Image Credit: Bnymdt/Pexels

Psychological Warfare is the Key to Beating Cyber Criminals – Here's Why

Hackers rely on psychological tactics to manipulate their victims and steal sensitive data. Let's give them a taste of their own medicine.

Spend long enough in cybersecurity circles and you'll soon hear about 'zero trust'. It's a key tenet that warns against automatically trusting anything online, such as users, machines, or resources; even those you're familiar with.

This principle is important because cybercriminals rely on abusing our trust and exposing our blind spots to steal sensitive data. Whether they're posing as tech support on a phone call, exploiting unprotected accounts, or sneaking through a forgotten backdoor in an old system, it's often human error that leads to the biggest data breaches.

Zero trust helps ensure that we double-check everything, verify everybody, and watch our backs at all times. And today, it's more crucial than ever.

Defensive Security Isn't Working

Cyber wars usually step in time with boots on the ground, and with conflict erupting around the world in recent years, the number of state-sponsored cyber threats is rising. These groups have the skills and funding to infiltrate government systems, disrupt financial networks, and bring down critical infrastructure.

Right now, security teams are on high alert for ransomware attacks, which have surged by 81% in the past year, and hackers' usual psychological tactics are proving successful – nearly half of organizations were hit by social engineering attacks in 2024. The advancement of Gen AI makes this even easier; hackers can now craft convincing scams at the click of a button.

In this battleground, unfortunately, zero trust isn't enough. New and increasingly advanced threats are emerging every day, and governments, companies – even individuals – are finding themselves either direct targets or collateral damage in the crossfire of international cyber conflicts.

Security teams can't have eyes everywhere, and technology can't stop people making the mistakes that inevitably lead to successful cyberattacks. Hackers only need to get lucky once, after all.

Cybercriminals have a key advantage too, a secret hideout where they can plan their attacks beyond the reach of law enforcement – the dark web.

Shining a Light on the Dark Web

The dark web is an unindexed and unregulated side of the internet, 50% of which hosts illegal content. You can't find it by typing 'dark web' into Google; it can only be accessed using specialist software that masks your IP address and location, such as Tor (the Onion browser).

Cybercriminals use the dark web to buy and sell hacking tools, software vulnerabilities, and stolen data, as well as to hatch plans for future attacks and share information in private forums.

These dark web forums would be a goldmine for law enforcement groups if they could get inside. The problem is that they can't. Most forums are guarded against newcomers and require a payment or loyalty offering (such as stolen data) to gain access. That's not to mention the strict hierarchies that dictate just how much information you're allowed to see once the door is open.

For the inner circle, though, the dark web is a community. Cybercriminals share a sense of trust in their anonymity, and that marks the beginning of their downfall; trust be *weaponized*.

Divide and Conquer

More security teams are waking up to the idea that psychological warfare can be used to bring down cybercriminal groups from the inside. The US National Security Agency, for instance, has announced it will deploy psychological warfare to combat ransomware gangs going forward.

It's a sound strategy. Hackers rely on psychological tricks to manipulate their victims and steal sensitive data, so what's to say the same tactics can't be used against them?

The timing couldn't be better. While global conflicts have led to an uptick in the number of cyberattacks and state-sponsored threat actors on the scene, they're also creating factions. Tensions are rising between major world powers, and hackers are second-guessing their allies. Who's a genuine collaborator, and who's quietly working for a state? Where do loyalties really lie?

Cybercriminal groups, even those tied to warring nations, often work within decentralized networks. They're scattered across the globe, using pseudonyms, and of course, communicating under the anonymous shroud of the dark web. This means that hackers (even more so than troops on the ground) are susceptible to infighting, desertion, and betrayal, which offers the perfect opportunity for security and law enforcement groups to poison the well. By spreading doubt, eroding trust, and turning threat actors against each other from within the dark web itself, security teams could finally gain the upper hand.

But how would this work? Security teams struggle to even gain access to dark web forums, let alone hold any sway over the cybercriminals there. The answer – ironically – could lie with dark web users themselves.

Wanted: Dark Web Whistleblowers

Dark web forums attract all kinds of people tied to cybercrime; not everyone is active, and not everyone is a criminal. Some are looking to expose what goes on in the shadows for reasons ranging from ethics and curiosity to personal vendetta.

By rewarding these insiders for coming forward with information, instead of punishing them for their past, the good guys could uncover a way to monitor, disrupt, and fracture cybercriminal networks from within.

Just as bug bounty programs let ethical hackers help expose software vulnerabilities, similar models could be applied to the cyber underworld, like in the form of global whistleblowing initiatives, which would target the vital organs of these dark web networks.

It's psychological warfare. It would force hackers to second guess their allies. For cybercriminals, even the prospect that their counterparts had turned themselves over would break their illusion of safety on the dark web – their anonymity would suddenly become a threat. It's a surefire way to disrupt the flow of illicit information and technology on the dark web, which would help security teams prevent cyberattacks before they're even formulated.

However, this strategy only works if there’s a system that supports it. While it needs whistleblowers and vigilantes to step forward to offer their help, it also requires a system that allows them to do so without fear of legal repercussions. These people would need to be offered a way out of their previous life, a chance to redeem themselves by fighting back against cybercrime in the best way they can – with their information, their access to the dark web, and their connections. And it’s up to us to open the door for them.

This strategy could be a stretch for law enforcement, but sometimes the boldest ideas come out on top. If cybercriminals have forced us to adopt zero trust, then perhaps it’s time we return the favor.