Daily Journal
Saturday, October 31, 2020 | Morning e-Edition

New AI Technology Mimics Thousands of Hackers Trying to Break into an Organization, Launched by FireCompass

Oct 14, 2020 Comments

SaaS platform for Continuous Automated Red Teaming (CART) to proactively identify security blind spots before hackers do

BOSTON, Oct. 14, 2020 /PRNewswire/ -- FireCompass today unveils its new artificial intelligence powered Continuous Automated Red Teaming (CART) platform that mimics thousands of hackers trying to break into an organization. The solution enables organizations to launch continuous safe attacks to identify blind spots before hackers do. Created by a team of serial cybersecurity entrepreneurs, FireCompass' product is already being used by top companies, including Sprint (now a part of T-Mobile), Security Innovation and others spanning multiple industries.

hackers do. Created by a team of serial cybersecurity entrepreneurs, FireCompass' product is already being used by top companies, including Sprint (now a part of T-Mobile), Security Innovation and others spanning multiple industries.

A hack is executed every 39 seconds and impacts one in three Americans every year. According to Gartner, "Nation-state actors and criminal organizations operate with a level of sophistication that surpasses the preventative and detection capabilities of most security and risk management teams."

"Organizations typically conduct security testing only a few times a year on a partial list of online assets, excluding shadow IT unknown to security teams. Meanwhile, hackers are always attempting attacks on the entirety of their assets," said Bikash Barai, Co-Founder of FireCompass. "At FireCompass, our vision is to make Continuous Automated Red Teaming (CART) available to all so that organizations can discover and test all their assets at all times – just like real attackers do."

FireCompass is reinventing traditional red teaming using the power of AI and SaaS. The solution runs continuously without the need for software, hardware or additional employee resources. It indexes the deep, dark and surface web using similar reconnaissance techniques as nation-state actors. The platform automatically discovers an organization's ever-changing digital attack surface, including unknown exposed databases, cloud buckets, code leaks, exposed credentials, risky cloud assets and open ports, etc. The attack engine then launches multi-stage attacks, which includes network attacks, application attacks and social engineering attacks, on the discovered digital surface to identify attack paths that are otherwise missed by conventional tools.

FireCompass' CART uniquely combines Attack Surface Management (ASM), and multiple security testing technologies, eliminating the need for multiple tools and significant manual effort. With FireCompass, scans that once took weeks and months can now be completed in hours or days. FireCompass' key capabilities include:

Continuous Automated Red Teaming (CART) Continuous safe attacks to test the effectiveness of security investments and discover security blind spots.Attack Surface Management (ASM) & Shadow IT Discovery Identification of orphaned domains/subdomains, risky IPs, exposed database/cloud buckets, code leaks, leaked credentials, exposed test/pre-production systems and Shadow IT risks.Ransomware Attack Surface Monitoring Internet scans to discover risky assets that can be exploited by malware and ransomware.

"To our surprise, FireCompass has exceeded our expectations," said a Risk Manager at Sprint (now a part of T-Mobile). "The tool has demonstrated reliability in the findings, and FireCompass has proven to be a valuable service provider."

Founded by industry veterans Bikash Barai, Nilanjan De and Priyanka Aash, FireCompass is backed by prominent investors and venture capitalist funds. The founders' previous endeavors include iViZ, which was acquired by Cigital/Synopsys (NASDAQ: SNPS) and CISO Platform, one of the largest communities of CISOs and security executives in the world. The team has multiple patents in IT security and have broken the best cybersecurity products, including McAfee, Microsoft Bit Locker, Sophos, AVG etc.

"FireCompass, with its veteran team and deep domain expertise, is well positioned to change the way the industry does red teaming today," said Som Pal Choudhury, FireCompass Investor, Board Member, and Partner at Bharat Innovation Fund.

To learn more about FireCompass, or to get a free analysis of your organization's attack surface from a hacker's point of view, visit www.firecompass.com.

About FireCompass

FireCompass is a SaaS platform for Continuous Automated Red Teaming (CART) and Attack Surface Management (ASM). FireCompass continuously indexes and monitors the deep, dark and surface web using nation-state grade reconnaissance techniques. The platform automatically discovers an organization's digital attack surface and launches multi-stage safe attacks, mimicking a real attacker, to help identify attack paths that are otherwise missed by conventional tools. FireCompass is led by serial cybersecurity entrepreneurs and backed by prominent investors and venture capitalist funds. To learn more, visit www.firecompass.com.

Media Contact Kat Knox Matter for FireCompass firecompass@matternow.com

View original content to download multimedia: http://www.prnewswire.com/news-releases/new-ai-technology-mimics-thousands-of-hackers-trying-to-break-into-an-organization-launched-by-firecompass-301152037.html

SOURCE FireCompass, Inc.