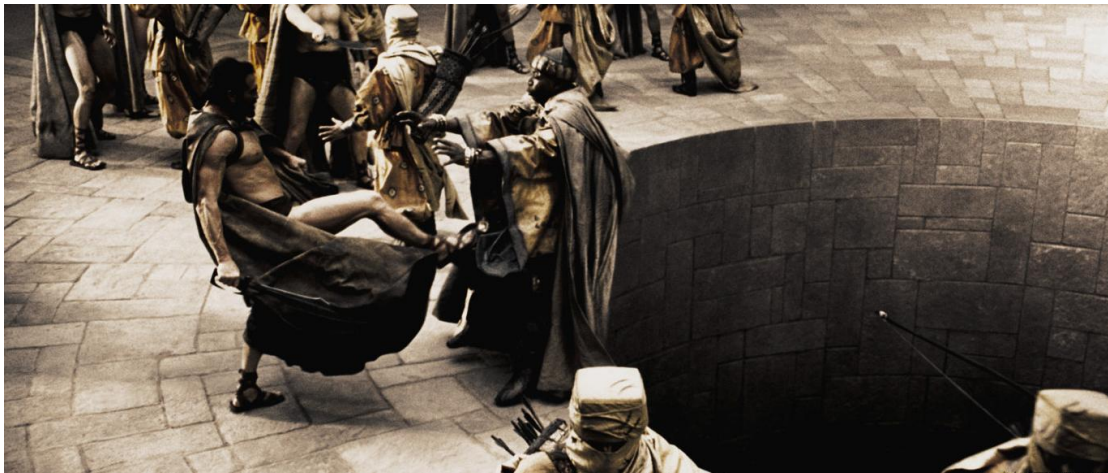


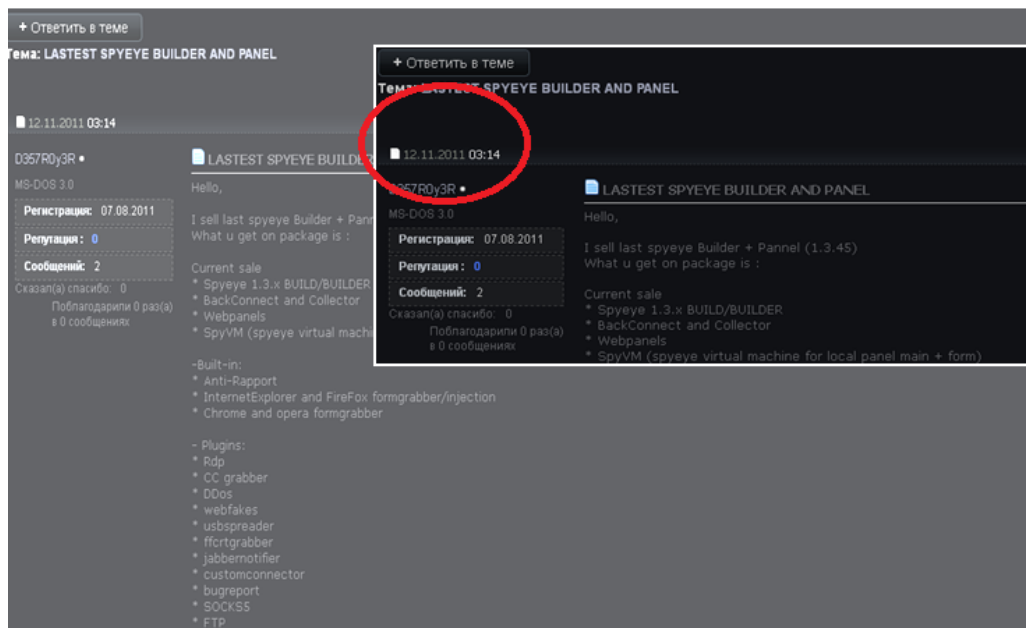
# SpyEye being kicked to the curb by its customers?

by Sean Bodmer, Sr. Research Analyst, Damballa



Since its first release a few years ago, SpyEye has been widely known as a highly effective competitive crimeware construction kit to the tried-and-true malware kit, Zeus. In Q2 2011, Damballa broke the news that the SpyEye builder 1.3.45 had been cracked by world renowned French researcher, Steven K, 'Xylitol,' a founding member of the RED Crew. As of Q3 2011, Damballa Labs identified 11 new criminal operators, who began using the cracked version of SpyEye. The cracked version had the 'nick/ident' removed from the builder so the criminals could operate without any ties to the original purchaser of the malware kit from the author team. This 'nick/ident' was a stored variable for the builder to use as a component of the built-in licensing system. The authors of SpyEye implemented it into the malware kit to prevent non-paid customers from accessing the powerful malware kit.

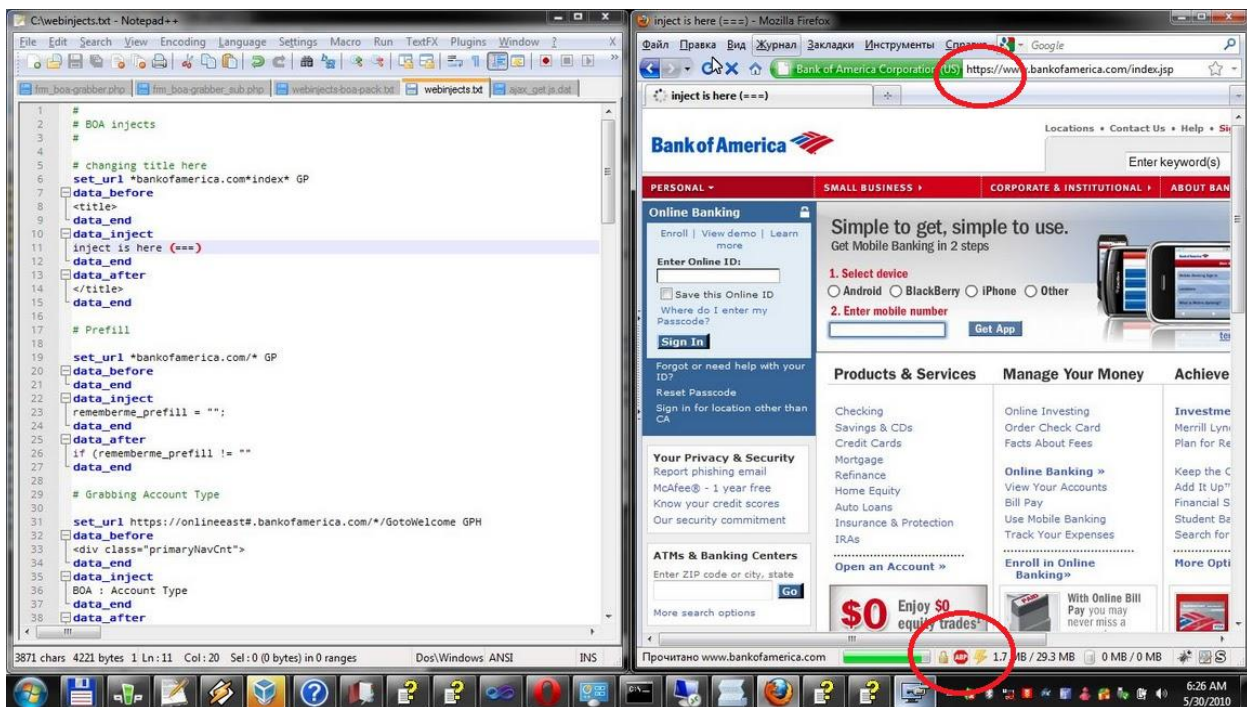
Looking online today, one will only see sales for 1.3.45 and older versions of SpyEye with no new add-ons or updates. In the December 2011 posting below, this criminal is still selling 1.3.45 with all of the plug-ins/add-ons that were available at that time. By this date, SpyEye had already been updated to 1.3.48, which was released on 10.1.2011 – a simple update designed to defeat the licensing system crack that had been developed by Xylitol, disclosed by Damballa Labs in August ([First Zeus, now SpyEye. Look at the source code now!](#) ).



### What's the impact?

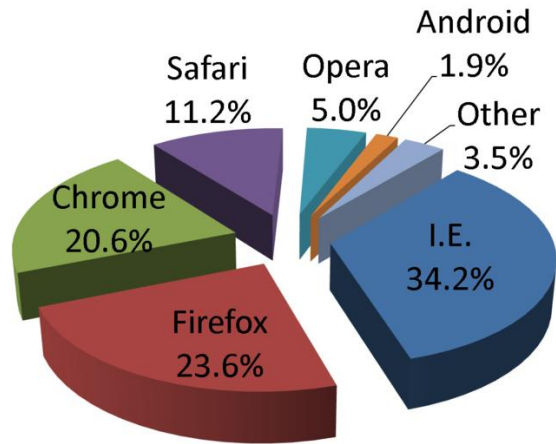
So what does this mean? Basically, SpyEye will begin losing its customer base and criminals will start using newer tools. In 2011, every web browser went through numerous versions and patches to keep their browsers secure from cyber criminals, especially ones who use malware like SpyEye that implement web injection techniques - a method that is used by the malware to siphon online accounts and especially to steal banking credentials and information. In the image below, SpyEye is shown to be very efficient at ensuring the victim is completely unaware of the theft while it is occurring.

Most users rely on visual cues to validate that their session is a secure https-based (SSL) session. Thus, they will comfortably input their banking account information into the site and login. However, many users are not aware that malware like SpyEye, Zeus, IcelX, TDL, Hiloti, Carberp, and many others have functionality commonly known in the security world as a 'web inject.' Below, the code on the left side of the browser is a sampling of the code used to perform a web inject on Bank of America customers. To read more on the SpyEye or Zeus web inject process, follow this link to a great article. [\(SpyEye & Zeus\) Web Injects - Parameters](#) by Malware at Stake.



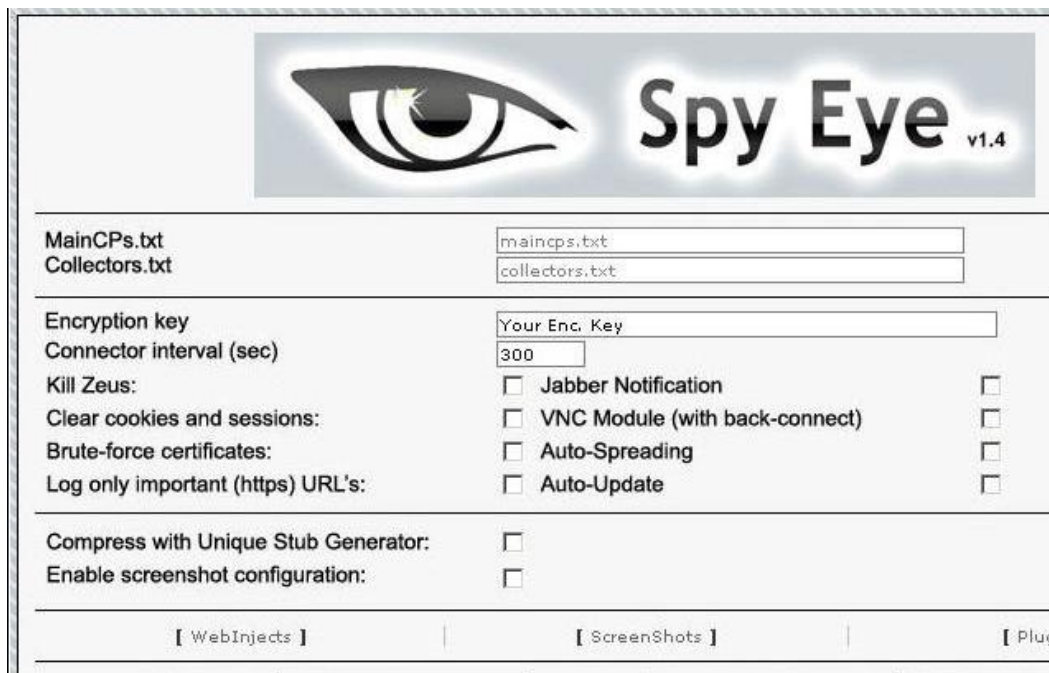
The longer criminals go without updating their malware kits, the better protected potential victims will be because browser vulnerabilities are patched and threat signatures are produced. The danger increases rapidly when new tools emerge to replace SpyEye as it becomes useless to criminals. Damballa is seeing growing evidence of this trend.

The graph below was prepared by Wikimedia for the month of October 2011, representing the breakdown of web browser usage at the time of the latest update to SpyEye. At that time, SpyEye had fully functional web injects for Internet Explorer (default) and support for additional browsers if the criminal purchased those additional add-ons. Between September 2011 and February 2012, all of the browsers below have gone through numerous security patches and versions. For example, in March 2011 Firefox released version 5 of their browser and by February 2012 they are at version 10. All of the other browsers listed below have gone through their own security updates and fixes, which have made the 1.3.48 web injects less effective and not as stable. They now have the potential to crash the browser repeatedly, thereby notifying the victim that 'something is afoot.'



**Browser Usage on Wikimedia  
October 2011**

Damballa is also tracking scammers (rippers), who are trying to sell fake versions where they have simply modified screenshots of the builder using image editing software to make the version of the builder 'look' newer or added fake buttons and/or features to the builder to deceive potential victims of the scam. Once the purchase is made, the buyer (victim) pays for the suite and receives an old version of SpyEye . This tactic of scamming ('ripping') other criminals is not new and occurs more frequently than one would think. As you can see below, someone has modified the builder of SpyEye version 1.x to appear as version 1.4, which they were attempting to sell online. This is one of many scams related to SpyEye. So, if you're a criminal reading this - let the buyer beware! It is ironic that criminals rip off other criminals.



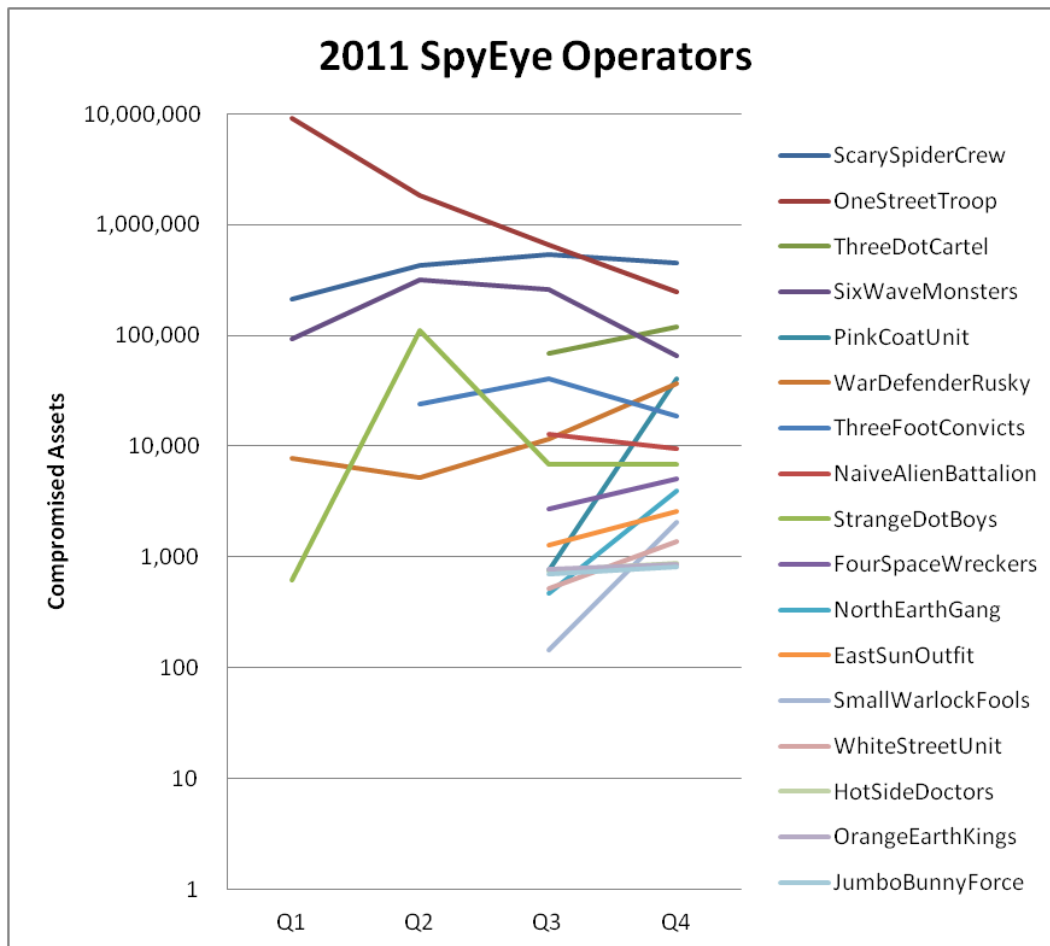
**What exodus?**

In late 2011, a handful of SpyEye developers (including Gribodemon) and resellers have disappeared from the Internet and stopped selling any new SpyEye builders or add-ons online. Some suspect they are hiding with all of the heat that plagued 'Slavik,' the author of Zeus, before he went underground for about a year.

In mid-November, the Damballa Labs team identified that the core build of SpyEye and the add-ons that were sold on underground forums were not being updated after Microsoft released major patches for Windows-based operating systems. So what is going on? There is a gaping hole in the tool box of cyber criminals as SpyEye (the once dominant tool, only 2nd in popularity to the TDL/TDSS kit) is being 'kicked to the curb' and something has to fill that void. Some security products are now easily detecting the latest SpyEye unarmored binaries and armoring tools will only take a criminal so far. How are cyber criminals filling their pockets today? First, let's look at the overall activity of SpyEye through 2011.

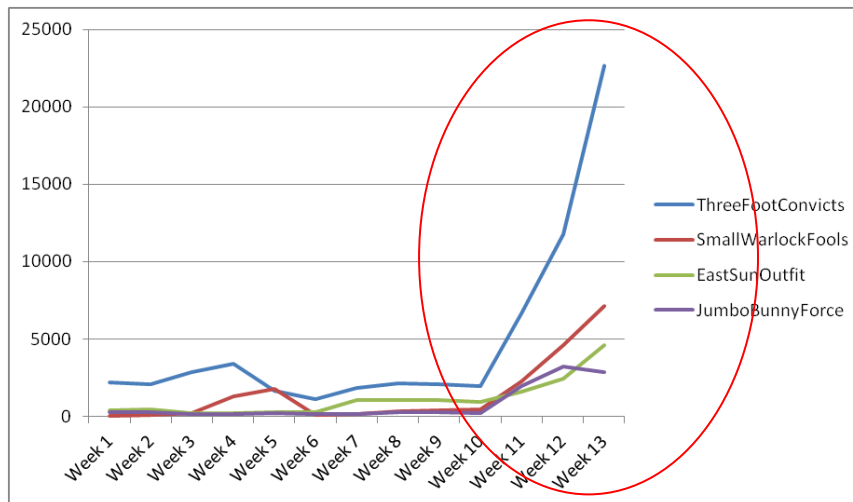
In the graph below, the names on the right are 'code names' that Damballa Labs uses to track specific criminal groups - each name ties directly to one of the groups we have identified and actively track. This logarithmic scale graph shows that in Q3 2011, there were eleven new criminal groups who began using SpyEye as their core criminal infrastructure tool. In addition, eight of the seventeen groups (or nearly half) were declining or showing no growth in Q4. Lastly, one of the groups who started out in Q3 was also taking a loss a few months later. What happened?

The lack of support and maintenance of SpyEye by the developers of the malware construction kit has left their customers (criminals) to hang out to dry.



Damballa discovered something else interesting. Four of the successful “SpyEye” criminal operators (or so we thought at the time) were not SpyEye anymore. Although the infrastructure had been SpyEye since at least January 2011, in December 2011 something happened. Four SpyEye operators swapped out their infrastructure almost overnight. Four separate groups from three corners of the globe started using Ice IX, which is a variant of a Zeus version 2 source code leak from Q2 2011.

Below is a non-logarithmic scale of the four criminal groups who started switching over to Ice IX in the last month of Q4. This specific course of events illustrates a similar event that occurs on a regular basis in the white hat side of Information Security - if the tool stops working, find a new one. Here there are four clear examples of what appears to be the start of a trend - useless malware tools being dumped for well-maintained and updated tools.



### Is SpyEye falling from grace in the underground?

The screenshot below is courtesy of an underground source and contains the current/latest dates of SpyEye's most recent updates. Notice the 'latest update' date for the FireFox grabber, 5.24.2011. This date puts the web injects for FireFox alone three complete versions behind where SpyEye's compatibility should be to ensure stable and stealthy theft of victim information and credentials.

```
!default [latest update: 2011.10.01 (client pack) ]
!rdp [latest update: 2011.07.07]
!socks
!ftp
!ffcertgrabber [latest update: 2011.05.24]
!ccgrabber
```

The updates to all of the major SpyEye add-ons are months behind and now causing browser crashes or are just plain not working. The lack of updates is causing SpyEye to rapidly decrease in popularity. The last update was on 10.1.2011, which was the release of SpyEye builder 1.3.48 - a quick fix for the crack that was released for 1.3.45. No other updates have followed since.

**The questions that arise are:**

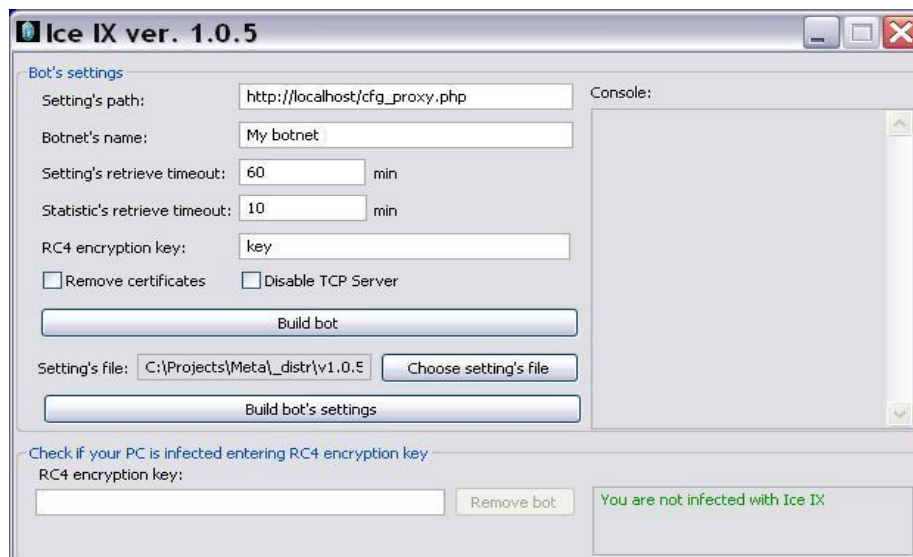
1. Why is this platform not being updated?
2. Why is the author team not responding to online/forum/support posts or inquiries?
3. What is in store for the future of SpyEye?

**A new frontier of tools, all thanks to Slavik...**

In Q2 2011, the source code for Zeus 2.0.8.9 was released, which was originally known to have been sold to Gribodemon in late 2010. Gribodemon was to become the new steward for the Zeus code base and would later integrate most of the Zeus functionality, specifically the web-injects and form grabber functionality into SpyEye. What was once thought of as the best of both worlds came to a halt in late 2011. However, earlier in 2011 another group was already working on a modified version of the Zeus v 2.0.8.9 malware kit and created Ice IX version 1.x, a complete revamp and enhancement of the original v2 Zeus code base.



This new version wasn't the construction of some CIA program as depicted in the film 'The Recruit' from 2003, where a computer virus called 'Ice-9' erased hard disks and traveled through un-protected power and utility lines to decimate every computer on Earth. Although the name suggests some resonance of a Kurt Vonnegut novel or some spooky CIA movie, the tool really has some highly evolved functionality that does seem to intrigue researchers in the security world. This new tool seems to be splitting a path right down the center of SpyEye's customer base.

**A brief introduction to Ice IX**

Although this simple looking builder seems benign enough, don't let it fool you. There is new functionality in this malware construction kit that has drastically increased the survivability of this tool over its predecessors. Here is a list of the latest identified functionality of Ice IX (as of this posting):

1. Keylogging
2. Grabs HTTP and HTTPS forms (IE, FF, Chrome)
3. Injects code into IE, IE-based browsers (AOL, Maxthon, etc), and FF
4. Grabs cookies, .sol files and saved forms data
5. Grabs the following FTP clients: FlashFXP, Total Commander, WsFTP 12, FileZilla 3, FAR Manager 1,2, WinSCP 4.2, FTP Commander, CoreFTP, SmartFTP
6. Grabs Windows Mail, Live Mail, Outlook - Contacts, Calendar, Notes, and Emails
7. SOCKS 5 with back-connect option
8. Screenshots in real time, or triggered by specific URLs
9. Gets certificates from "my" storage through the modified PFXImportCertStore API
10. All certificates are automatically sent to the C&C server for later re-use
11. Search for files on the logical drives using wildcards or install a specific file
12. TCP traffic sniffer
13. New methods for commands to control the infected victims
14. Ability to redirect victim notifications via email or voip from financial institutions
15. Protection against trackers. Now you can host your botnet on a regular hosting, not just bulletproof servers anymore
16. Better response rate and resilience - as the developers are constantly updating their product
17. Functionality updates and tech support
18. In-depth SDK for customers to create custom modules

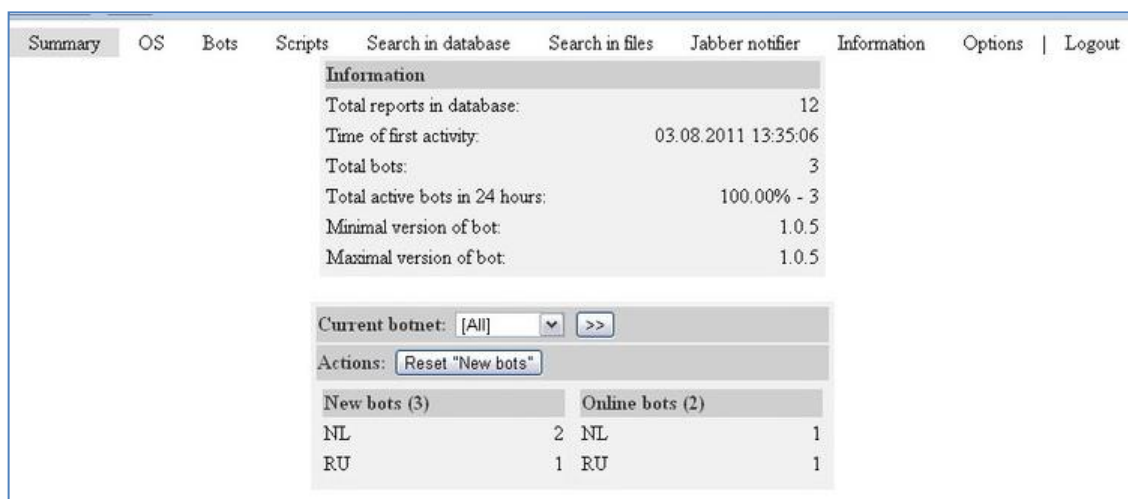
### Price for Ice IX

Ice IX is available at a more reasonable rate than SpyEye. In its heyday, the SpyEye builder plus all of the available add-ons cost as much as \$8,400. Ice IX charges:

- With hardcoded hosting: \$600/LR/WMZ. Malware + builder that generates the config file
- Unlimited builder license: \$1800/LR/WMZ

### Ice IX's C&C Interface

The 'not so sexy' but very functional control panel interface of Ice IX picks up where Zeus version 2 left off. Not visually appealing, but it isn't built for looks as the authors apparently spent most of their time refining, updating, and enhancing the malware's stealth, evasion, and survivability techniques. The Ice IX control panel has an easy to use interface common among crimeware kits today.

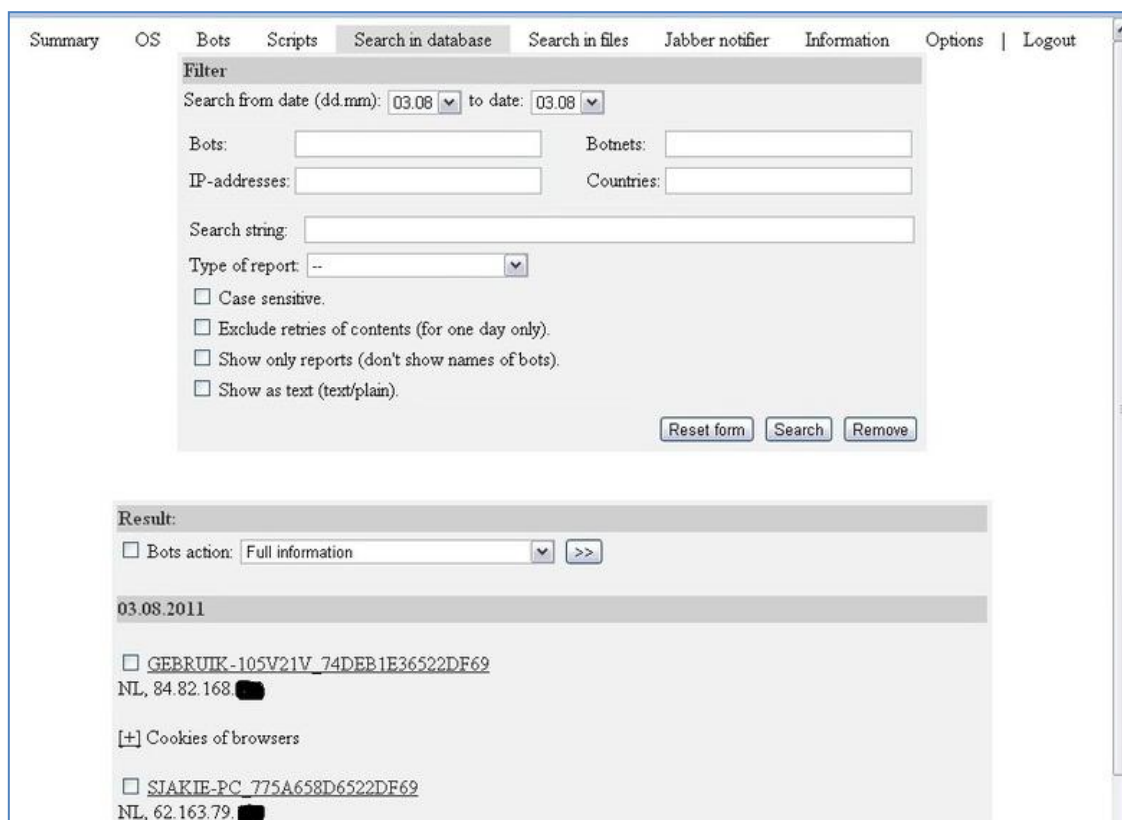


The screenshot shows the Ice IX control panel interface with the following elements:

- Navigation Tabs:** Summary, OS, Bots, Scripts, Search in database, Search in files, Jabber notifier, Information, Options, Logout.
- Information Section:**
  - Total reports in database: 12
  - Time of first activity: 03.08.2011 13:35:06
  - Total bots: 3
  - Total active bots in 24 hours: 100.00% - 3
  - Minimal version of bot: 1.0.5
  - Maximal version of bot: 1.0.5
- Current botnet:** [All] >>
- Actions:** Reset "New bots"
- Bot Lists:**
  - New bots (3):**

NL	2
RU	1
  - Online bots (2):**

NL	1
RU	1

A screenshot of the Damballa search interface. The interface has a navigation bar at the top with tabs for Summary, OS, Bots, Scripts, Search in database (selected), Search in files, Jabber notifier, Information, Options, and Logout. Below the navigation bar is a "Filter" section with the following fields: "Search from date (dd.mm):" and "to date:" both set to "03.08"; "Bots:" and "Botnets:" text input fields; "IP-addresses:" and "Countries:" text input fields; a "Search string:" text input field; and a "Type of report:" dropdown menu set to "--". There are four checkboxes: "Case sensitive.", "Exclude retries of contents (for one day only).", "Show only reports (don't show names of bots).", and "Show as text (text/plain)". At the bottom of the filter section are three buttons: "Reset form", "Search", and "Remove". Below the filter section is a "Result:" section with a "Bots action:" dropdown menu set to "Full information" and a ">>" button. The results are displayed under the date "03.08.2011" and include two entries: "GEBRUIK-105V21V\_74DEB1E36522DF69" with IP "NL, 84.82.168." and "SIKIE-PC\_775A658D6522DF69" with IP "NL, 62.163.79.". Each entry has a checkbox to its left.

Ice IX was initially released in April 2011, which is interesting considering the relatively short time period between the actual release of the Zeus v2 source code and the completion of this tool kit. The hypothesis between several leading industry researchers (who participate in a collective effort to gather counter intelligence on crimeware operators and attribute their campaigns to their identities) is that the developer of Ice IX is more than likely someone close to the original Zeus development team. Ice IX maintains the traditional malware/form grabbing functionality that cyber criminals have grown to love. It has also been dramatically overhauled and improved with only the framework of Zeus version 2 still noticeable to skilled developers or malware analysts.

The injection technologies steal information from secure web sessions by injecting code into the web browser during an SSL connection (typically while logging into a financial institution) where usernames, passwords, and security questions that help verify accounts can be collected. Through most of Q2 and Q3 of 2011, Ice IX maintained a low-flying pace. In Q4, several SpyEye groups turned to the 'properly maintained' Ice IX. This new variant also has new and improved functionality to 'redirect notification of fraudulent activity' from financial institutions. To learn more about this technique, read through two postings that cover this in-depth. The postings are published by Amit Klein, CTO of Trusteer. An extract of one of the posts reads:

"In addition to stealing bank account data, these Ice IX configurations are capturing information on telephone accounts belonging to the victims. This allows attackers to divert calls from the bank intended for their customer to attacker controlled phone numbers. I believe the fraudsters are executing fraudulent transactions using the stolen credentials and redirecting the bank's post-transaction verification phone calls to professional criminal caller services that approve the transactions."

More information on this new technique:

Ice IX Redirects bank phone calls to attackers [Protecting yourself on and offline from Ice IX](#)



## Summary

What is in store next? Damballa will monitor how things progress over the next few months. Maybe the SpyEye team is on vacation and has new modules in their development pipeline that have yet to be seen. Maybe Ice IX is the next big thing.

This Research Note covered:

- The decline of SpyEye during Q4 of 2011
- The emergence of Ice IX as a desired replacement for SpyEye
  - Gribodemon's own customers moved to Ice IX – an interesting piece of intelligence.
  - Ice IX developer states that his goal is to build on the success of Zeus and SpyEye and develop Ice IX to be a competitor to both. Similar to when SpyEye first threatened Zeus's reign of power.

Predictions:

- Ice IX is essentially a highly updated and modified version of Zeus version 2, which was already competitive with SpyEye. Now that Ice IX is readily available, cheaper, and has more functionality than SpyEye, Damballa expects more criminals to select more effective and stable tools over the SpyEye malware kit.

Precautions:

- Ensure systems and browsers are up-to-date and be aware of what emails or hyperlinks are clicked on. One wrong click may lead down the wrong path.

*Prepared by:  
Damballa Inc.  
<http://www.damballa.com>  
Copyright 2012. All rights reserved worldwide.*