lastline

Case Study

Major University Chooses Lastline for Quality of Detection, Ease of Use, and Intuitive Interface

The Challenge

Universities have a responsibility to not only provide reliable online access to support research, students' academic work, and general communication, they need to do so securely. It's essential that they protect students', faculty's, and staff's identity and personal information plus the university's intellectual property. This is made particularly challenging by the number of devices that all parties bring to campus every day and the general rate of turnover as students graduate and new ones arrive.

Universities are heavily targeted because of their typically open network that's needed to support research efforts and the volume, and value, of the data that's available, including research, IP, financial records, and even email addresses that can be used in subsequent phishing schemes. Accordingly, universities' security teams are continually looking to improve their ability to detect and prevent cyberattacks.

This university is one of the largest public universities in the US, serving 75,000 faculty, staff, and full-time, part-time, on-campus, and remote students. Their 14-member security team wanted to improve their ability to analyze malware in all inbound traffic in order to decrease the risk of a successful attack. The state's system-wide management had previously negotiated access to FireEye at a discounted price or possibly for free. This campus also was using Cuckoo malware analysis, and the security team considered both inadequate for their needs.

Considering that IT does not control all of the endpoints (e.g. student's phones and computers), they realized that an EDR solution would be insufficient and they needed a new solution to monitor their network. They launched an evaluation of possible solutions that included FireEye, VMRay, Joe Sandbox, and Lastline with the objective of finding the "best" tool, as per their Chief Security Officer. As part of the bake-off, Lastline deployed software to check all email and websites for possible malicious attachments or behavior, plus our Global Threat Intelligence Network (GTIN) that contains indicators of compromise (IOCs) from all previously detected malware samples, including some samples that specifically targeted this university.

The Solution

Lastline deployed its software for a 30-day trial in July 2019, and as a result of the trial, including side-by-side tests of each tool's ability to detect known and new malware threats, the university decided to purchase Lastline in September 2019.

The security team is very good and very technical, as one would expect at an academic institution. They selected Lastline because, as they commented, our software was significantly better in our analysis than the other products they already had or were also testing.

The team particularly liked Lastline's IP Reputation list and other information contained in the GTIN. They liked the simple user interface that was easy to understand, and "absolutely loved" the Timeline view that showed precisely when each element of an attack took place, from an email arriving, for example, to when a student clicked on a link, a potentially malicious attachment was downloaded, and any subsequent actions attempted by the malware.

"Lastline had great detection"

Executive Summary

Industry

Education

Organization

One of the largest public universities in the US with a total of 75,000 students, faculty, and staff.

14 people on the Security Team.

Challenge

Existing malware analysis tools were inadequate. Concern that they were missing malware-based attacks.

Results

- Purchased Lastline malware analysis and access to Global Threat Intelligence Network
- Significantly improved analysis and detection
- Quality of detection, ease of use, and intuitive interface led them to extend access to Level 1 analysts

The Results

During the 30-day test, the university's security team quickly defaulted to Lastline because they quickly realized that it achieved the CSO's mandate of being the best. They quickly replaced their current tools with Lastline, and, as per the Incident Response Supervisor for IT Security, "When you turned off the (test), the team was very disappointed." He further explained that during the month of testing, the team got very comfortable with Lastline and started using it in their internal workflow, replacing FireEye and Cuckoo. When it was turned off after the 30-day trial, they had to fall back to the old ways, which was difficult and less effective, and contributed to the quick decision to purchase and permanently implement Lastline.

Furthermore, the team felt that Lastline was so good at the analysis and so easy to use from the interface perspective that they were intending on extending access to Lastline software to Tier 1 analysts, which they didn't feel they could do with the other candidates.

> ***"Lastline was head and shoulders above the competitors."***

Summary

Lastline offers the industry's best file analysis and malware detection technology, as evidenced by achieving 100 percent breach detection three years in a row in a well-known independent test. The company's patented Deep Content Inspection™ emulates a complete operating system and hardware environment, delivering unmatched visibility into the malware, all programs and services it invokes, all operating system functions, CPU instructions, and all kernel activity. It deconstructs every malicious behavior engineered into an object entering via mail or web traffic so that we see all instructions that a program executes, all memory content, and all operating system activity. This visibility enables us to inventory unique file behaviors that other tools fail to detect.

This university quickly understood the benefit of these capabilities. They particularly liked Lastline's superior analysis, the easy-to-use interface, the Timeline feature, the level of detail provided about each detected malware sample, and the information provided in the GTIN that reflects all detections by Lastline's entire ecosystem of customers and partners.

> ***"Lastline met ALL our needs"***

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

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