WEBROOT
Smarter Cybersecurity™

The Future of Threat Intelligence

Featuring Perspectives from David Bennett

Worldwide VP Consumer & SMB Sales Webroot Inc.

TABLE OF CONTENTS

Background 3

A Collective Threat Intelligence Approach 3

The Role of Policy 4

Opportunities for Solution Providers 4

BACKGROUND

During the Second World War, Alan Turing developed what became known as one of the first computers. This device would eventually predict the daily settings of the German Enigma Code Machine in what was then considered near-real time. This development gave the Allies the ability to decode all intercepted Third Reich communications, and, in no small part, lead to the liberation of Europe.

Today, in our fully connected real-time world, the Internet of Things has raised the stakes on how we monitor and respond to security threats. We live in a world in which our refrigerators can contact service centers when they need a repair, our thermostats send us emails, and our televisions are connected to our social media accounts. Each of these new endpoints represents an instance in which data could be intercepted and our networks could be compromised. With increasing levels of interconnectivity and constant data transfer, the phrase "real time" has taken on a whole new meaning.

In May 2015, the FBI detained an ethical hacker who had plugged his laptop into the entertainment system underneath the seat of a commercial airliner in flight and successfully commanded the plane to climb. In effect, he had temporarily hijacked the jet. His purpose was to point out security flaws and help us realize that every access point requires protection—that the nature of threats changes constantly.

"The Internet of Things is the biggest game changer for the future of security," according to David Bennett, Vice President of Worldwide Consumer and SMB Sales at Webroot. "We have to figure out how to deal with Smart TVs, printers, thermostats and household appliances, all with internet connectivity, which all represent potential security exposures."

A COLLECTIVE THREAT INTELLIGENCE APPROACH

The climbing rate of technological advancement demands a new approach to protecting our data and assets from pranksters, thieves, and organized groups intent on fraud or cyberterrorism. This new path is comprehensive, real-time, collective threat intelligence. The days of waiting for an attack to happen, mitigating its impact and then cleaning up the mess are gone. We also can't just lock the virtual door with a firewall and hope nothing gets in; the stakes are too high. The goal must be to predict potential exposure in advance—and that's where threat intelligence comes in. According to Bennett, this new approach to threat intelligence must be:

» Real-time – the velocity and volume of threats increases on a daily basis. The technologies we use to protect our systems must be updated by the minute. We must have the ability to adjust to the nature and type of new threats as they appear. Data must be aggregated from sources globally and delivered as actionable information to the security professional.

» Contextual – Data must be parsed through sophisticated computer analytics so humans can make decisions based on actionable intelligence. An analyst must be given data with pre-connected dots in order to act quickly. There's little time for onsite security professionals to analyze reams of data when they suspect an attack is underway. By the time they figure out what's going on, the damage is done.

» Collective – It's not good enough to understand what's happening in just your local environment. An attack on one of your competitors or peers means you could be next. To analyze complex threat patterns, threat intelligence technology must be big data driven, cloud-based, and must aggregate activities from across companies and across geographies.

"Security professionals of the future must act like intelligence officers or analysts," according to Bennett. "They have to consume information that's already been parsed for them, and make decisions based on that intelligence." Bennett goes on to say, "Success will depend on how they are fed the data. How is it presented? Is it relevant? Have the irrelevant data points already been removed? Only then will they be able to make decisions in time to prevent breaches."

THE ROLE OF POLICY

In addition to a solid foundation in technology, strong cybersecurity is a matter of policy and awareness at the user level. "Security starts with information; making users aware of the type of threats that exist and teaching them how to be vigilant," says Bennett. But effective threat intelligence can't prevent users from being careless or ignorant regarding security. This means educating users on creating and maintaining stronger passwords, and imparting best practices for securing corporate information on their personal devices. According to Bennett, when developing security policies, IT organizations must consider three things:

» Policy flexibility – Companies can't simply lock down the whole network and expect to be able to serve their customers. There will always be exceptions and exceptions must be managed.

» Practicality – Does the policy make sense? For example, banning the use of personal devices for business just isn't realistic for firms with large field organizations who regularly work remotely.

» Feasibility – Policies must be achievable. A policy might sound good on the drawing board, but, in practice, prove impossible to enforce.

OPPORTUNITIES FOR SOLUTION PROVIDERS

Both pure play managed services firms and IT solution providers deliver services remotely as a way to provide support to SMB clients.. These services include basic server management and monitoring, all the way up to higher value services, such as managing backup and storage for key systems. These services are most valuable for customers who lack the internal resources necessary to effectively manage complex systems, or customers seeking to defer capital expenses in favor of leveraging operational budget. Cybersecurity is a perfect discipline to apply the managed services model. "The biggest untapped opportunity for our partners today is providing security as a managed service," according to Bennett. "Users are overwhelmed and just not capable of keeping on top of the rapid changes to the nature of threats."

Managed security services address one of the major problems users face today: the lack of access to talented security professionals. Particularly for SMB customers, finding and competing for talent with larger firms can be daunting. "Hiring and retaining the right personnel should not be a vulnerability in and of itself." Bennett continues, "Users who leverage security managed services remain protected through transitions in their IT staff, and lower the risk of losing institutional knowledge critical to their security procedures. In addition, managed security services represents one of the largest and most profitable growth opportunities today for solution providers."

Webroot has built a collective approach to threat intelligence, and continues to grow and lead the way with technology that collects and aggregates information in real time. Bennett states, "For our customers, Webroot technology works like having their own dedicated security firm to monitor their environment. We don't just collect data. We scrub it, make correlations globally, and pass on exactly what they need to reduce exposures. It's a big data approach to cybersecurity, and it's the only effective means to combat the ever-changing threats companies face."

For more information on Webroot and collective threat intelligence, visit webroot.com/partners.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
800 772 9383

Webroot EMEA
6th floor, Block A,
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0)870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900

DS _ 090115 _ US