New Security Innovation Fully Protects Against Highly Exploited Application Weakness

Waratek's Name Space Layout Randomization (NSLR) Makes Java-Based Application Vulnerabilities Impossible to Exploit

DUBLIN and ATLANTA – Jan. 25, 2016 – Waratek, a virtualization-based application security company, today announced that it has developed a new application security technique called Name Space Layout Randomization (NSLR) that neutralizes code injection attacks. The first of its kind, Waratek NSLR shares some principles used in Address Space Layout Randomization (ASLR), a memory-protection process for operating systems. The Waratek Application Security Platform now ships standard with NSLR protection built-in.

According to the 2016 Verizon Data Breach Investigation Report, web application attacks are the top source of data breaches today. To be successful, a code injection exploit needs to know the exact names of classes and packages that must be invoked. By randomizing Java class packages, Waratek NSLR prevents any code injection exploit from finding its targets.

"Current approaches for protecting against known code injection attacks involve applying a patch, fixing the vulnerability or disabling the flawed functionality, if possible. Alternatively, web application firewalls can mitigate some threats, but are often plagued by false positives," said John Matthew Holt, CTO of Waratek. "Waratek NSLR provides absolute protection against both known and unknown code injection vulnerabilities with zero false positives, and does not require making any changes to the application. It is a logical extension of the application protection capabilities we already provide using virtualization."

Waratek NSLR hardens the Java Virtual Machine by randomizing the JDK namespace, which prevents code injections from executing regardless of the vulnerability (known or zero-day) that is being exploited. This innovation was made possible by Waratek's virtualization-based implementation in an application's runtime.

For example, with Waratek NSLR enabled, the *java.lang.System* class will be randomized and renamed. Therefore, any exploit that attempts to invoke *java.lang.System* will fail, since it will not know the new randomized package name. Since Waratek NSLR generates a unique package name every time the JVM boots, it is impossible for exploit code developers to guess the new names.

The randomized host package names are transparent to the guest applications and cannot be viewed or accessed from the Java Virtual Container (JVC) created by the Waratek Application Security Platform. In addition, Waratek NSLR prevents brute force attacks by using 96-bit to 1024-bit names, which would likely require several thousands of years to crack. Finally, Waratek NSLR identifies when a code injection attack is attempted and logs the details as a security event.

Waratek NSLR is now available internationally with the latest version of the Waratek application security platform.

About Waratek

Waratek is a pioneer in the next generation of application security solutions. Based on patented virtualization technology, Waratek's Application Security Platform is highly accurate, easy to install, simple to operate and does not slow application performance – while providing protection against known and unknown vulnerabilities in current and legacy software in ways competitors cannot.

Waratek was recently named 2016's Best Application Security Solution by *Government Security News* and is the winner of the 2015 RSA Innovation Sandbox Award. JavaWorld notes that "Waratek is the only vendor that can boast of a large-scale production deployment with a Tier 1 global investment bank, the most significant deployment of (runtime protection) that exists for Java technology today."

Waratek is based in Atlanta, Georgia and Dublin, Ireland. For more information visit www.waratek.com

Media Contact:
Mike Gallo for Waratek
Lumina PR
212-239-8594
Mike@LuminaPR.com

# # #