An NCC Group Publication

The Demise in Effectiveness of Signature and Heuristic Based Antivirus: "Or has the death of AV been wildly exaggerated?"

Prepared by:
NCC Group's Technical Directors Forum

NCC Group's Technical Directors Forum represents the global senior technical leadership team from across NCC Group.

The Forum provides strategic direction for NCC Group's research, engineering and capability development and is the focal point for encouraging innovation across all of the Group's service offerings.

In addition to these internally focused activities, the Forum also provides analysis and comment on the technical issues facing our customers in today's fast moving cyber landscape.

Contents

1 Management Summary

Today there is an urgent emphasis being placed by vendors on the need for antivirus to be installed on an increasing number of computing platforms used within organisations.

The aim of this is to satisfy risk controls while also forming part of an organisation's technical information security strategy. This market demand for antivirus has led to a number of security products which do little to actually protect the user, their data or the organisation. This paper outlines why, in our opinion, the antivirus based approach adopted by organisations to technical risk management, not only fails to provide the protection it is designed to, but it in fact increases an organisation's susceptibility to attack.

The notion that antivirus is dead is certainly not new and the ineffectiveness of signature based antivirus has recently received attention from various quarters of the press.[1] These have in many ways reflected NCC Group's views, but may even fall short of the true extent of the problem.

Overall our view is that signature based antivirus is tackling a problem we had 20 years ago and is not relevant to many of today's threats for businesses, although we feel it still has a role in protecting the consumer. As a result, NCC Group's opinion is that security budgets might be more effectively directed into other areas of mitigation that offer a higher return on investment in terms of risk reduction.

2 Introduction

In this paper NCC Group first looks at the deficiencies with signature based antivirus as well the increased risks they introduce. We then look at the challenges that mobile computing introduces.

The intended audience of this paper is senior decision makers and technology strategists who have a responsibility for information security, risk management or policy formation within an organisation.

3 The ineffective nature of signature and heuristics based AV

3.1 Reality 1 – Signature based antivirus doesn't prevent unseen threats

In order for signature based antivirus to be effective, a particular sample or close relative needs to have been captured, analysed and a signature generated.

Looking at Symantec as one of the largest antivirus producers, we see that as of October 28, 2012 they maintain a database of over 20 million signatures[2] for their Endpoint Protection Product. According to Sophos in the calendar year of 2011[3] they were seeing 15,000 new samples a day or 54 million new samples a year, with Sophos noting:

[1] SC Magazine - 'Is the era of antivirus over?' - Tom Cross, director of security research, Lancope, 20th November 2012
http://www.scmagazine.com/is-the-era-of-anti-virus-over/article/269210/
Infosec Island (blog) - 'The Death of Antivirus Software' - Danny Lieberman, 24th January, 2012
http://www.infosecisland.com/blogview/19386-The-Death-of-Antivirus-Software.html
Tech Republic - 'Is the death knell sounding for traditional antivirus?' - Michael Kassner, August 27th 2012
http://www.techrepublic.com/blog/security/is-the-death-knell-sounding-for-traditional-antivirus/8317
[2] http://www.symantec.com/security_response/definitions.jsp
[3] http://www.sophos.com/en-us/security-news-trends/security-trends/2011-year-in-review.aspx

"*More and more, cybercriminals create and distribute malware generation engines and toolkits. And a significant portion of this malicious code features back doors, meaning detecting the payload of malware is increasingly difficult.*"

To combat this problem of antivirus vendors needing to personally identify then analyse either automatically or manually and generate signatures, they started to utilize heuristics as a means to detect malicious code in a fuzzy (nonspecific) manner.

Vendor based research into effectiveness of antivirus against banking Trojans in October 2012[4] concluded:

"*On machines on which the company's HitManPro product detected a banking Trojan, the average lifetime of said Trojan was 81 days when no anti-virus product was running. However, on machines that were running anti-virus software, the average lifetime was a mere 25 days.*"

Even taking into account the obvious partiality of the vendor, any demonstrated exposure should be of concern. The mere fact a vendor concluded that the lifetime of a new banking trojan on a fully protected machine was nearly 4 weeks will be a surprise to many.

When we look at alleged state sponsored threats such as Flame, antivirus companies such as F-Secure[5] have been quite open on the fact that while they did possess the samples in their collections they had effectively missed them for over 18 months.

This point is further reinforced by a recent study Imperva and The Technion – Israeli Institute of Technology[6] assessing the effectiveness of antivirus products. They found that Antivirus effectively stopped 5% of malicious code.

3.2 Reality 2 – Heuristics are readily bypassed

As implied above, in order to combat the increasing volume of malicious code and associated threats, antivirus products have for more than a decade increasingly relied on heuristics. Heuristics in the context of antivirus is a way of describing fuzzy matching. This fuzzy matching is for example based on:

- **File contents:** What is contained in a sample or program.
- **Basic behaviour:** Behavioural traits of a program.

The basic heuristic mechanisms are in reality implemented in a variety of different ways from simple string matching and program disassembly, through to more complex emulation or simulation. One of the major hurdles to content-based heuristics is the use of packers or obfuscators to make a piece of malware appear dissimilar to a previously seen incarnation. The increasing use of packers and obfuscators has led to antivirus firms investing significant effort in the reverse engineering and implementation of un-packers and de-obfuscators in their antivirus engines. However despite these efforts from AV vendors these heuristics still prove relatively trivial to bypass given a competent individual.

While the market to bypass antivirus heuristic and signature based detection for criminal purposes is

[4] https://www.virusbtn.com/news/2012/10_24.xml
[5] http://www.wired.com/threatlevel/2012/06/internet-security-fail/
[6] http://www.imperva.com/download.asp?id=324

well defined, the prevalence of antivirus products has made it necessary for legitimate operators to research into this area as well. One of the legitimate reasons is where antivirus is deployed on a host that is subject to a penetration test or red team assessment. In these situations the behaviour of the tools utilized by these teams exhibit the same behaviour as a malicious Trojan or exploit. As a result instead of just having cyber criminals or nation state actors looking for ways to bypass antivirus and utilizing it covertly, we instead have legitimate professionals actively researching how to and documenting the process of bypassing antivirus heuristics (2012 [7]).

3.3 Reality 3 – The trade-off between heuristics and false positives

The story of antivirus software and false positives is a long one, with examples ranging from antivirus detecting itself (2012[8]) through to the disabling of thousands of machines in a specific geography (2007[9]).

This trade-off between heuristics which are likely to detect more malicious code and heuristics which are easier to bypass but less prone to false positives is a fine line. This need has led to antivirus firms employing a number of strategies, ranging from whitelisting certain files by hash through to whitelisting all code produced by certain vendors. This vendor based whitelisting approach has resulted in threat displacement, with these vendors and their code signing capability becoming a target (2012[10]).

The need to minimise false positives will conversely minimise the possible effectiveness of heuristics based antivirus.

3.4 Reality 4 – Antivirus is complex software which isn't bug free

So far we've discussed how the detection technology implemented in antivirus software can be bypassed without the antivirus product itself being specifically targeted. When we start looking at the complex nature of antivirus software and how bugs can be used to bypass it, we see some interesting evidence. As far back as 2005[11] there is evidence of researchers targeting antivirus products with success. This subject area was then co-opted for a competition 3 years later in Race to Zero (2008 [12]).

Searching the Open Source Vulnerability Database[13] we see that there have been 156 reported instances of antivirus bypass over a 10 year period across all major vendors. This is over 1 per month.

4 Security Products are not always secure products

As mentioned above, security products are not bug free. While these bugs at times may be related to their ability to function as an antivirus they can also equally be related to the security of the product itself.

Looking at published vendor advisories we see that there are several examples of vulnerabilities in AV products themselves offering attackers opportunities to gain a foothold in the networks they are

[7] http://www.pentestgeek.com/2012/01/25/using-metasm-to-avoid-antivirus-detection-ghost-writing-asm/
[8] http://www.zdnet.com/sophos-antivirus-detects-own-update-as-false-positive-malware-7000004565/
[9] http://www.computerworld.com/s/article/9019958/Symantec_false_positive_cripples_thousands_of_Chinese_PCs
[10] http://www.zdnet.com/adobe-code-signing-infrastructure-hacked-by-sophisticated-threat-actors-7000004925/
[11] http://www.blackhat.com/presentations/bh-europe-05/bh-eu-05-wheeler-mehta-up.pdf
[12] http://www.securityfocus.com/brief/795
[13] http://osvdb.org/search/search?search%5Bvuln_title%5D=antivirus+bypass&search%5Btext_type%5D=titles&search%5Bs_date%5D=&search%5Be_date%5D=&search%5Brefid%5D=&search%5Breferencetypes%5D=&search%5Bvendors%5D=&search%5Bcvss_score_from%5D=&search%5Bcvss_score_to%5D=&search%5Bcvss_av%5D=*&search%5Bcvss_ac%5D=*&search%5Bcvss_a%5D=*&search%5Bcvss_ci%5D=*&search%5Bcvss_ii%5D=*&search%5Bcvss_ai%5D=*&kthx=search

designed to protect. For the first 10 months of 2012:

Vendor	Remote Compromise	Privilege Escalation	Bypass / Disable
F-Secure[14]	0	0	1
McAfee[15]	0	0	2
Symantec[16]	0	1	2

Note: The following vendors do not publish easily locatable lists of security updates – CA, Kaspersky, Panda and Sophos, who in November were forced to patch 7 critical issues ranging from remote compromise to denial of service[17].

The presence of vulnerabilities with varying degrees of impact in 2012 should not come as a surprise. However it should be a consideration to any organisation that is wishing to improve their security posture by deploying these products.

5 Mobile computing and antivirus

Mobile computing and antivirus is a contentious topic. On one side you have antivirus vendors who wish to sell products highlighting the increasing volume of malicious code. On the other you have the platform vendors and store owners attempting to garner trust in their platforms. In the middle you have organisations deploying these platforms who are applying security policies and procedures influenced by the PC era to mobile computing platforms.

The realities with regard to mobile computing and antivirus are:

- Antivirus on common mobile platforms (iOS, Android, Windows Phone 8 and BlackBerry) is not able to obtain the same low-level access as on PC based operating systems to prevent infection.
- Antivirus on common mobile platforms can at best detect infection after the fact, though it can potentially remove malware once detected.
- Common mobile platforms in enterprise configurations typically have effective whitelist based mechanisms to restrict which applications are authorised to run built-in. These controls alone are capable of mitigating malicious code aimed at these platforms.
- Tier 1 mobile application store owners (Apple, Google, Microsoft and Research In Motion) all actively undertake varying degrees of malicious code scanning within their app stores. While not a panacea they do provide comparable protection.
- Tier 1 app store maintainers (platform owners) are capable of remotely killing any application which is later detected as being malicious.

Given these facts NCC Group's opinion is that antivirus on mobile computing devices is not any longer an effective means of mitigation or remediation against malicious code. Indeed in an environment where security expenditure is tight, budget would probably be much more effectively spent on other risk mitigation measures.

6 Whitelist based prevention

[14] http://www.f-secure.com/en/web/labs_global/security-advisories

[15] https://kc.mcafee.com/corporate/index?page=answers&type=search&searchid=1351513387813&question_box=McAfee+Security+Bulletin+-+VirusScan

[16] http://www.symantec.com/security_response/securityupdates/list.jsp?fid=security_advisory

[17] http://www.informationweek.com/security/vulnerabilities/sophos-av-teardown-reveals-critical-vuln/240062599

In February 2012 the NSA publically stated[18] that it planned to use a whitelisting based approach to economically block malicious code.

A whitelist approach ensures that only authorised software and associated components can execute. While this approach may not always stop the initial successful exploitation of software vulnerabilities it will significantly complicate the exploitation process and in vast majority of cases mitigate persistence.

NCC Group supports the NSA's opinion in this regard. Specifically we believe that the money spent by organisations on buying and supporting desktop and mobile antivirus is better spent on producing, maintaining and supporting a whitelist approach on their computing estate.

As previously mentioned whitelisting is supported by most common mobile computing platforms as well as modern desktop computing operating systems such as Windows 7 and Apple Mountain Lion.

7 Threat behaviour based detection

Where whitelist based preventions cannot be deployed or deemed not sufficient there are other defensive strategies available to organisations looking to move away from signature and heuristic based antivirus for threat detection. The primary alternative being behaviour based detection. Behaviour based detection is where we can define expected (good) behaviour of code with anything outside of these parameters is considered suspicious. These behaviours may cover areas such as file system access, network traffic or operating system interaction.

The reason that pure behaviour based detection systems have never gained traction within desktop AV is because of user experience and risk of false positives. Firstly, desktop antivirus vendors are very sensitive to their products being perceived as slowing down the users' computing experience. Secondly a user's desktop and associated network activity is a very noisy and unpredictable place.

With the advent and subsequent mainstreaming of virtualisation, emulation and instrumentation behaviour based threat monitoring solutions have become an effective mechanism for flagging malicious samples we don't know about. What we've seen over the last 24 months is the commercialisation of technologies that have been available to antivirus vendors and researchers for 7 or 8 years to efficiently identify suspicious e-mail attachments, website URLs and programs among others.

As an example: When a Microsoft Office document is opened we expect some file system activity in certain locations and maybe a little network traffic. We don't expect a binary file to be downloaded, written to disk, executed and some form of persistence to occur. This malicious behaviour would be difficult to see in everyday use or come with such a huge performance penalty that it would be impractical to detect on a user's desktop. However with sanitized and highly instrumented environments cloning the desktop into a 'sandbox' becomes a viable detection mechanism where performance overheads can be more readily managed.

With the bringing to market of solutions and services based on the open source project Cuckoobox[19] (virtualization) as well as more expensive offerings such as Norman Sandbox[20] (emulation) and

[18] http://www.nextgov.com/health/2012/02/nsas-whitelisting-approach-economically-blocks-computer-viruses/50620/
[19] http://www.cuckoosandbox.org/
[20] http://www.norman.com/about_norman/technology/norman_sandbox/

FireEye[21] (virtualization), organisations can now benefit from in-line detection of threats based purely on their behaviour without the need for signatures.

NCC Group's opinion is that these solutions and services are significantly more capable that traditional antivirus.

8 Data loss prevention and detection

Antivirus and similar malicious code defences have historically been designed to prevent initial infection or compromise of a host. These same defences were then repurposed to try and defend against the exploitation of software vulnerabilities, the effectiveness of which has been demonstrated as lacking.

Gen. Michael Hayden (USAF-Ret.), former head of the NSA and the CIA provided an interesting perspective[22] on the problem.

"*We may be at the point of diminishing returns by trying to buy down vulnerability, maybe it's time to place more emphasis on coping with the consequences of a successful attack, and trying to develop networks that can "self-heal" or "self-limit" the damages inflicted upon them.*"

This more mature approach to network and system security is in NCC Group's opinion a viable way forward. As with the previously suggested approach of reinvesting money historically spent desktop antivirus on adopting a whitelist approach to software authorisation, that assertion that money currently invested in products such as Intrusion Prevention Systems could be effectively reinvested into data loss prevention and detection is equally valid.

NCC Group's suggested approach around data loss prevention (DLP) and detection is that it should be multi-faceted, including:

- Compartmentalised data storage and networks to a far greater extent than is current practice;
- Protection of data at rest and in transit through mechanisms such as IPSEC and file and database encryption;
- Multi-factor access control to data and networks including human based monitoring;
- Protective monitoring and audit capability around data access and exfiltration including human based monitoring;
- Exfiltration controls including human based monitoring;
- Open source intelligence monitoring and analysis.

By adopting an approach based on these principles as appropriate to your organisation's threat profile, incidents can be quickly identified, mitigated and resolved efficiently.

We have observed over the last fifteen years that buying products which aim to solve specific problems can be both expensive and ineffective. Instead going back to base principles which are proven over time instead of a 'sticking plaster' approach is in NCC Group's opinion the viable long term strategy.

[21] http://www.fireeye.com/
[22] http://www.gsnmagazine.com/node/25682

9 Traditional antivirus and the consumer

While this brief is intended for organisations, NCC Group felt it prudent to include a brief comment with regard to consumers.

To echo previous statements, the value of antivirus to consumers on mobile platforms is questionable for a number of the same reasons as organisations. Specifically that the application stores provide a level of malicious code detection as point of introduction combined with their ability to remove or uninstall an application if it is subsequently found to be malicious.

With regard to the desktop and consumers the story is a little more complex. Whilst some modern desktop operating systems are also introducing application store like functionality as well as sandboxing, for example Microsoft Windows 8, there is still some value in traditional signature based AV in the home for traditional operating systems.

The value of traditional antivirus in these situations is due to the usage differences in consumer computing, specifically the inability to lockdown the host in the same way as in the enterprise and the tendency to have a more loose and diverse approach to application installation and use. Whilst antivirus may not stop initial compromise or infection, it may reduce the length of time a host is compromised and minimize the overall clean-up cost and risk of data loss.

However NCC Group does not believe that paying for such solutions is necessary; products like Microsoft's Security Essentials [23] provide adequate and comparable protection for Windows computers. Alternatively Immunet[24] is an innovative approach for Microsoft Windows that leverages the cloud for rapid signature deployment. For Apple Mac OS X there are a number of free solutions available, including Avast[25] that provide, in the opinion of the authors, sufficient protection.

10 Conclusions

We have shown that the effectiveness of signature and heuristics based antivirus is questionable at best when lined up against modern malicious threats. While also at times increasing the available attack surface against the machine upon which it's installed.

NCC Group has also shown that antivirus on mobile computing is generally, in our opinion, not worth investing in for enterprises looking to manage their security exposure on these platforms.

We have suggested practical strategies for managing the risk of malicious code to replace the controls where organisations have historically relied on antivirus. These strategies include making more effective use of software configuration, deploying the features available in modern desktop and mobile computing operating systems and augmenting these with network based threat behaviour detection. These controls should then be combined with a comprehensive data loss prevention and detection strategy.