Brainae Journal of Business, Sciences and Technology
ISSN ''2789-374X (print)" "2789-3758 (online)
Volume 26, Issue 5, January 2023
http://www. brainajournal.com, info@brainae.org

# MALICIOUS SOFTWARE ATTACKS AND ANALYSIS ON NETWORK APPLICATION IN THE ORGANIZATION

**Authors:** [1]Mr. Martin NSENGIYUMVA, Dr. Michael Sanja MUTONGWA (PhD)®
Corresponding authors: nsengam01@gmail.com and msanja@uok.ac.rw/sanjammical@gmail.com
*University of Kigali, School of Graduate Studies
Mobile: +250787951396, **Tel:** +250 783 658 167
**Received:** 10 December, 2022; **Accepted:** 15 December 2022; **Published:** 25 January 2023
https://brainajournal.com/paper?Id=133

**ABSTRACT:**
The growth of the ICT usage in dairy activities has been the biggest social and technological change in recent times reduces barriers to trade, and is playing a huge role in supporting sustainable development in many countries, subsequently, the number of computer threats are growing, malicious software in circulation has increased in those last two years, according to Kaspersky Lab. solutions blocked 796,806,112 attacks launched from online resources located in 194 countries across the globe in this year. The Internet has become an essential part of everyday life. As a result, sensitive personal and credit cards information are examples of monetary gains to malware or virus writers. The main purpose of this project will highlight existing malware mechanisms and their protections and how the malware forensics techniques can be applied to counter future attacks. Likewise, the limitations of anti-virus programs and the current computer security is discussed. In beside, with the theoretical study of the technique of malware forensics that can be used against malware attacks, a practical case study carry out to attain better understanding of malware internals and current forensics tools. The output of this paper work determine a better malware forensics tools and techniques that can be used for efficient malware detection then show the limitations of the techniques for fighting current and future malware. Malware uses advanced techniques to protect and hide itself from both protection and forensics tools.
**Key Words:** *malicious software, attacks, analysis, network application, organization*

## 1. INTRODUCTION

A malware attack is a common cyber-attack where malware (normally malicious software) executes unauthorized actions on the victim's system. The malicious software (known as virus) encompasses many specific types of attacks such as ransomware, spyware, command and control, and more. Anyone with a computer connected to the internet and anyone with important data stored on their computer or network is at risk, including government or law enforcement agencies and healthcare systems or other critical infrastructure entities (Samanvay Gupta, 2013).
Malware is malicious software that enables unauthorized access to networks for purposes of theft, sabotage, or espionage. There are many types of malwares, and many attacks use a combination of several types to achieve their goals. Malware is usually introduced into a network through phishing, malicious attachments, or malicious downloads, but it may gain access through social engineering or flash drives as well (2020 Overwatch report, 2020).

Through the infrastructure, the attacks may use malware threats to attacks the IT infrastructure of an organizations that can operate in one of several modes. An attack can come through the wires, as a hostile program like examples: a virus, a Trojan horse program, as a denial-of-service attack. Some IT element may physically have destroyed like a critical data center and communications link may compromise; IT hardware may destroy. A trusted insider may be compromised such a person, for instance, may provide passwords that permit outsiders to gain entry; also, insiders may also be conduits for hostile software or hardware modifications (David A. Patterson, 2003).

Hackers in the network of the organization can causes many losses and sometime destruction of the organization infrastructures, some hackers called white hat hackers, this type are paid by legitimate companies and governments to test the security of a devices in the networks or systems of the organizations. The goal is not to steal or modify data but to help to protect it. While other called, black hat hackers want access to collected data for many reasons, including stealing data, selling it, damaging the reputation of a person or company, and causing political unrest (Cisco, 2018).

## 2. STATEMENT OF THE PROBLEM

In the network organization, the hackers can causes the losses and destruction of the business, the bad people called Black hat hackers access information in the network of an organization with different reasons like to steal those information, to sell the information to a third party, modify the data, disable functionality on devices of the organization, to disrupt or to damage the image of a legitimate company or enterprise, access devices, web pages, webservers, to create political conflicts or to make a political statement, access user IDs and passwords to steal identities, access data to commit a crime or hack into systems to prove that they can do it. Security best practices methods must be taken to ensure the authenticity, integrity, and security of the data or information of the organization must be maintained and monitored. (Cisco, 2018).

Malicious software, commonly named "malware," continuously presents one of the top security concerns, and causes remarkable worldwide financial losses for organizations.

All the above would protect critical infrastructure such as the National Backbone (NBB), National Data Center (NDC), 4G LTE last mile networks, e-Government systems, Energy Infrastructure, Banking and Finance systems, etcetera. Those infrastructures need to be highly protected both logically and physically. Computer malware are the Internet's enemy number one, Modern malware are complicated comparing to the old generation. They use many techniques to escape the detection of the anti-virus programs and tend to operate silently at the background.

Every day, hackers release attacks designed to steal confidential data and an organization's database servers are often the primary targets of these attacks. Databases are one of the most compromised assets (Verizon Data Breach Investigations Report, 2015).

"The reason databases are targeted, are the heart of any organization, due to the databases are storing customer records and confidential business data" said Morgan Gerhart, 2015. He added organizations are not protecting these crucial assets well enough (Roy Maurer, 2015).

The purpose of this project is to identify the techniques and tools used to protect Internet's users from the malware threats, in order to protect the network infrastructures and databases. As well as the understanding how, the malware is built and how the attackers use it, this is becoming important for software engineers, system administrators, and IT security field for securing the network of an organization.

## 3. OBJECTIVES OF THE STUDY

The study looks for relevancy techniques and tools used to be used in the organization to protect the organization network and internet's users from the malware threats. This study was guided by the flowing specific objectives:

i) To establish the effect of Malware threats on organization network.
ii) To examine out how Black hackers use malware threats on organization network.
iii) To analyze the effect of Infrastructure on organization network.
iv) To Find out the effect of Database framework on organization network.

## 4. RESEARCH HYPOTHESIS

This research verified by the alternate hypothesis.

**H1)** There is a significant effect of malware threats has on organization network,

**H2)** There is a significant effect of black hackers has on organization network,

**H3)** There is a significant effect of infrastructure has on organization network,

**H4)** There is a significant effect of database framework has on organization network,

## 5. CONCEPTUAL REVIEW

### Malware

The word malware derived from the two combination "malicious" and "software". Malware is data without appropriate approval. Like examples: adware, bots, ransomware, rootkits, spyware, Trojans, viruses, and worms.

By Understanding malware threats and other threats on the use of internet, in the modern world of today, the internet is a virtual networking medium that can be connected and used on a multiplicity of devices. It allows the users to send, receive, collect, store, update, delete, and many other different operations of the data across the world.

Internet usage is expanding its boundaries every day, as the technological advance is massively. The major uses of Internet are as flows: e-commerce, e-learning, knowledge sharing, social connectivity, variety of media, file transfer, communication, etc. (educba.com).


***Figure 1.: the top users of the internet. I will be explaining in details how it works.***

The uses of internet growing-up and technologies devices, the world is facing the main challenges of malware threats, also increasing in high speed all over the world, for data stolen, and infrastructures destructions, Investigate the infected user's local network and steal sensitive data.

Malware is a term used to describe malicious applications and code that can cause damage and disrupt normal use of devices. Malware can allow unauthorized access, use system resources, steal passwords, lock you out of your computer and ask for ransom, and more.

### Internet

The study support end users' awareness of their responsibility towards the security on their network connectivity that can influence protection of their data/ information of the organization and announce perception about the linkage between securities and services delivery. Finally, this study will be relevant to students of ICT as a reference material.

### White hat hacker

White hat hackers, this type of hackers is paid by legitimate companies and governments to test the security of devices in the networks or systems of the organizations (Cisco, 2018).

### Black hat Hacker

Black hat hackers want access to collected data for many reasons, including stealing data, selling it, damaging the reputation of a person or company, and causing political unrest. (Cisco, 2018).

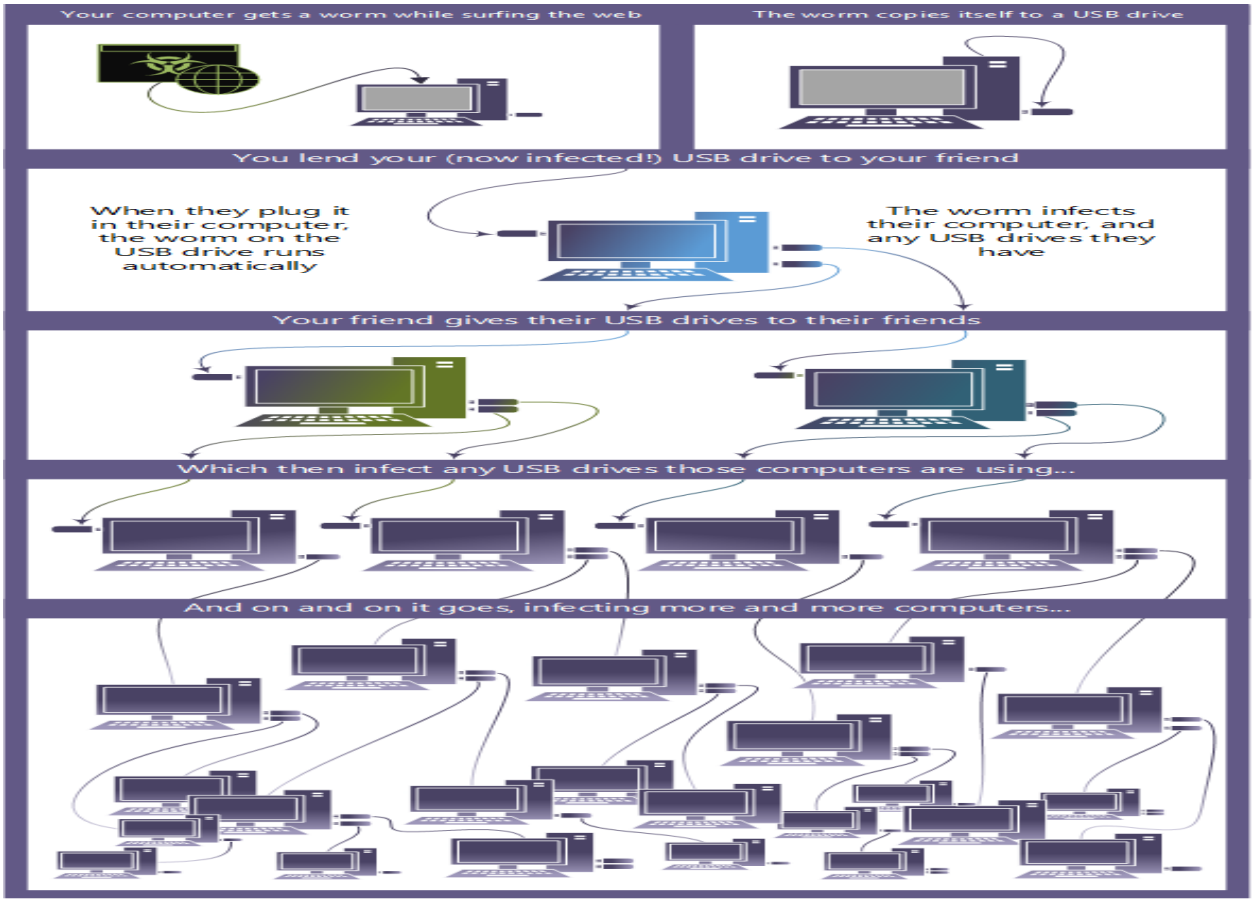



***Figure 2. This image shows how a worm can quickly spread through a shared USB drive***

The software enabled crime is not a new concept; computer enabled fraud and service theft evolved in equivalent with the information technology that enabled it. Since the advent of mainframe based automated bank account systems, financial institutions have been victims of malware-based cyber-attacks. Criminals altered software to transfer other people's money to accounts they controlled, and let down the accounts anonymously. Cybercriminals select their targets, if only by selecting the operating system platform on which malware may be processed.

## 6. THEORETICAL FRAMEWORK

This study familiarized with theory and models to validate how system security in institutions or organization public and private services are relates to theory. That has been briefly studied in the context of information. This study was used DeLone and McLean IS Success Model and others that related to the study like Theory of Reasonable Action (TRA) (Fishbein and Ajzen, 1975), Theory of Planned Behavior (TPB) (Ajzen, 1985, 1991), Decomposed Theory of Planned Behavior, (Taylor and Todd, 1995), the Technology Acceptance Model (TAM) (Davis, Bogozzi and Warshaw, 1989, Technology Acceptance Model 2 (TAM2) Venkatesh and Davis (2000) and Technology Acceptance Model 3 (TAM3) Venkatesh and Bala (2008), also use the software development life cycle model in development of simulated model and malware detection model analysis.

### DeLone and Malone's model for information system success

The information systems success model alternative names of the theory are: DeLone & McLean Information Systems Success Model, DeLone & McLean IS Success Model and D&M IS Success Model is an information systems (IS) theory which seeks to provide a comprehensive understanding of IS success by identifying, describing, and explaining the relationships among six of the most critical dimensions of success along which information systems are commonly evaluated.

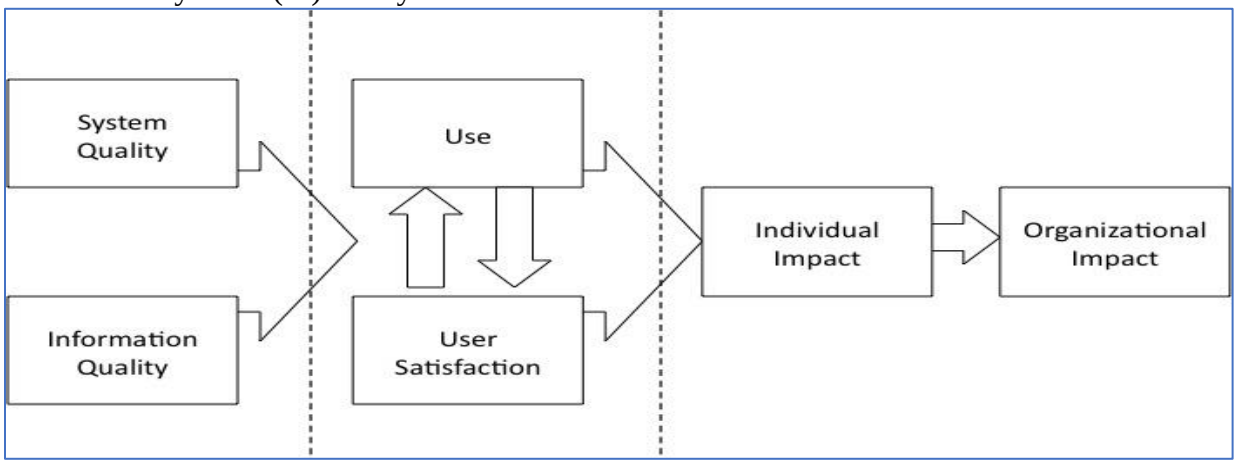



***Figure 3: Information Systems Success Model (DeLone & McLean 1992)***

The Information Systems Success Model (DeLone & McLean 1992) IS success model has been cited in thousands of scientific papers, and is considered to be one of the most influential theories in contemporary information systems research. After ten years of D&M IS success model publication, based on the evaluation of the many contributions to it, DeLone and McLean proposed an updated IS success model (DeLone & McLean 2002, 2003).

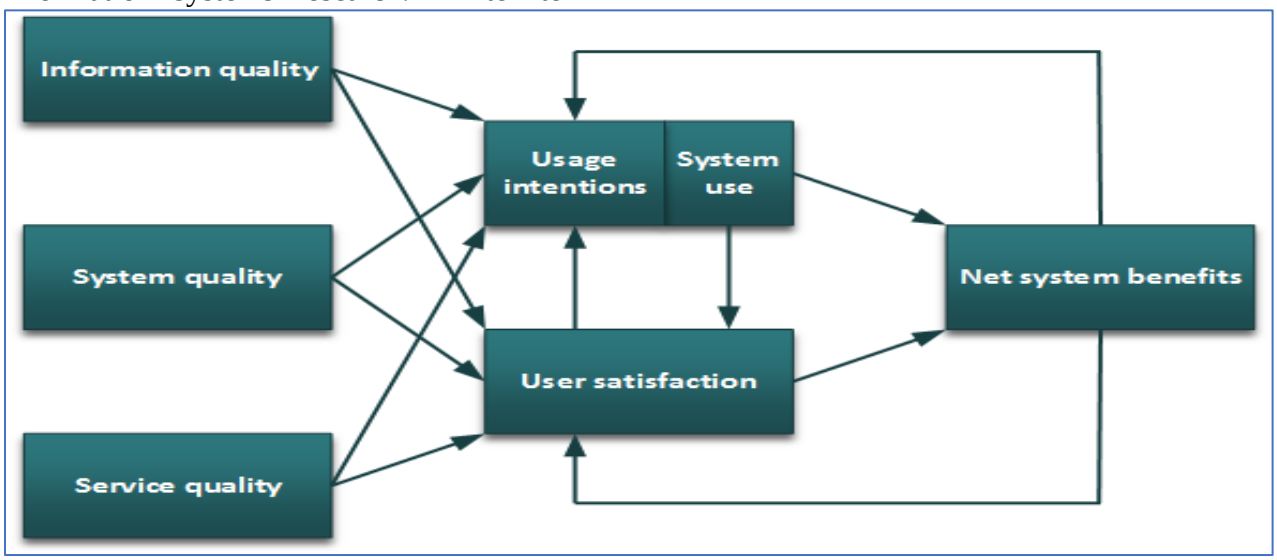



***Figure 4: Updated Information Systems Success Model (DeLone & McLean 2002, 2003)***

The DeLone & McLean IS success model has identified and describes the relationships among six critical dimensions of IS success: Information quality, System quality, Service quality, System use/usage intentions, user satisfaction, and net system benefits.

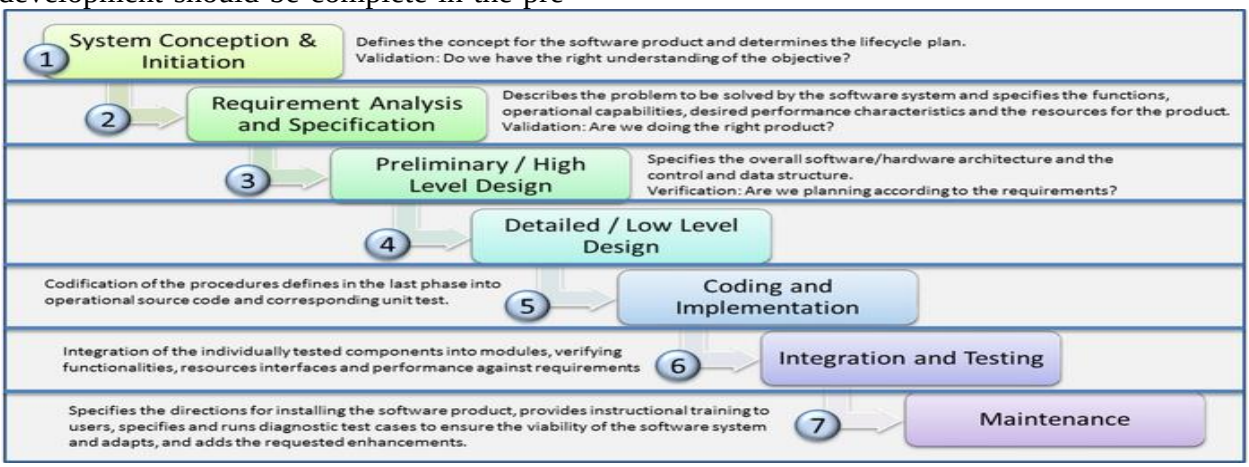
**Technology Acceptance Model Theory (TAM)**

Technology Acceptance Model (TAM) was introduced by Fred Davis in 1986 for his doctorate. TAM is specifically tailored for modeling users' acceptance of information

systems or technologies. User acceptance is a pivotal factor determining the success or failure of any information system project, (Davis, 1993).

**Software development life cycle (SDLC)**

Software development life cycle (SDLC) is a systematic process for building software that ensures the quality and correctness of the software built. SDLC process aims to produce high-quality software that meets customer expectations. The system development should be complete in the pre-defined time frame and cost. SDLC consists of a detailed plan which explains how to plan, build, and maintain specific software. Every phase of the SDLC life Cycle has its own process and deliverables that feed into the next phase.




***SDLC stands for Software Development Life Cycle and is also referred to as the Application Development life-cycle.***

**Concept framework for simulation application**

The concept framework for modeling and simulation techniques or methods are present in many areas, including system engineering, acquisition, training, analysis, experimentation, planning, testing, results as well as the recommendations from the simulation.

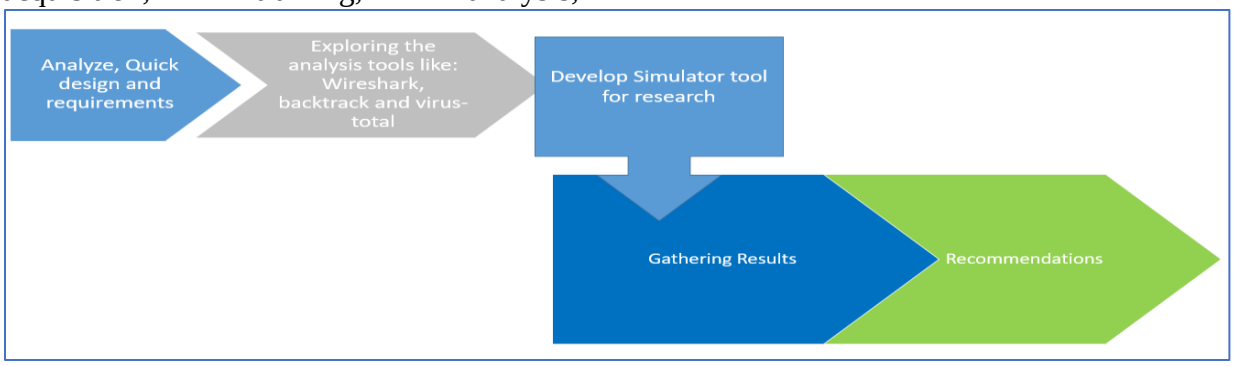



***Figure 5: Concept framework for simulation application***

This should be based on factors include (but are not limited to) proprietary architectures, lack of consistent and clearly defined development standards, model fidelity, and scalability issues that computer science and software engineering have yet to over-come. Develop standards and frameworks in the areas of conceptual modeling, because conceptual development stages carry implications for multiple decisions that heavily impact future stages of system development and performance.

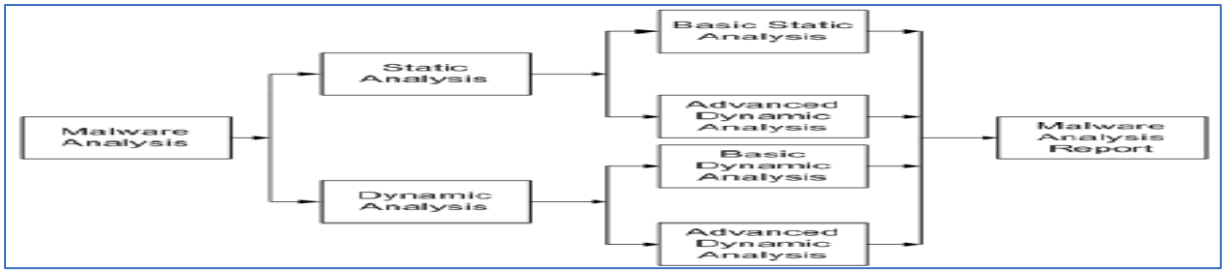



***Figure 6: Malware analysis stages***

## 7.MATERIALS AND METHODS

Cross-sectional surveys are studies aimed to gather data from a sample of population at a particular point in time. A survey is an investigation of the opinion, or behavior of a particular group of people, usually through asking them questions. In adopting cross sectional survey, data was collected from a large number of internet end users at one point in time. A sample size had been applied for quantitative. This means that every client fulfilling the eligibility criteria that had been presented and willing to take part of the study was being part of the sample. By calculating sample size Alain Bouchard states that when the population being investigated is less than or equal to one million people, it is made to match a sample of 96 individuals with margin of error of 10%. The following formula led to the size of people to question.

$nc = \frac{n}{1+\frac{n}{N}}$ , So $nc = \frac{n}{1+\frac{n}{N}} = \frac{n}{\frac{N+n}{N}} = n.\frac{N}{N+n} \Rightarrow nc = \frac{N \times n}{N+n}$

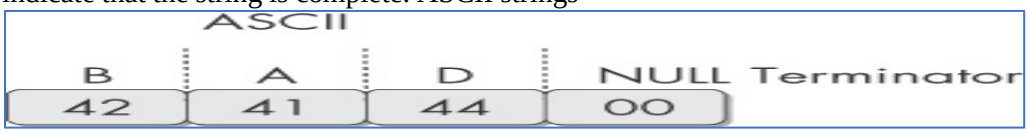
$\Rightarrow nc = \frac{271225 \times 96}{271225 + 96}$

$\boldsymbol{nc = \frac{26037600}{271321} = 95.96 \approx 96}$ Individuals

By collecting data, the researcher consulted different sources of information namely Secondary data and primary data. For gathering secondary data and information, existing Literature was used; previous studies related to these research objectives have been consulted such as Books; journals; available articles and reports from reliable sources, reports and different reports with the direct linkage with the topic. Existing literature was used specifically for the purpose of analyzing the factors affecting the organization applications security through the malware threats in Kigali. To collect primary data, questionnaire was designed to be filled by members that are part of our sample size namely MMI (Military Medical Insurance) staff, the researcher also prepared a focus group discussion were required to ensure the analysis based on the convergence of various evidences related about investigating factors affecting network and applications security.

## 8. FINDINGS AND DISCUSSIONS OF THE RESULTS

Searching through the strings can be a simple way to get hints about the functionality of a program. For example, if the program accesses a URL, then you will see the URL accessed stored as a string in the program. You can use the Strings program Both ASCII and Unicode formats store characters in sequences that end with a *NULL terminator* to indicate that the string is complete. ASCII strings use 1 byte per character, and Unicode uses 2 bytes per character. Figure shows the string BAD stored as ASCII. The ASCII string is stored as the bytes 0x42, 0x41, 0x44, and 0x00, where 0x42 is the ASCII representation of a capital letter *B*, 0x41 represents the letter *A*, and so on. The 0x00 at the end is the NULL terminator.




*ASCII representation of the string BAD*

Figure shows the string BAD stored as Unicode. The Unicode string is stored as the bytes 0x42, 0x00, 0x41, and so on. A capital B is represented by the bytes 0x42 and 0x00, and the NULL terminator is two 0x00 bytes in a row.


*Unicode representation of the string BAD*

When Strings searches an executable for ASCII and Unicode strings, it ignores context and formatting, so that it can analyse any file type and detect strings across an entire file (though this also means that it may identify bytes of characters as strings when they are not). Strings searches for However, those bytes may not actually represent that string; theycould be a memory address, CPU instructions, or data used by the program. Strings leaves it up tothe user to filter out the invalid strings. For example, the following excerpt shows the result of running Strings against the filebp6.ex:

Mail system DLL is invalid! Send Mail failed to send message.*5.* In this example, the bold strings can be ignored. Typically, if a string is short and does not correspond to words, it is probably meaningless. On the other hand, the strings GetLayout at *1* and SetLayout at *2* are Windows a three-letter or greater sequence of ASCII and Unicode characters, followed by string termination character. Sometimes the strings detected by the Strings program are not actual strings. For example, if Strings finds the sequence of bytes 0x56, 0x50, 0x33, 0x00, it will interpret that as the stringVP3.

C:>strings bp6.ex_
VP3VW3t$@D$499.124.22.1 *4*
e-@GetLayout *1*
GDI32.DLL 3
SetLayout *2*
M}C

functions used by the Windows graphics library. We can easily identify these as meaningful strings because Windows function names normally begin with a capital letter and subsequent words begin with a capital letter.

**Static Analysis in Practice**

In this practical for static malware analysis, we will use different tools, which are amazing software/application to analyses malicious files and more popular with literary types. However, it is strongly recommended that you use always all those tools we will discuss outside of your network.

**Antivirus Scanning: A Useful First Step**

When first analysing prospective malware, a good first step is to run it through multiple antivirus programs, which may already have identified it. However, antivirus tools are certainly not perfect. They rely mainly on a database of identifiable pieces of known suspicious code (file signatures), as well as behavioural and pattern-matching analysis (heuristics) to identify suspect files.

One problem is that malware writers can easily modify their code, thereby changing their program's signature and evading virus scanners. In addition, rare malware often goes undetected by antivirus software because it is simply not in the database. Finally, heuristics, while often successful in identifying unknown malicious code, can be bypassed by new and unique malware. Because the various antivirus programs use different signatures and heuristics, it is useful to run several different antivirus programs against the same piece of suspected malware. Websites such as Virus Total (http://www.virustotal.com/) allow you to upload a file for scanning by multiple antivirus engines.

Virus Total generates a report that provides the total number of engines that marked the file as malicious, the malware name, and, if available, additional information about the malware. Virustotal is a service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, Trojans, and all kinds of malware detected by antivirus engines.

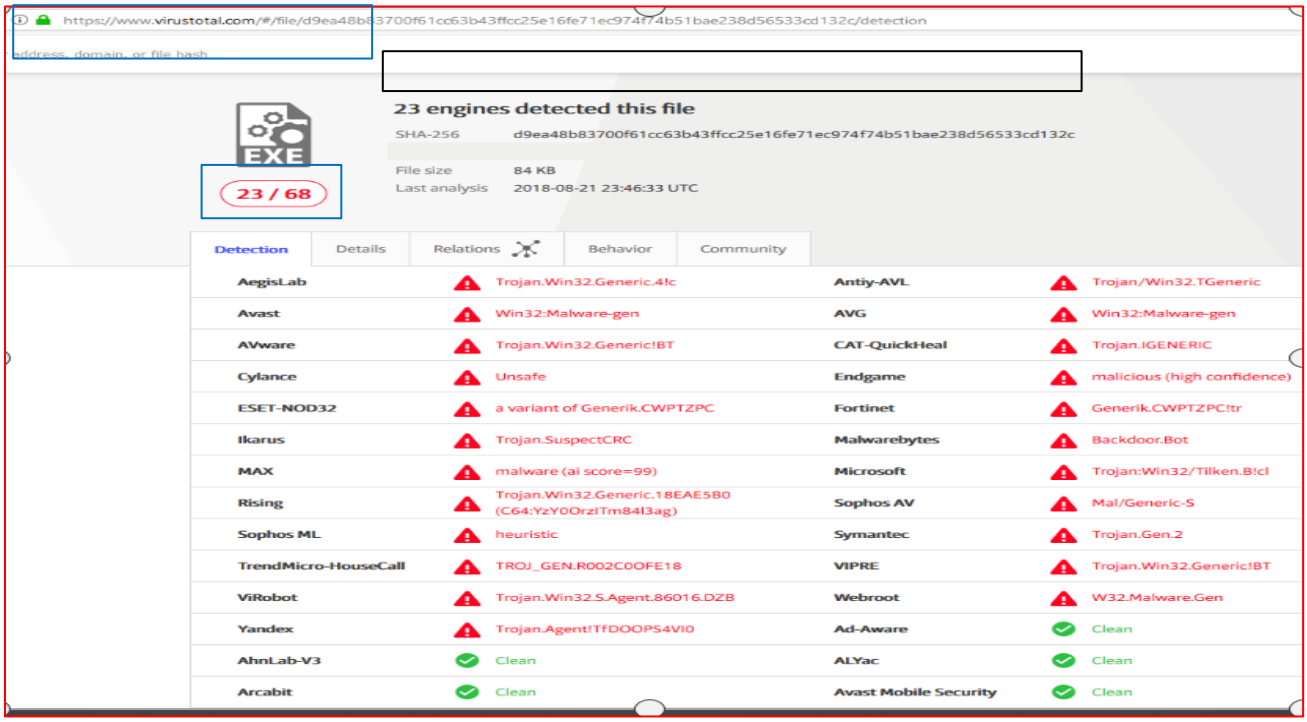


Figure Image on virustotal

**Detecting malware Packers with PEiD**

One way to detect packed files is with the PEiD program. You can use PEiD to detect the type of packer or compiler employed to build an application, which makes analysing the packed file much easier. Shows figure information is about UnPackMe.exe as reported by PEiD.

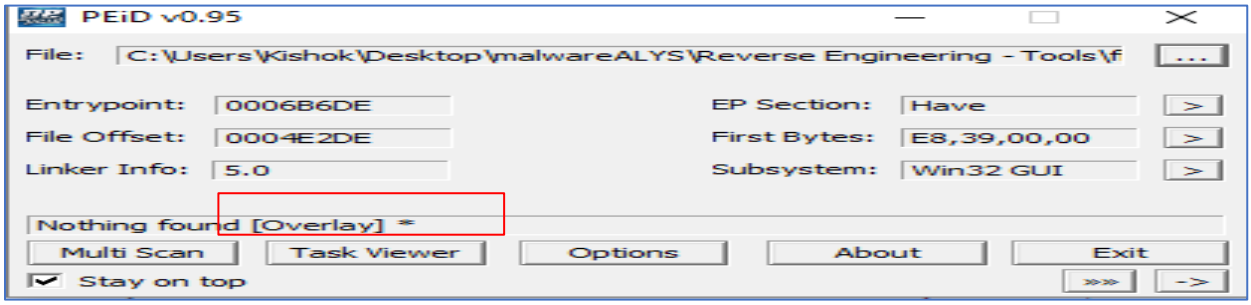


**Figure on the PEiD program found nothing packed**

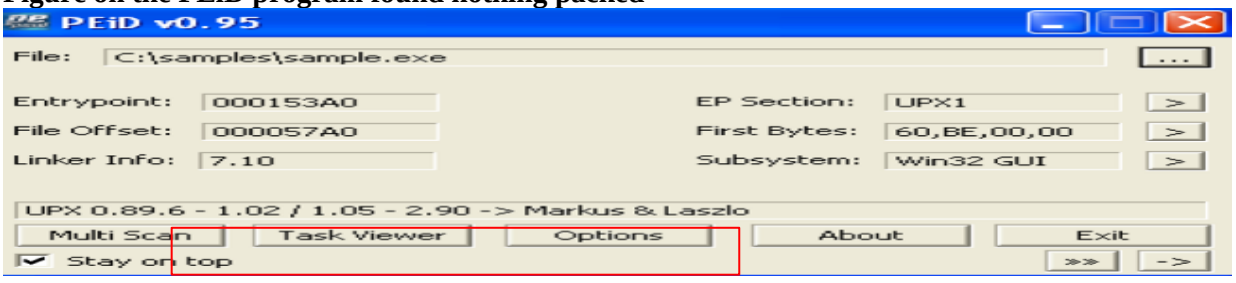


**Figure on The PEiD program**

Note: Many PEiD plug-ins will run the malware executable without warning! In addition, like all programs, especially those used for malware analysis, PEiD can be subject to vulnerabilities. For example, PEiD version 0.92 contained a buffer overflow that allowed an attacker to

execute arbitrary code. This would have allowed a clever malware writer to write a program to exploit the malware analyst's machine. Be sure to use the latest version of PEiD.

**Hashing: A Fingerprint for Malware Hashing**

Is a common method used to uniquely identify malware? The malicious software is run through a hashing program that produces a unique hash that identifies that malware (a sort of fingerprint). The Message-Digest Algorithm 5 (MD5) hash function is the one most commonly used for malware analysis, though the Secure Hash Algorithm 1(SHA-1) is also popular. For example, using the freely available md5deep program to calculate the hash of the Solitaire program that comes with Windows would generate the following output:

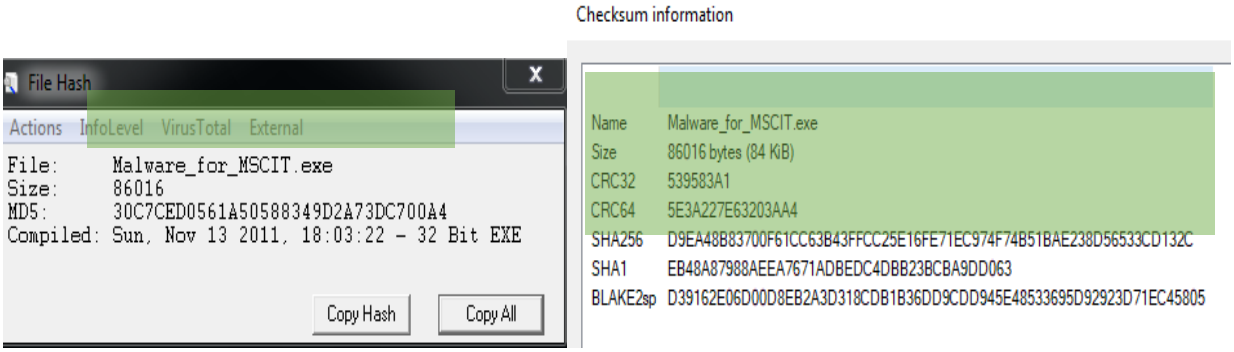



***Figure on Image on virustotal***

The GUI-based WinMD5 calculator, shown in Figure can calculate and display hashes for several files at a time. Once you have a unique hash for a piece of malware, you can use it as follows:

- Use the hash as a label.
- Share that hash with other analysts to help them to identify malware.
- Search for that hash online to see if the file has already been identified.

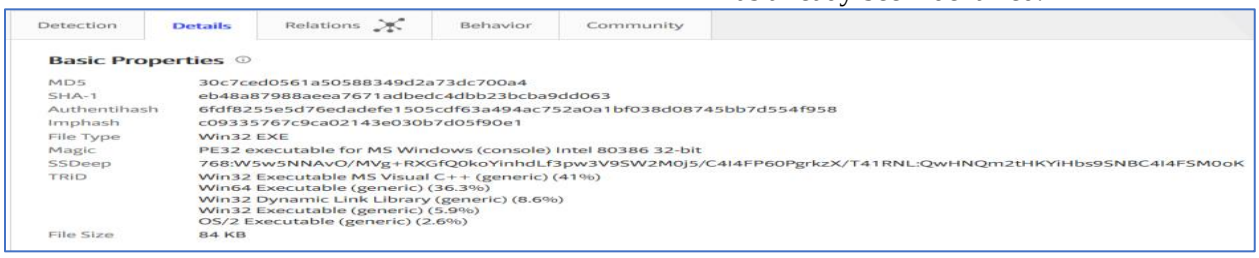



**Figure on Image on virustotal**

**Document analysis**

Documents are one of the primary ways attackers' compromise systems with malware. In this course, we are going to see how to analyze malicious documents to determine what they are doing to compromise a system. Some of the documents that we will see include how to examine Adobe PDF and Microsoft Office documents, ways to get around malicious script obfuscation techniques, and the tools and techniques you can use to speed up your analysis. You will see and know how to safely determine if a document is malicious and how to figure out what it does to compromise a system. Microsoft office applications such as Word, Excel and PowerPoint all have a history of being exploited by malicious authors from time to time. Since enterprise users and end users, malicious authors often use these applications target these documents to infect more users and extract valuable information from them. In this example. It dumps the parsed contents of sample.doc in <filename>. macros such as the one below. Malicious authors either by embedding shellcode in the document, which is executed by exploiting a vulnerability or by macrocode embedded as a macro in the document that in turn is executed when the user clicks 'ok' exploit these Microsoft applications.

**Applications for software reverse engineering**

It is hard to name the best software of reverse engineering tool, there quite a few of them and each one resolves some specific tasks of the multistep reversing process.

The most valuable tools for reverse engineering are the tools that work as disassembler and debugger at the same time. There are two common tools widely used nowadays; IDA Pro and OllyDbg. IDA Pro is the most powerful disassembler that decodes machine code into assembly language. There IDA plugins, which are also worth mentioning besides the disassembler itself.

One of the best aspects of IDA Pro is its ability to save your analysis progress: You can add comments, label data, and name functions, and then save your work in an IDA Pro database to return to later. IDA Pro also has robust support for plug-ins, so you can write your own extensions or leverage the work of others. To dig deeper into IDA Pro, *Chris Eagle's The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler, 2nd Edition (No Starch Press, 2011)* is considered the best available resource. It makes a great desktop reference for both IDA Pro and reversing in general

.

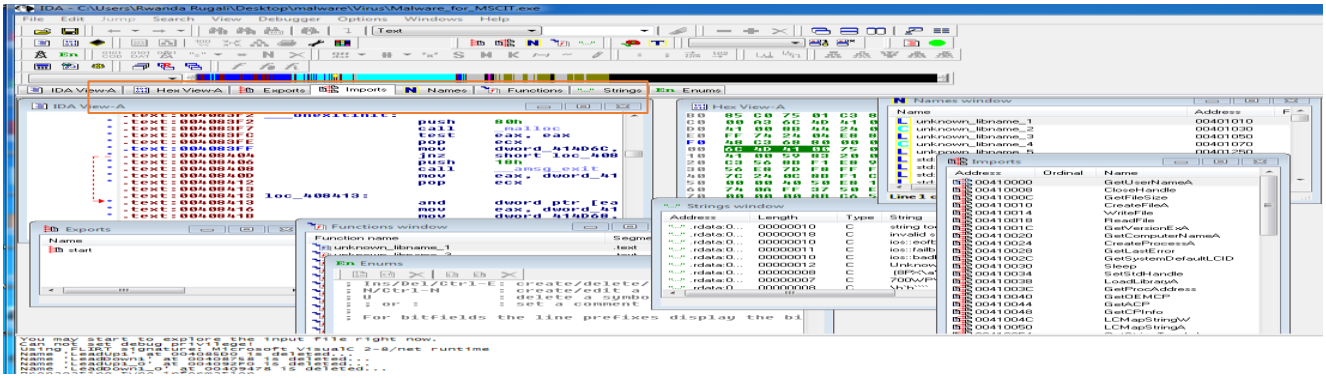


**Figure on Graph mode of the IDA Pro disassembly window**

**Dynamic analysis**

The purpose of a behavioural analysis is to execute the malware and to monitor its interactions with the environment. By doing so, an analyst can gain an initial understanding of what the malware is attempting to do as well as identify indicators of compromise that can be utilized to detect other infected systems.

Each of the items listed above are crucial pieces of information that we would want to know about a piece of malware. Therefore, we will need software utilities to monitor file system activity, registry activity, and network activity. It is important to note that a majority of the software utilities we used was designed on the Windows system that was infected with the malware. This is important because the malware could be designed to interfere with the monitoring software (rootkit). To ensure that the results of the monitoring tools are accurate. Before getting into the analysis, there are important precautions we have to take so that we should not miss anything and should not face any infection. So please make sure that we have followed below mentioned precautions:

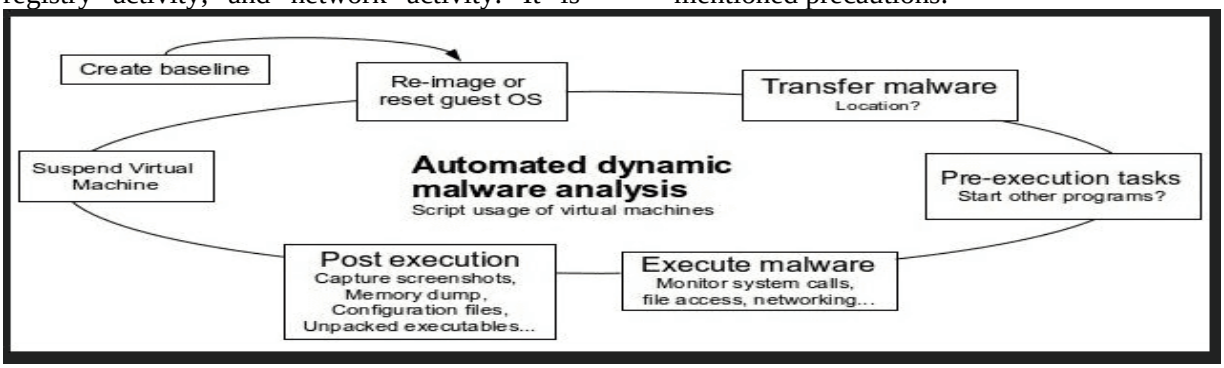


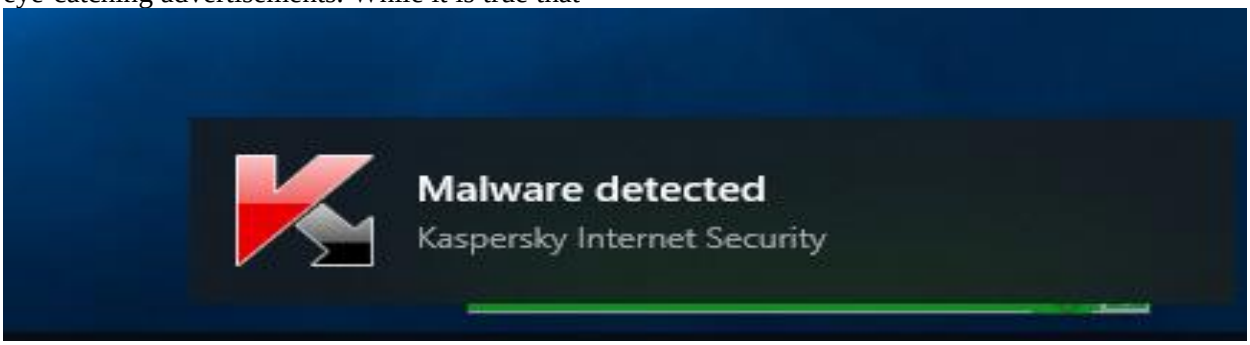

Figure on process of restore point of the Virtual machine. Why we have to avoid using Sandbox

in Production Network? There are many ways that malware can escape from the sandbox and it depends on who is building the malware.

**Antivirus**

Let us continue analyzing our malware named Malware_analysis_for_MSCIT.dll we used in static malware analysis, using dynamic analysis tools. First, to analyze well malware we start to check if the malware is harmful on the computer using our antivirus on my side I use Kaspersky, no matter the name of company which produce antivirus because various antivirus products have been on the market for many years, some users may fall into the trap of thinking that there is little to choose between the various products and that they all have similar malware detection capabilities. These users may decide to base their choice of antivirus product on relatively unimportant criteria such as whether it has an attractive design or it has featured in some eye-catching advertisements. While it is true that various antivirus programs have been available for a long period, the number and diversity of the threats that computers and other devices are subject to have changed massively in recent years.

Effective computer protection depends on the antivirus vendor's ability to adapt to new demands. When judged on their technical performance in detecting and protecting against malware, different antivirus products may differ greatly. To start this, lets us try many possible antiviruses I will first use what I installed on my virtual machine and then try or check on virustotal to see if it can detect the launched malware in my VMware machine, if I try to run it, this event happens.




My antivirus as a harmful file detects the malware as you see it on the above image. Then let us check in virustotal what will happen if we scan the file. We found about 43 antiviruses, which detect it as a malware see on this below figure.

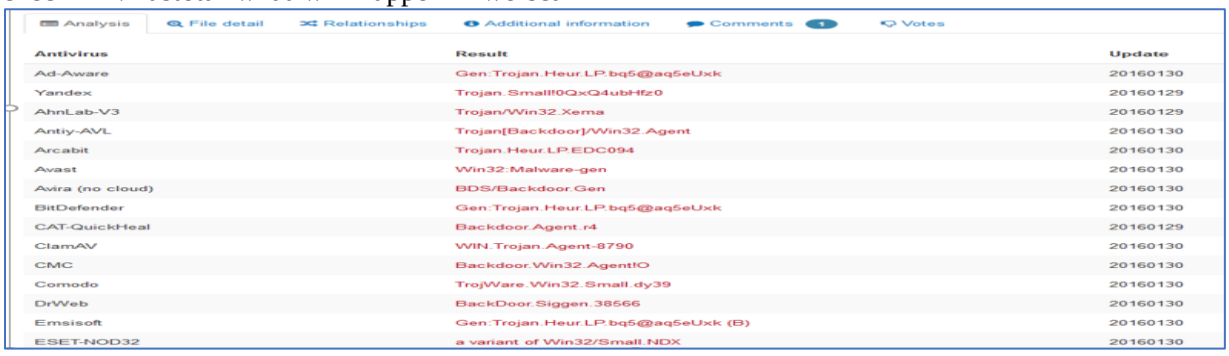



Figure on image malware_analysis.dll from virustotal

**Malware with IDA Pro**

There are many tools available for reverse engineering, but one disassembler stands alone. Nearly everyone in this industry uses IDA Pro to some extent. IDA Pro is a disassembler capable of taking binary programs where we do not have the source code and creating maps and multiple modes of understanding the binaries. It takes source code and represents it as assembler code so that we can better understand how the original code works. IDA Pro also has a in this part. Always the question we ask is to know how this

malware will be install itself! The only answer is in this next figure

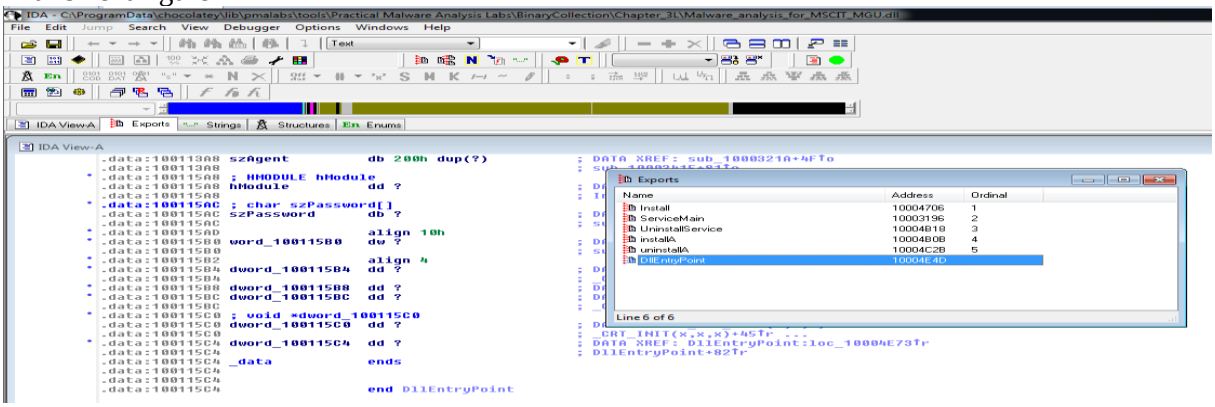



**Figure on IDA Pro shows how malware will be installed**

The malware install itself as a service. Using svchost.exe. The dll is added as parameter thus executing the malicious code. If we look at IDA Pro of the install function. You will easily see that it is trying to install a service via SCManager. It then adds description etc. via registry changes to hide itself in plain side. A call was made to get the current dll path and used that path to add to the service's registry as well.

**Process monitoring**

Process Monitor is a free tool from Microsoft that displays file system, registry, process, and other activities on the system. It's an invaluable tool for troubleshooting Windows problems as well as for malware forensics and analysis tasks. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware-hunting toolkit. Process monitor has the capability of monitoring, capturing and filtering all the artifacts.

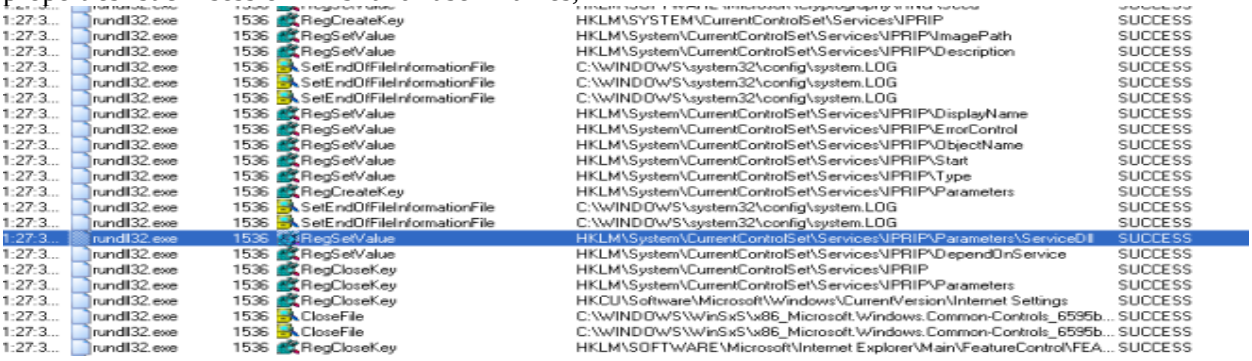



**Figure on Procmon RegSetValue**

However, the issue is, the tool is able to handle and capture the huge amount of data. Therefore, it is important to filter out the useless data from the haystack to identify the abnormal things and get the required artifacts. These filters are having many inclusions and exclusions to make the job easy. However, it is recommended to use your own filter list based on your requirement and analysis because there will many malicious processes, which is having legitimate windows process name. In this case, if you filter the windows process you might miss the malicious process activity. To see it Click on the filter button. (Or Ctrl + L) this image will be appeared.

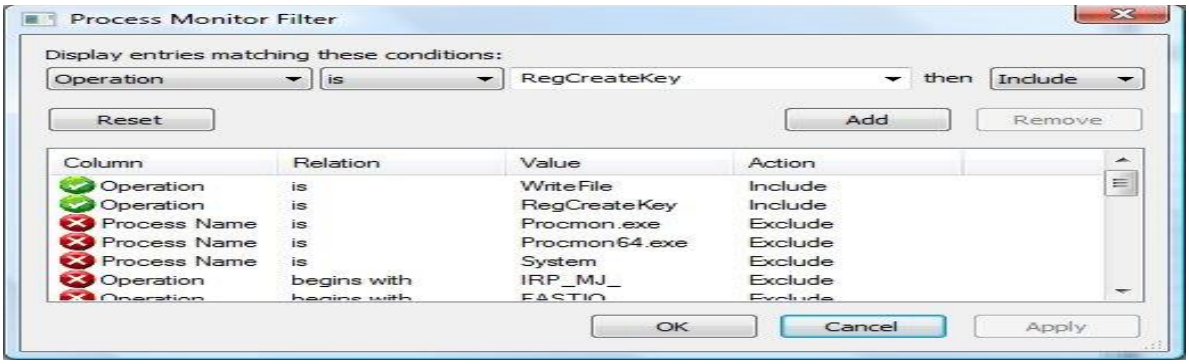



**Figure on Included and excluded in Procmon**

**Dynamic analysis with Regshot**

The next tool that will be installed is Regshot. Regshot is a utility that is utilized to preserve and compare two separate snapshots of the Windows registry. In malware behavioral analysis, Regshot is utilized to create a snapshot of the clean Windows virtual machine (VM) registry, create a snapshot of the infected Windows VM registry, and compare the two snapshots. Following the comparison process, Regshot generates a log that identifies registry keys and values created, modified, and deleted as well as files created and modified on the file system.

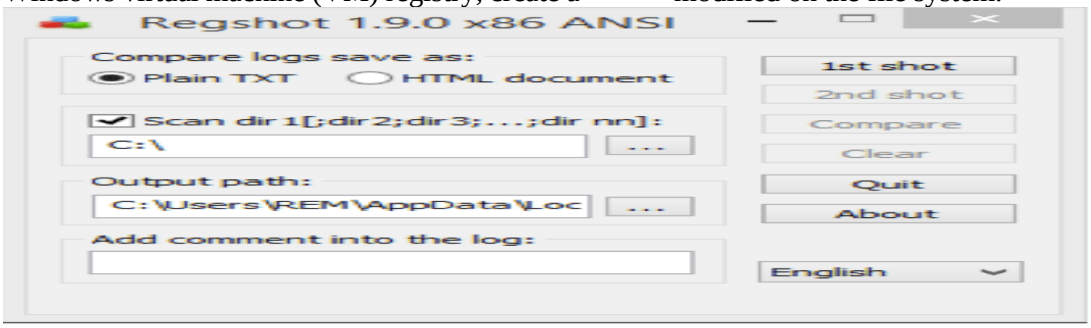



**Figure on Regshot ready to load malware**

The following graphic is a screenshot of the Regshot application taken after running our used malware named Malware_analysis.dll


**Figure on Regshot Registry added**

## Finding process running with Process Explorer

The fact that the display name (INA+) matches the information found in the registry tells us that our malicious service has started. Next, we open Process Explorer and attempt to find the process in which the malware is running by selecting FindHandle or DLL to open the dialog shown in We enter *malware_analysis_MSCIT.dll* and click Search. As shown in the figure, the result tells us that *malware_analysis_MSCIT.dll* is loaded by svchost.exe

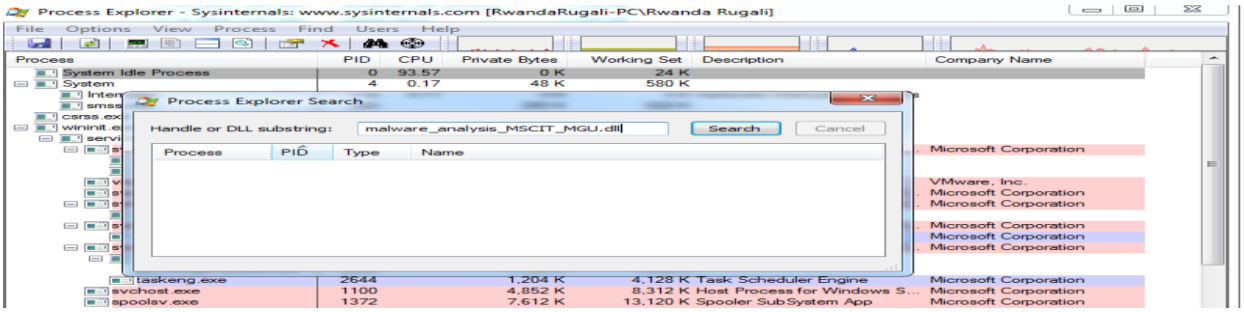



**Figure on Find Handle**

By going through the svchost.exe, we will come across a process in which *malware_analysis_MSCIT.dll* is loaded. That is the malicious process. For this case, the PID is 2468. This can be easily achieving by using the find handle (Ctrl-F) option in process explorer as shown below. In Process Explorer, we select **View→ Lower Pane View→DLLs** and choose the svchost.exe running with PID 2468. Figure 4-16 shows the result. The display name Intranet Network Awareness (INA+) shown at confirms that the malware is running in svchost.exe, which is further confirmed when we see at that Lab03-02.dll is loaded.

**Conclusion**

Meanwhile, on the malware analysis with dynamic analysis methods capable of providing more complete information about characteristics of malware, such as the information of malware to infect another program, as well as modifying the registry and create new files and folders. Also, malware in dynamic analysis can discover DLL of malware, the process of malware inside the system, as well as the network connection performed by malware against the server. While, malware analysis with the dynamic analysis method can provide information not previously found by other methods, the malware is able to turn off windows security systems such as firewalls, antivirus and system restore. Based on this research, the merging of the two methods of malware analysis that is static analysis and dynamic analysis is able to provide a more complete picture of the characteristics of malware malware_analysis.exe.

**Recommendations**

There is no way to eliminate all risk associated with outbound traffic short of closing all ports since attackers are very creative in hiding their activities testing for available protocols to tunnel and leveraging various obfuscation techniques. However, a good understanding of the techniques and risks should enable organizations to detect abnormalities and make informed decisions on improving and fine-tuning egress policy. Also, better education is as one of the suggested solutions for better IT security future. More educational efforts for IT security are required to educate software engineers, system administrators and computers' end users. Universities and colleges are urged to offer more IT security courses with the consideration for establishing a specialized degree in this field.

**REFERENCES**


1. Eldad Eilam. Reversing: Secrets of Reverse Engineering. Wiley Publishing; 2005
2. Palo Alto Network. Analysis of New and Evasive Malware in Live Enterprise Networks. Technical Report. 1st Edition, March 2013.
3. Vigna, G. 2014. Antivirus Isn't Dead, It Just Can't Keep Up. Technical Report. Lastline Labs, May 2014.
4. H. Zhao, M. Xu, N. Zheng, J. Yao, and Q. Ho. Malicious executables classification based on behavioral factor analysis. In International
5. C.Wang, J. Pang, R. Zhao, W. Fu, and X. Liu. Malware detection based on suspicious behaviour identification, in First International Workshop
6. DeLone, W. H.; McLean, E. R. (1992). "Information systems success: the quest

for the dependent variable". Information Systems Research.
7. DeLone, W. H. and McLean, E. R. (2002). Information Systems Success Revisited. Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS), Big Island, Hawaii, 238-249.
8. DeLone, W. H.; McLean, E. R. (2003). "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update". Journal of Management Information Systems.
9. International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013 1 ISSN 2229-5518 (Samanvay Gupta, 2013).
10. Critical Infrastructure Protection in the Fight against Terrorism, EC, Brussels, 20.10.2004.
11. 2000 Information Technology—Code of Practice for Information Security Management. ISO IEC 17799.
12. Top Database Security Threats and How to Mitigate Them, By Roy Maurer July 30, 2015.
13. Kaspersky Lab. Zero-day exploit (CVE-2018-8453) used in targeted attacks: October 10, 2018.