TAG CYBER

Agentless Visibility of Network Threats

I first met Christopher Kruegel and Giovanni Vigna, co-founders of *Lastline*, when I was programming cyber security conferences. The pair submitted talk abstracts for our largest conference. For those unfamiliar with the call for presenters (CFP) process It goes something like this: the conference team solicits presentation abstracts from would-be speakers. Then, a team of reviewers, typically comprised of an internal content expert plus external advisory board members, reviews submissions for fit, clarity, level of expertise, interest, etc. For larger conferences that receive hundreds or even thousands of proposals, the conference organizers might form subcommittees of 2-3 people to review all submission in a given topic area (e.g., “hackers and threats” or "security strategy”). For our conference, since we typically received fewer than 200 submissions, the entire committee reviewed and scored each submission.

My review committee consisted of me plus 6 advisory board members. Each reviewer would score an abstract a “yes,” which equaled 2 points, “maybe,” which equaled 1 point, or “no,” which equaled zero points. Of the total body of submissions, fewer than 5% ever received 14 points, meaning, every member had scored the proposed talk a “yes.” Both Vigna’s and Kruegel’s proposals were in that top 5%. They were accepted to speak at the event the coming spring.

Now, a skeptic might say speakers could game the system or point out that a well-written proposal doesn’t equal a standout conference talk. Sadly, both are true. However, in Vigna’s and Kruegel’s case, neither proved true. Drawing on their academic background—both are professors at UC Santa Barbara—they understood that the foundation of any good conference talk is research, first-hand experience, and the ability to covey a compelling story.

When they were selected, I didn’t know either Kruegel or Vigna personally, and I’d only heard of Lastline because of their proposals. Following their excellent presentations at the event, I learned more about them and their company, and Vigna generously contributed to articles and video interviews for my company’s content program.

Research roots

What impressed me about the Lastline founders’ work was their dedication to academic research and their willingness to share with the community. Although they run a vendor company, Krueger and Vigna, along with the third co-founder, Engin Kirda (a professor at Northeastern University and former faculty at institutions across Europe), are among three of the world’s most published cyber security researchers. Their fierce commitment to ongoing learning and evolution in the academic world is reflected in their output in the private sector.

Now in its ninth year, the idea for Lastline started with a research project on malicious behavior analysis. This took the founders down the path of network detection and response. On a recent call with Lastline’s Mustafa Rassiwala, Sr. Director Product Management, and Chad Skipper, VP of Product

Innovation, the pair explained that their platform often gets confused with endpoint detection and response (EDR), but, Skipper said, “Lastline Defender is not agents on endpoints; we use the entire network, layers 2-7, as the data source. Why? The network doesn’t lie. It’s the ground truth. It sees everything.”

Network focused

Customers deploy network sensors that collect and correlate network data (on-premises or in the cloud), multiple hosts, and channels (e.g., email). Additionally, Lastline has 100+ integration partners that provide threat telemetry from millions of end users. This massive collection of network data, said Rassiwala, gives them “the ability to learn about network behaviors on a scale others can’t.” This data collection becomes the training data for their machine learning, which, in turn, provides context around observed malicious behaviors.

The question then becomes: how does Lastline handle the growing prevalence of software-defined networks (SDNs), encrypted traffic, and cloud usage? As these shifts occur, not all traffic is available for analysis, and that can lead to blind spots. In those cases, Skipper said, the platform has encrypted traffic analytics that looks at header information and network metadata: router information, the length of packets, time stamps, certificates, and more. “You get a lot from the metadata,” he said, “and we train our machine learning models on metadata from malicious traffic. We can pull from VPC [virtual private cloud] logs and TAPs or proxies if the customer’s data is in the cloud.”

Although the team hesitates to use the word “sandbox” with customers, lest their technology be confused for a stand-alone sandboxing application, it is the file behavior observed in the sandbox that gives Lastline the ability to identify malicious behavior, allowing threat analysts and incident responders to inspect malware, safely execute advanced malware samples, and understand their behavior while remining invisible to the attacker. Unlike traditional sandboxes, however, Lastline’s detection uses hardware emulation techniques rather than relying on detonation in virtual machines. This results in fewer false positives, higher detection rates, and full visibility into malicious activity.

The ground truth

In an age when plenty of cyber security tools are focused on the latest trends, it’s refreshing to see a company focusing on the network—because it is the network, even if it’s a cloud network—where all the interesting things happen. Yes, data and the applications which contain data are what malicious adversaries are after, but the network is how they get there. Besides, cyber security isn’t an “either/or” decision. Good cyber security programs are layered, and the network is (quite literally) the pathway to protecting data/applications/systems on the network.

Whatever the future holds, the team at Lastline has an ardent commitment to improving network detection and response, as is evidenced by their multiple roles as product builders, researchers, and educators. Their continued ties to the greater cyber security community through research and educational outreach—both in an out of academic settings—provide an objectivity which allows whatever they build for the commercial market to remain grounded. It’s this triad of capabilities— a focus on the *network*, an academic *research* background, and a massive *channel* built from community relationships fortified by proven work—coupled with their approach to machine learning that make Lastline worth a look. If you’ve been thinking about improving your capabilities in network detection and response, network traffic analysis, IDS/IPS, file analysis or any of the plethora of categories combatting threats against your networks, give them a call and let us know what you learn.

About TAG Cyber: Founded by Dr. Edward Amoroso in 2016, New York-based TAG Cyber democratizes cyber security research and advisory services for enterprise professionals around the world. The TAG Cyber Security Annual provides free guidance on the cyber security industry based on fifty+ identified controls. The company also offers expert consulting services, as well as a Cyber Corps platform designed to help students learn the craft of cyber defense.

About the author: Katie Teitler is a senior analyst at TAG Cyber where she collaborates with security product companies on market messaging, positioning, and strategy. In previous roles, she has managed, written, and published content for two research firms, a cybersecurity events company, and a security software vendor. Katie is a co-author of “Zero Trust Security for Dummies.”