All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Why does it seem like more attacks are taking place?

Perhaps because more higher impact incidents are making the media these days. Perhaps there is an actual increase in threat actors, their activities, or the effectiveness of their activities. Perhaps the defenses have been spread too thin, perhaps … oh heck, perhaps all sorts of things. I know that in my career, I have been aware of many attach activities and successful actions by threat actors against corporate, government, and other interests that never got to the media, and of course another possibility is that we are seeing more reporting of what was already happening. Or perhaps the things now being done are harder to conceal because of the obvious nature of the consequences being realized.

My notional hypothesis about this

I think there may actually be a substantial increase in the quality and quantity of attacks underway, and that this may be related to Russia's increasing desire to do harm to the world in order to fight off the arms and expertise being provided to Ukraine. I notion that they may be conveying the thought to worldwide governments and/or their citizenry, either directly, through back channels, or as part of an influence operation, that we have a lot to lose and they are willing to take it.

I also think we are seeing more and more readily apparent attacks taking place with greater and more obvious effects.

Of course I may be completely wrong about this...

But nevertheless, I see increasing activity reaching my infrastructures and attempting to exploit various weaknesses that may or may not exist in specific systems we operate. So I think it is a real signal.

But really, the problem is we don't have a good way to measure this

If we did, we would actually know that something was going on, and possibly even what it was. Of course folks at the CISA, FBI, Secret Service, and other government agencies might know and be unable to tell us without harming their ability to know. And they have been surprisingly open about things they have found of late, which may indicate their desire to keep us better informed.

Nevertheless

Here we are. The defenders of cyberspace. And yet we aren't really sharing the information required to gain clarity around what is happening. And that makes decision-making less certain, which makes our ability to manage risks even less effective than it would otherwise be because of the other limitations we have. I think we should be sharing more and doing so more openly and transparently. Yes – I know – admitting weakness is hard to do. However...

Conclusions

We don't actually have a good way to measure what is taking place because we have no required reporting or standards of measurement. Maybe we need the government involved?

