

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

Валерия Кривко

Руководитель Пресейл Службы

2019

Конфиденциальность

Целостность



Доступность

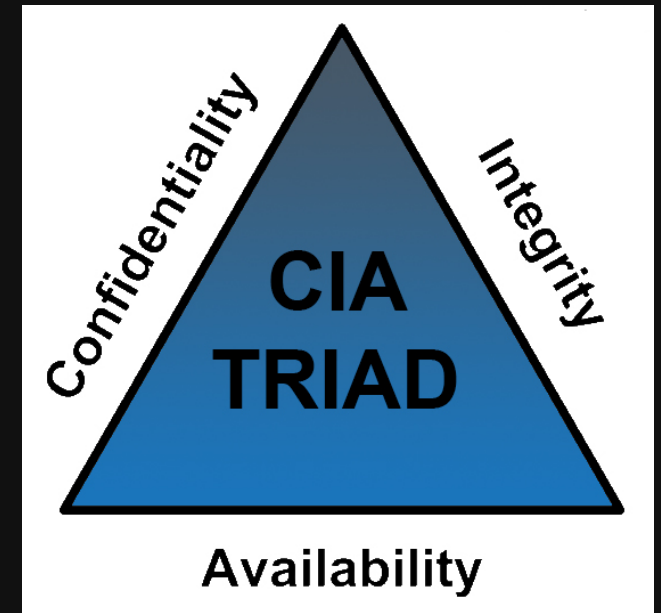
Начало истории ...

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?



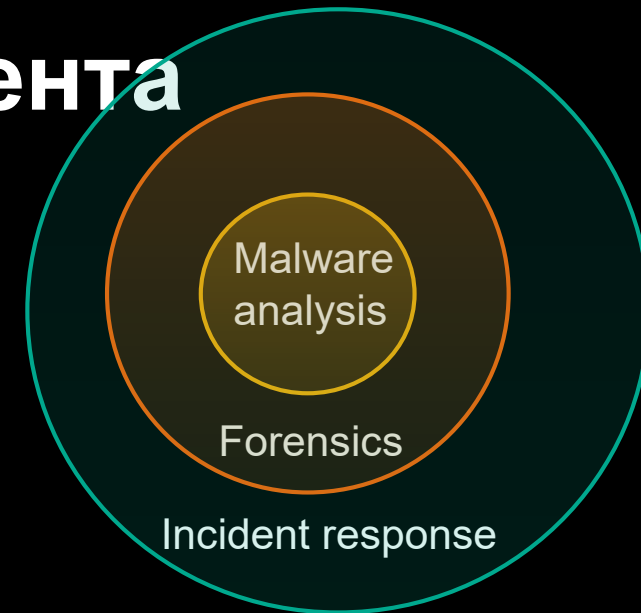
План расследования инцидента

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

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





+



=



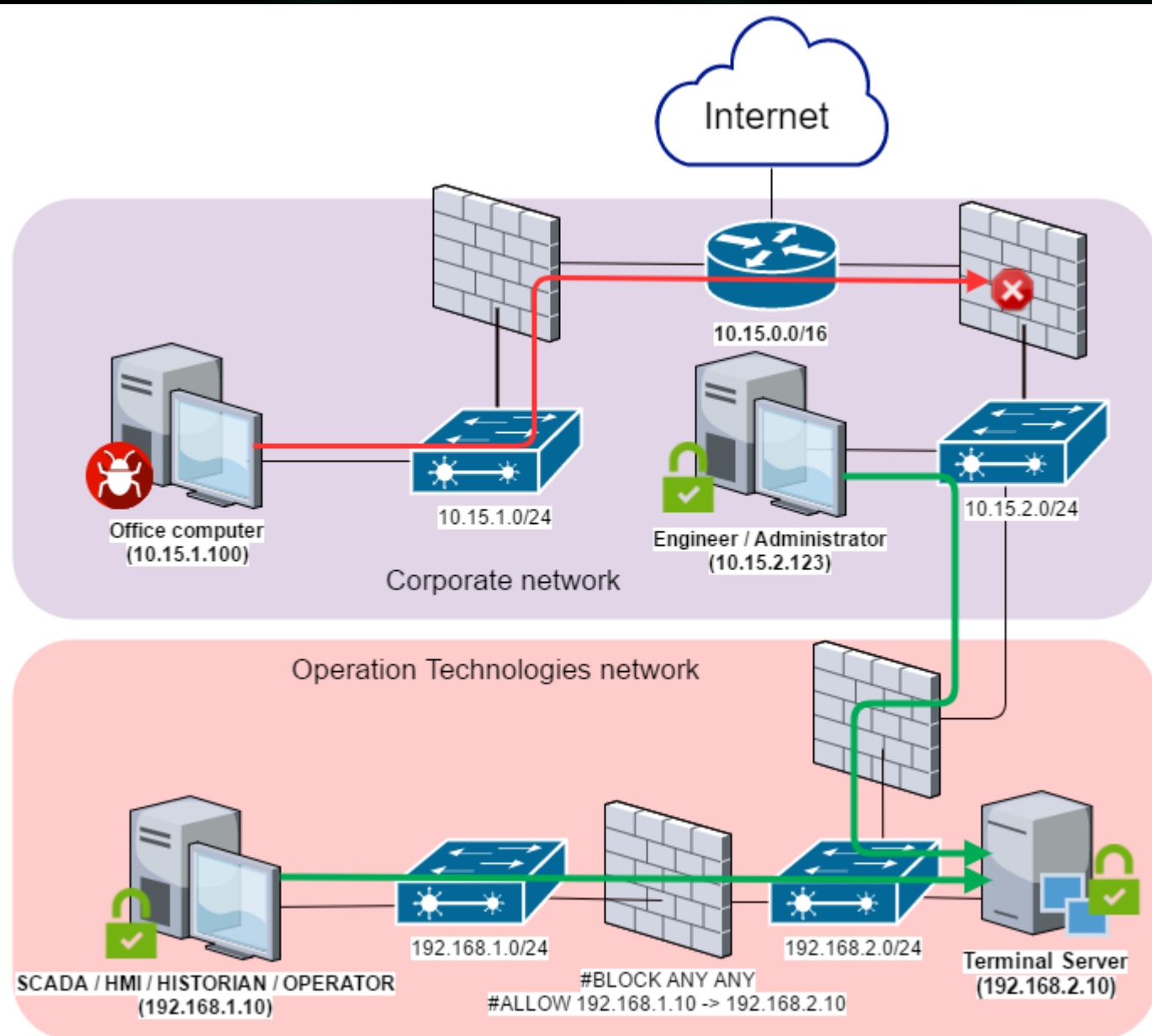
Как составить хронологию в сети большого предприятия ?

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

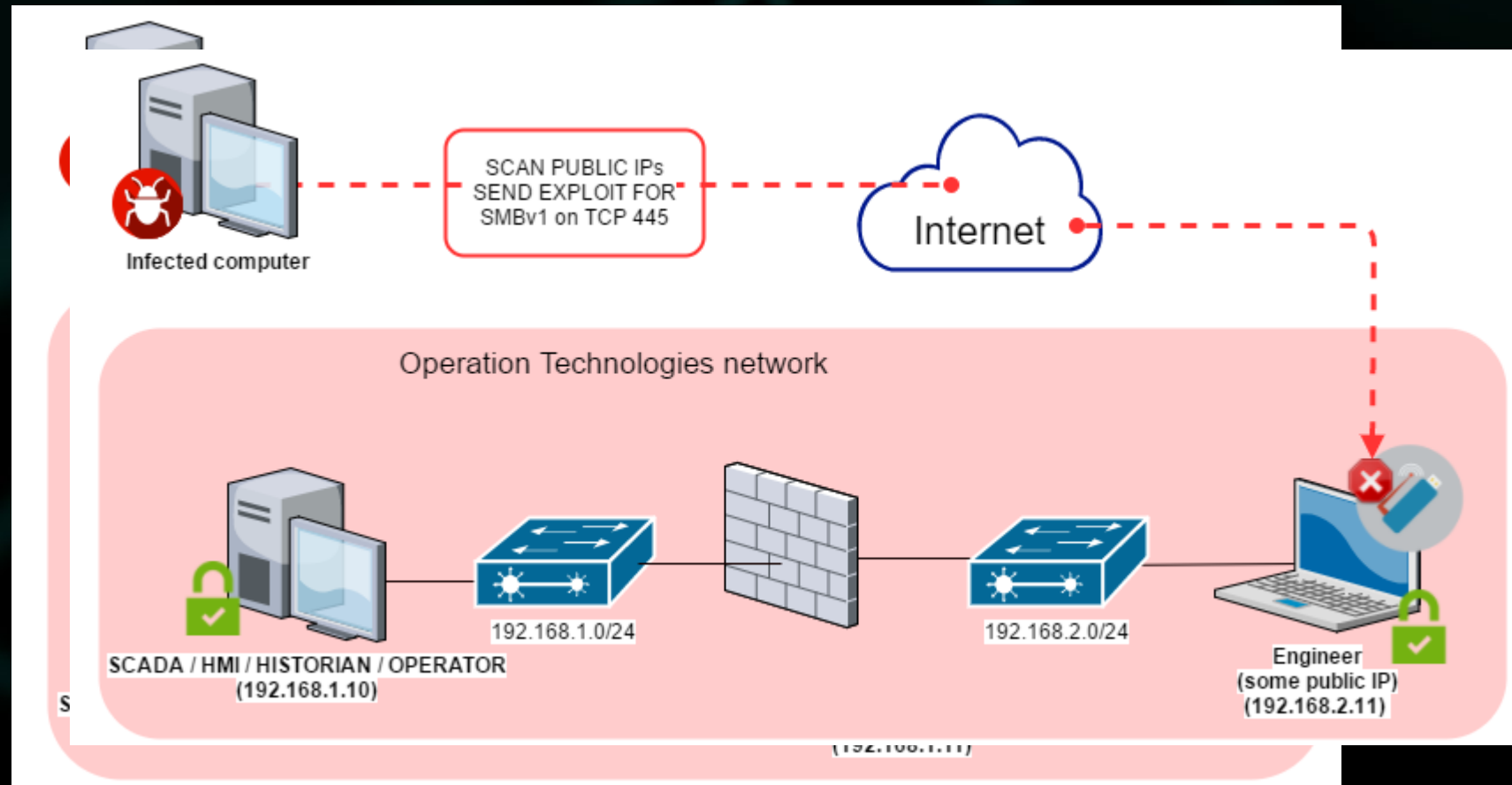
Реальность:

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

Хронология заражения



Другие способы инфицирования



Но это еще не все....

Re: New Order P08112016 - URGENT - Daily

FTP Explorer	Epic	Bitcoin Armory
Frigate3 FTP	Staff-FTP	PPCoin (Peercoin)
SecureFX	AceFTP	Primecoin
UltraFXP	Global Downloader	Feathercoin
FTPRush	FreshFTP	NovaCoin
WebSitePublisher	BlazeFTP	Freicoins
BitKinex	NETFile	Devcoin
ExpanDrive	GoFTP	Frankocoin
ClassicFTP	3D-FTP	ProtoShares
Fling	Easy FTP	MegaCoin
SoftX	Xftp	Quarkcoin
Directory Opus	FTP Now	Worldcoin
FreeFTP / DirectFTP	Robo-FTP	Infinitecoin
LeapFTP	LinusFTP	Ixcoin
WinSCP	Cyberduck	Anoncoin
32bit FTP	Putty	BBQcoin

Что делать?

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

sn = 000
ie = 2010-11-
160.188.116 pi
24 m = 537 ms
nection Clos
150.11.28

An aerial photograph of a city skyline at sunset. The sun is low on the horizon, casting a warm orange glow over the city. The sky is filled with scattered clouds, some of which are illuminated by the setting sun. The city buildings are silhouetted against the bright sky. In the foreground, a large, modern building with a curved facade is visible. The overall scene is a mix of urban architecture and natural light.

WE PROTECT WHAT MATTERS MOST

KASPERSKY LAB