Moose – the router worm with an appetite for social networks

welivesecurity.com/2015/05/26/moose-router-worm/

May 26, 2015

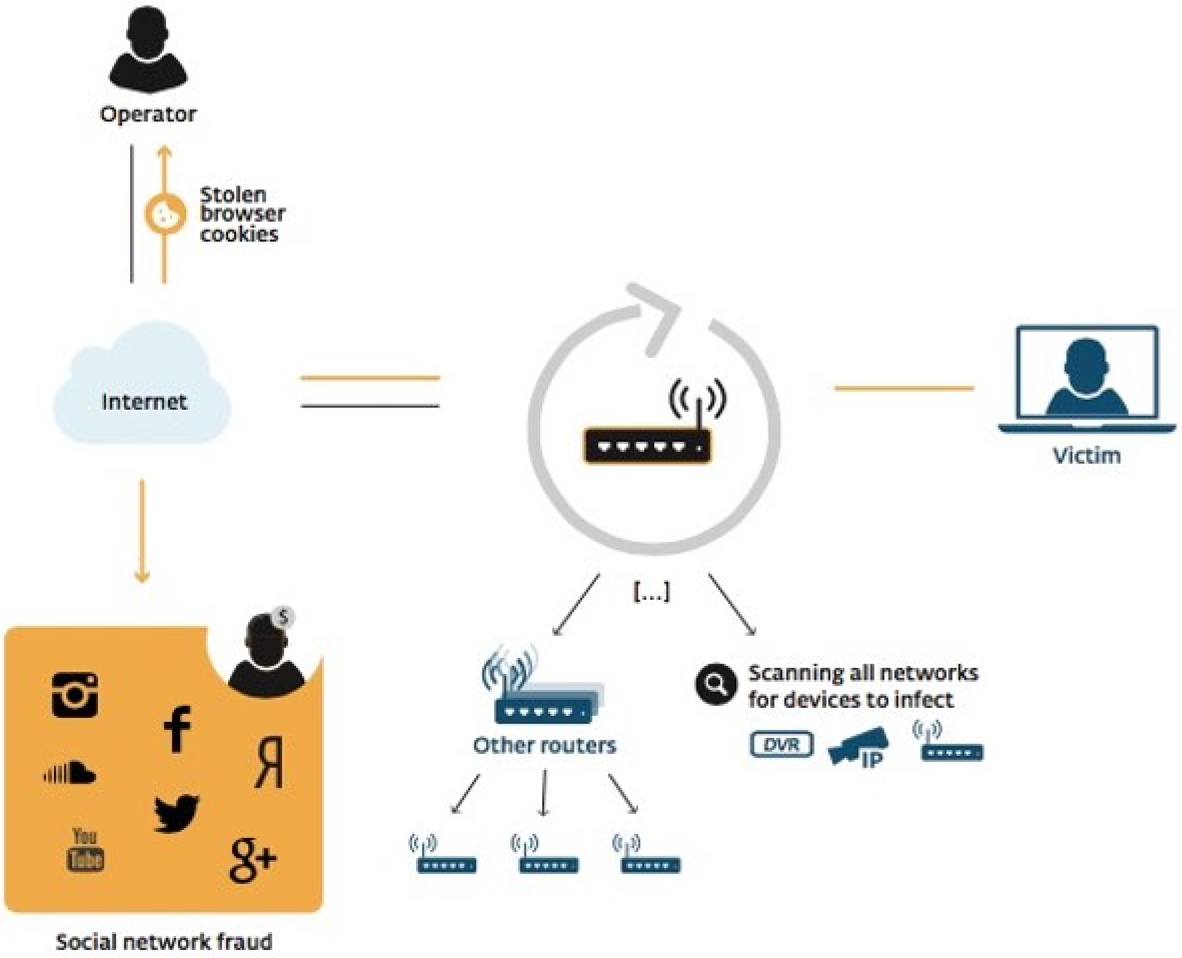
A new worm is infecting routers in order to commit social networking fraud, hijacking victims' internet connections in order to "like" posts and pages, "view" videos and "follow" other accounts.

26 May 2015 - 12:45PM

A new worm is infecting routers in order to commit social networking fraud, hijacking victims' internet connections in order to “like” posts and pages, “view” videos and “follow” other accounts.

ESET researchers have issued a technical paper today, analyzing a new worm that is infecting routers in order to commit social networking fraud, hijacking victims' internet connections in order to “like” posts and pages, “view” videos and “follow” other accounts.

The malware, dubbed Linux/Moose by researchers Olivier Bilodeau and Thomas Dupuy, infects Linux-based routers and other Linux-based devices, eradicating existing malware infections it might find competing for the router's limited resources, and automatically finding other routers to infect.



However, the Moose worm does not rely upon any underlying vulnerability in the routers – it is simply taking advantage of devices that have been weakly configured with poorly chosen login credentials.

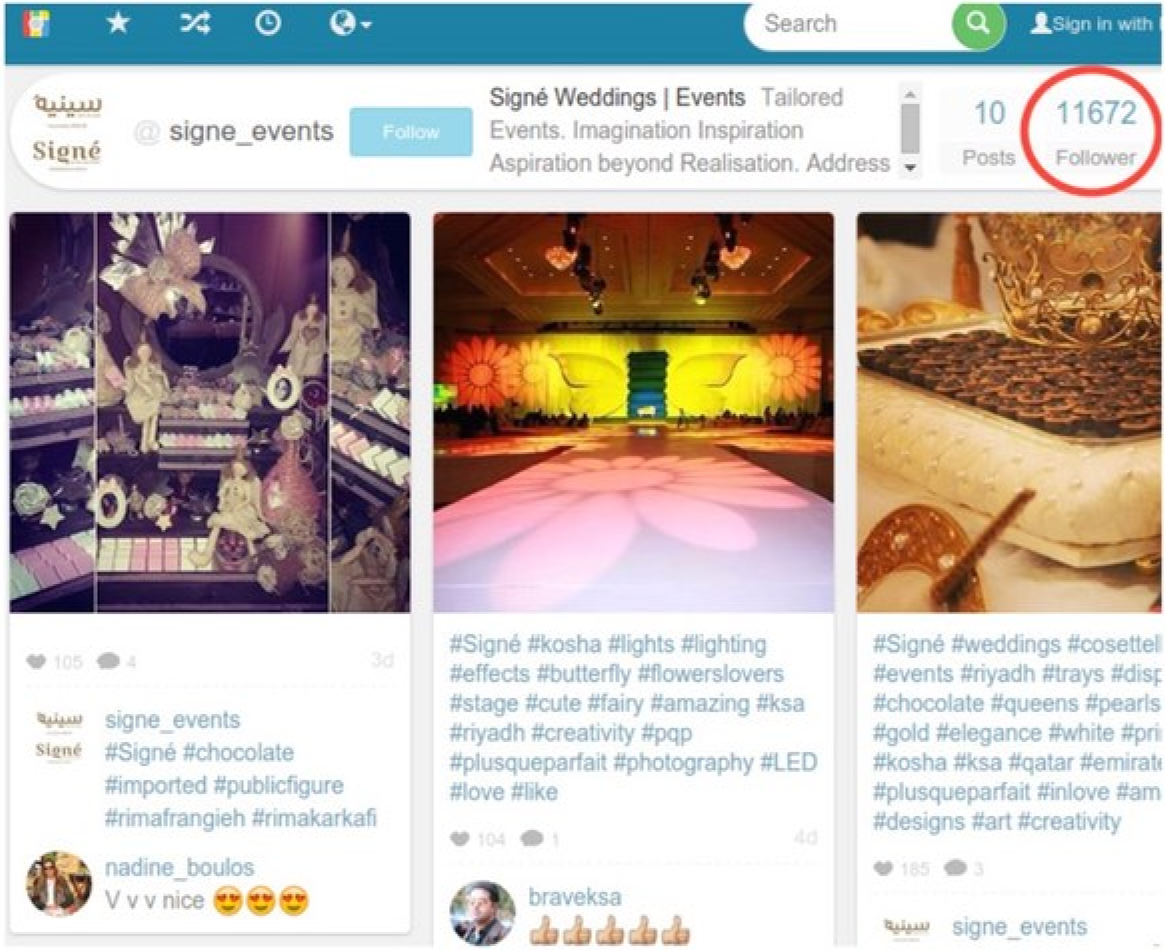
Unfortunately, this means that devices other than routers can be impacted by the worm in the form of accidental collateral damage. ESET's team believes that even medical devices, such as the Hospira drug infusion pump, could be infected by the Linux/Moose worm.

But the principal victims are likely to be routers – with devices from Actiontec, Hik Vision, Netgear, Synology, TP-Link, ZyXEL, and Zhone already identified as vulnerable.

ESET's detailed technical report provides an indepth analysis of the Moose worm, methods by which users can determine if they might have had their routers compromised, and cleaning instructions. Importantly, the technical report provides prevention advice to avoid reinfection.

Perhaps most interesting of all, however, is to try to understand the purpose of the Moose worm.

In their investigation, ESET's team observed the worm creating bogus accounts on sites such as Instagram, and automatically following users. In many cases the rise in followers was carefully staggered over some days, seemingly to avoid raising alarms in automated systems built by the social networks to identify suspicious behavior.



@ signe_events

Signé Weddings | Events Tailored Events. Imagination Inspiration Aspiration beyond Realisation. Address

10 Posts

11672 Follower

105 4 3d

signe_events #Signé #chocolate #imported #publicfigure #rimafrangieh #rimakarkafi

nadine_boulos V v v nice 😍😍😍

#Signé #kosha #lights #lighting #effects #butterfly #flowerslovers #stage #cute #fairy #amazing #ksa #riyadh #creativity #pqp #plusqueparfait #photography #LED #love #like

104 1 4d

braveksa 👍👍👍👍👍

#Signé #weddings #cosettel #events #riyadh #trays #disp #chocolate #queens #pearls #gold #elegance #white #pri #kosha #ksa #qatar #emirat #plusqueparfait #inlove #am #designs #art #creativity

185 3

signe_events

The sad truth is that there are many individuals and companies out there who are keen to manipulate their social media standing, and have no qualms about hiring third-parties who claim to have methods to bump up the number of views of a corporate video, boost the followers on a Twitter feed or get you more Facebook fans.

Often these third-parties will themselves contract the work out to other companies, and the danger is that one of these might – perhaps unwittingly – hire criminals with access to the botnet of Moose-compromised routers to conduct the social media fraud on their behalf.

The fact that these aren't *real* fans, or *real* views of the video is likely to go unnoticed or be swept under the carpet by marketing teams keen to impress their bosses.

As well as social networking fraud, ESET's paper considers that the malware could potentially be used for other activities – such as distributed denial-of-service attacks, targeted network exploration (where it works hard to dig deep past firewalls) and eavesdropping and DNS hijacking (which could lead itself to phishing and further malware attacks).

Once again, consumers are advised to be on their guard, ensure that they install the latest security patches and never use default or easy-to-crack passwords on their internet-connected devices.

For much more information about the threat, and how to protect yourself against it, read the technical paper from ESET's team of experts: "Dissecting Linux/Moose".

26 May 2015 - 12:45PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion