CASE STUDY

PSCU

DESCRIPTION

PSCU is a leading credit union service organization in the United States. Founded in 1977 and based in St. Petersburg, Florida, PSCU provides the payment products and services that credit unions require to compete with other financial services providers. These services include transaction authorization and settlement, 24/7/365 call center support, and online and mobile services. What this means is that if you are a member of a credit union and have a card balance inquiry, it's very likely that you've interacted with PSCU.

LOCATION

United States

OVERVIEW

PSCU employs 1,700 full-time employees who serve credit unions and their members. PSCU brings to bear significant resources to manage security and to protect their Member-Owners' data and adheres to PCI data security standards.

While running current best-of-breed firewall, web proxy/gateway, endpoint, and SIEM systems, PSCU's Chief Information Security Officer, Gene Fredriksen, knew that the PSCU network could still potentially sustain malware infections.

Gene observed, "The prevention solutions we had in place were already best-in-

> "The prevention solutions we had in place were already best-in-class, but we wanted an even higher level of detail to minimize and manage potential exposure."
>
> Gene Fredriksen, CISO

class, but we wanted an even higher level of detail to minimize and manage potential exposure."

Gene's team evaluated the performance of all pieces of the security infrastructure and considered adding new sandboxing technology and upgrading their SIEM in an attempt to address malware more effectively. However, Gene was not convinced such an upgrade would actually solve the problem.

THE SOLUTION

After evaluating a number of solutions, PSCU deployed Seculert's automated infection detection platform. Gene and his team particularly liked the short deployment cycle and the fact that not a single false positive malware report was generated during the following year.

During the first year of deployment, Seculert's automated infection detection platform identified eight unique malware families attempting outbound communications to malware servers. This discovery is based on automated log analysis of gateway outbound HTTP traffic logs generated and on Seculert's Botnet Interception technology. Of the eight families discovered, four were considered critical. The immediate and precise alerting enabled the PSCU Security Team to quickly remediate the threats. PSCU also found that the systems were not generating any false positive alerts, escalating the confidence in the Seculert information provided.

THE BENEFITS

The Seculert Platform only reports on malware infection incidents that are 100% verified. When a new or recurring infection is discovered, the Seculert Platform generates an actionable infection report which gives SOC and Incident Response teams all of the information they need to quickly and effectively to mitigate the infection.

CONCLUSION

PSCU discovered value in the approach of complementing their prevention/search solutions with a post-infection detection technology. Gene Fredriksen recently stated, "Having run the Seculert Platform for one and a half years now, we have found it to perform as promised. While the number of incidents involved is relatively small, there's a big difference given our business model between having almost no malware on our network and having some of these very sophisticated attacks on our network."

United States

2880 Lakeside Drive, Ste 228
Santa Clara, CA 95054
Tel: +1 408 560 3400

Israel

6 Efal Street, P.O. Box 3970
Petach Tikvah, IL 4952801
Tel: +972 3 919 3366

www.seculert.com

Toll Free (US/Canada): +1 855 732 8537
Tel (UK): +44 203 355 6444
Fax: +972 3 919 3636