July 4, 2014

Fourth of July Malware Campaign Targets Vacationers

Cybercriminals Launch Carefully Timed Malware Campaign to Coincide With Major US Travel Holiday

SUNNYVALE, CA -- (Marketwired) -- 07/04/14 -- Researchers from Proofpoint, Inc. (NASDAQ: PFPT), a leading security-as-a-service provider, have discovered a nasty piece of malware which is targeting vacationers who visit US travel sites, just in time for the July 4th holiday.

The discovery shows that popular travel destination websites for cities including Boston, Salt Lake City, Houston, Monterey, Rochester, Myrtle Beach, Victoria and Utah Valley have been exploited and are serving malware to unsuspecting visitors. Proofpoint can also confirm that the command-and-control infrastructure of the cyber criminals behind the attacks all appears to be based in the Ukraine.

In response to the discovery, Mike Horn, VP, Threat Response Products at Proofpoint, said: "This is a good example of how poorly protected websites play a big role in the distribution of malware. Users might be directed to these sites by a search engine and they have no idea that just by visiting the site they can become infected. We are also seeing a large number of phishing campaigns which direct people to the legitimate travel sites which have been infected with malware by the hackers. The attacks were brought to our attention by our Targeted Attack Protection technology."

When users visit one of the infected websites a web exploit kit is run that then downloads additional malware onto their machine. However, more concerning is the fact that the exploit being used has very low detection rates with traditional antivirus solutions. When Proofpoint tested the piece of malware they discovered it was able to bypass all but four out of the 51 antivirus products on Virus Total. This makes it a particularly dangerous exploit for consumers.

"Since the attack started on July 3rd, and some of the web pages are promoting 4th of July activities, this attack appears to have been carefully timed to coincide with the US holiday season," Horn said. "We suspect that the websites have been compromised for some time, but the attackers were carefully planning their attack for maximum impact."

About Proofpoint, Inc.
Proofpoint Inc. (NASDAQ: PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving and governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information. More information is available at www.proofpoint.com.

Proofpoint is a trademark of Proofpoint, Inc. in the U.S. and other countries. All other trademarks contained herein are the property of their respective owners.

Media Contact:
Lucy Harvey
lucy@eskenziapr.com
01144 20 71 832 840

Source: Proofpoint

News Provided by Acquire Media