November 2022

Rapid Detection of Network Threats by Analyzing Network Logs

Assaf Namer

Tracy Jiang

Rapid Detection of Network Threats by Analyzing Network Logs

ABSTRACT

Currently, there is no easy way to view and inspect network data surrounding a suspicious network event. Typically, analysts correlate findings across multiple services to capture network data indicative of security threats which is a time-consuming task that can delay response. This disclosure describes techniques that enable rapid response to network threats by mirror-capturing a real-time window of network traffic; by using in-line or out-of-band analysis to detect network events; and, once an event is detected, by generating a packet-capture (pcap) file from the mirrored data to enable correlating between network events and the pcap file. Visibility into the captured traffic is obtained by providing, within the logging service, a pointer to the pcap file and by describing potential threats visually in terms of severity, time, category, direction, protocol, port, etc. Time and effort needed to cross-reference network logs against threat-hunting systems/databases to evaluate adversarial packets is reduced.

KEYWORDS

- Cloud computing
- Logging service
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Security operations center (SOC)
- Network security
- Network forensics
- Deep packet inspection (DPI)
- Malware analysis
- Threat detection
- Bump in the wire (BIPW)
- Security posture

BACKGROUND

Logging services enable cloud computing providers to capture and display (e.g., to customers) a variety of data for the purposes of audit, debugging, optimization, etc. Such logs can be aggregated and filtered using particular, project-based criteria and directed to specific destinations, e.g., services, storage, databases, etc.

Network threats detected by intrusion detection (or prevention) systems (IDS/IPS), firewalls, etc. are also usually logged using logging services. However, threat findings buried in logs do not immediately provide to an analyst at a security operations center (SOC) or in a security engineering team insights into the data in the logged packets. Currently, there is no easy way to view and inspect network data. Typically, SOC analysts use a different service, parallel to the logging service, to capture network data indicative of security threats. Subsequently, they correlate the times of findings across multiple services to isolate the threat — a time-consuming task that can delay response and remediation.

DESCRIPTION

This disclosure describes techniques that enable rapid response to network threats by mirroring and capturing a real-time window of network traffic; by using in-line or out-of-band analysis to detect network events based on security policies; and, once an event is detected, by generating a packet-capture (pcap) file from the mirrored data to enable correlating between network events and the pcap file. The techniques provide visibility into the captured traffic by providing, within the logging service itself, a pointer to the pcap file and by describing potential threats visually in terms of severity, time, category, IP addresses, direction, protocol, port, etc. Details about potential intrusions, lateral movements, and other network-related threats become readily available. Reduced time and effort are needed to cross-reference network logs against

threat-hunting systems/databases to evaluate adversarial packets. Network threat findings such as malware patterns, known bad-file signatures, bad packet data, etc. surrounding the time of the findings are captured quickly and displayed within the logging service, obviating the need for use of multiple services for correlation of data.

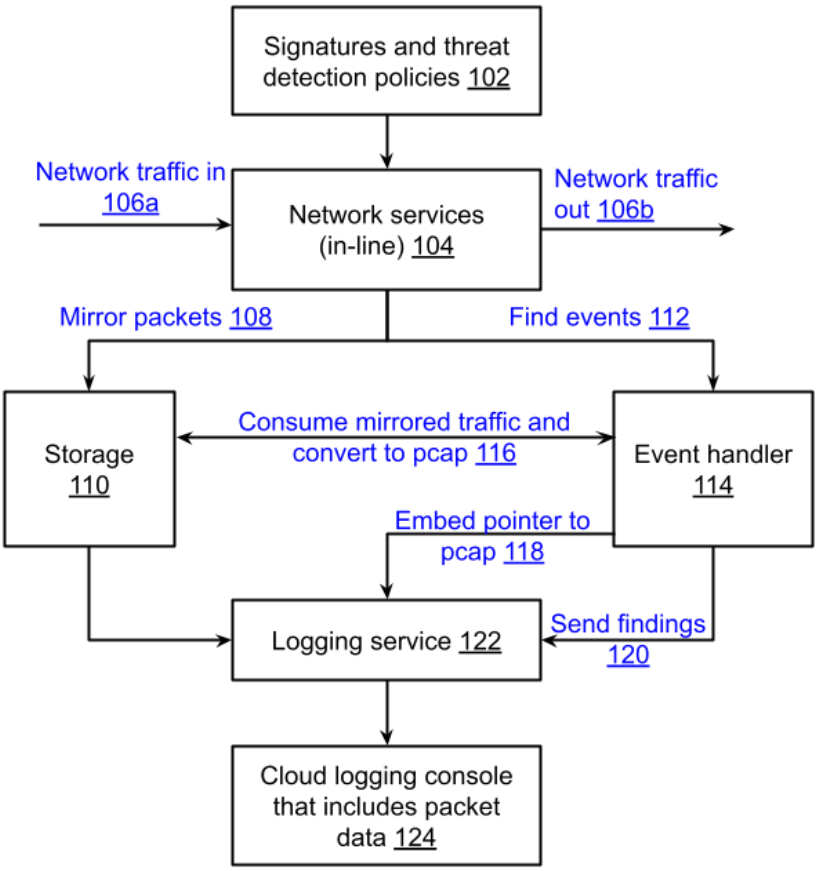

Fig. 1: Rapid detection of network threats by analyzing network logs

Fig. 1 illustrates rapid detection of network threats by analyzing network logs. A network service (104) that provides one or more of storage, email, file access/sharing, data filtering, printing, or other services is configured with threat detection and security policies, malware patterns, bad-file signatures, network rules, etc. (102). A moving window of traffic flowing (106a-b) through the network service is mirrored (108) and saved in memory or storage (110).

Under moving window storage, new traffic is stored in a fixed-length buffer such that it overwrites old data in the buffer. The length of the window can be measured in minutes (e.g., two minutes) or in bytes of data (e.g., 100 GB).

The network service emits findings (112) based on the configured policies. The findings can be generated using in-line analysis of network traffic (e.g., IPS) or out-of-band threat-detection services (e.g., IDS, security engines, bump-in-the-wire technology, etc.). Once a finding is emitted, e.g., a malware pattern found, an event handler (114) sends the findings (120) to a logging service (122).

In parallel, the event handler consumes traffic from the storage (110) and converts its data to a known traffic-format file, e.g., a packet capture (pcap) file (116). Compared to network speeds, consuming mirrored traffic and creating a pcap file may be slower. Therefore, when the pcap file is ready (which is typically after the event is sent to the logging service), a pointer to the pcap file (118) is embedded into the logging service. The event handler also sends relevant timestamps along with the pcap-file pointer. The logging service correlates between network events and pcap files, provides a pointer to the captured pcap file, and embeds within a visual display (124) of packets in a console, highlighting potential threats.

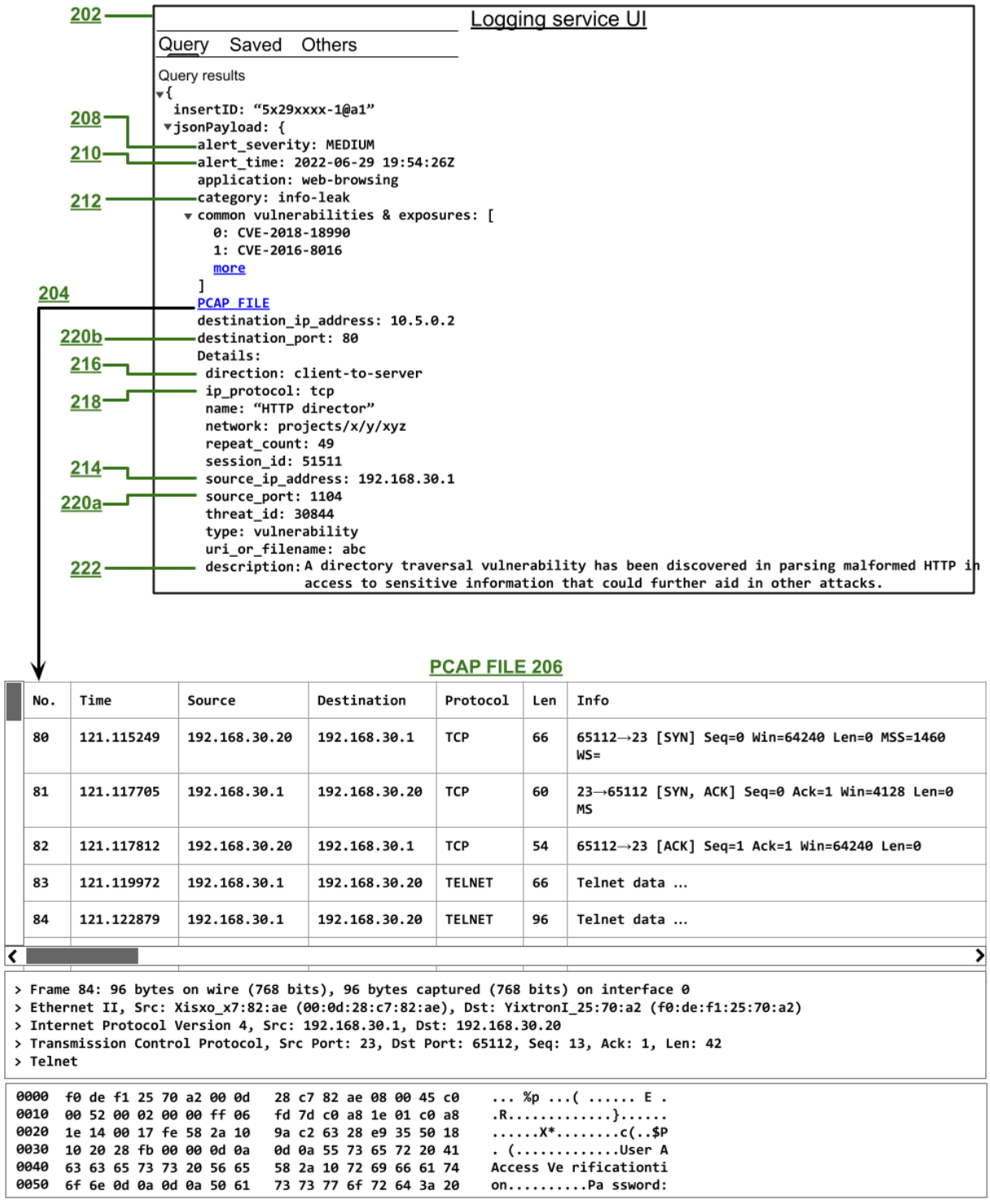

Fig. 2: An example logging-service user interface

Fig. 2 illustrates an example user interface (202) for a logging service enabled by the correlation of network events with pcap-file data. Potential threats and the pcap file are

embedded within the user interface and are easily accessible. This example uses IDS as a finding trigger. However, more generally, any managed or unmanaged network device can trigger a finding of suspicious network activity.

As illustrated in Fig. 2, potential threats and suspicious packets can be visually depicted for quick analysis within the console of the logging service by a pointer (204) to a pcap file (206) that includes the suspicious session. Aside from providing visibility into the captured traffic by providing a pointer to the pcap file, the potential threat is described in terms of its severity (208), time (210), category (212), IPs (214), direction (216), protocol (218), port (220a-b), description (222), etc. Details about potential intrusions, lateral movements, and other network-related threats are made readily available. Different levels of security and networking visibility can be provided to network administrators, security engineers, threat hunters, etc. After the session is analyzed, it is available as part of the logs, so that a customer of the cloud service can visit the logging service to get detailed visibility on the metadata and actual data in the network data stream.

The computing power, speed, and storage capacity of the cloud environment enables the rapid detection and processing of suspicious network events. Integrating threat detection into the logging service can greatly reduce the time taken for detailed information on suspicious events to show in logs, enabling response and remediation by the security team with a rapidity that is not feasible in non-cloud environments or by cloud providers that require their customers to use multiple services. Cloud monitoring, operations, intrusion detection, intrusion prevention, and the overall security posture of the organization are thus enhanced.

CONCLUSION

This disclosure describes techniques that enable rapid response to network threats by mirror-capturing a real-time window of network traffic; by using in-line or out-of-band analysis to detect network events; and, once an event is detected, by generating a packet-capture (pcap) file from the mirrored data to enable correlating between network events and the pcap file. Visibility into the captured traffic is obtained by providing, within the logging service, a pointer to the pcap file and by describing potential threats visually in terms of severity, time, category, direction, protocol, port, etc. Time and effort needed to cross-reference network logs against threat-hunting systems/databases to evaluate adversarial packets is reduced.

REFERENCES

1. "AWS Network Firewall - Amazon Web Services" available online at https://aws.amazon.com/network-firewall/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc accessed Oct 17, 2022.