Managerial Procedural Technical Controls for Rootkit

Prajwal Sonawane[1], Rajeshwari Gundla[2], Siddharth Nanda[3]
[1]*U.G. Student,* [2]*Faculty,* [3]*Senior Faculty*
SOE, ADYPU, Lohegaon, Pune, Maharashtra, India[1]
IT, iNurture, Bengaluru, India[2,3]

Abstract - A rootkit is a collection of malicious software programs which exploits the target system vulnerability to provide root level i.e administrator privileges to the attacker all while concealing its presence on the victim's system. Rootkit is a combination of the word "root" (the traditional name of the privileged account on Unix-like operating systems) and the word "kit" (which refers to the software components that implement the tool).To be put in simple words it is a annoying virus which not only eats up your system resources but also puts your important and private data at a huge risk.

Keywords - Rootkit, vulnerability, victim, API, Target, Controls, Bios

I. INTRODUCTION

Rootkits can be traced back to the year 1999 which was a trojan virus known as NTRootkit which was developed to the windows NT and was created by Greg Hoglund.[1] Over the years the names of rootkits have changed but their core algorithm and subline goals remains the same. Rootkits can be installed via two primary ways one of which is a threat agent manually installs the rootkit on the target system and other is via an automated software.

Once it gets installed on the target system via any means such as piggy backing or a trojan attack, it boots at the same time as the computer's operating environment i.e operating system or after the o.s which makes detecting it a tedious task for the antivirus.[1] As the rootkit has admin level privileges it uses them to hide its installation and make amends to the thepre installed antivirus to prevent its detection or removal.[2]

Rootkits have been used by many external players and not only by hackers and nation state actors. One of the most well known use of such is under the belt of Sony Music Company which during the digital media piracy war in 2005 used a sublime rootkit to restrict the user's ability to modify or copy the contents of the cd data. The rootkit was created by the First 4 Internet company under the idea of copy protection software but once the existence of the rootkit was made public by Mark Russinovich, a few blackguard attackers started taking advantage of the vulnerability, this cost SONY in millions and the company had to deal with consumer scandals for a decade.[2]

II. TYPES

A. Kernel Mode - In this mode the rootkit can control all the system processes as it is implemented within an operating system's kernel module. It severely impacts the stability of the target's system[2]

B. Firmware - These rootkits gain access to the software that runs devices, such as routers, network cards, hard drives or system BIOS.[2]

C. Bootkits - These rootkits gain access to the software that runs devices, such as routers, network cards, hard drives or system BIOS.[2]

D. User Mode - This type of rootkit is installed in a shared library and operates on the application layer of the targeted system where it can modify API behaviour.[2]

III. INSTALLATION

Piggybacking - In this type of installation the user unknowingly installs a rootkit which was bundled with a trusted software. When the user grants permission to the application allowing its installation, the rootkit which was bundled also stealthily gets installed in the background on the target system.[2]

Blended Threat - In this approach the rootkit is combined with two more components which are as follows:

i). Dropper - It is a program which can be used to exploit the target system via brute forcing its way in or through social engineering and install the rootkit inside the victim's system.

ii). Loader - It is the second phase of the BT attack, it launches after the dropper program has been initiated either by opening or executing a file. The loader exploits all the possible vulnerability to ensure that the rootkit boots up the target system startup.

IV. CONTROLS

No system can be 100% secured from any type of malicious attack, and every company needs to have a certain preventive measures and corrective controls on which they can rely. Following are 3 of the emphasize able controls:

A. Managerial Controls - Managerial controls are also known as administrative controls as they fall in the hands of the IT staff such as the network manager of system admin. Under managerial controls the IT personnels are required to perform the audits and software updates for the system.

All the managerial controls or activities can be divided into three sub domains. [3] [4]

i). Updations - Updates are the one the most important part of any software as they keep the software functional and patch any new found vulnerability. A great example of this is updated antivirus engines, it is impossible to write all the available threat detection algorithm into the antivirus software when they are being written, as new viruses are being created every second and new vulnerabilities are being found everywhere updations are the most convenient ways to keep our system secure and up to date with the latest threats and trends in security.

As operating system is the primary target for rootkit keeping it updated is must as new updates patch up old vulnerabilities and hot fixes are used to close any new found backdoors, if we keep our o.s updated to the latest, rootkit will not be able to find the backdoor or the vulnerability which it was designed to exploit in order to gain access of the system.[4]

ii). Monitor - Rootkit can be installed via two ways, but both of them requires an external interaction either human or software. Monitoring the system for any such unauthorised interaction can help save the victim from the tedious task of detection and removal of rootkit. Rootkits get installed on the system, if the user continuously monitors the system for any unauthorised downloads or installations the rootkit malware can be stopped even before it gets installed and infects the system.

The system admin should also be alert for any abnormal system behaviour such as changes which can only be done under admin privileges as this shows that the system has been compromised by a rootkit virus. Since rootkit can hide itself from antiviruses monitoring the system for abnormal behaviour is the only surefire way the system admin can detect the presence of a rootkit malware.[4]

iii). Audits - Audits are the regular checks conducted by an administrator. Audits can be a checklist which is used as supportive document to perform the regular checks. The checklist may require the admin to perform and cross check different tasks such as

1. Are all the systems updated
2. Is the antivirus and firewall running on the latest update
3. Are the routine weekly checks being conducted.
4. Are all the softwares being installed via trusted sites
5. Is the antivirus enabled
6. Are all the files malware free
7. Do all the users have the required security clearance

B. Procedural Controls - Procedure is an established or official way of doing something, it is a series of actions conducted in a certain order. Procedural control is a list of different types of procedures which are created and laid out for the end user by the managerial staff, that the user needs to follow in order for the smooth functioning of the company.

These procedures may contain certain security policies which the user should abide by when in the residence of the company, these rules help the IT staff to secure the systems and therefore the company from any unauthorised access or malware disaster. It can be divided into 4 sub domains for a better and in depth understanding.[4][5]

i). Data Storage and Protection Policies - Data is the most important asset of any organization no matter how big or small, if the organization is unable to protect their data properly then they may have to face issues with maintaining their company standards and also other legal predicament.

There should be written document about how the data is being stored in the system and the user as well as the admin staff should know about the company procedure of storing and retrieving data. Every type of data should require a user authentication and security clearance for maximum protection. If the data is no longer needed then it should be completely destroyed.

Just securing the data from theft is not enough, data loss can also be as precarious as data theft. There should be physical data storage policy which should contain information about the timely data backups. These backup should be stored on different servers so as to protect the data from being destroyed under any zero day attack. Depending on the size of data dump and the ability of the organization, backup frequency should be selected.

ii). Training - As new technologies are being discovered on daily basis, the users should be trained on how to use them properly without causing any malfunction which may pave way for a attacker to exploit the software or the system. After successful installation of a new system the the organization should conduct several training sessions so that the users become aware of the minute details of the system and become used to the new environment.

As rootkit starts by gaining the admin privileges if the user knows what are the admin rights and how the system works it will be easier for the user to detect any type of abnormalities in the system and he/she can report it to the admin as soon as possible.

iii). Admin and Physical Security Policies - Rootkit can get installed in a system manually, so it is very important to a have strict security policies. Any type of storage devices should not be allowed on company grounds. A system can be made secure by installing antivirus and performing regular checks, the most vulnerable part of any system is the the system user. There should be a thorough check of the staff entering and exiting the company premises. Use of any external system or router should be prohibited inside the company and the user should be barred of taking any sensitive data out of the organization.

Social engineering is the easiest way to get a rootkit installed on any system, humans are the biggest loophole in the security framework. Physical policies should be properly defined and thoroughly checked for any type of loopholes. They should be followed to the core in order to keep the organization secure from any malware attack.

iv). Awareness - Only creating the policies is not enough, they should be known to each and every person working on company grounds. It is the sole responsibility of the organization that the policies are made available to all the users to read and understand. There should be sessions conducted on addition of new policies and the users should be made aware of them.

C. Technical Controls - Technical Controls emphasizes more on the technological part and access privileges unlike the other control measures. It uses technology as a base to check the working of the security architecture, its a collection of processes which are followed to check the proper functioning of the systems, servers, firewalls, access controls etc.

It is collective documentation of procedures and policies which is defined by the administrative or networking teams in an organization. They are the protective measures which a company undertakes to secure itself from any kind of malware attacks. Technical controls itself is a huge domain and consists of smaller secondary attributes which we can branched into different sub domains.[5]

i). ACL - Every company should have an access control list which contains the name of the user and his privilege levels and the rights he/she has on any particular data. This list should be updated frequently and routine checks should be performed in order to check the consistency of the list.

The system admin should monitor and take required measures when a data is accessed by any unexpected data. Rootkits are installed via system network and no attacker will use their own user id to perform the exploit, the admin staff should conduct regular checks for odd timed access.

The staff who has left the organization should be striped of their privileges and rights as soon as their 3 month notice period is over. There should be frequent checks for remote and wireless users as they make the security architecture the most vulnerable keeping the network ports open which may be used exploiters to perform a DOS attack and plant a rootkit using shell commands.[5][6][7]

ii). System users - In the whole paper we talked about what admin staff should do, but the system user is the person who should be the most alert while using the system as he is the first person to get acknowledged of the fact that his/her system has been compromised by a rootkit malware.

The user should check their system for any abnormal behaviour or changes, especially the ones which require the application to have admin privileges to perform any a ctions. If the system user finds any signs of rootkit or any other vulnerability he/she should immediately report it to the admin staff and should disconnect their system from the network to avoid spreading of it throughout the organization.

Every user should be taught about the basics of system security in order to keep the vulnerability level to a minimum and also because they should know what they are suppose to do in order to mitigate the risk.[7]

iii). Security Council - The security council is a group of administrators of different domains such as network, system and information. Their task is to perform their respective duties when the organization is functioning normally as well as when it is under attack. The network admin should work on the network architecture, performing tasks such as documenting all the new connections to the organization's network. He/she should have an updated network diagram of connected networks at all times incase a branch of the network falls prey to any malware attack. A back up plan should be in place if the main network goes down or an isolation of any sub network is needed.

System administrator should constantly be updating the firewall policies, creating and adding rules, updating the old rules to so as they can not be used to create a new vulnerability by attackers. Monitor incoming and outgoing traffic and generate a detailed tracking report on frequent basis depending on the network load as it might help the forensic experts to find the exact packet which carried the malware inside the system and via which vulnerable port. He/she should also configure the antivirus software properly to suit the company needs. Timely maintenance and updation of softwares also comes under their tasks.

V. CONCLUSION

We now know what a rootkit is, how it gets installed and what are its types. The main purpose of this document was to make people aware of the malware, how it infects the system and how dangerous it is if not removed as soon as possible. This paper also gives brief information about the three different industrial control approaches. These are the controls which organizations take to prevent, mitigate or remove the malware from their network. Prevention is always better than cure, the security policies should be made by keeping this in mind but also there should be a corrective measure ready as no system is 100% secure every architecture has a vulnerability a weak link which can be found and exploited and a structure is only as strong as its weakest beam.

VI. REFERENCES

[1]. https://en.wikipedia.org/wiki/Rootkit accessed on 17/3/19

[2]. http://www.tech-faq.com/rootkit.html accessed on 20/3/19

[3]. Riley, R., Jiang, X. and Xu, D., 2009, April. Multi-aspect profiling of kernel rootkit behavior. In *Proceedings of the 4th ACM European conference on Computer systems* (pp. 47-60). ACM.

[4]. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Security_Guide/s2-sgs-ov-ctrl-tech.html accessed on 20/3/19

[5]. https://searchsecurity.techtarget.com/definition/rootkit accessed on 24/3/19

[6]. https://en.wikipedia.org/wiki/Rootkit accessed on 17/3/19

[7]. Chiang, K. and Lloyd, L., 2007. A Case Study of the Rustock Rootkit and Spam Bot. *HotBots, 7*(10-10), p.7.