

CYBER THREAT INTELLIGENCE REPORT Q2 2015

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

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



STOLEN CREDITS CARDS

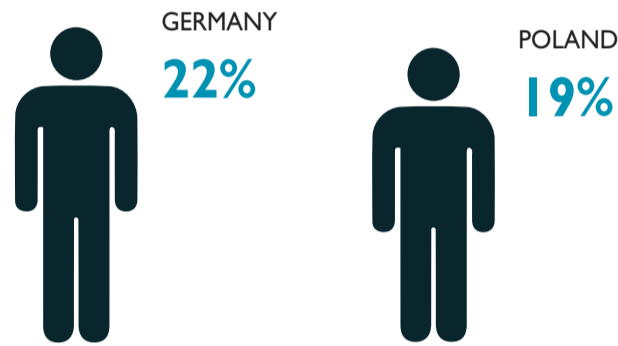
70% of the credit card thefts were in **US**, followed by Mexico, Canada and Australia.



CREDENTIAL THEFTS

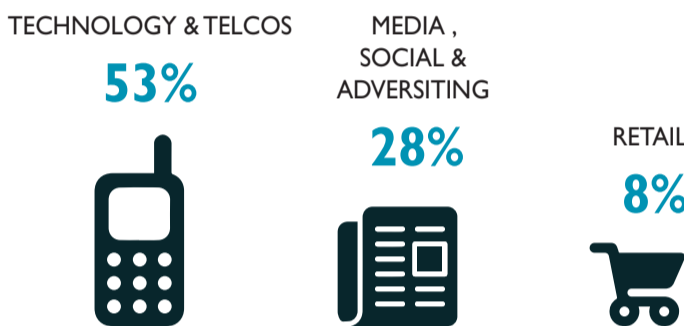
Geolocation

The highest amount of credential thefts has been in **Germany (22%)**, followed by **Poland (19%)**.



Thefts by industry

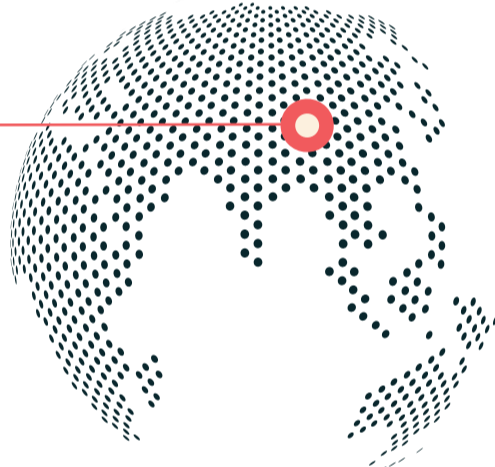
The most affected industries by credential thefts have been, once again, **Technology & Telcos (53%)** and **Media, Social Networks & Advertising (28%)**, followed by **retail (8%)**.



MALWARE

Geolocation

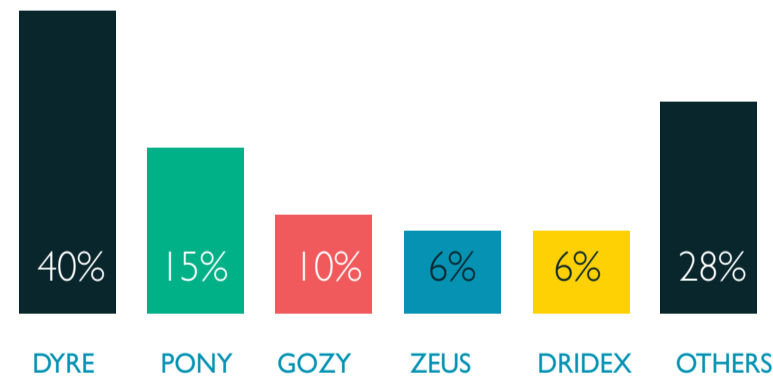
China continues in the **first position** in geolocation of malware crimeservers, **but the amount has gone down from 53% in the last quarter to 44%**.



US continues in the **second position**, hosting **25%** of the global malware crimeservers.

Types

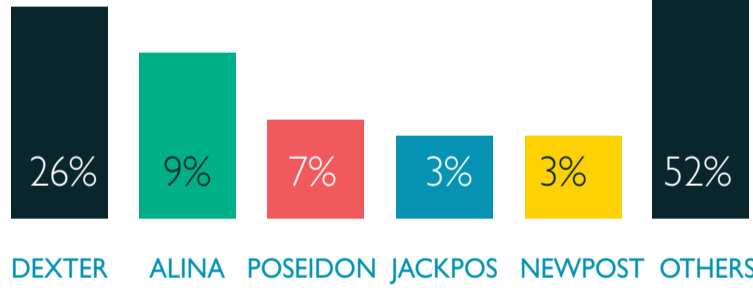
Dyre continues having a great influence. **Pony, Gozi, Zeus and Dridex** also need to be considered.



Types in POS

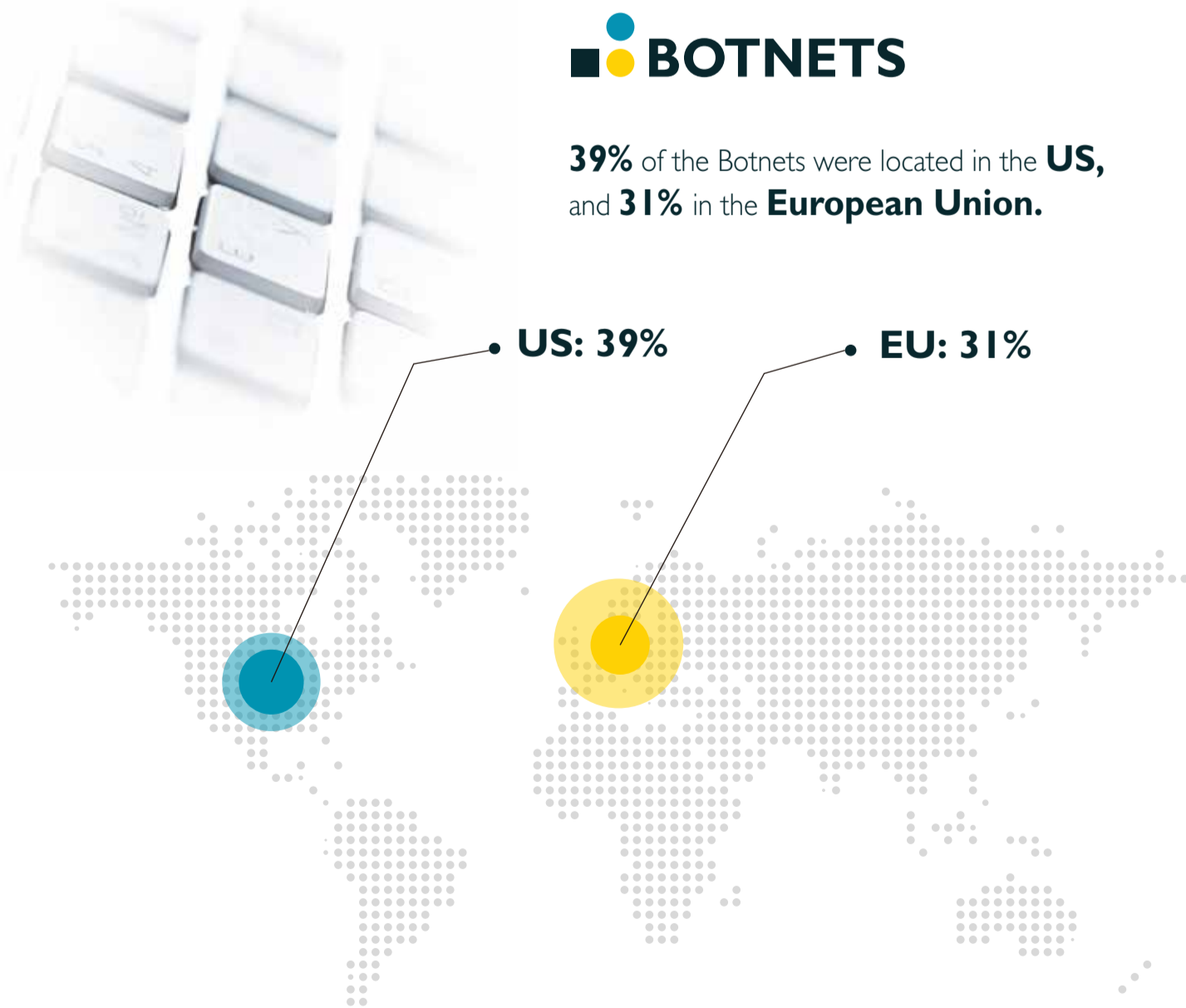
POS targeted malware is proliferating and new types such as **Poseidon, Jackpos, Newpostings**, and others have showed up lately.

The malware type that appear most often targeting POS is **Dexter**.



BOTNETS

39% of the Botnets were located in the **US**, and **31%** in the **European Union**.



*Find out more about Dyre and Dridex in our report: [Chasing the cybercrime: network insights of Dyre and Dridex Trojan bankers.](#)

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