proofpoint

January 16, 2014

Proofpoint Uncovers Internet of Things (IoT) Cyberattack

More Than 750,000 Phishing and SPAM Emails Launched From "Thingbots" Including Televisions, Fridge

SUNNYVALE, CA -- (Marketwired) -- 01/16/14 -- Proofpoint, Inc., (NASDAQ: PFPT), a leading security-as-a-service provider, has uncovered what may be the first proven Internet of Things (IoT)-based cyberattack involving conventional household "smart" appliances. The global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions and at least one refrigerator that had been compromised and used as a platform to launch attacks. As the number of such connected devices is expected to grow to more than four times the number of connected computers in the next few years according to media reports, proof of an IoT-based attack has significant security implications for device owners and Enterprise targets.

Just as personal computers can be unknowingly compromised to form robot-like "botnets" that can be used to launch large-scale cyberattacks, Proofpoint's findings reveal that cyber criminals have begun to commandeer home routers, smart appliances and other components of the Internet of Things and transform them into "thingbots" to carry out the same type of malicious activity. Cyber criminals intent on stealing individual identities and infiltrating enterprise IT systems have found a target-rich environment in these poorly protected internet connected devices that may be more attractive and easier to infect and control than PC, laptops, or tablets.

The attack that Proofpoint observed and profiled occurred between December 23, 2013 and January 6, 2014, and featured waves of malicious email, typically sent in bursts of 100,000, three times per day, targeting Enterprises and individuals worldwide. More than 25 percent of the volume was sent by things that were not conventional laptops, desktop computers or mobile devices; instead, the emails were sent by everyday consumer gadgets such as compromised home-networking routers, connected multi-media centers, televisions and at least one refrigerator. No more than 10 emails were initiated from any single IP address, making the attack difficult to block based on location -- and in many cases, the devices had not been subject to a sophisticated compromise; instead, misconfiguration and the use of default passwords left the devices completely exposed on public networks, available for takeover and use.

"Bot-nets are already a major security concern and the emergence of thingbots may make the situation much worse," said David Knight, General Manager of Proofpoint's Information Security division. "Many of these devices are poorly protected at best and consumers have virtually no way to detect or fix infections when they do occur. Enterprises may find distributed attacks increasing as more and more of these devices come on-line and attackers find additional ways to exploit them."

While IT experts have long predicted security risks associated with the rapidly proliferating Internet of Things (IoT), this is the first time the industry has reported actual proof of such a cyber attack involving common appliances -- but it likely will not be the last example of an IoT attack. IoT includes every device that is connected to the internet -- from home automation products including smart thermostats, security cameras, refrigerators, microwaves, home entertainment devices like TVs, gaming consoles to smart retail shelves that know when they need replenishing and industrial machinery -- and the number of IoT devices is growing enormously. IDC predicts that more than 200 billion things will be connected via the Internet by 2020[1]. But IoT devices are typically not protected by the anti-spam and anti-virus infrastructures available to organizations and individual consumers, nor are they routinely monitored by dedicated IT teams or alerting software to receive patches to address new security issues as they arise. The result is that Enterprises can't expect IoT-based attacks to be resolved at the source; instead, preparations must be made for the inevitable increase in highly distributed attacks, phish in employee inboxes, and clicks on malicious links.

"The 'Internet of Things' holds great promise for enabling control of all of the gadgets that we use on a daily basis. It also holds great promise for cybercriminals who can use our homes' routers, televisions, refrigerators and other Internet-connected devices to launch large and distributed attacks," said Michael Osterman, principal analyst at Osterman Research. "Internet-enabled devices represent an enormous threat because they are easy to penetrate, consumers have little incentive to make them more secure, the rapidly growing number of devices can send malicious content almost undetected, few vendors are taking steps to protect against this threat, and the existing security model simply won't work to solve the problem."

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 & 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.

[1] [source: http://www.zdnet.com/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things-7000021516/]

Media Contact:
Orlando Debruce
Proofpoint, Inc.
408-338-6829
Email Contact

Sarmishta Ramesh
Ogilvy Public Relations
303-527-4615
Email Contact

Source: Proofpoint

News Provided by Acquire Media