Six More US Retailers Attacked Like Target, Security Firm Says

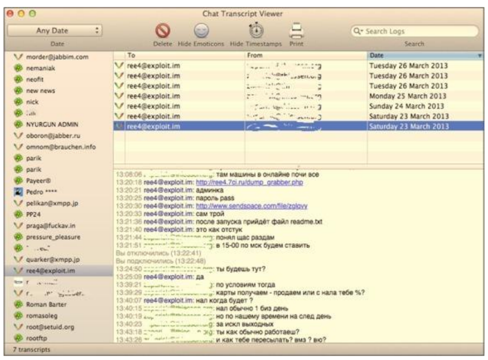
Jeremy Kirk
Jan 18, 2014 3:52 AM

Note from Pastor Kevin Lea follows this article.

Cybercriminals have stolen payment card data from six more U.S. retailers using similar point-of-sale malware that compromised Target, a computer crime intelligence company said Friday. The conclusion comes from a study of members-only forums where cybercriminals buy and sell data and malicious software tools, said Dan Clements, president of IntelCrawler, which conducted the analysis.

The retailers have not been publicly named, but IntelCrawler is providing technical information related to the breaches to law enforcement, Clements said in a telephone interview Friday.

IntelCrawler has also identified a 17-year-old Russian who it says created the BlackPOS malware, which intercepts unencrypted payment card data after a card is swiped. Security experts believe malware based on BlackPOS was used against Target.



The teenager, who goes by the online nickname “ree4,” sold more than 40 copies of BlackPOS to cybercriminals in Eastern Europe and elsewhere, according to forum postings IntelCrawler analyzed.

The forum posts indicate the teenager sold the malware for $2000 or for a share of the profits that came from monetizing stolen payment card details, Clements said. BlackPOS was also sold to “carding” websites such as .rescator, Track2.name and Privateservices.biz that trade in stolen card details, according to IntelCrawler.

BlackPOS was originally called Kaptoxa, which is Russian slang for potato. Clements said the Russian teenager eventually renamed the malware BlackPOS during a fresh marketing push.

Dallas-based security company iSight Partners wrote in a report earlier this week on the Target hack, which it called the “Kaptoxa operation.” It says the hackers used a high level of skill to gain stealthy access to the retailer’s network.

Since early 2013, IntelCrawler has seen a brisk trade in login credentials for POS terminals on underground forums, suggesting cybercriminals are still finding gaps in industry security recommendations for how payment card data is handled.

Cybercriminals were selling “remote desktop protocol” credentials for POS terminals, which would allow them access to the machines, Clements said. In many cases…

> *To read this article in its entirety, go to:*
> http://www.pcworld.com/article/2089480/six-more-us-retailers-hit-by-targetlike-hacks-security-firm-says.html#tk.nl_secur

Note from Pastor Kevin Lea: A friend of mine who is a computer security expert has further explained to me how this attack occurred and why the entire POS (point of sale) system must be changed (globally) to prevent the spread of this malware.

Currently, the unencrypted information of your card is pulled from the magnetic strip when you swipe it. This information then goes to the computer terminal at the checkout stand, where it is encrypted and sent into the commercial network for payment authorization. The Target Corporation hack attack started when the hackers found a weak security link in the massive computer network of Target (and now other retailers). Then, once inside, they installed the malware virus on every POS terminal for the company.

The malware program works by making a copy of the unencrypted card information while it is on the way to be encrypted in the same computer that the virus resides in, at the POS terminal. The information is collected over time (gathering over 60 million customer's data in the case of Target) and is then sent to the bad guys who planned the attack. Then these guys sell the info to a bunch of other bad guys. Those bad guys can take weeks, months or years before they use the hundreds-of-millions of victim's information to make their lives miserable, in various different ways.

Therefore, this problem is just beginning and cannot be stopped unless the POS process is changed (globally), which will cost very big dollars and take some time. In the mean time, every time you swipe your card there is a very real chance that someone is getting ALL the information that is on the magnetic strip.

Too bad the world has told the true God of the bible to get out of their lives, and demanded that the Bible not be taught to the masses of the world. If the bible were taught, more people might be "corrupted" by things like:

> Ex 20:15+17 "You shall not steal. "You shall not covet your neighbor's house; you shall not covet your neighbor's wife, nor his male servant, nor his female servant, nor his ox, nor his donkey, nor anything that is your neighbor's." NKJV

Jesus came to die on the cross for our sins, so that those who love Him and His laws can be forgiven of our foolishness and spend eternity with Him. I for one hate the fact that theft, violence, covetousness, and other evils have made life so miserable in this fallen world. I long for the day I can be with God forever, living under His laws, because Jesus opened the door to heaven for those who believe and trust in Him as their savior. Please join me, while there is time, if you haven't already.