Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 15, Issue 4

Data Breach Emulation Raises the Bar

By: David DeSanto

Your network is under siege. Both the nature of the Internet and hackers' use of automated tools mean that attacks occur around the clock. To ensure that the tools and policies you have in place are sufficient to protect your network and data, you need to continuously assess, validate, and identify any potential weaknesses, so you can address them before they can be exploited. Not all assessment methods are created equal, however. There is a critical difference between methods that rely on emulation and methods that rely on simulation, and data breach emulation methods provide a more accurate assessment of your security posture

Evolving Threat Landscape

There is no such thing as an impenetrable network or invulnerable security. The threat landscape is constantly evolving, so a network that is secure one day may be vulnerable the next. The total annual number of data breaches has risen consistently, and each year seems to crush the previous one in terms of the number of breached or affected accounts. According to Dark Reading, nearly 8 billion information records were exposed in 2017—the result of a record-breaking 5,207 reported data breaches.

Breach incidents aren't cheap, either. The Ponemon Institute found that the average cost of a data breach in 2017 was $3.62 million. The 2017 Cost of Data Breach Study breaks that figure down to an average of $141 per stolen record. That adds up pretty quickly, which is why it is critical to stay one step ahead of the evolving threat landscape by testing your security posture.

Purple Team Assessments

The only way to determine whether your network and data are really secure is to subject them to an attack—but you don't want to wait for cybercriminals to compromise your network. By testing your security tools and policies yourself, you can locate holes in your defenses and identify weaknesses and vulnerabilities that you can resolve or mitigate proactively, before an actual breach occurs.

Penetration testing—or Red Team assessments—have been around for many years. In recent years, organizations have also incorporated the defensive, or Blue Team, components for a more

thorough and realistic assessment, creating a combined “Purple Team” assessment strategy. But many companies only conduct assessments annually or quarterly. Infrequent assessments are certainly better than nothing, but attackers don’t wait to develop new exploitation and attack techniques on an annual or quarterly basis.

You need to assess and validate more frequently. While automated Purple Team assessment tools enable you to verify your security posture continuously, equally important is to assess the right way —which leads us to the difference between data breach emulation and data breach simulation.

Emulation vs. Simulation

On the surface, the terms simulation and emulation seem similar. It’s easy to dismiss or ignore any differences in meaning as a matter of semantics or marketing hype. However, when it comes to Purple Team assessments and validating your security posture, there is a distinct—and important—difference between simulation and emulation.

Let’s start with the actual definition of each word:

- To ***simulate*** something means to create a likeness or a model of it. So a simulated attack is a model of a real attack, created using artificial activity and other props.
- To ***emulate*** something means to imitate or mimic it. So an emulated attack uses real-world tools and techniques to create an actual attack.

Most penetration testing and Purple Team assessment tools rely on data breach simulation. While simulated attacks accomplish the goal of testing your security posture to some extent, they fall short. Data breach simulation attacks use artificial network artifacts and replayed traffic and network activity. The problem is that many security products can see through the attempted deception. They are capable of recognizing fake traffic and activity and therefore discount or ignore it. They either treat the simulated attack as phony or identify it as non-malicious traffic and let the traffic pass through or block it as an invalid network stream. The result is not a comprehensive or valid assessment of how your security will withstand an actual attack. In fact, reliance on simulated attacks can create a false sense of security in situations where the simulated attack is arbitrarily blocked or detected but in real life such an exploit or malware may get through defenses and do damage.

Data breach emulation, on the other hand, leverages tools, techniques, and procedures used by real-world attacks and malware to imitate an actual attack. Emulation uses the exploits, applications, and malware currently used by malicious actors, creating realistic attack scenarios that mimic what your network is likely to experience from a malicious attack.

“Assessing data breach readiness has been expensive, time-consuming and difficult, and plagued with gaps and deficiencies,” says Jon Oltsik, senior principal analyst, Enterprise Strategy Group. “Having the ability to use actual intruder activity on an ongoing basis to assess how live monitoring systems will perform is essential to knowing whether an organization can find an intruder before disaster strikes.”

Security Assessment with Data Breach Emulation

Data breach emulation provides enterprises with a more thorough and accurate assessment of their security posture. But to be effective, the real-world threats must actually be real-world. A good emulation tool relies on a repository of real attack threats that is continually updated to reflect what is happening right now. In other words, rather than relying on replayed traffic or fake network activity to expose your defenses to simulated attacks, effective data breach emulation uses threats that are in fact what an actual attacker puts on the wire.

In addition, useful data breach emulation assessments must use the threat repository in combination with knowledge of the latest emerging threats and experience defending against

current attacks. The threats are important, but so are the techniques and procedures—the methods—on which attackers rely. It is this combination that makes data breach emulation assessment so powerful, providing you with a more thorough and accurate assessment of your security posture.

One new data breach emulation solution on the market is the Spirent CyberFlood Data Breach Assessment. The combination of an internal Security Services team, a Threat Research team, and external partnerships across the threat intelligence community enable Spirent to continuously collect and use a wide variety of real-world attack threats.

A report from 451 Research on CyberFlood's Data Breach Assessment capabilities states that "CyberFlood's ability to model the performance impact of various security events provides a good deal of value to large enterprises with complex network and security architectures. The company continues to increase its value to customers by expanding its capabilities to the attacks most relevant to its customer base, which is exactly what it did with the launch of its breach-emulation feature, which focuses on more sophisticated multi-layer attack campaigns."

The 451 Research team also states that the data breach emulation capability builds on the existing strengths of CyberFlood and extends them to include automated Purple Team assessments. "This allows Data Breach Assessment to perform safe penetration tests from emulated attackers to emulated targets both controlled by CyberFlood, allowing enterprises to perform active monitoring within their networks."

Data Breach Emulation Raises the Bar

To ensure that you're prepared to defend against attackers, it's important to continuously assess and validate network security. Unfortunately, many network security solutions are sophisticated enough to recognize and avoid simulated attacks. Data breach emulation raises the bar by using current, real-world exploits and attack techniques.

If you are evaluating the tools available for performing automated security assessments, understanding the distinction between data breach simulation and data breach emulation will help you make the right choice. Tools that rely on data breach emulation can provide valuable insight into how your security infrastructure will hold up against a real-world attack, making them a superior choice for Purple Team assessments.