Video Malware - Behavioral Analysis

Rajdeepsinh Dodia, Priyanka Bhati, Kvvprasad, Anil Anisetti

Abstract: The counts of malware attacks exploiting the internet increasing day by day and has become a serious threat. The latest malware spreading out through the media players embedded using the video clip of funny in nature to lure the end users. Once it is executed and installed, then the behavior of the malware is in the malware author's hand. The spread of the malware emulates through Internet, USB drives, sharing of the files and folders can be anything which makes presence concealed. The "funny video" named as it connected to the film celebrity where the malware variant was collected from the laptop of the terror outfit organization .It runs in the backend which it contains malicious code which steals the user sensitive information like banking credentials, username & password and send it to the remote host user called command & control. The stealed data is directed to the email encapsulated in the malicious code. The potential malware will spread through the USB and other devices .In summary, the analysis reveals the presence of malicious code in executable video file and its behavior.

Key words: Malware, Malware Analysis, Key logger, Funny Video, dynamic analysis, malware detection, video malware

----------◆----------

1. INTRODUCTION

Malware is one of the most terrible and major security threats facing the Internet today. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The damage caused by the malicious code has dramatically increased in the past few years. One of the reasons is the rising popularity of the Internet, usage of smart phones. Current systems to detect malicious code (most prominently virus scanners) are based on syntactic signatures. Malware Analysis is the study of a malware by dissecting its different components and study its behavior on the host computer's operating system. The purpose of this paper is two folds: to help information security professionals and to aware user that malware come through any route. Malwares are spreading all over the world through internet and are increasing day by day and thus becoming the serious threat.

- *Rajdeepsinh Dodia, Priyanka Bhati, Kvvprasad, Anil Anisetti*
- *rajdeepsinhdodia22@gmail.com*
- *prriyanka00@gmail.com*
- *kvvp.knl@gmail.com*
- *anisetti0101@gmail.com*
- *Company: esflabs PVT LTD , Hyderabad, India www.esflabs.com*

Commercial anti-virus vendors are not able to offer immediate protection for zero day malwares as they need to analyze these to create their signatures. To overcome the limitation of signature based methods, 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 question that we address in this paper is as follows: How difficult to identify the malware when it is embedded with video. We tried to answer your question by analyzing through static and dynamic analysis and traced out the piece of code which causes this effect.

2. ANALYSIS

The new Malware that spreads across the country through the USB storage media, Internet and emails once it is executed; the video clip taken from the southern part of the Indian movie opens in windows media player. The Malware uses resource icon of windows media player to make fool but actually it is executable file by default. There are two methods of malware analysis which are reverse engineering and behavior analysis. Behavior analysis will study the malware interaction in-and-out of the infected host machine.

3. CONCEPTUAL FRAME WORK

Analyzing malicious software without executing it is called static analysis. In static analysis executable fingerprint does not

match with any other malware. The strings are encrypted and import disclose only one function is CorExeMain. The malicious funny video file uses 24 different icons as resources. Below figure shows the different icons in resource section of PE file (Fig1)

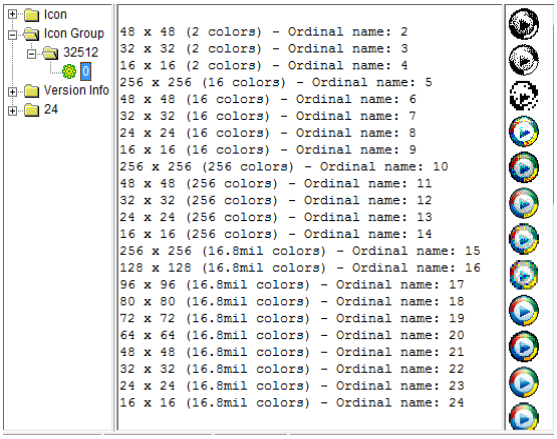

Fig. 1

The source code of malware samples is not readily available. That reduces the applicable static analysis techniques for malware analysis to those that retrieve the information from the binary representation of the malware. To overcome the limitation of static analysis, the funny video executable run 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. After executing funny video.exe, the file asks to choose the initial setting for windows media player after clicking on finish button. It creates process name wmplayer.exe to execute a south Indian movie's video and in the back end it creates another process name funny video.exe. (Fig2)

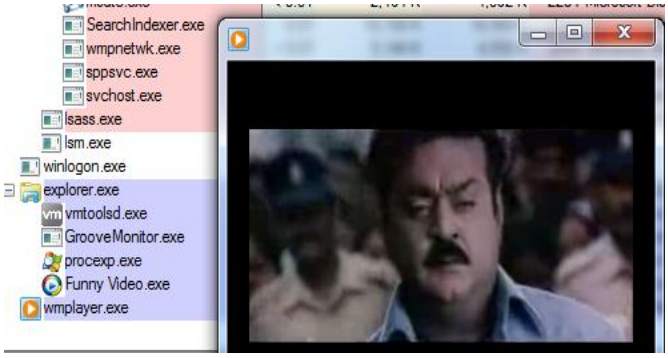

Fig. 2

The dynamic analysis is purely based on run time behavior analysis, this malicious video file run time monitoring reveals that it creates three files in SoundMax folder. (Fig3)

The following path are:-

C:\Users\%Username%\AppData\Roaming\SoundMax\realtekAudio.exe

C:\Users\%Username%\AppData\Roaming\SoundMax\funny.wm

C:\Users\%Username%\AppData\Roaming\SoundMax\smax

Fig. 3

RealtekAudio.exe is the copy of the funny video.exe file, because both have similar hash value. (Fig4)

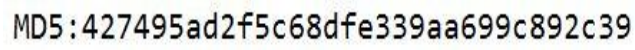

Fig. 4

Funny.wm extracts from the main funny video.exe file and placed in SoundMax folder. smax file has no extension and it is a log file that captures the keystrokes. This malware uses message hook named WH_KEYBOARD_LL for capturing keystrokes.(Fig 5)

Fig. 5

It uses SetWindowsHookEx function to capture the keystrokes from the system. So this malware trick the user to believe that it is a video file and in the back end it captures the keystrokes. For the experiment purpose, in the infected system if a users opens any account it captures the username and password and save in smax file (Fig 6). So it can also steal credentials from banking and other social media websites.

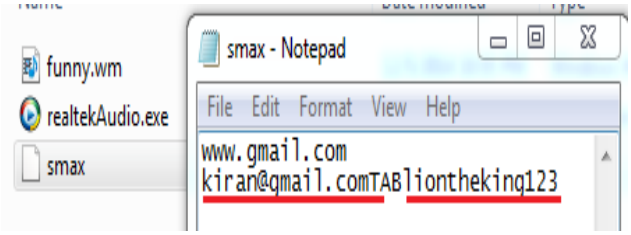

Fig. 6

Most of the malware use various locations in registry to remain persistent on the systems. Persistent means malware will active in the event of a reboot. This malicious video creates run key so that it will run at every reboot. (Fig7)

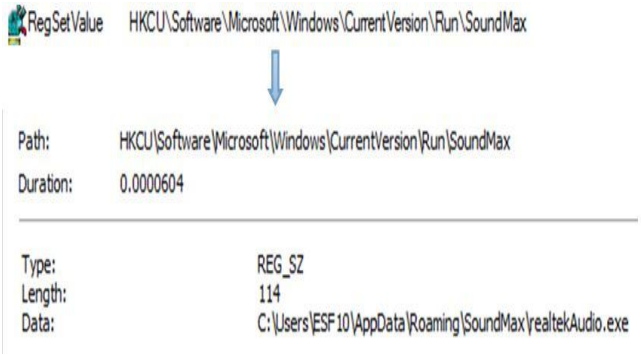

Fig. 7

These following registry modification done by the malware are:-
Key added:-
HKCU\Software\Soundmax\Settings\FirstRun= 12345
HKLM\Software\Microsoft\Tracing\Funny Video_RASAPI32
HKLM\Software\Microsoft\Tracing\setup_wm_RASAPI32
HKLM\Software\Microsoft\Tracing\wmplayer_RASMANCS
DeleteValueKey:-
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
HKCU\ Software\ Microsoft\ Windows\ CurrentVersion\ Internet Settings\ ProxyOverride
HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\AutoConfigURL
The Network Activity of this funny video is to send the DNS request to smtp.gmail.com (Fig 8).

Fig. 8

Funny Video sends smax file that stores keystroke to malware author's gmail account. The gmail account details is extracted, that is username and password of malware author where all the data is send (Fig 9).

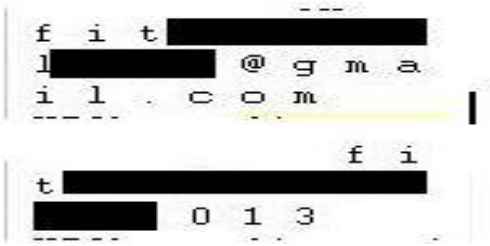

Fig. 9

To summarize, the contributions of this paper

- We propose a dynamic analysis technique that allows us to create comprehensive reports on the behavior of the malicious code.The program is driven with multiple processes and the specific actions were triggered .
- We evaluated a multiple number of real world malware samples and demonstrated and that we are able to identify the behavior that cannot be observed in single execution traces.

3. Conclusion

In this research paper, we have presented a system to explore a Funny video malware tricks the user to believe as genuine video file but it compromises the system with malware. This malware creates the registry key in auto-runs location and captures the keystrokes in smax file. The smax file contains the user activity that might be consists of banking Credentials , social network account details or any other personal information. These all information send to smtp.gmail.com using malware authors gmail account. Malware analysis is a growing area of expertise due to the new challenges presented by the modern malware.

Acknowledgment

Special thanks to the esflabs, Hyderabad for giving us time to work on this project and permission to present our results.

References

[1] https://msdn.microsoft.com/en-us/library/windows/desktop/ms644959(v=vs.85).aspx#wh_keyboard_llhook

[2] http://en.wikipedia.org/wiki/Malware

[3] http://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2013

[4] https://technet.microsoft.com/en-in/sysinternals/bb842062.aspx