4RAYS by SOLAR

SOLAR 4RAYS: ХРОНИКИ РАССЛЕДОВАНИЙ ИНЦИДЕНТОВ В 2025 ГОДУ

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 профессиональных взломщиков, преследующих финансовые цели или работающих в интересах иностранных правительств. Как правило, это инциденты, которые произошли по двум причинам: злоумышленники смогли обойти использовавшиеся в атакованных организациях автоматизированные средства защиты, или в организации просто не было 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 счете выстроить эффективную защиту ИТ-инфраструктуры от профессиональных киберпреступников.

В основе отчета — данные, собранные в ходе расследований, проведенных в 2025 году. Также исследование содержит данные 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. Этот отчет — финальная версия отчета, который мы публиковали в ноябре 2025 года.

Ключевые тренды

- Количество инцидентов, расследованных командой Solar 4RAYS в 2025 году, осталось ровно на том же уровне, что и в 2024-м.

- Количество атакованных профессиональными хакерами сфер экономики сократилось с 19 до 10: госорганы, промышленность, IT, здравоохранение и энергетика — в топе. Организации из отрасли энергетики попали в поле пристального внимания злоумышленников в 2025 году впервые за историю наших наблюдений.

- Доля атак с целью шпионажа выросла на два процентных пункта (п. п.) — 60% всех инцидентов были связаны с охотой за конфиденциальными данными. Атаки хактивистов упали на 3 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 2024 году на них приходилось около 70% расследованных инцидентов, то в 2025 году их доля сократился до 23%.

- В 2025 году увеличилось количество группировок и кластеров вредоносной активности. В 2024 году Solar 4RAYS отследили деятельность девяти группировок, а в 2025-м — уже 18. Многие из них — ранее неизвестные группы и кластеры.

- Каждый пятая расследованная атака длилась от 6 месяцев до года. Доля таких атак возросла на значительные 13 п. п. Это указывает на стремление атакующих к длительному присутствию в инфраструктурах компаний-жертв.

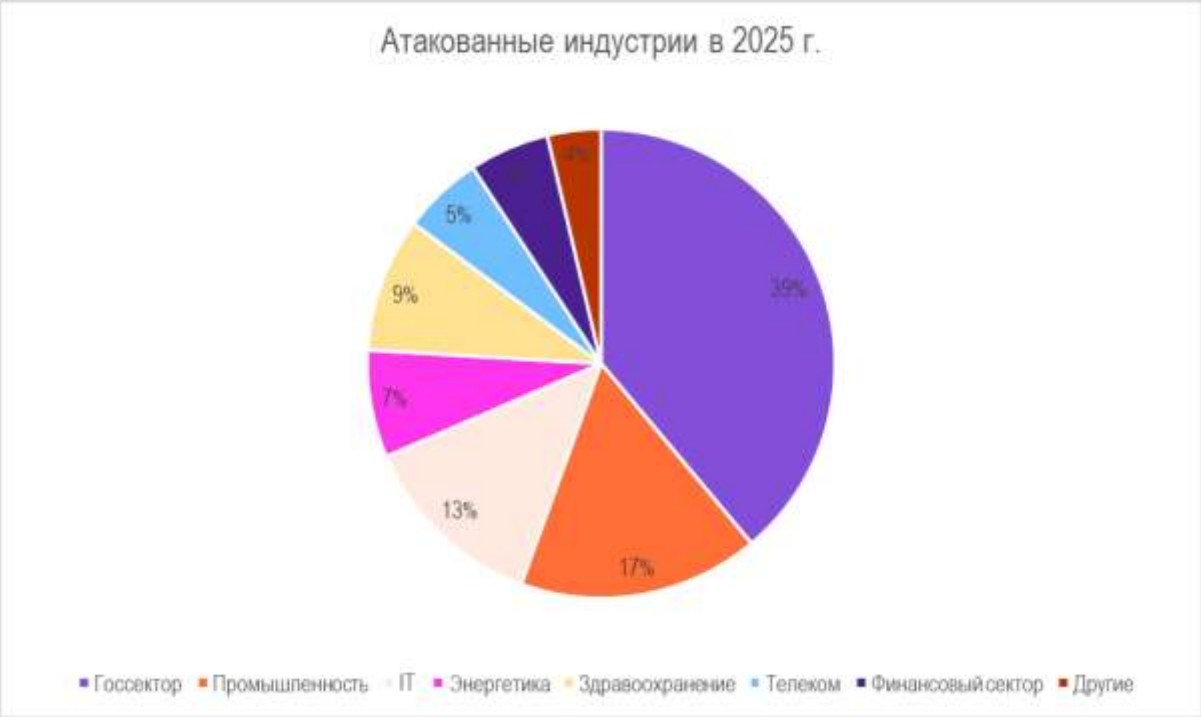
- Уязвимости в веб-приложениях остаются наиболее распространенным способом первоначального проникновения хакеров, **однако в 2025 году значительный рост показали атаки через подрядчиков. В 24% случаев атакующие проникали в организации именно так.** Годом ранее на такие инциденты приходилось всего 6%.

4RAYS by SOLAR

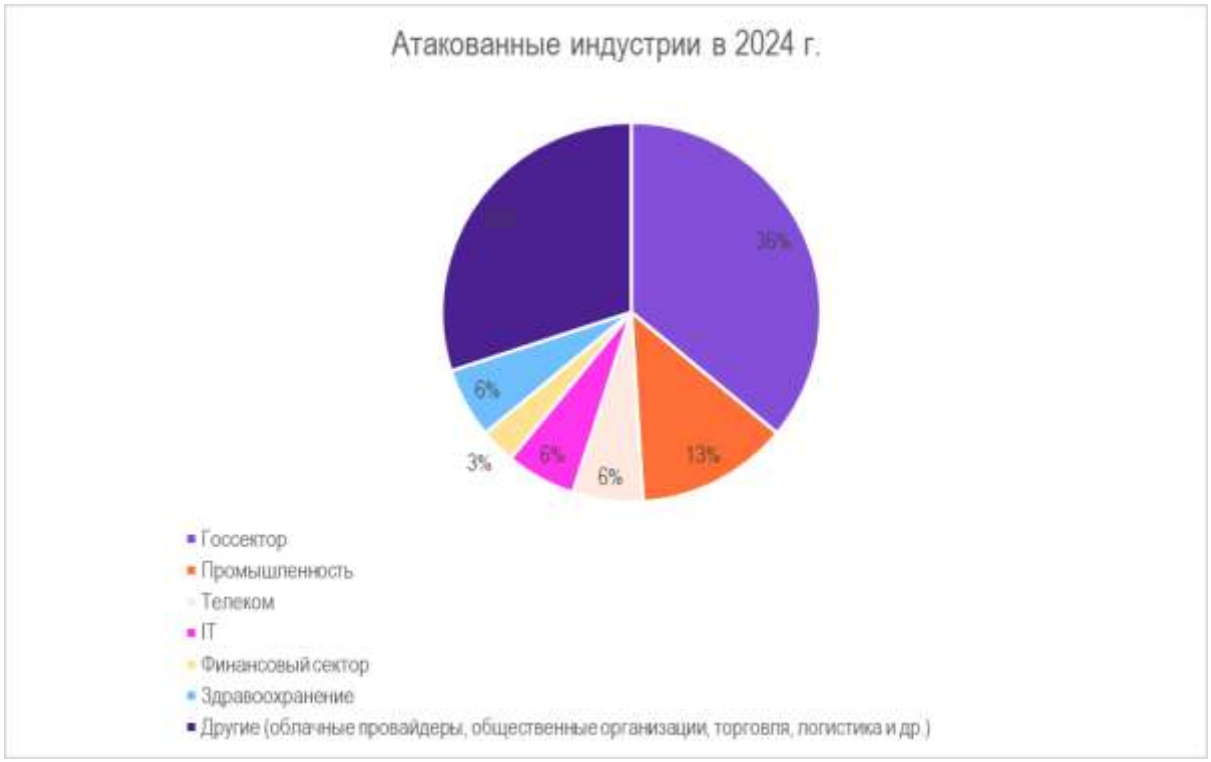
ОБЗОР ИНЦИДЕНТОВ

Кого атакуют

За 2025 год эксперты Solar 4RAYS расследовали киберинциденты в организациях из 10 различных отраслей, включая госсектор, телеком, промышленность, IT. В категорию «Другие» попали организации из сферы ретейла, транспорта и научных исследований.



По сравнению с 2024 годом незначительно (на 3 п. п.) выросла доля инцидентов в госсекторе, также увеличилась доля атак на промышленность и IT-компании — причем в отношении последней отрасли доля исследованных кибератак выросла почти в два раза — в том числе потому, что IT-компании часто являются подрядчиками других организаций и атакующие через них пытаются добраться до более крупных целей. Статус подрядчика часто означает наличие сетевой связанности у IT-компании и организации, в которую стремятся проникнуть атакующие. Как покажет статистика наиболее распространенных методов проникновения, представленная в этом отчете, атаки через доверительные отношения — растущий тренд этого года.
Кроме того, мы стали фиксировать инциденты на предприятиях сферы энергетики (7% инцидентов) — 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 — геополитические события тому способствуют.


Атакованные индустрии в 2024 г.
36%
13%
6%
6%
3%
6%
Госсектор
Промышленность
Телеком
IT
Финансовый сектор
Здравоохранение
Другие (облачные провайдеры, общественные организации, торговля, логистика и др.)

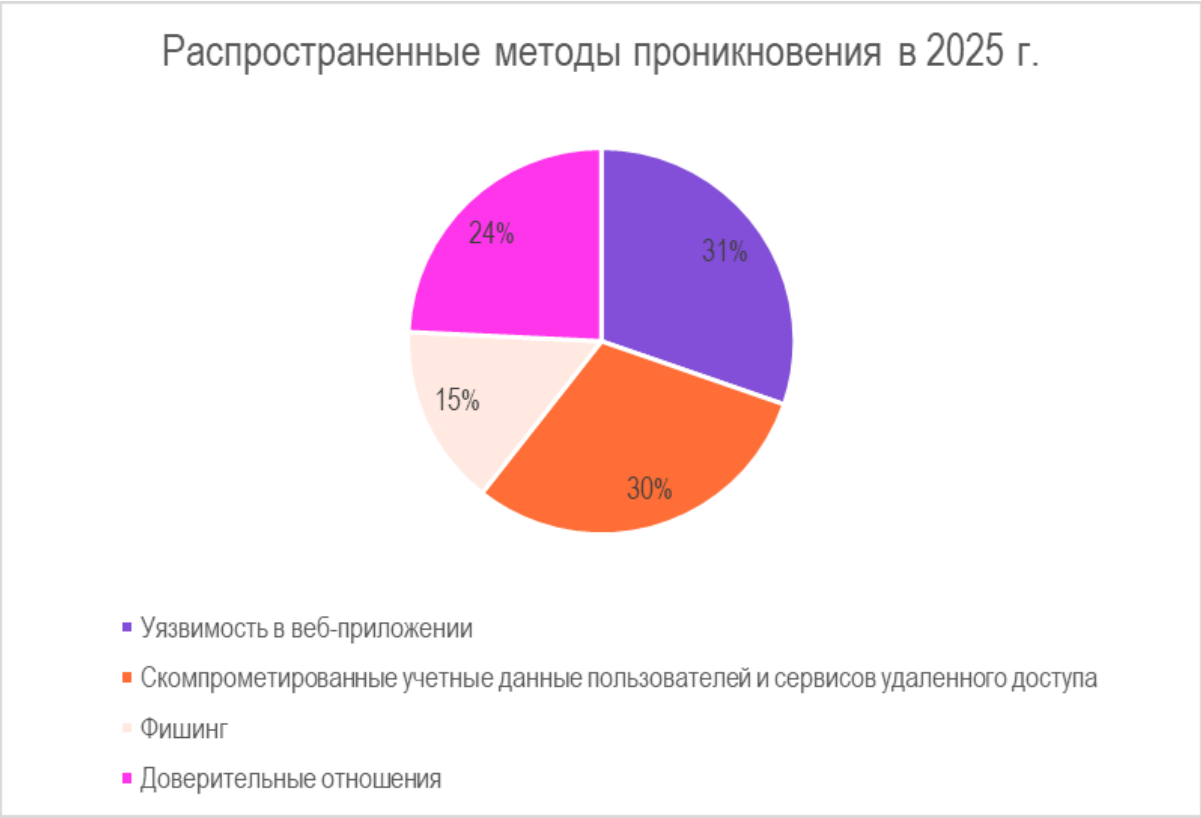
Цели атакующих

Доля атак с целью шпионажа по итогам 2025 года выросла на два п. п. в сравнении с 2024-м — с 58 до 60%.

Доля финансово-мотивированных атак осталась неизменной, а доля хактивизма немного снизились — с 19 до 16%. Когда мы сравнивали статистику за неполный 2025 год, падение доли хактивизма было более значительным — с 22% в 2024 году до 11% по итогам такого же периода 2025-го. Однако и в 2024-м, и в 2025-м в ноябре и декабре случилась серия политически мотивированных атак, которая сократила разрыв. И все же хактивизм демонстрирует тренд на снижение. Как мы и предсказывали в начале 2025 года, количество «громких» атак с политическими целями продолжает падать. Вместо этого злоумышленники чаще фокусируются на сложных и скрытных атаках.

Способы первоначального проникновения

В этом году мы заметили значительные изменения в распространенных методах первоначального проникновения.



Если в аналогичном периоде 2023 года 80% инцидентов происходило либо из-за уязвимости в веб-приложении, либо из-за скомпрометированных учетных данных, то в 2025 году стало значительно больше (24% против 6% в 2024 г.) сложных кибератак, в которых атакующие использовали доверительные отношения для первоначального проникновения. При этом доля успешных атак через уязвимости в веб-приложениях и скомпрометированные аккаунты упала.

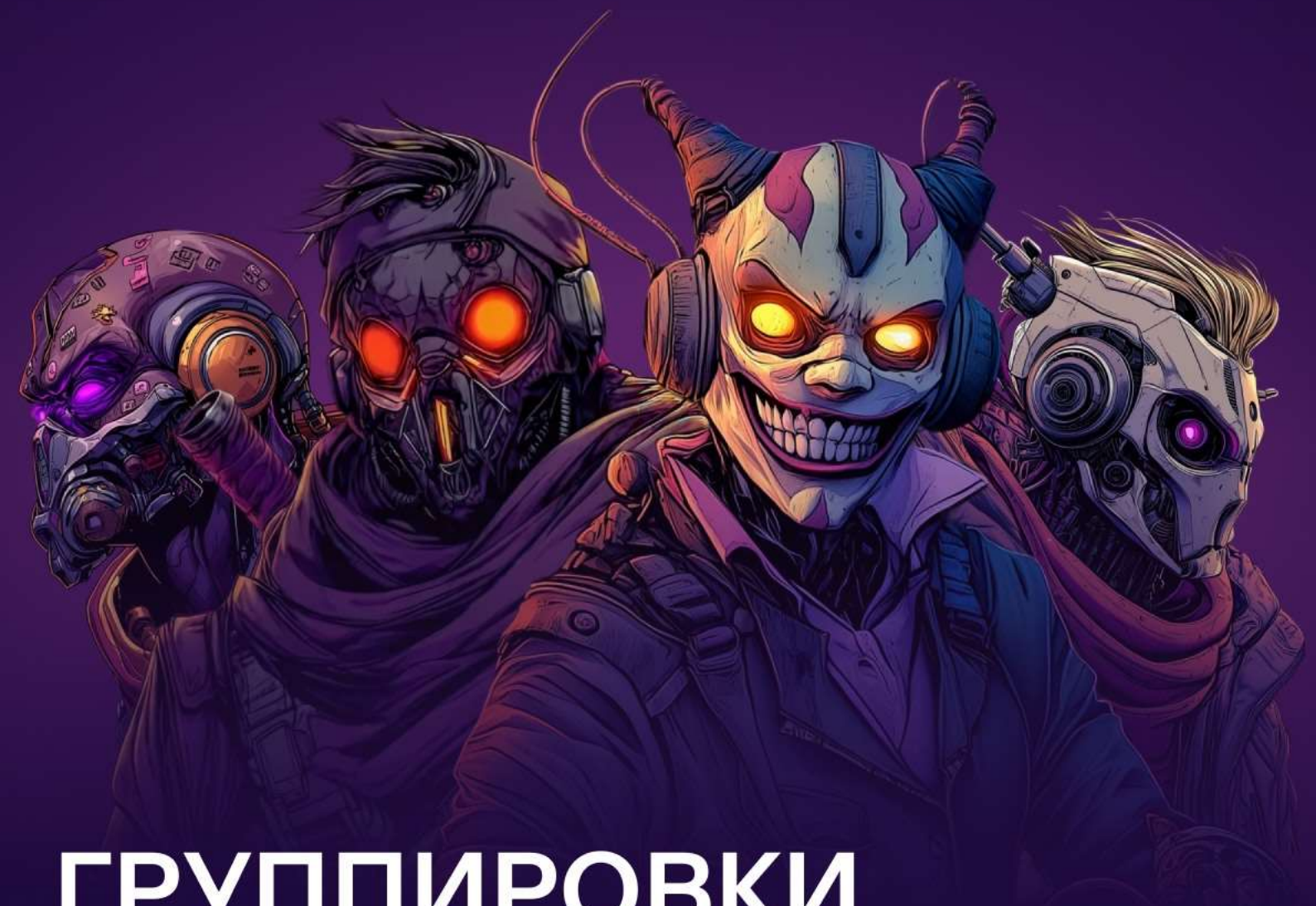
Это говорит о том, что отношения с подрядчиками должны стать зоной особого внимания для ИБ-команд организаций, так как атакующие очевидно все чаще эксплуатируют этот вектор. Рост количества инцидентов, где способом проникновения стала инфраструктура подрядчика, указывает и на то, что группировки стали вкладывать большее количество ресурсов в предварительную разведку и накапливание доступов, что указывает на рост профессионализма и ресурсной обеспеченности атакующих.

Длительность инцидентов

Метрика «Длительность инцидентов» описывает временной промежуток, в течение которого атакующие оставались в целевой инфраструктуре. По итогам 2025 года заметно (на 14 п. п.) выросла доля атак продолжительностью от шести месяцев до года, а также доля инцидентов длительностью до месяца (на 7 п. п).
Рост длительных инцидентов коррелирует с увеличением числа шпионских атак. Группировки, специализирующиеся на подобных операциях, стремятся к максимально долгому скрытному присутствию в атакованной инфраструктуре.

	2024 г.	**2025 г.**
До недели	25%	21%
До двух недель	13%	2%
До месяца	7%	14%
До 6 месяцев	21%	25%
До 1 года	9%	22%
До 2-х лет	14%	12%
2+ года	11%	2%

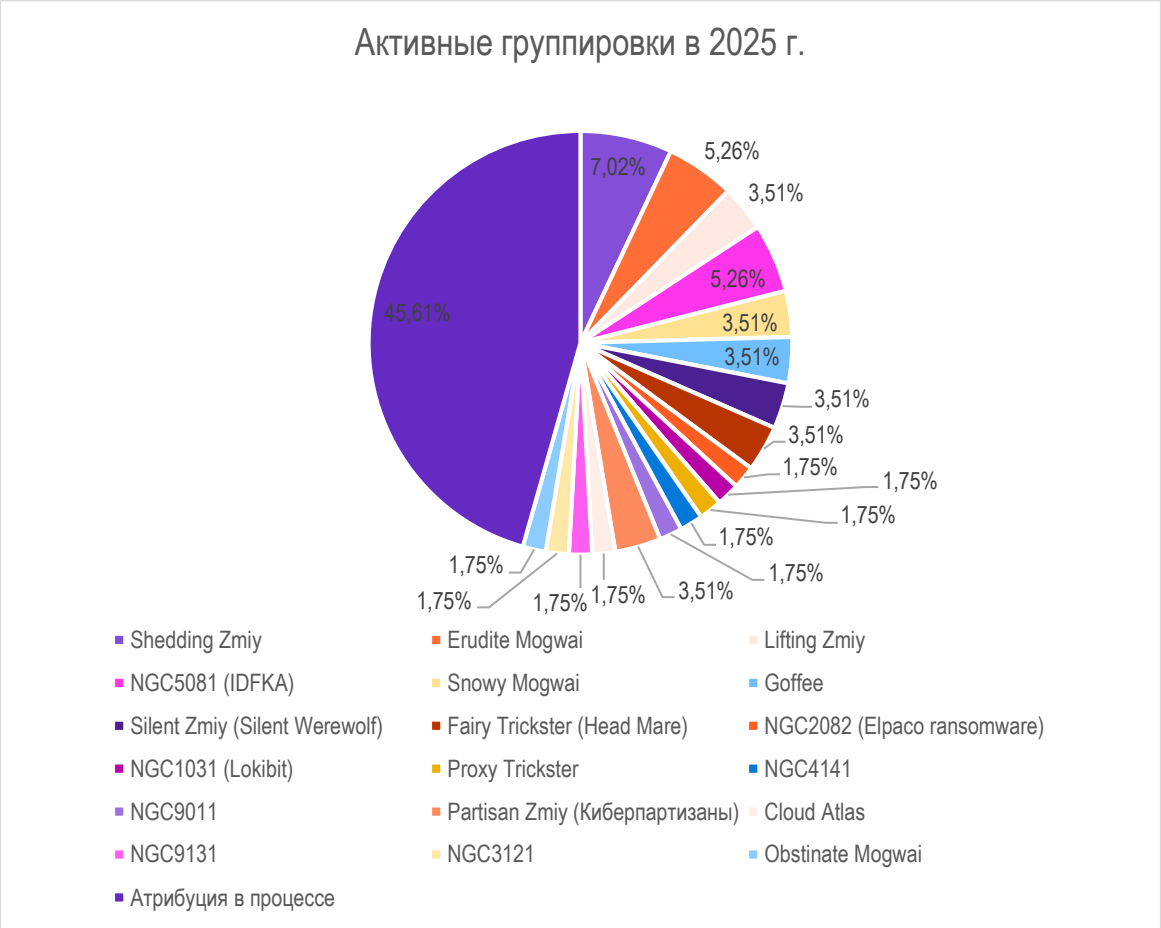
4RAYS by SOLAR



ГРУППИРОВКИ И КЛАСТЕРЫ ВРЕДОНОСНОЙ АКТИВНОСТИ

Активность группировок

Если попытаться описать ландшафт группировок и кластеров вредоносной активности за 2025 год, то мы бы выбрали «разнообразие». 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 прошествии года мы знаем, кто стоит за 54% инцидентов, но главное — мы обнаружили немало новых кластеров и групп: всего в 2025 году мы видели артефакты деятельности 18 групп и кластеров, семь их которых встретились нам впервые, в то время как за 10 месяцев 2024 года в поле нашего зрения попало восемь группировок и кластеров.



Как видно из графиков, 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 7%. 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 2024 году на них приходилось около 70% расследованных инцидентов, то в 2025 году их доля сократилась и составила менее чем 20%. Не исключено, что группировка снизила активность, чтобы обновить арсенал и вернуться к своим черным делам в новом году более подготовленной.

Менее активным стала 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, которые обладают 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 об одной 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 факт использования 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 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, страны Европы: Великобританию, Францию и другие, включая Россию.

Опираясь на данные из открытых источников, а также глядя на тактики, техники и инструменты 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 открытым источникам, группа была сформирована в 2020 году гражданами Беларуси. До 2022 года активно атаковала государственные структуры и средства массовой информации Беларуси. С тех пор фиксируется расширение ее активности и смещение географии атак на Российскую Федерацию. Сотрудничает с рядом восточно-европейских хакерских группировок.

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

В результате расследования инцидентов и исследования 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 восточно-европейское происхождение.

Первые следы атак данной группировки в России мы заметили в конце 2024 года. Самый громкий инцидент, связанный с группировкой, в 2025 году — летняя атака на инфраструктуру компании «Аэрофлот». Во второй половине года мы расследовали атаку группировки Partisan Zmiy, о которой расскажем в одной из ближайших статей.

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, 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 предпочитает публично не комментировать собственные атаки, стремится к анонимности и максимально скрытной деятельности, что характерно для профессиональных APT-группировок. За эту «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:

Атакует промышленные предприятия, медицинские учреждения, государственные организации.

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

Географически атаки направлены на Россию, Беларусь, Сербию.

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

GOFFEE

GOFFEE — проукраинская группировка атакующих, начавшая активную деятельность в 2022 году. Обладает обширными ресурсами, что позволяет проводить комплексные атаки. При этом атакующие не концентрируются на каком-то конкретном типе целей, а стараются атаковать как можно большее число жертв. В инцидентах, которые мы расследовали, 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 большой арсенал инструментов.

В рамках расследований были зафиксированы:

- Mythic Agent
- Cobalt Strike
- QwakMyAgent
- DumpIt

- SspiUacBypass
- Impacket PsExec
- Owowa
- PowerTaskel
- VisualTaskel

Цели:

Группировка сосредоточена на шпионаже и не ограничивается какой-то конкретной отраслью. Например, в этом году мы обнаружили несколько атак на IT-организации, а в позапрошлом году — на государственные организации.

Основной географической целью является Россия.

NGC5081

В октябре 2025 года мы впервые зафиксировали активность новой группировки — NGC5081. Она демонстрирует высокий уровень профессионализма и, судя по всему, действует в рамках целенаправленных атак на высокозащищенные организации. В отличии от большинства других группировок NGC5081 используют собственный уникальный инструментарий: в частности, написанный на языке Rust и оттого крайне сложный для анализа бэкдор IDFKA. NGC5081 отличаются скрытным поведением: мимикрировали под процессы и установленное легитимное ПО в системах, а также под подрядчиков жертвы в C2.

Инструменты:

- IDFKA
- TinyShell

Цели:

Атаки на телекоммуникационные компании на территории России.

Fairy Trickster (Rainbow Hyena, Head 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 столкнулись со следами их атак в России в середине 2024 года.

Инструменты:

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

Цели:

Группировка атакует организации любого сектора — от государственных структур до частных компаний. Основная направленность — монетизация атаки различными способами, будь то шифрование жертв с целью вымогательства или продажа конфиденциальных данных.

Географически их основными целями является Российская Федерация и Беларусь.

Другие группировки и кластеры вредоносной активности

На фоне устойчивого роста киберугроз в 2025 году 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 стран Среднего/Ближнего Востока. У LokiLocker/BlackBit есть ряд отличительных черт:

- Существует официальный портал «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/).

Отдельно был зафиксирован 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 затрудняет его анализ.

В нескольких случаях мы обнаруживали активность вредоносного ПО класса «червь» (worm) — 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.

4RAYS by SOLAR

НЕОБЫЧНЫЕ ТАКТИКИ И ТЕХНИКИ

За год активных расследований инцидентов команда 4RAYS столкнулась с множеством различных методов, используемых атакующими. Мы решили выделить наиболее «интересные» из них и систематизировать их при помощи матрицы **MITRE ATT&CK**. В результате мы выделили 6 тактик: Resource Development, Initial Access, Execution, Persistence, Lateral Movement и Defense Evasion, в которых зафиксировали наиболее любопытные техники.

Подготовка ресурсов (Resource Development)

Техники, которые использовали атакующие перед атаками:

Acquire Access ID: T1650

Acquire Infrastructure: Domains ID: T1583.001

Develop Capabilities: Malware ID: T1587.001

Develop Capabilities: Exploits ID: T1587.004

Compromise Infrastructure: Server ID: T1584.004 3742

Obtain Capabilities: Malware ID: T1588.001

Obtain Capabilities: Tool ID: T1588.002

Obtain Capabilities: Exploits ID: T1588.005

Obtain Capabilities: Vulnerabilities ID: T1588.006

Establish Accounts ID: T1585

Establish Accounts: Email Accounts ID: T1585.002 3693

Не только ваш сервер!

Даже если при инциденте не было утечки конфиденциальных данных или шифрования инфраструктуры, его игнорирование может сделать вас инструментом злоумышленников.

В одном из расследований мы обнаружили несколько скомпрометацию серверов, которые атакующие готовили для использования в качестве серверов командного управления (C2 — Command and Control). Первый сервер готовился как прокси-сервер. Второй мог выступать как C2, так и в роли прокси-сервера.

Компрометация серверной части инфраструктуры — это не только угроза для вашей организации, но и для подрядчиков/заказчиков. Серверы могут быть использованы для атак на другие компании, рассылки вредоносного ПО или проведения DDoS-атак. Иначе говоря, ваша инфраструктура становится частью инструментария атакующих для противоправных действий. В данном случае оперативное реагирование команды

4RAYS помогло предотвратить дальнейшее использование серверов злоумышленниками.

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.

Старый злой фишинг

Фишинг все еще остается одной из самых распространенных техник, используемых атакующими для получения первоначального доступа. Несмотря на развитие современных средств защиты информации, достаточно сложным является процесс их интеграции на все уровни инфраструктуры организации. Атакующим определенно повезет при отправке фишингового письма невнимательному пользователю, у которого нет установленных средств защиты.

Так, в 2025 году мы сталкивались с фишинговыми капаниями различных группировок, таких как Cloud Atlas с VBShower и VBCloud, Fairy Trickster с PhantomRemote. При расследовании инцидентов мы выявили группировки, активно использующие фишинг как способ первичного доступа. Например, Lifting Zmiy, применяющие BrokenDoor и др.

Ключевой элемент защиты от фишинга — не только технологии, но и человеческий фактор. Создание культуры осознанного обращения с электронной почтой и ссылками — основа устойчивой защиты.

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**, который предназначен для восстановления веб-приложения из резервной копий и 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 нам системы подрядчика, на которой работал скомпрометированный пользователь, не смог, так как подрядчик утверждал, что с его стороны компрометация невозможна.

Через две недели заказчик, не согласовав свои действия с нами, решил разблокировать скомпрометированную учетную запись, предварительно договорившись с подрядчиком о смене пароля УЗ. В результате буквально через 24 часа заказчик снова зафиксировал нелегитимный вход с помощью скомпрометированной учетной записи и инцидент повторился.

В итоге получив одобрение на исследование системы подрядчика с скомпрометированной учетной записью, нами 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 сталкиваемся с проблемами несоблюдения мер информационной безопасности на стороне подрядчика. Подробно о том, как защитить свою организацию от возможной атаки через доверительные отношения, 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: T1047

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 ею использовалось API веб-приложения.

Бывают случаи, когда встроенные функции веб-приложения помогают атакующим выполнять команды на атакуемой системе. Так, в одном из недавних инцидентов мы столкнулись с интересной функцией 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. Планировщик задач приложения имел специальную функцию автоматизации администрирования: он позволял создавать задачи, содержащие скрипты, которые выполнялись на уровне веб-приложения. Злоумышленники смогли использовать данную функцию путем вставки в скрипты для задач кода, который позволял выполнять команды уже на уровне операционной системы. Результаты выполнения атакующие получали через перехват ошибок веб-приложения — таким образом они 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 не только закрепить вредоносный файл на системе, но и его скрыть его от обнаружения. В одном из инцидентов мы столкнулись с такой комбинацией.

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 при запуске или перезагрузке легитимной службы Gitlab кроме запуска легитимного ПО также выполнялся запуск вредоносного ПО, что обеспечивало надежное и скрытое закрепление на системе.

Базы данных хранят не только данные

В одном из расследований атакующие использовали не самую распространенную технику закрепления — 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 ключевым 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. Подробнее о расследовании данного инцидента можно прочитать в нашем блоге.

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

За средствами защиты тоже нужно следить

При атаках злоумышленники 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 этому обнаружить не удалось, но такое нетипичное поведение антивируса невозможно без модификации его работы. В другом инциденте мы обнаружили свидетельства удаления антивирусного ПО через PsExec.

Маскировка включена

Маскировка вредоносного ПО и его процессов — неотъемлемая часть комплексных атак на инфраструктуру. Продвинутые группировки целенаправленно исследуют атакуемые системы с целью понять, какой способ сокрытия их активности будет наиболее подходящим. Особенно это актуально для Unix-подобных систем: при наличии у злоумышленников достаточных навыков они продолжительное время могут скрываться в зараженной инфраструктуре. Подтверждением этому может служить активность NGC5081, которая была подробно разобрана в одной из наших статей.

4RAYS by SOLAR

ВЫВОДЫ И РЕКОМЕНДАЦИИ

Мы завершали 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 шести месяцев мы можем сказать, что «затишье» прекратилось: во втором полугодии случилось 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.

Атакующие меняют тактики: растет количество инцидентов, где проникновение в организации случилось из-за недочетов в безопасности их подрядчиков, а 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 сфере 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 степени уверенности мы ожидаем, что в 2026 году обнаружим больше свидетельств использования злоумышленниками сервисов 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 — 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 видеть 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.