Exposing the EGO MARKET: the cybercrime performed by the Linux/Moose botnet

gosecure.net/2016/11/02/exposing-the-ego-market-the-cybercrime-performed-by-the-linux-moose-botnet/

Masarah Paquet-Clouston

November 2, 2016

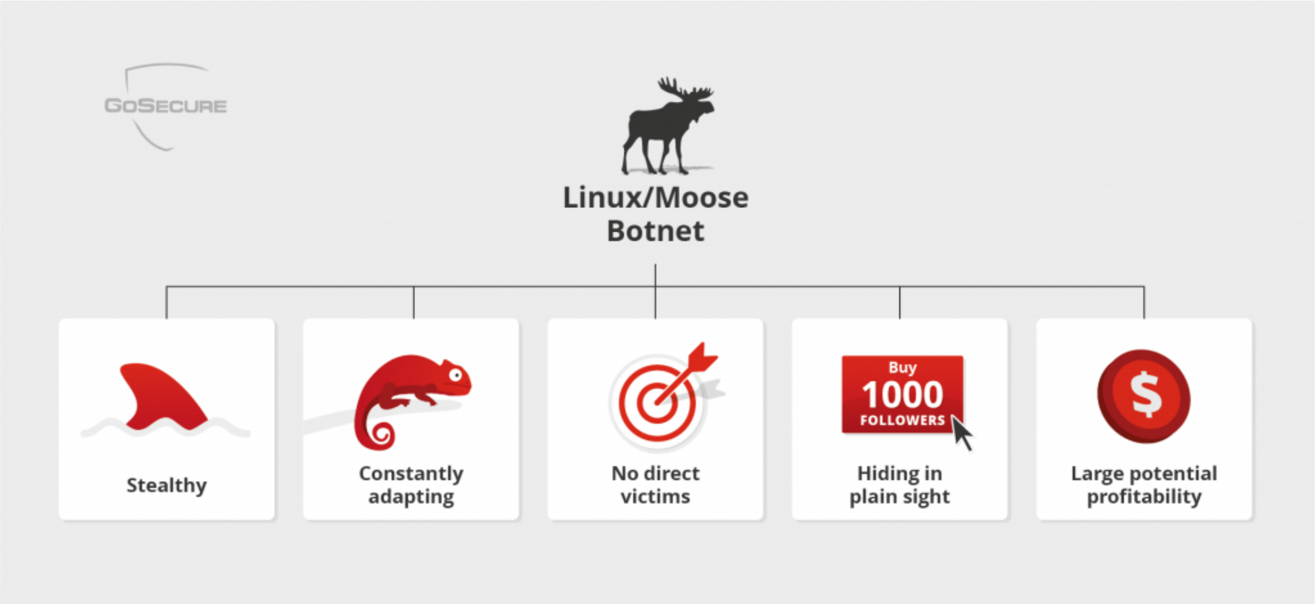
Cybercrime is an evolving phenomenon and offenders are continuously adapting to find new techniques to monetize their illicit activities. Our research paper and upcoming BlackHat Europe presentation – EGO MARKET: When People's Greed for Fame Benefits Large-Scale Botnets – is about Linux/Moose, a botnet that conducts social media fraud. This blog post is a summary of our paper.

Through our technical/social investigation, we found that the botnet is involved in a clever scheme that combines a stealthy infrastructure, constant technological adaptation, the inconspicuous activity of social media fraud with no direct victims, the ability to hide in plain sight and a large potential for profitability.

Social media fraud is:

> The process of creating false endorsements of social networks accounts in order to enhance a user's popularity and visibility. This can be achieved by liking posts (or any similar endorsement) or following a user.

The clever scheme of Linux/Moose:



Stealthy

Linux/Moose only targets IoT devices. The lack of antivirus and security software available for these devices allows the botnet to spread undetected. Moreover, the botnet is an embedded system threat with **no x86 architecture variant**; it can only run on embedded Linux systems of the MIPS and ARM architectures. This focus on embedded systems is rare as even the well-known embedded threats like *LizardStresser* (Linux/Gafgyt) and the recently discovered *Mirai* have x86 variants.

Since our industry’s best tools are built to detect and clean x86 threats, we can only deduce that the botnet operators aimed to proactively stay under the radar.

Constantly Adapting

The Linux/Moose botnet was first discovered by the ESET research team in 2015 and their analysis of the botnet was published in a technical report. The botnet’s infrastructure changed following the report, illustrating how offenders can adapt once their activities are exposed.

Linux/Moose Adaptations

1st change	The IP address of the C&C server is now XORed with a static value and passed as an argument into the executables instead of hard-coded in binary files. This means that out-of-context hunting by gathering files from Virus Total (VT) is no longer a viable means to track the botnet.
2nd change	The SOCKSv4 TCP port used by the botnet operators to proxy their traffic was updated from 10073 to 20012.
3rd change	Bot enrollment process changed and a correlation check was integrated between the infecting party and the victim in the C&C server. Simply mimicking an infected device and contacting the C&C is no longer sufficient to be considered as a bot by the botnet.
4th change	The network protocol with the C&C server was updated. The new protocol now mimics HTTP traffic on port 80 and the server displays a very common “It works!” page.

These changes are further described in a blog post released by ESET.

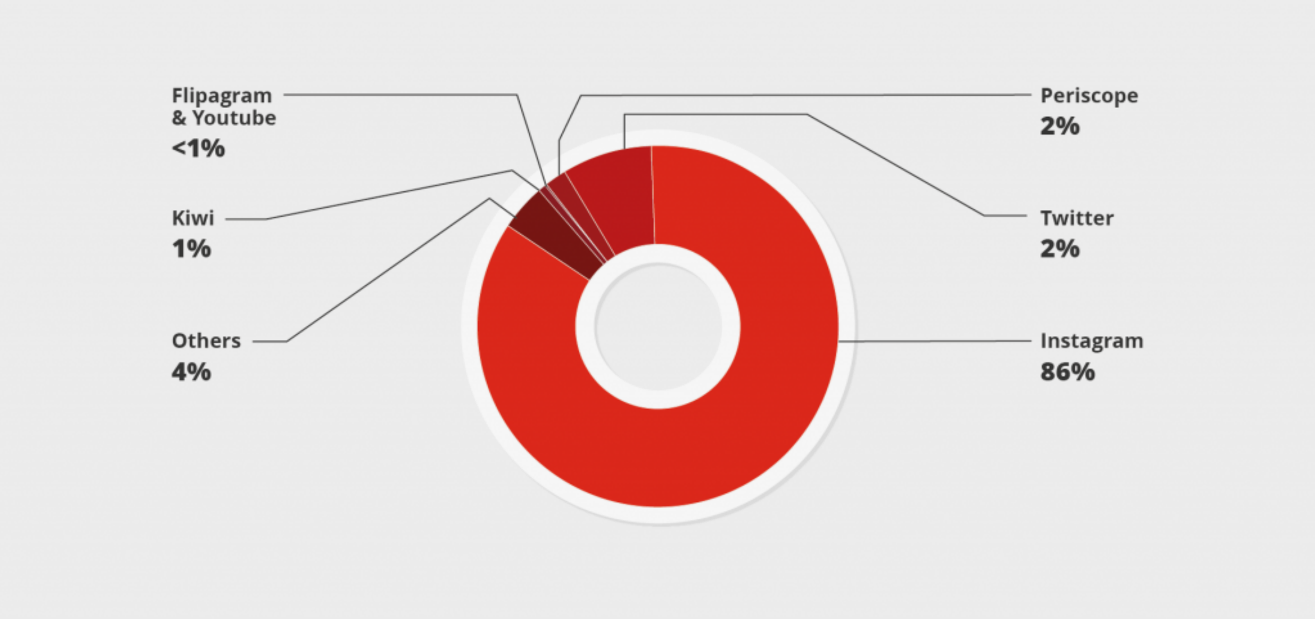
Man-in-the-Middle Attack on Linux/Moose

To further study the real effect of this botnet on social networks, we needed to see the traffic proxied by Linux/Moose's infected devices. To do so, we built a custom honeypot, deployed it worldwide and conducted an HTTPS man-in-the-middle attack on the proxied traffic. The complete description of the honeypot's architecture and the TLS attacks conducted are presented in the report.

The attack gave us invaluable information on the botnet's activities, such as which social media sites were targeted, as well as detailed information about all the requests made on each site.

No Direct Victims

Botnets are commonly known for distributed denial-of-service attacks (DDoS), sending spam or contributing to ad click fraud. We found that the Linux/Moose botnet operators are branching out to new and less risky activities. All of Linux/Moose's traffic aims at social media fraud. This was achieved by sending requests to log in on the social networks, create fake accounts and endorse other accounts. The most common fraud conducted by Linux/Moose is following a user on Instagram.

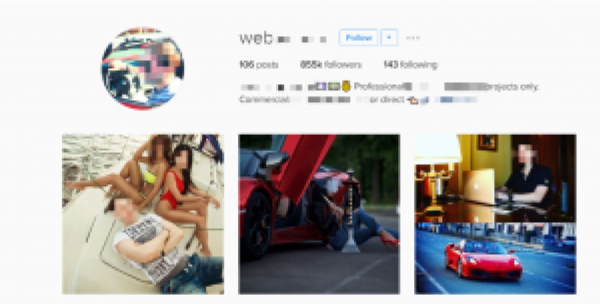


Distribution of Linux/Moose traffic on different social media websites

As opposed to Ransomware, Social media fraud **does not generate victims in need of defending.** Thus it is not an attractive target for law enforcement or for the international security industry. The indirect victims of social media fraud are the entities or people that use the number of followers and likes as a measure of the worth of a profile to hire a person, buy products from the profile or pay for advertisements. Instead of requiring law enforcement intervention, these victims are more likely to be more cautious in future transactions, **thereby giving a free pass to the botnet operators**.

Hiding in Plain Sight

The Linux/Moose botnet operators can **advertise on the *clear Web*, reaching large exposure**. Indeed, most sales of social media fraud go through websites and freelancer platforms available through an easy search on Google. The price on Instagram is, on average, **US $112.67 for 10,000 follows**. This is expensive considering that fake follows from Linux/Moose do not last. The fake accounts are often quickly flagged as spam by Instagram.

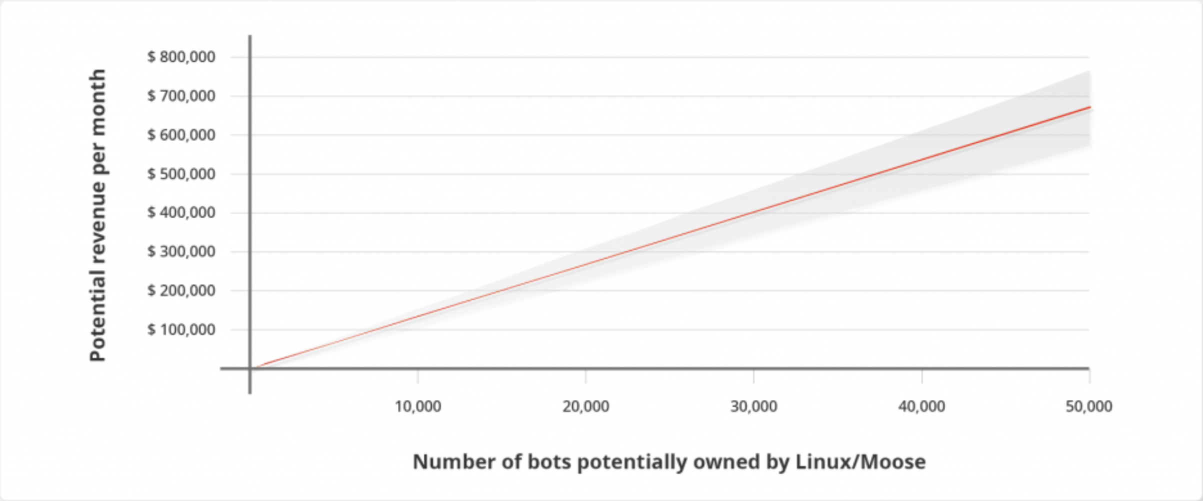


The nature of the demand shows how the fraud is driven by an **EGO Market**. Not only are the Linux/Moose operators selling their illegal activity in plain sight, **they reach a pool of customers that are not criminalized**.

The buyers of social media fraud found in Linux/Moose traffic are mostly small businesses, aspiring celebrities, and common people. Businesses centered around individuals, such as the adjacent profile showing a corporate account focused on the owner, were often found.

Large Potential Profitability

With a large botnet and all follows monetized, **the operators of Linux/Moose are sitting on a gold mine,** as shown in the graph below. Indeed, if all follows conducted by Linux/Moose on Instagram are monetized, the value generated by a single bot can go up to, on average, 13.05$ per month. However, to what extent the fraud is profitable for the botnet operators remains unclear. It depends on several factors such as the number of follows monetized, the size of the botnet and the number of actors sharing the money.



Regardless of the botnet's overall profitability, the Linux/Moose botnet evolves in an inconspicuous **EGO market** collecting money from normal people using regular credit cards. Further, it advertises its services on the *clear Web* and does not attract the attention of law enforcement. No connection to the criminal underworld is needed and there are no direct victims, yet the money is generated through illicit activities.

In the end, the Linux/Moose botnet participates in a clever scheme: it falls into an interstice that allows the botnet operators to continuously commit a cybercrime and profit from it in total impunity.

Indicators of Compromise (IoCs) are available in the appendix section of the report and from the ESET IoC repository.

Our full research paper is available here.

This research was partially financed by the MITACS Accelerate Program, under Project N. IT06861. We thank them for helping finance the project and also thank our partners, Université de Montréal and ESET, for helping us throughout the year.