

Отчет об атаках и инструментари профессиональных кибергруппировок



2021 год

Оглавление

Введение	3
Методология	4
Ключевые тренды 2021 года	6
Особенности группировок с высокой квалификацией	7
Особенности группировок среднего уровня	8
Статистика по техникам и инструментарию злоумышленников	9
Ключевые узлы инфраструктуры, являющиеся целью злоумышленников	18
Потенциальные риски для компаний	19

Введение

С каждым годом расслоение киберпреступников по уровням квалификации и конечным целям становится все очевиднее. На фоне постоянного роста общего числа киберинцидентов таргетированные атаки группировок со средним и высоким уровнем квалификации происходят все чаще. Так, в 2021 году аналитиками центра противодействия кибератакам Solar JSOC компании «Ростелеком-Солар» было зафиксировано свыше 300 атак, организованных профессиональными злоумышленниками. В 18% случаев за ними стояли высокопрофессиональные хакеры: кибернаемники и проправительственные группировки.

Остальные были реализованы организованными группировками среднего уровня квалификации (киберкриминалом). Представленный отчет подробно рассматривает основные цели, инструментарий и методы злоумышленников (от первого проникновения в инфраструктуру до векторов развития атаки) и будет полезен для определения ключевых мер информационной безопасности, необходимых для защиты от киберпреступников высокого уровня квалификации.



Методология

В качестве источников информации использованы:

- ◆ результаты анализа инцидентов и атак, выявленных командой Solar JSOC в рамках оказания регулярных услуг мониторинга и реагирования на кибератаки;
- ◆ результаты расследований, проводимых командой Solar JSOC CERT;
- ◆ агрегированная информация об атаках и вредоносном ПО, собираемая сетью ловушек (ханипотов) и сенсоров, размещенных на сетях связи и в центрах обработки данных на территории России;
- ◆ информация, получаемая в рамках коммерческих подписок от внешних поставщиков услуг и обмена данными с российскими и международными CERT.

Совокупно Solar JSOC обеспечивает контроль и выявление инцидентов для:

- ◆ **более 190** крупных организаций (общей численностью свыше 600 тыс. сотрудников) из разных отраслей экономики: банки, энергетика и нефтегаз, органы государственной власти и др.;
- ◆ **более 2 тыс.** внешних сервисов, опубликованных в интернете;
- ◆ **более 95 тыс.** серверов общего, инфраструктурного и прикладного назначения.

В основе нашего исследования лежит модель уровней нарушителей, которая учитывает значительное расслоение подходов злоумышленников к атакам на инфраструктуру. Согласно этой модели, выделяются пять основных категорий нарушителей, но в данном отчете собрана статистика об атаках, выполняемых профессиональными группировками, которые относятся к следующим категориям:

Уровень злоумышленника	Категория нарушителя	Типовые цели	Возможности нарушителя
3	Киберкриминал / организованные группировки среднего уровня квалификации	Приоритетная монетизация атаки: шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное ВПО (приобретение, обфускация или разработка), доступные уязвимости, социальный инжиниринг
4	Кибернаемники / продвинутые группировки	Нацеленность на заказные работы, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные данные по O-day-уязвимостям и ПО для их эксплуатации
5	Кибервойска / прогосударственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов	Самостоятельно найденные O-day-уязвимости в ПО и аппаратных решениях, разработанные и внедренные «закладки»



Ключевые тренды 2021 года

- ◆ В 2021 году аналитиками центра противодействия кибератакам Solar JSOC компании «Ростелеком-Солар» было зафиксировано **свыше 300 атак**, реализованных злоумышленниками со средним и высоким уровнем квалификации. Это на треть превышает показатели прошлого года.
- ◆ **В 18%** случаев за атаками стояли профессиональные злоумышленники: кибернаемники и проправительственные группировки. Их доля также выросла в сравнении с прошлым годом.
- ◆ **Свыше 92%** атак высокопрофессиональных группировок, зафиксированных в 2021 году, пришлось на объекты КИИ. Среди них чаще всего атакуют госсектор, энергетику, промышленность и ВПК.
- ◆ В 2020 году мы отмечали, что чаще всего злоумышленники для проникновения во внутреннюю инфраструктуру использовали фишинг и социальную инженерию. В 2021 году на фоне публикации O-day-уязвимостей в Microsoft Exchange профиль атак несколько изменился. Фишинг и социальная инженерия по-прежнему занимают ключевые позиции в портфеле инструментов атакующих, но теперь они делят лидерство с эксплуатацией уязвимостей в MS Exchange.



Особенности группировок с высокой квалификацией

Их отличительными особенностями являются:

- ◆ Нацеленность на объекты критической информационной инфраструктуры и крупный бизнес.
- ◆ В случае атак на объекты критической информационной инфраструктуры основные цели – монетизация за счет реализации собранных данных в рамках кибершпионажа или денежного вознаграждения за предоставление доступа в инфраструктуру, а также кибертерроризм.
- ◆ В случае атак на крупный бизнес основной целью является монетизация присутствия путем хищений или шантажа.
- ◆ Высокая сложность атак: самописное ПО, поиск 0-day-уязвимостей в эксплуатируемых сервисах жертв, большая длительность атак (с момента сбора сведений об инфраструктуре, OSINT, до момента закрепления может проходить до 8 месяцев).

Такие атаки почти всегда являются таргетированными. Это означает, что злоумышленники особенно внимательно подходят к каждому этапу атаки, начиная с разведки. Причем кибернаемники и проправительственные группировки не ограничивают OSINT только изучением ИТ-периметра жертвы. Их разведка проводится и в отношении подрядчиков организации. Тренды проникновения кибернаемников практически неизменны, но в 2021 году мы наблюдаем рост числа проникновений в инфраструктуру жертвы через подрядчиков, которые занимались внедрением информационных систем и ПО, а также разработкой и поддержкой ПО.

Эти группировки хорошо знакомы с логикой работы базовых средств защиты информации, что позволяет им оставаться незамеченными. Как правило, перед каждым этапом хакеры эмулируют всю инфраструктуру заказчика, в том числе и СЗИ, поэтому к моменту реальной атаки у них есть глубокое понимание, как обойти защиту. Такая таргетированность и высокая сложность тактик и техник требует от злоумышленников не только профессиональных навыков и времени, но и огромных финансовых вложений. Но в то же время ущерб от таких атак может исчисляться сотнями миллионов рублей. А если речь идет о КИИ, то подход к оценке ущерба в виде финансовых потерь не является исчерпывающим, в этом случае необходимо учитывать риски, связанные с влиянием на экономику страны в целом, безопасность жизнедеятельности граждан и политическую ситуацию.

Исходя из этого, роль и требования к экспертам-аналитикам, занимающимся мониторингом событий и инцидентов ИБ, возрастают многократно.

Особенности группировок среднего уровня

Атаки организованных группировок среднего уровня квалификации – киберкриминала – отличаются меньшей технической изощренностью. Они могут приобретать уже готовые решения в даркнете и предпочитают ВПО, которое распространяется по модели Software-as-a-Service.

При этом в отношении киберкриминала проще оценить нанесенный урон от атак, поскольку злоумышленники чаще всего преследуют цели прямой монетизации: вывод финансовых средств, получение выкупа за расшифровку данных, шантаж публикацией чувствительных сведений и технологий (например, атака группировки REvil на подрядчика Apple).



Статистика по техникам и инструментарию злоумышленников

Массовый инструментарий группировок среднего уровня*

Как правило, у группировок среднего уровня (киберкриминал) не хватает квалификации на полноценную разработку собственного ВПО, поэтому чаще всего они прибегают к покупке готовых решений в даркнете. Однако эксплуатацией купленных решений злоумышленники этого уровня занимаются сами, в отличие от атакующих с низкой квалификацией, которые чаще всего приобретают ВПО по модели Software-as-a-Service.

В 2021 году наибольшую популярность среди группировок среднего уровня имели следующие ВПО:

- AgentTesla (15%)
- Modified RMS (15%)
- Remcos RAT (15%)
- Formbook (10%)
- QBot (10%)
- TeamBot (5%)
- Phobos (5%)
- LambdaRAT (5%) и другие (20%)

Этот список популярных ВПО кардинально изменился по сравнению с предыдущим годом. Но в то же время можно отметить динамику роста популярности Remcos RAT.

*Статистика по деятельности кибернаемников и проправительственных группировок не публикуется в связи с ограничением доступа к данной информации для открытых источников.

Техники, применяемые для преодоления периметра и взлома инфраструктуры

Ключевые техники, используемые злоумышленниками для преодоления периметра и взлома инфраструктуры, не претерпели значительных изменений по сравнению с предыдущим годом. Тем не менее в связи с критическими уязвимостями в MS Exchange, обнаруженными в 2021 и 2020 годах, можно отметить значительный рост динамики эксплуатации уязвимостей внешнего периметра (с 2% до 10% год к году).

К ключевым техникам, используемым для реализации атаки и преодоления периметра, относятся:

Фишинг – использование почтовых рассылок с вредоносным ПО или вредоносными ссылками на веб-формы авторизации с целью получения логинов и паролей.

Эксплуатация уязвимостей внешнего периметра – выявление в рамках разведки уязвимостей в сервисах и их последующая эксплуатация.

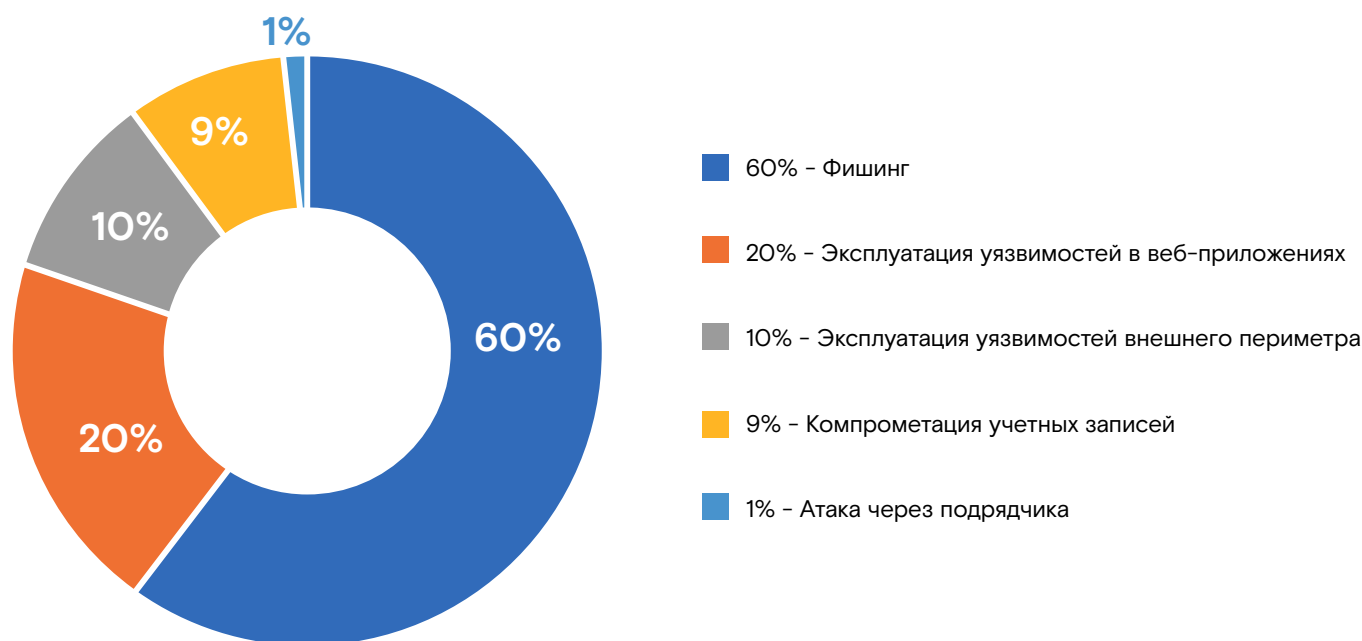
Эксплуатация уязвимостей в веб-приложениях – выявление и последующая эксплуатация уязвимостей или недостатков в реализации веб-приложений.

Компрометация учетных записей – брутфорс и поиск в интернете и даркнете скомпрометированных учетных записей пользователей, подрядчиков и системных утилит компании (выложенных в общем доступе, совпадающих с персональными учетными данными и т. д.).

Атака через подрядчика – компрометация инфраструктуры подрядчика для использования его учетных данных, паролей в атаке на основную организацию.

В случае если злоумышленники применяли комбинированный способ атаки, в данной статистике учитывался вектор, наиболее критический с точки зрения контроля и блокировки.

Как взламывали инфраструктуру группировки среднего уровня в 2021 году



Фишинг по-прежнему занимает лидирующую позицию среди техник злоумышленников среднего уровня. В первую очередь это связано с дешевизной и массовостью данного типа атак. При этом хакерам достаточно скомпрометировать хотя бы одну учетную запись для проникновения во внутренний периметр.

Согласно недавнему отчету, подготовленному экспертами отдела анализа защищенности «Ростелеком-Солар» на основе проводимых пентестов:

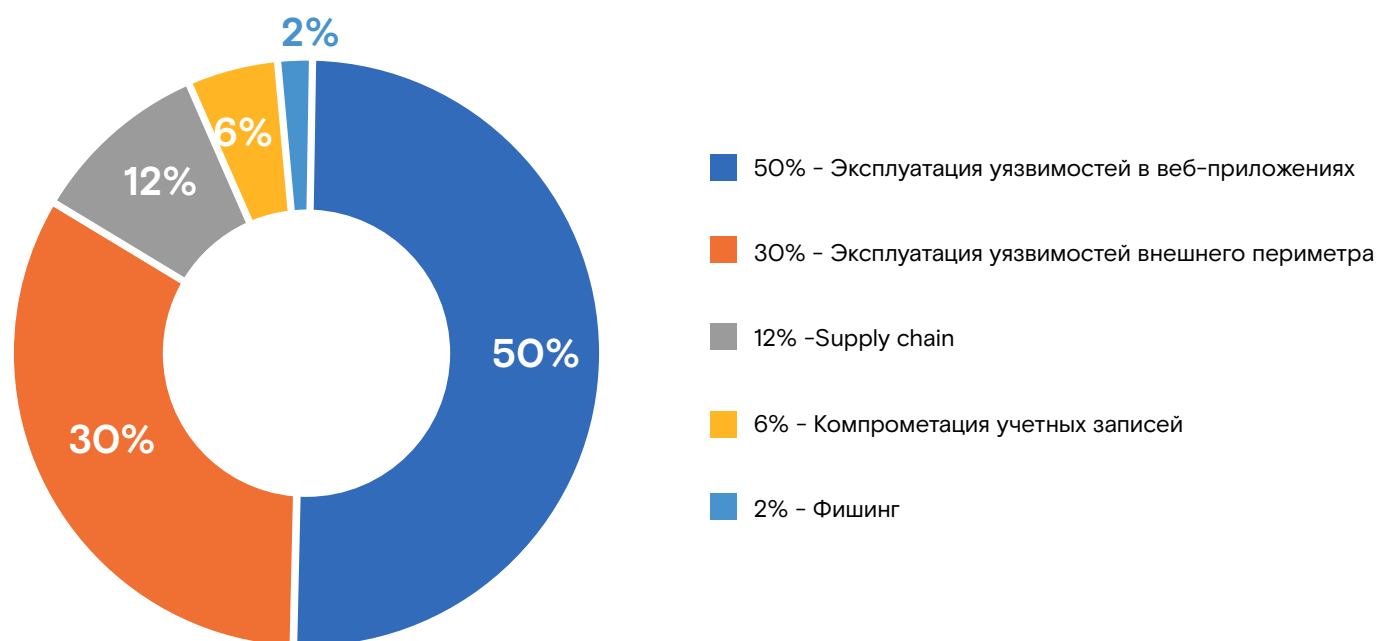
1% сотрудников открывают фишинговые письма с вредоносным docx-документом;

15% сотрудников проходят по ссылке на вредоносную веб-страницу;

19% сотрудников вводят свои данные на фишинговой веб-форме авторизации.

Если фишинговая атака не была вовремя обнаружена службами ИБ, то вероятность компрометации инфраструктуры близка к 100%. В частности, экспертам «Ростелеком-Солар» при проведении у заказчиков внутренних тестирований на проникновения за 2021 год в 100% случаев удалось полностью скомпрометировать инфраструктуру и захватить их домены, при этом во всех кейсах наши эксперты отметили уязвимость внутренней сети исследуемых систем перед злоумышленниками низкой квалификации.

Как взламывали инфраструктуру профессиональные группировки в 2021 году



Профессиональные злоумышленники также почти не изменили подхода к взлому периметра. Как и годом ранее, наиболее популярной техникой у них остается эксплуатация веб-уязвимостей. Это объясняется тем, что веб-приложения становятся все популярнее и возникает потребность усложнять и развивать их функционал. Из-за этого растет число ошибок со стороны разработчиков, что в свою очередь приводит к появлению уязвимостей и недостатков, используемых злоумышленниками. Более того, мы по-прежнему приходим к выводу, что веб-приложения объектов КИИ и органов госвласти (например, корпоративные порталы или веб-почта) слабо защищены и имеют огромное количество ошибок.

Фишинг, напротив, намного реже используется кибернаемниками и проправительственными группировками. Их атаки носят таргетированный характер, а это означает, что злоумышленникам свойственна скрытность и аккуратность. Фишинг – это более «грубая» массовая атака, и такие рассылки легко детектируются и быстро блокируются. Профессиональные злоумышленники чаще, чем киберкриминал, прибегают к атакам через подрядчика. Это объясняется тем, что такие атаки требуют определенной квалификации со стороны атакующих и их крайне сложно обнаружить со стороны Blue Team.

Техники, применяемые злоумышленниками для закрепления и развития атаки

Ключевые техники закрепления в инфраструктуре жертвы:

Механизмы автозагрузки – прописывание запуска инструментария в автозагрузку операционной системы и сокрытие этого запуска от защитных механизмов.

Системные службы – создание системной службы для функционирования инструментария.

Формирование драйвера – разработка собственного инструмента для максимального сокрытия от защитных алгоритмов.

Вредоносное ПО – применение для работы вредоносного ПО внутренних технологий управления Windows, WMI.

BITS-задачи – фоновые задачи передачи файлов.

Планировщик задач – для старта вредоносного ПО в определенное время.

Ключевые техники распространения по сети:

Pass-the-ticket / Pass-the-hash – кража аутентификационной информации пользователей с использованием слабой защиты аутентификации в Windows.

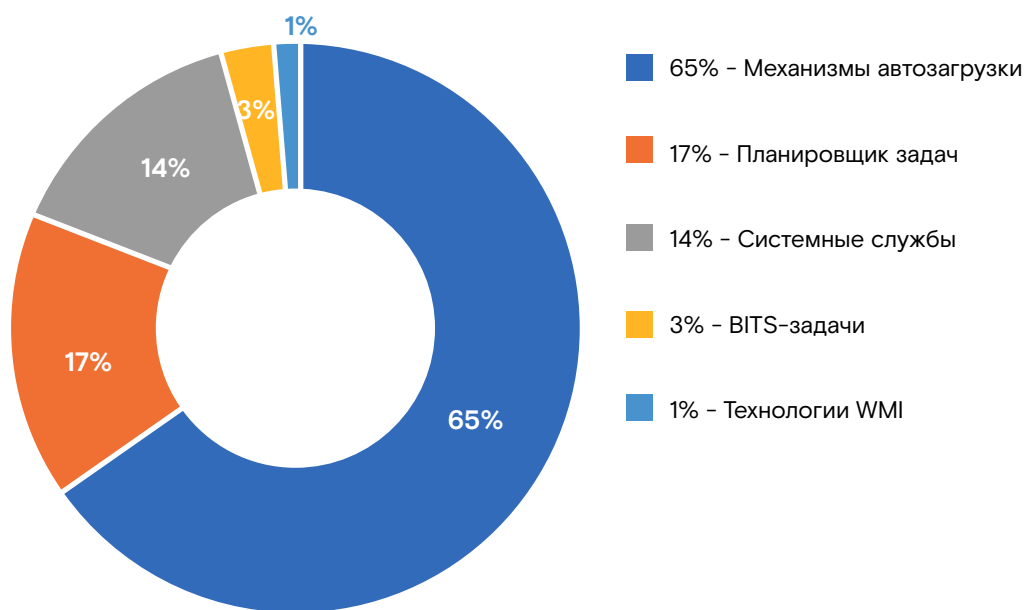
Использование удаленных сервисов: RDP, SMB, SSH. Применение административных протоколов с предшествующей кражей учетных записей пользователей.

Эксплуатация уязвимостей удаленных сервисов: RDP-, SMB-, веб-компоненты. Эксплуатация уязвимостей в административных протоколах.

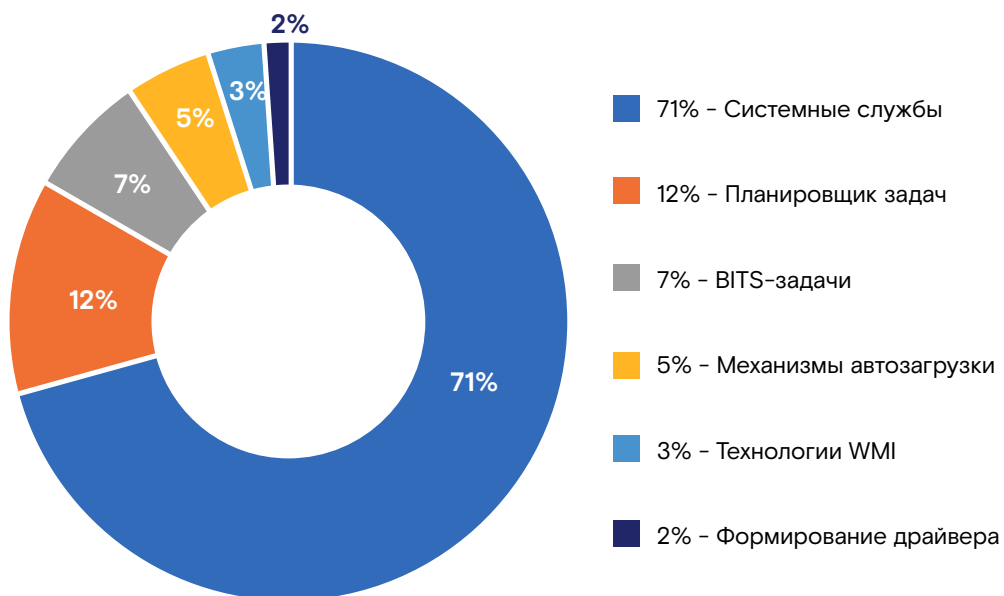
При использовании комбинированного способа атаки учитывался вектор, наиболее сложный для технического детектирования. По данной классификации мы выявили следующие тенденции и статистику в зависимости от типа группировки:

Статистика по применяемым техникам закрепления:

Группировки среднего уровня

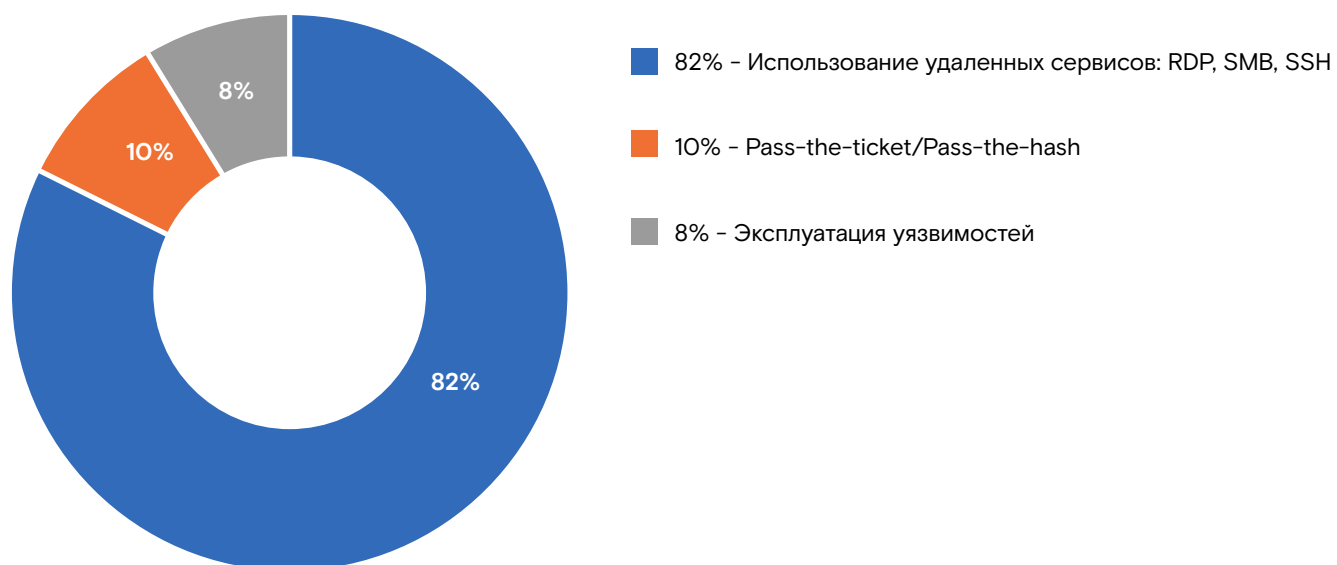


Профессиональные группировки

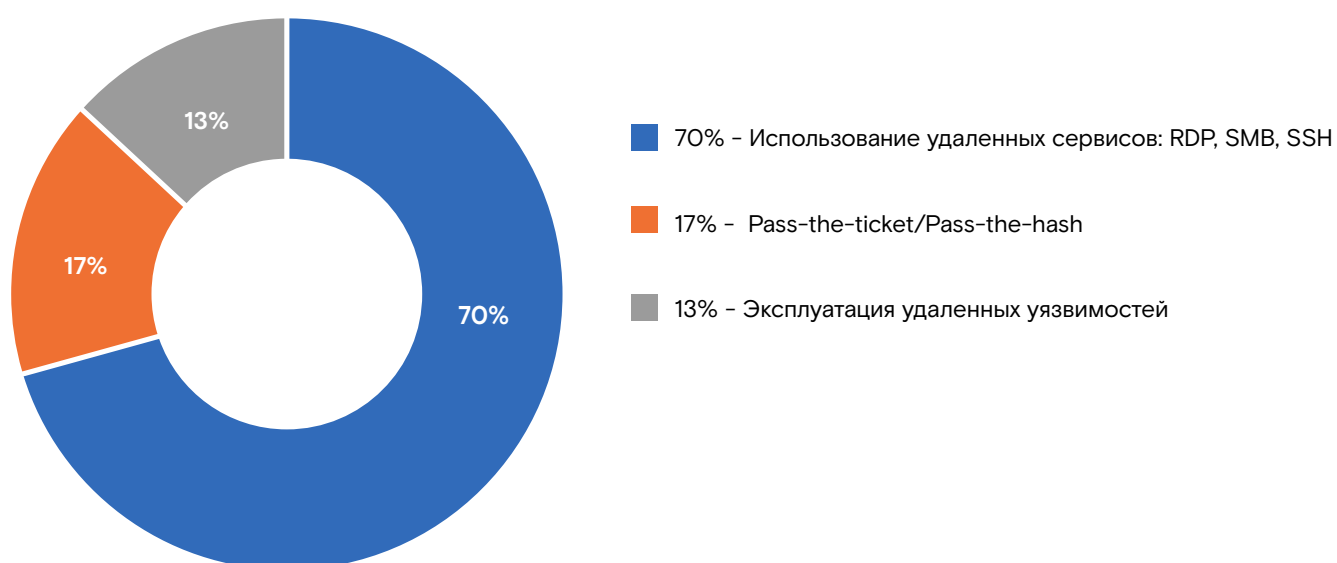


Статистика по применяемым техникам распространения:

Группировки среднего уровня



Профессиональные группировки

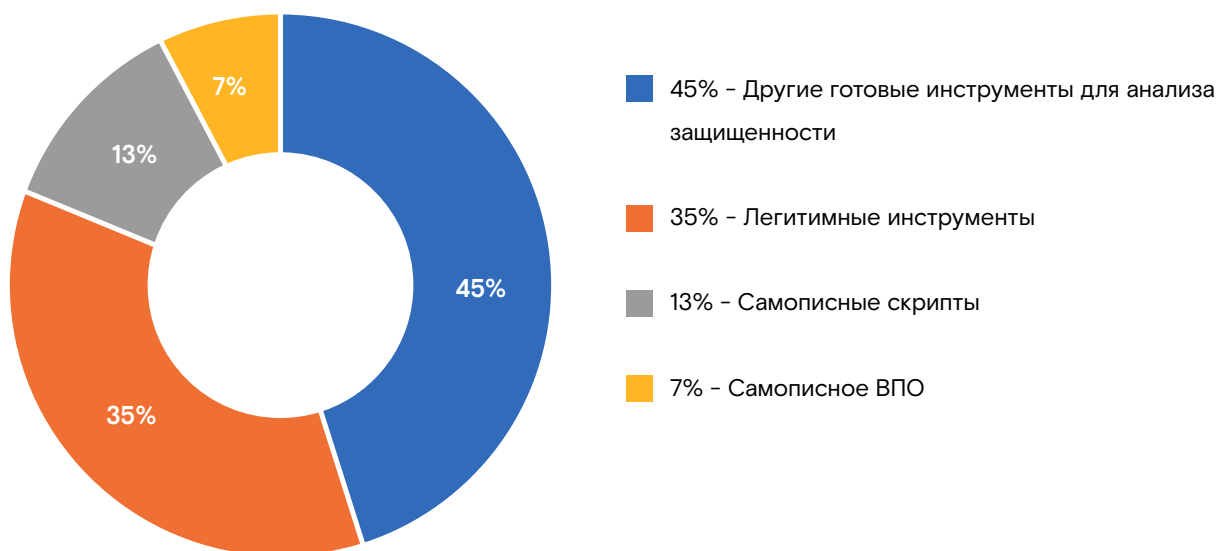


Программное обеспечение, используемое злоумышленниками для реализации вышеописанных векторов и техник:

- ◆ самописное ВПО;
- ◆ самописные скрипты;
- ◆ легитимные корпоративные или свободно распространяемые утилиты для удаленного администрирования;
- ◆ другие готовые инструменты для анализа защищенности.

При использовании комбинированного способа атаки учитывался вектор, наиболее сложный для технического детектирования.

Группировки среднего уровня



Профессиональные группировки



В целом видно существенное различие подходов, используемых группировками разного уровня для сокрытия своей активности.

Инструменты хакеров среднего уровня гораздо проще для реализации и могут быть детектированы командой защиты средней квалификации. Более профессиональные группировки используют подходы, требующие сложных алгоритмов выявления и продвинутых технологий защиты.

Ключевые узлы инфраструктуры, являющиеся целью злоумышленников

Очевидно, что раз группировки среднего уровня и кибернаемники и проправительственные группировки преследуют разные цели, то и узлы, на которые направлены их атаки, будут различаться. Так, группировки среднего уровня, преследуя цель прямой монетизации, чаще всего атаковали АРМ и транзитные серверы, обрабатывающие платежную информацию. Чаще всего в 2021 году они атаковали:

- Контроллер домена – **83%**
- АРМ и транзитные серверы – **85%**
- АРМ администраторов и пользователей с высокими привилегиями – **79%**
- Прикладные системы, хранящие финансовую информацию (АБС, ДБО, ERP, бухгалтерские системы) – **70%**

Конечной целью хакеров с высокой квалификацией чаще всего являлось получение доступа к почтовому серверу, что еще раз подтверждает направленность их деятельности на кибершпионаж. А в целом они атаковали:

- Почтовые серверы – **90%**
- АРМ администраторов и пользователей с высокими привилегиями – **80%**
- Контроллеры домена – **75%**
- АРМ руководителей и заместителей – **75%**

Потенциальные риски для компаний

Последствия атаки группировки среднего уровня

Узлы, атакуемые группировками среднего уровня, и используемые ими инструменты для закрепления и распространения еще раз доказывают, что их цель – прямая монетизация атаки. Также стоит отметить, что фокусом внимания для таких злоумышленников остаются финансовые организации и крупные промышленные компании, имеющие широко известные уязвимости на внешнем периметре. Ущерб и риски от такого рода атак по большей части легко поддаются расчету и редко когда превышают несколько десятков миллионов рублей. Как правило, мошенники получают свои средства либо в результате вывода денег с корреспондентских счетов, либо в качестве выкупа за расшифровку данных. С учетом того, что все большее распространение получает практика проведения резервного копирования и внедрения сервисов и продуктов ИБ, результативность подобного рода атак снижается с каждым годом.

Последствия атаки кибернаемников и проправительственных группировок

Как можно было заметить по приведенным выше данным, продвинутые киберпреступники чаще всего нацелены на кибершпионаж и дальнейшую реализацию собранных данных. Также они часто выполняют крупные заказы за значительное вознаграждение. Что касается кибертерроризма, то с учетом недостатков в защищенности объектов КИИ и госструктур риск подобного рода атак по-прежнему остается высоким. Радует, что за последние годы на территории России не было успешных кибертерактов.

С учетом высокой подготовки киберпреступников из профессиональных группировок и их внушительного финансирования подобного рода риски особенно критичны и должны нивелироваться в первую очередь. Однако противостоять подобным атакам возможно лишь с привлечением экспертов-аналитиков высокой квалификации и построением центров мониторинга и реагирования.



rt.ru
rt-solar.ru

solar@rt-solar.ru
+7 (499) 755-07-70