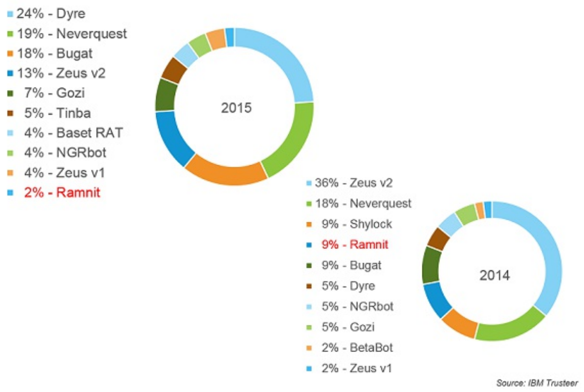
# The Ramnit Botnet is back after the law enforcement takedown

December 27, 2015 By Pierluigi Paganini

## The Ramnit botnet that has been disrupted by European law enforcement in February is back and it’s targeting online banking worldwide.

Security researchers at IBM Security have discovered a new variant of the popular Ramnit Trojan. This year law enforcement agencies from several European countries coordinated by the Europol have taken over a the botnet composed by over 3.2 Million computers worldwide, but now a new malicious infrastructure is in the wild.

Ramnit was first spotted in 2010 as a worm, in 2011, its authors improved it starting from the leaked Zeus source code turning the malware into a banking Trojan. In 2014 it had the pinnacle of success, becoming the fourth largest botnet in the world.



Source: IBM Trusteer

The discovery represents the return of Ramnit after the law enforcement takedown.

*"According to IBM X-Force researchers, that may have officially changed in December 2015. Not□ even a year after* Ramnit was taken down*, we are seeing what appears to be the first real re-□ emergence of the banking Trojan botnet. " Limor Kessem, cyber intelligence expert at IBM Trusteer, wrote in a* blog post*.*

The new Ramnit botnet uses a different command and control (C&C) infrastructure, the experts noticed that more than half of the infected machines are in Canada, followed by Australia, the US and Finland.

*What's new?*

The source code of new Ramnit variant spotted by IBM is quite similar to the predecessor by it uses shorter configuration files and implements web□ injections mechanisms like other threats (i.e. Dridex, Shifu). The researchers speculate that operators behind the Ramnit botnet have acquired the web injection mechanism from other cyber criminal groups, the experts noticed that the code injected into banking websites by the malware is obtained in real time from a remote server.

*"The only change in modus operandi is expressed in the* web injections *and the configuration file,□ which are both considered to be moving parts in the inner workings of any banking Trojan. Recent findings from IBM X-Force indicated that a number□ of other Trojans, like Shifu,* Dridex *and Neverquest, have been using the exact same* web injections *and remote servers, which can be indicative of gangs*

*purchasing software-as-a-service (SaaS) from the same injection developers." states the post.*

The experts noticed several infection vectors, including malvertising campaigns that rely on the popular Angler exploit kit

*"The new server commands newly infected machines that are receiving Ramnit through the Angler exploit kit. It regularly updates them with configurations and executable file builds. The new□ Ramnit also operates with a real-time* webinjection *server, selectively pulling attack schemes on the fly□ when infected users browse to a few major banks in Canada"*

The old Ramnit botnet was operated by a single criminal crew that has never sold the source code for the malicious agent.

*"From what we've learned so far, nothing seems to point to a notable change in terms of who is behind Ramnit. It is possible that a new gang has picked the project up, but attribution remains vague in this case," added Kessem.*

What about the future?

Experts believe the cyber criminals will expand their operation to other countries.

**Pierluigi Paganini**

**(Security Affairs – cybercrime, Ramnit botnet)**

Share it please ...

malware | Cybercrime | Europol | malvertising | Angler exploit kit | RAMNIT botnet

## SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at□ Bit4Id, firm leader in identity□ management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field,□ he is Certified Ethical Hacker at□ EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog□ "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone,□ ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

**European credit card payment terminals are plagued with serious flaws**

NEXT ARTICLE

**Darkweb, a look back at 2015 events and 2016 predictions**

## YOU MIGHT ALSO LIKE

Analyzing Ransom32, the first JavaScript ransomware variant

January 3, 2016 By Pierluigi Paganini

Are Russian hackers infecting critical infrastructure in Ukraine?

December 30, 2015 By Pierluigi Paganini

[redacted]

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top ^