WINDOWS LOGGING SERVICE

National Security Campus

Background

With the continued rise in cyber-attacks, the ability to search for and detect new threats as they occur has become a necessity. Searching an enterprise for indicators of compromise (IOCs) should take seconds not hours, and should not be restricted to vendor-specific tools. Monitoring for changes specific to one's environment provides opportunities to detect insider threats and previously unknown malicious activity. A rapid response is critical to preventing the spread of threats and persistence in one's environment.

Description

The Windows Logging Service (WLS) is a Windows service that provides enhanced operating system information via standard syslog messages to any syslog format compatible log server. Developed by the cyber security staff at the National Security Center (NSC) to aid in the detection of malicious activity, WLS augments traditional logging and forensic analysis with real-time reporting of contextual operating system (OS) information. WLS reads and sends all Windows event logs and adds extra data relevant to cyber security, such as cryptographic hashes and file metadata. In addition to event logs, WLS monitors a variety of system details that are often cited in incident reports as IOCs.

One of the primary data sources is the audit logs of process creation events. Windows can record each time a program is run and WLS uses this as a trigger to gather extra information about the current system state and to log any changes. Process information gathered includes cryptographic hashes such as MD5, SHA1, and SSDeep; and file metadata including version, language, and manufacturer, as well as session and signing information and entropy.

Other information gathered by WLS is typically only available by using interactive on-demand tools to view a snapshot of data at the time it is run. Providing this data in real-time and in context with process information allows for correlation of previously ambiguous data points and gives insight into OS and process interactions. The additional information can include loaded libraries (DLLs, plugins, etc.), named pipes, windows objects, and open ports. WLS can also provide certificate data, device and drive information, performance counters, registry changes, and Windows Management Instrumentation (WMI) data.

Advantages

WLS used in conjunction with a central log repository and log analysis tool creates a powerful combination that supports not only passive detection, but also active hunting for malicious activity and insider threats. Its reporting via syslog messages allows for integration with existing SIEM solutions and the key/value pair formatting is easily parsed without predefining schemas. Used in place of an existing Windows logging tool or as a first step into host-based logging, WLS provides a rich dataset in a highly compatible format to enhance environmental awareness and improve one's enterprise security posture.

Honeywell

The Department of Energy's National Security Campus is a multi-mission engineering, manufacturing and sourcing enterprise delivering trusted national security products and government services. Managed by Honeywell Federal Manufacturing & Technologies, LLC., for the DOE under contract number DE-NA0002839.

14520 Botts Road, Kansas City, MO 64147 | 816.488.2000 | OCTOBER 2015

Applications

This software has several key cyber security applications for any business:

- Centralized log collection
- Endpoint monitoring
- Meet audit requirements
- Digital forensics and incident response
- Malware hunting
- Insider threat detection

Intellectual Property Status

The National Security Campus licenses this product for commercial use, internal use, and government and academic use.

Keyword List

Forensics, Incident Response, DFIR, Insider, Threat, Malware, Logging, Audit

Contact

Kristin Murray
816-488-3045
kmurray@kcp.com