Technical Sciences

УДК 004.056.57

Anuar Dusembaev
PhD, Associate Professor
Kazakh-British Technical University
Buzaubakov R.A.
student
Kazakh-British Technical University

SECURITY AND MICROVISOR

Abstract: Every days thousands of new malware signatures are detected and this number is only growing. Intrusion based security products have become ineffective. This paper talks about new micro-virtualization technology which aimed to secure computers from undefeateble attacks and stop the malware.

Keywords: security, microvisor, micro-virtualization, malware.

Introduction

Internet security breaches are growing. Viruses are one of the major causes of the rising number of security breaches. In fact, Kaspersky[3] reports that in 2015 new 4 000 000 virus signatures were detected, most of them are malware infections that aimed to steal money via online access to bank accounts. All detectors must be evaluated for accuracy against four key metrics, namely the proportion of True Positive, True Negative, False Positive, False Negative results that the detector produces. The vital metric which is important is the False Negative. This metric is not identified and thus present the real danger to all the users. The quality of anti-malware software depends on the

occuracy between False Positive and False Negative metrics. Non of the detectors are perfect and thus no one can guarantee total safety.

Day-by-day the malware signature database is growing and thus requires user to be up-to-date every time. Symantec[4] created more than 10 million unique signatures in 2010 and this number is growing anually. Every day thousands of new malwares are created which means a one more possibility for False Negative metric. Unfortunately today's rapidly moving front of highly tailored

malware adapts fast, leaves no time for human assessment, and makes historical attack data sets used to tune detectors significantly less useful.

Zero-day trends

A zero day exploit is a cyber attack that occurs on the same day a weakness is discovered in software. By then, it's misused before a fix gets to be accessible from its maker. At first when a client finds that there is a security hazard in a software, they can report it to the product organization, which will then build up a security patch to alter the flaw. This same client may likewise take to the Internet and caution others about the flaw. Normally the system makers rush to make a fix that enhances program insurance, in any case, some of the time programmers catch wind of the blemish first and rush to endeavor it. When this happens, there is little protection against an attack because the software flaw is so new.

Organizations at danger from such flaw can utilize a few method for discovery, including utilizing virtual local area networks (LANs) to ensure transmitted information, by making utilization of a firewall, and utilizing a safe Wi-Fi system to secure against remote malware attacks. Additionally, people can minimize the danger by keeping their working systems and programming progressive or by utilizing sites with SSL (Security Socket Layer), which secures data being sent between the client and the site.

A zero-day attack, at its center, is a flaw. It is an obscure endeavor in the wild that uncovered a powerlessness in programming or equipment and can make confounded problems well before anybody understands something is wrong. Indeed, a zero-day attack leaves NO chance for discovery at first.

In 2015, Kaspersky Lab solutions detected ransomware on more than 50,000 computers in corporate networks, which is double the figure for 2014[3]. As for specific recommendations agains zero-day attack the anti-virus software developers can only suggest some strategies to reduce the possibility of a successful target attack and nothing else.

Proposed Solution

Instead of collecting the signatures of the malwares the right solution will be its determination in advance. The only way to achive this is by wrapping the process into separate environment. In 2012 Qubes OS[5] was released. It implements a Security by Isolation approach. The main idea of Qubes OS was that no software is perfect and thus there are lot's of lines of codes in any software that would make malicious software to take control over a machine. This idea broght the concept of micro-virtualization. Micro-virtualization is a new system architecture that uses hardware virtualization features, as offered on current CPUs, along with an innovative hypervisor called a Microvisor, to effortlessly hardware-isolate user-initiated activities or software programs operating on an endpoint[1]. In 2010 Bromium project was introduced which come up with idea of per-task introspection, simplifying the identification of forensic monitoring of malware as it runs isolation. Running a new light-weight micro-VM per user activity and providing visibility for only required resources made the malware attack impossible to success because everything is limited and each malware activity is recorded. The Microvisor makes sure mandatory access control for access to any privileged system resources to prevent privilege escalation, and it also immediately converts the format of harmful content that

accesses privileged resources (printers, clipboard, etc.) to stop potentially harmful content from striking the OS kernel.

Conclusion

In this paper we explored the existing solution for malware handling and analyzed its disadvantages. The development from programming driven to equipment based security guarantees an unrest in on-line security and it proclaims some unexpected advantages: However PCs can't recognize good from bad, they are good at implementing the standards of "need to know" – not with human factor errors. Micro-virtualization is a new way of securing desktop PCs. It isolates each singular process into separate micro-VM, offering security groups an environment where malware can’t succeed.

References

1. Dalziel, Henry. How to Defeat Advanced Malware: New Tools for Protection and Forensics. Syngress, 2014.

2. Bromium Project. Micro-virtualization technology overview. https://www.bromium.com/advanced-endpoint-security/our-technology.html

3. Overall statistics for 2015, Kaspersky Security Bulletin, 2015. https://kas.pr/KSB2015_pdf

4. Wired Business Media, January 06, 2012. “Symantec Confirms Hackers Accessed Source Code of Two Enterprise Security Products.”

5. Qubes OS homepage. https://www.qubes-os.org