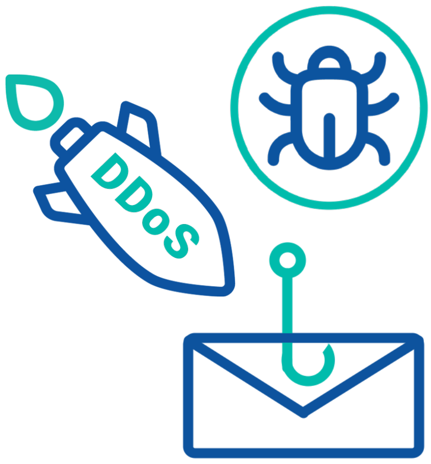
APPOSITE
TECHNOLOGIES

Apposite Attack Library



Ensure Network Security & Resilience

- ✓ Library of over 10,000 critical attacks, malware & CVEs
- ✓ Always up-to-date with new & evolving threats
- ✓ Mix valid application traffic and malicious attacks
- ✓ Measure the performance of network security devices
- ✓ Generate realistic threat scenarios for Cyber Ranges
- ✓ Build and maintain threat resilient networks

OVERVIEW

Apposite's Attack Library is an up-to-date and ever-evolving library of 10k+ cybersecurity threats including viruses, malware and other attacks for comprehensive network security testing. By simulating real-world attacks at scale, organizations can optimize security devices like next-generation firewalls, validate DDoS defenses, improve security performance, and ensure network resiliency.

Use the Apposite Attack Library with our AppStorm and AppPlayback solutions to generate malicious attacks and legitimate application traffic simultaneously, creating the most realistic and effective test environment possible.

Our unique design includes an intuitive search engine that allows you to easily search for and configure the exact mix of attacks for your specific test scenario. Emulate compromised devices and command centers then select the rate, length and scale of your attack in just a few short steps using our wizard-driven test configuration process.

Apposite's Attack Library is continually updated by our dedicated security team to include new and evolving cyber threats.

THREAT CATEGORIES

Viruses: Viruses and Malwares found in executables and file types.

Spyware: Command and Control (C2C) activities, where spyware collects data from infected users and communicates with remote attackers.

Ransomware: Traffic from malicious software which encrypts the files until the ransom is paid.

Vulnerabilities: Systems flaws in applications, networks and devices that attackers can exploit.

Backdoor: Attacks that bypass security measures to gain unauthorized access to the root of an application or network.

CVEs: Common vulnerability exploits that are publicly disclosed and available in catalogs maintained by Mitre and other companies.

Denial of Service (DoS): Attacks that render a targeted system unavailable, temporarily disrupting the system and dependent applications and services.

Fuzzing: An automated process of inserting massive amounts of random data into source code to find vulnerabilities.

Zero-day Attacks: Attacks which exploit software vulnerabilities that are unknown to the vendor or user.

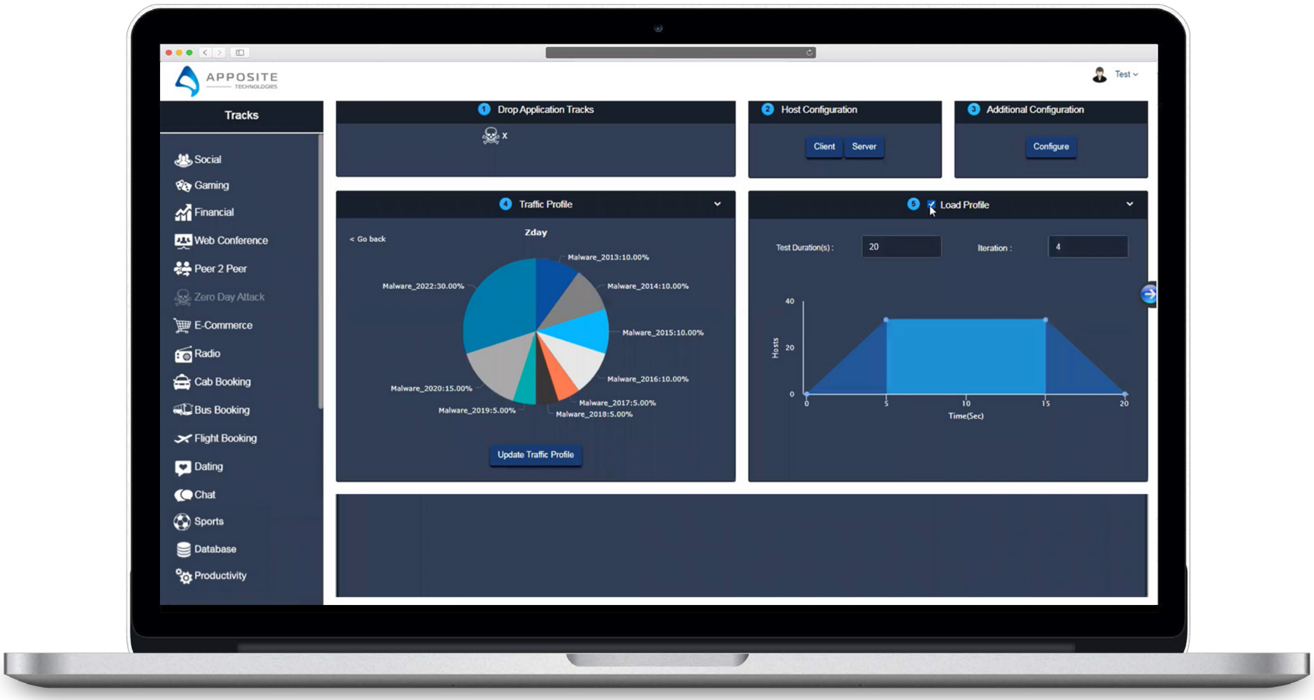
Product Capabilities

Apposite's Attack Library is backed by a dedicated security team that continuously researches the latest in vulnerabilities, threats, and attack methods to ensure our solution is always up to date. By releasing updates monthly, the Attack Library delivers the cutting-edge intelligence needed to protect your network and devices from ever-evolving cybersecurity threats. Our library consists of over 10,000 attacks - and growing - and thousands of real-world application traffic flows from social media to business economy, VoIP, and financial services.

Using the Attack Library with our AppStorm and AppPlayback solutions you can:

- Harden security defenses and measure the performance of networks and security devices
- Build networks and infrastructure that are resilient to cyber attacks
- Generate legitimate application traffic and malicious attacks simultaneously to benchmark the performance of application-aware devices and networks
- Validate DoS defenses, protect against zero-day attacks, and increase attack readiness
- Optimize security devices and systems such as next-generation firewalls, IPS and IDS systems, and SD-WAN gateways
- Emulate large-scale botnet attacks to stress test your network and discover hidden weaknesses
- Simulate realistic traffic scenarios for the best possible cyber range training environment
- Deliver an always-on user experience
- Choose from 1000's of predefined application flows for video streaming, social media, SaaS, E-commerce, finance, gaming, chat, web conference, and many others
- Capture your exact production network traffic and replay it at tremendous scale

USER INTERFACE



FEATURES

Apposite's Attack Library integrates seamlessly with our traffic generation solutions to deliver unmatched ease of use. Both AppStorm and AppPlayback run on the same platform and share the same modern, wizard-driven test configuration process allowing you to quickly set up complex tests utilizing both authorized traffic and malicious attacks from the Attack Library.

- Configure attacks to run sequentially or parallel
- Simulate brute force attacks by setting retries if attacks are blocked on the first attempt
- Control the rate of attack by setting packets per second
- Configure the percentage of malware from each year of CVEs dating back to 2013
- Emulate compromised devices and command centers
- Easily search for specific CVEs based on vendor name, CVE number, or type of attack using our intuitive search engine
- Specify the duration of attacks and how many cycles using the load profile
- View statistics in real-time or after the test is complete with our offline analyzer for each application and each attack
- Capture port level stats like total data transferred, throughput, packets per second, and latency

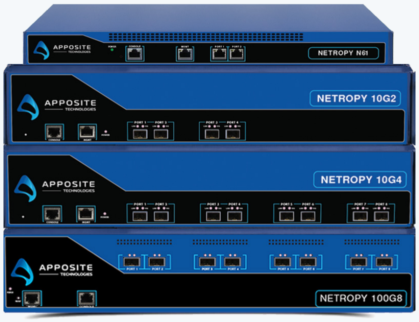
SUPPORTED SPYWARE TYPES

Adware	Programs that display potentially unwanted advertisements. Some adware modifies browsers to highlight and hyperlink the most frequently searched keywords on web pages. These links redirect users to advertising websites. Adware can also retrieve updates from a command-and-control (C2) server and install those updates in a browser or onto a client system.
Autogen	These payload-based signatures detect command-and-control (C2) traffic and are automatically generated.
Backdoor	A program that allows an attacker to gain unauthorized, remote access to a system.
Botnet	A botnet is a network of malware-infected computers ("bots") that an attacker controls. The attacker can centrally command every computer in a botnet to simultaneously carry out a coordinated action (like launching a DoS attack, for example).
Browser Hijack	A browser hijacker might take over auto search or track users' web activity and send this information to a C2 server.
Cyptominer	Download attempt or network traffic generated from malicious programs designed to use computing resources to mine cryptocurrencies without the user's knowledge.
Data Theft	A system sending information to a known C2 server.
DNS Security	DNS requests to connect to malicious domains.
Hacktool	Traffic generated by software tools used to conduct reconnaissance, attack or gain access to vulnerable systems, exfiltrate data, or create a command-and-control channel to surreptitiously control a computer system without authorization.
Keylogger	Keyloggers use various C2 methods to periodically sends logs and reports to a predefined e-mail address or a C2 server. Through keylogger surveillance, an attacker could retrieve credentials that would enable network access.
Networm	Program that self-replicates and spreads from system to system. Net-worms might use shared resources or leverage security failures to access target systems.
Phishing	A phishing website tricks users into submitting credentials that an attacker can steal to gain access to the network.
Spyware	Outbound C2 communication.

SUPPORTED VULNERABILITY TYPES	
Brute Force	A brute-force signature indicates that the frequency and rate at which the activity occurred is suspect. For example, many failed FTP logins in a short period likely indicates an attacker attempting password combinations to access an FTP server.
Remote Code Execution	Remote code execution (RCE) attacks allow an attacker to remotely execute malicious commands on someone else's computing device as if they were the logged in user.
Code Obfuscation	Code that has been transformed to conceal certain data while retaining its function. Obfuscated code is difficult or impossible to read, so it’s not apparent what commands the code is executing, or with which programs it is designed to interact.
DoS	A denial-of-service (DoS) attack is when an attacker attempts to render a targeted system unavailable, temporarily disrupting the system and dependent applications and services.
Exploit Kits	Exploit kit landing pages often contain several exploits that target one or many common vulnerabilities and exposures (CVEs), for multiple browsers and plugins.
Overflow	An overflow vulnerability is where a lack of proper checks on requests could be exploited by an attacker. A successful attack could lead to remote code execution with the privileges of the application, server, or operating system.
Phishing	When a user attempts to connect to a phishing landing page (likely after receiving an email with a link to the malicious site). A phishing website tricks users into submitting credentials that an attacker can steal to gain access to the network.
Protocol Anomaly	Protocol anomalies are protocol behaviors that deviate from standard and compliant usage. For example, a malformed packet, poorly written application, or an application running on a non-standard port would all be considered protocol anomalies and could be used as evasion tools.
SQL Injection	A common hacking technique where an attacker inserts SQL queries into an application’s requests, to read from or modify a database. This type of technique is often used on websites that do not comprehensively sanitize user input.

SUPPORTED VIRUS TYPES
Malicious APK (Android)
Malicious DMG (Apple)
Flash
Java-class
Macho (Mach Object files) for Mac
Office
PDF
Portable Executable (PE) like: • Object code, Fonts (FONs) • System files (SYS) • Driver files (DRV) • Window control panel items (CPLs) • DLLs (dynamic-link libraries) • OCXs (libraries for OLE custom controls or ActiveX controls) • SRCs(scripts that can be used to execute other files) • Estensible Firmware Interface (EFI) files • Program information files (PIFs)

Netropy Traffic Generation Solutions



Netropy Traffic Generation Solutions are available on high performance appliances and virtual machines (VMWare ESXi, KVM, Openstack). Configure tests with ease on a modern, browser-based UI or with a comprehensive RESTful API for increased automation. Run multiple tests at once and keep them running in the background, collaborate with your team, and easily connect and perform tests from anywhere.

Apposite's Netropy Traffic Generation solutions can be fully integrated with Apposite's Netropy Network Emulators to create the ultimate real-world test environment.

17835 Ventura Blvd Suite 211, Los Angeles, CA 91316 USA
www.apposite-tech.com | TEL: 1.310.477.9955 | info@apposite-tech.com