

<https://www.darkreading.com/vulnerabilities---threats/cybersecurity-an-asymmetrical-game-of-war/a/d-id/1329728?>

8/28/2017

10:30 AM



Hal Lonas

## Cybersecurity: An Asymmetrical Game of War

**To stay ahead of the bad guys, security teams need to think like criminals, leverage AI's ability to find malicious threats, and stop worrying that machine learning will take our jobs.**

In the cybersecurity industry, we've all heard the old adage, "We have to be right 100 percent of the time. Cybercriminals only have to be right once."

It may be daunting, but it's the reality in which the cybersecurity industry lives every day. We're facing an asymmetrical game of war and, unfortunately, we're up against an army of cybercriminals with a vast arsenal of weapons at their fingertips.

As in other combat arenas, asymmetrical warfare in cyberspace describes a situation where one side only has to invest modestly to achieve gains, while the other side must invest heavily to maintain an adequate defense. In the cybersecurity industry, the authors and promoters of malware and ransomware would be the former, while the security industry and potential victims make up the latter. This lopsided investment of time and resources is what makes this war asymmetrical.

Let's take the recent WannaCry ransomware attack, for example. It was a simple enough form of malware, however it took many by surprise. Through a unique combination of stolen technology and propagation, it was able to land on more than 400,000 machines — all with minimal effort on the part of the perpetrators.

Cybercriminals can afford to be creative, innovative, and test new attacks. Meanwhile security teams invest their resources in creating layers of cybersecurity defenses and basics like network segmentation and phishing education.

And here's a scary thought: what will happen when cybercriminals focus their energies on leveraging artificial intelligence (AI)?

AI in the wrong hands could cause an explosion of network penetrations, data theft, and a spread of computer viruses that could shut down devices left and right. It could lead to an AI arms race, with unknown consequences. Those little clues that give us hints that an email or web site aren't really what they claim to be can be cleaned up by a sufficiently smart AI capability. And that's scary.

While there is some machine power in polymorphic malware — malware that morphs when it lands on a new machine — this type of malware doesn't evolve every day. Ransomware took off a few years ago, and it hasn't changed much since then. We are seeing victims fall prey to the same types of attacks over and over again. Cybercriminals are still able to create complete chaos with their tried-and-true tools.

While we can't always predict what cybercriminals will try next, some of us are already leveraging AI and machine learning to stay ahead of them. It's not a silver bullet, but machine learning is fast-becoming an important, possibly essential tool for keeping ahead of, or at least quickly detecting, the latest types of attacks. It can improve security by looking at the network on an ongoing basis and leveraging a threat research team's abilities to create a sum greater than its parts. It sets a baseline to help you detect anomalous behavior. But to stay ahead of the bad guys, the security industry needs to accomplish a few things:

First, we need to think like cybercriminals. Their main motivation is simple — money. They're constantly thinking about what small action they can take to produce a large outcome, hence the popularity of phishing. They can push out millions of emails with relative ease, send victims to a short-lived site and reap big benefits. Cybercriminals may tweak their approach, for instance, impersonating technology companies instead of financial institutions (as we found in our [2017 Threat Report](#)), but the mechanisms remain the same. If we leverage machine learning to assist in the mundane or routine tasks of tracking and classifying, our creative minds can be free to think like criminals and come up with out-of-the-box solutions to the next attack.

Second, we need security products to incorporate AI into solutions that truly take advantage of its inherent advantages to find malicious threats. These solutions must incorporate intelligence from the best threat researchers and models ready to analyze data and find threats that are coming into businesses today. These solutions can be generic or vertical-specific. If we can create programs for more companies to leverage, we will get a leg up on cybercrime.

Finally, we need not fear that machine learning will take our jobs. The real threat comes from not utilizing machine learning. Such avoidance forces your best researchers to complete tedious work instead of being creative and innovative, dreaming up ways to anticipate new forms of attack and protect against them. Machine learning provides supplemental help so that threat researchers can work on

bigger issues. And because the human touch is essential to monitoring and shaping machine learning models, the result is a net increase in job creation.

If we want to even the playing field, we need to embrace machine learning to create a more secure world for everyone. While cybercriminals may not widely leverage machine learning today, it's only a matter of time before they catch up. And when that day comes, security teams everywhere need to be prepared.

[https://www.darkreading.com/author-bio.asp?author\\_id=4806](https://www.darkreading.com/author-bio.asp?author_id=4806)

## **Profile of Hal Lonas**

**Chief Technology Officer, Webroot** Member Since: 8/15/2017

Author

News & Commentary Posts: 1

Comments: 1

Hal Lonas is the chief technology officer at Webroot, a privately held internet security company that provides state-of-the-art, cloud-based software as a service (SaaS) solutions spanning threat intelligence, detection and remediation. Previously the senior VP of product engineering for Webroot, Lonas has 25+ years of experience in enterprise software and engineering. He joined Webroot via the acquisition of BrightCloud, where he was a founder and VP engineering. Lonas has held key engineering management positions with Websense (WBSN), ADP and others, and has co-authored several patents. He holds a Bachelor of Science in Aeronautics and Astronautics from MIT.