west protect

SAFE Alert!

Exploit of CapitalOne Breach

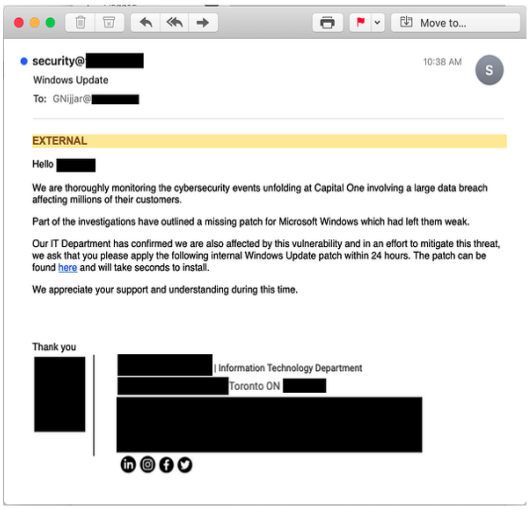
Aug 2019

Hackers Exploit CapitalOne Breach to offer fake "Microsoft Patch"

The bad guys are now exploiting news of the CapitalOne breach to push a malicious backdoor Trojan via a phishing email claiming to offer a Windows Security Update.

Clicking the link in that email downloads a file named KB3085604 (dot) exe — named to resemble Microsoft patch files and security updates.

The phishing email itself spoofs the targeted organization's IT department, and the language used is sufficiently informal (as well as a little technical and even awkward) to appear credible. See the phishing email example below:



As a result, some users just might fall for it — especially those working in organizations that occasionally ask employees to perform routine IT tasks (e.g., applying updates, updating AV definitions, etc.).

What should you do?

If you receive a similar email don't click on any links, especially not an .exe file, or reply to the email. If you are a WESTprotect customer and suspect a phishing email, you should forward the original email as an attachment to: 411@poweredbywest.com.