Ростелеком
Солар

Отчет об атаках и инструментарии профессиональных кибергруппировок

ЗА 2020 ГОД

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

За 2020 год центр мониторинга и реагирования на кибератаки Solar JSOC зафиксировал более 200 хакерских атак со стороны профессиональных кибергруппировок, включая массовые попытки воздействия на целые отрасли и сектора экономики.
Примерно в 30 случаях за атаками стояли злоумышленники наиболее высокого уровня подготовки и квалификации – кибернаемники и кибергруппировки, преследующие интересы иностранных государств. В числе наиболее частых целей – объекты критической информационной инфраструктуры России.

Целью наиболее профессиональных хакерских группировок обычно являются деструктивные действия и кибершпионаж. Ущерб от атак такого класса измеряется не только финансовыми потерями, но и влиянием на экономику страны в целом, безопасность жизнедеятельности граждан и политическую ситуацию. Только сопутствующий ущерб от компрометации инфраструктуры, такой как кража персональных данных сотрудников и клиентов, регулярных и репутационных рисков, возможности развития новых атак в случае успеха киберпреступников мог бы достичь десятков миллионов рублей. Совокупные же убытки от полномасштабной реализации такого рода атаки составили бы несколько миллиардов рублей.

Атаки организованных группировок среднего уровня квалификации – киберкриминала – отличаются меньшей технической изощренностью, однако тоже могут иметь серьезные последствия. Усилия подобных злоумышленников направлены преимущественно на прямую монетизацию: вывод финансовых средств или получение выкупа за расшифрование данных компании, – и ущерб от таких атак может измеряться сотнями миллионов рублей.

Представленный отчет 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

Отчет о выявляемых атаках профессиональных группировок киберпреступников базируется на следующих типах данных:

1. Анализ инцидентов и атак, выявленных командой Solar JSOC в рамках оказания регулярных услуг мониторинга и реагирования на кибератаки

2. Работы по расследованию инцидентов, проводимых командой Solar JSOC CERT в рамках коммерческих и пилотных активностей

3. Агрегированная информация об атаках и вредоносном ПО, собираемая так называемыми ловушками (honeypot), размещенными на сетях связи и в центрах обработки данных на территории РФ

4. Информация, получаемая в рамках коммерческих подписок от внешних поставщиков услуг и информационного обмена с российскими и международными CERT

Совокупно в рамках оказания сервиса заказчикам Solar JSOC обеспечивает контроль и выявление инцидентов для:

Более 140 крупных организаций (и более 600 тысяч сотрудников) в самых разных отраслях экономики: банки, энергетика и нефтегазовый сектор, органы государственной власти и др.

Более 1500 внешних сервисов, опубликованных в интернете

Более 70 тыс. серверов общего, инфраструктурного и прикладного назначения

В 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 вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, социальная инженерия
4	Продвинутые группировки (кибернаемники)	Нацеленность на заказные работы — сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные данные по zero-day-уязвимостям и ПО для их эксплуатации
5	Группировки, спонсируемые государствами	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов	Самостоятельно найденные zero-day-уязвимости в ПО и аппаратных решениях, разработанные и внедренные «закладки»

КЛЮЧЕВЫЕ ТЕНДЕНЦИИ 2020 ГОДА

За 2020 год зафиксировано более 200 атак со стороны киберкриминала (включая массовые атаки на отрасль/сектор экономики) и около 30 атак группировок более высокой квалификации.

Действия группировок среднего уровня не претерпели существенных изменений за последний год. Злоумышленники все чаще используют фишинг и социальную инженерию для проникновения в компанию. При реализации атаки применяется инструментарий средней сложности, детектируемый продвинутыми автоматизированными средствами мониторинга и защиты. Ущерб от таких атак в случае их успешной реализации составил бы не более нескольких десятков миллионов рублей.

Атаки более профессиональных группировок отличаются гораздо большей сложностью: их детектирование возможно только при непосредственном участии экспертов-аналитиков высшей квалификации и при условии, что в компании выстроена высокоразвитая инфраструктура информационной безопасности. В 2020 г. такие группировки для проникновения в целевые сегменты все чаще использовали атаки через подрядчиков, имеющих существенно более низкий уровень защищенности. **Потенциальный ущерб от подобных атак может измеряться несколькими сотнями миллионов рублей.**

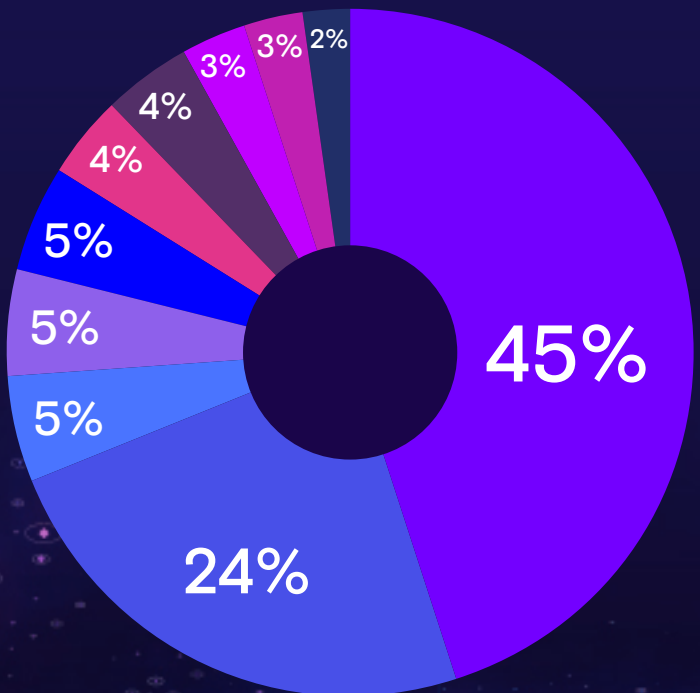
СТАТИСТИКА ПО ТЕХНИКАМ И ИНСТРУМЕНТАРИЮ ЗЛОУМЫШЛЕННИКОВ

МАССОВЫЙ ИНСТРУМЕНТАРИЙ ГРУППИРОВОК СРЕДНЕГО УРОВНЯ

Развитие сервисной модели на рынке киберкриминала позволяет злоумышленникам более эффективно строить атаки и фокусировать профильную экспертизу в рамках кластера знаний в области сервисных технологий. Группировки среднего уровня квалификации, как правило, не разрабатывают вредоносное ПО самостоятельно, а приобретают его в даркнете. Иными словами, статистика применения того или иного массового вредоноса фактически отражает статистику атак киберкриминала.

В 2020 году наибольшую популярность имели:

- RTM — 45%
- Emotet — 24%
- Remcos — 5%
- Nanocore — 5%
- Quasar — 5%
- LokiBot — 4%
- Pony — 4%
- Dharma — 3%
- Hawkey — 3%
- остальные — около 2%



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

В связи с высоким уровнем защищенности кредитно-финансовой отрасли (ключевого фокуса атак злоумышленников) наиболее успешными были атаки с использованием вирусов-шифровальщиков, позволяющих дестабилизировать состояние инфраструктуры. Тем не менее наличие системы резервного копирования и плана восстановления, как правило, останавливает компании от уплаты выкупа злоумышленникам и не позволяет им достигнуть ключевой цели — монетизации атаки.

ТЕХНИКИ, ПРИМЕНЯЕМЫЕ ДЛЯ ПРЕОДОЛЕНИЯ ПЕРИМЕТРА И ВЗЛОМА ИНФРАСТРУКТУРЫ

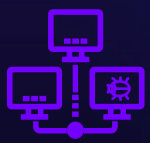
К ключевым техникам, используемым для реализации атаки и преодоления периметра, относятся:

использование уязвимостей на периметре — выявление уязвимых сервисов или слабых паролей/конфигураций периметрового оборудования для проникновения в инфраструктуру;

использование уязвимостей в веб-приложениях — выявление уязвимостей в веб-ресурсах и на порталах организации;

фишинг — использование почтовых рассылок с вредоносным ПО и с социальным контекстом для получения логина/пароля пользователя с целью доступа к инфраструктуре;

компрометация учетных записей — 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.);

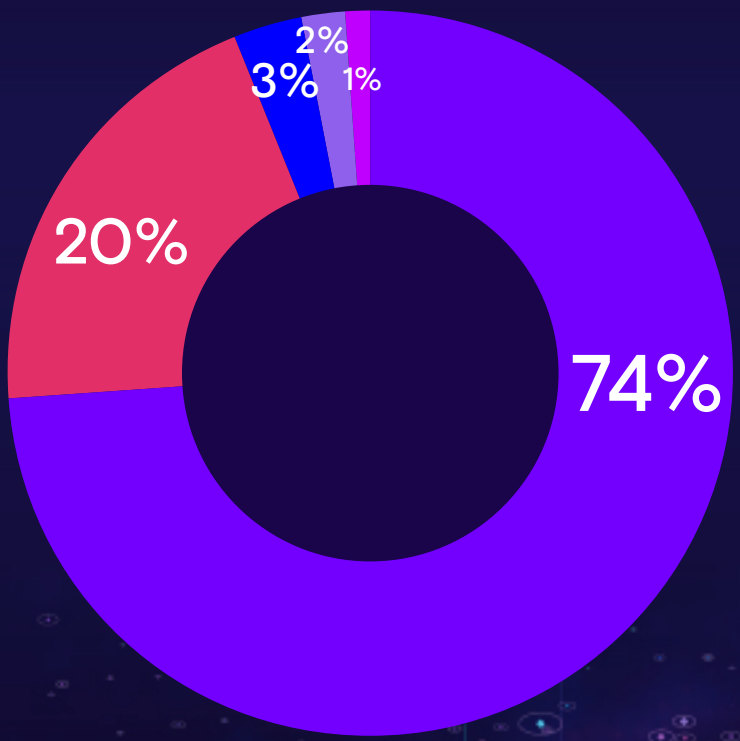


supply chain — компрометация инфраструктуры подрядчика для использования его учетных данных и паролей в атаке на основную организацию.

В случае если злоумышленники применяли комбинированный способ атаки, в данной статистике учитывался вектор, наиболее критический с точки зрения контроля и блокировки. Например, при реализации атаки на Exchange Server с помощью уязвимости CVE-2020-0688, для эксплуатации которой требуются учетные данные одного из пользователей, инцидент определялся как использование уязвимостей в веб-приложении, так как в данном случае более критична необходимость закрытия уязвимости (технической возможности полного контроля компрометации учетных данных за пределами компании не существует).

1. Тяготение группировок среднего уровня к конкретным техникам взлома довольно ярко отразилось в статистике 2020 года:

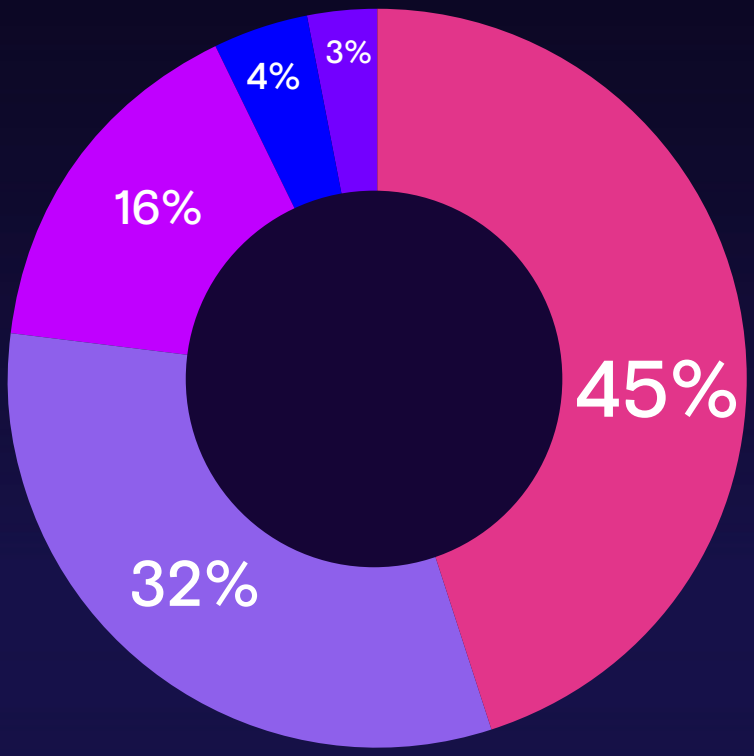
- фишинг — 74%
- атаки на веб-приложения — 20%
- компрометация учетных записей — 3%
- эксплуатация уязвимостей периметра — 2%
- supply chain — менее 1%



Продолжившееся развитие фишингового вектора объясняется удобством этого способа массовой атаки на сегмент/группу компаний при минимальных вложениях в обследование и анализ инфраструктуры жертвы. Количество ежегодно растущих утечек учетных данных с публичных и внутренних сервисов вывело вектор компрометации учетных записей на третье место. Атаки через подрядчика (supply chain) требуют длительной подготовки, поэтому крайне редко используются этой категорией злоумышленников.

2. Существенно отличается статистика по кибернаемникам и проправительственным группировкам, нацеленным на деструктивные действия и шпионаж с использованием более фокусного, индивидуального подхода к реализации атак:

- атаки на веб-приложения — 45%
- эксплуатация уязвимостей периметра — 32%
- supply chain — 16%
- компрометация учетных записей — 4%
- фишинг — 3%



Слабый уровень защищенности веб-приложений на объектах КИИ и в органах государственной власти делает данный вектор наиболее популярным для реализации атак. Также существенный вес имеют атаки через подрядчика, который, как правило, обладает высокими привилегиями на обслуживание не только корпоративных, но зачастую и закрытых технологических сегментов. Поэтому компаниям стоит обратить внимание на уровень защищенности подрядных организаций и выстроить максимально безопасный способ доступа подрядчиков в инфраструктуру.

ТЕХНИКИ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ ДЛЯ ЗАКРЕПЛЕНИЯ И РАЗВИТИЯ АТАКИ

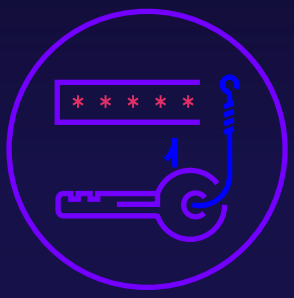
К ключевым техникам, используемым для закрепления в инфраструктуре жертвы, относятся:

механизмы автозагрузки прописывание запуска инструментария в автозагрузку операционной системы и сокрытие этого запуска от защитных механизмов;

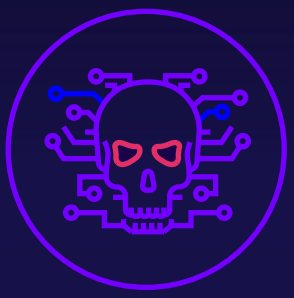
системные службы	создание системной службы для функционирования инструментария;
формирование драйвера	разработка собственного инструмента для максимального сокрытия от защитных алгоритмов;
вредоносное ПО	применение для работы вредоносного ПО технологий WMI — внутренних технологий управления Windows;
использование ОС	для работы инструментария BITS-задач — фоновых задач передачи файлов;
планировщик задач	для старта вредоносного ПО в определенное время.

К ключевым техникам, используемым для распространения по сети, относятся:

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

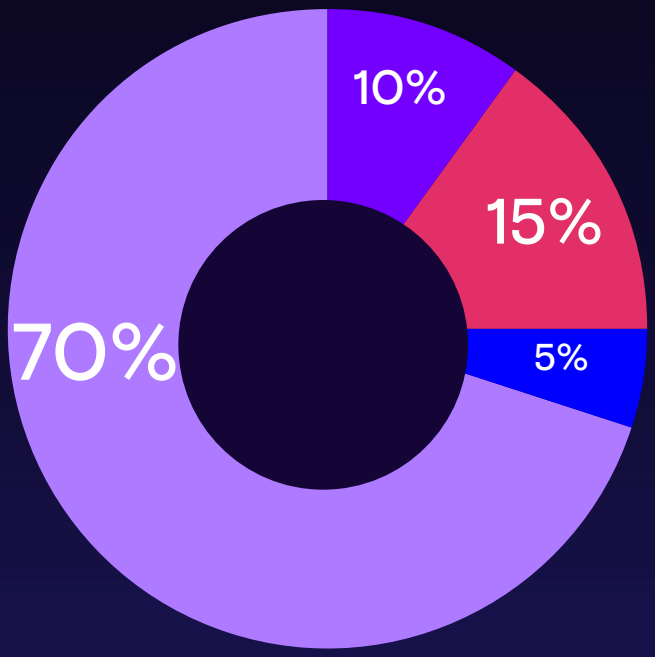


Эксплуатация уязвимостей удаленных сервисов: RDP-, SMB-, веб-компоненты. Эксплуатация уязвимостей в административных протоколах

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:

Закрепление

Группировки среднего уровня:

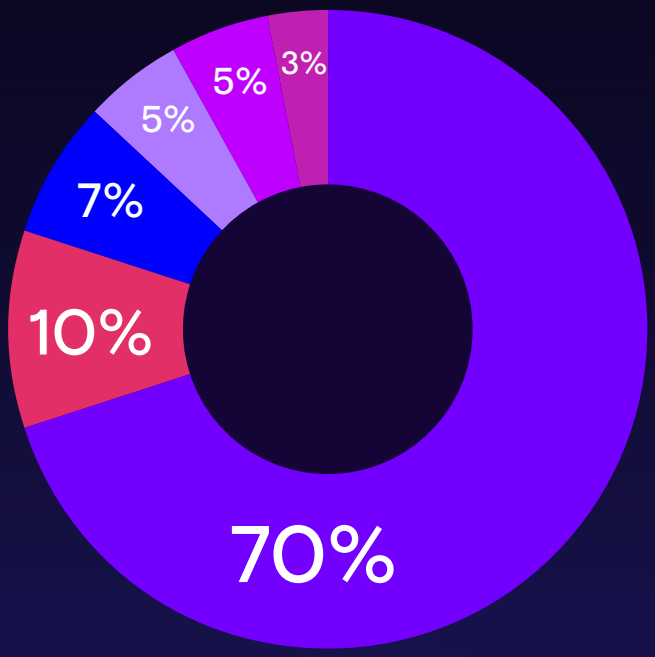


- Системные службы
- Использование планировщика задач
- Использование BITS-задач
- Механизмы автозагрузки

Формирование собственного драйвера — 0%

Использование технологий WMI — 0%

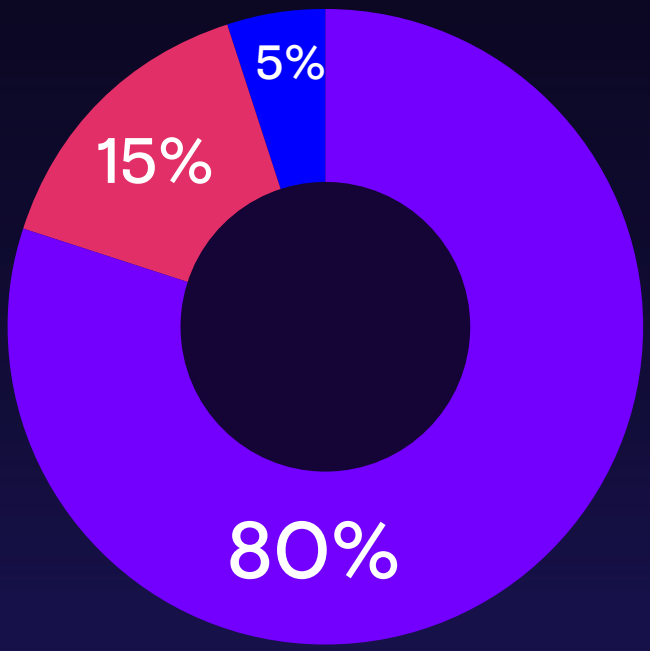
Кибернаемники и проправительственные группировки:



- Системные службы
- Использование планировщика задач
- Использование BITS-задач
- Механизмы автозагрузки
- Использование технологий WMI
- Формирование собственного драйвера

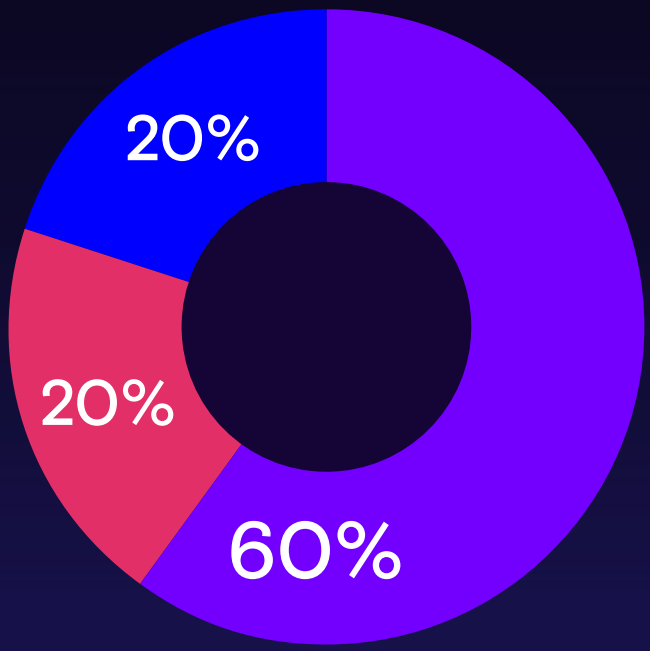
Распространение

Группировки среднего уровня:



- Использование удаленных сервисов: RDP, SMB, SSH
- Pass the Ticket / Pass the Hash
- Эксплуатация удаленных сервисов: RDP-, SMB-, веб-компоненты

Кибернаемники и проправительственные группировки:



- Использование удаленных сервисов: RDP, SMB, SSH
- Pass the Ticket / Pass the Hash
- Эксплуатация удаленных сервисов: RDP-, SMB-, веб-компоненты

Видно существенное различие подходов, используемых группировками разного уровня для сокрытия своей активности. Инструменты, применяемые группировками 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.

Подход к реализации вредоносного кода

Для реализации описанных выше техник злоумышленники обычно используют:

Самописное бинарное вредоносное **программное обеспечение**.

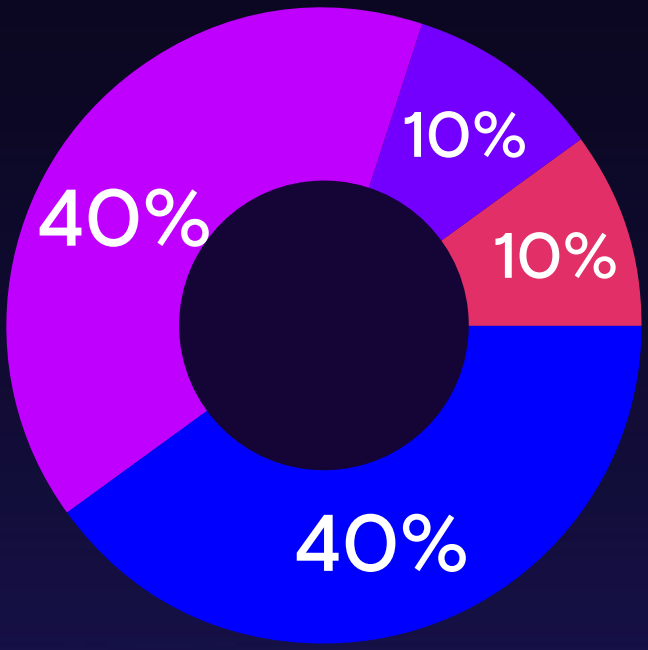
Самописные **скрипты** на различных интерпретируемых языках (Powershell, vbs, js, bat).

Легитимные корпоративные или свободно распространяемые **утилиты** для администрирования.

Различные доступные **инструменты и фреймворки** (для проведения анализа защищенности или вредоносное ПО, опубликованное в интернете).

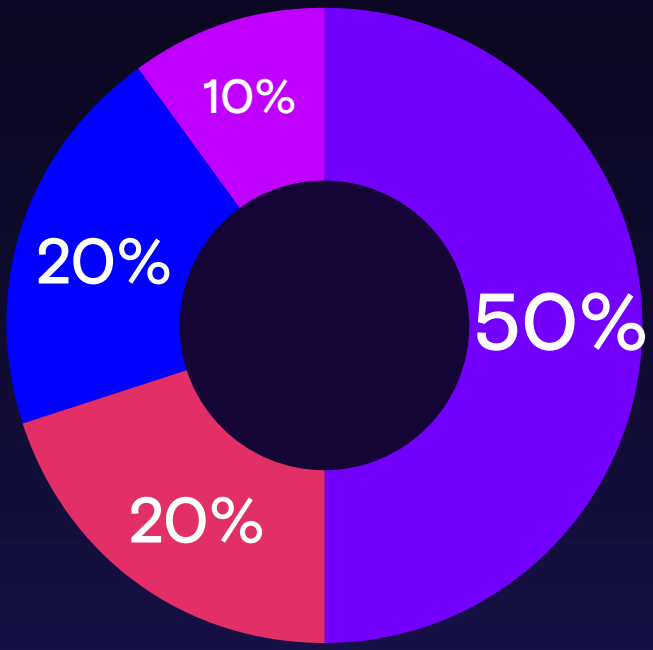
При использовании комбинированного способа атаки учитывался вектор, наиболее сложный для технического детектирования. По данной классификации мы выявили следующие тенденции и статистику в зависимости от типа группировки:

Группировки среднего уровня:



- Самописное бинарное вредоносное программное обеспечение
- Самописные скрипты на различных интерпретируемых языках (Powershell, vbs, js, bat)
- Легитимные корпоративные или свободно распространяемые утилиты для администрирования
- Различные доступные инструменты и фреймворки (для проведения анализа защищенности) или ВПО, опубликованное в интернете

Кибернаемники и проправительственные группировки:

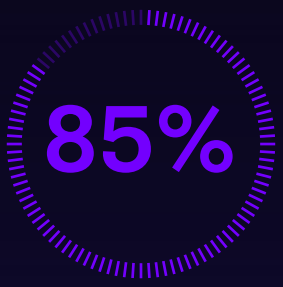


- Самописное бинарное вредоносное программное обеспечение
- Самописные скрипты на различных интерпретируемых языках (Powershell, vbs, js, bat)
- Легитимные корпоративные или свободно распространяемые утилиты для администрирования
- Различные доступные инструменты и фреймворки (для проведения анализа защищенности) или ВПО, опубликованное в интернете

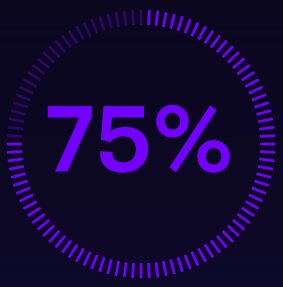
КЛЮЧЕВЫЕ УЗЛЫ ИНФРАСТРУКТУРЫ, ЯВЛЯЮЩИЕСЯ ЦЕЛЬЮ ЗЛОУМЫШЛЕННИКОВ

Группировки среднего уровня при проведении атак, как правило, были нацелены на получение доступа к следующим узлам инфраструктуры:

Контроллер домена для получения максимальных привилегий и возможности использовать различные учетные записи



АРМ и транзитные серверы, обрабатывающие платежную информацию с целью крупной монетизации атаки



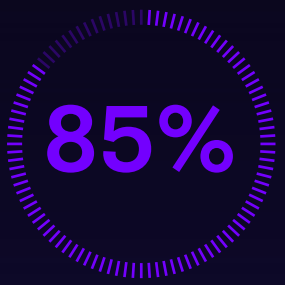
АРМ ИТ-администраторов с высоким уровнем привилегий

65% Системы ИТ-управления инфраструктурой (серверы инвентаризации, обновления, управления конфигурацией и т. д.) для получения наиболее полной информации об инфраструктуре

40% Системы ИБ-управления инфраструктурой (антивирусное ПО, системы защиты от несанкционированного доступа, сканеры уязвимостей) для получения возможности централизованного управления парком серверов и рабочих станций с высоким уровнем привилегий

45% Прикладные системы, хранящие финансовую информацию (АБС, ДБО, ERP, бухгалтерские системы) для возможности более типизированной монетизации через платежную информацию или вирусы-шифровальщики

Кибернаемники и проправительственные группировки в своих атаках, как правило, были нацелены на получение доступа к следующим узлам инфраструктуры:



Почтовые серверы
для получения доступа к критической информации, передаваемой по почте, и возможности реализации фишингового вектора изнутри организации

Контроллер домена
для получения максимальных привилегий и возможности использовать различные учетные записи

АРМ первых лиц, заместителей и секретарей
с целью получения ключевой конфиденциальной информации

80% АРМ ИТ-администраторов с высоким уровнем привилегий

75% Системы ИТ-управления инфраструктурой (серверы инвентаризации, обновления, управления конфигурацией и т. д.)
для возможности получения наиболее полной информации об инфраструктуре

65% Прикладные системы, обеспечивающие документооборот
для более типизированной монетизации за счет платежной информации или вирусов-шифровальщиков

50% Системы ИБ-управления инфраструктурой (антивирусное ПО, системы защиты от несанкционированного доступа, сканеры уязвимостей)
для получения возможности централизованного управления парком серверов и рабочих станций с высоким уровнем привилегий

40% Серверы и технологические рабочие станции управления технологическими процессами

РИСКИ ОТ РЕАЛИЗАЦИИ АТАК ГРУППИРОВКАМИ СРЕДНЕЙ И ВЫСОКОЙ КВАЛИФИКАЦИИ

Атаки группировок среднего уровня направлены на прямую монетизацию, и риски от их реализации посчитать достаточно просто. Неслучайно фокусом их внимания долгое время остается кредитно-финансовая сфера и возможность вывода денег с корреспондентских счетов / атаки на системы рейсов (АРМ КБР). При этом в целом по рынку наблюдается существенное снижение результативности проводимых атак, а максимальный ущерб от них достигает нескольких десятков миллионов рублей.

Расчет стоимости ущерба от атак более профессиональных группировок существенно сложнее и напрямую зависит от фактической цели. Например, крайне трудно оценить финансовые потери от риска долгосрочного шпионажа, но полученная злоумышленниками информация может повлиять на финансовое положение компании или даже государства в целом.

Сопутствующие риски компрометации инфраструктуры в результате кражи персональных данных сотрудников и клиентов компании (регуляторные, репутационные, а также риски развития атаки на инфраструктуру или пользователей), как правило, измеряются несколькими десятками миллионов рублей. Безусловно, наиболее крупный ущерб (исчисляемый сотнями миллионов рублей в случае одиночного объекта средней критичности и имеющий существенное значение для общества) несут атаки на технологические процессы и системы компаний.

Ростелеком
Солар

rt.ru
rt-solar.ru

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

Задать вопрос или
попробовать сервис

presale@rt-solar.ru