АННОТАЦИЯ СТАТЬИ SOLAR 4RAYS

REIGN OF KING: ТАКТИКИ И ИНСТРУМЕНТАРИЙ ГРУППИРОВКИ OBSTINATE MOGWAI

В этой статье мы, команда Solar 4RAYS, рассказываем историю наших расследований атак группировки Obstinate Mogwai. В фокусе – три инцидента в трех разных организациях.

Краткое описание

В ПЕРВОМ ИНЦИДЕНТЕ
Цель: телеком-компания

После подключения мы обнаружили, что группировка находится в сети организации почти два года. Сохранившиеся артефакты позволили проследить эволюцию ее инструментария и тактик, а также собрать информацию, которая помогает определить присутствие группировки в атакованной сети и противодействовать ей.

ВО ВТОРОМ ИНЦИДЕНТЕ
Цель: государственная организация

Атакующие проникли через подключение по VPN, используя скомпрометированную учетную запись. После запуска нескольких исполняемых скриптов они столкнулись с уже закрытой нами уязвимостью и не смогли продолжить атаку.

В ТРЕТЬЕМ ИНЦИДЕНТЕ
Цель: госкомпания атакована через доступы подрядчика

Мы столкнулись со своего рода уникальным случаем. Благодаря тому что в организации работала PAM-система Solar SafeInspect, нам удалось получить видеозапись действий атакующих: как они в удаленном режиме просматривали конфиденциальные документы, чтобы сделать скриншоты или записать скринкаст.
В этом случае злоумышленники не использовали никакого специфического ВПО, а только пользовались имеющимся доступом к атакованной системе и легитимными инструментами удаленного доступа.

ДОПОЛНИТЕЛЬНО

Кроме того, масштабное исследование деятельности группировки позволило нам обнаружить ее связь с другими азиатскими APT-группами.
В частности, с IAmTheKing, APT 31, Hafnium и Space Pirates.

Узнайте, как противодействовать
и получите индикаторы компрометации.

Читать статью

Для кого будет полезна статья

Threat Hunters и реверс-инженеры
Примеры анализа вредносного ПО

Threat-Intelligence-аналитики
Исследование артефактов деятельности и вредоносных инструментов киберпреступников для поиска новых атак и определения известных группировок

DFIR-специалисты
Анализ TTП атакующих, который пригодится в повседневной работе

Руководители ИБ- и ИТ-подразделений, профильные специалисты в области информационной безопасности
Практические знания, которые позволят быть в курсе актуальных кибеугроз

Если вы увидели подозрительную активность в своей сети и считаете, что тоже стали жертвой хакерской группировки, то узнайте, как Solar 4RAYS поможет обнаружить скрытую атаку.

4RAYS by SOLAR