A peek inside the Smoke Malware Loader - Webroot Blog

By Blog Staff

Published: 2012-02-04 · Archived: 2026-04-05 16:08:20 UTC


A peek inside the Smoke Malware Loader

by | Feb 3, 2012 | Threat Lab

Reading Time: ~ 3 min.

The competitive arms race between security vendors and malicious cybercriminals constantly produces new defensive mechanisms, next to new attack platforms and malicious tools aiming to efficiently exploit and infect as many people as possible.

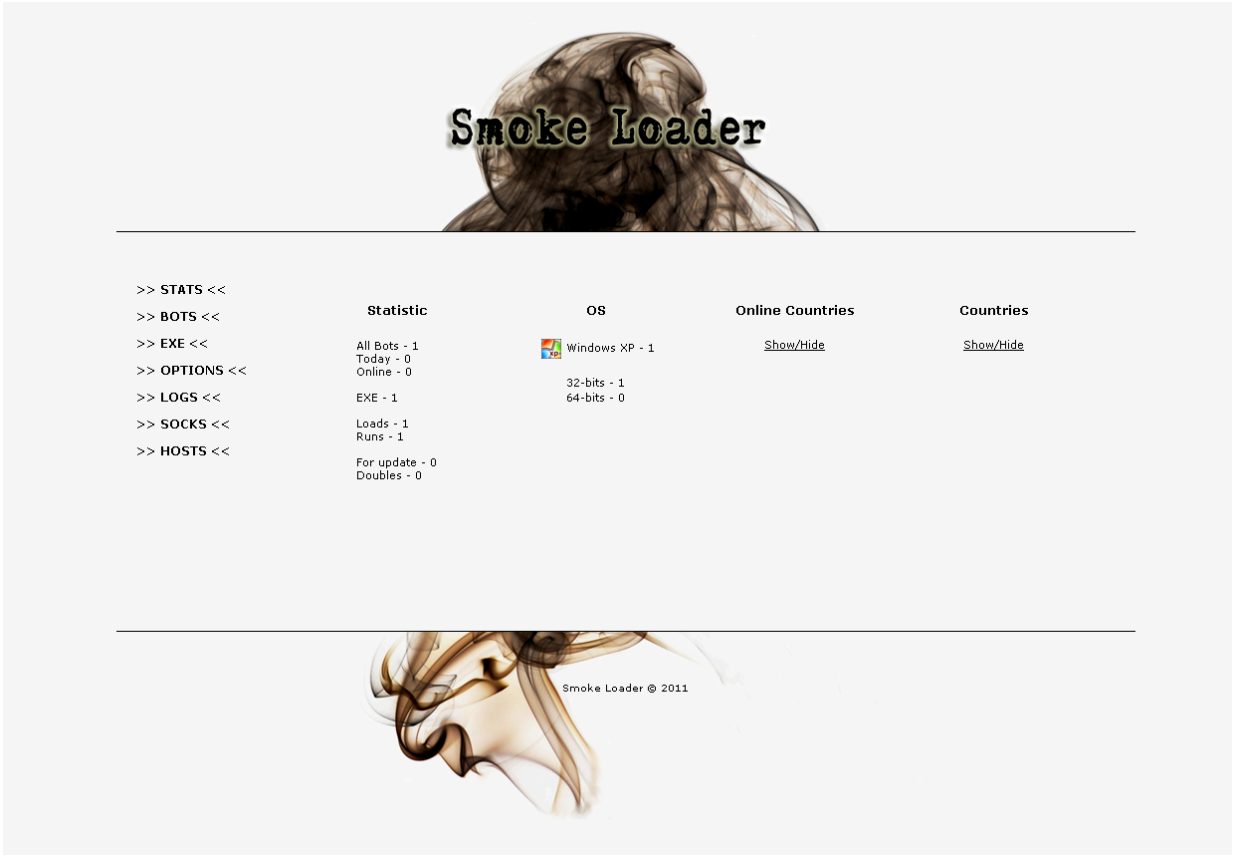
Continuing the “A peek inside…” series, in this post I will profile yet another malware loader. This time it’s the Smoke Malware Loader.

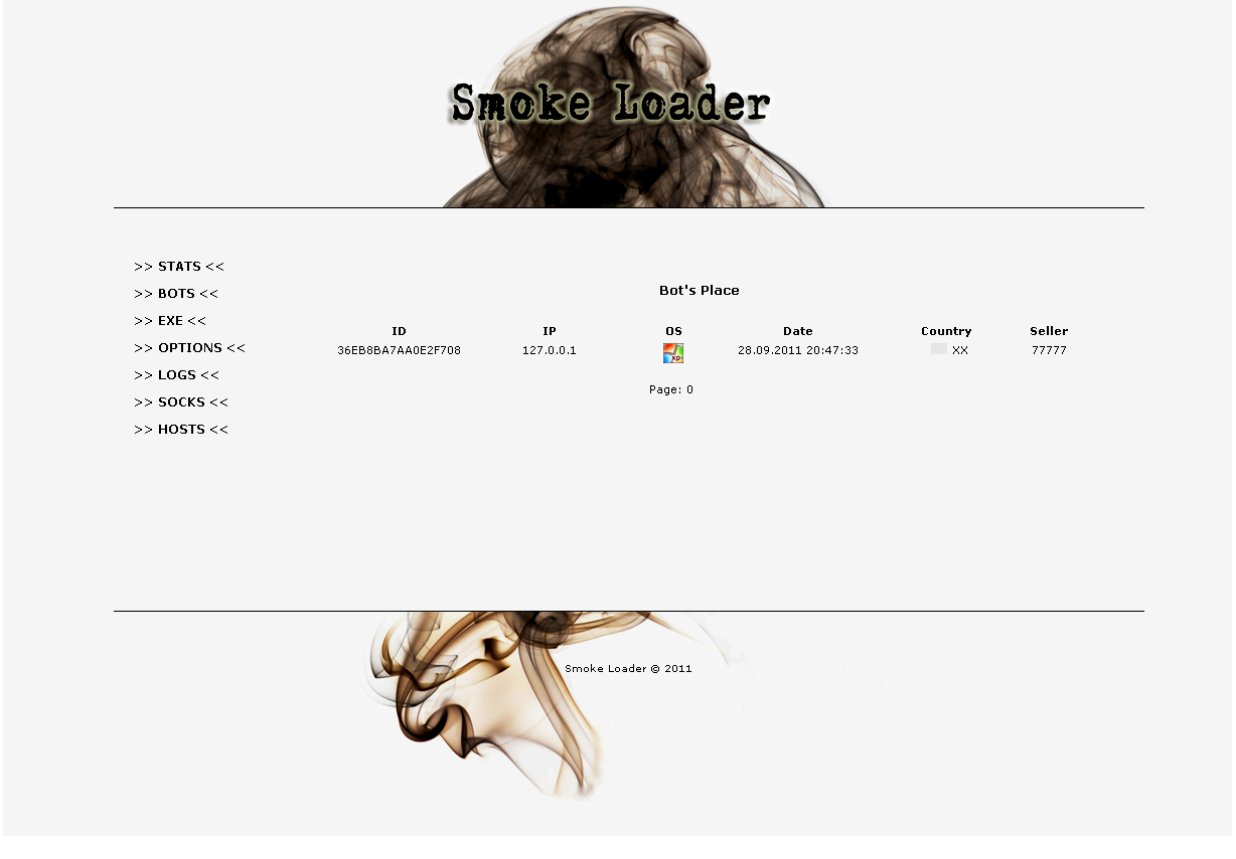
The Smoke Malware Loader is a modular malware loader, that comes with several different modules based on how much is the customer willing to spend.

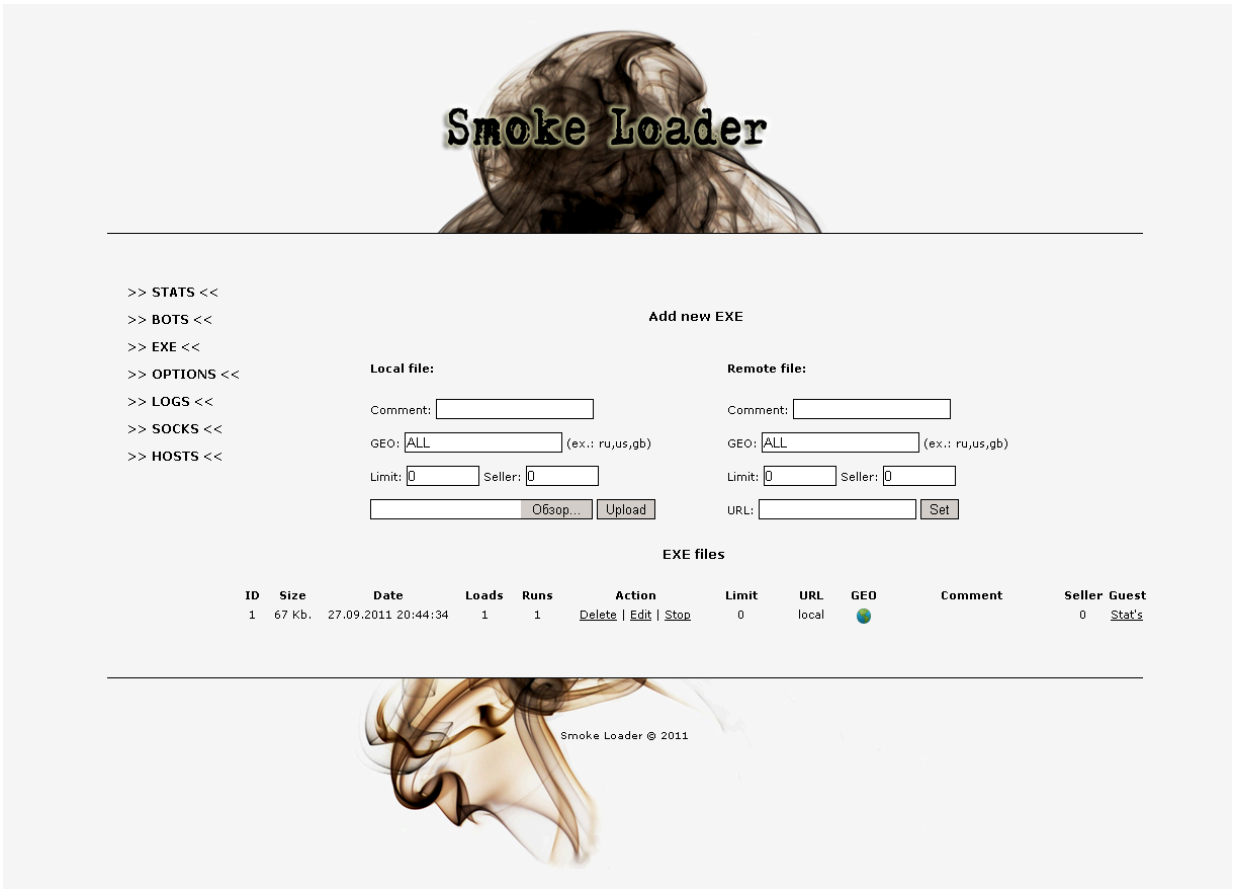
Some of its features include:

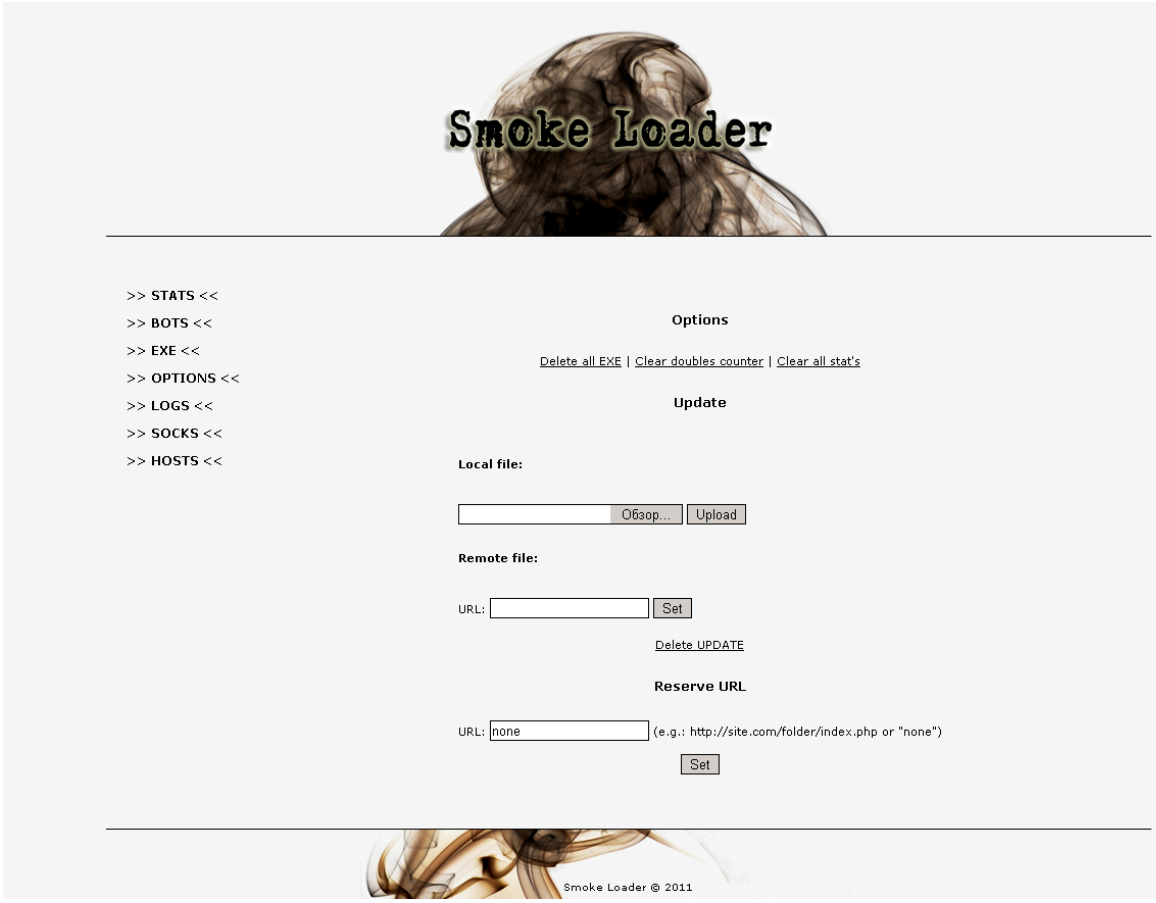
> – Progressive download different EXE and run *
>
> – Geo-targeting (download only for specific countries)
>
> – The ability to download files via a URL
>
> – Startup and invisible work (Masked by a trusted process) **
>
> – Detailed statistics on jobs- Self-renewal through the bot’s admin panel (locally or remotely) **
>
> – Protection against loss by blocking bots domain **
>
> – The small size of the loader ~ 12.6 kb ***
>
> – Ability to use Builder for “sellers” (more accurate statistics)
>
> – Statistics on re-launching (useful for assessing the quality of downloads, or traffic) **
>
> – “Guest” access to the statistics- Easy kriptovka (does not contain any additional dll, overlays, etc.)

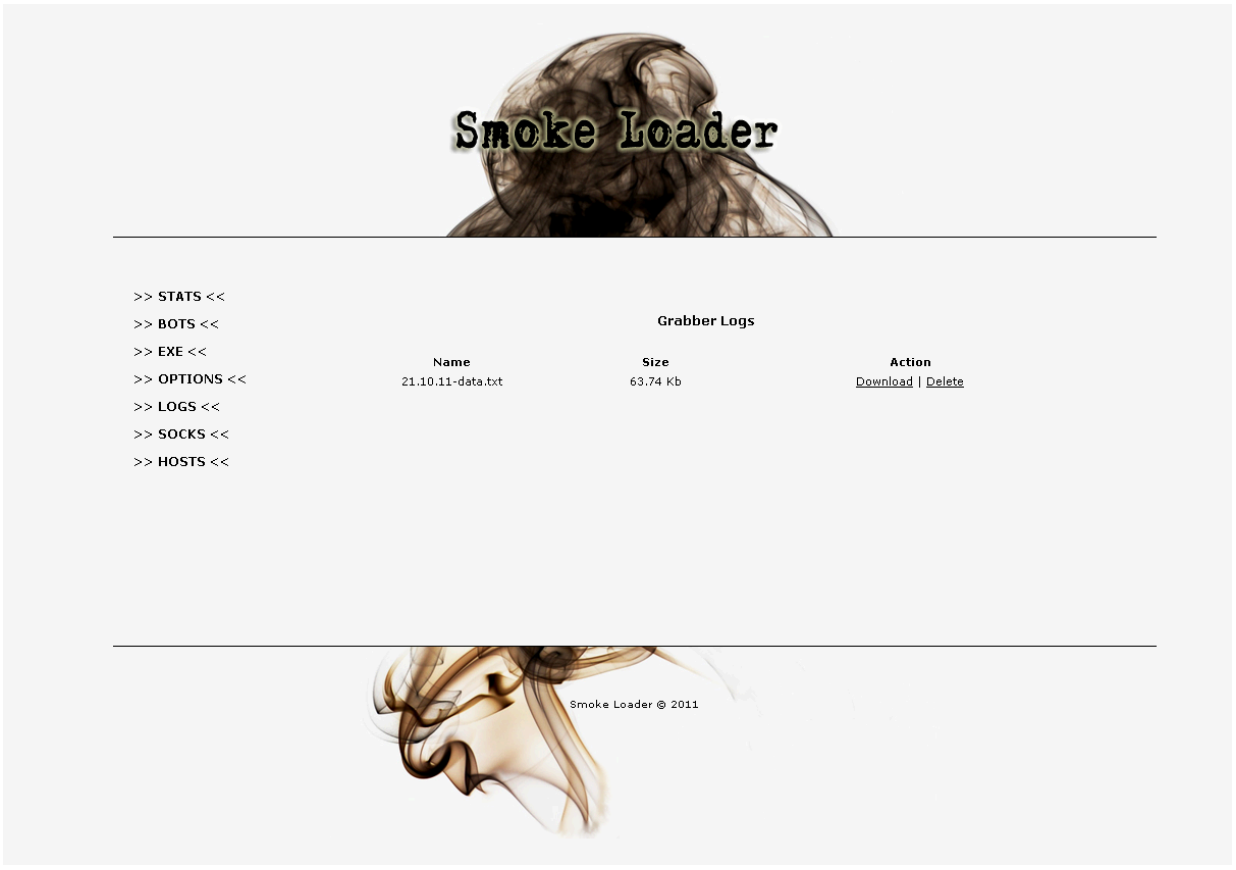
Screenshots of the command and control interface:

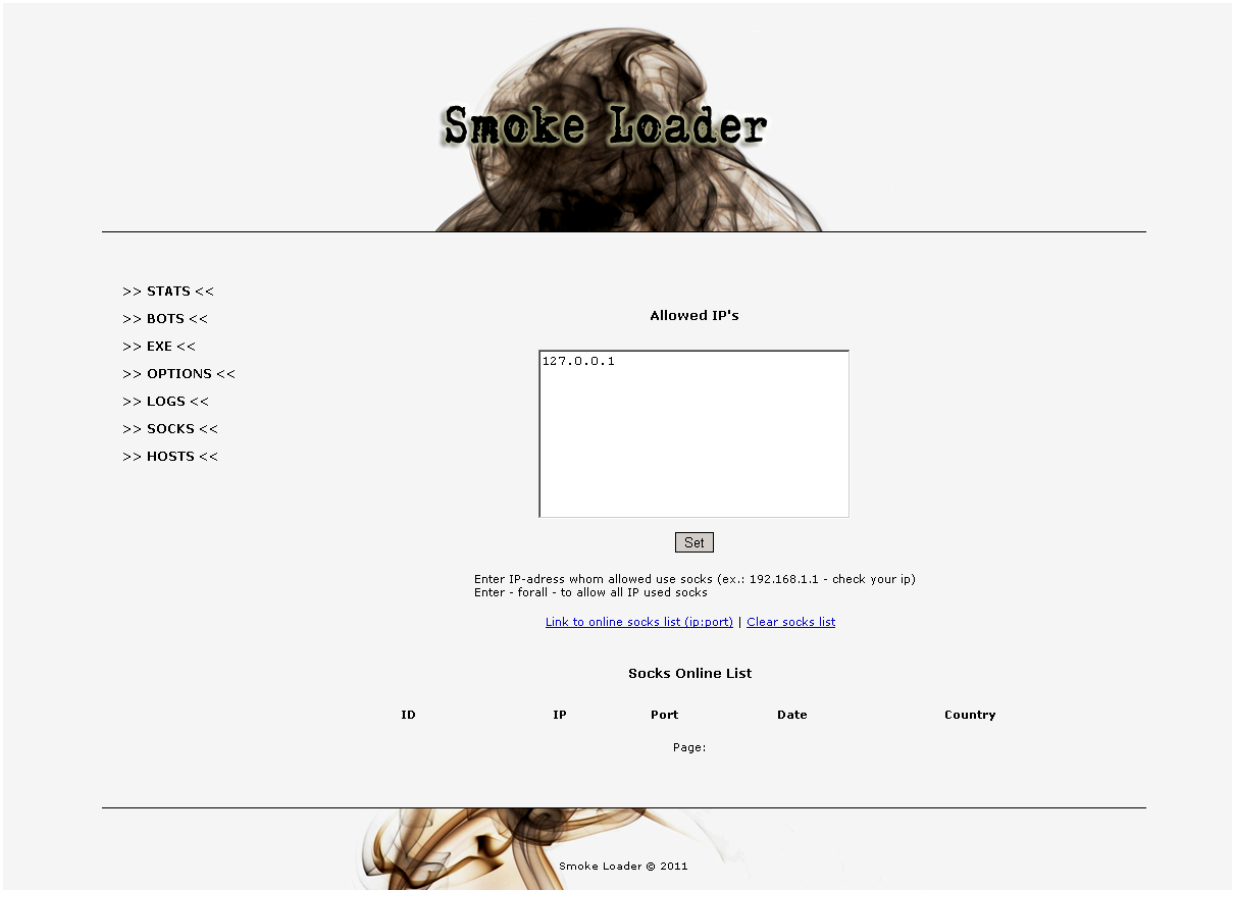

Smoke Loader
>> STATS <<
>> BOTS <<
>> EXE <<
>> OPTIONS <<
>> LOGS <<
>> SOCKS <<
>> HOSTS <<
Statistic
All Bots - 1
Today - 0
Online - 0
EXE - 1
Loads - 1
Runs - 1
For update - 0
Doubles - 0
OS
Windows XP - 1
32-bits - 1
64-bits - 0
Online Countries
Show/Hide
Countries
Show/Hide
Smoke Loader © 2011


Smoke Loader
>> STATS <<
>> BOTS <<
>> EXE <<
>> OPTIONS <<
>> LOGS <<
>> SOCKS <<
>> HOSTS <<
Bot's Place
ID
IP
OS
Date
Country
Seller
36EB8BA7AA0E2F708
127.0.0.1
28.09.2011 20:47:33
XX
77777
Page: 0
Smoke Loader © 2011


Smoke Loader
>> STATS <<
>> BOTS <<
>> EXE <<
>> OPTIONS <<
>> LOGS <<
>> SOCKS <<
>> HOSTS <<
Add new EXE
Local file:
Comment:
GEO: ALL (ex.: ru,us,gb)
Limit: 0 Seller: 0
Обзор... Upload
Remote file:
Comment:
GEO: ALL (ex.: ru,us,gb)
Limit: 0 Seller: 0
URL: Set
EXE files
ID Size Date Loads Runs Action Limit URL GEO Comment Seller Guest
1 67 Kb. 27.09.2011 20:44:34 1 1 Delete | Edit | Stop 0 local 0 Stat's
Smoke Loader © 2011


Smoke Loader
>> STATS <<
>> BOTS <<
>> EXE <<
>> OPTIONS <<
>> LOGS <<
>> SOCKS <<
>> HOSTS <<
Options
Delete all EXE | Clear doubles counter | Clear all stat's
Update
Local file:
Обзор... Upload
Remote file:
URL: Set
Delete UPDATE
Reserve URL
URL: none (e.g.: http://site.com/folder/index.php or "none")
Set
Smoke Loader © 2011


Smoke Loader
>> STATS <<
>> BOTS <<
>> EXE <<
>> OPTIONS <<
>> LOGS <<
>> SOCKS <<
>> HOSTS <<
Grabber Logs
Name
Size
Action
21.10.11-data.txt
63.74 Kb
Download | Delete
Smoke Loader © 2011


Smoke Loader
>> STATS <<
>> BOTS <<
>> EXE <<
>> OPTIONS <<
>> LOGS <<
>> SOCKS <<
>> HOSTS <<
Allowed IP's
127.0.0.1
Set
Enter IP-adress whom allowed use socks (ex.: 192.168.1.1 - check your ip)
Enter - forall - to allow all IP used socks
Link to online socks list (ip:port) | Clear socks list
Socks Online List
ID
IP
Port
Date
Country
Page:
Smoke Loader © 2011

The modular Smoke Malware loader comes with two additional modules. The first module steals passwords from popular applications, and sends them back to the malicious attackers. The second module is a **SOCKS-connection module**, turning malware-infected hosts into **stepping stones for anonymizing a cybercriminal's online activities**.

The first module successfully steals passwords from the following applications:

> 32bit FTP
> BitKinex
> BulletProof FTP Client
> Classic FTP
> CoffeeCup FTP
> Core FTP
> CuteFTP
> Directory Opus
> ExpanDrive
> FAR Manager FTP
> FFFTP
> FileZilla
> FlashFXP
> Fling
> FreeFTP/DirectFTP
> Frigate3 FTP
> FTP Commander
> FTP Control
> FTP Explorer
> FTP Navigator
> FTP Uploader
> FTPRush
> LeapFTP
> NetDrive
> SecureFX
> SmartFTP
> SoftX FTP Client
> TurboFTP
> UltraFXP
> WebDrive
> WebSitePublisher
> Windows/Total Commander
> WinSCP
> WS_FTP

And from the following browsers:

> Apple Safari
> Flock
> Google Chrome
> Internet Explorer
> Mozilla Browser
> Mozilla Firefox
> Mozilla Thunderbird
> Opera
> SeaMonkey

The full version of the passwords grabber also works on the following IM applications:

> &RQ
> AIM Pro
> Digsby
> Excite Private Messenger
> Faim
> GAIM
> Gizmo Project
> Google Talk
> ICQ/AIM
> ICQ2003/Lite
> ICQ99b-2002
> IM2 (Messenger 2)
> JAJC
> Miranda
> MSN Messenger
> MySpaceIM
> Odigo
> Paltalk
> Pandion
> Pidgin
> PSI
> QIP
> QIP.Online
> SIM
> Trillian
> Trillian Astra
> Windows Live Messenger
> Yahoo! Messenger

And how about the price? The price for the Smoke Malware Loader, including and excluding various modules is as follows:

> – Only the loader (the non-resident version) – 150 WMZ
> – Only the loader (TSR version) – 250 WMZ
> – Grabber LITE – 100 WMZ **
> – Grabber FULL – 150 WMZ **
> – SOCKS-module – 50 WMZ (version without bekkonekta) **
> – HOSTS-module – 25 WMZ **
> – Rebild loader – 10 WMZ
> – Update: minor fixes – for free, the rest is discussed separately
> – Can build to suit your needs grabber

The modular nature of the Smoke Malware Loader allows the seller of the bot to come up with flexible pricing plans, potentially lowering down the entry barriers into this market segment. The bot's password grabbing functionality is a great reminder of how you shouldn't save your passwords in the browser, as they become susceptible to extraction techniques like the ones used by the Smoke Malware Loader.

Use a third-party password managing tool, like **Webroot's Password Manager** for instance.

Related posts:

A peek inside the uBot malware bot

A peek inside the PickPocket Botnet

A peek inside the Cythosia v2 DDoS Bot

A peek inside the Umbra malware loader

*You can find more about Dancho Danchev at his **LinkedIn Profile**. You can also **follow him on Twitter**.*

About the Author

Blog Staff

The Webroot blog offers expert insights and analysis into the latest cybersecurity trends. Whether you're a home or business user, we're dedicated to giving you the awareness and knowledge needed to stay ahead of today's cyber threats.
