



HALL ASSOCIATES



Risk-Based Decision Making Commentary

6 March 2014 Newsletter

Thieves Jam Up Smucker's Web Site

Jam and jelly maker Smucker's last week shuttered its online store, notifying visitors that the site was being retooled because of a security breach that jeopardized customers' credit card data. Closer examination of the attack suggests that the company was but one of several dozen firms — including at least one credit card processor — hacked last year by the same criminal gang that infiltrated some of the world's biggest data brokers.

As Smucker's referenced in its FAQ about the breach, the malware that hit this company's site behaves much like a banking Trojan does on PCs, except it's designed to steal data from Web server applications.

PC Trojans like ZeuS, for example, siphon information using two major techniques: snarfing passwords stored in the browser, and conducting "form grabbing" — capturing any data entered into a form field in the browser before it can be encrypted in the Web session and sent to whatever site the victim is visiting.



A Message to Our Online Store Consumers

We greatly value the trust our consumers place in our Company and take very seriously our responsibility to protect sensitive and confidential information that consumers share with us.


We deeply regret that an incident resulting in the illegal and unauthorized access to data files within our Online Store occurred. Unfortunately, we believe the unauthorized user may have obtained access to the personal information of some of our consumers, including name, address, email address, phone, credit or debit card number, expiration date, and verification code. The unauthorized user utilized a sophisticated scheme to illegally obtain this personal information as it was being entered during the online checkout process.

We are extremely disappointed this incident occurred and sincerely apologize for any inconvenience this may cause. Please be assured, we continue to thoroughly investigate this matter with federal authorities, and have taken steps to rectify the cause of this incident with the Online Store website.

Again, we sincerely regret any concern this may cause and we assure you that we will diligently work to maintain the trust that our consumers place in our Company.

For more information, please review the provided FAQ responses or contact us Monday through Friday, 9 a.m. - 7 p.m. ET at 1-800-742-6729.

Sincerely,
The J. M. Smucker Company



The malware that tore into the Smucker's site behaved similarly, ripping out form data submitted by visitors — including names, addresses, phone numbers, credit card numbers and card verification code — **as customers were submitting the data during the online checkout process.**

What's interesting about this attack is that it drives home one important point about malware's role in subverting secure connections: Whether resident on a Web server or on an end-user computer, if either endpoint is compromised, it's 'game over' for the security of that Web session. With Zeus, it's all about surveillance on the client side pre-encryption, whereas what the bad guys are doing with these Web site attacks involves sucking down customer data post- or pre-encryption (depending on whether the data was incoming or outgoing). <http://krebsonsecurity.com/2014/03/thieves-jam-up-smuckers-card-processor/>



HALL ASSOCIATES



Chameleon Virus that Spreads Across WiFi Access Points like Common Cold

A Computer viruses could go Airborne over WiFi networks has been developed. Security researchers at the University of Liverpool in Britain have demonstrated a WiFi virus that can spread between computer networks just like the 'common cold' spreads between Humans. They have created a proof-of-concept which can infect the entire wireless network instead of a single computer at a time, that replaces the firmware of the vulnerable Access Point (AP) with a virus-loaded version, and then propagates itself to the next victim on the WiFi network.

The WiFi based virus named as 'Chameleon', and can self-propagate over WiFi networks from access point to access point, but doesn't affect the working of the Wireless Access Point. This Virus is able to identify WiFi access points that are not protected by encryption and passwords, according to the research paper. **It can badly hit less-protected open access WiFi networks available in coffee shops or airports.**

It propagates in the following sequence:

It establishes a list of susceptible APs within the range

Bypasses any encryption Security on the targeted AP

Bypasses the administrative interface on the targeted AP

Identify and Store AP System Settings

Replaces the AP firmware on with the virus-loaded firmware.

Import the victim original AP System Settings on newly loaded firmware

Let's Propagate! Back to Step one to next Target.

The experimental demonstration was performed in two cities, Belfast, NI and London, England. A random access point was infected with the virus which acted as a seed. The results were published in a research paper. **This type of attack is a serious threat for WiFi network security.** The research shows that this kind of attack **is undetectable** to any Antivirus and Wireless Intrusion Detection System (IDS). The Density of Access points (number of points) in a certain geographical area increases the security issues for wireless networks, because it spreads very quickly at high speed in an area having denser Access Point availability. "WiFi connections are increasingly a target for computer hackers because of well-documented security vulnerabilities, which make it difficult to detect and defend against a virus," says Marshall, Co-author of the research paper. However, the virus itself doesn't currently exist in the wild and was created for the demo purpose in the research lab only, though it is very likely that a malicious version could be created and released into the wild by cyber criminals and malware writers now that they know it is possible.

http://thehackernews.com/2014/02/chameleon-virus-that-spreads-across.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News++Security+Blog%29&_m=3n.009a.503.wb0ao05fi9.aod