*International Research Journal of Innovations in Engineering and Technology (IRJIET)*

ISSN (online): 2581-3048

Volume 5, Issue 2, pp 10-15, February-2021

https://doi.org/10.47001/IRJIET/2021.502003

# Proactive Technique for Securing Smart Cities against Malware Attacks Using Static and Dynamic Analysis

**Ms. Purnima Ahirao**

Assistant Professor, K J Somaiya College of Engineering, Somaiya University, Maharashtra, India

***Abstract*** - **Cloud environment and IOT are the buzzwords in recent times. The smart devices connected with IOT enabled sensors generate a lot of data which is then uploaded on the cloud for further Analysis. The Internet of Things (IOT) is currently shaping our cities to take the form of a Smart City with a lot of connected, convenient, and intelligent systems working together in a collaborative and integrated manner. [1] However, this change brings minute insights into human activities through the ample data that is generated via sensors, devices etc. So, Security remains the major concern over the data collected from the smart devices, IOT sensors, social media, etc. The cyber-attacks which are taking a rise in the day to day digital life poses a major threat to the data generated from the smart city system. One of the security challenges is the malware attack. The malware poses a greater threat to the system which processes enormous critical data thereby resulting in the overall damage of the system with respect to confidentiality of the information. This paper proposes a method which can be used for malware analysis and detection, which in turn will combat the cyber security attack caused due to malware inclusion in the system. The paper focuses on different tools and techniques being used for malware analysis and detection. The approach will be able to safeguard the integrated system using IOT and Cloud with the help of Malware analysis.**

***Keywords:*** IOT, Security, cloud, malware, big data, analysis.

## I. INTRODUCTION

Nowadays world's population is increasing day by day and by exponential increase in population also increases migration of the people from urban areas to cities. These peoples are establishing modern cities which can be connected digitally through Internet of Things. Smart cites improves lifestyle of people living in them also provide very good support to work in industries and connect people from urban to modern areas generate large amount of data from different IOT resources. These cities are generating big data about what people feel on social network and what they see. All these data will be providing opportunities for hackers to explore the vulnerabilities and deploy attack on the system. There are wide ranges of smart city technologies are being developed and deployed in urban area with operating system, sensor-based system, smart billing, smart energy, smart water supply. Smart cities are being focus on delivering smart services to people living in cities that are up-grading. In smart city information security defines critical part in providing security at different levels like Confidentiality, Integrity, Availability, sustainability and stability in services. Security being biggest concern of smart cities for storing data in cloud environment. Security and privacy are issues enlarged by volume and variety of Big Data [1]. Efficiency of the service has to be maintained when processing collected real time data in case of Smart cities. There is a pressing demand on technologies that try to enforce security and privacy in data transmission. The paper tries to address the security aspect of data and detect any due to malware in this paper.

## II. RELATED STUDY

Before going into the core of security challenges in Smart Cities we should look to the traditional aspect in cities. Urban areas are the best place for economic growth and the more evaluation of technology. Cities contain massive concentration on knowledge and higher education leading to upgradation of technological advancements. As per statistics, in 1800 only 2% of global population was urbanized. This has gradually increased to 13% in 1900 whereas the figure exponentially raised by 47% in 2000 and 50% in 2008. Hence it is estimated to be 60% in 2030 and 70% or even 75% in 2050. [5] The people perspective versus technological perspective differs heavily in case of smart city. “The smart city sector is still in the ‘I know it when I see it’ phase, without a universally agreed definition”. There seems to be lack of standard global meaning about the exact definition of smart city. The present definition however covers some common characteristics, features, and components revealing varied perspectives of smart cities. People in cities are going to use more efficient device to make work easier such as use of smart watch, smart cars, smart transportation system, also the use of better utilization of green energy source. These devices generate massive data of user through whatever they do on social network or through anything in form of electronic. People have to care about the security of private data such as smart card, ATM card, PIN, etc. The extensive use of ICT solutions is necessary to deal with real life urban challenges. The challenges are namely environmental sustainability, socioeconomic innovation, participatory governance, better public services, planning and collaborative decision-making. These challenges are to be handled while creating smart infrastructure, and can involve the citizens' personal stake for the betterment of their civic life. The use of ICT solutions can assure city administrations in providing better urban governance and management Transformation of application specific data into a useful information and knowledge is the direct implication of using ICT as prime enabler for smart cities.

IoT which involves the collaborative working of smarter hardware (smart phones, sensor nets, smart household appliances, etc.) along with ICT infrastructure can surely pave the way for the possibility of realization of smart cities is being enabled and thus become a major source of user and environment specific data. It is predicted that huge volume of data will be generated due to IoT devices and is bound to increase exponentially which can be classified as Big data. [5] The data collected from the or for the implementation of Smart city is going to be really huge. The main concern here is the security of the data, wherever it is stored. Different types of attacks are possible on this data, one of which is malware attack. The effects of caused by malware like Petya, Wanna Cry, Agent smith is tremendous and incurred huge loss to organizations as well as individual's in particular. These types of Malware are difficult to detect by Antivirus software due to its lack of signature pattern.

The proposed paper provides a proactive approach to detect malware on the system wherever the collected data is stored and inform the authorities so that immediate measures can be taken to eradicate the malware.

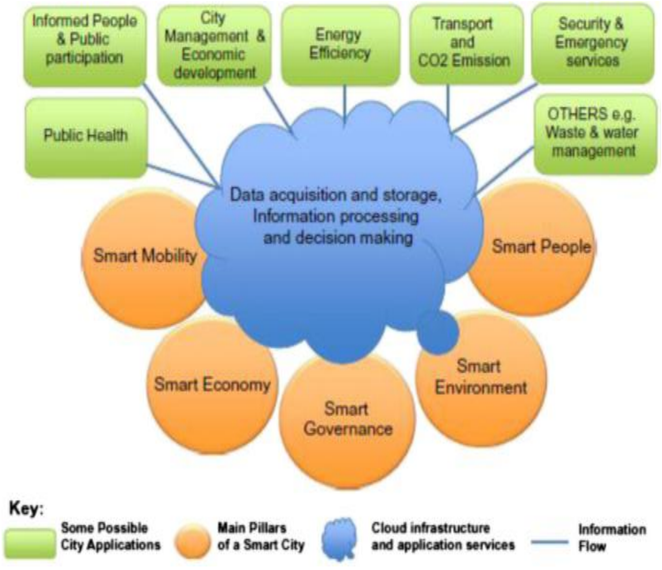

Informed People & Public participation
City Management & Economic development
Energy Efficiency
Transport and CO2 Emission
Security & Emergency services
Public Health
OTHERS e.g. Waste & water management
Data acquisition and storage, Information processing and decision making
Smart Mobility
Smart People
Smart Economy
Smart Governance
Smart Environment
Key:
Some Possible City Applications
Main Pillars of a Smart City
Cloud infrastructure and application services
Information Flow

**Figure 1: Proposed system**

## III. MALWARE AND ITS ANALYSIS

Malware is an abbreviated term meaning "malicious software." This is software that is specifically designed to gain access or damage a computer without the knowledge of the owner. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs and other malicious programs; the majority of active malware threats are usually worms or Trojans rather than viruses. Software can be considered as malware due to its intention of attacking and harming a computer system. New and sophisticated types of Malware are on the rise which leads to money fraud by the way of full-fledged and organized internet crime.

The original discovery of Malware was to explore if as experiments and pranks, but as a side effect it led to vandalism and destruction of targeted machines. The different versions of Malware available in the market today are for profit through forced advertising (adware), stealing sensitive information (spyware), spreading email spam or child pornography (zombie computers), and more importantly ransom amount (ransomware). The vulnerability of the Computer system with respect defects in the operating system design, having all of the computers on a network run the same OS, giving users too much permissions or just using the Windows OS (due to its popularity, can lead to Malware attacks. Malware plays a major part in most computer intrusion and attack incidents. A core set of tools and techniques for analyzing malware is available as against various types of malware being incarnated on a daily basis. Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it.

Malware analysis appears to be very critical for one who needs to react to Computer security attacks. It is a step by step process of performing analysis of the malicious software. To carry out malware analysis, the analyst has access to only the malware executable, which is not in a human readable form. To understand the software a variety of tools and tricks is to be used for revealing a small amount of information. There are two fundamental approaches to malware analysis: static and dynamic.[7]

- Static analysis involves examining the malware without running it.
- Dynamic analysis involves running the malware. Both techniques are further categorized as basic or advanced.

Table 2: Static Analysis vs Dynamic Analysis

| STATIC ANALYSIS | DYNAMIC ANALYSIS |
|---|---|
| ▪ Checks the code without trying to execute it<br>▪ Quick scan in white list<br>▪ Filtering: scan with different antivirus and check if they return same result with different name<br>▪ Weeding: remove the correct part of files as junk to better identify the virus<br>▪ Code analysis: check binary code to understand if it is an executable, e.g., PE<br>▪ Disassembling: check if the byte code shows something unusual | Check the execution of codes inside a virtual sandbox<br>▪ Monitor<br>▪ File changes<br>▪ Registry changes<br>▪ Processes and threads<br>▪ Networks ports |

## 3.1 Categorize of Malware Analysis Technique

### *1. Basic Static Analysis*

Basic static analysis consists of examining the executable file without viewing the actual instructions. Basic static analysis can confirm whether a file is malicious, provide information about its functionality, and sometimes provide information that will allow you to produce simple network signatures. Basic static analysis is straightforward and can be quick, but it's largely ineffective against sophisticated malware, and it can miss important behaviors.

### *2. Basic Dynamic Analysis*

Basic dynamic analysis techniques involve running the malware and observing its behavior on the system in order to remove the infection, produce effective signatures, or both. However, before you can run malware safely, you must set up an environment that will allow you to study the running Malware Analysis Primer malware without risk of damage to your system or network. Like basic static analysis techniques, basic dynamic analysis techniques can be used by most people without deep programming knowledge, but they won't be effective with all malware and can miss important functionality.

### *3. Advanced Static Analysis*

Advanced static analysis consists of reverse-engineering the malware's internals by loading the executable into a disassembler and looking at the program instructions in order to discover what the program does. The instructions are executed by the CPU, so advanced static analysis tells you exactly what the program does. However, advanced static analysis has a steeper learning curve than basic static analysis and requires specialized knowledge of disassembly, code constructs, and Windows operating system concepts.

### *4. Advanced Dynamic Analysis*

Advanced dynamic analysis uses a debugger to examine the internal state of a running malicious executable. Advanced dynamic analysis techniques provide another way to extract detailed information from an executable. These techniques are most useful when you're trying to obtain information that is difficult to gather with the other techniques.

### *4. Proposed Method*

Variety of sensors, smart phones, citizens and integrated (or linked) with city data repositories can be used to collect data for Smart cities to perform analytical reasoning and generate required information for decision-making for better urban governance. There is huge threat to this data due to various security aspects. Smart city implementation is possible only if the data collected from various sources is safeguarded against all types of cyber-attacks. [5] In this paper the focus is on the Malware attack which caused heavy damage to the system also the antivirus software are not equipped to handle such malware. The malware can be of any type one of which is ransomware. These are special type of malware which when downloaded on your system is able to lock the system until and unless some amount is given to the hackers. Example like petya, wannacry, Agent smith goes undetected due to its unknown signature pattern. These malwares may be downloaded by people through email or fraud websites. There are different ways used by hackers to deploy these malwares on to any system. [2] The proposed system will identify any new downloaded executable file on the system and then perform malware analysis on the file to classify it to safe and unsafe file. The method is proposed to detect the malware before it actually starts executing on the system.

### *5. Tools and techniques used for Analysis*

Constructing a lab for malware analysis requires the reader to contemplate the pros and cons of using physical hardware or virtual machines (VM). The author recommends leaning towards the use of virtual machines using the VMware Server product. VMware Server is a free download from the www.vmware.com website. VMware reduces the cost of hardware to needing only one or two physical machines. VMware allows many types of OS, including Windows and Linux, to be installed. Once of the best features of VMware is the snapshot. Before performing any type of analysis, taking a snapshot will save lots of time down the road. Another nice feature is the host only networking, which means the lab will only see itself. Also one should utilize the ability to disable

ISSN (online): 2581-3048
Volume 5, Issue 2, pp 10-15, February-2021
https://doi.org/10.47001/IRJIET/2021.502003

VMware's access to the network interface card. Remember, when using VMware, a large amount of RAM is needed. For Windows based and Linux systems that need a GUI, a minimum 512 MB of RAM should be used. For text-based Linux boxes a minimum 256 MB of RAM should be used.

Although virtualization of the malware lab is great for cost reduction, there are issues with using virtualization software. Some of the more sophisticated malware today will attempt to detect a VM. If the malware detects it is being run on a VM, it will not execute. After building the virtual machines, the operating systems installed in the malware lab will depend on the malware being analyzed and the operating systems used in the organization. The author normally will have a Windows XP Professional machine and a Linux machine loaded. The tools to be installed will depend on the type of analysis is to be performed. Although there is no hard and fast rule about which type to perform, the authors experience leads to performing the static analysis first, followed by the dynamic analysis. The information gathered during the static analysis will usually provide information needed for the dynamic analysis.

The aim is to build a defense in depth solution with the help of malware analysis. Well defined and implemented defense solution based on malware analysis would certainly reduce the attack vectors and false positives.

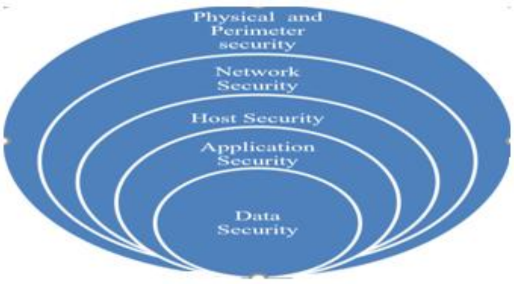
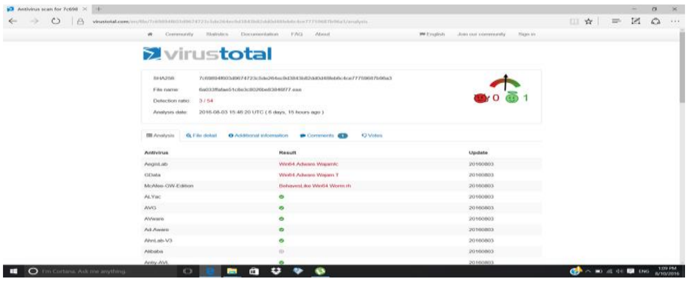


**Figure 2: Defense in depth model**

## IV. RESULTS AND DISCUSSION

### Basic static analysis

1. Antivirus tool to confirm maliciousness


Antivirus scan for 7c698

virustotal.com

virustotal

SHA256: [illegible]

File name: [illegible].exe

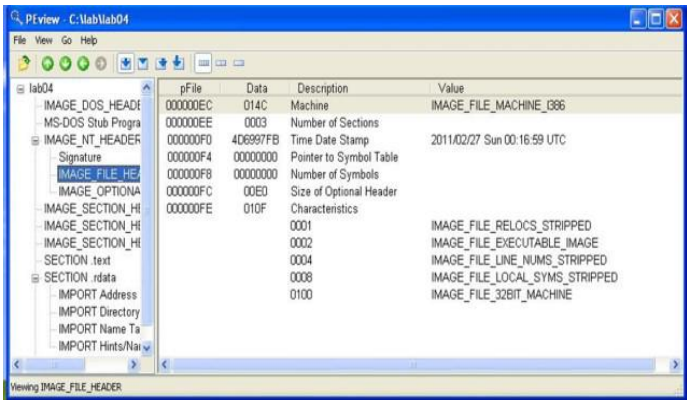
Detection ratio: 3 / 54

Analysis date: 2016-08-03 15:46:20 UTC ( 6 days, 15 hours ago )

| Antivirus | Result | Update |
|---|---|---|
| AegisLab | Win64.Adware.Wajam!c | 20160803 |
| GData | Win64.Adware.Wajam.T | 20160803 |
| McAfee-GW-Edition | BehavesLike.Win64.Worm.rh | 20160803 |
| ALYac | ✓ | 20160803 |
| AVG | ✓ | 20160803 |
| AVware | ✓ | 20160803 |
| Ad-Aware | ✓ | 20160803 |
| AhnLab-V3 | ✓ | 20160803 |
| Alibaba | ✓ | 20160803 |
| Antiy-AVL | ✓ | 20160803 |

**Figure 3: Malicious activity**

2. Compile time of the executable file in PEView

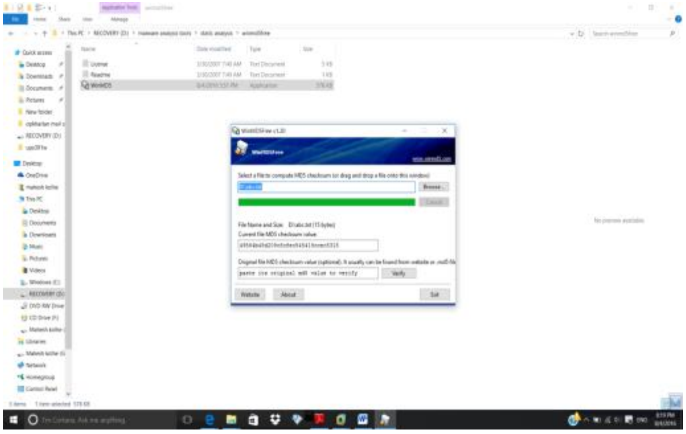

PEview - C:\lab\lab04

| pFile | Data | Description | Value |
|---|---|---|---|
| 000000EC | 014C | Machine | IMAGE_FILE_MACHINE_I386 |
| 000000EE | 0003 | Number of Sections | |
| 000000F0 | 4D6997FB | Time Date Stamp | 2011/02/27 Sun 00:16:59 UTC |
| 000000F4 | 00000000 | Pointer to Symbol Table | |
| 000000F8 | 00000000 | Number of Symbols | |
| 000000FC | 00E0 | Size of Optional Header | |
| 000000FE | 010F | Characteristics | |
| | | 0001 | IMAGE_FILE_RELOCS_STRIPPED |
| | | 0002 | IMAGE_FILE_EXECUTABLE_IMAGE |
| | | 0004 | IMAGE_FILE_LINE_NUMS_STRIPPED |
| | | 0008 | IMAGE_FILE_LOCAL_SYMS_STRIPPED |
| | | 0100 | IMAGE_FILE_32BIT_MACHINE |

Viewing IMAGE_FILE_HEADER

**Figure 4: Compile File**

3. Using hashing tool to identify malware solution present online


WinMD5Free v1.20

Select a file to compute MD5 checksum (or drag and drop a file onto this window)

File Name and Size: D:\abc.txt (15 bytes)

Current file MD5 checksum value:

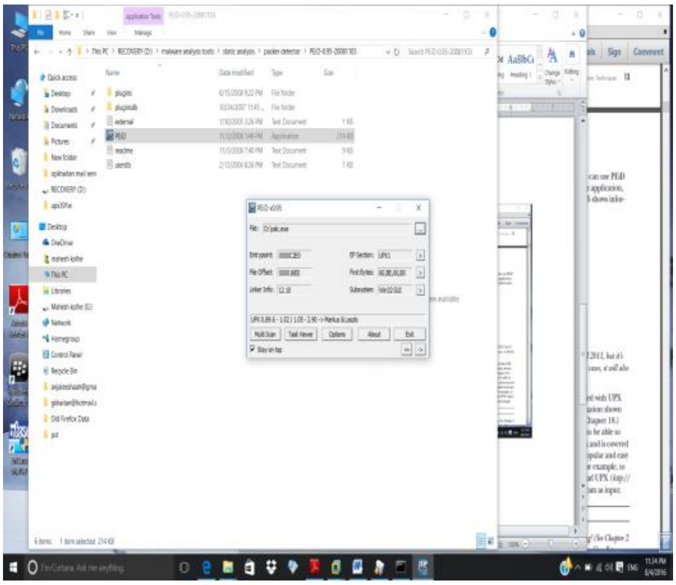
[illegible]

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

paste its original md5 value to verify

**Figure 5: Hashing**

4. Detecting packer Program detail by PEid


PEiD v0.95

File: D:\calc.exe

Entrypoint: [illegible]

File Offset: [illegible]

Linker Info: 12.10

EP Section: UPX1

First Bytes: [illegible]

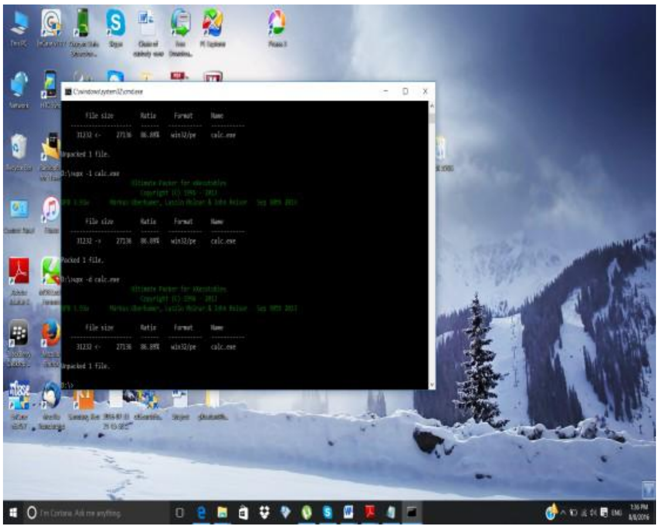
Subsystem: Win32 GUI

UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo

☑ Stay on top

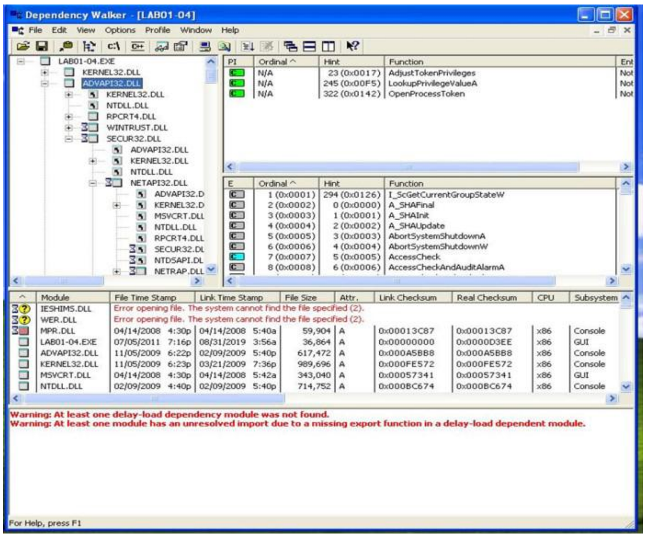
**Figure 6: Program details by PEid**

ISSN (online): 2581-3048
Volume 5, Issue 2, pp 10-15, February-2021
https://doi.org/10.47001/IRJIET/2021.502003



```
C:\windows\system32\cmd.exe

       File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     31232 <-     27136   86.89%   win32/pe     calc.exe

Unpacked 1 file.

D:\>upx -1 calc.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2013
UPX 3.91w       Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 2013

       File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     31232 ->     27136   86.89%   win32/pe     calc.exe

Packed 1 file.

D:\>upx -d calc.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2013
UPX 3.91w       Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 2013

       File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     31232 <-     27136   86.89%   win32/pe     calc.exe

Unpacked 1 file.

D:\>
```

Figure 7: Packing and Unpacking



Dependency Walker - [LAB01-04]
File Edit View Options Profile Window Help

```
LAB01-04.EXE
  KERNEL32.DLL
  ADVAPI32.DLL
    KERNEL32.DLL
    NTDLL.DLL
    RPCRT4.DLL
    WINTRUST.DLL
    SECUR32.DLL
      ADVAPI32.DLL
      KERNEL32.DLL
      NTDLL.DLL
      NETAPI32.DLL
        ADVAPI32.D
        KERNEL32.D
        MSVCRT.DLL
        NTDLL.DLL
        RPCRT4.DLL
        SECUR32.DL
        NTDSAPI.DL
        NETRAP.DLL
```

| PI | Ordinal ^ | Hint | Function | Ent |
|---|---|---|---|---|
| C | N/A | 23 (0x0017) | AdjustTokenPrivileges | Not |
| C | N/A | 245 (0x00F5) | LookupPrivilegeValueA | Not |
| C | N/A | 322 (0x0142) | OpenProcessToken | Not |

| E | Ordinal ^ | Hint | Function |
|---|---|---|---|
| C | 1 (0x0001) | 294 (0x0126) | I_ScGetCurrentGroupStateW |
| C | 2 (0x0002) | 0 (0x0000) | A_SHAFinal |
| C | 3 (0x0003) | 1 (0x0001) | A_SHAInit |
| C | 4 (0x0004) | 2 (0x0002) | A_SHAUpdate |
| C | 5 (0x0005) | 3 (0x0003) | AbortSystemShutdownA |
| C | 6 (0x0006) | 4 (0x0004) | AbortSystemShutdownW |
| C | 7 (0x0007) | 5 (0x0005) | AccessCheck |
| C | 8 (0x0008) | 6 (0x0006) | AccessCheckAndAuditAlarmA |

| Module | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Checksum | Real Checksum | CPU | Subsystem |
|---|---|---|---|---|---|---|---|---|
| IESHIMS.DLL | Error opening file. The system cannot find the file specified (2). | | | | | | | |
| WER.DLL | Error opening file. The system cannot find the file specified (2). | | | | | | | |
| MPR.DLL | 04/14/2008 4:30p | 04/14/2008 5:40a | 59,904 | A | 0x00013C87 | 0x00013C87 | x86 | Console |
| LAB01-04.EXE | 07/05/2011 7:16p | 08/31/2019 3:56a | 36,864 | A | 0x00000000 | 0x0000D3EE | x86 | GUI |
| ADVAPI32.DLL | 11/05/2009 6:22p | 02/09/2009 5:40p | 617,472 | A | 0x000A5BB8 | 0x000A5BB8 | x86 | Console |
| KERNEL32.DLL | 11/05/2009 6:23p | 03/21/2009 7:36p | 989,696 | A | 0x000FE572 | 0x000FE572 | x86 | Console |
| MSVCRT.DLL | 04/14/2008 4:30p | 04/14/2008 5:42a | 343,040 | A | 0x00057341 | 0x00057341 | x86 | GUI |
| NTDLL.DLL | 02/09/2009 4:40p | 02/09/2009 5:40p | 714,752 | A | 0x000BC674 | 0x000BC674 | x86 | Console |

```
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

Figure 8: Exe file performing function

The reports show that that the embedded file is the one that accesses the network functions. It calls URL Download to File, a function commonly used by malicious downloader's. It also calls WinExec, which probably executes the downloaded file. The results show that using malware analysis steps the malicious activity can be identified on the system having smart data. Some registry and memory analysis also showed that Trojan infected the usual windows booting process and then eventually gained the access of the system, damaging the system level security.

## V. CONCLUSION

With the advent of innovative technologies an opportunity to connect people and places can help in better city planning and management leading to Smart cities. Smart city progression aims at the collection, management, analysis and visualization of huge amount of data that is generated every minute in an urban environment due to socioeconomic or other activities. These cities need to protect the Big Data that Smart services and solutions produce and consume, and so they must be designed and planned with both physical and electronic security in mind. There are opportunities in smart city for data security and data privacy issues that are being discussed with respect to Malware Analysis and recent cyber security Attacks.

The analysis would be helpful in building a comprehensive security solution which shall dynamically catch the probable malicious files, analyses it and block in case of malicious file.

## REFERENCES

[1] Kalaikavitha, E., and Juliana Gnanaselvi. "Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology." *International Journal of Engineering and Science* 2, no. 10 (2013): 14-17.

[2] Giri, Debasis, and Parmeshwary Dayal Srivastava. "Cryptanalysis and improvement of a remote user authentication scheme using smart cards." *In 2008 International Symposium on Electronic Commerce and Security, pp. 355-361. IEEE, 2008.*

[3] Google, "Android Enterprise Security," *White Paper*, 2018.

[4] https://sensiblemicro.com/smart-watches-the-start-of-the-wearable-electronics-revolution/

[5] THE SMARTWATCH MARKET: Growth, Consumer Attitudes, And Why This Is The New Device Category To Bet On, Tony Danova. Online available: https://www.businessinsider.in/THE-SMARTWATCH-MARKET-GrowthConsumer-Attitudes-And-Why-This-Is-The-New-Device-Category-ToBet-On/articleshow/45116246.cms

[6] Aloul, Fadi, Syed Zahidi, and Wassim El-Hajj. "Two factor authentication using mobile phones." *In 2009 IEEE/ACS International Conference on Computer Systems and Applications*, pp. 641-644. IEEE, 2009.

[7] Saurabh, "Advance Malware Analysis Using Static and Dynamic Methodology," *2018 International Conference on Advanced Computation and Telecommunication (ICACAT), Bhopal, India*, 2018, pp. 1-5, doi: 10.1109/ICACAT.2018.8933769.

[8] https://subscription.packtpub.com/book/networking_and_servers/9781788392501/1/ch01lvl1sec13/4-types-of-malware-analysis

**Citation of this Article:**

Ms. Purnima Ahirao, "Proactive Technique for Securing Smart Cities against Malware Attacks Using Static and Dynamic Analysis" Published in *International Research Journal of Innovations in Engineering and Technology* - *IRJIET*, Volume 5, Issue 2, pp 10-15, February 2021. Article DOI https://doi.org/10.47001/IRJIET/2021.502003

*******