# Digital Warfare

ixia
A Keysight Business

The weapons used on the cybersecurity battlefield

## ATTACKERS ARSENAL

### Malware

Malicious software that comes in many different forms. Many malware instances morph or are regenerated daily so they can avoid signature-based detection systems.

### Phishing

Seemingly valid emails are sent to unsuspecting users to trick the user into clicking on an embedded link in the email and entering sensitive information or downloading malware.

### Botnet

An orchestrated army of infected hosts that unknowingly participate in malicious campaigns under the control of a botnet herder or controller.

### Advanced Persistent Threat (APT)

A multi-step network attack where the goal is to get inside, move around undetected, and steal data.

### DISTRIBUTED DENIAL OF SERVICE (DDoS)

An orchestrated attack from 100s or 1,000s of sources that flood a target with so much needless traffic that it cannot process legitimate traffic.

## DEFENDERS ARSENAL

### Inline Security

Perform active, real-time traffic inspection and detection without impacting network performance.

### Network Monitoring

Perform passive, out-of-band traffic inspection, detection, and recording for threat analysis.

### Context Aware DATA PROCESSING

Automatically recognizes rich metadata and hundreds of application signatures to deliver a stream of highly relevant, de-duplicated network traffic to all your security and monitoring tools.

### Threat Intelligence GATEWAY

Removes network traffic from sources known to distribute malware or participate in criminal activities.

### Security Fabric

Powerful network visibility that ensures resilient delivery of relevant traffic to security and monitoring tools.

Block attacks from entering and spot the threats inside.
Visit www.ixiacom.com/securityfabric to learn how.