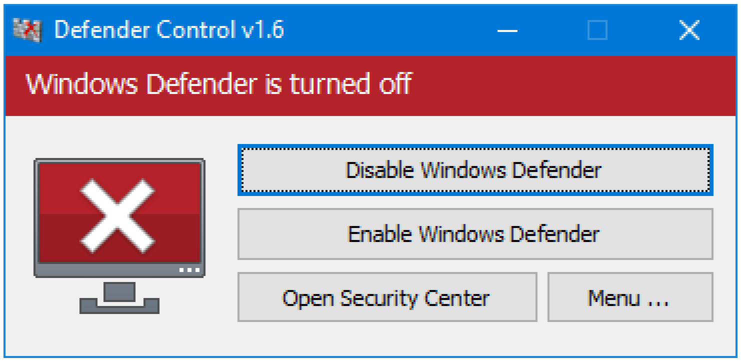
Defender Control

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

December 13, 2020



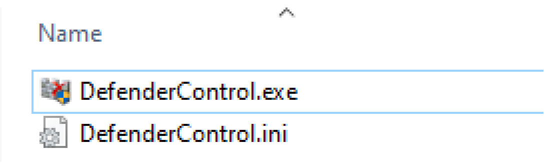
Windows Defender is turned off

Defender Control is a free software utility we've come across in various intrusions. The creators describe it by saying the following:

> What is certain however is that it [Windows Defender] will annoy users who want to disable it permanently on the computer they are working on. Defender Control is a small Portable freeware which will allow you to disable Windows Defender in Windows 10 completely.

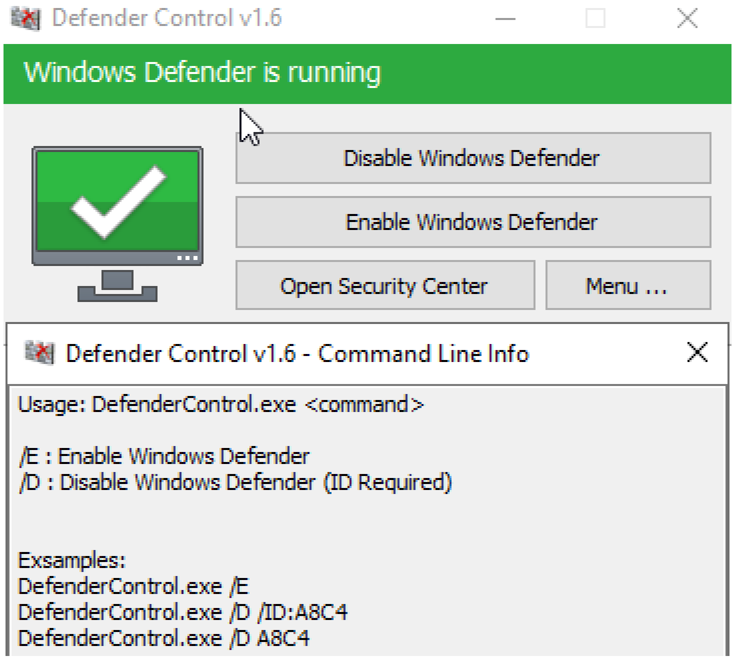
While we have not seen this in many of our recent intrusions with big game ransomware, it is common among the smaller players. Those like Dharma, Phobos, and Crysis. In our experience, these groups' main point of entry tends to be exposed RDP. After gaining access, these threat actors often do not take the time or effort to fully scope, or compromise a domain before ransoming, usually a single system. We've seen these threat actors get blocked by Defender and then minutes later Defender Control gets copied over and run.

Defender Control is two files, which are a portable executable and a configuration file.



Name
DefenderControl.exe
DefenderControl.ini

Defender Control can be run via GUI or command line

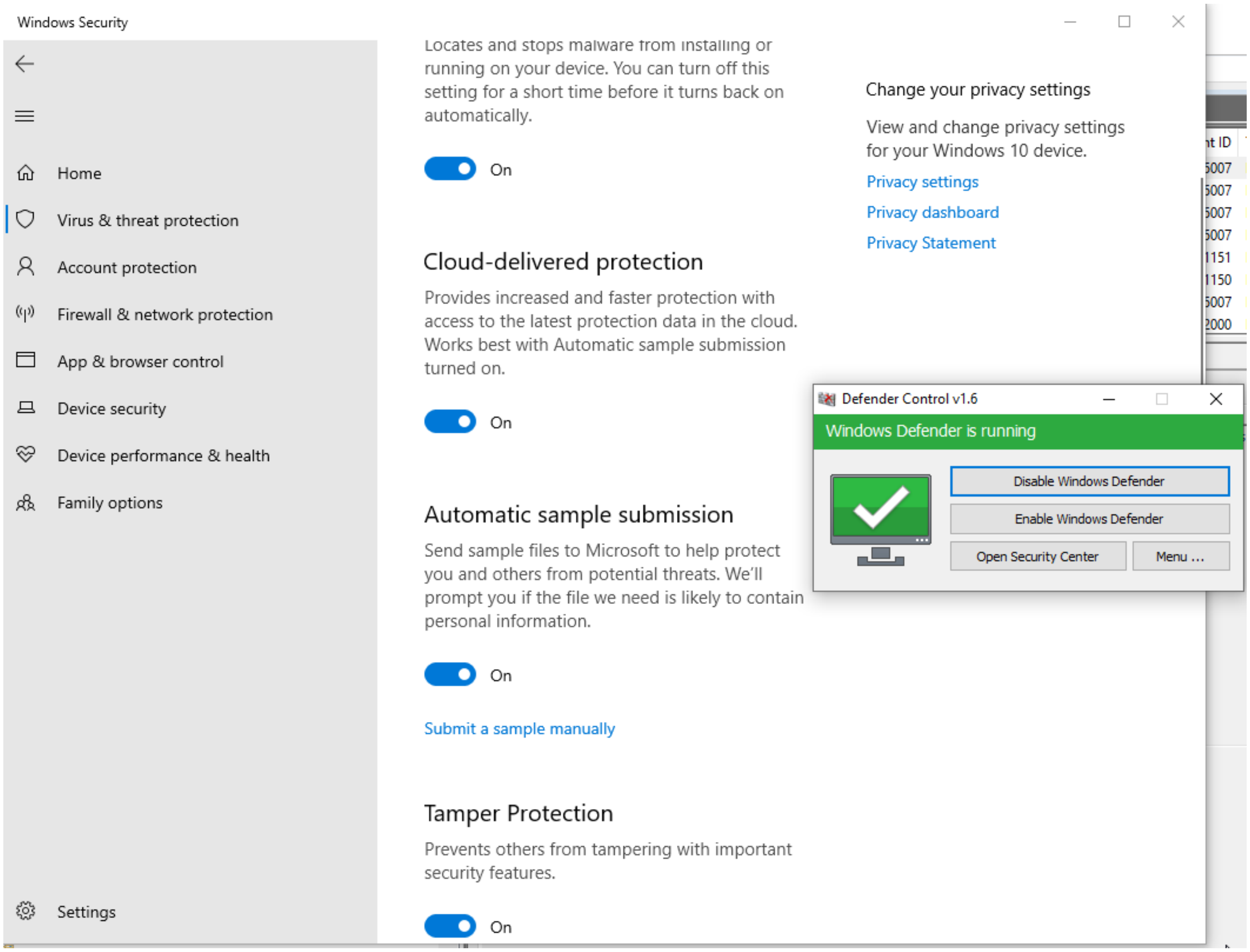


```
Usage: DefenderControl.exe <command>

/E : Enable Windows Defender
/D : Disable Windows Defender (ID Required)


Exsamples:
DefenderControl.exe /E
DefenderControl.exe /D /ID:A8C4
DefenderControl.exe /D A8C4
```

This is an up to date Windows 10 system, with all Windows Defender controls active.



Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

Submit a sample manually

Tamper Protection

Prevents others from tampering with important security features.

On

Change your privacy settings

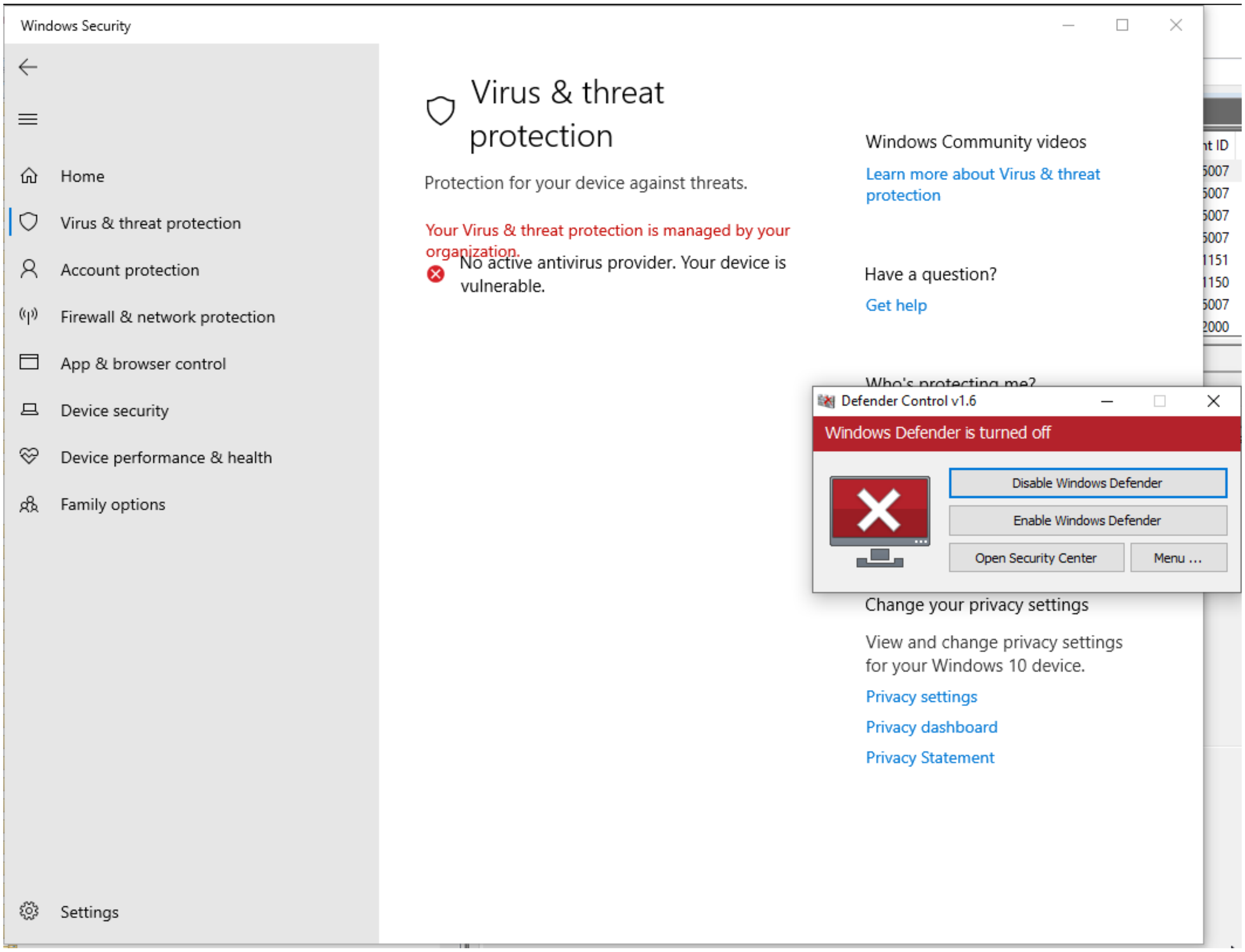
View and change privacy settings for your Windows 10 device.

Privacy settings

Privacy dashboard

Privacy Statement

Let's click Disable Windows Defender.



Virus & threat protection

Protection for your device against threats.

Your Virus & threat protection is managed by your organization.

No active antivirus provider. Your device is vulnerable.

View and change privacy settings for your Windows 10 device.

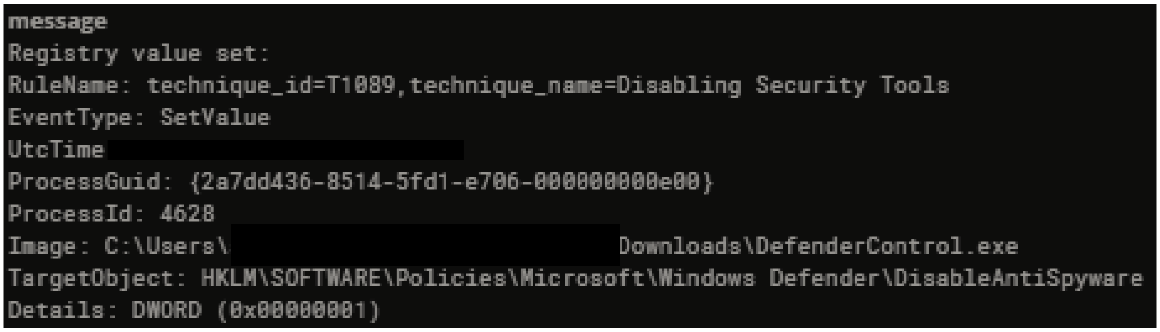
Windows Defender is turned off

We can now see that the entire menu has vanished, and Windows tells you that the Organization is managing Defender.

MITRE ATT&CK

Defense Evasion – T1562.001

Defender Control sets a couple registry values to disable Defender including this one:



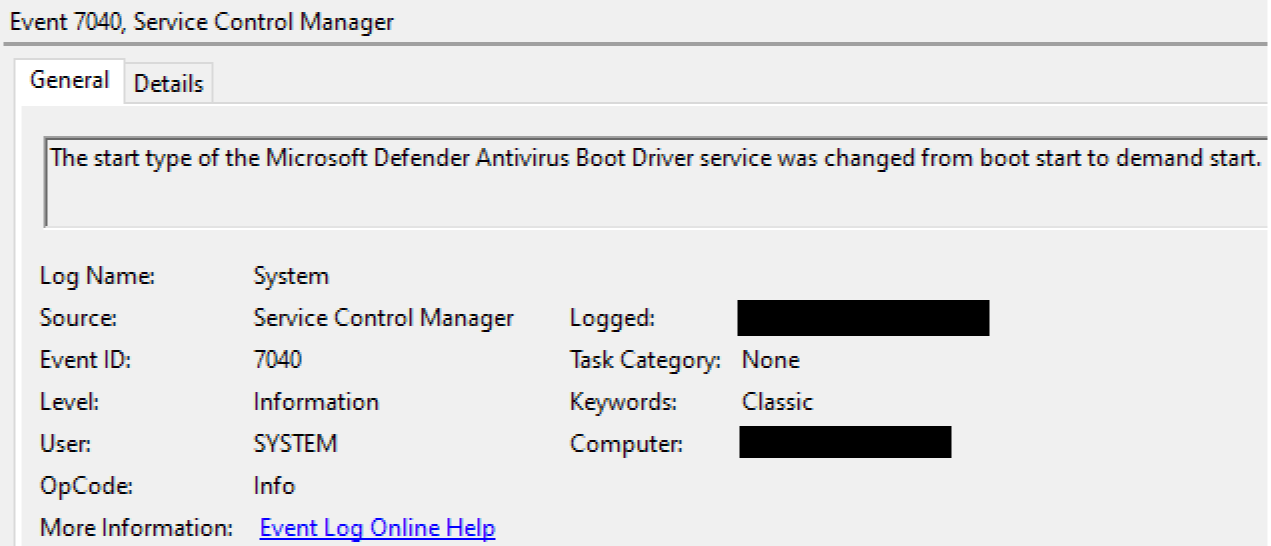
```
message
Registry value set:
RuleName: technique_id=T1089,technique_name=Disabling Security Tools
EventType: SetValue
UtcTime [redacted]
ProcessGuid: {2a7dd436-8514-5fd1-e706-000000000e00}
ProcessId: 4628
Image: C:\Users\[redacted]Downloads\DefenderControl.exe
TargetObject: HKLM\SOFTWARE\Policies\Microsoft\Windows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

`HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware DWORD (0x00000001)`

Defender Control also sets this value to disable the startup of the Defender service:

```
HKLM\System\CurrentControlSet\Services\WinDefend\Start DWORD (0x00000003)
```

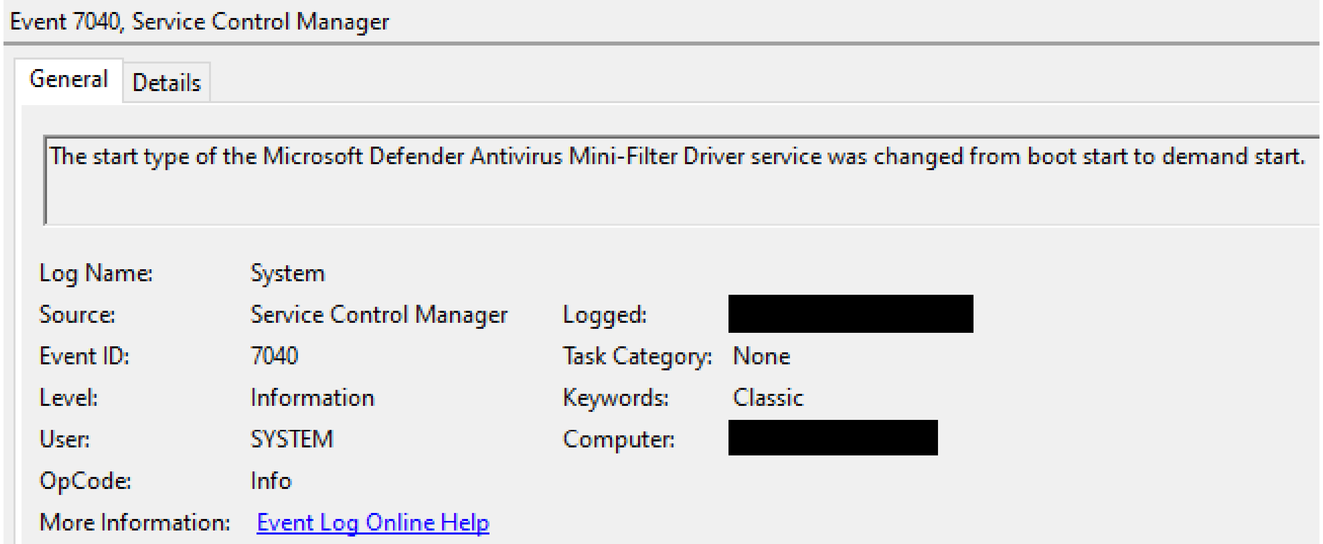
Which creates:



Event 7040, Service Control Manager

The start type of the Microsoft Defender Antivirus Boot Driver service was changed from boot start to demand start.

Log Name:	System		
Source:	Service Control Manager	Logged:	[redacted]
Event ID:	7040	Task Category:	None
Level:	Information	Keywords:	Classic
User:	SYSTEM	Computer:	[redacted]
OpCode:	Info		
More Information:	Event Log Online Help		

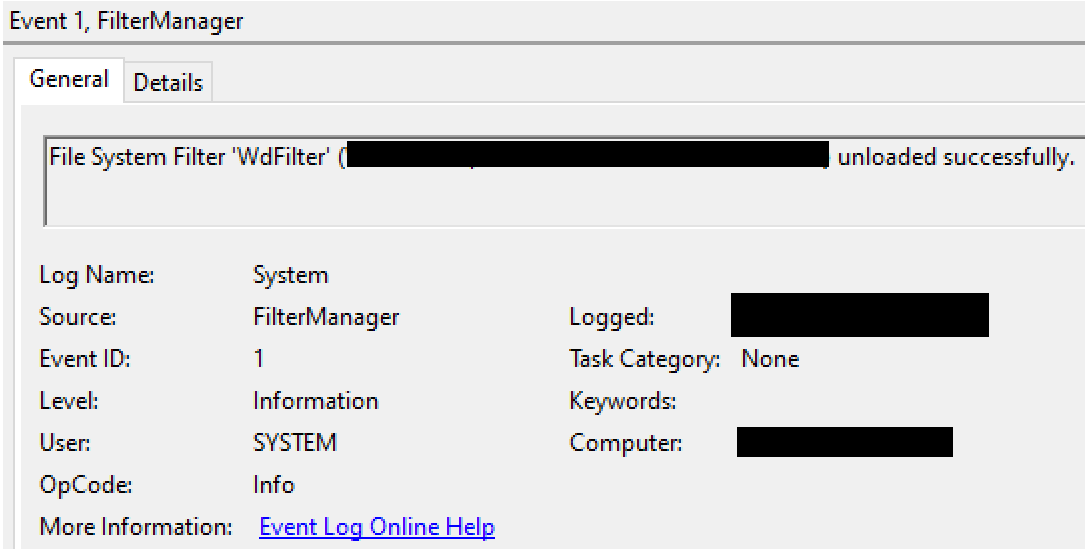


Event 7040, Service Control Manager

The start type of the Microsoft Defender Antivirus Mini-Filter Driver service was changed from boot start to demand start.

Log Name:	System		
Source:	Service Control Manager	Logged:	[redacted]
Event ID:	7040	Task Category:	None
Level:	Information	Keywords:	Classic
User:	SYSTEM	Computer:	[redacted]
OpCode:	Info		
More Information:	Event Log Online Help		

Defender Control also unloads the Defender driver:

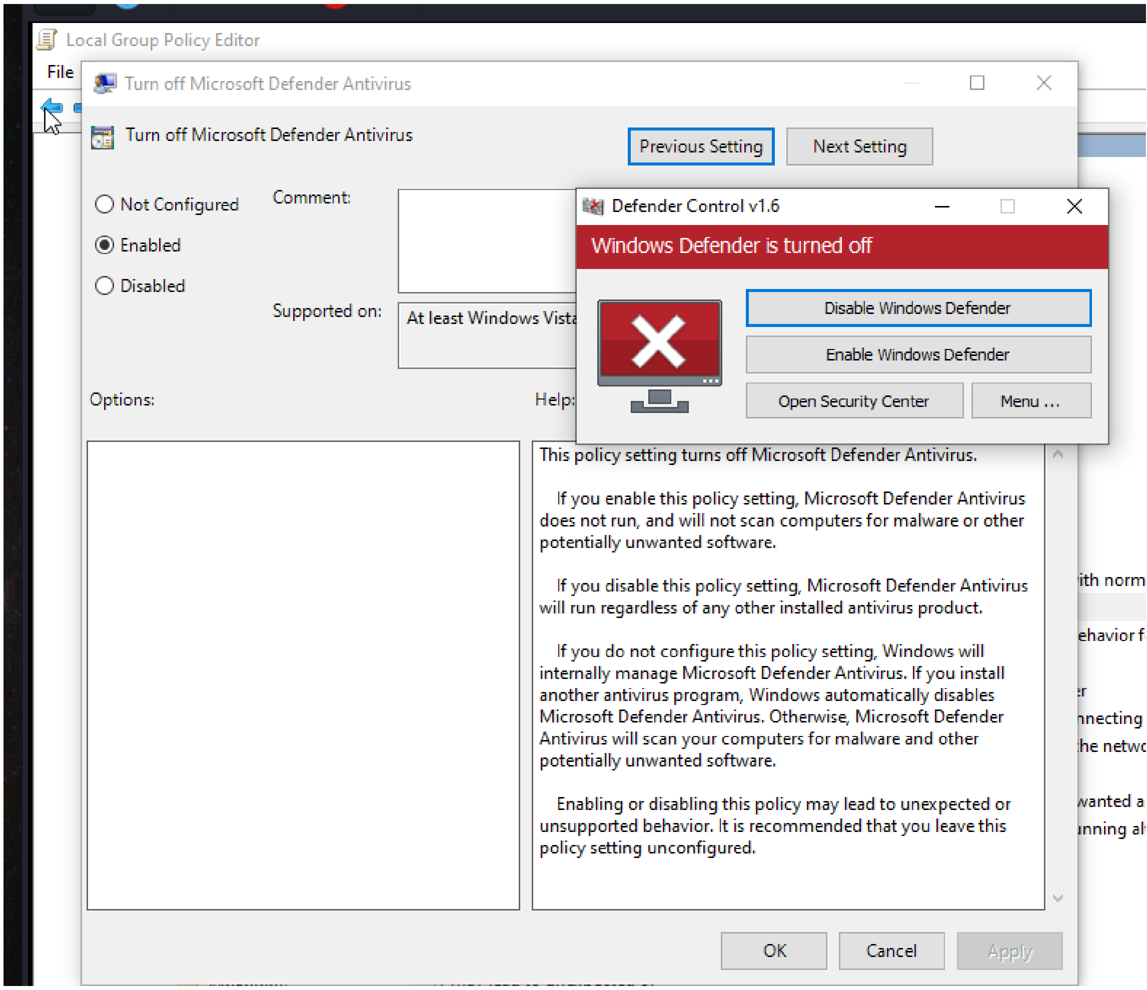


Event 1, FilterManager

```
File System Filter 'WdFilter' ([redacted] unloaded successfully.

Log Name:          System
Source:            FilterManager        Logged:         [redacted]
Event ID:          1                    Task Category:  None
Level:             Information          Keywords:
User:              SYSTEM               Computer:       [redacted]
OpCode:            Info
More Information:  Event Log Online Help
```

Here, we can see Defender Control turning off Defender via Local Group Policy Editor:



Local Group Policy Editor

Turn off Microsoft Defender Antivirus

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

Defender Control v1.6

Windows Defender is turned off

This policy setting turns off Microsoft Defender Antivirus.

If you enable this policy setting, Microsoft Defender Antivirus does not run, and will not scan computers for malware or other potentially unwanted software.

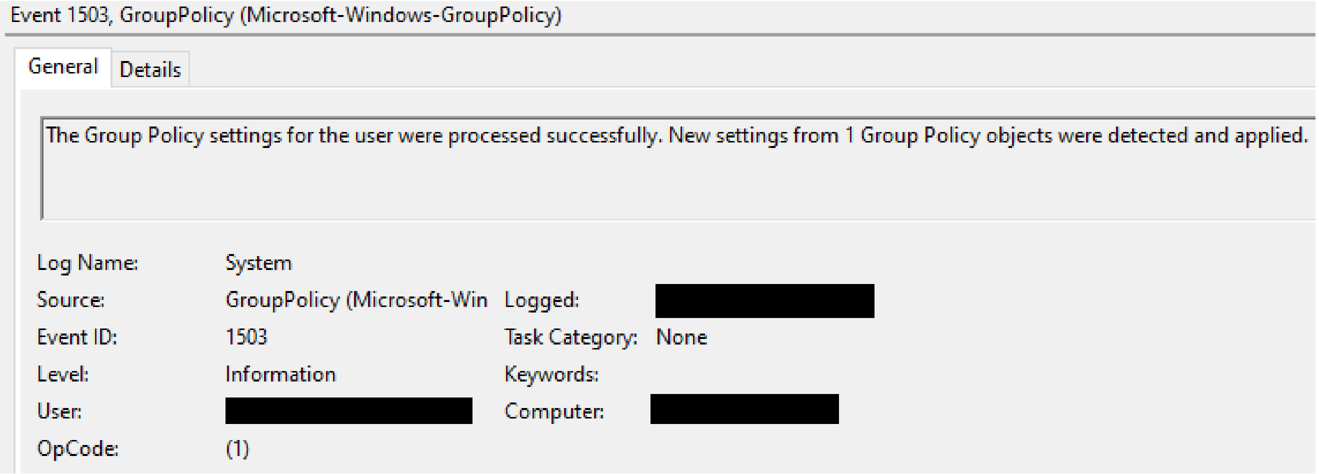
If you disable this policy setting, Microsoft Defender Antivirus will run regardless of any other installed antivirus product.

If you do not configure this policy setting, Windows will internally manage Microsoft Defender Antivirus. If you install another antivirus program, Windows automatically disables Microsoft Defender Antivirus. Otherwise, Microsoft Defender Antivirus will scan your computers for malware and other potentially unwanted software.

Enabling or disabling this policy may lead to unexpected or unsupported behavior. It is recommended that you leave this policy setting unconfigured.

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

Which creates:

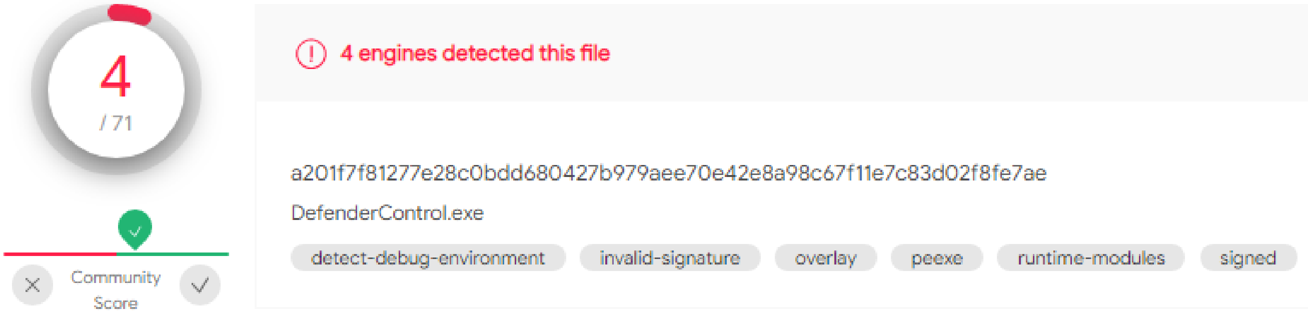


Event 1503, GroupPolicy (Microsoft-Windows-GroupPolicy)

The Group Policy settings for the user were processed successfully. New settings from 1 Group Policy objects were detected and applied.

```
Log Name:    System
Source:      GroupPolicy (Microsoft-Win   Logged:         [redacted]
Event ID:    1503                         Task Category:  None
Level:       Information                  Keywords:
User:        [redacted]                   Computer:       [redacted]
OpCode:      (1)
```

Version 1.6 Date: 12.10.2020



4 engines detected this file

a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae

DefenderControl.exe

detect-debug-environment invalid-signature overlay peexe runtime-modules signed

Enjoy our report? Please consider donating $1 or more to the project using Patreon. Thank you for your support!

IOCs

File Hashes

```
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+ejMZ1

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 '[email protected]' */
$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
8 of them
}
```

Internal case 1011