

4 December 2008

By: Lucian Constantin, Web News Editor

[Online Bill Payment Website Hijacked](#)

Users were redirected to a page serving malware



CheckFree
compromised domain
names put customers
at risk
CheckFree
Corporation

Two domain names belonging to the e-bill payment service CheckFree have been hijacked by an Eastern European cybercriminal gang. The DNS records for the domains have been altered to point to a malware distribution server.

CheckFree is one of the largest services that provide individuals with the ability to pay utility, insurance, mortgage and other bills online. The company founded in 1981 currently serves tens of millions of customers. The security breach involving their [checkfree.com](#) and [mycheckfree.com](#) domains occurred sometime on early Tuesday morning, and was fixed after a few hours.

All users that attempted to access the two websites during the few hours got redirected to a blank webpage hosted on a server in Ukraine, that attempted to install malware. According to a security analyst from Trend Micro, the application is a new Trojan designed to steal authentication credentials. The researcher told [The Register](#) that the same IP had also been previously used to push [malicious PDF files](#). The anti-spam organization Spamhaus also [lists](#) the same IP as hosting other domain names that were most likely hijacked in a similar fashion.

According to The Register, CheckFree spokeswoman Melanie M. Tolley noted that "it is taking time to determine exactly what type of malware we might be dealing with, but we are currently working on a program update that provides information to the customers about the incident and maintenance tips recommending that all of our users run scans with Symantec's scan utility, and install the latest patches for Adobe Reader, as well as make a regular practice of keeping their computer updated with the latest anti-virus software."

Details about how the domains have been hijacked are still scarce, but it has been speculated that the cybercriminals obtained access to the Network Solutions account used to manage the company's domain names. This is very likely, considering the recent account [phishing campaign](#) targeting the customers of two of the largest domain registrars, Network Solutions and eNom. The campaign is believed to be the cybercriminals' response to ICANN's [de-accreditation](#) of EstDomains, their favorite domain registrar.

The exact number of users that were affected by this incident is not known, but the company estimates that it is not a big one, considering that the problem was fixed by 8 am on Tuesday morning, Pacific Time. "The degree of exposure to users is dependent on how current their anti-virus software is and what browser they used to connect with," Tolley said, according to [Security Fix](#).