Eduardo Mirahyes
2342 Shattuck #144
Berkeley, CA 94704
mirahyes@hushmail.com

November 26, 2013

Brad Arkin
Chief Security Officer
Adobe
P.O. Box 483
Chanhassen, MN 55317

Re: ***Security incident between Sept 11 & 17***

I am well acquainted with the hacker who broke into your security system. He has been on my back, and I, his whipping boy for going on seven years. I am on your list because I subscribed to the service which converts pdf documents back into Word for editing.

Until recently, only safe way to conserve documents was in pdf, but since you had the security breach, this hacker has been able to corrupt documents*, already in pdf format.* Although the suffix remains pdf, rather than showing the Adobe logo, they become corrupted to show *"scratch paper"* so that they go out containing virus, which gets installed into the computers on which it is opened.

I provide an on-line Elliott-Wave Market-Timing service, ***Exceptional Bear***. I am by far the best, including the top performance of any professional in 2008, exceeding 360%, immediately this rogue hacker began chipping away, so that in a matter of six weeks half the performance was gone, from the computers of 3rd party verification service. As you might well understand without 3rd party verification, there's no credibility in this business. When I explained past performance could be cut in half, Timertrac dropped me. In the meantime, I attempted to establish a record on Collective2, here too he broke into the system and reversed my positions from long to short and vice-versa, resulting in verified, corrupted losses rather than my own. At Collective2 he also ***feigned identity theft,*** you must understand that identity theft is a *low value* undertaking for a top level hacker who makes off with millions at a time. He is far beyond petty identity theft, in fact

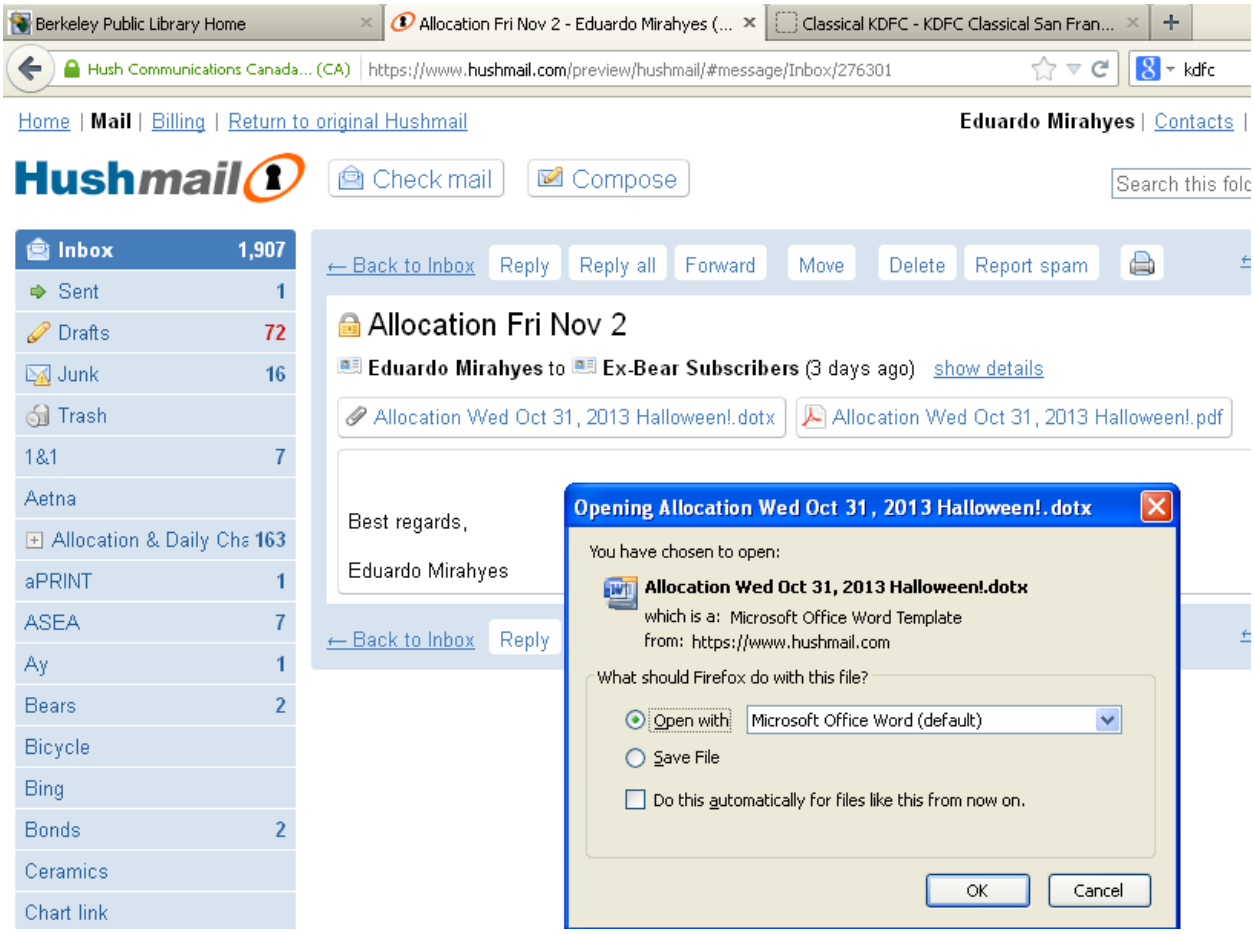
he is tops at phishing for passwords, and then wires out the entire corporate funds to Russia (he utilizes a Russian proxy server, so he is known as the Russian hacker, *according to Pat Peterson*, head of Cisco Security, meanwhile he lives right here in Sunnyvale, CA. His *botnet* allows him to learn of undeclared funds, where the victim cannot report the crime, ***without incriminating himself for tax evasion.***

Last year I had a security breach, which your tech support was highly inept at handling; this hacker inserted code into my *pdf account interface*, so that it would alert his server when I log on. In this way, he located me in a previously cached location, where I had made sure there were no other possible leaks or security breaches, including use of flash drives, or the on-line Stockcharts.com, which was similarly, *tagged* long ago. Nevertheless need to access these daily. In all has destroyed 57 computers, including 12 Macs. Even when I attempted to use off-line only, he inserted a software modem, which *would revert my completed documents to the original draft* on the day they were to be published on the web.

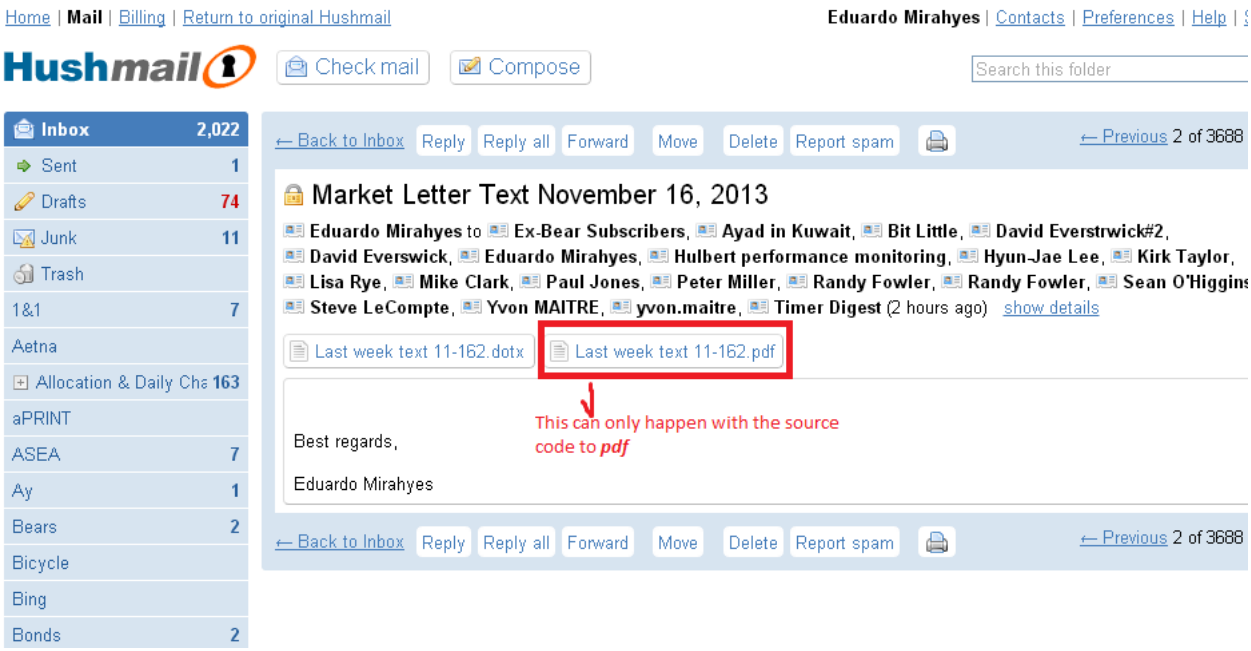
So that you are aware of his capabilities, he has hacked into the *Microsoft Updates server*. In this way, he can get past any security system, under the guise of Microsoft updates. Any computer registered under my name, gets taken over by a shell program, and within weeks, often long enough so that it cannot be returned, he sends the command ***"Kills Windows",*** complete with the Microsoft digital signature. Even off-line he inducts new wireless computers to his ***botnet*** via the cell phone technology – he has at least one and likely several cellphone companies under his control. In Macs these show ups as *three Apache logos*, which at least until last year, could be easily identified by the *sequential programming on Apple's operating system*. Most users are not even aware. For example, when I went to use my sister's computer, as a back-up, he was already in the background, and added a Million KB as filler, so my report to clients became too large to go out wirelessly.

When I attempted to use ***Ubuntu,*** he similarly *broke into their servers* and inserted code became downloaded for months, at least in the SF Bay Area. Like your report, it was disclosed as a ***breach in security***. However the *identity theft threat is just a smoke screen* to throw you off. He did the identical thing with Collective 2.

Below is how a *file should look*, as an editable ***document template*** and ***pdf***

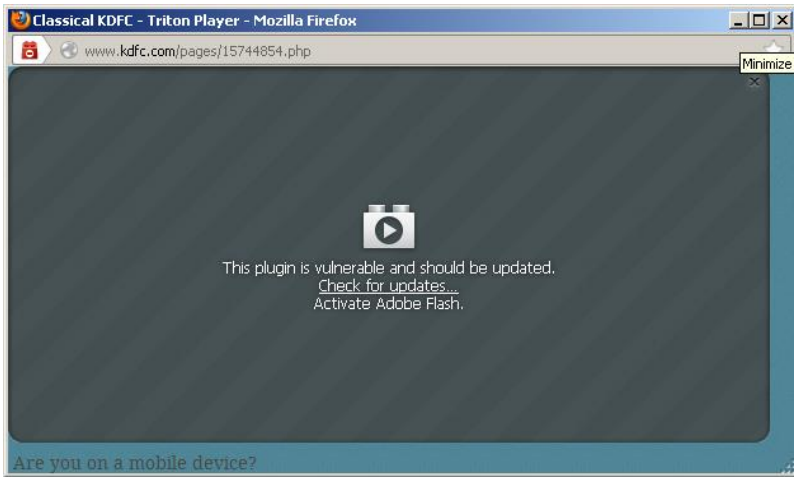


Instead what I get is below…these are *hacked,* which causes all the computers which open this file to malfunction.

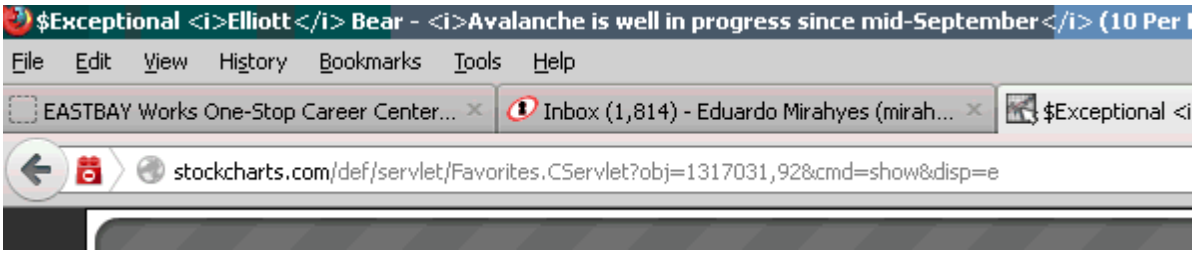


Note above the ***pdf logo is missing***; in its place a piece of paper with the corner chewed off!

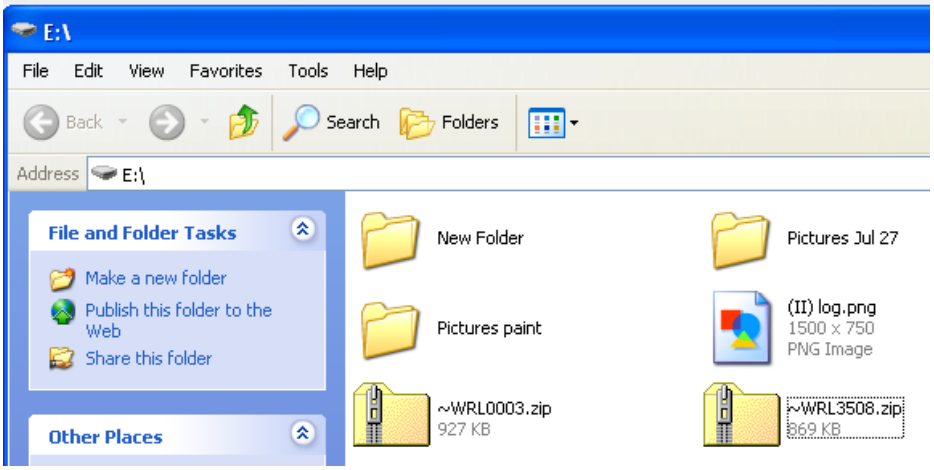
Below, the red leggo peg *overrides security* and demands an update, in the meantime it blocks all music. This is ***false*** vulnerability, *intended to be substituted with his pre-hacked update,* ***this is why he needed the code***



Below the same red peg overrides security on Flash in Stockcharts



Below are the ***two virus files*** ***used to corrupt the pdf*** I have them compressed and saved them, I would like to send them to you, but only for action no half-way measures…*instead of the FCC, you need to contact the* ***FBI*****,** they are the only ones with the technology to track this monster…and I can lead you to him. *He is only afraid of the FBI* and he knows better than either one of us in this matter!



This is a serious matter which compromises the security of many ***Adobe-***flash based applications.

Please email me with a telephone number which I can call from a payphone…my cellphone is also filtered and hacked.

Sincerely,

Eduardo Mirahyes