POINT OF VIEW

Use the 2023 MITRE ATT&CK® Evaluations Results for Turla to Inform EDR Buying Decisions

Organizations Need New Tools to Defend Against Today's Threat Landscape

Executive Summary

According to the 2023 Fortinet Global Threat Landscape Report, Fortinet observed a significant shift in attacker activities. These changes include more activity among advanced persistent threat (APT) groups like Turla, a rise in ransomware frequency and complexity, increased botnet activity, as well as a shift in MITRE ATT&CK framework techniques, tactics, and procedures (TTPs) used by malicious actors.[1] The data also shows that fewer organizations are successfully detecting ransomware today than in the past (13% in 1H 2023 versus 22% five years ago).[2] This reaffirms that advanced attackers are shifting tactics to become more sophisticated.

As attack tactics advance, your security strategy must evolve, too. And with the proliferation of devices and applications, companies have more endpoints to protect than ever before, making endpoint security a critical aspect of any risk management program.

In round five of the MITRE ATT&CK Evaluations, the average vendor only detected 83% of the sub-techniques associated with Turla.[3]

However, it can be challenging to separate fact from fiction regarding different endpoint detection and response (EDR) solutions, especially as you're reading marketing materials or reviewing vendor-sponsored reports. The MITRE ATT&CK Evaluations results should be a critical component of your evaluation process, as this information provides valuable, unbiased insight into the true capabilities of various offerings.

The Buyer's Peril

Endpoint security has a deep-rooted history and with the expanding market, and there's an influx of vendors that claim to have unique offerings. Many buyers, overwhelmed by these claims, turn to third-party analysts to narrow down their options. However, it's crucial to realize that many of these analyst reports are grounded in survey data, resulting in reports focused primarily on others' opinions of a specific technology. As such, these reports don't always reflect the real-world effectiveness of the products against active threats. Also, some agencies charge vendors to write favorable reports, further muddying the waters for potential customers who need to evaluate and compare various security solutions.

Use MITRE ATT&CK Evaluations to Provide Clarity During the Buying Process

Fortunately, MITRE Engenuity, a technology foundation, offers cyber-defense testing for some security technologies. The MITRE Engenuity ATT&CK Evaluations assesses various endpoint protection platform (EPP) solutions using carefully selected threat scenarios, showcasing multiple observable behaviors. In each of the five evaluation rounds, MITRE chooses one or two specific strains to use. These are then divided into different test scenarios, evaluating whether each technology effectively protects against the attack and detects each sub-technique. The chosen strains are noteworthy because of their involvement in real-world attacks and the diversity of adversary TTPs they employ.

A Closer Look at the MITRE ATT&CK Round Five Evaluations

The fifth round of the MITRE ATT&CK Evaluations focused on the threat group Turla. Recognized for its sophistication and persistence, Turla has been responsible for numerous cyber-espionage campaigns over the past two decades.

MITRE's choice to evaluate security solutions based on their response and ability to provide key insights into Turla-related TTPs was strategic. By focusing on Turla, MITRE aimed to highlight the diverse and advanced nature of the challenges that cybersecurity solutions must address today.

Because Turla's activities span Windows and Linux environments and include a diverse set of TTPs—ranging from stealthy information extraction to exploiting system vulnerabilities—these strains MITRE selected offer a rigorous test for any EDR or extended detection and response (XDR) solution. The intent behind using Turla as the foundation for this round was to provide buyers and reviewers with insights into how various security solutions perform when confronted with advanced, multifaceted threats. This fifth evaluation round sought to answer a pressing question for many enterprises: Can a chosen solution offer detailed insights against an adversary as daunting as Turla?

What We Can Learn from the MITRE ATT&CK Evaluations Results

The MITRE Engenuity ATT&CK Evaluations, in its fifth cycle, featured 30 vendors just like in round four with Wizard Spider and Sandworm, but with four different participants. For interest's sake, the four new entrants fielded less-than-mediocre results and didn't bring anything unique to the table. Additionally, one participant was removed from the public results, bringing the final count to 29 vendors.

When compared to round four in 2022, the average visibility rate was 87% across all 29 vendors. In round five in 2023, that figure dropped to 83%. This wasn't surprising since the evaluation was handling such a well-crafted malware strain such as Turla. When evaluating vendors, take a close look at the average visibility rate. How did the solutions you know stack up?

Conclusion

The round five MITRE ATT&CK Enterprise Evaluations offered security decision-makers a detailed examination of how various EPP solutions handled the challenges posed by Turla, an advanced nation-state espionage malware strain.

To extract the most value from the evaluations, it's imperative to carefully analyze the research. Look at how much insight vendors provided within the Windows and Linux tests. Examine the percentage of sub-techniques identified through analytics. Another critical consideration is identifying vendors that exhibited configuration changes leading to detection delays, as highlighted by the evaluators. These delays could lead to an attack, bypassing defenses and causing damage.

[1] "FortiGuard Labs 1H 2023 Global Threat Landscape Report," Fortinet, August 7, 2023.

[2] Ibid.

[3] "MITRE Engenuity ATT&CK Evaluations: Fortinet," MITRE Engenuity, 2023.

October 4, 2023 3:30 PM

2362220-0-0-EN