



PT

# APT-атаки на госучреждения в России

Обзор тактик и техник  
2019

[ptsecurity.com](http://ptsecurity.com)

## Содержание

Об исследовании	2
Госучреждения не готовы к АРТ-атакам	4
Все начинается с фишинга	6
Что еще, кроме фишинга	6
Почему антивирус не сработал	7
Найти главное	9
На пути к цели	10
Если остановить не удалось	11
Финишная прямая	12
Вы их за дверь, а они — в окно	13
Что делать, чтобы не стать жертвой АРТ-атаки	14
Тепловая карта тактик и техник АРТ-атак (группировки, атакующие госучреждения)	16
Тепловая карта тактик и техник АРТ-атак (все группировки, атакующие компании в России)	17



## Об исследовании

Ранее мы рассказали о том, что такое сложные целенаправленные атаки (атаки типа advanced persistent threat, АРТ-атаки), какие инструменты используют злоумышленники для таких атак, и оценили, сколько они могут стоить. Мы пошли дальше и проанализировали поведение 22 АРТ-группировок, атаковавших российские организации на протяжении последних двух лет<sup>1</sup>. Среди целей группировок есть множество организаций, входящих в рейтинги крупнейших компаний России и являющихся лидерами в своих отраслях.



68%

Государственные  
учреждения



59%

Промышленные  
компании



45%

Финансовая  
отрасль



41%

Топливо-  
энергетический  
комплекс

Распространенные категории жертв (доля атакующих АРТ-группировок)

Мы провели опрос<sup>2</sup> среди посетителей сайта компании Positive Technologies, аудитории интернет-портала [SecurityLab.ru](https://securitylab.ru)<sup>3</sup> и участников ряда отраслевых сообществ, в которые входят эксперты по ИТ и ИБ из различных сфер отечественного бизнеса, — с целью оценить готовность российских компаний к противодействию сложным целенаправленным атакам. Далее мы расскажем о результатах этого опроса. Если кратко — противостоять АРТ-атакам готовы немногие.

Для того, чтобы эффективно защищаться, необходимо понимать, как именно преступник будет атаковать и какие у него мотивы. Каждую группировку можно охарактеризовать уникальной совокупностью мотивов, инструментов и методов, однако у киберпреступников есть и общие черты. В этом отчете рассмотрена специфика АРТ-атак на российские государственные учреждения — министерства, ведомства, администрации. Мы попытаемся показать, как будет действовать атакующая группа, если решит взломать вашу организацию. И конечно — предложим вариант защиты.

1. Опыт экспертов Positive Technologies показывает, что интервал до двух лет позволяет составить наиболее актуальную картину тактик и техник атаки.
2. В опросе приняли участие 306 респондентов. Доля представителей госучреждений составила 13%.
3. 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.

Г **АРТ-атака на госучреждение** — это сложная целенаправленная атака на информационные системы государственных учреждений, как правило для осуществления кибершпионажа. Мотивами также могут быть саботаж, подрыв репутации государственных структур, дестабилизация политической обстановки.

Поведение АРТ-группировок описано в соответствии с MITRE ATT&CK (Enterprise). Злоумышленники выбирают техники в зависимости от собранных на этапе разведки сведений об атакуемой организации, своего опыта и инструментов. В случае неудачи в ход идут альтернативные техники. В конце отчета мы привели тепловые карты (heat maps), основанные на матрице MITRE ATT&CK, с наиболее часто используемыми техниками атак на государственные организации.

Г **MITRE ATT&CK** — это база знаний, разработанная и поддерживаемая корпорацией MITRE на основе анализа реальных АРТ-атак. Представляет собой наглядную таблицу тактик атаки, для каждой из которых дан перечень возможных техник. Позволяет структурировать знания об АРТ-атаках и категоризировать действия злоумышленников.

Помимо данных, собранных в ходе опроса специалистов по ИТ и ИБ, упомянутого выше, для анализа были использованы результаты расследований киберинцидентов и работ по ретроспективному анализу событий безопасности в инфраструктуре компаний, а также результаты постоянного мониторинга активности действующих сегодня АРТ-группировок экспертами Positive Technologies Expert Security Center. Дополнительно использовалась информация из общедоступных отчетов о деятельности АРТ-группировок, подготовленных ведущими компаниями в области ИБ.

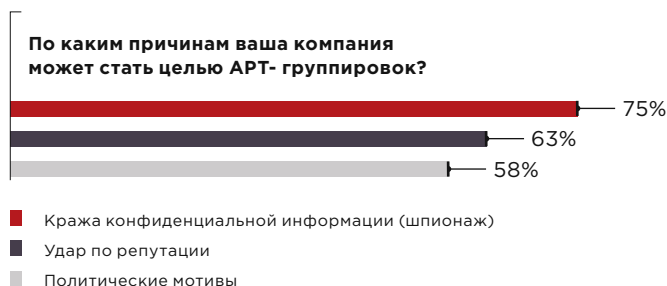


# 68%

**АРТ-группировок, нацеленных на Россию, атакуют государственные учреждения**

## Госучреждения не готовы к АРТ-атакам

Две трети АРТ-группировок, атакующих сегодня российские организации, нацелены на госучреждения. В информационных системах государственных организаций хранятся и обрабатываются критически важные данные, в которых заинтересованы кибершпионы, и поэтому такие организации находятся под постоянной угрозой кибератак. Три четверти участников нашего опроса, представляющих госучреждения, согласны, что кража информации может стать мотивом для АРТ-атаки.



Топ-3 предполагаемых целей АРТ-атак  
(доля респондентов, представляющих госучреждения)

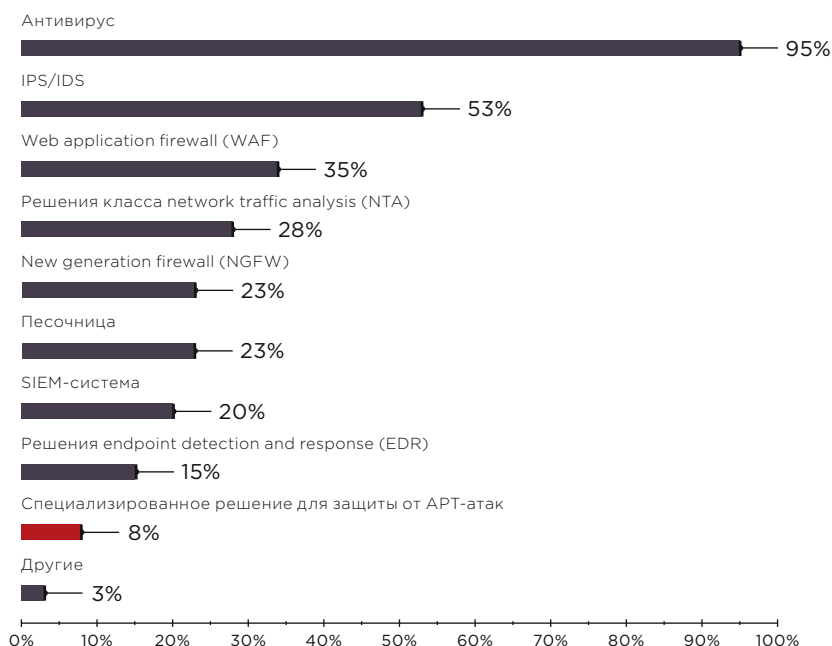


Топ-3 последствий кибератак  
(доля респондентов, представляющих госучреждения)

**Только 17% респондентов — работников госучреждений отметили, что защита от АРТ-атак является приоритетным направлением развития ИБ в их организации**

Более половины (57%) респондентов, работающих в государственных организациях, констатировали, что риск успешной кибератаки является для них крайне значимым. Но в то же время 45% участников опроса отметили, что организация не готова противостоять АРТ-группировкам. Мы полагаем, что многие организации, которые уверены, что не подвергались целенаправленным атакам, или считают, что не представляют интереса для преступных кибергруппировок, — даже не подозревают о том, что уже могли попасть под прицел злоумышленников. Как следует из ответов респондентов, в государственных организациях преимущественно используются лишь базовые средства защиты, которые не способны обнаружить и вовремя остановить сложные атаки. Неэффективность действующих систем защиты, слабое представление о кибербезопасности среди госслужащих, отсутствие практики расследования инцидентов — все эти факторы создают предпосылки для успешного взлома.

### Какие технические средства защиты информации применяются в компании?



Используемые средства защиты  
(доля респондентов, представляющих госучреждения)

48%

респондентов отметили, что в организации **не проводится обучение сотрудников основам кибербезопасности**

68%

респондентов **не уверены в достаточной квалификации специалистов по ИБ** в их организации для выявления и расследования киберинцидентов

23%

респондентов сообщили, что в организации **отсутствует практика выявления и расследования киберинцидентов**

Если организация стала мишенью APT-группировки, то рано или поздно злоумышленникам удастся осуществить атаку. Но означает ли это, что от APT-группировок бессмысленно защищаться? Атакуя государственные учреждения, кибершпионы в первую очередь нацелены на кражу информации. Но при ее скрытом копировании ценные сведения не пропадают, как пропадают деньги со счетов в случае финансово мотивированных атак. Из-за этого присутствие злоумышленников в инфраструктуре может оставаться незамеченным долгое время, вплоть до нескольких лет. Если атаку невозможно предотвратить, то надо постараться ее остановить до того момента, когда критически важные данные будут похищены. Для этого необходимо понимать, как действуют киберпреступники внутри инфраструктуры в поисках ценной информации.



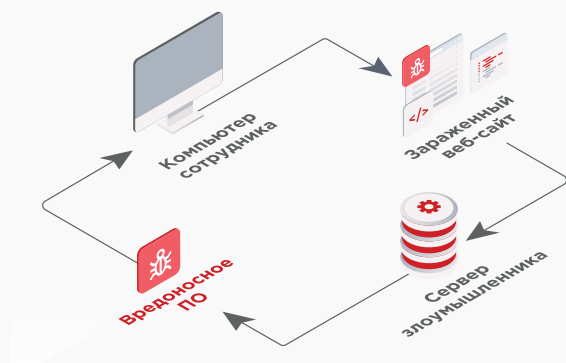
## Все начинается с фишинга

Большинство АРТ-группировок (87%) начинают атаки на государственные учреждения с целенаправленного фишинга. Сотрудникам рассылаются электронные письма, цель которых — вынудить получателя открыть приложенный файл или перейти по ссылке. Как показывают наши работы по оценке осведомленности сотрудников различных организаций в вопросах ИБ, каждый третий получатель фишингового письма запускает вредоносный файл. В результате атаки взломщик получает контроль над компьютером. Если вы работаете в госучреждении, и оно стало целью АРТ-группировки, то ваш компьютер может оказаться первым звеном в цепочке сложной атаки. Поэтому советуем внимательно относиться ко всем письмам, которые приходят на электронную почту: не открывайте файлы из писем от незнакомых отправителей, не переходите по ссылкам, если вы не знаете точно, куда они ведут.

Скорее всего, АРТ-группировка приложит к письму вредоносный файл (spearphishing attachment), который трудно отличить от любых других, которые вы получаете в переписке с коллегами ежедневно. Такие письма рассылают 87% АРТ-группировок, атакующих государственные организации. Как правило, вредоносное вложение маскируется под документ в формате Microsoft Office; в любой государственной организации обрабатывается множество подобных документов.

## Что еще, кроме фишинга

Фишинг не единственная опасность. Некоторые АРТ-группировки могут применять и другие техники, например технику drive-by compromise.



### Что такое drive-by

Это техника атаки, при которой вредоносные программы незаметно загружаются на компьютер жертвы при посещении скомпрометированных ресурсов. Типовая схема атаки: сотрудник попадает на зараженный сайт, откуда вредоносный скрипт перенаправляет его на сервер злоумышленника. Далее запускается эксплойт — программа, использующая уязвимости в ОС и приложениях. Через бреши на компьютер проникает вредоносное ПО, которое в случае успешного завершения загрузки дает злоумышленнику контроль над зараженной системой.

Для атак типа drive-by APT-группировки выбирают сайты, которые посещают сотрудники государственных организаций. Этот метод называется watering hole, или strategic web compromise. Он не так распространен, как фишинг: 27% группировок применяли его в отдельных кампаниях. Атаки watering hole сложнее в исполнении, поскольку злоумышленникам предварительно требуется взломать определенные сайты, что увеличивает трудозатраты и время на проникновение. В то же время, согласно результатам нашего исследования, злоумышленник может получить полный контроль над каждым пятым сайтом и его сервером, а значит — каждый пятый сайт является потенциальной платформой для размещения вредоносного ПО. Если в вашей организации разрешена загрузка файлов с интернет-сайтов, не скачивайте ничего лишнего на компьютер. Не разрешайте установку программ, которые рекомендуют сайты: установка ПО — это работа системного администратора.

Каждая вторая APT-группировка, кроме фишинговых писем и заражений типа drive-by, хотя бы раз на этапе проникновения использовала другие техники. Получить доступ к внутренней инфраструктуре злоумышленники могут за счет уязвимостей в приложениях, доступных из интернета (exploit public-facing application); пример такого приложения — веб-сайт организации. Злоумышленники могут атаковать организацию через компании, сотрудники которых имеют доступ к инфраструктуре жертвы, например через подрядчика IT-услуг (trusted relationship).



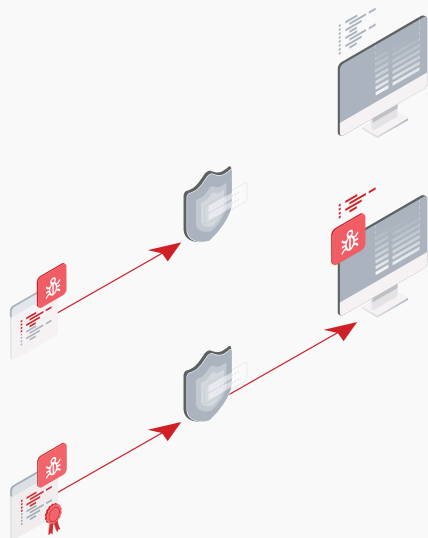
**Г** Чтобы гарантировать успех атаки и не быть обнаруженными, **злоумышленники используют уязвимости нулевого дня**

## Почему антивирус не сработал

Без должной маскировки вредоносное ПО будет обнаружено средствами защиты. Но почему в случае с АРТ-атакой этого не происходит? Дело в том, что злоумышленники отдают предпочтение новым уязвимостям, для которых еще не выпущены обновления безопасности. Это так называемые уязвимости нулевого дня. Такие уязвимости для АРТ-группировок — гарантия успеха. Поскольку на момент взлома об уязвимости не знают ни производитель ПО, ни разработчики средств защиты, то и способа (сигнатуры) для обнаружения вредоноса, который использует такую уязвимость, пока не существует.

Еще один способ обхода средств защиты связан с использованием цифровых сертификатов (техника code signing). Преступники просто подпишут свой код, причем не исключено, что для этой цели они незаконно воспользуются действующим сертификатом другой компании.





## Code signing: как это работает

Средства защиты лояльно относятся к файлам с цифровыми подписями, считая их доверенными. Подписав зловред, злоумышленники рассчитывают обмануть механизмы безопасности. Сертификаты для таких целей продаются в дарквебе. Они могут попадать в руки злоумышленников в результате атак supply chain. Так, злоумышленники взломали сервер ASUS и распространяли под видом обновлений вредоносное ПО, подписанное сертификатом компании.

Но одной цифровой подписи недостаточно для обхода антивируса. Злоумышленники обфусцируют (запутывают) вредоносный код, шифруют его и используют специальные упаковщики, противодействуя таким образом анализу средствами защиты.

Злоумышленники умеют детектировать не только версии антивирусного ПО, но и установленные в системе средства виртуализации, например песочницы (virtualization/sandbox evasion). Песочницы предоставляют изолированную среду, в которой можно безопасно запускать различные программы для анализа их алгоритма работы на предмет вредоносной активности. Если зловред «понимает», что находится в виртуальной среде, он прекращает свою работу. Для противодействия анализу в исходный код инструмента из арсенала группировки MuddyWater «вшит» список программ, которые часто используют вирусные аналитики. Обнаружив присутствие такой программы, вредоносное ПО переходит в «тихий режим».

Две трети (67%) АРТ-группировок удаляют вредоносные файлы, которыми больше не пользуются. Например, атакующая российские правительственные ресурсы группировка Cloud Atlas использует вредонос VBShower, который умеет удалять временные файлы, свидетельствующие о присутствии злоумышленников. Кроме того, взломщики, зная, что антивирусные средства регулярно сканируют компьютеры в поисках вредоносных программ, научились обходиться без файлов. Существуют техники, которые позволяют киберпреступникам выполнять вредоносные действия прямо в оперативной памяти, не оставляя никаких следов на жестком диске. Такие вредоносы принято называть «бестелесными», поскольку они существуют только в оперативной памяти компьютера и перестают работать после перезагрузки.

93%

кодируют и шифруют  
вредоносный код  
Obfuscated Files or Information

67%

используют бестелесный  
вредоносный код  
Process Injection

40%

проверяют наличие  
песочницы  
Virtualization/Sandbox Evasion

27%

подписывают вредоносные файлы  
цифровой подписью  
Code Signing

Техники противодействия обнаружению (доля АРТ-группировок)

## Найти главное

В государственных организациях документация проходит через ряд компьютеров сотрудников (секретаря, руководителя, его заместителя, руководителя структурного подразделения и непосредственных исполнителей), и на каждом из них могут оставаться копии ценных документов либо доступ к ценным хранилищам. Злоумышленникам остается лишь найти те компьютеры, владельцы которых занимают достаточно высокие должности и ввиду выполняемых обязанностей имеют доступ к большому объему информации. Безусловно, интересуют преступников также и базы с персональными данными, и ваша система электронного документооборота, если она используется.

### Какая информация может заинтересовать злоумышленников

- Персональные данные сотрудников и других граждан
- Сведения в области внешней политики и экономики
- Научно-исследовательские и проектные работы
- Финансовая отчетность

После проникновения киберпреступники первым делом проведут разведку, чтобы понять, как устроена ваша внутренняя сеть: выяснят диапазоны IP-адресов, изучат сегментацию сети. На компьютерах большинства сотрудников установлена Windows, поэтому злоумышленники наверняка воспользуются встроенным интерпретатором PowerShell. Например, в трояне группировки Treasure Hunter предусмотрен отдельный модуль для выполнения PowerShell-команд.

60%

АРТ-группировок, атакующих  
государственные организации,  
используют PowerShell

## Г Что такое PowerShell

PowerShell — это инструмент администрирования и среда выполнения сценариев для ОС Windows. Может использоваться взломщиками на всех этапах атаки.



Компьютеры под управлением Windows внутри сети обычно объединены в домены. Это делают для того, чтобы было удобнее администрировать инфраструктуру организации. Цель атакующих — скомпрометировать учетную запись администратора домена. Зачем им это? Киберпреступники изначально не знают, где именно хранится интересующая их информация, поэтому попытаются проникнуть во все важные системы, и для этого им необходимо обойти парольную защиту. Сделать это они могут заполучив пароль администратора домена. После этого можно заходить на серверы и в компьютеры сотрудников как к себе домой.

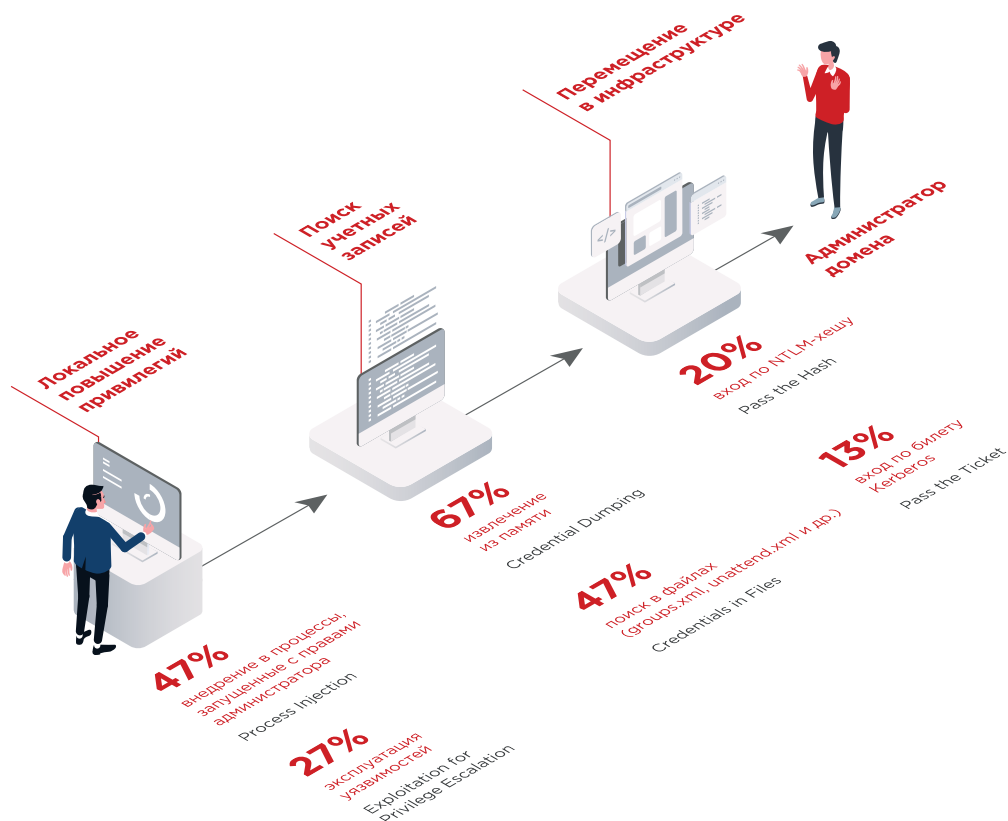
## На пути к цели

Прежде чем злоумышленники доберутся до учетной записи администратора домена, им потребуется выполнить множество действий, для которых недостаточно прав обычного пользователя компьютера или домена. С этого момента группировка может оставить множество следов (артефактов) в инфраструктуре, обнаружив которые вы сможете поймать преступника, что называется, за руку.

Зачастую для продолжения атаки злоумышленникам необходимо повысить свои привилегии в скомпрометированной системе до прав локального администратора. Сделать это можно разными способами. Например, киберпреступникам помогают бреши в установленных на компьютерах приложениях. Техника называется *exploitation for privilege escalation*, ее используют 27% APT-группировок, атакующих государственные организации. Кроме того, существуют хакерские утилиты для выполнения произвольного кода в контексте процесса, запущенного с правами администратора (*process injection*); их используют 47% APT-группировок.

Получив возможность выполнять действия с правами локального администратора, злоумышленники, скорее всего, воспользуются инструментами для извлечения учетных данных прямо из памяти системных процессов (техника *credential dumping*). Например, группировка LuckyMouse для этих целей использует утилиту Wrapikatz. Пароли хранятся в виде хеш-значений, что должно защищать их от злоумышленников, но для атакующих это давно не проблема, поскольку особенности NTLM (протокола аутентификации в Windows) позволяют получать доступ к компьютерам не по паролю, а по его хеш-значению; техника называется *pass the hash*. Если используется система аутентификации Kerberos, то злоумышленники могут прибегнуть к технике *pass the ticket*. Все подобные перемещения злоумышленника вы сможете отследить, нужно лишь уметь искать следы в сетевом трафике.

Не исключено, что применять техники извлечения паролей из оперативной памяти взломщикам не придется, ведь если системный администратор организации недостаточно позаботился о безопасности, то злоумышленники найдут учетные данные в служебных файлах. Эти методы крайне эффективны при «горизонтальном перемещении», когда атакующие подключаются с одного компьютера на другой в сети, захватывая контроль над большим количеством систем и расширяя свое влияние на инфраструктуру.



Развитие атаки до получения прав администратора домена (доля APT-группировок)

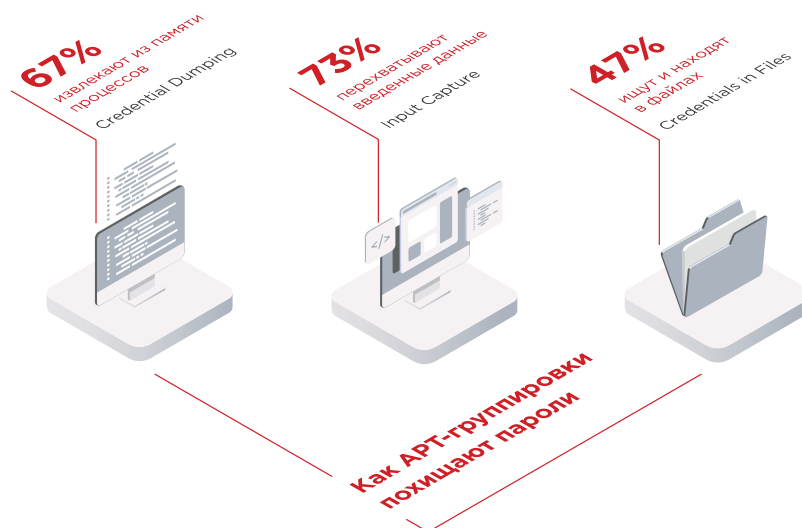
При всем разнообразии техник атаки и способов скрыть свое присутствие — обнаружить злоумышленников на этапе перемещения в инфраструктуру возможно. Перемещаясь между системами, злоумышленники оставляют следы в сетевом трафике, а значит, их действия можно отследить. На этом этапе атакующие еще не взяли под контроль всю инфраструктуру и не успели похитить критически важные данные — и это самое подходящее время для того, чтобы их остановить.

## Если остановить не удалось

Получив учетную запись администратора домена, злоумышленники, скорее всего, установят на компьютеры ключевых лиц организации (генерального директора, руководителей подразделений, заместителей, бухгалтеров и даже секретарей) шпионское ПО, которое делает снимки экрана, аудио- и видеозаписи. Злоумышленники могут запустить кейлоггеры — программы, позволяющие перехватывать нажатие клавиш и похищать таким образом любую информацию, которую пользователь вводит с клавиатуры (техника input capture). Кейлоггеры пользуются большой популярностью среди злоумышленников, они есть, например, в арсенале таких группировок, как DarkHotel, LuckyMouse, Lazarus.

Тотальный контроль за действиями первых лиц организации дает возможность злоумышленникам читать их переписку и даже отправлять распоряжения от их имени. Кроме того, с помощью кейлоггеров атакующие перехватывают пароли от бизнес-систем с критически важной информацией, доступа к которой нет у рядовых сотрудников. Но

зачастую кейлоггеры не требуются, ведь некоторые пользователи хранят учетные данные для доступа к различным системам прямо в текстовых файлах на компьютерах (credentials in files) или сохраняют параметры сессии, чтобы не вводить пароль при следующем входе.



Техники кражи паролей (доля АРТ-группировок)

Шпионское ПО, которое используют взломщики, также имеет механизмы защиты от обнаружения. Однако на данном этапе у злоумышленников уже достаточно прав, чтобы отключить или перенастроить системы защиты, поэтому обнаружить действие вредоносного ПО не удастся.

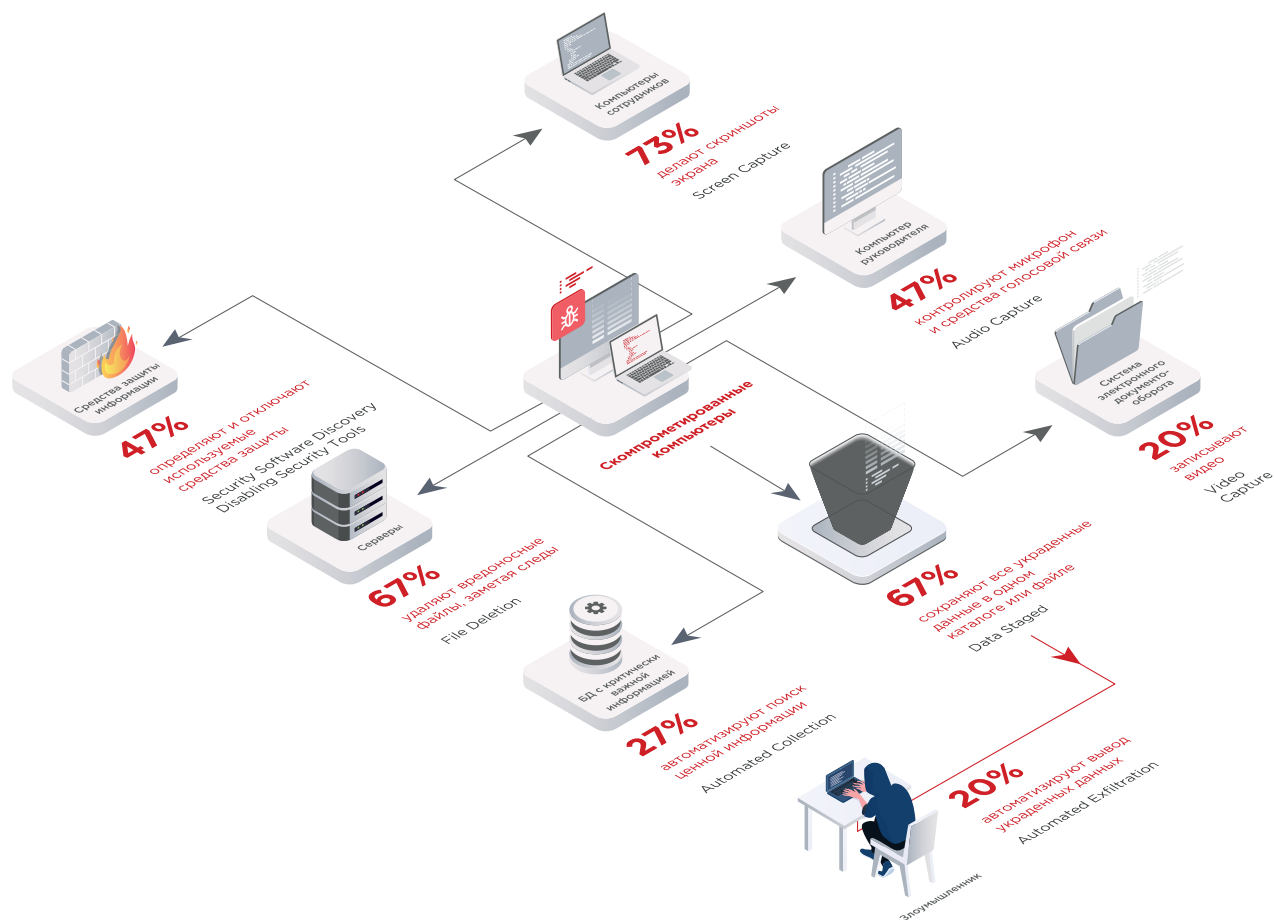
## Финишная прямая

После того как злоумышленники получают доступ к системам, где вы обрабатываете и храните важные данные, они приступят к выводу похищенной информации. Это последний этап атаки, на котором ее еще не поздно остановить, и важно это сделать до того, как данные утекут. Для этого важно понимать, как действуют атакующие после того, как найдут сведения, за которыми пришли.

Как правило, все похищенные данные взломщики собирают в одном месте (в файле или папке на скомпрометированном узле), откуда потом отправляют их на свои серверы в интернете или в сети Tor. Перед отправкой данные могут помещаться в архивы с паролем.

Нередко процесс подготовки данных к передаче вовне автоматизирован. Функции шифрования и сжатия может взять на себя основной шпионский троян, но могут использоваться и специально написанные для этой цели скрипты, например на языке PowerShell. Не исключено, что злоумышленники решат готовить данные для передачи вручную с использованием легитимных инструментов, например архиватора WinRAR. Шифрование данных перед отправкой позволяет злоумышленникам обходить средства защиты от утечек информации (data loss prevention, DLP).





Техники злоумышленников в ходе развития атаки (доля АРТ-группировок)

Как правило, для любого сетевого взаимодействия, в том числе и для передачи украденных данных, злоумышленники выбирают стандартные протоколы (HTTP, HTTPS, DNS), создают туннели. Это делается для того, чтобы обойти межсетевые экраны, которые могут блокировать порты для передачи данных по другим протоколам. Но далеко не всегда межсетевой экран имеет безопасную конфигурацию. Если он разрешает подключения на так называемых нестандартных, или пользовательских портах, то злоумышленники могут воспользоваться этим (техника uncommonly used port). К такому методу прибегают 40% АРТ-группировок. Например, киберпреступники из состава Gorgon Group используют для связи с командным сервером троян NanoCore, который работает через нестандартный порт 6666.

60%

используют стандартные порты (80, 443, 53 и др.)  
Commonly Used Port

40%

используют нестандартные порты  
Uncommonly Used Port

## Вы их за дверь, а они — в окно

Важно понимать, что злоумышленники обязательно попытаются закрепиться в инфраструктуре, чтобы долго шпионить за вашей организацией. Они должны иметь возможность вернуться в скомпрометированную инфраструктуру, даже если вредоносное ПО было

удалено, компьютеры перезагружены, а пароли изменены. Для этого используется множество техник, приведем лишь некоторые примеры. Взломщики могут настраивать автозагрузку программ (registry run keys / startup folder), создавать новые или модифицировать существующие сервисы (new service, modify existing service), оставлять бэкдоры для удаленного доступа, например веб-шеллы (web shell).

93%

настраивают  
автозапуск программ  
Registry Run Keys / Startup Folder

60%

создают новые сервисы  
New Service

27%

модифицируют  
существующие сервисы  
Modify Existing Service

13%

внедряют веб-шеллы  
Web Shell

Техники закрепления в инфраструктуре (доля АРТ-группировок)

Преступники стараются действовать максимально скрытно, чтобы не пришлось использовать резервные каналы доступа к инфраструктуре. Например, каждая пятая АРТ-группировка настраивает передачу данных таким образом, чтобы она осуществлялась только в определенные промежутки времени, по расписанию. Так, группировка TaskMasters активно использует задачи по расписанию на разных этапах атаки.

## Что делать, чтобы не стать жертвой АРТ-атаки

Очевидно, что для противостояния сложным целенаправленным атакам необходим особый подход. АРТ-группировки, атакующие госучреждения, как правило нацелены на длительный контроль над всей инфраструктурой. Такой контроль им может понадобиться не только для шпионажа, но и в целях саботажа или ведения информационной войны. Злоумышленники могут годами таиться в инфраструктуре и перейдут к активным действиям только в момент обострения геополитической обстановки. Это позволяет выбрать такую стратегию противодействия, когда ключевой задачей ИБ становится не пресечение атаки как таковой, а выявление киберинцидента и своевременная реакция на него.

Но как же обнаружить АРТ-атаку, если предотвратить проникновение невозможно? Ключевую роль в решении этой задачи может сыграть ретроспективный анализ событий безопасности в комплексе с глубоким анализом сетевого трафика. Ретроспективный подход позволяет использовать актуальный на сегодняшний день набор сигнатур, который еще не существовал в момент осуществления атаки, а это существенно повышает результативность обнаружения киберинцидентов, случившихся ранее. Наличие копии сетевого трафика и журналов систем защиты за длительный период времени позволяет провести

детальное расследование и отследить цепочку действий злоумышленника в сети, обнаружить вектор проникновения, определить весь перечень скомпрометированных узлов. Только убедившись, что вы обезвредили все «закладки» преступников, вы сможете действительно нейтрализовать угрозу. Если этого не сделать, то АРТ-группировка через некоторое время вернется обратно.

Такой подход позволит обнаружить злоумышленника в инфраструктуре даже по прошествии нескольких месяцев после проникновения. И конечно, подход этот потребует высокой квалификации специалистов в области ИБ.

Актуальность АРТ-атак будет только расти в связи с внедрением во все сферы деятельности госслужащих новых информационных технологий. Важно признать, что защититься от профессиональных киберпреступников с помощью стандартного набора средств уже невозможно. Преступники постоянно модернизируют методы атак, готовят эксплойты для новых уязвимостей в считанные часы, ищут неизвестные ранее пути достижения преступных целей. Поэтому готовность организаций перестраивать системы защиты, принимать и внедрять новые подходы и решения может сыграть ключевую роль в выявлении победителя в вечном противостоянии.



- Глубокий анализ сетевого трафика
- Поведенческий анализ
- Мониторинг событий ИБ
- Ретроспективный анализ



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

(группировки, атакующие госучреждения)

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
	Mshst	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		Mshst							
		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 Doppelgänger							
		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							



# Тепловая карта тактик и техник АРТ-атак

(все группировки, атакующие компании в России)

---

## О компании

[ptsecurity.com](http://ptsecurity.com)  
[pt@ptsecurity.com](mailto:pt@ptsecurity.com)  
[facebook.com/PositiveTechnologies](https://facebook.com/PositiveTechnologies)  
[facebook.com/PHDays](https://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.