James Benerd Ankhs
December 18 at 6:48 PM ·

Cyberattacks are fair game for a kinetic response. Anyone want to challenge that?

2 21 Comments

Like Comment

Neil Gre
Not me. 1
Like · Reply · 1d

James Benerd Ankhs replied · 1 Reply

Dara V
Maybe explain it first? Its vague enough to not make a lot of sense. Like is this a different thing than a normal blue team effort or are you talking offensive counteroperations

Like · Reply · 1d · Edited

James Benerd Ankhs replied · 10 Replies

William Mantly
The blame lays solely on those who maintain and make decisions for the systems that got hacked. This is a consequence of relying on closed sourced vendors and low-cost H1b workforce.

Like · Reply · 5h 1

James Benerd Ankhs

Like · Reply · 4h

William Mantly
no, the message needs to be "incompetence gets what it deserves". I have no want to start a war over this.

Like · Reply · 4h

1

William Mantly
I have worked on designing, implementing, and maintaining highly secured networks. An attack like this only doable because of incompetence and lack of operations discipline.

Like · Reply · 2h

James Benerd Ankhs
William Mantly this is the mentality that says you don't get to shoot somebody who breaks into your house if your locks weren't good enough.

Do you know specifically how they got into the systems? AFIK that is not known yet.

I also think that "nobody gets hacked unless they are incompetent" is just something said by people who are in the mentality of marketing their skills. Nothing is perfect or fail-safe.

Like · Reply · 1h

William Mantly
You cant compare a computer network connected to the cesspool that is the internet to a physical location.

The details of the hack may not be know, what is know is that somehow the Solar Windows software became poisoned and allowed malicious access i… **See More**

Like · Reply · 27m

William Mantly
You are 100% correct "Nothing is perfect or fail-safe", that's what migration is king in cybersecurity. You must operate with the understanding that breaches happen, malicious actors do malicious shit. How can we design our networks and systems to mitigate the inevitable? That is the difference between skill and relying on vendors. In this event, incompetence and laziness played are a larger role than the hackers.

Like · Reply · 2m

12

William Mantly

Check this out, open a bash terminal to a public-facing server with ssh and see how many attempts have been made to get access:

`zgrep -E "sshd.*Failed password" /var/log/auth.log* | wc -l`

Mine is 184,390 for the past 4 weeks.

Like · **Reply** · 1m

Write a reply…

Write a comment…

12