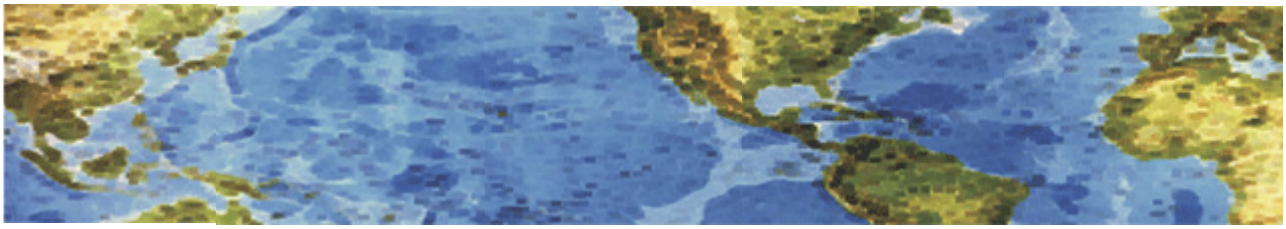
HALL ASSOCIATES



Risk-Based Decision Making Commentary
5 September 2014 Newsletter

Mysterious Fake Cell Phone Towers Are Intercepting Calls All Over The US

Seventeen fake cell phone towers were discovered across the U.S. last week, according to a report in Popular Science. Rather than offering you cell phone service, the towers appear to be connecting to nearby phones, bypassing their encryption, and either tapping calls or reading texts.

Les Goldsmith, the CEO of ESD America, used ESD's CryptoPhone 500 to detect 17 bogus cell phone towers. ESD is a leading American defense and law enforcement technology provider based in Las Vegas. With most phones, these fake communication towers are undetectable. But not for the CryptoPhone 500, a customized Android device that is disguised as a Samsung Galaxy S III but has highly advanced encryption.

Goldsmith told Popular Science: " Interceptor use in the U.S. is much higher than people had anticipated. One of our customers took a road trip from Florida to North Carolina and he found eight different interceptors on that trip. We even found one at South Point Casino in Las Vegas." The towers were found in July, but the report implied that there may have been more out there. Although it is unclear who owns the towers, ESD found that several of them were located near U.S. military bases. "Whose interceptor is it? Who are they, that's listening to calls around military bases? Is it just the U.S. military, or are they foreign governments doing it? The point is: we don't really know whose they are," Goldsmith said to Popular Science.

It's probably not the NSA — that agency can tap all it wants without the need for bogus towers. They can just go to the carrier to tap your line. ComputerWorld points out that the fake towers give themselves away by crushing down the performance of your phone from 4G to 2G while the intercept is taking place. So if you see your phone operating on a slow download signal while you're near a military base ... maybe make that call from somewhere else.

In an amazing coincidence, police departments in a handful of U.S. cities have been operating "Stingray" or "Hailstorm" towers, which - you guessed it - conduct surveillance on mobile phone activity. They do that by jamming mobile phone signals, forcing phones to drop down from 4G and 3G network bands to the older, more insecure 2G band, a much older protocol that is easier to de-crypt in real-time. *For more information, check out the Popular Science article noted below and several Fox News articles.*

http://finance.yahoo.com/news/mysterious-fake-cellphone-towers-intercepting-162645809.html
http://www.popsci.com/article/technology/mysterious-phony-cell-to wers-could-be-intercepting-your-calls

HALL ASSOCIATES

Banks: Credit Card Breach at Home Depot

Multiple banks say they are seeing evidence that **Home Depot** stores may be the source of a massive new batch of stolen credit and debit cards that went on sale this morning in the cybercrime underground. Home Depot says that it is working with banks and law enforcement agencies to investigate reports of suspicious activity.

Contacted by this reporter about information shared from several financial institutions, Home Depot spokesperson **Paula Drake** confirmed that the company is investigating. "I can confirm we are looking into some unusual activity and we are working with our banking partners and law enforcement to investigate," Drake said, reading from a prepared statement. "Protecting our customers' information is something we take extremely seriously, and we are aggressively gathering facts at this point while working to protect customers. If we confirm that a breach has occurred, we will make sure customers are notified immediately. Right now, for security reasons, it would be inappropriate for us to speculate further – but we will provide further information as soon as possible."

There are signs that the perpetrators of this apparent breach may be the same group of Russian and Ukrainian hackers responsible for the data breaches at **Target**, **Sally Beauty** and **P.F. Chang's**, among others. The banks contacted by this reporter all purchased their customers' cards from the same underground store – **rescator[dot]cc** — which on Sept. 2 moved two massive new batches of stolen cards onto the market.

In what can only be interpreted as intended retribution for U.S. and European sanctions against Russia for its aggressive actions in Ukraine, this crime shop has named its newest batch of cards "American Sanctions." Stolen cards issued by European banks that were used in compromised US store locations are being sold under a new batch of cards labeled "European Sanctions."

It is not clear at this time how many stores may have been impacted, but preliminary analysis indicates the breach may extend across all 2,200 Home Depot stores in the United States. Home Depot also operates some 287 stores outside the U.S. including in Canada, Guam, Mexico, and Puerto Rico.

Several banks contacted by this reporter said they believe this breach may extend back to late April or early May 2014. If that is accurate — and if even a majority of Home Depot stores were compromised — this breach could be many times larger than Target, which had 40 million credit and debit cards stolen over a three-week period.

http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/

5 September 2014