Direct Kernel Object Manipulation

[redacted]

Indiana University of Pennsylvania

Abstract

Direct Kernel Object Manipulation (DKOM) is a rootkit strategy, which hides, potentially harmful process, files, and network connections (Butler). Direct Kernel Object Manipulation may also be used to cause several other devastating threats to a computer system. The objective of this paper is to discuss the different threats Direct Kernel Object Manipulation posses, the process of a Direct Kernel Object Manipulation attack on a computer system, and strategies to detect a Direct Kernel Object Manipulation attack. Also this paper will explain the processes of how Direct Kernel Object Manipulation can be used to attack both Windows and Linux operating systems. Direct Kernel Object Manipulation is a relatively new security threat for computer systems and has surpassed other rootkit attacks such as hooking and trojanized programs.

DIRECT KERNEL OBJECT MANIPULATION

Introduction

Direct Kernel Object Manipulation, is considered the future of the rootkit attacks (. Due to the fact Direct Kernel Object Manipulation is such a new threat to computer system security, it is one of the most effective rootkit attacks because they are the least detectable. The reason why computer systems are so vulnerable to Direct Kernel Object Manipulation is because the technique allows a person to manipulate objects within the Kernel section of a computer system.

Background

The effectiveness of rootkits is based upon the ability to remain hidden (Butler and Silberman). Direct Kernel Object Manipulation Rootkits remain a substantial threat to computer systems because they are much more complex then other types of Rootkits (Florio). Rootkits are broken down into two categories, Ring 3 mode containing user mode rootkits and also Ring 0 mode operating Kernel rootkits (Florio). The Kernel rootkits category is much more complex then user mode rootkits because they work within the kernel (Florio) .The creator of a Direct Kernel Object Manipulation Rootkit must also be a very knowledgeable programmer because of how complex the process is for the development of a Direct Kernel Object Manipulation Rootkit (Florio).

Topic Description

The Kernel mode of an operating system is secure memory that is responsible for the many vital components such as processes, tokens, and ports (Butler). What makes Direct Kernel Object Manipulation so threating is that it bypasses the usual protections that are set in place because it is hidden and it is able to infiltrate vital kernel memory. (Florio). The process by

which Direct Kernel Object Manipulation rootkit is able to infiltrate a computer system helps us to understand how to protect ourselves from any Direct Kernel Object Manipulation rootkit attacks.

A general guide for a Direct Kernel Object Manipulation rootkit attack begins with an individual gaining a high level of access to a computer (Butler). Then that individual would need to install a rootkit onto the computer system (Butler). Next, the rootkit that was previously installed would then hide numerous processes, files, network connections, and even a backdoor (Butler) . This backdoor is especially dangerous because it would allow the individual the ability to access the computer system at another time, which neutralizes the security of the crucial memory stored in the kernel (Butler). Also due to the very nature of rootkits being components of the operating system, they have access to the kernel memory (Butler).

This process of a Direct Kernel Object Manipulation rootkit attack can be broken down more in much more detail (Florio). In essence the Direct Kernel Object Manipulation rootkit changes the list of active processes within the operating system (Florio). The Direct Kernel Object Manipulation rootkit does this by manipulating data within the EPROCES structures (Florio). Every Windows computer system contains EPROCESS structures, which are all connected one after another by what is called a double-link list (Florio)

Threads are the only things that run in the EPROCESS structures by swapping the active status of one thread to another runs them (Florio). The Direct Kernel Object Manipulation rootkit actually unlocks its own EPROCESS from the list of EPROCESS structure and then links the EPROCESS list that is directly before the unlocked one and the one directly after the unlocked EPROCESS list which effectively hides the unlocked EPROCESS structure (Florio).

This allows for the unlocked process to become virtually undetectable by the task manager and does not even affect the affect the system. (Florio)

In the Linux operating system, the Direct Kernel Object Manipulation rootkit manipulates what are called “task_struct’s” (Butler). These are the equivalent to the EPROCESSs of the Windows operating system (Butler). In a Direct Kernel Object Manipulation rootkit attack on Liniux system requires the attack to “remove a process from the list of prev_task and next_task.” (Butler). An important part of the Direct Kernel Object Manipulation rootkit attack on a Linux operating system is also ensuring the Linux scheduler does not freeze when it is determining whether a certain process is good or not. (Butler)

There are several tools that be used to detect a Direct Kernel Object Manipulation rootkit attack. One tool is called Backlight Beta, which is a hidden tool and is effective at detecting files (Butler and Silberman). Another tool is called IceSword 1.12, which is complex tool, which is actually able to detect hidden files, ports, and socket communications (Butler and Silberman). One of the most complex and effective tools to detect Direct Kernel Object Manipulation rootkit attacks is called RAIDE (Butler and Silberman). RAIDE is a tool that combines the strategies of all other rootkit detection tools and also provides the user of a computer with more detailed information about different hidden processes that may potentially be a Direct Kernel Object Manipulation rootkit. (Butler and Silberman)

Conclusion

It is vital that programs such as Blacklight Beta, IceSowrd 1.12, and RAIDE are all utilized in the process of defending against Direct Kernel Object Manipulation rootkit attacks (Butler and Silberman). It is vital because of how important the security is for the memory with the kernel. Also both individuals and business need to be able to rely on the memory stored on

their computer to be protected. Even though, Direct Kernel Object Attacks are very complex and hard to detect there are still tools that can be utilized to detect and fight back against Direct Kernel Object Manipulation.

References

Butler, J. (n.d.). DKOM (Direct Kernel Object Manipulation). Retrieved September 27, 2015, from https://www.blackhat.com/presentations/win-usa-04/bh-win-04-butler.pdf

Butler, J., & Silberman, P. (n.d.). RAIDE: Rootkit Analysis Identifcation Elimination. Retrieved September 27, 2015, from http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Silberman.pdf

Florio, E. (2005, December 1). When Malware Meets Rootkits. Retrieved September 27, 2015, from https://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf