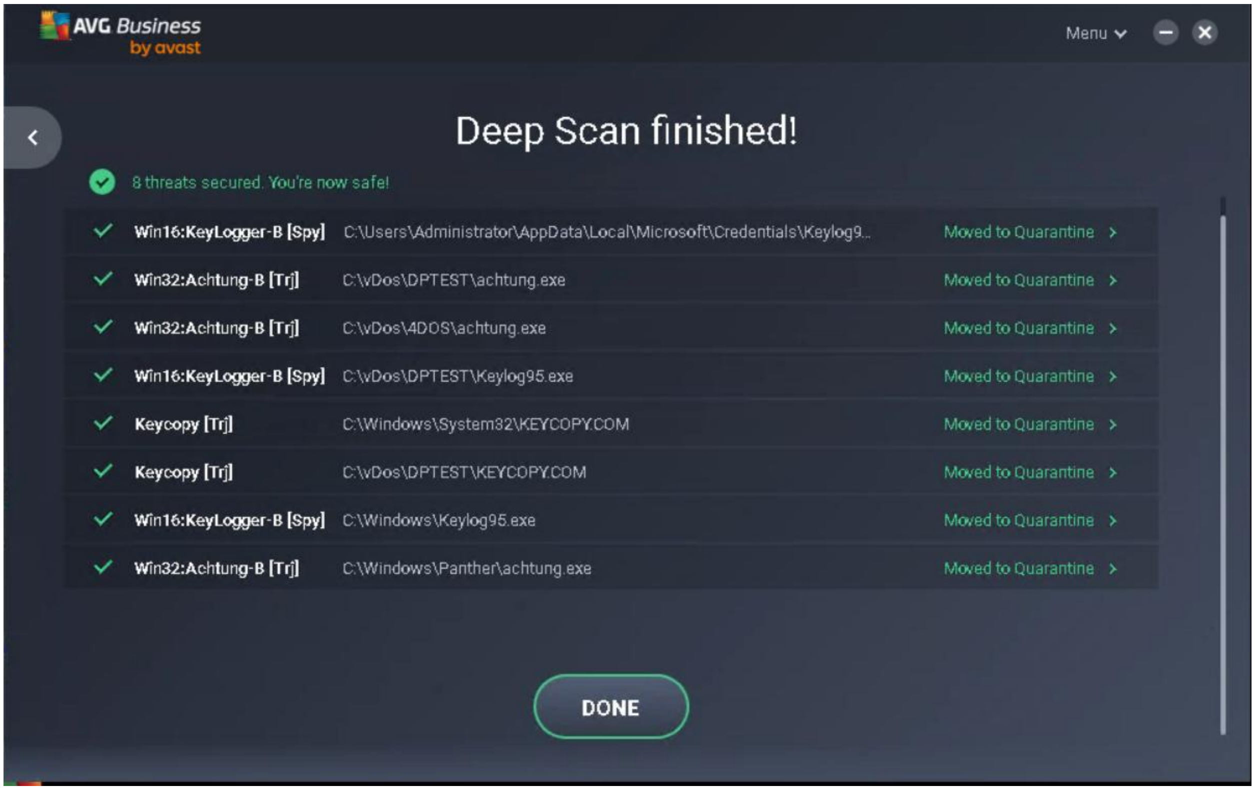
LAB 9: INVESTIGATING AND RESPONDING TO SECURITY INCIDENTS

By: Jason Hodge

Overview: In this lab I used AVG Business Antivirus software to identify and manage threats to the system. I also did research on a couple threats and wrote security reports to that effect.

Section 1:

Scan Summary (Detections)

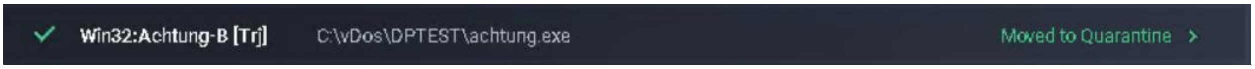


Deep Scan finished!

8 threats secured. You're now safe!

✓	Win16:KeyLogger-B [Spy]	C:\Users\Administrator\AppData\Local\Microsoft\Credentials\Keylog9...	Moved to Quarantine ›
✓	Win32:Achtung-B [Trj]	C:\vDos\DPTEST\achtung.exe	Moved to Quarantine ›
✓	Win32:Achtung-B [Trj]	C:\vDos\4DOS\achtung.exe	Moved to Quarantine ›
✓	Win16:KeyLogger-B [Spy]	C:\vDos\DPTEST\Keylog95.exe	Moved to Quarantine ›
✓	Keycopy [Trj]	C:\Windows\System32\KEYCOPY.COM	Moved to Quarantine ›
✓	Keycopy [Trj]	C:\vDos\DPTEST\KEYCOPY.COM	Moved to Quarantine ›
✓	Win16:KeyLogger-B [Spy]	C:\Windows\Keylog95.exe	Moved to Quarantine ›
✓	Win32:Achtung-B [Trj]	C:\Windows\Panther\achtung.exe	Moved to Quarantine ›

Achtung.exe threat



✓ Win32:Achtung-B [Trj] C:\vDos\DPTEST\achtung.exe Moved to Quarantine ›

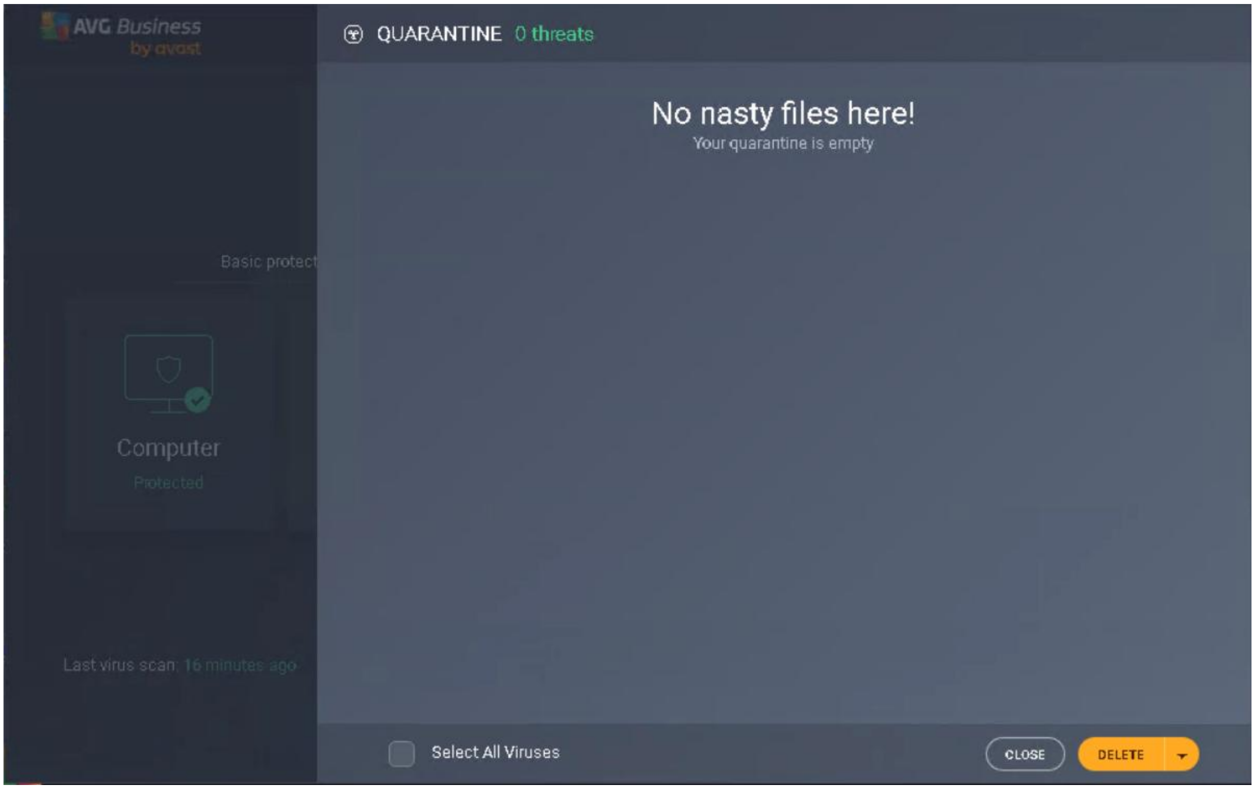
Achtung.exe is an entangle worm virus that presents a serious vulnerability which should be fixed immediately. It can take screenshots and record keystrokes. Personal information may then be sent via email or file transfer protocol (FTP) to a parent company.

According to Safer Networking these are the instructions on removing Achtung.exe

Before you can delete files, you must first stop all the Achtung processes that are running in memory.
Do this by ending all processes from the Task Manager.
Press CtrL+ALT+DELETE to open the Windows Task Manager. If you see multiple "tabs," click on the "Processes" tab. For each process that you would like to kill, find the process name in the list, click it to select it, and click the "End Process" button.

https://www.safer-networking.com/removeachtung.php

Empty Quarantine Area



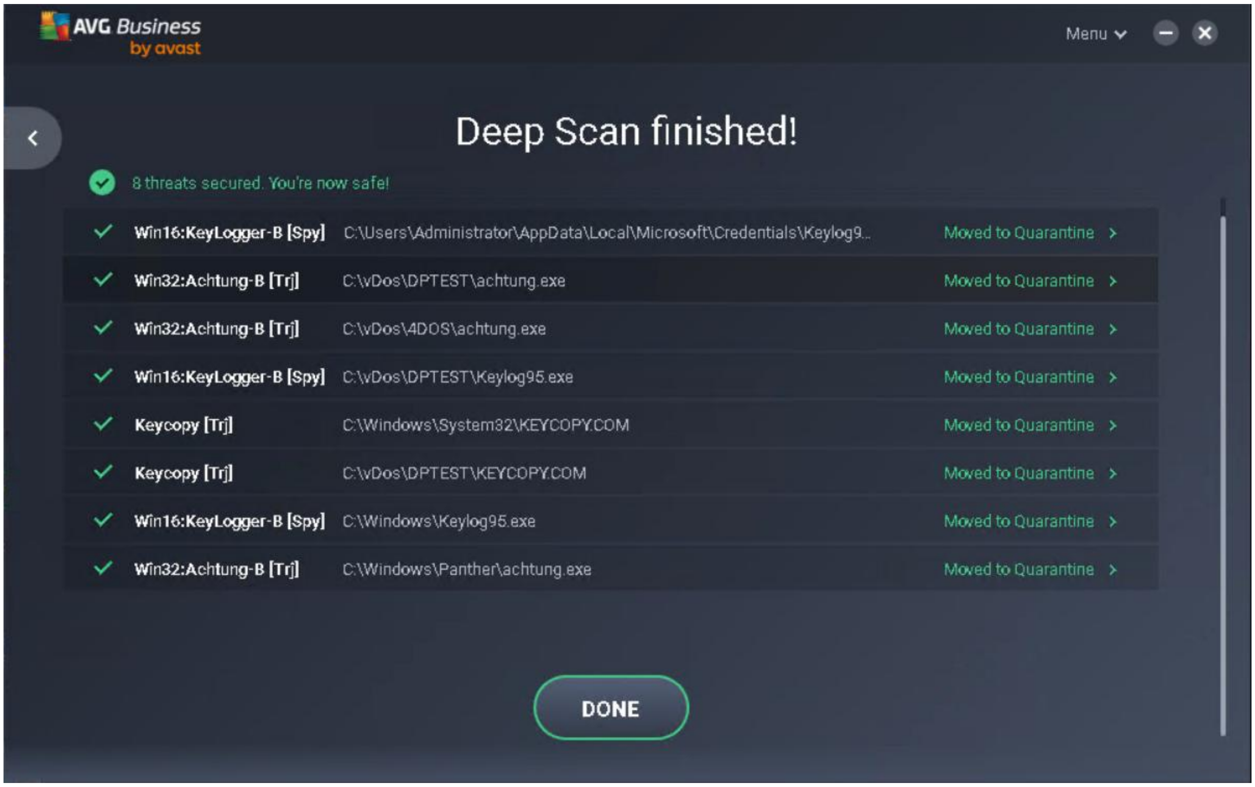
QUARANTINE 0 threats

No nasty files here!

Your quarantine is empty

Section 2:

Scan Summary (Detections)

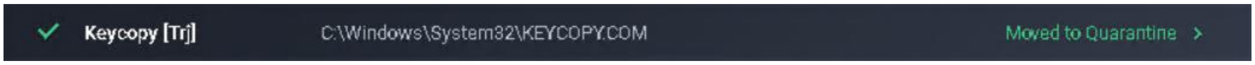


Deep Scan finished!

8 threats secured. You're now safe!

Win16:KeyLogger-B [Spy]	C:\Users\Administrator\AppData\Local\Microsoft\Credentials\Keylog9..	Moved to Quarantine
Win32:Achtung-B [Trj]	C:\vDos\DPTEST\achtung.exe	Moved to Quarantine
Win32:Achtung-B [Trj]	C:\vDos\4DOS\achtung.exe	Moved to Quarantine
Win16:KeyLogger-B [Spy]	C:\vDos\DPTEST\Keylog95.exe	Moved to Quarantine
Keycopy [Trj]	C:\Windows\System32\KEYCOPY.COM	Moved to Quarantine
Keycopy [Trj]	C:\vDos\DPTEST\KEYCOPY.COM	Moved to Quarantine
Win16:KeyLogger-B [Spy]	C:\Windows\Keylog95.exe	Moved to Quarantine
Win32:Achtung-B [Trj]	C:\Windows\Panther\achtung.exe	Moved to Quarantine

KEYCOPY.COM threat



Keycopy [Trj]	C:\Windows\System32\KEYCOPY.COM	Moved to Quarantine

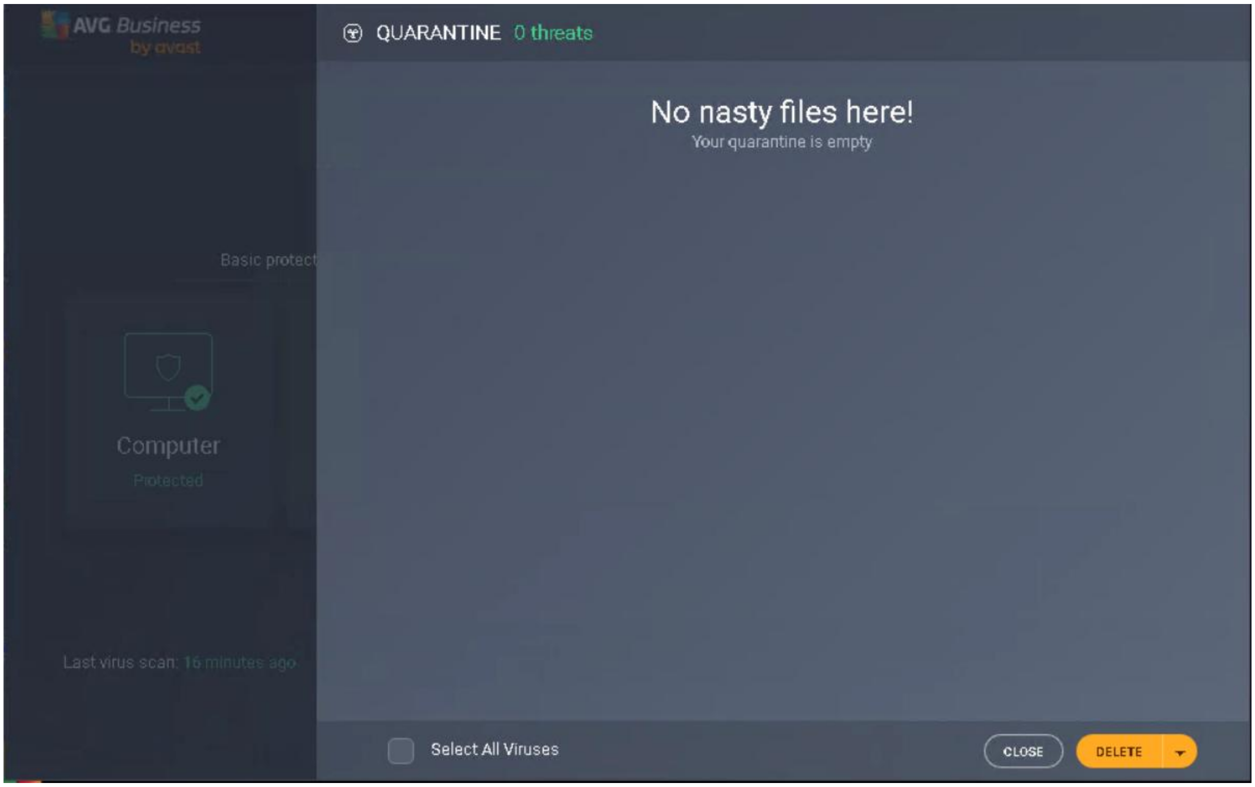
KEYCOPY.COM is malware that can damage a system completely by tracking user activity such as applications used, history, and keystrokes.

According to Malware Protection Blogspot these are the instructions on removing KEYCOPY.COM

> To completely remove Keycopy malware from your computer, you need to delete the Windows registry keys and registry values, the files and folders associated with Keycopy.
>
> 1. Use Task Manager to terminate the Keycopy process.
> 2. Delete the original Keycopy file and folders.
> 3. Delete the system registry key parameters

4. Update your antivirus databases or buy antivirus software and perform a full scan of the computer.

Empty Quarantine Area



QUARANTINE 0 threats

No nasty files here!

Your quarantine is empty

Last virus scan: 16 minutes ago