

Internal Memorandum

To: Paula Alexander <hal.cio@seccdc.org>

CC: judge_29@seccdc.org

From: hal29@seccdc.org

Date: February 23, 2019

Memo #:004

Re: Malware Scan

**Hierarchical
Access
Limited
Corporation**



www.halcorp.biz

Greetings CIO,

As per your request, our team has downloaded and installed antivirus software on all of our systems. For our Windows systems, we have chosen to use Malwarebytes and Windows Defender and for our Linux systems ClamAV was our choice. A malware scan was performed on all systems and some potentially malicious items were found the Server 2008R2 system which have been quarantined pending further investigation by our team. In accordance with HAL company policy an incident response form will be completed for all identified threats. Below are screenshots showing the completed scans for each system.

Phantom:

```
----- SCAN SUMMARY -----
Known viruses: 3798335
Engine version: 0.98.7
Scanned directories: 1
Scanned files: 1014
Infected files: 0
Data scanned: 152.99 MB
Data read: 152.77 MB (ratio 1.00:1)
Time: 24.333 sec (0 m 24 s)
```

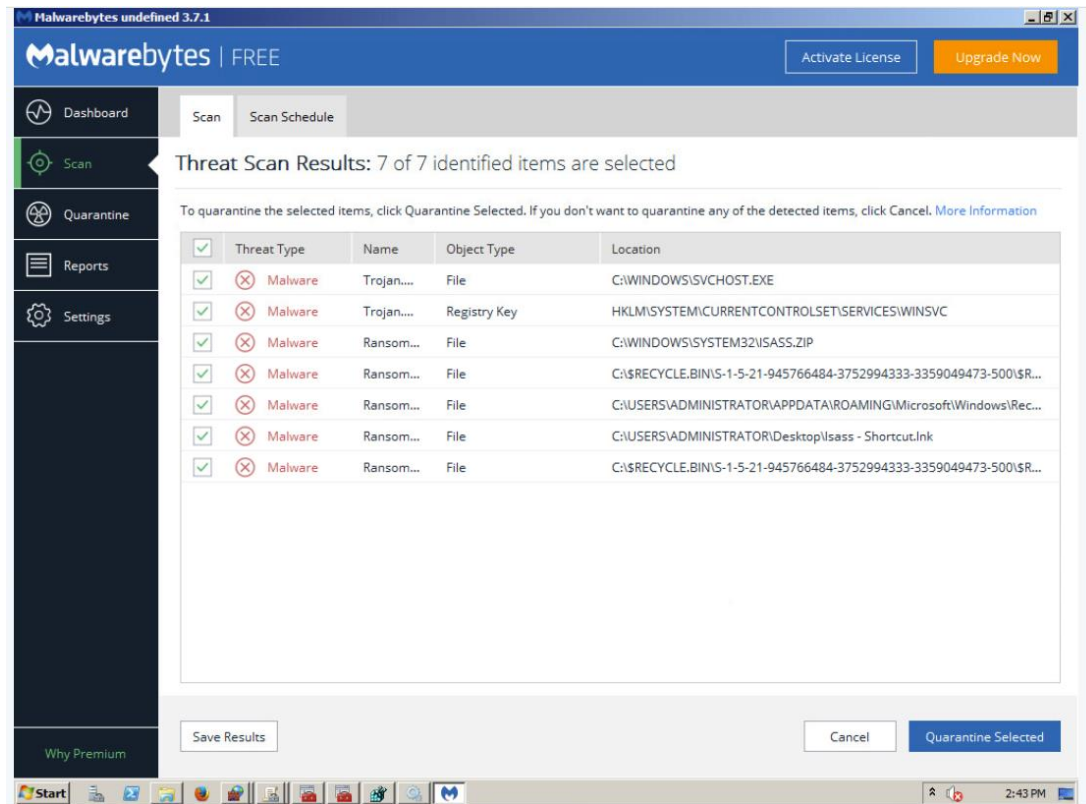
Debian 7.8:

```
----- SCAN SUMMARY -----  
Known viruses: 6817247  
Engine version: 0.99  
Scanned directories: 1  
Scanned files: 6  
Infected files: 0  
Data scanned: 2.32 MB  
Data read: 1.56 MB (ratio 1.49:1)  
Time: 21.392 sec (0 m 21 s)  
root@debian:~#
```

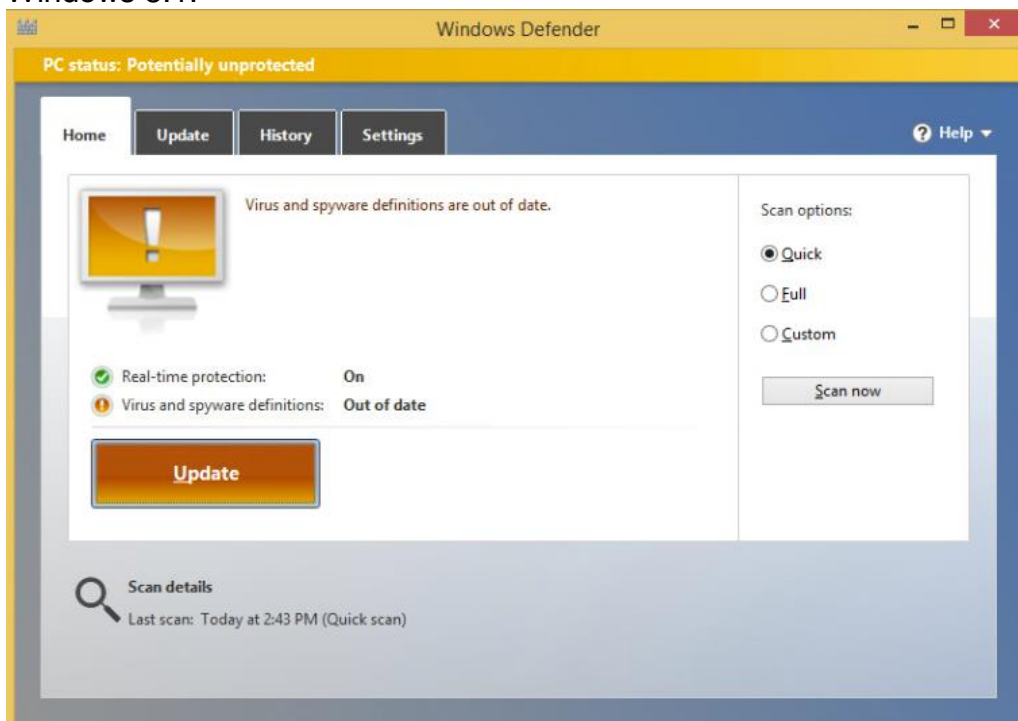
Ubuntu 12.04:

```
----- SCAN SUMMARY -----  
Known viruses: 3798335  
Engine version: 0.98.7  
Scanned directories: 1  
Scanned files: 110  
Infected files: 0  
Data scanned: 1.66 MB  
Data read: 0.98 MB (ratio 1.70:1)  
Time: 9.891 sec (0 m 9 s)
```

Windows Server 2008R2:



Windows 8.1:



Splunk:

```
----- SCAN SUMMARY -----  
Known viruses: 3798335  
Engine version: 0.98.7  
Scanned directories: 1  
Scanned files: 501  
Infected files: 0  
Data scanned: 51.18 MB  
Data read: 52.46 MB (ratio 0.98:1)  
Time: 15.090 sec (0 m 15 s)
```

CentOS 6.0:

```
----- SCAN SUMMARY -----  
Known viruses: 3798335  
Engine version: 0.98.7  
Scanned directories: 1  
Scanned files: 21  
Infected files: 0  
Data scanned: 31.88 MB  
Data read: 2.61 MB (ratio 12.20:1)  
Time: 13.956 sec (0 m 13 s)
```

Fedora 21:

```
----- SCAN SUMMARY -----  
Known viruses: 3798335  
Engine version: 0.98.7  
Scanned directories: 1  
Scanned files: 19  
Infected files: 0  
Data scanned: 31.88 MB  
Data read: 2.61 MB (ratio 12.20:1)  
Time: 14.114 sec (0 m 14 s)
```

Windows 10:

```
[ -All ]
Restores all the quarantined items based on name

[ -FilePath <filePath> ]
Restores quarantined item based on file path

[ -Path ]
Specify the path where the quarantined items will be
If not specified, the item will be restored to the original location
-AddDynamicSignature -Path <path>
Adds a Dynamic Signature specified by <path>

-ListAllDynamicSignatures
Lists SignatureSet ID's of all Dynamic Signatures added via MAPS and MPCMDRUN -AddDynamicSignature

-RemoveDynamicSignature -SignatureSetID <SignatureSetID>
Removes a Dynamic Signature specified by <SignatureSetID>

PS C:\Program Files\windows defender> .\MpCmdRun.exe -scan 1
Bad Command line - Command Line - Option should start with ' '

CmdTool: Failed with hr = 0x80070667. Check C:\Users\minion\
CmdTool: Invalid command line argument
PS C:\Program Files\windows defender> .\MpCmdRun.exe -scan
Bad Command line - Command Line - Option should start with ' '

CmdTool: Failed with hr = 0x80070667. Check C:\Users\minion\
CmdTool: Invalid command line argument
PS C:\Program Files\windows defender> .\MpCmdRun.exe -scan
Scan starting...
Scan finished.
PS C:\Program Files\windows defender> ne
```

```
PS C:\Windows\system32> Get-MpComputerStatus

AMEngineVersion           : 1.1.15700.8
AMProductVersion          : 4.18.1810.5
AMServiceEnabled          : True
AMServiceVersion          : 4.18.1810.5
AntispywareEnabled        : True
AntispywareSignatureAge   : 0
AntispywareSignatureLastUpdated : 2/23/2019 7:37:21 AM
AntispywareSignatureVersion : 1.287.616.0
AntivirusEnabled          : True
AntivirusSignatureAge     : 0
AntivirusSignatureLastUpdated : 2/23/2019 7:37:21 AM
AntivirusSignatureVersion : 1.287.616.0
BehaviorMonitorEnabled    : True
ComputerID                : 2F072E41-320B-422C-88B9-53B83DA09899
ComputerState             : 0
FullScanAge               : 4294967295
FullScanEndTime           : 
FullScanStartTime         : 
IoavProtectionEnabled     : True
LastFullScanSource        : 0
LastQuickScanSource       : 1
NISEnabled                : True
NISEngineVersion          : 1.1.15700.8
NISSignatureAge           : 0
NISSignatureLastUpdated   : 2/23/2019 7:37:21 AM
NISSignatureVersion       : 1.287.616.0
OnAccessProtectionEnabled : True
QuickScanAge              : 0
QuickScanEndTime          : 2/23/2019 3:08:03 PM
QuickScanStartTime        : 2/23/2019 2:52:19 PM
RealTimeProtectionEnabled : True
RealTimeScanDirection    : 0
PSComputerName            :
```

Regards,
Team 9

In accordance with HAL Memorandum policy, the entire header must be completed or the recipient may not acknowledge this as an official memorandum. Professional communications methods and decorum must be observed at all times.