International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2000-000X
Vol. 1 Issue 6, August – 2017, Pages: 197-201

Software Engineering Security

Modern Malware

Mourad M.H. Henchiri
Lecturer: dept. of Information, Systems University of Nizwa, CEMIS,
Nizwa, Oman
mourad@unizwa.edu.om

Abstract: *Digitization is the era of today, and today's success is measured based on the integration within digital competitors. It's a life contest to be available between all challenges in your surrounding fields and precisely the today's technology. With the help of the Universities, the software engineering is becoming an industry nowadays with strong reputation. And the available realisations on the markets are proofs, and at the same time are targets for the dark side of the digital world; through diversified electronic attacks which are the non authorised data usage or non-permitted frontiers bypassing by non-authorised objects; either human users or automated applications. As per the year 2019 the world would be in need of five millions of digital security experts, yet, the availability will be one million less[1]. As first scientific study through this research is that to prove that IT specialists have to go after dedicated security intense explorations and trainings [2]. Also, this study would prove that theoretical certificates would not promote individuals to the practical skills required within the real-world-fields of action. Thus, our realisation here in this study, brings to the hand of all, the ease of use of the common security practices to defend what hackers might think of and act in. Here, the main idea of this paper is a real forensic driven solution implemented based on the usage of powershell packages and libraries to deploy the best memory traces tracking when investigating attacks traces over a designated storage memory. Besides to a modern dominating attack's scenario and defense solution, that would face any one of us, which is the ransomware.*

Keywords: Digital security, IT specialists, hackers, crackers, forensics, vulnerabilities

1. INTRODUCTION

Reaching a secured framework; whether a network or a software solution, versus every and each malware attack, is a continued and a non-stop activity of all security solutions providers[3]. yet, this is a hard to achieve wish since the modern malware are personal scripts, user-defined, which means they are written instantly, proper, and with different implementation tools. And for this reason no respective hash or pre-existing filters to detect such realizations. And as per the main successful attacks are to succeed in trespassing the available security and have the use of the vulnerabilities for the longest time periods without being detected.

In the Microsoft environments, technology is deeply effective and complex when in action to achieve any soft process or service[4]. The case in action here, to demonstrate this given, is the Microsoft Messaging Protocol(MMP), which is a service system friendly, by default is set to off. Here, attackers take the advantage of planting their malware to activate this protocol, which would never be detected based on soft filters and security soft solutions. The MMP here would be the backdoor and the remote controlling tool to the attackers.

Modern malware are smart complex technology adoption within secure environments, their actions are successful and effective when ever watched and analysed.

The effective scenario, presented here, using the MMP in help, is only an experimental successful realisation example that all Microsoft users must know and be aware of. On the basis of the MMP, and through this paper, we would reveal the issues in security caused when misusing the MMP, through an automatic solution for a better security deployment; an automated activity of when to on or off the MMP service. In this paper we put the choice on a cracker basis:

- Forensic techniques against hackers; think like a hacker to grab all and every single data from an investigated memory (Section VI).
- The choice of evaluation techniques when facing the Ransomware scenarios affects the solution case when remedial actions are set. We identify and discuss these symptoms in Section VII of this paper.

2. HACKER'S MIND FOR THE BEST SECURITY

Clearly noticed, that everyone in the IT security world lives in continuous fear that they may be vulnerable to the next high-profile breach. And the list is large and goes on: Specific Targets, Large Trends and manufacturers and even single end users with the necessary skills. And this is not all, though there are dozens of other incidents. Things has to change, and it will ever so slowly.

Paula Januszkiewicz, CEO of CqureAcademy[8], has been going around the world talking about continuous security validation. Rather than reacting to events as they unfold, Paula says organizations need to change their mindsets and think of continuously challenging their security defenses and security operations center teams via the right trainings based on breach simulations.

Besieged as they are by attacks from nation-states and cybercriminals, Paula says companies need to focus on the latest technologies with their back-end hiddenness, as well as understand what the hacker wants to steal, and then map it to a cyber-kill chain and break the steps in that kill chain.

Today the reality is demonstrated as follows: variety of attacks with different techniques happens and they will happen as long as there are humans who use digital solutions on this planet. However they should not succeed nor reach if you properly protect your infrastructure. Did you check the available weakness right now in your IT security system? Isn't it better to find it before an untrusted source or hacker does that for you?

If you underestimate, be sure that even a small scale security breach could leave your business in poor undesired condition. Frequently and daily, you can apply basic behaviors to bring your company to a secure state from attack. You will not be happy to know that a hacker is using the same paths often to enter your system! In conclusion the issue we face, related to the information security is a spread business issue! Let's put you into the hacker's role, and perform all the activities they would to better understand the threats.

From the best practices that would be absorbed for a better skill, we set the following:

- Penetration tests, in order to check for misconfiguration and vulnerabilities
- The newest threats to the infrastructure
- Facts around management, monitoring and hardening
- New technologies that are needed to keep up with the evolving insecure world

3. PHYSICAL ACCESS

In modern environments, security tackles modern issues; thus, physical infrastructure is a crucial target to different malware. Vulnerabilities available in physical environments are numerous, yet, most of them are controlled and given measures when used[5]. Thus, physical attacks are selective, when all of them might give results, but, because of the default accounts of different physical infrastructure equipment, physical security is raised to a higher level. Vulnerabilities here, could be categorised under three groups:

1- Off-line mode access
2- Autoruns tools
3- Encryption/Decryption

The security here, pushes us to defend those scenarios; accordingly and respectively:

1- Preventing the off-line mode access, whether from the domain level or the machine level.
2- Autorun tools cannot play in modern environment by default, yet, when activated, be careful and trust investigators.
3- In Microsoft environments, data must be encrypted, in order to apply security policies

4. DATA IN SECURITY

In the digital world, every person is secured, safe and in stable state; because nobody in the digital world care about you as you are, yet, they certainly care about your data[6]. Intruders, spies, attackers and even script kiddies care about your data. All kinds of data are available for attack and vulnerable to different kinds of attacks and data bleach, mainly[5]:

1. Injection; two main and major attacks based on the injection are analyzed, which are:

a. Steganography: the art of camouflage; hidden a complete file inside another file, file type and extension is not the matter, usually is successful. And once the injection is done, it is almost undetectable, means not to be detected, the resulting file is only seen and the one injected is hidden and to be seen only after the appropriate extraction steps.

b. Codes injection: technical analysis proves that the injection of a script inside of an executable is the best practice to spread your solutions and achieve your goals. Thus, scripts and codes are to be used clear written solutions or executable, then injected in different installing packages and setup files(might be pirated software). Once the setup or the installing package is executed the hidden and injected solution is launched silently and its process is effective.

2. impersonation

Reaching roles with unauthorized permissions is an act of impersonation; raising privileges, removing authorizations, according access and editing users accounts…

The scenario of impersonating an activity or a user account is successful when bad configurations are set and different access scenarios are possible which represents vulnerabilities; mainly the off line access, and also when privileges are given to non-skilled objects which by turn has access to the registry keys.

3. Phishing

Which are the main prior techniques hackers and crackers think of. And they are effectively successful [7].

Social engineering is the legend of success to the phishing attacks in all scenarios. Not only the digital world I sunder attack by the phishing scenarios, but, from all network access methodologies and all networks; computer networks, mobile networks, cellular networks and even satellite networks.

5. INTERCEPTING COMMUNICATION

From the major concerns in wireless communication we narrowed the research after a long analytical study to the access methods, which has to raise up the security level when authenticating and awarding access. This concern is vital also when designing wired infrastructures to avoid all kinds of attacks and mainly intrusions. This security takes in consideration the communication through firewalls, the secured set up of remote access and also domains configuration to avoid network based attacks like the ARP poisoning and DNS poisoning. Thus, intercepting communication is the concern of all, IT professionals, experts, technicals and theoretical professors.

6. FORENSIC TECHNIQUES AGAINST HACKERS (MODERN NOTES FROM PRACTICAL COMPARATIVE STUDY)

Advanced security solutions in current era are really modern, brave to act when necessary effective when facing detectable intrusions. Yet, all with no exception comes to a level of complete ineffective toward the user-defined malware; modern malware, no suspect to follow or process to filter not even a service to put under control.

Thus, the following technique is given birth right for the modern user-defined attacks; forensics are the real-world investigation and revealing of all kinds of traces [8]. This process has to be automated for the purpose of amelioration; security solution reputation amelioration.

In this section we present the first part of the contributions of the paper; the forensic demonstration here is a key definition of the solution against hackers and attackers trying to evade the effects.

First priority is selecting the utility; in our case, we are using a VHD file. Then reading the drive contents and we ask the Master File Table.

The scenario within the algorithm below treats an extracted executable file with the memory index 38:

```
$VHDPath="C:\vhdFile.vhdx"

$disk= Mount-VHD -Path $VHDPath


Install-Module PowerForensics

Import-Module PowerForensics -Verbose

Get-ForensicFileRecord -VolumeName x: | Where-Object {$_.Deleted}
```

```
$fr=Get-ForensicFileRecord –VolumeName x: -Index 38
$fr | select *
$fr.Attribute

$fd=$fr.Attribute | Where-Object {$_.name –eq 'DATA'}
$fd.DataRun

Get-ForensicVolumeBootRecord -VolumeName x:
    Invoke-ForensicDD –InFile \\.\X: -Offset (8267*4096) –BlockSize (130*4096) –Count1 –OutFile c:\oFile
```

It is crucial to declare that you got to download the "PowerForensics" library. Here, in this context and scenario, we have information in output about the data kept on a disk for this file "oFile".

Status of the File is seen:

- Sparse
- not sparse
- where it starts; the cluster number its length in clusters

The good news is that if it is not kept on the disk in one piece; split into multiple fragments, it is not more complicated at all but it requires more PowerShell commands which makes the process more error prone.

7. RANSOMWARE TECHNIQUES AND SCENARIOS

The best description of a ransom ware is stating a real world scenario; we have followed, analyzed then concluded the results for a scientific purpose to present it in public. Here, we give the indices of the happened ransom ware attack; which it started at an incoming mail payload; a link to an audio message through the dropBox. All the criteria here proves that the attack is about to start, or in another sight, the mail receiver is on a risk of being paralyzed electronically. Till date of this research study no voice messages to be shared through the drop Box [8]. Yet, here it is a proof of that the scenario is playing the game of dominating by influence; if the mail succeeds in influencing the reader so that this attack is succeeded. The main aim of a such attack is to gain an access to the victim's device then a full control, the control based on a ransomware is the total encryption of all data available on the related storage equipment. Such attacks are tacking a deep care of conveyance; they have to be very conveying to every reader, which is the victim, in order to reach the target of the attack.

In this section we present the second part of the contributions of the paper; the ransomware is software that might be affecting your device as a final state of a fallacy; not trusted digital communication. In this scenario we treated the example of encrypting the Most Recently Used files (MRU):

```
Sub MostRecentAttack()

    Dim E As Integer


    For E = 1 To RecentFiles.Count

      Selection.TypeText  Text:=RecentFiles(E).Name

      Selection.TypeParagraph

    Next E

End Sub
```

For security purposes we presented only the browsing program used to detect the Most Recently Used files within the Microsoft environment, and written in VBA [9].

8. CONCLUSION

Evading the hackers hook is an aim, since the modern malware properties is a strength and success when communicating with current systems. They may impersonate identities, processes and even services without being suspected. Microsoft environment is giving birth to new technology that empowers security potential to both; users and enterprises. And from the research outcomes, the security starts from the personal knowledge and skills. It would raise the level of reconnaissance to a higher level where automated security solutions cannot achieve such reconnaissance. Modernizing the technological signature of a given corporation is the first step to face the high wave of change and the deep technical necessity to avoid been behind the market challenges and to be ready and able to prevent external intrusions. Though this security and technical issues prevention is dedicated and proper to specific measured contexts when realized, yet, it is to be valid for both platforms; genuine licensed, mainly Microsoft, and free open source. The scenario of forensics given birth in this research is the step to the cultural trust between the technical obscurity, which hides all frustrating knowledge, and the concerned users, interested by the current research outcomes.

REFRENCES

[1] Forbes/Tech Steve Morgan, JAN 2, 2016 THE LITTLE BLACK BOOK OF BILLIONAIRE SECRETS
[2] Best Information Security Certifications For 2017 2017 Purch http://www.tomsitpro.com/articles/ information-security-certifications,2-205.html
[3] AN OVERVIEW OF THE SECURITY CONCERNS IN ENTERPRISE CLOUD COMPUTING, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011
[4] Microsoft Security Intelligence Report - Download Center Volume 16 | July through December, 2013 Available at:http://download.microsoft.com/download/7/2/b/72b5de91-04f4-42f4- a587-9d08c55e0734/ microsoft_security_ intelligence_report_volume_16_engli sh.pdf
[5] Security Journal Nedap Security Management Issue, 2014 http://www.nedapsecurity.com/sites/default/files/ nedap_security_journal_2014.pdf
[6] Data Security and Privacy in Cloud Computing Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages http://dx.doi.org/10.1155/2014/190903
[7] Study of Ethical Hacking International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 2014
[8] Where Windows hackers 2017, Available: https://cqureacademy.com/level up
[9] GenBroker - OLE Automation Support.doc – v8 Copyright 2004 ICONICS Available at: https://partners.iconics.com/