SCYTHE Automates Security Validation, Red Team/Blue Team Testing

Abstract

Red team/blue team exercises and other adversarial simulations are a great way to test the performance of security solutions, as well as the ability of security teams to respond to different cyber threats and assess where improvements are needed. However, the exercises are costly to conduct with any regularity, especially at scale. GRIMM, a security consulting and penetration testing company, found a way to automate such tests. The result is a new product called CROSSBOW, and a new security startup, called SCYTHE. Both were launched in mid-October 2017.

Event

On October 17, 2017, security consulting and vulnerability assessment provider GRIMM launched a new platform called CROSSBOW. CROSSBOW allows customers to simulate a range of threat campaigns at scale against production infrastructure to assess how well existing defenses and security teams can stand up against such threats. The CROSSBOW platform is made up of a threat catalog of different campaigns found in the wild, and is curated by the new startup's engineers, who reverse engineer the threats they find. These engineers then build templates based on those threats. The threat catalog includes a series of pre-scripted replicas of what specific campaigns do, performing all the same actions as the real threats.

Using a graphical command and control interface, users can create and manage custom campaigns that draw on 30+ modules in the catalog that simulate how real-world threat campaigns work. Users log into the interface and can select the campaigns they want to simulate from a dashboard. Then, a server creates the payload specific to that campaign. Operators can set up a start and end date and time for the campaign, select the communications protocols they want their endpoints to use to communicate with the CROSSBOW server, and a payload that behaves just as the real-world threat would is delivered to the customer's Windows endpoints.

Reporting that integrates into Splunk details the chronology of what happened during the campaign, and provides a summary on the degree of compromise. Reports display all actions taken by the catalog's capabilities modules and their return value, which can be used to measure performance and indicate which security solutions were successful and which failed.

CROSSBOW can be deployed on-premises on a server, or it can be delivered as a SaaS. CROSSBOW leverages "gray infrastructure," which constantly changes domains, IP addresses, and geographies, so the network traffic from each campaign appears to be unique. An API also enables more advanced customers to build their own custom threat campaigns. Although it initially only supports Windows endpoints, plans are in the works to extend testing to Linux, Mac, and mobile endpoints.

Along with the CROSSBOW launch, GRIMM also spun out a new company called SCYTHE to take CROSSBOW to market. GRIMM itself is a security consulting company that provides a range of professional services across multiple threat vectors. Although GRIMM is providing the initial funding for the new startup, it also hopes to attract additional external funding to take CROSSBOW to market in a product-focused company.

Context

Red team/blue team testing has gained popularity over the last year or so as organizations seek to mature their security strategies. Red teams, typically consisting of outside contractors, are employed to find vulnerabilities in technology, people, and processes, so the subject of such testing can improve their defenses before an actual attacker exploits vulnerabilities found during the drills. However, because of the cost and complexity involved in setting up such tests, they can only be done a few times a year—typically only by large or very large enterprises that have a fairly mature security operation in place.

The lack of skills available in the industry to develop exploits from tools such as metasploit or meterpreter to run a red team drill also inspired the creation of CROSSBOW. A small- to medium-sized business may be able to muster such testing every couple of years and perhaps do limited trainings in between. SCYTHE aims to change that equation by bringing a much greater level of automation to the task. The point and click graphical interface is designed so operators need very little training to set up testing. For the most part, they merely need to know which tests they want to run, and GRIMM/SCYTHE will provide some level of guidance for that. This should allow customers to perform more frequent testing exercises in order to improve their organization's security posture against real-world threats.

CROSSBOW can be used on multiple levels to not only train security professionals on how to improve their response to different types of threats, but to train end users on security awareness through staged phishing campaigns. It can also be extended to third-party suppliers who have access to an enterprise's network—if they agree to such testing. This can be a real boon for large enterprises that have the leverage to get supply chain partners to agree to the tests in order to avoid being compromised by partners with a connection into the enterprise network.

EMA Perspective

In some ways, CROSSBOW acts like a virtual red team, but the attacks can be automated at scale. Given the current popularity of red team/blue team exercises, they could attract significant interest and help customers avoid the pitfalls of working with outside contractors. It takes the risk out of dealing with an external red team that may or may not be working in the client's best interest and may or may not have the skills necessary to conduct such drills. Some companies claiming to have red team expertise do little more than extended pen testing. By automating testing of the environment, customers can avoid the management headaches involved in manual testing between two groups who have diametrically opposed tactical objectives.

Of course, there's always some risk in relying on a startup that may or may not have long-term staying power—especially one that is seeking early-round funding. But as the breach headlines continue to stack up, large enterprises quaking at the thought of being the next Equifax will likely downplay that risk. CROSSBOW's development was stirred by a very large enterprise that experienced a significant breach.

Given the ever-changing nature of an enterprise's IT assets and the tendency for configurations to drift, the ability to constantly probe for weaknesses and fix those vulnerabilities in a virtuous circle represents a holy grail for IT security practitioners.