Smart Card Alliance Discussion of Sykipot Trojan Attack

January 24, 2012

On January 12, 2012, Alienvault Labs reported that they discovered a new variant of the Sykipot Trojan that would allow it to attack computers that use the Windows® operating system and PIN-protected smart cards that are used for multi-factor authentication to secure networks and information systems. This document was developed by the Smart Card Alliance to provide additional relevant information about this attack as it relates to the smart card present in the infected computer.

According to Alienvault, the attack was implemented as follows:

- The attacker uses a spear-fishing attack to targeted users to get them to open an Adobe PDF attachment. The attachment takes advantage of an Adobe software vulnerability to load the Sykipot malware onto the user's computer.
- When the user logs in with his smart card, the Sykipot malware uses a keylogger to steal the PIN for the smart card and reads the certificates from the Windows local certificate store on the user's computer.
- When the user has the smart card inserted in the reader, Sykipot can use the stolen PIN and certificates and can act as the user to access protected information. The user is unaware that the compromise is occurring. The card must be present for the malware to access protected resources.

The Sykipot Trojan is like any malware that exploits computer software. Once it is covertly installed, it sits on a user's computer and collects information from the user's PC activity. This particular variant of malware captures the PIN-entry keystrokes that are responding to any application that prompts for a PIN (e.g., operating system logon, web browsers, middleware user interface), reads the user's certificates from the Windows key store, and then uses these credentials to login to protected resources.

This attack relies on the malware obtaining privileges from the compromised operating system to be recognized as a trusted application by the authentication system. The malware sits between the protected resource and the smart card and directs authentication requests to the authentication system, using the legitimate smart card to respond to these requests. The card must be present for the malware to access protected resources.

The attack can be prevented by cleaning the operating system, protecting the operating system against the malware, and updating or patching the software application that introduced the malware to the system. While integrity of the smart card was not compromised, credentials stored on the smart card may have been used for unauthorized transactions. The smart card PIN should be reset and, as a best practice, new public key certificates should be issued to the user, with the compromised certificates added to the revocation list and validation services.

Organizations need a comprehensive, layered security strategy to protect networks and information systems from increasingly sophisticated hackers. Key elements of security include:

- Educating users on safe computing practices and on potential phishing attacks.

- Maintaining up-to-date anti-malware, anti-virus and anti-keylogger software on all systems, as well as implementing other tools to analyze user activity and conduct network forensics.
- Ensuring that the software on the user computer is configured for the strongest security (e.g., Windows policy settings for enhanced security, AppLocker, browser security).
- Implementing strong multi-factor authentication (i.e., something you have, something you know, something you are) to validate users' identities.
- Protecting sensitive resources with encryption and strong access control policies and methods.

Examples of specific countermeasures for this type of attack include:

- Implementing an external reader with PIN pad for smart card secure PIN entry. The PIN pad would communicate directly with the smart card without going through the computer and would not be vulnerable to keyloggers.
- Hardening the authentication system to establish a secure path between the user, keyboard and the card to protect the PIN from end-to-end and remove the opportunity for malware to capture the PIN.

Multi-factor authentication using smart cards provides the strongest security against unauthorized access to networks and information systems. For example, DoD has cited dramatic results from their implementation of the Common Access Card (CAC) – network intrusions falling 46 percent when the CAC was used to replace passwords. The recent Sykibot attack reaffirms the need for organizations to implement and continually monitor and upgrade security measures and to maintain an active education program for users.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.