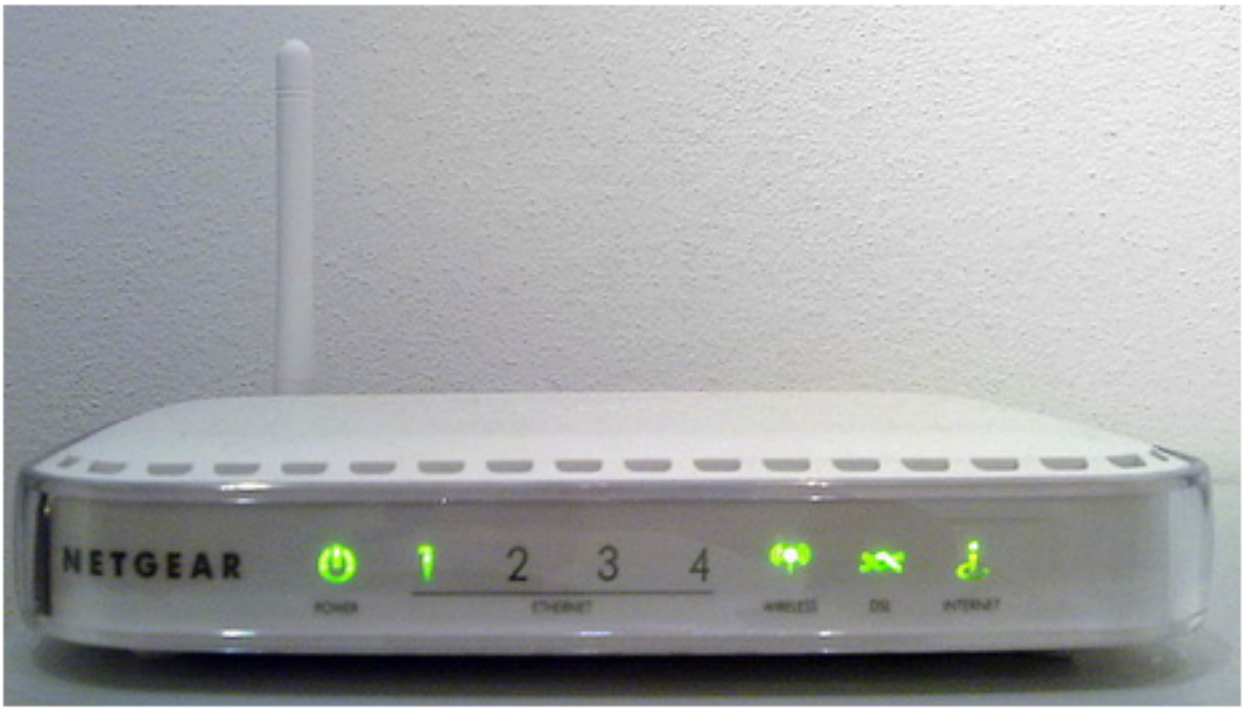
SIGN IN

RISK ASSESSMENT —

Home routers under attack in ongoing malvertisement blitz

DNSChanger causes network computers to visit fraudulent domains.

DAN GOODIN - 12/16/2016, 9:42 PM



Gionnico

As you read these words, malicious ads on legitimate websites are targeting visitors with malware. But that malware doesn't infect their computers, researchers said. Instead, it causes unsecured routers to connect to fraudulent domains.

Using a technique known as steganography, the ads hide malicious code in image data. The hidden code then redirects targets to webpages hosting DNSChanger, an exploit kit that infects routers running unpatched firmware or are secured with weak administrative passwords. Once a router is compromised, DNSChanger configures it to use an attacker-controlled domain name system server. This causes most computers on the network to visit fraudulent servers, rather than the servers corresponding to their official domain.

Patrick Wheeler, director of threat intelligence for security firm Proofpoint, told Ars:

These findings are significant because they demonstrate clearly that ubiquitous and often-overlooked devices are being actively attacked, and once compromised, these devices can affect the security of every device on the network, opening them up to further attacks, pop-ups, malvertising, etc. Thus, the potential footprint of this kind of attack is high and the potential impact is significant.

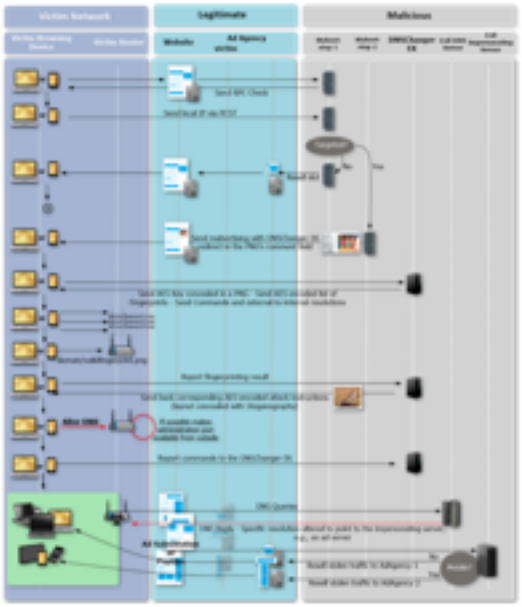
Lots of moving parts

The ads first check if a visitor's IP address is within a targeted range, a behavior that is typical of many malvertising campaigns, which aim to remain undetected for as long as possible. If the address isn't one the attackers want to target, they serve a decoy ad with no exploit code in it. In the event the IP address is one the attackers want to infect, they serve a fake ad that hides exploit code in the metadata of a PNG image. The code, in turn, causes the visitor to connect to a page hosting DNSChanger, which once again checks the visitor's IP address to ensure it's within the targeted range. Once the check passes, the malicious site serves a second image concealed with the router exploit code.

"This attack is determined by the particular router model that is detected during the reconnaissance phase," a Proofpoint researcher who uses the moniker Kafeine wrote in a blog post. "If there is no known exploit, the attack will attempt to use default credentials." In the event there are no known exploits and no default passwords, the attack aborts.

DNSChanger uses a set of real-time communications protocols known as webRTC to send so-called STUN server requests used in VoIP communications. The exploit is ultimately able to funnel code through the Chrome browser for Windows and Android to reach the network router. The attack then compares the accessed router against 166 fingerprints of known vulnerable router firmware images. Proofpoint said it wasn't possible to name all the vulnerable routers, but a partial list includes:

- D-Link DSL-2740R
- COMTREND ADSL Router CT-5367 C01_R12
- NetGear WNDR3400v3 (and likely other models in this series)
- Pirelli ADSL2/2+ Wireless Router P.DGA4001N
- Netgear R6200



Enlarge / DNSChanger attack chain.

Enlarge / A fake DNSChanger ad.

The malicious ads are delivered in waves lasting several

days at a time through legitimate ad networks and displayed on legitimate websites. Proofpoint's Wheeler said there isn't enough data to know how many people have been exposed to the ads or how long the campaign has been running, but he said the attackers behind it have previously been responsible for malvertisements that hit more than 1 million people a day. The campaign was still active at the time this post was being prepared. Proofpoint didn't identify any of the ad networks or websites delivering or displaying the malicious ads.

As Ars reported last week, a similar malvertising campaign—images with hidden code that double-check IP addresses—also reached more than 1 million people a day. Proofpoint said the two campaigns aren't related.

FURTHER READING
Millions exposed to malvertising that hid attack code in banner pixels

DNS servers translate domain names such as arstechnica.com into IP addresses such as 50.31.151.33, which computers need to find and access the site. By changing router settings to use an attacker-controlled server, DNSChanger can cause most, if not all, connected computers to connect to impostor sites that look just like the real ones. So far, the malicious DNS server used by DNSChanger appears to be falsifying IP addresses to divert traffic from large ad agencies in favor of ad networks known as Fogzy and TrafficBroker. But the server could be updated at any time to falsify lookups for Gmail.com, bankofamerica.com, or any other site. In such a scenario, fortunately, HTTPS protections would flag the impostor.

The best defense against these attacks is to ensure routers are running the latest available firmware and are protected with a long password that's generated randomly or through a technique known as diceware. Disabling remote administration, changing its default local IP address can also be helpful, and hardcoding a trusted DNS server into the OS network settings can also be helpful.

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 136 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Sponsored Stories

Powered by

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS

WIRED Media Group
Use of this Site constitutes acceptance of our User Agreement (effective 1/2/14) and Privacy Policy (effective 1/2/14), and Ars Technica Addendum (effective 5/17/2012). Your California Privacy Rights. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.