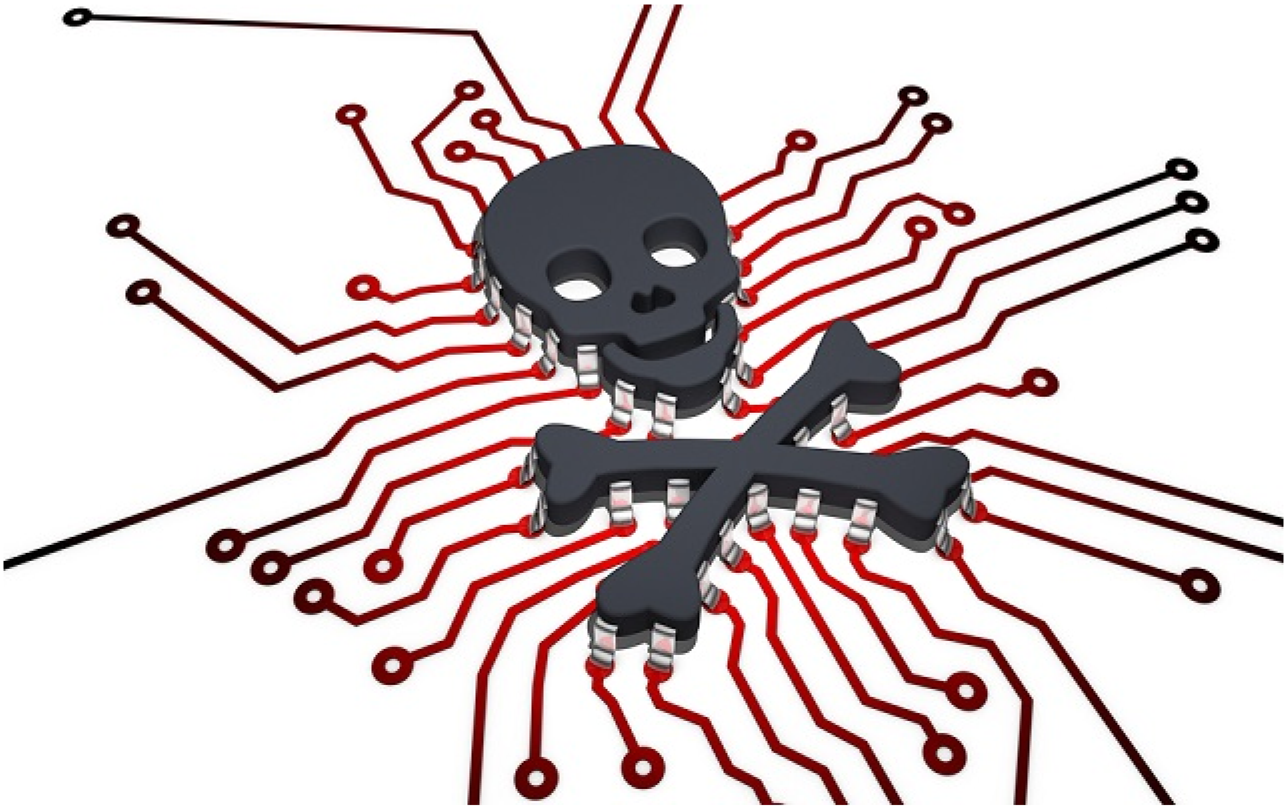
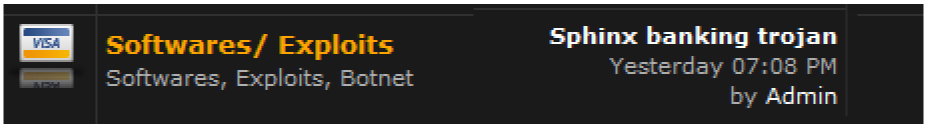
Sphinx: New Zeus Variant for Sale on the Black Market

web.archive.org/web/20160130165709/http://darkmatters.norsecorp.com/2015/08/24/sphinx-new-zeus-variant-for-sale-on-the-black-market/

August 24, 2015



The 0Day marketplace was a busy beaver this weekend. I've been waiting and watching Sphinx for the past 10 days to see if the 0Day admin would verify this new threat:



Softwares/ Exploits
Softwares, Exploits, Botnet

Sphinx banking trojan
Yesterday 07:08 PM
by Admin

New Zeus Variant

On Sunday evening, Sphinx, a new variant of the Zeus banking trojan was admin-verified. Sphinx is coded in C++ and based on ZeuS source code and operates fully through the Tor network using a Tor hidden service. This variant is listed as being immune to sinkholing, blacklisting, and the ZeuS tracker.

The seller claims that you do not need bulletproof hosting (generally immune from takedown requests) when operating a Sphinx botnet, though he still recommends it.

Sphinx Features (as listed in the forum with minor edits):

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:

By intercepting windows functions, Sphinx is able to intercept certificates when they are in use. For example: for signing a file – this is useful for getting file-signing certificates for signing your
malware to bypass all anti-virus

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

The Sphinx kit is currently selling for $500 USD per binary, with Bitcoin and DASH as the only accepted method of payment. To purchase: the seller has you register on a website where an address for both BTC and DASH are generated.

After the payment is received the buyer account is automatically validated and rights to edit the config and request a build are granted. Upon finalization of the purchase, all wheeling and dealing is handled via XMPP. The seller also includes escrow.

No further activity has been noted regarding Sphinx since the admin verified this new malware. Though there was some rattling of bones when someone made mention of security researchers possibly discovering it and blogging about it – all transactions appear to be occurring behind closed doors now.

-