5 октября 2017 г.

Роман Астраханцев

МИЭМ НИУ ВШЭ

СКБ 171

Wannacry

Оглавление

[I. С ЧЕГО ВСЁ НАЧИНАЛОСЬ 2](#_Toc495530095)

[II. ПРИНЦИП РАБОТЫ 5](#_Toc495530096)

[III. КТО ПОБЕДИЛ? 7](#_Toc495530097)

[IV. КТО ВИНОВАТ? 8](#_Toc495530098)

[V. КАК ЗАЩИТИТЬСЯ И БЫТЬ ГОТОВЫМ 9](#_Toc495530099)

[ПРИЛОЖЕНИЯ 10](#_Toc495530100)

# I. С ЧЕГО ВСЁ НАЧИНАЛОСЬ

Программы блокирующие или затрудняющие работу с операционной системой появились более десяти лет назад, и за прошедшие годы они не претерпели никаких революционных изменений. Шифровальщики и локеры всех мастей всегда стремились к одному — сделать нормальную работу с ОС невозможной (шифруя файлы пользователя, блокируя экран смартфона, не позволяя загрузить операционную систему и так далее), а за разблокировку зараженного компьютера или мобильного устройства всегда требовали выкуп.

## **Сводка крупнейших мировых вирусных атак за период 1988-2017 год:**

### **Таблица 1. Крупнейшие компьютерные вирусные атаки в мире.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Год | Название вируса | Сценарий распространения вируса | Масштаб поражения | Ущерб |
| 1998 | Червь Морриса | Через ошибки в системе безопасности операционной системы | 6 000 ПК | 96,5 млн. долл. |
| 1998 | CIH | Электронные письма, сменные носители, сеть Интернет | 500 000 ПК | 1 млрд. долл. |
| 2000 | ILOVEYOU | Электронное письмо с темой «ILOVEYOU» | 3 млн. ПК | 10-15 млрд. долл. |
| 2001 | Code Red | Замена содержимого страниц на поражённом сайте | 400 000 ПК | 2,6 млрд. долл. |
| 2003 | Sobig F | По электронной почте письмом с вложением | 2 млн. ПК | 5-10 млрд. долл. |
| 2004 | Mydoom | Электронное письмо с темой «Привет», «Тест», «Ошибка», «Система доставки почты», «Уведомление о доставке» и др. | 500 000 ПК | 2,6 млрд. долл. |
| 2007 | Storm Worm | Электронное письмо | 10 млн. ПК |  |

От тюрьмы, от сумы и от хакерского взлома не застрахован никто. Квантовая сеть долгое время считалась безоговорочно безопасной. Но шведские физики даже в ней обнаружили уязвимости. Хакеры-любители тренируются на социальных сетях, других персональных сервисах, банковских картах. Профессионалы бросают вызов информационным системам государственных служб и правительств и персональным устройствам в глобальном масштабе.

В мае 2017 года все масштабы компьютерных вирусов-предшественников затмила вирус шифровальщик WannaCry.

[](https://xakep.ru/wp-content/uploads/2017/05/127037/Wana_decrypt0r_2.0.png)

**Рис. 1. *WannaCry версия 2.0***

WannaCry, также известный под названиями Wana Decrypt0r, WCry, WannaCrypt0r и WannaCrypt, был обнаружен отнюдь не в середине мая 2017 года, когда начались атаки, взбудоражившие весь мир. Впервые вирус был замечен специалистами еще в феврале 2017 года, но не произвел на них большого впечатления, по сути, являясь совершенно заурядным вымогателем, каких в настоящее время насчитываются десятки, если не сотни.

Почему началась эпидемия, если WannaCry – это рядовой вымогатель? Дело в том, что в середине мая 2017 года разработчики WannaCry выпустили вторую версию вредоноса, после чего тот стал распространяться со скоростью лесного пожара и посеял в сети настоящую панику.

Такой эффективности авторам WannaCry удалось добиться благодаря тому, что они в буквальном смысле взяли на вооружение эксплоиты из арсенала спецслужб.

Еще летом 2016 года группа хакеров, называющих себя The Shadow Brokers, сумела похитить хакерский инструментарий у специалистов АНБ. Долгое время хакеры тщетно пытались продать попавшее в их руки «кибероружие», но им не удалось провести аукцион или найти прямого покупателя, после чего, в апреле 2017 года, группировка опубликовала украденные данные совершенно бесплатно, в открытом доступе.

Именно готовыми инструментами из арсенала АНБ (а точнее эксплоитами ETERNALBLUE и DOUBLEPULSAR) и воспользовались создатели WannaCry, превратив заурядного с технической точки зрения шифровальщика в SMB-червя, от которого на данный момент пострадали уже более 400 000 устройств и сотни организаций по всему миру.

**Диаграмма 1-2. Отношение пострадавших машин на базе Windows.**

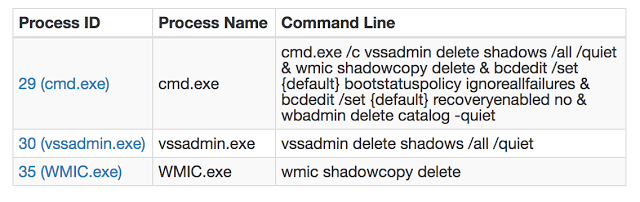
# II. ПРИНЦИП РАБОТЫ

Изначальный файл mssecsvc.exe запускает другой файл с названием tasksche.exe. Затем проверяется домен-выключатель, после чего создается служба mssecsvc2.0. Эта служба исполняет файл mssecsvc.exe с иной точкой входа, нежели во время первого запуска. Второй запуск получает IP-адрес зараженной машины и пытается подключиться к 445 TCP порту каждого IP-адреса внутри подсети. Когда зловред успешно подключается к удаленной машине, то устанавливается соединение и происходит передача данных. Судя по всему, где-то в процессе этой передачи используется известная уязвимость, которая была закрыта обновлением MS 17-010. На данный момент нету полного понимания трафика SMB, и при каких именно условиях зловред может распространяться, используя дыру в безопасности.

Файл tasksche.exe проверяет все диски, а также расшаренные по сети папки и подсоединенные устройства, которые привязаны к буквам, вроде 'C:/', 'D:/' и т.д. Малварь затем ищет файлы с расширениями, которые перечислены в программе (и приведены ниже), и шифрует их, используя 2048-битное RSA шифрование. Пока файлы шифруются, создается папка 'Tor/', куда кладется файл tor.exe и 9 файлов dll, которые он использует. Дополнительно создаются taskdl.exe и taskse.exe. Первый из них удаляет временные файлы, а второй запускает @wanadecryptor@.exe, который показывает пользователю окно с требованием заплатить. Файл @wanadecryptor@.exe отвечает только за вывод сообщения. Шифрование файлов происходит в фоне с помощью tasksche.exe.

Файл tor.exe запускается с помощью @wanadecryptor@.exe. Этот новый процесс начинает соединение с узлами Tor. Таким образом WannaCry сохраняет анонимность, проводя весь свой трафик через сеть Tor.

Что типично для программ-вымогателей, программа также удаляет любые теневые копии на компьютере жертвы, чтобы сделать восстановление еще более сложным. Делается это с помощью WMIC.exe, vssadmin.exe и cmd.exe



**Рис 2. Примеры использования вирусом различных способов помощи себе.**

WannaCry использует различные способы, чтобы помочь своему выполнению. Так оно используется attrib.exe, чтобы менять флаг +h (скрытие), а также icacls.exe, чтобы дать полные права всем юзерам: «icacls. /grant Everyone:F /T /C /Q».

Примечательно, что программа имеет модульную архитектуру. Вероятно, что все исполняемые файлы в ней написаны разными людьми. Потенциально, это может значить, что структура программы может позволять запускать различные зловредные сценарии.

После завершения шифрования, вредоносная программа показывает окно с требованием выкупа за файлы. Интересный момент заключается в том, что окно является исполняемым файлом, а не картинкой, файлом HTA или текстовым файлом.

Жертвам следует понимать, что не существует обязательства преступников действительно предоставить ключи для расшифровки после оплаты выкупа.

# III. КТО ПОБЕДИЛ?

Вирус-вымогатель WannaCry, с помощью которого 12 мая неизвестные киберпреступники атаковали компьютерные сети ведомств и компаний в семи десятках стран мира, удалось остановить.



**Рис. 3. Маркус Хатчинс, тот, кто спас мир.**

Вирус WannaCry был на время остановлен благодаря регистрации доменного имени iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, пишет The Guardian.

По данным газеты, программист Маркус Хатчинс вместе с коллегой Дарианом Хассом проследили, что вирус обращается по такому адресу. Они решил зарегистрировать домен, чтобы проследить его активность. Оказалось, адрес был зашит в коде вируса на тот случай, если его нужно будет затормозить. Так и вышло.

Сам Маркус Хатчинс признался, что понятия не имел, к каким последствиям приведет регистрация домена. Свое открытие он прокомментировал скромно: "Теперь я могу добавить в свое резюме строчку: "Случайно остановил международную кибератаку".

# IV. КТО ВИНОВАТ?

С одной стороны, косвенно «поблагодарить» за «вымогательский апокалипсис», развернувшийся по всему миру, можно хакерскую группировку The Shadow Brokers. Ведь именно The Shadow Brokers сделала достоянием общественности опасные киберинструменты АНБ.

Однако с тем же успехом обвинить в случившемся можно и сами спецслужбы, которые создали эксплоиты ETERNALBLUE и DOUBLEPULSAR, и долгое время умалчивали о критической уязвимости в SMB. Именно так уже поступил главный юрисконсульт компании Microsoft Брэд Смит (Brad Smith).

Также можно возложить ответственность на компанию Microsoft, которая исправила уязвимости еще в марте 2017 года, подготовила патчи для устаревших, неподдерживаемых ОС в феврале 2017 года, но предпочла не привлекать к проблеме внимания, а также «придерживала» патчи для Windows XP, Windows 8 и Windows Server 2003 до тех пор, пока катастрофа не разразилась в полной мере.

И конечно не стоит забывать о самих создателях WannaCry. До сих пор доподлинно неизвестно, на ком именно лежит ответственность за происшедшее. Как утверждают специалисты компании Symantec и «Лаборатории Касперского», с большой долей вероятности шифровальщика разработали северокорейские хакеры из небезызвестной группировки Lazarus, за которой эксперты наблюдают уже много лет. Специалисты компании Flashpoint, в свою очередь, провели лингвистический анализ WannaCry и обнаружили «китайский след».

Тем не менее, как уже было сказано выше, настоящий корень проблемы – это халатность и повсеместное невнимание к вопросам информационной безопасности. Патч, защищающий от WannaCry стал доступен еще в марте 2017 года, за два месяца до начала атак. А первые предупреждения об уязвимостях в протоколе SMB появились еще раньше. По сути, все пострадавшие от атак WannaCry поплатились за свою беспечность, так как за два месяца они не сумели найти времени на установку критических обновлений, о выходе которых было широко известно.

# V. КАК ЗАЩИТИТЬСЯ И БЫТЬ ГОТОВЫМ

Если говорить о защите от WannaCry, всем, кто по какой-то причине еще не установил обновление MS17-010, настоятельно рекомендуется сделать это немедленно. Также, учитывая серьезность ситуации, компания Microsoft выпустила экстренные патчи для давно неподдерживаемых ОС: Windows XP, Windows 8 и Windows Server 2003, поэтому пользователям этих систем так же следует озаботиться обновлением.

У тех, кто уже пострадал от деятельности вымогателя, есть шанс восстановить свои файлы, не выплачивая выкуп злоумышленникам. Хотя полноценного дешифровщика для WannaCry все еще нет, эксперты создали несколько инструментов, которые работают с Windows XP и x86-версиями Windows 7, 2003, Vista, Server 2008 и 2008 R2. При соблюдении рядя условий, эти утилиты помогут расшифровать пострадавшую информацию.

Однако нужно понимать, что проблема уже не ограничивается одним только WannaCry. Шифровальщик практически сразу породил множество подражателей, а уязвимость в SMB и инструменты спецслужб уже активно примеряют другие хакеры. Сейчас специалисты сходятся во мнении, что в будущем подобных атак будет становиться только больше, и если WannaCry был достаточно примитивной угрозой, то в дальнейшем атаки станут более комплексными и изощренными.

# ПРИЛОЖЕНИЯ

**Таблица 2. ИНДИКАТОРЫ КОМПРОМЕТАЦИИ от McAfee, Cisco Talos иPayload Security.**

| **IP** | **Port** | **Proto** | **Source** | **Geo** | **ASN** | **Organization** | **Tor type** | **VT Status** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 104.131.84.119 | 443 |  | McAfee | US | 393406 | Digital Ocean | Exit Node | [Clean](https://virustotal.com/cs/url/649ada66fcae90155e99c670fc9c4ad7be70d1c5d1be00549a2df7fefc93b8d4/analysis/1494663124/) |
| 128.31.0.39 | 9101 | TCP | Payoad Security | US | 3 | MIT | Exit Node | [Malicious](https://virustotal.com/cs/url/3b0218b040e7159af07de716aaa53305155af25b8531052dbe6c3332241e3b92/analysis/) |
| 128.31.0.39 |  |  | Cisco Talos |  |  |  | Yes | [Malicious](https://virustotal.com/cs/url/3b0218b040e7159af07de716aaa53305155af25b8531052dbe6c3332241e3b92/analysis/) |
| 136.243.176.148 | 443 | TCP | Payoad Security | DE | 24940 | Hetzner Online AG | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/136.243.176.148/information/) |
| 146.0.32.144 | 9001 |  | Cisco Talos | DE | 24961 | myLoc managed IT AG | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/146.0.32.144/information/) |
| 163.172.153.12 | 9001 | TCP | Payoad Security | GB |  | ONLINE SAS | Yes | [Malicious](https://www.virustotal.com/en/ip-address/163.172.153.12/information/) |
| 163.172.185.132 | 443 | TCP | Payoad Security | GB |  | ONLINE SAS | Yes | [Malicious](https://www.virustotal.com/en/ip-address/163.172.185.132/information/) |
| 163.172.25.118 | 22 |  | McAfee | GB |  |  | Yes | [Malicious](https://www.virustotal.com/en/ip-address/163.172.25.118/information/) |
| 163.172.35.247 | 443 | TCP | Payoad Security | FR |  | ONLINE SAS | Exit, Guard | [Maybe clean](https://www.virustotal.com/en/ip-address/163.172.35.247/information/) |
| 171.25.193.9 | 80 | TCP | Payoad Security | SE | 198093 | Foreningen for digitala fri- och rattigheter | Exit node | [Malicious](https://www.virustotal.com/en/ip-address/171.25.193.9/information/) |
| 178.254.44.135 | 9001 |  | McAfee | DE | 42730 | EVANZO e-commerceGmbH | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/178.254.44.135/information/) |
| 178.62.173.203 | 9001 | TCP | Payoad Security | NL | 200130 | Digital Ocean | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/178.62.173.203/information/) |
| 185.97.32.18 | 9001 | TCP | Payoad Security | SE | 44581 | AllTele Allmanna Svenska Telefonaktiebolaget | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/185.97.32.18/information/) |
| 188.138.33.220 |  |  | Cisco Talos | DE | 8972 | intergenia AG |  | [Malicious](https://www.virustotal.com/en/ip-address/188.138.33.220/information/) |
| 188.166.23.127 | 443 |  | Cisco Talos | NL | 202018 | Digital Ocean | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/188.166.23.127/information/) |
| 192.42.115.102 | 9004 |  | McAfee | NL | 1103 | SURFnet | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/192.42.115.102/information/) |
| 193.23.244.244 | 443 |  | Cisco Talos | DE | 50472 | Chaos Computer Club e.V. | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/193.23.244.244/information/) |
| 198.199.64.217 | 443 |  | McAfee | US | 46652 | ServerStack | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/198.199.64.217/information/) |
| 2.3.69.209 | 9001 |  | Cisco Talos | FR | 3215 | Orange | Exit Node | Clean |
| 212.47.232.237 |  |  | Cisco Talos | FR | 12876 | Tiscali France | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/212.47.232.237/information/) |
| 213.239.216.222 | 443 |  | McAfee | DE | 24940 | Hetzner Online AG | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/213.239.216.222/information/) |
| 213.61.66.116 | 9003 | TCP | Payoad Security | DE | 8220 | COLT Technology Services Group Limited | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/213.61.66.116/information/) |
| 213.61.66.116 |  |  | Cisco Talos | DE | 8220 | COLT Technology Services Group Limited | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/213.61.66.116/information/) |
| 217.172.190.251 | 443 | TCP | Payoad Security | DE | 8972 | intergenia AG | Exit Node | Clean |
| 217.79.179.77 |  |  | Cisco Talos | DE | 24961 | myLoc managed IT AG |  | Clean |
| 38.229.72.16 |  |  | Cisco Talos | US | 23028 | Team Cymru |  | [Malicious](https://www.virustotal.com/en/ip-address/38.229.72.16/information/) |
| 50.7.151.47 | 443 | TCP | Payoad Security | US | 174 | FDCservers.net | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/50.7.151.47/information/) |
| 50.7.161.218 | 9001 |  | Cisco Talos | NL | 174 | FDCservers.net | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/50.7.161.218/information/) |
| 51.255.41.65 | 9001 |  | McAfee | FR | 16276 | OVH SAS | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/51.255.41.65/information/) |
| 62.138.10.60 | 9001 |  | McAfee | DE | 61157 | Heg mas | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/62.138.10.60/information/) |
| 62.138.7.231 | 9001 | TCP | Payoad Security | DE | 61157 | Heg mas | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/62.138.10.60/information/) |
| 79.172.193.32 |  |  | Cisco Talos | HU | 29278 | Deninet KFT | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/79.172.193.32/information/) |
| 81.30.158.223 |  |  | Cisco Talos | DE | 24961 | myLoc managed IT AG Vserver Netz | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/81.30.158.223/information/) |
| 82.94.251.227 | 443 |  | McAfee | NL | 3265 | XS4ALL Internet BV | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/82.94.251.227/information/) |
| 83.162.202.182 | 9001 | TCP | Payoad Security | NL | 3265 | XS4ALL Internet BV | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/83.162.202.182/information/) |
| 83.169.6.12 | 9001 |  | McAfee | DE | 20773 | Host Europe GmbH | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/83.169.6.12/information/) |
| 86.59.21.38 | 443 |  | McAfee | AT | 3248 | Tele2 Telecommunication GmbH | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/86.59.21.38/information/) |
| 89.45.235.21 |  |  | Cisco Talos | SE | 1653 | SUNET/NORDUnet | Yes | [Malicious](https://www.virustotal.com/en/ip-address/89.45.235.21/information/) |
| 94.23.173.93 | 443 | TCP | Payoad Security | FR | 16276 | OVH.CZ s.r.o. | Exit Node | [Malicious](https://www.virustotal.com/en/ip-address/94.23.173.93/information/) |