Zeus evolution: Trusteer analyses geographical location of attack websites

Below is a media alert from ***AMIT KLEIN,*** *Trusteer's CTO new research on the evolution of Zeus, with a growing number of Web sites that host Zeus variants, as well as the rising volume of networks hosting Command & Control servers for the Zeus botnet swarms.*

1. The geographical IP distribution of sites hosting Zeus configurations.
2. Which organisations/service providers have the dubious distinction of ranking high in the Zeus Command & Control (C&C) site stakes.
3. The geographical IP distribution of sites used as a Zeus C&C platform.

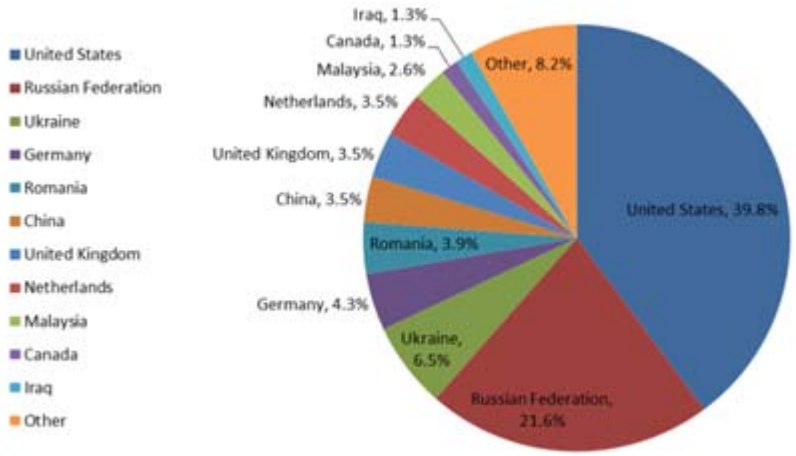
Zeus continues to evolve – but Trusteer is tracking its progress

Despite having been around for four years, Zeus continues to be a thorn in the side of the IT security industry and its business users, mainly because of its constantly evolving profile.

This evolving profile is driven in part by the ease with which black hat hackers can develop the malware for new and varied applications.

Our ongoing research here at Trusteer confirms the evolution of Zeus, with a growing number of Web sites that host Zeus variants, as well as the rising volume of networks hosting Command & Control servers for the Zeus botnet swarms.

Over the last four months Trusteer's research teams have been analysing the geographical IP distribution of sites hosting Zeus configurations.



Our research shows that the US (39.8 per cent), Russia (21.6 per cent) and Ukraine (6.5 per cent) were the top three countries, with Eastern Europe accounting for 32.0 per cent of Zeus configs.

That doesn't mean other countries are off the hook, as China, Malaysia, Iraq and Canada - along with Germany, the UK and the Netherlands in the EU territories - are also responsible for Web sites with hosted Zeus environments.

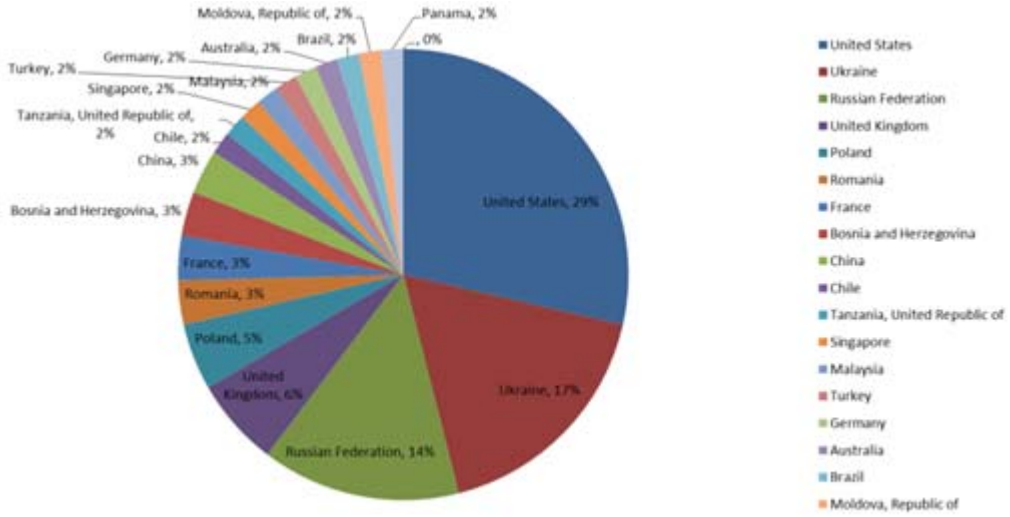
Our research team have also analysed which organisations/service providers have the dubious distinction of ranking high in the Zeus Command & Control (C&C) site stakes.

ISP	%Sites	GEO IP of C&C Sites
Informex	7%	Ukraine
PE Bondarenko Dmitriy Vladir	5%	Russian Federation
GoDaddy.com	5%	United States
GlobalNet	3%	Bosnia and Herzegovina
THEPLANET.COM INTERNET	3%	United States
PAN-SAM Ltd.	3%	Ukraine
UK2 - Ltd	3%	United Kingdom
S.Point	2%	Ukraine
Netserv Consult SRL	2%	Romania
LLC Management, informatior	2%	Ukraine
Delfa network	2%	Russian Federation
Oversee.net	2%	United States
Delta-X LTD	2%	Ukraine
Dayco Telecom, C.A.	2%	Panama
Distributed Management Infor	2%	United States
ModusLink Corporation	2%	United States
Embratel	2%	Brazil
Node4 Limited	2%	United Kingdom
E-planet	2%	Russian Federation
CIS NEPHAX	2%	Poland

Analysing 20 of the organisations that account for over half of the C&C controllers reveals that five of the 20 service providers - Informex, PAN-SAM Ltd.,S.Point, LLC Management, and informationaland Delta-X LTD - are on the Ukrainian networks and responsible for 16 per cent of Zeus C&C servers.

Another five service providers are on the US networks and responsible for 14 per cent of Zeus C&C systems, with GoDaddy.com accounting for a hefty 5 per cent of American Zeus C&C sites.

Based on this research, our analysts tested the accessibility of sites used as a Zeus C&C platform.



The analysis of sites IP accessible over the last 80 days makes for some interesting reading, as 29 per cent were found to be US Web sites, with Ukraine (17 per cent) and Russia (14 per cent) once again joining the US on the Zeus hall of shame podium.

Delving into the research reveals some interesting data, such as the UK accounting for 6 per cent, and the rising technology nation of Poland accounting for 5 per cent of IP accessible C&C systems.

Equally surprising was the inclusion of Bosnia and Herzegovina in the `charts' with three per cent - no mean feat for a country of 3.8 million citizens.

More than anything, these detailed statistics show that the `global Internet' is fast becoming highly diversified, but the increasing usage of automated registration and servicing systems on the Internet means that human operator monitoring of hosted systems is become less frequent in those countries with good Internet access.

As well as driving the cost of hosting downwards, this has the worrying effect of making it all too easy to register and set up a C&C and/or Zeus-infected Web site plus allied systems, and using the platform to infect the general Internet user community.

Trusteer will continue to monitor and report the continuing evolution of Zeus and its many variant infections, detailing the results for our many friends on the Internet.