Sphinx, a new variant of Zeus available for sale

By Pierluigi Paganini

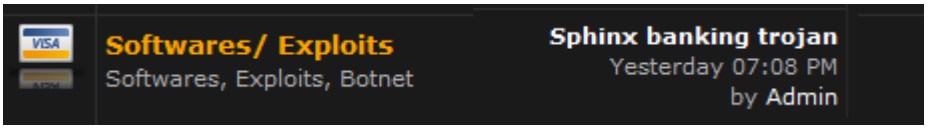
Published: 2015-08-26 · Archived: 2026-04-05 19:13:07 UTC

Sphinx, a new variant of Zeus available for sale in the underground

A new variant of the popular Zeus banking trojan dubbed was Sphinx is appeared for sale on the black market, it operates entirely through the Tor network.

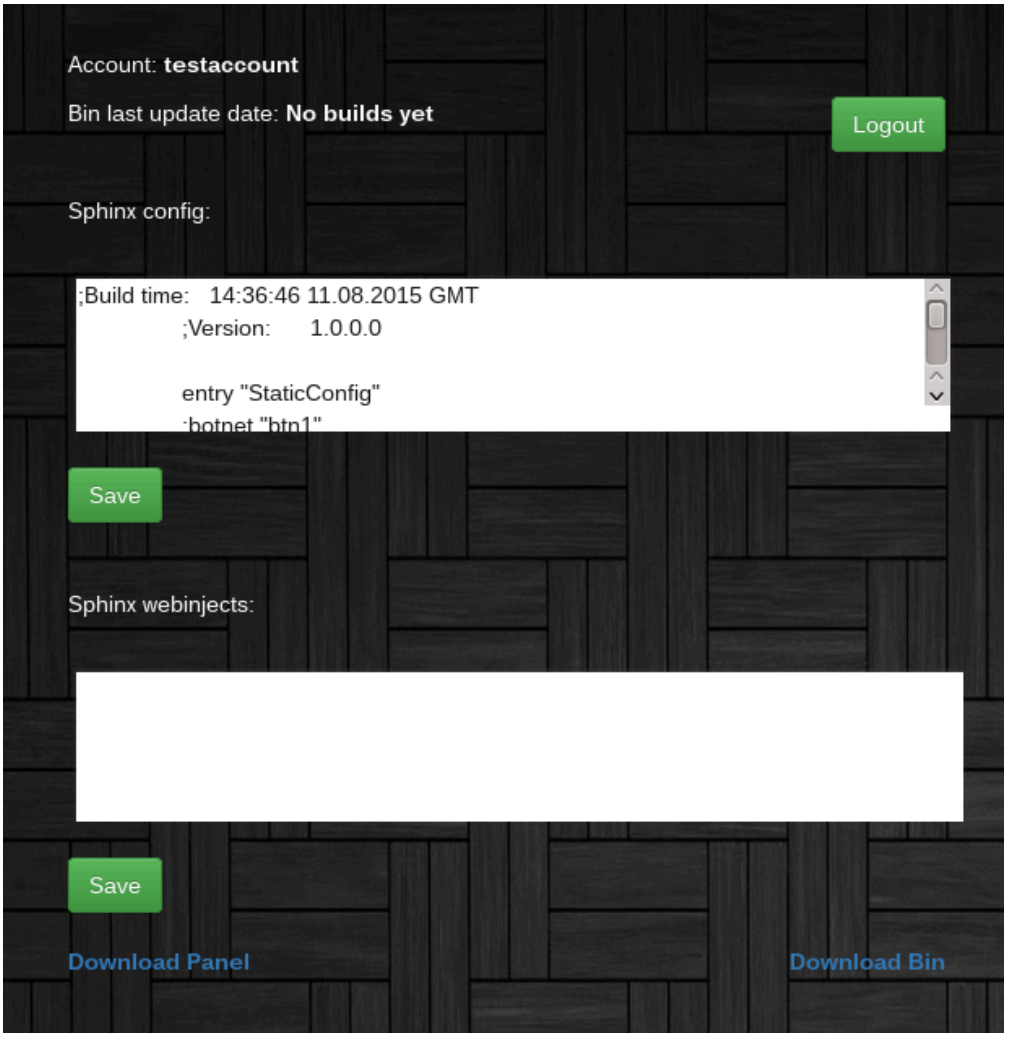
A few days ago a new variant of the popular Zeus banking trojan was offered for sale on the black market, its name is Sphinx.

Sphinx code is written in C++ and is based on the source code of the ZeuS trojan. The authors have designed it to operate through the Tor network. According to the author, Sphinx is immune to sinkholing, blacklisting, and the ZeuS tracker.



The Sphinx kit is currently available for sale at $500 USD per binary, the seller accepts Bitcoin and DASH as a method of payment. Buyer need to register on a website to make the payment, once registered both BTC and DASH addresses are generated.

When the seller will receive the payment, buyer account is enabled and will get the rights to edit the config and request a build.



The seller sustains that operators that will buy it do not need bulletproof hosting, below the list of feature implemented in the Sphinx Features:

Malware:

- *Formgrabber and Webinjects for latest Internet Explorer, Mozilla.*
- *Firefox and Tor Browser with cookie grabber and transparent page redirect(Webfakes).*
- *Backconnect SOCKS, VNC.*
- *Socks 4/4a/5 with UDP and IPv6 support.*
- *FTP, POP3 grabber.*
- *Certificate grabber.*
- *Keylogger.*

Certificate grabber:

Sphinx is able to intercept certificates when they are in use to establish a secure connection or for signing a file. It is very common in the criminal underground to abuse digital certificates, for example to digitally sign malware

code with digital certificates of a trusted organization in order to to bypass antivirus solutions.

Backconnect VNC:

This is the most essential feature of a banking trojan. It allows you to make money transfers from the victims computer. Your VNC is done on a different desktop than the victim's desktop, so its completely hidden.

You can steal money from the bank while the victim is playing multiplayer games or watching movies. Forget about configuring the browser, because when carding with Sphinx you don't need to.

With Backconnect VNC you can also remove anti-virus/rapport software from the victim's computer. Port-forwarding for the victim is not required due to the use of Reverse connection.

Backconnect SOCKS:

Use your victims as a SOCKS proxy. Port-forwarding is not required due to use of Reverse connection.

Webinjects:

Used for speeding up report gathering. With Webinjects you can change the content of a website and ask for more information. You can do such things as asking for credit-card data from victims PayPal/Amazon/Ebay/Facebook for successful login.

Webinjects use ZeuS format. You have to create your own web injects or use those that are publicly available. Sphinx uses ZeuS format so all released webinjects for Zeus/Spyeye/Citadel are compatible.

Webfakes:

Used to do phishing attacks without having to trick the victim into going in to a fake domain. For example: When configured for bankofamerica, the user is transparently redirected to your phishing site without changing the url.

Installation:

At the moment, the bot is primarily designed to work under Windows Vista/Seven, with enabled UAC, and without the use of local exploits. Therefore, the bot is designed to work with minimal privileges (including the user "Guest").

In this regard the bot is always working within sessions-per-user. The bot can be set for each user in the OS, and the bots do not know about each other. When you run the bot as a "LocalSystem" user it will attempt to infect all users on the system.

When you install Sphinx, the bot creates its copy in the user's home directory. This copy is tied to the current user and OS, and cannot be run by another user. The original copy of the same bot that was used for installation, will be automatically deleted, regardless of the installation success.

Communication:

Session with the server through a variety of processes from an internal "white list" that allows you to bypass most firewalls. During the session, the bot can get the configuration to send the accumulated reports, report their

condition to the server, and receive commands to execute on the computer.

The session takes place via HTTP-protocol, all data sent by a bot and received from the server is encrypted with a unique key for each botnet.

Webpanel:

Sphinx command and control (C&C) has not changed from ZeuS. Old ZeuS fans will be pleased to use this comfortable bot network control system again. Its coded in PHP using extensions mbstring and mysql.

Features:

- XMPP notification.
- Statistics.
- Botlist.
- Scripts

XMPP notification:

You can receive notifications from the Control Panel in a Jabber-account.

At the moment there is the possibility of receiving notifications about a user entering defined HTTP/HTTPS-resources. For example: it is used to capture a user session at an online bank.

Scripts:

You can control the bots by creating a script for them. Currently, syntax and scripting capabilities, are very primitive.

Botlist:

- Filtering the list by country, botnets, IP-addresses, NAT-status, etc.
- Displaying desktop screenshots in real time (only for bots outside NAT).
- Mass inspection of the Socks-servers state.

Displays detailed information about the bots:

- Windows version, user language and time zone.
- Location and computer IP-address (not for local).
- Internet connection speed (measured by calculating the load time of a predetermined HTTP-resource).
- The first and last time of communication with the server.
- Time online.
- Ability to set comment for each bot.

Statistics:

- Number of infected computers.
- Current number of bots in the online.

- The number of new bots.
- Daily activity of bots.
- Country statistics.
- Statistics by OS.

The seller suggests “using Internet Explorer traffic for the exploit-kit in order to get maximal profit while using Sphinx.”

At the time I was writing the Tor website site http://dagxkme5nbxm5nkh.onion reported in the ad appears down.

Stay Tuned!

[adrotate banner=”9″]	[adrotate banner=”12″]

Pierluigi Paganini

(Security Affairs – Zeus banking trojan, Sphinx)

[adrotate banner=”5″]

[adrotate banner=”13″]
