Atlanta Private Detective Exposes Tool That Hacks Into Gmail Accounts

Published on 05/05/09

Eagle Investigative Services has discovered that the Open Resource free proxy server Tor, used in part to block traffic analysis from companies like Google, is vastly insecure and can be used by hackers to steal passwords and other information used in phishing attacks. The Atlanta private investigators are thankful they run everything on Apple Macs so the damage was able to be quickly contained.

Atlanta, Georgia - An Atlanta private detective has been running the open-resource proxy server Tor on a Mac for the past week. Tor is an anonymizer - it allows you to surf the net anonymously - up to a point. It uses so-called onion routing - layer upon layer of servers scattered across the world.

Tor can't (and doesn't try to) protect against an attacker who can monitor both traffic going into the Tor network and traffic coming out of the Tor network. (The United States government can monitor any broadband internet traffic under the Communications Assistance For Law Enforcement Act and can see both ends of the Tor connection.)

Tor tries to protect against traffic analysis from companies like Google who are interested in tracking internet users viewing and buying habits by placing cookies on your computer. But is not totally successful at that either. It doesn't have the ability to prevent traffic confirmation.

Eagle Investigative Services Inc. spokesperson Malcolm Lambe said -

"We downloaded Tor onto one of our Intel iMacs. Not to do anything covert - we were mainly interested in seeing how stable and fast it was. And it seemed to work very well. There was no interruption to our daily online work - it was just running in the background.

We use Google Adwords program for our online marketing and were in the middle of monitoring a new campaign.

I couldn't sleep one night and logged into Adwords at 3 a.m. to see how the new campaign was going. I got the shock of my life when I saw someone had hacked into the account, had set up a new campaign with a daily spend of $4000 and had already milked the account of $1000 in bogus clicks.

In consultation with Google (who noticed and shut down the entire account pretty quick) we formed the opinion that the hackers had got into the Adwords account via the linked Gmail account password. Most probably through Tor."

This was confirmed after the Atlanta private detective did some online research and discovered that there was indeed a security hole. A hole that had been recently demonstrated at a Black Hat Conference in Washington in February this year.

A hacker ran a tool called "SSLstrip" on a server hosting a Tor anonymous browsing network. During a 24-hour period, he harvested 254 passwords from users visiting sites including Yahoo, Gmail, Ticketmaster, PayPal, and LinkedIn. The users were fooled even though SSLstrip wasn't using the proxy feature that tricks them into believing they were at a secure site. Tor users entered passwords even though the addresses in their address bars didn't display the crucial "https".

Malcolm Lambe said -

"Many people search for anonymous proxies on the internet to use. They then just surf via these proxies - seems most are either hacked or accidently acting as proxies - hackers do it deliberately and log everything that goes through these servers - they pick up thousands of passwords, account names etc by everyone using them and launch phishing attacks".

The Atlanta private investigators are thankful they run everything on Apple Macs so the damage was able to be quickly contained. Tor was removed to the Trash. The Admin account password and all site passwords were changed. Then a full system maintenance program was run with Onyx - a Universal Binary application that works with all Macintosh PowerPC and Intel computers running Mac OS X version 10.5 or later (Leopard). No further problems have been noticed and (for now) all email and site accounts seem to be secure.

Eagle Investigative Services:
http://www.atlantaprivatedetective.com

Eagle Investigative Services, Inc. based in Atlanta, Georgia, is owned and operated by James E. Carsten, who has served as Chief Protection Detail to the Secretary Of Defense, and has spent many years as an Army CID (criminal investigations) investigator, working on cases ranging from murder and South American drug trafficking to embezzlement.

###

Malcolm Lambe

33963268667

malcolmlambe@gmail.com

****
Link To Article: https://prmac.com/release-id-5511.htm
****