Digital Forensic Analysis Of Malware Infected Machine- Case Study

Amulya Podile, Keerthi Gottumukkala, Krishna Sastry Pendyala

Abstract: Internet banking has created a convenient way for us to handle our business without leaving our home. Man-in-the-Browser, is a special case of Man-in-the-middle attack targeted against customers of Internet banking. One of the capabilities of Man-in-the-Browser Trojan is modification of html referred to as html injection that allows the attacker to alter the html of a page before it is sent to the browser for interpretation. In this paper the authors discussed about forensic analysis of “RAM, Volatile data, system logs and registry” collected from bank customer computer infected with Trojan and confirmed the source of attack, time-stamps, and the behavior of the malware by using open source and commercial tools.

Index Terms: Digital Evidence, Digital Fingerprint, HTML Injection, Man in the Browser, RAM, Registry, Volatile data

1 INTRODUCTION
MAN-IN-THE-BROWSER, a form of security threat in which a proxy Trojan infects a web browser by taking advantage of vulnerabilities in browser security and modifies web pages, transaction content or inserts additional transactions, all in a completely covert fashion invisible to the user and web application host. Carberp, Silent banker, SpyEye, Zeus [1] are the most important man-in-the-browser Trojans developed targeting banking & financial industry. Zeus, nick named as “the king of banking Trojan” [2] and first known piece of Malware sold via license till 2011, entered the malware scene in 2007. Zeus can infect windows PCs having Internet Explorer and Firefox browsers. The mobile variant called ZitMo (Zeus in the mobile) entered the market in 2012 and has the ability to infect Windows, Android, Symbian, BlackBerry OS and defeats SMS-based banking “out of band” two-factor authentication. Industry reports indicate that the most popular Malware next to Stuxnet that caused panic is Zeus. In this paper authors discussed about forensic analysis of “RAM, volatile data, system logs and registry” collected from bank customer computer and confirmed the source of attack, time-stamps and the behavior of the malware by using open source and commercial tools. This report helped the bank from regulatory and legal liability.

2 BRIEF FACTS OF THE CASE
ABC bank (the client name changed) is one of the banks offering net-banking services to its customers. One of the customer (Air Ticketing Company) of ABC Bank while performing on-line transaction on April, 2nd, 2014, has observed additional fields on the bank net-banking authorization page like date of birth, mother’s maiden name, sort code etc., apart from regular fields like name, card number, expiry date and security code. The customer furnished the information “assuming that the bank must have changed” the requirements from April, 1st, 2014 (start of a new financial year in India) and lost more than $ 0.6 million in four days starting from April 2nd, 2014. The customer appealed to the bank to pay-back the money informing the fault is on bank’s side for not taking “reasonable security practices”. Fig. 1 shows the net banking authorization page with extra fields, as observed by the customer of ABC bank. As per the Section 43A of Indian Information Technology Act, 2000 [3] the banks and other intermediaries who have failed to maintain reasonable security procedures must pay adequate damages as compensation to victims who lost money in net/on-line banking. And also as per Information Technology (Intermediaries Guidelines) rules 2011 it is obligatory on the part of banks to report cyber security incidents to the Computer Emergency Response Team- In (CERT-In). ABC bank hired the Fraud Management & Digital Forensic team under Enterprise Security and Risk Management (ESRM) practice of TCS, to conduct forensic analysis of customer machine to identify the presence of any malware and the root cause of the incident with the timelines.

- Amulya Podile is currently working as a Digital Forensic and Malware Analyst at Tata Consultancy Services Limited, Hyderabad, India. PH: +91 9000399823. E-mail: amulya.podile@gmail.com
- Keerthi Gottumukkala is currently working as a Digital Forensic Analyst at Tata Consultancy Services Limited, Hyderabad, India. PH: +91 9177551988. E-mail: keerthi.gottumukkala@tcs.com
- Krishna Sastry Pendyala is currently working as Practice Head for Fraud Management & Digital Forensics at Tata Consultancy Services Limited, Hyderabad, India. PH: +91 9490433296. E-mail: sastry.pendyala@tcs.com

Fig. 1. Net Banking Authorization Page with Extra Fields
3 DIGITAL FORENSIC INVESTIGATION

When the Digital Forensics team visited the victim’s company the suspected infected machine was in “switch-on” mode. The Forensic team conducted the investigation in two stages [4]:

Stage 1: Collection of digital evidence
Stage 2: Analysis of collected digital evidence.

3.1 Stage 1 - Collection of digital evidence

The Digital Forensic team first imaged the Random Access Memory (RAM) forensically in.dd format on to a forensically sterile media using FTK Imager. The team also collected registry files, event log files, internet history and other volatile data from the suspected machine such as list of running programs/processes, network connections and dll files loaded from the live system. The integrity of digital evidence is maintained throughout the entire investigation by generating the hash value, the “digital finger print” of the evidence. The tools used for collecting the evidence are FTK Imager and Digital Evidence Forensic Tool kit (DEFT).

3.2 Stage 2 - Analysis of collected digital evidence

Digital Forensic analysis was carried out on three sources of evidence collected – memory dump, registry and event logs.

3.2.1 Memory dump analysis

RAM/Memory dump analysis is very crucial because, the Windows registry is loaded into memory upon the startup of Windows which stores program and system data used by both applications and the operating system [5], [6]. Memory analysis of the registry can also provide access to many artifacts including the most recently used (MRU) list programs, programs run at startup, programs launched from the desktop among others. The RAM dump collected was parsed using Volatility, a free memory analysis tool & framework written in Python, for parsing and analyzing the memory dump files. Volatility supports 32-bit and 64-bit versions of Windows, Linux kernels, Mac OS X (10.5-10.9) and android phone (32 –bit and 64-bit) memory dumps. Volatility has many plug-ins useful for identification of malware infection. A few important ones are:

1. Connscan – to list TCP connections;
2. Pstree- to show processes in parent/child tree
3. Pslist – to scan for hidden or terminated processes
4. connections– to list open connections;
5. dlllist – to list loaded DLLs for each process;
6. malhink – to detects hidden and injected code;
7. pslist- to print list of loaded processes
8. svscans – to detect hidden services
9. apihooks– to detects hooks into user and kernel mode processes

The list of running processes were extracted from the RAM dump. The list shows some processes are hidden. The list of extracted processes is given at Fig. 2

Fig. 2. List of processes of the RAM extracted using Volatility Framework

The process tree that was extracted from the RAM dump shows a process named “emvije.exe (PID 1688)”. This process is a child process of the “explorer.exe (PID 1240)” and is not associated with any application/program. The screen shot of the process tree is given at Fig. 3.

Fig. 3. Process Tree of the RAM extracted using Volatility Framework

The list of network connections were also extracted from the RAM dump. From these connections it appears that a connection has been established between the local system using PID 1240- explorer.exe and the IP address “24.177.33.91”. This was suspicious because the explorer.exe as such does not initiate any connection. The screenshot of the connections from the dump is given in Fig. 4.
Fig. 4. Network connections extracted from the RAM using Volatility Framework

The list of network connections also shows that the local IP address of the system is “111.112.113.52”. A “whois” lookup was launched to determine the ownership and country of IP address. The IP lookup reveals that it belongs to “China Telecom-NINGXIA”. The Process ID that is associated with these connections is “3696(jucheck.exe)” which is also a child process for “explorer.exe (1240)”. The screenshot showing the local IP address is given at Fig. 5.

Fig. 5. Network connections showing external IP Address communication extracted from the RAM using Volatility Framework

The RAM dump was analyzed using the “malfind” plugin of Volatility framework to extract the process dumps associated with each process that is running. The malfind plugin extracts the process dumps that are infected with malware. The 35 process dumps produced by the volatility were uploaded to “virustotal.com” to check if the processes present in the dumps are infected with any malware. Four process dumps “explorer.exe, jucheck.exe, igfxpres.exe, jusched.exe” were reported to contain high detection ratio for the presence of malware. The above four process dumps were found contain a malware named “PWS: Win32/Zbot.gen!GO”. The malware is also known as “Zeus Game over”, a Trojan which can hook API addresses and inject code into webpages to monitor online banking activities.

3.2.2 Registry Analysis
The Registry files were parsed by using registry viewer and were examined [7], [8] to identify the evidence related to malware. One of the characteristic behavior of PWS: Win32/Zbot.gen!GO malware is disabling the windows firewall by altering the registry key:

HKLM\System\Controlset002\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\EnableFirewall and sets the value to “0”. The same alteration was found in the registry and the screenshot is given at

Fig. 6. The alteration happened on 01-April-2015. Another characteristic of this malware is altering the registry key:

HKLM\System\Controlset002\Services\SharedAccess\Star t to “2”. The same alteration was found in the registry and the screenshot is given at Fig. 7.

Fig. 7. Alteration of the registry key

The registry analysis also revealed the IP address of the system as “111.112.113.50” and the IP hook-up shows the service provider as “China Telecom-NINGXIA”. The IP address of the system was updated to “111.112.113.50”. Fig. 8 gives the IP address from registry, including the time-stamps.
3.2.3 Event Log Analysis

Event log file, AppEvent.Evt, when parsed and analyzed by using EnCase version 7.1 software revealed that the antivirus “Quick Heal Total Security” present the system was uninstalled in the system on 01-April-2014 at 11:49:36 AM. Fig. 9 gives the screenshot for the event log entry.

4 FINDINGS

Following are the important findings on forensic analysis of Indicators of compromise:

1. The Trojan named “PWS: Win32/Zbot.genlGO infected process explorer.exe and also the child processes of explorer.exe such as ”juchek.exe”, “igfxpres.exe”, “jusched.exe”.
2. The Antivirus “Quick Heal Total Security” was uninstalled in the system on 01-April-2014 at 11:49:36 AM.
3. The malware could have been installed in the system on 01-April-2014. This observation is based on the following changes that have taken place in the system.
4. The Antivirus was uninstalled in the on 01-April-2014 at 11:49:36 AM.
5. The IP address of the system was updated to “111.112.113.50” on 01-April-2014, at 02:02:53 PM.
6. Windows Firewall was disabled on 01-April-2014 at 02:46:21 PM.
7. The last entry in the registry is 01-April-2014 02:46:21 PM.
8. The Last entry in the event log files “AppEvent.Evt” and “SysEvent.Evt” is 01-April-2014 02:46:21 PM.

5 CONCLUSION

Forensic analysis of RAM, volatile data, event logs and registry is very crucial in investigation of windows infected machine. Forensic analysis of these indicators of compromise in this case revealed not only the source of attack but also the nature and behavior of malware. Infecting the explorer.exe, disabling the firewall, changing the event logs, registry, creating an executable with random name, hooking API address and injecting code into webpages to monitor online banking activities are few features of this variant of Zeus Trojan. The results obtained corroborated the facts of the case with timelines and protected the bank from legal and regulatory liability.

ACKNOWLEDGMENT

The authors wish to thank Haritha Annangi, Anwesh Mandadi, PVS Murthy and Satish Thiagarajan for their continuous support.

REFERENCES