SLASHNEXT

Press Release

NOVEMBER 7, 2017

SLASHNEXT

SlashNext Launches Revolutionary Internet Threat Protection System to Displace Aging Signature and Sandbox Technologies

Internet Access Protection System Blocks Social Engineering and Phishing Attacks by Putting a Human-like Machine Against Attackers

PLEASANTON, Calif., Nov. 7, 2017 – SlashNext, provider of third-generation Internet security solutions, today announced the company's broad market release of the SlashNext Internet Access Protection System to protect organizations from cross platform social engineering and phishing, malware, exploits and callback attacks. The system goes beyond first generation signature-based and second generation sandbox-based technologies and deploys human-like intelligence and cognitive thinking to stop these Internet attacks targeting unsuspecting employees as their entry points.

Today, automatic software updates and enhanced security offered in modern browsers prevent most software exploits such as buffer overruns and privilege escalations, but social engineering and phishing attacks exploit human vulnerabilities by deceiving victims into taking actions that will breach their company and their connected client's networks. In fact, social engineering and phishing attacks are the fastest growing security threat for organizations today, representing 43% of all Internet access threats, nearly double that of malware and viruses, according to the Verizon Data Breach Digest.

"Social engineering and phishing attacks are becoming the prime attack vector since cyber-criminals realize unsuspecting people create the easiest way to bypass traditional anti-virus and sandbox technologies," said Fran Howarth, Senior Analyst with Bloor Research. "A new approach to Internet threat detection is needed. SlashNext answers that need, using cognitive computing technologies that mirror human learning to enable systems to stop Internet threats targeting a variety of operating systems such as Windows, Linux, OSX, Android and iOS."

"For years, we've relied on a well-defined boundary to protect our assets, but things are changing. With the rapid pace of change in modern advanced threats, employees cannot be expected to evaluate a particular threat's risk, and information security teams are hard-pressed to stay abreast of all new threat information and rethink their security approach," said Raun Nohavitza, vice president of IT at Centrify. "To address this challenge, we deployed the SlashNext Internet Access Protection System. It allows us to apply broad threat intelligence and the cumulative expertise of seasoned security experts to automatically block malicious activity that would otherwise reach our employees."

In a recent review of more than 50 deployments, SlashNext identified dozens of instances of zero-day social engineering and phishing, exploits and malware attacks that had gone undetected by the customers' existing firewalls, sandbox, data-exfiltration prevention tools and next gen anti-virus software.

"The ever-changing threat landscape we face today requires a revolutionary approach to security -- one that is built upon an entirely new mindset that is beyond and independent of existing technologies that we've seen," said Promod Haque, Senior Managing Partner of Norwest Venture Partners. "SlashNext represents the next generation of security through its unique ability to think outside the sandbox."

The SlashNext solution is deployed via a simple, 20-minute installation process that requires zero policy configuration or ongoing maintenance. Once installed, the system employs a patent pending threat protection technology that includes:

- A cross platform protocol analysis engine that processes gigabits of Internet bound traffic in real-time to extract a complex set of artifacts. These artifacts are essentially the telltale signs of a malicious attack
- The artifacts are further processed by a cognitive computing machine that uses massive cloud computing power to convert these features into clear Indicators of Compromise (IOCs)
- The IOCs are then handed over to hundreds of reasoning engines that behave like a team of decision-makers working together to reach a single verdict, "100% Malicious" or "Not Malicious"
- Once a decision is made, the final outcome is shared back with all the decision makers as part of a peer feedback mechanism that gives the system its unique self-learning capability. This process is a huge contrast to machine learning based systems that need to be manually trained repeatedly by data scientists and an exact replication of a team of human threat researchers who process raw data, compile evidence, analyze using cognition, discuss and then collectively reach a decision.

"The last few years have seen an explosion of social engineering and phishing attacks that don't rely on malware or exploits to penetrate defenses. That's left businesses urgently in need of an innovative new approach to security that goes far beyond the sandbox," said Gaurav Garg, Founding Partner of Wing Venture Capital. "By harnessing the power of cognitive computing in its system, SlashNext is taking cyber defense to a completely new level."

Availability

The SlashNext Internet Access Protection System is available immediately in North America via a subscription-as-a-service model that includes product support and built in threat intelligence.

Blog by CEO Atif Mushtaq: www.slashnext.com/blog

About SlashNext

SlashNext has reinvented Internet threat prevention systems with a new approach to protecting users and systems every time they connect to the Internet.

The SlashNext Internet Access Protection System leverages cognitive computing, a process that mimics how the human brain senses, reasons and responds to stimulus, to process and detect complex and interlinked Internet access attacks including social engineering and phishing, malware, exploits and callbacks.

SlashNext CEO Atif Mushtaq founded the company after serving nine years as a senior scientist for FireEye, where he was a leading architect of the company's core malware detection system based on signatures and sandbox based technologies. Atif has been at the forefront in the fight against cybercrimes and has worked with law enforcement and other global organizations to take down some of the world's biggest cyber crime networks. In 2012, his efforts took down one of the largest email spam networks operating out of Russia, causing the worldwide spam level to drop by 50% in a single day.

SlashNext received $9 million in Series A funding in April from Norwest Venture Partners and Wing Venture Capital. Norwest Venture Partners has a track record of investing in cutting edge cyber security companies including FireEye, the maker of world's first sandbox based malware detection technology.

To learn more about SlashNext and to keep up on the latest news, visit: www.SlashNext.com and follow @slashnextinc on Twitter.

Media Contact

Lumina Communications
SlashNext@LuminaPR.com
800-930-8643

SLASHNEXT.

(800) 930-8643
info@slashnext.com
www.slashnext.com
4301 HACIENDA DRIVE, STE 550 PLEASANTON, CA 94588