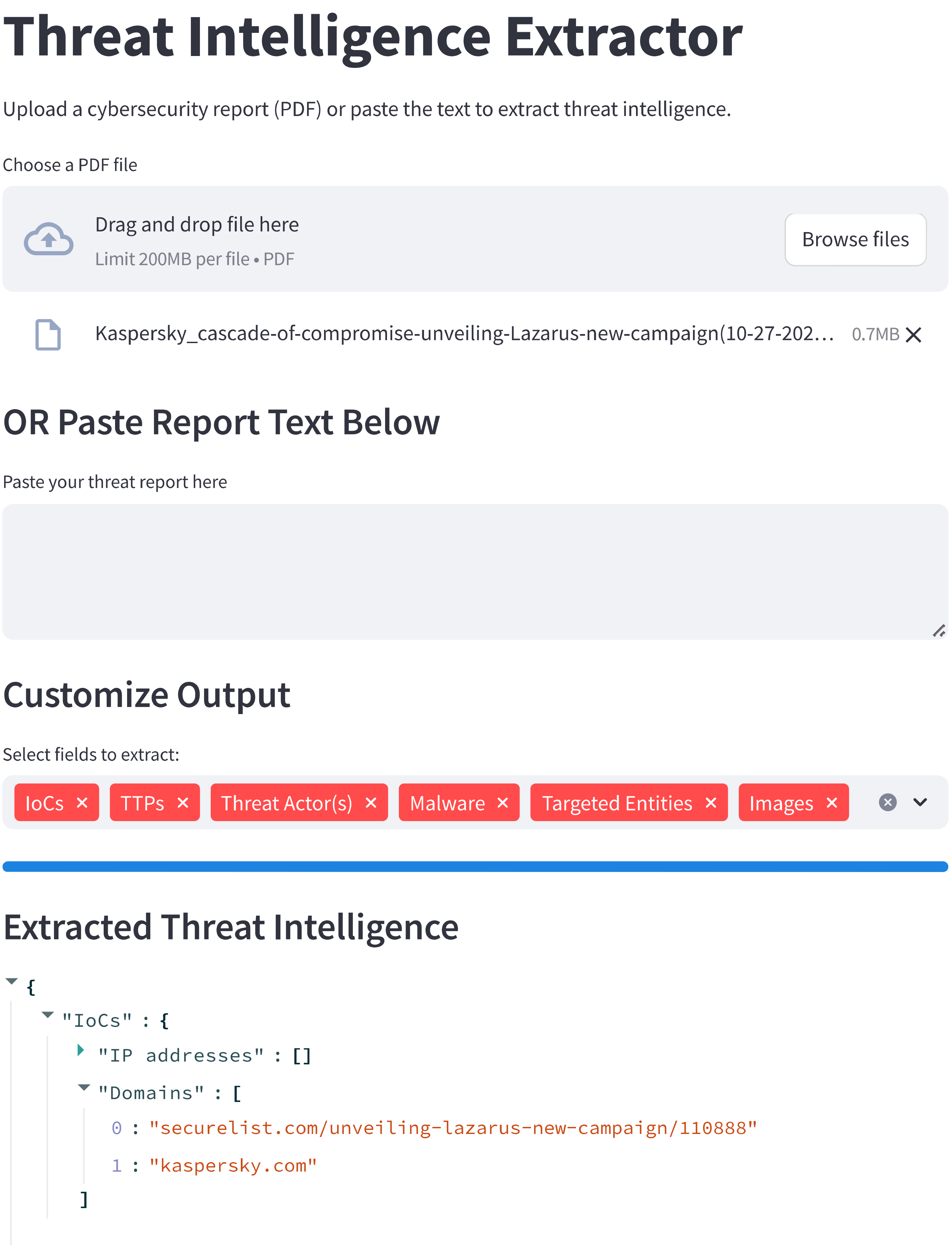


Threat Intelligence Extractor

Upload a cybersecurity report (PDF) or paste the text to extract threat intelligence.

Choose a PDF file

Kaspersky_cascade-of-compromise-unveiling-Lazarus-new-campaign(10-27-202… 0.7MB

OR Paste Report Text Below

Paste your threat report here

Customize Output

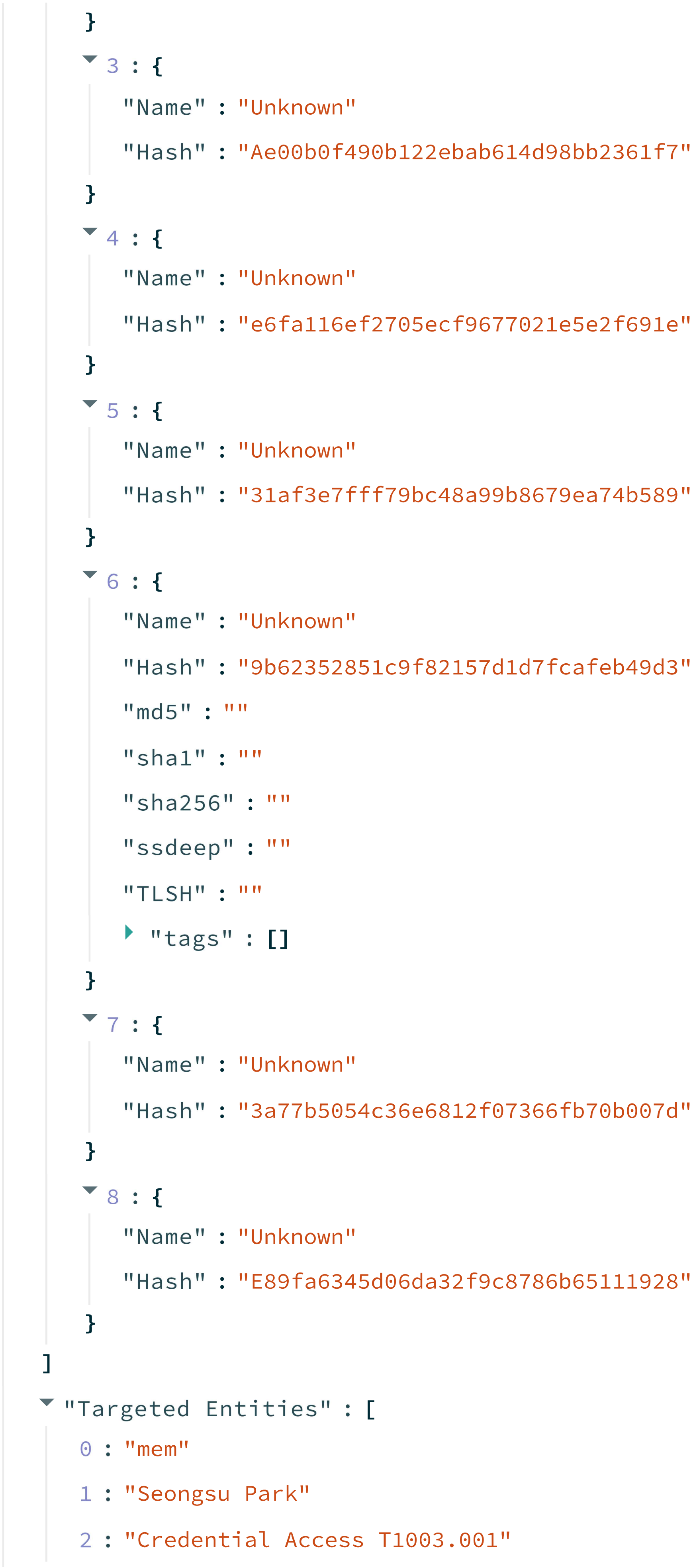
Select fields to extract:

IoCs × TTPs × Threat Actor(s) × Malware × Targeted Entities × Images ×

Extracted Threat Intelligence

```
{
  "IoCs" : {
    "IP addresses" : []
    "Domains" : [
      0 : "securelist.com/unveiling-lazarus-new-campaign/110888"
      1 : "kaspersky.com"
    ]
    "Email addresses" : [
      0 : "intelreports@kaspersky.com"
    ]
    "File hashes" : [
      0 : "9b62352851c9f82157d1d7fcafeb49d3"
      1 : "3a77b5054c36e6812f07366fb70b007d"
      2 : "88a96f8730b35c7406d57f23bbba734d"
      3 : "e6fa116ef2705ecf9677021e5e2f691e"
      4 : "31af3e7fff79bc48a99b8679ea74b589"
      5 : "E89fa6345d06da32f9c8786b65111928"
      6 : "9cd90dff2d9d56654dbecdcd409e1ef3"
      7 : "Ae00b0f490b122ebab614d98bb2361f7"
      8 : "54df2984e833ba2854de670cce43b823"
    ]
  }
  "TTPs" : {
    "Tactics" : [
      0 : {
        "TA0001" : "Initial Access"
      }
      1 : {
        "TA0002" : "Execution"
      }
      2 : {
        "TA0003" : "Persistence"
      }
      3 : {
        "TA0004" : "Privilege Escalation"
      }
      4 : {
        "TA0005" : "Defense Evasion"
      }
      5 : {
        "TA0006" : "Credential Access"
      }
      6 : {
        "TA0007" : "Discovery"
      }
      7 : {
        "TA0009" : "Collection"
      }
      8 : {
        "TA0010" : "Exfiltration"
      }
      9 : {
        "TA0011" : "Command and Control"
      }
    ]
    "Techniques" : []
  }
  "Threat Actor(s)" : [
    0 : "mem"
    1 : "Credential Access T1003.001"
    2 : "CPU"
    3 : "shv"
    4 : "hxxps://www[.]muijae[.]com"
    5 : "Control T1071.001"
    6 : "hxxps://pediatrics[.]or[.]kr/PubReader/build_css[.]php"
    7 : "Next"
    8 : "CCBrush"
    9 : "SID"
    10 : "LPEClient"
    11 : "C:\ProgramData\ntuser.008.dat
         C:\ProgramData\ntuser.009.dat
         C:\ProgramData\ntuser.001.dat
         C:\ProgramData\ntuser.002.dat"
    12 : "SIGNBTLG"
    13 : "XDR"
    14 : "CCButton"
    15 : "ifi"
    16 : "Command"
    17 : "Lazarus"
```

```
        18 : "hxxps://hspje[.]com:80/menu6/teacher_qna[.]asp"
        19 : "SIGNBTKE"
        20 : "Privilege Escalation T1547.012
             "
        21 : "SIGNBTFI"
        22 : "T1083"
        23 : "AES"
        24 : "hxxps://www[.]droof[.]kr/Board"
        25 : "uci"
        26 : "SIGNBT"
        27 : "secDelete"
        28 : "TREX"
        29 : "HTTP POST"
        30 : "SIGNBTGC"
        31 : "Malware Technologies"
        32 : "UID"
        33 : "DWORD"
        34 : "Tactic Techniques
             Initial Access T1189"
        35 : "Function"
        36 : "CCBitmap"
        37 : "3/11SIGNBTLG Initial"
    ]
    "Malware" : [
        0 : {
            "Name" : "Unknown"
            "Hash" : "9cd90dff2d9d56654dbecdcd409e1ef3"
        }
        1 : {
            "Name" : "Unknown"
            "Hash" : "88a96f8730b35c7406d57f23bbba734d"
        }
        2 : {
            "Name" : "Unknown"
            "Hash" : "54df2984e833ba2854de670cce43b823"
```



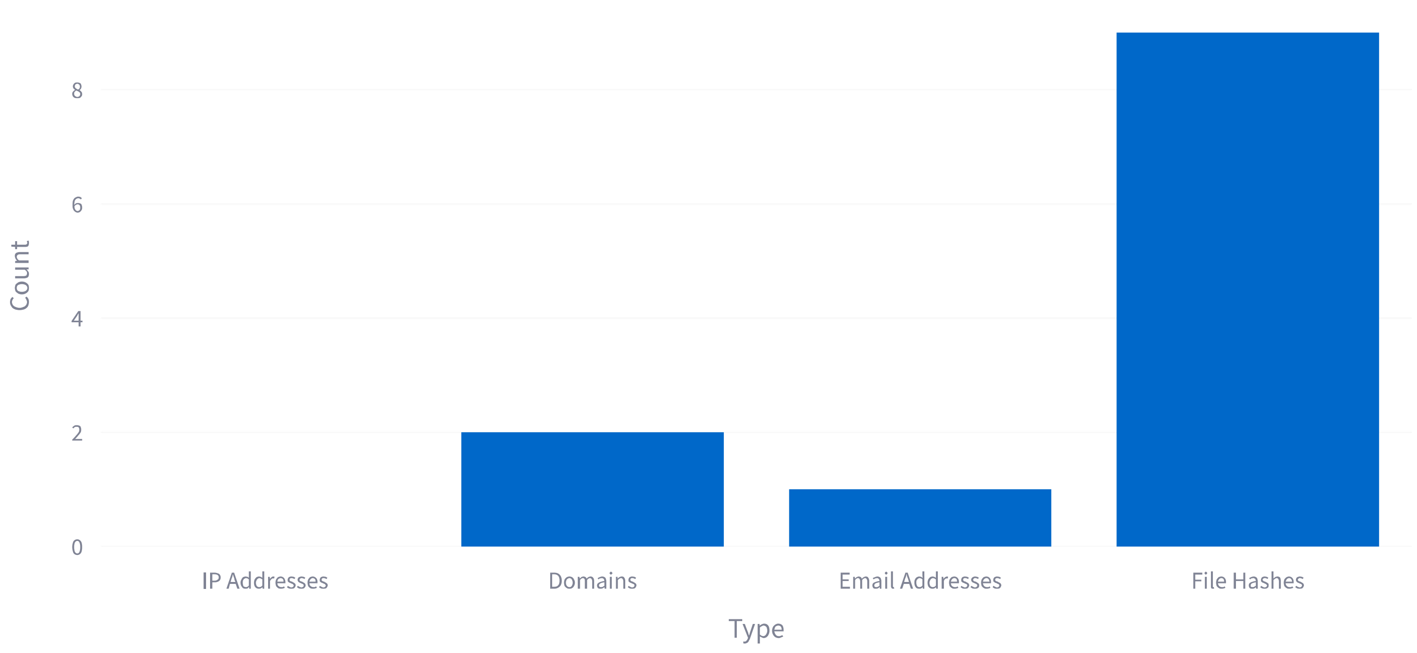
```
    }
  ▾ 3 : {
      "Name" : "Unknown"
      "Hash" : "Ae00b0f490b122ebab614d98bb2361f7"
    }
  ▾ 4 : {
      "Name" : "Unknown"
      "Hash" : "e6fa116ef2705ecf9677021e5e2f691e"
    }
  ▾ 5 : {
      "Name" : "Unknown"
      "Hash" : "31af3e7fff79bc48a99b8679ea74b589"
    }
  ▾ 6 : {
      "Name" : "Unknown"
      "Hash" : "9b62352851c9f82157d1d7fcafeb49d3"
      "md5" : ""
      "sha1" : ""
      "sha256" : ""
      "ssdeep" : ""
      "TLSH" : ""
    ▸ "tags" : []
    }
  ▾ 7 : {
      "Name" : "Unknown"
      "Hash" : "3a77b5054c36e6812f07366fb70b007d"
    }
  ▾ 8 : {
      "Name" : "Unknown"
      "Hash" : "E89fa6345d06da32f9c8786b65111928"
    }
]
▾ "Targeted Entities" : [
    0 : "mem"
    1 : "Seongsu Park"
    2 : "Credential Access T1003.001"
```

```
3 : "CPU"
4 : "shv"
5 : "conn"
6 : "hxxps://www[.]muijae[.]com"
7 : "Control T1071.001"
8 : "hxxps://pediatrics[.]or[.]kr/PubReader/build_css[.]php"
9 : "Shareaza"
10 : "setSleep"
11 : "Next"
12 : "T1574.002"
13 : "CCBrush"
14 : "SID"
15 : "XU"
16 : "LPEClient"
17 : "C:\ProgramData\ntuser.008.dat
     C:\ProgramData\ntuser.009.dat
     C:\ProgramData\ntuser.001.dat
     C:\ProgramData\ntuser.002.dat"
18 : "SIGNBTLG"
19 : "T1132.002"
20 : "XDR"
21 : "CCButton"
22 : "system%\ualapi.dll"
23 : "ifi"
24 : "Command"
25 : "Lazarus"
26 : "hxxps://hspje[.]com:80/menu6/teacher_qna[.]asp"
27 : "SIGNBTKE"
28 : "Privilege Escalation T1547.012
     "
29 : "SIGNBTFI"
30 : "T1083"
31 : "AES"
32 : "hxxps://mainbiz[.]or[.]kr"
33 : "hxxps://www[.]droof[.]kr/Board"
```

```
    34 : "uci"
    35 : "measure[.]asp"
    36 : "SIGNBT"
    37 : "secDelete"
    38 : "TREX"
    39 : "HTTP POST"
    40 : "SIGNBTGC"
    41 : "Malware Technologies"
    42 : "UID"
    43 : "DWORD"
    44 : "Tactic Techniques
         Initial Access T1189"
    45 : "Function"
    46 : "CCBitmap"
    47 : "3/11SIGNBTLG Initial"
  ]
}
```

Indicators of Compromise (IoCs)

IoCs by Type



Tactics, Techniques, and Procedures (TTPs)

Tactics:

```
[
    0 : {
      "TA0001" : "Initial Access"
    }
    1 : {
      "TA0002" : "Execution"
    }
    2 : {
      "TA0003" : "Persistence"
    }
    3 : {
      "TA0004" : "Privilege Escalation"
    }
    4 : {
      "TA0005" : "Defense Evasion"
    }
    5 : {
      "TA0006" : "Credential Access"
    }
    6 : {
      "TA0007" : "Discovery"
    }
    7 : {
      "TA0009" : "Collection"
    }
    8 : {
      "TA0010" : "Exfiltration"
    }
    9 : {
      "TA0011" : "Command and Control"
    }
]
```

Techniques:

```
▸ []
```

Threat Actor(s)

```
▾ [
  0 : "mem"
  1 : "Credential Access T1003.001"
  2 : "CPU"
  3 : "shv"
  4 : "hxxps://www[.]muijae[.]com"
  5 : "Control T1071.001"
  6 : "hxxps://pediatrics[.]or[.]kr/PubReader/build_css[.]php"
  7 : "Next"
  8 : "CCBrush"
  9 : "SID"
  10 : "LPEClient"
  11 : "C:\ProgramData\ntuser.008.dat
       C:\ProgramData\ntuser.009.dat
       C:\ProgramData\ntuser.001.dat
       C:\ProgramData\ntuser.002.dat"
  12 : "SIGNBTLG"
  13 : "XDR"
  14 : "CCButton"
  15 : "ifi"
  16 : "Command"
  17 : "Lazarus"
  18 : "hxxps://hspje[.]com:80/menu6/teacher_qna[.]asp"
  19 : "SIGNBTKE"
  20 : "Privilege Escalation T1547.012
       "
  21 : "SIGNBTFI"
  22 : "T1083"
  23 : "AES"
  24 : "hxxps://www[.]droof[.]kr/Board"
```

```
    25 : "uci"
    26 : "SIGNBT"
    27 : "secDelete"
    28 : "TREX"
    29 : "HTTP POST"
    30 : "SIGNBTGC"
    31 : "Malware Technologies"
    32 : "UID"
    33 : "DWORD"
    34 : "Tactic Techniques
         Initial Access T1189"
    35 : "Function"
    36 : "CCBitmap"
    37 : "3/11SIGNBTLG Initial"
]
```

Malware Details

```
[
    0 : {
      "Name" : "Unknown"
      "Hash" : "9cd90dff2d9d56654dbecdcd409e1ef3"
    }
    1 : {
      "Name" : "Unknown"
      "Hash" : "88a96f8730b35c7406d57f23bbba734d"
    }
    2 : {
      "Name" : "Unknown"
      "Hash" : "54df2984e833ba2854de670cce43b823"
    }
    3 : {
      "Name" : "Unknown"
      "Hash" : "Ae00b0f490b122ebab614d98bb2361f7"
    }
    4 : {
      "Name" : "Unknown"
      "Hash" : "e6fa116ef2705ecf9677021e5e2f691e"
    }
    5 : {
      "Name" : "Unknown"
      "Hash" : "31af3e7fff79bc48a99b8679ea74b589"
    }
    6 : {
      "Name" : "Unknown"
      "Hash" : "9b62352851c9f82157d1d7fcafeb49d3"
      "md5" : ""
      "sha1" : ""
      "sha256" : ""
      "ssdeep" : ""
      "TLSH" : ""
      "tags" : []
    }
    7 : {
      "Name" : "Unknown"
      "Hash" : "3a77b5054c36e6812f07366fb70b007d"
    }
    8 : {
      "Name" : "Unknown"
      "Hash" : "E89fa6345d06da32f9c8786b65111928"
    }
]
```

Targeted Entities

```
[
  0 : "mem"
  1 : "Seongsu Park"
  2 : "Credential Access T1003.001"
  3 : "CPU"
  4 : "shv"
  5 : "conn"
```

```
6 : "hxxps://www[.]muijae[.]com"
7 : "Control T1071.001"
8 : "hxxps://pediatrics[.]or[.]kr/PubReader/build_css[.]php"
9 : "Shareaza"
10 : "setSleep"
11 : "Next"
12 : "T1574.002"
13 : "CCBrush"
14 : "SID"
15 : "XU"
16 : "LPEClient"
17 : "C:\ProgramData\ntuser.008.dat
C:\ProgramData\ntuser.009.dat
C:\ProgramData\ntuser.001.dat
C:\ProgramData\ntuser.002.dat"
18 : "SIGNBTLG"
19 : "T1132.002"
20 : "XDR"
21 : "CCButton"
22 : "system%\ualapi.dll"
23 : "ifi"
24 : "Command"
25 : "Lazarus"
26 : "hxxps://hspje[.]com:80/menu6/teacher_qna[.]asp"
27 : "SIGNBTKE"
28 : "Privilege Escalation T1547.012
"
29 : "SIGNBTFI"
30 : "T1083"
31 : "AES"
32 : "hxxps://mainbiz[.]or[.]kr"
33 : "hxxps://www[.]droof[.]kr/Board"
34 : "uci"
35 : "measure[.]asp"
36 : "SIGNBT"
```

```
  37 : "secDelete"
  38 : "TREX"
  39 : "HTTP POST"
  40 : "SIGNBTGC"
  41 : "Malware Technologies"
  42 : "UID"
  43 : "DWORD"
  44 : "Tactic Techniques Initial Access T1189"
  45 : "Function"
  46 : "CCBitmap"
  47 : "3/11SIGNBTLG Initial"
]
```

Extracted Images

The `use_column_width` parameter has been deprecated and will be removed in a future release. Please utilize the `use_container_width` parameter instead.

Extracted Image

Summary

Total IoCs Extracted: 12

Total TTPs Identified: 10

Total Threat Actors Identified: 38

Total Malware Identified: 9

Total Targeted Entities Identified: 48

Total Images Extracted: 1

Download Results

Download Threat Intelligence as JSON