November 6, 2014

FortiGuard Researchers Detect and Prevent New Sophisticated Point-of-Sale Threat

New Backoff PoS Malware Variant "211G1" Contains New Techniques for Evading Analysis and Detection Mechanisms

SUNNYVALE, CA -- (Marketwired) -- 11/06/14 -- Fortinet® (NASDAQ: FTNT) -- a global leader in high-performance network security -- announced that FortiGuard researchers have discovered an even newer variant of the "Backoff" Point-of-Sale malware family, "211G1," leveraging sophisticated techniques to hinder the analysis process and evade detection.

The newest version, detected as W32/Backoff.C!tr.spy, is now equipped with a packer, code that maps the image to its original base address before continuing to execute, putting even more roadblocks to the analysis process. The malware hides itself in the user's Application Data folder but, unlike the previous version, randomly selects a name from a predefined list. The malware is designed to steal credit card numbers off Point of Sale terminals, which could potentially result in millions of stolen cards if a major retailer is hit. ***Fortinet is one of two security companies able to specifically identify and block this malware today.***

On November 3rd, FortiGuard researchers reported an updated version of "Backoff," dubbed ROM, which performed many of the same functions as its predecessor, but leveraged a slew of new techniques that made the threat more difficult to detect and analyze. This version circumvented security controls by disguising itself as a media player with the file name *mplayer.exe* and dropping a file in the user's Application Data folder.

FortiGuard researchers have observed that the malware authors are continuing to modify the threat in order to bypass security detection, and recommend that users maintain updated antivirus software to better protect themselves from this evolving threat.

About FortiGuard Labs
The FortiGuard Labs global research team continuously monitors the evolving threat landscape. More than 200 researchers and automated detection and prevention technology provide around the clock coverage to ensure your network stays protected. FortiGuard Labs delivers rapid product updates and detailed security knowledge, providing protection from the latest threats.

About Fortinet
Fortinet (NASDAQ: FTNT) helps protect networks, users and data from continually evolving threats. As a global leader in high-performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low-performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content. Learn more at www.fortinet.com, or follow Fortinet at the Fortinet Blog, Google+, Linkedin or Twitter.

FTNT-O

Media Contact
Stefanie Hoffman
Fortinet, Inc.

408-486-5416
shoffman@fortinet.com

Investor Relations Contact
Michelle Spolver
Fortinet, Inc.
408-486-7837
mspolver@fortinet.com

Source: Fortinet