Web 2.Oh No!

Peter Silva, 2009-09-01

Although this breach happened about a month ago, there is still plenty of fallout and follow up that's occurring. Briefly, an entity in the Ukraine was able to gain access to Checkfree's DNS settings (hosted with Network Solutions), change the DNS record and then re-directed traffic destined for the valid www.checkfree.com site to their own back-alley server. For 10 hours on Dec 2, visitors attempting to pay their bills were actually being attacked. The malicious server hosting the fake Checkfree site then attempted to install keystroke logging software to capture password credentials. The initial report indicated that only a small number of folks might have been infected since, they claim, certain conditions (such as out of date anti-virus definitions) had to be in place for the breach to be successful. The mycheckfree.com site used to have those 4 parameters but have since removed them. Now comes word that they are alerting a heck of a lot more than just a few folks – 5 million more.

You might be thinking, 'I don't use Checkfree so I have nothing to worry about.' Well, you might. I had the same initial feeling but realized that **MY** bank uses Checkfree for bill pay. I logon and one of the tabs is, obviously, 'Bill Pay.' When I click on that, it takes me to a bank branded Checkfree application where I do my thing.

Concerned, I called my bank (this was mid-last month) and the first rep was aware of the situation but didn't have any additional info (since the bank didn't 'train' everyone on how to respond to this).....yet, another rep was lucky enough to be in the know. He said that as far as they knew, we (me/my bank) were fine. I'm not completely buying it. Many banks have their own payment systems but institutions large and small, including Bank of America (not my bank), use Checkfree for bill payments.

My colleague Lori MacVittie has written numerous articles on the security perils of Web2.0 so this post really isn't a 'fix it this way,' or 'install that,' or 'DNS damnation....again.' It is more to inform, better yet – alert you that you might want to investigate your own situation since this came out during the busy holiday season and might have been overlooked. Check your Checkfree, whether you go directly or via your bank's payment system – that is, of course, if you do online banking. The one thing it did was make all those people who diligently write checks every month feel a bit more secure. *(Yes, there are other hazards of writing and sending checks but not on this post)* :-)

Similarly, you might have missed the American Express XSS vulnerability reported in mid-December since it didn't get a lot of press. Many of us (and probably you) have Corporate AMEX cards for business expenses. Again, just a nudge to be aware.

Happy New Year and be careful out there.

ps

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113