CLOUD AV

Cloud On Security Overlay Network

Kalika Nerkar, Vaishnavi Dod, Prof. Kirti Dongre
Information Technology, Rajiv Gandhi College Of Engineering And Research
Nagpur, India
Email-id: kalika.nerkar@gmail.com, vaish.doda@gmail.com

Abstract— One of the most widely used tools for detecting and removing unwanted files is an antivirus software. Many modern threats and its increasing complexity has resulted in vulnerabilities that are being exploited by malware cannot be detected by antivirus software. A new model for malware detection on end hosts based on providing antivirus as an in-cloud network service can be advocated by this software. Several important benefits including better detection of malicious software is provided by this approach. We are exploring this idea in cloud-based antivirus system named as Cloud-AV.

I. INTRODUCTION

Detecting malicious software is a complex problem. One of the most widely used tools for detecting and removing unwanted files is an antivirus software. Our main objective is to deploy an antivirus software in a cloud and to access that software on the machines that are connected or linked to the cloud. This approach will also analyze whether the system is safe or not. This approach of antivirus software can be vulnerable for long period of time. The end system will be updated according to the updates of antivirus software.

II. DETECTION FUNCTIONALITY

Antivirus act as a service network

The capability of an antivirus software is currently provided as efficiently and effectively by host based antivirus software. We are thinking of doing that each machine independently run a small process for detection of new files and then send that files to the main machine for further analysis .

In general practice we used to install any application on different computer system which has the drawbacks like time consumption, more cost and extra memory utilization.

To overcome these drawbacks and providing more flexibility, effectiveness, we are designing a cloud based antivirus application.

For exploring this new concept of antivirus software, we are proposing a cloud based antivirus system that consists of components like, a host that run on end hosts like desktops, laptops, and that identifies new files for analysis; a network service that receives files from hosts and identifies dangerous or unwanted files and removes it.

CloudAV is deployment and evaluation of a cloud antivirus system. Cloud-AV provides better detection techniques against new threats with respect to the single old technique of an antivirus software.

III. ANTIVIRUS SOFTWARE LIMITATIONS

Most successfully and widely used tools for removing unwanted files is an antivirus software . Antivirus software is deployed on most desktops and workstations in enterprises across the world.

The deployment of antivirus software in a unique way leads to ever expanding malicious software and tools.

As the construction of malicious software has shifted from the work of novices to a commercial and financially lucrative enterprise, antivirus vendors must expand more resources to keep up. The rise of boot nets and targeted malware attacks for the purposes of spam, fraud, and identity theft present an evolving challenge for antivirus companies.

The two important trends is that in case of a unique antivirus software technique, there are no regular updates of a newly formed dangerous viruses in a system where this can be lead to danger for that system on which the software is deployed because it is not aware of newly created viruses and their signatures. Second is that the increasing complexity of antivirus software and services has indirectly resulted in vulnerabilities that can and are being exploited by malware. That is, malware is actually using vulnerabilities in antivirus software as means to infect systems.

IV. APPROACH

Before getting into details of the approach, it is important to understand the environment in which such an architecture is most effective. We propose our approach on the same threat model as present in a host-based antivirus system and assume a cloud based antivirus system would run as an additional layer of protection to augment already existing security systems such as those inside an organizational network like an enterprise.

Some practicable deployment environments include:

Enterprise networks: Enterprise networks are to be used in highly controlled environments in which desktop and server software is controlled by IT administrators. In addition, enterprises typically have good network connectivity with low latencies and high bandwidth between workstations and back office systems.

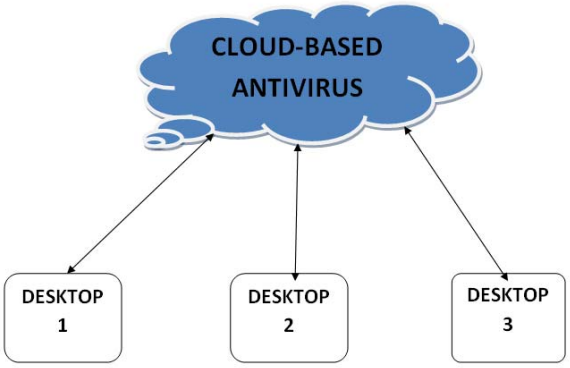
In-Cloud Detection:-

The core of the proposed approach is moving the detection of malicious and unwanted files from end hosts and into the network. This idea was originally introduced and we significantly extend and evaluate the concept in this paper.

There is currently a strong trend toward moving services from end host and monolithic servers into the network cloud. In addition, there have been several attempts to provide network services as overlay networks.

Moving the detection of malicious and unwanted files into the network significantly lowers the complexity of host-based monitoring software. Clients no longer need to continually update their local signature database, reducing administrative cost. Simplifying the host software also decreases the chance that it could contain exploitable vulnerabilities. Eventually, a lightweight host agent allows the service to be extended to mobile and resource-limited devices that lack sufficient processing power but remain an enticing target for malware.

V. ARCHITECTURE



In the above diagram of Cloud-AV we have created an antivirus software which is able to detect and delete a virus from a file or a machine.

This antivirus is later deployed on the cloud where all other systems are linked to the cloud

so that they can use this application anywhere anytime with a cloud.

This cloud based approach saves the time as well as money and space. So this method of deployment and detection of virus is an effective way as compared to the old antivirus software system.

CONCLUSION

- We have proposed a new model for antivirus deployment by providing antivirus functionality using a cloud service as CloudAV.
- This particular technique provides notable advantages over traditional host-based antivirus including better detection of malicious software.
- Using this technique is more effective and provides better protection against threats.

REFRENCES

1. Hashizume, K.; Rosado, D.G.; Fernandez-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. *J. Internet Serv. Appl.* 2013, *4*, 5.
2. A Survey on Cloud Computing Security, Challenges and Threats|Whitepapers|TechRepublic. Available online: http://www.techrepublic.com/whitepapers/a-survey-on-cloud-computingsecurity-challenges-and-threats/3483757 (accessed on 18 March 2012).
3. Issa M. Khalil , Abdallah Khreishah and Muhammad Azeem," Cloud computing security: A survey." Available online: http://www.techrepublic.com/whitepapers/survey-on-antivirus-detection-techniques/2572716
4. Algirdas Avizienis. The n-version approach to fault-tolerant software. *IEEE Transactions on Software Engineering*, 1985.
5. Paul Baecher, Markus Koetter, Thorsten Holz, Maximillian Dornseif, and Felix Freiling. The nepenthes platform: An efficient approach to collect malware. In *9th International Symposium On Recent Advances In Intrusion Detection*. Springer-Verlag, 2006.
6. Josh Ballard. An Eye on the Storm: Inside the Storm Epidemic. 41st Meeting of the North Americian Network Operators Group, October 2007.