Deloitte is a sitting duck: Key systems with RDP open, VPN and proxy 'login details leaked'

By Iain Thomson

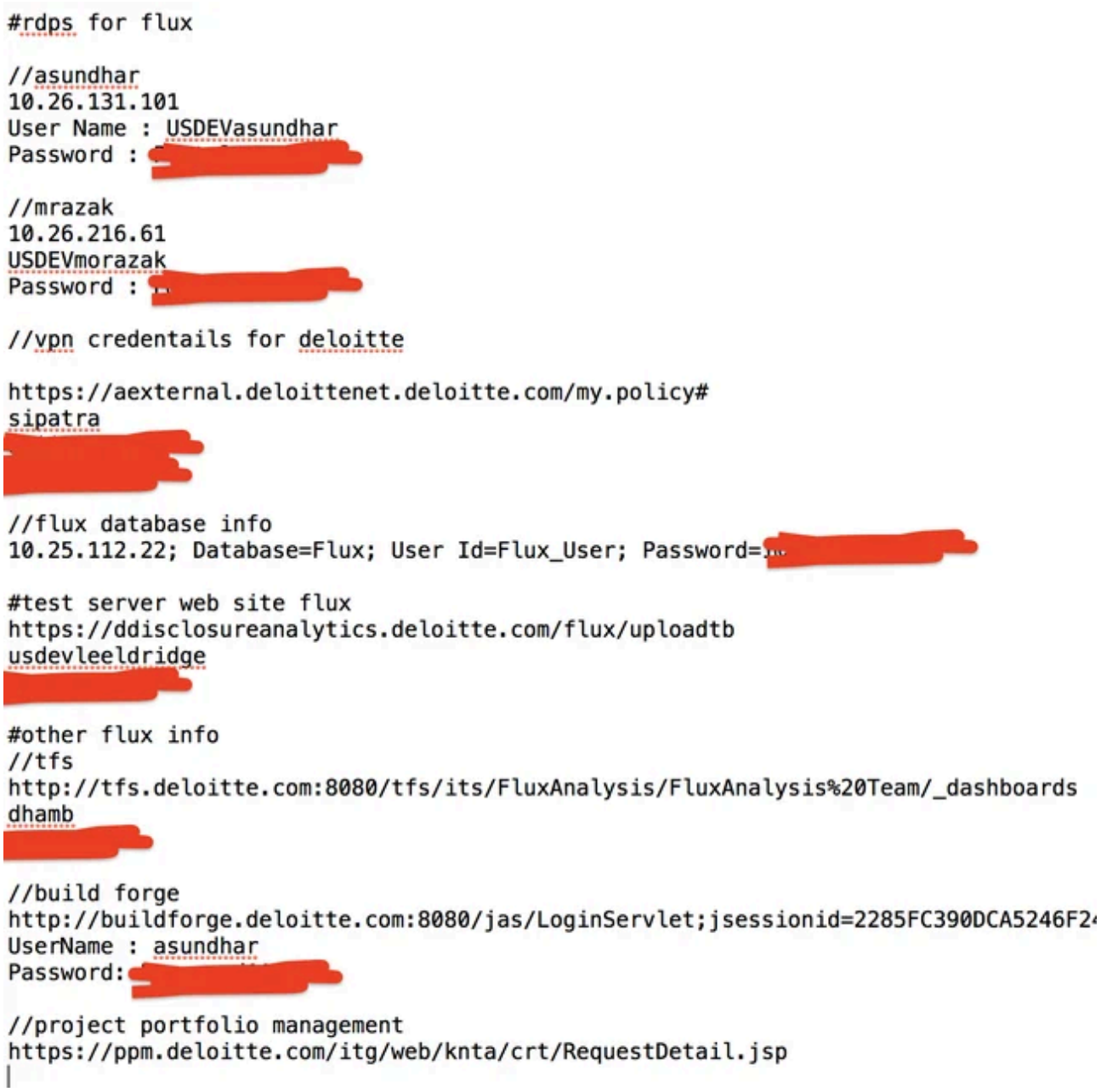
Published: 2017-09-26 · Archived: 2026-04-05 17:19:35 UTC

Monday’s news that multinational consultancy Deloitte had been hacked was dismissed by the firm as a small incident.

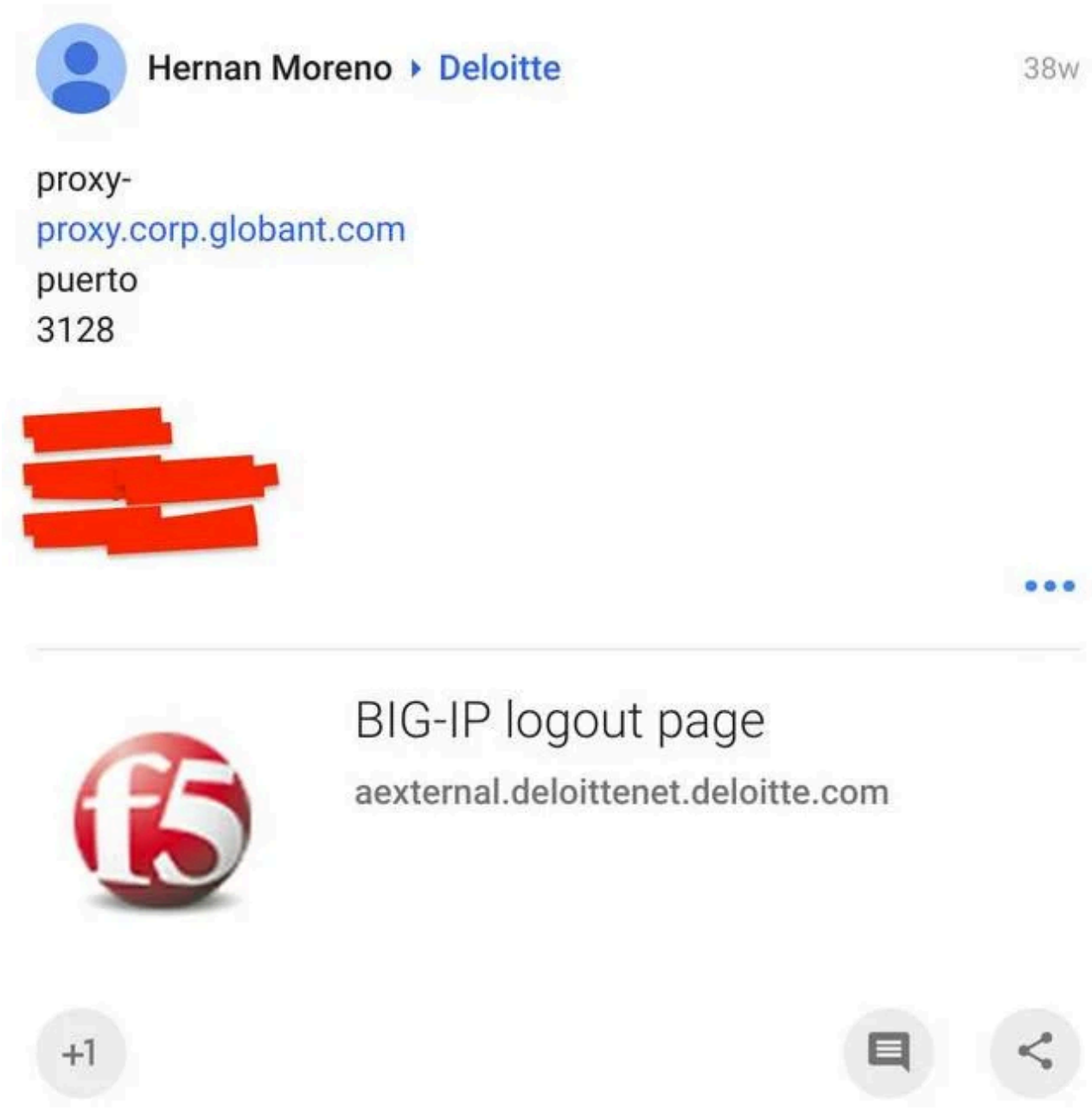
Now evidence suggests it's no surprise the biz was infiltrated: it appears to be all over the shop, security wise.

On Tuesday, what seemed to be a collection of Deloitte's corporate VPN passwords, user names, and operational details were found lurking within a public-facing GitHub-hosted repository. These have since been removed in the past hour or so. In addition, it appears that a Deloitte employee uploaded company proxy login credentials to his public Google+ page. The information was up there for over six months – and was removed in the past few minutes.

We were tipped off to these pages by an eagle-eyed reader, and grabbed a couple of screenshots of the potentially offending data:



Screenshot of some of the alleged VPN details for accessing Deloitte's network that leaked onto GitHub – we've censored what looks like passwords



Screenshot of a portion of the Google+ page with Deloitte proxy login information

On top of these potential leaks of corporate login details, Deloitte has loads of internal and potentially critical systems unnecessarily facing the public internet with remote-desktop access enabled. All of this gear should be behind a firewall and/or with two-factor authentication as per industry best practices. And likely the best practices Deloitte recommends to its clients, ironically.

“Just in the last day I’ve found 7,000 to 12,000 open hosts for the firm spread across the globe,” security researcher Dan Tentler, founder of Phobos Group, told *The Register* today. “We’re talking dozens of business units around the planet with dozens of IT departments showing very different aptitude levels. The phrase ‘truly exploitable’ comes to mind.”

For example, he found a Deloitte-owned Windows Server 2012 R2 box in South Africa with RDP wide open, acting as what appears to be an Active Directory server – a crucial apex of a Microsoft-powered network – and with, worryingly, security updates still pending installation. Other cases show IT departments using outdated software, and numerous other security failings.

Here's an example system with NetBIOS open:

> Hey look, a deloitte server with 445 exposed to the internethttps://t.co/BMFJqG0s3m
> production tax dns server
> what could possibly go wrong? pic.twitter.com/IeHSf7L1Vz
>
> — Dan Tentler (@Viss) September 25, 2017

Here's what appears to be an Active Directory server with RDP open...

> 'a;sljfasdfjadjaserfaweakjwtgfaehasrhfasd;laksfkasrohawghasedjas;faskdga'seraowhjasjdfasdlfasgajhsdfjarfhoae;ahd
> pic.twitter.com/54O2PDy7zV
>
> — Dan Tentler (@Viss) September 25, 2017

...complete with administrative users and, if you look closely, Windows Updates still pending:

> pic.twitter.com/iGlTg4Kqh8
>
> — Dan Tentler (@Viss) September 26, 2017

And as other infosec experts have spotted, plenty of other stuff is sitting online, searchable using Shodan, waiting to be prodded by miscreants and other curious minds:

> Deloittes' US offices have everything from Netbios to RDP to Exchange Admin (single factor) etc etc
> etc. They should get an auditor. pic.twitter.com/C8aoN5YQMn
>
> — Kevin Beaumont 🙃 (@GossiTheDog) September 25, 2017

These systems could be used as crucial footholds for hackers into the consultancy giant's internal networks.

The Google+ page appeared to show that a Deloitte employee has been writing down VPN access controls on his personal page in full view of everyone. Using Google's vaunted search facilities, a hacker could easily find enough information to launch an attack with a good chance of success.

All this is embarrassing for Deloitte, which billed itself as the top IT security consultancy in the industry. The firm makes millions selling its tech guru services to others for a hefty price – and yet seems to ignore potentially gaping holes in its own IT infrastructure.

The details now emerging are also rather embarrassing for analyst firm Gartner, which in June named Deloitte the world's best IT security consultancy for the fifth year in a row. Gartner has yet to respond to a request for information on how its conclusion was reached.

It doesn't help that Deloitte isn't much liked by other security researchers for its business practices. The firm has a reputation for low-balling contractors on fees – particularly for penetration testing – and the schadenfreude of Deloitte being so bad at its own security has delighted some.

> Deloitte always wanted to break pentest prices, less than 1k / man day. Well, now you can see what you get for that price.
>
> — Responder (@PythonResponder) September 25, 2017

"Between Equifax and Deloitte, starting to see though the tissue paper of corporate America's security industry companies making huge claims, when in reality it's a whole bunch of hypocrites," said Tentler.

"You'd think Deloitte claims to have all this super elder-god style security talent. If that was the case they might consider using that talent on its own infrastructure."

Deloitte has not responded to a request for comment. ®
