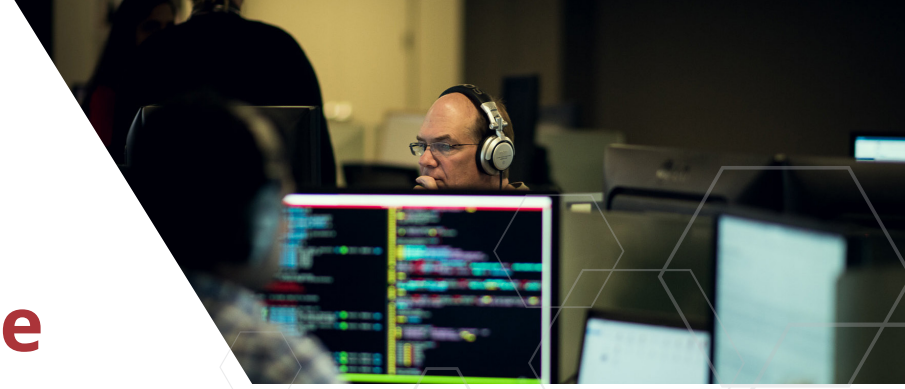
esentire®



INCIDENT REPORT

The Mirai Malware Breach

In October 2016, a massive Distributed Denial of Service (DDoS) attack targeting a well-established internet provider impacted millions of Wi-Fi-enabled devices. This DDoS attack caused an international outage, affecting popular websites such as Twitter, PayPal, GitHub, Amazon, Netflix and many more. This particular attack was attributed to a malware variant called Mirai.

An eSentire client using esNETWORK™ for real-time network threat detection and prevention was also impacted by this malware.

Here's the full report.

At 2:10 PM, the client deployed a new Polycom Video Conferencing system. Shortly thereafter, the eSentire Security Operations Center (SOC) witnessed multiple inbound connections occurring. Something or someone was attempting to infiltrate the client's network from multiple origin points including Asia, North America and Europe. An analyst instantly issued a block to prevent any further communication with the client's network.

The analyst immediately connected with the client to notify them of the malicious activity. The inbound connection attempts were not unusual traffic for the client, so they advised the analyst to whitelist it.

The analyst, however, was adamant that the client should take immediate action because they correlated that the contents of the inbound connections matched signatures of the Mirai malware variant.

The analyst blocked further communication from the attack source to ensure the client's assets were secured. The SOC suggested that the client apply configurations to their firewall and the targeted system to ensure full protection. Once complete, analysts concluded that the attacks were no longer occurring on the network.

When it comes to cyber-attacks, every second counts.

Contact us to learn more about how eSentire Managed Detection and Response™ can help protect your organization from cyber-attacks with 24x7 human monitoring, hunting, and threat remediation.

esNETWORK™ has the ability to interrupt traffic from many attack sources, protecting our clients' assets from known and unknown threats.

eSentire Asset Manager Protect, a global blacklisting feature provided by esNETWORK™, blocks known malicious IPs from infiltrating our clients' networks. As new IPs are added to the blacklist, the information propagates eSentire's ecosystem in a matter of seconds, protecting its global network of client sensors.