

Cyberattack traced to hacked refrigerator, researchers report

17 January 2014



A LG representative shows a smartphone with Home Chat in front of a LG smart refrigerator at the 2014 International CES, January 10, 2014 in Las Vegas, Nevada

Call it the attack of the zombie refrigerators. Computer security researchers said this week they discovered a large "botnet" which infected Internet-connected home appliances and then delivered more than 750,000 malicious emails.

The California security firm Proofpoint, Inc., which announced its findings, said this may be the first proven "Internet of Things" based cyberattack involving "smart" [appliances](#).

Proofpoint said hackers managed to penetrate home-networking routers, connected multi-media centers, televisions and at least one refrigerator to create a botnet—or platform to deliver malicious spam or phishing emails from a device, usually without the owner's knowledge.

Security experts previously spoke of such attacks as theoretical.

But Proofpoint said the case "has significant

security implications for device owners and enterprise targets" because of massive growth expected in the use of smart and connected devices, from clothing to appliances.

"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 kinds of attacks normally associated with personal computers.

The [security firm](#) that these appliances may become attractive targets for hackers because they often have less security than PCs or tablets.

Proofpoint said it documented the incidents between December 23 and January 6, which 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. No more than 10 emails were initiated from any single device, making the attack difficult to block based on location

"Botnets are already a major [security](#) concern and the emergence of thingbots may make the situation much worse," said David Knight at Proofpoint.

"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 online and attackers find additional ways to exploit them."

© 2014 AFP

APA citation: Cyberattack traced to hacked refrigerator, researchers report (2014, January 17) retrieved 14 October 2019 from <https://phys.org/news/2014-01-cyberattack-hacked-refrigerator.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.