Threat-Vector Segregation for Endpoint Security

Sagar G. M-Tech, RACE REVA.

Abstract— With X number of companies working for cybersecurity, Y number of products, and Z number of solutions,[1] till date we rely on restricting users from visiting any unknown/malicious websites or unknown/malicious links on the corporate machine [Laptop]. Considering the threat vector of an Endpoint connecting to the internet, [2] in this paper, we are formulating a solution for the problem, by segregating the threat vector from the endpoints and giving extended access to the user to perform all the activity. The proposed solution will also ease the working of an IT management team in case of any malware infection to the endpoints, in a matter of seconds the endpoints can be back online working, downtime of network or machines will be minimal. The proposed solution can also be utilized for training the cybersecurity engineers, with the example of the live malware infection and propagation without affecting the corporate endpoint or the network.

Index Terms— Endpoint Security, Laptop, Minimal Downtime, Threat Vector Segregation, Unknown-Unknowns, Virtualization, Zero-day

1 Introduction

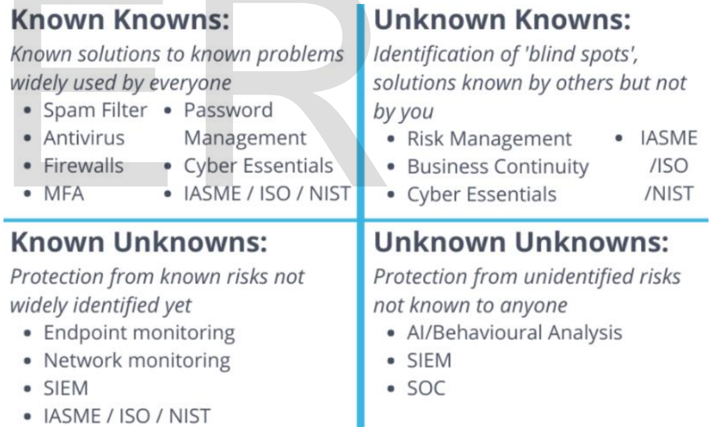
There is an increase in the number of cyber incidents taking place every year, where there are many companies, international organizations are working towards limiting the impact of the cyber incident, many technological innovations and standards are been created.[1] With the increase in the number of standards and cybersecurity solutions, it has been a direct impact on the ease of use. There shall be always a tradeoff between ease of use and security when considered, in the verge of considering security, standards, compliance ease of use is been neglected. Users always find a turnaround option to circumvent the security solution implemented giving the reason for their work requirements.
The primary objective of this study is to segregate the attack surface of the corporate network and trying to segregate them so that it will not be infecting or propagating in the corporate network via an endpoint, and also by giving users a more free hand to access multiple websites and understand the practical scenarios of phishing emails or drive-by download scenarios or a ransomware attacks.
The proposed solution can also be utilized for training purposes, rather than giving a closed environment or simulated training, this paper will also enhance the learning curve of users concerning cybersecurity and the acts that are being performed by the hackers targeting the corporate machines
It also facilitates the IT infrastructure management team so that they can easily monitor the target surface if there is any infection or malicious activity that is been taking place in the endpoint, by restarting the partial endpoint the entire endpoint would be reverted to the known good safe state, reimaging of the entire system can be avoided by this solution
There would be a seamless integration between the two operating environments given to the end-user so the user will not feel any difference in working.

2 Objectives

The primary objective of this study is to segregate the attack surface of the corporate network and trying to segregate them so that it will not be infecting or propagating in the corporate network via an endpoint, and also by giving users a more free hand to access multiple websites and understand the practical scenarios of phishing emails or drive-by download scenarios or a ransomware attacks. [3]

Four possibilities of a threat vectors:

1. Known–Knowns
2. Unknown–Knowns,
3. Known–Unknowns,
4. Unknown–Unknowns.



Known Knowns:
Known solutions to known problems widely used by everyone
- Spam Filter
- Antivirus
- Firewalls
- MFA
- Password Management
- Cyber Essentials
- IASME / ISO / NIST

Unknown Knowns:
Identification of 'blind spots', solutions known by others but not by you
- Risk Management
- Business Continuity
- Cyber Essentials
- IASME /ISO /NIST

Known Unknowns:
Protection from known risks not widely identified yet
- Endpoint monitoring
- Network monitoring
- SIEM
- IASME / ISO / NIST

Unknown Unknowns:
Protection from unidentified risks not known to anyone
- AI/Behavioural Analysis
- SIEM
- SOC

Figure 1: Threat vector types

Details of all four quadrants of the threat vector, and the current technologies associated with the quadrant to mitigate the risk out of those quadrants, are shown in figure- 1.[2] In this paper, we mainly concentrate on the last quadrant unknown unknowns, where there are limited set off tools available in the market to address this quadrant, all these tools listed in the quadrant requires a lot of customization [industry specific], hence the malicious actor always can compromise these systems via the last quadrant (unknown unknowns).
This paper can be a good fit in the last quadrant unknown unknowns because the solution proposed, does not need any customization for its implementation part, it would be similar to a plug and play software where the entire threat vector is being isolated from the corporate environment and can be brought into action immediately.

3 Problem Statement

The problem statement is being derived out of the daily corporate user, working on the endpoint implementing his day-to-day activity,[4] where the day-to-day activity comprises of visiting many third-party websites and responding to all the emails from outside the organization. Cybersecurity trained user is also facing difficulty in identifying the phishing emails or links to justify genuine, where hackers are coming up with every new methodology's to look links as genuine and also because of all the activities are time-bound and has to be completed within a certain duration of time.

Because of the work scenarios are considered above the user will be responsible to access many of the links that have been provided via email that may be landing up on malicious websites, in the verge of working on the activity user may click on the phishing links which will be resulting in downloading a malicious content by drive-by download methodology, downloading a ransomware file or clicking on phishing, wishing or smashing links any of this activity may compromise the endpoint and also traverse the corporate network, and the current solution being used is trying to block the unknown websites or less trusted websites, and treating after the infection starts propagation.

As many startups are working in the current domain there would be N number of websites created every day, working on the legitimacy of the websites and the content within that will be a tedious job for any company or the endpoint solutions.

4 Literature Review

The list of top 500 companies that are contributing to cybersecurity is being listed in this website inspired learning. Hence 500+ companies are working on cybersecurity to provide a safe and secure environment for all the corporate users as well as individuals, still, it has been seen that there is a continuous increase in the cyberattack on all the endpoints. Where the endpoint is been accumulated with multiple software running in the background to protect the asset. [1]

There are different categories of threat intelligence, where we will get the input from the threat intel providers, and an unknown threat that is not detected yet zero-day. The same has been elaborated on in this paper. [2]

Sandboxing is a technology that is been used to create a safe, isolated environment on the base machine to verify the functionality of the malware, by creating a fully functional machine and interpreting a model workplace, and monitoring activities performed by the malware once the endpoint has been infected and tried to find hash off it, all these activities shall not infect the base machine or the corporate network associated with it.[3]

This is an annual report from Proofpoint, where this survey has been conducted across multiple corporate giants concerning cybersecurity awareness of the users that have been trained for cybersecurity. This report details the problem faced by individuals using their corporate endpoints. This can also be used as a basis for this project as users are still facing difficulty in the deciding factor when it's regarding the security, and the count of malicious content delivered to the endpoint despite the technology used to avoid things. [4]

European Union agency for cybersecurity has given a press release regarding the threat landscape of cyber attacks in the year 2020 mentioning the sophistication targeted widespread and undetected threats which have been propagating throughout the endpoints located at home business governments and critical infrastructure. To infiltrate any network the primary way would be to compromise the endpoints, which means to compromise the endpoints can be multiple and weakest points the CyberLink is also humans, who are prone to do mistakes. [5]

There are different variants in malware, one which would infect windows machine, one which would infect Linux machine and the other variant would be cross-domain malware which can infect both the operating system. Malware action in Linux system is different when compared to its windows alternative, infection of the malware and the existence of the malware, their functionality is being described in this paper. [6]

There are multiple variants of Linux available in the market, which can be used as a full pledge operating system, or a tiny Linux to run on the old machines, or machines utilized for sandboxing. As most Linux are open-sourced operating systems the complete code is visible to the developer and any customization can be done with project-specific. One of the open-sourced operating systems that consumes a very little amount of ram during its idle state is Antix. The complete details of the AntiX development and utilization can be found in this link.[7]

5. Project Methodology

Currently with all the advanced cybersecurity solutions and companies working toward a solution of blocking, still users are delivered with phishing emails, ransomware attachments, malware, propagating via emails, and malicious websites. According to the survey of Proofpoint 2020, there is a huge gap where a user or a trained employee of cybersecurity can easily detect phishing, ransomware, malware, smishing, vishing links, or attachments. People with higher privileges on their endpoint machine will be unknowingly accessing those links and getting the endpoint compromised, as well as the corporate network.

To avoid this kind of scenario to be occurring on the corporate laptop, segregation to the corporate internal network (INTRANET), and the external access (INTERNET) of the endpoint, a solution is being provided by utilizing all the existing technologies efficiently.

According to the ENISA threat landscape report of 2020, the top 15 threats are: [5]

1. Malware
2. Web-based Attacks
3. Phishing
4. Web Application Attacks
5. SPAM
6. Distributed Denial of Service (DDoS)
7. Identity Theft
8. Data Breach
9. Insider Threat
10. Botnets
11. Physical Manipulation, Damage, Theft, and Loss
12. Information Leakage
13. Ransomware
14. Cyber Espionage
15. Crypto-jacking

Out of 15 threats 14 can be avoided by the use of this solution

5.1 Technology utilized

Three main technologies would be diploid as the solution for the problem statement defined

1. Virtualization/Hypervisor
2. Sandboxing
3. Network segregation.

Virtualization: This technology is used to creating a separate segregated compute environment, on an existing operating system, allocation of the resource to the newly created machine can be changed based on project need.
There are two types of hypervisors available in the market type 1 type 2.
Type 1, for example, Microsoft hyper V
type 2 for example VM Ware workstation.
Any of the above mentioned can be utilized to create virtualized environment but will differ in the utilization of the underlying resources of the base machine. Baselining of the operating system deployed onto the virtualized environment must be done, when the virtualized environment is being restarted or turned off it would be returning to its baseline state this feature is named as a snapshot in the hypervisors. This feature has been efficiently used during the solution phase in this paper.

Sandboxing: This technology would be used to create a safe, simulated, isolated environment on the base machine, to check the malware in action, without affecting the base machine and the network associated with it. Linux operating system is being utilized as a part of sandboxing technology in this solution. [3]

Network segregation: This technology would be logically segregating the network traffic, to segregate the threat vector.

5.2 High-level design

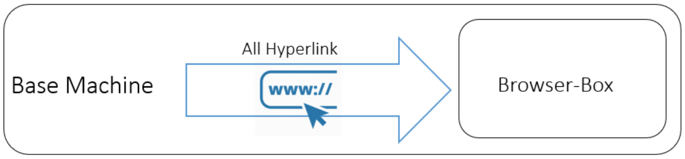


Figure 2: High-level design

The above picture shows the high-level diagram solution for the problem statement considered, the user to be provided with a micro virtual machine by employing the hypervisor in the endpoint. It is recommended to utilize a Linux operating system for the virtualized environment as this will create an additional layer of security utilizing cross-platform technology.[6] There are small Linux operating system that has a very small footprint on the base machine for example AntiX, which would take around 140 MB of RAM in its idle state (micro virtual machine).[7] The integrator will be free to choose to adopt an open-source hypervisor or licensed hypervisor based on the criticality of the device that has been deployed and the user using it. There shall be a seamless integration between the base machine and the hypervisor. Considering the threat vector for an endpoint all the hyperlinks shall be navigated from the base machine to the safe state machine browser box, add the browser box user will have a facility to freely browse any content in the website malicious /non-malicious, clicking on any phishing email to verify, any drive-by download attack will infect the safe state machine, as the safe state machine is running on a hypervisor, the hypervisor has the functionality to revert to the snapshot taken or known good safe states. Buy this the workload of the IT personnel to identify the endpoint that has been infected and reimaging the entire endpoint, losing of data at the endpoint can be avoided.

5.3 Detail design

Figure 3 shows the detailed diagram solution for the problem statement considered.
The base machine mentioned in the above figure is the physical machine of the user, endpoint, corporate laptop, browser box easy virtualized environment, the virtual machine created upon the base machine by utilizing hypervisor technology.

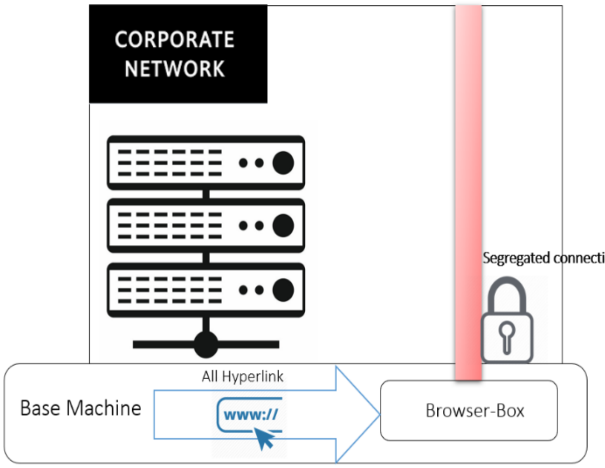


Figure 3: Detailed design of the solution

There shall be software built upon, similar to the web browser, for example, Internet Explorer, where all the hyperlinks clicked on the base machine navigated towards the browser box if the link is public-facing, else if the hyperlink is something related to an intranet that shall be navigated to a different web browser. Linux machine shall be utilized as the operating system of the browser box to efficiently utilize the cross-platform technology of spreading of malware, the initiated browser box will have a dedicated separate network connection so that it shall not communicate to the corporate internal network, malware, or ransomware infecting the machine that is public-facing browser box that shall be contained in the browser box itself (sandboxing)as the network for the browser box has been segregated even if the ransomware or the malware tries to propagate through the network that shall not affect the corporate internal network. hence this solution can be considered as a plug and play device where there is no need for any customization specific to the user, although the selection of the hypervisor virtual machine operating system, the technology used for segregating the network traffic, the software is written for the seamless integration between the base machine and the browser box would be industry-specific or integrator specific.

5.4 Operations

Two different types of scenarios can be considered for the user, and the problem statement considered

- User accessing Internet
- User accessing Intranet

All the Internet-facing hyperlinks on the base machine shall be redirected to the Browser-Box. All the activities of the users on the Internet example downloading content /tools /Software's /documents should be restricted in the browser box itself, in case of any infection to the browser box the infection shall be contained in the browser box for example ransomware infecting the browser box shall encrypt all the data of the browser box, in the case of the ransomware tries to propagate via the network, the browser box network is not connected to the corporate network. Hence the base machine, as well as the corporate network is safe and the malware is being contained in the virtualized environment browser box.

IT team can also utilize this technology as a sandbox environment to analyze the malware, behavior of the malware, operation of the malware and can contribute to the open-source threat Intel if required.

Users will not be able to access the corporate internal network via the browser box. To access the internal network user can utilize the normal Internet Explorer for example Google Chrome.

6 Conclusion

Segregation of the Intranet traffic and the Internet traffic by giving two different operating environments to the user to access intranet and Internet and this segregates the threat landscape of the entire corporate sector so that monitoring, maintaining of the threat landscape, and securing the corporate network would be eased.

A blend of this solution proposed can also be utilized as a part of corporate cybersecurity training which would be more effective than closed environment training.

This solution shall be helpful for all the corporates to handle the unknown unknown threats without any customization making. This would be similar to a plug and play device multiple other endpoint solutions can be avoided by the use of this technology a detailed study on this is to be made on what security products can be replaced, while the above-mentioned solution is being deployed.

7 References

[1] Inspiredelearning.com, "Cybersecurity 500," *Inspired eLearning*, 2017. https://inspiredelearning.com/wp-content/uploads/2017/06/cyber-500-list.pdf.

[2] S. D. Kim, "Characterizing unknown unknowns," 2012, [Online]. Available: https://www.pmi.org/learning/library/characterizing-unknown-unknowns-6077.

[3] C. Greamo and A. Ghosh, "Sandboxing and Virtualization," *IEEE Secur. Priv. Mag.*, vol. 9, no. 2, pp. 79–82, 2011, [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5739643.

[4] ProofPoint, "ProofPoint.pdf," 2019. doi: 0400-002-01-01.

[5] Press(at)enisa.europa.eu, "ENISA Threat Landscape 2020," *EU for cybersecurity*, 2020. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020.

[6] E. Cozzi, M. Graziano, Y. Fratantonio, and D. Balzarotti, "Understanding Linux Malware," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2018-May, pp. 161–175, 2018, doi: 10.1109/SP.2018.00054.

[7] Open-Source, "AntiX." [Online]. Available: https://antixlinux.com/documents/.