4RAYS by SOLAR

SOLAR 4RAYS:
ХРОНИКИ DFIR

Отчет по итогам первого
полугодия 2025 года

ОГЛАВЛЕНИЕ

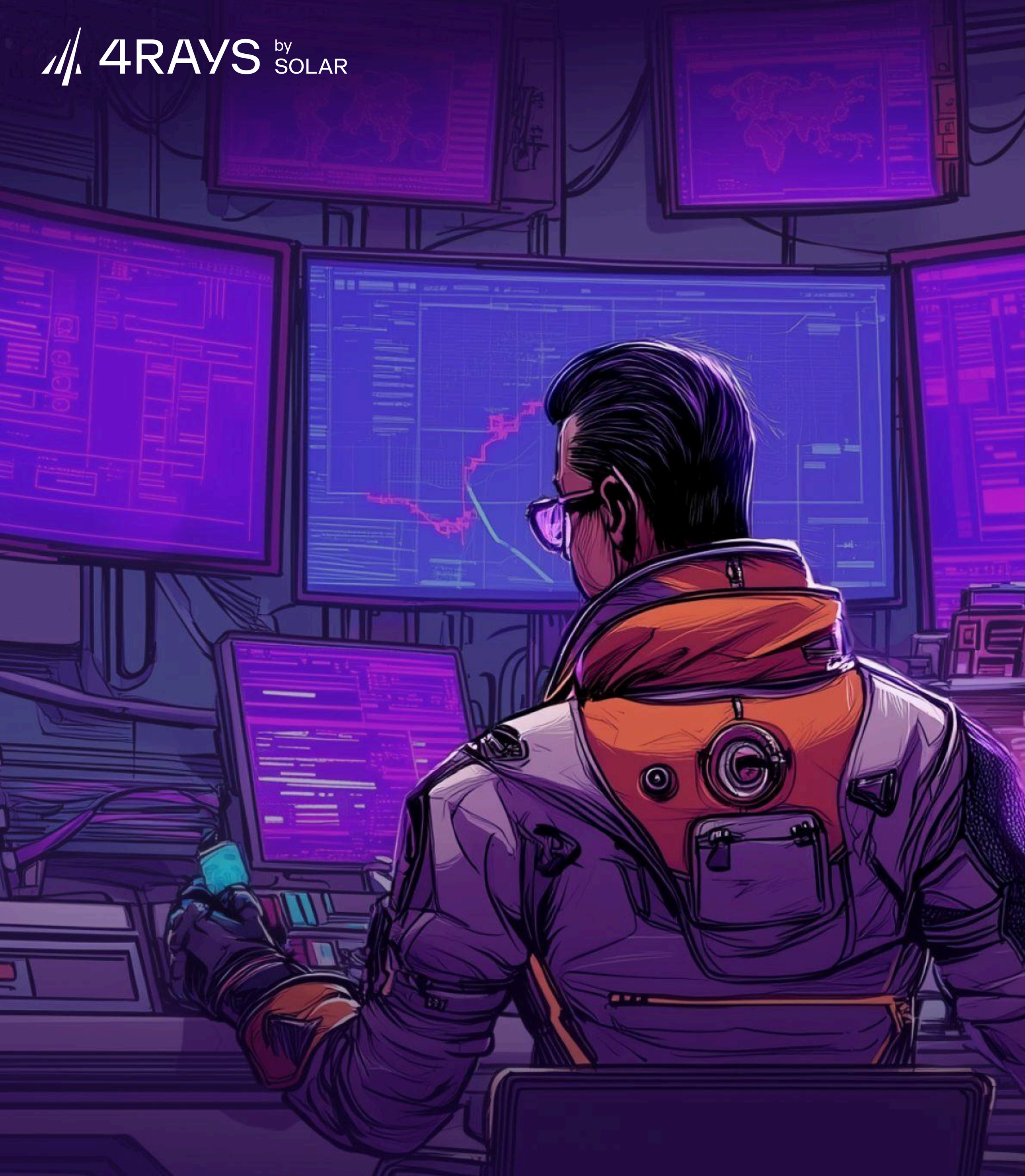
ВВЕДЕНИЕ И МЕТОДОЛОГИЯ

- Команда центра исследования киберугроз Solar 4RAYS ГК «Солар» участвует в расследовании десятков ИБ-инцидентов в российских частных и государственных организациях. В большинстве случаев речь идет об атаках, осуществленных профессиональными кибергруппировками, преследующими финансовые цели или работающими в интересах иностранных правительств. Как правило, это инциденты, которые произошли потому, что злоумышленники смогли обойти использовавшиеся в атакованных организациях автоматизированные средства защиты, либо потому, что в организации просто не имелось соизмеримых угрозе ИБ-инструментов.
- В ходе расследований эксперты Solar 4RAYS собирают различные данные о характеристиках атак, анализ которых позволяет сформировать представление об актуальных тактиках, техниках и процедурах злоумышленников, оценить уровень ИБ-риска для конкретной организации и в конечном итоге выстроить эффективную защиту ИТ-инфраструктуры от профессиональных киберпреступников.
- В основе отчета — данные, собранные в ходе расследований, проведенных за первое полугодие 2025 года, и их сравнение с аналогичным набором сведений, собранных за первое полугодие 2024 года. Исследование содержит информацию о наиболее атакуемых отраслях, квалификации злоумышленников и их мотивации. Кроме того, в отчете представлен обзор основных кибергруппировок, с деятельностью которых эксперты Solar 4RAYS столкнулись в ходе расследований, и наиболее распространенных техник, использованных в этих атаках. Сравнивая данные за разные периоды, мы проследим, как за год изменился ландшафт сложных киберугроз.

КЛЮЧЕВЫЕ ТРЕНДЫ

1. Количество сфер экономики, в которых работают атакованные организации, сократилось с 10 до 6. Атакующие фокусируются прежде всего на госсекторе, промышленности и ИТ-компаниях.
2. Главные цели атакующих — получение конфиденциальных данных (шпионаж) и финансовая выгода. Доля атак хактивистов сокращается.
3. На эксплуатацию уязвимостей в веб-приложениях и использование скомпрометированных учетных данных в первом полугодии 2025 года пришлось 86% успешных первоначальных проникновений. Эта цифра не изменилась с прошлого года.
4. Среди самых активных группировок — проукраинская Shedding Zmiy и восточноазиатская Erudite Mogwai. Расследованиям действий последней мы посвятили немало времени. Хотя инцидентов с ее участием было не слишком много, группировка атакует комплексно, и ее тактики и техники требуют тщательного расследования. При этом большого количества атак других ранее известных нам группировок мы не наблюдаем. Пока по большей части инцидентов нельзя сделать однозначных выводов о происхождении атакующих, что свидетельствует либо о возможной смене тактик и техник известных группировок, либо о появлении новых.

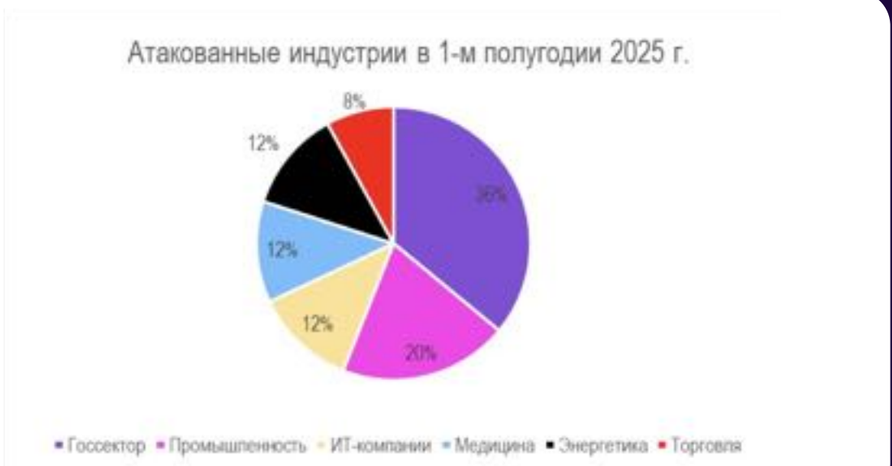
4RAYS by SOLAR



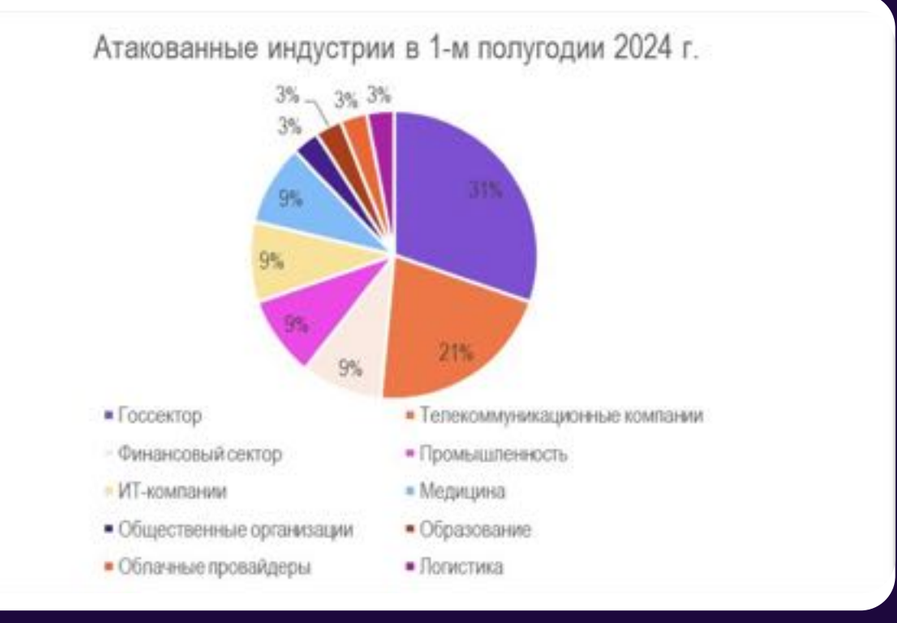
ОБЗОР ИНЦИДЕНТОВ

КОГО АТАКУЮТ

В первом полугодии 2025 года эксперты центра Solar 4RAYS расследовали инциденты в организациях из шести индустрий.



В том же периоде 2024 года индустрий было десять. Примечательно, что доля атак на госсектор увеличилась на 5 процентных пунктов (п. п.), а на промышленность — на целых 11 п. п. Заметно подросла также доля инцидентов в медицинских организациях и ИТ-компаниях (3 п. п.).



В прошлом периоде мы отмечали тренд на максимальное расширение типов атакованных индустрий. В фокусе злоумышленников оказывались не только традиционные для сложных кибератак цели, связанные с государственными органами, финансовыми операциями и крупными отраслями экономики, но и, на первый взгляд, незначительные в разрезе потенциально ценного для профессиональных злоумышленников «улова» цели (например, образовательные и общественные организации). Это стало одним из ключевых трендов не только первого полугодия, но и всего 2024 года.

Результаты первого полугодия указывают на возможную смену тенденции: атакующие теперь фокусируют усилия на ключевых управленческих и экономических сферах (госсектор, промышленность, энергетика). Хотя в первом полугодии стало известно о нескольких громких инцидентах, связанных с атаками на телеком (например, об атаке группировки Lifting Zmiy на крупного телеком-провайдера в Сибири), среди наших расследований значимых инцидентов в организациях из финансовой сферы и телекома не оказалось.

При этом следует учитывать, что на распределение атакованных индустрий в том числе влияет профиль организаций, которые к нам обращаются, и потому данные не обязательно точно отражают ситуацию на ландшафте угроз. Значимым индикатором здесь может быть список индустрий, атаки на которые мы видим из года в год. Организации из госсектора, промышленности и ИТ остаются в фокусе интереса злоумышленников.

ЦЕЛИ АТАКУЮЩИХ

Как и в прошлом периоде, основной целью атакующих стал шпионаж (68%) и финансовая выгода (20%).

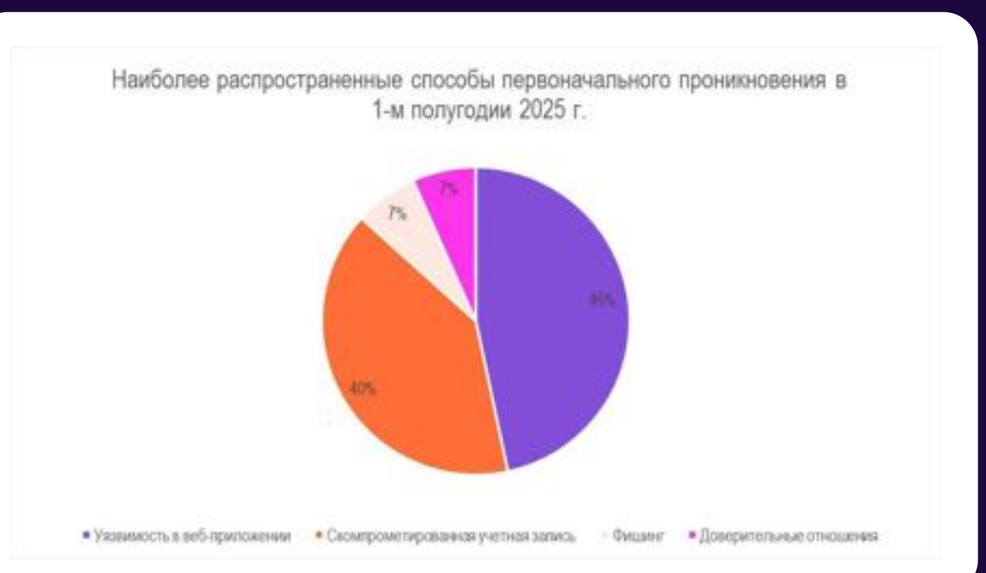
По сравнению с предыдущим именно эти две цели «набрали» 7 и 8 п. п. соответственно. А вот доля хактивистских атак, в том числе тех, которые направлены на публикацию и/или уничтожение конфиденциальных данных, заметно сократилась: с 12 до 8%. Уровень злоумышленников, вовлеченных в атаки на российские организации, вырос, а «легких» (то есть плохо защищенных) целей становится меньше. Всё большая доля инцидентов приходится на деятельность профессиональных атакующих, которые стремятся заполучить ценную информацию или финансовую выгоду, а не просто новостные заголовки.

Иногда шпионская атака может приносить и финансовую выгоду, поскольку конфиденциальная информация, похищенная из некоторых целей (например, объектов, связанных с энергетикой, ВПК и т. д.), высоко ценится на черном рынке. За прошедшее полугодие мы не видели конкретных свидетельств шпионских атак, чьей конечной целью являлась бы перепродажа конфиденциальной информации, но это не означает, что их не было. Рост доли шпионских атак может быть связан в том числе со стремлением злоумышленников заработать на продаже украденных данных.

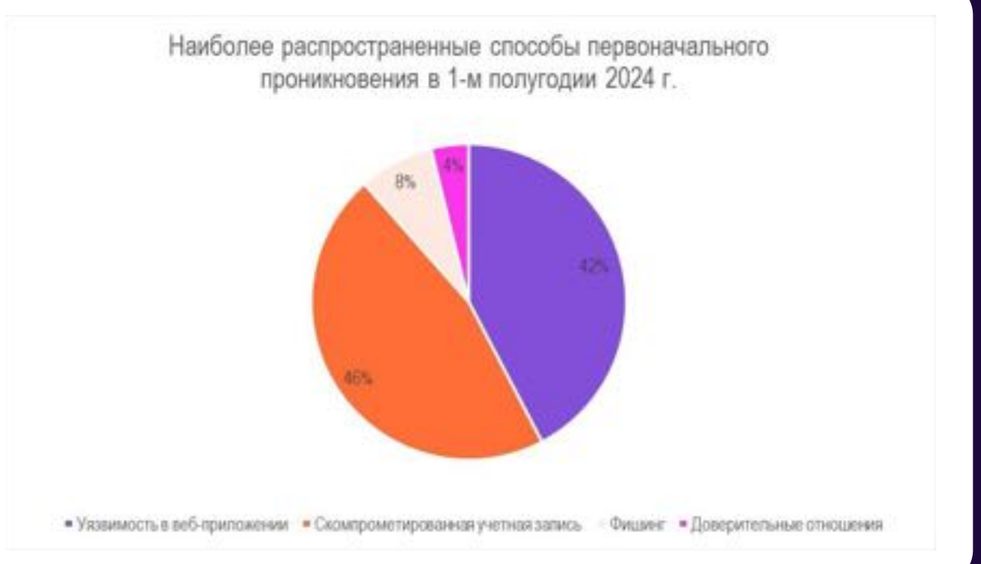
Подводя итоги прошлого года, мы прогнозировали, что число таких атак продолжит сокращаться, и не исключено, что в первом полугодии 2025 года этот прогноз начал сбываться.

СПОСОБЫ ПЕРВОНАЧАЛЬНОГО ПРОНИКНОВЕНИЯ

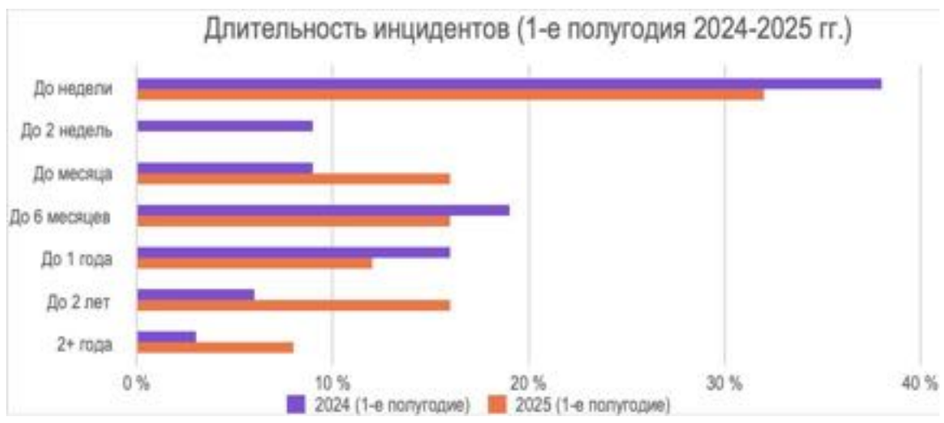
Лидеры в списке наиболее часто встречающихся способов первоначального проникновения в первом квартале 2025 года те же, что и годом ранее: уязвимости в публично доступных веб-приложениях и скомпрометированные учетные записи.



Как видно на графиках, за год распределение способов поменялось лишь немного, что свидетельствует о стабильной работоспособности наиболее распространенных способов: веб-приложения продолжают оставаться уязвимыми, а учетные данные продолжают утекать.



ДЛИТЕЛЬНОСТЬ ИНЦИДЕНТОВ



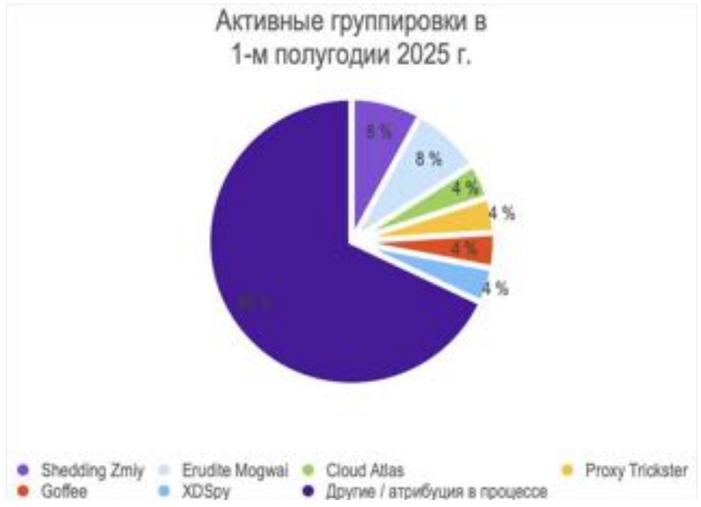
Метрика «Длительность инцидентов» описывает временной промежуток, в течение которого атакующие оставались в целевой инфраструктуре. В первом полугодии заметно (на 7 п. п.) выросла доля инцидентов продолжительностью до месяца и до двух лет (10 п. п.). За длительными инцидентами ожидаемо оказались атакующие, нацеленные на шпионаж. Хотя было и исключение: в одном из расследований мы обнаружили в инфраструктуре заказчика заурядный майнер, который проработал там незамеченным около 10 лет.

4RAYS by SOLAR

ГРУППИРОВКИ И КЛАСТЕРЫ ВРЕДОНОСНОЙ АКТИВНОСТИ

СТАТИСТИКА

Результаты анализа активных группировок в первом полугодии 2025 года удивили нас самих. После большого разнообразия, наблюдавшегося в 2024 году, мы столкнулись с затишьем: если в первом полугодии 2024 года мы атрибутировали почти все расследованные инциденты к известным группировкам и кластерам вредоносной активности, то год спустя с уверенностью можем атрибутировать пока лишь четверть расследованных нами инцидентов к пяти известным группам: Shedding Zmiy, Erudite Mogwai (aka Space Pirates), Cloud Atlas, Goffee, XDSpy, — а также к одной новой группировке, Proxy Trickster (о которой мы недавно выпустили статью).



Во всех остальных 68% инцидентов мы либо столкнулись с новыми кластерами или группировками, либо имеем дело с обновлением инструментария и инфраструктуры известных ранее групп, либо ранее известные нам группы просто не попали в наш фокус в закончившемся полугодии. Справедливости ради отметим, что анализ информации по самым свежим инцидентам из первой половины 2025 года еще продолжается, и в ближайшем будущем «туман неизвестности» относительно как минимум части этих инцидентов развеется.

Впрочем, уже сейчас мы можем сказать, что в расследованных инцидентах мы не видели тактик и техник, характерных для активных в прошлом группировок Moonshine Trickster, Morbid Trickster, Obstinate Mogwai и Lifting Zmiy. У этого может быть две основных причины:

— наши заказчики не входят в число целей этих группировок;

— после серии публикаций о себе в 2023–2024 гг. группировки ушли на дно или обновили тактики и инструментарий.

Примечательно, что проукраинская группировка Shedding Zmiy, деятельность которой мы отслеживаем с 2023 года, в первом полугодии сократила свою активность практически втрое, что опять же может говорить о двух изменениях: атакующие либо сознательно сократили активность, чтобы уйти от повышенного внимания экспертов по ИБ, либо внесли значительные изменения в тактики и техники, что временно затрудняет атрибуцию атак. Вместе с тем, как показывает наш анализ веб-панели Bulldog Backdoor, которую Shedding Zmiy использует для управления атаками, группировка продолжает разрабатывать новые инструменты и совершенствовать старые.

Shedding Zmiy

ИНСТРУМЕНТЫ

Mimikatz;

SoftPerfect Network Scanner;

nmap;

fscan;

Psexec;

RemCom;

ssh-snake

chisel;

resocks;

gsocket;

Metasploit;

Sliver;

Cobalt Strike.

Вредоносное ПО:

CobInt;

Ekipa RAT;

DarkGate;

SystemBC;

Bulldog Backdoor;

FaceFish;

Kitsune;

Megatsune;

XDHijack loader;

Nim loader;

Spark RAT;

Puma rootkit;

knife (multitool);

Pumatsune;

Gecko;

Gwyntik;

Mycelium;

Mushroom;

Mosquito;

Teardrop;

Octopus;

BADSTATE framework.

ОБЩАЯ ИНФОРМАЦИЯ

ЦЕЛИ АТАК:
Шпионаж и уничтожение инфраструктуры

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

ПРОИСХОЖДЕНИЕ:
Проукраинская группировка атакующих, специализирующаяся на шпионаже и — до 2025 года — атаках, направленных на уничтожение инфраструктуры. Мы подробно рассказывали о группе в серии статей об инцидентах и вредоносных инструментах.

Shedding Zmiy

ОСОБЕННОСТИ

Основной целью группы является шпионаж. В 2023–2024 годах часть ее атак также заканчивались уничтожением инфраструктуры, но в 2025 году таких инцидентов, связанных с Shedding Zmiy, мы пока не наблюдали.

В некоторых случаях группировка публиковала украденные данные в открытом доступе. В своих атаках злоумышленники фокусируются на самых разных областях: от государственных организаций до телекоммуникационных, технологических и прочих компаний.

В первом полугодии 2025 года мы видели атаки группировки на организации из госсектора и сектора IT, медицинские организации и предприятия из сферы энергетики.

В 2024 году группа нередко взламывала публичные веб-приложения небольших компаний, не представляющих для них какой-либо ценности с точки зрения шпионажа или уничтожения данных. Эти доступы группировка потом использовала для скрытной доставки инструментов в атаках на своих основных жертв. Для этих же целей использовались легитимные ресурсы Pastebin и Webhook.site.

В 2025 году мы наблюдали косвенные свидетельства сохранения основных тактик. В частности, группа продолжает использовать технику Valid Accounts для первоначального проникновения в целевую организацию. Как минимум в одном инциденте нам удалось это подтвердить.

Кроме того, в прошедшем полугодии нам удалось обнаружить и проанализировать уникальный инструмент, который группировка использует для управления зараженными инфраструктурами, — веб-панель Bulldog. Функциональность панели позволяет получить детальное представление о масштабах деятельности Shedding Zmiy. С ее помощью атакующие могли (или до сих пор могут) централизованно собирать информацию с зараженных систем, управлять вредоносным ПО на зараженных системах, взламывать новые системы, собирать новые импланты для атак и т. д.

В нашем опыте это единственная группировка, демонстрирующая столь структурированный подход к проведению целевых атак. Подробный разбор функциональности панели можно прочитать здесь.

Так как Shedding Zmiy практикует шпионаж, длительность проникновения в инфраструктуру жертвы может быть очень большой, в расследованиях первого полугодия 2024 года мы наблюдали атаки продолжительностью от недели до полутора лет.

В первом полугодии 2025 года ситуация изменилась мало: хотя в одном случае злоумышленники продержались в инфраструктуре всего пять дней, в большинстве инцидентов атакующим удается сохранять присутствие в инфраструктурах организаций в течение периодов от 10 месяцев до двух лет. Это говорит о сохраняющемся высоком уровне опасности, исходящей от этой группировки.

Erudite Mogwai

(AKA SPACE PIRATES)

ОБЩАЯ ИНФОРМАЦИЯ

ЦЕЛИ АТАК:
Шпионаж

ЖЕРТВЫ:
Государственные учреждения, ИТ-компании, авиационно-космическая и электроэнергетическая индустрии, научно-исследовательские институты.

ПРОИСХОЖДЕНИЕ:
Erudite Mogwai (aka Space Pirates) — одна из активных APT-группировок, специализирующихся на краже конфиденциальной информации и шпионаже. Действует она как минимум с 2017 года. Впервые деятельность Erudite Mogwai была описана в 2019 году специалистами из компании Positive Technologies, которые дали группировке название Space Pirates. С тех пор их методы, инструменты и цели продолжали развиваться. В наше поле зрения группа попала летом 2023 года в ходе расследования атаки на ИТ-инфраструктуру российской госорганизации. Последний на сегодняшний день раз мы столкнулись с ней весной 2025 года.

ИНСТРУМЕНТЫ

Среди актуальных инструментов, используемых злоумышленниками на данный момент, можно выделить:

- LuckyStrike Agent — многофункциональный бэкдор на .NET, способный использовать в качестве C2 OneDrive, не встречался в предыдущих атаках;
- 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;
- модифицированные версии mimikatz для кражи учетных данных.

ОСОБЕННОСТИ

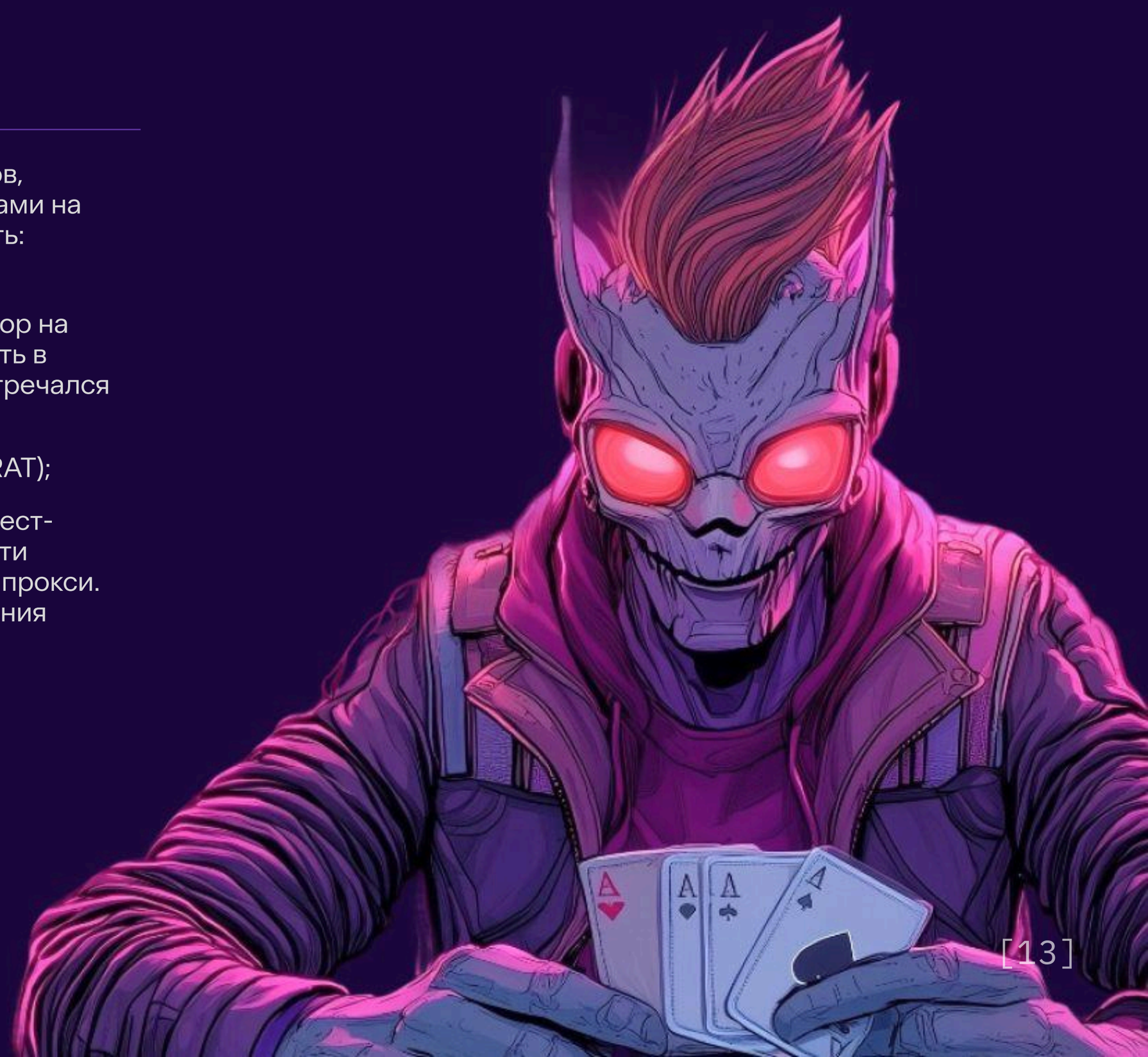
Группировка атакует государственные учреждения, ИТ-департаменты различных организаций, а также предприятия, связанные с высокотехнологичными отраслями, такими как авиационно-космическая и электроэнергетическая индустрии. Географически их атаки были нацелены на организации в России, Грузии и Монголии.

В первом полугодии 2025 года мы наблюдали атаки группировки на организации в сфере энергетики и госсектора.

Характерные тактики, техники и инструменты, применяемые группировкой, позволяют предположить, что она имеет восточноазиатское происхождение.

РАССЛЕДОВАНИЯ

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



Proxy Trickster

ОБЩАЯ ИНФОРМАЦИЯ

ЦЕЛИ АТАК:
Финансовая выгода

ЖЕРТВЫ:
Организации по всему миру (58 стран)

ПРОИСХОЖДЕНИЕ:
Неизвестно

ИНСТРУМЕНТЫ

masscan;

кастомные bash-скрипты для установки перечисленных ниже утилит;

gs-netcat;

майнер XMRig;

Proxyjacking-утилиты: Packetshare.io, Pawns.app, Traffmonetizer, Earn.fm, Honeygain и Repocket.

ОСОБЕННОСТИ

Группа финансово мотивированных киберпреступников-оппортунистов с неизвестной географической локализацией. С ее деятельностью мы столкнулись весной 2025 года, расследуя инцидент в одной из российских IT-компаний.

Предположительно через уязвимости в веб-приложениях группировка взламывает корпоративные серверы, чтобы установить софт для проксирования трафика за деньги и майнинга криптовалют.

Группа атакует корпоративные серверы по всему миру, предположительно используя известные уязвимости в публично доступных сервисах (например, Selenium Grid).

РАССЛЕДОВАНИЯ

Профиль группировки в блоге Solar 4RAYS →

ДРУГИЕ ГРУППИРОВКИ И КЛАСТЕРЫ ВРЕДОНОСНОЙ АКТИВНОСТИ

В первом полугодии 2025 года мы также столкнулись с фишинговыми рассылками, относящимися к активности группировки Cloud Atlas.

Группировка известна с 2014 года, специализируется на шпионских операциях в организациях разной направленности по всему миру и, предположительно, является «наследницей» операции Red October, раскрытой «Лабораторией Касперского» в 2013 году. Данных, позволяющих надежно определить происхождение операторов Cloud Atlas, нет. В публикации о Red October «Лаборатория Касперского» приводила языковые артефакты, оставленные в коде ВПО разработчиками, указывающие на то, что они могут быть русскоговорящими. В ходе нашего расследования в 2024 году мы тоже столкнулись с похожей уликой: в одном из обнаруженных скриптов английское слово domain было буквально транслитерировано с русского: domen_scan.ps1.

Также, по данным «Лаборатории Касперского», Cloud Atlas чаще всего атакует цели на территории России. Получается, что русскоязычные атакующие нападают на российские организации с целью шпионажа. Такая совокупность признаков может указывать на то, что атакующие действуют в интересах одной из стран постсоветского пространства, например Украины, ведь проукраинские группировки в последние годы регулярно атакуют российские инфраструктуры. Однако в атаках, описанных в 2019 году, среди целей обнаружились и украинские государственные организации, правда только на территориях Украины, на которых в то время происходил военный конфликт.

Помимо рассылок в 2025 году, мы сталкивались с Cloud Atlas нечасто: в мае 2023 года мы наблюдали характерную для группировки фишинговую рассылку в адрес российской государственной организации. Тогда инцидент длился не более 10 дней. Расследуя атаку в сентябре 2024 года, мы обнаружили свидетельства, указывающие на то, что Cloud Atlas находился в сети атакованной организации более двух лет. Атаки, зафиксированные в 2025 году, длились несколько дней.

Кроме того, весной 2025 года мы столкнулись с развитием инцидента, который расследовали еще в 2021 году. Речь идет о новых атаках с помощью бэкдора VipNet. В апреле 2025 года наша команда в рамках проведения Compromise Assessment в одной из организаций госсектора обнаружила вредоносный файл в каталоге с резервной копией ViPNet.

Анализ файлов из архива driv_fsa.lzh показал, что пакет обновления ViPNet содержал вредоносный инструментарий, который в процессе выполнения загружал из зашифрованного файла в память атакуемой системы вредоносный бэкдор. Его загрузчик был скомпилирован в ноябре 2021 года. Этот факт вернул нас в 2021 год, когда при расследовании инцидента в инфраструктуре заказчика мы столкнулись с аналогичной картиной. На конференции PHDays-11 в докладе «Как Жуи и Диндин провели прошедший год в России», посвященном инструментарию, а также тактикам и техникам восточноазиатских APT-группировок за 2021 год, мы уже рассказывали в том числе об этой атаке, где злоумышленники использовали недостаток безопасности в системе обновления ПО ViPNet для доставки и запуска вредоносной полезной нагрузки.

Все новое — хорошо забытое старое. Незадолго до нашего расследования 2025 года коллеги из «Лаборатории Касперского» выпустили краткий отчет о, предположительно, новом бэкдоре, который мимикрировал под обновления ПО ViPNet и использовал схему запуска, загрузчик и, возможно, бэкдор, аналогичные тем, что мы видели в наших расследованиях.

Коллеги по индустрии отнесли атаки 2021 года к деятельности группировки BlueTravaller (aka TaskMasters). Мы пока воздерживаемся от атрибуции, поскольку данных для нее еще мало, но с высокой долей уверенности можем сказать, что это восточноазиатские APT.

Кроме того, в первом полугодии мы видели фишинговые рассылки, связанные с распространением вредоноса DarkWatchman RAT, а помимо этого, рассылки для сбора NTLM-хешей, предположительно связанные с деятельностью группировки, которую коллеги по индустрии называют Phasehifters, Sticky Werewolves и Angry Likho.

4RAYS by SOLAR

ИНТЕРЕСНЫЕ ТЕХНИКИ И АТАКИ 2025

РАСПРОСТРАНЕННЫЕ ТЕХНИКИ АТАКУЮЩИХ

Для этого раздела нашего отчета мы взяли информацию о действиях атакующих в рамках инцидентов, расследованных командой Solar 4RAYS. Матрица MITREATT&CK позволяет достаточно гибко и подробно разбирать атаки на тактики/техники, тем самым давая ответы на вопрос: «Почему атакующие осуществляют какие-то действия и как именно они это делают?» Мы решили сфокусироваться на четырех тактиках (Initial Access, Persistence и Lateral Movement и Evasion), на которых мы в этом полугодии видели любопытное применение техник.

Первоначальное проникновение (Initial Access)

Распространенные техники, зафиксированные в инцидентах.

- Trusted Relationship ID: T1199;
- Exploit Public-Facing Application ID: T1190;
- Valid Accounts: Default Accounts ID: T1078.001;
- Valid Accounts: Local Accounts ID: T1078.003;
- Replication Through Removable Media ID: T1091;
- External Remote Services ID: T1133;
- Phishing: Spearphishing Attachment ID: T1566.001;
- Phishing: Spearphishing Link ID: T1566.002.

Взлом доступных из сети приложений

В исследуемом периоде зафиксированы следы успешной эксплуатации уязвимостей CVE-2022-41040 и CVE-2022-41082 (ProxyNotShell), эксплуатация неправильно сконфигурированного ПО Bitrix, а также случай атаки через уязвимость в собственном приложении организации. А еще в одном случае вредоносный веб-шелл, скорее всего, загрузили через функциональность загрузки изображений.

Вход через скомпрометированные учетные записи

В одном из инцидентов злоумышленники использовали аккаунт по умолчанию в ПО Cisco: в нем, вероятно, забыли сменить пароль при настройке, и атакующие этим воспользовались. В другом случае атакующие использовали шлюз подрядчика для входа. При этом у подрядчика признаков компрометации шлюза обнаружено не было, но были следы входа валидной учетной записи, которую злоумышленники, вероятно, сумели скомпрометировать ранее. Зафиксировали мы и совсем уж экзотическое исполнение техники — с помощью инсайдера. В одном из инцидентов злоумышленник физически подходил и подключал мост, предназначенный для подключения портативных жестких дисков. Для входа в систему использовалась действительная учетная запись.

Фишинг

Из квартала в квартал мы регулярно видим несколько инцидентов, связанных с фишингом. Этот способ первоначального проникновения хоть и не является самым распространенным в расследованиях, которые довелось провести нам, но всё же регулярно используется атакующими. Не в последнюю очередь потому, что пользователи регулярно открывают такие письма и переходят по сомнительным ссылкам. В первом полугодии мы видели несколько подобных атак, но они едва ли чем-то выделяются: либо вредоносное вложение, либо ссылка на внешний ресурс, с которого скачивается вредоносный код.

Закрепление (Persistence)

Распространенные техники, зафиксированные в инцидентах.

- Create Account: Local Account ID: T1136.001;
- Valid Accounts: Local Accounts ID: T1078.003;
- Valid Accounts: Domain Accounts ID: T1078.002;
- External Remote Services ID: T1133;
- Server Software Component: Web Shell ID: T1505.003;
- Boot or Logon Autostart Execution: Print Processors ID: T1547.012;
- Boot or Logon Initialization Scripts ID: T1037;
- Scheduled Task/Job: Scheduled Task ID: T1053.005;
- Create or Modify System Process: Windows Service ID: T1543.003;
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder ID: T1547.001;
- Compromise Host Software Binary ID: T1554;
- Event Triggered Execution: Component Object Model Hijacking ID: T1546.015;
- Event Triggered Execution: Unix Shell Configuration Modification ID: T1546.004;
- Event Triggered Execution: Installer Packages ID: T1546.016;
- Scheduled Task/Job: Cron ID: T1053.003;
- Hijack Execution Flow: DLL ID: T1574.001;
- Account Manipulation: SSH Authorized Keys ID: T1098.004;
- Hijack Execution Flow: Dynamic Linker Hijacking ID: T1574.006;
- Hijack Execution Flow: DLL ID: T1574.001.

В одном из расследований атакующие использовали не самую распространенную технику — Server Software Component: SQL Stored Procedures ID: T1505.001.

В одном из инцидентов мы обнаружили достаточно редкий способ закрепления. После первичного доступа злоумышленники создали в базе данных веб-приложения / приложения для ВКС бэкдор, состоящий из функции и триггера. Ввод данных в поля для аутентификации с ключевым словом/строкой позволял выполнять произвольные команды SQL, в том числе с помощью функции COPY сохранять данные из запроса в файлы на системе. При этом обнаружить данный бэкдор без средств мониторинга достаточно тяжело, так как запрос с ключом перехватывается функцией и не логируется.

В другом кейсе мы видели применение техники Compromise Host Software Binary ID: 1554, в рамках которой неизвестные атакующие закрепились в системе, подменив легитимную утилиту Activator.exe ВПО MeshAgent.

Горизонтальное перемещение (Lateral Movement)

Распространенные техники, зафиксированные в инцидентах.

- Remote Services: Remote Desktop Protocol ID: T1021.001;
- Exploitation of Remote Services ID: T1210;
- Remote Services: Windows Remote Management ID: T1021.006;
- Remote Services: Remote Desktop Protocol ID: T1021.001;
- Remote Services: SMB/Windows Admin Shares ID: T1021.002;
- Remote Services: SSH ID: T1021.004;
- Use Alternate Authentication Material: Pass the Hash ID: T1550.002.

В расследованных инцидентах злоумышленники активно применяли WinRM, SMB, RPD и SSH в качестве инструментов для горизонтального перемещения. RDP встречался нам чаще других. В одном из расследований мы также видели применение техники pass the hash. Другими словами, на этом этапе атакующие действуют предсказуемо, не применяя каких-либо экзотических техник. Возможно, потому, что стандартные распространенные техники продолжают работать.

Уклонение от обнаружения (Evasion)

Распространенные техники, зафиксированные в инцидентах.

- Obfuscated Files or Information: Encrypted/Encoded File ID: T1027.013;
- Indicator Removal: File Deletion ID: T1070.004;
- Indicator Removal: Clear Windows Event Logs ID: T1070.001;
- Impair Defenses: Disable or Modify Tools ID: T1562.001;
- Impair Defenses: Disable or Modify System Firewall ID: T1562.004;
- Masquerading: Match Legitimate Resource Name or Location ID: T1036.005;
- Modify Registry ID: T1112;
- Hide Artifacts: NTFS File Attributes ID: T1564.004;
- Hide Artifacts: Hidden Files and Directories ID: T1564.001;
- Indicator Removal: Clear Persistence ID: T1070.009;
- Impair Defenses: Disable or Modify Tools ID: T1562.001;
- Valid Accounts: Domain Accounts ID: T1078.002;
- System Binary Proxy Execution: Msiexec ID: T1218.007;
- File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification ID: T1222.002;
- Obfuscated Files or Information: Encrypted/Encoded File ID: T1027.013;
- Compromise Host Software Binary ID: T1554.

На стадии уклонения от обнаружения продолжаем видеть случаи, когда атакующие стремятся нарушить работу защитного ПО. Примерно в каждом десятом расследованном инциденте атакующие пытались или успешно применяли техники, направленные на отключение защитных средств. Например, в одном из расследований мы видели свидетельства того, что защитное решение, работавшее в организации, не фиксировало вредоносные веб-шеллы, атакующих, хотя на тот момент они уже были внесены в антивирусные базы. Прямых свидетельств этого обнаружить не удалось, но такое нетипичное поведение антивируса невозможно без модификации его работы. В другом инциденте мы обнаружили свидетельства удаления антивирусного ПО через PsExec.

Конечно, во всех случаях эти действия производились уже после первоначальной компрометации.

Кроме того, для уклонения от обнаружения атакующие активно применяют мимикрию под легитимное ПО и обфускацию вредоносного кода.

ВЫВОДЫ И РЕКОМЕНДАЦИИ

Первое полугодие 2025 года оказалось относительно спокойным в контексте характера расследованных нами инцидентов. Сократилось количество индустрий, в которых работают атакованные организации, существенно упало число атак, целью которых является уничтожение инфраструктуры целевой организации или публикация похищенных данных. Большая часть сложных кибератак, которые мы расследовали за эти шесть месяцев, преследовали цель либо похитить конфиденциальные сведения, либо заработать. Станет ли это «успокоение» устойчивым трендом, покажет дальнейшее наблюдение за ландшафтом.

Атакующие демонстрируют более фокусный подход к выбору целей для атак, чем раньше. Если 2024 год мы заканчивали с выводом «Атакуют всех», поскольку в течение года разнообразие атакованных индустрий только росло, то в первом полугодии 2025 года число сфер деятельности упало почти вдвое. Это может свидетельствовать о том, что злоумышленники стараются фокусироваться только на самых ценных с точки зрения шпионажа организациях: из государственного сектора, промышленности, ИТ-сферы, медицины. Это обстоятельство — важный сигнал для ИБ-команд подобных организаций.

Чтобы снизить вероятность возникновения киберинцидента с серьезными для атакованной организации последствиями, мы рекомендуем не пренебрегать следующими мерами безопасности:

1. Пристальное внимание уделяйте актуальности ПО. Атаки через уязвимости в веб-приложениях — всё еще самый популярный вектор первоначального проникновения.
2. Строго контролируйте удаленный доступ в инфраструктуру, особенно для подрядчиков.
3. Предельно ответственно относитесь к соблюдению парольных политик, пользуйтесь сервисами мониторинга утечек учетных записей (например, Solar AURA) и вовремя их обновляйте: использование утекших учетных записей для первоначального проникновения — второй по популярности способ первоначального проникновения.
4. Серьезно относитесь к уведомлениям о возможной компрометации от Национального координационного центра по компьютерным инцидентам (НКЦКИ) и частных компаний, обладающих экспертизой в области ИБ.
5. Создайте инфраструктуру бекапов, следуя принципу «3—2—1», который предполагает наличие не менее трех копий данных, хранение копии как минимум на двух физических носителях разного типа и наличие минимум одной копии за пределами основной инфраструктуры.
6. Используйте продвинутые средства защиты (EDR, SIEM) наряду с классическим защитным ПО, чтобы иметь возможность отслеживать события в инфраструктуре и вовремя обнаруживать нежелательные.
7. В случае подозрения на атаку не медлите с оценкой компрометации, а лучше — делайте ее на регулярной основе.
8. Повышайте киберграмотность сотрудников, ведь успешная атака на основе социальной инженерии возможна даже в самой защищенной инфраструктуре.
9. Следите за тем, чтобы служба ИБ имела постоянный доступ к последним сведениям о ландшафте киберугроз конкретного региона и индикаторам компрометации. Например, подпишитесь на наш телеграм-канал «Четыре луча». В нем мы публикуем информацию о самых свежих опасных уязвимостях, а также новых тактиках и техниках группировок атакующих.

4RAYS by SOLAR

БОЛЬШЕ КЕЙСОВ, РАССЛЕДОВАНИЙ И ДРУГИХ ПРАКТИЧЕСКИХ МАТЕРИАЛОВ

Блог

rt-solar.ru/solar-4rays →

Телеграм

@FOUR_RAYS →