Lancope’s StealthWatch® System leverages flow data from existing network infrastructure to create an always-on sensor grid for detecting today’s top threats. Often times, it is discovered that threats are originating from inside the network as a result of systems that have been compromised. Under the remote control of botnet operators or other nefarious external parties, these internal systems spread infections, steal data and wreak havoc on enterprise resources. Through sophisticated behavioral analysis and cutting-edge threat research, Lancope delivers unparalleled internal visibility and security context, preventing cyber-attacks from taking over corporate and government networks.

StealthWatch correlates flow data with a global threat feed from Lancope’s StealthWatch Labs Intelligence Center (SLIC) to provide enhanced detection capabilities for advanced malware, including botnet activity. Combining real-time intelligence on threats from criminal organizations with insight on suspicious network activity allows StealthWatch to uniquely provide information around the full security incident.

What is SLIC?
The StealthWatch Labs Intelligence Center (SLIC) is Lancope’s research initiative through which global intelligence on the Internet’s top threats is delivered to customers and the public at large. Lancope’s research group, known as StealthWatch Labs, conducts both in-house research and taps into a broad community of third-party experts and partners to aggregate emerging threat information from around the world. This intelligence is shared via SLIC through a public portal, as well as a threat feed that customers can choose to incorporate into their StealthWatch deployment. Publicly available threat intelligence from SLIC can be found at http://www.lancope.com/slic.

Advanced Botnet Detection
The SLIC Threat Feed offers advanced botnet detection capabilities, continuously monitoring customer networks for thousands of known command-and-control (C&C) servers and automatically adding new botnets to its radar as they are identified in the wild. From there, StealthWatch generates alarms and Concern Index™ events to flag these communications for administrators so they can be swiftly mitigated.

StealthWatch botnet detection functionality includes:
► Detection of either attempted or successful C&C communications
► Reporting on the specific botnet name responsible for the infection
► Detection of C&C servers operating within a network
► In-depth traffic reporting and analysis of the C&C communications
► Accelerated priority of other suspicious network activity from infected hosts
► Visual tagging of malicious hosts for fast identification
► Correlation of user and device information for the infected hosts to add context
► Utilization of application metadata such as HTTP URLs from the StealthWatch FlowSensor™ to increase accuracy of detection

The SLIC Threat Feed draws upon global threat intelligence to provide another layer of protection against the spread of malware.
The SLIC Threat Feed - How It Works

Today’s threat landscape has rendered conventional solutions such as antivirus, firewalls and IDS/IPS far less effective. In order to remain ahead in the cybercrime arms race, organizations must now obtain **end-to-end situational awareness** into everything happening across their networks. StealthWatch provides a comprehensive picture of network activity for combating a robust range of security and performance issues – including zero-day attacks and advanced persistent threats (APTs) – across both physical and virtual environments. Unlike many conventional security technologies, the system does not rely on signature updates to detect anomalous behaviors that could signify risks.

The SLIC Threat Feed provides an added layer of protection against the spread of malware by **incorporating in-depth intelligence on known bad hosts on the Internet** into the StealthWatch System, eliminating the need for more costly point solutions. Using their existing StealthWatch appliances, customers can choose to add the SLIC Threat Feed license to their deployment to automatically pull in updated threat information on an hourly basis. Customers do not have to worry about collecting their own threat intelligence and inputting it into StealthWatch. Instead, the threat feed is continuously delivered via a compressed, encrypted communication channel for optimal security and efficiency.

Behavioral Analysis + Global Threat Intelligence = Unmatched Protection

By collecting and analyzing NetFlow, IPFIX and other types of flow data, StealthWatch provides **additional threat context** by revealing what infected hosts are doing within the network. This in-depth behavioral analysis enables StealthWatch to detect the various stages of an attack from the initial malware infection to network reconnaissance, internal malware propagation, command-and-control traffic and data exfiltration.

StealthWatch pinpoints the specific port, protocol and URL used for suspicious communications to increase accuracy of detection. The system can also identify the exact users and devices communicating with malicious IP addresses, holding users accountable for operating infected machines on the network and helping to address BYOD challenges.

With StealthWatch, organizations benefit from a robust range of security capabilities:

- Sophisticated behavioral analysis + global threat intelligence
- End-to-end network visibility and protection
- Cost-effective monitoring for APTs, targeted attacks and insider threats
- Expedited troubleshooting and remediation
- Improved security, forensics, performance and compliance

Learn more | Request a demo

sales@lancope.com