КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как изменится ваша ИБ в 2020 году

Dr.WEB®
с 1992 года

Вячеслав Медведев
ООО «Доктор Веб»

ТЕЛЕФОН: +7 495 789-45-87

EMAIL: v.medvedev@drweb.com

6 февраля 2020
Уфа

Dr.WEB®
с 1992 года

Мы постоянно рассказываем о росте количества угроз, новом функционале, возможностях, которые могут использовать наши клиенты

Давайте в этот раз сделаем по иному. Посмотрим, что получается, когда советы не используются

Dr.WEB®
с 1992 года

Компания Dr.Web занимается анализом компьютерных инцидентов (тем что в просторечии называется расследованием преступлений), выступает в роли эксперта по таким делам.

И что удивительно – ситуации бывают самые разные. А вот причины, которые послужили основой возникших проблем – почти всегда одинаковы

Dr.WEB®
с 1992 года

Пример реального инцидента

Dr.WEB®
с 1992 года

Вводная:

Весной 2019 года в службу технической поддержки «Доктор Веб» обратился корпоративный клиент с жалобой на проблемы в работе сервера. Нагрузка на вычислительные мощности была очень высокой и возникала словно из ниоткуда.

Dr.WEB®
с 1992 года

Перед экспертами было поставлено несколько задач.

- Обнаружить причину необычно высокого потребления ресурсов.
- Отследить источник и способ атаки, чтобы пресечь дальнейшее распространение вредоносной программы. Сделать подробное описание атаки.
- На основании проведенного исследования разработать рекомендации по усилению мер безопасности в сети клиента.
- Помочь правоохранительным органам найти виновного в атаке.

Dr.WEB®
с 1992 года

Заражение начиналось с RCE-уязвимости в легальном продукте.

Факт, просто факт

- Уязвимости есть всегда. Только они еще не известны

Dr.WEB®
с 1992 года

Через эксплойт на стороне пострадавшего клиента создавалась административная учетная запись для доступа по RDP.

Возможные причины:

- Работа программ с административными правами
- Отсутствие запрета на запуск нового ПО
- Слабые пароли

Dr.WEB®
с 1992 года

Злоумышленник вручную заходил на сервер по RDP и, используя легитимное ПО ProcessHacker, «убивал» установленный антивирус или просто отключал его напрямую через GUI

Dr.WEB®
с 1992 года

Возможные проблемы

- Наличие удаленного доступа
- Запущенные ненужные сервисы
- Установка неразрешенного ПО
- Разрешение на загрузку драйверов
- Наличие прав пользователя на отключение антивируса
- Отсутствие централизованной защиты
- Отсутствие контроля за изменением состава ПО
- Отсутствие белого списка ПО
- Отсутствие пароля на доступ к настройкам антивируса
- Отсутствие пароля на удаление ПО или пароль, совпадающий с паролем доступа в систему

Dr.WEB®
с 1992 года

Получив доступ в систему, злоумышленник загружал на сервер троянца-майнера и запускал его.
В дальнейшем расследование показало, что в планах злоумышленника был запуск шифровальщика

Заметили проблему – займитесь анализом или обращайтесь к нам!

Dr.WEB®
с 1992 года

В результате исследования этого носителя и используемых «Доктор Веб» ханипотов было обнаружено еще несколько эксплойтов. Было выявлено несколько видов ранее неизвестных антивирусу Dr.Web вредоносных программ и список жертв, атакованных аналогичным образом.
Среди пострадавших оказались пользователи самых разных антивирусных продуктов.
После анализа полученных исходных кодов нового вредоносного ПО вирусная база Dr.Web пополнилась новыми записями.

Dr.WEB®
с 1992 года

Выяснив какое ПО связано с активностью троянца, мы обратились к его разработчику, который передал нам для анализа НЖМД **руководителя** (!) своей разработки.

Именно там мы нашли исходники эксплойтов

Вывод. Доверяй, но проверяй. Увы, но если вы разработчик ПО, то всегда есть вероятность, что в вашем коллективе есть крыса. Анализируйте свое ПО на наличие недокументированного функционала. Репутация – ваше все

Dr.WEB®
с 1992 года

Виновный наказан?

Совместно с правоохранительными органами и разработчиком данного ПО, удалось установить злоумышленника и возбудить уголовное дело.

Dr.WEB®
с 1992 года

Самое главное:

Благодаря экспертизе, разработчику удалось закрыть уязвимость, переосмыслить подходы к разработке ПО с учетом текущих требований к информационной безопасности, установить соответствующий контроль за выпускаемой продукцией/услугой и предпринять соответствующие меры для недопущения подобных инцидентов в будущем.

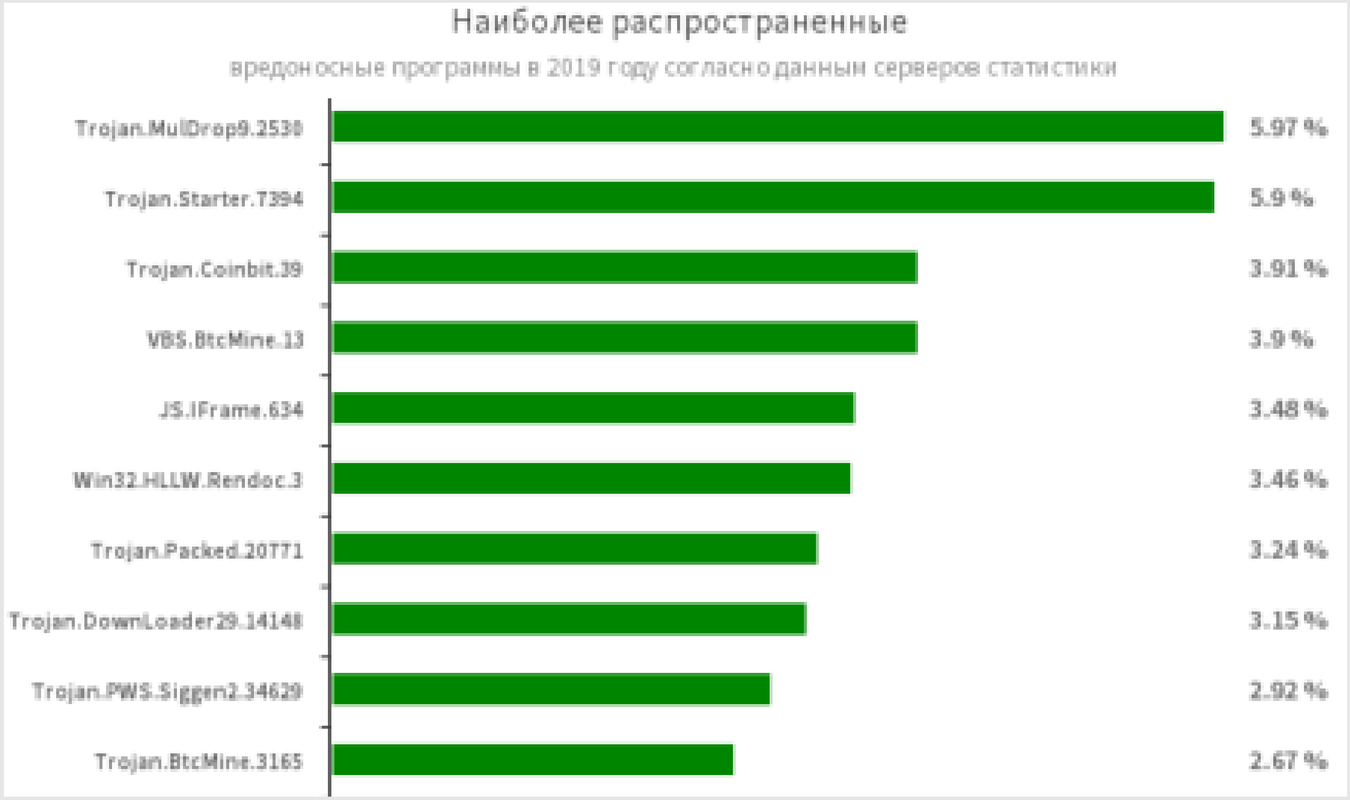
Но стоит особо отметить, что в данном случае жертва еще «легко отделалась». Злоумышленник, получив доступ в систему, устанавливал туда троянца-майнера, который «всего лишь» сильно загружал ресурсы системы, не нанося прямого урона. Поскольку речь идёт о весьма специфическом ПО, которое обычно находится на том же сервере, что и, например, приложения типа 1С, ситуация могла развиваться иначе.

Dr.WEB®
с 1992 года

Если произошла нештатная ситуация (пропали деньги или данные, утекли пароли к корпоративным ресурсам, компьютеры работают с перебоями и т. д.) и вы предполагаете, что причина в действиях вредоносного ПО, закажите экспертизу ВКИ в компании «Доктор Веб».

Dr.WEB®
с 1992 года

По данным серверов статистики «Доктор Веб», в 2019 году чаще всего обнаруживались троянцы и скрипты, выполняющие майнинг криптовалют на устройствах без ведома пользователей. Активными были троянцы, которые устанавливали различное вредоносное ПО.



#CODEIB

Dr.WEB®
с 1992 года

Итого

Dr.WEB®
с 1992 года

Для предотвращения инцидентов:

- ✓ Устанавливайте обновления
- ✓ Используйте белый список ПО
- ✓ Контролируйте изменений состава ПО
- ✓ Никаких админских прав у пользователей
- ✓ Надежные пароли, отличающиеся для пользователей и программ
- ✓ Централизованное управление защитой и/или пароль на доступ к антивирусу
- ✓ Минимум прав у пользователей
- ✓ Отключайте ненужные сервисы

Dr.WEB®
с 1992 года

Низкая зависимость Dr.Web от сигнатур

Эвристический анализатор

Технология Origins Tracing

Модуль эмуляции исполнения

Технология Fly-Code

Комплексный анализатор упакованных угроз

Технология Script Heuristic

Технология анализа структурной энтропии
и много других технологий

Dr.WEB®
с 1992 года

Технологии Dr.Web

✓**Dr.Web Process Heuristic**

✓**Dr.Web ShellGuard**

Dr.Web не просто не позволяет вредоносным объектам внедриться в процессы других программ, а контролирует процессы изнутри.

Dr.WEB®
с 1992 года

Несигнатурные методы детектирования неизвестных угроз Dr.Web Enterprise Security Suite

- Возможность обнаружения угроз без постоянного обращения к вирусным базам — что положительно сказывается как на быстродействии, так и качестве обнаружения новейших угроз
- Обнаружение угроз до фактического исполнения их кода
- Обнаружение популярных в данный момент действий злоумышленников — использования вредоносных майнеров, загрузчиков вредоносного ПО — как активных, так и предназначенных к запуску во всех областях системы.

Dr.WEB®
с 1992 года

Для защиты от угроз, неизвестных антивирусному ядру, Dr.Web позволяет использовать:

- Ограничение доступа к заведомо вредоносным ресурсам
- Ограничение прав пользователя
- Контроль запускаемых программ

Dr.WEB®
с 1992 года

Dr.Web — это дисциплина в использовании Интернета

Сотрудник не отключит антивирус, которые не дает ему зайти на игровой сайт, дать доступ к соцсетям или открыть письмо с трояном — благодаря ЦУ.

Dr.WEB®
с 1992 года

Dr.Web — это контроль доступа к ресурсам и данным

Белый список сменных носителей, ограничения по доступу к нерекомендуемым ресурсам…

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Благодарим за внимание!

Номер службы технической поддержки

8-800-333-7932

Запомнить просто! –
возникла проблема – набери DRWEB!

8-800-33-DRWEB

Убедитесь, что на ваших компьютерах нет вирусов

Dr.WEB®
с 1992 года

#CODEIB