# Windows Accelerator Pro Analysis

February 12, 2014

Andrew Kerr
me@andrewjkerr.com

Practical #1 | CIS4930

# Table of Contents

# Executive Summary

Windows Accelerator Pro attempts to pass itself off as an antivirus and is something I would consider scareware. Once the setup is initiated, the program installs itself inside the Application Data folder of that user, adds itself to the login sequence, causes certain Windows programs to not open, and scares the user by “scanning” their system and then saying that the user has malware on their system (spoiler: they don’t.)

The malware was packed, but, luckily, we were provided with the unpacker (rl!dePacker.) The programs imports seemed normal for an antivirus, but the registry edits were not. There was a lot of activity on printers for some reason as well as keys added for popular Windows utilities (such as msconfig) which would make it easy for the user to disable the malware.

There was a database file (results1.db) that was created in the Application Data folder on reboot, but there were only a lot of other file reads/directory traversals that were done by the malware. The malware reached out to the network to check the IP, get some files (presumably for a remote shell), and attempt to process payment.

The fact that programs stop working and the nagging pop ups are good host based indicators that the malware has been installed, but checking for connections to www.download.windowsupdate.com would be a good way for IPS to detect the malware.

# Static Analysis

1. Yes! The Entropy scan in PEiD reports that it is packed and the lack of imports in Dependency Walker both confirm the suspicion that the malware is indeed packed.
2. The headers report that the compilation date is January 1, 2014 at 15:18:18 UTC.
3. Windows GUI! In the IMAGE_OPTIONAL_HEADER, Subsystem is set to 'IMAGE_SUBSYSTEM_WINDOWS_GUI'.
4. All functions imported by the malware seem to be normal for an anti-virus software.
5. Running strings on the unpacked malware provided some interesting results:
    a. The following IP addresses: 128.115.62.35, 210.1.58.100, 64.51.8.67, 180.47.8.10, 87.23.232.71, 56.82.12.124, 130.89.78.134
    b. What looked like random warnings that AVs normally don't check for: "Microsoft Corporation keys", "Your bank account details", "Your passwords for sites"
    c. Warnings that look like it could potentially be nagware: "Warning! Your system is not cleaned yet!"
    d. "PayForm" shortly followed by "Internet Explorer_Server" could represent nagware that needs to be paid to be deactivated.
    e. I've never heard of an AV that checks for torrents... sounds like scareware as well: "Receiving this notification means that you have violated the copyright laws. Using Torrent for downloading movies and licensed software shall be prosecuted and you may be sued for cybercrime and breach of law  under the SOPA legislation."
    f. From the strings "http://checkip.dyndns.org/", "IP Address:", "</body>", it appears that the malware is getting the current IP address of the machine - possible for a remote shell.
    g. A quick Google search on some of the Strings that being with "?AVC" reveal that a lot of malware contains those strings.
    h. "InternetOpenA" and "ShellExecuteExW" are quite close together - could mean a remote shell.
    i. "PPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDIN

GPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADD" is quite the unusual string.

6. The malware appears to have the following sections:
    a. rsrc - appears to have data about the resources of the graphical user interface.
    b. 7676 - appears to contain a manifest of some sorts. Some Googling has led me to believe that the malware used side-by-side assembly.
    c. ap0x - appears to contain data about imports that the packer used. Looking at the unpacker, it seems that ap0x was the developer and this section of the PE looks to contain data used by the packer.
7. Resource hacker seems to show only an icon and then the data from the rsrc header. Doesn't look like anything other than just images.

# Dynamic Analysis

1. After installation, the machine immediately reboots to the AV running a "scan" that you cannot cancel. The AV window does not go away until the "Allow Unsafe Startup" option is clicked. After accessing the desktop, a lot of programs are not available (regshot, Task Manager, etc) under the guise that they were trying to communicate with the outside world. There were also numerous pop ups detecting uTorrent (which was not installed on the machine) and random network attempts.
2. FakeDNS got requests for the following:
    a. http://checkip.dynsdns.org
    b. http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt
    c. http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
3. Running a Wireshark capture on Remnux revealed that the malware attempted to connect to two different IP addresses to process the payment:
    a. 93.115.82.248
    b. 94.185.80.155
4. There were quite a few registry key changes for the following:
    a. Printers
    b. EventSystem
    c. Image File Execution Options: MpCmdRun.exe, MpUXSrv.exe, MSASCui.exe, msconfig.exe, msmpeng.exe, and msseces.exe were all given a value of "Debugger: "svchost.exe"" (important! Prevents these programs from running.)
    d. ShellNoRoam
    e. Added value for \winlogin\Shell to execute the "guard-xxxx.exe" (important! Causes the malware to start at login.)
5. Procmon picked up guard-xxxx.exe creating a result1.db file in the C:\Documents and Settings\Administrator\Application Data folder. Procmon also logged the malware traversing through the C drive and reading/executing various files.
6. The malicious process is called "guard-xxxx.exe" with xxxx being a random string of four characters. It appears that, on boot, guard-xxxx.exe is started and then, once the window is exited and the unsafe startup option is checked, explorer.exe is called from guard-xxxx.exe and then it goes on with the normal start up executables. Also, upon opening the payment form, mshta.exe is started by the malware to display the payment form.

# Indicators

Well, the first indicator that the malware is present on the system would be if the user were unable to open up any programs without a pop up in the lower right hand corner saying that the application was infected, but there are obviously other host based indicators. The malware edits several registry keys (the most obvious being the keys for msconfig and other Windows utilities.) The value pair “Debugger: svchost.exe” are added to those utilities effectively rendering them useless.

There is also a change of the login sequence. When the user logs in, guard-xxxx.exe will be executed and, when closed, then explorer.exe executes and the login sequence resumes. The creation of a “results1.db” file in the Application Data directory of the current user would also indicate that the Windows Accelerator Pro has been installed.

In the Strings, there are five IP addresses listed, but never connected to. However, the malware does try to connect to two different IP addresses when the user goes to pay for the “anti virus”: 93.115.82.248 and 94.185.80.155. The malware will also attempt to connect to checkip.dynsdns.org.

# Disinfection

- Remove guard-xxxx.exe in C:\Documents and Settings\User\Application Data to something else and restart. This will make sure that the malware does not execute upon reboot.
- Remove the database file in C:\Documents and Settings\User\Application Data.
- Remove the "Debugger" value in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\filename for MpCmdRun.exe, MpUXSrv.exe, MSASCui.exe, msconfig.exe, msmpeng.exe, and msseces.exe were all given a value of "Debugger: "svchost.exe""