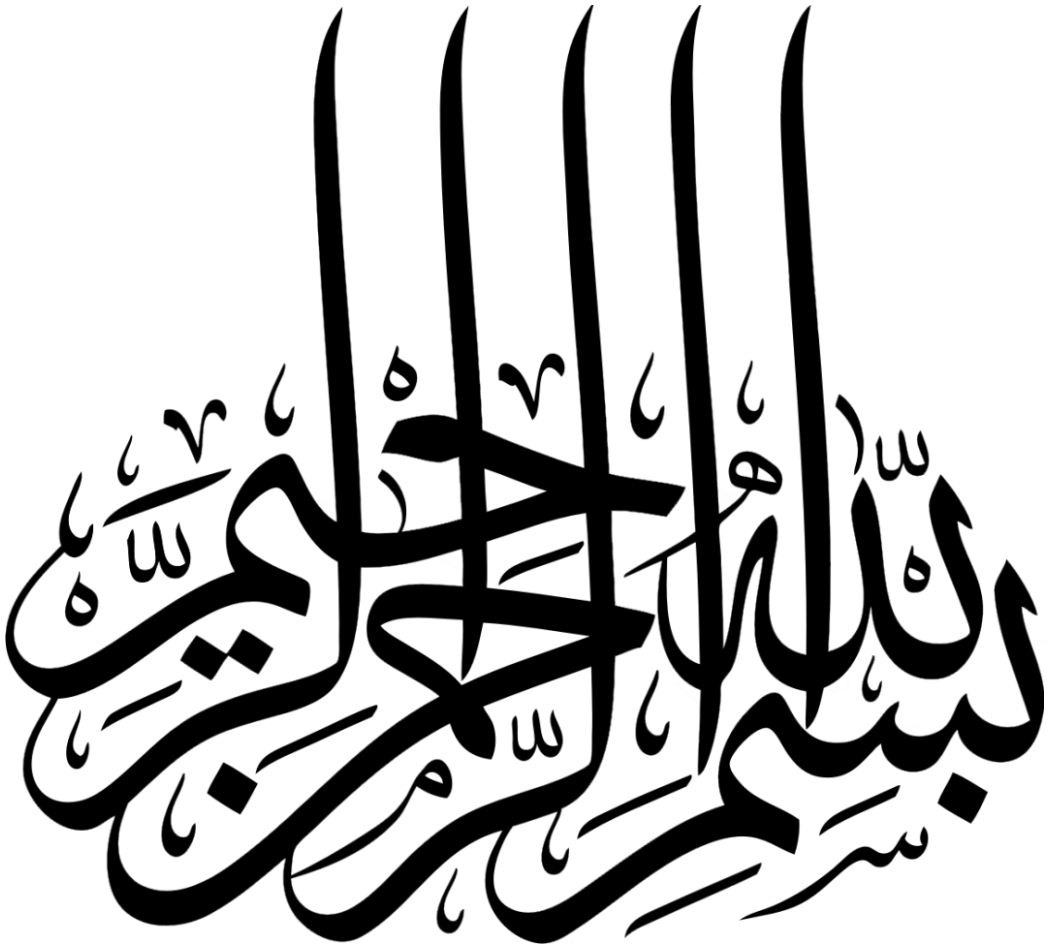

بسم الله الرحمن الرحیم

Defender Control

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه ۴
آشنایی بیشتر با Defender ۵
فرار از شناسایی ۷
IOCs ۱۰

مقدمه

Defender Control یک ابزار کاربردی رایگان است که در نفوذهای مختلف با آن برخورد کرده‌ایم. سازندگان آن را اینگونه توصیف می‌کنند:

آنچه مسلم است این است که Windows Defender کاربرانی را که می‌خواهند آن را به طور دائمی در رایانه‌ای که روی آن کار می‌کنند غیرفعال کنند، آزار خواهد داد. Defender Control یک ابزار رایگان کوچک و قابل حمل است که به شما امکان می‌دهد Windows Defender را در ویندوز ۱۰ به طور کامل غیرفعال کنید.

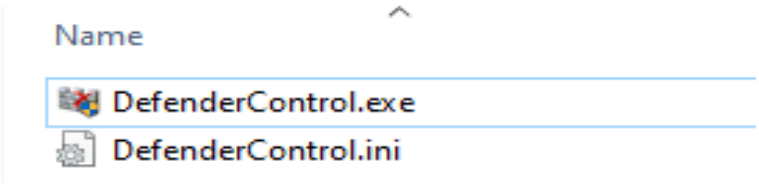
اگرچه ما این را در بسیاری از نفوذهای اخیر خود با باج‌افزارهای شکار بزرگ[1] ندیده‌ایم، اما در میان بازیگران کوچکتر مانند Dharma، Phobos و Crysis رایج است. بر اساس تجربه ما، نقطه ورود اصلی این گروه‌ها تمایل به RDP در معرض دید[2] دارد. پس از به دست آوردن دسترسی، این تهدیدگران اغلب زمان یا تلاشی را صرف نقشه‌برداری کامل یا به خطر انداختن یک دامنه قبل از باج‌گیری نمی‌کنند و معمولاً یک سیستم واحد را هدف قرار می‌دهند. ما دیده‌ایم که این تهدیدگران توسط Defender مسدود می‌شوند و دقایقی بعد، Defender Control کپی و اجرا می‌شود.

[1] big game ransomware
[2] exposed RDP

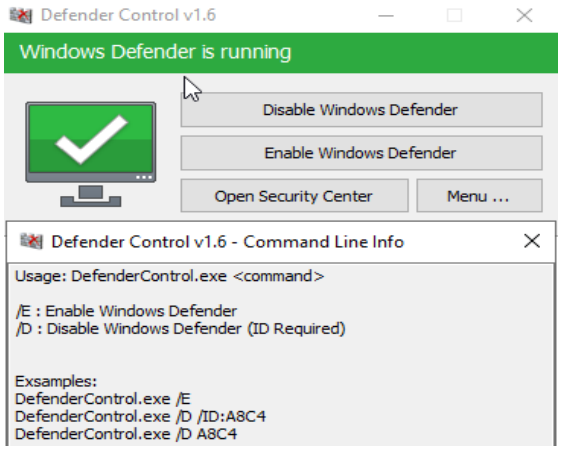
آشنایی بیشتر با Defender

Defender Control شامل دو فایل است:

یک فایل اجرایی قابل حمل[3] و یک فایل پیکربندی[4].

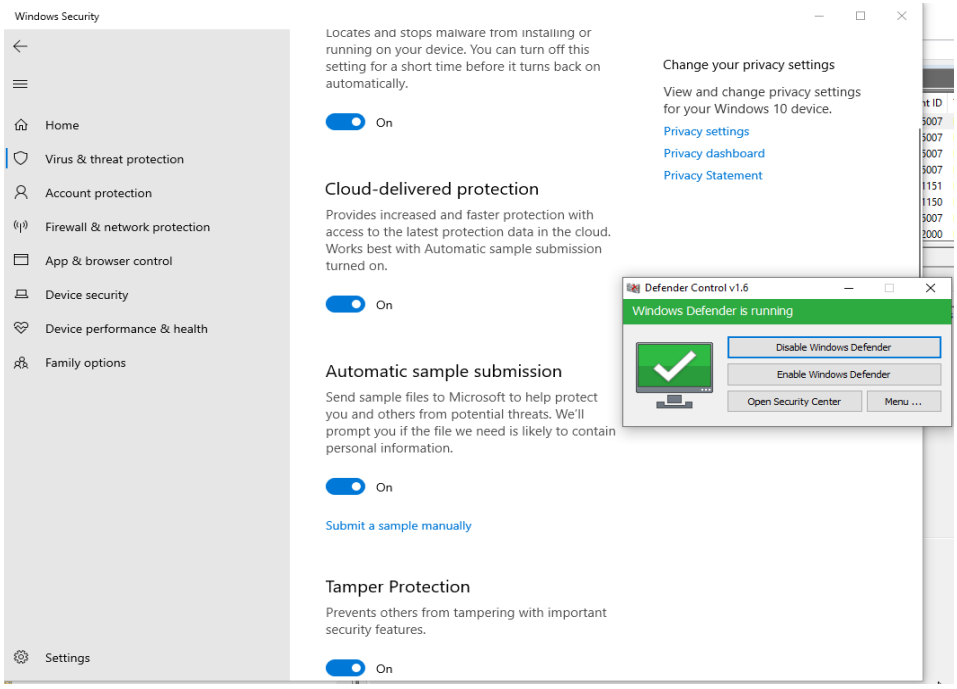


Defender Control را می‌توان از طریق رابط کاربری گرافیکی یا خط فرمان اجرا کرد.

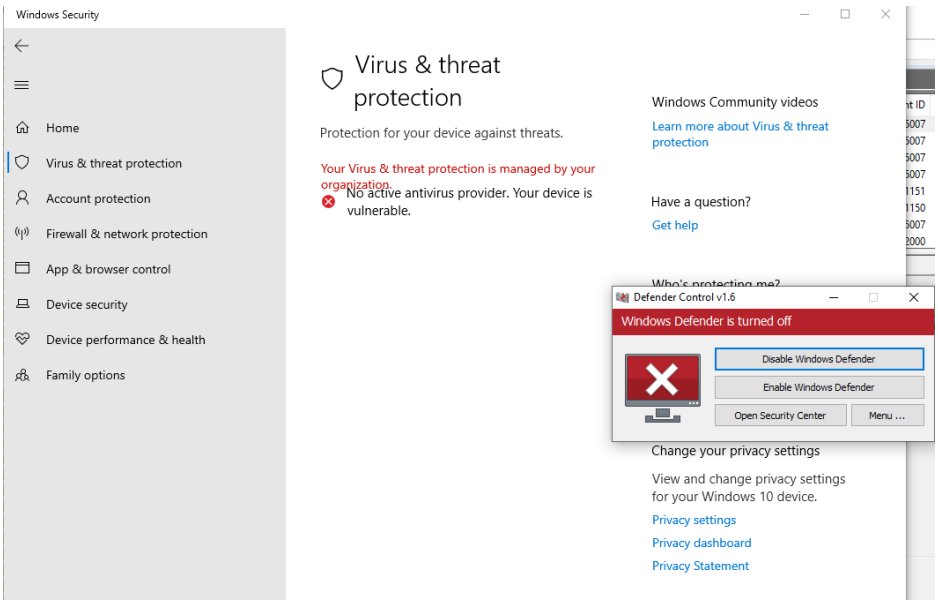


[3] portable executable
[4] configuration file

این یک سیستم ویندوز ۱۰ به‌روز است که تمام کنترل‌های Windows Defender در آن فعال هستند.



روی گزینه غیرفعال کردن Windows Defender کلیک می‌کنیم.



حالا می‌توانیم ببینیم که کل منو ناپدید شده است، و ویندوز به شما می‌گوید که سازمان در حال مدیریت دیفندر است.

فرار از شناسایی

Defender Control چندین مقدار رجیستری را برای غیرفعال کردن دیفندر تنظیم می‌کند، از جمله این یکی:

```
message
Registry value set:
RuleName: technique_id=T1089,technique_name=Disabling Security Tools
EventType: SetValue
UtcTime
ProcessGuid: {2a7dd436-8514-5fd1-e706-000000000e00}
ProcessId: 4628
Image: C:\Users\                    Downloads\DefenderControl.exe
TargetObject: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
Details: DWORD (0x00000001)
```

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware

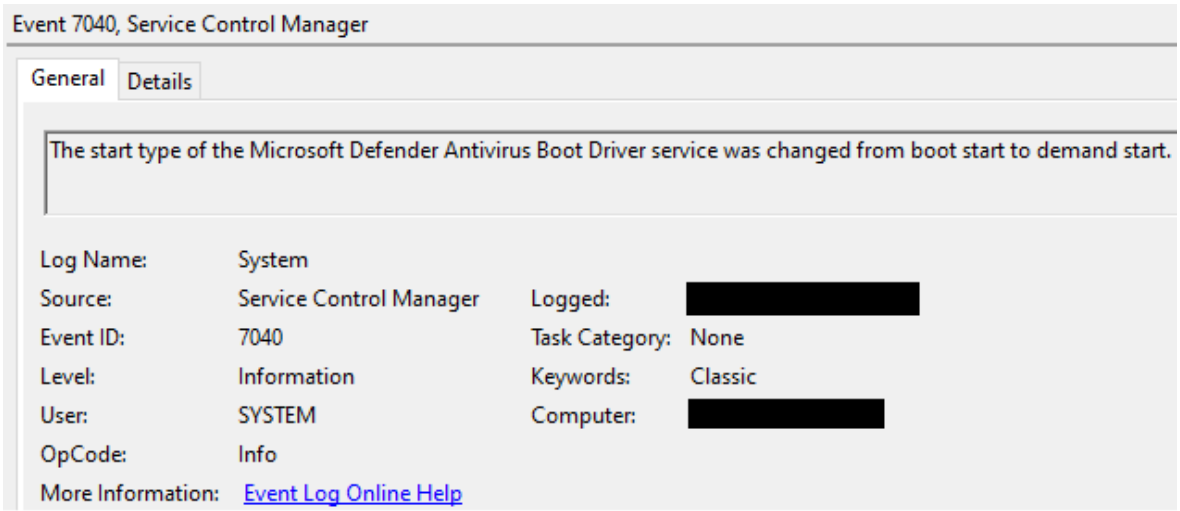
DWORD (0x00000001)

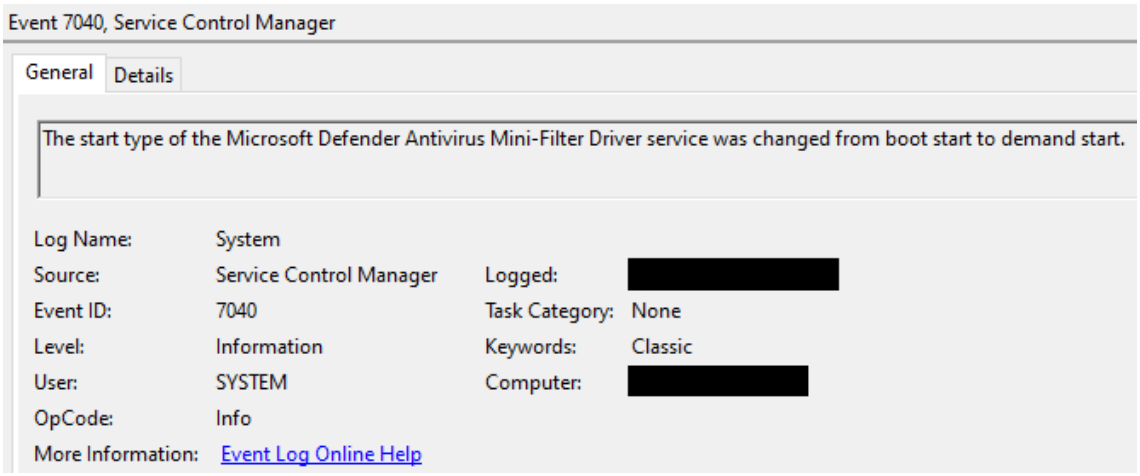
Defender Control همچنین این مقدار را برای غیرفعال کردن راه‌اندازی سرویس دیفندر تنظیم می‌کند:

HKLM\System\CurrentControlSet\Services\WinDefend\Start

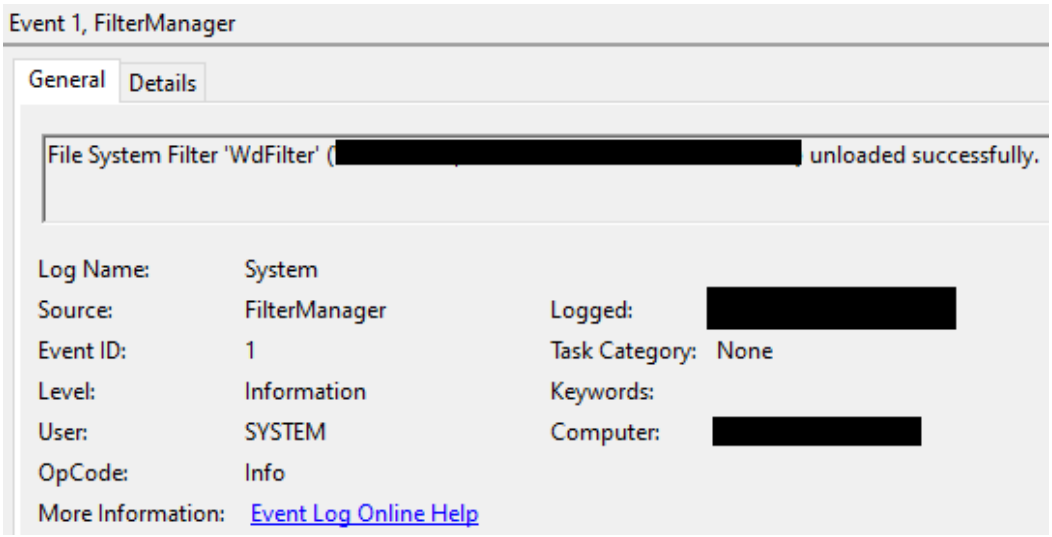
DWORD (0x00000003)

که لاگ زیر را ایجاد می‌کند:

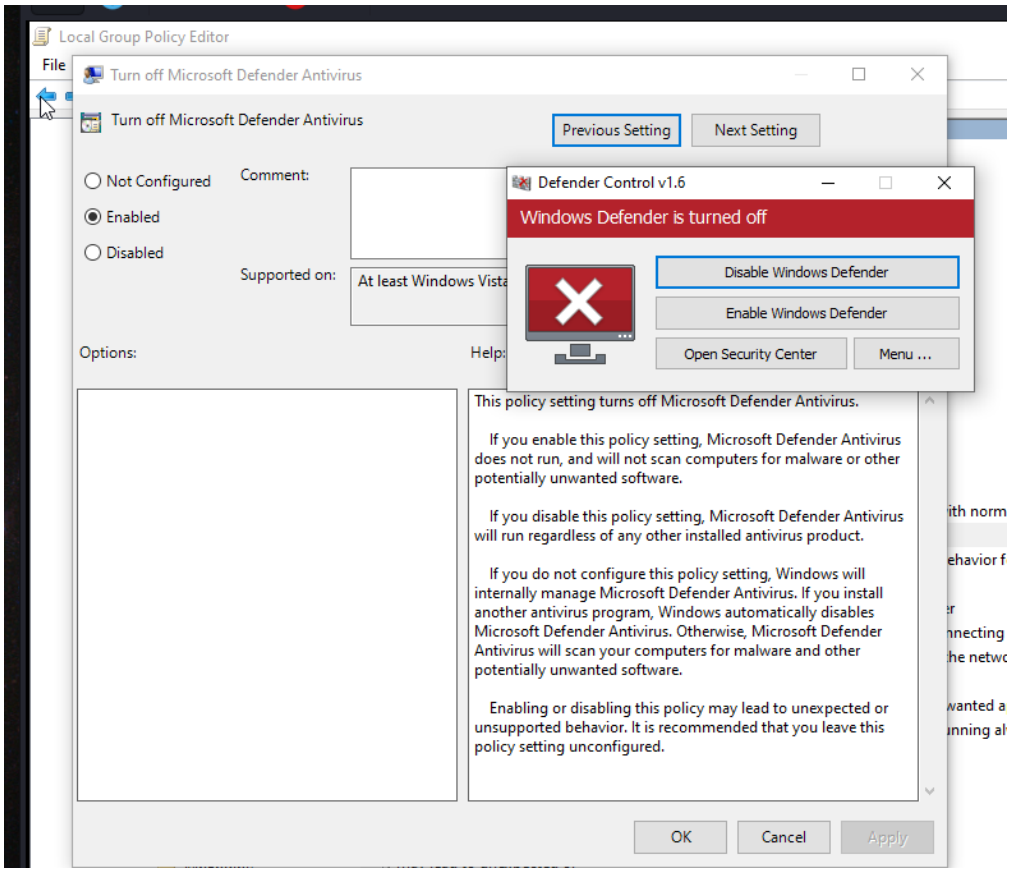




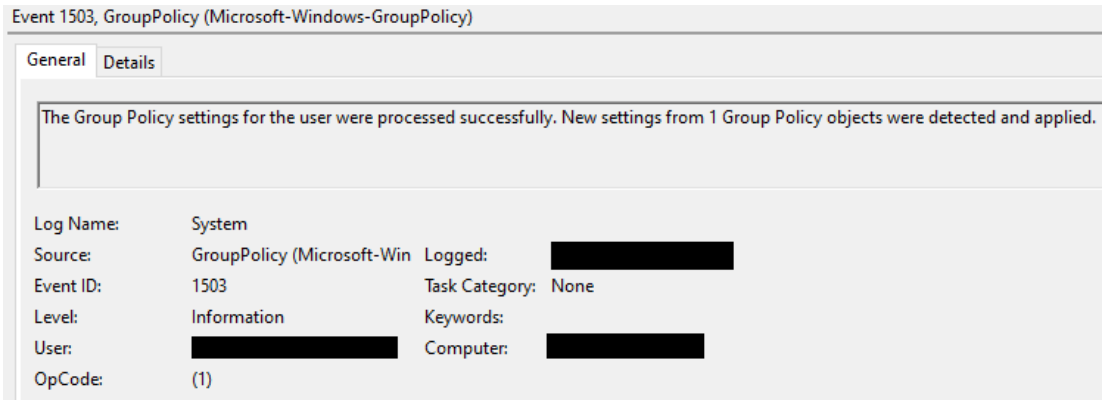
Defender Control همچنین درایور دیفندر را unload می‌کند:

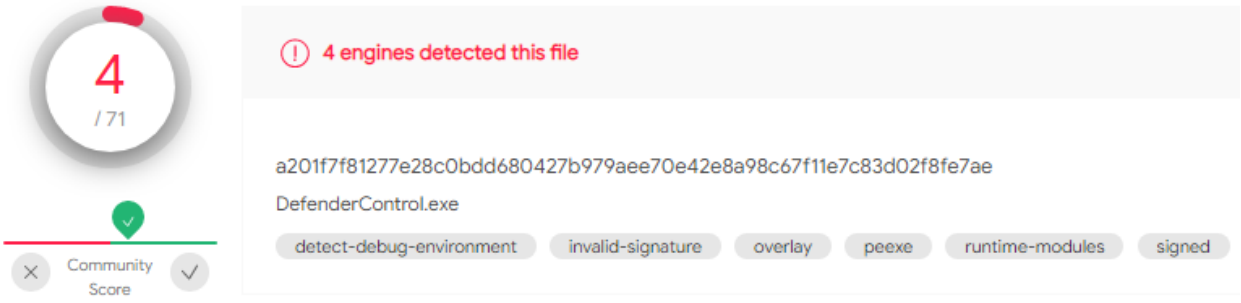


در اینجا، می‌توانیم ببینیم که Defender Control از طریق Local Group Policy Editor، دیفندر را خاموش می‌کند:



Group Policy Management Editor> Administrative templates > Windows components > Microsoft Defender Antivirus > Turn off Microsoft Defender Antivirus





IOCs

DefenderControl.exe

MD5 3a24a7b7c1ba74a5afa50f88ba81d550

SHA-1 5da4de1dbba55774891497297396fd2e5c306cf5

SHA-256 a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae

Vhash 085046655d157220b02002300a66z1410043ze2za0030e039z

Authentihash 93c6e1f59f79d000ebad4873c57e716394e359526e241445e0c75d4494b03be2

Imphash aaaa8913c89c8aa4a5d93f06853894da

Rich PE header hash 09983e500a3e996337593d644224f769

SSDEEP
12288:baWzgMg7v3qnCi3ErQohh0F4JCJ8lnydQ79QudhzYOejoiQv2ju8S0c/J:uaHMv6CDrjRnydQu+ejMZ1R

TLSH
T14005C012B3D680B6D99378B5297BE32BEB3575194327C4C7A7E02F729F111409B3A3A1

DefenderControl.ini

MD5 4416f7bea63b8af85f5590a3bdf6261b

SHA-1 549b43af5454b32848f500dcbea39acc49be0498

SHA-256 84caed9ee666f5004481e2b6e3233f37adf8106f6d821085caa4dcbd1221b876

SSDEEP
384:J9VBz+Kj3ehWYn/qmt4yJbo3nBaY+BvroUVB5j1vIdo7apRVWpIpClFG:J5BOhJ/nRCaYczoUM6apHd

TLSH T15233001A46EA621AF2F35B10E6F01F734B36BD95687C904C0ED55E8C18E0E609562FFB

YARA

*/

YARA Rule Set

Author: The DFIR Report

Date: 2020-12-05

Identifier: DefenderControl

Reference: https://thedfirreport.com/

/*

/Rule Set/ ----------

import "pe"

rule DefenderControl_Executable{

meta:

description = "DefenderControl - file DefenderControl.exe"

author = "The DFIR Report"

reference = "https://thedfirreport.com"/

date = "2020-12-05"

hash1 = "a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae"

strings:

$s1 = "/AutoIt3ExecuteScript" fullword wide

$s2 = "/AutoIt3ExecuteLine" fullword wide

$s3 = "SCRIPTNAME" fullword wide /* base64 encoded string 'H$H=3@0/* '

$s4 = "PROCESSGETSTATS" fullword wide

$s5 = "WINGETPROCESS" fullword wide

$s6 = "SHELLEXECUTE" fullword wide

```
$s7 = "SHELLEXECUTEWAIT" fullword wide
$s8 = "#NoAutoIt3Execute" fullword wide
$s9 = "PROCESSWAIT" fullword wide
$s10 = "PROCESSEXISTS" fullword wide
$s11 = "HTTPSETUSERAGENT" fullword wide
$s12 = "PROCESSSETPRIORITY" fullword wide
$s13 = "PROCESSORARCH" fullword wide
$s14 = "PROCESSCLOSE" fullword wide
$s15 = "PROCESSWAITCLOSE" fullword wide
$s16 = "PROCESSLIST" fullword wide
$s17 = "SENDCOMMANDID" fullword wide
$s18 = "FILEGETVERSION" fullword wide
$s19 = "LOGONDOMAIN" fullword wide
$s20 = "INETGETBYTESREAD" fullword wide
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
 )pe.imphash() == "aaaa8913c89c8aa4a5d93f06853894da" or all of them(
{
rule DefenderControl_Config_File}
meta:
description = "DefenderControl - file DefenderControl.ini"
author = "The DFIR Report"
reference = "https://thedfirreport.com"/
date = "2020-12-05"
        hash1 = "84caed9ee666f5004481e2b6e3233f37adf8106f6d821085caa4dcbd1221b876"
        strings:
```

```
$s1 = "15=\"&Commando Lijn Info\"" fullword wide
$s2 = "15=\"&Command Line Info\"" fullword wide
$s3 = "15=\"&Info de ligne de commande\"" fullword wide
$s4 = "06=\"La protezione in tempo reale " fullword wide
$s5 = "pt logu start" fullword wide
$s6 = "o em Tempo Real est" fullword wide
$s7 = "06=\"La protection en temps r" fullword wide
$s8 = "15=\"&Info Linea di Comando\"" fullword wide
$s9 = "15=\"&Informatii Comenzi de Linie\"" fullword wide
$s10 = "11=\"&Defender postavke\"" fullword wide
$s11 = "15=\"&Eingabeaufforderungsinformation\"" fullword wide
$s12 = "01=\"miestas.org\"" fullword wide
$s13 = "02=\"Windows Defender is running\"" fullword wide
$s14 = "05=\"Windows Defender Service nicht gefunden\"" fullword wide
$s15 = "05=\"Windows Defender service niet gevonden\"" fullword wide
$s16 = "05=\"Service Windows Defender introuvable\"" fullword wide
$s17 = "nea de comandos\"" fullword wide
$s18 = "15=\"&Inf. da linha de comando\"" fullword wide
$s19 = "; www.sordum.org" fullword wide
$s20 = "11=\"&Configura" fullword wide
condition:
uint16(0) == 0xfeff and filesize < 100KB and
 ٨of them
{
```

منبع:

https://thedfirreport.com/2020/12/13/defender-control/