International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015
ISSN 2091-2730

Malware in Beautiful Three Dimensional (3D) visual Models - Analysis

PRIYANKA BHATI [1] K.V.V. PRASAD [2] ANISETTI ANIL [3]

prriyanka00@gmail.com kvvp.knl@gmail.com anisetti0101@gmail.com

Digital Forensic Analyst POLICE INSPECTOR Director,

eSF Labs,Hyderabad SATCOMBAT-OCTOPUS-AP eSF Labs Ltd, Hyderabad

Hyderabad- INDIA

Abstract: As the more number of users are connected to the internet the computer users are targeted by the various potential malwares. The number of malware increasing day by day had become a serious threat. The malware that has irritative and destructive functionality has become wild now days. As everyone use internet and downloading is common need for user. Unfortunately, the smart (3D) Three Dimensional visual model images are freely available in the archives of the websites. Some of the specified models which are very much useful for the defense organizations to design their security posts, navigate through high resolution 3D world environment created by fusing the 3D model images which can be useful to present the information in a realistic view to the senior management. Once the 3D images which binds with malware are downloaded and executed the malware will takes the advantage and infects the target machines and makes the network machines infected and spread through the removable media. Whenever the user restarts the infected system then it displays the black screen only. One of the leading GIS & Remote sensing organizations while inducting training to the Government Police Officers [2] who is working in the SATCOMBAT Computer Forensic Division faces this type of malware infection in their network. The GIS maps and Terra Explorer software intuitively placed on the Digital globe for terrain 3D analysis exclusively for Military defense critical infrastructures, Law enforcement Agencies were frequent access to the Geo spatial files.

This paper includes the analysis of malware and its spreading mechanism. Behavior analysis shows the functionality of the malware. In summary, the analysis reveals the malicious intention of malware author

Keywords -Dynamic Analysis, Military Defence, Malware, Virus in folders, Malware Behavior, Performance, Security, 3D Models, Malware in Digital Globe, Malware in three Dimensional Models ,Malware threat in GIS Software

INTRODUCTION

Malware attack is one of the most terrible and major security threats facing the Internet today. Normal users are unaware of these kinds of threats. One of the reasons is the rising popularity of the downloading. Malware can be downloaded unintentionally from internet presuming that these are genuine files. In this paper we analyze the malware downloaded from the archives of the 3D visualization model images.

Malware is a growing area of expertise and need skill set to analyze in virtual environment to meet the latest challenges.

Malware Analysis is the study of a malware by dissecting its different components and studies its behavior on the host computer's operating system. Malware analysis techniques are being followed, which can be either static or dynamic. The malware analysis techniques help the analysts to understand the risks and intention associated with a malicious code sample. The malware name is

system3_.exe and it contains the folder icon. In windows operating system by default the extension of files are not visible, so it fools the user in believing that it is a folder but actually it is a executable file.

2. ANALYSIS

There are different methodologies used in malware analysis. We used static and dynamic analysis of malware. Analyzing malicious software without executing it is called static analysis.

The malware download with Three Dimensional (3D) visual model images named as *system3_.exe*. Start with unique fingerprinting of malware.

The MD5 hash of system3_.exe is ***2EEE4E87DC250DDA8064C 22E0F3A8498***. It contains the folder icon as resources as shown in figure. It displays all icons stored as resources.

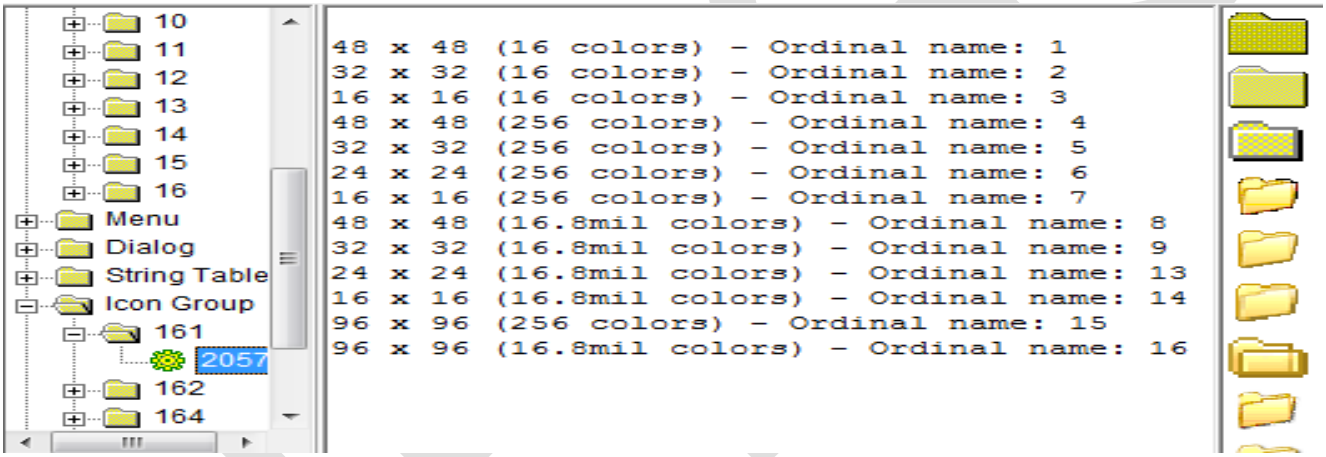

Fig. 1. Resource section

We run the system3_.exe within a controlled environment and monitoring its action in order to analyze the malicious behavior is called dynamic analysis. In this analysis, VMware is used as a secure environment to perform dynamic analysis.

3. BEHAVIOR OF MALWARE

This malware has the functionality of virus and creates its copy into system32 and temp folder in below mention path:

3.1 File Created:

C:\Documents and Settings\ESF10\LocalSettings \Te mp\00066237_Rar\system3_.exe

C:\WINDOWS\system32\system3_.exe

C:\WINDOWS\system32\autorun.inf

C:\ljbl.pif

C:\autorun.inf
C:\WINDOWS\Tasks\At1.job
It creates schedule job to execute itself everyday at 9:00 am.

3.2 Spreading Mechanism:

Malware search for any drive and copy itself into that drive. So if you connect any removable media into infected system it makes copies into USB. Afterwards, when you attach the same pen drive in another system it autoruns the virus and infects the system. The NewFolder.exe is a copy of system3_.exe binary as their hash value is same.

3.3 Files Created via USB infection:

[Any Drive]:\ autorun.inf

[Any Drive]:\ New Folder.exe

[Any Drive]:\ iblx.exe (random name)

[Any Drive]:\ New system3_.exe

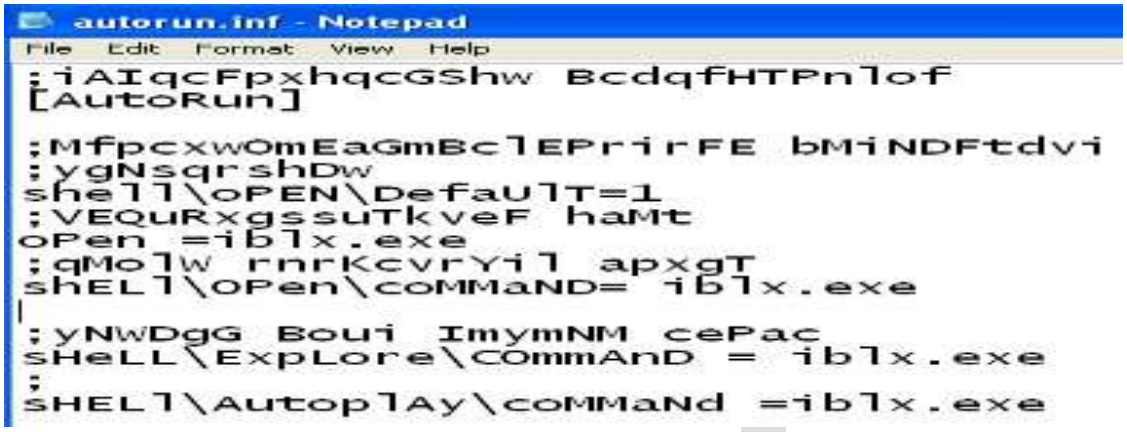

Fig. 2. Autorun file that automatically execute virus

REGISTRY MODIFICATION

Persistent mechanism

Most of the malware use various locations in registry to remain persistent on the systems. Persistent means malware will execute at every reboot. It creates two registry keys to remain persistence.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell: explorer.exe system3_.exe

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Yahoo Messengger: C:\WINDOWS\system32\system3_.exe

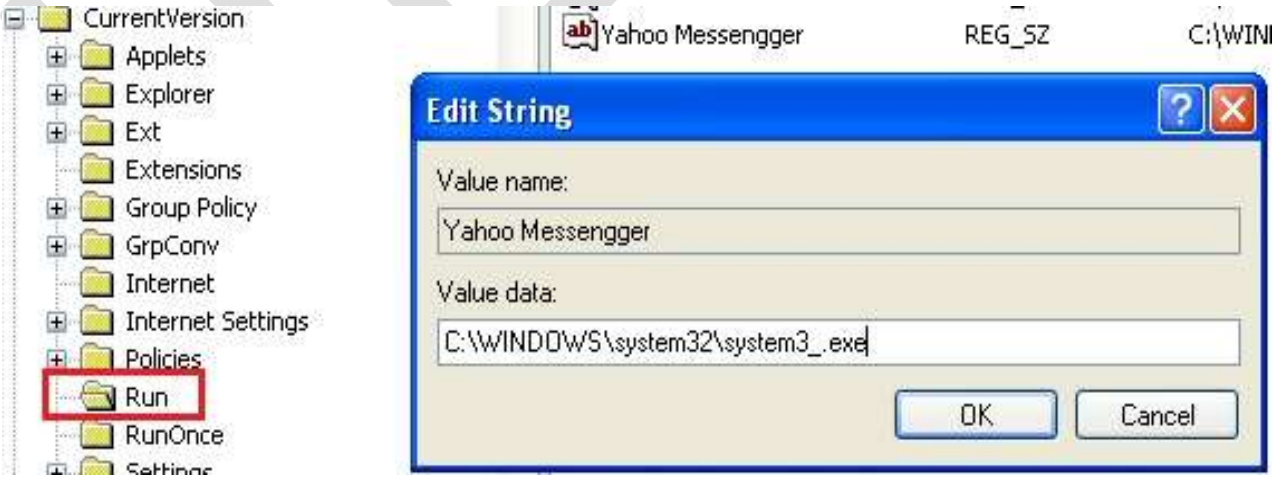

Fig. 3. Malware create registry key to autostart

4.2 Modified Registry Value:

The below registry entries confirm that the malware disables the Firewall notification message, Antivirus disable notification message and Window update disable notification message.

Path:

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: Random data

HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusDisableNotify: 0x00000001

HKLM\SOFTWARE\Microsoft\Security Center\FirewallDisableNotify: 0x00000001

HKLM\SOFTWARE\Microsoft\Security Center\UpdatesDisableNotify: 0x00000001

HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusOverride: 0x00000001

HKLM\SOFTWARE\Microsoft\Security Center\FirewallOverride: 0x00000001

4.3 Internet Explorer modification:

It also modifies the default page, default search, search page and start page of internet explorer browser shown in below registry keys:

HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\Default_Page_URL: "http://www.mydreamworld.50webs.com"

HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\Default_Search_URL: "http://www.mydreamworld.50webs.com"

HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\Search Page: "http://www.mydreamworld.50webs.com"

HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page: "http://www.mydreamworld.50webs.com"

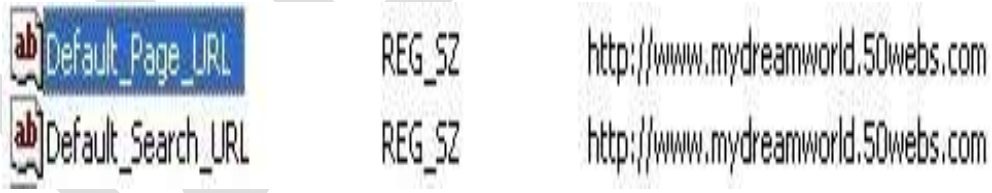

Fig. 4. Internet Explorer modification

4.4 Random registry values added:

Malware created 916 random registry values. It contains the random value & data. Here, below list & figure displays only few of registry values.

HKU\S-1-5-21-583907252-162531612-682003330-1003\Software\Aipwr\E1_0: 0x62E483CA

HKU\S-1-5-21-583907252-162531612-682003330-1003\Software\Aipwr\E2_0: 0x00001DE2

HKU\S-1-5-21-583907252-162531612-682003330-1003\Software\Aipwr\1207202201\826692421: 0x0000009E

HKU\S-1-5-21-583907252-162531612-682003330-1003\Software\Aipwr\1207202201\1653384842: 0x00000000

a1_0	REG_DWORD	0x62e483ca (1659143114)
a1_1	REG_DWORD	0xc9d4153c (3386119484)
a1_10	REG_DWORD	0xe471f503 (3832673539)
a1_100	REG_DWORD	0xed754da9 (3983887785)
a1_101	REG_DWORD	0x5f67f313 (1600647955)
a1_102	REG_DWORD	0x4a9db7fb (1251850235)
a1_103	REG_DWORD	0x658ff958 (1703934296)
a1_104	REG_DWORD	0x60faddb1 (1627053489)
a1_105	REG_DWORD	0x01365f94 (20340628)

Fig. 5. Random registry value

5. NETWORKING ACTIVITY

Malware tries to communicate with many websites. Below screenshot displays the DNS request send by the malware. Most of these URL are randomly generated by malware except those two underlined URL that is ***Ilo.brenz.pl*** and ***ant.trenz.pl.*** These two URL is malicious URL and might install another malware into the system.

Domain Requested	
ccbixb.com	www.balu011.0catch.com
ilo.brenz.pl	www.balu011.0catch.com
fzuyxv.com	h1.ripway.com
ekrzei.com	www.balu012.0catch.com
ant.trenz.pl	www.balu012.0catch.com
yzhowh.com	h1.ripway.com
aybxbp.com	ant.trenz.pl
giiyqp.com	www.balu013.0catch.com
broekhuisjuweliers.nl	www.balu013.0catch.com
btech.ac.th	h1.ripway.com
ilo.brenz.pl	www.balu014.0catch.com
btr.gen.tr	www.balu014.0catch.com
burakasansor.com	h1.ripway.com

Fig. 6. DNS request send by malware

After all these infection, commonly user get irritated and restart the system. So, when system reboots this malware displays only black screen. It also kills the process of task manager, registry editor, System Configuration, cmd and explorer.exe.

The 3D visualization models looks like this and it is the burden of the user for any damage caused by these models.

Fig. 7. 3D model images

6. CONCLUSION

In this research paper we have shown that the 3D model images downloaded from internet is not always safe enough as it brings malware with them. Malicious *System_3.exe* tricks the user by using folder icon resource. This virus creates entry in autoruns location and makes its copy in drives. In that drives it replicates inside different folder with the same name of folder with extension .exe. It also modifies the default page, default search, search page and start page of internet explorer browser by making changes in different registry location. The system3.exe virus spreads through removable devices and sends DNS request to ***Ilo.brenz.pl*** and ***ant.trenz.pl.***

7. ACKNOWLEDGMENTS

Special thanks to M/s e-Security Forensics Labs pvt. Ltd Hyderabad and M/s RSI Softech Pvt Ltd,Hyderabad for giving us the time to work on this project and permission to present our results. This analysis will give alert to all the Revenue, Military Defense and Civil engineering designers on security precautions

REFERENCES:

1. Google Scholars
2. www.bing.com
3. www.google.com
4. Various research articles