DISSECTING A MALWARE ATTACK

A malware can sneak into a system in the guise of a mail-attachment or the system can get infected by simply visiting a malicious website. User is often taken off-guard while the malware sneaks into the system and compromises its integrity.

RAJ K. RAINA
Technical Director
rk.raina@nic.in

Edited by
MOHAN DAS

Malware (short for malicious Software) is the main player behind most computer security incidents. It is a code/program that disrupts normal computer operation or steals information from computer without user's knowledge. Malware Analysis is one of the key defenses employed to contain and mitigate the security incidents in cyber space.

Govt. of India has a huge IT user base handling critical data. The constant malware attacks make it imperative to have a general understanding of how the malware works. A malware cannot get into a system by itself and can neither execute of its own. It always requires a user intervention to execute its mission. The malware attacks can be reduced/ minimized to a large extent by understanding the nature of malwares and this is where the "Malware Analysis" plays its role.

In the event of an attack, Analysis of Malwares provides valuable intelligence for gearing up and developing signatures for the security devices in place. The signatures applied at gateways help to identify infected machines and to deter/stop further occurrences of similar attacks. And signatures updated in the enterprise security solutions are percolated to the end-points to remove the infections.

MALWARE A CAMOUFLAGE

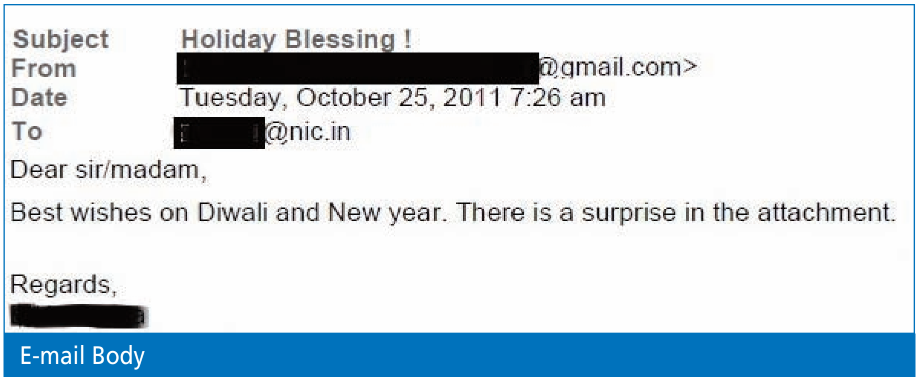
Malware disguises in packages such as Games, Cool Animations, FAKE Anti-virus, a Pornographic image/movie on the web. These packages entice the user to unlatch the regular security of his system. A malware can also sneak into a system in the guise of a mail-attachment or by simply visiting a malicious website. User is often taken off-guard while the malware sneaks into the system & compromises its integrity.

MALWARE ATTACK – A CASE

The Dissection of a malware will give you an insight into how a malware peeps into a system and steals the information wonderfully.

This particular malware attack used mail as the transport mechanism for targeting users working at sensitive places in NICNET. The email appeared to be coming from a known high ranking officer and contained instructions which would tempt the recipient to open the attachment that the mail contained.

An e-mail bearing subject "HOLIDAY BLESSINGS" was received by a large number of users



Subject Holiday Blessing !
From [redacted]@gmail.com>
Date Tuesday, October 25, 2011 7:26 am
To [redacted]@nic.in

Dear sir/madam,

Best wishes on Diwali and New year. There is a surprise in the attachment.

Regards,
[redacted]

E-mail Body

from a mail-account apparently belonging to a high level Officer in Government of India. The mail contained an attachment "DiwaliGift.doc" which was screened OK by all Antivirus solutions in place as on given date/time. The body of the e-mail contained the message that had direct relevance to the attachment.

ATTACHMENT

The mail attachment in the form of a doc file was specially crafted so that the system with a vulnerable MS-WORD application gets compromised by opening a backdoor for the remote attacker, allowing the remote attacker to collect useful information from the system and transmit the same to the master.

The doc file "DiwaliGifts.doc" had an embedded malware that exploits CVE2010-3333 vulnerability in MSWORD 2007 and below.

DYNAMIC ANALYSIS REVELATIONS

On opening the attachment, a one-page greetings message is displayed with the title "HAPPY DIWALI". The message appears a genuine one correlated with the festival timing. It does not infuse any doubt in the mind of the user about the intentions of the embedded malware in the document.

While the document opens with a festival greeting, certain files get dropped in the victim's computer's "%temp%" directory in the background. The system attempts for DNS resolution and connects to one of the following domains:

kittyshop.kilu.org- hosted on-
78.46.104.43

www19.subdomain.com- hosted on-
78.46.104.43

treeshop.kilu.de- hosted on-
78.46.103.46

www13.subdomain.com- hosted on-
78.46.103.46

The system further starts sending and receiving information. The dropping of the files and then initiating connections happen in the background without users knowledge.

After some time, the files in %temp% directory get automatically deleted, a ploy by the attacker to remove the traces.

The actual process sequence is shown below:

CODE ANALYSIS -- FINDING

Static analysis of the word file shows that the doc file attachment has three (3) files wrapped into one.

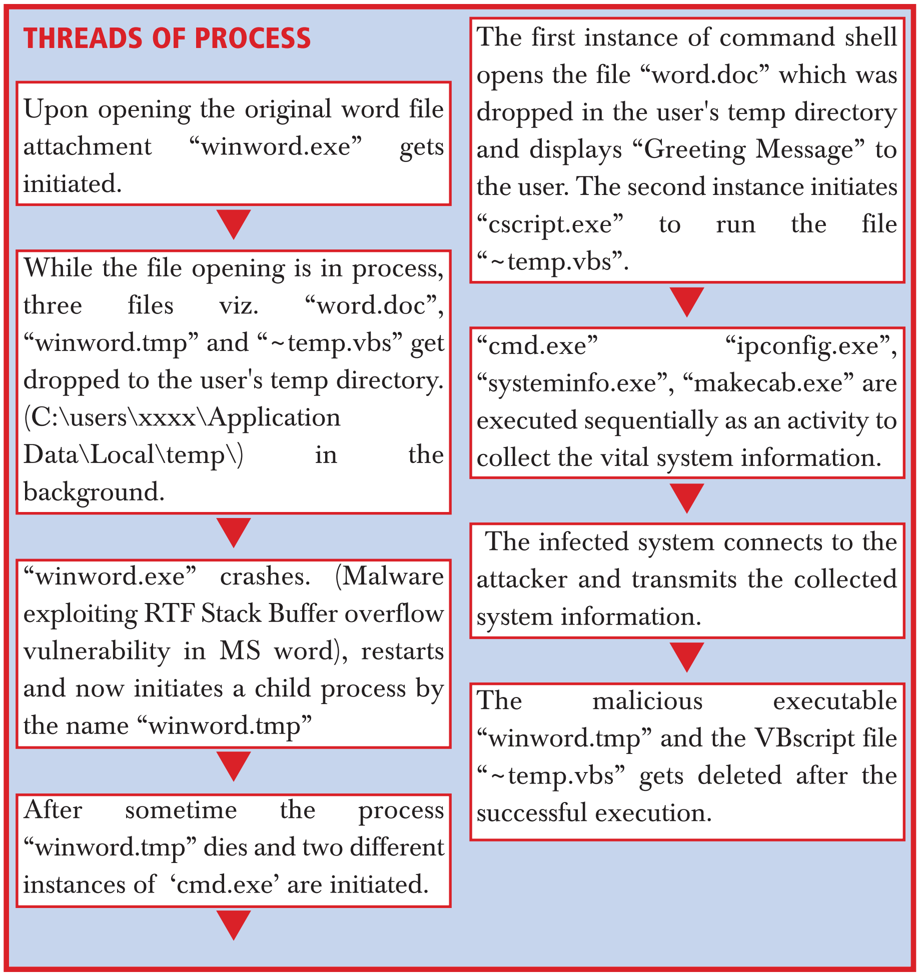
1. An executable file
2. A VB script file
3. A MS word file

Ms. ANJANA CHOUDHARY
DDG, Cyber Security Division

Multitude of malicious samples confronts NICNET on a regular basis. While Antivirus solutions help to detect and eradicate most of the infections, some malwares have the capability to bypass the security solutions and find their way inside the NICNET. These malwares belong to the category of targetted attacks and/or zero-day-attacks.

When these attacks are encountered or informed, the cyber security team identifies and collects the malware sample. This sample is subjected to thorough analysis to understand how malware tries to fulfill the harmful intent of the attacker. The Malware Analysis results help us to gear up our security solutions to identify the infected machines and plan for the removal of infection from these systems.

It is mostly observed that an infected client is without an Antivirus Solution or has an outdated signature file. We constantly educate & recommended to have a latest Antivirus solution installed and have the system software and application softwares patched as a precautionary measure to overcome the malware threats to a large extent.



THREADS OF PROCESS

Upon opening the original word file attachment "winword.exe" gets initiated.

While the file opening is in process, three files viz. "word.doc", "winword.tmp" and "~temp.vbs" get dropped to the user's temp directory. (C:\users\xxxx\Application Data\Local\temp\) in the background.

"winword.exe" crashes. (Malware exploiting RTF Stack Buffer overflow vulnerability in MS word), restarts and now initiates a child process by the name "winword.tmp"

After sometime the process "winword.tmp" dies and two different instances of 'cmd.exe' are initiated.

The first instance of command shell opens the file "word.doc" which was dropped in the user's temp directory and displays "Greeting Message" to the user. The second instance initiates "cscript.exe" to run the file "~temp.vbs".

"cmd.exe" "ipconfig.exe", "systeminfo.exe", "makecab.exe" are executed sequentially as an activity to collect the vital system information.

The infected system connects to the attacker and transmits the collected system information.

The malicious executable "winword.tmp" and the VBscript file "~temp.vbs" gets deleted after the successful execution.

The executable has some encrypted portions which when decrypted indicate the domain where the information is posted by the malware and also has reference to the file "~temp.vbs"

Why Malware Analysis?

- Know how malware works
- Contain an ongoing attack
- Identify the Infected Clients
- Assess any data leakage
- Plan removal of infection from clients

"If you ever encounter a suspicious file or Email, please forward the same to Malware Lab. mallab@nic.in for analysis"

The file "~temp.vbs" is a VB Script file and its code reflects the activities that the malware is designed to carry out. The analysis of "~temp.vbs" indicates the malware activities in chronological order as:

- Saves directory listing of all drives is each respective drive as "[drive letter].tmp"
- Saves network information of the machine in a file "j.tmp"
- Executes "systeminfo" and saves the result is saved in a file "k.tmp".
- Saves Tasklist output(running processes information) to the file "m.tmp"
- The content of tmp files so created is combined in a new file "L.tmp" and then "makecab.exe" command is used to compress it in a new file "1.cab"
- The result of these commands is now posted(transmitted) to the attacker using HTTP POST
- All the .tmp files created are deleted from the system
- Code to delete the dropped malicious files "~temp.vbs" and "winword.tmp" is also in the script file indicating the automatic removal of these malicious files after they are executed.

The code analysis collaborate the earlier findings that the malware collects vital information from the system and posts it to the attacker. It further removes the traces and this all is happening in quick succession and without users' knowledge.

CONCLUSION

A malware attack is very difficult to be sensed by an end-user as it does not leave any trace of the information robbery and yet the system stands robbed. The only way we can safeguard our data/machines from Malware attack is through cautious approach in web-surfing, handling our mail attachments, and not falling prey to the temptations of free software like fake Antivirus or music/videos and last but not the least by keeping the software's patched and Antivirus updated.

FOR FURTHER INFORMATION
Raj K. Raina Technical Director
Room no. 209, Cyber Security Division
A1B3, 2nd Floor, NIC
A-Block, CGO Complex, New Delhi
Contact : 9868935127, 011-24305127,
0120-2417585