threatpost
The Kaspersky Lab Security News Service

Monday, October 22nd, 2012

October 16, 2012, 10:41AM

Gathering Threat Intelligence With Open Tools

(/en_us/blogs/gathering-threat-intelligence-open-tools-101612)

by **Dennis Fisher** (/author/Dennis Fisher)
Follow @DennisF
(https://twitter.com/DennisF)

Threat intelligence is one of the go-to buzz phrases for many people in the security industry right now, and it's thrown in so many contexts and situations, it's quickly becoming almost meaningless. Most people understand that they need to get better information about what's happening both on their own networks and in the broader landscape, but few people are talking about how exactly to go about gathering that data, outside of trying to sell you a SIEM installation.

The issue, then, isn't whether you need better threat intelligence, but what tools can help you accomplish that task.

"Targeted attacks are the norm now and a lot of the threats are bypassing traditional security monitoring tools and a lot of the approaches we've been taking aren't going to be effective," said Kevvie Fowler, practice leader, intelligence analysis at TELUS and founder and principal consultant at Ringzero.

Editor's Pick

Adobe Extends Security of Reader and Acrobat With Better Sandbox, Force ASLR
(/en_us/blogs/adobe-extends-security-reader-and-acrobat-better-sandbox-force-aslr-101712)

Some Wordpress Themes, Thousands of Sites Open to XSS Vulnerability
(/en_us/blogs/some-wordpress-themes-thousands-sites-open-xss-vulnerabilities-100312)

CRIME Attack Uses Compression Ratio of TLS Requests as Side Channel to Hijack Secure Sessions
(/en_us/blogs/crime-attack-uses-compression-ratio-tls-requests-side-channel-hijack-secure-sessions-091312)

Threatpost Newsletter Sign-up
(/en_us/node/1690)

"People have been preaching this for a while and saying you need to go out and get this thing called intelligence. But no one gets down to specifics, it's just motherhood and apple pie. Just use Google and that will address the gaps in your security program."

One of the problems is that people often confuse data with intelligence. The two are not interchangeable, Fowler said, and in fact the collection of data is just one step in the process of producing intelligence. Many organizations have giant piles of data laying around that they've collected from their IDS, SIEMs and other security devices, but they're not sure what to do with it or how to derive any value from it.

"People need direction to go out and tackle that mound of information and pull out what's valuable to you," Fowler said. "Intelligence is relevant information that's got actionable advice attached to it. If you hand that to someone, it should tell people what it is, why it's important and what they can do about it. Pull out the relevant data and feed it into your SIEM and make an intelligent decision based on that information."

Fowler, who gave a talk on this topic at the SecTor conference recently with Naveed ul Islam, a security intelligence architect at TELUS, said that many of the tools that are best-suited for the task of intelligence gathering are freely available online and you just need to know how to use them and what to do with the results.

One of the main tools that Fowler and Islam like to use is SiloBreaker (http://www.silobreaker.com), a search engine that returns content not just from Web sites, but from a variety of other sources, as well, including social media networks. It will aggregate data by

category and users can search in specific categories, such as IT or science.

Islam also recommended that IT staffs take advantage of simple tools such as Google Alerts or Social Mention (http://socialmention.com/), a site that enables users to set up real-time alerts for specific topics or keywords as they're mentioned on various social networks. NewsPet (https://code.google.com/p/news-pet/) is another useful tool, Islam said. It's a trainable news reader that will learn what's important to the user as she places items into specific categories. The beauty of these tools is not only that they're effective at finding relevant needles in massive haystacks of irrelevant data, but they're free.

"A lot of organizations we talk to about intelligence have constrained budgets and whether you're small or large you can use open-source intelligence," Fowler said. "Any organization can do this."

Commenting on this Article will be automatically closed on January 16, 2013.

Comments

Post new comment

Your name:

Anonymous

E-mail:

The content of this field is kept private and will not be shown publicly.

Comment: *

Save Preview