telecomkh.com

http://www.telecomkh.com/en/internet/products-and-services/8670
Ixia’s ThreatARMOR delivers Zero-Day Malware Immunity
29/09/16

Date: ***Thu, 09/29/2016 - 13:35***

Automatically blocks malware/ransomware mutations

Areg Alimian, Senior Director Solutions Corporate Marketing, Ixia, at NetEvents 2016 Global Press & Analyst Summit, Silicon Valley, CA

PHOTO / telecomkh.com

Ixia, a leading provider of network testing, visibility, and security solutions, announced that the company’s ThreatARMOR™ solution, a key component of Ixia’s Security Fabric™, adds Zero-Day Malware Immunity™ (ZDMI), which blocks mutated versions of malware that use sophisticated obfuscation techniques to evade detection by signature-based security engines. The Ixia Security Fabric provides robust resilience, context-aware intelligent data handling, and security intelligence, ensuring the right data gets to the right tools every time even when encrypted, and enhancing the performance of existing security tools.

Hackers continue to mutate and mask malware in innovative ways. In 2015, they launched more than 1 million pieces of malware every day. Researchers scramble to bring new products to market to counter these ever-evolving—or, mutated—threats. These defenses, while powerful, have to process exponential increases in threats every year. The Ixia Security Fabric helps relieve those burdens by blocking zero day mutations at their source.

Powered by feeds from the Ixia Application and Threat Intelligence Research Center, the Security Fabric can completely filter out unknown and zero-day attack mutations by blocking them based on their IP launch source rather than analyzing those millions of attacks one at a time. By reducing bad traffic and their associated alerts, the Security Fabric makes existing security tools and teams more effective.

Zero-Day Mutations

A recent example of a Zero Day Mutation, in which malware changed to escape detection by signature-based antivirus and intrusion detection systems, was a variant of ransomware called Locky. Zero-Day Mutations often target users through emails containing a document with macros. When the user opens it, the macro connects to the attacker's remote server to download the ransomware which enabled Locky infections to hit 100,000 per day this year.

Ixia's Threat Intelligence

Ixia takes a comprehensive approach to strengthening applications with security solutions that are kept up to date with a feed from the company's Application Threat Intelligence (ATI) Research Center, which is continuously updated. The ATI Research Center performs both manual and automated analysis of malware and techniques used by hackers to compromise networks, 24x7, 365 days a year.

"Ixia's ATI Research Center captures and analyzes thousands of new malware samples, including mutations, daily," stated Steve McGregory, Senior Director of Application and Threat Intelligence at Ixia. "We pay particular attention to their networking activity – what domains they search for, what sites they connect to for downloading new instructions or executables, and where they send exfiltrated data. We cross-reference all of those, and plug them into our machine learning and big data analytics engine to help ensure that our customers' networks are protected."

Zero-Day Malware Immunity with ThreatARMOR

ThreatARMOR leverages the Ixia ATI feed to protect customers from malicious sites and reduces security alerts by using the attack's IP address to block it. This means that even if a user accidentally opens a malicious document, the ransomware download attempt is blocked, nullifying the attack before other protections are even aware of the new threat.

ThreatARMOR delivers Zero Day Malware Immunity because it is not a signature-based solution. It blocks attacks based on an expansive "Rap Sheet" cloud database which contains up-to-date information about the proliferation of malicious IPs currently in use. Only sites with extensive proof of malicious activity are blocked, and clear on-screen evidence is provided by ThreatARMOR's Rap Sheet.