



APT-атаки

на кредитно-финансовую сферу в России

Обзор тактик и техник

Содержание

Что такое АРТ-атака	3
Об исследовании	6
Фишинг — просто и эффективно	7
Если фишинг не срабатывает	7
Почему атака остается незамеченной	8
Социальная инженерия вместо эксплойтов	10
Закрепление в сети	11
Где искать следы АРТ-атак	12
Сотрудники под наблюдением	13
Связь с командным центром	13
Кража денег — еще не финал	14
Как узнать об АРТ-атаке до потери денег	14

Г Что такое АРТ-атака

Финансовая сфера — одна из самых заманчивых для киберпреступников. Как сообщает [ФинЦЕРТ](#), за 2018 год было зафиксировано 687 атак на организации кредитно-финансовой отрасли. Из них 177 являлись целевыми, то есть были направлены непосредственно на получение финансовой выгоды.

58 млн ₽

составил ущерб
от действий АРТ-группировок
Cobalt и Silence в 2018 году

Целевые атаки, которые проводятся хорошо подготовленными преступными группировками, представляют для организаций наибольшую опасность. Такие атаки принято называть атаками типа advanced persistent threat, а преступные группировки, которые стоят за ними, — АРТ-группировками. По данным [ФинЦЕРТ](#), в 2018 году российские банки потеряли как минимум 44 млн рублей в результате действий АРТ-группировки Cobalt и не менее 14,4 млн рублей от действий Silence.

Г **Атака типа advanced persistent threat (АРТ-атака)** — это хорошо организованная, тщательно спланированная кибератака, которая направлена на конкретную компанию или целую отрасль. За АРТ-атакой, как правило, стоят преступные группировки, имеющие значительные финансовые ресурсы и технические возможности.

Далеко не каждая компания готова противостоять АРТ-атакам. При подготовке исследования мы провели опрос¹, где предложили пользователям рассказать, какие средства используются в их организации для защиты от кибератак, и оценить, сможет ли организация справиться со сложными угрозами. Опрос проводился на сайте компании Positive Technologies, среди аудитории портала SecurityLab.ru² и в ряде отраслевых сообществ, в которые входят эксперты по ИТ и ИБ из различных сфер отечественного бизнеса. Как выяснилось, лишь 22% респондентов, представляющих финансовую отрасль, считают, что их компания в состоянии отразить атаки АРТ-группировок. Нас полученные результаты не удивили. Ежегодно мы выполняем десятки работ по тестированию на проникновение и оценке возможности реализации рисков АРТ-атак в различных организациях, и в [исследовании 2018 года уже отмечали](#), что в 58% банков злоумышленник может получить доступ к тем или иным критически важным системам — к управлению банкоматами, системам межбанковских переводов, карточному процессингу или платежным шлюзам.

1 В опросе приняли участие 306 респондентов. Доля представителей кредитно-финансовой сферы составила 13%.

2 Сайт SecurityLab.ru — один из лидеров российского интернета в сфере информационной безопасности. Ежемесячная аудитория портала насчитывает около полумиллиона посетителей, большая часть из которых — программисты, специалисты по ИТ и ИБ, руководители соответствующих отделов.

Риск успешной кибератаки является критически опасным для компаний, где работают 68% респондентов. Две трети представителей финансовой отрасли (63%) на практике сталкивались с последствиями кибератак, и 34% признали, что организация понесла прямые финансовые потери. При всем этом только 39% участников отмечают, что защита от АРТ-атак — приоритетное направление развития ИБ в компании. Вероятно, пока не все организации воспринимают АРТ-атаки как отдельную угрозу, для противодействия которой нужен особый подход.

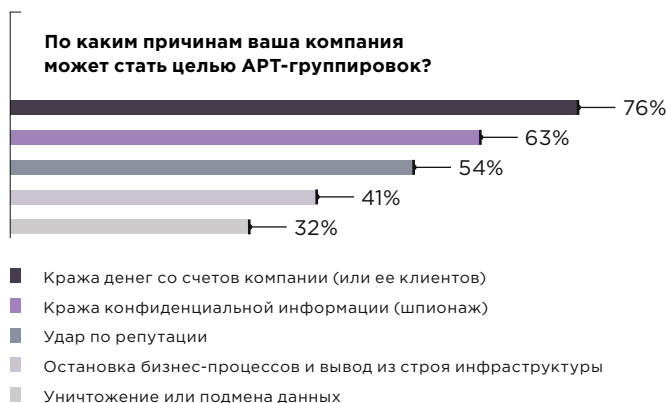


Рисунок 1. Топ-5 предполагаемых целей АРТ-группировок
(доля респондентов, представляющих финансовые компании)



Рисунок 2. Топ-5 последствий кибератак
(доля респондентов, представляющих финансовые компании)

Более половины участников (54%) сообщили, что расследования киберинцидентов осуществляются силами внутреннего подразделения ИБ, хотя каждый второй из них не уверен в том, что квалификации собственных специалистов по ИБ достаточно для проведения расследования. Только треть респондентов (29%) заявила, что компания обращается за помощью к внешним экспертам. Кроме того, как показал опрос, в некоторых компаниях используются лишь базовые средства защиты, которых недостаточно для своевременного выявления сложных целенаправленных атак и полноценного анализа произошедших событий.

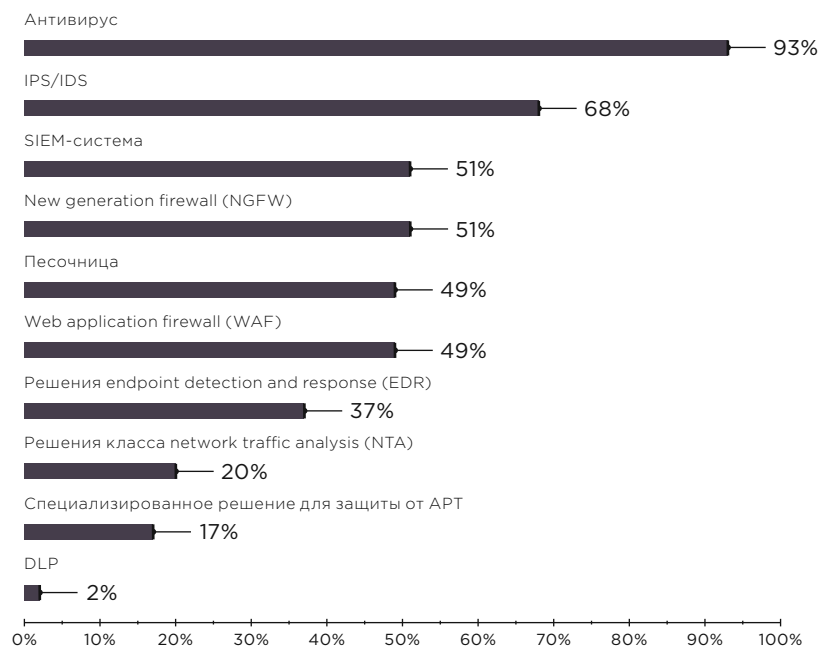


Рисунок 3. Средства защиты, используемые в компаниях
(доля респондентов, представляющих финансовую отрасль)

Для того чтобы построить эффективную стратегию защиты, необходимо понимать, как действуют различные АРТ-группировки и какие мотивы лежат в основе их поведения. Мы разделяем АРТ-группировки на два типа — кибершпионские и финансово мотивированные. Перед ними стоят разные задачи, и это отражается на выборе методов атаки. Для финансовых организаций главная угроза исходит от тех злоумышленников, чья цель заключается в простом и быстром обогащении.

В одном из последних исследований мы уже рассказывали о том, что такое АРТ-атаки. Тогда мы сфокусировались на инструментах злоумышленников и посчитали примерную стоимость проведения атаки. В этой статье мы рассмотрим, как именно АРТ-группировки атакуют российские компании из кредитно-финансовой сферы: какие техники преступники используют, чтобы проникнуть в инфраструктуру компании, и как они действуют внутри, а также выясним, на каких этапах можно выявить атаку и предотвратить кражу денег.

Об исследовании

По нашим оценкам, в последние два года³ кибератаки в отношении российских компаний проводили 22 АРТ-группировки. В данном исследовании мы будем рассматривать тактики и техники десяти АРТ-группировок. Пять из них атаковали российские организации кредитно-финансовой отрасли. Еще пять групп не были замечены в атаках на финансовую сферу в России, но поскольку в списке их жертв значатся иностранные финансовые компании, мы полагаем, что они представляют потенциальную угрозу для финансовых организаций на территории Российской Федерации, а также для их дочерних компаний, находящихся за рубежом. Отметим, что организация может являться как непосредственной целью злоумышленников, так и промежуточным звеном в более сложной цепочке атаки supply chain compromise.

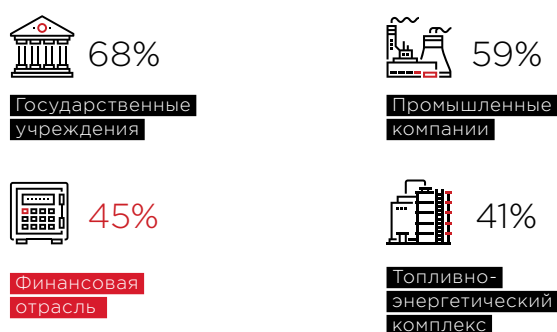


Рисунок 4. Распространенные категории жертв (доля группировок)

В целом атаки развиваются по одному сценарию и похожи между собой. Но у каждой преступной группировки формируется собственный шаблон поведения. Он зависит от состава участников, их навыков, предыдущего опыта, наличия доступа к конкретным инструментам. По мере развития группировка совершенствует свои методы, отбирая наиболее подходящие и отказываясь от бесперспективных стратегий. Например, группировка Silence на заре своей деятельности безуспешно пыталась атаковать системы межбанковских переводов, пока не переключилась на банкоматы и карточный процессинг.

Поведение АРТ-группировок описано в соответствии с [MITRE ATT&CK](#) (Enterprise). В конце отчета мы привели тепловые карты (heat maps), основанные на матрице MITRE ATT&CK, где отражены наиболее часто используемые техники атак на финансовые организации.

MITRE ATT&CK — это база знаний, разработанная и поддерживаемая корпорацией MITRE на основе анализа реальных АРТ-атак. Представляет собой структурированный в виде наглядной таблицы список тактик, для каждой из которых указан список возможных техник атаки. Позволяет структурировать знания об АРТ-атаках и категоризировать действия злоумышленников.

³ Опыт экспертов Positive Technologies показывает, что интервал до двух лет позволяет составить наиболее актуальную картину тактик и техник атаки.

Данные для анализа основаны на результатах исследований киберинцидентов и работ по ретроспективному анализу событий безопасности в инфраструктуре компаний, а также на результатах постоянного отслеживания активности действующих сегодня АРТ-группировок экспертами Expert Security Center компании Positive Technologies (PT ESC). Дополнительно использовалась информация о деятельности АРТ-группировок из общедоступных отчетов, подготовленных ведущими компаниями в области ИБ.

Фишинг — просто и эффективно

Финансовые организации, как правило, становятся целью финансово мотивированных злоумышленников, которые стремятся быстро проникнуть в сеть и вывести из нее деньги. Этим преступникам не столь важно, какая именно компания станет их жертвой: из множества целей они выберут наиболее доступную. Поэтому они предпочитают как можно более простые способы проникновения, и главный среди них — рассылка электронных писем, содержащих вредоносную программу, или фишинг.

Фишинг — это самый распространенный и эффективный способ проникновения в корпоративную сеть любой компании, и финансовые организации не исключение. По нашим оценкам, 75% банков уязвимы для фишинговых атак. В ходе атаки злоумышленники рассылают сотрудникам организации электронные письма, содержащие документ в популярном формате, чаще всего Microsoft Word, либо ссылку на веб-ресурс. Письму придается максимально правдоподобный вид, оно выглядит очень убедительно и может ничем не отличаться от официального сообщения регулятора или письма делового партнера, поэтому человеку сложно распознать подделку. Открыв полученное вложение, пользователь запустит на своем рабочем компьютере вредоносную программу. Этот метод настолько зарекомендовал себя среди киберпреступников, что к нему прибегала каждая АРТ-группировка, замеченная в атаках на кредитно-финансовую сферу.

Если фишинг не работает

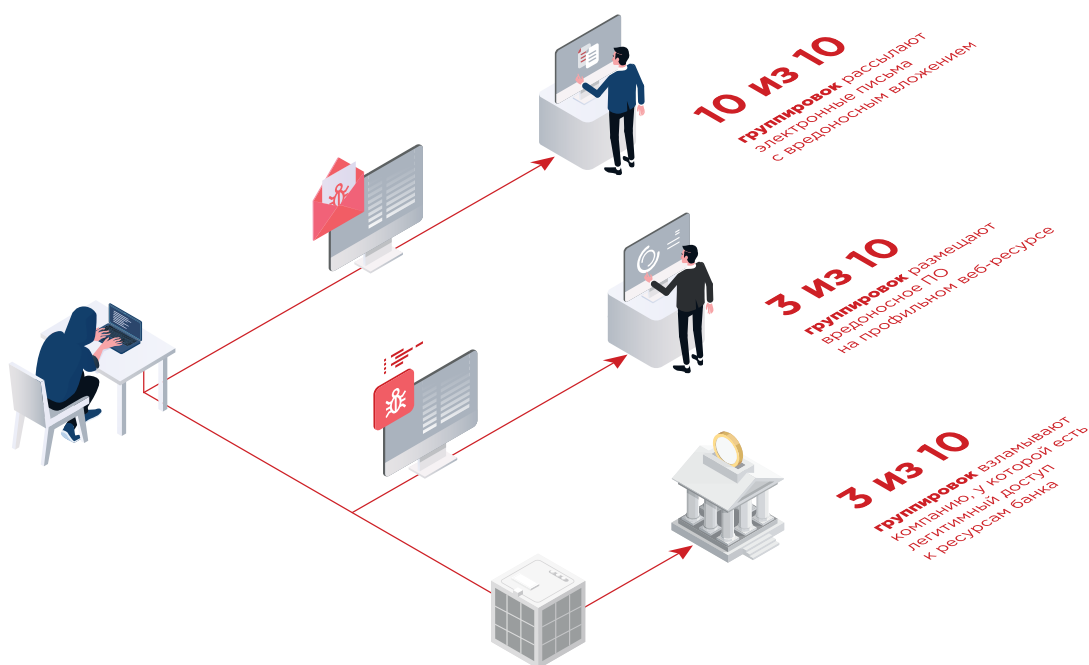
В России в последние два года источником вредоносного ПО в финансовых организациях становились фишинговые письма. Однако за рубежом рассматриваемые нами АРТ-группировки использовали в своей деятельности и другие способы проникновения в инфраструктуру. Не исключено, что в дальнейшем эти же техники будут направлены против российских компаний, поэтому о них тоже следует знать. Два часто встречающихся способа проникновения, drive-by compromise и trusted relationship, связаны с предварительной компрометацией ресурсов менее защищенных организаций.

Drive-by compromise, или watering hole — это распространение вредоносного ПО через профильный веб-ресурс, который посещают сотрудники компании. Злоумышленники взламывают такой сайт и размещают на нем вредоносный код. При посещении зараженного сайта на компьютер пользователя загружается хакерская программа. В России в 2018 году с подобными атаками столкнулись юридические лица, являющиеся клиентами финансовых организаций, когда скомпрометированные ресурсы использовались для распространения трояна Buhtrap.

5 из 10

группировок
используют скомпро-
метированные ресурсы
сторонних компаний
для распространения
вредоносного ПО

Техника *trusted relationship* подразумевает взлом инфраструктуры сторонней организации, которая работает с целевой, например является подрядчиком или обеспечивает техническую поддержку. У сотрудников таких компаний зачастую имеется легитимный доступ к интересующим злоумышленников ресурсам. Точно так же атака на головную компанию может начинаться со взлома менее защищенной дочерней. Кстати, от имени доверенной или просто известной в отрасли организации злоумышленники могут осуществлять рассылку писем с вредоносными вложениями. В конце 2018 года эксперты PT ESC обнаружили новую кибергруппу, атакующую финансовый сектор. Как выяснилось в ходе расследования инцидента, часть фишинговых писем была отправлена со скомпрометированного ящика сотрудника компании «Альфа-Капитал». Группировка Cobalt в IV квартале 2018 года проводила рассылку от лица взломанных банков Unistream и Kassa Nova в Казахстане.



Почему атака остается незамеченной

В финансовых организациях обычно выделяется достаточно большой бюджет на информационную безопасность: в крупных банках он достигает 300 млн рублей в год. Соответственно, система защиты в таких организациях находится на высоком уровне. Для того чтобы остаться незамеченным, необходимо действовать крайне осторожно, поэтому неудивительно, что обход защиты (*defense evasion*) — это самая многочисленная категория по количеству используемых техник.

Чтобы избежать обнаружения антивирусом, вредоносное ПО доставляется в инфраструктуру в упакованном и зашифрованном виде (техники *obfuscated files or information* и *software packing*). Вредоносный код может быть подписан скомпрометированным цифровым сертификатом реально существующей компании (*code signing*), что позволяет выдать его за легитимное приложение. Сертификаты могут быть переиспользованы разными группировками. Так, одним и тем же сертификатом подписывали свои программы Silence и Cobalt.

Еще одна из популярных техник обхода антивирусных решений — внедрение вредоносного кода в память другого процесса, запущенного в системе (process injection). Если же требуется создать новый сервис, например для последующего добавления в автозагрузку, применяется техника masquerading: любой новый сервис будет тщательно замаскирован под легитимный.

Киберпреступники стараются не оставлять следов на рабочих станциях. Поэтому в последнее время в атаках все чаще применяются скриптовые языки программирования: с их помощью можно выполнять команды непосредственно в оперативной памяти компьютера без сохранения исполняемых файлов на жестком диске. В системах Windows особенно популярен инструмент для выполнения сценариев PowerShell. Многие APT-группировки, например Silence и Lazarus, создают новые версии своего ПО с использованием PowerShell.

Мы уже отмечали, что вредоносное ПО сейчас разрабатывается как модульное, то есть состоящее из нескольких частей, каждая из которых выполняет ограниченный набор задач. На компьютеры загружаются только те программные модули, которые нужны на данном этапе атаки. Такой подход помогает снизить риск обнаружения и не позволяет исследователям изучить все части хакерского инструментария. Программы злоумышленников умеют также определять, не находятся ли они в виртуальной среде или песочнице, которые используются для анализа ПО, и безопасно ли подгружать остальные модули.

Для сокрытия каналов управления и дополнительной маскировки могут использоваться известные веб-сервисы. К примеру, группировка Carbanak использовала сервисы Google Docs и Pastebin для хранения своих скриптов.

Г Как APT-группировки обходят системы защиты



9 из 10 группировок

используют вредоносные скрипты
Scripting

8 из 10 группировок

шифруют вредоносное ПО
Obfuscated Files or Information

6 из 10 группировок

внедряют вредоносный код в память легитимного процесса
Process Injection

5 из 10 группировок

маскируют новые сервисы
Masquerading

4 из 10 группировок

подписывают вредоносный код цифровым сертификатом
Code Signing

4 из 10 группировок

используют популярные веб-сервисы для хранения вредоносных файлов
Web Service

4 из 10 группировок

проверяют наличие песочницы
Virtualization/Sandbox Evasion

Злоумышленники стараются уничтожать индикаторы компрометации, то есть те признаки, по которым можно определить, что доступ к компьютеру получили посторонние лица. С рабочих станций удаляются лишние файлы, стираются соответствующие записи журналов Windows и средств защиты (indicator removal on host). ФинЦЕРТ сегодня организует удобный и эффективный канал обмена информацией о киберинцидентах между финансовыми организациями, поэтому сокрытие следов компрометации необходимо еще и для того, чтобы не быть обнаруженными в последующих атаках.

Социальная инженерия вместо эксплойтов

После того как сотрудник компании открывает вложение из фишингового письма и запускает вредоносную программу, злоумышленник получает возможность выполнять команды на его компьютере. Но рядовой сотрудник имеет ограниченный набор привилегий и не может выполнять некоторые действия в системе. Для того чтобы продолжить развитие атаки в инфраструктуре, необходимо обладать правами администратора, то есть повысить привилегии.

Внедрение вредоносного кода в память легитимного процесса, который уже запущен с максимальными правами (process injection), — один из возможных способов повышения привилегий. Его используют 60% группировок, атакующих российские финансовые организации. Помимо этого, злоумышленники часто эксплуатируют широко известные уязвимости в установленном ПО и ОС (exploitation for privilege escalation), для которых доступны публичные эксплойты.

В операционную систему Windows встроен механизм User Account Control (UAC), который запрашивает подтверждение пользователя, если некая программа пытается выполнить действия, требующие прав администратора, например при внесении изменений в реестр Windows или создании новой учетной записи. Если пользователь разрешит программе выполнить эти действия, то она продолжит работу в привилегированном режиме. Обход механизма UAC (техника bypass user account control) позволяет вредоносному ПО работать с повышенными привилегиями, не вызывая лишних оповещений.

Социальная инженерия помогает злоумышленникам не только проникнуть в сеть. Вместо того чтобы обходить UAC, группировка RTM убеждала пользователя разрешить выполнение вредоносной программы. Преступники формировали поддельное окно, изображающее процесс проверки системного реестра, а затем показывали сообщение об ошибке, которое выглядело как стандартное сообщение Windows. Пользователю предлагалось выбрать один из двух вариантов для исправления ошибки. При нажатии на любую из кнопок всплывало настоящее окно UAC, но к этому моменту пользователь был уже уверен, что имеет дело с легитимной системной утилитой, и разрешал дальнейшие действия. В результате хакерская программа продолжала работу с максимальными правами.

Закрепление в сети

Хотя в рассматриваемых нами примерах целью АРТ-группировки является не шпионаж, а кража денег, проведение атаки все равно занимает время: в течение нескольких дней, а иногда и недель злоумышленники изучают сеть, ищут ключевые узлы, наблюдают за рабочими процессами — и только готовятся к краже. По данным ФинЦЕРТ, в среднем с момента проникновения в инфраструктуру до момента хищения проходит 20–30 дней. Чтобы оставаться в инфраструктуре все это время и не потерять связь с управляющим сервером, необходимо надежно закрепиться в сети.

Что такое закрепление в сети

Даже простая перезагрузка компьютера может стать проблемой для злоумышленников, если они не успеют установить надежный канал связи между сетью жертвы и своим командным сервером; всю атаку придется начинать с самого начала. Закрепление означает обеспечение постоянного доступа к узлам сети, невзирая на периодические перезагрузки, изменения паролей пользователей, потерю контроля над отдельными рабочими станциями и другие возможные изменения.

Самая популярная техника закрепления в инфраструктуре — добавление новых сервисов в автозагрузку (registry run keys / startup folder). Так поступают 9 из 10 группировок. В этом случае вредоносное ПО будет автоматически запускаться при каждой загрузке ОС.

Другой распространенный способ обеспечить выполнение вредоносного кода в системе — создание новых задач в планировщике заданий Windows (scheduled task). Планировщик заданий позволяет указать команды, которые будут автоматически выполнены по заданному расписанию. К технике scheduled task прибегает каждая вторая АРТ-группировка.



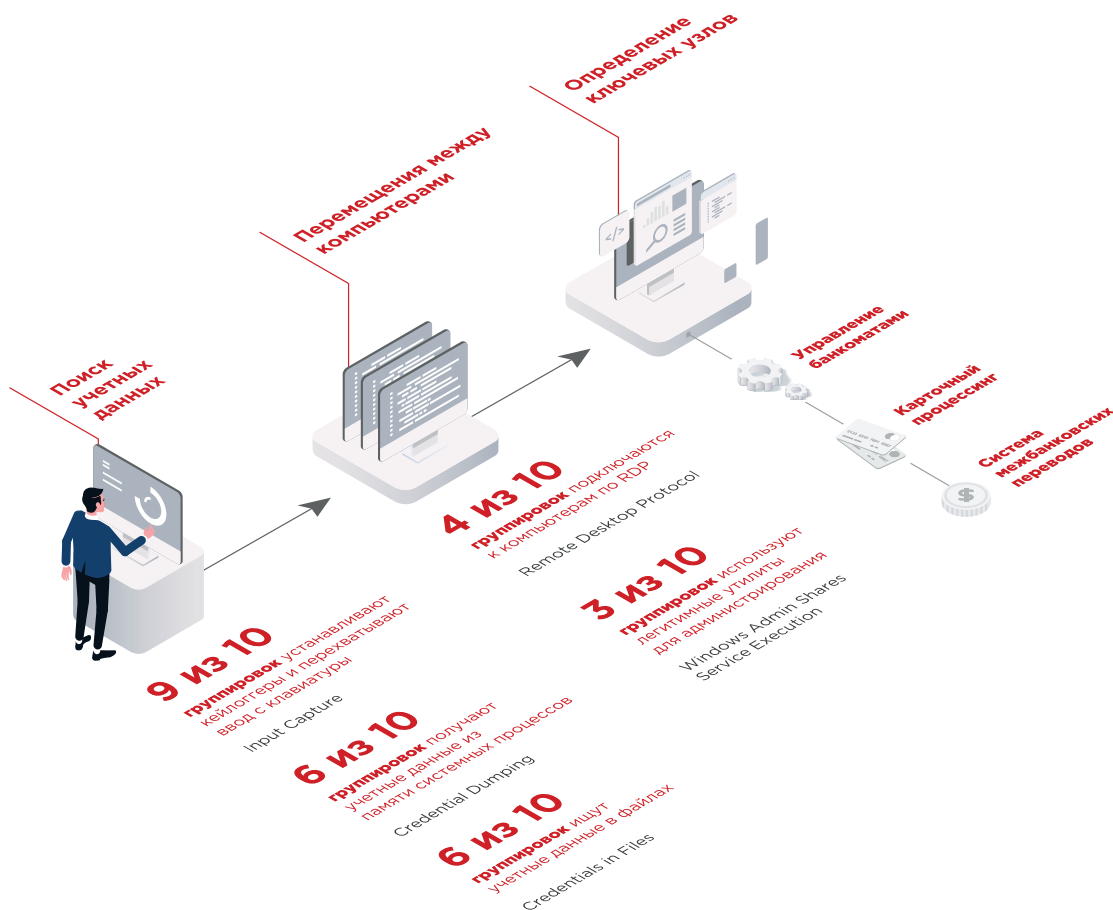
Где искать следы АРТ-атак

Каждая группировка преследует собственные цели и атакует те системы финансовой организации, с которыми умеет работать. К примеру, Silence предпочитает выводить деньги через сеть банкоматов и карточный процессинг, а группировка Cobalt успешно похищала деньги еще и через систему межбанковских переводов SWIFT. Злоумышленникам важно быстро сориентироваться внутри сети и определить узлы, на которых находятся искомые банковские системы или рабочие станции операторов.

Активное изучение сети сопровождается множеством перемещений между различными узлами и быстрым сбором сведений о компьютерах: атакующим нужно понять, представляют они интерес или нет. На этом этапе злоумышленники оставляют множество свидетельств своего присутствия в сетевом трафике. Анализ трафика может выявить АРТ-атаку до того, как атакующие получают доступ к критически важным системам.

Перемещение между компьютерами обычно осуществляется с помощью легитимных утилит, которые используют в своей работе системные администраторы, например PsExec (техники service execution и Windows admin shares), или по протоколу RDP, который применяется для удаленного доступа к рабочим столам.

Учетные данные для доступа к компьютерам злоумышленники получают, применяя классическую технику credential dumping — извлечение паролей (или хеш-сумм паролей) пользователей ОС из памяти системных процессов. В ходе атаки нужно не просто попасть на компьютер пользователя, но и получить учетные данные для доступа к банковским системам, поэтому 90% группировок устанавливают на зараженные рабочие станции кейлоггеры — вредоносное ПО, способное перехватывать ввод данных с клавиатуры (техника input capture). Учетные данные могут также храниться в конфигурационных файлах (credentials in files) и ключах реестра (credentials in registry).



Сотрудники под наблюдением

Злоумышленникам важно подробно изучить ПО, которым пользуются в компании. Чтобы вывод средств прошел быстро и без осечки, необходимо знать стандартные рабочие процессы, принятые в конкретной организации, и порядок осуществления операций. Кроме того, следует предусмотреть риск срабатывания средств защиты и выяснить, можно ли их отключить. Добравшись до ключевых узлов, группировка переходит к активному изучению банковских систем; и это последняя возможность предотвратить кражу денег.

На этом этапе преступники наблюдают за действиями сотрудников при работе с банковским ПО. Они используют специальные программы, которые позволяют незаметно для пользователя делать скриншоты экранов (screen capture), записывать небольшие видео (video capture) и перехватывать вводимые с клавиатуры данные (input capture). Некоторые группировки, к примеру [Cobalt](#) и [Lazarus](#), используют для этих целей модифицированные версии утилит для администрирования Ammyy Admin, TeamViewer и VNC.

Если атака все еще не выявлена, то скоро в распоряжении преступников оказываются все необходимые учетные записи и информация о правилах работы с банковскими системами, не говоря уже о том, что большая часть инфраструктуры, скорее всего, уже давно находится под их контролем. Теперь остановить атаку практически невозможно.



Связь с командным центром

Командный центр — это внешний сервер, с которого злоумышленники управляют ходом атаки. Связь с этим сервером в 70% случаев осуществляется по широко распространенным протоколам, таким как HTTP или HTTPS. Такой трафик легко замаскировать под легитимный. Половина группировок использует стандартные порты (commonly used port), которые обычно не блокируются межсетевым экраном. Впрочем, некоторые группировки, к примеру [Lazarus](#) и [Treasure Hunter](#), разрабатывают собственные протоколы передачи данных. Вероятно, это делается с целью затруднить расследование и анализ сетевого трафика.

Данные шифруются перед отправкой, чтобы обойти средства защиты от утечек информации (DLP-системы). Четыре из десяти группировок используют для этого известные алгоритмы шифрования, а еще четыре — их модификации.

40%

группировок
используют программы
для вывода из строя
компьютеров организации
после кражи денег

Кража денег — еще не финал

Кража денег — это еще не окончание атаки. В отличие от кибершпионов, злоумышленникам не требуется скрывать сам факт атаки: о краже станет известно незамедлительно. Однако им важно затруднить расследование инцидента и сделать так, чтобы вредоносное ПО не попало в руки специалистов по информационной безопасности: появление новых сигнатур и индикаторов компрометации может сильно осложнить дальнейшую деятельность группировки. Поэтому на завершающем этапе АРТ-группировка будет пытаться уничтожить все следы атаки, что означает удаление или шифрование всех данных на рабочих станциях, уничтожение структуры жестких дисков. Так поступали Lazarus и Cobalt, подобные функции заложены в ПО, которое использует группировка RTM.

Если злоумышленникам удалось вывести из компании деньги, значит, их привилегий достаточно для того, чтобы полностью вывести из строя инфраструктуру. Это будет сделано незамедлительно после подтверждения успешности атаки. Восстановление инфраструктуры — долгий и затратный процесс. Ущерб от простоя инфраструктуры и нарушения бизнес-процессов может быть сопоставим с той суммой, которую компания потеряла непосредственно в результате кражи. В феврале 2019 года после кибератаки мальтийский банк, Bank of Valletta, почти на сутки приостановил деятельность всей своей сети, включая услуги интернет-банкинга, работу банкоматов и POS-терминалов. Кроме того, просто восстановить работоспособность систем недостаточно, потребуется провести тщательное расследование произошедшего, и на это тоже нужно время.

Как узнать об АРТ-атаке до потери денег

Предотвратить АРТ-атаку невозможно, но ее можно своевременно выявить и остановить. Важно сделать это до того, как будут затронуты критически важные системы организации. С момента компрометации инфраструктуры до кражи денег в среднем проходит около трех-четырех недель. Злоумышленники находятся в сети настолько долго, насколько требуется для изучения банковских систем, однако после того, как вся необходимая информация получена, вывод средств проводится за считанные часы. Поэтому для каждой организации кредитно-финансовой сферы очень важно выбрать стратегию защиты, которая позволит обнаружить действия злоумышленников как можно раньше.

Традиционные решения уже не в силах обеспечить защиту от угроз уровня АРТ. Как показывает практика, киберпреступники научились обходить и антивирусы, и песочницы. Избежать потери денег можно лишь в том случае, если в организации реализован комплексный подход к безопасности и используются современные средства защиты.

Чтобы вовремя выявить атаку, необходимо, прежде всего, ясное понимание происходящего в инфраструктуре. Постоянный мониторинг событий ИБ вкупе с глубоким анализом сетевого трафика позволит заметить аномальную активность в сети на ранних стадиях.

Деятельность ФинЦЕРТ способствует снижению числа успешных атак на организации кредитно-финансовой сферы. К сожалению, не все активно включены в процесс обмена информацией об инцидентах, и это не дает возможности другим участникам узнать о новых угрозах и заранее подготовиться к ним. При этом менее защищенные организации ставят под угрозу остальные компании, поскольку, не сумев самостоятельно справиться с последствиями инцидента, могут сами стать источником распространения вредоносного ПО. Мы рекомендуем финансовым организациям активно участвовать в обмене информацией о кибератаках и индикаторах компрометации.

Стоит заметить, что необходимо не только знать о новейших индикаторах компрометации, но и применять технические решения, которые используют такие индикаторы для поиска следов атаки в копии сетевого трафика за длительный период времени, то есть поддерживают возможность ретроспективного анализа трафика. Такой подход помогает выявить присутствие злоумышленников в инфраструктуре даже в том случае, если в момент проведения атаки еще не существовало сигнатур для ее обнаружения.

Чтобы противостоять угрозе АРТ-атак, организациям следует регулярно пересматривать подход к защите, который должен соответствовать современным реалиям. Необходимо понимать тактики и техники киберпреступников, обмениваться сведениями об актуальных угрозах в отрасли, готовиться незамедлительно реагировать на возникающие события ИБ, а также привлекать к сотрудничеству высококвалифицированных специалистов в области расследования инцидентов.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Disk Structure Wipe
Hardware Additions	Compiled HTML File	AppCert DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Appinit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Service Stop
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Stored Data Manipulation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Transmitted Data Manipulation
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Runtime Data Manipulation
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Firmware Corruption
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Resource Hijacking
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Network Denial of Service
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Endpoint Denial of Service
	Mshhta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityfd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshhta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelganging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

80-100%60-80%40-60%20-40%0-20%

Тепловая карта тактик и техник АРТ-атак (группировки, атакующие финансовые компании)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Disk Structure Wipe
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Service Stop
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Stored Data Manipulation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Transmitted Data Manipulation
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Runtime Data Manipulation
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Firmware Corruption
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Resource Hijacking
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Network Denial of Service
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Endpoint Denial of Service
	Mshsta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SiD-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshsta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelganging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

80-100%
60-80%
40-60%
20-40%
0-20%

Тепловая карта тактик и техник АРТ-атак (все группировки, атакующие компании в России)

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.