"WANNACRY" RANSOMWARE ANTIDOTES

by Francis Chao
fchao2@yahoo.com

TUCSON COMPUTER SOCIETY

WINNERS WINdows usERS

apcug

An International Association of Technology & Computer User Groups

Web location for this presentation:

http://aztcs.org

Click on “Meeting Notes”

SUMMARY

After a computer is infected with "WannaCry" ransomware, there are lots of free software programs for removing the infection. However, the "WanaKiwi.exe" program for unencrypting data files did not work for us.

TOPICS

- WanaKiwi.exe Unencryption Program

MAY 15, 2017 SECURITY UPDATE FROM MICROSOFT

- Microsoft's "Security Update for Windows XP SP3 (KB4012598)"
  - See https://www.microsoft.com/en-us/download/details.aspx?id=55245

MARCH 12, 2017 SECURITY UPDATE FROM MICROSOFT

- "Microsoft Security Bulletin MS17-010 - Critical" for "Windows 7" and higher is described at
  - https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  - and
  - https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

MAY 12, 2017 UPDATE FOR "WINDOWS DEFENDER"

- Microsoft's May 12, 2017 update for "Windows Defender" and "Microsoft Security Essentials" is able to remove and block "WannaCry".
  Like other antivirus products, they cannot unencrypt files that have been encrypted by "WannaCry".

MAY 15, 2017 SECURITY UPDATE FROM MICROSOFT

- Microsoft's "Security Update for Windows XP SP3 (KB4012598)"
  - See https://www.microsoft.com/en-us/download/details.aspx?id=55245

MAY 22, 2017 UPDATED "MALICIOUS SOFTWARE REMOVAL TOOL"

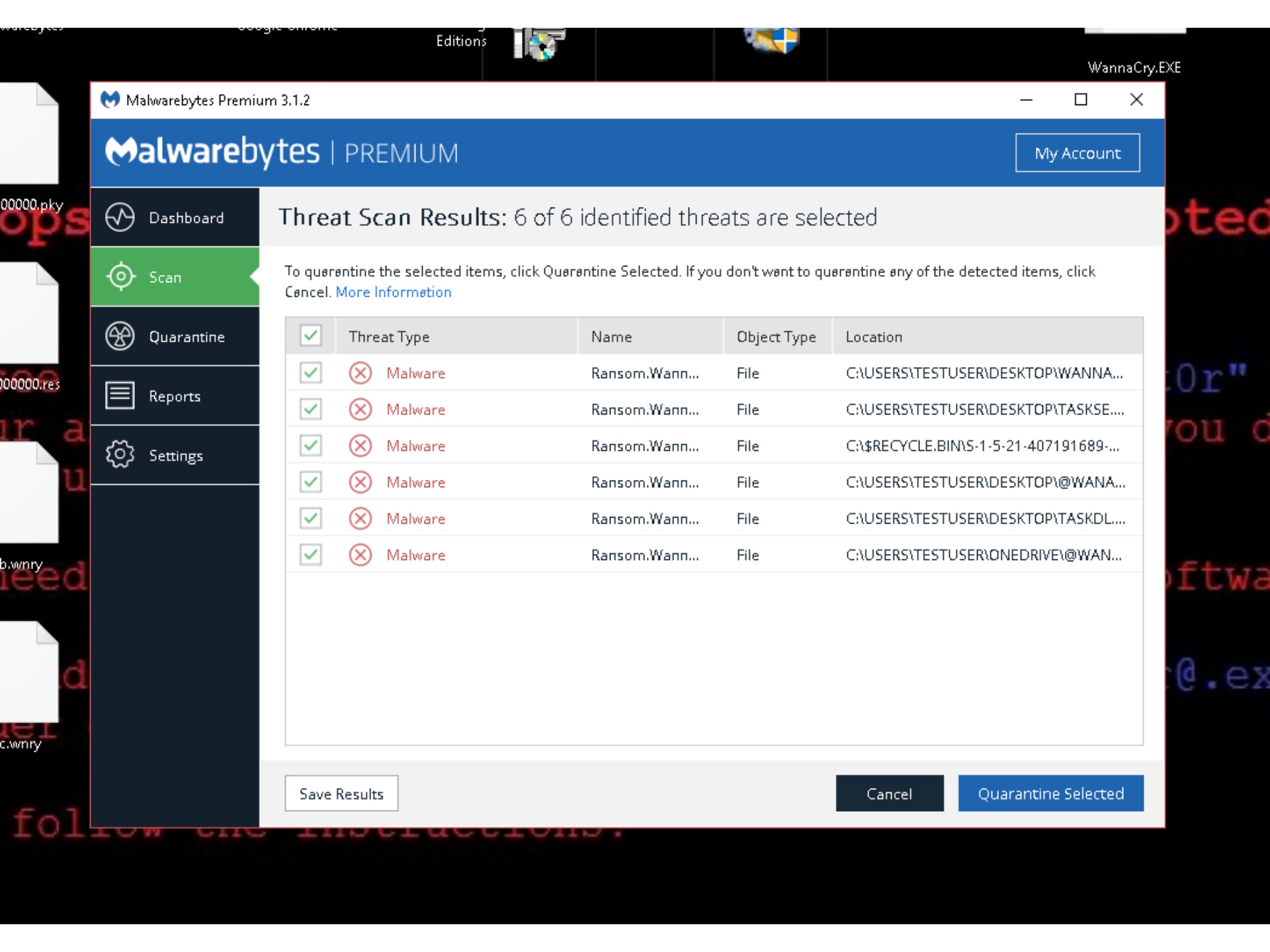
- Unlike Microsoft's May 9, 2017 monthly version of the "Malicious Software Removal Tool", the May 22 version is able to remove "WannaCry".
  Like other antivirus products, they cannot unencrypt files that have been encrypted by "WannaCry".

CYBERREASON'S FREE "RANSOMFREE" PROGRAM

- See https://ransomfree.cybereason.com/

MALWAREBYTES

- The free version of "Malwarebytes 3 Premium" can remove "WannaCry" but, as expected, it cannot unencrypt the data files that "WannaCry" has damaged
- You can get "Malwarebytes.." at https://www.malwarebytes.com/mwb-download/

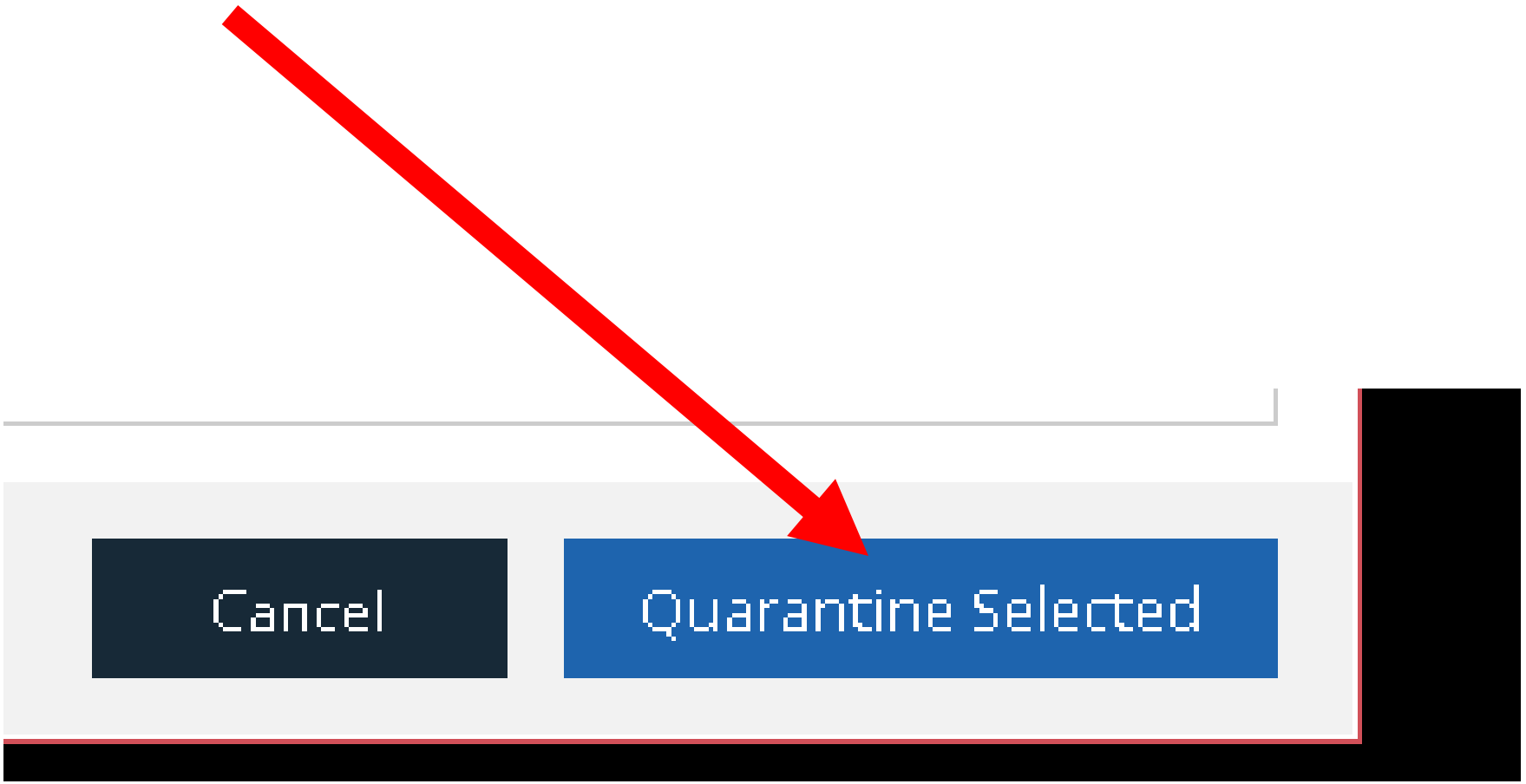

Editions
WannaCry.EXE
Malwarebytes Premium 3.1.2
Malwarebytes | PREMIUM
My Account
Dashboard
Scan
Quarantine
Reports
Settings
Threat Scan Results: 6 of 6 identified threats are selected
To quarantine the selected items, click Quarantine Selected. If you don't want to quarantine any of the detected items, click Cancel. More Information
Threat Type
Name
Object Type
Location
Malware
Ransom.Wann...
File
C:\USERS\TESTUSER\DESKTOP\WANNA...
C:\USERS\TESTUSER\DESKTOP\TASKSE....
C:\$RECYCLE.BIN\S-1-5-21-407191689-...
C:\USERS\TESTUSER\DESKTOP\@WANA...
C:\USERS\TESTUSER\DESKTOP\TASKDL....
C:\USERS\TESTUSER\ONEDRIVE\@WAN...
Save Results
Cancel
Quarantine Selected

To quarantine the selected items, click Quarantine Selected. If you don't want to quarantine any of the detected items, click Cancel. More Information

Threat Type	Name	Object Type	Location
Malware	Ransom.Wann...	File	C:\USERS\TESTUSER\DESKTOP\WANNA...
Malware	Ransom.Wann...	File	C:\USERS\TESTUSER\DESKTOP\TASKSE....
Malware	Ransom.Wann...	File	C:\$RECYCLE.BIN\S-1-5-21-407191689-...
Malware	Ransom.Wann...	File	C:\USERS\TESTUSER\DESKTOP\@WANA...
Malware	Ransom.Wann...	File	C:\USERS\TESTUSER\DESKTOP\TASKDL....
Malware	Ransom.Wann...	File	C:\USERS\TESTUSER\ONEDRIVE\@WAN...

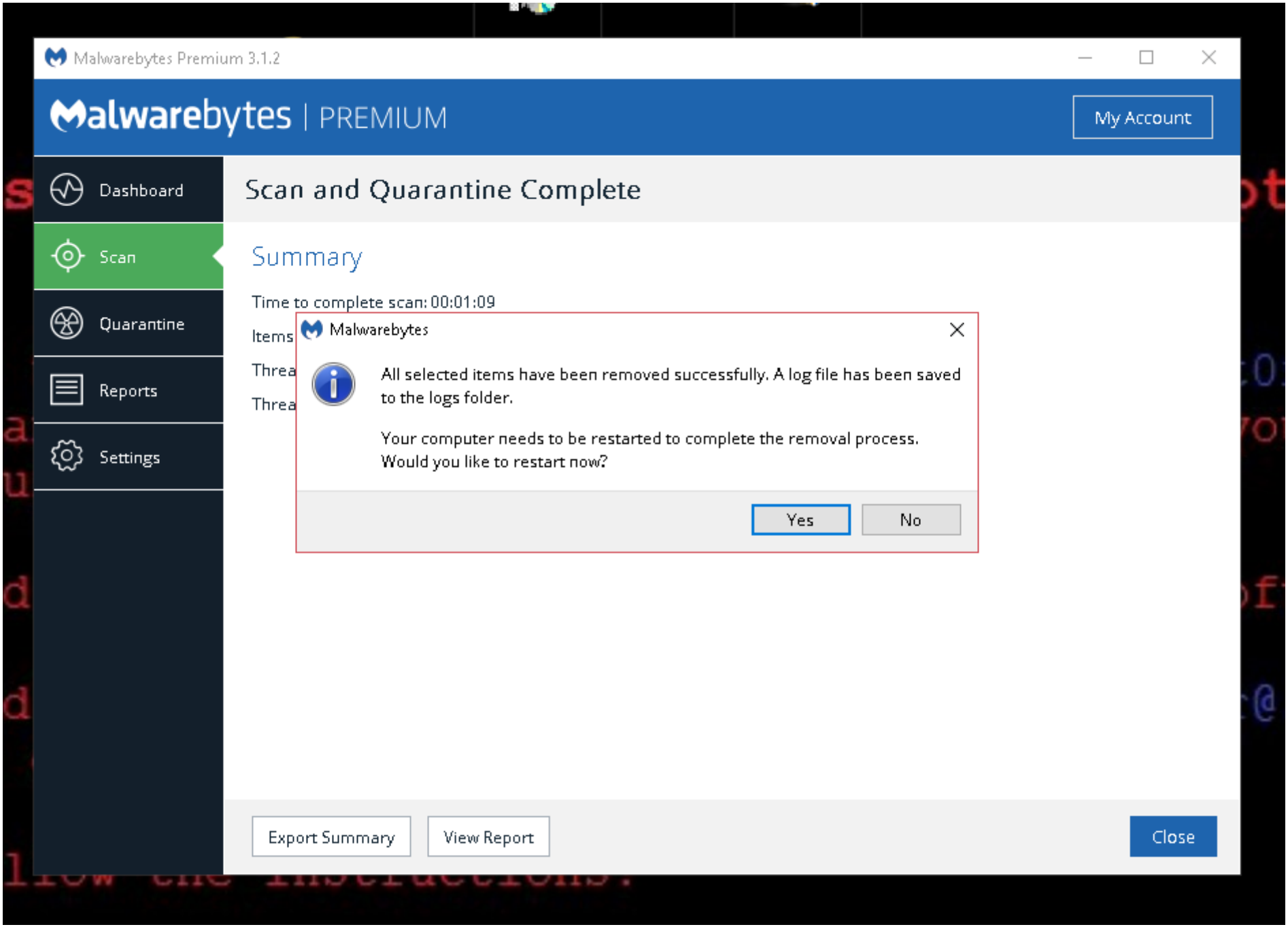
MALWAREBYTES (continued)

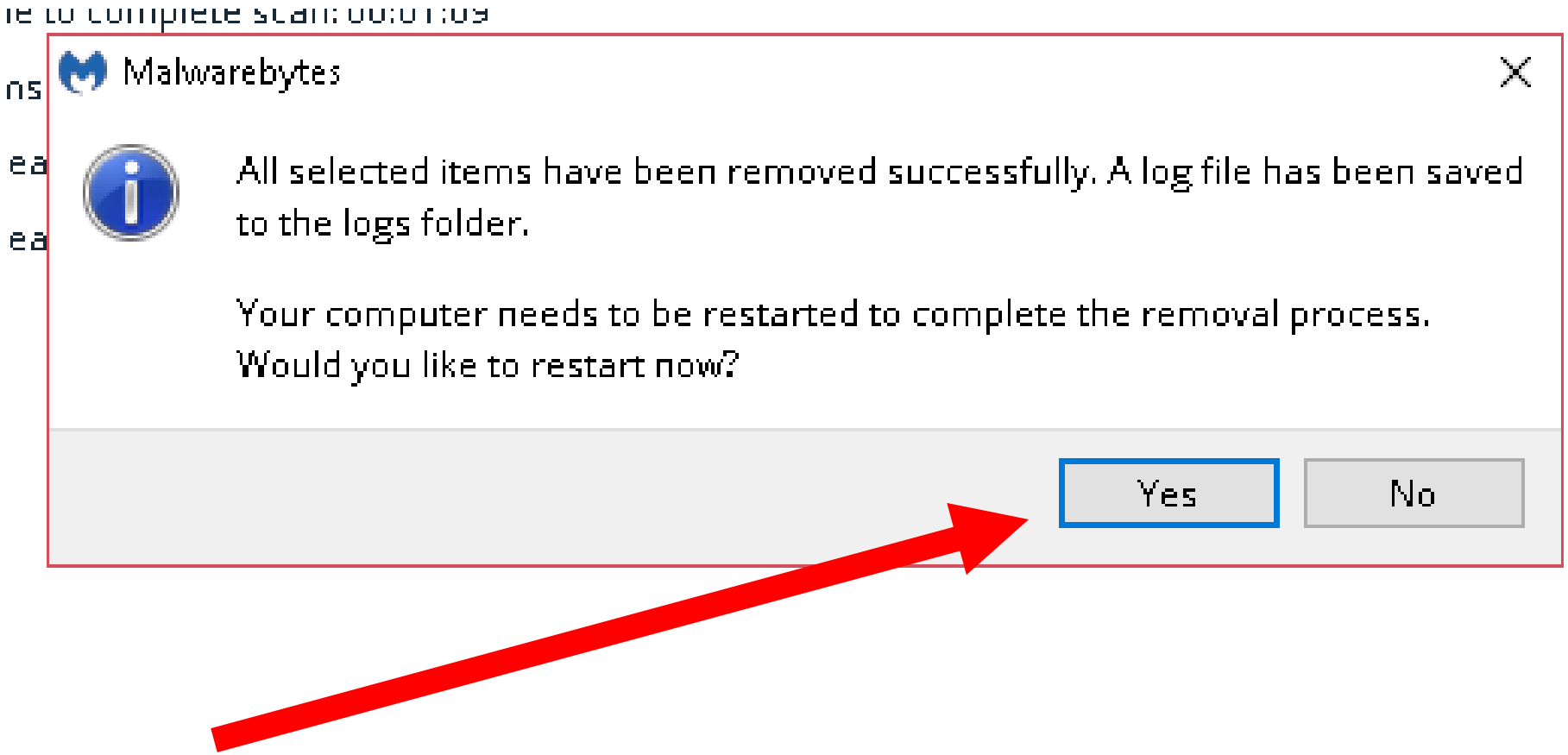
- Click on "Quarantine Selected" after the "Malwarebytes.." scan finished.


Cancel
Quarantine Selected

MALWAREBYTES (continued)

- Then click on "Yes" to re-start the computer:


Malwarebytes Premium 3.1.2
Malwarebytes | PREMIUM
My Account
Dashboard
Scan
Quarantine
Reports
Settings
Scan and Quarantine Complete
Summary
Time to complete scan: 00:01:09
Items
Threa
Threa
Malwarebytes
All selected items have been removed successfully. A log file has been saved to the logs folder.
Your computer needs to be restarted to complete the removal process. Would you like to restart now?
Yes
No
Export Summary
View Report
Close


Malwarebytes
All selected items have been removed successfully. A log file has been saved to the logs folder.
Your computer needs to be restarted to complete the removal process.
Would you like to restart now?
Yes
No

WANAKIWI UNENCRYPTION PROGRAM

- The WanaKiwi program can decrypt some of the data files that have been encrypted by WannaCry
- See https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d

WANAKIWI UNENCRYPTION PROGRAM (continued)

- You can download WanaKiwi from https://github.com/gentilkiwi/wanakiwi/releases
- Then run wanakiwi.exe from an elevated command prompt window

"RECUVA" CAN SOMETIMES RECOVER DATA FILES

- The free edition of the "Recuva" program can sometime recover data files that have been encrypted by "WanaCry"
  You can download "Recuva" at https://www.piriform.com/recuva

"SHADOW EXPLORER" CAN SOMETIMES RECOVER DATA FILES

- The "Shadow Explorer" program can sometime recover data files that have been encrypted by "WanaCry"
  You can download "Shadow Explorer" at http://www.shadowexplorer.com/downloads.html