



CYBER THREAT INTELLIGENCE REPORT Q3 2015

Blueliv has carried out the following analysis of worldwide cyber threat activity statistics for the third quarter 2015.

Cyber threats detected and analyzed by Blueliv during the third quarter 2015



STOLEN CREDITS CARDS

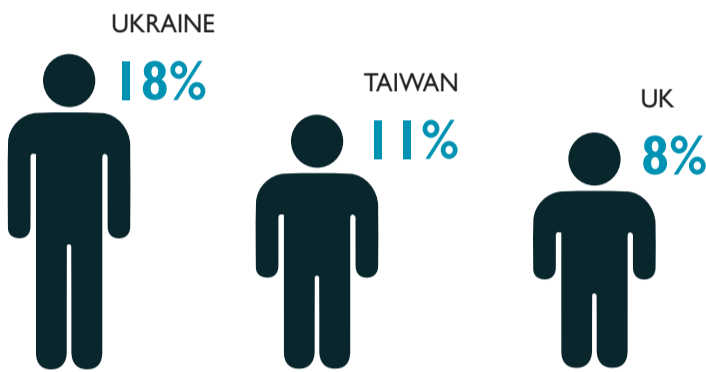
70% of the credit card thefts were in **US**, followed by **South Korea**, **Mexico** and **Canada**.



CREDENTIAL THEFTS

Geolocation

The highest amount of credential thefts has been in **Ukraine (18%)**, followed by **Taiwan (11%)** and **UK (8%)**



Thefts by industry

Regarding industries, **Media, Social Networks & Advertising, Technology & Telcos, Gambling & Gaming, Financial Services and Retail** have been the most affected ones.



MALWARE

Geolocation

US and **China** continued being the countries with the highest amount of malware.

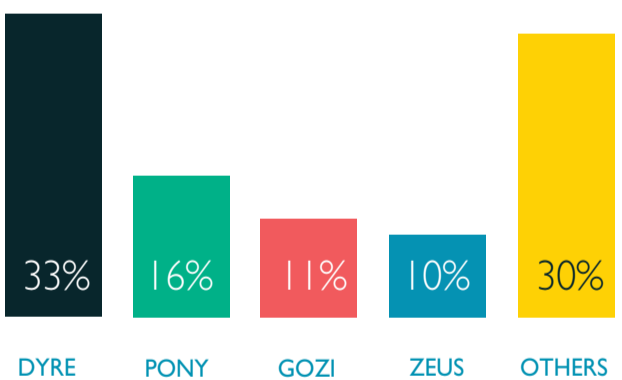
34% of the malware was located in **US**



28% of the malware was located in **China**

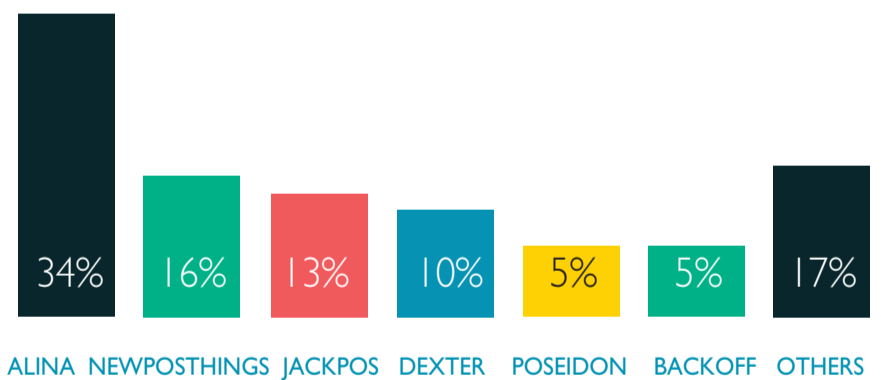
Types

Dyre continues having a great influence, 33% of the analyzed malware samples were Dyre. **Pony, Gozi** and **Zeus** also need to be considered, with 16%, 11%, and 10% respectively.



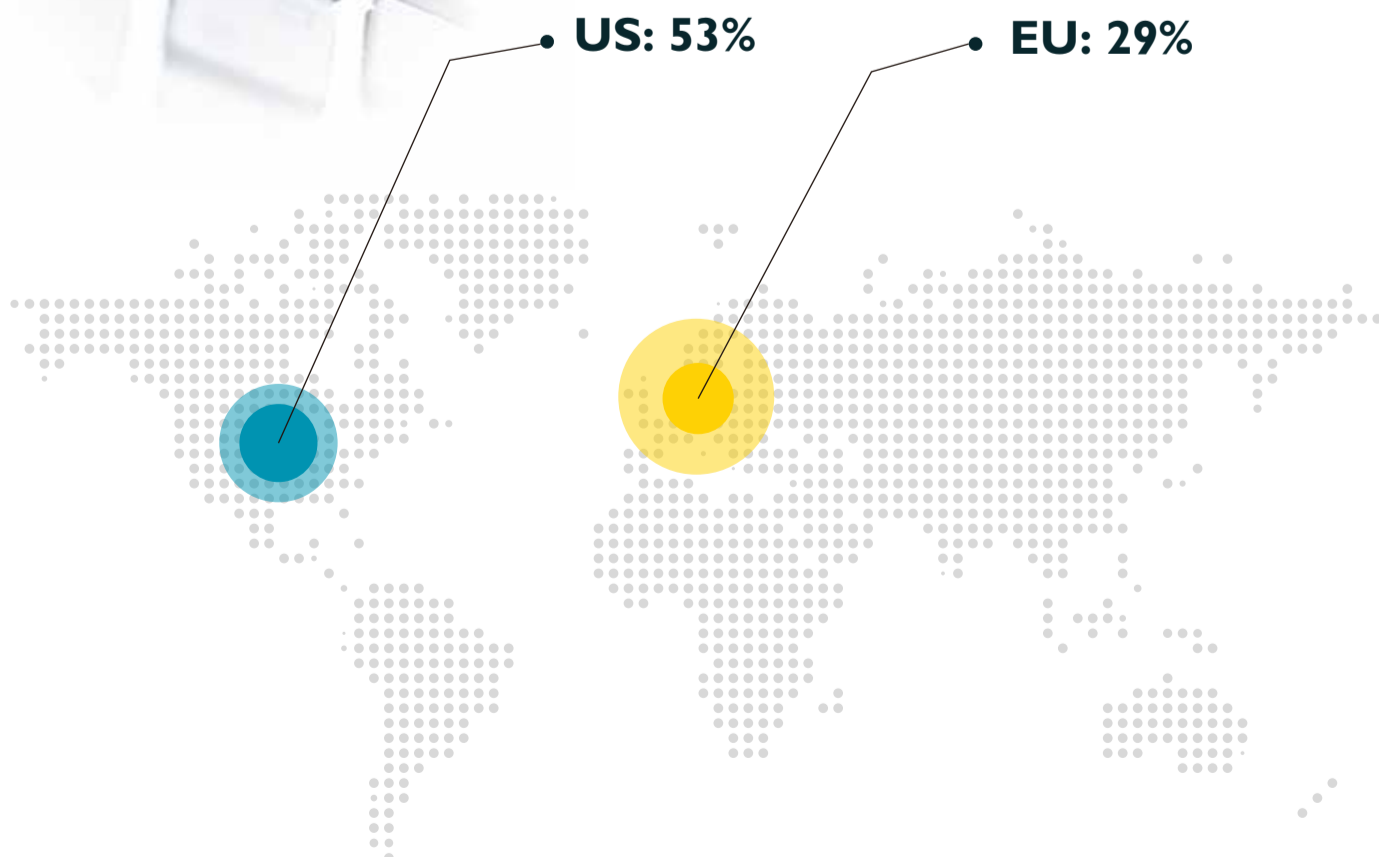
Types in POS

Alina, Newposthings and **Jackpos** have been the most active malware types targeting POS, followed by **Dexter, Poseidon** and **Backoff**.



BOTNETS

53% of the botnets were located in **US** and **29%** in the **European Union**.



Join our collaborative Community to fight against cyber crime: map.blueliv.com