Обзор существующих инструментов, техник и методик для расследования инцидентов в технологических системах.

Валерия Кривко

Руководитель Пресейл Службы

2019

KASPERSKY lab

Конфиденциальность

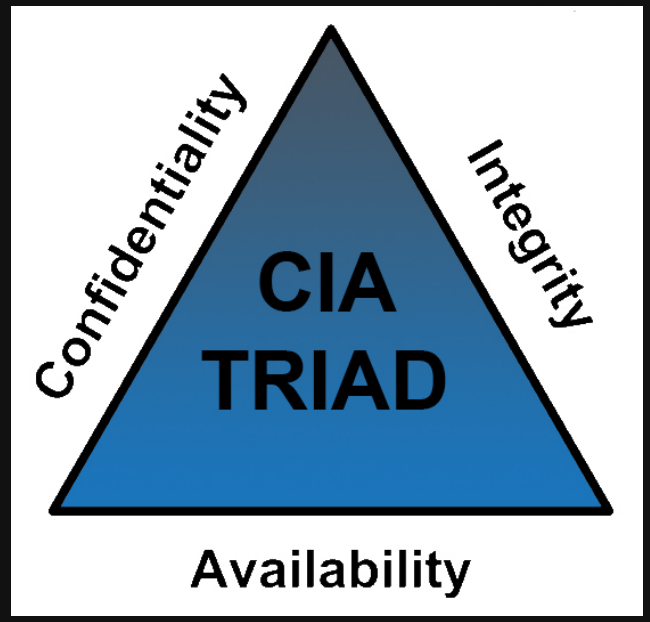
Целостность

Доступность

Начало истории …

Информация от клиента:

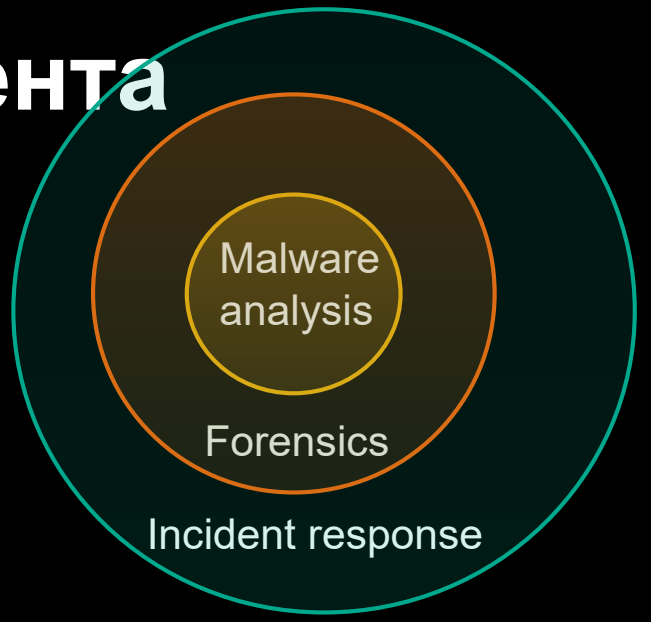
1. Более 150 машин инфицированы
2. Корпоративная и технологическая сеть поражены
3. Машины операторов перезагружались, синий экран смерти BSOD



Клиент сформулировал вопросы:

1. Что произошло? Какой угрозе или атаке подверглась инфраструктура ?
2. Какие векторы атак были использованы?
3. Какие системы были поражены?
4. Какой ущерб был нанесен?

План расследования инцидента



Сбор улик:
1. Образы диска, дампа памяти
2. трафик
3. Логи, программы контроллеров, прошивки
Любые улики могут быть полезны!

1. Найти все машины содержащие подозрительные данные
2. Создать хронологию инцидента
3. Найти первую инфицированную машину

Найти подозрительные данные в собранных уликах
Понять причину перезагрузки и синего экрана смерти

Collect data → **Stop malware propagation** → **Identify and analyze threat** → **Find all affected machines** → **Forensics at first affected system** → **Mitigation, Reporting**

Если используется антивирус

Понять вектор атаки

KASPERSKY lab

Что важно сделать на первом этапе?

- Сбор улик очень важный этап в расследовании инцидентов
- Конечно, для клиента в приоритете остановить активную фазу заражения
- Но, прекратить заражение это значит удалить все улики

- Использовать утилиты с бэкапированием и логированием

Принцип работы WannaCry

KASPERSKY lab

+

=

KASPERSKY lab

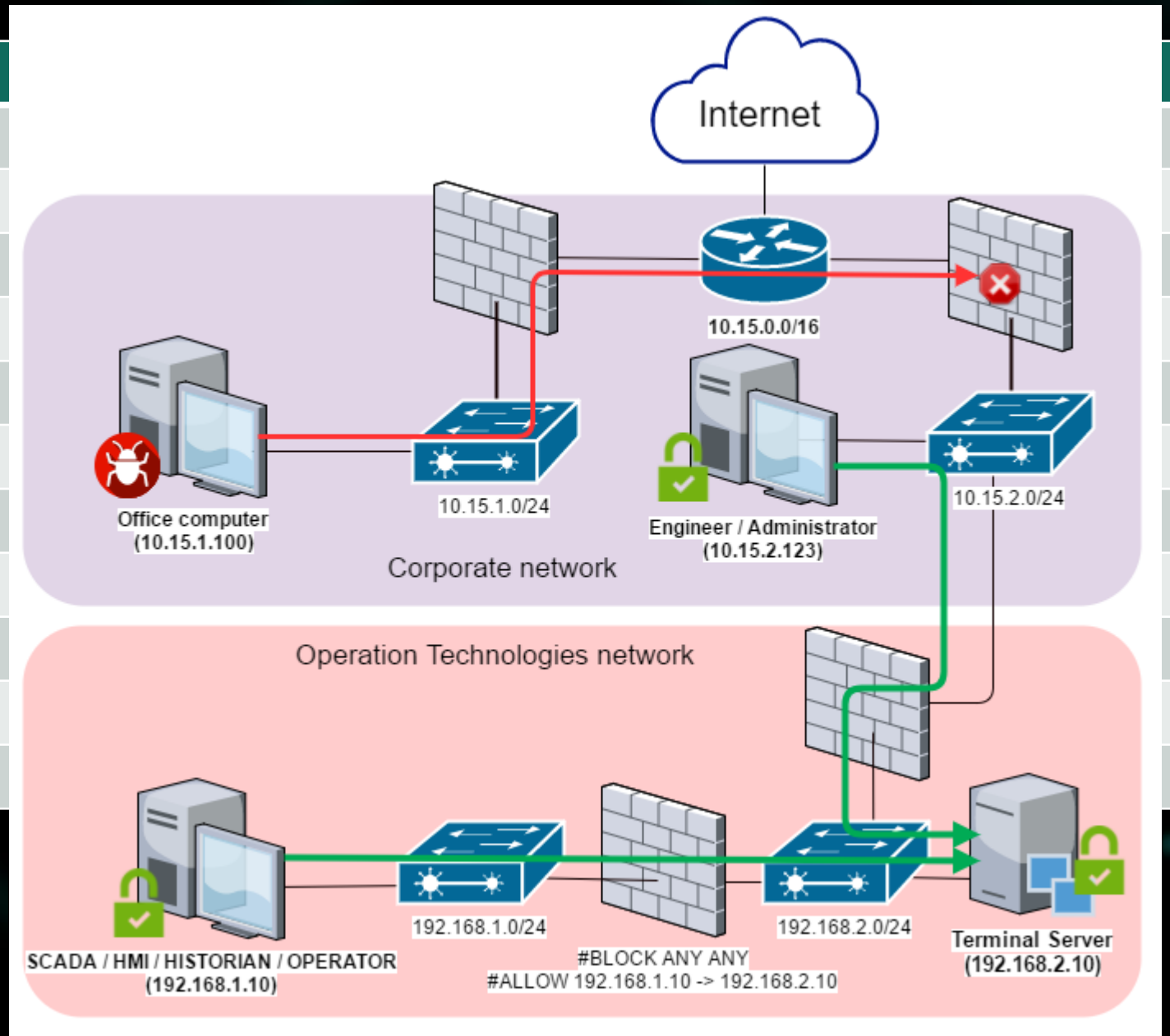
Как составить хронологию в сети большого предприятия ?

1. Логи сетвого оборудования
2. Логи защитных решений - AV
3. Улики образа диска (файловая система, дамп памяти, реестр, и тд)

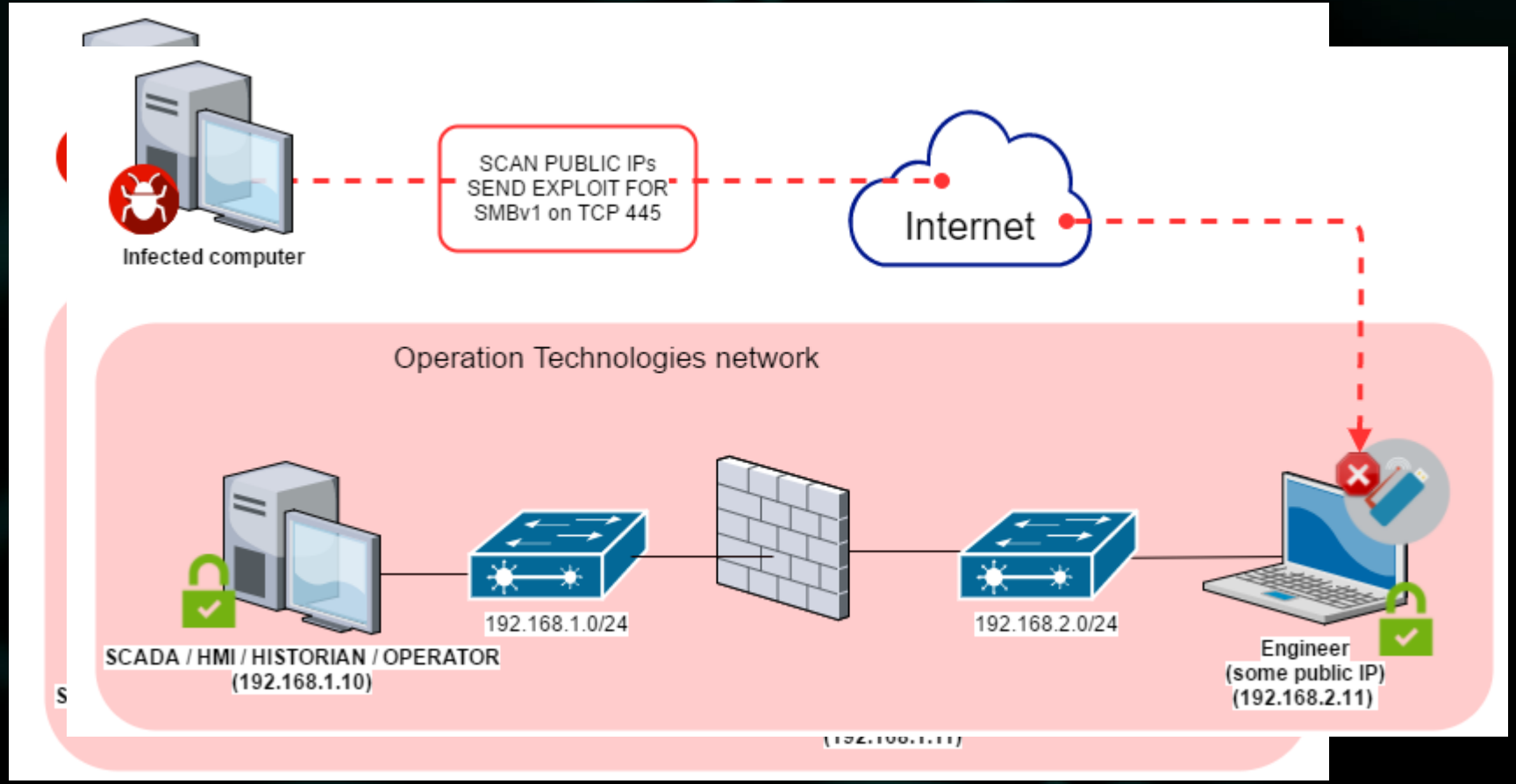
Реальность:

1. Нет логов сетевого оборудования
2. AV со старыми сигнатурными базами

Хронология заражения



Другие способы инфицирования

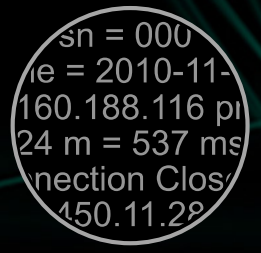


Но это еще не все....

KASPERSKY lab

Что делать?

- ✓ Установить современный AV с централизованным управлением на все машины, регулярно обновлять базы
- ✓ Использовать специализированные решения для защиты индустриальной инфраструктуры - KICS
- ✓ Изменить конфигурацию сетевой инфраструктуры
- ✓ Включить логирование для всех серверов, ПЛК, сетевых устройств, систем безопасности
- ✓ Тренинги, аудит и прочее



KASPERSKY lab


WE PROTECT WHAT MATTERS MOST
KASPERSKY lab