SC Magazine: EDR (alone) won't protect your organization from advanced hacking groups

written by Nick Landers | July 12, 2021

On July 12, 2021, NetSPI Director of Research Nick Landers was featured in an article from *SC Magazine*:

Endpoint detection and response systems can often serve as a frontline defense for many organizations, collecting and storing telemetry from dispersed employee devices and using it to detect malicious activities or behaviors. However, a recent experiment by academic researchers at the University of Piraeus in Greece indicates they are far from a silver bullet when it comes to protecting your organization….

Nick Landers, director of research at penetration testing company NetSPI, told SC Media that that it's rare for one team or company to even have access to such a wide range of EDR systems and any research that can test and compare different

products in the EDR market is valuable in and of itself.

He said the results outlined in the study largely mirror his experience with customers, and that many advanced threat actors generally rely on two strategies for evading detection by EDR systems: using completely unique or novel tactics that can frustrate heuristic analysis or data algorithms, and "not making noise in general" by understanding what telemetry EDR systems collect and measure.

"I think the ones we see that are the most effective are ones where the attacker understands the data [the EDR system is] collecting and keeps generation of that data low," he said.

However, Landers said his main takeaway from the study is not necessarily that EDR products are shoddy or not worth the cost (though he again lamented the lack of access that independent third parties typically have to test such systems), but rather a "more constructive" reinforcement of the need for multiple layers of security to ensure any one tool or process doesn't become a single point of failure.

"I think looking at the minutiae and finger-pointing and trying to identify specific products and their specific failings is a fault that belongs to everyone in the industry," he said. "But [EDR systems] are valuable tools and while I might not agree with their strategy or their marketing or cost or licensing model or availability, I think they do contribute to a defense in depth strategy and that's ultimately what we should all be striving for."

To learn more, read the full article here: https://www.scmagazine.com/news/network-security/edr-alone-wont-protect-your-organization-from-advanced-hacking-groups