



THE MALWARE REPORT

Why Log Analysis is a Key Layer of Defense

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

Chima Njaka, director of product management at LogLogic

The Malware Report Transcript

Title: Why Log Analysis is a Key Layer of Defense

Episode: 118

Location: http://www.eset.com/podcasts/042109_ESET_LogLogic.mp3

April 23, 2009

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant, and you're listening to The Malware Report with Randy Abrams live from the 2009 RSA Conference in San Francisco. Along with Randy, we also have Chima Njaka, director of product management at LogLogic here as a guest today to talk about the importance of layered defense and log file analysis. So, I'm going to pass it over to Randy to have a discussion on log file analysis.

Randy Abrams: Thanks, Matt. I often tell people that defense is a lot more than just installing antivirus software and thinking you're secure. One of the most overlooked aspects of defense I think is auditing and paying attention to what your security software says. I've invited Chima today

so he can explain a little bit more about what log analysis is and why it's important.

Chima Njaka: Sure, thanks Randy. Log analysis is an integral part of your overall layer of defense. Log analysis involves looking at the activity records from everything that may be within an enterprise environment. I'm talking about things like applications - any applications you might have running in your environment, any of the platforms that those applications might be running on, perhaps any of the network devices that may be routing those events across the enterprise. Looking at your log data is really in some sense a lot like shining a light on what's going on within your environment. Everything that's going on, there's this activity log recording of that particular event. You can take and track somebody's activities basically all the way through your environment. We use this at LogLogic. Our solution allows companies to collect that information, archive it, report and alert on the information and use it in various ways, using various log powered applications to support both security compliance and IT operations for that particular enterprise.

Randy Abrams: Right. There's so much more log data generated nowadays. Your firewall has logs, your antivirus has logs, your network management tools all have logs and no human has time to go through all that data. Does your product heuristically analyze all that data and say, "These are key points and when you correlate these things, this is an attack signature."?

Chima Njaka: We have a new product - our Security Event Manager is specifically tied to automated correlation and has its own capabilities there. In general, we do have other heuristics analysis of the log data to enable a core operator who has to sift through what is typically a huge amount of data and drill down right to the detail of the information they might be interested in looking at. You want to confine your searches or

reports to those scope devices within your environment of particular interest to you and various other things. Once that is scoped down, certainly our solution is one that will allow you to very quickly resolve and show that you're in compliance in that environment. There is a ton of data typically from a lot of log sources coming in to the environment and you need to have a solution like ours to manage the huge volume of log data. I mean we're talking about tens of thousands, if not hundreds of thousands of messages per second and storing that in some fashion; collecting it to allow you to record and use that log data intelligently going forward is quite important as an overall layer to your security posture.

Randy Abrams: Right, it's an important layer. Companies like TJMaxx had a huge data breach and found out the hard way. They'd been breached for many months before they discovered it and intelligent log correlation and analysis could have helped them find and contain the damage a lot more quickly.

Chima Njaka: Yes, that's one example. Another good example I'm sure you're all aware of is OctoMom, the woman who recently gave birth to eight kids. She was a patient at Kaiser Permanente and there was some medical staff there that had legitimate reasons or legitimate access to her log data, but for curiosity reasons went and checked her medical records just out of curiosity. That was an unauthorized use of that data and that information. There's somewhat of a bit of difference between "Am I allowed to access this data," and "Am I supposed to be looking at this data right now?" This was an example of people who had legitimate access to the log data, but didn't have a legitimate reason to be looking at the log data.

Randy Abrams: I understand that LogLogic also adds management capabilities to enforce compliance of policy in addition to the log management.

Chima Njaka: Right. We've got a compliance manager that allows you to automate the whole workflow of looking at the log data, checking off that you have seen the log data or looked at these various reports; it's not just enough for you to collect the log data but to show you've actually looked at the log data. We've got nice executive dashboards enabling an auditor or an executive to look and see their compliance posture with regard to control objectives and these particular regulations - PCI for one. We've got great tools to automate that whole process and make it much more efficient and effective for users.

Randy Abrams: This is really interesting and good information. I wish we had more time, but we don't. If you can tell people where they can go to find out more information about your company that would be great. Thank you so much for being a guest on the show today.

Chima Njaka: No worries. Thank you, Randy. Definitely, if you have more questions about log management intelligence in general or LogLogic in particular, please come to our Web site at www.loglogic.com for more information. Thank you very much for this opportunity.

Matt Grant: This has been Matt Grant and you're listening live to the Malware report live from the RSA Conference.

[End of recorded material]