4RAYS by SOLAR

# ЧТО НУЖНО ЗНАТЬ О ЦЕЛЕВЫХ КИБЕРАТАКАХ 2024

[Аналитика и кейсы]

2025

# План вебинара

[01] О ЦЕНТРЕ ИССЛЕДОВАНИЙ SOLAR 4RAYS

[02] АНАЛИТИКА ЦЕЛЕВЫХ КИБЕРАТАК В 2024

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

[03] РАЗБОР 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

## ВНУТРЕННИЕ ИСТОЧНИКИ

**200+ МЛРД**

событий в сутки регистрируют автоматизированные сенсоры

**3+ МЛН**

подтвержденных инцидентов в сутки на основе данных автоматизированных сенсоров

**1+ МЛН**

действий злоумышленников фиксирует сеть ханипотов

**200+**

проведенных расследований

**600+**

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

## ДАННЫЕ ТЕЛЕМЕТРИИ

от собственных СЗИ и сервисов ИБ

## ВНЕШНИЕ ИСТОЧНИКИ

**100+**

специализированных сайтов, блогов и других ресурсов

**200+**

новостей о киберугрозах в месяц

# Команды Solar 4RAYS

## THREAT HUNTING

Разработка детектирующей логики на хостовом и сетевом уровне на основе постоянного анализа публичных и приватных TI/DFIR-отчетов

Формирование и проверка гипотез по детектированию и поиску актуальных/продвинутых техник и ВПО

Исследование эффективности различных методов обнаружения угроз в различных ОС

## DIGITAL FORENSIC

Расследование инцидентов

Выявление следов компрометации (Compromise Assessment)

Рекомендации по повышению защищенности на основе данных расследований и Compromise Assessment

## THREAT INTELLIGENCE

Сбор, анализ и обогащение данных – формирование TI Feeds

Отслеживание группировок, выявление их тактик, техник, мотивации, целей атак

Анализ инструментария группировок

## **РЕДАКЦИЯ БЛОГА SOLAR** 4RAYS

Выпуск статей и отчетов об актуальных киберугрозах

# Поставка знаний об актуальных киберугрозах

## АНАЛИЗ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ

Сбор, обработка, категоризация и оценка релевантности данных

Ретроспективный анализ событий

## АНАЛИЗ ИНСТРУМЕНТАРИЯ ЗЛОУМЫШЛЕННИКОВ

Статический и динамический анализ вредоносного кода

Выявление особенностей, известного почерка

## АНАЛИЗ ТАКТИК И ТЕХНИК ЗЛОУМЫШЛЕННИКОВ

Сбор, обработка и обогащение данных

Воспроизведение в лабораторных условиях

## АНАЛИЗ ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ

Оповещения о новых уязвимостях, наличии для них PoC, а также методах смягчения

**СВЕДЕНИЯ О ВРЕДОНОСНОМ ПО И СЕТЕВОЙ ИНФРАСТРУКТУРЕ АТАКУЮЩИХ**
**ПРАВИЛА ОБНАРУЖЕНИЯ УГРОЗ В СЕТЕВОМ ТРАФИКЕ И В СОБЫТИЯХ НА ХОСТАХ**

↓

СЕРВИСЫ SOLAR JSOC, SOLAR MSS

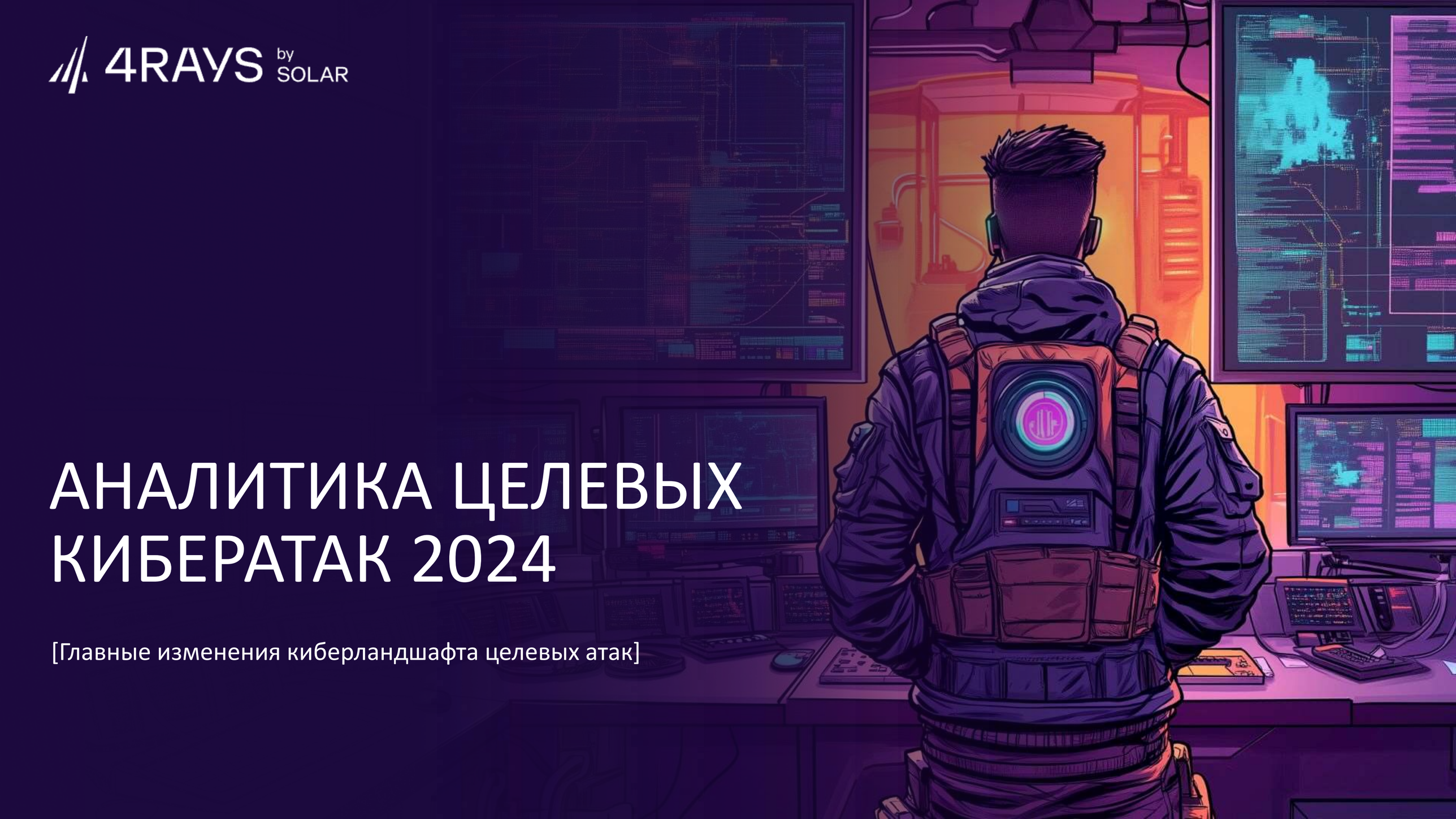
ПРОДУКТЫ SOLAR WEBPROXY, SOLAR NGFW

IP | URL | Доменные имена | Хеши | Правила детектирования

4RAYS by SOLAR

# АНАЛИТИКА ЦЕЛЕВЫХ КИБЕРАТАК 2024

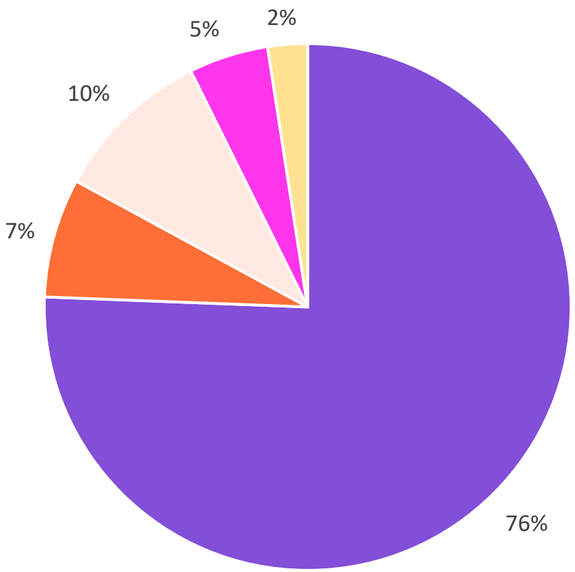
[Главные изменения киберландшафта целевых атак]



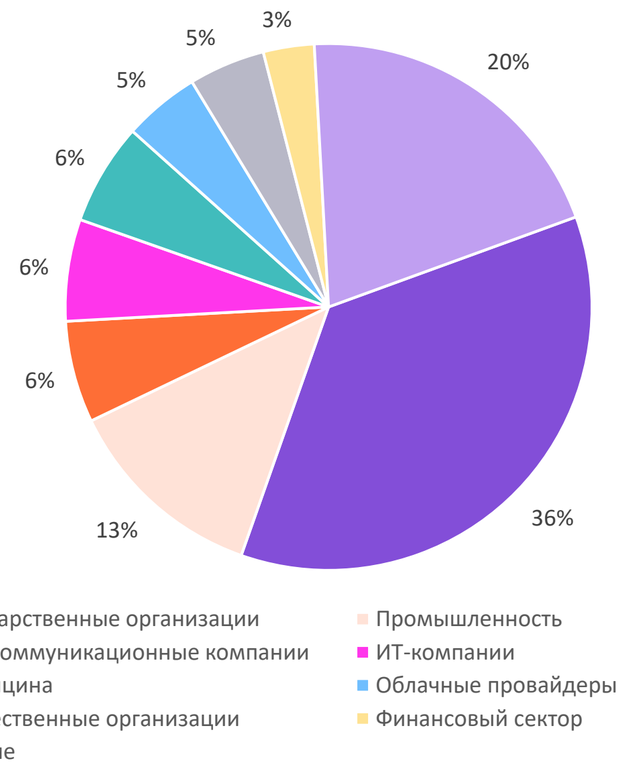
# Атакованные отрасли

Злоумышленники (особенно заявляющие о действиях в интересах Украины) стараются атаковать гораздо более широкий спектр организаций, в безопасности которых им удалось обнаружить дыры, а не только «традиционные» цели из госсектора и промышленности.

## 2023 год




## 2024 год

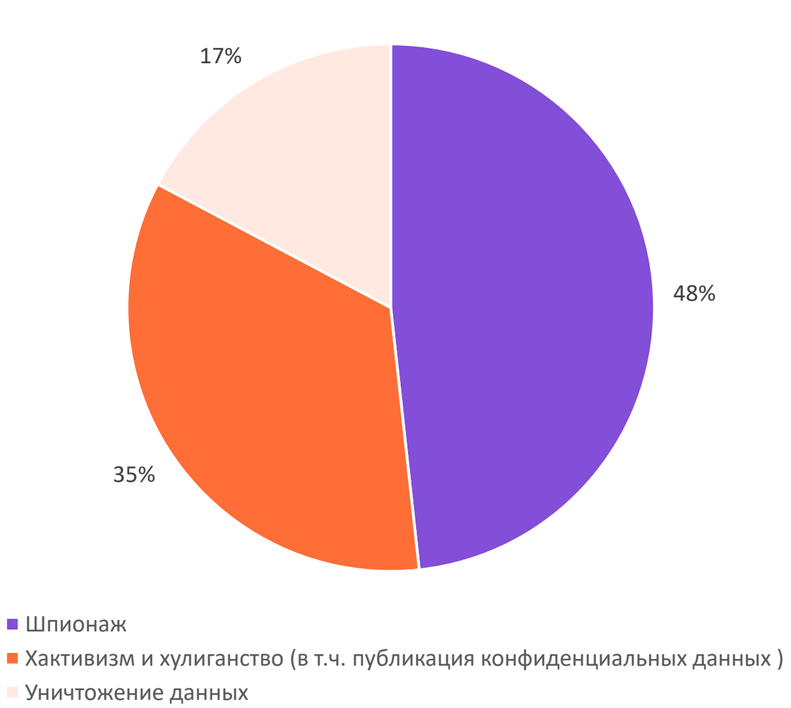



Источник: отчет Solar 4RAYS

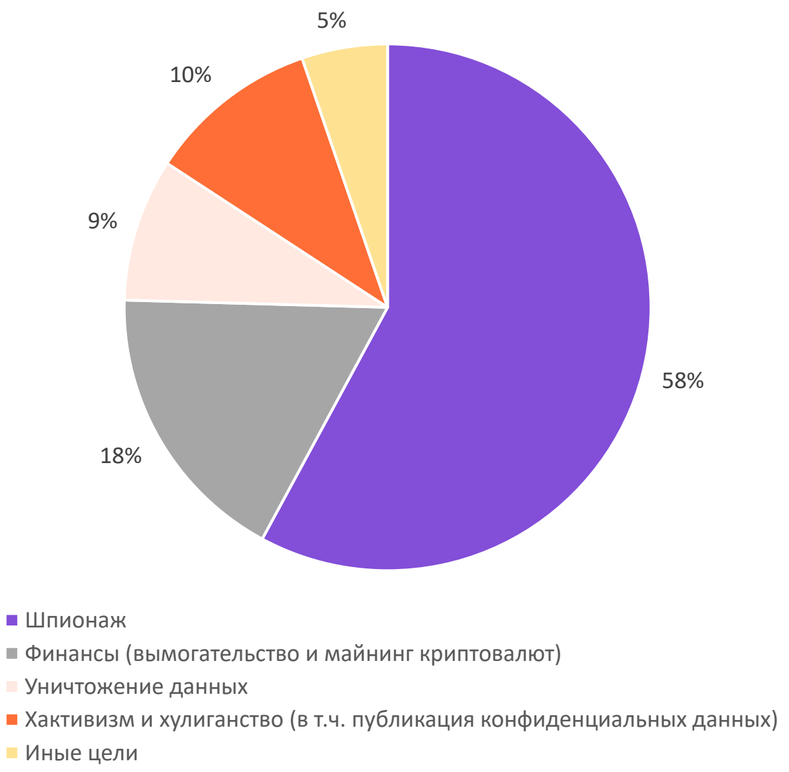
# Цели атакующих

Хищение чувствительной информации в больших объемах (шпионаж) — главная цель атакующих в 2024 году.

## 2023 год




## 2024 год



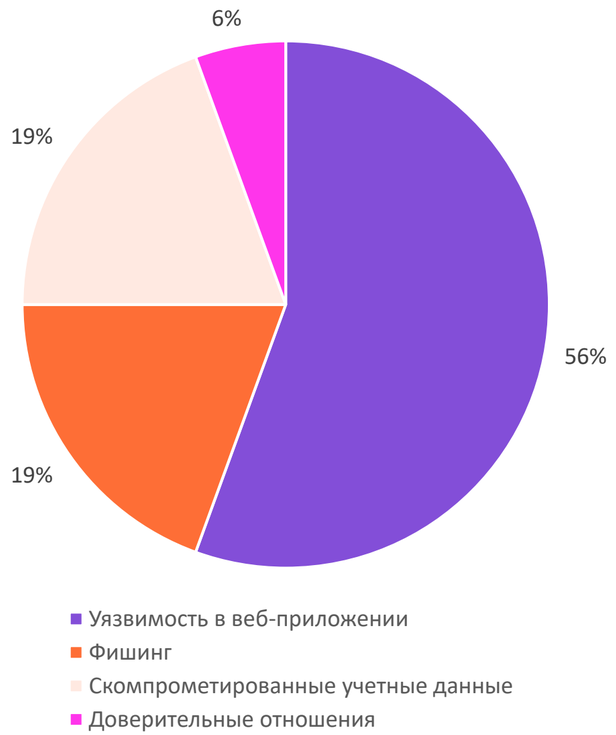

Источник: отчет Solar 4RAYS

# Способы проникновения в инфраструктуру

Самым распространенным способом первоначального проникновения в атакованные инфраструктуры второй год остаются уязвимости в корпоративных приложениях, доступных из интернета (почтовые серверы, отдельные компоненты веб-серверов, базы данных, системы контроля версий, трекеры задач, базы знаний и т. д.).

Однако в 2024 году доля таких инцидентов сократилась на 10 процентных пунктов, до 46%.

## 2023 год




## 2024 год


Источник: отчет Solar 4RAYS

# Длительность инцидентов

В 2024 году было выявлено больше атак, продолжительность которых не превышала недели. Годом ранее большая часть атак длилась от 1 до 6 месяцев с момента первичного проникновения до реализации.

Также мы стали выявлять больше атак длительностью до двух лет и более – в 2023 году на их долю пришлось 13%, а в 2024 – уже 25%.

В этом году мы участвовали в расследовании нескольких атак, продолжительность которых составляла около 3,5 лет, а в одном случае следы компрометации имеют возраст более семи лет.

| Длительность | 2023 | 2024 |
|---|---|---|
| До недели | 22% | 25% |
| До двух недель | 8% | 13% |
| До месяца | 16% | 7% |
| До шести месяцев | 35% | 21% |
| До года | 6% | 9% |
| До 2-х лет | 5% | 14% |
| 2+ года | 8% | 11% |

Источник: отчет Solar 4RAYS

# Тренды 2024

## ТОП-3 СПОСОБОВ ПРОНИКНОВЕНИЯ В ИНФРАСТРУКТУРУ: ФИШИНГ УСТУПИЛ СКОМПРОМЕТИРОВАННЫМ АККАУНТАМ

- 1-е место: уязвимость веб-приложений
- 2-е место: скомпрометированные аккаунты
- 3-е место: фишинг

Проникновение через злоупотребление доверительными отношениями не занимает ведущую позицию в статистике, однако не стоит недооценивать этот вектор получения первоначального доступа.

Практически всегда подрядчики имеют привилегированные учетные записи, а иногда и права на выполнение различного рода действий. И доступ к различным системам и сегментам сети оказывается избыточным.

Также трудности в выявлении нелегитимной активности таких УЗ связаны с возможностью выполнения подрядных работ в любое время суток.

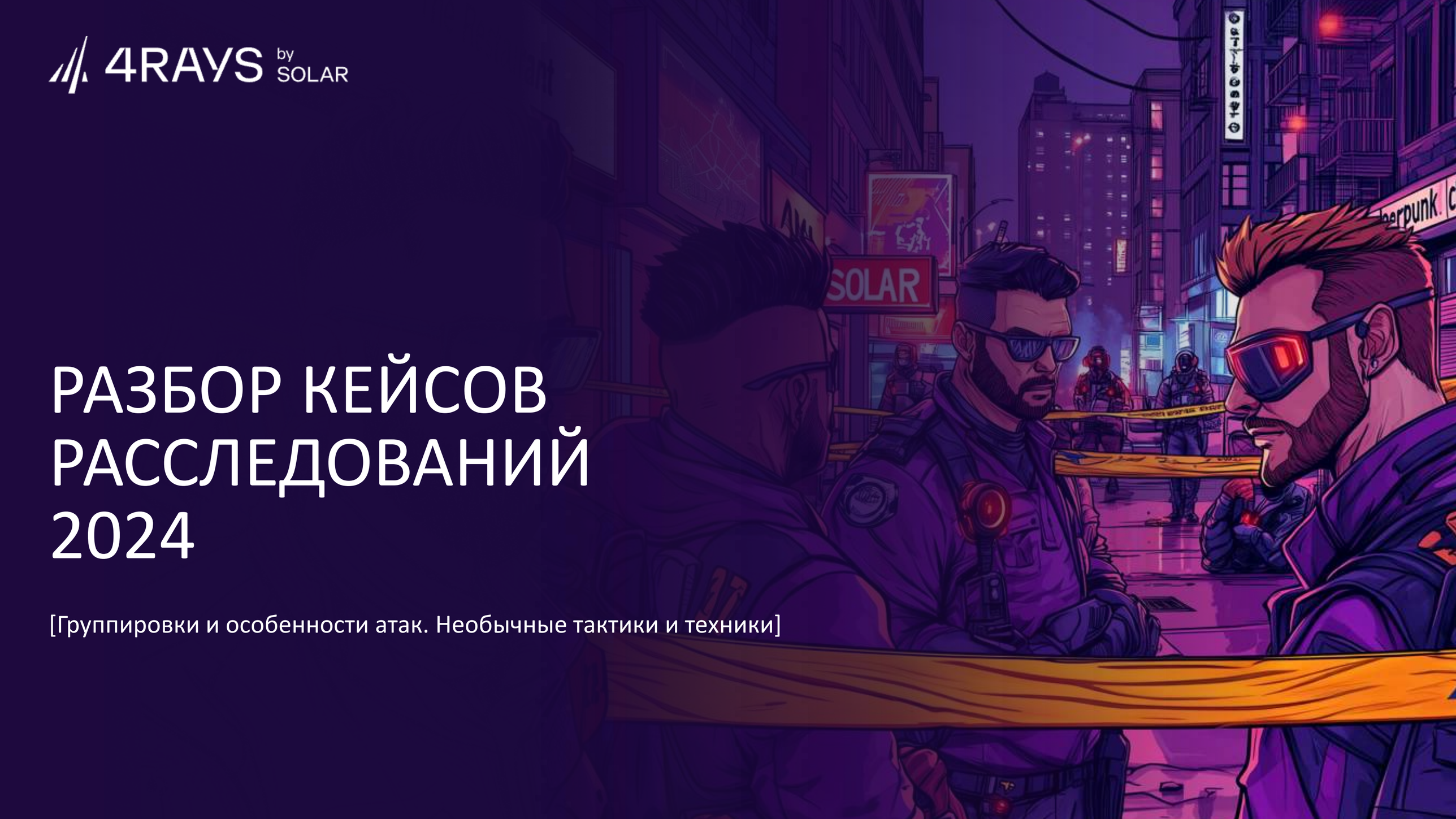
## СОХРАНЯЕТСЯ ТРЕНД НА РАЗНООБРАЗИЕ АТАКУЕМЫХ ОТРАСЛЕЙ

Например, одна из расследованных нами атак была направлена на религиозную организацию.

## ВРЕМЯ МЕЖДУ ПУБЛИКАЦИЕЙ PoC И НАЧАЛОМ «БОЕВОЙ» ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ СОКРАЩАЕТСЯ

Некоторые группировки стараются максимально оперативно эксплуатировать свежие уязвимости. Атакующим нужно всего несколько часов, чтобы взять Proof-of-concept и использовать его в реальных атаках, пользуясь тем, что многие могли не успеть применить патчи безопасности.

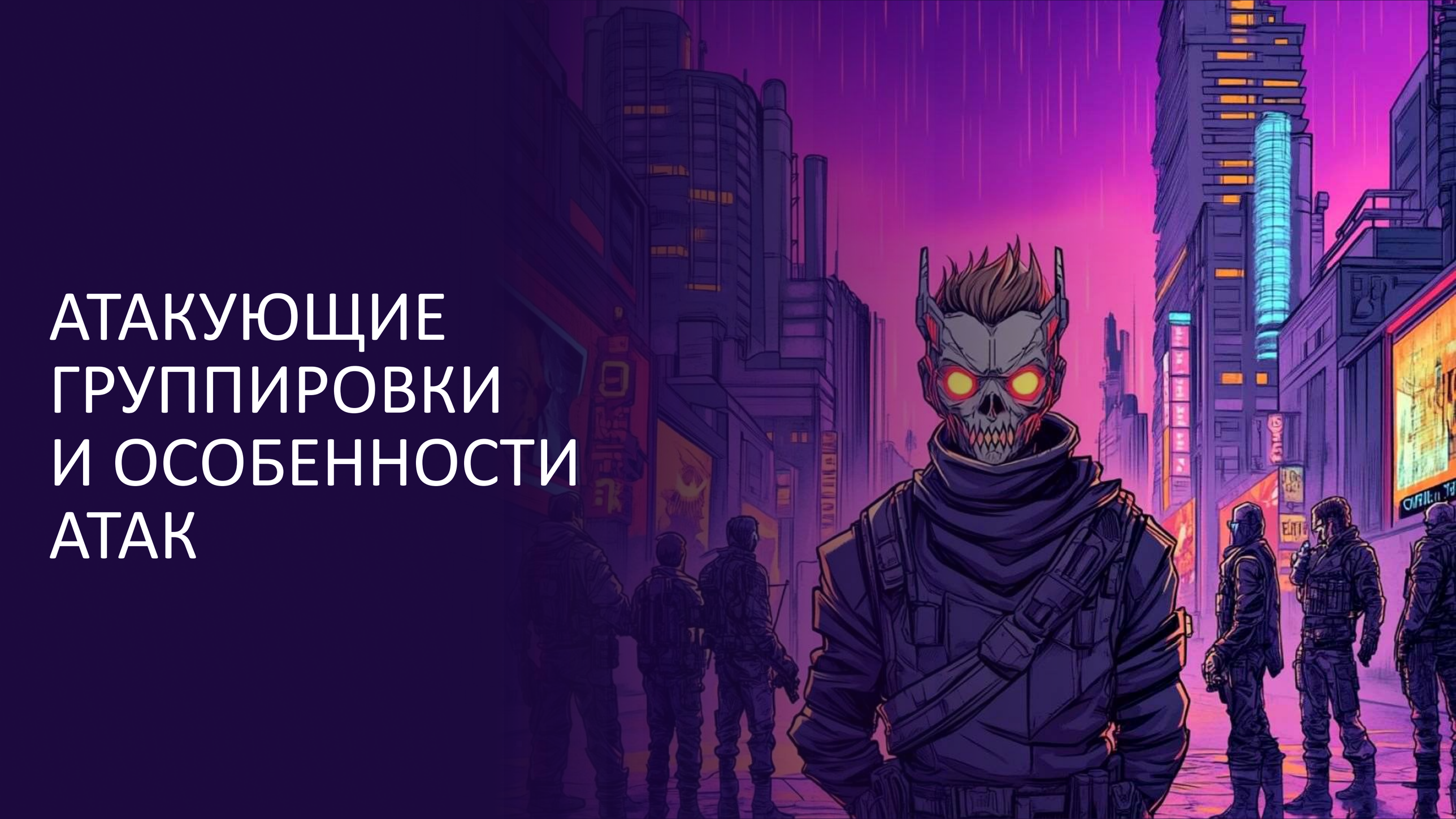
4RAYS by SOLAR




# РАЗБОР КЕЙСОВ РАССЛЕДОВАНИЙ 2024

[Группировки и особенности атак. Необычные тактики и техники]

# АТАКУЮЩИЕ ГРУППИРОВКИ И ОСОБЕННОСТИ АТАК



# Shedding Zmiy

## ЦЕЛИ АТАК

Шпионаж и уничтожение инфраструктуры

## ЖЕРТВЫ

ИТ-компании, компании энергетического сектора, телеком, государственные организации и т. д.

## ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка (предположительно украинская)

## КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

Puma/Kitsune (Новое)

Bulldog Backdoor

Gsocket

Facefish

Sliver

Mimikatz

SoftPerfect Network Scanner

nmap

fscan

Psexec

RemCom

ssh-snake

chisel

resocks

Metasploit

Cobalt Strike

## ОСОБЕННОСТИ АТАК

Наращивают арсенал, начинают использовать ПО, которое ранее не использовали. В 24 году наблюдали еще не описанный в наших предыдущих статьях образец – SparkRAT. В конце года обнаружили новый руткит Puma/Kitsune.

Применяют опыт APT-групп из других регионов:

- утилиты fscan- техники DLL sideloading
- эксплуатация уязвимости десериализации ViewState, активное злоупотребление которой с 2020 года свойственно азиатским группировкам

## ДЕТАЛИ РАССЛЕДОВАНИЯ

Разбор 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 →

# Lifting Zmiy

## ЦЕЛИ АТАК

Шпионаж и уничтожение инфраструктуры

## ЖЕРТВЫ

Телеком-провайдер, государственные организации

## ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка (предположительно украинская)

## КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

mig-logcleaner

NHAS/reverse_ssh

ssh-it

ssh-snake

Empire

Responder

proxychains3

crackmapexec

kerbrute

## ОСОБЕННОСТИ АТАК

Не применяют сложные техники Initial Access, полагаются на «слитые» аккаунты.

Используют оборудование для управления лифтами для размещения C2.

## ДЕТАЛИ РАССЛЕДОВАНИЯ

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


# Obstinate Mogwai

## ЦЕЛИ АТАК

Шпионаж

## ЖЕРТВЫ

Государственные организации
и их подрядчики

## ПРОИСХОЖДЕНИЕ

Азиатская группировка

## 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

Профиль группировки: в блоге Solar 4RAYS →

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

# Erudite Mogwai (AKA SPACE PIRATES)

## ЦЕЛИ АТАК

Шпионаж

## ЖЕРТВЫ

Государственные организации, ИТ-компании, авиационно-космическая и электроэнергетическая индустрии, научно-исследовательские институты.

## ПРОИСХОЖДЕНИЕ

Азиатская группировка

## КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

LuckyStrike Agent – многофункциональный бэкдор на .NET, способный использовать OneDrive в качестве C2.

Shadowpad Light (aka Deed RAT)

Кастомный Stowaway – пентест-утилита, из функциональности которой оставлено SOCKS5-прокси. Используется для продвижения в сети жертвы.

Различные open-source-утилиты для сканирования сети и KeyLogger

## ОСОБЕННОСТИ АТАК

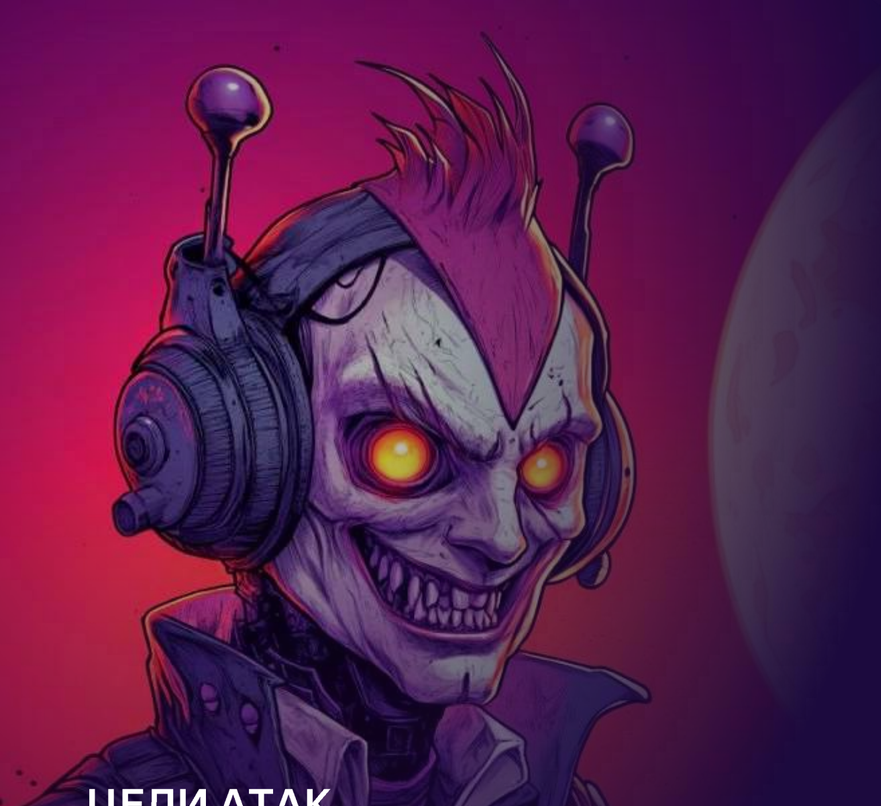
Используют кастомное ВПО.

Особенность со строчками в Stowaway и отсылками к популярным произведениям.

Применяют различные техники, присущие азиатским APT.

## ДЕТАЛИ РАССЛЕДОВАНИЯ

Разбор характерных черт группировки и эволюция версий Stowaway в блоге Solar 4RAYS →



# Moonshine Trickster (AKA WEREWOLVES)

## ЦЕЛИ АТАК

Финансовая выгода

## ЖЕРТВЫ

Государственные, коммерческие организации и все, кто заплатит

## УРОВЕНЬ

Кибермошенники

## ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка

## КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

LockBit

Cobalt Strike

## ОСОБЕННОСТИ АТАК

Атакуют через spear-фишинг с вредоносными rtf-файлами.

Шифруют инфраструктуру и вымогают деньги.

# Morbid Trickster (MORLOCK)

## ЦЕЛИ АТАК

Финансовая выгода

## ЖЕРТВЫ

Государственные, коммерческие организации и все, кто заплатит

## ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка (предположительно украинская)

## 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: длительность атак – от 2 недель до 2 месяцев.

Имеется сильное пересечение индикаторов с Shedding Zmiy.

# Fairy Trickster (AKA HEAD MARE)

## ЦЕЛИ АТАК

Финансовая выгода, но также известны кейсы уничтожения данных

## ЖЕРТВЫ

Государственные, коммерческие организации и все, кто заплатит

## УРОВЕНЬ

Кибермошенники

## ПРОИСХОЖДЕНИЕ

Восточноевропейская группировка (предположительно украинская)

## КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

PhantomRAT

и другие

## ОСОБЕННОСТИ АТАК

Мы обнаружили только фишинговые рассылки на своих заказчиков, которые не привели к развитию таких атак, в связи с чем 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.

В ТГ-канале, в котором группировка отчитывалась об успехах, отсутствуют обновления с конца августа 2024 года.

# NGC4020

## ЦЕЛИ АТАК

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

## ПРОИСХОЖДЕНИЕ

Пока неизвестно

## КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

QuasarRAT

java-reverse-tcp

Кастомная утилита для обхода АВПО

## ОСОБЕННОСТИ АТАК

Для первоначального проникновения использовали уязвимость в приложении для удаленного управления DameWare Mini Remote Control.

После успешной атаки на системах размещали 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 использовали кастомную утилиту для обхода АВПО, эксплуатирующую уязвимость CVE-2023-36802
в драйвере MSKSSRV.SYS driver.


# NGC6160

(AKA STONEWOLF)

## КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

Meduza Stealer

## ОСОБЕННОСТИ АТАК

Используют фишинг для первоначального проникновения.

Meduza Stealer – это коммерческий вредоносный инструмент, который содержит механизм самоуничтожения при обнаружении системы на территории СНГ.

Мы видели его в нескольких атаках. Механизм предположительно встроил создатель инструмента, но NGC6160 тем не менее атакует цели на территории «запретных стран».

## ЦЕЛИ АТАК

Предположительно кража учетных данных

## ПРОИСХОЖДЕНИЕ

Пока неизвестно

# NGC5160

## КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ

Эксплойт под уязвимость/уязвимости в CommuniGate Pro

## ОСОБЕННОСТИ АТАК

Используют уязвимость или уязвимости нулевого дня в почтовых серверах CommuniGate для доступа к переписке на предприятиях государственного сектора, ВПК и НКО.

## ЦЕЛИ АТАК

Шпионаж

## ПРОИСХОЖДЕНИЕ

Пока неизвестно

4RAYS by SOLAR

# НЕОБЫЧНЫЕ ТАКТИКИ И ТЕХНИКИ 2024

# Модификация легитимных утилит в атаках Shedding Zmiy

Подмена атакующими легитимных утилит ps, ss, netstat и htop на Linux-машинах 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"
```

# Продвинутая техника отключения защитного решения в одном из расследований инцидента

1

Атакующие загрузили на хост исполняемый файл, в случае запуска которого не от административной УЗ выполнялось повышение привилегий через CVE-2023-36802

2

Далее в каталог установки антивирусного решения загружался драйвер с расширением .sys, который запускался службой ZeroRingProx, регистрирующей драйвер в группе FSFilter Bottom

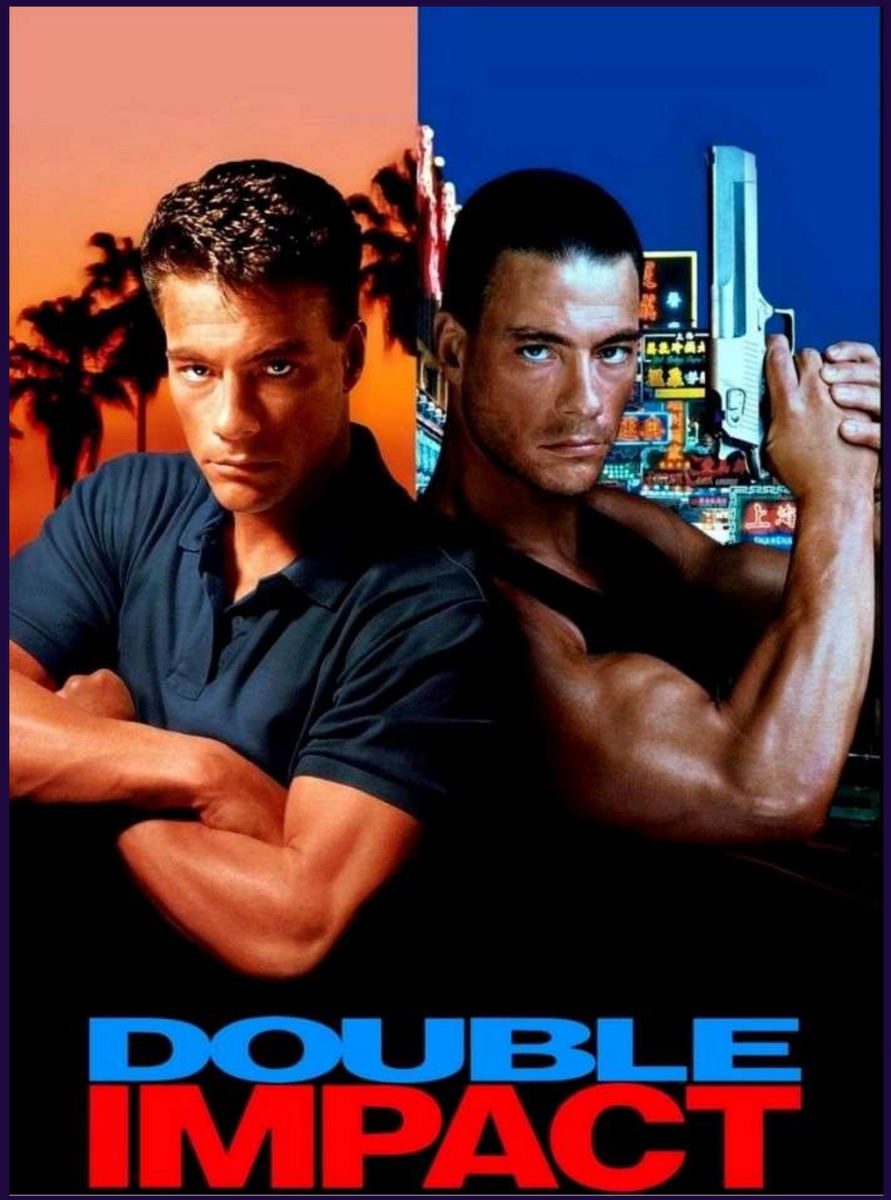
3

В результате дальнейшей цепочки действий защитные компоненты решения отключались

Официальный ответ вендора

Кейс расследования NGC4020

# Двойной удар: компрометация двумя APT-группировками




Мы проанализировали несколько критичных систем одной государственной организации.

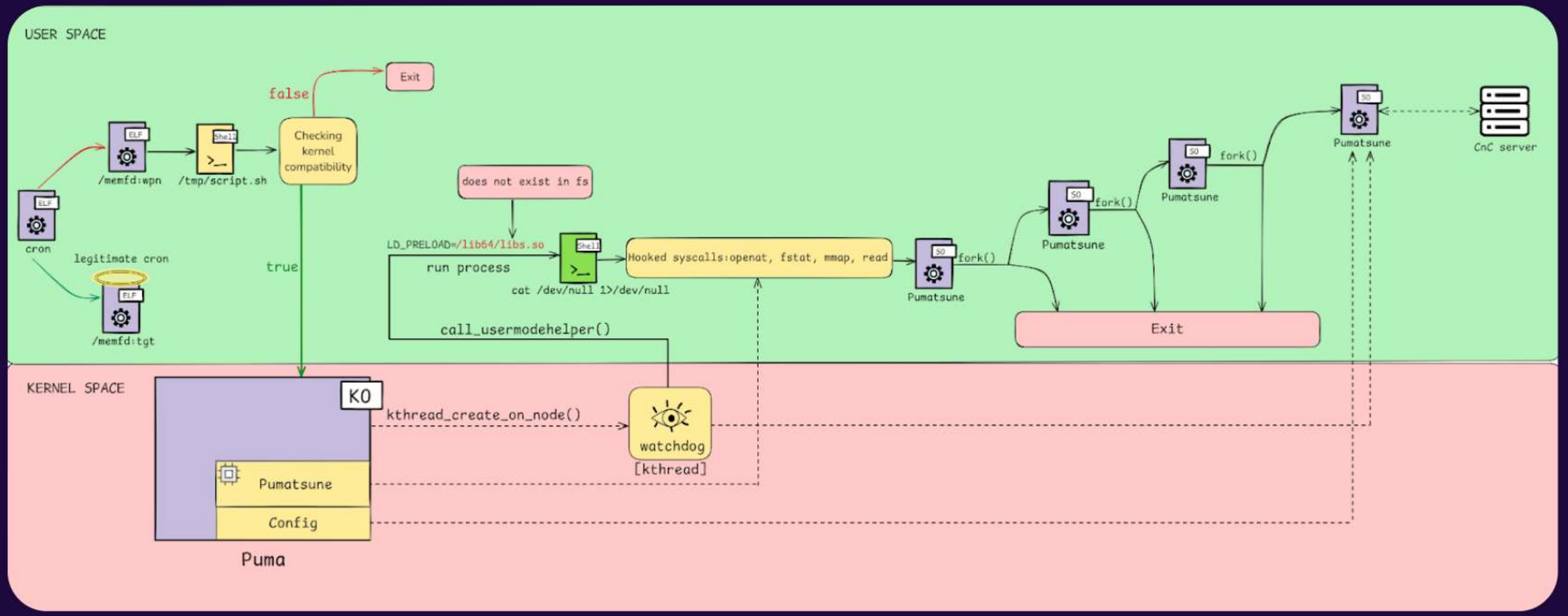
В рамках помощи с расследованием инцидента обнаружили «интересный факт» – компрометацию сети сразу двумя APT-группировками, причем обе на момент выявления инцидента были активны:

1. На Linux-системах обнаружили присутствие группировки Hellhounds, при этом исследованные артефакты указывали на пребывание группировки в инфраструктуре более 2 лет.

2. На одном из серверов под управлением Windows обнаружили закрепление группировки Erudite Mogwai (aka Space Pirates), созданное за 5 месяцев до момента выявления.

# Максимум скрытности с одновременным применением комбинации техник для уклонения от обнаружения

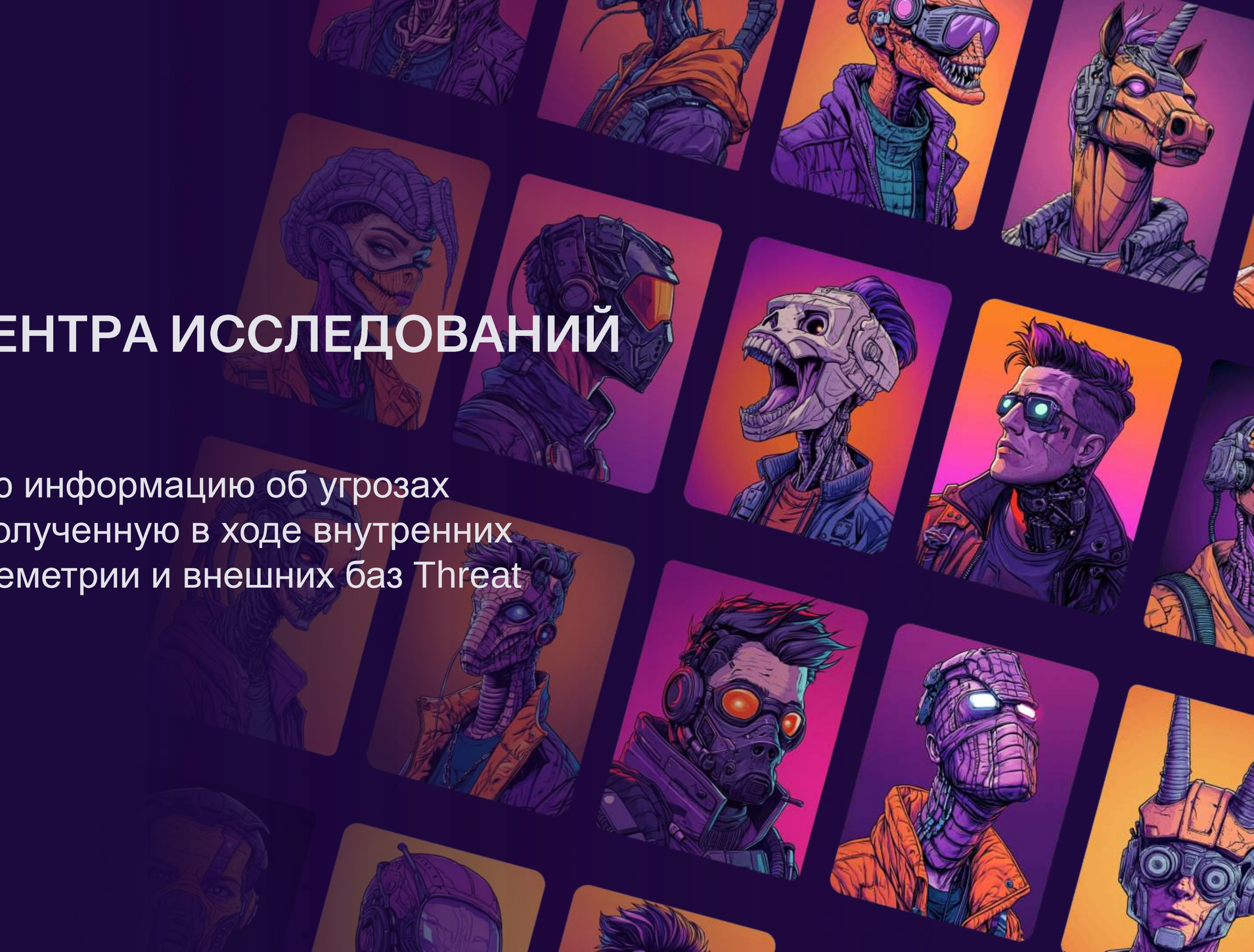
T1601.001 - Modify System Image: Patch System Image
T1620 - Reflective Code Loading
T1014 - Rootkit



4RAYS by SOLAR

# БАЗА УГРОЗ ЦЕНТРА ИССЛЕДОВАНИЙ SOLAR 4RAYS

Собираем актуальную информацию об угрозах и технологиях атак, полученную в ходе внутренних исследований, из телеметрии и внешних баз Threat Intelligence



# Выводы и прогнозы

## ВЫВОДЫ

Атакующие используют все более продвинутые тактики проникновения и последующего развития атаки, в т. ч. учатся отключать СЗИ

Проукраинские атакующие все чаще целятся в виртуализацию, т. к. поражение этой части инфраструктуры позволяет максимизировать ущерб

Растут требования к скорости реагирования на новые уязвимости: группировки начинают использовать эксплойты «в бою» уже через несколько часов после их публикации

## ПРОГНОЗЫ

Атакующие продолжат инвестировать в разработку – в атаках будет применяться больше кастомных вредоносных инструментов

Атаки на LINUX продолжатся и усилятся

Профессионализм атакующих продолжит расти, и они будут атаковать крупные, хорошо защищенные инфраструктуры

# Рекомендации

## ИНВЕНТАРИЗАЦИЯ АКТИВОВ И КОНТРОЛЬ ОБНОВЛЕНИЙ

Проведение инвентаризации крайне необходимо для формирования четкого представления о всей инфраструктуре и взаимосвязях ее элементов, в том числе определения полного перечня систем и приложений, требующих регулярного обновления.

## ПОСТОЯННОЕ ОБУЧЕНИЕ СОТРУДНИКОВ

Необходимо уделять должное внимание не только квалификации ИБ- и ИТ-персонала, но и регулярно повышать уровень осведомленности сотрудников в области 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.
До начала работ с подрядчиком необходимо убедиться в том, что он уделяет должное внимание своей ИБ, а его инфраструктура не скомпрометирована.

## 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.

## ПОРОЙ ЗЛОУМЫШЛЕННИКИ УДИВЛЯЮТ СВОЕЙ СКРЫТНОСТЬЮ, ПОЭТОМУ НЕ СТОИТ ПРЕНЕБРЕГАТЬ РЕГУЛЯРНЫМ 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 →

«Четыре луча» в телеграм →