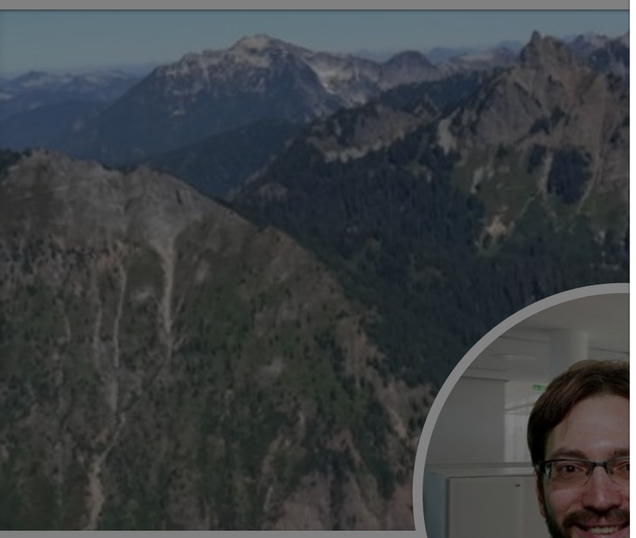
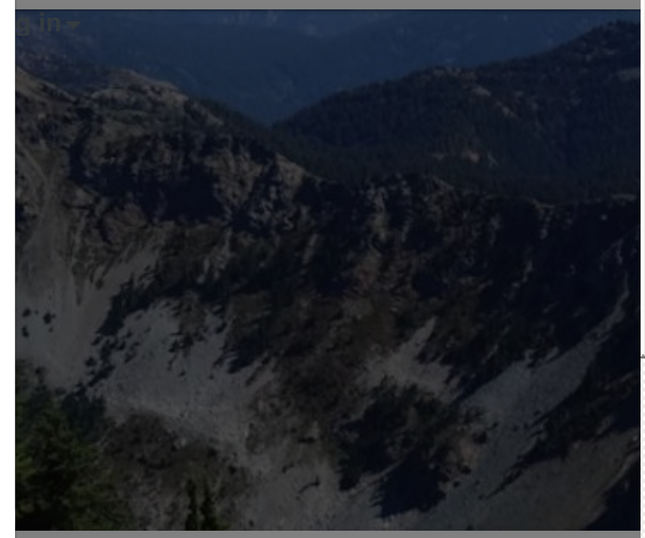
By using Twitter's services you agree to our Cookies Use. We and our partners operate globally and use cookies, including for analytics, personalisation, and ads.





John Lambert @JohnLaTwC

Follow

Story time. This one is about a feature in Windows called ASLR.

11:37 AM - 8 Feb 2019

339 Retweets **782** Likes

16 339 782

John Lambert @JohnLaTwC · 11h

It was 2005. We were working on Windows Vista. Most remember it as the release with the maligned User Account Control feature. For us in Trustworthy Computing it was the first full Windows cycle where we could apply all the security engineering tools we had from start to finish.

2 15 98

John Lambert @JohnLaTwC · 11h

Efforts such as fuzzing file parsers, scrubbing the code of 'banned APIs' across millions of lines of code, fixing masses of potential bugs from static analysis, and driving initiatives to deal with newly discovered 'diseases' like mismatched container COM instantiation.

1 47

John Lambert @JohnLaTwC · 11h

We hired the most spectacular group of researchers I've seen assembled from NGS, iSEC Partners, IOActive, and n.runs, gave them source code, access to Windows engineers, and told to hack without boundaries. My words to them in an early meeting were "you are here to blow sh*t up"

1 9 99

John Lambert @JohnLaTwC · 11h

A quieter effort was going on to shore up our memory safety mitigations. Mitigations touch the holiest of holies in the OS: the compiler, the memory manager, the loader. Areas you just don't mess with late in an OS release.

1 40

John Lambert @JohnLaTwC · 11h

The breathing room created by hardware Data Execute Protection we added in XP SP2 was gone. Exploits were using return to libc attacks and taking advantage of the fact that much of the memory layout in a Windows process was predictable.