Crytica Security's Malware Detection in the Age of AI-Generated Malware

An Introductory Overview

Crytica Security
7655 Town Square Way
Suite 212
Reno, NV 89523

Website: CryticaSecurity.com
Email: info@cryticasecurity.com

1. THE COMING WAVE OF ARTIFICIAL INTELLIGENCE GENERATED MALWARE

"Dig into every industry, and you'll find AI changing the nature of work."–Daniela Rus

For the last decade cybersecurity systems have used Artificial Intelligence (AI) to enhance their own efficacy. "AI" has become a buzzword synonymous with, and even the *sine quo non* of, "the latest and greatest" cybersecurity systems. However, far less attention has been focused on the possibilities and the uses of AI by the enemy, to enhance the abilities of the malware used to attack information systems. Recently, especially with the very public advent of popularly available AI systems, such as ChatGPT, the realization that AI can be used as an offensive tool, not just a defensive one, has reached the public consciousness. In particular, it is now obvious that, just as a system such as ChatGPT can synthesize documents, music, photos, and more, from a vast library of existing source materials, so too can AI systems synthesize new and effective malware; and do so at a speed and efficacy impossible to achieve using just human programmers. With this newest development of AI, malware production has entered the "industrial age".

The most sophisticated malware attacks are those that are polymorphic and/or preemptive. That is, they can change their own "signatures" and attack patterns, and/or they can disable the existing defensive systems currently in place to defend against them. Such malware, while not extremely difficult to create, has been beyond the ken of the casual cybercriminal. Now however, with the new AI tools available, even the most unsophisticated cybercriminals and malicious state actors can create myriads of new polymorphic and preemptive malware. This potential tsunami of AI-Generated malware will easily be able to overrun and overwhelm most of the currently available cybersecurity detection systems.

2. CRYTICA'S ABILITY TO DETECT EVEN AI-GENERATED MALWARE

Crytica Security, Inc. has developed a detection platform that is up to the task of defeating this new wave of AI-Generated malware. Crytica's malware detection platform can detect totally new malware. It is not fooled by all of the variations of polymorphic malware. It is even impervious to the disruptions caused by preemptive malware.

Crytica Security, Inc. has created a unique malware detection platform that has been designed and implemented based upon a new paradigm for malware detection, and upon the principle that cybersecurity systems must be resilient to attacks against them. Crytica detects any unauthorized change to a system's instruction sets. It does so at the time of malware injection, "Injection Detection™". It does not need to wait for the appearance of malicious behavior nor upon historical patterns of previously identified malware. And Crytica's malware detection platform absorbs attacks against it, a true defense-in-depth. It does not rely upon impenetrable walls, but rather upon flexible dynamic defenses.

For more information on Crytica's malware detection platform, its ability to interface with, strengthen and support other cybersecurity tools, its ability to detect even AI-Generated malware at the time of injection, and its resilience to attacks launched against it, contact Crytica Security, Inc.

Website: CryticaSecurity.com
Email: info@cryticasecurity.com