



Wazuh Integration With Windows Defender

SAMEER HASSAN

Wazuh lab

GitHub-link: [GitHub - sameerhassancode/Wazuh-labs](https://github.com/sameerhassancode/Wazuh-labs)

Linkedin: <https://www.linkedin.com/in/sameer-hassan-15a428255/>

Integrating Windows Defender Logs with Wazuh

Windows Defender, Microsoft's built-in antivirus software, dominates the free antivirus market for PC users, holding nearly 40% of the market share according to the 2023 Antivirus Market Report. You can explore the full report here: <https://www.security.org/antivirus/antivirus-consumer-report-annual>.

For enterprise environments, Microsoft also offers **Windows Defender for Endpoint**, which expands the scope of its security capabilities. Integrating this tool with **Wazuh** significantly enhances endpoint security visibility. However, Wazuh doesn't natively support Windows Defender logs, so additional configuration is necessary to bridge that gap.

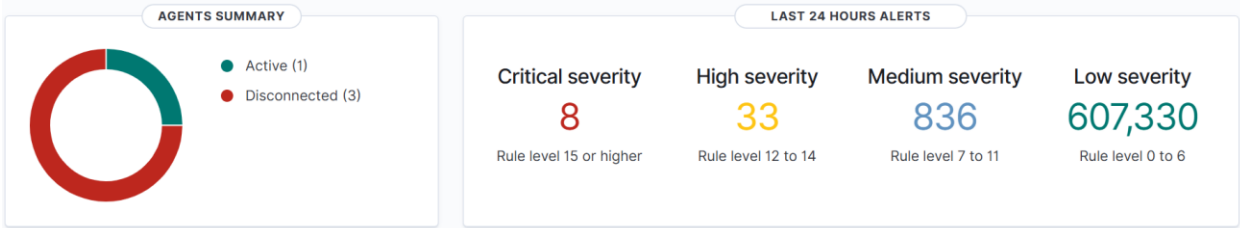
Understanding the Value of Windows Defender Logs

Before setting up the integration, it's important to understand what these logs contain. They provide critical insights into security-related activities—such as malware detections, scanning processes, and threat mitigation events.

These logs are essential for **Security Operations Center (SOC) analysts**, as they help assess endpoint health, detect malicious behavior, and support in-depth incident investigations. The logs typically include:

- Scan results and schedules
- Threat detection alerts
- Update histories
- Quarantine actions and remediation
- Firewall and network activities
- Real-time protection status

Wazuh-Dashboard:



Agent:

Agents (1) Show only outdated Deploy new agent Refresh Export formatted More

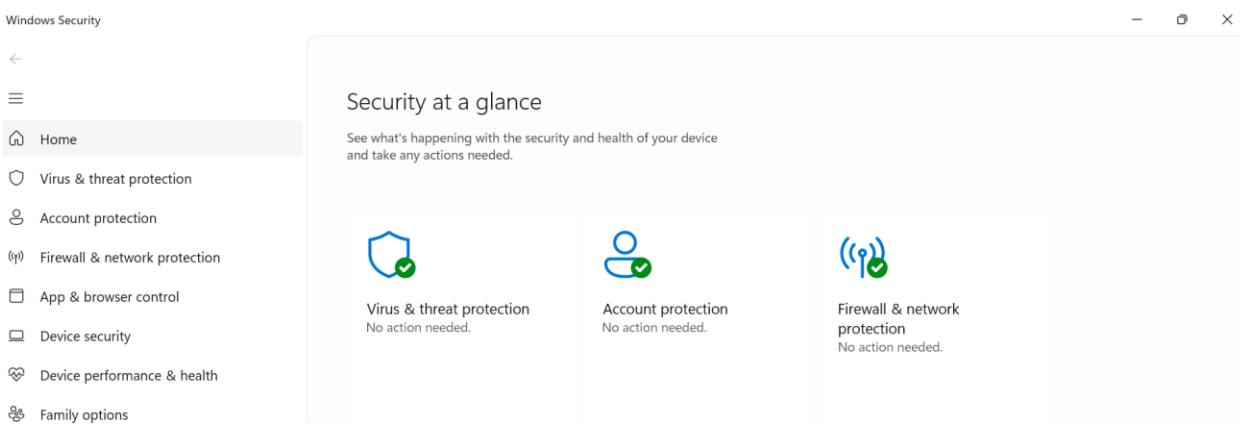
status=active

WQL

<input type="checkbox"/>	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
<input type="checkbox"/>	001	Win-001	192.168.0.107	default	Microsoft Windows 11 Pro 10.0.26100.4351	node01	v4.12.0	active ⓘ	👁️ ⋮

Rows per page: 10 < 1 >

Windows defender:



Connect with the Wazuh through SSH:

[illegible]

Get the root access and go to default directory:

```
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# cd /var/ossec/etc/
[root@wazuh-server etc]# ls
client.keys      internal_options.conf  local_internal_options.conf  ossec.conf      ossec.conf.save.1  rules      sslmanager.cert  ssmpt
decoders         lists                  localtime                 ossec.conf.save  rootcheck          shared       sslmanager.key
[root@wazuh-server etc]# cd shared
[root@wazuh-server shared]# cd default/
[root@wazuh-server default]# ls
agent.conf      cis_rhel6_linux_rcl.txt      cis_win2012r2_domainL2_rcl.txt  system_audit_rcl.txt
cis_apache2224_rcl.txt      cis_rhel7_linux_rcl.txt      cis_win2012r2_memberL1_rcl.txt  system_audit_ssh.txt
cis_debian_linux_rcl.txt    cis_rhel_linux_rcl.txt      cis_win2012r2_memberL2_rcl.txt  win_applications_rcl.txt
cis_mysql5-6_community_rcl.txt  cis_sles11_linux_rcl.txt    merged.mg                       win_audit_rcl.txt
cis_mysql5-6_enterprise_rcl.txt  cis_sles12_linux_rcl.txt    rootkit_files.txt               win_malware_rcl.txt
cis_rhel5_linux_rcl.txt      cis_win2012r2_domainL1_rcl.txt  rootkit_trojans.txt
[root@wazuh-server default]#
```

Open the Agent.conf file:



The screenshot shows a terminal window with the title "root@wazuh-server:/var/osse". The nano text editor is open, editing a file named "agent.conf". The editor's status bar at the top indicates "GNU nano 8.3" and the file name "agent.conf". The visible content of the file is a comment: `<!-- Shared agent configuration here -->`. The cursor is positioned at the end of this line. The terminal window has standard Linux window controls (minimize, maximize, close) in the top right corner.

Add these tags:

<localfile>

<location> </location>

<log_format></log_format>

</localfile>



```
root@wazuh-server:/var/osse x + v
GNU nano 8.3 agent.conf Modified
<agent_config>

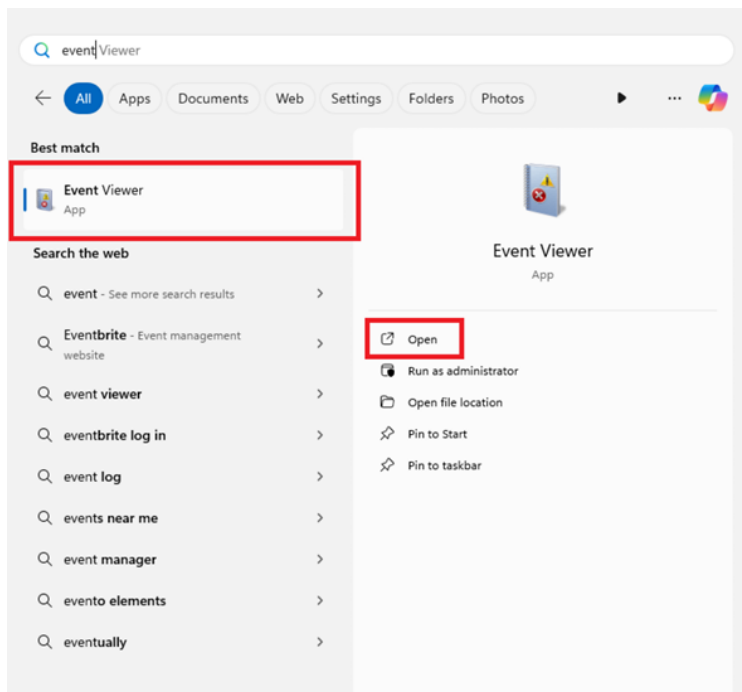
  <!-- Shared agent configuration here -->

  <!-- Sameer Hassan -->

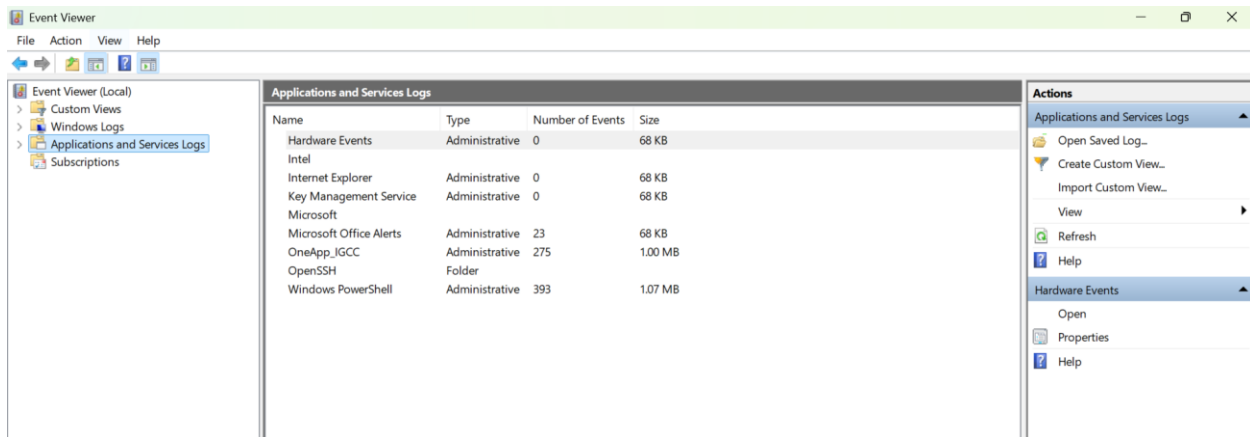
  <localfile>
  <location> </location>
  <log_format></log_format>
  </localfile>

</agent_config>
```

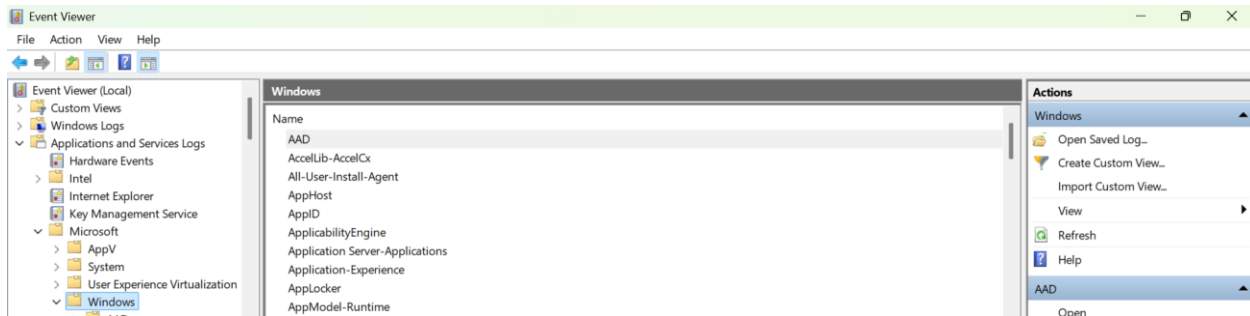
Now open event viewer:



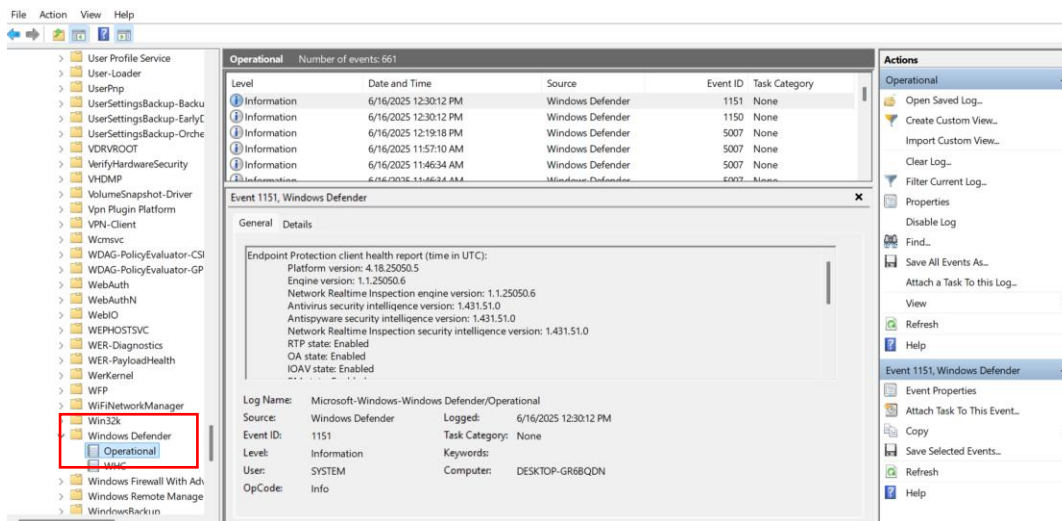
Click on Application and services logs:



After Application and services logs click on Microsoft then Windows:

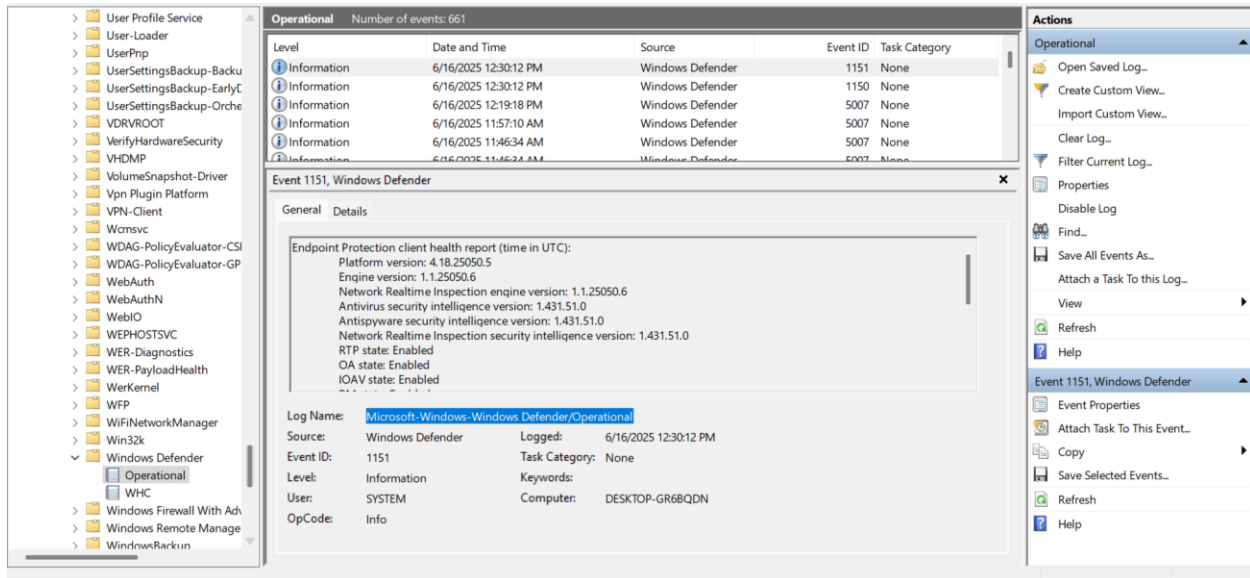


After clicking Windows search and open Windows Defender:



Now copy the log name:

Microsoft-Windows-Windows Defender/Operational



After copying Paste it in the agents.conf file in location tag

```
<localfile>
<location>Microsoft-Windows-Windows Defender/Operational</location>
<log_format></log_format>
</localfile>
```

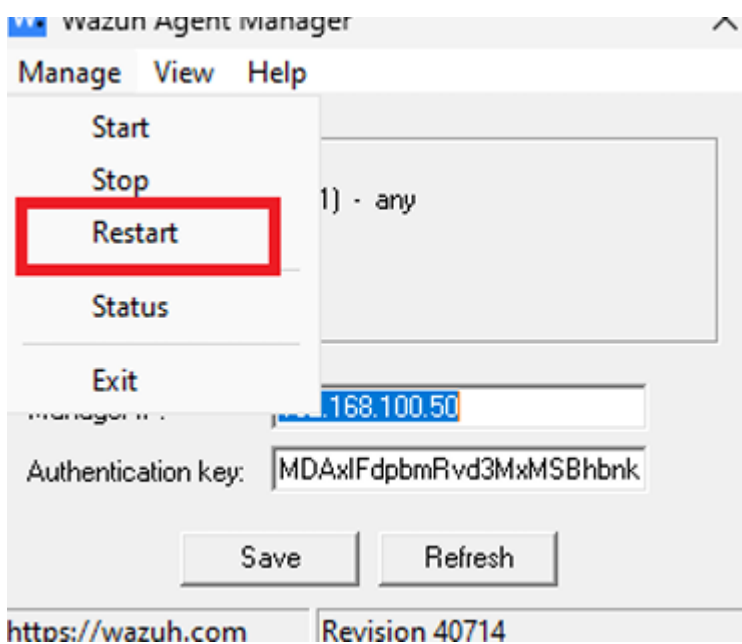
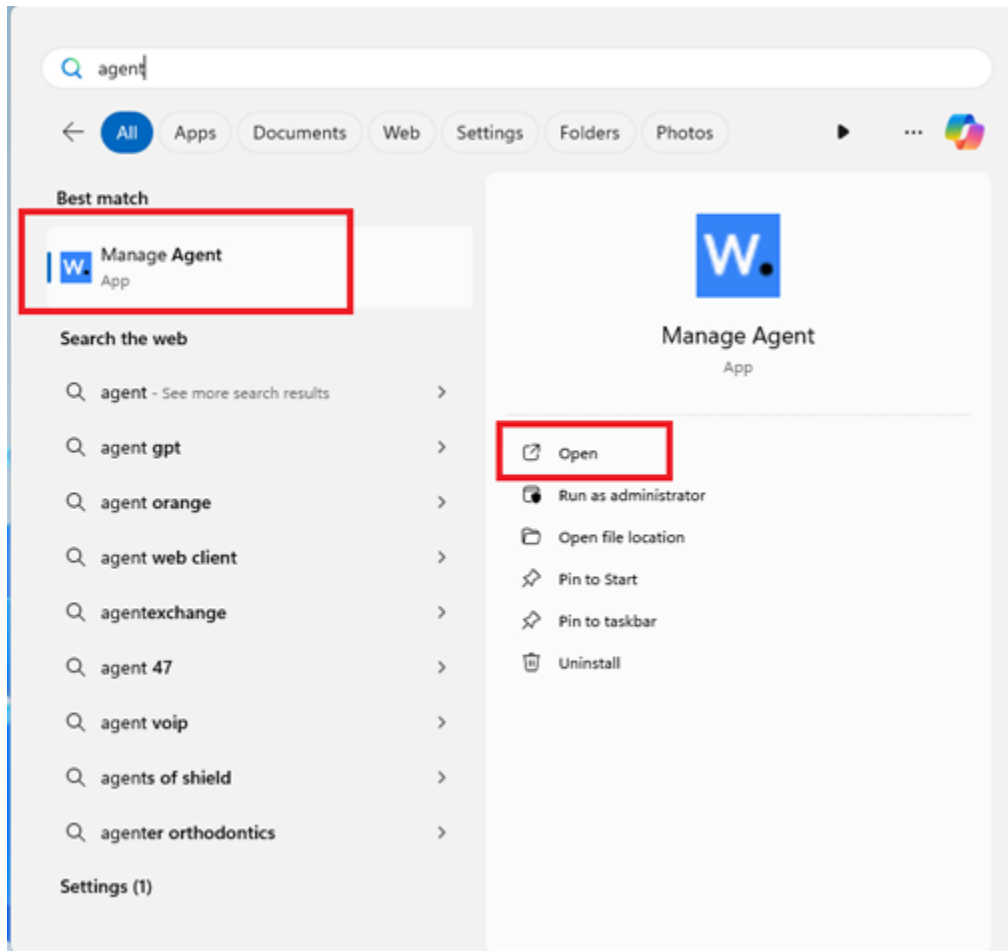
And for log_format tag write eventchannel:

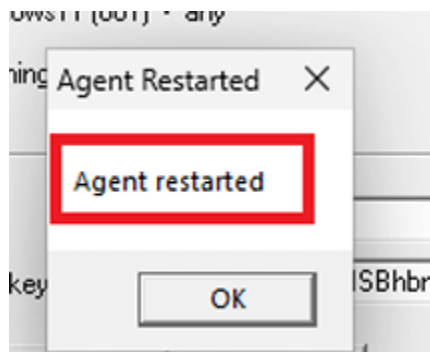
```
<localfile>
<location>Microsoft-Windows-Windows Defender/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
```

Save the file and restart Wazuh manager:

```
[root@wazuh-server default]# systemctl restart wazuh-manager.service |
```

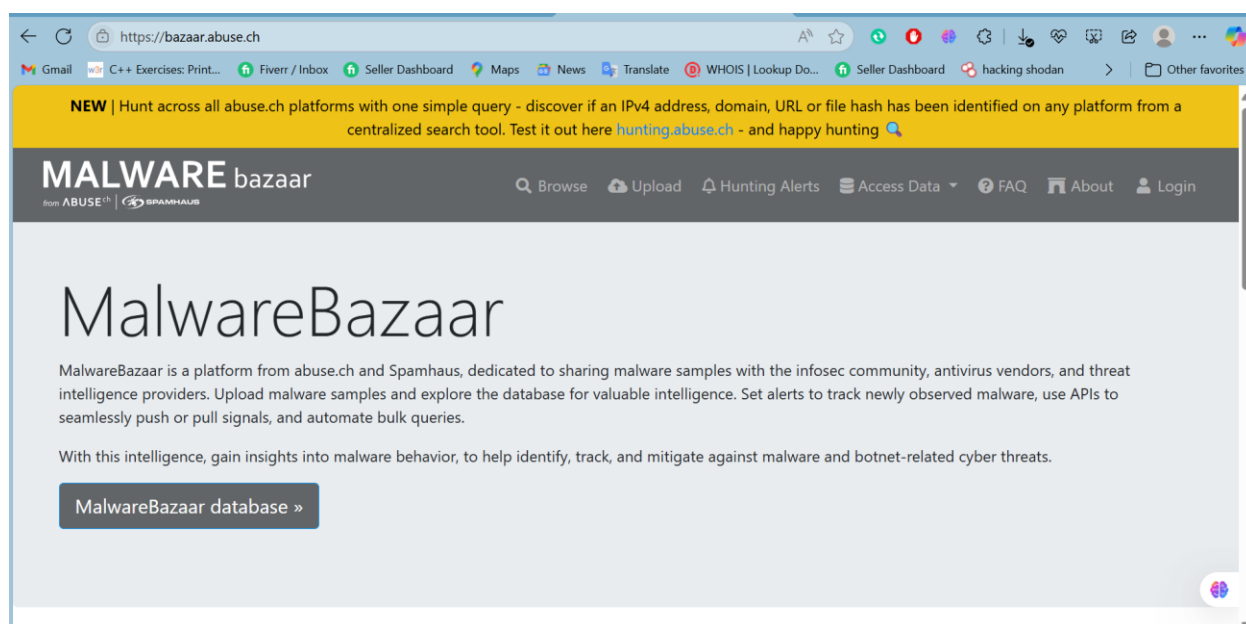
Now open Wazuh-agent:





Now Open Malware Bazar:

[MalwareBazaar](https://bazaar.abuse.ch) | [Malware sample exchange](#)



Scroll down and click on access the database



Select any Malware and download it:

Note: Run this it's safe and senitized

Link: [MalwareBazaar | SHA256](#)

[a9ca76d8913c120d2edcb433cdaced1f13921ad438cb2f56f0b882ae460b36d4](https://bazaar.abuse.ch/download/a9ca76d8913c120d2edcb433cdaced1f13921ad438cb2f56f0b882ae460b36d4/)

SHA1 hash:	755e66a2476deeb070f23099960310203376caa6
MD5 hash:	42291d28ef54572653de7d7caabdd855
humanhash:	magazine-undress-sierra-snake
File name:	ywwdglr (2).exe
Download:	download sample
File size:	76'135'102 bytes
First seen:	2025-06-16 19:50:10 UTC
Last seen:	Never
File type:	exe
MIME type:	application/x-dosexec
imphash	5a594319a0d69dbc452e748bcf05892e (21 x ParallaxRAT, 15 x NetSupport, 14 x PureLogStealer)
ssdeep	1572864:qXJ5kAg1DMniPJARMozCQaEVsILdaEmstwRFUpHiu9e/d7CnsR:qXJKAc87XaELip45Ia6

<https://bazaar.abuse.ch/download/a9ca76d8913c120d2edcb433cdaced1f13921ad438cb2f56f0b882ae460b36d4/>

Zip password is: infected

MalwareBazaar Database

This page let you download the following malware sample: **SHA256 a9ca76d8913c120d2edcb433cdaced1f13921ad438cb2f56f0b882ae460b36d4**

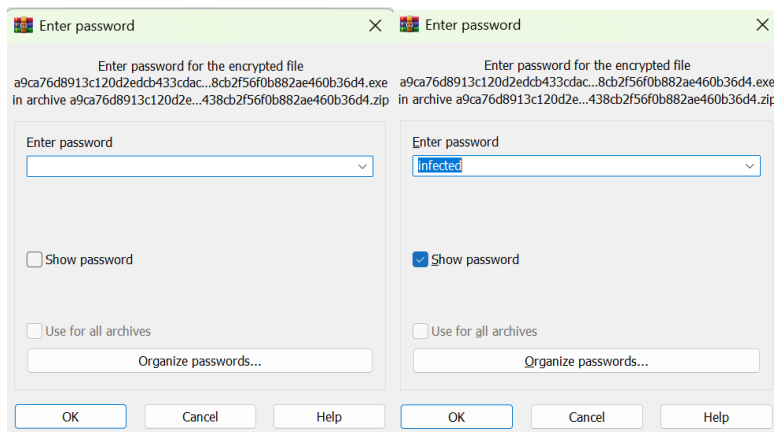
Caution!

You are about to download a malware sample. By clicking on "download", you declare that you have understood what you are doing and that MalwareBazaar can not be held accountable for any damage caused by downloading this malware sample!

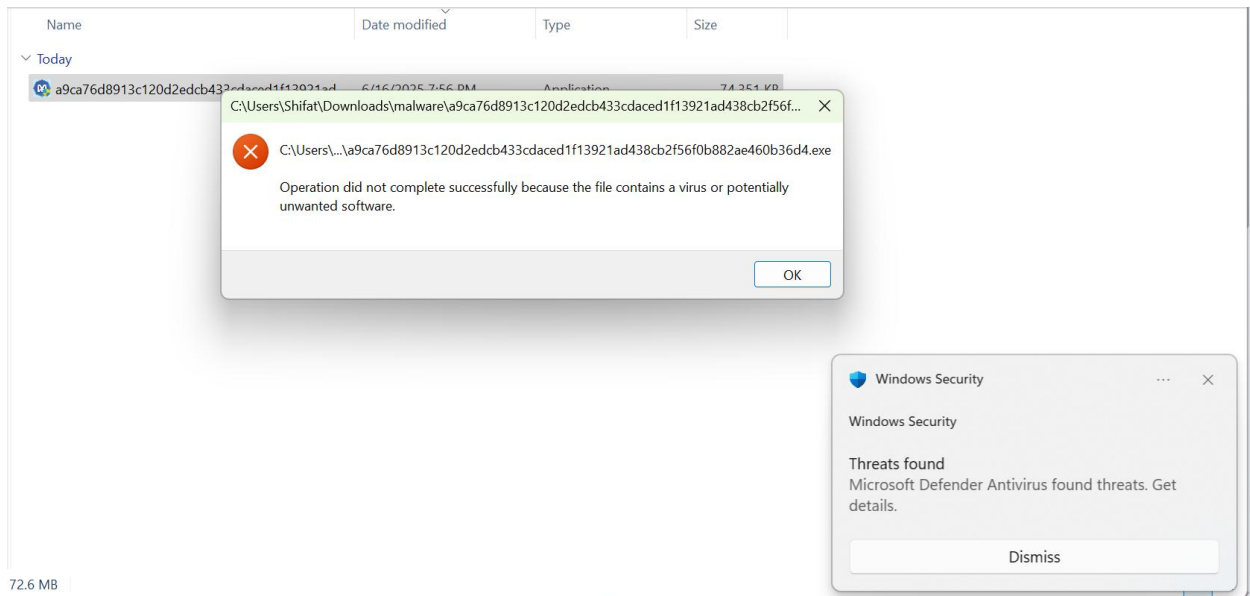
ZIP password: infected

Download

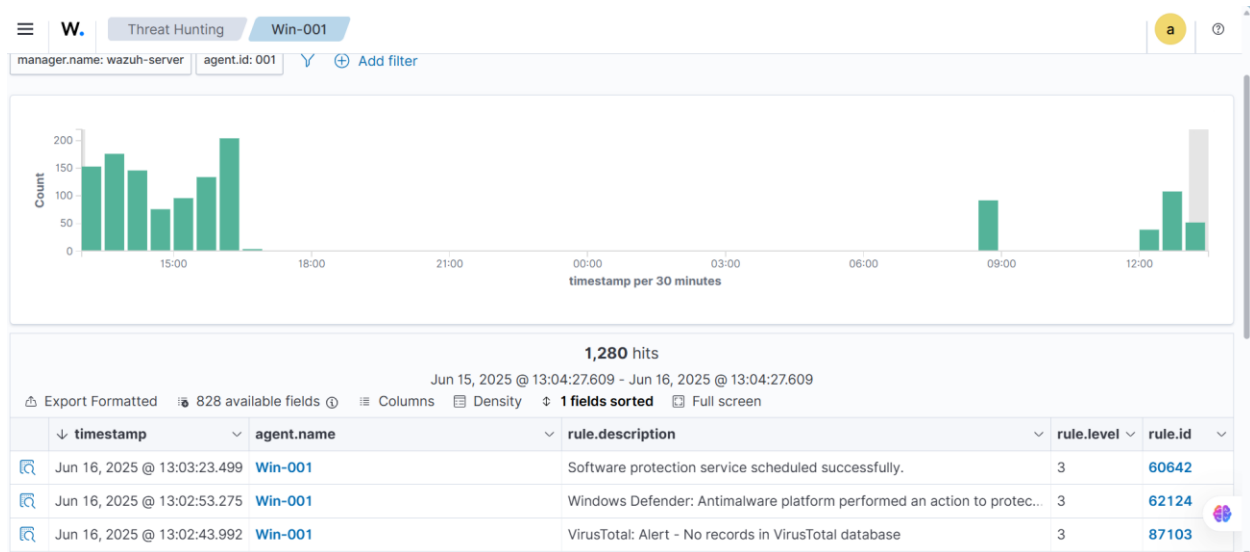
Extract it using the password infected:



Now run the malware:




After that open the Wazuh Dashboard and security events:



Document Details




View
surrounding
documents 

View single
document 



n ID

② data.win.eventdata.execution Name Suspended

② data.win.eventdata.fwLink <https://go.microsoft.com/fwlink/?link=amp;name=Trojan:Win32/Wacatac.H!ml&threatid=2147814523&enterprise=0>   

② data.win.eventdata.origin ID 1

② data.win.eventdata.origin Name Local machine

② data.win.eventdata.path file:_C:\\Users\\Shifat\\Downloads\\malware\\a9ca76d8913c120d2edcb433cdaced1f13921ad438cb2f56f0b882ae460b36d4.exe

② data.win.eventdata.post Clean Status 0

② data.win.eventdata.pre Execution Status 0

② data.win.eventdata.process Name C:\\Windows\\explorer.exe



② data.win.eventdata.product Name Microsoft Defender Antivirus

Document Details

[View surrounding documents](#)

[View single document](#)

?

data.win.eventdata.state

2

?

data.win.eventdata.status Code

103

?

data.win.eventdata.threat ID

2147814523

?

data.win.eventdata.threat Name

Trojan:Win32/Wacatac.H!mlme

?

data.win.eventdata.type ID

8

?

data.win.eventdata.type Name

FastPath

t

data.win.system.channel

Microsoft-Windows-Windows Defender/Operational

t

data.win.system.computer

DESKTOP-GR6BQDN

t

data.win.system.eventID

1117

t

data.win.system.eventRecordID

669

t

data.win.system.keywords

0x8000000000000000

t

data.win.system.level

4

t

data.win.system.message

"Microsoft Defender Antivirus has taken action"

Document Details

[View surrounding documents](#)

[View single document](#)

t

_index

wazuh-alerts-4.x-2025.06.16

t

agent.id

001

t

agent.ip

192.168.0.107

t

agent.name

Win-001

?

data.win.eventdata.action ID

2

?

data.win.eventdata.action Name

Quarantine me

?

data.win.eventdata.additional Actions ID

0

?

data.win.eventdata.additional Actions String

No additional actions required

?

data.win.eventdata.category ID

8

?

data.win.eventdata.category Name

Trojan

?

data.win.eventdata.detection

{7D8F8465-0008-4A3B-A611-EAECB00CC96F}

Summary:

Combining Windows Defender logs with Wazuh can significantly strengthen your security operations. Wazuh, an open-source platform for threat detection and compliance, allows for centralized log collection and real-time analysis. When paired with Windows Defender logs, it provides a holistic view of endpoint activity across your network.

This integration empowers security teams to correlate data from diverse sources, swiftly identify potential threats, and respond effectively. Wazuh's alerting and reporting features further reinforce your ability to maintain a resilient and secure IT environment.

In short, this setup bolsters cyber defenses and supports proactive risk management.

Need training on Wazuh ?

Contact number: +923355345678

Email: sameeerishassan@gmail.com

Linkedin: <https://pk.linkedin.com/in/sameer-hassan-15a428255>

Other SIEM

1. IBM Qradar
2. Splunk
3. Azure Sentinel