Кто будет охранять охранников?

Ошибки тех, кто отвечает за то, чтобы ошибок не было

Евгений Питолин
Управляющий директор

KASPERSKY

Ваши сотрудники

Американская онлайн-школа American College of Education

- не смогло найти общий язык с системным администратором
- Триано Уильямс не пожелал переезжать (раньше работал удале
- При увольнении сменил пароль от ее Google-аккаунта, лишив бывших коллег доступа к электронной почте и учебным матери более 2 тыс. студентов.
- Google не помог (адрес регистрации был личным)

Английская IT-компания Esselar

- Ричард Нил, IT-директор компании, ушел из нее в результате конфликта
- дождался дня, когда представители Esselar проводили демо для страховой компании Aviva
- взломал около 900 мобильных телефонов сотрудников Aviva и удалил с устройств всю информацию

Американское архитектурное бюро Steven E. Hutchins Architect Inc

- Помощница директора Мэри Кули (Marie Lupe Cooley) увидела в газете объявление о поиске работника на свою позицию
- удалила архив с проектами компании за последние семь лет. (2,5 млн долларов ущерба)
- нового сотрудника, как выяснилось, искали в компанию, принадлежащую супруге директора.

Как защититься от обиженных сотрудников?

- Ведите реестр прав сотрудников в IT-среде, а также аккаунтов и ресурсов, к которым у них есть доступ.
- Время от времени проверяйте, анализируйте и пересматривайте списки прав. Не забывайте отзывать неактуальные разрешения.
- Регистрируйте корпоративные ресурсы только на корпоративные адреса. Доменные имена, аккаунты в соцсетях, панель управления сайтами — это активы организации, и раздавать их персоналу неправильно.
- Все права доступа и аккаунты бывшего работника блокируйте как можно раньше, в идеале — как только вы объявите ему об увольнении.
- Не обсуждайте возможные сокращения и реорганизации штата в общедоступных местах, а размещая объявление о поиске нового работника на редкую должность, помните, что его могут увидеть не только соискатели.
- Старайтесь всегда поддерживать хорошие человеческие отношения с сотрудниками и доброжелательную атмосферу в компании. Зачастую людьми, совершающими громкие кибератаки на бывшего работодателя, движет не жадность, а задетые чувства.
- **Проводите среди сотрудников профилактику защиты цифровых активов, формируйте чувство ответственности за них.**

Ваши программисты

на GitHub обнаружено более 100 тысяч проектов,

в которых в открытом виде хранятся

- Токены, криптографические ключи и другие секретные данные.
- более полумиллиона таких объектов, более 200 тысяч — уникаль
- Есть токены, сгенерированные крупными компаниями,
  такими как Google, Amazon MWS, Twitter, Facebook, MailChimp, и т

Какие данные попали в общий доступ?

- Данные для входа в аккаунты администраторов крупных сайтов.
- API-ключи, позволяющие от имени приложений пользоваться функциями API
- Криптографические ключи, значительная часть которых используется для аутентификации вместо пароля, а не вместе с ним. Таким образом, зная один только ключ, можно получить доступ ко многим ресурсам, в том числе к частным сетям.

Чем грозит утечка токенов и криптоключей?

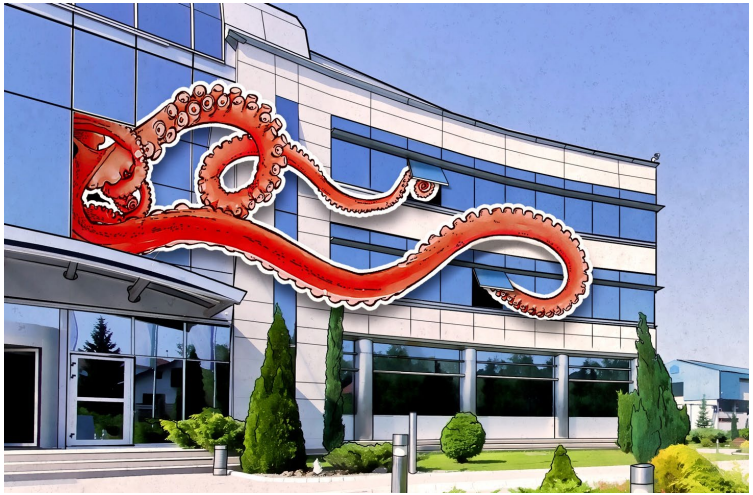
- рассылки и посты от имени опубликовавшей их компании.
- Фишинг по вашему листу рассылки (например, если вы пользуетесь MailChimp).
- Активное использование платных возможностями сервиса (например, мощностями Amazon AWS)

Как остановить расслабленных программистов?

Чтобы вашими токенами или ключами не воспользовались злоумышленники, мы рекомендуем вам:

- Обратить внимание ваших разработчиков на то, что загружать в открытые хранилища действительные токены и ключи — вредно и опасно. Программисты должны понимать, что перед отправкой кода нужно отдельно проследить, чтобы секретных данных в нем не было.
- Поручить ответственному за разработку сотруднику проверить, нет ли в проектах вашей компании на GitHub конфиденциальной информации, и если есть — удалить ее. Тут важно отметить, что удалить ее надо правильно, чтобы информация не осталась в «истории изменений».
- Если ключи или токены были обнаружены — сменить их. Неизвестно, кто успел посмотреть код и сохранить его у себя.
- **Постоянно повышать осведомленность сотрудников в области информационной безопасности, чтобы первый пункт этого списка был им очевиден.**

Ваши MSP-провайдеры



MSP-провайдер как вектор заражения

Стать «звеном» в атаке через цепочку поставок — ситуация неприятная для любой организации. Для компании, предоставляющей MSP-услуги, это вдвойне неприятно.

Особенно если среди оказываемых услуг есть и управление системами безопасности

- киберпреступность тщательно изучает MSP-инструменты и ждет, пока кто-нибудь не допустит ошибку.
- дождались — через уязвимость в софте MSP-компании неизвестные рассылали трояна-шифровальщика.
- Уязвимость была в плагине ConnectWise ManagedITSync, который служит для взаимной интеграции между платформой автоматизации ConnectWise Manage и системой удаленного мониторинга и управления Kaseya VSA.
- Уязвимость позволяет удаленно вносить изменения в базу данных Kaseya VSA. В результате злоумышленники могут добавлять пользователей с любыми правами доступа и ставить любые задачи. Например, по загрузке вредоносного ПО на все компьютеры клиентов MSP-провайдера.

Можно ли выбрать безопасного MSP-провайдера?

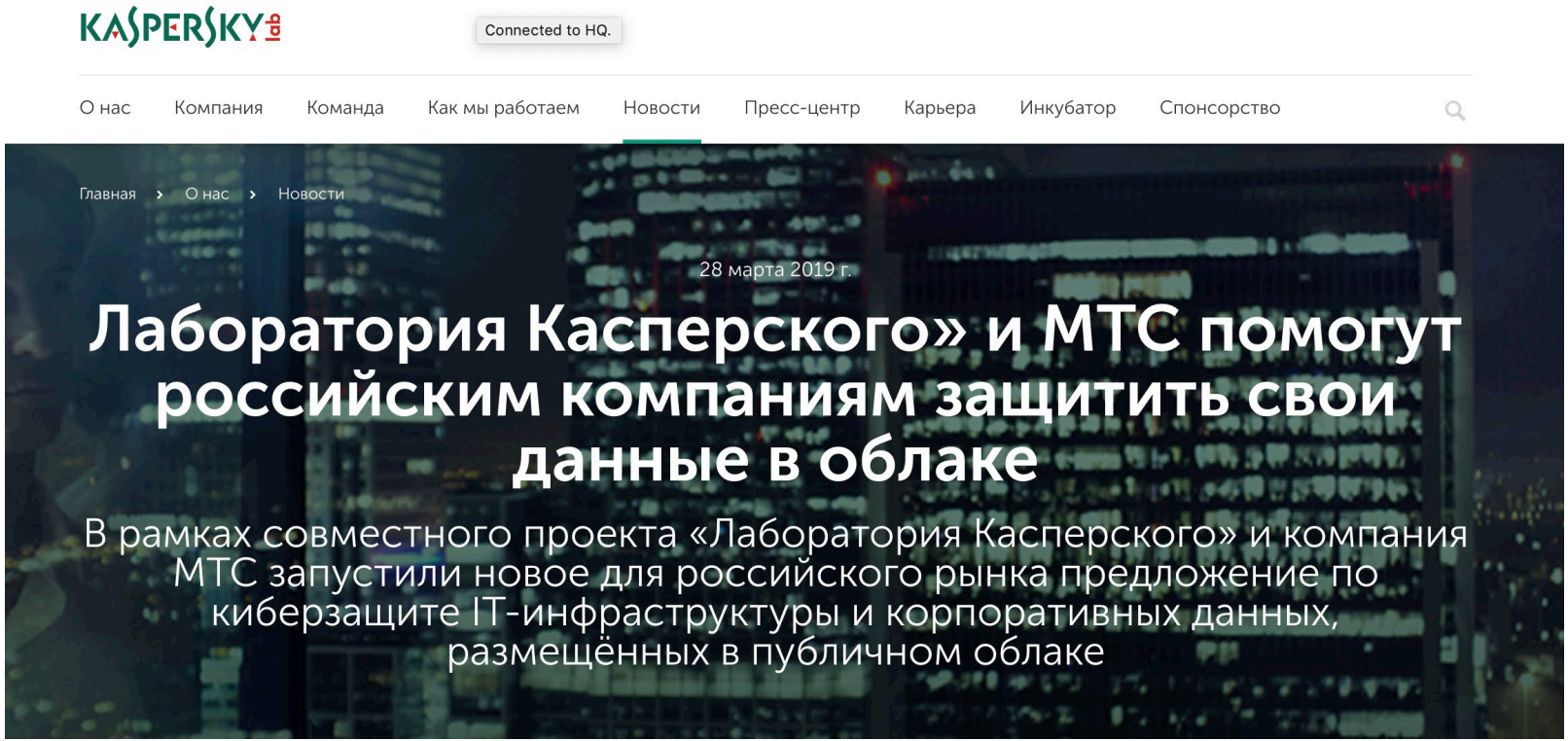
Детали инцидента

- По данным исследователей, уязвимость была использована неизвестными для атаки шифровальщика-вымогателя GandCrab. То есть, пользуясь тем, что Kaseya имеет доступ ко всем конечным устройствам с правами администратора, злоумышленники создали задачу, которая скачивала вредонос на компьютеры и запускала его.
- После этого агентство Cybersecurity and Infrastructure Security Agency (CISA) выпустило предупреждение об активности китайских киберпреступников, которые активно интересуются MSP-провайдерами.

Что делать?

- Для начала — не забывать обновлять программное обеспечение интеграции и взаимодействия.
- Самое главное – выбрать себе провайдера, который комплексно подошел к вопросу защиты своих клиентов
    - Защитил ЦОД и виртуальные платформы
    - Обеспечил адекватные тарифы с включенными ИБ-решениями
    - Позаботился о защите собственных платформ взаимодействия

Можно ли выбрать безопасного MSP-провайдера?



Ваши поставщики компьютеров

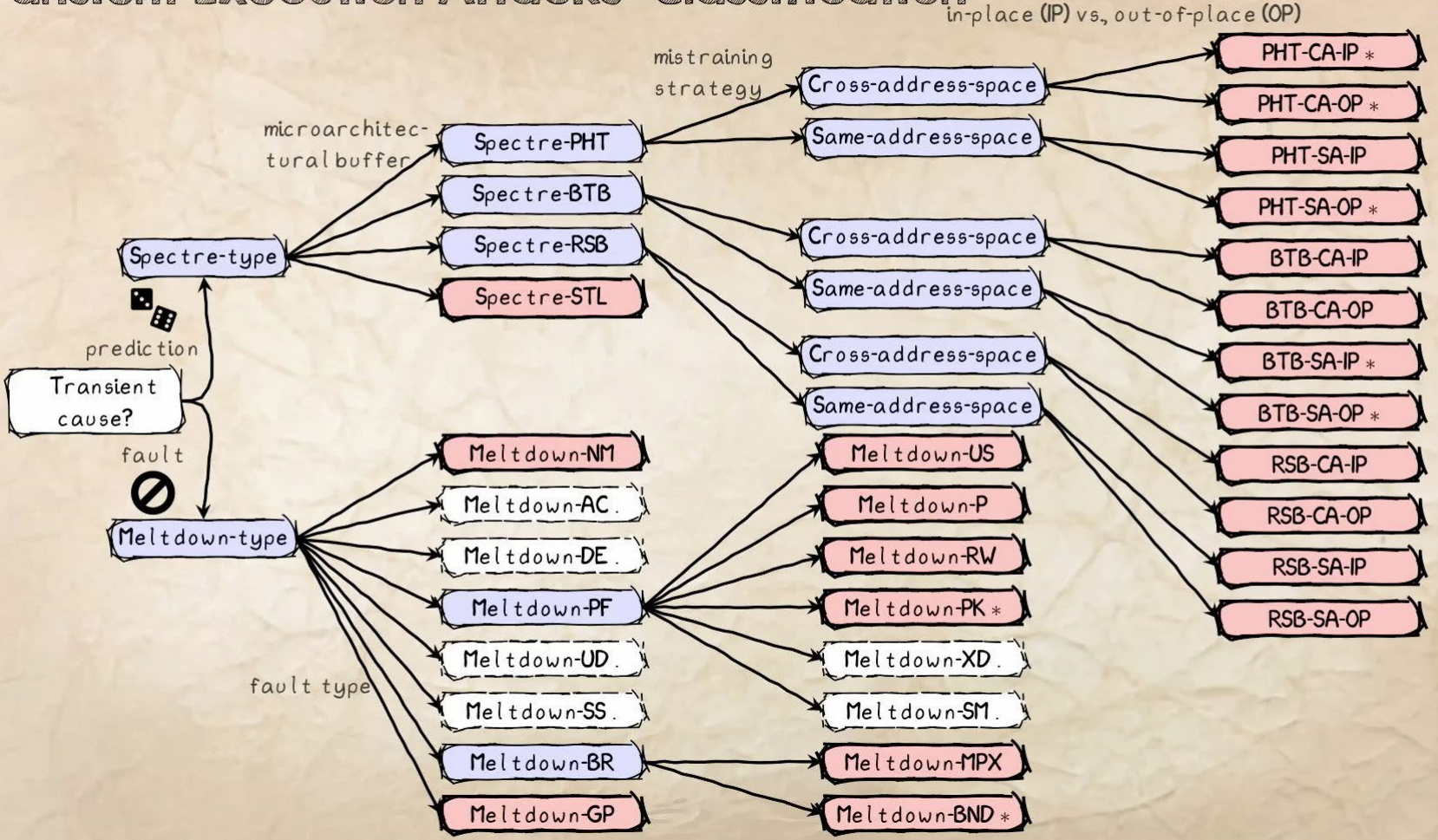
После обнаружения первых Meltdown и Spectre

- исследователи стали намного активнее копать в этом направлен
- разработчики процессоров используют и другие оптимизации
- Исследователи из университета Граца упоминают
- 14 вариаций Meltdown-подобных уязвимостей
- 13 Spectre-подобных уязвимостей
- 27 штук разных аппаратных уязвимостей в процессорах

Раньше AMD заявляла, что ее процессоры не подвержены уязвимостям класса Meltdown, но исследователи смогли обнаружить вариант Meltdown (его назвали Meltdown-BR), который очень даже работал на процессорах AMD.

То есть на текущий момент процессоры трех крупнейших мировых разработчиков — AMD, ARM и Intel — подвержены как Meltdown, так и Spectre. Spectre и Meltdown — это аппаратные уязвимости, они существуют на уровне компьютерного «железа», и программными заплатками их полностью просто не исправишь.

Transient Execution Attacks: Classification



Будущее Spectre и Meltdown

- В октябре 2018-го Intel объявила о том, что в новых процессорах (речь про поколение, которое появится в 2019 году) на аппаратном уровне будет реализована защита от Spectre и Meltdown.

- AMD также собирается залатать одну из вариаций Spectre в новом поколении процессоров с архитектурой Zen 2, которое должно выйти в 2019-м.

- ARM тоже обещает исправления на аппаратном уровне, заявляя, что «все грядущие процессоры будут защищены от Spectre-подобных атак».

НО! речь идет именно о новых устройствах.

- Тем же, кто приобрел компьютер, смартфон или какое-то другое устройство на базе процессоров Intel, AMD или ARM в 2018 году или раньше, остается устанавливать патчи для всего на свете, которые ощутимо снижают производительность.

Ваши поставщики ПО

Мы обнаружили, вероятно,

один из крупнейших инцидентов такого рода

Киберпреступники добавили бэкдор

в утилиту ASUS Live Update,

которая доставляет обновления BIOS, UEFI и ПО

на ноутбуки и настольные компьютеры ASUS,

а затем распространяли программу через официальные каналы

- превращенная в троян утилита была подписана легитимным сертификатом и размещена на официальном сервере обновлений ASUS, что позволило ей долгое время оставаться незамеченной.
- преступники позаботились даже о том, чтобы размер у вредоносной утилиты был точно таким же, как у настоящей.
- более 57 000 пользователей установили утилиту с бэкдором
- преступники нацелились на 600 определенных MAC-адресов, хэши которых были зашиты в различные версии утилиты.

Ваши поставщики ПО

т ли вашего MAC-адреса в списке целей?

https://shadowhammer.kaspersky.com/

Ваши ОС

Уязвимость CVE-2019-0797

- Данные были переданы в Microsoft;
- соответствующий патч уже выпущен.

- Данная уязвимость позволяет получить доступ к сети или устройству жертвы.
- Написан эксплойт, нацеленный на 8-ю и 10-ю версии Windows.
- Брешь в графической подсистеме для расширения локальных привилегий дает полный контроль над атакуемым компьютером. Это уже четвёртый эксплойт нулевого дня, который был найден нами в MS

Продукты «Лаборатории Касперского» детектируют уязвимость как HEUR:Exploit.Win32.Generic, HEUR:Trojan.Win32.Generic и PDM:Exploit.Win32.Generic.

Как помочь себе с этой проблемой?

- как можно скорее установить патч Microsoft для исправления этой уязвимости;
- убедиться в том, что ПО, используемое в организации, регулярно обновляется, в том числе после выпуска патчей (помочь автоматизировать эти процессы могут защитные продукты с функциями анализа уязвимостей и управления обновлениями);
- выбрать надёжное защитное решение для бизнеса, которое использует технологии поведенческого анализа
- использовать комплексные инструменты защиты от APT-атак
- **убедиться в том, что сотрудники отдела информационной безопасности имеют доступ к актуальной информации о киберугрозах - сервисам, предоставляющие аналитические отчеты об APT-угрозах.**
- **проверить, насколько хорошо сотрудники знакомы с основами безопасного поведения.**

Ваши поставщики оборудования

Уязвимости в телекоммуникационном оборудовании
были "устранены" через блокировку запросов от утилиты curl

Исследователи обнаружили, что компания – производитель
лишь создала видимость устранения уязвимостей в выпущенном в янв
обновлении прошивки к маршрутизаторам.

Вместо реального устранения проблем в скриптах web-интерфейса, в обновлении прошивки были внесены изменения в настройки http-сервера nginx, блокирующие обращение при помощи утилиты curl, которая использовалась в прототипе эксплоита и примерах для проверки наличия уязвимости.

После установки обновления прошивки 1.4.2.20 с заявленным "устранением" проблем, устройства как и раньше остаются уязвимыми. Обновление прошивки с корректным исправлением пока не выпущено и ожидается в середине апреля Неисправленными остаются три уязвимости. Две проблемы (CVE-2019-1653) позволяют без аутентификации обратиться к скриптам и получить содержимое файла конфигурации устройства, включая хэши паролей (возможен доступ по хэшу, без подбора исходного пароля), а также ключи к VPN и IPsec. Третья уязвимость (CVE-2019-1652) позволяет выполнить любую команду в системном окружении устройства через манипуляции с параметрами в форме генерации сертификатов.

Как помочь себе с этой проблемой?

- **убедиться в том, что сотрудники отдела информационной безопасности имеют доступ к актуальной информации о киберугрозах - сервисам, предоставляющие аналитические отчеты об APT-угрозах.**
- **Своевременно задавать производителю вопросы об обновлении ПО**

Все тлен и безысходность

Экспертные и аналитические мнения

Выход?