EIN PRESSWIRE

IPCopper: Monitoring and Securing Legacy Apps

PORTLAND, OR, USA, December 19, 2017 /EINPresswire.com/ -- While many legacy apps continue to provide value, maintaining and securing them presents a challenge to IT security teams, since patches and upgrades are no longer available. IT teams are left in a situation where on the one hand they must maintain accessibility to and usability of the legacy applications and equipment, while on the other hand securing them from those would take advantage of vulnerabilities to cause mischief.

IPCopper, Inc.

Legacy apps were designed for a different era and environment than today’s networks and likely have limited or no security or event logging features. They were designed and developed for a particular function, but typically with few features for monitoring and management. The only choice is to bring in external equipment to manage, monitor and secure them.

This is not a one-time problem, but rather an ongoing task as today’s applications and equipment will become tomorrow’s newest legacy apps, each with their own unique parameters and behaviors.

The peculiar challenge is that it would fall on the external appliance(s) to figure out normal vs. not-normal behavior and intervene or alert as necessary, without hindering legitimate communications or disrupting the production or business environment. Several tools are necessary to handle the day-to-day management of legacy apps and protect them from malicious actors, including tools to monitor their network activity; to filter what communications are allowed to reach (and leave) them; to collect and store full packets; and to search through their network communications, both current and historical. Given that a typical enterprise employs a large number of disparate apps and equipment, designed by different developers for different purposes, these external appliances must be flexible enough so as not to interfere with the apps’ functions, but robust enough to handle all that gets thrown at them.

The first step is to determine and set parameters for normal behavior. In many business and production environments, certain legacy apps and equipment may typically communicate only during business hours and only with certain hosts or external IP addresses. In other environments, for example in a 24-hr healthcare setting, communications with legacy apps would be around-the-clock, however, with different levels of usage at different times. In order to adequately monitor legacy applications and equipment without generating hordes of pesky false-positive alerts, either situation requires the ability to create multiple scenarios to describe normal network activity at different times.

Monitoring a typical legacy app may require three or more scenarios to cover idle/after-hours behavior and active/business-hours behavior plus, for example, the spikes in traffic that occur during scheduled backup/maintenance. While low bandwidth usage and packet rates during business hours would require attention, after hours the same low bandwidth and packet rate would be normal. Equally, monitoring is greatly facilitated by graphical visualizations of the data, making it possible to see at a glance if all is running smoothly within normal ranges.

In addition to the alerts enabled by scenario-based network monitoring, the second element in securing legacy apps is blocking or filtering unwanted traffic in a precise and nimble fashion, with the ability to fashion sophisticated rule sets with automated triggers set to take automated actions. This may include switching to a more restrictive rule set or sending out multiple alerts, should network conditions indicate that a DoS or other type of attack is in progress.

The third element is the ability to use the feedback from the monitoring system to research and find problems as they are discovered. When an industrial controls system behaves strangely or a data feed connection becomes choppy, operators need a way to find out why. This entails having a quick and efficient way to be able to dive deeper into the relevant network traffic and take a look at the packet headers and payloads.

Lastly, when it comes to researching an anomaly or diagnosing a problem, nothing beats keyword and signature searches for finding and flagging packets. Keyword signature searches using a system that can go through the packets at multi-gigibit speeds exponentially enhance investigative abilities and shorten the time-to-resolution of any number of issues.

These four elements are key to effectively monitoring and securing legacy applications and equipment – rather than flying blind, operators would be able to see the digital terrain and react intelligently. The IPCopper USC8032 combines all of these four functions – monitoring, blocking/filtering, packet capture and keyword signature search – in one state-of-the-art appliance that not only delivers superior performance but also yields unique symbioses from the integration of these functions. High bandwidth rates plus high packet rates, even with thousands of rules enabled, ensure that the USC8032 can handle both the hordes of small packets that a malfunctioning legacy app may throw at it as well as peak multi-gigabit traffic on busy business networks.

For more information, please visit www.ipcopper.com/product_usc8032.htm.

IPCopper, Inc.
503-290-0110
email us here
Media @ IPCopper

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.