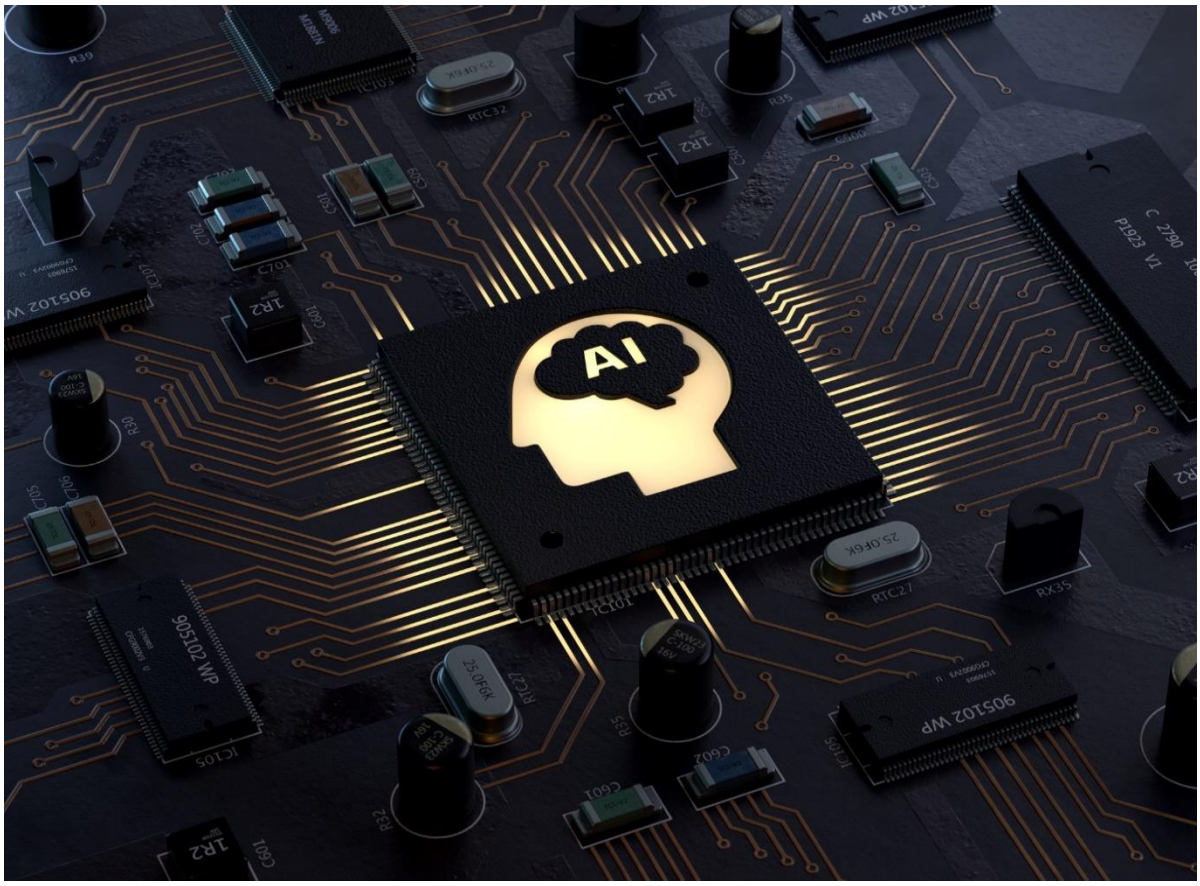
Whitepaper: Using AI to Defeat Cybercriminals

Jeanne Zepp



Introduction

The threat cybercriminals pose to federal information systems and networks is real and pervasive. Defending against unauthorized intrusions is a full-time effort undertaken by federal agencies and the contractors, like Electrosoft, that support them.

Artificial intelligence (AI) basically refers to the use of automation to emulate the performance of humans in tasks such as problem solving, pattern detection, decision making, and similar functions. Machine learning (ML), positioned as akin to human intelligence, is the quality whereby algorithms can "learn" or improve task performance over time. In some cases, ML is intentional via use of specific data to hone performance. In others, it is a function of ongoing repetition.

AI comes with built-in advantages. They include round-the-clock availability, suitability for rote tasks, and fewer errors in task performance.

AI and Cybersecurity

Reactive Capabilities

In cybersecurity, early detection is paramount. AI offers both speed and algorithmic precision in evaluating large amounts of data, identifying suspicious activities/behaviors, and even detecting zero-day attacks in real time. Its pattern recognition capabilities surpass those of human analysts, adding to AI's early detection credentials. Further, AI can better separate real threats from miscues or lower priority issues, sparing analysts from time-intensive research tasks and allowing them to focus on critical events.

AI can counter a relatively new and impressive threat: the bot. Beyond expected actions (bot recognition and blocking), AI offers enhanced security features (e.g., stronger captchas) and the capability to create honeypots that attract bots and allow analysis of their functioning in controlled environments. AI and ML also shine in their capacity to recognize and detect new malware variants based on experience with earlier versions.

Speedier detection allows IT staff to quickly institute defensive measures. However, AI can undertake defensive action on its own, for example, by redirecting system traffic to unaffected servers. Also, AI can block suspect IP addresses and incoming emails believed to contain phishing schemes as well as close compromised accounts.

Proactive Capacities

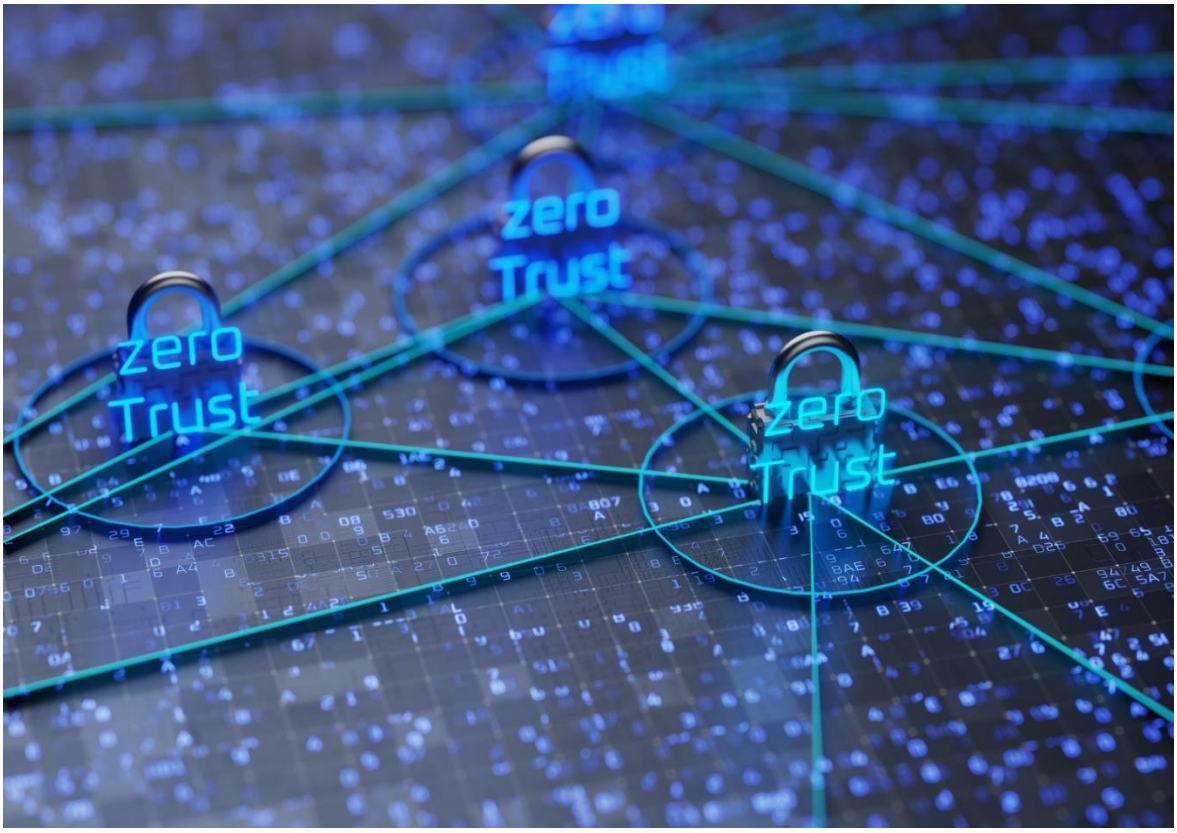
AI can function in proactive ways, too. It can scan systems and identify vulnerabilities in need of strengthening. Moreover, it can automate system functions, such as patch management, to assure software vulnerabilities are remedied quickly.

AI heightens secure authentication measures, which, if undermined, offer a common gateway into systems or networks. AI allows multifactor authentication, whereby systems

can request and process in real time something known (password or PIN), something possessed (PIV card or token), or something unique to you (biometrics such as a fingerprint).

Predictive Forecasting

Last, but not least, AI/ML offers predictive forecasting capabilities. The same features that discover suspicious activity and unusual behavior patterns can warn analysts of events that could be indicative of future attack plans. Knowing that something nefarious may be afoot enables an organization to boost defenses and institute other preventive measures. Of course, it is not an exact science but, as the old adage goes, "an ounce of prevention is worth a pound of cure." Attacks can be devastating and expensive in terms of organizational disruption, new or replacement system software and hardware, data recovery, and forensics.



Prediction capabilities increase when AI and natural language processing work in tandem. By drawing on sources such as the Cybersecurity & Infrastructure Security Agency's

Cybersecurity Alerts & Advisories, as well as other information sources such as studies, news articles, and the like, AI tools increase their capacity to discern the latest attack precursors and prevent them.

Leveling the Playing Field

Cybercriminals have untold resources, some derived from the sponsors of their crimes and some furnished by their victims (ransoms). Safe to say, most organizations don't possess the same deep pockets or the learning opportunities that a life of crime offers.

Attackers are continually creating new bots, new malware, and honing their phishing attacks. In addition, use of AI to create deepfakes is a potent weapon on many levels. Non-reality-based audios and videos can prompt individuals and organizations to take actions that they normally wouldn't consider. Here, AI is at once the creator of criminal tools and the executor of the crime.

Many organizations desire strong cybersecurity but such an objective is resource-intensive in terms of the budget needed to support personnel, equipment, and other tools. The automation AI and ML offer help level the playing field. Here, contractors can play an important role through outsourced management of Security Operations Centers, for example.

How Electrosoft Is Advancing Cybersecurity

Electrosoft is playing a key role in the federal technology and cybersecurity arena – and has done so for over 20 years. The impact of our efforts grows every day. Our accomplishments include

- Assisting the National Institute of Standards and Technology (NIST) in developing and implementing the National Cybersecurity Online Informative References (OLIR) Program, an effort to standardize references and make them more consistent, organized, and useful to cybersecurity practitioners.

- Assisting NIST efforts to update the NIST Cybersecurity Framework to version 2.0.
- Sponsoring multiple webinars/technology summits and sharing thought leadership content to promote greater understanding of federal Zero Trust Cybersecurity Principles.
- Partnering with the National Initiative for Cybersecurity Education to update the National Cybersecurity Workforce Framework.
- Providing subject-matter expertise and project management capabilities to support the development and update of multiple standards and guidelines addressing cybersecurity, identity management, and encryption.
- Developing a replicable Security Operations Center (SOC) model featuring continuous monitoring of information security operations, robust privacy programs, and information system security risk management.
- Operating SOCs in various federal agencies and accumulating a solid record of performance.
- Participating in major digital transformation efforts that make cybersecurity a centerpiece of federal modernization efforts.

Electrosoft is proud of its accomplishments and is confident that its contract awards and positioning on many federal cybersecurity-related BPAs, IDIQs, and multiple award schedules will only serve to deepen our expertise in the months and years to come.

Contact Us

To learn more information about Electrosoft and our capabilities, contact us at info@electrosoft-inc.com.

About Electrosoft

Electrosoft delivers a diversified set of technology-based solutions and services differentiated by thought leadership and innovation. Fueling the success of our government and commercial customers since 2001 through outstanding value and trust, we couple our domain knowledge and experience with proven, mature management practices to deliver the right solutions on time and within budget. These practices include an ISO 9001:2015 registered Quality Management System (QMS) and Capability Maturity Model Integration (CMMI) Level 3 assessed processes. Headquartered in Reston, Virginia, Electrosoft is an 8(a) certified Small Disadvantaged Business (SDB) and an 8(m) certified Economically Disadvantaged Woman-Owned Small Business (EDWOSB). For more information about Electrosoft, visit our website at www.electrosoft-inc.com.