MediaGet — Lurkmore

> **Анонимус!**
> На эту тему есть смехуечки: Копипаста:MediaGet.

«Очень плохая программа.Никому не советую ее скачивать.Комп.тормозит ужасно.Теперь незнаю как удалить его.Не могу ее найти что бы удалить.Посоветуйте как ее удалить. »

— Отзыв с форумов

«Программа полная хуйня! Инет тупит по-чёрному, вирусов дохрена! Удаляется не с первого раза! Без этой прогры качается всё намного быстрее, не то, что по этому е***ому Гету »

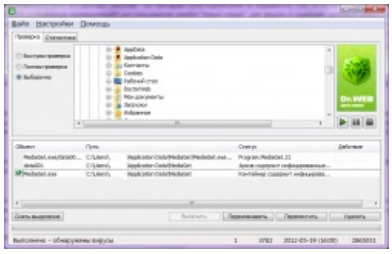
— Исчерпывающе

MediaGet — первый и единственный торрент клиент от российских разработчиков, по совместительству являющийся многофункциональным трояном, выполняющего одновременно функции как бота, так и бэкдора и загрузчика-дроппера. Регулярно обновляется и существует во множестве версий. Кроме того, это ещё способ заработка в интернете, с оплатой от 50 копеек за каждый распространённый по рефералу троян, благодаря чему софтварные сайты завалены установщиками троянов, а подфорумы захламлены хвалебными отзывами ботов и распространителей.

Взаимоисключающие параграфы

Основной функционал

В своей основе представляет собой сетевого бота, маскирующегося под P2P качалку и создающего типичный коммерческий ботнет. Даже ничего не качая, поднимает коннекты десятками тысяч и держит их в состоянии установленных соединений, причем координированных географически и направленных на какую-либо область — обычно на регионы США, Латинской Америки или Австралии, генерируя SYN-флуд, UDP-флуд, прочий флуд, и создавая мусорный трафик. Благодаря чему сервера, на которые направлен DDoS, и даже провайдеры могут отправить юзера в бан-лист по IP. Но, как правило, MediaGet просто забивает пакетами канал, и у проблематичного юзера начинает барахлить или тупо отрубается интернет.



Это он заблокировал инет!

> Устроился настройщиком в интернет провайдер, так только за два месяца у четырёх клиентов из за этой проги не работал интернет.
>
> Пошел к первому, настройки вроде ОК, с нашей стороны проблем нет, полез в запущенные процессы и автозагрузку, докапался я до этого MediaGet — это полная жопа!! Из-за него просто не работает интернет, я его деспетчером задач (завершит дерево процессов, иначе восстанавливается) и сразу всё работает, запускаю — нет пропадает (хотя подключение не обрывается), снёс её после некоторых затруднений, он ставит на свою директорию Local SettingsApplication DataMediaGe устанавливая неизменяемый(!) для пользователя атрибут «только чтение», для защиты от удаления — долбанул unloker’ом.
>
> Последующих клиентов та же херня, снес это дерьмо и всё сразу заработало. MediaGet в состоянии покоя, ничего не качая и не раздавая, открывает кучу новых соединений — до 17-25 тысяч(!!) и держит их в состоянии установленных соединений. Основной его функционал — троян типа сетевого бота. Он ещё различные шпионские модули загружает и в систему устанавливает, как опыт с песочницами антивирусов показывает.

— Проблемы эникейщика

А ещё MediaGet, благодаря своему функционалу DDoS-бота, довольно эффективно борется с работой домашних роутеров и прочих маршрутизаторов, которые просто не рассчитаны на ретрансляцию исходящего потока DDoS'a на пару десятков тысяч коннектов, и как следствие, зависают, ложатся или работают с серьёзными перебоями. Бывает, отрубаются даже достаточно дорогие роутеры, спокойно держащие работу µTorrent'a, DC++ и eMule, при проброс портов и канале 100 Мбит, с раздачей инета на несколько компов. Это заставляет юзера, который столкнулся с этой проблемой, менять роутер, покупать новый, более дорогой, или даже отказываться от его использования. Сходным образом может ломать работу этого вашего USB ADSL-модема.

Дополнительные возможности

«как удалить ето гавно??? »

— *Ламер*

Поскольку MediaGet помимо основного функционала DDoS-бота является ещё и троянским загрузчиком, загружающим и устанавливающем свои модули в систему, то с системой юзеров MediaGet'а через определённое время может происходить следующее.

Реклама

Установка рекламных модулей, проплаченных рекламодателем для установки на указанное число машин. И в том случае, если комп юзера оказывается в числе этих машин, в браузере появляется куча левой рекламы вроде увеличения груди, проверьте свой интеллект, вы выиграли миллион, ваш индивидуальный гороскоп за SMS, всевозможным онлайн-игровым трешаком и прочим разводом-заманухой. В случае установки рекламного модуля другого типа происходит тихая и незаметная подмена результатов поиска или ссылок. Благодаря чему многие антивирусы определяют его качестве adware или Adware.downloader'a.

Spyware

Установка шпионских модулей, отслеживающих действия пользователя, — загружаются и устанавливаются почти всегда. Кроме того, иногда присутствуют программы, ворующие пароли, преимущественно от социальных сетей, в результате чего со вскрытых аккаунтов начинает валить спам.

«Работа» с другими торрент-клиентами

С вероятностью 95% ломает работу других торрент-клиентов, внося изменения в систему, благодаря чему, они не работают или работают с черепашьей скоростью, после чего нубьё утверждает, что MediaGet быстрее качает. Изменения в системе остаются и после удаления зловреда.

И ещё немного

Ну и если юзеру совсем «везёт», то устанавливаются модули распределённых вычислений (BtcMine), благодаря чему, у юзеров начинает тормозить комп. Вообще, как правило, вычислительные модули должны мягко нагружать процессор, дабы догадливый юзер не снёс прогу, но из-за своей быдлокодерской кривизны нередко грузят одно из ядер процессора на 100%. Загрузка процессора в этом случае обычно колеблется от 15 до 50% при простое, как правило, появляются левые процессы в диспетчере задач.

Стоит отметить, что все вышеперечисленные подгружаемые модули в каждом отдельном случае могут быть разные, следовательно, симптомы заражения могут быть совершенно разные. У одного может быть УМВР, у другого — 100% загрузка одного из ядер, у третьего — левая реклама поверх страниц браузера, у четвёртого — незаметная подмена результатов поиска, а у пятого накрылся доступ в инет. Хотя, конечно, универсальный ответ — все работает, и сетование на кривизну рук и недоразвитость мозгов — практически всегда беспроигрышный вариант, особенно в троллинге. А для сомневающихся ещё существует проверка на VirusTotal и virusscan.

Значение для представителей скорой компьютерной помощи

Основная статья: ***Скорая компьютерная помощь***

Для этой категории лиц данная прога превратилась в источник профита, связанного с необходимостью восстановления доступа в инет, что встречается уже чаще необходимости снятия баннеров Winlock'а и прочей вирусной поебени.

> Действительно, программа отличная. Функцианала много, интуитивно понятный интерфей + красивое оформление. Пользуюсь ей довольно долго и в целом очень успешно. Работаю в довольно известной ремонтной мастерской и клиенты часто обращаются с просьбой установить одну единственную программу которая может качать практически с любых сервисов, будь это обычный ftp или torrent, и MediaGet как нельзя лучше подходит для этих целей!
>
> Ко всему прочему, особое достоинство программы в том, что она может "повесить" сеть и интернет, и клиенту приходится наз вызывать сново и сново. Благодаря этой программе у сотрудников нашей организации скоро будут виллы на Кнарах. А фраза"...Это подтверждается тем, что мы постоянно сотрудничаем с ведущими производителями антивирусов, чтобы их продукты не определяли нашу программу как вирус..." достойна особого внимания и почестей. Это гениальная идея договориться с разработчиками антивирусов о том. что бы данная программа была исключением. Огромное спасибо разработчикам! Ждем новых версий

> программы с новыми "фишками"!

— *Представитель ООО «Вектор»*

Это не отменяет радости некоторых работников провайдера (как и было показано выше) в случае наличия договорённости по обслуживанию абонентов на месте.

ПОДСМОТРЕНО В MEDIAGET

В 2016 году дырявость MediaGet была замечена аноном по кличке ОП. Каким-то образом он смог встроить в самые популярные у быдла торренты т. н. «ратник» (он же njRAT) и получить полный контроль над их пекарнями. Но вместо банального майнинга или кражи фоток он начал проводить прямые трансляции издевательств над компами (чего стоит только курсор в форме МПХ или ВНЕЗАПНО вылезающий на весь экран Meatspin). А учитывая наличие у большинства жертв веб-камер и их бурной реакции на происходящее, зрелище снискало неплохую популярность (более 30 000 подписчиков в закрытой группе ВКудахте). Стримы не проводились с конца 2017 года, но **архив** доступен на ютубчике. Спасибо, Олег Анатолич!

Как удалить это говно?

> Мляяяяяяяя сука как её удалить люди нигде в инете инфы нет!!!!!!!!!!!!!!!!!!!
>
> при том что закачалась без спроса...суки
>
> ааааааааа удалить то теперь как

— *Несдержанная реакция*

Многие антивирусы его начали удалять, но если ваш антивирь не детектит, можно воспользоваться традиционным методом:

1. Открываем диспетчер программ (он же appwiz.cpl)
2. Удаляем MediaGet
3. Чистим реестр и остатки какой-нибудь прогой. Можно и самому до реестра добраться. Если вместе с MediaGet была установлена херня от Mail.ru или Тындекса — тоже удаляем. Долбаните MediaGet2 unlocker-ом, если он ставит неизменяемый тег «только для чтения».
4. Чистим вирусы антивирем (если детектятся, если нет, чистим ручками)
5. ???
6. PROFIT!

См. также

- Wishmaster
- Гешефт
- Звонилка
- Крякер инета

Software

12309 1C 3DS MAX 8-bit Ache666 Alt+F4 Android BonziBuddy BrainFuck BSOD C++ Chaos Constructions Cookies Copyright Ctrl+Alt+Del Denuvo DOS DRM Embrace, extend and extinguish FL Studio Flash FreeBSD GIMP GNU Emacs Google Google Earth I2P Internet Explorer Java Lolifox LovinGOD Low Orbit Ion Cannon Me MediaGet MenuetOS Microsoft Miranda Movie Maker MS Paint Open source Opera PowerPoint PunkBuster QIP Quit ReactOS Rm -rf SAP SecuROM Sheep.exe Skype StarForce Steam T9 Tor Vi Windows Windows 7 Windows Phone 7 Windows Phone 8 Windows Vista Wine Winlogon.exe Wishmaster Word ^H ^W Автоответчик Антивирус Ассемблер Баг Билл Гейтс и Стив Джобс Блокнот Бот Ботнет Браузер Варез Винлок Вирусная сцена Генерал Фейлор Глюк Гуй Даунгрейд Демосцена Джоэл Спольски Донат Защита от дурака Звонилка Интернеты Кевин Митник Китайские пингвины Костыль Красноглазики Леннарт Поттеринг Линуксоид Линус Торвальдс Лог Ман Машинный перевод Мегапиксель

Интернет

Интернеты 127.0.0.1 ADSL Bitcoin CMS DDoS Frequently asked questions GPON I2P Internet White Knight IPv6 IRC MediaGet Miranda NO CARRIER QIP Ru@razlogoff.org SEO Skype Tor TOS Via WAP Ёбаное BT Админ Акадо Американские интернеты Анонимус Аська Бан Бесплатный хостинг картинок Блог Блогосфера Бот Ботнет Браузерка Бугагашечки Бурление говн Вап-чаты Веб 1.0 Веб 2.0 Вики Виртуал Вордфильтр Голосование ногами Гостевуха Диалап Дом.ру Домашняя страница Дорвей Единый реестр запрещённых сайтов Жаббер Заповеди интернета Заработок в интернете Идентификация пользователей в интернете Известные интернет-флешмобы Имиджборд Инвайт Интернет-магазин Интернет-сервисы Искра Кик Кириллические домены Кликбейт Коммент Комьюнити Лесенка Лог Локалка Макхост Мем Микроблог Мобильный интернет Модератор Некропост Ник Оптимизатор Ответы Офлайн Оффтопик Письма счастья Подкаст Поисковая бомба Покровитель интернетов Пост Правила интернетов Предыдущий оратор Премодерация Пруфлинк Рерайтинг Ростелеком Сабж Сетевые онанисты Симпафка Синдром вахтёра Ситилайн Скайнет Скриншот Смайл Социальная сеть