Can Windows 11 Stop Well-Known Ransomware Variants? An Examination of Its Built-in Security Features Supplementary Materials

Yousef Mahmoud Al-Awadi [1], Ali Baydoun [1,*] and Hafeez Ur Rehman [1,2]

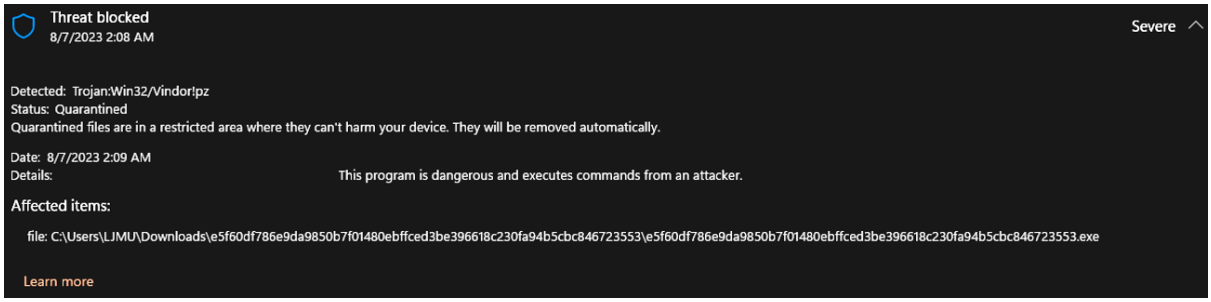

Figure S1. Evident of detecting the MortalKombat ransomware by Windows Defender.

Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Vindor!pz&threatid=2147847321&enterprise=0
Name: Trojan:Win32/Vindor!pz
ID: 2147847321
Severity: Severe
Category: Trojan
Path: file:_C:\Users\LJMU\Downloads\e5f60df786e9da9850b7f01480ebffced3be396618c230fa94b5cbc846723553.exe
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: System
User: NT AUTHORITY\SYSTEM
Process Name: Unknown
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x00000000
Error description: The operation completed successfully.
Security intelligence Version: AV: 1.395.125.0, AS: 1.395.125.0, NIS: 1.395.125.0
Engine Version: AM: 1.1.23070.1005, NIS: 1.1.23070.1005

Figure S2. Windows Defender logs after detection the MortalKombat variant.

Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
Name: Trojan:Win32/Vindor!pz
Path file: C:\Users\LJMU\Downloads\70d6105900816937f3c74dce0c044f03ac72df99485cc9f76bf4e0a47bc3e0da.exe

Figure S3. Windows Defender logs showing the detection of the MortalKombat ransomware download.

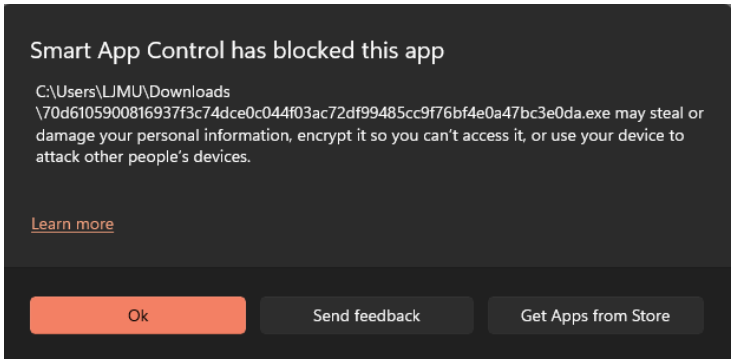

Figure S4. Smart App Control popup when attempting to run the MortalKombat executable.

Figure S5. Windows Defender detecting Cerber upon extraction.

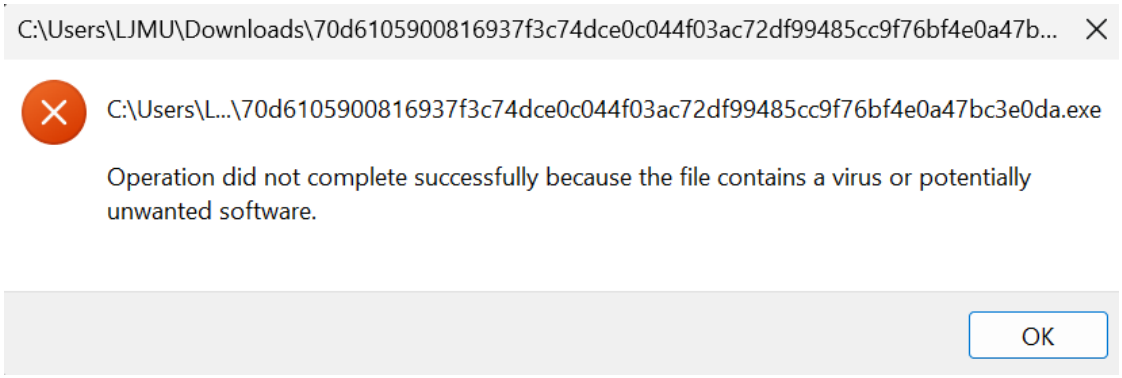

Figure S6. Windows Defender prevented the user from manually executing the Cerber exe.

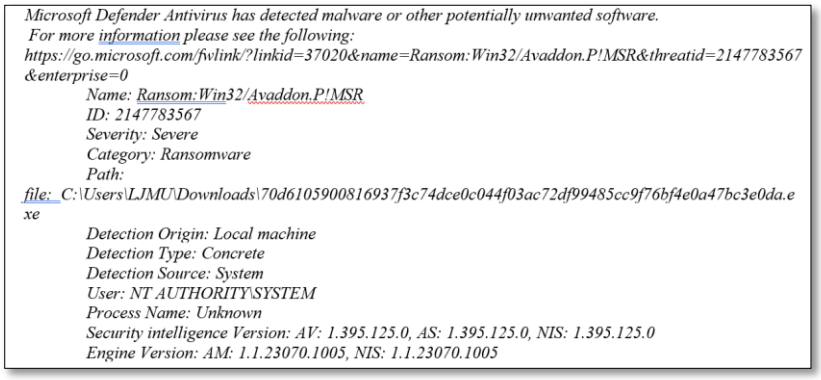

Figure S7. Windows Defender logs showing the detection of the Cerber ransomware.

Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
Name: Ransom:Win32/Ayaddon.P!MSR
Path: file:_C:\Users\LJMU\Downloads\70d6105900816937f3c74dce0c044f03ac72df99485cc9f76bf4e0a47bc3e0da.exe

Figure S8. The Windows Defender logs entries in the hardened environment indicating the detection of Cerber ransomware.

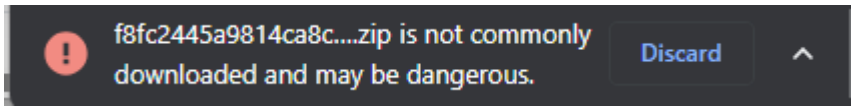

Figure S9. Chrome giving the user the option to allow executables.

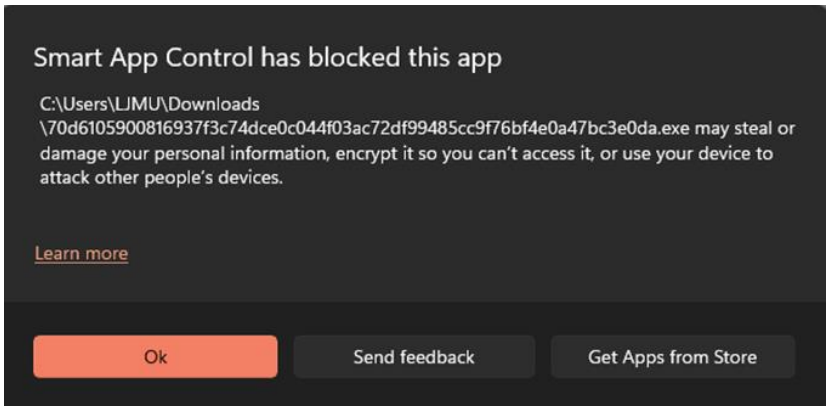

Figure S10. Smart App Control popup when attempting to run the Cerber executable.

Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Script/Sabsik.TE.A!ml&threatid=2147780197&enterprise=0
Name: Trojan:Script/Sabsik.TE.A!ml
ID: 2147780197
Severity: Severe
Category: Trojan
Path:
file:_C:\Users\LJMU\Downloads\f8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86.zip;
webfile:_C:\Users\LJMU\Downloads\f8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86.zip|https://bazaar.abuse.ch/download/f2c07b4b5860ca15a2e8/|pid:7360,ProcessStart:133361698951018348
Detection Origin: Internet
Detection Type: FastPath
Detection Source: Downloads and attachments
User: DESKTOP-35BSJ0S\LJMU
Process Name: Unknown
Security intelligence Version: AV: 1.395.125.0, AS: 1.395.125.0, NIS: 1.395.125.0
Engine Version: AM: 1.1.23070.1005, NIS: 1.1.23070.1005
==========
Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Script/Sabsik.TE.A!ml&threatid=2147780197&enterprise=0
Name: Trojan:Script/Sabsik.TE.A!ml
ID: 2147780197
Severity: Severe
Category: Trojan
Path:
file:_C:\Users\LJMU\Downloads\f8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86.zip;
webfile:_C:\Users\LJMU\Downloads\f8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86.zip|https://bazaar.abuse.ch/download/f2c07b4b5860ca15a2e8/|pid:7360,ProcessStart:133361698951018348

Figure S11. Windows Defender Logs showing the detection of Hive Ransomware in the Default testing environment.

Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Script/Sabsik.TE.A!ml&threatid=2147780197&enterprise=0
Name: Trojan:Script/Sabsik.TE.A!ml
ID: 2147780197
Severity: Severe
Category: Trojan
Path:
file:_C:\Users\LJMU\Downloads\f8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86.zip;
webfile:_C:\Users\LJMU\Downloads\f8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86.zip|https://bazaar.abuse.ch/download/f2c07b4b5860ca15a2e8/|pid:7360,ProcessStart:133361698951018348
Detection Origin: Internet
Detection Type: FastPath
Detection Source: Downloads and attachments
User: NT AUTHORITY\SYSTEM
Process Name: Unknown
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x00000000
Error description: The operation completed successfully.
Security intelligence Version: AV: 1.395.125.0, AS: 1.395.125.0, NIS: 1.395.125.0
Engine Version: AM: 1.1.23070.1005, NIS: 1.1.23070.1005

Figure S12. Windows Defender Logs showing action taken to protect local machine from Hive Ransomware.

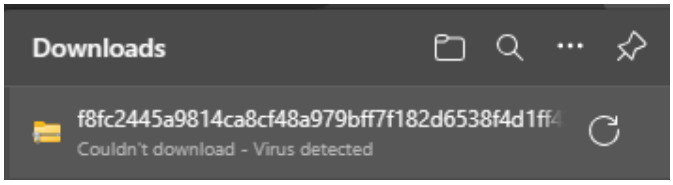

Figure S13. Hive Ransomware being detected in transit in Microsoft Edge browser.