# THREAT: Pandora DDoS Toolkit

**GSI ID:** 1052

**Risk Factor - Medium**

**OVERVIEW**

- The Pandora DDoS Toolkit was allegedly developed by the same Russian individual, 'sokol,' who authored the Dirt Jumper toolkit.

- The tool was leaked to malware forums in February 2012 and is now available on various underground websites for US$800. Analysts have obtained a copy of the panel code and executable builder, and have included a download link in the Appendix.

An advertisement for the toolkit states that 10 bots controlled by this toolkit will take down weak sites; 30 bots will bring down medium-sized sites with little protection; 100 bots caused depositfiles.com to hang, and 1,000 bots slowed the most popular search engine in Russia, yandex.ru.

The tool generates five attack types, including both infrastructure and application layer attacks:

- HTTP min
- HTTP download
- HTTP Combo
- Socket Connect
- Max Flood

The author randomizes the HTTP headers information Referer and User-Agent to make pattern identification more difficult.

**ANALYSIS OF THE LEAK**

Like Dirt Jumper v3, Pandora is a pre-packaged toolkit that appears to be authored by the same individual, who goes by the alias 'sokol.' The Pandora DDoS Toolkit was selling on various underground forums for US$800 as of May 2012.

- Individuals within the underground malware community that leaked Pandora were initially skeptical of the authenticity of the leak, as no source code was included for the builder. The similarities to the command and control (C&C) panel, and the behavior of the payload, led many to believe it was a Dirt Jumper rip-off. However, after several weeks of open source analysis from the malware development community, it was determined to be a legitimate leak and a follow-up to the Dirt Jumper series by the malware author known as 'sokol.' Furthermore, the Russian language informational page on the C&C panel discloses that the project is from the same author as Dirt Jumper.

- Within the C&C panel code, there are many variables entitled $sokol. These same variables are also present in Dirt Jumper C&C panels.

- There are several Pastebin articles as well as several underground forum posts that advertise the Pandora DDoS Toolkit for US$800 by an allegedly different malicious actor. The vendor indicated he prefers payment in WebMoney (WMZ), a Russian e-currency. However, these Pastebin articles are dated March

2012 and are attributed to an individual going by the handle of SHYLLER; therefore this might be a third party individual attempting to make money from the public toolkit by reselling it and marketing it as a as private kit.

The following is an English language translation of the advertisement by SHYLLER:

```
Private DDoS bot PANDORA

    Hello, my name is SHYLLER!Today I want to offer you a unique new DDoS bot called "PANDORA"
    To test the bot 1 Bot puts zafan.ru
    10 bots put weak sites.
    30 bots put medium-sized sites with little protection.
    100 bots hang depositfiles.com (screenshot attached)
    1000 bots slowed down the work of the yandex.ru (The most popular search engine in russia, as you have
google xDD)for some time.

    Information
    1. Product description
    From the creator of Dirt Jumper and Simple!
    The key DDoS system 2012!
    New, universal ddos botnet PANDORA!
    This unique product combines the best moments from all the created earlier versions.
    Bot written with the participation of the clients of the previous version of the author.
    Yes arrive with Your Pandora!!!
    2. Operating instructions
    The bot has Five modes of attack.
    1. Requests on the TCP protocol, without receiving a response.
    A connection is broken so that the server continues to wait until the client receives a response.
    And at this time is already running another request.
    Thus not only that is 100% load on apache, database, channel, but there are many half-open connections,
which creates a queue on a server and additional burden on apache.
    To the methods of possible attack as on the specific script, and so on ports!
    2. Almost the same as the first method, but unlike him, this type of attack takes the answer, creating
another type of load.
    Namely: Employment connect, traffic, load apache in return information.
    3. This method of attack combines the first and the second.
    Bot in turn queries the first method, then the second.
    4. And this method is written solely on top of sockets. Bot performs connect to the server, and while he
did not refuse to accept the information, the bot will send the traffic.
    Port, you can specify any.
    5. The method that allows you to score a channel. Queries with a very large packages.
    The numbering of the attack starts FROM SCRATCH!
    The bot also there is a system timeout.
    In the field you need to specify the timeout in milliseconds. Timeout is performed in each thread
separately.
    In order to stop the attack to specify zero the number of threads.
    All methods of attacks support the ability to strike at the port. The fourth method of attack beats only
for IP. (if you specify a domain, he himself will determine the IP.)

    The price of the product 800$(it is desirable payment webmoney)

    Contact with me icq 6556666

    http://s1.ipicture.ru/uploads/20120219/21s6m8Nf.jpg
    http://s1.ipicture.ru/uploads/20120219/TbxIV6R6.jpg
```

**Figure 1: Translation interpreted by Google Translate**

Below is an advertisement of the toolkit being offered free on underground Russian forums.

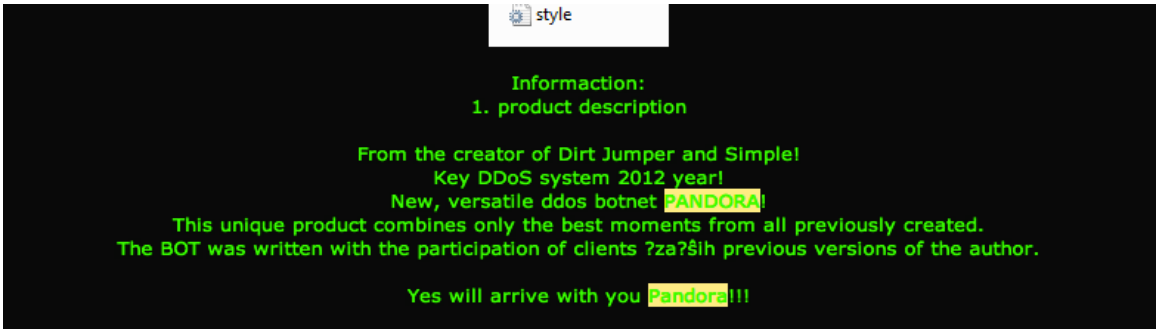


Figure 2: Advertisement for the Pandora toolkit on an underground Russian forum

There was a discussion on a Russian forum about the value of the Dirt Jumper source code, upon which the Pandora toolkit is built. One post states that the Dirt Jumper builder source code is probably worthless, to which forum member kingmonstr responded that is worth about US$5,000. Kingmonstr seemed to run the botnet and DDoS section of this particular forum, and appeared knowledgeable about the kits and the underground.


Figure 3: Comment on an underground Russian forum by an apparently knowledgeable forum moderator responding that the Dirt Jumper builder source code is worth US$5,000.

**ANALYSIS OF COMMAND AND CONTROL (C&C)**

The Pandora C&C panel operates similarly to the Dirt Jumper C&C panel. Both toolkits make use of fake 404 redirects, and will not load the login page unless the botmaster knows the username to place into the GET request. These fake 404s may identify specific variants, so it is possible to determine toolkit versions based on these responses.

- **Pandora Login Page**

  http://xxx.xxx.xxx.xxx/pandora/admin.php

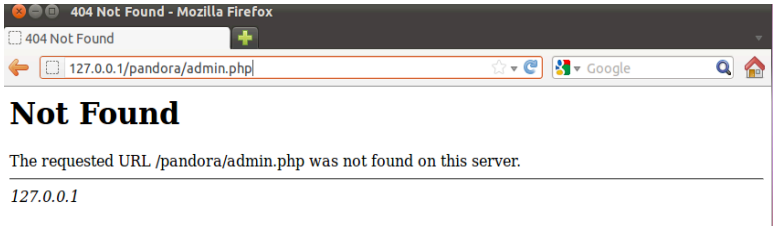


**Figure 4: Without the login in the GET request, the panel will return a 404 error.**

http://xxx.xxx.xxx.xxx/pandora/admin.php?login=admin


**Figure 5: The login parameter needs to be in the GET request with the correct username.**

- **Pandora Informational Page**


**Figure 6: The Pandora information page reveals that it is a follow-up to Dirt Jumper.**

- **Pandora Attack Page**


**Figure 7: The attacker enters targets in the gray box, and sets the threads and timeout.**

A difference between Pandora and Dirt Jumper is that there is no Stop button. Attackers must stop attacks by setting the threads to zero.

**PRODUCT DESCRIPTION**

The following is an English translation via Google Translate of the toolkit's own product description, including five attack types:

```
From the creator of Dirt Jumper and Simple!
Key DDoS system in 2012!
A new, universal ddos botnet Pandora!
This unique product combines only the best moments from all the previously
created versions.
The bot is written with the participation of clients yuzayuschih previous
version of the author.
```

Yes, Pandora will come to you!

Two. The instruction manual

Boat has five modes of attack.

One. "HTTP min" requests over TCP, without receiving an answer.
Connect is broken so that the server continues to wait until the client receives a response.
And at this time is already running another query.
So besides that is 100% load on apache, db, channel, and is set half-open connections, which creates a queue on the server and the additional load on apache.
This method can attack both on the specific script, and the ports!

Two. "HTTP download" Almost the same as the first method, but unlike him, this type of attack takes the answer, creating a different kind of load.
Namely: Employment konnekta, the traffic load on the Apache with the impact of information.

Three. "HTTP Combo" This method of attack combines the first and second.
Boat in turn performs a request by the first method, then the second.

4. "Socket Connect" But this method is written exclusively on the sockets. Boat performs connection to the server, and while he did not refuse to accept the information, the bot will send traffic.
You can specify any port.

Five. "Max Flood" method which allows the hammer channel. Executes queries with very large packages.

The numbering starts with zero attack!

At the bot has a system of time-outs.
In the box you need to specify the timeout in milliseconds. Time-out is performed in each stream separately.
In order to stop the attack you need to specify the number of zero flows.

All methods of attacks, support the ability to strike at the port. The fourth method of attack beats only by IP. (If you specify a domain, it will determine the IP.)

**Russian**

Информация
1. Описание продукта

От создателя Dirt Jumper и Simple!
Ключевая DDoS система 2012 года!
Новый, универсальный ddos ботнет ПАНДОРА!
Этот уникальный продукт сочетает в себе только самые лучшие моменты со всех созданных ранее версий.
Бот написан при участии клиентов юзающих предыдущие версии автора.

Да прибудет с Вами Пандора!!!

2. Инструкция эксплуатации

Бот имеет Пять режимов атаки.

1. "HTTP min" Запросы по протоколу TCP, без получения ответа.
Коннект разрывается таким образом, что сервер продолжает ждать пока клиент получит ответ.
А в это время уже выполняется ещё один запрос.
Таким образом мало того что идёт 100% нагрузка на апач, бд, канал, но и остаётся множество полуоткрытых соединений, что создаёт очередь на сервере и дополнительную нагрузку на апач.
Данным методом возможна атака как на конкретный скрипт, так и на порты!

2. "HTTP download" Практически тоже самое что и первый метод, но в отличии от него данный вид атаки принимает ответ, создавая другой вид нагрузки.
А именно: Занятость коннекта, трафик, нагрузка на апач при отдачи информации.

3. "HTTP Combo" Данный метод атаки совмещает в себе первый и второй.
Бот по очереди выполняет запросы то первым методом, то вторым.

4. "Socket Connect" А этот метод написан исключительно на сокетах. Бот выполняет коннект к серверу, и пока тот не откажется принимать информацию, бот будет отправлять трафик.
Порт можно указывать любой.

5. "Max Flood" Метод который позволяет забить канал. Выполняет запросы с очень большими пакетами.

Нумерация атак начинается С НУЛЯ!

У бота имеется система таймаутов.
В соответствующем поле нужно указать время таймаута в миллисекундах. Таймаут выполняется в каждом потоке отдельно.

Для того, чтобы остановить атаку нужно указать нулевое количество потоков.

Все методы атак поддерживают возможность удара по порту. Четвёртый метод атаки бьёт только по IP. (если вы указываете домен, он сам определит IP.)

**TYPES OF ATTACKS**

In this section, PLXsert will analyze the communication and five types of attacks that can be launched by the Pandora Bot Toolkit. The attack types will help identify behavior patterns unique to this script. Furthermore, they will assist in validating the proper DDoS detection and mitigation strategies.

**Communication between bot workstation and C&C**

The infected workstations beacon to the C&C panel with a broken GET request that sends a u parameter with hashed information that identifies the bot within the C&C MySQL database. Poor coding and a typographical error on the part of Pandora's author results in a GET request being sent as an ET request without specifying the HTTP version. Some web servers, such as Apache, will interpret the ET request as a GET request and respond with a valid 200 OK code. However, a web server such as nginx will return a 400 Bad Request error.

If successful, the C&C replies with an attack string that instructs the infected bot on the type of attack, duration of attack, connect-back intervals, timeouts, and the target.

- **Request**
  - ET /pandora/?u=fh38fj39gj39dj9fj9fj2ghggd2423f2
    Host: 192.168.206.140
    User-Agent: Mozilla/100

- **Response**
  - HTTP/1.1 200 OK
    Date: Fri, 28 May 2012 18:17:23 GMT
    Server: Apache/2.2.20 (Ubuntu)
    X-Powered-By: PHP/5.3.6-13ubuntu3.6
    Vary: Accept-Encoding
    Content-Length: 43
    Content-Type: text/html

    []0|2|25|60|1000|http://www.victim.com

**ATTACK SIGNATURE**

Each of the attack types has a unique signature.

- **Attack Type 0 - HTTP min**
  - GET / HTTP/1.0
    Host: www.victim.com
    Keep-Alive: 300
    Connection: keep-alive
    User-Agent: Mozilla/2.0 (compatible; MSIE 3.02; Update a; AK; Windows NT)
    Referer: yp7271xks8.net ←- randomized Referer

- **Attack Type 1 - HTTP Download**
  - GET / HTTP/1.0
    Host: www.victim.com
    Keep-Alive: 300
    Connection: keep-alive
    User-Agent: Mozilla/5.0 (compatible; BecomeBot/2.0beta; http://3vs768vm.comwebmasters.html)
    Referer: ae9d7.ru ←- randomized Referer

- **Attack Type 2 - HTTP Combo**
  - GET / HTTP/1.0
    Host: www.victim.com
    Keep-Alive: 300
    Connection: keep-alive
    User-Agent: Mozilla/4.7 (compatible; WhizBang;
    http://www.nzcx40h80i.com/crawler) ←- randomized User-Agent
    Referer: mm55hn11i.info ←- randomized Referer

- **Attack Type 3 - Socket Connect**
  - When Attack Type 3 is selected, the infected machines send improper ET requests (instead of proper GET requests) due to a typographical error within the payload itself. The Socket Connect attack will send large amounts of periods [.....], and makes use of HTTP 1.1 instead of HTTP 1.0. Servers such as nginx will not interpret the request properly due to the typographical error of an ET request instead of a GET request.

    - **Request**
      ET www.victim.com HTTP/1.1
      Host: www.victim.com
      User-Agent: Mozilla/100
      ……..[...]

    - **Response**
      400 Bad Request
      nginx/1.0.6

- **Attack Type 4 - Max Flood**
  - The Max Flood attack, known as Attack Type 4, uses a POST flood that has a content length of over 1 million bytes.

    POST / HTTP/1.0
    Host: www.victim.com
    Keep-Alive: 300
    Connection: keep-alive
    User-Agent: Mozilla/5.0 (compatible; heritrix/1.5.0-200506231921
    http://5z3kefh1dz5xy.nla.gov.au/crawl.html) ←randomized User-Agent
    Content-Type: application/x-www-form-urlencoded
    Content-Length: 1000002
    Referer: 43333w26.ru ←- randomized Referer
    z=0a6q9t54yy25pj23p5hbs4m1b9ek8fr1f00bk7lsl1d2z7sm3w9befdk240m4x8f20f944hj4s491r6iboby
    0m7suf2ygj7os79y9k5n8dge248v0af1so6u225x06u75d4f94b5ae0tt84f8tdhw706l0bvv07702cy75u1iu
    m7e67zgp8fm9675c9k804m4o4pa2b2og
    ←random payload equals 1000002 bytes→

**RECOMMENDED MITIGATION**

alert tcp $EXTERNAL_NET any -> any $HTTP_PORTS ( \
msg: "action=block, custid=*xx*, timeout=3600, comment='Pandora'"; sid: *xxxxxx*; \
content: "HTTP/1.0"; \
content: "GET /?=”; \
content: "Host\: *target domain*"; \
content: "Keep-Alive\: 300"; \
content: "User-Agent\: Mozilla"; \
content: !"Accept\:"; \
pcre: "/(\.com)|(\.ru)|(\.info)|(\.net)|(\biz)/"; )

alert tcp $EXTERNAL_NET any -> any $HTTP_PORTS ( \
msg: "action=block, custid=xx, timeout=3600, comment='Pandora'"; sid: xxxxxx; \
content: "ET HTTP/1."; \

```
content: !"GET";
content: "Host\: target domain"; \
content: "User-Agent\: Mozilla/100";)

alert tcp $EXTERNAL_NET any -> any $HTTP_PORTS ( \
msg: "action=block, custid=xx, timeout=3600, comment='Pandora'"; sid: xxxxxx; \
content: "POST /?=4 HTTP/1.0"; \
content: "Host\: target domain"; \
content: "Keep-Alive\: 300"; \
content: "Connection\: keep-alive"; \
content: "User-Agent\: Mozilla"; \
content: "Content-Type\: application/x-www-form-urlencoded"; \
content: "Content-Length\: 1000002"; \
pcre: "/(\.com)|(\.ru)|(\.info)|(\.net)|(\biz)/"; )
```

**ADDITIONAL NOTES**

Third Party Analysis - Russian malware blogger Onthar.in has put together a brief analysis of the Pandora toolkit as it relates to Dirt Jumper v5. His conclusion is that they are essentially the same product with slight modifications to the C&C, builder and payload. He concludes that the User-Agent list in the Pandora payload is identical to the Dirt Jumper v5 payload. He concludes it is low quality modification to an existing public toolkit. - http://onthar.in/articles/pandora-ddos-bot-analysis (Russian language)

**CONTRIBUTORS**
PLXsert

**APPENDIX**
External resources:

- Private DDoS bot PANDORA - http://pastebin.com/ka6XS2mC
- OpenSC.ws Leaked Pandora DDoS - http://www.opensc.ws/cracked-malware/18731-leaked-pandora-ddos-bot-very-strong.html
- Onthar.in Pandora vs. DJv5 Analysis (Russian Language) - http://onthar.in/articles/pandora-ddos-bot-analysis

**About PLXsert:**

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post-attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

**About Prolexic:**

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit **www.prolexic.com**, follow @Prolexic on **Twitter**, email **sales@prolexic.com**, or call **+1 (954) 620 6002**.