NETSCOUT

NEWS RELEASE

Arbor Networks Uncovers Multi-Stage Attack Campaign Targeting Asian Governments and NGOs

2016-01-11

Worked with Regional CERT to Mitigate Threat

BURLINGTON, Mass., January 11, 2016 – Arbor Networks Inc., the security division of NETSCOUT (NASDAQ: NTCT), today released a new ASERT Threat Intelligence Report detailing an attack campaign involving various government websites and non-governmental organizations. This threat campaign involves a newly-discovered Remote Access Trojan (RAT) named 'Trochilus.' Believed to be driven by East Asian threat actors, Trochilus is part of a seven-piece malware cluster that offers threat actors a variety of capabilities, including espionage and the means to move laterally within target networks in order to achieve more strategic access.

This is the first instance of the Trochilus RAT observed by Arbor's Security Engineering & Response Team (ASERT) on the global Internet. ASERT is unaware of any public reference to this malware being used in targeted threat campaigns.

In 2015, Arbor Networks and other research organizations discovered the PlugX and EvilGrab malware targeting government websites in Asia. After delivering initial findings to the regional Computer Emergency Response Teams (CERTs), additional malware was subsequently discovered and removed from related sites. The presence of new malware after the initial notification process from Arbor indicates an ongoing campaign and suggests persistent, resourceful actors are involved. In addition to updating security policies in Arbor's products, ASERT regularly shares its operational insight with the threat intelligence and incident response community, hundreds of international CERTs and thousands of network operators around the world.

This ASERT Threat Intelligence Report includes a brief history of the Trochilus malware family, an overview of how the malware operates and a deeper technical analysis of the entire threat campaign to include PlugX, EvilGrab and

the 9002 RAT malware also deployed. For access to the full report, please visit: http://arbor.link/xo0jq

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's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market-leading analytics for dynamic incident response, historical analysis, visualization and forensics. 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, together with data from the ATLAS global threat intelligence system, can be found at the ATLAS Threat Portal.

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.

CONTACT INFORMATION

Kevin Whalen
Arbor Networks

Phone: 781-362-4377

kwhalen@arbor.net

- See more at: http://www.netscout.com/press-release/arbor-networks-uncovers-multi-stage-attack-campaign-targeting-asian-governments-and-ngos/#sthash.pavSeuH4.dpuf