4RAYS by SOLAR

Как понять, что вашу инфраструктуру атаковала кибергруп-пировка

Памятка Solar 4RAYS

W: RT-SOLAR.RU/SOLAR-4RAYS

Содержание

Признаки атаки

1

Обращение из инфраструктуры компании к известным сетевым индикаторам компрометации

Как обнаружить:

- Мониторинг SOC
- Проактивные действия штатных ИБ-специалистов
- Уведомления от ИБ-провайдеров/вендоров
- Уведомление от госорганов [1]

[1] Например, в одном из расследований заказчик получил уведомление от НКЦКИ о множественных фактах обращения из его инфраструктуры к доменным именам, являющимся командными адресами одной из отслеживаемых нами APT-группировок

2

Подозрительная активность в корпоративной инфраструктуре

Как обнаружить:

- Пропал доступ к каким-либо системам и сервисам
- Активность учетных записей в нехарактерные временные промежутки
- Доступ учетных записей к системам, с которыми они обычно не взаимодействуют
- Сообщения сотрудников об аномальном поведении используемых устройств (например: «курсор самостоятельно двигался по экрану»)
- Разрушение ИТ-инфраструктуры (шифрование или удаление данных)
- Сообщения о публикации данных в открытом доступе [2]
- Обнаружение следов вредоносной активности по результатам проведения процедуры оценки компрометации инфраструктуры

[2] Именно так началось расследование нескольких атак, за которыми стояла группировка Shedding Zmiy. Атаки могут обсуждаться на форумах в даркнете, в Telegram-каналах и других соцсетях

Где искать следы

Если сосредоточиться на следах первоначального проникновения, то в зависимости от выбранной злоумышленниками техники их можно обнаружить в системах:

- На которых развернуты уязвимые версии публично доступных приложений
- Доступных пользователям, которым были разосланы фишинговые письма
- К которым имеют доступ подрядные организации в рамках доверительных отношений

Дальнейшее продвижение в инфраструктуре жертвы и, соответственно, наличие следов зависит от мотивации злоумышленников.

Мотивация	Цель атаки
Шпионаж	[01] Организация-подрядчик • Разведка и сбор информации о компании • Получение доступов к инфраструктурам клиентов [02] Системы, содержащие ценные данные: • Системы электронного документооборота • Базы знаний (аналогичные Confluence) • Репозитории (GitHub, Gitlab) • Файловые серверы • Гипервизоры • Пользовательские системы, в том числе привилегированных пользователей
Уничтожение информационной инфраструктуры	Максимальный контроль над сетью: получение доступа к привилегированным учетным записям и ключевым системам (контроллер домена, системы управления виртуализацией, серверы бэкапов, системы оркестрации контейнеров, критические с точки зрения бизнес-процессов сервисы и т. д.)

Как распознать профессиональных хакеров

Признаки APT-группировки:

Уникальные инструменты (самописные бэкдоры и другие утилиты)

Сложность техник и процедур, например:

- эксплуатация уязвимостей, для которых нет публичных proof-of-concept (POC)
- закрепление в системе в нетипичных местах
- supply chain compromise
- использование непопулярных техник (типа Execution Guard Rails: вредоносные файлы запускаются только на определенных хостах)

Как хакеры прячутся в инфраструктуре, или методы маскировки APT-группировок

[01]

Шифрование строк

[02]

Обфускация файлов

[03]

Точечность атаки

[04]

Наличие большого количества проверок жертвы

[05]

Ограничение доступа к серверу управления по географическому местоположению или другим параметрам

[06]

Максимальная скрытность

Распространенные техники и тактики известных APT-группировок

Закладки в легитимных утилитах (sshd и другие)

Использование редких уязвимостей (пример: десериализация VIEWSTATE)

Supply Chain attack (пример: xz backdoor)

Социальная инженерия (целевой фишинг)

Эксплуатация уязвимостей в проприетарном ПО, используемом в атакованной организации

Использование в качестве серверов управления легитимных сервисов и оборудования (Telegram, Github, Youtube, облачные хранилища, оборудование для управления лифтами и т. д.)

Эксплуатация особенностей протоколов не по их прямому назначению (icmp-, DNS-туннелирование)

Эксплуатация непопулярных протоколов (QUIC, MQTT) для связи с серверами управления

APT-группировки обладают практически неограниченными ресурсами и постоянно совершенствуют свои тактики, техники и процедуры, чтобы быть на шаг впереди стороны защиты

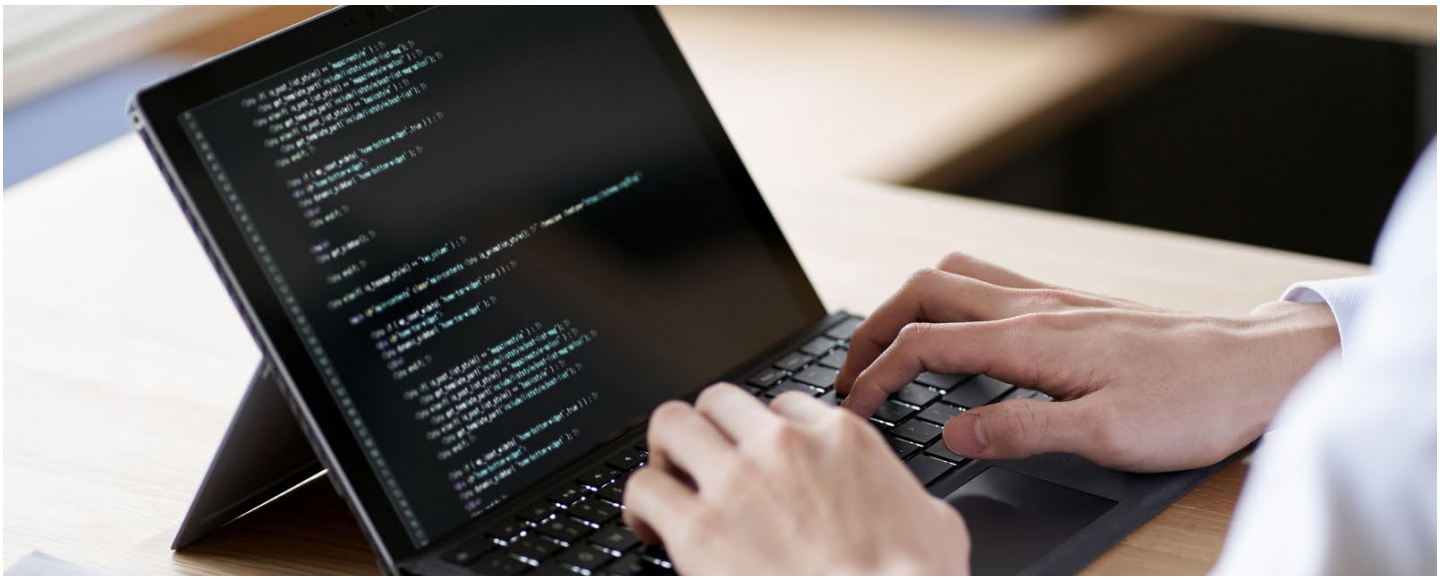
Инструменты, которые применяют группировки

Решения для туннелирования трафика, которые позволяют обойти файрволы и организовать связь там, где ее не должно быть:

- gsocket (gs-netcat)
- ngrok
- nhas reverse ssh
- revsocks
- resocks
- chisel
- neo-regeorg

Различные RAT-утилиты, предоставляющие удаленное управление хостом жертвы:

- Bulldog backdoor (go-red)
- Facefish rootkit
- Kitsune rootkit
- Sliver
- CobInt
- Cobalt Strike
- Mythic
- DFK RAT
- Trochilus RAT
- Donnect
- Dimano RAT



Как защититься

Чтобы повысить уровень киберзащиты компании, стоит применять следующие практики, актуальные для противодействия как APT-угрозам, так и массовым кибератакам:

1

Досконально знать свою инфраструктуру, все используемые в ней технологии, публично доступные приложения, связи собственной инфраструктуры с другими и т. д.

2

Оперативно обновлять все используемое в инфраструктуре ПО (системное, прикладное, средства защиты)

3

ИБ-служба должна регулярно обновлять свои знания о ландшафте киберугроз конкретного региона (штудировать публичные отчеты, можно приобрести подписку на TI-платформы, предоставляемые вендорами) и проактивно подходить к процессу защиты

4

Применять лучшие практики для организации удаленного доступа в инфраструктуру как собственных работников, так и подрядных организаций

5

Грамотно подходить к вопросу создания резервных копий данных [1]

[1] Например, использовать правило “3-2-1”, которое гласит: имейте не менее трех копий данных, храните копии как минимум на двух физических носителях разного типа, одну копию храните удаленно, вне офиса

6

Регулярно повышать уровень осведомленности сотрудников по вопросам ИБ, проводить обучения, делать тестовые фишинговые рассылки и т. п.

7

Постоянно проводить мониторинг активности в инфраструктуре и использовать средства защиты:

- Настроить аудит
- Внедрить SIEM-систему
- Внедрить EDR-решения для защиты рабочих станций
- Внедрить решения для детектирования/блокировки атак на сетевом уровне (IDS/IPS/NTA/NGFW)

Чтобы поймать атаку «на подлете», необходим мониторинг SOC и применение комплексных защитных решений, которые получают регулярные обновления детектирующих логик и контента, созданных на основе анализа актуальных киберугроз.

Если у вас есть подозрения, что в вашей инфраструктуре «поселились» агенты группировки, которые пока себя не проявили, и есть риск шпионажа или блокировки инфраструктуры, проводите регулярные работы по выявлению следов компрометации инфраструктуры (Compromise Assessment). Они могут выполняться как внешней экспертной командой (сервис-провайдера), так и силами самой компании (если у нее есть собственный SOC и команда реагирования).

Выявление следов компрометации с командой Solar 4RAYS

Поможем обнаружить признаки присутствия злоумышленников в инфраструктуре до наступления последствий

Провести оценку компрометации

О команде центра исследования киберугроз Solar 4RAYS:

200+

Расследований инцидентов различной сложности, включая продвинутые атаки группировок иностранных спецслужб

10+ лет

Практического опыта отражения атак и изучения тактик киберпреступников любого уровня

60+

Профессиональных группировок в поле зрения

4RAYS by SOLAR

Доступ к крупнейшей в РФ базе знаний о киберугрозах