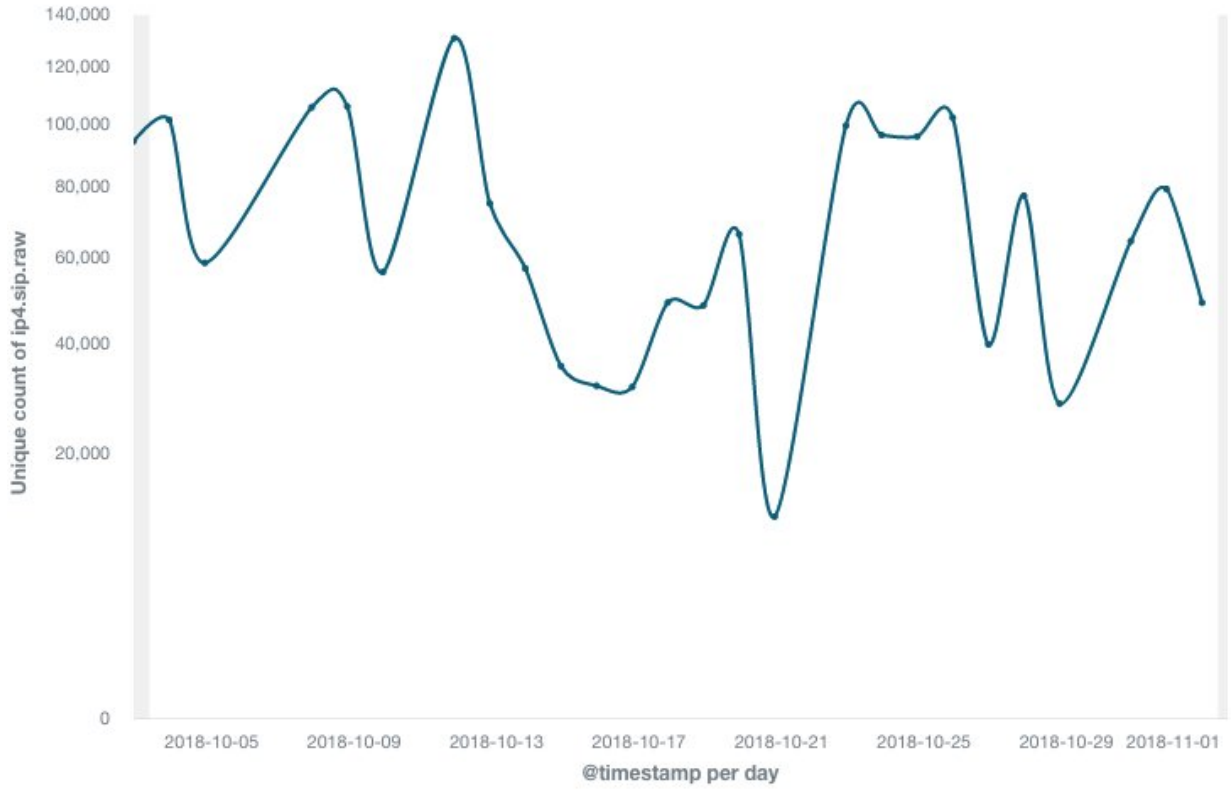
Researchers discover how routers may be recruited into botnet army

November 14 2018, by Nancy Owano



Credit: 360Netlab Scanmon

This is one November headline that made a lot of readers nervous: A reporter gave reasons for why you should change your Internet password now. Kari Paul in *MarketWatch* was one of several sites reporting on a

botnet army out there, using malware to infect computers and turn them into bots.

The botnet turns home routers into email spammers. (Believed to be used for sending spam emails, and unlike other botnets, this one "does not appear to be used for performing DDoS attacks," said Greg Synek in *TechSpot*.)

MarketWatch listed names of companies whose routers potentially are at risk; the companies mentioned did not respond to it to comment at the time of this writing.

"So far, between 100,000 and 300,000 devices are infected and that number could grow, researchers say," according to Paul. *Naked Security* author John Dunn said the botnet has infected *at least* 100,000 routers in the US, India and China since September.

Why, what goes wrong? Without you even realizing it, your home network could be used to send harmful spam, as targeted devices have been harnessed to send out massive amounts of spam emails.

The starting points of the discovery lead to a network security lab; the *360Netlab* site presented the story, authored by the network security engineer Hui Wang and RootKiter.

The two researchers said the amount of infection was very large; the number of active scanning IP in each scan event was about 100,000; the proxy network was implemented by the attacker; the proxy communicates with well-known mail servers such as Hotmail.

"Since September 2018, 360Netlab Scanmon has detected multiple scan spikes on TCP port 5431, each time the system logged more than 100k scan sources, a pretty large number compared with most other botnets

we have covered before."

By October they got their honeypot tweaks and customizations right and "successfully tricked the botnet to send us the sample."

How is this working? Paul: "The attack is exploiting a security vulnerability initially found in 2013 on the Universal Plug and Play (UPnP) feature, which allows a device on the same network to discover each other more seamlessly."

The botnet covers devices including models from a number of companies, not just one.

So what did security-watching observers have to say? Interestingly, *Naked Security* said the router escapade is performed using an "ancient security flaw." Dunn wrote, "The UPnP, of course, is Universal Plug and Play, a longstanding and widely abused networking protocol designed to make it easy for devices to talk to one another without the need for complicated configuration." Dan Goodin in *Ars Technica* was expressing similar thoughts about UPnP, which, "as researchers have warned for years, often opens up serious holes inside the networks that use it."

In the bigger picture, botnets are tantalizing target opportunities for hackers with ill intentions. Dunn noted that "router compromises have been a running theme on Naked Security for years and still keep coming.

"Under a subheading "Botnet hell," Dunn wrote that "Botnets are a way to steal someone else's computing resources and distribute traffic across lots of ISP networks in a way that makes its activity harder to shut down than if it were coming out of a small group of servers."

Goodin, meanwhile, said it was not clear how routers infected with BCMUPnP_Hunter can be disinfected. Nonetheless, he added, "Usually,

simply rebooting a compromised router is enough."

More information: blog.netlab.360.com/bcmpupnp_h … o-email-spammers-en/