4 Ways Artificial Intelligence Can Fortify Cyber

Many devices in the IoT ecosystem remain unprotected.

Kevin McCaney
Mon, 10/30/2017 - 13:20

Cyber news in recent weeks highlighted the accelerating cycle of attack and counterattack that goes on in the alleyways of the web. It also offers clues to how artificial intelligence systems can help keep cyberthreats from doing extensive damage.

This month, a botnet was reported to be quietly but quickly spreading among internet of things devices around the world, with the potential to “take down the internet,” at least temporarily, by using millions of compromised devices to launch distributed denial-of-service attacks. Dubbed IoTroop, as well as the more Halloween-themed Reaper, the botnet had conscripted at least 2 million devices in
more than a million organizations as of Oct. 19, according to Check Point Research, which first identified it.

-- Sign up for our weekly newsletter to receive the latest analysis and insights on emerging federal technologies and IT modernization.

For the moment, IoTroop is laying low, in what Check Point described as the calm before the “next cyber hurricane.” Another security firm, NewSky Security, reported hackers had been developing attack scripts for the botnet. Reaper appears to be a more sophisticated attack tool from the same group that last year used a botnet worm called Mirai to launch a DDOS attack that left some major websites — including Twitter, Netflix and The New York Times — offline for several hours.

For government and other organizations looking to protect their networks, data and uptime, this development, sadly, is business as usual.

Threats are always creeping around the internet below the radar of most people, avoiding attention until it’s too late. A day after Check Point’s disclosure about IoTroop, for instance, the Homeland Security Department’s US-CERT and the FBI warned about an advanced persistent threat “targeting government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors.” US-CERT said the intrusion campaign was used to gain access to the networks of major players in the energy sector. It was a pretty routine announcement.

Attacks such as IoTroop can often be mitigated once identified. The vendors of targeted devices have been issuing patches to fix the vulnerabilities in their devices. But the attackers behind IoTroop also are updating their exploits, potentially leading to an ongoing loop of software fixes.

The biggest problem is that many devices, particularly those connected to the IoT, are largely left unprotected in the first place. Mirai spread by exploiting manufacturers’ default user names and passwords to gain access, while Reaper targets unpatched vulnerabilities.

What are some of the ways AI can help in this accelerated cycle?

**Automation**
Talking about AI in cybersecurity for the moment mostly means talking about machine learning, a subset of AI in which machines can learn from example and reach conclusions or take actions they have not been specifically programmed for. Automation increases the speed and breadth of a system, enabling it to handle the cloud-based big data techniques being employed to counter cyber crime. The learning aspect helps systems recognize the variety of methods employed by phishing or other malware attacks. It also can help in isolating malware that has entered a network or in identifying the changes in normal network behavior when malware executes.

**Threat Detection and Response**

Speed is of the essence in fending off an attack or mitigating its damage — and the closer to doing it in real time, the better. AI and machine learning can help by automating and refining the process. Vectra Networks surveyed 459 IT pros at last summer’s Black Hat conference about their organization’s security operations centers. The upshot from Vectra’s results: When comparing detection and remediation times among three groups — teams of 10 or more analysts without AI, AI-only systems and teams of 10 or more analysts working with AI — Vector found AI-only systems responded quicker than human-only teams, but the best detection and remediation times came from teams of analysts working with AI.

**IoT Security**

Devices on the internet of things — such as medical monitors, weather gauges and cameras targeted by Mirai and Reaper — are typically low-power devices without much processing capacity, which can make them difficult to secure through conventional security techniques. But AI and machine learning algorithms are being developed to monitor IoT devices to detect signs of unusual behavior.

**Keeping Pace**

Information technology, being by nature readily available, cuts both ways. The history of the internet demonstrates that — the first computer worm turned up in 1988, when the internet was still the research-oriented Arpanet and consisted of 88,000 computers. Quantum computing is still largely on the drawing board, but the
National Institute of Standards and Technology is already anticipating quantum computing attacks on current encryption standards. Likewise, with artificial intelligence. Cybersecurity experts say hackers already use basic AI techniques and expect them to leverage more advanced AI to customize attacks or make them more adroit at avoiding detection. Future network security may depend on fighting AI with AI.

View printer friendly version
Eye on AI
Artificial Intelligence
AI
cyber