CSO
FROM IDG
June 19, 2018 www.csoonline.com

REVIEW

Review: Corelight adds security clues to network packet analysis

In the tradition of other great network analysis tools like Bro and Sourcefire, Corelight gives security pros deep insight into data traffic on the systems they defend.

By Roger A. Grimes, Columnist, CSO

Thinkstock

I've long been a huge fan of network packet analysis. Like math in the real world, I believe network packets are the only truth to what is going on with your network. Sniff your network and you'll find out the problem, or at least be pointed in the right direction to the culprit. Back in the Novell network days, I was a fan of an early (and now deceased) network packet sniffer called LANAnalyzer. Then I got turned on to Ethereal, which became Wireshark.

Those were great tools for pure network packet sniffing, but they were not the perfect, optimized tools for more efficiently detecting security issues. Then I was lucky enough to be in one of the first Snort SANS classes taught by its creator Martin Roesch. I've still got plastic little Snort pigs all around my house and office.

Snort was great, like an antivirus network sniffer on steroids, but it quickly became overwhelming if you deployed too many Snort sensors in a big environment. Many enterprise Snort users felt rescued when Marty turned it up to 11 by developing a commercial version called Sourcefire, which improved speed, manageability and capabilities.

For more than a decade, there wasn't a company I worked at that didn't address every new location connection by placing another Sourcefire appliance on the network egress/ingress point. Most enterprise network security managers didn't consider a network secure unless they had a Sourcefire box involved. Sourcefire was eventually bought by Cisco.

The geekiest of the network packet security geeks fell in love with open source Bro, which was created and released over 23 years ago by Vern Paxson, now a Fellow for the Association of Computing Machinery (ACM), which means he's an early founder of important technologies and a big deal.

Bro captures network packets and parses everything it sucks up into useful information. Most people think of Bro as a network intrusion detection system, and it is that, but it's more. It can do traffic analysis, forensic investigations, application level analysis, file tracking, and let anyone drill down into the tiniest bit of captured information. Best of all it, it does it using stateful analysis, meaning you can easily see users, files and endpoints across different connections and sessions. Bro also comes with a scripting language. It works on Linux, BSD, and Mac systems. Over 10,000 different companies have tried or run Bro. Unlike most other open source projects that tend to die of neglect within a year of their release, Bro has a continued large and supportive ecosystem.

Like Snort, Bro can easily become cumbersome when overrun by too much network traffic, when using multiple sensors, or trying to understand or write scripts. Did I mention that Bro is command-line only? It is not unusual to hear stories of teams of people spending months deploying and customizing Bro. It's awesomely powerful, but not easy to deploy.

Enter Corelight

Corelight is the equivalent of Snort going to Sourcefire. Corelight is Bro on steroids. It comes on an appliance with a GUI and is easy to deploy and operate. It can handle deep packet inspection on networks up to 25Gbps, which is over 10 times what the typical open source deployment can handle. That's without its "adaptive shunting" ability, which allows network traffic to be further refined to just what is important. Corelight claims to have appliances in eight of the Fortune 50 companies.

Corelight's specialty is to act as hardware-based "middleware" sitting between packet aggregators, adding and transforming the data, and then sending the transformed data upstream to your other traditional logging/alerting/detection devices like security information and event management (SIEM) and log management systems. It turns packets into more useful data.

One of best ways it transforms the data is to assign unique IDs per session to connections and files, which allows those users and files to be followed over different connections — not only in the Corelight product, but in the upstream products. I can capture and reconstruct specific files and broad categories of files right out of the packet stream. You can add different analyzer scripts to detect things such as a sudden increase in entropy in different file streams, which could indicate a ransomware attack.

Corelight is easy to install

Whereas Bro could take weeks to install, Corelight and its customers report that they can have a Corelight sensor up and working in 15 minutes. During the demo I had at the recent Gartner Security and Risk Management Summit, it looked like one of the simplest setups I've ever seen. Basically, you define which packet aggregators you want Corelight to collect from and where you want the transformed data sent to, along with a handful or two of other configuration settings. Corelight comes with a hardware accelerator NIC, comprehensive API, and can even help you identify previously undetected packet loss at your packet aggregators.

I saw only two potential issues: One, it doesn't support native packet capture (PCAP) ingress. PCAP is a common open source packet capturing software that is used in other open source network packet capturing software programs, like Netflow and TCPDump. The other issue was that although you can connect to multiple Corelight sensors within the management console, you can't see aggregated data or manage multiple sensors at the same time. You have to connect to each Corelight sensor individually and the data is only displayed individually.

A Corelight user's account

I interviewed Ken Hanson, a principal engineer and Corelight user for over 18 months. He's a big fan of the product. I asked him what he loved most about Corelight, and he wasn't shy. "It's the ability to pull a very detailed level of data and enrich existing data. It's unreal. I analyzed Corelight's data using Splunk, and together there wasn't a question I couldn't ask of our network," he said.

"You can look for anomalies, even inside of encrypted traffic. It is great for tracking lateral movement of advanced persistent threat adversaries. The problem with firewalls alone is that you can only track network traffic north to south," Hanson added. "Even most IDSs aren't that good at tracking lateral movement. Corelight, with its unique user and file IDs made it easy, and especially easy to get great detail when I need it. Corelight gives you access to a lower level of data when you have Indicators of Compromise that aren't picked up by a firewall session."

Corelight is a network security person's dream. Some people might think it's not as sexy as some of the other security appliance you could buy, but it transforms network data adding value and detail that you won't get anywhere else, especially at near wire speeds. If you do network packet analysis for a living you're going to want to get a demo of this product.

For more information visit: www.corelight.com
or email us: info@corelight.com