Does Cyber Crucible test all possible ransomware exhaustively?

Cyber Crucible operates off of kernel level behavioral modeling, to discover data theft, credential theft, and ransomware encryption behaviors very quickly. The behavioral decisions are made using information from process behavior, memory-derived behaviors, and certain types of file-sourced behaviors, to make a decision right as the extortion is about to occur.

Despite the very large number of ransomware and extortion-themed software samples, they can be behaviorally categorized into a relatively small number of sets.

On the surface, though, “skin-deep” defenses used by a variety of security tools have a very large number of extortion tools to try to counter. It is important to understand our behavioral analytics run much deeper into the attacker tools and tradecraft, dramatically reducing the need for some type of (impossible) exhaustive testing of all possible malware at all times.

The Cyber Crucible developers categorize the kernel level memory, process, and file behaviors of an extortion tool, then ensure it fits into one of the known defensive capabilities. Occasionally, similar to a vaccine, the formula can be tailored slightly to produce a more accurate response.

Very rarely does something completely new appear.

The Cyber Crucible team works exhaustively to preemptively uncover novel techniques that are not yet observed in our customer base, or in threat intelligence.

The effect?

1. Cyber Crucible’s extortion tool defense is complete against all known ransomware variants.

2. New ransomware variants are blocked before they even hit the first customers. We don’t even know what to call most of the software we defend for around 120 days, until researchers “catch up”.

3. Ransomware and extortion tool developers sometime call us to see what we’re up to, to try to work out an angle. Unfortunately, frustration from our presence appears to sometimes spur evolution on their part, which makes other tools even less effective.

4. We welcome testing of our software. When penetration testers, malware analysts, or adversary emulation professionals enter the sale process - we get excited!

Revision #2
Created 2026-05-18 20:27:26 UTC by Dennis Underwood
Updated 2026-07-13 19:57:09 UTC by Dennis Underwood