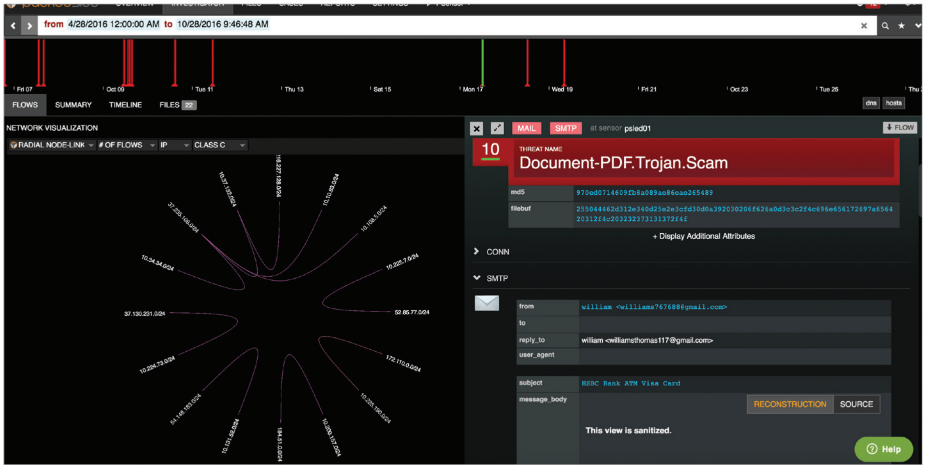
SC MEDIA
INDUSTRY INNOVATOR

Next-generation security monitoring and analytics

PacketSled



10

THREAT NAME
Document-PDF.Trojan.Scam

md5 970ed0714609fb8a089ae86eae265489

filebuf 255044462d312e340d25e2e3cfd30d0a392030206f626a0d3c3c2f4c696e656172697a6564 20312f4c2032323731313 72f4f

from william <williams767688@gmail.com>

to

reply_to william <williamsthomas117@gmail.com>

user_agent

subject HSBC Bank ATM Visa Card

message_body

This view is sanitized.

We run PacketSled in our SC Labs as part of our honeynet analysis. In fact, the analytics – attacks against the honeynet, for example – reported in the "Threat Hunter" blog come directly from our PacketSled deployment, so it is no surprise that we have a lot of experience with this Innovator. PacketSled is, usually, a SaaS tool but there is an on-premises version as well. We especially like the support feature that consists of clicking a button on the desktop to open a chat session with an engineer. We never have seen that level of support response in any of the products we have reviewed and it provides a real benefit both to new users and experienced users with a difficult problem.

Another feature that we like is the query language that lets users focus in on issues that may be related to an event in the enterprise. The core that supports that query language is Bro, the network analysis framework. The queries are simplicity themselves to write, but if you don't quite have the knack of Bro yet, the query manager has an autocomplete function.

PacketSled has multiple screens, each with a particular function. The main screen is the overview and it shows a comprehensive picture of sensor activity. From this screen, users also can open cases set up in the Investigator screen. It is on the Investigator screen where users can initiate queries that can be in the Bro-like query language, which resembles regular expressions. Additionally, there are automated captures that look specifically for such things as suspected command-and-control servers accessing (or being accessed by) your enterprise.

What's coming? More and deeper analytics of course. You never can have enough of that. Also, enrichment, such as full export and import of Stix profiles – a particular hot button for us – and more visualizations. With all of that, this Innovator is carving its place in the marketspace in high style.

– Peter Stephenson, technology editor

packetsled

Offices in Seattle and San Diego
6285 Lusk Blvd., San Diego, CA 92121
www.packetsled,com
Phone: 858-225-2352
Contact: sales@packetsled.com

DETAILS

Vendor PacketSled
Flagship product PacketSled
Price Pricing is consumption and retention based starting at $35,000.
Web packetsled.com
Innovation Applying advanced analytics to threat hunting and evolving an analyst's tool into an analyst's tool that also has very strong monitoring, detection, case management and alerting functions.
Greatest strength Strong analytics and versatility.We run PacketSled in our SC Labs as part of our honeynet analysis. In fact, the analytics – attacks against the honeynet, for example – reported in the "Threat Hunter" blog come directly from our PacketSled deployment, so it is no surprise that we have a lot of experience with this Innovator. PacketSled is, usually, a SaaS tool but there is an on-premises version as well. We especially like the support feature that consists of clicking a button on the desktop to open a chat session with an engineer. We never have seen that level of support response in any of the products we have reviewed and it provides a real benefit both to new users and experienced users with a difficult problem.

Reprinted from the December 2016-January 2017 issue of SC Magazine • www.scmagazine.com