waratek

Application Security Platform

RSAC Innovation Sandbox 2015 WINNER

Making Code Injections Attacks Impossible

Applications today are generally protected by ineffective Web Application Firewalls (WAFs) and other tools that rely heavily on instrumentation or filters to guess if a call is a malicious attack or a permissible action. Such heuristic-based approaches often produce false positives at an unacceptably high rate.

Code injection attacks – Number Six on MITRE's list of CVEs with more than 2000 associated vulnerabilities - exploit specific application vulnerabilities. A malicious attacker who attempts to introduce a Code Injection exploit in Java needs to know the exact names of classes and packages to be invoked.

Making the Java class packages randomized, would make any exploit unsuccessful; in effect, it would defeat *any code injection exploit*.

Introducing Name Space Layout Randomization - NSLR

Name Space Layout Randomization or NSLR is the equivalent of Address Space Layout Randomization (ASLR) for Java-based applications. Developed by Waratek, NSLR hardens the Java Virtual Machine (JVM) by randomizing the JDK namespace (Java packages), which makes code injection exploits so difficult to execute that they become unfeasible.

For example, with NSLR enabled, the *java.lang.System* class will be randomized and renamed to something like *java$85rbuLjHNERijUhN.lang.System*. Any exploit that tries to invoke *java.lang.System* will automatically fail. For attackers to successfully execute an attack they would need to know the randomized package name. For additional protection Waratek randomizes the package each time the JVM boots.

Attempts to brute force the system and retrieve the randomized package name will not work, either. Waratek's standard configuration includes NSLR with a minimum level of security at 96-bit names, which would likely require several thousand years to crack the encryption. Names can be randomized up to up to 1024 bits.

Current and emerging application security technologies rely on heuristics that generate False Positives. Not Waratek. Our patented technology is based on virtualization techniques that determine if an operation is an attack or a permissible request with 100% accuracy.

If we produce a false positive, we'll give you $10,000 for each instance.

Schedule your free demonstration or Proof of Concept at Waratek.com

JAVAWORLD SOLUTIONS FOR JAVA DEVELOPERS

"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." ***JavaWorld,*** Oct 20, 2016

Highly Accurate | Easy to Install | Simple to Operate

About Waratek

Waratek 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.

Waratek takes your application security program beyond a WAF without using heuristics. Based on patented virtualization technology, Waratek's application security platform produces zero false positives, requires no code changes, tuning or instrumentation, and takes minutes to install - providing instant protection from the OWASP Top Ten as well as Zero Day attacks. These are benefits that cannot be provided by your current WAF or emerging technologies like RASP using instrumentation or filters.

Named 2016's Best Application Security Solution by Government Security News, Waratek is the winner of the 2015 RSA Innovation Sandbox Award.

Waratek $10,000 False Positive Guarantee Terms and Conditions

1. Waratek offers protection against vulnerabilities included in the 2013 Open Web Application Security Project (OWASP) Top Ten list of security flaws.

2. In the event Waratek identifies a permissible action as a false positive on a live system, Waratek will issue a credit in the amount of $10,000 per unique event. For example:
   a. If Waratek identifies a permissible action as an impermissible "A1-Injection" as classified by the 2013 OWASP Top Ten, you are entitled to a $10,000 credit for the event.
   b. If Waratek subsequently identifies a permissible action as an impermissible "A3 – Cross Site Scripting," you are entitled to an additional $10,000 credit.

3. Any credit issued under this guarantee is not redeemable or convertible to cash.

4. Credits must be claimed against any balance due upon the next scheduled invoice under an existing contract or as a credit against the first payment in any contract renewal, whichever comes first.

5. Any false positive must be reported to Waratek within 72 hours of the event and be verified to qualify for the credit(s) available under this guarantee.

6. Waratek reserves the right to cancel or modify this guarantee at any time upon timely notice to customers. Credits issued prior to any program modification will not be affected by any subsequent program changes.