



**Demand More**  
More applications. More flexibility. More security.

ACTIVIDENTITY  
part of HID Global

LEARN MORE

SEARCH

Home News SC Conference Blog SC Awards 2012 Products SC TV Jobs Issue Archive Subscribe Whitepapers

Text "follow scmagazineuk" to 86444 @scmagazineuk @sceditor @danraywood LinkedIn

RSS | Login | Register

SC Magazine UK > News > Chinese attacks target US government agencies and smartcards

## Chinese attacks target US government agencies and smartcards

Dan Raywood January 13, 2012

PRINT EMAIL REPRINT TEXT: A|A|A

Tweet 7

Like

Evidence has been revealed that attacks are being made against US government agencies, using a new strain of the Sykipot malware to compromise smartcards.

According to Security Information and Event Management (SIEM) vendor AlienVault, the attacks originate from China and target agencies including the US Department of Defense.

Jaime Blasco, lab manager at AlienVault, said this is the first report of Sykipot being used to compromise smartcards, with this latest version designed specifically to take advantage of smartcard readers running ActivClient – the client application of ActivIdentity, whose smart cards are standardised at the Department of Defense and a number of other US government agencies.

Blasco said one of the original versions of Sykipot was a Trojan horse application that opened a backdoor into the infected PCs. Symantec detected Sykipot just under two years ago and deems it to be very low risk with low distribution, but with 'medium' damage-capability levels.

Blasco believed that this new strain originated from the same Chinese authors that created a version of Sykipot late last year that delivered a variety of spammed messages with the lure of information on the next-generation unmanned 'drones' developed by the United States Air Force.

He said that he and his team have seen attacks that compromise smartcard readers running Windows Native x509 software, while attackers are now using a version of Sykipot that dates back to March 2010 and has been used in dozens of other attacks executed in the past year.

Spearphishing tactics are used to distribute the malware and, once installed, it uses a keylogger to steal PINs for the cards.

"When a card is inserted into the reader, the malware acts as the authenticated user and can access sensitive information. The malware is then controlled by the attackers and then told what and when to steal the appropriate data," he said.

"It's worth noting that back in January 2011, just ahead of this new strain of Sykipot being released, our colleagues at another security vendor called this type of a attack 'smartcard proxies' in one of their reports. Although the report did not provide specifics on the attack methodologies being used, the term is useful in describing this latest style of attack vector."

Last November, the US National Counterintelligence Executive directly named the government of China as one of the most aggressive collectors of US economic information and technology (alongside Russia), saying that US corporations and cyber-security specialists had reported an onslaught of advanced persistent threats originating from IP addresses in China.

Also, in December, US cyber-security analysts and experts reported that 12 groups were behind the bulk of China-based cyber attacks stealing critical data from US companies and government agencies.



### RELATED ARTICLES

- Mitsubishi Heavy Industries attack puts Japan's defence contractors on alert
- McAfee's Shady RAT investigation reveals mass attacks over five year period
- Spear phishing experiment on LinkedIn leads to two-thirds of recipients clicking through to an external domain
- Spear phishing preferred by cyber criminals to traditional spam campaigns

### MORE NEWS

- Businesses prepared for consumerisation when it comes to email
- Sourcefire moves into malware analytics
- Anonymous plans fresh offensive against Sony
- Megaupload takedown spurs retaliation from Anonymous
- Ransomware attacks on the rise

GL Garrad Hassan



Click here to find out why you should attend

PEOPLE RECENT POPULAR

### Recent Comments



**Credible Witness** This website ought to rebrand to 'Anonymous News Service'. It's getting a little old.  
**Anonymous plans fresh offensive against Sony - SC Magazine UK · 6 hours ago**



**Dante** The Article was quite good.  
**Sourcefire moves into malware analytics - SC Magazine UK · 17 hours ago**



**Annie white** The concept detection engine instead of antivirus is quite interesting.  
**Sourcefire moves into malware analytics - SC Magazine UK · 18 hours ago**



**hareesa** need to recover the sim card +9607913090  
**Symantec reveals hacking and theft of source code - SC Magazine UK · 20 hours ago**



**munawaxr** need to recover the sim card +9607913090  
**Proliferation of mobile devices boosts number of security events - SC Magazine UK · 23 hours ago**

community on DISQUS



celestix

Find out more

authenticate / mobilise / enable

White Papers