

Research: AMP (Any Means Possible)

Demonstrating Security by Emulating Real-World Targeted Attacks

Nearly all organizations have data that, if accessed or manipulated by an attacker, would be detrimental to the organization. This may include customer data, internal source code, financial information, or classified material. This data is considered highly sensitive, and invaluable.

Now imagine that a well-funded, well-equipped, and well-motivated attacker group is after the exact set of data that your organization holds. They have an arsenal of effective zero-day exploits, signature-less custom-written malware, and a myriad of skills that can be used to infiltrate your organization through multiple attack vectors, some of which may not even require a computer. How well would your security processes effectively keep your critical data secured under such attacks?

Any Means Possible Methodology

eEye Research offers the Any Means Possible (AMP) penetration testing service. Simply stated, this service effectively emulates the scenario of a nefarious and well-tooled attacker team in order to allow your security posture to be tested in a defense exercise rather than a real-world situation. In the same fashion used by well-skilled attacker groups, eEye Research leverages zero-day exploits, custom-developed malware, and a very diverse skill set that is able to simulate nearly every attack scenario that might occur against your network.

Penetration Testing vs. Auditing

A successful security audit does not prove that your critical data is protected. Rather, it proves that you have put security measures in place that can effectively block the majority of basic attacks that are seen on the web. More often than not, security mechanisms suggested by audits are little more than hurdles for well-educated attacker groups. Unfortunately, the majority of so-called "penetration tests" are little more than point-and-click or tool-driven audits. Although they are still important, they are typically only challenging the low-hanging-fruit of your organization.

Customer-Tailored Penetration Tests

The scope, target ("flag"), and scenarios are at the discretion of the AMP customer. If the customer is most concerned with insider-threats, spear-phishing, or more advanced exploitation scenarios, this can be emulated to the order based on the request of the customer. This allows the customer to dictate the process of the penetration test, and can help them to more effectively implement change based on the results of this engagement.

About eEye Digital Security

Since 1998, eEye Digital Security has made vulnerability management simpler and more effective by providing the only unified vulnerability and compliance management solution that integrates assessment, mitigation, and protection into a complete offering. With a proven history of innovation, eEye has consistently been the first to uncover critical vulnerabilities and prevent their exploit. eEye leverages its world-renowned research to create award-winning solutions that strategically secure critical IT assets and the data they hold. Thousands of mid-to-large-size private-sector and government organizations, including some of the most complex IT environments in the world, rely on eEye solutions to protect against the latest known, unknown and zero-day vulnerabilities.

Free Security Resources

Retina Community: Powered by the renowned Retina Network Security Scanner technology Retina Community is a completely FREE vulnerability assessment solution for up to 32 IPs.

[Download >>](#)

Vulnerability Expert Forum: Monthly webinar that includes analysis on recently announced vulnerabilities.

[Register >>](#)

Zero-Day Tracker: This free resource gives you up-to-date threat info and how to handle each Zero-Day vulnerability.

[View >>](#)

Contact Your eEye Account Manager Today

www.eeye.com/contact | 866.339.3732 | sales@eeye.com



eEye Digital Security®