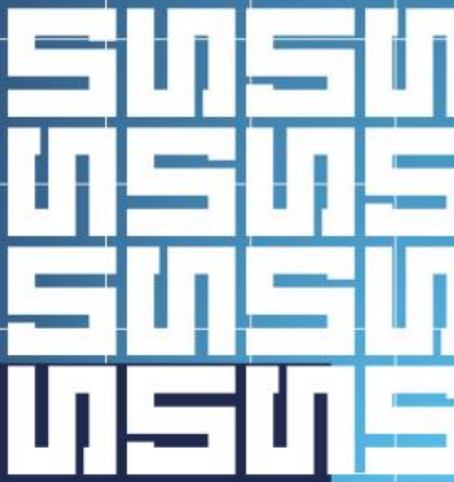
SOC Tech

Технологии SOC



Доверяй, но проверяй: Расследования Trusted Relationship атак

Михаил Прохоренко,
Руководитель управления по борьбе с киберугрозами BI.ZONE

Что происходит?

Количество trusted relationship атак неуклонно растет.

Тренды этого года:

- Атаки через хостинг провайдеров
- Атаки через провайдеров услуг IT сопровождения
- Атаки через провайдеров облачных сервисов
- ...

Что дальше?

Кто за этим стоит?

Как защищаться?

Начало истории

Крупная организация, зрелая система безопасности.

- На сервере с базой данных клиентского портала обнаружено исполнение подозрительных команд.
- unset HISTFILE – отключает запись команд в историю, иногда используется админами.
- Активность происходит ночью, с Proton VPN
- Для подключения используется ключ подрядчика

Трудности

Одна из главных трудностей расследования атак на доверенные отношения – необходимость уговорить на расследование вторую сторону (подрядчика).

Что выяснили?

- Некто ломает сервера Bitrix
- Выбирает компании которые делают/поддерживают сайты, обслуживают инфраструктуру
- Выясняет, кого обслуживает подрядчик
- Крадет ключи для доступа к инфре заказчиков
- Подключается, сливает данные
- Шантажирует/просит выкуп/деньги за раскрытие информации об уязвимости

TTPs

Техника	Реализация
Эксплуатация уязвимостей (T1190)	Bitrix
Кража учетных данных (T1555)	Ключи SSH
Зачистка логов (T1070)	unset HISTFILE, wtmp
Разведка сети (T1046)	nmap
Доступ в сеть через хакерские утилиты (T1588.002)	Использует исключительно gsocket и ProtonVPN
Кража данных через веб-сервис (T1041)	Устанавливает Adminer для выгрузки баз данных

TTPs

- gsocket (https://github.com/hackerschoice/gsocket)
  - Очень удобная утилита для атакующих
  - Скачивание и закрепление на системе одной командой
  - Работает через публичные relay-серверы
  - Доступ внутрь сети по паролю (который также одновременно ID)

TTPs

- Adminer (https://www.adminer.org/)
  - Популярная утилита для работы с
- В ней было много уязвимостей раньше
- Сейчас атакующие ей не очень часто пользуются
  - Зачем, если есть DBeaver etc.
- Но наш хакер ее любит

Атакующий зачищает историю, но у нас есть EDR

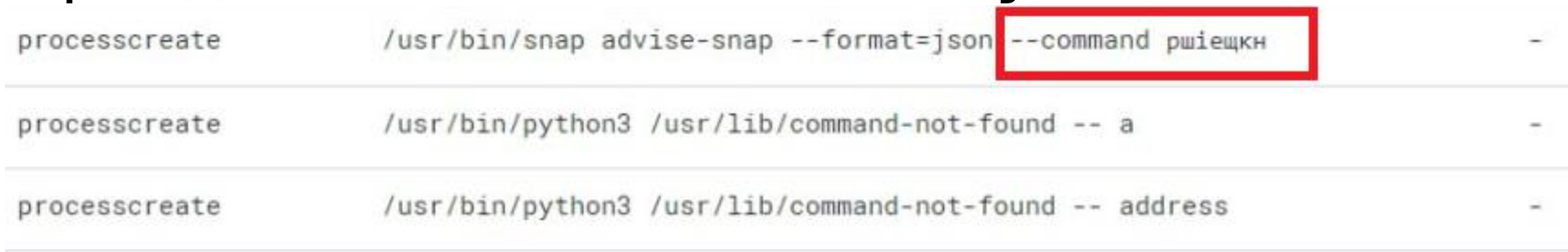
consolecommand	unset HISTFILE; unset SSH_CONNECTION; unset SSH_CLIENT ; unset LC_TERMINAL; unset LC_TERMINAL_VERSION
processcreate	/usr/bin/xauth -q -
processcreate	sh -c '/usr/bin/xauth -q -'
consolecommand	history -c

Схема атаки

- Пробивает Bitrix
- Заходит, ставит gsocket
- Исследует логи/файловую систему в поисках паролей/ключей
- Заходит к клиентам подрядчика с украденными ключами
- Сливает данные
- Базы через Adminer, файлы через SSH/gsocket

Атрибуция

- Похоже на Leak Wolf (NLB) (сначала нам так показалось)
- Но по факту нет
- Правда какой-то момент атакующий забыл



UA

- Каких-либо других IOC`ов (домены, IP) пока что нет

Атрибуция

- Инструментарий атаки пересекается Sneaking Leprechaun
- Общая схожесть действий атакующих
- В одном из инцидентов атакующие удалили бекдор Kitsune
  - Взамен него установили gsocket

Атрибуция

Профиль группировки Sneaking Leprechaun:

- Активны с середины 2022 года
- Для проникновения в сеть используют уязвимости Bitrix, Confluence и Webmin
- Крадут данные и требуют выкуп за их сохранение в тайне
- Для закрепления используют Rootkit собственной разработки: Kitsune (основан на коде RAT Azazel)

Что в итоге

- Провели расследование у клиента и подрядчика
- Часто подрядчик не хочет/не может позволить себе расследование
- Атаки на подрядчика — супер-выгодно для атакующих
- Профит атакующего гарантирован, можно взломать еще десяток компаний (легко)
- Известные хакерские группировки пополняют свои арсеналы этим типом атак

Вывод

Тренд сохранится и количество таких атак будет лишь возрастать

Как защищаться?

- Настраивать максимальную сетевую изоляцию систем подрядчика/заказчика
- Доступ только по 2FA
- Разграничение доступа пользователей
- Перенос киберрисков на уровне договоров с подрядчиками

- Подключать централизованный мониторинг
  - EDR/auditd/другое
  - Сетевой трафик к/от публичных VPN

SOC Tech

Технологии SOC

Вопросы/ответы?