93 Percent of Cybersecurity Researchers Say Non-Malware Attacks Pose More Risk to Businesses than Commodity Malware, Carbon Black Research Finds

Submitted by: C8 Consulting
Tuesday, 28 March 2017

---

87 percent of cybersecurity researchers say they don’t yet trust artificial intelligence (AI) and machine learning (ML) to replace human decision making in security

Maidenhead, UK.—March 28, 2017 — Carbon Black (https://www.carbonblack.com/), the leader in next-generation endpoint security, today announced the results of its latest research report, “Beyond the Hype,” (https://www.carbonblack.com/2017/03/28/beyond-hype-security-experts-weigh-artificial-intelligence-machine-learning-non-ma
which aggregates insight from more than 400 interviews with leading cybersecurity researchers who discussed non-malware attacks, artificial intelligence (AI) and machine learning (ML), among other topics.

The results were definitive, pointing to the following trends:

- The vast majority (93%) of cybersecurity researchers said non-malware attacks pose more of a business risk than commodity malware attacks.

- Nearly two thirds (64%) of cybersecurity researchers said they’ve seen an increase in non-malware attacks since the beginning of 2016. There non-malware attacks are increasingly leveraging native system tools, such as WMI and PowerShell, to conduct nefarious actions, researchers reported.

- AI is considered by most cybersecurity researchers to be in its nascent stages and not yet able to replace human decision making in cybersecurity. 87% of the researchers said it will be longer than three years before they trust AI to lead cybersecurity decisions.

- Three quarters (74%) of researchers said AI-driven cybersecurity solutions are still flawed.

- 70% of cybersecurity researchers said ML-driven security solutions can be bypassed by attackers. Nearly one-third (30%) said attackers could “easily” bypass ML-driven security.

- Cybersecurity talent, resourcing and trust in executives continue to be top challenges plaguing many businesses.

“Based on how cybersecurity researchers perceive current AI-driven security solutions, cybersecurity is still very much a ‘human vs. human’ battle, even with the increased levels of automation seen on both the offensive and defensive sides of the battlefield,” said Carbon Black Co-founder and Chief Technology Officer, Michael Viscuso. “And, the fault with machine learning exists in how much emphasis organisations may be placing on it and how they are using it. Static, analysis-based approaches relying exclusively on files have historically been popular, but they have not proven sufficient for reliably detecting new attacks. Rather, the most resilient ML approaches involve dynamic analysis - evaluating programmes based on the actions they take.”

In addition to key statistics from the research, the report also includes a timeline of notable non-malware attacks, recommendations for incorporating AI and ML into cybersecurity programs and an “In Their Own Words” section, which includes direct quotes from cybersecurity researchers and unique perspectives on the evolution of non-malware attacks.

Said one cybersecurity researcher: “Non-malware attacks will become so widespread and target even the smallest business that users will become familiar with them. Most users seem to be familiar with the idea that their computer or network may have accidentally become infected with a virus, but rarely consider a person who is actually attacking them in a more proactive and targeted manner.”

For a full look at the Carbon Black research, click here
(https://www.carbonblack.com/2017/03/28/beyond-hype-security-experts-weigh-artificial-intelligence-machine-learning-non-ma

Methodology

For this report, Carbon Black interviewed 410 security researchers in late December 2016 and early January 2017. Two screening questions determined eligibility. Participants were required to work as researchers in IT, engineering or security operations in one of the following roles for at least one year: security engineer/analyst; security executive (CISO, CSO); security director; incident responder; security consultant; security operations centre (SOC) analyst); security data scientist, pen-tester; or threat researcher. Participants currently employed by security vendors,
were disqualified from participating.

About Carbon Black

Carbon Black is the leading provider of next-generation endpoint security. Carbon Black’s Next-Generation Antivirus (NGAV) solution, Cb Defense, leverages breakthrough prevention technology, streaming prevention, to instantly see and stop cyberattacks. Cb Defense uniquely combines breakthrough prevention with market-leading detection and response into a single, lightweight agent delivered through the cloud. With more than 7 million endpoints under management, Carbon Black has more than 2,500 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks.

Contact:

Contact:
Paula Elliott
C8 Consulting
paula@c8consulting.co.uk
0118 949 7736

Michael Bartley
C8 Consulting

michael@c8consulting.co.uk
0118 949 7750