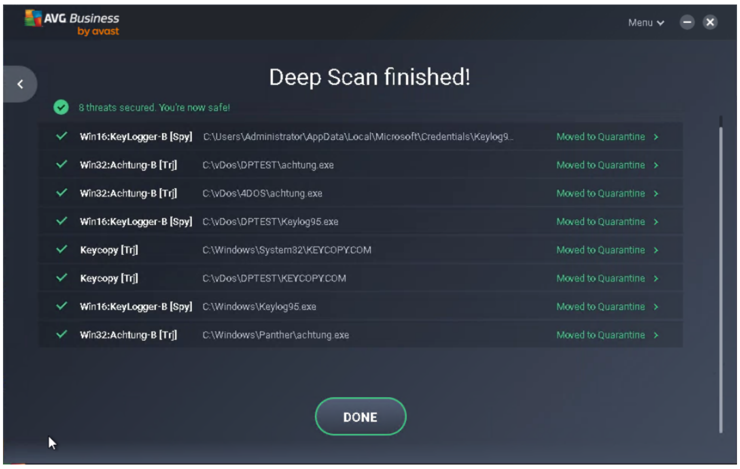
CEN4088.01 Lab 9 Due 11/25/19

Brandon Thompson 5517

November 25, 2019

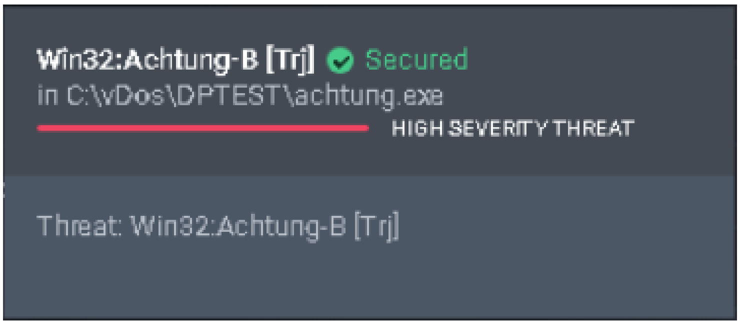


Deep Scan finished!

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

Figure 1: AVG scan summary of TargetWindows02.

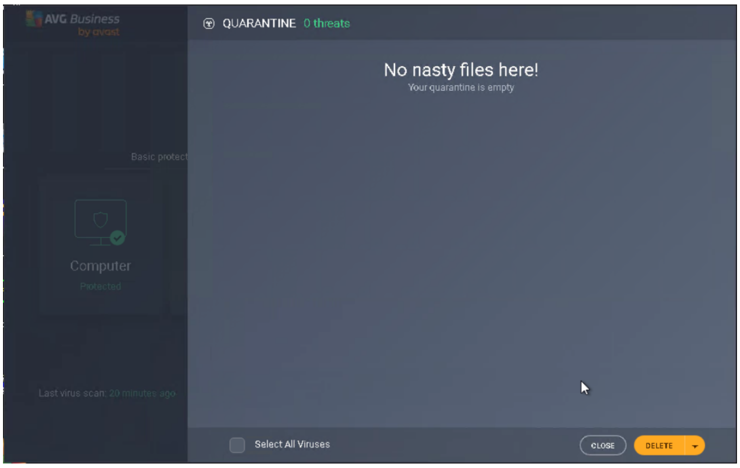


Win32:Achtung-B [Trj] ✓ Secured
in C:\vDos\DPTEST\achtung.exe
HIGH SEVERITY THREAT

Threat: Win32:Achtung-B [Trj]

Figure 2: Details of `achtung.exe` threat.

The `achtung.exe` file is associated with a virus called Entangle Worm (W32.Entangle.Worm). The entangle worm is a mass-mailing worm that will send itself to all addresses in the windows address book and copy itself to the %System% and %temp% environments. To remove the worm, ensure that virus definitions are updated and scan the system with AVG Business.



No nasty files here!

Your quarantine is empty

Figure 3: Empty quarantine area (virus vault).

Security Incident Report Part 1

Incident Report #: IR-83631
Report Date and Time: 11/21/19 10:00 AM
Technician: Brandon Thompson
Site Location: Virtual machine IP 172.30.0.10 (Windows Server 2016)

Identification (type and how detected): Part of lab exercise.

Virus scan detected: Keylogger and Avalanche (`achtung.exe`).
Triage (impact): Virtual machine 172.30.0.10 only.

Containment (Steps taken):

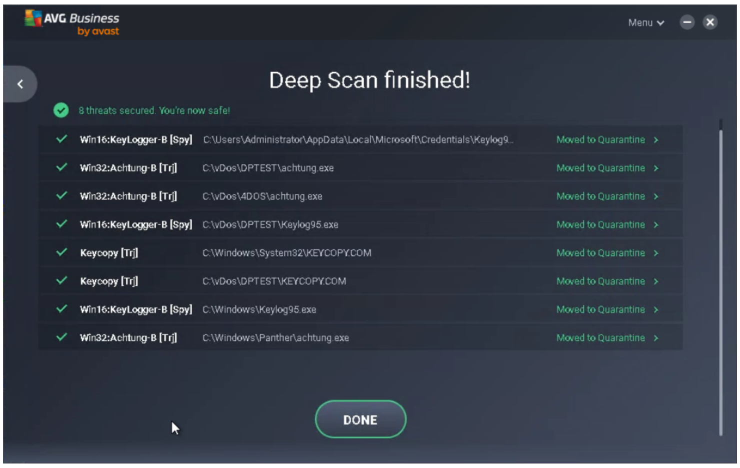
1. Disabled wireless on virtual machine.
2. Ran manual virus detection

Investigation (Cause): worm placed on machine for education purposes.
Recovery and Repair (Resolution):

Used antivirus software to quarantine and eradicate the malware.
Implemented scanning of email for malware and spam.
Lessons Learned (Debriefing and Feedback):

Antivirus software on systems should be configured to scan all hard drives regularly to identify any file system infections and, optionally, to scan other storage media as well. Users should also be able to launch a scan manually as needed.

Users should be educated on protecting themselves from viruses by running only company authorized Antivirus software, not opening suspicious e-mail attachments, not responding to suspicious or unwanted e-mails.

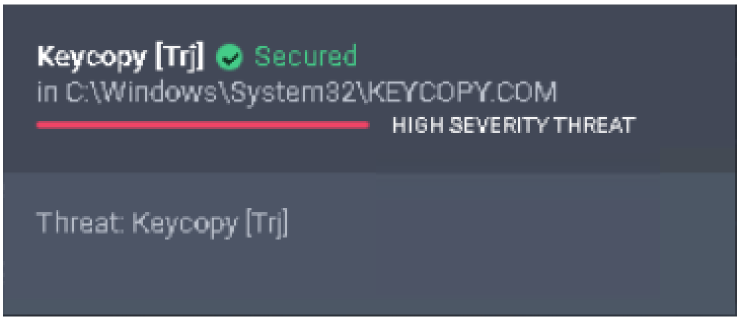


Deep Scan finished!

✓ 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 >

Figure 4: AVG scan summary of TargetWindows02.



Keycopy [Trj] ✓ Secured
in C:\Windows\System32\KEYCOPY.COM
HIGH SEVERITY THREAT

Threat: Keycopy [Trj]

Figure 5: Details of KEYCOPY.COM

The `KEYCOPY.COM` file is associated with a keylogger virus that records keystrokes and applications to retrieve usernames and passwords to gain access to secure information. Keycopy.com gains access to the computer through installing malicious software or files from untrusted websites. To remove the keycopy.com virus from the system ensure virus definitions are up to date and scan the system with AVG Business.

Security Incident Report Part 2

Incident Report #: IR-83632
Reported Date and Time: November 25, 2019
Technician: Trevor Dash
Site Location: Virtual machine IP 172.30.0.10 (Windows Server 2016)

Identification (type and how detected): Part of lab exercise.

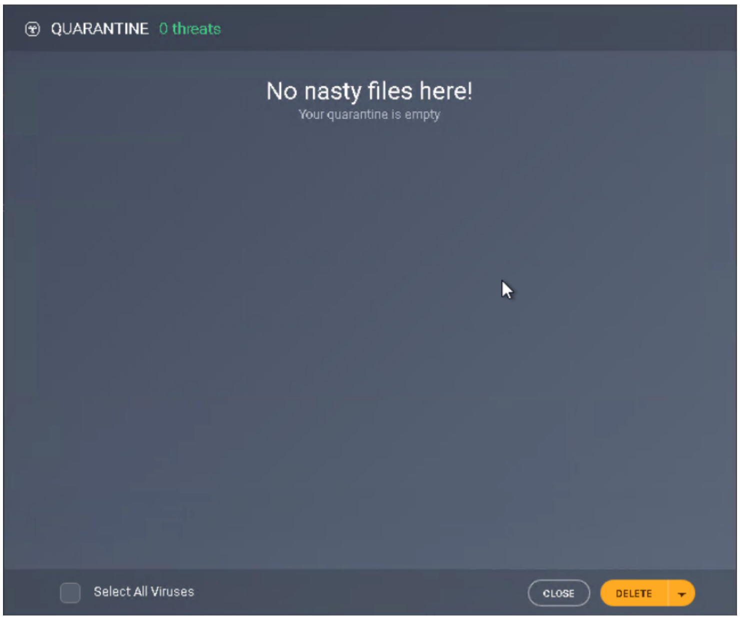


Figure 6: Empty quarantine area.

Virus scan detected: Keylogger Virus (`KEYCOPY.COM`).
Triage (impact): Virtual machine 172.30.0.10 only.

Containment (Steps taken):

1. Disabled wireless on virtual machine.
2. Ran manual virus detection

Investigation (Cause): worm placed on machine for education purposes.
Recovery and Repair (Resolution):

Used antivirus software to quarantine and eradicate the malware.
Implemented scanning of email for malware and spam.
Lessons Learned (Debriefing and Feedback):

Antivirus software on systems should be configured to scan all hard drives regularly to identify any file system infections and, optionally, to scan other storage media as well. Users should also be able to launch a scan manually as needed.

Users should be educated on protecting themselves from viruses by running only company authorized Antivirus software, not opening suspicious e-mail attachments, not responding to suspicious or unwanted e-mails.