

WikiLeaks опубликовала новую порцию документов ЦРУ о кибершпионаже

Wikileaks опубликовала новую порцию конфиденциальных документов о хакерской деятельности ЦРУ из серии Vault 7. Публикация описывает проект CherryBlossom («Цветение вишни»). Он позволяет отслеживать и вмешиваться в действия пользователей Wi-Fi.

CherryBlossom ЦРУ разработало совместно с некоммерческим научно-исследовательским институтом Стэнфорда (SRI International), сказано [в пресс-релизе Wikileaks](#).

Проект объединяет средства мониторинга интернет-активности и заражения компьютеров вредоносными программами через уязвимости в защите. В частности, CherryBlossom ориентирован на взлом беспроводных устройств — роутеров и точек доступа Wi-Fi.

[Что не так с очередной утечкой Wikileaks](#)



Такие устройства обычно используются как часть инфраструктуры интернета в частных домах, общественных местах (барах, гостиницах, аэропортах), малых и средних компаниях, а также в корпоративных офисах. Поэтому эти устройства являются идеальным объектом для атаки вида «Man-In-The-Middle» (атака посредника). Злоумышленники могут легко отслеживать и управлять интернет-трафиком подключенных пользователей.

Вклинившись в поток передаваемых данных вредоносный код может внедриться в операционную систему и использовать уязвимости в приложениях на устройстве жертвы для кражи данных или совершения других действий.

Заражение происходит удалённо, физический доступ к устройству нужен злоумышленникам лишь в самых редких случаях. Подробный механизм действия программ из проекта CherryBlossom описан в слитых Wikileaks [документах](#).

Первый пакет документов ЦРУ из серии Vault 7 был опубликован 7 марта. Утечка включала более 8,7 тысяч документов ЦРУ и файлов, хранившихся в изолированной внутренней сети Центра по киберразведке. В опубликованных документах описывались уязвимости в популярных во всем мире программах и приложениях. WikiLeaks скрыла их детали и [обещала](#) раскрыть только IT-компаниям, поддерживающим безопасность этих продуктов. Состоялось ли сотрудничество, не сообщается.

Публикация второго пакета документов об инструментах шпионажа «Пандемия» (Pandemic) состоялась 1 июня.

Атака посредника или атака «человек посередине» (Man in the middle (MITM)) — вид атаки в криптографии, когда злоумышленник перехватывает и подменяет сообщения, которыми обмениваются корреспонденты, причём ни один из последних не догадывается о его присутствии в канале. Взломщик подключается к каналу между контрагентами и вмешивается в протокол передачи, удаляя или искажая информацию.

👍 [Порекомендовать текст](#)

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)
- [ВКонтакте](#)

Связаться с редакцией Бабра:
newsbabr@gmail.com



Автор текста: **Полина Чехова**,
журналист.

На сайте опубликовано **494**
текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: [@babr24_link_bot](#)
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь

Телеграм: [@bur24_link_bot](#)
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова

Телеграм: [@irk24_link_bot](#)
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская

Телеграм: [@kras24_link_bot](#)
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская

Телеграм: [@nsk24_link_bot](#)
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин

Телеграм: [@tomsk24_link_bot](#)
эл.почта: tomsk.babr@gmail.com

[Прислать свою новость](#)

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"

Телеграм: @babrobot_bot

эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)