Xcitium ZeroDwell Brings Zero Trust to the Endpoint and Stops Unknown Malware

EMA IMPACT BRIEF

Abstract

Comodo Cybersecurity, an American company headquartered in New Jersey that specializes in endpoint protection, recently announced its rebrand under the name Xcitium. Coinciding with the rebrand is their release of ZeroDwell Containment technology designed to neutralize ransomware, malware, and cyber-attacks.

Background – Why Traditional Malware Detection and Response are Not Enough

With over 450,000 new malware samples per day, vendors simply cannot keep up. Not only does this present a challenge in the man-hours needed to analyze and create signatures for this tremendous number of daily threats, but it also creates logistical challenges in providing accurate detection signatures while keeping the size of those signatures manageable for organizations to deploy. Furthermore, traditional antivirus technology requires knowledge of the malware or its behavior. Malware authors are now writing their software to evade antivirus and intrusion detection, even through heuristic and behavior-based detection.

The fact of the matter is, the security industry is struggling to keep up, and the common problem in all current antivirus technologies is that they rely on detection as the first step. Xcitium solves that problem by eliminating detection as the first step, instead relying on execution containment of unknown applications. This unique approach removes the implicit trust of applications until they're verified as safe, without blocking user access to the application or interrupting productivity.

Key Ramifications

The following are the key ramifications of Xcitium's release of ZeroDwell Containment:

- Utilizing containment, which is a protection vs. detection technology, organizations can implement proactive defenses of unknown threats. Even new malware created to specifically target an organization will be prevented from infecting systems, without detection signatures.
- User productivity is uninterrupted thanks to ZeroDwell Containment, allowing users to continue using the unknown application while preventing the application from accessing the rest of the system until it can be analyzed. This means no productivity impacts to organizations.
- Real-time scanning through Xcitium's Verdict Cloud gives trusted results regarding the safety of an application, only releasing the application from isolation once it has been verified as non-malicious.

Through leveraging Xcitium's ZeroDwell Containment technology, organizations can avoid productivity impacts of false positive detections while the security team gains peace of mind that malware will be unable to infect the system.

EMA Perspective

Beyond the marketing hype, zero trust is an extremely overused term with different meanings to different vendors. While most zero trust approaches have focused on identity, Xcitium's approach is unique in that it focuses on not trusting software applications, even when user identity is validated. For far too long, information systems have implicitly trusted applications to be legitimate until antivirus or intrusion detection determine otherwise. By eliminating the detection step and automatically treating applications as untrusted until trust is validated, companies establish a much more secure computing environment.

EMA believes that in order to truly make advancements against malware, the cybersecurity industry must embrace novel approaches that do not rely on detection after the fact, but take proactive measures to reduce or even eliminate the risk of infection. Xcitium's approach is a welcome change from traditional malware protection, and EMA believes that organizations should evaluate more proactive measures, such as ZeroDwell Containment.

4213.121422