lastline

Case Study

Telecomm Giant Uses Lastline to Protect Against Advanced Threats

The Challenge

High availability is essential to the success of telecommunications providers. The growing set of cyberthreats from organized crime and hostile nation-states have put telecommunications providers at continual risk of network downtime or failure. Providers are required to deliver Emergency 911 services or face potential investigation and penalties by the Federal Communications Commission (FCC) for any interruption.

Telecommunications networks are high-value targets. Physical infrastructure attacks can enable attackers to commit fraud, access billing systems, and divert financial assets. For example, criminals use telecom infrastructure to enable SIM cards for use on their own infrastructure, as well as enabling traffic in other countries for which compensation is never received by the provider. Cyberthieves can also attack the networks that connect the physical transmission infrastructure and other network devices. The risks include PBX hacking, subscription fraud, and voice phishing. In short, once an attacker is inside the network, the potential for fraud, financial loss, and data theft is almost endless.

To protect its corporate networks, the provider had deployed both antivirus and email security appliances. The email and antivirus technologies were not enough to protect its networks and failed with regularity, resulting in increasing penetration of its networks by cyber threats. At the same time, the growing volume of alert traffic continued to overwhelm its security operations center (SOC) team. The SOC team was spending too much time on threats that were not severe enough to merit attention and not receiving alerts for some truly dangerous threats that were penetrating its defenses.

This telecommunications carrier determined that it urgently needed to find better security controls for the detection of sophisticated email-based threats. It had two essential technologies on its short list—perimeter defense to better detect and identify sophisticated threats, and threat intelligence to provide the latest information on advanced threats that could be integrated with its cyber defense efforts in real time.

The Solution

The telecommunications provider decided to deploy Lastline with its email systems to protect against malicious URLs, binaries, and attachments. Lastline's team completely integrated and deployed Lastline Defender™ across all of the carrier's multiple distributed data centers within a matter of hours. This installation was managed remotely and over the course of a single night.

Lastline's analysis, powered by machine learning and expert systems, interacts with suspect malware and creates a detailed inventory of every malicious behavior engineered into the code. It delivers the detailed information the organization needs to respond faster to evasive threats. This automated visualization of the timeline of events, the indications of compromise, and the unfolding kill chain uniquely empowered the telecom's analysts to make better and faster decisions, as well as to focus their energy on the most dangerous threats.

Executive Summary

Industry

Telecommunications

Company

Operates one of the largest wireless telecommunications networks in the United States, serving millions of customers.

Challenge

- Existing security solutions failed to identify and stop attacks
- Small security staff overwhelmed with unresolved investigations and endpoint cleanup and redeployment
- High volume of false positives and extraneous alerts wasted limited staff resources

Results

- Dramatically reduced the number of successful system compromises
- Decreased the number of investigations launched
- Accelerated threat detection and response

"We begin every instance of malware analysis by sending the file to Lastline. If we see something interesting, we then dig in as deep as we can."

"The corporate email security team loves Lastline because it catches stuff that two of our other security solutions miss. When I was looking for a sandbox utility for email, I performed a side-by-side comparison between Lastline and those other tools. Lastline outperformed both of them by a large margin."

The Results

Lastline® immediately provided improved detection of email-based threats. As a natural evolution, the telecommunications provider decided to expand its deployment to also monitor web traffic. Lastline was then able to correlate both the web and email threat data, thus allowing it to map out the entire attack footprint and improve efficiency. Lastline's combined solutions lowered the number of end-user systems infected via email and, most importantly, substantially reduced the amount of time spent by the SOC team on spurious alerts. This enabled the SOC team to focus on the true high-priority alerts. These integrated views of incidents of compromise regularly save hours per day for their incident response team.

"Lastline not only detected this new threat, but they also extracted it despite it being encrypted. This allowed me to look at the detailed report right away."

The time saved in incident response had another positive effect: it enabled the security team time to focus on other tasks to improve the organization's digital security posture. For instance, the security team began running a script that uses Lastline's APIs to distribute indicators of compromise (IoCs) generated from the analysis of email attachments. The team then pushed the IoCs to a threat stream feed designed to associate severity and confidence information with IoCs. Matches with the threat stream feed triggered responses that updated the firewalls in the enterprise network to block these malicious IPs. This highly automated workflow, along with other security-minded processes, helped decrease the number of investigations overall.

"I love Lastline's flexibility with integrations and the fact that we can use Lastline's API to customize our tools on the network. I'm continually impressed by how Lastline's solutions go above and beyond other tools in the same area of focus."

Summary

Lastline's NDR platform detects and contains sophisticated threats before they disrupt your business, on-premises or in the cloud. It delivers the cybersecurity industry's highest fidelity insights into advanced threats entering or operating in your entire network, enabling your security team to respond faster and more effectively to threats.

The Lastline Defender Platform uses a combination of three complementary AI-powered technologies to detect the advanced threats that other tools miss and significantly reduce false positives:

- Artifact analysis to detect malicious content attempting to enter your network via web or email
- Network Traffic Analysis (NTA) to detect lateral movement of evasive threats already inside your network
- Intrusion Detection/Prevention (IDPS) to detect known threats

This unique combination enables deterministic detections and eliminates most false positives. You can respond faster and more effectively, with fewer resources.

Request a Lastline demo today

Lastline, Inc.
1825 S. Grant Street, Suite 635
San Mateo, CA 94402

Americas: +1 877 671 3239
www.lastline.com
info@lastline.com