VOLKSWAGEN
GROUP RUS

Методы защиты от основных угроз виртуальной инфраструктуре

07.03.2022 / Андрей Минаев

PUBLIC
ОБЩЕДОСТУПНО

Classification: Public

Угрозы со стороны производителя ПО. Блокировка обновлений средств обеспечения безопасности

VOLKSWAGEN
GROUP RUS

Без обновлений баз сигнатур многие средства безопасности бесполезны:

- Antivirus
- IPS
- WAF
- Anti-Spam
- Secure Web Gateway (Web Proxy)
- SIEM

Решение:

- Переход на Российские решения
- Сервисы по обновлению от интеграторов

Популярно:

Avast временно приостановил свою деятельность на территории Российской Федерации.

При необходимости, мы будем рады помочь или ответить на ваши вопросы на странице Службы поддержки.

Fortinet® (NASDAQ: FTNT), a global leader in broad, integrated, and automated cybersecurity solutions, today announced that it ceased operations within Russia. This included the suspension of Fortinet sales, support, and professional services. Fortinet continues to follow all security protocols and U.S. and other applicable government regulations and guidelines.

Угрозы со стороны производителя ПО. Саботаж

Производитель, либо его сотрудник сознательно наносит ущерб клиенту используя удаленный доступ.

Решение:

- Ограничить удаленный доступ производителя к ПО
- Отключить функции Call-Home
- Резервное копирование
- Резервное копирование конфигураций оборудования
- Наличие DRP/ARP

Угрозы со стороны производителя ПО. Саботаж. Вредоносный код с обновлением. Обновлять нельзя оставить.

VOLKSWAGEN
GROUP RUS

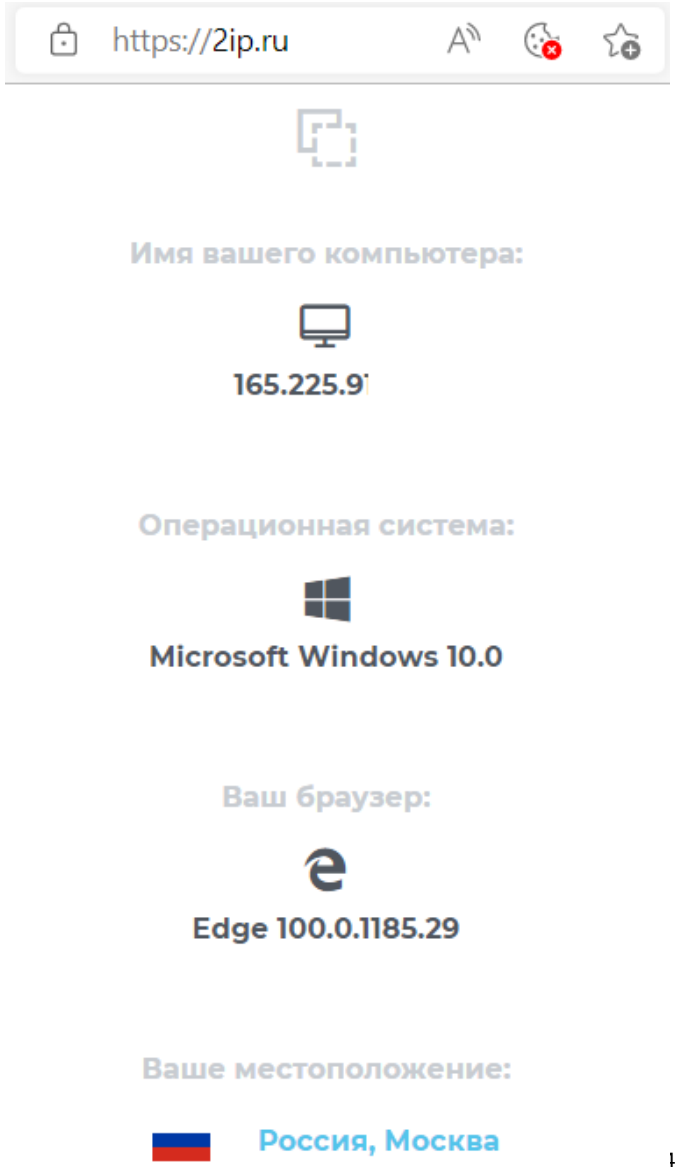
Производитель, либо его сотрудник сознательно наносит ущерб клиенту, встраивая вредоносный код в приложение. Пример: JavaScript фреймворк Vue.js. В open-source модуль node-ipc был встроен вредоносный код, который повреждает файлы на системе, если она из России.

Решение:

- Ограничить доступ системы в интернет. Либо совсем, либо только к конкретным ip через FW, либо к конкретным URL через Secure Web Gateway (Web Proxy).
- Организовать обновление систем через локальный репозиторий или выделенную систему обновлений
- Резервное копирование

https://clck.ru/emn4V

https://clck.ru/emnR2

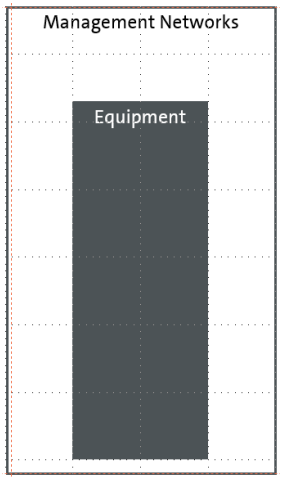


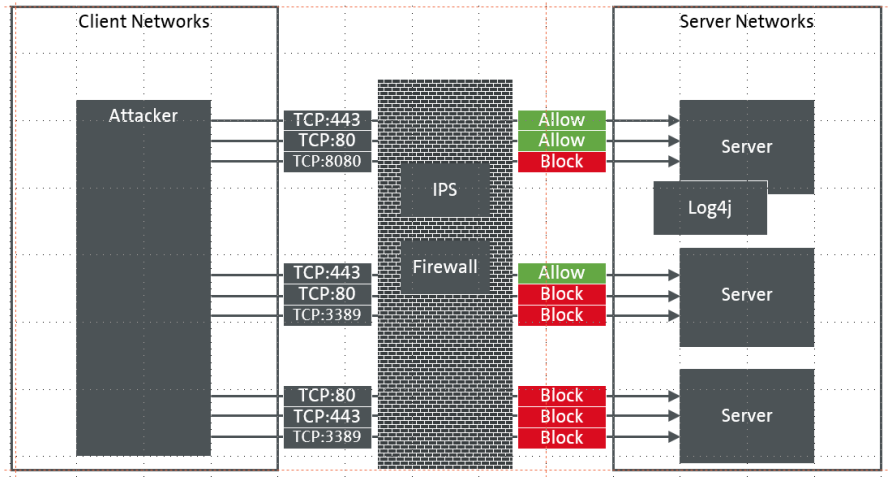
Угрозы со стороны производителя ПО. Блокировка обновлений

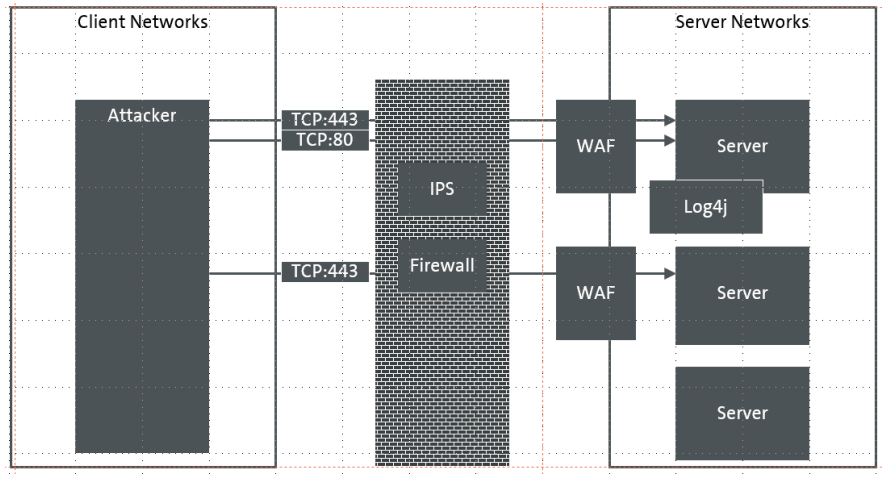
Уязвимости в софте находятся каждый день. Если софт не обновлять, то через некоторое время он становится опасным.

Решение:

- Ограничить доступ к приложениям
- Сканирование сети на уязвимости
- Удаление систем, за которые никто не отвечает и которыми никто не пользуется
- Сегментирование сети (снижение площади атаки):
  - Отделение клиентов от серверов с помощью Firewall
  - Выделение интерфейсов управления системами (Virtualization, Storage, Network, etc.) в отдельные служебные сети, доступ администраторов в которые осуществлять только через промежуточные сети.
- WAF между пользователями и приложениями





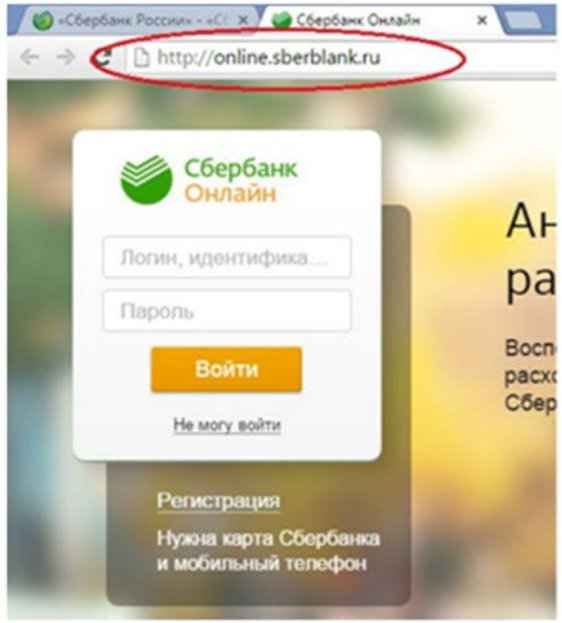


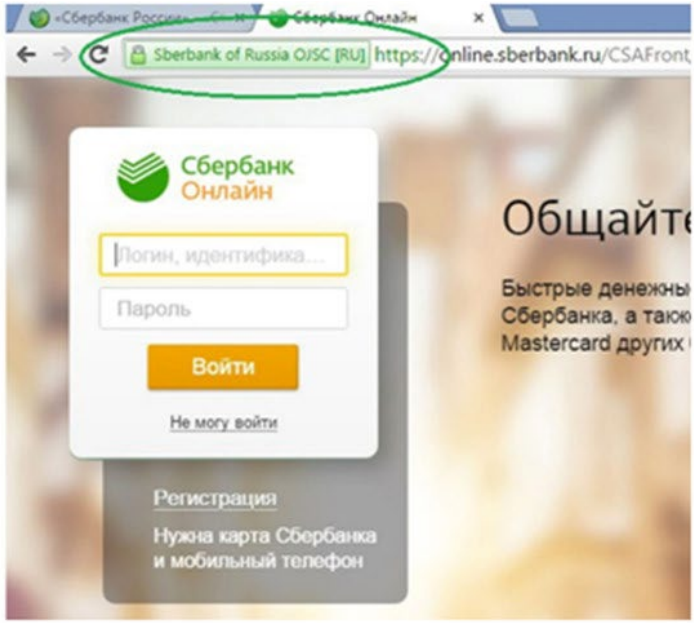
Фишинг, утечка паролей администраторов

От целевых фишинговых атак очень сложно защищаться.

Решение:

- Обучение пользователей
- Внедрение 2FA с помощью централизованных IDP решений
- Отдельные админские учётки для администрирования рабочих станций и для администрирования серверов
- PAM для админских учёток





DDOS атаки

DDOS атаки на сайты и системы компании. Если у вас нет публичного ресурса, это не значит, что вы в безопасности. Небольшие и дешёвые атаки на сеть компании, которые способны её положить (100 Mbit/s – 1 Gbps). Угроза работы VPN и других решений.

Решение:

- Дублирование сервисов в разных публичных подсетях
- Включение защиты от DDOS
- Запрет на доступ к сети из других стран

DDOS атаки на DNS

Системы могут стать недоступны из-за DDOS атак на DNS сервера.

Решение:

- Поднимайте secondary DNS зоны на сторонних DNS серверах
- Мигрируйте на другого DNS провайдера с защитой от DDOS

Выводы

- ✓ Проанализируйте риски со стороны поставщиков для всех ваших систем
- ✓ Спланируйте мероприятия по предотвращению этих рисков
- ✓ Ограничьте доступ система-интернет, пользователь – система
- ✓ Делайте резервное копирование
- ✓ Включайте 2FA

Андрей Минаев

Andrey.Minaev@vwgroup.ru

www.vwgroup.ru