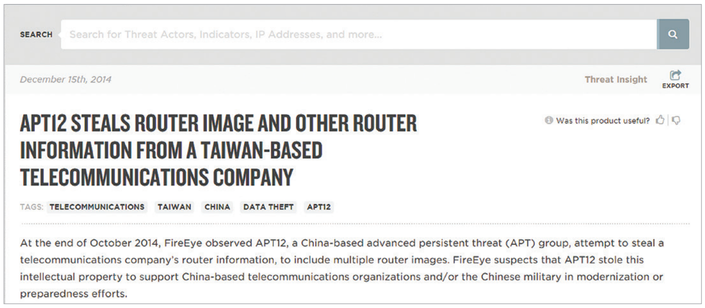
SEARCH
Search for Threat Actors, Indicators, IP Addresses, and more...
December 15th, 2014
Threat Insight
EXPORT
Was this product useful?
TAGS: TELECOMMUNICATIONS TAIWAN CHINA DATA THEFT APT12

APT12 STEALS ROUTER IMAGE AND OTHER ROUTER INFORMATION FROM A TAIWAN-BASED TELECOMMUNICATIONS COMPANY

At the end of October 2014, FireEye observed APT12, a China-based advanced persistent threat (APT) group, attempt to steal a telecommunications company's router information, to include multiple router images. FireEye suspects that APT12 stole this intellectual property to support China-based telecommunications organizations and/or the Chinese military in modernization or preparedness efforts.

FireEye

Threat Intelligence

FireEye Threat Intelligence is part of the overall FireEye suite of security products. It is, in fact, the primary intelligence component and is used to help drive other FireEye products providing active blocking at networks, endpoints and mobile devices. The service – available as a subscription – has three available levels: Dynamic Threat Intelligence (DTI), Advanced Threat Intelligence (ATI) and Advanced Threat Intelligence Plus (ATI+). The differences among these three services are largely based on the level of detail in the reports you receive and the number of included services. In addition to proactive notifications and alerts, there is a portal from which users can access significant threat intelligence and conduct their own research.

The resources are prodigious. The system conducts more than 50 billion virtual machine analyses per day, including 400,000 unique malware samples and more than one billion non-malware events. This all is possible due to FireEye's deep insertion into the global threatscape. We liked that it updates every hour. With the speed at which cybercrime is moving, that level of update frequency is not, by any means, overkill.

The relationships of the three levels of service to each other is part of the strength of the threat intelligence suite. DTI largely is a machine-to-machine connection that enables detection and response when connected to the FireEye products. By adding ATI, you add context.

Users access the Threat Intelligence system through the FireEye Intel Center. This is a way to get direct intelligence from FireEye and gives users the ability to document, manage and share their own intelligence with other users. In the Intel Center users can look at current threats and drill down for more information.

The primary focus of the FireEye system is malware and that is, in today's threatscape, appropriate. However, the company does collect considerable data on non-malware-based attacks and exploits. By combining these two attack types users can get a comprehensive view of the threatscape as it applies to them. Tying the threatscape to the user's enterprise infrastructure is a powerful step in proactively protecting the enterprise data.

As users interact with the portal a lot of things go on under the covers. For example, as new threats, malwares and hostile addresses, URLs and domains are researched, the FireEye system creates encyclopedia entries. This adds to the knowledge base and gives the analyst more to work with. Malware that the user discovers can be submitted to the FireEye sandbox for analysis.

FireEye, Inc.
1440 McCarty Blvd
Milpitas, CA 95035
Phone: 877-FIREEYE (877-347-3393)
www.fireeye.com

DETAILS

Product Threat Intelligence

Company FireEye
https://www.fireeye.com/

Price Depends on services ordered.

What it does Cyber threat intelligence and proactive threat-based management of FireEye network security tools.

OUR BOTTOM LINE

FireEye is a venerable player in the threat analysis and response space. With its acquisition of Mandiant they have added materially to their knowledge base, and users of the Threat Intelligence system benefit by that.

We had the impression that the availability of ATI and ATI+ depended on having the rest of the FireEye network protection system in place since those modules include DTI.

This is an extremely powerful system for gathering, analyzing and acting on cyberthreat intelligence. The wealth of available data is impressive and FireEye is an experienced player with a heavy recorded history of data going back 10 years or more. We do wish, however, that this wealth of analytical power was readily available as a standalone service for threat analysts who are not necessarily part of a network defense team.