The Silicon Review

SPECIAL EDITION

MAY 2017

HOLD THAT THOUGHT !! / PG- 8

LEADERSHIP TECHNOLOGY CEO NEWS BUSINESS FEATURES CIOs

SR 2017

50 Most VALUABLE BRANDS Of The Year

CHRISTOPHER KRUEGEL | CO-FOUNDER | CEO

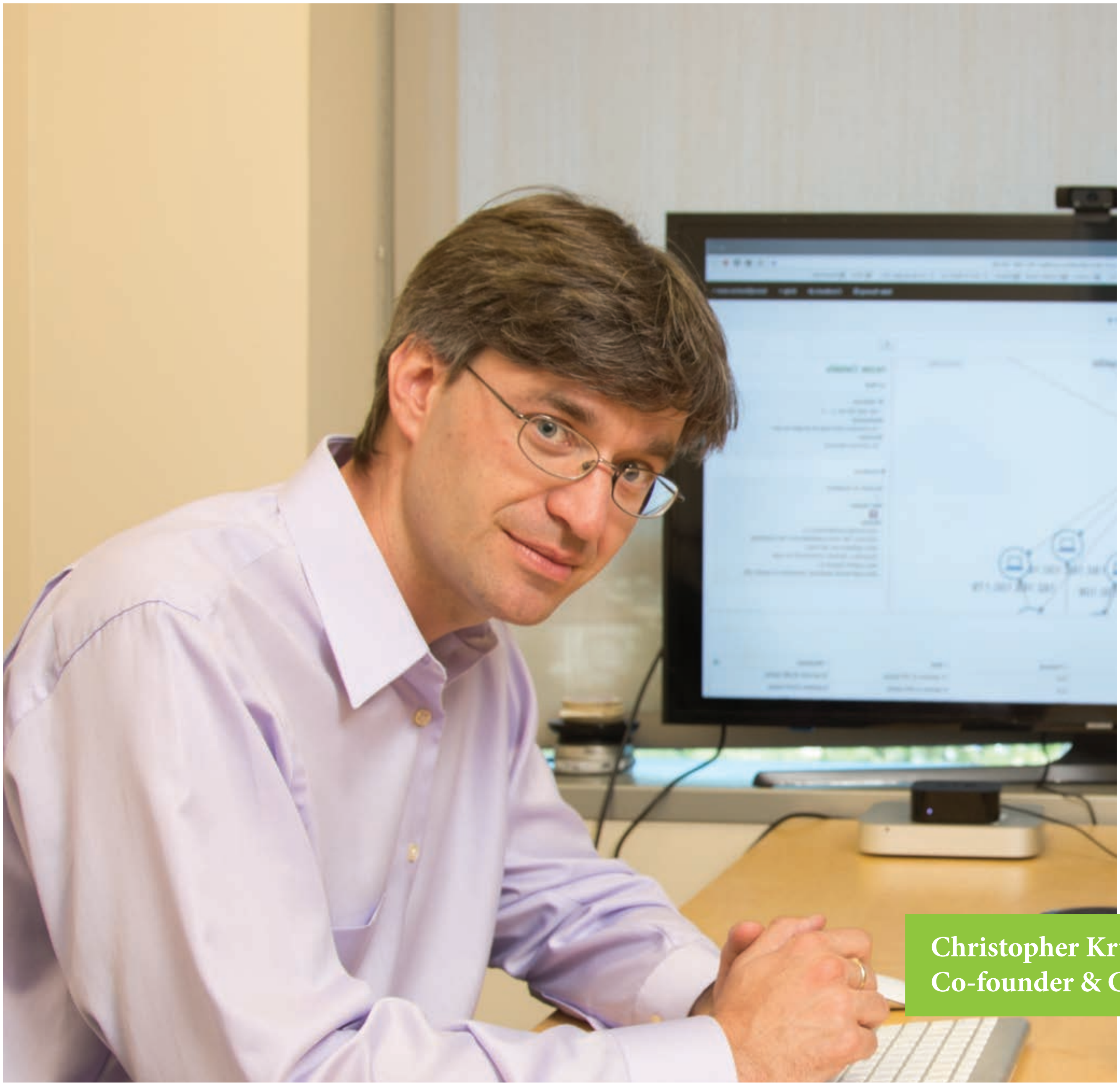
Defeating advanced malware before it infiltrates your network:

Lastline

www.thesiliconreview.com

Defeating advanced malware network: Lastline

"Our mission is to enable our customers to defend their organizations against advanced, evasive malware that cause costly data breaches".



Christopher Kruegel, Co-founder & CEO

before it infiltrates your

COVER STORY

lastline™

Today, organizations are facing a host of cyber threats, some with severe impacts that will require security measures that go beyond traditional solutions. Enterprises must secure mobile devices, cloud services, the Internet of Things (IoT), and integrated supply chains. Accordingly, they are looking for how to ensure that security measures are in place to detect and rapidly respond to threats anywhere across the attack surface. As Dr. Gary Hinson says, *"Security is like brakes in your car. It slows you down, but it also makes it possible for you to go a lot faster."*

It seems like every week we see headlines indicating that another large corporation has suffered a major data breach, over half of which are the direct result of malware. This is happening even though corporations with more than 1,000 employees are spending an average of $15M a year on enterprise security. Despite that massive investment, companies are still struggling to deal with the fact that every day the odds are increasing that they will be the victims of a data breach. With every improvement in security technology, the criminals counter-punch with new innovative attacks that include sophisticated malware that evades detection. The extreme lack of qualified candidates to fill open security analyst positions doesn't help. As most security professionals will agree, it is not a matter of if, but when.

In response, many enterprises recognize the importance of gaining visibility into how malware operates and are investing in advanced malware protection technologies that decrease the risk of data breaches and increase security team productivity. These forward thinking organizations are increasingly turning to companies like Lastline for assistance.

Lastline was co-founded in 2011 by Christopher Kruegel and is

Innovation distinguishes between a leader and a follower

Meet the ingenuity

Christopher Kruegel, Co-founder/ CEO: Christopher Kruegel has deep expertise in computer and communications security, focusing on malware analysis and detection, web security, and intrusion detection. He is a member of the Computer Science faculty at UC Santa Barbara and regularly serves on program committees of leading computer security conferences. Chris has published more than 100 peer-reviewed papers in top computer security conferences, and has been the recipient of the NSF CAREER Award, MIT Technology Review TR35 Award for young innovators, IBM Faculty Award, and several best paper awards. Chris was also the head of a working group that advised the European Commission (EC) on defenses to mitigate future threats against the Internet and Europe's cyber-infrastructure.

headquartered in Redwood City, California. Christopher's motivation throughout his academic and professional career has been to understand malware and thereby, improve defenses against cyber crime. After getting his PhD in computer science in 2002, he embarked on his mission to defeat malware and subsequently founded Lastline. Lastline is dedicated to creating innovative solutions that provide the best defense against, and the most complete visibility into the behavior of advanced malware. The company's technology rapidly detects advanced malware that other security solutions miss, provides additional context that delivers complete visibility into the threat, and eliminates resulting breaches, saving money and time for their customers, while protecting their valuable data and brand reputation.

The quality of a leader is reflected in the standards they set for themselves

In conversation with the ingenious–Christopher Kruegel

What was the inspiration behind setting up Lastline?

I started my post-doctorate career as a professor of computer science at Vienna University of Technology and then at UC Santa Barbara. Two of my peers in academia, Dr. Engin Kirda and Dr. Giovanni Vigna, shared my interest in understanding malware and how to detect it. We researched and wrote papers about a technique known as sandboxing, which would become a cornerstone technology, not only for Lastline but for other players in the security industry. As a team, we developed two system, one called Anubis (for analyzing unknown files), and one called Wepawet (for analyzing web pages), which soon had more than 100,000 monthly users.

We set the trend of using behavioral analytics and machine learning to detect attacks and identify malware before it became mainstream in the industry. Our work on using these techniques to detect threats has become the basis for much of the detection technology in use today.

After pioneering these novel malware detection techniques and recognizing the resulting demand for a commercial solution, we started Lastline to help organizations innovate the way they prevent data breaches caused by advanced persistent threats, targeted attacks, and evasive malware.

How does Lastline prevent data breaches? And how does it create visibility into evasive malware?

To defeat malware, you must know malware. Starting with my academic career and continuing today at Lastline, we study and understand malware better than anyone else. Armed with this knowledge, we designed technology to detect all phases of a malware-based attack and provide the enterprise security team with visibility, context, and integrations required to quickly detect, understand and defeat the attack.

The company analyzes all executable content introduced to a company's network, regardless of the point of entry, and then uses our patented Deep Content Inspection™ capability to gain complete insight into the specific actions that any file was designed to execute. Our unique system emulation architecture does not provide evidence to the malware that it is being examined, so the malware behaves as if it's on a victim's machine, exhibiting all of its activities and giving us a level of visibility that other solutions cannot deliver.

Lastline's Full System Emulation (FUSE™) interacts with the malware at the memory and processor levels, not just at the OS and application levels. As a result, it can see through evasion techniques and detect all of the specific activities a file was designed to carry out, such as checking security settings, trying to detect if it's in a sandbox or running on a VM, or executing code injections. Malware can't execute a behavior that we can't see, all while in a secure environment.

Despite our solution's very high rate of malware detection (we achieved 100 percent detection effectiveness in NSS Labs' test), a sandbox alone is insufficient for detecting all threats, as there are other ways for threats to gain access to a network, such as through compromised personal devices and through unprotected parts of the network such as partner gateways. We gain further visibility into attacks by collecting and analyzing network traffic.

Knowing the specific behaviors that the malware was designed to execute provides the key to quickly defeating an attack. Any activity that malware attempts across a network, such as contacting its C&C server or moving laterally to other systems, can immediately be linked to the infected device and the attack becomes visible. With insights into the specific devices and actions involved in the attack, the security team can quickly take action to block malicious activity and clean infected systems.

Why is context such an important element of advanced malware detection?

Lastline aggregates and correlates local events to provide analysts with a single, complete view of not only what a malicious file is designed to do, but also any C&C contact and anomalous network traffic that may be been caused by malware introduced by other means. For example, instead of delivering individual alerts for each action, which overwhelms SOC teams with low-level information, we merge related events from the same attack into a single incident, providing a complete view of an attack to speed investigation and remediation.

The analysis is further informed by the Lastline Global Threat Intelligence Network, which consolidates details about malicious files and their associated behavior from all customers and partners in the Lastline community (in an anonymized fashion). Details include active command and control (C&C) servers, objects with zero-day exploits, Indicators of Compromise (IoCs), toxic web sites and malware distribution points identified as having breach intent. Information in the Threat Intelligence Network from previous attacks can inform new analysis to speed detection and helps analysts quickly take specific actions to prevent damage. Our threat data ensures that as soon as one of our users experiences a new threat, all of our customers have access to full details. This keeps their threat detection capabilities up to date as the threat landscape changes, and it supports proactive defense.

Informed by local analysis and global threat intelligence, our technology shows everything malware has done – how and where it entered the network, communications with C&C servers, other systems that have been attacked by lateral movement, and more – so security teams know how to completely eradicate the malware from their network.

How do integrations complement visibility and context to improve the prevention of malware-based data breaches?

Enterprises have dozens of

stand-alone appliances and applications that must be managed and maintained.

Our philosophy is to fit into existing security architectures to improve the effectiveness of other solutions while providing added malware insights and detection. Lastline can ingest data from other solutions to inform our analysis and provide additional context for suspicious activity.

For example, through our integration partners, an unknown file can be submitted to Lastline for analysis, speeding intervention efforts by identifying latent threats.

In addition, Lastline can push information to other solutions to improve their effectiveness, such as sending blocking rules to NGFWs (Next-Generation Firewalls) or UTM (Unified Threat Management) devices, send breach event information to SIEMs (Security Information Event Management), block connections via Intrusion Prevention Systems, or add evasive malware understanding to Secure Web or Email Gateways.

The net result is unmatched file- and network-based detection of advanced malware before it can carry out an attack, full context to focus and speed intervention, and a *"fit-in"* mentality that improves the effectiveness of our technology as well as that of our integration partners. I hear from customers regularly how they are detecting malware sooner in the attack chain where it's easier to mitigate, investigating a much higher percentage of alerts, and improving the efficiency of their security teams.

Lastline in the field!

Lastline provides protection to a national media company against advanced threats that elude standard virus protection systems. Security teams at this organization considered a number of options, including FireEye, before selecting Lastline's software platform.

"Lastline has provided a non-obvious solution to an obvious threat, by embracing that most attacks are socially engineered and no solution should rely on signature detection."

Lastline alerts the organization's corporate IT team of at-risk hosts that are active on the network. The team is able to respond to the threats before they do any damage.

The company can now rest knowing their users and their own corporate assets have another layer of defense shielding them from advanced persistent threats, zero-day attacks, and evasive malware.

Lastline's salient partners

Lastline has an ecosystem of dozens of partners around the world with proven technology integrations. Our ecosystem includes technology partners such as Carbon Black, Guidance Software, Barracuda Networks, Check Point Software, Symantec, and Tripwire; strategic partners, including Forcepoint, WatchGuard, SecureWorks, and SonicWall; and a global network of channel partners.

Awards and Accolades

Lastline has been honored and recognized as a leading provider of Advanced Malware Protection solutions by numerous industry leaders, publications, analysts from around the world. Here are glimpses of the Lastline's achievements.

The company was honored as Gold Winner of the Info Security Products Guide Global Excellence Award, Golden Bridge Awards Grand Trophy Winner, Cyber Security Excellence Award for Advance Persistent Threat Protection, and the SINET 16 Innovator award.

> "At Lastline, 'good enough' isn't. The goal is to get it right."