A Detailed Study of Endpoint Protection Using Antivirus by Extending its Capabilities

Saptarshi Laha
M.Sc. Cybersecurity
School of Computing
National College of Ireland
Dublin, Ireland
x18170081@student.ncirl.ie

Samruddhi Patil
M.Sc. Cybersecurity
School of Computing
National College of Ireland
Dublin, Ireland
x18202667@student.ncirl.ie

Somesh Saxena
M.Sc. Cybersecurity
School of Computing
National College of Ireland
Dublin, Ireland
x18176895@student.ncirl.ie

***Abstract*—This paper emphasizes the difference between traditional antivirus mechanisms and their endpoint protection counterparts. Then it highlights the additional functionalities that an endpoint protection suite possesses over an antivirus. Further, it discusses the probability of attacks occurring in the absence of an endpoint protection system and suggests methods to prevent such attacks in a cost-effective manner essential to the scenario in question. Finally, a few real-world examples are provided, where the lack of an endpoint security system led to huge financial losses, or damage to company reputation, along with, how implementing this mechanism would greatly reduce the company's attack surface to potential attackers.**

Keywords—endpoint protection, antivirus, endpoint security, threats, firewall, IDS, IPS

I. Introduction

Traditional antivirus solutions refer to antivirus solutions built for home use or small business use purposes where the attack surface is rather small to have multiple entry points of vulnerable or malicious code. In large scale organizations, a single, core antivirus component on every system is only a part of the equation of the whole group of security tools assigned or incorporated within the said environment. These security tools not only monitor everything from access logs to checking for file safety, but also allow remote clients to connect to the organization's network without hindering workflow and maintaining the same standard of security.

As noticeable, a single antivirus component is barely able to perform industry level security operations as it's just a single unit of protection. Therefore, organizations tend to depend on solutions built for the industry or a large organizational sector. These security products are often called Endpoint Security products, Endpoint Protection products or in layman's terms is referred to as Endpoint Protection Antivirus. Although, as we will notice shortly, the Antivirus term for such a product is usually a misnomer.

II. Traditional Antivirus Mechanisms

Antivirus is a specially designed group of software to protect a single system against execution or exposure to malicious code by simply blocking downloads which the antivirus feels are malicious or automatically deleting or quarantining files. These methods are performed based on a few parameters:

A. Machine Code Scans

In machine code scanning, an antivirus usually has a database of signatures that it investigates to achieve the same. The database consists of potentially malicious or malicious signatures in a hexadecimal format. The making of signatures is made as unique as possible to correctly identify malware from regular usable software, although, this method is not perfect and hence can lead to detection and removal or quarantining of false positives. The antivirus uses the signatures present in the database to correctly identify if a file is malicious or not based on the presence of any of the signatures in the machine code of the file.

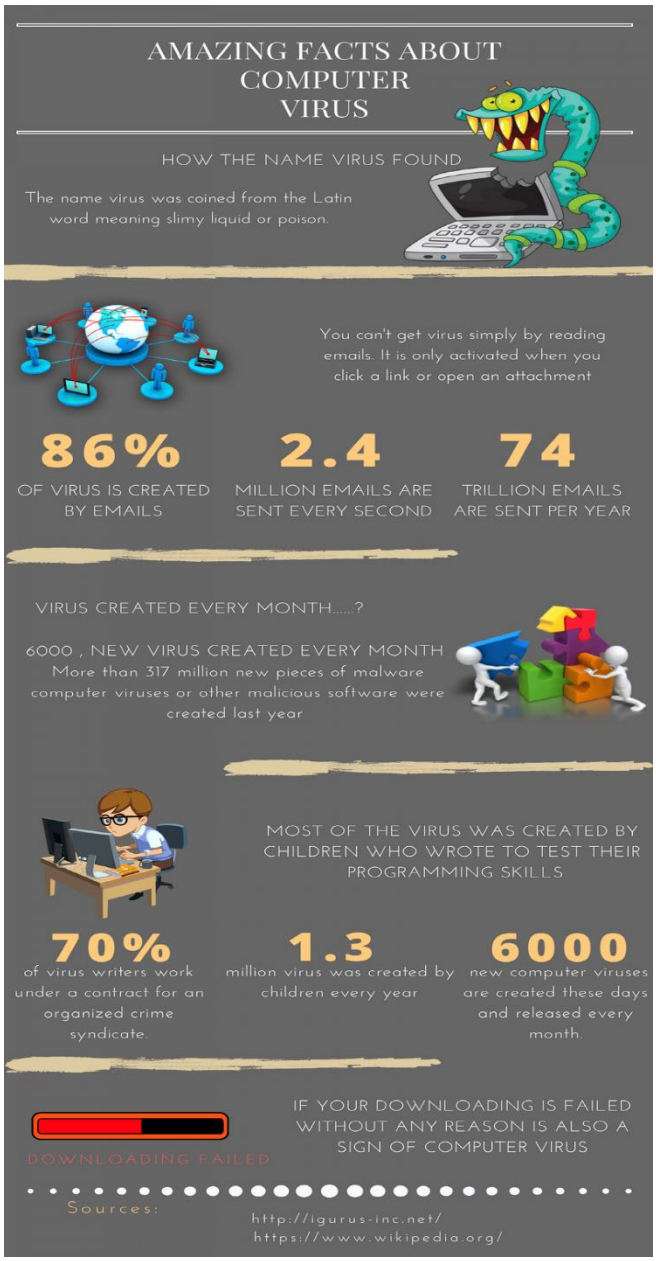


Fig 1. Computer Virus Facts[7]

B. *Memory Scans*

In a memory scan, the same logic applies as that in machine code scans, but this is performed for malware that is more complex than the previous type mentioned. This type of malware generally uses a packer to unpack the actual encrypted executable code on runtime instead of having a perfectly normal and unencrypted executable binary. In this case, the antivirus performing initial Machine Code Scans will fail to analyze if a file is malware or regular software. The only point of detection lies during its execution. The same signature table can be used to scan for the malware but instead of static scanning, the malware needs to executed for it to unpack the instructions in memory thereby allowing the antivirus to analyze the actual code instead of encrypted code and perform actions based on it.

C. *Heuristics*

In a heuristic scan, the antivirus uses smart detection standards to detect if a file is malicious or not. This scan can be during static or dynamic analysis of malware by the antivirus. The heuristic engine looks for anomalies in the system triggered by software and flags the same as malware based on previous records of such activity leading to a malware attack. Heuristics can lead to a hit or miss scenario, and, hence, a weighting factor is used along with other scan mechanisms to lead to an outcome. If an antivirus were to depend only on heuristics, it would probably flag every file for not complying with the standards of use during any specific unique execution of code.

D. *Sandboxing*

Sandboxing is a relatively new concept in which the malware is executed in a safe or sandboxed environment away from the actual user-space to perform all the other scans and diagnostics possible on the malware and thereafter analyze based on the report if the software is truly a malware. This is a very important mechanism and is extremely useful as in the earlier versions of Windows, for example, the memory scanners could be subverted by the malware sample once executed due to certain other vulnerabilities and open services thereby avoiding detection and also executing malicious code on the system while the antivirus was active. With recent massive updates to Windows and antivirus systems, this is, however, no longer possible, and memory scans take place in a sandbox than in the real-time environment of the user. Reports generated in the sandbox are used to flag a piece of software as malware or treat it as the regular software.

E. *Wire Sniffing*

Wire sniffing or network traffic monitoring refers to sniffing of network traffic, much like Wireshark, thereby performing the machine code scans during the download phase, reducing scan time and increasing the performance of the system. This scan is possible because the actual raw bytes or machine code is transmitted during an upload or download in case the file is not compressed or encrypted. The antivirus can, therefore, scan the network traffic and analyze if a malware sample is being uploaded or downloaded instead of legitimate software and block the same. Wire sniffing also helps antivirus provide other additional security features to the users such as website monitoring, analyzing phishing pages, etc. at an additional cost, which is out of the scope of a general antivirus.

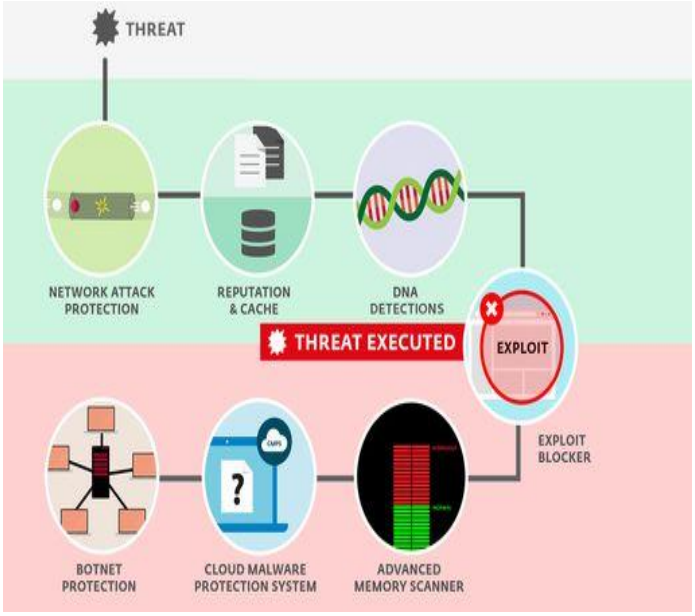


Fig 2. Multiple Methods to Detect Threats or Virus[5]

Thus, it is very clear from the activities of antivirus that it only performs local system scans for malicious code and at times also sniffs traffic to increase the performance of the system by reducing the time taken to scan the file statically. Anything beyond that is not in the scope of traditional or current day antivirus models. Hence, antivirus companies generally tend to name their products differently for antiviruses with additional features such as Quick Heal takes the naming scheme of Internet Security and Total Protection[1]. Industries have a very different requirement altogether. They need a comprehensive all in one solution or defense mechanism against a variety of attacks against all its networks and systems. Hence, antivirus only plays a small part in the entirety of this role assigned to the defense mechanism in place. Often enough there is special industry-grade software developed by the same companies developing a home or small business antiviruses such as Quick Heal, and, it is named Endpoint & Data Protection by Seqrite (Quick Heal)[2] or Comodo Endpoint Security[3]. These are massive suites of software rather than just an antivirus, and, encompass tasks that the traditional antivirus performs along with extending it to industry standards to implement a wide array of other defense mechanisms.

III. Endpoint Protection Mechanisms

Endpoint protection does not refer to a single software, rather it is a suite of different software components interacting and working together in a client-server architecture model to achieve a common goal of defending not just one device but rather an entire network where every single remote device that connects to the network acts as an entry point for malware or other such threats. By virtue of the product, the actions it performs are much more varied and it is provided in the software as a service model by most renowned security companies. Within the network, there would be an endpoint security software, located on a centrally managed and accessible server or gateway. There would be a client software located in every endpoint or endpoint device. The security software authenticates logins made from the endpoints and simultaneously updates client software when needed. Different commercial products advertise various aspects of their system, but the general actions that an endpoint security suite performs are as follows[3]:

A. Containment with auto-sandboxing

All unrecognized processes and applications are auto-sandboxed to run in a restricted environment.

B. Web URL filtering

Advanced interface to create rules as required – user-specific, sweeping, or as granular as desired.

C. Firewall

It offers high-level security against inbound and outbound threats, stealths computer ports, manages network connections, and blocks confidential data transmission by malicious software.

D. Antivirus

Features multiple technology-based automatic detections, cleansing and quarantining of suspicious files to eliminate malware and viruses.

E. File Lookup Services (FLS)

Cloud-based instant analysis of unknown files that checks file reputation against Comodo's master whitelist and blacklists.

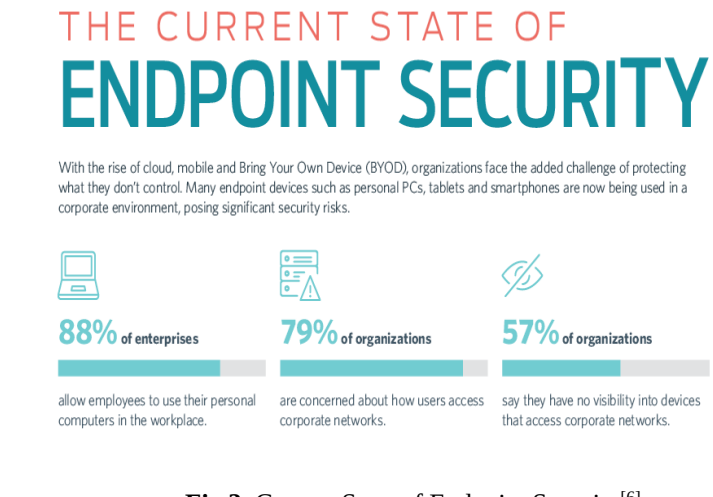


Fig 3. Current State of Endpoint Security[6]

F. Host Intrusion Protection System (HIPS)

Monitors important operating system activities to ensure protection against malware intrusion.

G. Viruscope (Behavior Analysis)

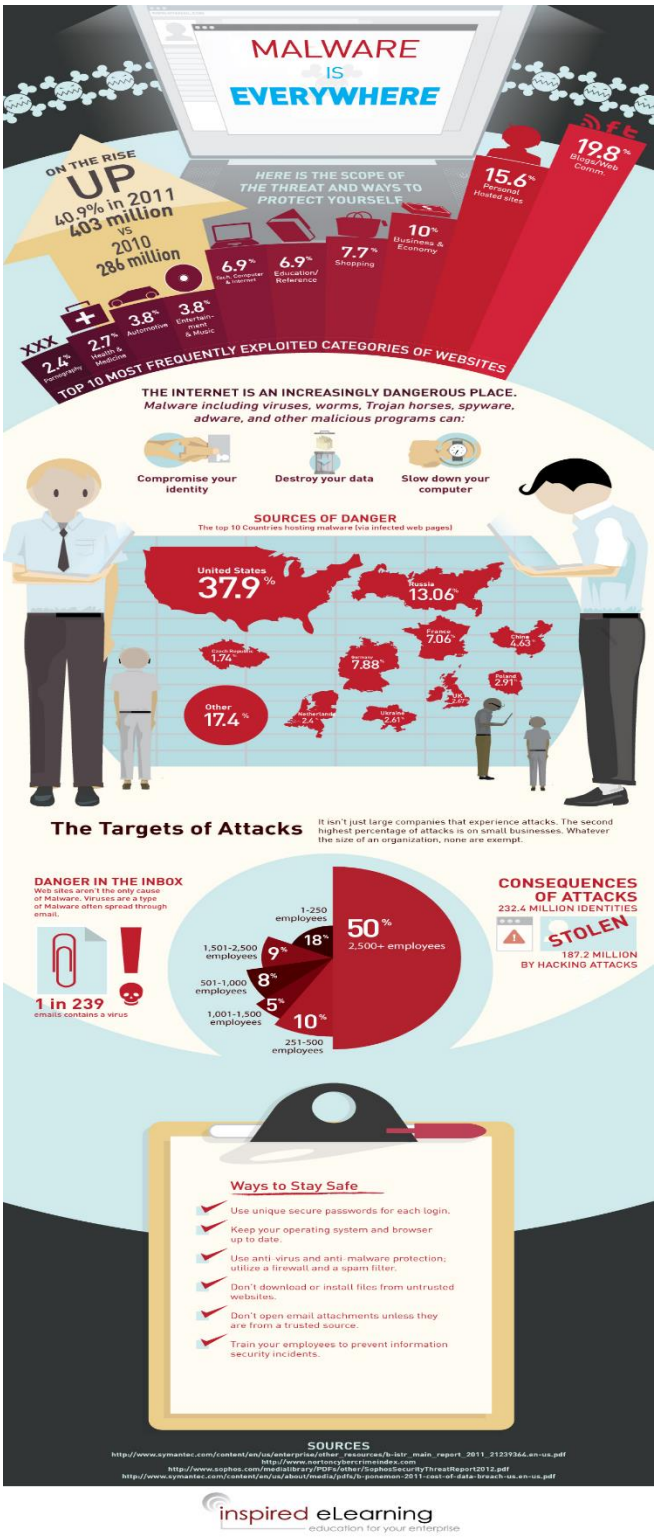
The behavior of all processes is monitored for potentially harmful action.

IV. Probability of Threats Occurring & Prevention

Not having endpoint protection can affect any enterprise severely, as, even if the company invests in hardware firewalls, intrusion detection and prevention systems, antivirus, etc. they won't be filling in all the gaps in their environment from the security perspective, and, a potential attacker can leverage one such attack vector and abuse it to perform unintended or malicious activities. The probability of such an event occurring depends on the nature of the organization in question. In case, the organization deals with valuable and sensitive data (such as in this case), it can be highly valuable for the competitors in the market to try and exploit the system in place to compromise the data withheld in the systems, or leak it, to tarnish the name of the organization. The organization in question fits all the categories of the scenario mentioned above and, therefore, is a likely target for potential competitors and hackers alike. Apart from that since the organization consists of 150 employees, which are planned to grow to 500, it is an up and

Fig 4. Malware is Everywhere![8]

coming organization, and, is a potential target to bug hunters and bug exploiters alike, where the bug exploiter will



take credit in exploiting the system in place to leak sensitive information to the public, thereby damaging the reputation of the organization, whereas, a bug hunter will report it to the company for a certain sum of money and help them fix the issue.

A sub-group of attacks can originate from zero-day vulnerabilities or other unpatched resources. These need to be

manually patched on short and specific time intervals to avoid attacks exploiting such vulnerabilities.

The best prevention mechanism is the installation of an endpoint security system or suite, as outlined by the company delivering the product. Other temporary solutions include installing smaller but critical security components as the business improves which makes up the endpoint security suite. Following these steps will initially keep the cost low while maintaining a certain standard of security. However, an initial analysis needs to be performed on every single attack surface to determine the ones most likely to get exploited by an intruder. Over time, however, as the organization grows, the same needs to be upgraded massively, in a step by step manner if need be, or an entire renovation, which is mandatory to maintain the standard and further upgrade the security of the whole system, if the cost is a limiting factor.

V. Previous Attacks and Affect on Business

The attacks mentioned here are in order to convince the reader not to overlook the installation of an endpoint security system, lest, they should fall prey to one such elaborate scheme of the exploit as mentioned here.

Phishing is a widespread attack that compromises user credentials or other such sensitive information. If a phishing mail seeps into the enterprise mail server or system, it can be devastating for the employee falling prey to the attack along with compromising the information potentially of value to the company. There are very many instances of such phishing emails seeping into company emails and wreaking havoc by leaking sensitive information. An endpoint security system is crafted to filter out such emails, along with blocking the origins of such emails.

Zero-day vulnerabilities are pervasive, but very few are as highly reported as the eternal blue exploit reported by NSA. This is because of the WannaCry[4] ransomware that abused the exploited was able to infect multiple millions of computers worldwide. If such a ransomware attack is imminent on the systems of an enterprise, the enterprise can lose corporate data worth millions of euros which will be irrecoverable due to the nature of the virus. Endpoint protection comes with sandboxes inbuilt that quarantine such files, thereby preventing such exploits from infecting the system or causing potential harm. WannaCry also spread to internal networks automatically, which can be blocked by the presence of an endpoint protection suite.

Background bitcoin mining applications are on the rise ever since cryptocurrency gained its share of fame. These applications run silently on the victim's system using up resources to mine cryptocurrency. These applications tend to spread through internal networks. If such an application finds its way into the organization's server, it can use a major share of the organization's computing power to mine cryptocurrency while hindering other valuable tasks to the company. Endpoint protection can prevent such attacks by monitoring processes running and validating them against a database of approved and legitimate applications.

These few examples provide insight from the very fundamental misuse of applications to industry level attacks such as ransomware spread, which can affect the company in case of missing endpoint protection. In no manner is this list complete or comprehensive. A simple google search on all the attacks in the past decade lists instances where an individual or a company overlooked its security parameters which led to an attack ranging from very minor to extremely critical. In other words, an endpoint protection suite is an essential software package that needs to be installed by the client on their systems to prevent or at least mitigate the effects of devastating or minor attacks alike. Not complying with the same, only opens up an organization to potential attackers wanting to tarnish the name of the company or steal valuable data for fun and profit.

In this case, by installing an endpoint protection suite, we will not only reassure our potential customers or clients that we ensure a safe work environment digitally, which will improve customer relations and faith in our company. Apart from that, it will also ensure safe and secure business practices on the company's part which is essential to any developing organization which intends to keep its data away from attackers and exploits. Without having an endpoint protection system in place, many other potential clients might have a hard time trusting the services we provide since it deals with sensitive data handling and thus can decrease the revenue for the company, thereby hindering its growth rate and profits.

A fantastically informative infographic describing the previous cybersecurity breaches can be found here: https://www.atlascloud.co.uk/wp-content/uploads/2019/04/Cyber-Security-Breaches-Survey-2019-Infographic.png

Acknowledgment

We want to thank the authors of the referred links for providing us with relevant information for us to be able to complete this CA Assignment well within time.

We would also like to thank our lecturer Mr. Vikas Sahni for allowing us to choose this fascinating topic of our interest, which allowed us to broaden our spectrum in terms of understanding the mechanisms of antivirus and its critical differences from endpoint protection systems and much more. This topic also helped get us up to speed with the current affairs in the cybersecurity world.

References

[1] "Quick Heal - Antivirus for Home Users", Quickheal.com, 2019. [Online]. Available: https://www.quickheal.com/home-users. [Accessed: 19- Nov- 2019].

[2] "Enterprise Security Solutions | Network Security | Seqrite", Seqrite.com, 2019. [Online]. Available: https://www.seqrite.com/. [Accessed: 19- Nov- 2019].

[3] "What is Endpoint Security? | Comodo Endpoint Protection for Enterprise", Comodo, 2019. [Online]. Available: https://www.comodo.com/endpoint-protection/endpoint-security.php. [Accessed: 19- Nov- 2019].

[4] "WannaCry ransomware attack", En.wikipedia.org, 2019. [Online]. Available: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack. [Accessed: 20- Nov- 2019].

[5] "NEW 2020 Antivirus and Internet Security Solutions", Eset.com, 2019. [Online]. Available: https://www.eset.com/uk/. [Accessed: 20- Nov- 2019].

[6] W. security? et al., "[Resolved] Company Kyrus - Kyrus technologies is a company", Kyrustechnologies.blogspot.com, 2019. [Online]. Available: http://kyrustechnologies.blogspot.com/. [Accessed: 21- Nov- 2019].

[7] "Amazing facts about computer virus | Visual.ly", Visual.ly, 2019. [Online]. Available: https://visual.ly/community/Infographics/computers/amazing-facts-about-computer-virus. [Accessed: 22- Nov- 2019].

[8] "Malware is Everywhere | Visual.ly", Visual.ly, 2019. [Online]. Available: https://visual.ly/community/infographic/computers/malware-everywhere. [Accessed: 22- Nov- 2019].