NRI Dream up the future.

lakyara

2011

Kyara, which means "precious" in ancient Japanese,
is an aromatic resin regarded as the highest quality of all agarwood.
"lakyara [la-kǽla]" aims to deliver the same quality as Kyara together with
NRI's endeavour for continuous excellence and innovation to provide
the most advanced and up-to-date information to our readers worldwide.

vol.128 (12.December.2011)

Online banking security

Nomura Research Institute, Ltd.

Losses from increasingly frequent hacking of online bank accounts have reportedly grown to an all-time high. It is time to rethink currently feasible security measures based on a detailed understanding of how the malware used to commit these crimes functions.

Spate of losses from online banking fraud

Fraudulent funds transfers via online banking platforms have increased in frequency since spring 2011. Such fraud is perpetrated by criminals using legitimate authentication information stealthily obtained with computer malware. Using this information, they transfer funds from victims' accounts through online banking systems' normal processes. According to some reports, over 100 such fraudulent transfers involving 53 financial institutions have occurred in Japan since April 2011, resulting in total losses in excess of ¥270 million, an all-time record. In response, financial institutions issued warnings to retail customers, but it is questionable whether they did so based on an accurate understanding of the malware used to commit these crimes. In the spirit of the proverb "If you know your enemy and know yourself, you can prevail in 100 battles," I present an introduction to the technologies used by the "enemy" and then propose countermeasures.

Highly sophisticated crimeware

The malware usually blamed for information security breaches is called Zeus/SpyEye, software programs dedicated to information theft. Designed to fraudulently obtain personal information for criminal purposes, such programs are also called crimeware. While Zeus/SpyEye themselves possess functions capable of capturing information used by all Web applications, they are referred to as "banking malware" for two reasons. First, their initialization files contain pre-configured settings that target well-known financial institutions' online banking systems. Secondly, they are mainly used to capture financial information.

Additionally, versions of Zeus/SpyEye are being developed for smartphones in addition to PCs. Several mobile applications have been discovered that gather information and transmit it to external servers.

Contrary to the general perception that malware has a fixed function, Zeus/SpyEye's operational code and settings files are separated from each other. Additionally, Zeus/SpyEye can be operated by remote control at any time. They are consequently extremely versatile in comparison to conventional malware that targets specific systems. By virtue of such, they are conveniently adaptable to hackers' individual objectives.

Zeus/SpyEye are the only malware whose final version is dependent on how the hacker configures the settings. This configuration requires only a few mouse clicks to complete. Finished versions differ from each other in terms of how they operate and the servers with which they communicate, making their distinctive features difficult to identify. Zeus/SpyEye also utilize sophisticated concealment technologies to evade detection by subscription antivirus products and hide themselves in victims' information terminals, where they capture targeted information.

Captured information, most notably including information regarding targeted online systems, is transmitted in encrypted format to the hacker. Hackers endeavor to cover their criminal tracks through such means as temporarily using disposable servers located around the world.

Functions of crimeware

The key information-gathering functions of current mainstream versions of malware are as follows.

A. Capture of information transmitted between browsers and targeted systems

The malware captures all information pertaining to targeted online systems that is input by users into their browsers. It also captures all information used by the system to identify the user. Additionally, some malware is programmed to prompt users to input more information (e.g., PINs, security codes) by displaying fake input screens.

Malware can also capture digital certificates and other files used to authenticate the user's terminal, potentially rendering terminal authentication ineffective.

B. Surreptitious screenshots

Hackers can view users' terminal screens at any time. Accordingly, when the user is accessing an online system that uses one-time passwords[1] displayed on the terminal screen by a software token[2], a hacker could input the valid password before the user does. If the system utilizes random number tables for authentication, the hacker could capture the random number table itself by utilizing the information-capture function described above in combination with multiple surreptitious screenshots.

C. Remote control of the user's terminal itself

Zeus/SpyEye provide remote desktop connectivity. Hackers can access targeted online systems via infected terminals. By doing so, they outsmart authentication schemes that use terminal-specific fixed identifiers or digital certificates.

Online banking security measures

As described above, Zeus/SpyEye pose a threat to authentication schemes that utilize user information or terminal-specific information. Given that users' environment cannot be completely protected in a clean state, online banking security needs a rethink based on the assumption that all information that the system requires users to input will eventually be compromised.

Zeus/SpyEye only capture information; they are not capable of directly intervening in the communication session between the user and online system. Unauthorized access does not occur until the hacker manually inputs the stolen information into the system. There is a sizable time lag between the theft of the information and the stolen information's use. Online systems should be configured so that each major process (e.g., information display, fund deposits/withdrawals, purchases) requires authentication by such means as one-time passwords issued by a hardware token[3]. Authentication data stolen by hackers would then no longer be valid by the time the hacker inputs the stolen data.

Systems would be even more secure if this approach could be applied to post-login user identification processes also. If, instead of identifying users by means of data that remain constant for every login, systems were to use data that change more frequently (e.g., at every screen transition) to identify users, such data, if stolen, would be invalid by the time the hacker attempts to use them.

Lastly, implementing such security measures will presumably entail formidable obstacles in terms of cost, system operation, or other such factors. However, having a detailed understanding of the "enemy" will hopefully help rectify misinformation and eliminate confusion about ineffective security measures. Banks should flexibly rethink online security from the standpoint of how their systems are used. For example, they might initially require only large depositors to use hardware tokens. Through such an approach, they could better ascertain what security measures are currently feasible.

Note

1) Disposable passwords that are usable only once.

2) PC, smartphone, or mobile phone software applications that generate one-time passwords. The discussion herein mainly pertains to PC applications that generate one-time passwords.

3) A hardware device that generates one-time passwords. Hardware tokens currently in use are mainly card and keyfob models.

Author's Profile

Takenori Kiuchi

Security Consultant
Technical Consulting Services Department

E-mail : kyara@nri.co.jp

Inquiries to : Financial Technology and Market Research Department
Nomura Research Institute, Ltd.
Marunouchi Kitaguchi Bldg.
1-6-5 Marunouchi, Chiyoda-ku, Tokyo 100-0005, Japan
E-mail : kyara@nri.co.jp

http://www.nri.co.jp/english/opinion/lakyara