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

securelist.com/ice-ix-the-first-crimeware-based-on-the-leaked-zeus-sources/29577/

Research

Research

24 Aug 2011

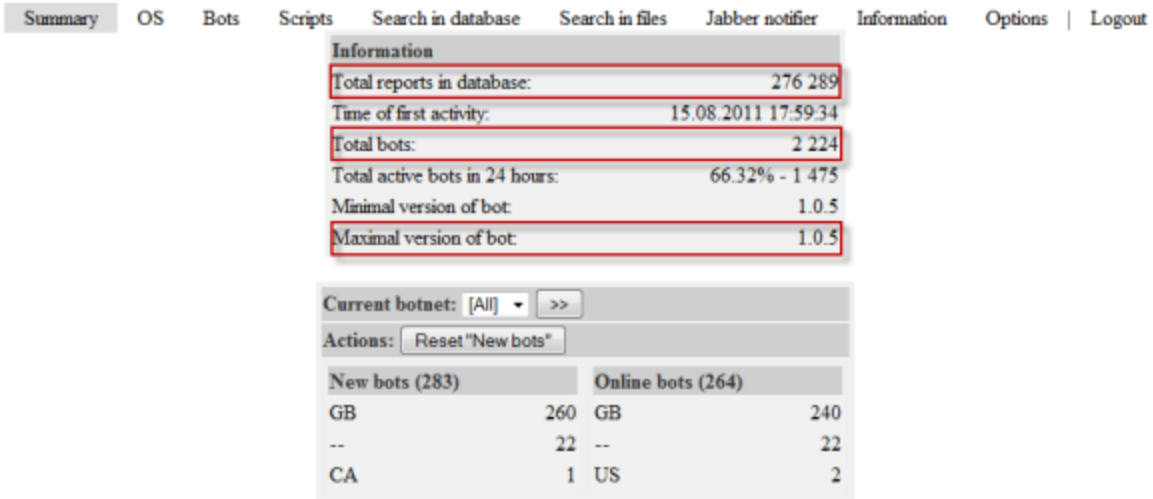
minute read

Authors

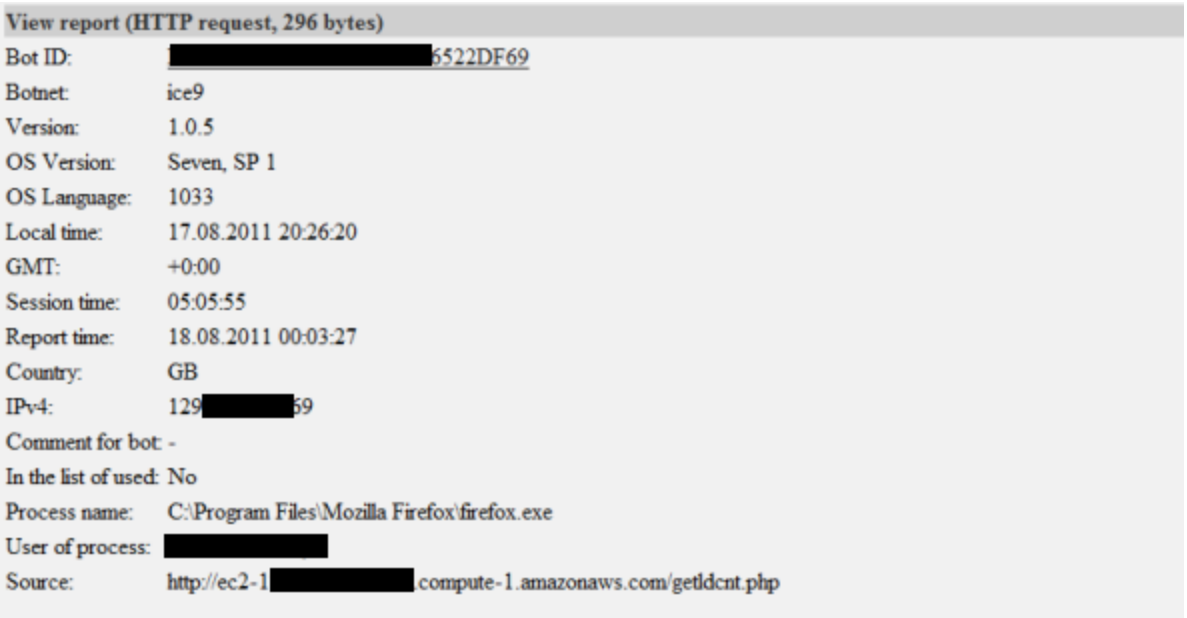
Expert Jorge Mieres

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!

- Botnets
- Malware Creators
- Malware Technologies
- ZeuS

Authors

Jorge Mieres

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

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

Jumcar. Peruvian Navy? Who could be behind it? [Third part]

Jumcar. Timeline, crypto, and specific functions. [Second part]

Jumcar. From Peru with a focus on Latin America [First part]

AlbaBotnet, another new crime wave in Latin American cyberspace

New crimeware attacks LatAm bank users

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.

-
-
-