exe" and
       59
56
       60
                  /* suspicious parent powershell args */
57
                  (process.parent.name : "powershell.exe" and
58
       61
                   process.parent.args : ("-enc", "IEX", "*wp-
59
              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
                  )
       65
61
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=*",
```

| 67       | 71       | "*davclnt.dll,DavSetCookie*",   |
|----------|----------|---|
| 68       | /1       | - "*PhotoViewer.dll*ImageView Fu*",   |
| 00       | 72       |   |
| 69       | 72       | <pre>+ "*PhotoViewer*ImageView_Fu*",  "*url.dll,FileProtocolHandler*",</pre>    |
| 70       | 73<br>74 | dri.dii, riierrotocoinandier ,  |
| 70       | 74       | "*zzzzInvokeManagedCustomActionOutOfProc*",                                     |
| 71       | 75       | "*,DeferredDelete*",  |
| 71       | 75<br>76 | "*:\\WINDOWS\\system32\\spool\\*",  |
| 72       | 76       | "*:\\Program Files (x86)\\*",   |
| 73<br>74 | 77       | "*:\\Program Files\\*",   |
| 74<br>75 | 78<br>79 | /* Issue #282 - FP */   |
|          | 79       |   |
| 76       | 0.0      | - "*cryptext.dll,CryptExtAddPFX*",  |
|          | 80       | + "*cryptext*CryptExt*",  |
| 77       | 81       | "*dfshim.dl1*ShOpenVerbShortcut*",  |
| 78       | 82       | "*\\Documents\\DocuShare\\*",   |
| 79       | 83       | /* T  |
| 80       | 84       | /* Issue #371 */  |
| 81       | 85       | W# 16 1 177 1165 5775   |
|          |          | <pre>"*ndfapi.dll,NdfRunDllDiagnoseWithAnswerFile*",</pre>                      |
| 82       | 86       |   |
|          |          | "*FirewallControlPanel.dll,ShowNotificationDialog*"                             |
|          |          | ,   |
| 83       | 87       | "*type=renderer*log-file=*",  |
| 84       | 0.0      | - "*lang=*log-file=*") and not  |
|          | 88       | + "*lang=*log-file=*",  |
|          | 89       | +   |
|          | 90       | + "*shell32*OpenAs_RunDLL*",  |
|          | 91       | + "*dfshim*ShOpenVerbExtension*",   |
|          | 92       | + "*printui*PrintUIEntry*",   |
|          | 93       | + "*mshtml*PrintHTML*",   |
|          | 94       | + "*shell32*#44*",  |
|          | 95       | + "*shell32.dll*ShellExec_RunDLL*#*",   |
|          | 96       | + "*EDGEHTML*#*"  |
|          | 97       | + ) and not   |
| 85       | 98       | <pre>+     (process.command_line : "*.tmp*" and</pre>                           |
| 86       | 99       | <pre>(process.command_line : "*.tmp*" and     process.parent.executable :</pre> |
| 00       |          |   |
|          |          | ("?:\\Windows\\System32\\msiexec.exe",  |
|          | 100      | "?:\\Windows\\ <mark>System32</mark> \\msiexec.exe") and                        |
|          | 100      | + process.parent.executable :  ("2:\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\         |
|          |          | ("?:\\Windows\\System32\\msiexec.exe",  |
| 0.7      | 101      | "?:\\Windows\\SysWOW64\\msiexec.exe") and                                       |
| 87       | 101      | process.parent.args : "-Embedding") and   |
| 88       | 102      | not process.args :  |
|          |          | "?:\\ProgramData\\Parallels\\RASLogs\\tmp*.tmp,Stop                             |
|          |          |   |

```
Memshell" and
  89
         103
                  not (process.args :
                "?:\\Users\\Public\\IBM\\ClientSolutions\\Start_Pro
                grams\\Windows_*\\acsnative.dll*" and
  90
         104
                        process.parent.executable :
                "?:\\Users\\Public\\IBM\\ClientSolutions\\Start_Pro
                grams\\Windows_*\\acslaunch_*.exe") and
  91
                  not process.parent.executable : ("?:\\Program
                Files\\Common
                Files\\BullGuardInstall\\BullGuard*.exe",
                "?:\\Program Files (x86)\\Intuit\\QuickBooks 20??
                \\QBW??.EXE")
         105
                  not process.parent.executable :
        106
                               ("?:\\Program Files\\Common
                Files\\BullGuardInstall\\BullGuard*.exe",
         107
                                "?:\\Program Files
                (x86)\\Intuit\\QuickBooks 20??\\QBW??.EXE",
         108
                                "?:\\Program
                Files\\Intuit\\QuickBooks 2022\\QBW.EXE") and
        109
                  not (user.name : "user" and process.args :
                "file.dll, #*")
         110
  92
  93
        111
  94
              - optional_actions = []
        112
  95
                [[actions]]
         113
                action = "kill_process"
  96
  97
         114
                field = "process.entity_id"
                state = 0
  98
         115
  99
         116
         117
              + [[optional_actions]]
        118
              + action = "rollback"
         119
         120
                [[threat]]
 100
         121
                framework = "MITRE ATT&CK"
 101
 102
         122
                [[threat.technique]]
     ....
 behavior/rules/defense_evasion_script_execution_via_macos... 「☐
     <u></u>
                @@ -12,7 +12,7 @@ reference = [
  12
          12
                     "https://kyle-bailey.medium.com/detecting-
                macos-gatekeeper-bypass-cve-2021-30657-
                cc986a9bc751",
```

```
13
         13
                     "https://objective-
                 see.com/blog/blog_0x64.html",
                 1
  14
          14
  15
              - version = "1.0.9"
          15
              + version = "1.0.10"
  16
          16
  17
          17
                query = '''
  18
          18
                 sequence with maxspan=5m
     Τ...
  behavior/rules/defense_evasion_script_execution_via_micro... 📙
                @@ -7,7 +7,7 @@ id = "f0630213-c4c4-4898-9514-
     <u></u>
                746395eb9962"
                license = "Elastic License v2"
   7
           7
                name = "Script Execution via Microsoft HTML
   8
           8
                Application"
                os_list = ["windows"]
   9
              - version = "1.0.10"
  10
              + version = "1.0.11"
          10
  11
          11
                query = '''
  12
          12
  13
          13
                process where event.action == "start" and
     ····
                @@ -52,15 +52,21 @@ process where event.action ==
     <u></u>
                "start" and
                      /* Execution of HTA file from mounted ISO
  52
          52
  53
          53
                      (process.pe.original_file_name : "mshta.exe"
                and
  54
          54
                       process.parent.name : ("explorer.exe",
                 "cmd.exe", "powershell.exe") and
                 process.working_directory : "?:\\")
  55
                    )
                    ) and
          55
          56
          57
                  /* FPs */
                   not (process.parent.executable :
                 "C:\\Windows\\SysWOW64\\runonce.exe" and
                        process.args : "\"&
          59
                 'C:\\System.sav\\util\\HpseuHostLauncher.ps1'\"\",
                 0 : window.close)")
                 . . .
  56
          60
  57
          61
```

```
58
              - optional_actions = []
  59
          62
                [[actions]]
                action = "kill_process"
  60
          63
                field = "process.entity_id"
  61
          64
  62
          65
                state = 0
  63
          66
          67
              + [[optional_actions]]
          68
              + action = "rollback"
          69
  64
          70
                [[threat]]
  65
          71
                framework = "MITRE ATT&CK"
  66
          72
                [[threat.technique]]
     ....
 behavior/rules/defense_evasion_script_execution_via_msxsl... 「니
     .
                @@ -8,20 +8,22 @@ license = "Elastic License v2"
                name = "Script Execution via MSXSL"
   8
           8
   9
          9
                os_list = ["windows"]
  10
          10
                reference = ["https://lolbas-
                project.github.io/lolbas/OtherMSBinaries/Msxsl/"]
              - version = "1.0.8"
  11
          11
              + version = "1.0.9"
  12
          12
          13
                query = '''
  13
          14
                sequence by process.entity_id with maxspan=1m
  14
                 [process where event.action == "start" and
  15
          15
                process.pe.original_file_name == "msxsl.exe"]
                 [library where dll.name : ("scrobj.dll",
  16
          16
                "jscript.dll", "vbscript.dll", "jscript9.dll")]
          17
  17
  18
          18
  19
              - optional_actions = []
  20
          19
                [[actions]]
                action = "kill_process"
  21
          20
                field = "process.entity_id"
  22
          21
                state = 0
  23
          22
  24
          23
              + [[optional_actions]]
              + action = "rollback"
          25
          26
  25
          27
                [[threat]]
                framework = "MITRE ATT&CK"
  26
          28
  27
          29
                [[threat.technique]]
```

```
....
 behavior/rules/defense_evasion_scriptlet_execution_via_cm... 📮
     <u>†</u>
                @@ -8,20 +8,22 @@ license = "Elastic License v2"
   8
           8
                name = "Scriptlet Execution via CMSTP"
   9
           9
                os_list = ["windows"]
                reference = ["https://lolbas-
  10
          10
                project.github.io/lolbas/Binaries/Cmstp/"]
  11
              - version = "1.0.8"
              + version = "1.0.9"
          11
  12
          12
          13
                query = '''
  13
  14
          14
                sequence by process.entity_id with maxspan=1m
                 [process where event.action == "start" and
  15
          15
                process.pe.original_file_name == "CMSTP.EXE"]
          16
                 [library where dll.name : "scrobj.dll"]
  16
  17
          17
  18
          18
  19
              - optional_actions = []
          19
                [[actions]]
  20
                action = "kill_process"
  21
          20
  22
          21
                field = "process.entity id"
  23
          22
                state = 0
          23
  24
          24
              + [[optional_actions]]
              + action = "rollback"
          25
          26
                [[threat]]
  25
          27
          28
                framework = "MITRE ATT&CK"
  26
  27
          29
                [[threat.technique]]
     ····
```

```
14
              - version = "1.0.8"
              + version = "1.0.9"
         15
  15
         16
                query = '''
  16
  17
         17
                sequence by process.entity_id with maxspan=1m
     ....
 behavior/rules/defense_evasion_scriptlet_proxy_execution_... 📮
     .
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
                name = "Scriptlet Proxy Execution via PubPrn"
   8
   9
          9
                os_list = ["windows"]
                reference = ["https://lolbas-
  10
         10
                project.github.io/lolbas/Scripts/Pubprn/"]
              - version = "1.0.8"
  11
              + version = "1.0.9"
         11
  12
         12
         13
                query = '''
  13
  14
         14
                process where event.action == "start" and
                @@ -17,12 +17,14 @@ process where event.action ==
     .
                "start" and
  17
         17
                 process.command_line : ("*localhost*script:http*",
                "*127.0.0.*script:http*")
  18
         18
  19
         19
  20
              - optional_actions = []
                [[actions]]
  21
         20
                action = "kill_process"
  22
         21
  23
         22
                field = "process.entity_id"
  24
         23
                state = 0
  25
         24
              + [[optional_actions]]
         25
         26
              + action = "rollback"
         27
  26
         28
                [[threat]]
  27
         29
                framework = "MITRE ATT&CK"
  28
         30
                [[threat.technique]]
```

```
behavior/rules/defense_evasion_shadow_copy_service_disabl...
```

```
@@ -7,20 +7,22 @@ id = "b2409cd4-3b23-4b2d-82e4-
     †
                bbb25594999a"
                license = "Elastic License v2"
   7
          7
                name = "Shadow Copy Service Disabled via Registry
   8
          8
                Modification"
                os_list = ["windows"]
   9
              - version = "1.0.4"
  10
              + version = "1.0.5"
         10
  11
         11
  12
         12
                query = '''
         13
                registry where
  13
  14
         14
                 registry.path:
                "HKLM\\SYSTEM\\ControlSet*\\Services\\VSS\\Start"
                and registry.data.strings : "4" and
  15
         15
                 not process.executable :
                "?:\\Windows\\System32\\services.exe" and
                process.executable : "?*"
                . . .
  16
         16
  17
         17
              - optional_actions = []
  18
  19
         18
                [[actions]]
                action = "kill_process"
  20
         19
         20
                field = "process.entity_id"
  21
  22
         21
                state = 0
  23
         22
              + [[optional_actions]]
         23
         24
              + action = "rollback"
         25 +
  24
         26
                [[threat]]
  25
         27
                framework = "MITRE ATT&CK"
         28
                [[threat.technique]]
 behavior/rules/defense_evasion_solarmarker_backdoor_regis...
    <u></u>
                @@ -12,7 +12,7 @@ reference = [
  12
         12
                    "https://www.ired.team/offensive-
                security/persistence/hijacking-default-file-
                extension",
  13
         13
                    "https://www.binarydefense.com/mars-deimos-
                solarmarker-jupyter-infostealer-part-1/",
  14
         14
                ]
  15
              - version = "1.0.5"
```

```
15
              + version = "1.0.6"
  16
          16
                query = '''
  17
          17
  18
          18
                sequence by process.entity_id with maxspan=1m
                @@ -25,12 +25,14 @@ sequence by process.entity_id
     .
                with maxspan=1m
                  registry.data.strings : "*PowerShell*" and
  25
          25
                 length(registry.data.strings) >= 200]
  26
          26
  27
          27
               - optional_actions = []
  28
  29
          28
                [[actions]]
          29
                action = "kill_process"
  30
                field = "process.parent.entity_id"
  31
          30
  32
                state = 0
          31
          32
  33
          33
              + [[optional_actions]]
          34
              + action = "rollback"
          35
  34
          36
                 [[threat]]
                 framework = "MITRE ATT&CK"
  35
          37
  36
          38
                 [[threat.technique]]
     ····
 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"]
              - version = "1.0.8"
  12
          12
              + version = "1.0.9"
  13
          13
                query = '''
  14
          14
  15
          15
                process where event.action == "start" and
     +
                @@ -79,7 +79,8 @@ process where event.action ==
     <u></u>
                 "start" and
          79
  79
                       "powershell.exe",
  80
          80
                       "pwsh.exe",
                       "cmd.exe"
  81
          81
  82
                     )])
          82
                    )]) and
```

```
83
                    not (process.args :
                "https://dl.duosecurity.com/*" and
                process.parent.args :
                "?:\\ProgramData\\NinjaRMMAgent\\scripting\\*")
  83
         84
  84
         85
  85
                optional_actions = []
         86
     +
 ∨ 66
behavior/rules/defense_evasion_suspicious_control_panel_d... 📮
                @@ -0,0 +1,66 @@
          1 + [rule]
          2 + description = """
          3 + Identifies DLL load of an unsigned or untrusted
                Control Panel Item by the Explorer process.
                Adversaries may load a
          4 + malicious DLL when Control Panel is executed via
                setting the CPLs subkey to the payload path.
          5 + """
          6 + id = "1dbf6ac3-540a-4214-8173-9aa93232da38"
          7 + license = "Elastic License v2"
            + name = "Suspicious Control Panel DLL Loaded by
                Explorer"
          9 + os_list = ["windows"]
         10 + reference = ["https://docs.microsoft.com/en-
                us/previous-
                versions/windows/desktop/legacy/hh127454(v=vs.85)"]
         11 + version = "1.0.3"
         12 +
         13 + query = '''
         14
             + sequence with maxspan = 5s
         15
             + [library where process.name : "explorer.exe" and
         16
         17
                (dll.code_signature.trusted == false or
                dll.code_signature.exists == false) and
             + not dll.path:
         18
                          ("?:\\Program Files\\*",
         19
                           "?:\\Program Files (x86)\\*",
         20
         21
                           "?:\\Windows\\System32\\*",
                           "?:\\Windows\\SysWOW64\\*",
         22 +
                           "?:\\Windows\\assembly\\*")] by
         23
                process.entity_id
         24
```

```
25
    + [process where event.action == "start" and
      process.parent.name : "explorer.exe" and
26
   + /* CLSID_ControlPanelProcessExplorerHost */
27
        process.parent.args : "/factory,{5BD95610-9434-
28
      43C2-886C-57852CC8A120}" and
29
        /* false positives */
30
        not (process.name : "rundll32.exe" and
31 +
32 +
             process.args :
33
                  ("printui.dll, PrintUIEntryDPIAware",
34
      "?:\\WINDOWS\\system32\\spool\\DRIVERS\\*PrintJobSt
      atus",
                   "fdprint, InvokeTask")) and
35
    + not (process.name : "mmc.exe" and process.args :
36
      "?:\\windows\\system32\\devmgmt.msc") and
   + not process.executable :
      ("?:\\windows\\system32\\DevicePairingWizard.exe",
      "?:\\Windows\\System32\\spool\\drivers\\x64\\3\\E_Y
      ARNYWE.EXE")
38 + ] by process.parent.entity_id
39
40
   +
41 + optional_actions = []
42 + [[actions]]
43 + action = "kill_process"
44 + field = "process.entity_id"
45 + state = 1
46
   + [[threat]]
47
48 + framework = "MITRE ATT&CK"
49 + [[threat.technique]]
50 + id = "T1218"
51 + name = "System Binary Proxy Execution"
52 + reference =
      "https://attack.mitre.org/techniques/T1218/"
+ [[threat.technique.subtechnique]]
54 + id = "T1218.002"
55 + name = "Control Panel"
56
   + reference =
      "https://attack.mitre.org/techniques/T1218/002/"
57
58
59
```

60

+ [threat.tactic]

```
61 + id = "TA0005"
         62 + name = "Defense Evasion"
         63 + reference =
                "https://attack.mitre.org/tactics/TA0005/"
         64 +
         65 + [internal]
         66 + min_endpoint_version = "7.16.0"
 behavior/rules/defense_evasion_suspicious_execution_from ... 「  
                @@ -7,7 +7,7 @@ id = "42d2bbfb-a2fb-4327-b701-
     <u></u>
                89ead6044ca1"
                license = "Elastic License v2"
   7
                name = "Suspicious Execution from a Mounted Device"
   8
          8
   9
                os_list = ["windows"]
              - version = "1.0.10"
  10
              + version = "1.0.11"
         10
         11
  11
                query = '''
         12
  12
                sequence with maxspan=1m
  13
         13
  behavior/rules/defense_evasion_suspicious_execution_via_m... 📙
     .
                @@ -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
              - version = "1.0.4"
  14
         14
              + version = "1.0.5"
         15
  15
                query = '''
  16
         16
  17
         17
                process where event.action == "start" and
                @@ -41,7 +41,9 @@ process where event.action ==
     <u></u>
                "start" and
         41
                  not (process.parent.executable :
  41
                "?:\Users\*\AppData\Local\Temp\*" and
                process.parent.args_count >= 2 and
```

```
42
         42
                       process.args :
                "?:\\Users\\*\\AppData\\Local\\Temp\\*\\*.msi") and
  43
         43
  44
              - not process.args : ("?:\\Program Files (x86)\\*",
                "?:\\Program Files\\*")
         44
             + not process.args : ("?:\\Program Files (x86)\\*",
                "?:\\Program Files\\*") and
         45
                  not (process.parent.name : "msiexec.exe" and
         46
                process.parent.args : "-Embedding")
         47
  45
  46
         48
  47
         49
                optional_actions = []
 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
   8
          8
                Device"
   9
                os_list = ["windows"]
              - version = "1.0.6"
  10
              + version = "1.0.7"
         10
  11
         11
                query = '''
  12
         12
                sequence by process.entity_id with maxspan=1m
  13
         13
     +
   46
```

```
6 + id = "1faebe83-38d7-4390-b6bd-9c6b851e47c4"
7 + license = "Elastic License v2"
8 + name = "Suspicious ImageLoad via ODBC Driver
      Configuration Program"
9 + os_list = ["windows"]
10 + reference = ["https://lolbas-
      project.github.io/lolbas/Binaries/Odbcconf/"]
11 + version = "1.0.2"
12 +
13 + query = '''
14 + process where event.action == "start" and
   + (process.pe.original_file_name == "odbcconf.exe"
      or process.name : "odbcconf.exe") and
16 + process.args : ("-a", "-f", "/a", "/f")
17 + '''
18 +
19 + [[actions]]
20 + action = "kill_process"
21 + field = "process.entity_id"
22 + state = 0
23 +
24 + [[optional_actions]]
25 + action = "rollback"
26 +
27 + [[threat]]
28 + framework = "MITRE ATT&CK"
4 + [[threat.technique]]
30 + id = "T1218"
31 + name = "System Binary Proxy Execution"
32 + reference =
      "https://attack.mitre.org/techniques/T1218/"
33 + [[threat.technique.subtechnique]]
34 + id = "T1218.008"
35 + name = "Odbcconf"
36 + reference =
      "https://attack.mitre.org/techniques/T1218/008/"
37 +
38
39 +
40 + [threat.tactic]
41 + id = "TA0005"
42 + name = "Defense Evasion"
43 + reference =
      "https://attack.mitre.org/tactics/TA0005/"
44 +
```

```
45 + [internal]
         46 + min_endpoint_version = "7.15.0"
 behavior/rules/defense_evasion_suspicious_imageload_via_w... 📙
               @@ -0,0 +1,40 @@
        . . .
          1 + [rule]
          2 + description = """
          3 + Identifies abuse of the Microsoft CertOC utility to
               load an arbitrary DLL. This behavior is used as a
               defense evasion
          4 + technique to blend-in malicious activity with
               legitimate Windows software.
          5 + """
          6 + id = "6fcbf73f-4413-4689-be33-61b0d6bd0ffc"
          7 + license = "Elastic License v2"
          8 + name = "Suspicious ImageLoad via Windows CertOC"
          9 + os_list = ["windows"]
         10 + reference = ["https://lolbas-
               project.github.io/lolbas/Binaries/Certoc/"]
         11 + version = "1.0.2"
         12 +
         13 + query = '''
         14 + process where event.action == "start" and
         15 + (process.pe.original_file_name == "CertOC.exe" or
               process.name : "certoc.exe") and process.args : "-
               LoadDLL"
         16 + '''
         17 +
         18 + [[actions]]
         19 + action = "kill_process"
         20 + field = "process.entity_id"
         21 + state = 0
         22 +
         23 + [[optional_actions]]
         24 + action = "rollback"
         25 +
         26 + [[threat]]
         27 + framework = "MITRE ATT&CK"
         28 + [[threat.technique]]
         29 + id = "T1218"
         30 + name = "System Binary Proxy Execution"
         31 + reference =
               "https://attack.mitre.org/techniques/T1218/"
```

```
32
         33 +
         34 + [threat.tactic]
         35 + id = "TA0005"
         36 + name = "Defense Evasion"
         37 + reference =
                "https://attack.mitre.org/tactics/TA0005/"
         38
             + [internal]
         39
             + min_endpoint_version = "7.15.0"
 ...ior/rules/defense_evasion_suspicious_imageload_via_win... 📮
     <u></u>
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
   8
          8
                name = "Suspicious ImageLoad via Windows Update
                Auto Update Client"
          9
                os_list = ["windows"]
   9
                reference = ["https://dtm.uk/wuauclt/"]
  10
         10
              - version = "1.0.6"
  11
              + version = "1.0.7"
         11
  12
         12
  13
         13
                query = '''
  14
         14
                sequence by process.entity_id with maxspan=1m
                @@ -27,12 +27,14 @@ sequence by process.entity_id
    -‡-
                with maxspan=1m
         27
  27
                "?:\\ProgramData\\Symantec\\Symantec Endpoint
                Protection\\*.dll"))]
                . . .
  28
         28
  29
         29
              - optional_actions = []
  30
  31
         30
                [[actions]]
                action = "kill_process"
  32
         31
                field = "process.entity_id"
  33
         32
                state = 0
  34
         33
  35
         34
         35
              + [[optional_actions]]
         36
              + action = "rollback"
         37
  36
         38
                [[threat]]
  37
         39
                framework = "MITRE ATT&CK"
  38
                [[threat.technique]]
         40
     ····
```

```
behavior/rules/defense_evasion_suspicious_ntdll_image_loa... [ ]
                @@ -7,7 +7,7 @@ id = "5eb3c0b3-8d11-439d-b26d-
     <u></u>
                d7623c5b3723"
                license = "Elastic License v2"
   7
                name = "Suspicious NTDLL Image Load"
          8
   8
                os_list = ["windows"]
   9
              - version = "1.0.4"
  10
              + version = "1.0.5"
         10
         11
  11
                query = '''
  12
         12
         13
                sequence by process.entity_id with maxspan=1m
  13
     +
```

```
behavior/rules/defense_evasion_suspicious_parent_child_re... 📮
                @@ -7,7 +7,7 @@ id = "18a26e3e-e535-4d23-8ffa-
     †
                a3cdba56d16e"
                license = "Elastic License v2"
   7
                name = "Suspicious Parent-Child Relationship"
   8
          8
   9
          9
                os_list = ["windows"]
  10
              - version = "1.0.5"
              + version = "1.0.7"
         10
  11
         11
  12
         12
                query = '''
  13
         13
                process where event.action == "start" and
                @@ -21,18 +21,16 @@ process where event.action ==
     .‡.
                "start" and
                    */
  21
         21
                   (process.name : "autochk.exe" and not
  22
         22
                process.parent.name : "smss.exe") or
  23
         23
  24
                   (process.name : ("consent.exe",
                "RuntimeBroker.exe", "TiWorker.exe") and not
                process.parent.name : ("svchost.exe",
                "RuntimeBroker.exe") and
         24 +
                   (process.name : ("consent.exe",
                "RuntimeBroker.exe") and not process.parent.name :
                ("svchost.exe", "RuntimeBroker.exe") and
```

| 25  | 25  | not process.parent.executable : "?:\\Program   |
|-----|-----|--|
|     |     | Files\\ThreatLocker\\threatlockerconsent.exe") or  |
| 26  |     | - (process.name : "SearchIndexer.exe" and not  |
|     |     | process.parent.name : "services.exe") or   |
| 27  |     | - (process.name : "dllhost.exe" and not  |
|     |     | <pre>process.parent.name : ("services.exe",</pre>  |
|     |     | "svchost.exe") and   |
| 28  |     | <pre>- not process.parent.executable : ("?:\\Program</pre>   |
|     |     | Files (x86)\\*", "?:\\Program Files\\*")) or   |
| 29  |     | - (process.name : "smss.exe" and not   |
|     |     | <pre>process.parent.name : ("System", "smss.exe")) or</pre>  |
|     | 26  | + (process.name : "SearchIndexer.exe" and not  |
|     |     | <pre>process.parent.name : ("services.exe",</pre>  |
|     |     | "SearchIndexer.exe")) or   |
|     | 27  | + (process.name : "smss.exe" and not   |
|     |     | process.parent.name : ("System", "smss.exe",   |
|     |     | "sihost.exe")) or  |
| 30  | 28  | (process.name : "wininit.exe" and not  |
|     |     | process.parent.name : "smss.exe") or   |
| 31  |     | - (process.name : ("lsass.exe", "LsaIso.exe") and  |
| 31  |     | not process.parent.name : "wininit.exe") or  |
|     | 29  | ,  |
|     | 23  | <pre>+ (process.name : ("Isass.exe", "LsaIso.exe") and not process.parent.name : ("wininit.exe",</pre> |
|     |     | "lsass.exe")) or   |
| 22  | 20  |  |
| 32  | 30  | (process.name : "services.exe" and not   |
| 2.2 | 2.4 | process.parent.name : "wininit.exe") or  |
| 33  | 31  | (process.name : "spoolsv.exe" and not  |
|     |     | process.parent.name : ("services.exe",   |
|     |     | "spoolsv.exe")) or   |
| 34  | 32  | (process.name : "taskhost.exe" and not   |
|     |     | <pre>process.parent.name : ("services.exe",</pre>  |
|     |     | "svchost.exe")) or   |
| 35  |     | - (process.name : "taskhostw.exe" and not  |
|     |     | <pre>process.parent.name : ("services.exe",</pre>  |
|     |     | "svchost.exe")) or   |
|     | 33  | + (process.name : "taskhostw.exe" and not  |
|     |     | <pre>process.parent.name : ("services.exe",</pre>  |
|     |     | "svchost.exe", "taskhostw.exe")) or  |
| 36  | 34  | <pre>(process.name : ("wmiprvse.exe",</pre>  |
|     |     | "wsmprovhost.exe", "winrshost.exe") and not  |
|     |     | <pre>process.parent.name : "svchost.exe") or</pre>   |
| 37  | 35  | (process.name : "sihost.exe" and not   |
|     |     | <pre>process.parent.name : ("svchost.exe",</pre>   |
|     |     | "sihost.exe")) or  |
|     |     |  |
|     |     |  |

| 38       | 36              | <pre>(process.name : ("winlogon.exe", "csrss.exe", "SearchProtocolHost.exe", "fontdrvhost.exe", "userinit.exe", "dwm.exe", "LogonUI.exe", "taskhostw.exe") and</pre> |
|----------|-----------------|--|
| <b>.</b> |                 | @@ -54,15 +52,20 @@ process where event.action == "start" and  |
| 54       | 52              | "?:\\Program Files   |
|          |                 | <pre>(x86)\\Adobe\\Acrobat DC\\Acrobat\\*\\AcroCEF.exe",</pre>   |
| 55       | 53              | "?:\\Program Files   |
|          |                 | (x86)\\Adobe\\Acrobat Reader   |
| 56       | 54              | <pre>DC\\Reader\\AcroCEF\\RdrCEF.exe",</pre>   |
| 30       | 54              | Files\\Adobe\\Acrobat Reader   |
|          |                 | DC\\Reader\\AcroCEF\\RdrCEF.exe") and  |
| 57       |                 | - not (process.name : "dwm.exe" and  |
|          |                 | <pre>process.code_signature.subject_name == "Teramind</pre>  |
|          |                 | <pre>Inc." and process.code_signature.trusted == true)</pre>   |
|          | 55              | + not (process.name : "dwm.exe" and  |
|          |                 | <pre>process.code_signature.subject_name == "Teramind</pre>  |
|          |                 | <pre>Inc." and process.code_signature.trusted == true) and</pre>   |
|          | 56              | + not (process.name : "SearchProtocolHost.exe" and   |
|          |                 | <pre>process.parent.name : "rundll32.exe" and</pre>  |
|          |                 | process.parent.args :  |
|          |                 | "AppXDeploymentExtensions.OneCore.dll,ShellRefresh"  |
|          |                 | ) and  |
|          | 57              | + not (process.parent.executable :   |
|          |                 | "?:\\Windows\\System32\\smss.exe" and  |
|          | 58              | <pre>process.parent.args : "-SpecialSession") and + not (process.parent.executable : "?:\\Program</pre>  |
|          | 56              | Files\\Sandboxie\\SandboxieDcomLaunch.exe" and   |
|          |                 | process.name : "RuntimeBroker.exe")  |
| 58       | 59              |  |
| 59       | 60              |  |
| 60       |                 | - optional_actions = []  |
| 61       | 61              | [[actions]]  |
| 62       | 62              | action = "kill_process"  |
| 63       | 63              | <pre>field = "process.entity_id"</pre>   |
| 64       | 64              | state = 0  |
| 65       | 65<br><b>66</b> | + [[optional_actions]]   |
|          | 67              | + action = "rollback"  |
|          | 68              | +  |
| 66       | 69              | [[threat]]   |
| 67       | 70              | framework = "MITRE ATT&CK"   |

```
68
         71
                [[threat.technique]]
 ∨ 52 ■■■■■
behavior/rules/defense_evasion_suspicious_troubleshooting...
               @@ -0,0 +1,52 @@
          1 + [rule]
          2 + description = """
          3 + Identifies the execution of the Microsoft
                Diagnostic Wizard to open a diagcab file from a
                suspicious path and with an
          4 + unusual parent process. This may indicate an
                attempt to execute malicious Troubleshooting Pack
                Cabinet files.
          5 + """
          6 + id = "d18721f0-dce0-4bbc-a56a-06ea511b025e"
          7 + license = "Elastic License v2"
          8 + name = "Suspicious Troubleshooting Pack Cabinet
                Execution"
          9 + os_list = ["windows"]
             + reference = ["https://irsl.medium.com/the-trouble-
                with-microsofts-troubleshooters-6e32fc80b8bd"]
         11 + version = "1.0.3"
         12 +
         13 + query = '''
         14 + process where event.action == "start" and
         15 + (process.name : "msdt.exe" or
                process.pe.original_file_name == "msdt.exe") and
                process.args : "/cab" and
         16 +
         + process.parent.name : ("firefox.exe",
                "chrome.exe", "msedge.exe", "explorer.exe",
                "brave.exe", "whale.exe", "browser.exe",
            + "dragon.exe", "vivaldi.exe", "opera.exe",
         18
                "iexplore", "firefox.exe", "waterfox.exe",
                "iexplore.exe", "winrar.exe",
             + "winrar.exe", "7zFM.exe", "outlook.exe",
         19
                "winword.exe", "excel.exe") and
         20
         21
             + process.args : ("?:\\Users\\*\\Downloads\\*",
                                "\\\\*",
         22
         23
                "?:\\Users\\*\\Content.Outlook\\*",
         24
                                "?:\\Users\\Public\\*",
```

```
25
                                "?:\\Users\\*\\AppData\\*",
         26 +
                                "http*",
                                "ftp://*")
         27 +
         28 + '''
         29
         30 + [[actions]]
         31 + action = "kill_process"
         32 + field = "process.entity_id"
         33 + state = 0
         34 +
         35 + [[optional_actions]]
         36 + action = "rollback"
         37 +
         38 + [[threat]]
         39 + framework = "MITRE ATT&CK"
         40 + [[threat.technique]]
         41 + id = "T1218"
         42 + name = "System Binary Proxy Execution"
         43 + reference =
               "https://attack.mitre.org/techniques/T1218/"
         44
         45 +
         46 + [threat.tactic]
         47 + id = "TA0005"
         48 + name = "Defense Evasion"
         49 + reference =
               "https://attack.mitre.org/tactics/TA0005/"
         50
             + [internal]
         51
             + min_endpoint_version = "7.15.0"
 ...or/rules/defense_evasion_suspicious_windows_defender_e... ☐
    <u></u>
               @@ -10,7 +10,7 @@ os_list = ["windows"]
  10
         10
               reference = [
  11
         11
                   "https://docs.microsoft.com/en-
               us/powershell/module/defender/add-mppreference?
               view=windowsserver2019-ps",
         12
  12
             - version = "1.0.5"
  13
         13 + version = "1.0.6"
         14
  14
               query = '''
  15
         15
  16
         16
               sequence with maxspan=1m
```

```
....
                @@ -34,12 +34,14 @@ sequence with maxspan=1m
  34
         34
                   process.args : ("-ExclusionPath", "-
                DisableRealtimeMonitoring", "-
                DisableScriptScanning", "-DisableArchiveScanning")]
                by process.parent.entity_id
  35
         35
  36
         36
  37
              - optional_actions = []
  38
         37
                [[actions]]
                action = "kill_process"
  39
         38
                field = "process.entity_id"
  40
         39
         40
                state = 0
  41
  42
         41
              + [[optional_actions]]
         42
         43
              + action = "rollback"
         44
         45
                [[threat]]
  43
                framework = "MITRE ATT&CK"
  44
         46
  45
         47
                [[threat.technique]]
     ....
 behavior/rules/defense_evasion_suspicious_windows_defende...
                @@ -7,7 +7,7 @@ id = "56751d32-cded-41ad-a273-
     ...
                e6860820c4c3"
                license = "Elastic License v2"
   7
          7
   8
                name = "Suspicious Windows Defender Registry
                Modification"
   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=5s
     +
 behavior/rules/defense_evasion_suspicious_windows_explore... 📮
                @@ -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"]
            - version = "1.0.4"
10
       10
            + version = "1.0.6"
11
       11
              query = '''
12
       12
13
       13
              process where event.action == "start" and
              @@ -16,13 +16,17 @@ process where event.action ==
  .
              "start" and
                 /* miners injecting into Explorer */
16
       16
       17
                  process.args : ("etc", "easyminer*", "ton",
17
              "Rg", "eth", "Toncoin", "mmrig", "--cinit-*",
              "pool.*", "--coin=*", "--cpu-*") or
18
       18
       19
                  /* excute a malicious DLL by clsid */
                  (process.args : "shell:::{*" and not
       20
              process.args : "shell:::{52205fd8-5dfb-447d-801a-
              d0b52f2e83e1}") or
       21
19
       22
                  /* Explorer with unusual process arg length */
                  (length(process.command_line) >= 200 and
20
       23
              process.args count == 3 and not process.args :
              "/select*") or
21
       24
                 /* commonly abused lolbin as parent */
22
       25
                 (process.parent.name : ("rundll32.exe",
23
              "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_Ru
              nDLL")) or
                  not (process.parent.name : "rundll32.exe" and
       28
       29
                       process.parent.args :
              ("?:\\Windows\\System32\\SHELL32.dll,RunAsNewUser_R
              unDLL",
              "AppXDeploymentExtensions.OneCore.dll,ShellRefresh"
              ))) or
26
       30
                  /* unusual parent process by path */
27
```

```
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
                    (process.executable :
  38
         42
                "?:\\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 */
                    (process.name : "explorer.exe" and
  41
                process.command_line : "*.exe *.exe*" and not
                process.args : "*/select*" and not
                process.command_line : "*:\\Program Files*")
                    (process.name : "explorer.exe" and
         45
                process.command_line : "*.exe *.exe*" and not
                process.args : "*/select*" and not
                process.command_line : "*:\\Program Files*") and
         46
                    not process.parent.executable : "?:\\Program
         47
                Files (x86)\\BleachBit\\bleachbit.exe"
  42
         48
                    )
                . . .
         49
  43
  44
         50
     ....
 behavior/rules/defense_evasion_suspicious_windows_lua_scr... 📮
                @@ -7,7 +7,7 @@ id = "8f237d98-1825-4c27-a5cd-
     <u></u>
                e38bde70882a"
   7
           7
                license = "Elastic License v2"
                name = "Suspicious Windows LUA Script Execution"
   8
           8
   9
           9
                os_list = ["windows"]
  10
              - version = "1.0.5"
         10
              + version = "1.0.6"
  11
         11
                query = '''
  12
         12
  13
         13
                sequence by process.entity_id with maxspan=1m
                @@ -17,12 +17,14 @@ sequence by process.entity_id
     .‡.
                with maxspan=1m
```

```
17
          17
                  [network where event.action ==
                 "connection_attempted"]
  18
          18
  19
          19
              - optional_actions = []
  20
  21
          20
                 [[actions]]
  22
                action = "kill_process"
          21
  23
          22
                field = "process.entity_id"
          23
                state = 1
  24
  25
          24
          25
              + [[optional_actions]]
              + action = "rollback"
          26
          27
                 [[threat]]
  26
          28
                framework = "MITRE ATT&CK"
  27
          29
  28
                 [[threat.technique]]
          30
     ····
 behavior/rules/defense_evasion_suspicious_wmic_xsl_script... 📮
                @@ -8,7 +8,7 @@ id = "18371ec4-ee2f-465b-8757-
     <u></u>
                ee726914006c"
   8
                license = "Elastic License v2"
   9
           9
                name = "Suspicious WMIC XSL Script Execution"
         10
                os_list = ["windows"]
  10
              - version = "1.0.9"
  11
              + version = "1.0.10"
          11
  12
          12
                query = '''
  13
          13
  14
          14
                sequence by process.entity_id with maxspan=2m
                @@ -31,12 +31,14 @@ sequence by process.entity_id
     ....
                with maxspan=2m
  31
          31
                 [library where dll.name : ("jscript.dll",
                 "vbscript.dll")]
                 . . .
  32
          32
  33
          33
  34
              - optional_actions = []
  35
          34
                 [[actions]]
                action = "kill_process"
  36
          35
  37
          36
                field = "process.entity_id"
  38
          37
                state = 0
  39
          38
              + [[optional_actions]]
```

```
40
              + action = "rollback"
         41
         42
                [[threat]]
  40
         43
                framework = "MITRE ATT&CK"
  41
  42
         44
                [[threat.technique]]
     ....
 behavior/rules/defense_evasion_unusual_dll_extension_load... 📮
                @@ -7,7 +7,7 @@ id = "76da5dca-ffe5-4756-85ba-
     †
                3ac2e6ccf623"
                license = "Elastic License v2"
   7
           7
                name = "Unusual DLL Extension Loaded by Rundll32 or
          8
   8
                Regsvr32"
                os_list = ["windows"]
   9
              - version = "1.0.6"
  10
         10
              + version = "1.0.7"
  11
         11
         12
                query = '''
  12
  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.d
                11")
  18
         18
  19
         19
                 [library where process.name : ("rundll32.exe",
                "regsvr32.exe") and
  20
              - not dll.name : ("*.dll", "*.cpl", "*.tmp",
                "*.exe", "*.tlb") and
              + not dll.name : ("*.dll", "*.cpl", "*.tmp",
         20
                "*.exe", "*.tlb", "*.scr", "*.dll.mui", "*.ime",
                "*.tsp", "*.rbf") and
                  not (dll.name : ("*.ocx", "*.ax") and
  21
         21
                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",
```

```
26
                "?:\\Windows\\SysWOW64\\liunt.ime",
          25
                                   "?:\\Windows\\System32\\*.ime",
                                   "?:\\Windows\\SysWOW64\\*.ime",
          26
  27
          27
                "?:\\Windows\\System32\\spool\\drivers\\*",
  28
          28
                                   "?:\\Program Files (x86)\\*",
  29
                                   "?:\\Program Files\\*")]
                                   "?:\\Program Files\\*",
          29
                                   "?:\\Windows\\SysWOW64\\*.bpl")
          30
                and
          31
              + not dll.hash.sha256:
                ("cfd375eb124d1fba73f2d46705a43ed30e8aaadca7627bab7
                718f674fb82df38",
          32
                "4af03da6cda5d673725b671dbb3fccfc4badc0651af9065216
                bdcddb0fef7adf",
          33 +
                "bf03c44224a2932e4c12ce02e12059f5c37b7d7ebfbbe4f260
                3b324c368ba2b9",
          34
                "9e318b33d7ae4ece36cdcd345ff6815816f9efcaf9a9b94399
                9c6d80ae043e91")
          35
                 ]
                . . .
  30
          36
          37
  31
              - optional_actions = []
  33
          38
                [[actions]]
  34
                action = "kill_process"
          39
  35
          40
                field = "process.entity_id"
                state = 0
  36
          41
  37
          42
          43
              + [[optional_actions]]
              + action = "rollback"
          44
          45
                [[threat]]
  38
          46
                framework = "MITRE ATT&CK"
  39
          47
  40
          48
                [[threat.technique]]
     +
 behavior/rules/defense_evasion_unusual_network_connection... 📮
                @@ -7,7 +7,7 @@ id = "2e708541-c6e8-4ded-923f-
     <u></u>
                78a6c160987e"
```

```
7
          7
                license = "Elastic License v2"
   8
                name = "Unusual Network Connection via RunDLL32"
                os_list = ["windows"]
   9
           9
  10
              - version = "1.0.9"
              + version = "1.0.10"
          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
              - optional_actions = []
  21
  22
          21
                [[actions]]
  23
          22
                action = "kill_process"
                field = "process.entity_id"
  24
          23
  25
          24
                state = 1
          25
  26
              + [[optional_actions]]
          26
              + action = "rollback"
          27
          28
  27
          29
                [[threat]]
                framework = "MITRE ATT&CK"
  28
          30
  29
          31
                [[threat.technique]]
     ····
 . . .
behavior/rules/defense_evasion_windows_error_manager_repo...
                @@ -8,7 +8,7 @@ id = "3d16f5f9-da4c-4b15-a501-
     <u></u>
                505761b75ca6"
                license = "Elastic License v2"
   9
           9
                name = "Windows Error Manager/Reporting
                Masquerading"
  10
          10
                os_list = ["windows"]
              - version = "1.0.8"
  11
              + version = "1.0.9"
          11
  12
          12
                query = '''
  13
          13
  14
          14
                sequence by process.entity_id with maxspan=5m
```

```
@@ -17,12 +17,14 @@ sequence by process.entity_id
     .
                with maxspan=5m
                  [network where event.action ==
  17
         17
                "connection_attempted" and process.name :
                ("wermgr.exe", "WerFault.exe")]
         18
  18
  19
         19
  20
              - optional_actions = []
  21
         20
                [[actions]]
                action = "kill_process"
  22
         21
  23
                field = "process.entity_id"
         22
  24
         23
                state = 0
  25
         24
              + [[optional_actions]]
         25
         26
              + action = "rollback"
         27
         28
                [[threat]]
  26
  27
         29
                framework = "MITRE ATT&CK"
  28
         30
                [[threat.technique]]
     ....
 ...rules/defense_evasion_windows_firewall_exception_list ... 「☐
     †
                @@ -10,7 +10,7 @@ os_list = ["windows"]
  10
         10
                reference = [
  11
         11
                    "https://docs.microsoft.com/en-
                us/troubleshoot/windows-server/networking/netsh-
                advfirewall-firewall-control-firewall-behavior",
  12
         12
                1
  13
              - version = "1.0.9"
         13
              + version = "1.0.10"
  14
         14
  15
         15
                query = '''
  16
         16
                sequence with maxspan=1m
    --‡--
                @@ -23,12 +23,14 @@ sequence with maxspan=1m
  23
         23
                   ] by process.parent.entity_id
                . . .
         24
  24
  25
         25
              - optional_actions = []
  26
  27
         26
                [[actions]]
                action = "kill_process"
  28
         27
                field = "process.entity_id"
  29
         28
  30
         29
                state = 0
```

```
31
         30
         31
             + [[optional_actions]]
              + action = "rollback"
         32
         33
  32
         34
                [[threat]]
                framework = "MITRE ATT&CK"
  33
         35
  34
                [[threat.technique]]
         36
 behavior/rules/defense_evasion_windows_installer_with_sus... 📮
     <u></u>
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
                name = "Windows Installer with Suspicious
   8
                Properties"
          9
                os_list = ["windows"]
   9
         10
                reference = ["https://lolbas-
  10
                project.github.io/lolbas/Binaries/Msiexec/"]
              - version = "1.0.4"
  11
              + version = "1.0.5"
         11
  12
         12
  13
         13
                query = '''
  14
         14
                sequence with maxspan=1m
```

```
behavior/rules/discovery_external_ip_address_discovery_vi... 💾
                @@ -7,7 +7,7 @@ id = "51894221-7657-4b56-9406-
     †
                e080e19ad159"
   7
                license = "Elastic License v2"
          7
   8
                name = "External IP Address Discovery via a Trusted
                Program"
                os_list = ["windows"]
   9
              - version = "1.0.8"
  10
              + version = "1.0.9"
         10
         11
  11
                query = '''
  12
         12
  13
         13
                sequence by process.entity_id with maxspan=5m
                @@ -62,12 +62,17 @@ sequence by process.entity_id
     ...
                with maxspan=5m
  62
         62
                  ]
                . . .
  63
         63
```

```
64
         64
  65
              - optional_actions = []
         65
                [[actions]]
  66
                action = "kill_process"
  67
         66
  68
         67
                field = "process.entity_id"
                state = 0
  69
         68
  70
         69
         70
              + [[optional_actions]]
              + action = "rollback"
         71
         72
         73
              + [[optional_actions]]
              + action = "rollback"
         74
         75
                [[threat]]
  71
         76
                framework = "MITRE ATT&CK"
  72
         77
  73
                [[threat.technique]]
         78
     ····
 behavior/rules/discovery_external_ip_address_discovery_vi... 📮
                @@ -7,16 +7,17 @@ id = "dfe28e03-9b0b-47f5-9753-
     <u></u>
                65ed2666663f"
   7
                license = "Elastic License v2"
                name = "External IP Address Discovery via Untrusted
   8
           8
                Program"
   9
                os_list = ["windows"]
              - version = "1.0.8"
  10
              + version = "1.0.9"
         10
  11
         11
                query = '''
  12
         12
  13
                sequence by process.entity_id with maxspan=1m
         13
  14
         14
  15
         15
                 /* execution of an unsigned PE file followed by
                dns request to public ip discovery web services */
  16
         16
  17
                  [process where event.action == "start" and
                user.id: "S-1-5-21-*" and
         17
                  [process where event.action == "start" and not
                user.id : "S-1-5-18" and
  18
         18
                   not process.code_signature.trusted == true and
                   process.executable : ("?:\\Users\\*",
  19
                "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*",
                "?:\\Windows\\Tasks\\*")]
```

```
19
                    process.executable : ("?:\\Users\\*",
                 "?:\\ProgramData\\*", "?:\\Windows\\Temp\\*",
                 "?:\\Windows\\Tasks\\*") and
          20
                    (process.Ext.relative_file_creation_time <= 300</pre>
                 or process.Ext.relative_file_name_modify_time <=
                 300) ]
          21
                   [dns where
  20
  21
          22
                     dns.question.name :
  22
          23
     +
                 @@ -53,14 +54,17 @@ sequence by process.entity_id
     .
                with maxspan=1m
  53
          54
                           "ip4.seeip.org",
                           "*.geojs.io",
  54
          55
                           "*portmap.io"
  55
          56
  56
                          )]
                          )
          57
          58
                 . . .
          59
  57
  58
          60
              - optional_actions = []
  59
  60
          61
                 [[actions]]
                 action = "kill_process"
  61
          62
  62
                 field = "process.entity_id"
          63
  63
              - state = 1
          64
              + state = 0
          65
              + [[optional_actions]]
          66
          67
              + action = "rollback"
  64
          68
  65
          69
                 [[threat]]
  66
          70
                 framework = "MITRE ATT&CK"
     ....
                 @@ -76,4 +80,4 @@ name = "Discovery"
  76
          80
                 reference =
                 "https://attack.mitre.org/tactics/TA0007/"
  77
          81
  78
          82
                 [internal]
  79
              - min_endpoint_version = "7.15.0"
          83
              + min_endpoint_version = "8.4.0"
 behavior/rules/discovery_potential_security_software_disc... 📮
     <u></u>
                 @@ -8,7 +8,7 @@ license = "Elastic License v2"
```

```
8
          8
                name = "Potential Security Software Discovery via
                Grep"
          9
                os_list = ["linux", "macos"]
   9
  10
         10
                reference = ["https://objective-
                see.com/blog/blog_0x4F.html"]
              - version = "1.0.7"
  11
              + version = "1.0.8"
         11
  12
         12
  13
         13
                query = '''
  14
         14
                process where event.type == "start" and
     +
 behavior/rules/discovery_potential_virtual_machine_finger... [ ]
     <u></u>
                @@ -8,7 +8,7 @@ license = "Elastic License v2"
   8
          8
                name = "Potential Virtual Machine Fingerprinting
                via Grep"
                os_list = ["macos"]
   9
          9
                reference = ["https://objective-
  10
         10
                see.com/blog/blog_0x4F.html"]
              - version = "1.0.6"
  11
         11
              + version = "1.0.7"
  12
         12
                query = '''
         13
  13
  14
         14
                process where event.type == "start" and
     Τ.
  behavior/rules/execution_command_shell_activity_started_v... 📮
                @@ -4,7 +4,7 @@ id = "b8a0a3aa-0345-4035-b41d-
     <u></u>
                f758a6c59a78"
                license = "Elastic License v2"
   4
          4
                name = "Command Shell Activity Started via
   5
          5
                RunDLL32"
                os_list = ["windows"]
   6
              - version = "1.0.6"
   7
```

7

8

9

10

8

9

10

+ version = "1.0.7"

process where event.type == "start" and

query = '''

https://github.com/elastic/protections-artifacts/commit/746086721fd385d9f5c6647cada1788db4aea95f#difff5deb07688e1a8dec9530bc3071967b2da5c16b482e671812b864c37beb28f08

| <b>.</b> |    | @@ -22,7 +22,8 @@ process where event.type == "start" and   |
|----------|----|---|
| 22       | 22 | <pre>not (process.args :     ("launchalpsdelltouchpad://Mainpage/path2?     param=start",     "alpsdelltouchpadsettings://Mainpage/path2?     param=start") and</pre> |
| 23       | 23 | <pre>process.parent.args : "?:\\WINDOWS\\System32\\main.cpl") and</pre>   |
| 24       | 24 | <pre>not (process.command_line : "*REG QUERY HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Cryptograp hy*" and</pre>   |
| 25       |    | <pre>- process.parent.args :    "?:\\WINDOWS\\system32\\PcaSvc.dll,PcaPatchSdbTask" )</pre>   |
|          | 25 | <pre>+ process.parent.args :    "?:\\WINDOWS\\system32\\PcaSvc.dll,PcaPatchSdbTask" ) and</pre>   |
|          | 26 | <pre>+ not (process.args :    "launchalpsdelltouchpad://Mainpage/path2?    param=start" and process.parent.args :    "Vxd_launch_UI")</pre>                           |
| 26       | 27 | ***   |
| 27       | 28 |   |
|          |    |   |
| 28       | 29 | 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

