Advanced Persistent Threat Analysis

Providing Enhanced APT Analysis for Security Incident Response

Network Forensics for the 10Gig World

OVERVIEW

Key Use Cases

- How and when did this attacker get into my network?
- What is the extent of the compromise?
- How long did this compromise last?
- How many other hosts were affected?

Solution

- Capture and index all network traffic for back-in-time analysis
- Analyze security incidents to isolate root cause and improve defenses
- Integrate seamlessly with existing security dashboards and SIEM tools for quick and efficient incident response workflow

Results

- Improved threat visibility
- Efficient utilization of analyst resources
- Automated and efficient incident workflow from alert to analysis and resolution
- Improved threat deterrence through thorough analysis of ongoing events

REQUIREMENTS

Government agencies, large enterprises, and telecom operators all face a growing number of well-coordinated, sophisticated network threats. These Advanced Persistent Threats (APTs) are often strategically delivered in stages over multiple days, weeks, or even months – extended timeframes that allow security teams to identify threat activity at several stages in the unfolding attack. The right analytic tools make it possible to successfully monitor, analyze, and discover malicious behavior. With full packet capture for in-depth, back-in-time visibility across the network, network security personnel can discover current attacks and thwart future threats.

When an intrusion is suspected, incident responders rely on packet, connection, and log data. Event logs and connection (or flow) data provide high-level indications of anomalous behavior including the timing, IP addresses, and protocols involved, but analysts need to quickly drill down to relevant packet and session content for a complete picture of what really happened. With resolution down to specific timeframes, packets, connections, and sessions, full packet capture lets analysts see exactly what data may have been stolen, how certain threats bypassed security defenses, how long they've been in the network, and how far they spread.

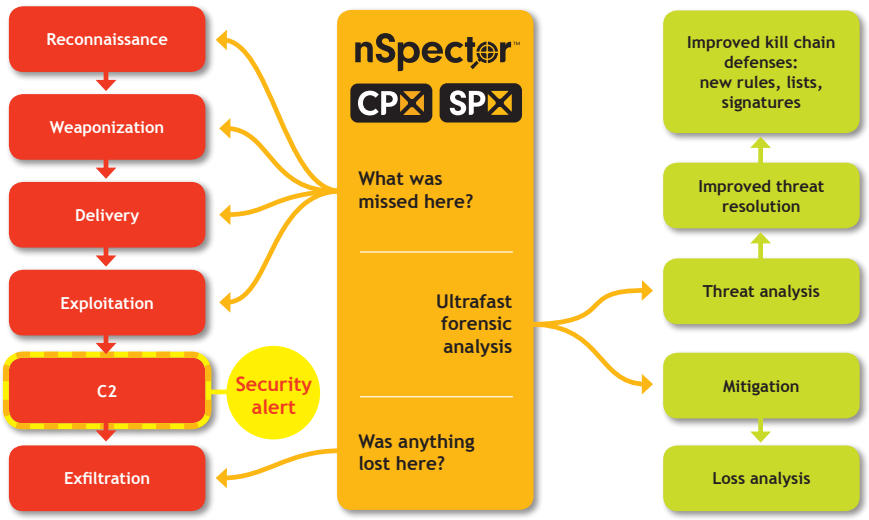
SOLUTION

The Capture Probe eXtreme (CPX) was built to capture network traffic at ultrafast data rates for extended time periods on local or fiber-attached storage arrays at petabyte scale. Its sophisticated multi-level patent-pending index, built from connection-level metrics, provides access to historical network traffic stored in standard pcap format along with full session analysis and reconstruction of the pcap data. The CPX also exports NetFlow v5, v9, and IPFIX-formatted flow records that can be used with existing flow-based security solutions for added visibility.

Accessible via the easy-to-use web UI or a RESTful API, CPX enables analysts to leverage existing custom scripts and utilities, allowing simple integration into their current workflow. An API integration to network SIEM tools delivers quick access to recorded data from familiar alerting environments, minimizing time and costs of deployment and training.

Incident Responders

Decreasing Mean Time-to-Resolution and Improving Defenses



ANALYSIS EXAMPLE A typical example might involve alerts from a next-gen firewall indicating malicious activity by a user or infected host.

An analyst quickly pivots from an alert within the firewall console to a connection-level view of the traffic recorded on a CPX appliance. The view shows the addresses, protocols, and ports involved, highlighting several web sessions and an IRC connection. CPX full-session analysis provides details of the web sessions and IRC communication, quickly highlighting the IRC connection to a suspect host out of country. The IRC session shows it includes command and control information, including a downloaded binary executable. Downloaded and further analysis of the binary from the CPX console shows the binary is malicious.

An analyst can use the CPX's ability to scan days' or weeks' worth of indexed traffic records to isolate the original time and source of the bot installation. Reconstructing email traffic and DNS records might reveal the source as a phishing email. This site, and signatures from the phishing email and IRC binary file download, can now be added to the existing security "kill chain" tools (IPS, firewall, DLP, and malware analysis) to prevent reinfections. And, since the time of the original infection is now known, CPX can review previously recorded traffic for similar successful or attempted attacks on other hosts within the same network and verify that no lateral file transfers or suspicious behavior took place. This is a key capability in assuring the security team that the host did not have time replicate the malware internally.

CONTACT US

Find out how nPulse Technologies can help provide enhanced APT analysis for your business. Visit www.npulsetech.com

THE BOTTOM LINE: Using the new CPX with session analysis, incident responders can significantly reduce the time researching network events. CPX can quickly provide valuable insight into, and quick analysis of, network threats including phishing attacks, botnet activity, insider data loss, and APT attacks. In addition, by helping to improve existing security tools and processes with back-in-time incident analysis, CPX helps keep the network safe while keeping it – and business – operational.

About nPulse Technologies, Inc.

nPulse Technologies is the performance leader in network forensics. Leading financial institutions, government agencies, telecommunications carriers and other organizations rely on nPulse solutions to enhance security monitoring, shorten incident response times, and increase returns on existing security investments.

For network forensic analysts looking to signficantly reduce incidence response time, nPulse solutions enable expeditious reconstruction of the kill chain. Unlike competitive solutions that are unable to operate at 10Gbps sustained and take hours to analyze network traffic, our solutions are designed to perform at 10Gbps full duplex, capturing, inspecting, and exposing indications of compromise within minutes, all at a fraction of the cost.

For more information, visit www.npulsetech.com.