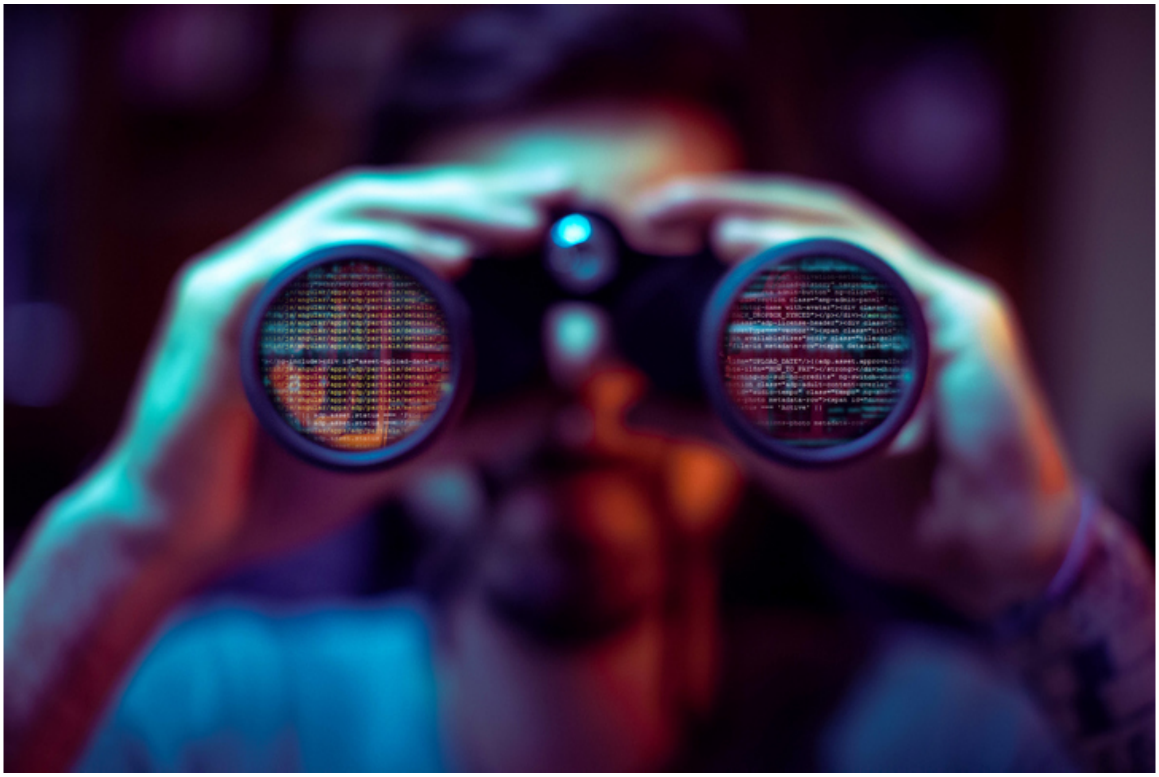


As malware grows more complex, protection strategies need to evolve – and quickly

It's time to change misperceptions about whitelisting and false positives

By David Strom

The days of simple anti-malware protection are mostly over. Scanning and screening for malware has become a very complex process, and most traditional anti-malware tools only find a small fraction of potentially harmful infections. This is because malware has become sneakier and more defensive and complex.

The basics haven't changed: Back in the early days of the PC, malware made use of Internet Relay Chat channels to communicate with its control server: today, they have migrated to the web.

Today's malware uses a number of very sophisticated methods to try and defeat the protection tools. As one Forrester analyst has written, "Attackers often penetrate user endpoints with new malware that eludes the AV detection. As a result, security professionals must consider a different approach, one that doesn't rely solely on an increasingly hard-to-manage signature blacklist." This means that security vendors have to work harder to find and block the most subtle attacks, especially ones that don't leave many fingerprints.

This article examines the latest advanced measures that are being used by today's malware to defeat the standard protective products. It explains why these traditional methods aren't appropriate and why application whitelisting can be effective. It also discusses some of the misconceptions about false positives and some recent third-party AV test results that build a strong case for a whitelisting approach to application security.

Evasion techniques

There are several types of advanced malware evasion techniques, and vendors also use some of them as protection mechanisms.

Polymorphic malware. This type of malware adapts to a variety of conditions, operating systems, and circumstances and tries to evade security scans and protection products to infect your endpoints. It is called polymorphic because every time it executes, it shifts its signatures, attack methods, and targets to make it difficult to identify and catch it.

Fileless malware. This type of malware gathers small bits of code that is already written and memory-resident into a coherent attack. The "fileless" designation is somewhat misleading, since you still need something stored in memory on the target machine. This malware, like other types, tries to leave as little evidence as possible to indicate that the endpoint has been infected. Using techniques such as return-oriented programming, malware can execute standard DLLs and other executable sequences of code that can compromise an otherwise uninfected system. This means that apps themselves – even ones that have been carefully crafted – can be a threat.

VM/Sandbox detectors. Some malware types have built-in activation delays to avoid detection: when they are deposited on an endpoint, they simply do nothing for several minutes, hoping to evade detection. Others will look for registry keys, drivers, or specific program files to see if they are running inside a VM or other type of sandbox. If it finds these files, it will also end its operations. Others will look at whether there is an actual person operating the computer, seeing if there are cached files or other evidence that the endpoint has been recently created.

Scripting-based attacks. Another avoidance technique is to execute malware using built-in Windows scripting engines such as Powershell or Microsoft's HTML Application Host. These attacks typically take advantage of process hooking and don't leave any file-based residues on the endpoint. If your detection systems can't see the script execution or understand the command-line arguments, you can't figure out that this is malware.

The latest exploit: DoubleAgent. The most recent obfuscation technique goes by the name of DoubleAgent. It takes advantage of an undocumented feature in Microsoft Application Verifier, a Windows feature that lets developers do runtime verifications of their applications for finding and fixing security issues. Unfortunately, it has an undocumented feature that Cybellum researchers discovered, which gives attackers a way to replace the legitimate verifier with a rogue verifier so they can gain complete control of the application. AV vendors have recently issued patches to correct this flaw, but again this demonstrates that malware writers are getting better at finding these sorts of hidden mechanisms to avoid discovery and being blocked.

The rise of ransomware

Ransomware takes these stealthy characteristics to a new level. It uses both polymorphic and fileless techniques to avoid detection until it encrypts targeted files. And then it comes right out and tells you that your PC is infected, your files are locked, and if you ever want to see your data again, you have to pay up. It is a very effective and a growing threat.

Ransomware isn't new by any means: the first instance of what we now know as ransomware appeared in 1989. But ransomware has improved dramatically over the years. Indeed, it exhibits some of the better trends of software engineering. Cyber criminals ply their trade with exemplary customer service, use the cloud to package and deliver their products, and have a first-rate understanding of the psychology of their intended victims.

Let's look at the recent trends with this type of malware.

There is tremendous growth in ransomware. A recent IBM report found that 4,000 ransomware attacks occurred daily in 2016, four times more than the previous year. Seventy percent of businesses previously hit by ransomware indicated that they had paid the ransom to recover company data. Of that portion, half paid over $10,000 and a fifth paid over $40,000. In another survey, Proofpoint found traces of Locky ransomware in almost every malicious file attachment it observed in Q3 of 2016. This represented a 64% jump from the first quarter.

Ransomware continues to be dangerous. Most ransomware schemes depend on social engineering ploys to trick victims into activating the malware. But really, it is all about the monetary benefit for the attackers. This discussion on the underlying and operations of Cryptowall by Imperva shows how the malware is designed. The authors write: "The ransomware advertises a different fee depending on the geographical location of the victim. Interestingly, the ransom amount for the USA is

US$700 whereas for Israel, Russia, and Mexico, it's only US$500. The malware authors clearly know average incomes, and change ransom demands based on geolocation to keep the payments affordable. If the victim doesn't pay the ransom before the timer runs out, the ransom doubles to US$1,000." This shows prior criminal experience and understanding how we all think: act now to pay less!

Typical ransomware actors offer "better support than users get from their own Internet service providers," Angela Sasse, a psychologist and computer scientist at University College London, said in a Nature magazine article.

Making matters worse, Ransomware-as-a-Service is on the rise. Ransomware now is packaged as a SaaS subscription. A typical cybercriminal signs up via a Tor server, and provides their Bitcoin address where they will receive the payouts. You can configure your ransom demands and what text you will use for the popup message that appear after the infection has been delivered to the target PC. The ransomware authors even extract their 25% commission on any funds collected through their service. Can you say convenient? Soon anyone will be able to go out on the dark web and shop for their own ransomware for their criminal enterprise.

Making a case for whitelisting

One way to resolve both ransomware and advanced stealth techniques is to make use of **application whitelisting**. The idea behind whitelisting is, instead of playing "whack a mole" as Bruce Schneier wrote in this blog post, a whitelist starts out by blocking everything except what has been proven as a trusted application on its list. "This leads to faster endpoint performance and overall better protection against zero-day threats when compared to traditional antivirus techniques," Forrester researcher Chris Sherman writes.

This isn't new technology by any means. For example, "the iPhone works on a whitelist: if you want a program to run on the phone, you need to get it approved by Apple and put in the iPhone store," Schneier writes. Facebook and Google also have closed environments and make some effort at vetting third-party apps running on their platforms.

There are numerous vendors in the whitelisting space including AppSense, Avecto, Carbon Black, CyberArk, Digital Guardian, Kaspersky Lab, Lumension Security, McAfee, Microsoft, PC Pitstop, and Trend Micro. **They use whitelisting to try to reduce the overall attack surface**, make an endpoint more secure, and increase the value of their endpoint protection products.

But not all whitelisting products are created the same, and there have been some recent innovations and improvements. First is the transfer of responsibility for vetting the apps from the end-user IT organization to the vendor. PC Pitstop, for example, employs a team of researchers that will respond within 24 hours if an unknown app has been blocked. In the past, vendors let the IT staffs figure this out, which was one of the reasons why whitelisting apps have not traditionally been well received.

This app vetting is important, because by their very nature whitelisting generates **false positives**, meaning that the unknown app is benign. Indeed, that is inherent in the entire whitelisting process, because you will come across apps that you don't know about but that are ordinary pieces of software being used for the first time. The issue is how the false positive is resolved to the end user.

This brings up another point: the **way the unknown app is blocked matters,** especially if the blocked app is removed from a system and the app turns out to be a good app. Many AV products that use blacklists block specific apps and remove them immediately from the endpoint's hard drive as a protective measure. If they turn out to be good apps, they have to be restored before being run on the user's PC. That isn't very convenient, and could backfire in the case where an AV product misidentifies something that is a legitimate piece of code. This happened years ago with the McAfee AV tool that removed network drivers on 300,000 XP PCs, creating what The Register called "a world of hurt" when the computers became inoperable.

Other products make the false positive process easier **by just blocking the app's execution**. If the app later is vetted as a good app, it is much easier to allow it to run in this situation.

Another issue is **the granularity of the detection**. Many of the detection programs rely on file hashes and digital signatures. That is an issue mainly because a small percentage of apps use these indications. One study shows less than 15% of all apps use signatures and I have found early builds of even Microsoft desktop apps lack them initially. Moreover, these signatures can be compromised, as a recent story on hacks to SHA-1 encryption shows. A better method is to **examine the actual processes that are being used by each executable**, and what references they have to other software that comes with the operating system. This is how scripting attacks are created, because until recently, most AV tools weren't looking at processes that were not inherently malware but could be exploited for malicious purposes.

How PC Matic works

One security tool that provides a unique approach to protecting against ransomware and other advanced malware is PC Pitstop's PC Matic. The software combines a curated application whitelist with quick assessment turnaround to identify unknown, good, and bad executable programs. Building from more than a decade of experience, the company recently added new process hooking techniques for identifying fileless infections.. The combination of existing and constantly evolving technologies provides a solid defense that leverages a large data repository of a wide range of malware behavior and known good applications. This library is updated regularly as new attacks are discovered. As more customers use the PC Matic whitelist, the more accurate it becomes.

Let's look more closely at the core components of PC Matic and its Super Shield 3.0 engine. First is its **curated application whitelist**. Because it uses both human and automated methods to add approved files to its application whitelist, PC Matic is very effective at protecting customer endpoints. Unlike other whitelisting products, PC Matic doesn't place the burden of verification on its customers, but makes use of PC Pitstop's research department to verify unknown files. Researchers can examine the root psychological cause of why users click on malware and bring a real understanding to how a typical user begins the malware chain and infection process – which makes the Super Shield engine more effective in identifying malicious activity.

As an example, when a new scripting attack occurs, analysts log the event and break down the malware into components to see how it operates. If the code is used by regular software, it would be added to the appropriate blacklist or whitelist. Either way, making note of this exploit would be a simple matter of adding a single entry to the PC Pitstop servers, rather than rolling out an update to a signature database as many other AV products do. Once an app has been approved, it is available to every customer.

The second key component is PC Matic's **treatment of false negatives**. Unlike other products that make use of blacklists only, PC Matic has no false negatives because of the way it first denies any unknown executable. Most AV products look at the scripts themselves, rather than at the various scripting engines that run the scripts. The problem with scripting, however, is that by changing just a few lines of code, bad actors can evade any detection that is looking for a particular signature or hash. PC Matic looks beyond what the actual script is doing, into the processes that are calling the script itself and the parameters being sent to the scripting engine in its evaluation of whether or not it is
a good application. **This is called process hooking.** Since PC Matic examines this in very granular detail, it can prevent the script from being called in the first place.

The downside of PC Pitstop's approach is that it does generate some false positives. This is inherent in any whitelisting approach. But IT teams can override this if they see a known good app that they wish to run. If they aren't sure, they send the information back to PC Pitstop for further analysis, and can receive the decision within 24 hours. This makes for a nice combination of both types of "lists" because blacklists are updated when a false negative occurs, and whitelists are updated when a false positive occurs.

PC Matic's ability to stop scripting attacks through process hooking is enabled by the implementation, in December 2016, of **Microsoft's Detours technology** as a foundational element. The idea behind Detours is just what its name implies: It takes various Windows function calls and re-routes them through an analysis engine to make sure they aren't doing evil things. Detours isn't dependent on any particular application framework or OS component. So if a malware author was trying to trick the OS into thinking it is benign, it would show up in the Detours monitoring process. Other AV products use a portion of Detours in their scanning engines for particular circumstances. Or they create special third-party drivers so they can hook particular executables. Other than Detours, PC Matic doesn't use any third-party drivers, because it goes through Detours for all executables.

PC Pitstop knows which processes can be used by malware to cause trouble: that is their secret sauce. For example, a common technique is to escalate access privileges so some code can take over a system or infect others across the network. If you are using process hooking, this is easy enough to spot and prevent. Because of PC Pitstop's long history with malware analysis, its software can watch for other processes and stop them before any malware invades a system.

Detours has been around for more than a decade and is part of Microsoft's latest Defender AV tool that comes with Windows 10. Defender incorporates some solid protection features, and has proven that Detours makes sense as a solid foundation to build an AV product upon.

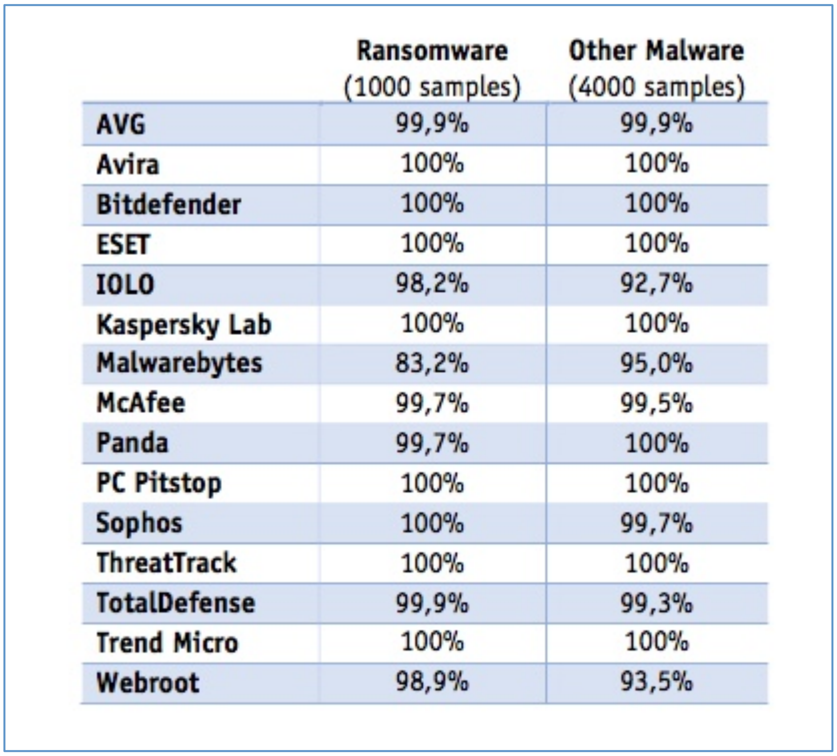
Since its new process hooking technique was implemented in early January, PC Pitstop claims that no customer has been infected.

Third-party test results

It is often hard for IT managers to evaluate independent AV test labs results because the conditions of these tests can be difficult to parse. The labs also use different qualifications to satisfy the needs of particular vendor participants. One issue is that false positives are very different from false negatives. The two situations are treated differently by AV testing organizations. For example, AV Comparatives requires its participating vendors to have a false positive rate lower than .05% to be part of their tests. They report on each product's false negative rates, but include any value in their tests. Presenting false negative rates and false positive rates in absolute terms is somewhat confusing and doesn't seem very fair.

The consumer version of PC Pitstop in **tests by Virus Bulletin** show it blocks 100% on both reactive (online) and proactive (offline) detection. This underscores the power of their application whitelist technology. There simply isn't another product even close with PC Matic's detection rates.

The AV Comparatives test from February 2017 on the consumer product also shows 100% blocking on all ransomware and other malware samples as shown in the table below. Several of these vendors didn't catch every malware sample.



	Ransomware (1000 samples)	Other Malware (4000 samples)
AVG	99,9%	99,9%
Avira	100%	100%
Bitdefender	100%	100%
ESET	100%	100%
IOLO	98,2%	92,7%
Kaspersky Lab	100%	100%
Malwarebytes	83,2%	95,0%
McAfee	99,7%	99,5%
Panda	99,7%	100%
PC Pitstop	100%	100%
Sophos	100%	99,7%
ThreatTrack	100%	100%
TotalDefense	99,9%	99,3%
Trend Micro	100%	100%
Webroot	98,9%	93,5%

Conclusion

Fighting modern malware isn't easy. Malware creators are more adept at evading established detection methods and hiding their craft deep within the normal operations of typical Windows endpoints. Ransomware will continue to pose significant challenges to IT teams. A preventative approach that involves using carefully curated application whitelists to block attackers is the only established method to block 100% of all malware – without inhibiting end users' ability to remain productive.

David Strom is one of the leading experts on network and Internet technologies and has written and spoken extensively on topics such as VOIP, convergence, email, cloud computing, network management, Internet applications, wireless and Web services for more than 25 years. He has had several editorial management positions for both print and online properties in the enthusiast, gaming, IT, network, channel, and electronics industries, including the editor-in-chief of *Network Computing* print, Digital Landing.com, ReadWrite.com and Tom's Hardware.com. He presently edits and curates the Inside Security newsletter