КОД БЕЗОПАСНОСТИ

Опыт применения технологий виртуализации для защиты конечных точек

Опасность от уязвимостей растёт

- Злоумышленники смещают фокус с уязвимостей в приложениях на уязвимости в ОС

- Информация об этих уязвимостях добывается спецслужбами, а потом утекает на свободный рынок

Защититься трудно

Даже после выхода обновлений для базового ПО проблема остается.

Корпоративные пользователи не могут оперативно обновить базовое ПО на своих компьютерах и серверах

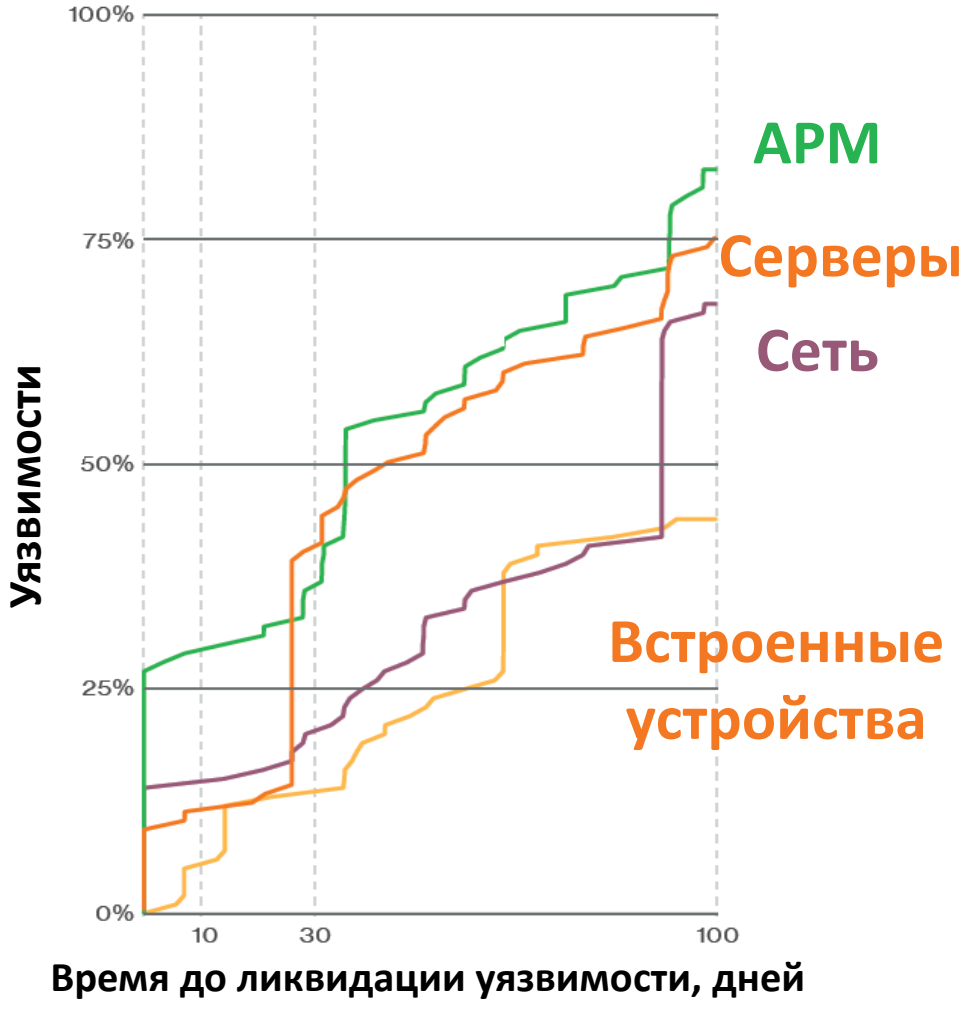
- За **три месяца** до эпидемии WannaCry Microsoft выпустил патч, предотвращающий заражение
- Несмотря на это, WannaCry заразил более **500 тыс. компьютеров** по всему миру*

* - По информации с сайта Malwaretech.com

КОД БЕЗОПАСНОСТИ

Как обновляются элементы ИТ-инфраструктуры?

- АРМ и другие пользовательские устройства обновляются сразу после обнаружения уязвимостей
  - И второй раз через месяц
- Серверы – **ближе к концу первого месяца**
- Сетевое оборудование – **ближе к концу первого квартала**
- Встроенные устройства обновляются редко и не до конца

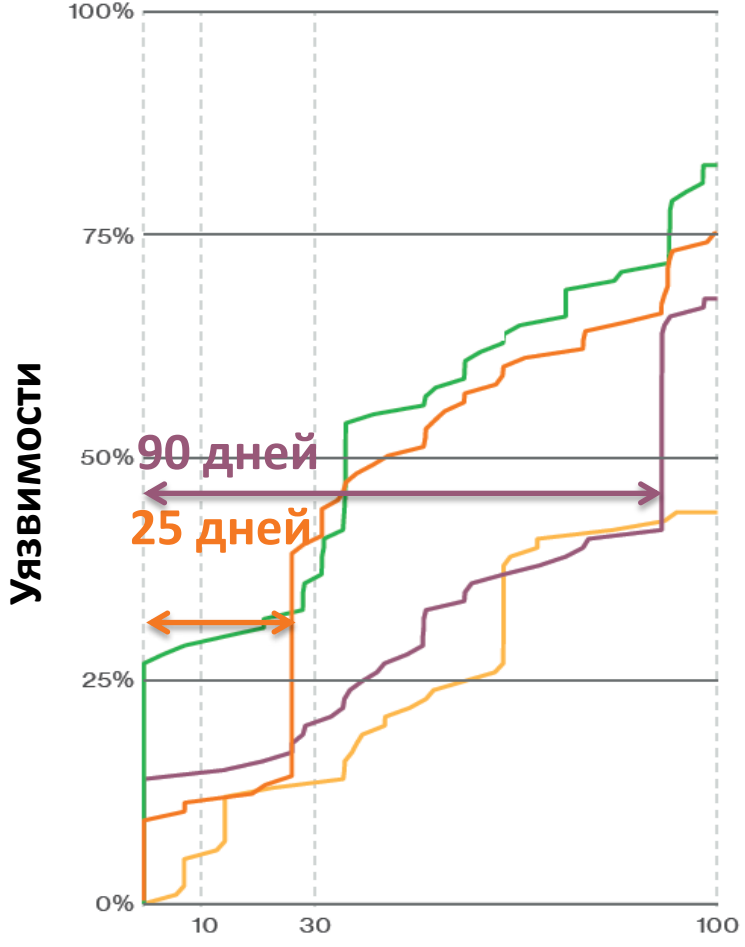


*Verizon Data Breach Investigation Report ‘17

КОД БЕЗОПАСНОСТИ

Как обновляются элементы ИТ-инфраструктуры?

- АРМ и другие пользовательские устройства обновляются сразу после обнаружения уязвимостей
  - И второй раз через месяц
- Серверы – **ближе к концу первого месяца**
- Сетевое оборудование – **ближе к концу первого квартала**
- Встроенные устройства обновляются редко и не до конца

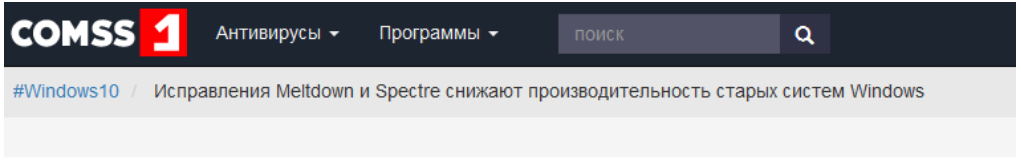


*Verizon Data Breach Investigation Report ‘17

КОД БЕЗОПАСНОСТИ

Почему тяжело обновлять корпоративную инфраструктуру?

- Долгое ожидание технологического окна
- Недостаток ресурсов для тестирования
    - «У нас 1000 критических уязвимостей, мы можем вовремя обновить только 100»
- Патч негативно сказывается на работе системы
    - См последние обновления для защиты от Meltdown и Spectre



Исправления Meltdown и Spectre снижают производительность старых систем Windows

2018-01-10 | Автор Comss.one | комментарии

11:43 / 8 Января, 2018

Исправляющий Meltdown/Spectre патч приводит к сбою в работе систем на базе AMD

Последствия

Действия злоумышленника:

- Деактивация средств защиты
- Закрепление в системе
- Разведка и продвижение по внутренней сети
- Поиск и извлечение информации

Последствия для организации:

Кража ценной информации
Незапланированная остановка деятельности
Потеря репутации

Что делать?

По умолчанию считать ОС уязвимой средой

Контролировать ОС «снаружи»

Отслеживать попытки влияния на средства защиты

КОД БЕЗОПАСНОСТИ

Доверенная среда – защита от удаленного злоумышленника

- **Загружается до операционной системы** и работает параллельно
- Использует недоступные ОС ресурсы:
  - Выделенное ядро процессора
  - Область оперативной памяти

Подтверждено ФСБ*

- **Механизм используется в сертифицированном ФСБ продукте Jinn-client**

**** Для работы требуется Процессор с поддержкой технологий виртуализации VT-x или AMD-V**

Возможности доверенной среды

- Контроль целостности драйверов
  - При загрузке
  - В процессе работы
- Поддержка «белого списка» драйверов
- Регулярная проверка целостности процессов
- Защита от завершения процессов

КОД БЕЗОПАСНОСТИ

Задачи доверенной среды

Возможность	Задача
Контроль целостности драйверов	Защита от подмены драйвера при загрузке ОС и эксплуатации уязвимости драйвера
Поддержка «белого списка» драйверов	Невозможность работы посторонних драйверов
Регулярная проверка целостности процессов	Невозможность эксплуатации уязвимости процесса в процессе работы
Защита от завершения процессов	Невозможность деактивации системы защиты

КОД БЕЗОПАСНОСТИ

Преимущества доверенной среды

Сокращение «окна возможностей» злоумышленников	Повышение доверия к механизмам защиты конечных точек
Обнаруженные уязвимости меньше влияют на уровень защиты информационной системы	Внешний контроль работы ОС обеспечивает более высокий уровень защиты

КОД БЕЗОПАСНОСТИ

Защита конечных точек: Концепция «Кода Безопасности»

КОД БЕЗОПАСНОСТИ

Резюме

- Закрыть все уязвимости сразу – нельзя
- Злоумышленники активно этим пользуются
- Для надежной защиты элементов инфраструктуры необходим независимый контроль над ОС
- Доверенная среда позволяет организовать такой контроль без дополнительного оборудования

СПАСИБО ЗА ВНИМАНИЕ!

Александр Немошкалов

ООО «Код Безопасности»

info@securitycode.ru

www.securitycode.ru

КОД БЕЗОПАСНОСТИ