Verizon finds US developer outsourced his job to China so he could surf Reddit and watch cat videos

Emil
Protalinski

16 January '13, 07:35am

Follow

No, this is not the Onion, it's not April Fools, and I'm not making this up. All of this comes straight from Verizon, or more specifically, a case study from 2012 outlined by its security team.

See also – Verizon investigator: How one US developer could have gotten away with outsourcing his job to China

The story goes a little something like this. A developer at a US-based critical infrastructure company, referred to as "Bob," was caught last year outsourcing his work to China, paying someone else less than one fifth of his six-figure salary to do his job. As a result, Bob had a lot of time on his hands; in fact, during the investigation, his browsing history revealed this was his typical work day:

- 9:00 a.m. – Arrive and surf Reddit for a couple of hours. Watch cat videos.
- 11:30 a.m. – Take lunch.
- 1:00 p.m. – Ebay time.
- 2:00 – ish p.m Facebook updates – LinkedIn.
- 4:30 p.m. – End of day update e-mail to management.
- 5:00 p.m. – Go home.

Again, I want to emphasize that I haven't invented this schedule for the sake of making this story more interesting or to have a snazzy headline. This comes straight from Verizon; take that as you will.

Apparently Bob had the same scam going across multiple companies in the area (this part is a little unclear given that he clearly couldn't physically go into work for all of them), earning "several hundred thousand dollars a year," and only paying the Chinese consulting firm "about fifty grand annually." At the unnamed company, he apparently received excellent performance reviews for the last several years in a row, even being hailed the best developer in the building: his code was clean, well-written, and submitted in a timely fashion.

Folks, you can't make this stuff up. Here are the rest of the crazy details, which Verizon says it released because although this wasn't a large-scale data breach that made headlines, the case had a unique attack vector.

Apparently the scheme was discovered accidentally. Verizon received a request from the US company asking for help in understanding anomalous activity it was witnessing in its VPN logs: an open and active connection from Shenyang, China.

This was alarming because the company had implemented two-factor authentication for these VPN connections, the second factor being a rotating token RSA key fob. Yet somehow, although the developer whose credentials were being used was sitting at his desk staring into his monitor, the logs showed he was logged in from China.

This unnamed company initially suspected some kind of unknown (0-day) malware that was able to initiate VPN connections from Bob's desktop workstation via external proxy, route that VPN traffic to China, and then back. When Verizon investigated, it eventually noticed that the VPN connection from Shenyang was at least six months old, which is how far back the VPN logs went, and it occurred almost daily and occasionally spanned the entire workday.

Unable to explain how an intruder could have possibly been accessing the company's internal system on such a frequent basis, Verizon decided to look more closely at Bob, since it was his credentials that were being used. Here's how his the case study described him:

> *Employee profile –mid-40's software developer versed in C, C++, perl, java, Ruby, php, python, etc. Relatively long tenure with the company, family man, inoffensive and quiet. Someone you wouldn't look at twice in an elevator.*

All it took was a look a forensic image of Bob's desktop workstation to discover hundreds of PDF invoices from a Chinese consulting firm in Shenyang. How did he get around the security requirements? He physically FedExed his RSA token to China.

See also – Verizon investigator: How one US developer could have gotten away with outsourcing his job to China

Image credit: Andreas Krappweis