

o



Virus Total Integration with Splunk

Collection of Window logs.

Report Made by:

Arshman Abbas

Linkdin Profile link:

www.linkedin.com/in/arshman-abbas-89a95732a

Learning Objectives

Introduction :

- Splunk
- Virus Total
- Why we Integrated (Purpose)

Objectives :

- Collect Windows logs
- Detect malicious hashes
- Integrate Virus Total lookup
- Install & access Splunk
- Add Windows Event Logs (Application, System)
- Install Virus Total app and upload in Splunk for Integration.
- Monitor Results

What is Splunk?

Splunk is a powerful tool that collects, processes, and analyzes machine-generated data in real time. It helps organizations monitor systems, troubleshoot issues, detect security threats, and improve performance by turning raw log data into useful insights. With its search and visualization features, Splunk enables faster decision-making and greater visibility into IT environments.

What is VirusTotal?

VirusTotal is an online platform that scans files, URLs, and file hashes to detect malware and other threats. It checks the input against a wide range of antivirus engines and threat intelligence sources to determine if it's safe or harmful. Cybersecurity professionals use VirusTotal to investigate and confirm whether a file or activity is potentially malicious.

Purpose of Integrating Virus Total with Splunk

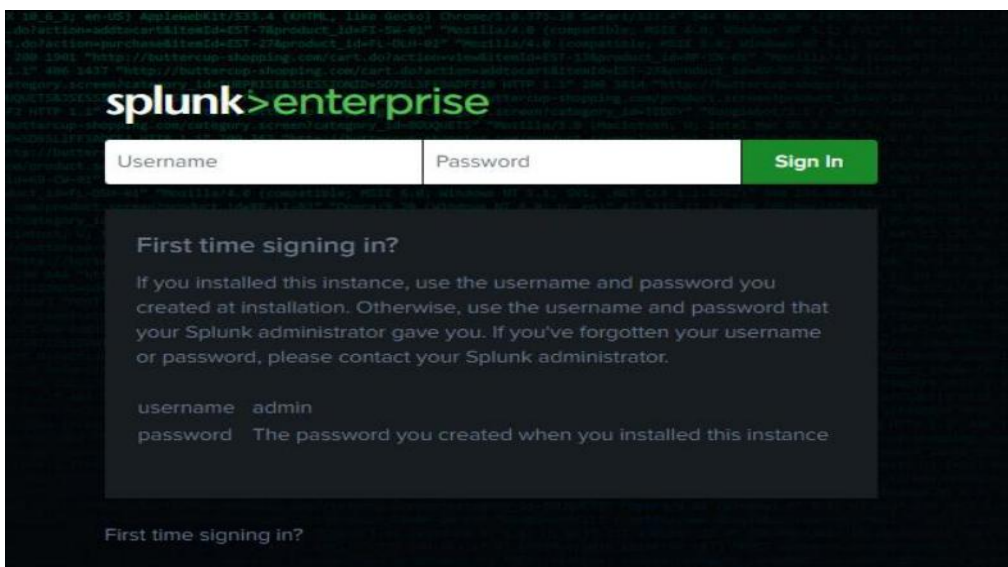
Integrating VirusTotal with Splunk strengthens threat detection by automatically checking file hashes found in log data. While Splunk collects and indexes log information, VirusTotal adds threat intelligence by labeling those hashes as safe, suspicious, or malicious. This combination enables security analysts to quickly spot and investigate threats in real time using enriched, actionable data.



WORK SET UP

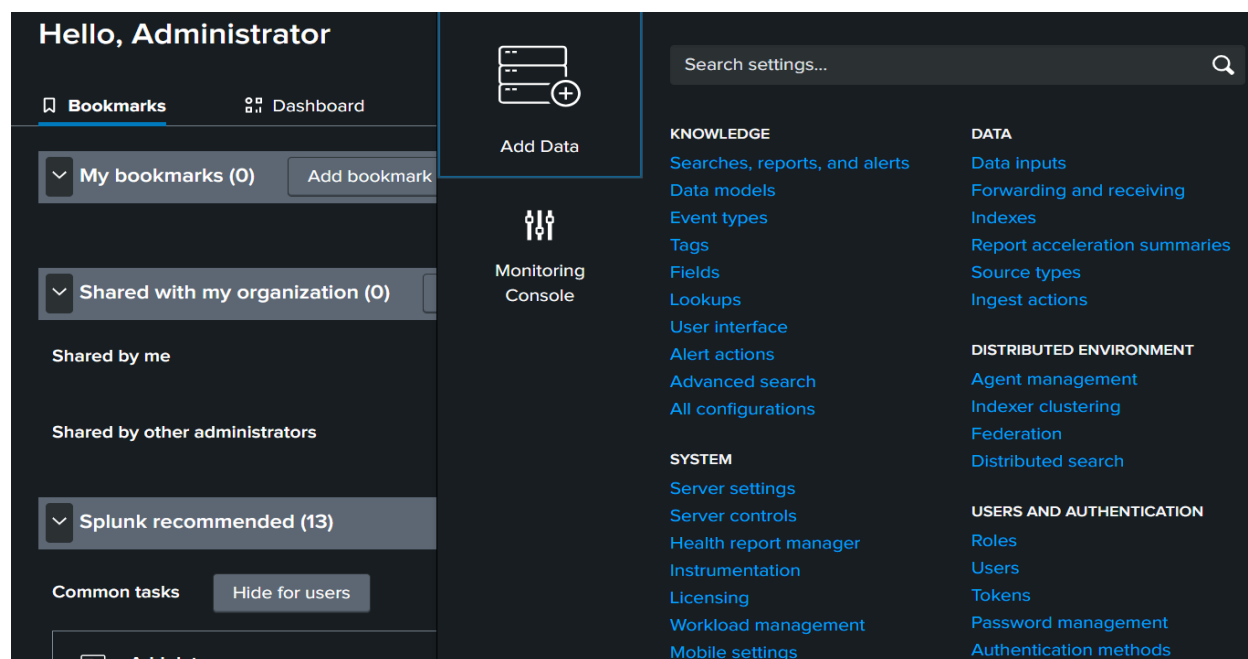
Step 1:

First download the Splunk SIEM Tool from the main page of Splunk splunk.org and assign your credentials. Then a interface would appear “**Enter Username**”and“**Password**” that you had assigned earlier. Press Enter to proceed.



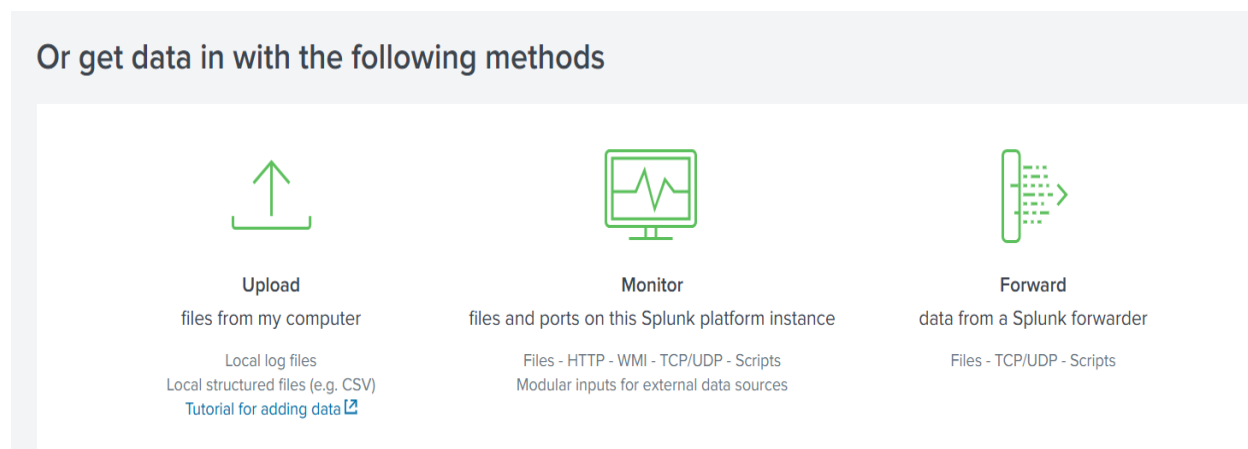
Step 2:

Now click the Settings Option in Splunk then “**Add Data**” option will appear select this.



Step 3:

Scroll down and choose the **Monitor**.



Step 4:

From the sidebar, select the "**Local Event Logs**" option and choose two logs: System and Application logs.

unk>enterprise Apps Administrator 1 Messages Settings Activity Help

Add Data Select Source Input Settings Review Done < Back Next >

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

← Select an option

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring

for local Windows Event Log channels where installed applications, send data. This monitor runs once for every Event Log input that

Available item(s)	add all >	Selected item(s)	< remove
Application		Security	
Security		System	
Setup			
System			
ForwardedEvents			
DirectShowFilterGraph			
DirectShowPluginControl			
Is_Hyphenation/Analytic			
EndpointMapper			

Select the Windows Event Logs you want to index from the list.

Step 5:

Click **Next**. The Host field and Index options will appear. Splunk automatically assigns a default host and index at this stage, so you typically don't need to change them manually.

Add Data

Select Source
Input Settings
Review
Done

< Back
Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Host field value

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index [Create a new index](#)

Step 6:

Open VirusTotal in your browser and sign into your account. Then, click on your profile icon and then select **API key**. Copy the API Key.

API KEY

This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality. By submitting data using your API key, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the [sharing of your Sample submissions with the security community](#). Please do not submit any personal information; we are not responsible for the contents of your submissions. [Learn more](#)

API QUOTA ALLOWANCES FOR YOUR USER

Upgrade API

You own a standard free end-user account. It is not tied to any corporate group and so it does not have access to Premium services. You are subjected to the following limitations:

Access level	⚠ Limited , standard free public API	Upgrade to premium
Usage	Must not be used in business workflows, commercial products or services.	
Request rate	4 lookups / min	
Daily quota	500 lookups / day	
Monthly quota	15.5 K lookups / month	

API reference

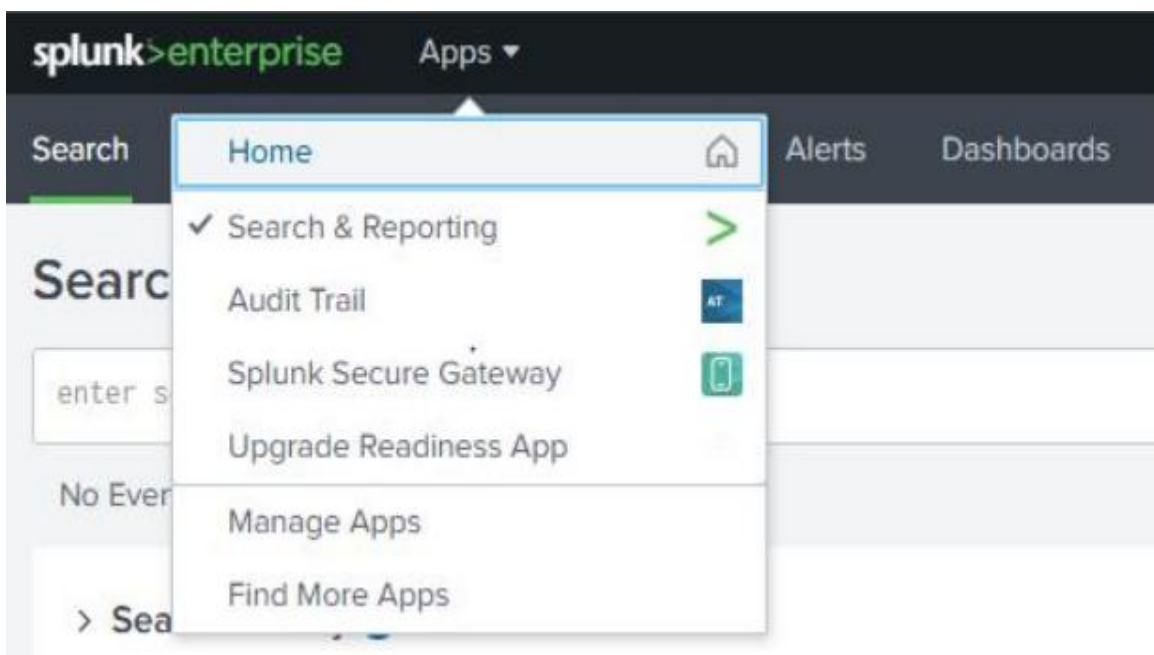
Python client

Golang library

Command-line interface

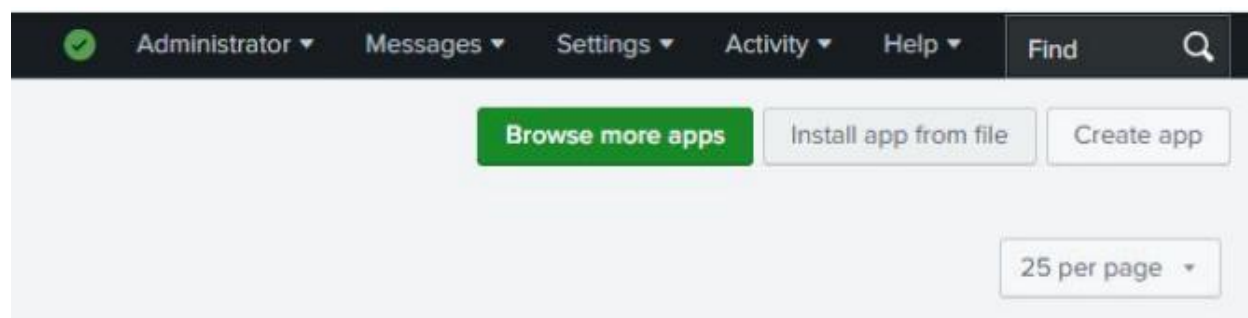
Step 7:

After saving the API key in the VirusTotal app setup, navigate to the Apps menu and open the Search & Reporting app. In the search bar, run a query (e.g., index=*sourcetype=WinEventLog:*) to view your Windows logs in the Results panel.



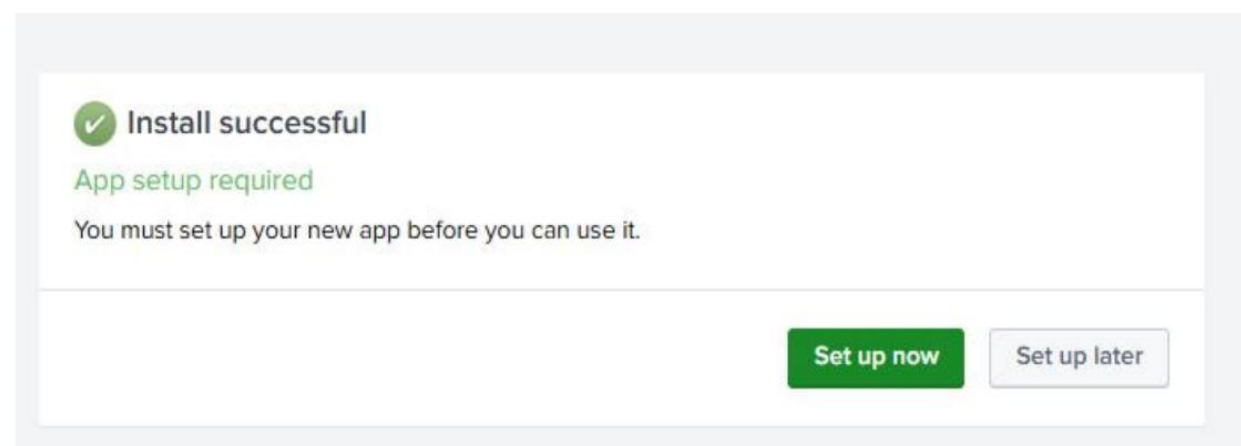
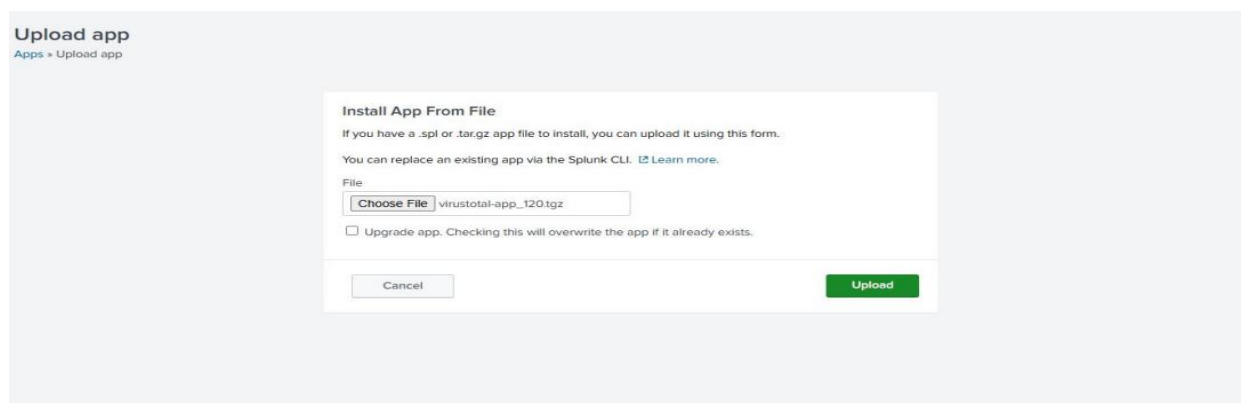
Step 8:

Download the **Virus total app** from Splunk base. Then Go to **Apps > Manage Apps > Install app from file**, upload the downloadedVirusTotal app file from Splunk-base, and complete the setup by saving your API key



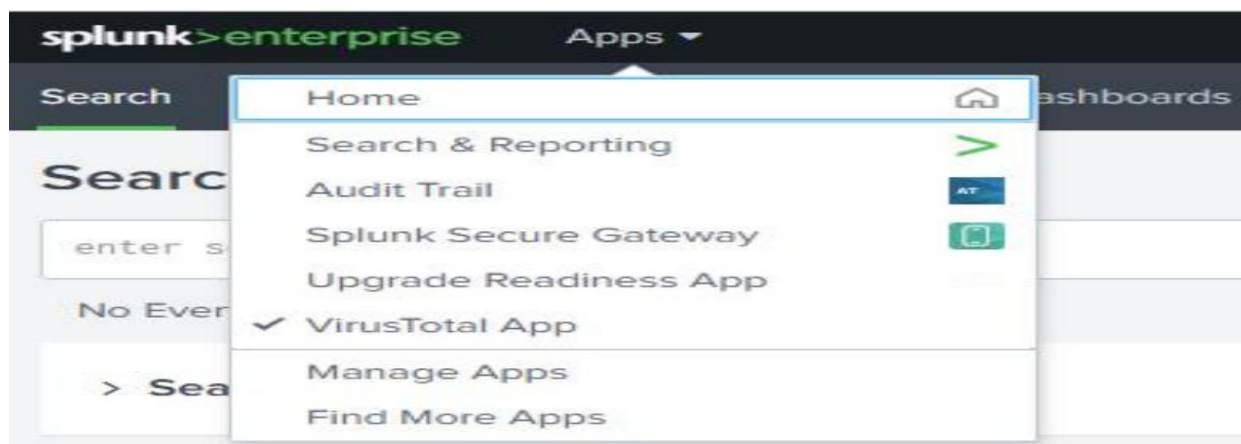
Step 9:

Select the downloaded Virus Total app file. Click Upload. After the install completes, if it says “App setup required”, click Set up now. Enter your VirusTotal API key there and save it. After this, click Set up now.



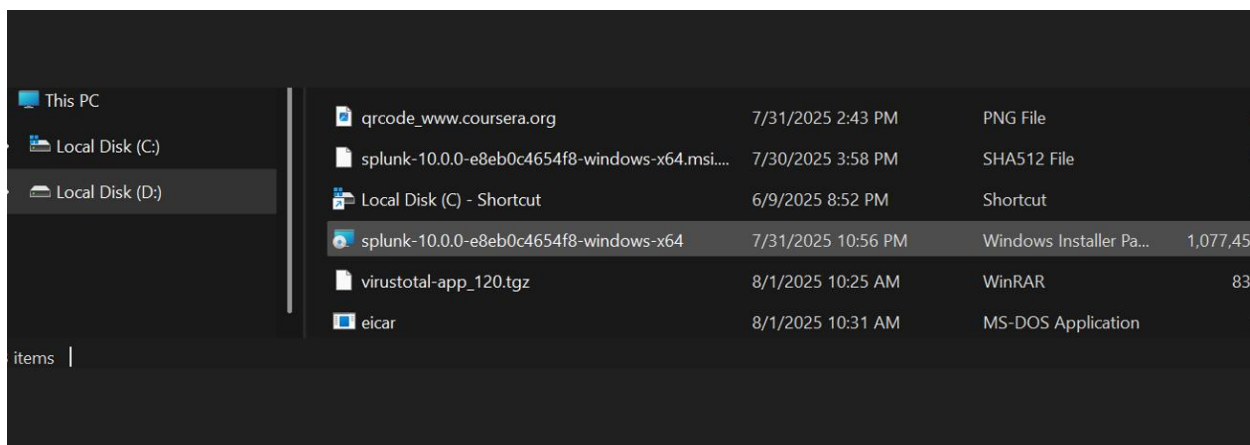
Step 10:

Now Virus total is Integrated successfully with Splunk. You can see it in the home Section.



Step 11:

Test the Sample Malware file **Eicar**(easily downloadable from internet) to check our Integration.



Step 12:

Restart Splunk using **powershell** and then interpret Virus total results in Splunk.

```

Administrator: Windows PowerShell
PS C:\Program Files\Splunk\bin> .\splunk restart
>>
Splunkd: Stopped

Splunk> Take the sh out of IT.

Checking prerequisites...
  Checking http port [8000]: open
  Checking mgmt port [8089]: open
  Checking appserver port [127.0.0.1:8065]: open
  Checking kvstore port [8191]: open
  Checking configuration... Done
New certs have been generated in 'C:\Program Files\Splunk\etc\auth'.
  Checking critical directories... Done
  Checking indexes...
    (skipping validation of index paths because not running as LocalSystem)
    Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main
summary
  Done
  Checking filesystem compatibility... Done
  Checking conf files for problems...
  Done
  Checking default conf files for edits...
  Validating installed files against hashes from 'C:\Program Files\Splunk\splunk-10.0.0-e8eb0c4654f8-windows-x64-manifest'
  All installed files intact.
  Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Splunkd: Starting (pid 2880)
  
```

Here the results are visible in Splunk:

```
"source": "virustotal",
"file_name": "eicar.com",
"file_hash": "44D88612FEA8A8F36DE82E1278ABB02F",
"malicious_engines": 55,
"total_engines": 60,
"detection_ratio": "55/60",
"severity": "high",
"scan_date": "2025-07-06",
"status": "malicious",
"host": "WIN10-HBK"
}
```

Collapse

host = DESKTOP-MAIANMK | source = virustotal:detection:log | sourcetype = VT4enlunk

Step 13:

We also queried hash on Virus total for Additional Verification.

8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71

60/67 security vendors flagged this file as malicious

Reanalyze Similar More

8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71

eicar.com

Size: 70 B | Last Analysis Date: 2 hours ago

powershell idle attachment long-sleeps via-tor

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 21

Crowdsourced YARA rules

- Matches rule **malw_eicar** from ruleset **MALW_Eicar** at <https://github.com/advanced-threat-research/Yara-Rules> by Marc Rivero | McAfee ATR Team
 - Rule to detect the EICAR pattern - 2 hours ago
- Matches rule **Multi_EICAR_ac8f42d6** from ruleset **Multi_EICAR** at <https://github.com/elastic/protectons-artifacts> by Elastic Security

Dynamic Analysis Sandbox Detections

- The sandbox **Zenbox** flags this file as: MALWARE.TROJAN

THE END

