Carefirst Blue Cross Breach Hits 1.1M

krebsonsecurity.com/2015/05/carefirst-blue-cross-breach-hits-1-1m/

CareFirst BlueCross BlueShield on Wednesday said it had been hit with a data breach that compromised the personal information on approximately 1.1 million customers. There are indications that the same attack methods may have been used in this intrusion as with breaches at **Anthem** and **Premera**, incidents that collectively involved data on more than 90 million Americans.

According to a statement CareFirst issued Wednesday, attackers gained access to names, birth dates, email addresses and insurance identification numbers. The company said the database did not include Social Security or credit card numbers, passwords or medical information. Nevertheless, CareFirst is offering credit monitoring and identity theft protection for two years.

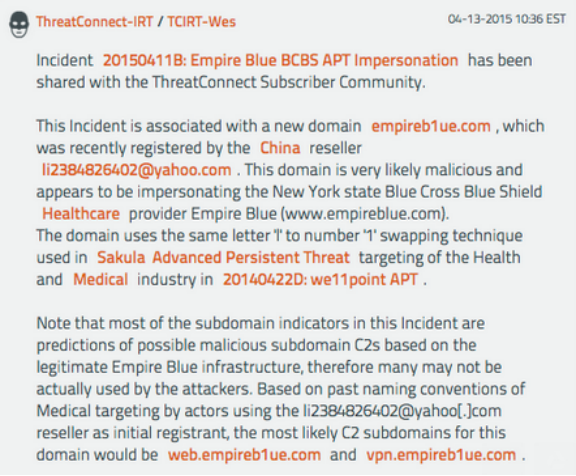
Nobody is officially pointing fingers at the parties thought to be responsible for this latest health industry breach, but there are clues implicating the same state-sponsored actors from China thought to be involved in the Anthem and Premera attacks.

As I noted in this Feb. 9, 2015 story, Anthem was breached not long after a malware campaign was erected that mimicked Anthem's domain names at the time of the breach. Prior to its official name change at the end of 2014, Anthem was known as Wellpoint. Security researchers at cybersecurity firm **ThreatConnect Inc.** had uncovered a series of subdomains for we11point[dot]com (note the "L's" in the domain were replaced by the numeral "1") — including myhr.we11point[dot]com and hrsolutions.we11point[dot]com.

ThreatConnect also found that the domains were registered in April 2014 (approximately the time that the Anthem breach began), and that the domains were used in conjunction with malware designed to mimic a software tool that many organizations commonly use to allow employees remote access to internal networks.

On Feb. 27, 2015, ThreatConnect published more information tying the same threat actors and modus operandi to a domain called "**prennera[dot]com**" (notice the use of the double "n" there to mimic the letter "m").

"It is believed that the prennera[dot]com domain may have been impersonating the Healthcare provider Premera Blue Cross, where the attackers used the same character replacement technique by replacing the 'm' with two 'n' characters within the faux domain,



the same technique that would be seen five months later with the we11point[dot]com command and control infrastructure," ThreatConnect observed in a February 2015 blog post.

Turns out, the same bulk registrant in China that registered the phony Premera and Anthem domains in April 2014 also registered two Carefirst look-alike domains — **carefIrst[dot]com** (the "i" replaced with an "L") and **caref1rst[dot]com** (the "i" replaced with the number "1").

Additionally, ThreatConnect has unearthed evidence showing the same tactics were used on **EmpireB1ue.com** (note the "L" replaced with a number "1"), a domain registered April 11, 2014 (the same day as the phony Carefirst domains). **EmpireBlue BlueCross BlueShield** was one of the organizations impacted by the Anthem breach.