The Treat Of The Future Fileless Malware

Name : Gunathilaka S.B.M.B.S.A

Registration number : IT20028046

TABLE OF CONTENT

01 **ABSTRACT**

Give a simple idea about fileless malware and what I am going to discuss

02 **INTRODUCTION**

Explain about fileless malware

03 **Evolution of fileless malware**

explain fileless malware evolution

04 **FUTURE DEVELOPMENTS**

What happens to fileless malware in the future.

05 **CONCLUSION**

Key points about fileless malware

06 **REFERENCES**

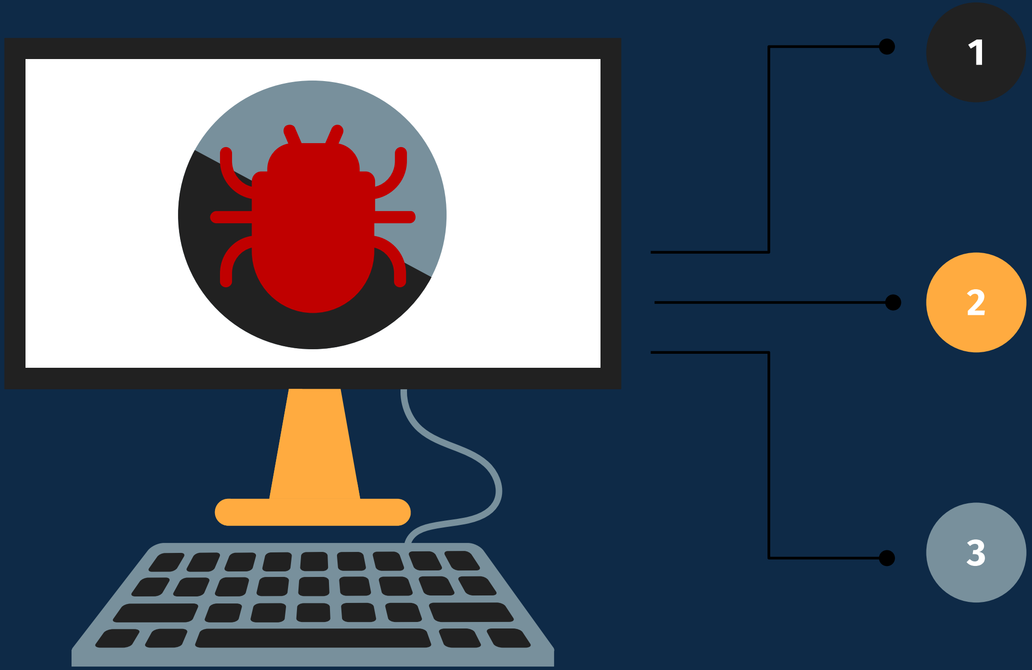
1. Abstract

- Harmful programs like virus, Trojan can be caught by general antivirus programs.
- But the fileless malware cannot detect usual security solutions
- There are some fileless malware attacks in history.
  Ex : Dark avenger , Frodo , operation cobalt kitty
- Fileless attacks and fileless malware both use tools like PowerShell to perform their infection.
- We discuss what is a fileless malware ,the evolution of fileless malware, future developments.
- In addition we talk about analyzing, detect and some other areas about fileless malware.

2. Introduction

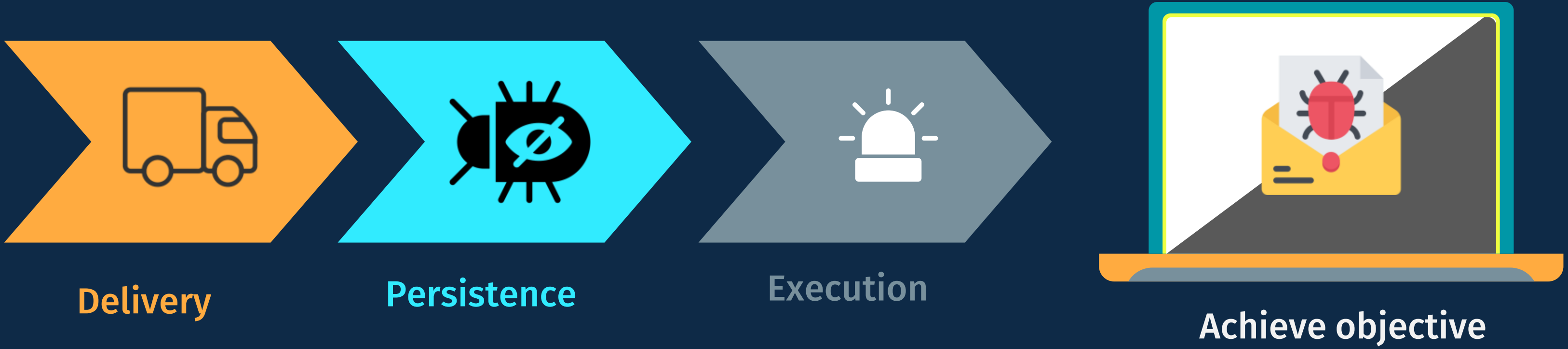
- Type of malware but advanced than other traditional malware programs.
- This kind of malware develops for stealth attacks and evades basic security solutions.
- Fileless malware doesn’t need space on the hard disk .it directly spreads its infection on main memory (RAM).
- The attacker tries to gain access to whitelisted programs like PowerShell ,WMI to download additional malware parts and other malicious activities.
- To keep malware persistent it uses some techniques. We talk about persistence under the fileless persistence topic.
- The threat actor who needs to compromise a system first needs to send the payload to the victim.so he uses some methods to pass the payload to the victim. They are shown in the next slide.

❖ **Attacker use some techniques to deliver the payload to the victims machine.**



1. Vulnerability exploitation
2. Malicious document with macros
3. Executable files

Life Cycle of Fileless Malware



Types of Fileless malware

❖ There are two types of Fileless malware

1. RAM resident Fileless malware
2. RAM resident Fileless malware

Additional areas covered in introduction

01 Fileless malware evasion techniques

02 Fileless malware detection

03 Fileless malware mitigation

3. Evolution of fileless malware

- After the .NET framework was released by Microsoft it makes the malware creation process easier.
- After inventing the .NET framework attackers able to create more advanced malware and it helps them to stay ahead of antivirus companies.
- During malware development on the .NET framework is easier with PowerShell.
- Using PowerShell attacker can keep the malware persistent, inject scripts to memory and download additional scripts when needed.
- PowerShell also helps to evade security solutions.
- Many parties including antivirus campanies,other organizations detected the fileless malware attacks and they published on the internet to aware about fileless malware including antivirus companies

4. Future developments

- How will the fileless malware looks like in the future. Attackers use more advanced techniques with fileless malware.

- The fileless malware is hard to detect and control even now.so in the future, it will direct to very harmful cybercrimes.

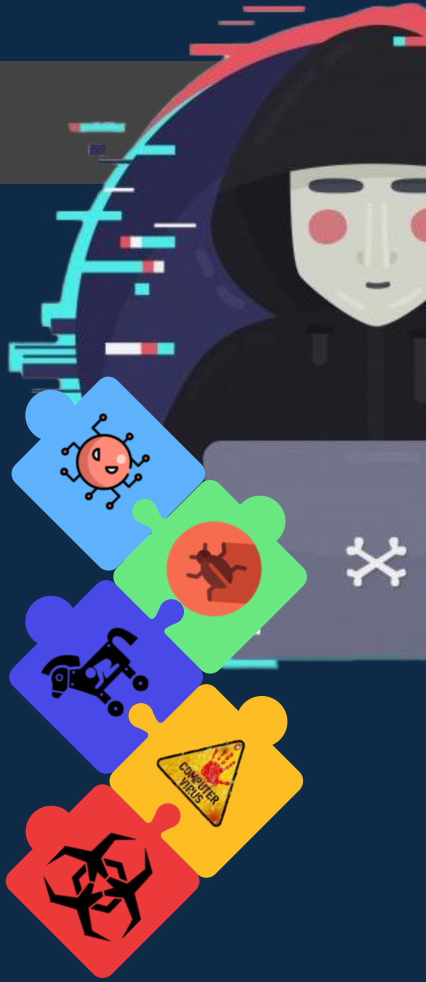
- They will be using artificial intelligence for malware creation and operating malware.

- Other malware or malicious executables will extract features in fileless malware and fileless malware detection could be very hard.

- The fileless malware evolves and from time to time it will rise again.so we can expect powerful fileless attacks in the future.

5. Conclusion

- Fileless malware is the next step of the next malware generation.so we need some knowledge about fileless malware to prevent it. signature-based antimalware solutions still unable to detect this fileless malware so we need to invent new prevention methods or solutions. this report gives a brief idea about fileless malware, the evolution of fileless malware, future developments .in addition fileless malware detection ,analysis and mitigation techniques are discussed in the report.



6. References

- McAfee Labs, McAfee Labs Threats Report June 2018, USA, 2018 Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf

- Kaspersky Lab, “Fileless attacks against enterprise networks,” 2017. [Online]. Available: https://securelist.com/fileless-attacks-againstenterprise-networks/77403/

- Verizon Labs, “Data Breach Investigations Report-2017, Verizon." [Online]. Available: https://www.ictsecuritymagazine.com/wpcontent/uploads/2017-Data-Breach-Investigations-Report.pdf

- Candid Wueest, Himanshu Anand, Symantec, “ISTR living off the land and fileless attack technique (2017)” Available: https://www.coursehero.com/file/38434149/Living-Off-the-Land-and-Fileless-Attack-Techniquespdf/

- Sudhakar, Sushil Kumar, “An emerging threat Fileless malware: a survey and research challenges” [Online], Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0043-x

- Vala khushali, “A Review on Fileless Malware Analysis Techniques”, Available: https://www.researchgate.net/publication/341870307_A_Review_on_Fileless_Malware_Analysis_Techniques

Thank You !