4RAYS by SOLAR

ХРОНИКИ ЦЕЛЕВЫХ КИБЕРАТАК 2024

Аналитика, кейсы и рекомендации

Спикеры

РОМАН ДОЛГИЙ

Руководитель направления
специальных сервисов Solar JSOC

ГЕННАДИЙ САЗОНОВ

Инженер группы расследования
инцидентов Solar 4RAYS

План вебинара

4RAYS by SOLAR

[01] О центре исследований Solar 4RAYS

[02] Аналитика целевых атак в I полугодии 2024

- Атакованные отрасли
- Кто атакует. Длительность атак
- Векторы проникновения

[03] Разборы кейсов расследований

- Атакующие группировки и особенности атак
- Необычные тактики и техники

[04] Выводы и рекомендации

[05] Ответы на вопросы

Solar 4RAYS. Всегда актуальные знания об угрозах

4RAYS by SOLAR

ВНУТРЕННИЕ ИСТОЧНИКИ

200+ МЛРД

событий в сутки регистрируют автоматизированные сенсоры

3+ МЛН

сработок в сутки на автоматизированных сенсорах

1+ МЛН

действий злоумышленников фиксирует сеть ханипотов

200+

проведенных расследований

600+

проектов по оценке защищенности (от пентеста до эмуляции APT-атак)

ДАННЫЕ ТЕЛЕМЕТРИИ

фиксирует сеть ханипотов

ВНЕШНИЕ ИСТОЧНИКИ

100+

специализированных сайтов, блогов и других ресурсов

200+

новостей о киберугрозах в месяц

Команды Solar 4RAYS

THREAT HUNTING

- Атакованные отрасли
- Кто атакует. Длительность атак
- Векторы проникновения

DIGITAL FORENSIC

- Расследование инцидентов
- Выявление следов компрометации (Compromise Assessment)
- Рекомендации по повышению защищенности на основе данных расследований и Compromise Assessment

THREAT INTELLIGENCE

- Отслеживание группировок
- Анализ инструментария
- Мониторинг инфраструктуры злоумышленников

РЕДАКЦИЯ БЛОГА SOLAR 4RAYS

- Выпуск статей и отчетов об актуальных киберугрозах

Поставка знаний об актуальных киберугрозах

4RAYS by SOLAR

АНАЛИЗ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ

- Оценка данных на релевантность
- Ретроспективный анализ событий

АНАЛИЗ ИНСТРУМЕНТАРИЯ ЗЛОУМЫШЛЕННИКОВ

- Reverse Engeneering, статический и динамический анализ вредоносного кода
- Выявление особенностей, известного почерка

АНАЛИЗ ТАКТИК И ТЕХНИК ЗЛОУМЫШЛЕННИКОВ

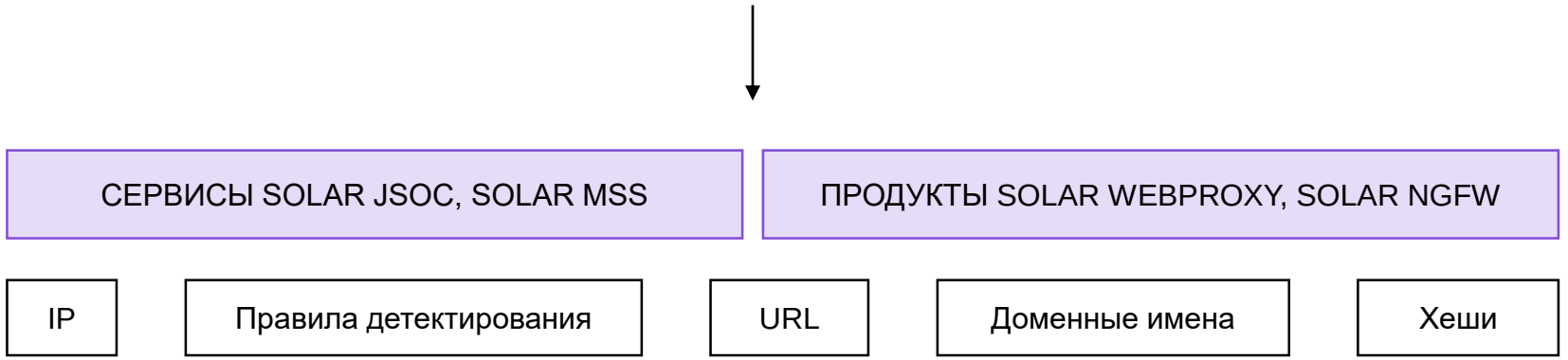
- Оценка данных
- Воспроизведение в лабораторных условиях

АНАЛИЗ ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ

- Оповещение с рекомендациями

ФОРМИРОВАНИЕ ПРАВИЛ ДЕТЕКТИРОВАНИЯ ДЛЯ ХОСТОВОЙ И СЕТЕВОЙ ЧАСТИ

ФОРМИРОВАНИЕ ПРОФИЛЯ ИНФРАСТРУКТУРЫ И ЕГО РАСШИРЕНИЕ



4RAYS by SOLAR

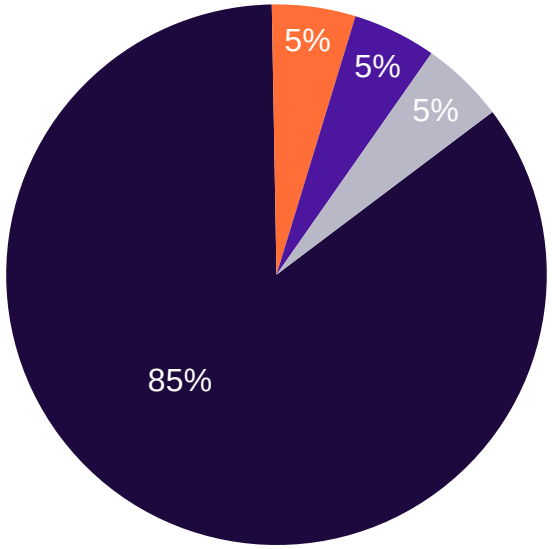
АНАЛИТИКА ЦЕЛЕВЫХ КИБЕРАТАК 2024

Главные изменения киберландшафта целевых атак

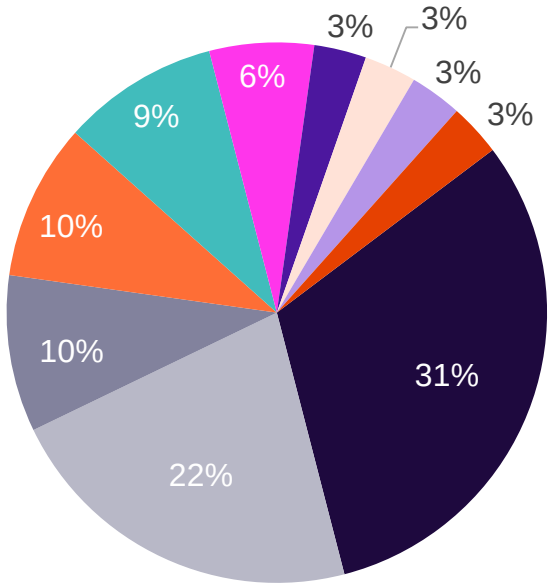
Атакованные отрасли

- Государственные организации
- Промышленность
- ИТ-разработка
- Телеком
- Облачные провайдеры
- Здравоохранение
- Общественные организации
- Финансовый сектор
- Образование
- Логистика

I ПОЛУГОДИЕ 2023 ГОДА



I ПОЛУГОДИЕ 2024 ГОДА



Источник: отчет Solar 4RAYS

ПРИЧИНЫ УВЕЛИЧЕНИЯ РАЗНООБРАЗИЯ ОТРАСЛЕЙ

К нам стали чаще обращаться:
за проверкой компрометации инфраструктуры,
за проведением расследования инцидента

В 2023–2024 году проукраинские группировки взламывают буквально все, до чего могут дотянуться

Типы атакующих

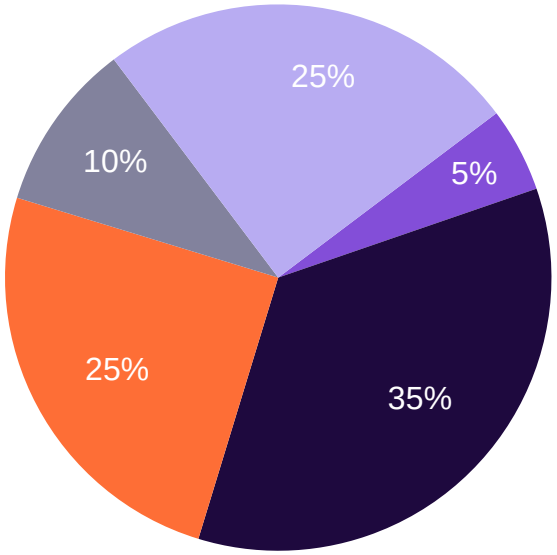
4RAYS by SOLAR

[1 УРОВЕНЬ] АВТОМАТИЧЕСКИЕ СКАНЕРЫ И МАССОВЫЕ ЗАРАЖЕНИЯ	Ищут IT-инфраструктуры с низким уровнем защиты для дальнейшей перепродажи информации о них или использования в массовых атаках
[2 УРОВЕНЬ] КИБЕРХУЛИГАНЫ И ХАКТИВИСТЫ	Ищут стандартные уязвимости с целью прокачки своих навыков и мелкого хулиганства. Редко самостоятельно занимаются монетизацией взлома. Используют общедоступные инструменты для анализа защищенности. Нередко мотивируют свои атаки политическими причинами
[3 УРОВЕНЬ] КИБЕРМОШЕННИКИ	Цель – прямая финансовая выгода путем кражи денег, получения выкупа и использования вычислительных мощностей атакуемой компании для майнинга криптовалютных активов. Часто объединяются в организованные группировки
[4 УРОВЕНЬ] КИБЕРНАЕМНИКИ	Действуют в интересах заказчика либо охотятся за крупной монетизацией, например, за счет продажи базы клиентских данных в даркнете. Объединяются в иерархические группы, самостоятельно разрабатывают инструменты и методики взлома
[5 УРОВЕНЬ] ПРОПРАВИТЕЛЬСТВЕННЫЕ ГРУППИРОВКИ	Служат интересам государственных структур. Ориентированы на перехват полного контроля над инфраструктурой. Отличаются максимально длительным скрытым присутствием внутри периметра

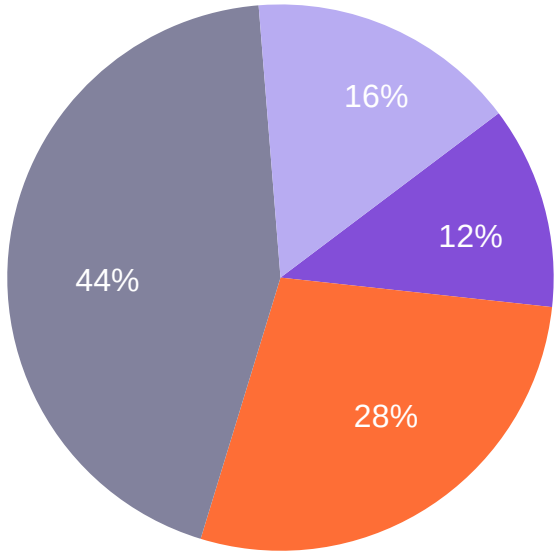
Уровни атакующих: изменения за год

Проправительственные группировки
Киберхулиганы/Хактивисты
Кибермошенники
Кибернаемники
Автоматические сканеры / массовые заражения

I ПОЛУГОДИЕ 2023 ГОДА



I ПОЛУГОДИЕ 2024 ГОДА

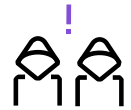


Источник: отчет Solar 4RAYS

Уровни атакующих: изменения за год

Уровень атакующих	Первая половина 2023 года	Первая половина 2024 года
Автоматические сканеры / массовые заражения	5%	12%
Киберхулиганы/Хактивисты	35%	0%
Кибермошенники	25%	28%
Кибернаемники	10%	44%
Проправительственные группировки	25%	16%

Каждая четвертая атака имеет финансовые мотивы



Рост доли кибернаемников обусловлен в основном ростом активности группировки Shedding Zmiy

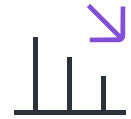
Российским организациям в основном угрожают группировки из Азии и Восточной Европы (Украины)

Источник: отчет Solar 4RAYS

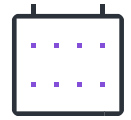
Длительность атак: изменения за год

Уровень атакующих	Первая половина 2023 года	Первая половина 2024 года
До 1 недели	20%	34%
До 2 недель	10%	13%
До 1 месяца	20%	6%
До 6 месяцев	30%	19%
До 1 года	10%	13%
До 2 лет	10%	6%
2+ года	-	9%

Примерно треть инцидентов длилась не больше недели. В 2023 году доля таких инцидентов была ниже на 14 п. п.



Доля инцидентов, в которых атакующие оставались в целевой сети от одного до шести месяцев, упала на 11 п. п. – до 19%
Причина: организации учатся быстрее реагировать на аномалии в своих ИТ-инфраструктурах



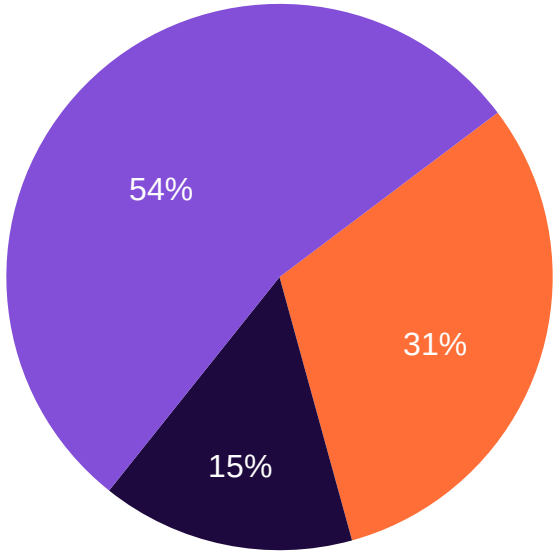
В 2024 году также обнаружились инциденты, длившиеся два года и больше.
В первой половине 2023 года примеров столь длительных операций эксперты Solar 4RAYS не наблюдали

Источник: отчет Solar 4RAYS

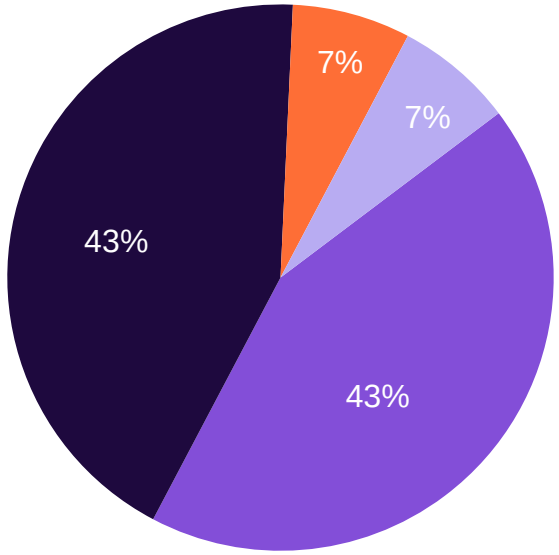
Способы проникновения в инфраструктуру

- Уязвимость в веб-приложении
- Скомпрометированные аккаунты
- Фишинг
- Доверительные отношения

I ПОЛУГОДИЕ 2023 ГОДА



I ПОЛУГОДИЕ 2024 ГОДА



Источник: отчет Solar 4RAYS

Тренды за период июль-август 2024

4RAYS by SOLAR

СОХРАНЯЕТСЯ ТРЕНД НА РАЗНООБРАЗИЕ АТАКУЕМЫХ ОТРАСЛЕЙ
Например, одна из расследованных нами атак была направлена
на религиозную организацию

ВСЕ ТОТ ЖЕ ТОП-3 СПОСОБОВ ПРОНИКНОВЕНИЯ В ИНФРАСТРУКТУРУ
1-ое место Уязвимость веб-приложений
2-ое место Скомпрометированные аккаунты
3-ое место Фишинг и Доверительные отношения

ХАКТИВИСТЫ ПРОЯВИЛИСЬ ВО ВТОРОМ ПОЛУГОДИЕ
Более 2 атак

4RAYS by SOLAR

РАЗБОРЫ КЕЙСОВ РАССЛЕДОВАНИЙ 2024

Группировки и особенности атак.
Необычные тактики и техники

АТАКУЮЩИЕ ГРУППИРОВКИ И ОСОБЕННОСТИ АТАК 2024

Группировка Lifting Zmiy

4RAYS by SOLAR

ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка (предположительно украинская)

УРОВЕНЬ

Проправительственные группировки

ЦЕЛИ АТАК

Шпионаж и уничтожение инфраструктуры

ЖЕРТВЫ

Телеком-провайдер, государственные организации

КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

- mig-logcleaner
- NHAS/reverse_ssh
- ssh-it
- ssh-snake
- Empire
- Responder
- proxychains3
- crackmapexec
- kerbrute

ОСОБЕННОСТИ АТАК

- Не применяет сложные техники Initial Access, полагается на «слитые» аккаунты
- Использует оборудование для управления лифтами для размещения C2

ДЕТАЛИ РАССЛЕДОВАНИЯ

Подробный разбор и рекомендации по обнаружению атак Lifting Zmiy в блоге Solar 4RAYS

Группировка Shedding Zmiy

4RAYS by SOLAR

ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка (предположительно украинская)

УРОВЕНЬ

Кибернаемники

ЦЕЛИ АТАК

Шпионаж и уничтожение инфраструктуры

ЖЕРТВЫ

ИТ-компании, компании энергетического сектора и государственные организации

КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

- Mimikatz
- SoftPerfect Network Scanner
- nmap
- fscan
- Psexec
- RemCom
- ssh-snake
- chisel
- resocks
- gsocket
- Metasploit
- Sliver
- Cobalt Strike
- Bulldog Backdoor

ОСОБЕННОСТИ АТАК

- Наращивают арсенал, начинают использовать ПО, которое ранее не использовали. В этом полугодии наблюдали еще не описанный в наших предыдущих статьях образец – SparkRAT
- Применяют опыт TTP-групп из других регионов:
  - утилиты fscan
  - техники DLL sideloading
  - эксплуатация уязвимости десериализации ViewState, активное злоупотребление которой с 2020 года свойственно азиатскими группировками

ДЕТАЛИ РАССЛЕДОВАНИЯ

Разборы расследований 7 кейсов атак. К статье →

Разбор: как Shedding Zmiy использует недозакрытую уязвимость Microsoft. К статье →

Углубленный технический анализ инструментария Shedding Zmiy. К статье →

Инструкция по обнаружению эксплуатации уязвимостей из арсенала Shedding Zmiy. К статье →

Группировка Obstinate Mogwai

ПРОИСХОЖДЕНИЕ

Азиатская группировка

УРОВЕНЬ

Проправительственные группировки

ЦЕЛИ АТАК

Шпионаж

ЖЕРТВЫ

Государственные организации
и их подрядчики

КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

- Donnect (новое семейство)
- DimanoRAT (новое семейство)
- Nbtscan
- SharpHound
- CMPSpy
- RDCMan
- SmbExec
- Azazel
- Venom proxy
- Inveigh
- Antak
- SessionGopher
- dns-dump
- autokerberoast

ОСОБЕННОСТИ АТАК

- Используют кастомное ВПО
- Атакуют не только государственные организации, но и их подрядчиков для дальнейшего злоупотребления доверительными отношениями между инфраструктурами
- Применяют различные техники, присущие азиатским APT
- Эксплуатируют уязвимости десериализации ViewState

ДЕТАЛИ РАССЛЕДОВАНИЯ

Разбор: как уязвимость десериализации ViewState играет на руку группировкам в блоге Solar 4RAYS

Группировка Moonshine Trickster (Werewolves)

ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка

УРОВЕНЬ

Кибермошенники

ЦЕЛИ АТАК

Финансовая выгода

ЖЕРТВЫ

Государственные, коммерческие организации и все, кто заплатит

КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

- LockBit
- Cobalt Strike

ОСОБЕННОСТИ АТАК

- Атакуют через spear-фишинг с вредоносными rtf-файлами
- Шифруют инфраструктуру и вымогают деньги

Группировка Morbid Trickster (Morlock)

ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка (предположительно украинская)

УРОВЕНЬ

Кибермошенники

ЦЕЛИ АТАК

Финансовая выгода

ЖЕРТВЫ

Государственные, коммерческие организации и все, кто заплатит

КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

- LockBit
- Babuk
- Anydesk
- Ngrok
- Mimikatz
- Sliver
- Localtonet
- gsocket
- Meterpreter
- Chisel
- Resocks
- Facefish
- SoftPerfect Network Scanner
- XenAllPasswordPro

ОСОБЕННОСТИ АТАК

- Шифруют инфраструктуру и вымогают выкуп
- Ненадолго задерживаются в инфраструктуре:
  – от 2 недель до 2 месяцев длительность атак
- Имеется сильное пересечение индикаторов с Shedding Zmiy

Группировка Fairy Trickster (Head Mare)

ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка (предположительно украинская)

УРОВЕНЬ

Кибермошенники

ЦЕЛИ АТАК

Финансовая выгода, но также известны кейсы уничтожения данных

ЖЕРТВЫ

Государственные, коммерческие и все, кто заплатит

КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

- PhantomRAT
- другие

ОСОБЕННОСТИ АТАК

- Мы обнаружили только фишинговые рассылки на своих заказчиков, которые не привели к развитию таких атак, в связи с этим не располагаем полным набором тактик, техник и процедур группы
- По заявлениям других компаний, фишинг с указанным инструментом они атрибутируют группе Head Mare (название одноименного Telegram-канала)
- Указанная группа взяла на себя ответственность за громкую атаку на логистическую компанию в конце мая 2024 года. В результате атаки была приостановлена деятельность компании на несколько недель

Группировка NGC4020

ПРОИСХОЖДЕНИЕ

Пока неизвестно

УРОВЕНЬ

Пока неизвестно

ЦЕЛИ АТАК

Построение ботнета.
Пока мы не наблюдали попыток продвижения вглубь инфраструктуры или какого-то деструктивного воздействия

КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

- QuasarRAT
- java-reverse-tcp
- Кастомная утилита для обхода АВПО

ОСОБЕННОСТИ АТАК

- Для первоначального проникновения использовался эксплойт для приложения, публично доступного по нестандартному порту
- После успешной атаки на системах размещались утилиты QuasarRAT и реверс-шелл на java. Обе указанные утилиты размещаются в свободном доступе, в связи с чем атрибуцию по ним проводить не имеет смысла
- Также в атаках использовалась кастомная утилита для обхода АВПО, эксплуатирующая уязвимость CVE-2023-36802 в драйвере MSKSSRV.SYS driver

4RAYS by SOLAR

НЕОБЫЧНЫЕ ТАКТИКИ И ТЕХНИКИ АТАК 2024

Запись экрана для сбора конфиденциальных данных, или как Solar SafeInspect помог расследовать атаку

4RAYS by SOLAR

АТАКУЮЩИЕ

[01]

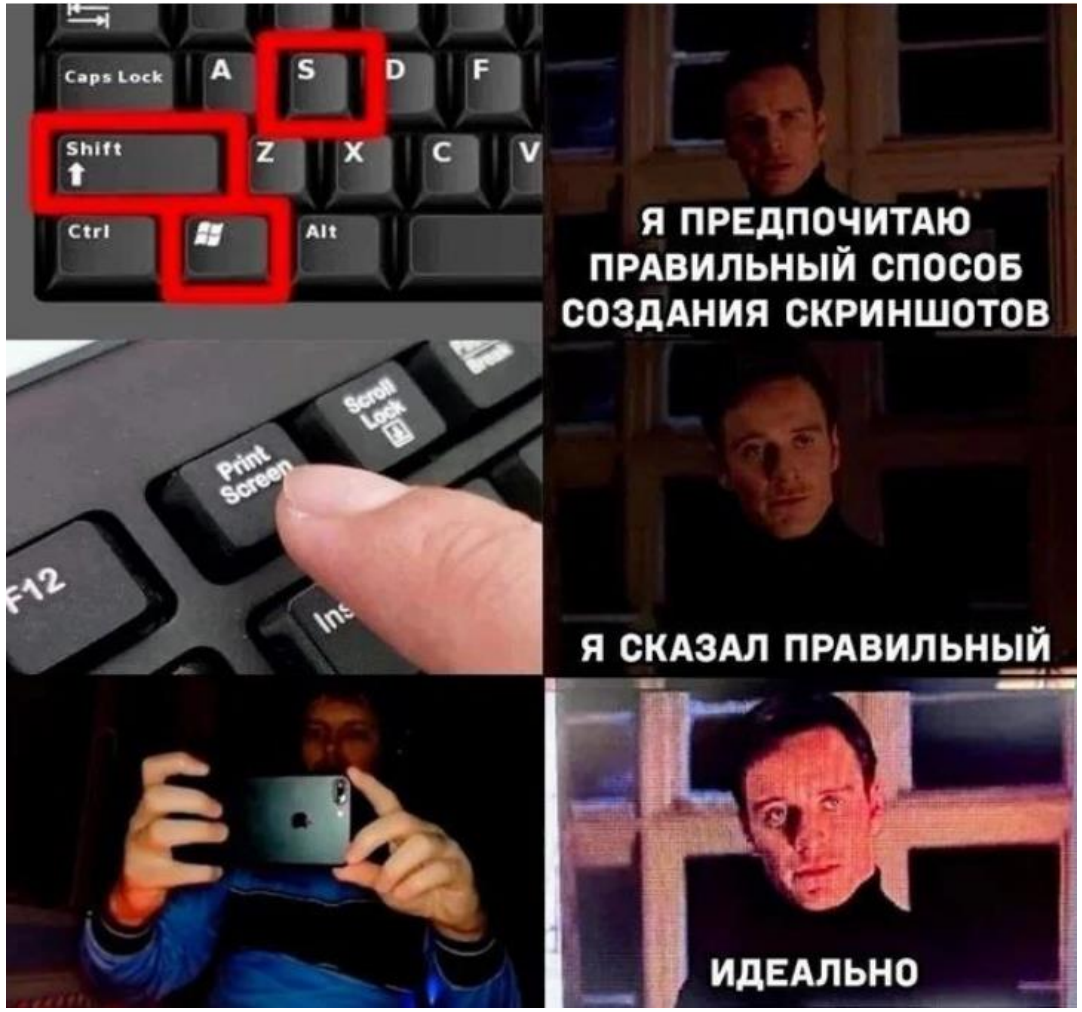
Получают доступ от имени привилегированной УЗ подрядчика к терминальному серверу

[02]

Тут же получают доступ к конфиденциальным документам жертвы, которая использует этот сервер для доступа к системе электронного документооборота

[03]

Не подозревают, что данная RDP-сессия была записана PAM-системой Solar SafeInspect



При просмотре записи было отчетливо видно, как атакующие открывали документы интересующей их тематики и постранично их просматривали, делая паузы на несколько секунд, с высокой долей вероятности именно в этот момент они делали скриншоты или вовсе вели запись экрана на системе, с которой осуществлялась атака

Заражение легитимных утилит в атаках Shedding Zmiy

4RAYS by SOLAR

Подмена атакующими на Linux-машинах легитимных утилит ps, ss, netstat и htop на «пропатченные»

В выводе результатов работы этих утилит скрывались данные о вредоносной утилите gs-netcat, используемой атакующими

```
filtering_proc_name_value dq offset aAcpi
                                        ; DATA XREF: mw_check_filtering_value+7↑o
                                        ; "^acpi"
                dq offset aAcpi_0       ; "acpi"
                dq offset aAcpi_1       ; "[acpi]"
                dq offset unk_427C78
                dq offset unk_427C8C
                dq offset unk_427CA0
                dq offset unk_427CB4
                dq offset unk_427CC8
                dq offset unk_427CDC
                dq offset C2
                dq 0
filtering_c2_value dq 0                 ; DATA XREF: main:loc_401630↑o
                dq offset aRlsUpdRknNet ; "rls.upd-rkn.net"
                dq offset a892311325    ; "89.23.113.25"
                dq offset aMtpUpdRknNet ; "mtp.upd-rkn.net"
                dq offset a91219150197  ; "91.219.150.197"
```

Любопытная техника отключения защитного решения в одном из расследований инцидента

4RAYS by SOLAR

Обход защиты exploitation for defense evasion id: t1211 – не самая популярная техника, по нашему опыту, но имеет интересную реализацию

1

Атакующие загрузили на хост исполняемый файл, предназначенный для эксплуатации уязвимости повышения привилегий CVE-2023-36802

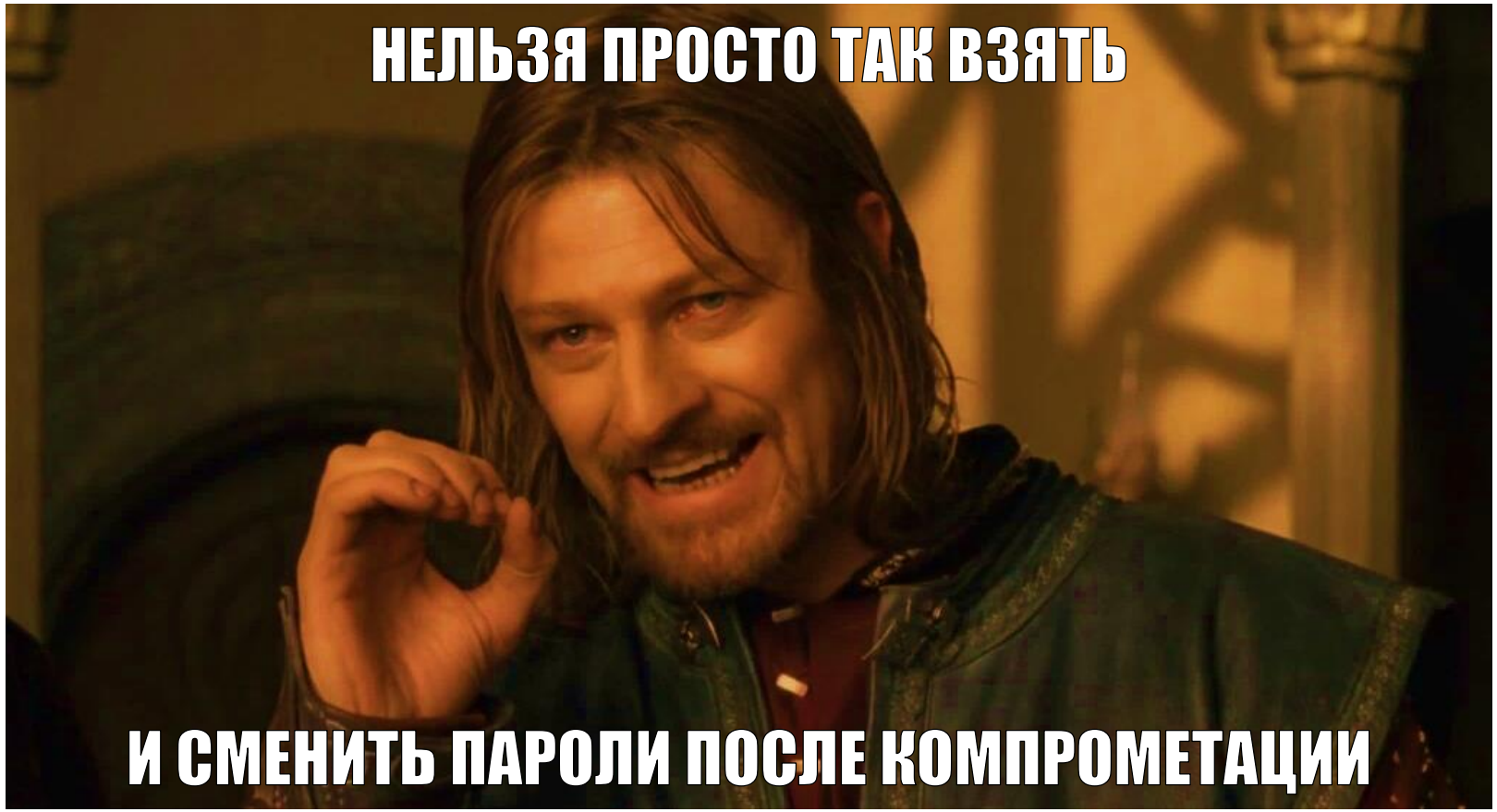
2

После запуска файла в каталог установки антивирусного решения загружался драйвер с расширением .sys, который запускался службой ZeroRingProxy

3

В результате действий атакующих защитные компоненты решения отключались

Старая УЗ – подходящая УЗ



В одном из кейсов для первоначального доступа использовалась легитимная учетная запись, скомпрометированная год назад!

Случай, подчеркивающий важность регулярной смены учетных данных в корпоративных (да и не только) инфраструктурах

Выводы

СЛОЖНОСТЬ АТАК РАСТЕТ, А УРОВЕНЬ ЗАЩИЩЕННОСТИ – НЕ ВСЕГДА

ЦЕЛЬЮ МОЖЕТ СТАТЬ ЛЮБАЯ ОРГАНИЗАЦИЯ, ТАК КАК ПРОУКРАИНСКИЕ АТАКУЮЩИЕ СИСТЕМАТИЧЕСКИ ВЗЛАМЫВАЮТ САМЫЕ РАЗНЫЕ ОТРАСЛИ

ОРГАНИЗАЦИЯМ НУЖНО ЭВОЛЮЦИОНИРОВАТЬ, ЧТОБЫ БЫТЬ ГОТОВЫМИ К УГРОЗАМ

Рекомендации

КОНТРОЛЬ ОБНОВЛЕНИЙ

Проводить регулярную инвентаризацию используемого ПО и оперативно его обновлять

ПОСТОЯННОЕ ОБУЧЕНИЕ СОТРУДНИКОВ

Регулярно повышать уровень осведомленности сотрудников по вопросам ИБ:

- Проводить обучения
- Делать тестовые фишинговые рассылки и т. п.

УДАЛЕННЫЙ ДОСТУП И ВЗАИМОДЕЙСТВИЕ С ПОДРЯДЧИКАМИ

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

БЭКАПЫ ДЛЯ СОХРАННОСТИ БИЗНЕС-ПРОЦЕССОВ

Грамотно подходить к вопросу создания резервных копий данных. Например, использовать правило «3-2-1», которое гласит: имейте не менее трех копий данных, храните копии как минимум на двух физических носителях разного типа, а одну копию храните удаленно, вне офиса

КОНТРОЛЬ ПЕРИМЕТРА И ДОСТАТОЧНОСТИ СРЕДСТВ ЗАЩИТЫ

Постоянно проводить мониторинг активности в инфраструктуре и использовать продвинутые средства защиты. Настроить аудит, внедрить SIEM-систему и EDR-решения для защиты рабочих станций

ПРОКАЧКА TI ЭКСПЕРТИЗОЙ ИЗ ПУБЛИЧНЫХ И НЕПУБЛИЧНЫХ ИСТОЧНИКОВ

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

В СЛУЧАЕ ПОДОЗРЕНИЙ НА АТАКУ НЕ МЕДЛИТЬ С ПРОВЕДЕНИЕМ ОЦЕНКИ КОМПРОМЕТАЦИИ ИНФРАСТРУКТУРЫ

Практика расследований Solar 4RAYS показывает, что вовремя проведенная оценка компрометации позволяет остановить атаку с потенциально катастрофическими последствиями еще на начальной стадии

4RAYS by SOLAR

Больше кейсов, расследований и других практических материалов

Опыт, факты и знания об актуальных киберугрозах

[Получить новые знания]

[Провести оценку компрометации]