Ice IX, the first crimeware based on the leaked ZeuS sources

By Jorge Mieres

Published: 2011-08-24 · Archived: 2026-04-06 01:36:24 UTC

Research

Research

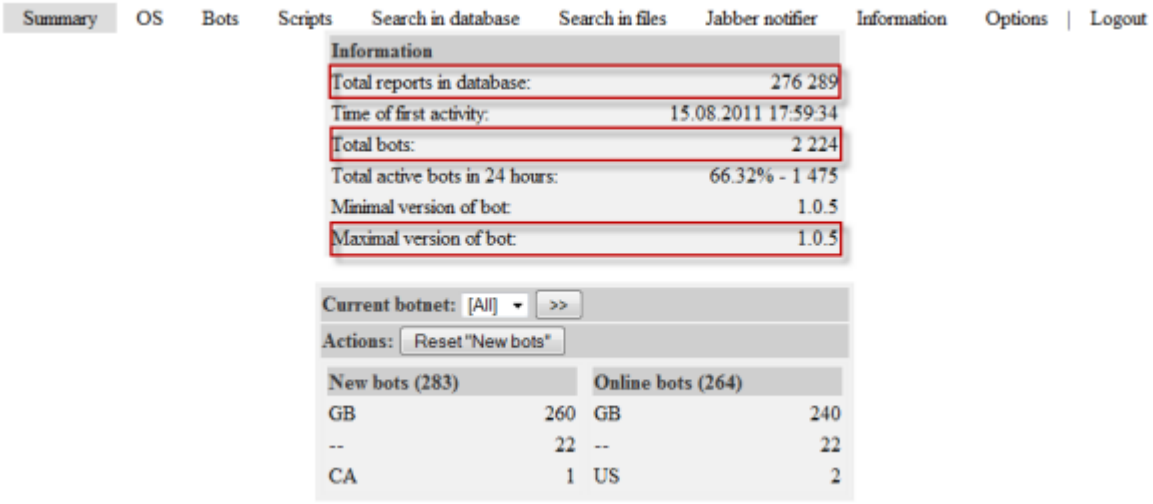
24 Aug 2011

1 minute read

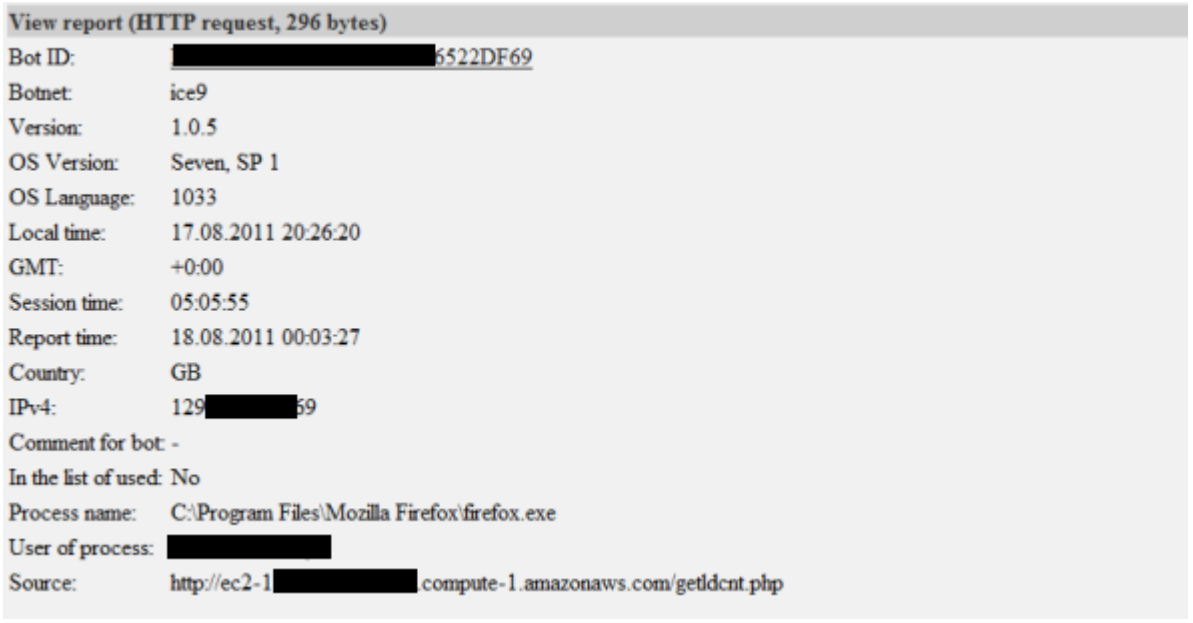
- Expert Jorge Mieres

After rumors about the supposed merger between SpyEye and **ZeuS**, and the public release of the source of the latter, it was logical that the range of possibilities opened up even more for new cybercriminals into the ecosystem of crimeware.

Consistent with this, it was only a matter of time for the emergence of new packages based on ZeuS crimeware, which is now realized. **Ice IX Botnet** is the first new generation of web applications developed to manage centralized botnets through the HTTP protocol based on leaked ZeuS source code.



The crimeware of this style is designed to steal banking information. So, it is very clear that we must focus attention on these threats and take into account that this “modified version of ZeuS” has been *In-the-Wild* since the beginning of year. The following picture is evidence Amazon Elastic Compute Cloud (Amazon EC2) data theft by this browser hooking malware:



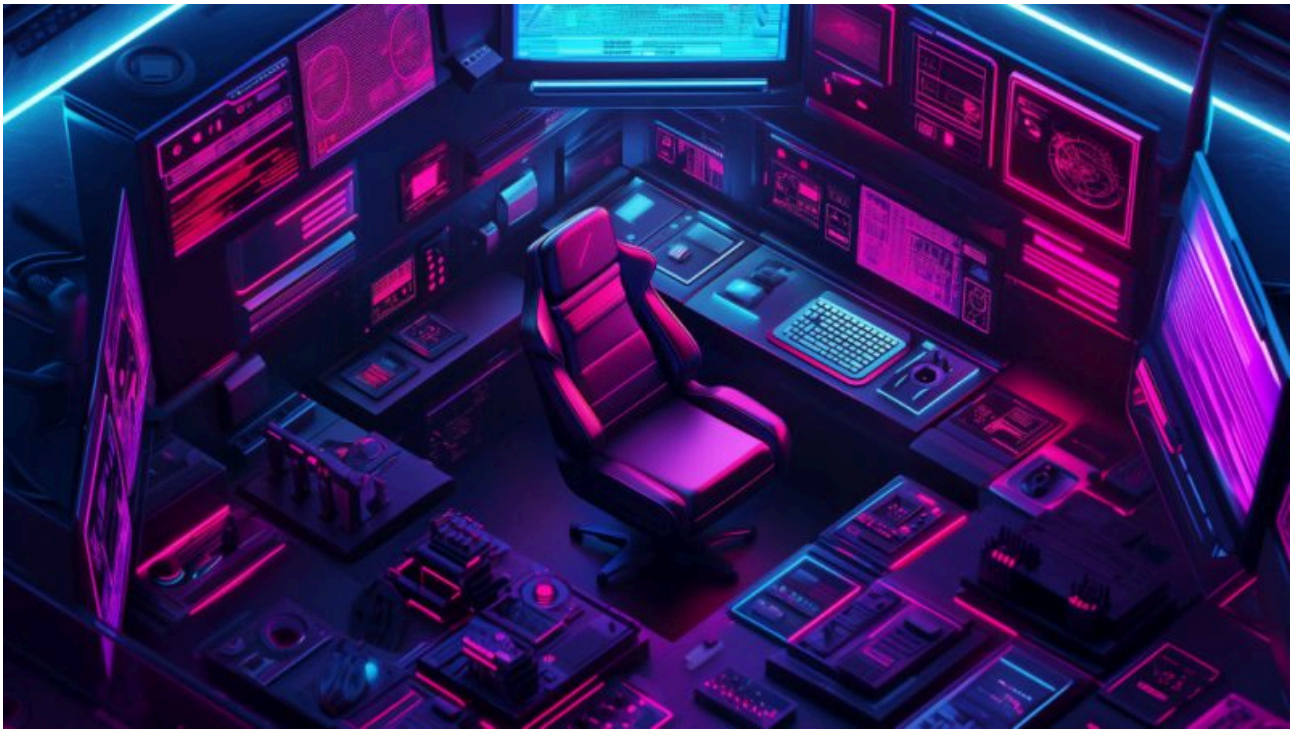
View report (HTTP request, 296 bytes)	
Bot ID:	[redacted]6522DF69
Botnet:	ice9
Version:	1.0.5
OS Version:	Seven, SP 1
OS Language:	1033
Local time:	17.08.2011 20:26:20
GMT:	+0:00
Session time:	05:05:55
Report time:	18.08.2011 00:03:27
Country:	GB
IPv4:	129[redacted]69
Comment for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Mozilla Firefox\firefox.exe
User of process:	[redacted]
Source:	http://ec2-1[redacted].compute-1.amazonaws.com/getldcnt.php

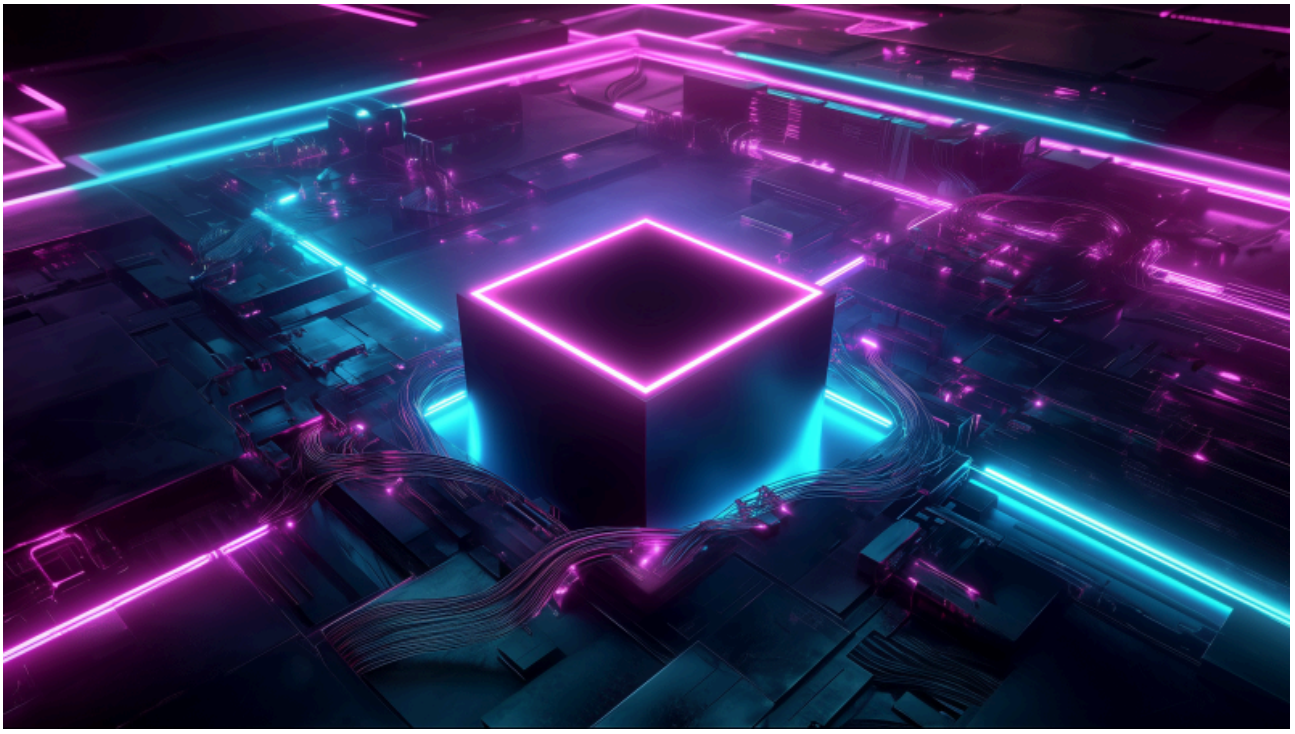
The latest version of **Ice IX Botnet** is 1.0.5, and it is selling for a very competitive $1800 in the underground markets.

It is clear that from now on, more new crimeware will be based on ZeuS code. New developers, hoping to profit from cybercrime, will attempt to create their own new alternatives based on this source.

At Kaspersky Lab, we investigate the impact of not only this particular threat but also new emerging crimeware. We work to keep you informed!

Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
