4RAYS by SOLAR

SOLAR 4RAYS:
ХРОНИКИ DFIR

Отчет по итогам
10 месяцев 2025 года

Введение

Команда Центра исследования киберугроз Solar 4RAYS ГК «Солар» участвует в расследовании десятков ИБ-инцидентов в российских частных и государственных организациях. В абсолютном большинстве случаев речь идет об атаках, осуществленных группами профессиональных взломщиков, преследующих финансовые цели или работающих 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 у организации не было соизмеримых угрозе ИБ-инструментов.

В ходе расследований эксперты Solar 4RAYS собирают 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 счете выстроить эффективную защиту ИТ-инфраструктуры от профессиональных киберпреступников.

В основе отчета — данные, собранные в ходе расследований, проведенных за 10 месяцев 2025 года, включая статистику по наиболее атакуемым отраслям, квалификации злоумышленников и их мотивации. Кроме того, в отчете представлен обзор основных кибергруппировок, с деятельностью которых эксперты Solar 4RAYS столкнулись в ходе расследований.

Ключевые тренды

- Количество инцидентов, расследованных командой Solar 4RAYS за десять месяцев 2025 года, сократилось в сравнении с тем же периодом 2024 года на 18%.

- Количество атакованных профессиональными хакерами сфер экономики сократилось с 16 до 10: госорганы, промышленность, энергетика и IT — в топе. Организации из отрасли энергетики попали в поле пристального внимания злоумышленников в 2025 году.

- Доля атак с целью шпионажа выросла на 7 процентных пунктов (п. п.), а атаки хактивистов упали на 11 п. п. Атакующие фокусируются на более скрытных атаках против масштабных целей — крупных организаций из значимых сфер экономики.

- Масштаб деятельности проукраинских группировок значительно уменьшился. Если в первые десять месяцев 2024 года на них приходилось около 70% расследованных инцидентов, то в 2025 году их доля составляет менее 20%.

- В 2025 году увеличилось количество группировок и кластеров вредоносной активности. Если в 2024 году Solar 4RAYS отслеживали восемь группировок, то в 2025 году их стало 18. Многие из них — ранее не известные группы и кластеры.

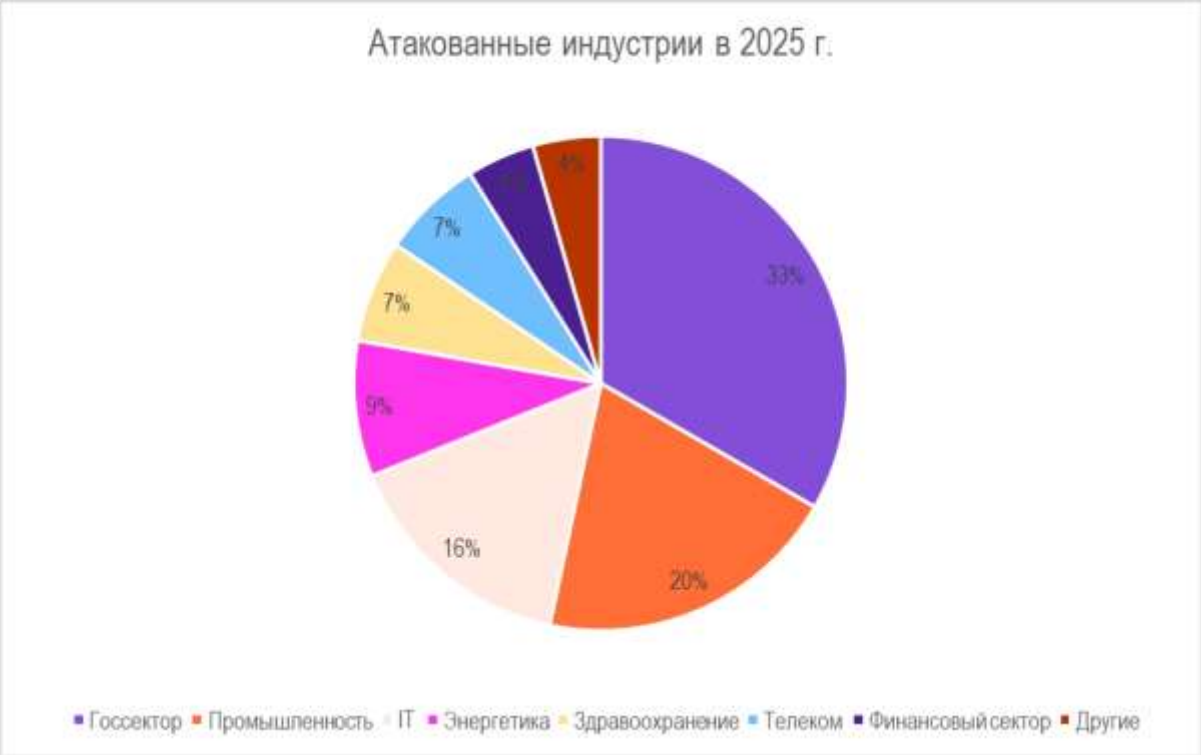
- Каждый пятая расследованная атака длилась от 6 месяцев до года. Доля таких атак возросла на значительные 12 п. п. Это указывает на стремление атакующих к длительному присутствию в инфраструктурах компаний-жертв.

- Уязвимости в веб-приложениях остаются наиболее распространенным способом первоначального проникновения хакеров, однако в 2025 году значительный рост показали атаки через подрядчиков. В 27% случаев атакующие проникли в организации именно так. Годом ранее на такие инциденты приходилось всего 12%.

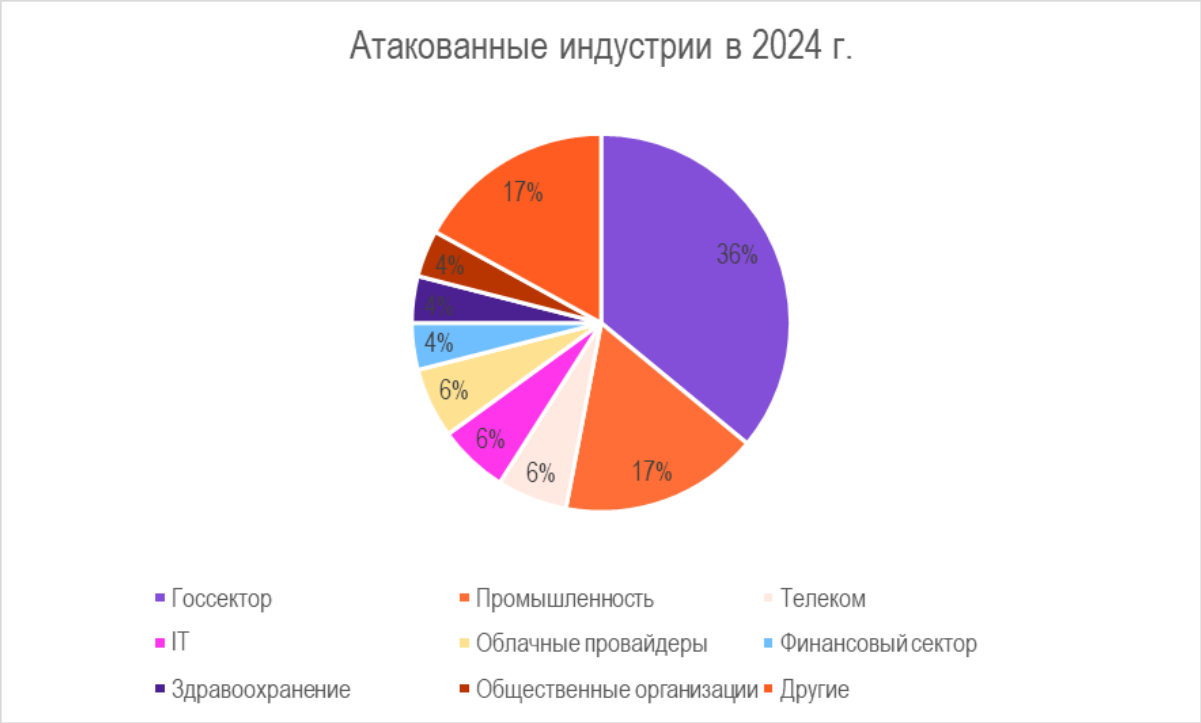
Обзор инцидентов

Кого атакуют

За 10 месяцев 2025 года эксперты Solar 4RAYS расследовали киберинциденты в организациях из 10 различных отраслей, включая госсектор, телеком, промышленность, IT. В категорию «Другие» вошли организации из сферы ретейла, транспорта и науки.



По сравнению с аналогичным периодом 2024 года немного (3 процентных пункта) сократилась доля инцидентов в госсекторе, но возросла доля атак на промышленность и IT-компании. В последнем случае — на 10 п. п. Кроме того, мы стали фиксировать инциденты на предприятиях в сфере энергетики — в 2024 году расследований в этой отрасли не проводилось.



Атаки на энергетику обусловлены растущим интересом группировок (преимущественно действующих в интересах иностранных государств) к этой сфере российской экономики, чему способствует обострение геополитической ситуации. Атак на IT-компании стало больше, в том числе потому, что это все еще рабочий способ проникновения в целевую организацию: многие компании из этой сферы выступают подрядчиками для других, зачастую более крупных и хорошо защищенных организаций. Статус подрядчика часто означает наличие сетевой связанности у IT-компании и организации, в которую стремятся проникнуть атакующие. Как показывает статистика наиболее распространенных методов проникновения, приведенная в этом отчете, атаки через доверительные отношения — растущий тренд этого года.

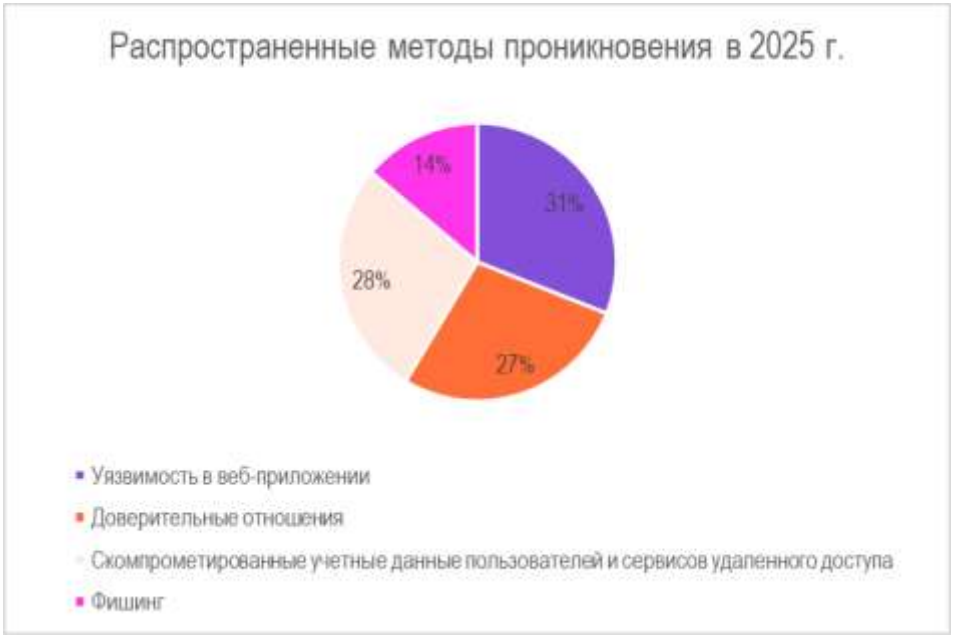
Цели атакующих

Доля атак с целью шпионажа по итогам десяти месяцев 2025 года выросла на 7 п. п. в сравнении с тем же периодом 2024 года — с 54 до 61%.

А вот доли финансово мотивированных атак и атак с целью хактивизма заметно снизились — в особенности доля хактивистских атак (с 22 до 11%). Как мы и предсказывали в начале года, количество «громких» атак для достижения политических целей продолжает падать. Вместо этого злоумышленники чаще фокусируются на сложных и скрытных атаках.

Способы первоначального проникновения

В этом году мы заметили значительное изменение распространенных методов первоначального проникновения.



Если в аналогичном периоде 2024 года 80% инцидентов происходили либо из-за уязвимости в веб-приложении, либо из-за скомпрометированных учетных данных, то в 2025 году стало значительно больше (27 против 8% в 2024 г.) инцидентов, в которых атакующие использовали доверительные отношения для первоначального проникновения. При этом доля успешных атак через уязвимости в веб-приложениях и скомпрометированные аккаунты сократилась.

Это говорит о том, что отношения с подрядчиками должны стать зоной особого внимания для ИБ-команд организаций, так как атакующие очевидно все чаще

эксплуатируют этот вектор. Рост количества инцидентов, где способом проникновения была инфраструктура подрядчика, указывает и на то, что группировки стали вкладывать больше ресурсов в предварительную разведку и накапливание доступов, что, в свою очередь, свидетельствует о повышении уровня профессионализма и ресурсной обеспеченности атакующих.

Длительность инцидентов

Метрика «Длительность инцидентов» описывает временной промежуток, в течение которого атакующие оставались в целевой инфраструктуре. По итогам 10 месяцев 2025 года заметно выросла (на 12 п. п.) доля атак продолжительностью от шести месяцев до года, а также инцидентов длительностью от года до двух лет (на 8 п. п).

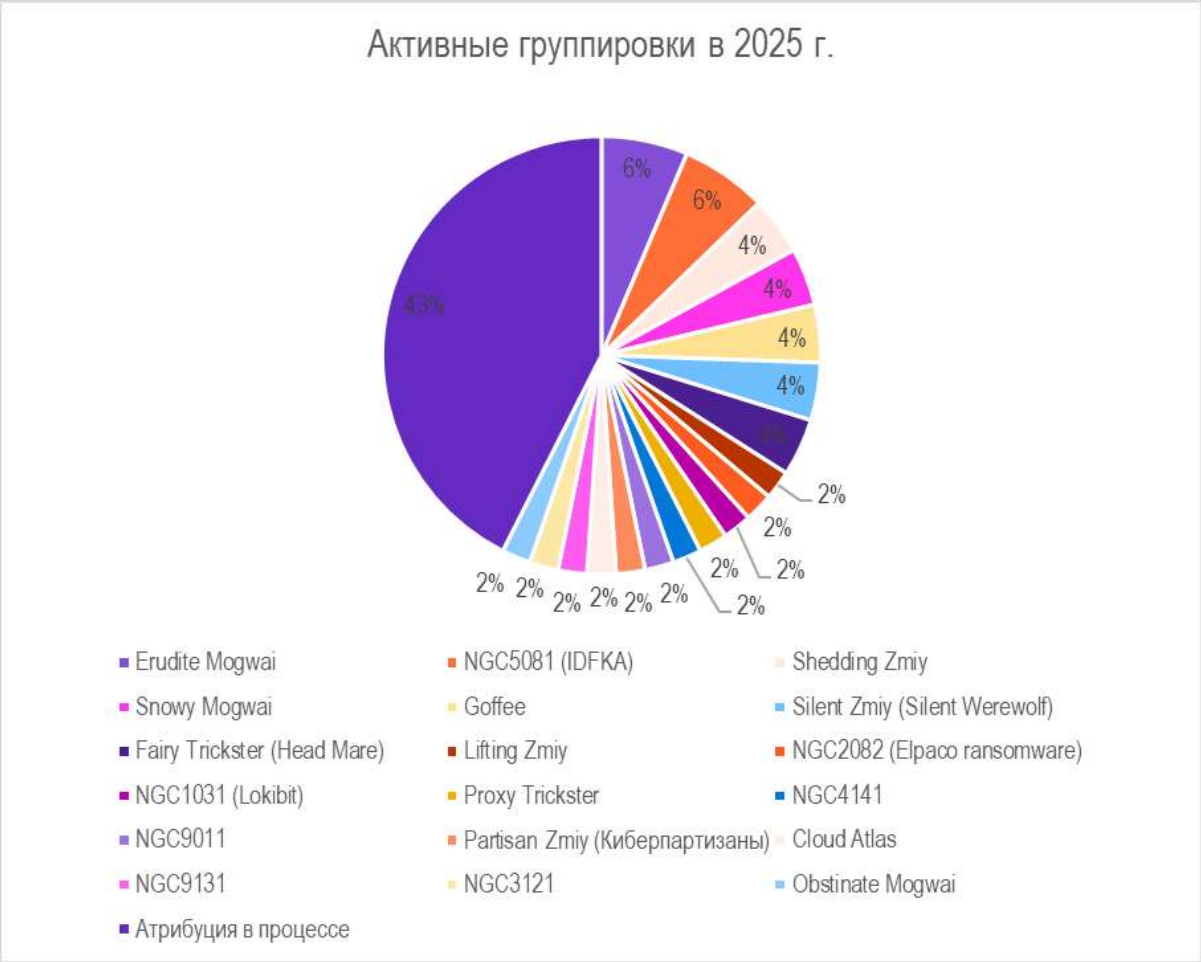
	Десять месяцев 2024 г.	**Десять месяцев 2025 г.**
До недели	20%	23%
До двух недель	10%	0
До месяца	16%	14%
До 6 месяцев	32%	25%
До 1 года	6%	19%
До 2 лет	6%	14%
2+ года	10%	5%

Рост количества длительных инцидентов коррелирует с увеличением числа шпионских атак. Группировки, специализирующиеся на подобных операциях, стремятся к максимально долгому скрытному присутствию в атакованной инфраструктуре.

Группировки и кластеры вредоносной активности

Активность группировок

Если попытаться описать ландшафт группировок и кластеров вредоносной активности за десять месяцев 2025 года, то мы бы выбрали определение «разнообразный». В нашем отчете за первое полугодие мы констатировали затрудненную атрибуцию: на тот момент мы столкнулись с большим количеством инцидентов, не относящихся ни к одному из известных нам кластеров, и атрибутировать удалось лишь 32% атак. По истечении 10 месяцев мы знаем, кто стоит за 57% инцидентов, но главное — мы видим немало новых кластеров и групп. Всего в 2025 году мы получили артефакты деятельности 18 групп и кластеров. Семь их них встречаются нам впервые.



В то время как за 10 месяцев 2024 года в поле нашего зрения попали восемь группировок и кластеров.

Как видно из диаграммы, самое значительное изменение коснулось активности группировки Shedding Zmiy, чью деятельность мы отслеживали в течение двух последних лет. Доля инцидентов, которые мы относим к этому кластеру, упала с 37 до 2%. В предыдущие два года эта группа своей активностью привлекла пристальное внимание ИБ-специалистов. Многие элементы ее арсенала стали хорошо известны, и, вероятно, поэтому группировка снизила масштабы деятельности. В целом масштаб деятельности проукраинских группировок значительно уменьшился. Если в первые десять месяцев 2024 года на них приходилось около 70% расследованных инцидентов, то в 2025 году их доля составляет менее 20%.

Снизила активность и другая в прошлом заметная группировка — Obstinate Mogwai. Зато Erudite Mogwai по сравнению с прошлым годом набирает обороты вместе с новой группировкой, которую мы называли Snowy Mogwai и чуть подробнее о которой расскажем в следующем разделе.

Некоторые группы стабильно присутствуют в чарте уже второй год. Помимо Shedding Zmiy и Obstinate Mogwai, это Fairy Trickster (Head Mare), Cloud Atlas и Lifting Zmiy. Последняя группировка пропала с наших «радаров» после серии инцидентов в первой половине прошлого года, но во второй половине 2025 года вновь начала атаковать.

Также мы зафиксировали невиданное ранее количество кластеров активности, обладающих уникальной морфологией, но пока не продемонстрировали достаточно артефактов деятельности, которые позволили бы нам привязать их к какой-либо ранее известной группировке или выделить в устойчивую новую: NGC1031, NGC9011, NGC9131, NGC5081, NGC3121, NGC2082 и NGC4141. Подробнее о некоторых из них мы расскажем в следующем разделе.

Характеристики активных группировок

Snowy Mogwai (UNC5174)

Snowy Mogwai — APT-группировка, также известная как UNC5174. Началом ее активности принято считать 2023 год, когда аналитики компании Mandiant зафиксировали применение данной группировкой уязвимости CVE-2023-46747 для удаленного выполнения кода с помощью интерфейса F5 BIG-IP Traffic Management (программы для балансировки нагрузки на сервер). Атакующие имеют характерный инструментарий в виде загрузчиков VShell и SNOWLIGHT, а также обширную сетевую инфраструктуру. Группа расследования 4RAYS наблюдает первые следы их атак начиная с осени 2024 года.

Ключевые инструменты, зафиксированные при расследовании:

- VShell
- SNOWLIGHT
- GOREVERSE

Цели: группировка атакует компании в сфере телекоммуникационных услуг и информационных технологий, научно-исследовательские и государственные организации с целью шпионажа. Также Snowy Mogwai была замечена при атаках на энергетические компании.

Географически их атаки были направлены на США, Канаду, Индию, страны юго-восточной Азии, государства Европы: Великобританию, Францию и другие, включая Россию).

Опираясь на данные из открытых источников, а также знания о тактиках, техниках и инструментах атакующих, можно утверждать, что группировка имеет восточноазиатское происхождение, в связи чем в соответствии с нашей таксономией мы присвоили ей наименование Snowy Mogwai.

Partisan Zmiy (Киберпартизаны)

Partisan Zmiy — хактивистская группировка, также известная как «Киберпартизаны». Согласно информации из открытых источников, группа сформировалась в 2020 году гражданами Беларуси. В течение двух лет она активно атаковала государственные структуры и средства массовой информации Беларуси, а начиная с 2022 года фиксируется смещение географии ее атак и расширение активности на Российскую Федерацию. Сотрудничает с рядом восточноевропейских хакерских группировок.

Несмотря на очевидные действия по привлечению внимания к своей активности, «Киберпартизаны» выходят за рамки типичного хактивизма, проявляя признаки высокой организованности и продвинутых технических навыков, что характерно для APT-группировок.

В результате расследования инцидентов и изучения их деятельности можно со средней степенью уверенности предположить, что помимо хактивизма группа специализируется на шпионаже. В связи с чем мы классифицируем «Киберпартизанов» как Partisan Zmiy — подкатегорию APT-группировок, имеющих восточноевропейское происхождение.

Мы заметили первые следы их атак в России в конце 2024 года.

Группировка обладает большим инструментарием:

- Vasilek
- Prianik
- 3proxy
- Gost proxy
- ProcDump
- Forklift
- PartisansDNS

Цели: группировка атакует государственные организации, транспортные и телекоммуникационные компании. Их основная задача — создать общественный резонанс и привлечь внимание к своей активности, а также нанести прямой ущерб жертве.

Географически их атаки были нацелены на Россию и Республику Беларусь.

Silent Zmiy (XDSpy)

Silent Zmiy — группировка атакующих, также известная как XDSpy, активность которой впервые зафиксирована в 2011 году. В отличие от многих других группировок проукраинской направленности Silent Zmiy не стремится публично комментировать собственные атаки, и вообще тяготеет к анонимности и максимально скрытной деятельности, что характерно для профессиональных APT-группировок. За их «молчаливость» мы назвали группировку Silent Zmiy. Обладает характерным инструментарием. Чаще всего, точкой первичного доступа являются фишинговые письма.

Ключевые инструменты:

- XDSpy
- CHMDownloader
- DSDownloader
- XDigo
- forfiles
- ETDownloader
- NSDownloader

Цели: промышленные предприятия, медицинские учреждения, государственные организации.

В отношении этой группировки мы наблюдали только фишинговые рассылки на заказчиков осенью 2025 года, которые не привели к развитию атаки, в связи с чем мы не располагаем полным набором тактик, техник и процедур этой группы. Недавнюю активность Silent Zmiy (XDSpy) описывали наши коллеги из компании BI.ZONE.

Географически атаки направлены на Россию, Республику Беларусь, Сербию.

Учитывая выбор целей и специфику фишинговых писем атакующих, можно с низкой степенью уверенности утверждать, что они являются выходцами из Восточной Европы.

GOFFEE

GOFFEE — проукраинская группировка атакующих, начавшая активную деятельность в 2022 году. Обладает обширными ресурсами, что позволяет ей проводить комплексные атаки. При этом атакующие не концентрируются на каком-то конкретном типе целей, а стараются атаковать как можно большее число жертв. В исследованных нами инцидентах для первичного доступа ими использовались скомпрометированные учетные записи VPN, а также уязвимая конфигурация веб-приложения. Впервые команда Solar 4RAYS столкнулось с активностью данной группировки в 2022 году.

Группировка имеет обширный арсенал инструментов. В рамках расследований были зафиксированы:

- Mythic Agent
- Cobalt Strike
- QwakMyAgent
- DumpIt
- SspiUacBypass
- Impacket PsExec
- Owowa
- PowerTaskel
- VisualTaskel

Цели: группировка сосредоточена на шпионаже, не ограничиваясь какой-то конкретной отраслью. Например, в этом году мы зафиксировали несколько атак на IT-организации, а в позапрошлом году — на государственные организации.

Основной географической целью является Россия.

Fairy Trickster (Rainbow Hyena, Hade Mare)

Fairy Trickster — группировка, также известная как Hade Mare. Началом ее деятельности считается 2023 год. Fairy Trickster активно публикует информацию о своей деятельности в открытых источниках. Несмотря на заявленную хактивистскую направленность, группировка ведет активную деятельность по шифрованию жертв с целью вымогательства, а также собирает конфиденциальную информацию с целью ее продажи. Впервые Solar 4RAYS обнаружил следи их атак в России в середине 2024 года.

Инструменты:

- MeshAgent
- LockBit 3.0
- PhantomProxyLite
- Rust SOCKS5 Proxy
- T1ck3tDump
- PhantomTaskShell

Цели: группировка атакует организации любой сферы деятельности — от государственных структур до частных компаний. Основная направленность атак — монетизация атаки различными способами, будь то шифрование жертв с целью вымогательства или продажа конфиденциальных данных.

Географически их основными целями является Российская Федерация и Республика Беларусь.

Другие группировки и кластеры вредоносной активности

На фоне устойчивого роста киберугроз на момент октября 2025 года мы зафиксировали увеличение количества инцидентов, связанных с использованием шифровальщиков, которые распространяются по модели Ransomware-as-a-Service.

Ransomware-as-a-Service (RaaS) — это бизнес-модель, используемая киберпреступниками, при которой вредоносное ПО распространяется по аналогии с лицензионным ПО. Данная модель позволяет атакующим получить готовое вредоносное ПО для извлечения прибыли из кибератак.

Одним из таких шифровальщиков, распространяемых по модели RaaS, является LokiLocker / BlackBit, который был обнаружен в рамках расследования одного из инцидентов.

Образец ВПО, полученный при расследовании, был написан на языке RUST. По данным из открытых источников, данный шифровальщик ассоциируется с группировками из региона Ближнего/Среднего Востока. У LokiLocker / BlackBit есть ряд отличительных черт:

- Наличие официального портала Black Bit Premium, с которого атакующие загружают вредоносное ПО на скомпрометированные системы.
- Владельцы RaaS самостоятельно компилируют программу-вымогатель для атакующих.

Подробный анализ семейства LokiLocker / BlackBit доступен в публикации наших коллег из команды F6 (https://www.f6.ru/blog/lokilocker-blackbit-ransomware/).

Также нами был выявлен шифровальщик ELPACO-team ransomware. Отличительной особенностью ELPACO-team ransomware является наличие удобного графического интерфейса, который позволяет оператору гибко использовать вредоносное ПО в зависимости от своих потребностей. Более того, атакующий может использовать специальный файл конфигурации для более быстрой настройки. После завершения шифрования шифровальщик удаляется с системы, что препятствует его анализу.

В нескольких случаях мы обнаруживали активность вредоносного ПО класса «червь» (worm). В обоих случаях данные образцы остались от ранее произошедших инцидентов. Важно отметить, что для правильного реагирования на инциденты необходимо проверять всю инфраструктуру на наличие следов компрометации, иначе в ней могут остаться следы заражения.

В октябре 2025 года мы впервые зафиксировали активность новой группировки — NGC5081, которая демонстрирует высокий уровень профессионализма и, судя по всему, действует в рамках целенаправленных атак на высокозащищенные

организации. В отличие от большинства группировок NGC5081 используют собственный уникальный инструментарий, о котором мы расскажем в ближайшей статье нашей команды.

Интересные тактики и техники

Как и в предыдущем отчете за первое полугодие, мы решили систематизировать и проанализировать ключевые методы, используемые злоумышленниками в инцидентах, расследованных командой Solar 4RAYS. В основу анализа, как и в прошлый раз, ляжет матрица **MITREATT&CK**. Мы выделили 5 тактик Initial Access, Execution, Persistence, Lateral Movement и Defense Evasion, в которых отметили наиболее интересные техники.

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: Domain Accounts ID: T1078.002;

Valid Accounts: Local Accounts ID: T1078.003;

Replication Through Removable Media ID: T1091;

External Remote Services ID: T1133;

Phishing ID: T1566;

Phishing: Spearphishing Attachment ID: T1566.001;

Phishing: Spearphishing Link ID: T1566.002.

Правильно настроенный веб-сервис — безопасный веб-сервис

За последний год мы неоднократно сталкивались с инцидентами, в которых атакующие эксплуатировали стандартные или небезопасные настройки веб-сервисов. Так, в одном из инцидентов злоумышленники получили доступ к панели администрирования веб-приложения, использовав учетную запись с правами, эквивалентными правам системного администратора. Сама учетная запись имела словарный пароль. При этом доступ к интерфейсу можно было получить из внешней сети, что привело к компрометации части инфраструктуры.

В другом инциденте на веб-сервере с ПО Bitrix использовалась некорректная настройка веб-приложения. При установке ПО Bitrix важно полностью завершить базовую настройку веб-приложения, иначе атакующие смогут получить доступ к файлу **restore.php**. Данный файл предназначен для восстановления веб-приложения из резервной копий, что позволяет ему размещать файлы на веб-сервере, чем и воспользовались злоумышленники, разместив на системе вредоносное ПО.

Доверительные отношения — слабое звено в безопасности

В 2025 году мы наблюдаем значительный рост количества атак через доверительные отношения между организациями (дочерними компаниями, поставщиками, подрядчиками и др.). Связь заказчика и подрядчика, построенная на доверии, часто становится уязвимым местом в информационной безопасности.

Чтобы проиллюстрировать данный тезис, приведем пример инцидента, в котором злоумышленники использовали учетную запись пользователя одного из подрядчиков для атаки на инфраструктуру заказчика. При реагировании мы уведомили заказчика о необходимости блокировки данной учетной записи. Заказчик рекомендации выполнил, однако договориться о предоставлении для анализа системы подрядчика, на котором работал скомпрометированный пользователь, не смог — подрядчик утверждал, что с его стороны компрометация невозможна.

Через две недели заказчик, не согласовав свои действия с нами, решил разблокировать скомпрометированную учетную запись. Предварительно он договорился с подрядчиком о смене пароля учетной записи. После чего заказчик через 24 часа снова зафиксировал нелегитимный вход скомпрометированной учетной записи и инцидент повторился.

Получив в итоге систему подрядчика с скомпрометированной учетной записью на исследование, был подтвержден факт ее компрометации. Отдельно стоит отметить, что в системе были обнаружены файлы, содержащие пароли в открытом виде, что является грубейшим нарушением правил информационной безопасности.

К сожалению, это не единичный случай. Достаточно часто в рамках расследования инцидентов мы выявляем проблемы у заказчика при соблюдении им мер информационной безопасности. Подробно о том, как защитить свою организацию от возможной атаки через доверительные отношением, мы писали в посте в нашем телеграм-канале.

Выполнение (Execution)

Распространенные техники, зафиксированные в инцидентах:

Command and Scripting Interpreter: PowerShell ID: T1059.001;

Command and Scripting Interpreter: Windows Command Shell ID: T1059.003;

Command and Scripting Interpreter: Unix Shell ID: T1059.004;

Command and Scripting Interpreter: Visual Basic ID: T1059.005;

Command and Scripting Interpreter: Python ID: T1059.006;

Deploy Container ID: T1610;

Scheduled Task/Job ID: T1053;

Scheduled Task/Job: Cron ID: T1053.003;

Scheduled Task/Job: Scheduled Task ID: T1053.005;

System Services ID: T1569;

System Services: Service Execution ID: T1569.002;

User Execution: Malicious File ID: T1204.002;

Windows Management Instrumentation ID: T1047ю

Использование легитимных функций веб-приложения для выполнения вредоносных задач

Одной из распространенных техник, используемых злоумышленниками при атаках на веб-приложения, является эксплуатация его встроенных функций, предназначенных для управления и автоматизации. Характерным примером использования таких функций может служить инцидент, описанный в нашей статье про группировку NGC4141, где для доставки вредоносного ПО использовалось API веб-приложения.

Но нередки случаи, когда встроенные функции веб-приложения помогают атакующим выполнять команды на атакуемой системе. Так, в одном из недавних инцидентов мы обнаружили интересную функцию у веб-приложения, которая позволяла создавать задачи и выполнять их в рамках приложения.

Использовав учетные данные пользователя с привилегиями root, атакующие смогли пройти аутентификацию в веб-интерфейсе приложения и получить доступ к панели администрирования. Панель администрирования имела специальную функцию «Планировщик задач» для автоматизации администрирования веб-приложения. «Планировщик» позволял создавать задачи, содержащие скрипты, которые выполнялись на уровне веб-приложения. Злоумышленники смогли проэксплуатировать данную функцию путем вставки в скрипты для задач кода, который позволял выполнять команды на уровне операционной системы. Результаты выполнения атакующие получали через перехват ошибок веб-приложения. Таким образом атакующие проводили разведку на атакуемой системе.

При расследовании инцидентов, связанных с веб-приложениями, помимо общего анализа артефактов на системе необходимо исследовать и принципы работы веб-приложения. Потому что именно они могут служить инструментом в руках атакующих.

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: Systemd Service T1543.002;
- 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.

Опасные комбинации

Одна из самых устойчивых и эффективных техник атакующих — это закрепление в системе через системные сервисы. При расследовании инцидентов мы достаточно часто сталкивались с ее применением. Техника позволяет не только запустить вредоносное ПО, но и скрыть активность атакующих.

Более сложной техникой закрепления является компрометация исполняемых файлов на системе жертвы. Согласно **MITRE ATT&CK,** злоумышленники могут внедрить вредоносный код в легитимный компонент программы, что значительно усложняет их обнаружение. Однако данная техника распространяется не только на бинарные файлы, но и на скрипты.

Сочетание этих двух техник позволяет достичь не только закрепления вредоносного файла на системе, но и его сокрытие от обнаружения. В одном из инцидентов мы видели такую комбинацию.

Вредоносное ПО не было напрямую связано с легитимным сервисом Gitlab, однако использовало его для запуска.

Атакующие модифицировали легитимный скрипт Gitlab, отвечающий за запуск компонентов данного ПО. В результате модификации при запуске или перезагрузке легитимной службы Gitlab кроме запуска легитимного ПО также выполнялся запуск вредоносного ПО, что обеспечивало надежное и скрытное закрепление на системе.

Базы данных хранят не только данные

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

Злоумышленники, получив права системного администратора, создали в базе данных PostgreSQL веб-приложения TrueConf Server бэкдор, состоящий из функции и триггера. Ввод данных в поля для аутентификации с ключевыми словом/строкой позволял выполнять произвольные SQL-запросы, в том числе с помощью функции COPY сохранять данные из запроса в файлы на системе, например для создания веб-шеллов.

Само создание бэкдора стало возможным лишь благодаря правам системного администратора, полученным в рамках компрометации инфраструктуры, и не связано с какой-либо уязвимостью приложения или его базой данных. При этом обнаружить данный бэкдор, не обладая достаточной экспертизой в области баз данных, достаточно тяжело, так как запрос с ключом перехватывается функцией и не логируется.

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 ходе анализа расследованных инцидентов мы отмечаем, что атакующие продолжают активно использовать классические техники для горизонтального перемещения по зараженной инфраструктуре. Наиболее распространенными инструментами на этом этапе остаются RDP, SSH, SMB.

Атакующие не прибегают к экзотическим или сложным методам для горизонтального перемещения, так как вышеуказанные протоколы удаленного подключения позволяют:

- полноценно взаимодействовать с атакуемой системой;
- эксплуатировать уязвимые политики/настройки в инфраструктуре;
- маскировать свою активность под деятельность системных администраторов.

Уклонение от обнаружения (Defense 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.

Маскировка включена

Маскировка вредоносного ПО и его процессов — неотъемлемая часть комплексных атак на инфраструктуру. Продвинутые атакующие целенаправленно исследуют атакуемые системы с целью понять, какой способ сокрытия своей активности будет наиболее подходящим. Особенно это актуально для Unix-подобных систем, которые при наличии достаточных навыков у злоумышленников позволяют им продолжительное время скрываться в зараженной инфраструктуре. Подтверждением этому может служить активность атакующих в одном из следующих инцидентов.

Для скрытия вредоносного программного обеспечения атакующие, разместив и запустив его, удалили его файл. В памяти системы остался вредоносный процесс, замаскированный путем мимикрии под легитимный. При этом для каждой системы имя вредоносного процесса подбиралось индивидуально. В случае перезагрузки процесс был бы остановлен, однако для работы ВПО были выбраны системы, которые практически не перезагружались, что обеспечило атакующим стабильное закрепление на системе.

Помимо этого, атакующие обладали обширной сетевой инфраструктурой, которая имитировала доменные имена заказчика, что также способствовало сокрытию их активности.

Выводы и рекомендации

Мы заканчивали анализ ландшафта сложных киберугроз в первом полугодии 2025 года тезисом о том, что период прошел относительно «спокойно». Меньше атакованных индустрий, меньше разрушительных атак, а группировки, до этого представлявшие наибольшую угрозу, снизили активность. По итогам прошедших с тех пор четырех месяцев мы можем сказать, что «затишье» сменилось «оживлением»: во втором полугодии последовало несколько громких заявлений об атаках на транспортные и торговые организации, и мы зафиксировали рост интенсивности атак на важные отрасли, такие как промышленность, IT и энергетика. Очевидно, что атакующие сменили тактики — выросло количество инцидентов, где проникновение в организации происходило из-за недочетов в безопасности их подрядчиков, в дополнение к этому число группировок и кластеров значительно выросло. Мы предполагаем, что в 2026 году доля атак с целью шпионажа против критических для экономики России отраслей, как минимум, не снизится — растущая напряженность в сфере геополитики будет тому способствовать. В отношении коммерчески мотивированных атак основной угрозой останется вымогательство — в 2025 году мы стали чаще встречать атаки с помощью ПО, распространяемого по модели Ransomware-as-a-Service, что может указывать на снижение порога входа в этот криминальный бизнес. Наконец, со средней степенью уверенности мы ожидаем, что в 2026 году обнаружим больше свидетельств использования злоумышленниками технологии искусственного интеллекта в подготовке и проведении целевых атак.

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

1. Усильте контроль за подрядчиками, у которых есть сетевая связанность с вашей инфраструктурой. Строго контролируйте удаленный доступ в инфраструктуру, особенно для подрядчиков. Атаки через них — растущий тренд.
2. Пристальное внимание уделяйте своевременному обновлению ПО и защите веб-приложений (WAF). Атаки через уязвимости в веб-приложениях остаются самым распространенным способом первоначального проникновения, а WAF поможет заблокировать вредоносный трафик и предотвратить взломы на уровне приложений.
3. Соблюдайте парольные политики, пользуйтесь сервисами мониторинга утечек учетных записей и вовремя их обновляйте. Использование утекших учетных записей для входа в информационную систему — 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. Создавайте бэкапы, 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 получать полную картину значимых для безопасности событий в инфраструктуре и вовремя обнаруживать нежелательные.
7. Делайте оценку компрометации регулярно и в случае подозрения на атаку не медлите с привлечением специалистов по реагированию на инциденты.
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.