International Journal of Advanced Computer Research
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
Volume-5 Issue-18 March-2015

Security as a Serious Challenge for E-Banking: a Review of Emmental Malware

Sirwan Geramiparvar[1*] and Nasser Modiri[2]
Graduate student, school of electrical and computer engineering and information technology, Islamic Azad University, Zanjan branch, Iran [1]
Assistant professor, school of electrical and computer engineering and information technology, Islamic Azad University, Zanjan branch, Iran [2]

Received: 15-February-2015; Revised: 28-March-2015; Accepted: 30-March-2015

Abstract

Nowadays, security is considered to be one of the requirements of all the big and small industries and service and information organizations. Specifically in the advanced e-banking systems, due to the financial and personal issues of the clients and the banks credits, not only is essential and important, but also an inseparable part of all the banking steps and operations. This paper aims to analyse the behaviours of the financial malwares and their threats towards security and provide their behavioural patterns specially Emmental using metric-based model and finally solutions to stop and prevent such threats and attacks by the malwares.

Keywords

E-banking security, financial malwares, malware metrics, metric-based model, Operation Emmental.

1. Introduction

Information technology and communication provided an opportunity for monetary and financial fields so that the efficiency in this area experienced a considerable growth and progress in the last two decades. But this opportunity is now a requirement, in a way that one cannot recommend a non-electronic solution for the development of banking industry. Beside the progresses tanks to the transactions each being of high financial value, there are people seeking for innate and structural and procedural weaknesses and non-operational weak points that can entail losses.

*Author for correspondence

This means that the value, validity and accuracy of the banking procedures are bound with the presence of electronic security. Failures of any kind in providing security can bring cause damages to the whole banking and the reliability of the bank. Basics of e-banking industry such as information banking and financial and banking data systems, hardware and communication equipment, information technology personnel, systems users, systems and equipment producers, and companies providing payment services, are subjects to two kinds of security problems: abusing the weak points of the basics mentioned, and unintentional happenings due to their malfunctions. Statistics in the security companies' websites show an increasing and dramatic rise in the number of malwares and cyber-attacks. According to the statistics provided by Kaspersky™ in 2013 on all the malwares and attacks registered in the world, 6.2% of the malwares, equal to 28 million, are created for financial abuse purposes or have attacked financial systems. Recently, TrendMicro™ has investigated, in a technical report, a dangerous malware called Operation Emmental that passes over the two-stage passwords systems and behaves in a very complicated way. This paper tends to investigate the behaviour of these malwares and analyse them and identify their behaviour and functional pattern according to the metric-based model. This paper consists of 5 main parts and in the next part, the literature and a summary of the available models is provided to investigate and analyse the malwares and cyber-attacks. In the third part, an explanation, the way of distribution, function, and the influences of the mentioned malware and the modelling of the malware behaviour according to Gadelrab model and metric-based model is provided. In part 4, we will investigate the findings and the results of the modelling, and an evaluation of the behaviour and the performance pattern of the financial malwares

especially Operation Emmental and solutions to take into account will be provided. Finally conclusion and future works will be presented in the fifth part.

2. Related Works

In identifying and classifying the computer malwares, the academic studies and researches are divided into three groups namely: signature-based methods, behavior-based methods, and heuristic methods. Each of these methods in turn is simulated in a virtual environment like virtual machine and are analyzed observing the behavior and performance using the dynamic method, or according to the physical properties and systematic behaviors (change, removal, etc.) using the static method. But in the procedural investigation of attacks and malwares, there exist 2 malware resources and 3 models. Malware resources include Swimmer ontological model [5] and MAEC model belonging to MITRE. Of the procedural models, the first model belongs to Howard and Longstaff presented in 1998 [6] in simple words providing a procedural investigation using a certain flow graph. They divided the attack procedure into seven phases. In the first phase are the attackers (hackers, spies, etc.) and in the second phase are the tools used by them like user commands, information exchange, etc. In the third phase one can see the threats, like the faults in designing, implementing and structuring. Actions used for the attack can be found in the fourth phase, such as sniffing, reading, copying, etc. The fifth phase is the targets of the attacks, like the data, bank accounts, etc. The next phase is for the unauthorized results like denial of service, stealing resources, etc. Finally, the seventh phase includes the attacks such as destruction, political or financial purposes, etc. although the model is too simple, but it was an inspiration for numerous models afterward. The next model under investigation presented in 2007 by Gadelrab and his colleagues [4], has five dimensions. The five dimensions of malwares procedure consist of resource of the attack (distant or near), gaining or increasing access (root, system, user, normal), vulnerability (configuration, implementation), carrier (network traffic or a normal action) and target (operating system, memory, etc.). They tested and implemented their model with eight test statuses and the results of the evaluations by IDS indicated efficiency and success of the model and the model was later improved in 2010 by Saber and his colleagues [2] and a better one was provided. In 2008, the second model of Gadelrab and his colleagues [3] was developed. They tested 39 samples of analyzed malwares from the CME (Common Malware Enumeration) list and evaluated the patterns of the analyzed attacks. They found out that the attack steps may be divided into eight steps, including: reconnaissance (R), victim browsing (VB), execute program (EP), gain access (GA), implement malicious code (IMC), compromise data integrity (CDI), denial of service (DOS), and hide trace (HT). According to these steps, they investigated and analyzed some well-known malwares such as Code Red-I, Code Red-II, Sasser, Trinoo, etc. It is worth mentioning that this model deals with the attack process itself only not with the implementation of the details and the attack implementation commands like buffer overwriting or code sequence. Using the second model of Gadelrab and studying a large number of CWEs (Common Weakness Enumeration) and CAPECs (Common Attack Pattern Enumeration & Characterization), Geramiparvar and Modiri [1] introduced nine metrics as the criteria of identifying and classifying computer malwares and cyber-arracks in 2014. Furthermore, they prioritized the metrics and, using the fuzzy analytical hierarchy process (FAHP), based on the level of the influence by each one of the metrics on making the attack step or on the eight attack phases, the weights and notability of the metrics was obtained and they introduced their metric-based model.

3. Distribution method and performance scenario of Emmental

Defined in one sentence, Emmental is the porous Swiss cheese reminding us of many holes through which one can go inside. This malware is a virus capable of passing through two-stage verification systems. This cyber-attack is one of the most dangerous and complicated viruses and attacks known so far. It can pass through two-step verification systems although they have been of the safest verification and security systems. The attack begins when the user receives an email from a reputable company (like Google, Microsoft, e-Bay, etc.) containing an attachment with an .RTF suffix behind which there is another file. If the user is curious enough to execute the file, there appears a warning message on the screen saying you have opened a file with a .CPL suffix that can be harmful. After the .CPL file is executed, another file is created

named netupdater.exe which seems to be for updating Windows but is actually a fake update and activates a malware. The user is redirected to a fake page for banking transactions. On a phishing page, the customer enters information like username, account number, and other numbers as required. Then the PIN is asked (for verification). In the next step, OTP is required that can be obtained by the applications on the cell phone. Normally, this code is sent to the person with levels of delay through SMS. Now, the phishing page requires the person to install an application on their cell phone by which a message is sent so the code in the message can be entered into the website. The website seems safe but it is a fake one and its mobile application cannot be trusted. As it appears to be the case, the SMS sent by the bank is not received and the user has to click on "No SMS received from the bank". After clicking on the link, there opens a page requiring the application to be installed. Following that, the user enters the password generated by the fake application into the website. The application holds a number of pre-generated passwords and every time it displays one of them. At this time, the website checks whether the password entered is one of the pre-defined ones. It is not even helpful for the users to guess the passwords since they cannot pass the fake verification step. All of these trends to persuade the user to keep the application on their cell phone because otherwise, as claimed by the fake website, the user can no longer use the bank online. The installation of this application enables the attacker to gain full control and power over the user's online bank sessions. In fact, the application prevents the bank SMS from being sent to the user and the message is automatically directed to the attacker. Having received the message, the attacker has full online access to the user's account. The report provided by TrendMicro (producing PC-Celine) about the performance of Emmental shows the distribution of this malware in Austria, Switzerland, Sweden, and some other European countries and Japan and most of the attacks are reported to be from Russian-speaking countries.

3.1 The influences of the malware

of the negative and harmful influences of this malware are the following:

- Change in the address and DNS settings to a point on which the attacker has access and control. From now on, the attacker gains control of the infected systems in internet to access different domains.
- Installing a new root for SSL certificates in the infected systems. This step enables the attacker to establish phishing attacks without the user's browser warning. This is because when the .CPL file was executed, a fake Windows certificate was created.
- This malware, after doing what was mentioned above, removes itself automatically and makes it hard for it to be searched for and found in the system. Therefore, in case it is not detected before being removed, it will never be found although antiviruses are used. The infection occurs only in the configuration of the system.

3.2 Analysis of the malware based on Gadelrab model

We are going to investigate the stages of the Emmental virus based Gadelrab eight-phased model and provided its behaviour graph. As it was mentioned in the attack method, the attacker sends a fake email to the victim claiming to have been sent by one of the reputable companies. After the email is opened, the .CPL file should be executed to gain more access and implant the malicious code. After the execution, a fake certificate is created and the victim is guided to a phishing bank webpage located on the attacker's server. The username and password are entered and the attacker waits until they receive the OTP from the bank. While the customer is busy working on a fake webpage, the attacker is withdrawing illegally and doing the desired operations. The attacker removes the traces after everything is done so that it is impossible even for the antiviruses to detect anything. Therefore, the stages of the attack are presented schematically in Figure 1. According to this analysis, the stages of the attack based on the eight-phased model are: GA, IMC, EP, CDI, IMC, GA, EP, and HT.

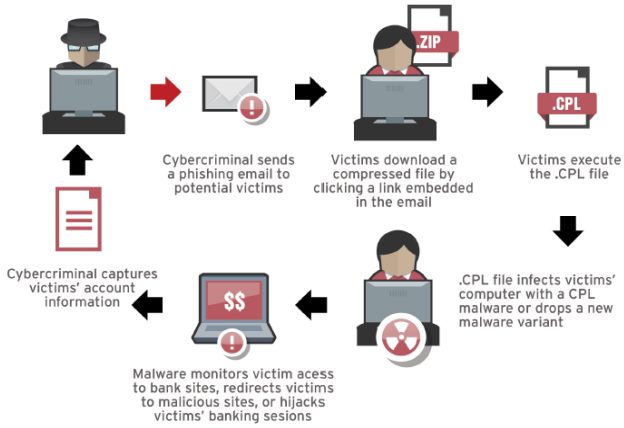

Figure 1: Schematic process of .cpl file attacks

3.3. Analysis of the malware based on the metric-based model

As mentioned in part three, in their study, Geramiparvar and Modiri introduced nine metrics as criteria to identify and classify malwares extracted from the management weak points deep within the system and structure (configuration). The nine metrics are presented in Table 1 in order of priority and importance.

Table 1: Malware and cyber-attacks metrics

No	Metric	Description
1	Input validation	How do we know that the input data is valid and reliable?
2	Authentication	What is your identity?
3	Authorization	What can you do?
4	Installation and configuration management	Who will run your application? Which one of databases are you connected to? How to make these preferences secure?
5	Sensitive Data	How applications protect passwords & sensitive data?
6	Session Management	How applications manage and protect client sessions?
7	Message Encryption	How do you protect credential data (privacy)? How do you prevent data and libraries from being distorted (integrity)?
8	Exception Management	What do you do if an application or calling for a stored procedure fails? How many sensitive system level details would be disclosed?
9	Auditing and Logging	It describes what action was done by anyone at any given time.

Now we want to investigate and analyze the influences of the metrics on the attack steps. After the email is opened (out of curiosity or anything else), there can be found an attachment that includes a file in it. If in the installation and configuration management metric an appropriate policy for the personalization of the email inbox is used and not every attached file (especially the .CPL ones) are opened and executed or using the metrics, the control and access to the resources and operations and inbox is personalized appropriately, the first phase of the attack (GA), being the access to the control panel settings and gaining access due to the user's ignorance, is prevented. In the next stage, after the new file netupdater.exe is created, the second phase of the attack (IMC) starts and the installation and configuration metric has an important role. This phase would be prevented if the suspicious file was not executed. If this file is executed, the third phase (EP) starts and once again the installation and configuration metric plays an important role because this phase could be stopped through preventing the infected file from being executed and, if so, the connection to the attacker's server and granting access to the resources would be made impossible. In the fourth stage (CDI), the DNS settings are changed and the new address to access the attacker's server is provided where installation and configuration and verification metric plays an important role and can prevent sudden and suspicious DNS change through validating the validity of the changer. The next step (IMC) a new root for SSL certificates is installed so that, in case even the https of the infected server is used, no security warning is shown to the user. Also at this stage the installation and configuration management and session management metric plays an important role and the installation of the root can be prevented through appropriate configurations and settings. Having entered the username and password and having received the OTP from the bank, the attacker is verified and gains access to the account (GA). At this stage session management is important since the attacker's access can be prevented through appropriate session management and identifying the attacker. After gaining access, the attacker starts banking operations (EP) and hides traces (HT) after it is done. At this stage, through appropriate logging and saving histories, one could prevent the malware and its harmful influences. Therefore, based on the metric-based model, the malware signature hierarchical analysis can be written as follows: GA (Author OR CFGmngmnt), IMC (CFGmngmnt), EP

(CFGmngmnt), CDI (CFGmngmnt OR Authent), IMC (CFGmngmnt OR Session), GA (Session), EP, HT (log).
By signature, we mean a unique characteristic representing behavior and behavioral patterns of a malware. This signature or behaviors of the kind can lead to the identification of Emmental or similar malwares.

4. Findings and results

Comparing the two Gadelrab model and metric-based model shows that the first model only introduces some generalities and sequences of the 8 attack phases. In addition to the stages of the attack and their sequences, the second model, however, tells us what weaknesses malwares and cyber-attacks use based on what metric they access the attack steps. Furthermore, this model turns out to be more accurate in finding out the classes and similar malwares. Using the results of this model, one can find that some weaknesses are innate, some are structural and some are system ones. But one should not forget the weaknesses and the mistakes made by humans. To provide a solution in order to prevent malwares from operating, the followings are suggested:

- Never trust unknown emails, even if they are sent from reputable companies.
- Never open suspicious emails usually containing a link or an attachment inside. Do not download the attached files. The settings of the email Inbox should be in a way that suspicious files are prevented from being received.
- Do not execute suspicious files manually or automatically (even if named as something familiar). The security settings must be done in a way that before any file us installed, besides security controls, questions are asked to make sure the resource is trustable.
- The system must have a safe configuration; i.e. before any execution and installation, the security must be provided and the secure installation of the software must already be possible (for example, the SSL certificates should not be easily changed).
- Considering the increasing number of Android malwares, secure applications should be made. Do not install untrusted applications coming from unknown resources.
- For the systems and sessions (the interaction between the user and bank applications like the internet bank, mobile bank), powerful and trusted encoding software and software and hardware security configurations, if possible, must be used.
- For the verification systems and in order to prevent potential abuses, biometric verification systems and systems like Tokens and VoIP's can be used.
- Powerful logging systems can be used that can prevent the removal of any log or transaction and is able to pursuit suspicious or unknown transactions or IPs on a daily or weekly basis.
- Financial systems of any kind that deal with financial, bank and personal information of people must be controlled and investigated with penetration test softwares before being installed and distributed.
- Use DMARC technology that can help the users prevent phishing attacks and that verifies original emails and domain names

of the significant characteristics of analyzing malwares according to the metric-based models, one can name the following:

- This model can be used as syntax to express the behavioral characteristics and signatures of the malwares. In fact, it can be a new language to show the malware patterns and explain their performances.
- It is introduced according to the recommended models of describing the malwares and it benefits from rich dictionary and databases like CWE, CVE and CAPEC.
- It is capable of being used in software security systems such as antiviruses, firewalls, Pentest products and hardware products like UTM and in parts like IDSs and IPSs.
- It is compatible with the implementation controls of information security management system (ISMS) regarding metrics like managing the configuration and installation, controlling the access and monitoring etc.

5. Conclusion and Future Work

Today, most of the malwares are unconsciously focusing on banking and financial systems to steal the electronic money. As security is a serious challenge (opportunity and threat) for electronic banking (due to the high risk for bank security and reputability), it is essential to prevent financial malwares from penetrating the bank systems. In this study, we tried to investigate one of the most complicated and harmful financial malwares named Emmental, and to identify and model its behavior and behavioral pattern. These malwares can be prevented from entering the computers through classifying and saving their behavior and provide ways to prevent and counter them and implement the patterns in systems like IDSs and IPSs. Studying the metric-based model shows that the malicious codes and attackers use weaknesses in the system and configuration and the ignorance by the user. Due to the necessity of establishing and considering security in banking, financial and personal issues of the customers, and due to the importance of making electronic and internet banking systems trustable to them, it is better for the authorities to redefine, design and implement safe banking systems, safe ground works, safe internet, safe mobile applications, safe electronic money, etc. It is worth mentioning that because the attacks are nowadays more complicated, combined and in a wider range, the older and common solutions are no longer of use and there is a need for newer and more capable ones. Today, there are many unanswered questions, some of which are the applications coming from unknown resources. An attacker may attack or start a malware from one country and stop the attack due to bugs or refraining from being detected, and a while later, another attacker from another country continue the process. Sometimes even the phase or the level of the attack is unidentifiable. These all can be dealt with and invested on in future researches. The human factor is a challenge and GAP in security and in information security management systems. Appropriate security models and training courses should be redefined for the purpose of reducing the security gap and trying to solve this problem.

References

[1] M. Sirwan Geramiparvar, N. Modiri, "Presenting a Metric-Based Model for Malware Detection and Classification", International Journal of Computer & Information Technology (IJOCIT), Vol. 2, Issue, 4, 2014, pp. 528-539.

[2] M. Saber, T. Bouchentouf, A. Benazzi, M. Azizi, "Amelioration of Attack Classifications for Evaluating and Testing Intrusion Detection System", Journal of Computer Science, Vol. 6, Issue 7, 2010, pp. 716-722.

[3] M. Gadelrab, A. Abou El Kalam, Y. Deswarte, "Execution Patterns in Automatic Malware and Human-Centric Attacks", Seventh IEEE International Symposium on Network Computing and Applications, July 10-12, Cambridge, Massachusetts, USA, 2008.

[4] M. Gadelrab, et. al, "Defining categories to select representative attack test-cases", Proceedings of the ACM workshop on Quality of protection, ACM New York, NY, USA, 2007, Pages 40-42.

[5] Swimmer, M. "towards an Ontology of Malware Classes".[Online]http://www.scribd.com/doc/24058261/Towards-an-Ontology-of-Malware-Classes.

[6] John D. Howard & Thomas A. Longstaff, "A Common Language for Computer Security Incidents", SANDIA Report, SAND 98-8667, 1998.

Sirwan Geramiparvar is received his B. Sc. degree in Software Engineering from Shahid Beheshti University of Tehran in 2005. Currently, he is an IT manager in the QMB bank of IRAN. His areas of research include Information security management system (ISMS- ISO 27000 series), E-banking Security, financial malwares, cyber-security, business continuity management system (BCMS-ISO 22301), fuzzy systems, ITIL. He conducted several researches in his area of interest. He is a member of RABQSA and ISMS Implementer/auditor. He has some of publications in various journals and conferences.
Email: Sirwan_gp@yahoo.com

Nasser Modiri is received his PhD. degree in computer networks from Sussex University in 1991. Currently, he is CEO in Ayandegan Company from 1991 and assistant professor in IAU University, Zanjan branch. His areas of research include software testing, security, developing, maintenance … Information security management system (ISMS- ISO 27000 series), cyber-security, business continuity management systems. He has a lot of publications in software affairs and security issues in reputable magazines and journals.