NETSCOUT

NEWS RELEASE

Arbor Networks Security Engineering & Response Team (ASERT) Releases Analysis of CryptFile2 Ransomware Server

2016-12-15

Ransomware Threat Development Continues

BURLINGTON, Mass.--(BUSINESS WIRE)--Dec. 15, 2016-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), today released a new **ASERT** Threat Intelligence Report that reveals TTPs (tactics, techniques, procedures) of threat actors distributing the CryptFile2 ransomware threat to victims worldwide.

According to an interagency report from the U.S. federal government titled **How to Protect Your Networks from Ransomware**, there have been 4,000 ransomware attacks per day in 2016, a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. The report goes on to say, "Ransomware targets home users, businesses, and government networks and can lead to temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation."

"Most analysis of ransomware activity tends to focus on endpoint malware activity, encryption method and in some cases how to decrypt without paying a ransom. ASERT has delivered visibility into the threat from the server side which is far less common. This analysis provides unique insight and context to this malware family, and it is our hope that it can be used to improve situational awareness, inform detection capabilities and improve defensive posture with regards to ransomware staging and distribution," said Curt Wilson, ASERT senior threat intelligence analyst.

Unique Global Perspective

In addition to the unique insight provided via Arbor's ATLAS infrastructure, a collaborative project with more than

300 network operators who have agreed to share anonymous traffic data totaling 140Tbps (approximately one-third of all internet traffic), ASERT has extensive visibility into advanced threat actor and global malware activity. From this informed perspective, ASERT develops campaign oriented threat intelligence for customers, complete with the context and confidence information required to detect and stop specific threats, and continuously enhance security posture over time. When a new campaign or distributed denial-of-service (DDoS) attack vector is detected, an attack policy is created, distributed and installed in Arbor's products via the ATLAS Intelligence Feed.

ASERT brings a diverse set of expertise, from Fortune 25 Computer Emergency Response Teams (CERTs) to former law enforcement, threat mitigation vendors and well-known malware research organizations. ASERT shares operationally viable intelligence with hundreds of international CERTs and with thousands of network operators via intelligence briefs like this one and security content feeds.

For access to the full report, please visit the **ASERT blog**.

About Arbor Networks

Arbor Networks, the security division of **NETSCOUT**, helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor Networks Spectrum™ advanced threat solution delivers complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of attack campaigns, malware and malicious insiders. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context so customers can solve problems faster and reduce the risks to their business.

To learn more about Arbor products and services, please visit our website at **arbornetworks.com** or follow on Twitter **@ArborNetworks**. Arbor's research, analysis and insight is shared via the **ASERT blog**. For a global data visualization of DDoS attacks that leverages our ATLAS intelligence, visit the **Digital Attack Map**, a collaboration with Jigsaw, an incubator within Alphabet, Google's parent company (NASDAQ: GOOGL).

Trademark Notice: Arbor Networks, the Arbor Networks logo and ATLAS are all trademarks of Arbor Networks, Inc. All other brands may be the trademarks of their respective owners.

View source version on businesswire.com: **http://www.businesswire.com/news/home/20161215005198/en/**

Source: Arbor Networks Inc.

Arbor Networks

Kevin Whalen, 781-362-4377

kwhalen@arbor.net