HAFNIUM DETECTION CONTENT

HAFNIUM (also known as UNC2639, UNC2640, UNC2643, and Ant) are a group known to target Internet-facing servers and applications. Thought to have begun in January 2021, the group launched a widespread global campaign targeting on-premise Microsoft Exchange servers, including 2013, 2016, and 2019.

As a part of its Community Defense Measures (CDM) program, Cyborg Security has designed advanced detection content to enable organizations to detect various phases of the HAFNIUM activity including exploitation, webshell creation, post-exploitation, and removal of adversarial indicators on the system.

CYBORG SECURITY

Phase 1 - Exploitation

Microsoft Exchange Server RCE (CVE-2021-26855)

Splunk

```
method="POST" uri IN ("/owa/auth/Current/themes/resources/*", "/owa/auth/Current/*",
"/ecp/default.flt", "/ecp/main.css", "/ecp/*.js")
| stats values(_time) as Occurrences, values(uri) as URIs, values(method) as httpMethods
count by host
| convert ctime(Occurrences)
```

Elastic

```
{
  "bool": {
    "must": [
      {
        "bool": {
          "should": [
            {
              "query_string": {
                "query": "/.*/\\/[Oo][Ww][Aa]\\/[Aa][Uu][Tt][Hh]\\/[Cc][Uu][Rr]+[Ee][Nn][Tt]\\/.*/",
                "fields": [
                  "url"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*\\/[Ee][Cc][Pp]\\/(Dd][Ee][Ff][Aa][Uu][Ll][Tt]\\.[Ff][Ll][Tt]|[Mm][Aa][Ii][Nn]\\.[Cc][Ss]+|*\\.[Jj][Ss]).*/",
                "fields": [
                  "url"
                ]
              }
            }
          ]
        }
      },
      {
        "bool": {
          "must": [
            {
              "query_string": {
                "query": "/[Pp][Oo][Ss][Tt]/",
                "fields": [
                  "http.request.method"
                ]
              }
            }
          ]
        }
      }
    ]
  }
}
```

Phase 2 - Webshell Creation

Exchange Vulnerability (CVE-2021-25655) HAFNIUM Webshell Creation

Splunk

```
index=sysmon source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventID=11
TargetFilename="*\inetpub\wwwroot\aspnet_client\system_web*"
| regex TargetFilename="(\\\)([a-zA-Z0-9]{8}\.aspx)$"
| stats values(Computer) as sourceHosts, values(Image) as processPaths by TargetFilename
```

Elastic

```
{
   "bool": {
       "must": [
           {
               "query_string": {
                   "query": "/.*[a-zA-Z0-9]{8}\\.[Aa][Ss][Pp][Xx]/",
                   "fields": [
                       "file.path",
                       "file.name"
                   ]
               }
           },
           {
               "query_string": {
                   "query": "11",
                   "fields": [
                       "event.code"
                   ]
               }
           },
           {
               "query_string": {
                   "query": "/.*\\inetpub\\wwwroot\\aspnet_client\\system_web.*/",
                   "fields": [
                       "file.path"
                   ]
               }
           }
       ]
   }
}
```

Phase 3 - Post Exploitation Activities

Dump LSASS via comsvcs DLL

Splunk

```
index=sysmon source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
Image="*\\rundll32.exe" CommandLine="*comsvcs.dll*" CommandLine="*MiniDump*"
| stats values(_time) as Occurrences, values(Image) as processPaths, values(CommandLine)
as processCommandLines count by Computer
| convert ctime(Occurrences)
```

Elastic

```
{
 "bool": {
   "must": [
     {
       "query_string": {
         "query": "/.*\\\\[Rr][Uu][Nn][Dd][Ll][Ll]32\\.[Ee][Xx][Ee]/",
         "fields": [
           "process.executable"
         ]
       }
     },
     {
       "query_string": {
         "query": "/.*[Cc][Oo][Mm][Ss][Vv][Cc][Ss]\\.[Dd][Ll][Ll].*/",
         "fields": [
           "process.command_line",
           "process.args"
         ]
       }
     },
     {
       "query_string": {
         "query": "/.*[Mm][Ii][Nn][Ii][DD][Uu][Mm][Pp].*/",
         "fields": [
           "process.command_line",
           "process.args"
         ]
       }
     }
   ]
 }
}
```

Phase 3 - Post Exploitation Activities

Dump LSASS via procdump

Splunk

```
index=sysmon source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
Image="*\\procdump.exe" CommandLine="*lsass*" (CommandLine="*-ma*" OR CommandLine="*-
mm*")
| stats values(_time) as Occurrences, values(Image) as processPaths, values(CommandLine)
as processCommandLines count by Computer
| convert ctime(Occurrences)
```

Elastic

```
{
 "bool": {
   "must": [
     {
       "bool": {
         "must": [
           {
             "query_string": {
               "query": "/.*\\\\[Pp][Rr][Oo][Cc][Dd][Uu][Mm][Pp]\\.[Ee][Xx][Ee]/",
               "fields": [
                 "process.executable"
               ]
             }
           },
           {
             "query_string": {
               "query": "/.*[Ll][Ss][Aa][Ss][Ss].*/",
               "fields": [
                 "process.command_line",
                 "process.args"
               ]
             }
           }
         ]
       }
     },
     {
       "bool": {
         "should": [
           {
             "query_string": {
               "query": "/.*\\-[Mm][Aa].*/",
               "fields": [
                 "process.command_line",
                 "process.args"
               ]
             }
           },
           {
             "query_string": {
               "query": "/.*\\-[Mm][Mm].*/",
               "fields": [
                 "process.command_line",
                 "process.args"
               ]
             }
           }
         ]
       }
     }
   ]
 }
}
```

Phase 4 - Cleanup

Exchange Vulnerability (CVE-2021-25655) HAFNIUM Clearing Tracks

Splunk

```
index=sysmon source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
((CommandLine="*inetpub\\wwwroot\\aspnet_client*" AND CommandLine="*del*" AND
CommandLine="*owa\\auth\\Outlook*" AND CommandLine="*.aspx*") OR (CommandLine="*attrib*"
AND CommandLine="*+h*" AND CommandLine="*+r*" AND CommandLine="*+s*" AND
CommandLine="*Outlook*" AND CopmmandLine="*.aspx*" "*inetpub\\wwwroot\\aspnet_client*"))
| stats values(_time) as Occurrences, values(Image) as processPaths, values(CommandLine)
as processCommandLines count by Computer
| convert ctime(Occurrences)
```

Elastic

```
{
  "bool": {
    "should": [
      {
        "bool": {
          "must": [
            {
              "query_string": {
                "query": "/.*[Ii][Nn][Ee][Tt][Pp][Uu][Bb]\\\\[Ww][Ww][Ww][Rr][Oo][Oo][Tt]\\\\[Aa][Ss][Pp][Nn][Ee][Tt]_[Cc][Ll][Ii][Ee][Nn][Tt].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*[Dd][Ee][Ll].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*[Oo][Ww][Aa]\\\\[Aa][Uu][Tt][Hh]\\\\[Oo][Uu][Tt][Ll][Oo][Oo][Kk].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*[Aa][Ss][Pp][Xx].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            }
          ]
        }
      },
      {
        "bool": {
          "must": [
            {
              "query_string": {
                "query": "/.*[Aa][Tt][Tt][Rr][Ii][Bb].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*\\+[Hh].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*\\+[Rr].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*\\+[Ss].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*[Oo][Uu][Tt][Ll][Oo][Oo][Kk].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*[Aa][Ss][Pp][Xx].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            },
            {
              "query_string": {
                "query": "/.*[Ii][Nn][Ee][Tt][Pp][Uu][Bb]\\\\[Ww][Ww][Ww][Rr][Oo][Oo][Tt]\\\\[Aa][Ss][Pp][Nn][Ee][Tt]_[Cc][Ll][Ii][Ee][Nn][Tt].*/",
                "fields": [
                  "process.command_line",
                  "process.args"
                ]
              }
            }
          ]
        }
      }
    ]
  }
}
```