LOG FILE PROTECTION

Simon Bain *provides an explainer on log files: what are they, why do they matter and how do we protect them?*

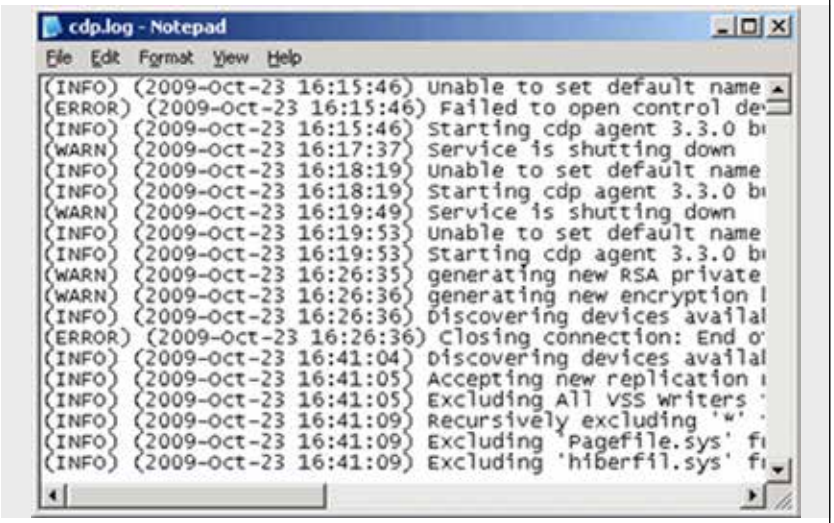
Log files come with many challenges. Firstly, they exist as enormous volumes of data. Almost everything that a user does is recorded, meaning that they quickly pile up, and not all of them are useful. Secondly, they aren't all uniform as they come in various shapes and sizes, serving various purposes. Event logs, system logs, access logs and server logs are just some of the various types that are collected and stored. This large volume of data means that processing and analysing logs for use can be both extremely time-consuming and complex.

And thirdly, you often need access to them, but you always need to protect them at the same time. According to advice from the NCSC, good logging practices provide the ability to understand, trace and react to system and security events. Cyber criminals will seek to get their hands on a company's log files in order to identify vulnerabilities, force changes, steal data and hold users to ransom. Adequately protecting them is therefore paramount. But what is a log file?

A log file is a record of actions taken on or by an application within a computer system. They are the primary data source for network observability. They usually contain information about usage patterns, activities and operations within an operating system, application, server or another device. They can also contain IP address, emails and law-protected information. Crucially, they record what is happening without knowing why it is happening. In other words, logs are not intelligent. Instead, they are simple read/write text files full of valuable information with often very little in place to protect them.

Log file monitoring and analysis increases the observability of the network, creating transparency and allowing visibility into the cloud computing environment. It can show what is happening within the system, including design malfunctions and malicious activity. This threat intelligence allows IT teams to identify where particular system improvements might be needed, can support security efforts and be used to capture the behaviours of end users. They're also useful for meeting compliance requirements and can be leveraged for audits.

The biggest risk that comes with log files is often complacency. Senior leaders often don't take the threat of attack seriously enough and protect them adequately. In reality, if hackers get access to log files, their content can be invaluable. Specifically, criminals can inject false entries, delete specific logs to erase traces or modify details like timestamps and IP addresses. They can even disable logging services to stop any activity from being recorded in order to hide that an attack has happened.



Logs can also be relatively easily exfiltrated and stolen as they're often in plaintext with no encryption to protect them. This means your data can be stolen and shared or used to exploit you. Either way, once it falls into the wrong hands it can become very costly to get it back or recover.

The first step is recognising that although log files may not look useful on the surface to the untrained eye, they almost always contain a map and keys to the inner workings of your business and should be treated as such. On the market currently, there exists specialist security software that watches for anomalous activity that might indicate an attack commencing or indicate that one is already in progress. If not acted upon fast enough, logs can also be used to clean up after the attack. It is possible to cause such a mess in the logs that visibility is lost for weeks.

Technology such as OmniIndex's LoggerBC can enable log files to remain encrypted at all times while allowing actionable AI threat intelligence from these fully encrypted log files. LoggerBC works on a native and private AI: Boudica. Boudica analyses encrypted log files to identify patterns, threats and vulnerabilities in a system and alert users to any potential threats in real-time with easy integration into Google Looker.

Powerful fully homomorphic encryption technology ensures that log files are encrypted at all times and never left vulnerable to attack. Log files are also stored in a private and secure blockchain to ensure they can't be accessed by criminals and are protected from the threat of ransomware. Protecting log files is no easy task, but can be achieved with the latest technologies. Without it, businesses remain at risk to attack, breach and exploitation ●

Almost everything a user does on a computer is recorded as a log file

Simon Bain is CEO at OmniIndex.