

Dear valued customer,

On Friday, January 13th Dan Raywood from the [SC Magazine blog](#) reported that the security lab Alienvault [detected a new version of Sykipot](#), a computer trojan originally identified 2 years ago by the company [Symantec](#), the anti-virus software vendor. The aforementioned computer virus is understood to run a so-called "spear phishing" attack against smart card keyboard based PIN entry.

The attack occurs when a smart card is inserted into a reader, at which time the malware acts as an authenticated user which can be controlled by the attackers thereby enabling attacker's access to both card based information and on-card functionality such as creation of a digital signature. This attack targets one of the corner stones of the trust level assumed when one uses a smart card and stored PKI credential, as the use of the PKI credential cannot be assured to be under the control of the smart card user.

Whilst not targeted by the current version of the malware, charismathics software could theoretically be targeted by this kind of computer virus. charismathics have reviewed the attack method and we have concluded:

- A key logger recording the entry of a credential such a username, password or PIN is a general threat to computer systems, and is not related to the smart card technology in question.
- The attack against the US government agencies was directed specifically against ActivIdentity's ActivClient.
- As such, in the current version, the Sykipot trojan is not able to affect the charismathics CSSI product range.

Operating system or network based key loggers have long been established as exposures to securing smart card based environments.

Mitigators to this style of attack include:

- The use of Secure PIN Entry smart card readers which "contain" the PIN within the smart card reader/PIN PAD/display device much as EFTPOS card readers do in the retail environment. Such a deployment is fully supported by charismathics middleware, albeit cost and ease of use considerations have typically to date limited its adoption to the highest assurance applications.
- Trusted Computer Platforms (TPM) also offer protection against malware but unfortunately they have not been implemented to the extent that smart card APIs like ActivClient or charismathics CSSI are able to detect unauthorized access to their command interface.

- Active utilization use of up-to-date anti-virus software in conjunction with monitoring of keyboard connections will also reduce the likelihood of undetected intrusion - this Trojan needs to be treated like any other virus.

Accordingly, charismathics underlines the importance of the Secure PIN Entry mode of the CSSI software client and the use of current anti-virus products in conjunction with the application of contemporary risk management practices. Using this approach, the risk of the described attack scenario is reduced significantly.

charismathics will continue to monitor this form of threat against smart card middleware. If you believe that you require help on your risk mitigation measures please contact the charismathics offices or your local charismathics and our partners will be happy to assist you in optimizing the integration of your ID scheme according to your needs.

We appreciate your business and the confidence in our products.

Sven Gossel
CEO, charismathics inc.

Press contacts:



charismathics Inc.
Daniela Previtali
Director Product Marketing
Tel.: +39 348 3836293
Fax: +49 89 30906729
daniela.previtali@charismathics.com
www.charismathics.com



charismathics has been pioneering the global identity management arena since 2003.

With iEnigma®, the company re-invented the smart card and decade-old visions of designing screens and keyboards onto smart cards finally become reality. Only one set of credentials serves all needs for a digital identity, whether in the office or on the road. The user is in full control of his credentials, not only visually, but is able to manage his digital identities himself and directly on the phone.

The charismathics Smart Security Interface CSSI® is a comprehensive and agnostic PKI client framework. Extremely versatile, it supports all computer platforms, myriads of smart card operating systems and token profiles, various technologies (including Trusted Platform Modules, RFID tokens, GSM SIM modules) and third party applications. Unparalleled flexibility translates into tremendous independence for enterprises from hardware lifecycles and proprietary software schemes, empowering them to combine different vendors of token management systems and hardware simultaneously, thus dramatically reducing their financial investment in PKI infrastructures.

charismathics is offering security products and services for a variety of industries ranging from corporate to finance, from e-government to health services, from e-education to telecommunications.

For graphics media resources, please visit: www.charismathics.com/media

© All trademarks, trade names, service marks, and logos referenced herein belong to their respective organizations and companies.

charismathics