Spirent CyberFlood

Advanced Malware | Applications and Security Test 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.

⊖spirent®

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 20 million malware infestations were detected by malware programs in 2020 alone.

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 countermeasures 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.

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.

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.
- 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.

yberSecurity Assessment					
A Coverall grades haved on the result from Prevent Scenarios and Detect Scenarios					
	"The overall CyberSecurity Assessmen 50% of the overall test score is	t grade is calculated by giving th given to Prevent Scenarios and	e following weights to the test criter 50% to the Detect Scenarios.	ie:	
	ated by taking the Success / Hailure onto	on, 29m, C270m, 79m, Dreich, 69	m, Posen and ballow	nimum requirement set.	
summary	ated by taking the Success / Hailure onto	na goais defined in the test an on. 24m, cirton. 74m, Direch et Scenarios	a measuring it they rail below the min m, relation and balow.	nimum requirement set.	
summary	aced by taking the success / karure cris Antidina and aceive, limit	on, 24%, cr70%, 74%, preo% et Scenarios Prevent Scenarios	m, Posen and ballow	nimum requirement set.	
** *lest score is calcul Summary Feat CyberSecurity /	aced by taking the success / karure cris Antidina and aceive, limit	on.linn, corton, rom, oneon, et Scenarios Prevent Scenarios (175)	m, Posen and ballow	nimum requirement set.	
** *lest some is calcul Summary Rote LyberSecurity / Descri Lorem ipsum dolor sit ar	and by taking the success / source on antices and access and Name Kssessment UU1	on, 24%, cr70%, 74%, preo% et Scenarios Prevent Scenarios	m, Posen and ballow	Started at: February 22, 2015 10:43:22 A.M.	
** *lest some is calcul Summary Rote LyberSecurity / Descri Lorem ipsum dolor sit ar	Name uses by taking the success / Haure one Among and above, with Name usessment (J01 ption.	Scenarios Prevent Scenarios (175) Detect Scenarios	Created by:	Started ac February 22, 2015 10.4322 AM. Finished at: February 22, 2015	
*** Lett corre is calcu Summary Lyber/Security / Descri Lorem ipsum dolor sit ar als: PhaseIllus in juston no	Anno an anno an Nome Sissessment (01) pidon: er angana maleu anda pharatra	Scenarios Scenarios Prevent Scenarios (175) Detect Scenarios (1,250)	Created by:	Started ac February 22, 2015 10.4322 AM. Finished at: February 22, 2015 11.1522 A.M.	
*** Fest score is calcul Summary Lyber/Security / Descri Lorem ipsum dolor sit ar ale Dissellin in jurith ne Scenarios Type	Nome Nome Seessment (01 pdos: exconsectour adiposcing emigna makesark planeter Scenarios Profiles	Scenarios (175) Prevent Scenarios (175) Detect Scenarios (1,250) Scenarios Total	Created by Wedminin Comjenski Client to Server Status	Started at: February 22, 2015 10:43:22 A.M. Finished at: February 22, 2015 11:15:22 A.M. Server to Client Status	
*** Field some is called Summary Cyber-becurity / Desor Lorrem (system rise) Scenarios Type Prevent Scenarios	Neme Neme Sessment 001 prion consector education consector educati	Scenarios Scenarios Prevent Scenarios (173) Detect Scenarios (1,250) Scenarios Total 100	Created by: Wedeninit Ounjanuski Client to Server Status Biocked (85%)	Started at Started at February 22, 2015 10-4322 A.M. Finished at February 22, 2015 11-1522 A.M. Server to Client Status Blocked (SHI)	

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

cybexflood	R Dashboard	I 🔘 Test Builder 🗸 🕞 Profile Builder 🗸 📾 Projects 😰 Library			
Search profiles Q		CyberSecurity Assessment (molfind) Synt X			
Sort by Name (A/2) Showing Profiles (585) Expand All A Apps (24)	•	Start Delay Present Scenario Detext Scenario St 0 Set Applications Applications Maleane Setext Scenario Group Setext Scenario Group	V Schend: Game Traffic Text Criteria		
4 Attacks (8) D155 Presection (5) D155 Presection (5) D156 (9) Mathware (10) Monitors (2) Networks (5) Networks (5) Presection (7)	• • • •	Tecl Mode Service and presents Tecl Quere (E.K. A Orectament) Orectament	0 0		
Restarters (2) Security Mix (1) Subnets (125) Tests (202) Traffic Mixes (5)	• • • •	Scenario profiles Prevent Scenarios 28420 total / 28420 selected Wese not selected Amacka 3002 total / 3003 selected	Search scenario		
 Traffic Replays (7) ▼ Virsual Routers (12) ✓ 		Convert Server Convert Server Convert Server NOD, Deployage Artitivey File Spland ServerSed ArtHer Investing Stack Overfile Son VESS ArtHer Investing Server Demail of Service Son ServerSed ServerSed ServerSed ServerSed ServerSed Son ServerSed ServerSed ServerSed ServerSed ServerSed ServerSed Son ServerSed Se	 Company Incl Supported Attacks Attacks Attacks Attacks Attacks Attacks Attacks Attacks Attacks 		
		Struct struce sources coding during free thereby costs from Sources touched address free thereby costs from proven there for there there is a structure of the structure (B1) sources the and discovers(B1) sources the and discovers(B1)	Atlacia Category Mat Elegenee Communication Communication		
		Exch Login, sphood photo: Cach Login, sphood photo: (20) HS2, much Login, and mail and logics (21) HS2, much Logins and mail and logics (21) Multiverer: 1550/7 Isolal / 1590/7 selected	Productivity V Productivity V Communication Montilamenus V		
		Marrier 1307 18/07 19/07 19/07 III Scattering IIII Scattering IIII Scattering </td <td>Congry Michael Shapen Advanced Malane Advanced Malane Advanced Malane Advanced Malane Advanced Malane Advanced Malane</td>	Congry Michael Shapen Advanced Malane Advanced Malane Advanced Malane Advanced Malane Advanced Malane Advanced Malane		

Flexible test configuration

Ordering Information

Description	Part Number
CyberFlood Advanced Malware Content-1Yr	CF-C-ADVMALWARE-1Y
CyberFlood Attacks Content-1Yr	CF-C-ATTACKS-1Y
CyberFlood Standard Malware Content-1Yr	CF-C-MALWARE-1Y
CyberFlood Testcloud Apps Content-1Yr	CF-C-TESTCLOUD-1Y
Cyberflood Cybersiege Global IP Traffic Selector-1Yr	CF-SW-IANA-1YR

TestCloud is also available in multi-year and bundled package, please contact Spirent Sales for more information.

Americas 1-800-SPIRENT

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

Europe and the Middle East

+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific

+86-10-8518-2539 | salesasia@spirent.com

spirent

© 2020 Spirent Communications, Inc. All of the company names and/or brand names and/or product names and/or logos referred to in this document, in particular the name "Spirent" and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice. Rev G | 10/20 | www.spirent.com