cyberflood

Advanced Malware

Applications and Security Test Solutions

Background

According to data compiled by cyber crime coalitions such as Anti-Phishing Working Group, malware has infected nearly a third of the world's computers. What's worse, is the numbers continue to grow as based on ongoing research from Kaspersky, McAfee, AV-Test and others showing over a 600% increase in the number of malware programs in the wild from 2012 to 2017.

Businesses may face long-term impacts such as loss of competitive position or outright organizational failure. Many instances of infection by malware result in advanced persistent threats (APTs) entering the protected network.

Testing malware counter measures with outdated and unrealistic samples is not only ineffective; it's a dangerous business practice. Potentially, one can be exposed to today's more intelligent and nefarious malware. Spirent's CyberFlood Advanced Malware provides current and up to date samples along with hyper-realistic application traffic to properly test and stress security solutions.

A Proper Test and Stress Security Solution

Robust testing of security systems requires test equipment that can generate real malware payloads and emulate network traffic from already-infected systems. A variety of security systems are used to detect and prevent malware. These include:

- Firewalls and network intrusion prevention systems (IPS)
- Unified threat management (UTM) systems
- Content filtering and data loss prevention systems
- In-line sandboxing and advanced AI based malware detection solutions

Newer security technologies on these systems go further and can detect breaches by identifying already infected end-points within the protected network. This is often done using various types of network based behavioral profile analyses.

Even with all these security systems and capabilities in place, malware still manages to infect target systems. In order to stop malware, all security systems must be carefully tested and validated using a wide range of malware-based attacks to ensure they are working properly. Complete testing of security systems also requires a proper testing methodology that considers performance, availability, security and scale. Collectively these four variables, when viewed holistically, provide for reliable test results.

Testing with Malware — Combining Quality & Quantity

Spirent's Advanced Malware testing solution provides the means to verify your network's ability to defend against today's sophisticated malware constructs with an up to date database of malware samples and from a variety of test vectors.

Up-to-date Malware Database

- Testing with a mostly obsolete database of malware is of no use. Spirent continually provides newly-found and zero day malware constructs that are automatically made available for testing via our TestCloud™ content subscription providing thousands of malware and propagation samples for vast test coverage.

Extensive Malware Types

- In addition to providing an ever growing database of malware content, Spirent provides coverage for a wide area of malware types including: Worms—Viruses—Trojans—Spyware—Root Kits—File Infectors—Adware—Bots—Backdoors—and more.

Malware Test Vector Coverage

- Test the binary transfer of Malware via HTTP, email and other transports—determine what is blocked or not, and what security polices work the most effectively in your environment.
- Command and Control Call Back—By emulating live infected host behavior you can test that policies are picking up on "phone home" and other malware messaging behavior.
- Test under high-load of hyper-realistic application traffic to add further realism and pressure to security services and devices. This determines security solutions impact on the performance of actual user traffic.
- After client initiated messaging, test attack scenarios where CyberFlood emulated servers attack clients with specific vulnerabilities.

cybeflood

Advanced Malware

SPIRENT

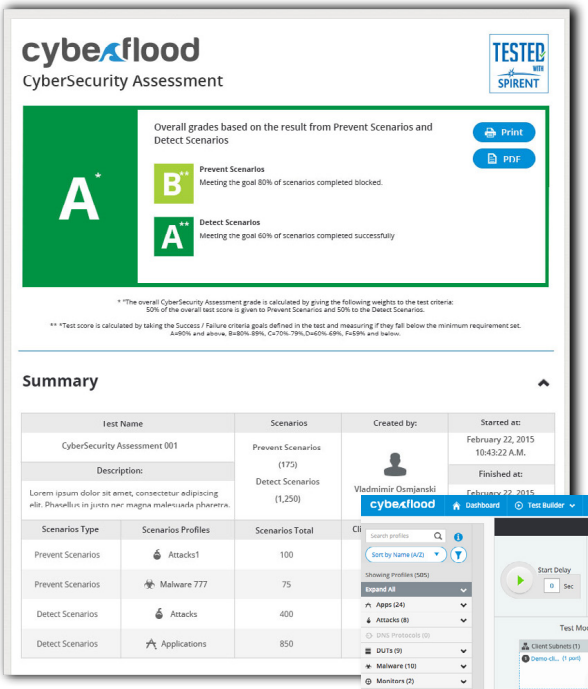
Spirent Services

Spirent Global Services provides a variety of professional services, support services and education services—all focused on helping customers meet their complex testing and service assurance requirements. For more information, visit the Global Services website at www.spirent.com or contact your Spirent sales representative.

Advanced Malware Testing

Quickly setup and execute audit tests to determine how well security services and polices report or block malicious content. Test configuration can concentrate on specific malware constructs or the entire database can be used to verify malware detection on a broad level.

- Test malware sent upstream only or bi-directionally.
- Add realistic application background traffic to realistically stress the system with legitimate traffic.
- Understand the impact of malware detection against legitimate traffic and user experience.
- Malware traffic can be emulated from multiple subnets, including regional IP ranges, creating true real-world conditions.
- New malware samples are continually added, providing the latest and zero-day level exploits for you to test with.



At-a-glance test grade reports showcase levels of Pass/Fail criteria for each new test run

Flexible test configuration

Anti-Phishing Working Group, Kaspersky, McAfee, AV-Test are trademarks of their respective owners.

spirent.com Follow us @SpirentSecurity

AMERICAS 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

EUROPE AND THE MIDDLE EAST
+44 (0) 1293 767979 | emeainfo@spirent.com

ASIA AND THE PACIFIC
+86-10-8518-2539 | salesasia@spirent.com

Rev D | 07/18