PC Matic… Is It As Amazing As Seen on TV?

Carsten Eiram
Chief Research Officer
(Twitter: @CarstenEiram & @RiskBased)

Table of Contents

1. Introduction

PC Matic is a combined security and system performance optimization solution provided by PC Pitstop, LLC and claims to provide "*superior security protection over all security products, free or otherwise, on the market*"[1]. On the security side, the product offers anti-malware and anti-adware protection along with patch management by "*automatically [closing] security holes in commonly used free software.*"[1]

PC Pitstop, the developers of PC Matic, initially provided utilities for diagnosing and fine-tuning PCs. Later, the company branched into the security field. The company is well known for their advertisements on TV in major US metropolitan areas and particularly the quite exceptional claims being made about the capabilities of their security solutions.

The combination of these claims by the vendor and negative feedback on the Internet about the company and their products led to a third party suggesting we look into both the security of the PC Matic product and claims. This whitepaper details our findings including serious vulnerabilities discovered in PC Matic. It is intended to, hopefully, answer questions and concerns that existing and potential customers of PC Pitstop may have when evaluating, if PC Matic is the right security solution for them.

PC Pitstop is not affiliated with Risk Based Security nor are they a competitor. PC Pitstop did not request this assessment of their product and were not aware of it until contacted about the vulnerability findings.

Information about the disclosure process and timeline can be found in Appendix B. It should be noted that PC Pitstop's support team and security contact were very responsive and forthcoming.

2. Vulnerable Program Details

Details for tested products and versions:

Vendor:	PC Pitstop, LLC.
Product:	PC Matic
Version:	1.1.0.62

NOTE: Other versions than the one listed above are likely affected.

[1] http://www.pcmatic.com/

3. Summary

The following are some of the significant points uncovered by our analysis and discussed in details within this report.

PC Pitstop claims that PC Matic is better than the competition and the only security solution ever needed[2]. However, PC Matic was discovered to have many serious vulnerabilities. These allow a malicious website to retrieve various information from a user's system without the user's knowledge or even compromise it. Furthermore, an attacker able to intercept traffic from a user's system and PC Pitstop's servers (i.e. Man-in-the-Middle) can similarly gain knowledge of sensitive information or execute code on a user's system. In fact, the design of PC Matic is considered problematic and a redesign is suggested.

PC Pitstop states that PC Matic won first place in the April 2014 Virus Bulletin RAP test and detected more malware than the competition. While true that PC Matic blocked more malware, it became unstable and even collapsed several times during tests and also blocked many non-malicious files. According to Virus Bulletin, due to the instability and many false positives, PC Matic did not receive an award and thus not win first place (see section 6.4).

PC Pitstop claims that PC Matic protects systems running Windows XP, so they can safely be used even if "*abandoned*" by Microsoft. However, PC Matic is not able to properly protect these systems. In fact, we consider less secure with PC Matic installed, as websites can execute arbitrary code on the systems due to vulnerabilities in PC Matic itself (see section 5.1).

PC Pitstop claims that PC Matic closes security holes. However, the patch management capabilities were determined to be limited at best. Commonly used software is not supported while some supported products were not properly listed as requiring updates. Furthermore, many supported products already provide their own update features that are better than downloading the updates unsafely via PC Matic. PC Matic also failed to warn of missing critical security updates for the underlying Windows 7 OS (see section 6.2).

PC Pitstop claims that PC Matic is 100% made in USA and that they do not believe in outsourcing. While the intent of their statement may refer to internally developed code, a significant part of the functionality provided by PC Matic comes from third party components not developed internally at PC Pitstop. Some of these components even contain code that is very likely not developed within the USA. PC Matic also relies on a threat engine where some development and research potentially may occur outside the USA (see section 6.3).

[2] http://www.pcmatic.com/

4. Design

The first step of assessing a product is to understand which components it is comprised of, what functionality these provide, and how they work. By default, PC Matic installs components to "`%ProgramFiles%\PCPitstop\`" and subdirectories, and the more relevant ones are:

PCPitstopScheduleService.exe

This is a service used to run scheduled scans on the system. Scans are performed by running: "`wscript //B checkschedule.wsf`". During installation, the "PCPitstopSVC" account, which is part of the "Administrator" group, is created on the system. The service runs with this account's permissions. The account is (usually[3]) hidden via the "`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList`" registry key and does not permit interactive login.

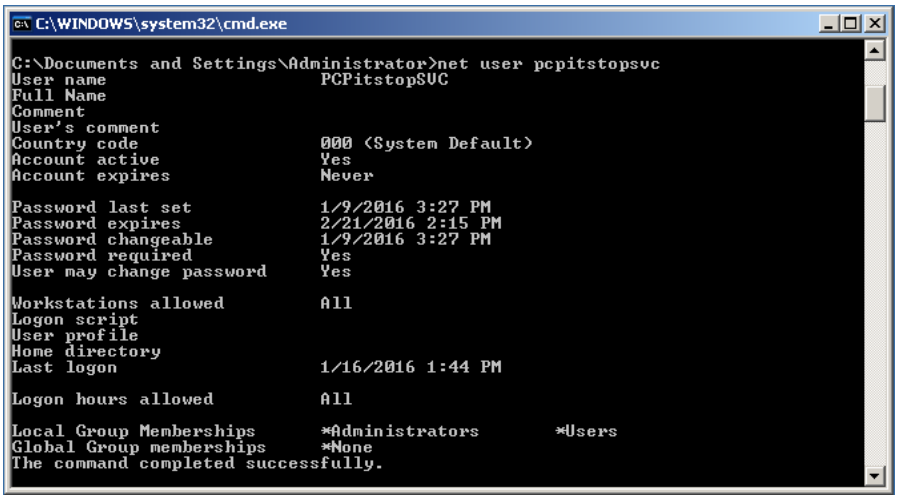

Fig 1: Details for the created PCPitstopSVC account

checkschedule.wsf

This is a Windows Script File (WSF) that e.g. `PCPitstopScheduleService.exe` runs via Microsoft Windows Script Host. The script just instantiates the MSXML2.ServerXMLHTTP COM object and retrieves http://www.pcpitstop.com/Nirvana/scheduledscancheckpack.js, which contains the actual code being executed.

scan.wsf

This Windows Script File is similar to `checkschedule.wsf`, but runs code from http://www.pcpitstop.com/Nirvana/scheduledscanpack.js.

[3] http://forums.pcpitstop.com/index.php?/topic/205524-pcpitstop-svc-is-showing-as-a-user-at-login/

PCMatic.exe

This is the main executable, but basically just acts as a frame relying on the Trident engine (Internet Explorer) to display web content. The homepage is a local file named `Splash.html`, which loads http://utilities.pcpitstop.com/Nirvana/default.htm. Most content displayed and interacted with is from the utilities.pcpitstop.com subdomain.

Reminder-PCMatic.exe

This executable is basically the same as `PCMatic.exe`, but runs on startup and uses a different configuration file (`Reminder-PCMatic.ini`). The homepage is not the local `Splash.html` file but http://utilities.pcpitstop.com/Nirvana/reminder.htm.

InfoCenter.exe

This is another executable set to run on startup. Depending on the configuration, a scheduler may run `checkschedule.wsf` and `scan.wsf`.

PCMaticAdBlockerEngine.exe / PCMaticAdBlocker.dll

This is the ad-blocking component for IE and is based on Adblock Plus[4]. It is unclear how many changes, if any, were made to the original code, which is an open-source project copyrighted by Eyeo GmbH.

PC Matic Chrome Extension

This is the ad-blocking component for Google Chrome and has extension id *okmhneofinpilciglijihehjpaegledb*. According to chrome web store statistics there are 30,200 users. The extension is branded as “PC Matic Ad Blocker, an extension of uBlock”, but comparing it to the upstream uBlock extension, it’s largely the same as commit 8d0ce5f9d52adee135b2133bfd1ea90f2d471c1f[5] from June 1st, 2015 and primarily just rebranded.

PC Matic Firefox Plugin

This ad-blocking component for Firefox is also based on uBlock. It was not further reviewed.

pcmatic.cab

As previously described, content displayed in the GUI is primarily loaded from the http://utilities.pcpitstop.com/ website. In order for the website to control the actions performed by the PC Matic executable, it requests to install some ActiveX controls and related libraries when started for the first time. These ActiveX controls (`pcpitstop.dll`, `DiskMD3Ctrl.dll`, `PCPitstop2.dll`, `PCPitstop3D.dll`, and `PCPitstopAntivirus2.dll`) are required for the PC Matic software to operate. The ActiveX controls are marked safe-for-scripting and not site-locked, meaning they can be instantiated in Internet Explorer and scripted to by any website.

[4] https://adblockplus.org/
[5] https://github.com/chrisaljoudi/uBlock/tree/8d0ce5f9d52adee135b2133bfd1ea90f2d471c1f

5. Vulnerability Details

5.1. Unsafe Methods Supported By Installed ActiveX Controls

The bundle of ActiveX controls installed on the user's system provide various insecure methods and properties. The following is a sample of some of these methods, which can be called by any website without restrictions.

ProgID	Method / Property	Functionality
PCPitstop3D.Perf.1	TraceFileOpen()[6]	Overwrite files with trace output (see next method)
PCPitstop3D.Perf.1	Trace()[3]	Write user-controlled content to specified trace file
PCPitStop.disk.1	DirSizeKB()	Enumerate directories on the user's system
PCPitStop.sys.1	WindowsVersion()	Obtain various information about the OS
PCPitstop2.Exam.1	KillProcess()	Terminates a specified process
PCPitstop2.Exam.1	CopyFile()	Copy any file to/from any location (incl. external)
PCPitstop2.Exam.1	RunExecuteable()[7]	Run an executable on the system
PCPitstop2.Exam.1	HTTPDownload()	Download arbitrary file to system
PCPitstop2.Exam.1	InstallDriver()	Create process based on supplied arguments
PCPitstop2.Exam.1	DeviceDriverInstallArguments	Supply command line arguments for InstallDriver()
PCPitstop2.Exam.1	ElevatePermissions()	Grant 'SeBackupPrivilege' to current process
PCPitstop2.Exam.1	IsRunning()	Enumerate running processes

Fig. 2: Subset of unsafe ActiveX control methods

It should be noted that these methods likely won't work in later versions of Internet Explorer when running in Protected Mode. Internet Explorer on Windows XP systems (see also the "6.1 Supports And Protects Windows XP" section) has no such restrictions. This allows any website to use the listed methods to e.g. kill processes, retrieve files from the user's system, and even plant and execute files to run arbitrary code.

5.2. Social Engineering To Use Restricted ActiveX Control Properties / Methods

For most methods and properties provided by the ActiveX controls in `PCPitstop.dll`, the developers of PC Matic did - contrary to the methods mentioned above - actually implement a security check. This suggests they were aware that the functionality provided should be considered unsafe. These restricted methods work even when IE is running in Protected Mode and allow e.g. retrieving system information including CPU, disks, OS, and BIOS details, list installed applications and running processes, IE cookies, read registry keys etc.

[6] Also supported by the PCPitstopAntiVirus.AntiVirus.1 ActiveX control in PCPitstopAntivirus2.dll
[7] sic

To warn users when a website tries to use these unsafe methods or properties, a check is implemented at the beginning of many of the functions to display a message box with a warning. The default message box informs the user that the PC Pitstop utility is about to gather data from the system and that users should only proceed by pressing “OK” if on the PC Pitstop website.

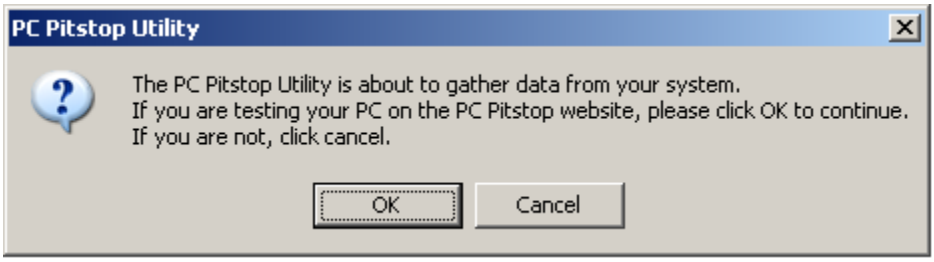

Fig. 3: Default message box when using restricted property or method

Relying on users to determine whether or not it is safe to proceed is bad practice; even more so when considering the PC Matic target audience. The warning message is quite descriptive, though, and would likely cause many users to click “Cancel” if displayed by a random website.

This leads to the `Enable2()` method provided by the PCPitStop.sys.1 ActiveX control in `PCPitstop.dll`. This method does not display a warning when called and is defined as:

```
long Enable2([in] short i);
```

The method allows any website to control which of the six warning messages is displayed. Some of these do not warn users as well as the default warning message and may even encourage users to permit unsafe code to run. This significantly increases the risk of users clicking the “OK” button.

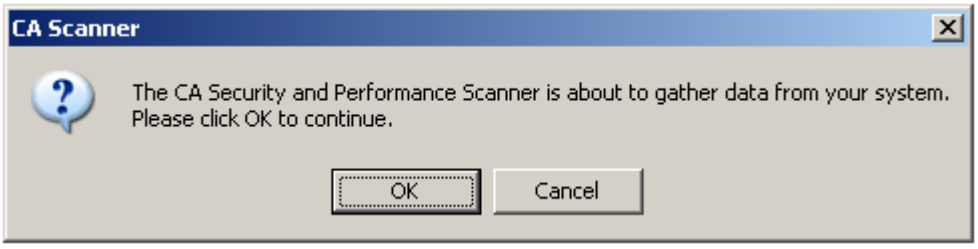

Fig. 4: Message box that users are more likely to accept, as it instructs them to click “OK”

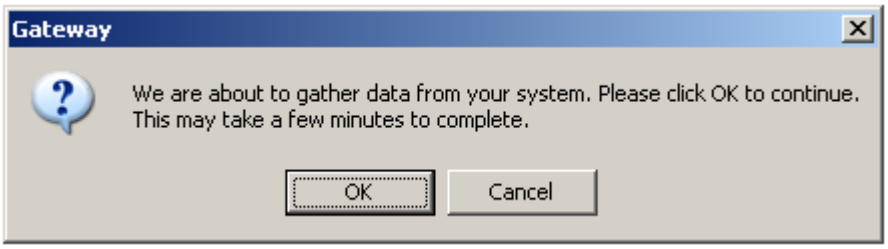

Fig. 5: Message box that users are more likely to accept, as it instructs them to click “OK”

Once a user clicks “OK”, a malicious website can use any of the unsafe, restricted properties and methods without further user interaction or warnings.

5.3. Bypass of Restricted ActiveX Control Properties / Methods Warning Dialog

Instead of displaying alternative warnings to increase the likelihood of users accepting to run unsafe code, attackers can just bypass the whole warning dialog altogether.

The PCPitStop.sys.1 ActiveX control also provides such a feature via the `Confirm3()` method. No warning is displayed when calling the method defined as:

```
long Confirm3(
                [in] BSTR Company,
                [in] BSTR Product,
                BSTR Confirmation);
```

As long as the method is supplied three random strings, it suppresses the warning messages for any unsafe methods and properties. This allows a website to use unsafe, restricted methods and properties without user interaction, knowledge, or approval during the current browser session. As previously mentioned, this allows gathering a lot of sensitive system information.

5.4. Unsafe Restricted Methods / Properties Site Restriction Bypass

The PCPitstop2.Exam.1 ActiveX control provided by `PCPitstop2.dll` also support various unsafe methods and properties. Similar to the ActiveX controls in `PCPitstop.dll`, many of these have a check implemented to prevent unauthorized use. The check here is different, as it does not rely on users making the decision, but instead checks the domain that instantiates the ActiveX control. The check only permits use of restricted functionality if the domain is “pcpitstop.com”, “local”, or “localhost” (or the URI handler is “file://”).

The concern with such a check is that a cross-site scripting (XSS) vulnerability on any web pages hosted on the pcpitstop.com domain would allow attackers to bypass it. Furthermore, the check permits using HTTP, which allows anyone capable of intercepting traffic to manipulate the commands being sent from the PC Pitstop servers.

5.5. Man-in-the-Middle System Compromise

Many components of PC Matic communicate with PC Pitstop servers over HTTP, as briefly covered when describing the more relevant components making up PC Matic in the "4. Design" section.

Web content from the utilities.pcpitstop.com website displayed by `PCMatic.exe` is loaded over HTTP. As this executable relies on the aforementioned ActiveX controls to perform sensitive actions on a user's system, and pcpitstop.com is a domain trusted to use restricted functionality, a MitM (Man-in-the-Middle) attacker or similar may perform arbitrary administrative actions on the user's system. Furthermore, a lot of sensitive information e.g. various system information, drivers and services installed, and running processes gathered from a user's system is also sent to the PC Pitstop web server over HTTP. Content is similarly loaded unsafely by `Reminder-PCMatic.exe`.

The `PCPitstopScheduleService.exe` service running with administrative privileges and other executables run the `checkschedule.wsf` and `scan.wsf` Windows Scripting Host files. These execute external code also accessed over HTTP from http://www.pcpitstop.com/Nirvana/scheduledscancheckpack.js and http://www.pcpitstop.com/Nirvana/scheduledscanpack.js. This allows a MitM attacker to execute arbitrary code with administrative privileges on a user's system.

Even if the code was accessed over HTTPS, the code being executed from the web server also contains references to web content retrieved over HTTP. As examples, the following functions in http://www.pcpitstop.com/Nirvana/scheduledscancheckpack.js call the `DownloadFile()`[8] function or similar to download content insecurely over HTTP and without checking signatures.

Function	Download
runServiceAsAdmin()	http://files.pcpitstop.com/cab/ntrights.exe
updateActiveX()	http://files.pcpitstop.com/cab/updateCab.zip
updateActiveX()	http://files.pcpitstop.com/cab/pcmatic_cab_md5.txt
downloadAndRunDotNetFrameworkInstaller()	http://www.pcpitstop.com/utilities/dotNetFx40_Client_x86_x64.exe
updatePushControllerScript()	http://files.pcpitstop.com/cab/PushController.txt

Fig. 6: Functions downloading content insecurely

MD5s are also downloaded insecurely from http://utilities.pcpitstop.com/Nirvana/pcpitstopmd5s.txt.

[8] Please see Appendix C for the function code

5.6. Logging of Password Information

The scheduler logs events to world-readable checkschedule log files. On Windows XP systems, these are found at `C:\Documents and Settings\All Users\Application Data\PCPitstop\` while at `C:\ProgramData\PCPitstop\` on later OS versions.

One of the events logged is when the administrative 'PCPitstopSVC' user is created. While a randomly generated 12 character string is set as password, it is disclosed in the log file in an entry similar to: "`cmd /c net user PCPitstopSVC MhXFbmM7iOK8 /add`". Any local user can read the file to gain knowledge of the password. As previously mentioned, the account is usually not allowing interactive logins, but there have been cases[9] where it accidentally was permitted. In such cases, any local user can gain administrative privileges on the system.

6. Other Concerns

Apart from the uncovered vulnerabilities described in the previous section "5. Vulnerability Details", we also examined some of the claims made by PC Pitstop concerning the capabilities of PC Matic. These findings are listed in this section.

6.1. Supports And Protects Windows XP

March 2014, PC Pitstop published advertisements[10,11] for PC Matic about how it protects even Windows XP systems that Microsoft "*abandoned*" by no longer providing security patches[12]. Instead of upgrading to a more modern version of Windows, which has better security features, PC Matic is claimed to offer protection for Windows XP systems that can safely be used even after Microsoft stopped releasing security updates.

As detailed in the "5.1 Unsafe Methods Supported By Installed ActiveX Controls" section, PC Matic installs safe-for-scripting ActiveX controls that provide unsafe methods, which should not be supported by "safe" ActiveX controls. Internet Explorer on Windows XP systems is more permissive and allows ActiveX controls to perform sensitive actions that later versions of IE running in Protected Mode do not. This means that on Windows XP systems with PC Matic installed, any visited website can perform highly sensitive actions on the user's system without the user's knowledge including placing files on the system and executing commands to compromise it.

Based on this and other parts of this analysis, it is clear that not only are the claims of PC Matic safely protecting Windows XP systems exaggerated, but we consider Windows XP systems with

[9] http://forums.pcpitstop.com/index.php?/topic/205524-pcpitstop-svc-is-showing-as-a-user-at-login/
[10] https://www.youtube.com/watch?v=oPK-R2rCJFM
[11] https://www.youtube.com/watch?v=rYSOdNSaz0M (if you want the UK version)
[12] http://techtalk.pcpitstop.com/2014/03/10/pc-matic-continues-support-xp/

PC Matic installed as less secure than systems without. Windows XP is outdated and no security solution is able to adequately protect users, who should instead migrate to a newer, supported version of Windows. It is recommended to not use PC Matic to protect Windows XP systems.

6.2. Closes Security Holes

PC Matic is claimed to close security holes in common software like Java and Flash Player[13]. Basically, PC Pitstop promises that PC Matic contains patch management capabilities to ensure installed software with known security holes is updated to the latest secure version if one exists. Such a feature can be quite useful, as it helps to reduce the risk of a user's system being compromised by ensuring that fixes are installed automatically as soon as they are available.

The following should in no way be considered a comprehensive test of the implemented patch management capability, but as the results show, no such test is really needed. Even a cursory test clearly suggests that the patch management capabilities should be considered limited at best.

The approach used was to download older versions of software known to contain vulnerabilities with fixes available based on our own Vulnerability Intelligence solution, VulnDB[14]. The software was chosen based on our knowledge of prevalent software as well as consulting a list of the most popular Windows downloads at http://download.cnet.com/most-popular-software/. This may not necessarily reflect the most common software used by PC Matic users, but PC Pitstop does suggest that all commonly used software is covered.

A table of tested software, vulnerable versions, and test results can be found below:

Software	Version	Detected?
Apple Quicktime	7.7.4 (1680.86)	YES
Mozilla Firefox	43.0.1	NO
Oracle Java	8u51	YES
Adobe Reader	11.0.10	YES
VLC media player	2.1.3	NO
IrfanView	4.32	NO

Fig. 7: Patch management capability test results

The test results confirmed that PC Matic indeed does provide patch management for Oracle Java and Adobe Flash Player as advertised. Other software often installed on Windows systems does not appear to be fully covered, though.

It was also found that the signature for Mozilla Firefox, a popular browser, was outdated: PC Matic suggested that the installed version 43.0.1 was the latest available. However,

[13] https://youtu.be/oPK-R2rCJFM?t=46
[14] https://vulndb.cyberriskanalytics.com/

vulnerabilities were reported in this version on December 22, 2015 and also in the following version 43.0.2 on January 26th, 2016[15]. The test was on January 31, 2016 when the latest version was 44.

Finally, the test was conducted on a Windows 7 32-bit system that had not been updated since November 2015 i.e. not patched in two months. PC Matic failed to warn about the missing OS security updates. In fact, the most alarming issue is that the software does seemingly not even check for missing OS security updates.

Further evaluation of the patch management capabilities by monitoring the traffic sent to utilities.pcpitstop.com showed an HTTP POST request[16] to /Nirvana/SaveSecurityTests.asp that seems to disclose a complete list of supported products along with information on whether or not the product was installed. If so, PC Matic only provides patch management for the following 24 products at the time of writing:

1. 7-Zip
2. Adobe AIR
3. Adobe Flash Player
4. Adobe Reader / Adobe Reader XI
5. Apple iTunes
6. Apple Quicktime
7. Apple Safari
8. FileZilla
9. Foxit Reader
10. Google Chrome
11. Mozilla Firefox
12. Mozilla Seamonkey
13. Mozilla Thunderbird
14. OpenOffice
15. Opera
16. Oracle Java
17. PC Matic
18. PDF Creator
19. PDF XChange Viewer
20. Real Player
21. Skype
22. Winamp
23. WinRAR
24. Wireshark

[15] https://www.mozilla.org/en-US/security/known-vulnerabilities/firefox/
[16] Please see Appendix A for a snippet of the request details

Many of these products already provide their own automatic update capabilities or similar. This reduces the value of the PC Matic patch functionality. Also, updated versions seem to be installed from software.pcpitstop.com over HTTP and not the vendors' own websites. The update for Apple Quicktime was e.g. downloaded from `http://software.pcpitstop.com/2014/10/QuickTimeUpdater_7.76.80.95.exe`, making it susceptible to MitM attacks.

It is clear from these results that this is an inferior patch management solution and not something users should rely on, as the value provided is insignificant.

6.3. Only Developed In America

In many of the advertisements on TV and PC Pitstop's Youtube channel claims are made that PC Matic is an all American product[17,18,19,20,21]. Even when questioned recently (January 21st, 2016) on his personal blog if any components were not developed in USA[22], the CEO, Rob Cheng, answered: "*We do everything internally including our software development. The only thing that we outsource is payroll.*"[23]. From the advertisements and that response, it is very clear that not only does PC Pitstop and its CEO claim that all of their own code is internally developed in USA, but that it is also the case for any components used in the products.

While the claims may be true for PC Pitstop's own code in their products, we have already established that PC Matic is a suite of utilities where some definitely were not developed internally at PC Pitstop. Furthermore, some of them were not developed in the USA.

As example, the ad-blocking capability is a rebranded version of uBlock. This code is currently maintained by Chris Aljoudi of USA, but the codebase was forked from HTTP Switchboard by Raymond Hill of Canada.[24] We've similarly established that the ad-blocking component for IE is based on Adblock Plus, which is primarily maintained by a German company.

The threat engine is VIPRE. This was developed by Sunbelt Software, which was later acquired by GFI Software. Eventually, VIPRE spun off as ThreatTrack, which has two offices in USA, but also offices in Spain, Philippines, and Australia[25]. This means that ThreatTrack may have some development and threat research in countries outside USA e.g. Philippines, which specifically is a country that PC Pitstop criticizes their competition for outsourcing R&D to "*in their blind pursuit*

[17] https://www.youtube.com/watch?v=Xl0qdCBYB8g
[18] https://www.youtube.com/watch?v=nt8cOKZz8hQ
[19] https://youtu.be/306FmHpf8HI?t=57
[20] https://www.youtube.com/watch?v=3Ojsw6VaJZM
[21] https://www.youtube.com/watch?v=jRLbL0i_9NY
[22] http://chengrob.com/blog/2016/01/new-years-2016/#comment-288665
[23] http://chengrob.com/blog/2016/01/new-years-2016/#comment-288667
[24] https://en.wikipedia.org/wiki/UBlock
[25] http://www.threattracksecurity.com/company.aspx

of profits"[26].

We find that the claim of PC Matic being 100% made in America is misleading. While the code developed internally at PC Pitstop may be 100% developed in-house in the USA, PC Matic is comprised of quite a few third party components that are not. Based on the findings, it could lead one to believe that such statements are merely marketing claims trying to appeal to "patriot" customers within the USA.

6.4. Best Proactive Score Ever on Virus Bulletin's RAP Test

PC Pitstop boasts in advertisements about the impressive results generated by PC Matic in the April 2014 Virus Bulletin RAP test[27] due to their whitelisting approach. While PC Pitstop claims that they "*detected*" more malware than competitors, it is important to note the big difference between actually detecting malware vs. just blocking it from running based on a whitelist approach. In fact, while PC Matic did manage to block more malware than the competition, PC Pitstop does not share in their TV ads[28] that PC Matic overall failed the RAP test due to a whopping 1,065 false positives[29] i.e. detecting a lot of legitimate programs as malicious.

The comments from the VB team further reported "*the product collapsing several times under the pressure of dealing with lots of files, even clean ones, and shutting down protection completely several times during the test process*". The whitelisting was reportedly *"causing alerts on a large number of samples in our clean sets, including components of software from HP, IBM, Microsoft, ATI, Lenovo, Samsung, Lexmark, SAP, Sony and Oracle, as well as a raft of others from smaller software houses and open-source projects*"[30].

These problems resulted in PC Matic failing the test and not receiving a VB100 award that month. PC Pitstop's CEO claims that "*PC Matic won first place in the Virus Bulletin RAP test*"[31], but we were unable to confirm that claim.

6.5. Protection From Viruses That Others Don't Detect

PC Matic is said to provide "*superior protection from modern viruses that others don't detect*"[32]. Reviewing the product, it does not seem to use a unique, internally developed malware scanning engine. Instead, it relies on VIPRE from ThreatTrack[33]. Claims that PC Matic can protect against malware that others can't detect when using an OEM scanning engine seem questionable.

[26] https://youtu.be/mXAg1f1BhoY?t=11
[27] http://techtalk.pcpitstop.com/2014/07/31/pc-matic-breaks-virus-detection-record-virus-bulletins-rap-test/
[28] https://www.youtube.com/watch?v=CWJj_qwxmsE
[29] https://www.virusbtn.com/vb100/archive/test?id=199
[30] https://www.virusbtn.com/virusbulletin/archive/2014/04/vb201404-comparative#id3161066
[31] https://www.youtube.com/watch?v=CWJj_qwxmsE
[32] https://youtu.be/oPK-R2rCJFM?t=37
[33] http://www.threattracksecurity.com/

The claim is most likely tied to their use of an internally developed whitelisting approach of applications and not some superior technology. As commented in the "6.4 Best Proactive Score Ever on Virus Bulletin's RAP Test" section above, their whitelisting approach has significant flaws and leads to many false positives.

This underlines the main problem with such an approach: While it is not feasible to block all threats using a blacklist, it is similarly not possible to permit all legitimate applications using a whitelist. This results in many legitimate applications not being able to run, which makes the whitelist approach unusable except for systems with only the most common software installed. A whitelist is such a simple and cheap approach that if it indeed was superior, all modern AV solutions would be using it. Instead, these rely on a combination of blacklists and a lot of other more advanced detection features.

This makes it seem a bit ironic when PC Pitstop refers to modern day security software as "*archaic and useless*"[34], yet their solution relies on other components for threat detection and adware blocking. Only the PC optimization feature and whitelist approach seems to be fully internally developed.

6.6. Blocks ALL Modern Threats

In one of the many advertisements, PC Pitstop claims that PC Matic protects against all modern threats including ransomware, APT, and polymorphic viruses[35]. This claim is questionable, as no security solution can effectively block all modern threats. The capabilities to protect against such threats also seem to primarily rely on the used VIPRE threat engine. In fact, considering the uncovered vulnerabilities and our analysis, PC Matic currently makes it easy for advanced attackers to compromise a system on which it is installed.

6.7. Bad Reviews

When searching for reviews of PC Matic, it is easy to find a lot of negative feedback[36,37,38] with many calling it a scam. The CEO, Rob Cheng, is often active in those threads[39] and makes a significant effort to explain to people that PC Pitstop is a legitimate company offering legitimate products that are better than the competition.

[34] https://www.youtube.com/watch?v=mXAg1f1BhoY
[35] https://youtu.be/306FmHpf8HI?t=27
[36] http://www.complaintslist.com/computer-software/pc-matic/
[37] http://www.bleepingcomputer.com/forums/t/523305/pc-matic-whats-the-good-or-bad-word/
[38] http://reviewopedia.com/pc-matic-reviews
[39] http://www.bleepingcomputer.com/forums/t/523305/pc-matic-whats-the-good-or-bad-word/page-5#entry3902559

On top of this, PC Matic receives some very contradictory reviews on e.g. Amazon[40] where out of currently 288 reviews, 37% are 1 star while the majority of the other reviews are in the complete opposite end of the spectrum with 18% as 4 star and 42% as 5 star. It is always questionable when a product receives reviews like this.

It should be noted that the "PC Matic - 5 PCs" option on Amazon currently has 853 reviews with most being 5 stars (82%) and 4 stars (12%)[41]. It is unclear why there is such a significant discrepancy between the reviews of the two product options. Not surprisingly, but perhaps suspiciously, this is also the page that is referenced by the PC Matic web page[42] when advertising how "*PC Matic has a tremendous 4.6 out of 5 star rating on Amazon!*". The former product page on Amazon with the questionable mix of very bad and very good reviews is not mentioned at all.

6.8. YouTube Channel Restricts Comments

The vendor of PC Matic, PC Pitstop, operates the YouTube channel: *pcpitstopvideo*. The channel mainly contains advertisements as shown on TV. At the time of writing there are 113 videos published since November 2006.

One thing that stands out is that PC Pitstop restricts user comments. Of the 113 available videos on the Youtube channel only 30 have comments enabled. Those are primarily older videos from 2006 to 2010 after which restriction of comments seems to have become the norm. Only a few newer videos have comments enabled, which seems accidental.

A common red flag for questionable companies with YouTube channels is that they do not permit users to comment on their videos. While there may be valid reasons for a company restricting video comments, in many cases it is a strong indication that they are worried about what customers / users might write. Any company trying to restrict public customer feedback should be approached carefully by would-be customers. Indeed one of the newer videos with comments enabled does contain negative feedback, calling the PC Matic product a "*scam*"[43].

[40] http://www.amazon.com/PC-Pitstop-LLC-PCM-102-Matic/product-reviews/B0046ZLW1G/ref=cm_cr_pr_viewopt_srt?sortBy=recent
[41] http://www.amazon.com/PC-Matic-5-PCs-Download/product-reviews/B004KPKSRQ/ref=cm_cr_pr_viewopt_srt?ie=UTF8&showViewpoints=1&sortBy=recent
[42] http://www.pcmatic.com/
[43] https://www.youtube.com/watch?v=hq7QTbhEXjc

7. Conclusion

The analysis uncovered critical vulnerabilities in PC Matic. A cursory review of the code indicates that from a code maturity perspective, PC Pitstop did make some effort to ensure the software is not riddled with basic vulnerabilities like classic buffer overflows. The uncovered vulnerabilities were primarily caused by very bad design decisions. In fairness, many awful design decisions and vulnerabilities have been covered in so-called security products throughout the years - even in products from major vendors. Lately, a slew of critical vulnerabilities have been reported in security products from vendors that many consider reputable.

One major concern with PC Matic in its current form is that even if PC Pitstop addresses all the reported vulnerabilities, the base design of having executables running with Administrator privileges while executing code from web pages is problematic. The PC Pitstop web server becomes a very critical point of failure. Should attackers be able to successfully compromise it, the impact would not be limited to the web server, but allow attackers to automatically take full control of all client systems with PC Matic installed. The mass impact would be disastrous. Home users and businesses using the product have to have considerable faith in PC Pitstop being able to secure the company's web server. With no defense-in-depth precautions this is a significant concern, and our advice is a complete redesign of PC Matic.

On WinXP systems, which PC matic is still advertised to support, the security impact is even worse. Any website can currently extract sensitive system information and run arbitrary code without a user's knowledge if visiting a malicious website.

One major question raised by some customers and other people is whether or not PC Matic should be considered a scam. Based on this analysis, we believe that it would be unfair to categorize PC Matic as a scam[44]. The product does provide various security features as advertised, and PC Pitstop also seems to be a legitimate company and even had a very responsive support team and security contact.

The more important question this report attempted to address is how good a security product PC Matic really is. Does it add more security than security concerns when installed, and how comprehensive and valuable are the provided security features? We do generally view security products critically, as many often introduce a wider attack surface than they protect. We leave the conclusion up to the individual users, but it is safe to say that PC Matic is certainly not the panacea that the PC Pitstop marketing department tries to advertise it as. It is clear that either they are unaware of the issues or both the CEO and marketing team are overselling and overstating the capabilities of PC Matic. One may even get the impression that the marketing seems to "prey" on the uninformed by targeting a demographic that is not considered PC savvy via TV advertisement and a similar style of marketing.

[44] http://www.merriam-webster.com/dictionary/scam

As always, we recommend to be critical of which software is installed on systems, and even if a security product is legitimate and not a scam, it may still not do wonders for your computer's security state. At least we can say: "*No, PC Matic is not as amazing as advertised on TV*"; many so-called security products rarely are.

Most consumers and businesses are not in position to verify themselves if a product is performing the way that it has been advertised. We continue to focus on providing easy to understand ratings about vendors, how they protect customer data and the security of software products they produce.

8. About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

8.1. Company History

Risk Based Security, Inc. (RBS) was established to support organizations with the technology to turn security data into actionable information and a competitive advantage. We do so by enhancing the research available and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

8.2. Solutions

VulnDB - Vulnerability intelligence, alerting, and third party library tracking based on the largest and most comprehensive vulnerability database. Available as feature-rich SaaS portal or powerful API. Vendor evaluations including our Vulnerability Timeline and Exposure Metrics (VTEM) as well as Cost of Ownership ratings.

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss. It also allows monitoring of domains for data breaches and leaked credentials as well as implementing a continuous vendor management program with our PreBreach data.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Vulnerability Assessments (VA) and Pentesting - Regularly scheduled VAs and pentests help an organization identify weaknesses before the bad guys do. Managing the most comprehensive VDB puts us in a unique position to offer comprehensive assessments, combining the latest in scanning technology and our own data. Detailed and actionable reports are provided in a clear and easy to understand language.

Security Development Lifecycle (SDL) - Consulting, auditing, and verification specialized in breaking code, which in turn greatly increases the security of products.

Appendix A: Part of Data Posted to /Nirvana/SaveSecurityTests.asp

VersionUpdates%22%3A%5B%7B%22Name%22%3A%22Adobe%20Reader%20MUI%22%2C%22CommonName%22%3A%22Adobe%20Reader%20MUI%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Adobe%20Reader%20XI%22%2C%22CommonName%22%3A%22Adobe%20Reader%20XI%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Real%20Player%22%2C%22CommonName%22%3A%22Real%20Player%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22PDF%20Creator%22%2C%22CommonName%22%3A%22PDF%20Creator%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Adobe%20Flash%20Player%20Plugin%22%2C%22CommonName%22%3A%22Adobe%20Flash%20Player%20Plugin%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Wireshark%201.8.4%20(32-bit)%22%2C%22CommonName%22%3A%22WireShark%22%2C%22CurrentVersion%22%3A%221.8.4%22%2C%22LatestVersion%22%3A%221.8.4%22%2C%22installed%22%3A1%7D%2C%7B%22Name%22%3A%22Skype%22%2C%22CommonName%22%3A%22Skype%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Adobe%20Shockwave%22%2C%22CommonName%22%3A%22Adobe%20Shockwave%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22OpenOffice%22%2C%22CommonName%22%3A%22OpenOffice%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Adobe%20Flash%20Player%20ActiveX%22%2C%22CommonName%22%3A%22Adobe%20Flash%20Player%20ActiveX%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22PDF%20XChange%20Viewer%22%2C%22CommonName%22%3A%22PDF%20XChange%20Viewer%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22WinRAR%22%2C%22CommonName%22%3A%22WinRAR%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Opera%22%2C%22CommonName%22%3A%22Opera%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Winamp%22%2C%22CommonName%22%3A%22Winamp%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Mozilla%20Firefox%22%2C%22CommonName%22%3A%22Mozilla%20Firefox%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22QuickTime%22%2C%22CommonName%22%3A%22QuickTime%22%2C%22CurrentVersion%22%3A%227.74.80.86%22%2C%22LatestVersion%22%3A%227.76.80.95%22%2C%22url%22%3A%22http%3A%2F%2Fsoftware.pcpitstop.com%2F2014%2F10%2FQuickTimeUpdater_7.76.80.95.exe%22%2C%22installed%22%3A1%2C%22preCommandLine%22%3A%22%22%2C%22postCommandLine%22%3A%22%22%7D%2C%7B%22Name%22%3A%22Mozilla%20SeaMonkey%22%2C%22CommonName%22%3A%22Mozilla%20SeaMonkey%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Safari%22%2C%22CommonName%22%3A%22Safari%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Java%2032%22%2C%22CommonName%22%3A%22Java%2032%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Adobe%20AIR%22%2C%22CommonName%22%3A%22Adobe%20AIR%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22FileZilla%22%2C%22CommonName%22%3A%22FileZilla%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22iTunes%22%2C%22CommonName%22%3A%22iTunes%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Foxit%20Reader%22%2C%22CommonName%22%3A%22Foxit%20Reader%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Mozilla%20Thunderbird%22%2C%22CommonName%22%3A%22Mozilla%20Thunderbird%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%227-Zip%22%2C%22CommonName%22%3A%227-Zip%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Google%20Chrome%22%2C%22CommonName%22%3A%22Google%20Chrome%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Adobe%20Reader%22%2C%22CommonName%22%3A%22Adobe%20Reader%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Java%2064%22%2C%22CommonName%22%3A%22Java%2064%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22WinRAR5.X%22%2C%22CommonName%22%3A%22WinRAR5.X%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22Adobe%20Flash%20Player%20PPAPI%22%2C%22CommonName%22%3A%22Adobe%20Flash%20Player%20PPAPI%22%2C%22installed%22%3A0%7D%2C%7B%22Name%22%3A%22PC%20Matic%201.1.0.62%22%2C%22CommonName%22%3A%22PC%20Matic%22%2C%22CurrentVersion%22%3A%221.1.0.62%22%2C%22LatestVersion%22%3A%221.1.0.62%22%2C%22installed%22%3A1%7D%5D%2C%22browserAddons%22%3A%7B%22ie%22%3A%7B%22registryEntries%22%3A%5B%7B%22ProductName%22%3A%22PCMatic%20AdBlocker%22%2C%22extensionId%22%3A%22%7BFFCB3198-32F3-4E8B-9539-4324694ED664%7D%22%7D%5D%2C%22dbEntries%22%3A%5B%5D%7D%2C%22chrome%22%3A%7B%22registryEntries%22%3A%5B%5D%2C%22dbEntries%22%3A%5B%5D%7D%2C%22firefox%22%3A%7B%22registryEntries%22%3A%5B%5D%2C%22dbEntries%22%3A%5B%5D%7D%7D%2C%22endTime%22%3A1454248518162%7D&uidcook=undefined&cidcook=12374763454906727&codebase=pcmatic

Appendix B: Disclosure Timeline

2016-02-11: Email sent to secure@pcpitstop.com and security@pcpitstop.com. Both bounce. Email forwarded to support@pcpitstop.com.

2016-02-11: Prompt response received from support team, David Austin, and ticket created in their support ticketing system.

2016-02-12: Summary of vulnerability findings provided. Requested that the person responsible for product security at PC Pitstop emails for further details and to discuss coordination.

2016-02-12: Prompt acknowledgement of receipt and thanks received from David Austin. Information has been passed on to the appropriate people.

2016-02-12: Email received from Dodi Glenn, VP of Cyber Security, confirming that he and his development team are reviewing the provided information.

2016-02-19: Some of these vulnerabilities publicly disclosed by third party[45]

2016-02-20: PC Pitstop informed that since some of these issues are now public without the public report fully covering the threats to users, this report is now scheduled for publication sometime the coming week.

2016-03-02: Public disclosure.

[45] http://rum.supply/2016/02/19/pcmatic.html

Appendix C: DownloadFile() Function

```
function DownloadFile(url, saveAs, checkSignature) {

        alert("downloading file: " + url);
        alert("saving to: " + saveAs);

        if (checkSignature) {
                alert("creating Exam control now");
                Exam = new ActiveXObject("PCPitstop2.Exam.1");
                alert("Exam control created");
        }

        var objHTTP = WScript.CreateObject("MSXML2.ServerXMLHTTP");

        var lResolve = 30 * 1000;
        var lConnect = 60 * 1000;
        var lSend = 30 * 1000;
        var lReceive = 1800 * 1000; // 30 minutes to receive
        objHTTP.setTimeouts(lResolve, lConnect, lSend, lReceive);


        objHTTP.open("GET", url, false);
        objHTTP.send();

        while ((objHTTP.readyState != 4) && (objHTTP.readyState != 'complete')) {
                WScript.Sleep(100);
        }

        if (objHTTP.status != 200) {
                alert("The " + url + " file was not found." + " The returned status is " + objHTTP.status);
           return;
        }

        var objADOStream = new ActiveXObject("ADODB.Stream");
        var fso = new ActiveXObject("Scripting.FileSystemObject");
        objADOStream.Open();
        objADOStream.Type = 1; //adTypeBinary

        objADOStream.Write(objHTTP.responseBody);
        objADOStream.Position = 0;    //Set the stream position to the start

        if (fso.FileExists(saveAs)) fso.DeleteFile(saveAs);
        objADOStream.SaveToFile(saveAs);
        objADOStream.Close();
```

```
        if (checkSignature && typeof(Exam)!="undefined") {
                var fileCheck = Exam.GetFile(saveAs, null);
                if(!fileCheck.hasValidSignature) {
                        if (fso.FileExists(saveAs)) fso.DeleteFile(saveAs);
                        alert("File failed signature check " + saveAs);
                        return;
                } else {
                        alert("Successfully downloaded " + saveAs);
                }
        } else {
                alert("Not Checking Signature or Exam ActiveX control not found");
        }

}
```