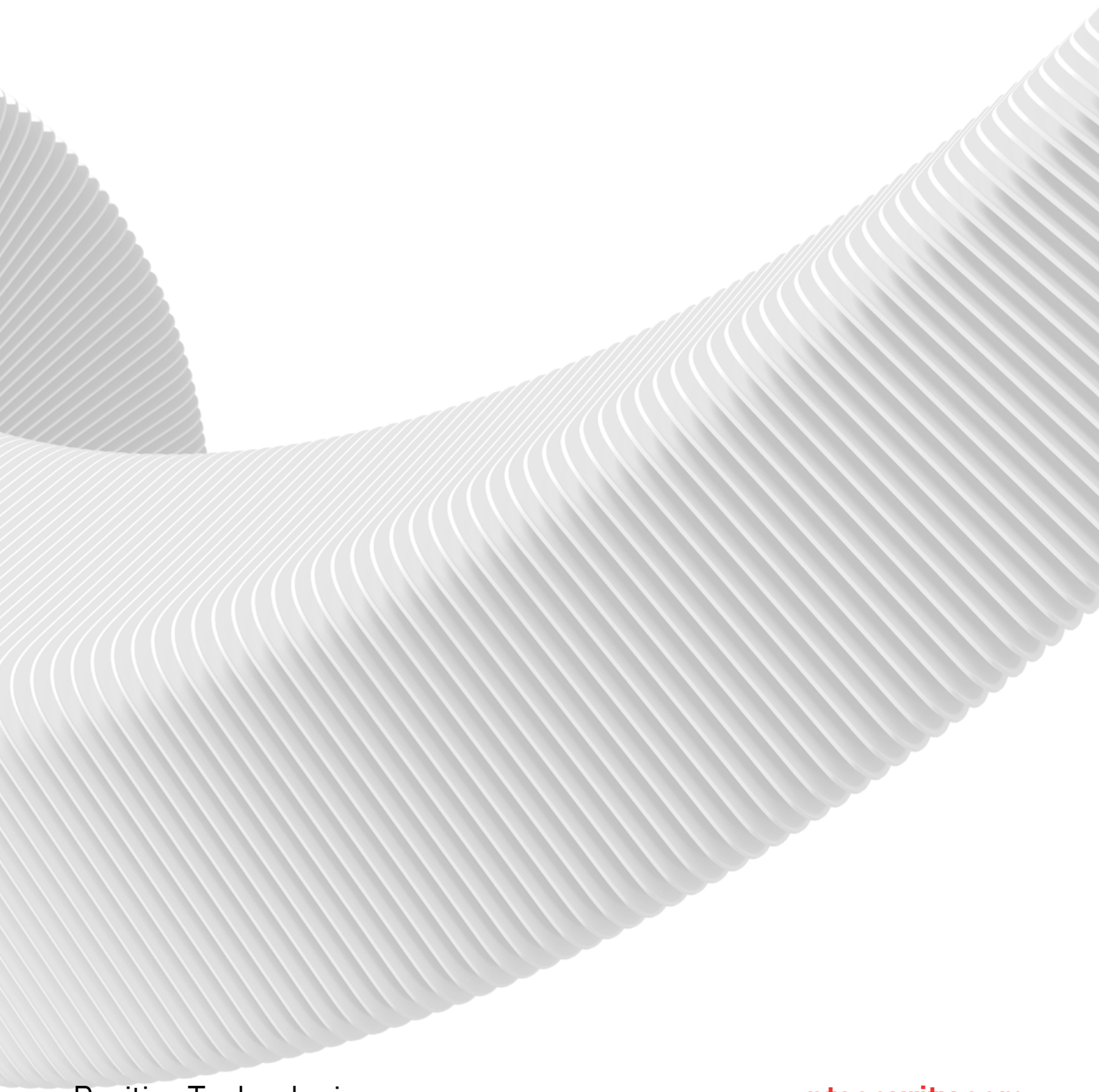
Как действуют APT-группировки на Ближнем Востоке



Positive Technologies

ptsecurity.com

Содержание

Ближний Восток на мушке у APT-группировок

Значительная доля экономики Ближневосточного региона обеспечивается добычей полезных ископаемых. Большая часть роста мировой добычи нефти приходится именно на Ближний Восток, в том числе на Саудовскую Аравию и Объединенные Арабские Эмираты (ОАЭ). Здесь сосредоточено большое количество промышленных компаний и предприятий топливно-энергетического комплекса. Эти организации, наряду с правительственными структурами, активно используют информационные технологии. Цифровизация привела к значительному экономическому и социальному росту в ближневосточных странах. Все эти факторы в совокупности делают регион привлекательной мишенью для кибератак.

В поле зрения наших специалистов попали сведения о 141 успешной атаке на страны Ближнего Востока. Более 80% атак имели целенаправленный характер. Один из основных мотивов киберпреступников, атакующих Ближний Восток, — хищение ценной информации. Так, в ходе исследования интересов киберпреступников к странам Персидского залива наши специалисты выяснили, что персональные данные, логины и пароли для онлайн-сервисов и конфиденциальная документация компаний являются одними из самых обсуждаемых товаров на теневых площадках в дарквебе.

Ближневосточный регион регулярно подвергается атакам со стороны APT-группировок — киберпреступных групп, совершающих многоэтапные и тщательно спланированные атаки, направленные на конкретную отрасль экономики или группу отраслей. Их цель на Ближнем Востоке — информация, которая может дать политические, экономические и военные преимущества. Кроме того, некоторые APT-группировки замечены в хактивистских кампаниях и операциях, направленных на саботаж.

Лидеры списка наиболее атакуемых стран — Саудовская Аравия и ОАЭ. На их территории расположены офисы компаний со всего мира, они считаются важными игроками на Ближнем Востоке и поэтому являются желанными целями множества группировок, атакующих регион.

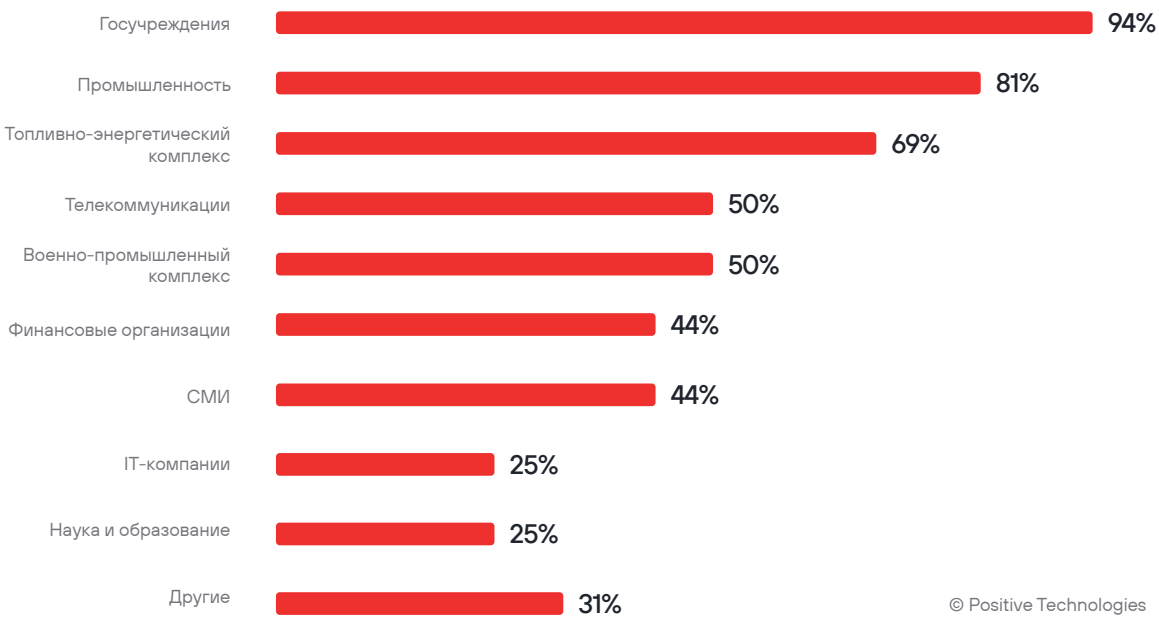
Рисунок 1. Топ-7 целей в Ближневосточном регионе (доля APT-группировок)

88%	75%	63%	56%	50%	50%	44%
Саудовская Аравия	ОАЭ	Израиль	Иордания	Египет	Кувейт	Ливан

Список отраслей, наиболее часто атакуемых APT-группировками, выглядит довольно типично. Почти все рассмотренные группировки, действующие в странах Ближнего Востока, хотя бы раз совершали атаки на госучреждения и промышленность, а 69% группировок атаковали топливно-энергетический комплекс. Стоит отметить, что государственные учреждения являются наиболее привлекательными целями для всех злоумышленников: на их долю в 2022–2023 годах пришлось 22% от общего числа атак на организации стран Ближнего Востока.

Можно выделить военно-промышленный комплекс, который из-за специфики региона находится довольно высоко в рейтинге. Ближневосточные СМИ, по сравнению с другими регионами, также часто становятся целями атак и исторически сохраняют высокое место. Помимо этого, после начала израильской операции в секторе Газа военно-промышленный комплекс и СМИ стали еще чаще подвергаться атакам, в том числе со стороны группировок, представленных в этой статье. В пятерке атакуемых отраслей фигурирует телекоммуникационная отрасль. Это связано с атаками группировок китайского происхождения, поскольку телекоммуникации издавна были одной из их главных целей в связи с повышенным интересом к технологии 5G.

Рисунок 2. Атакуемые отрасли (доля APT-группировок)



Далее мы рассмотрим, какие техники использовали APT-группировки, действующие в странах Ближнего Востока, на разных этапах атак, а также поговорим о том, какие меры необходимо предпринимать организациям, чтобы не стать жертвами APT-атак и не понести серьезный ущерб.

Как киберпреступники готовились к атакам

Комплексные целенаправленные атаки начинаются с разведки. Нападающие могут проводить широкомасштабные сетевые сканирования (Active Scanning) в поисках подходящих целей. В результате у злоумышленников появляется информация, которой достаточно для начального этапа проникновения. К такой информации относится, например, список публичных систем, подверженных известным уязвимостям (T1595.002). Кроме того, злоумышленники могут собирать списки поддоменов и открытых веб-каталогов, чтобы в дальнейшем использовать их для размещения веб-шеллов (T1595.003). Например, группа Volatile Cedar использовала в этих целях утилиты DirBuster и Gobuster.

Группировка APT35, атаковавшая на Ближнем Востоке преимущественно Саудовскую Аравию и Израиль, собирала информацию о сотрудниках целевых организаций (Gather Victim Identity Information), в том числе номера мобильных телефонов. Они могли использоваться для отправки сообщений со ссылками на мобильные вредоносные программы для шпионажа и кражи данных. Группа отслеживала IP-адреса (T1590.005) и местоположение (T1591.001) посетителей своих фишинговых сайтов. Кроме того, злоумышленники идентифицировали ценные адреса электронной почты (T1589.002), чтобы использовать их в своих атаках как отправную точку. Группировка Hexane предварительно устанавливала личности руководителей, сотрудников кадровых отделов и отделов информационных технологий целевых организаций (T1591.004).

За разведкой следует этап подготовки инструментальной базы для проведения атак. Злоумышленники могут регистрировать поддельные домены (T1583.001) и создавать учетные записи электронной почты (T1585.002) или аккаунты в социальных сетях (T1585.001) для проведения целенаправленного фишинга. Так, группировка APT35 регистрировала аккаунты в LinkedIn и других соцсетях, чтобы связываться с жертвами и через сообщения и голосовую связь убеждать их открыть вредоносные ссылки.

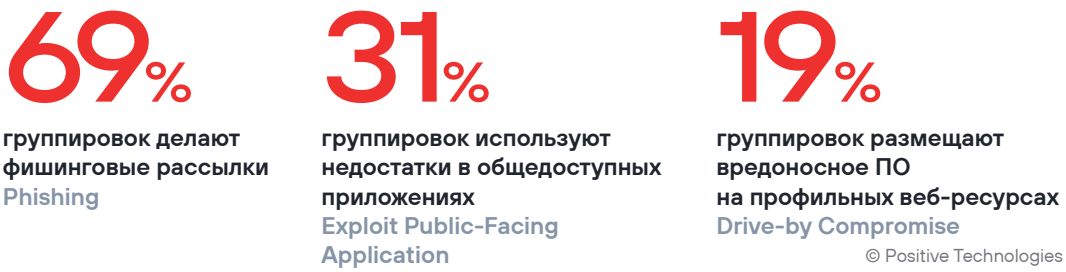
Как получали первоначальный доступ

Чтобы попасть во внутреннюю сеть, киберпреступникам нужна точка проникновения — рабочий компьютер сотрудника или сервер, который они заразят вредоносным ПО и с которого начнут дальнейшее перемещение по сети организации. Большинство APT-группировок начинают атаки на корпоративные системы с целенаправленного фишинга (Phishing). Чаще всего речь идет о рассылках писем с вредоносным содержимым (T1566.001, T1566.002). Помимо электронной почты, некоторые злоумышленники (APT35, Bahamut, Dark Caracal, OilRig) использовали для фишинговых атак социальные сети и мессенджеры (T1566.003).

Группировки APT35, Bahamut и Dark Caracal заражали жертв вредоносным ПО методом watering hole. При таких атаках злоумышленники компрометируют веб-ресурсы, которые посещают будущие жертвы, после чего с этих ресурсов на их компьютеры незаметно загружаются вредоносные программы (Drive-by Compromise).

Некоторые злоумышленники получали доступ к внутренней инфраструктуре из-за уязвимостей в ресурсах, доступных из интернета (Exploit Public-Facing Application). Например, группировки APT35 и Moses Staff для первоначального доступа и получения контроля над жертвами задействовали связку уязвимостей ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) на серверах Microsoft Exchange. Группы APT35 и MuddyWater эксплуатировали критически опасную уязвимость Log4Shell в библиотеке Apache Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-44832).

Рисунок 3. Наиболее распространенные техники получения первоначального доступа



Как удерживали позиции

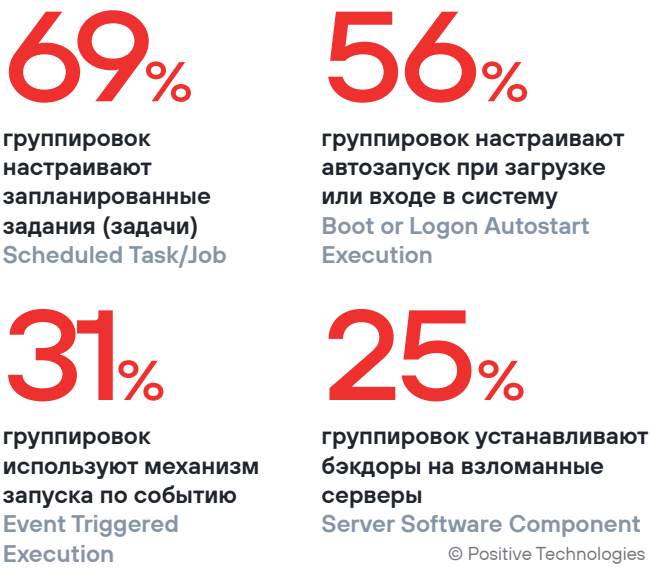
После получения первоначального доступа атакующие стремятся закрепиться в инфраструктуре. Они предпринимают меры, чтобы иметь возможность вернуться в компанию жертвы. Для закрепления в системе 69% APT-группировок используют планировщик заданий (Scheduled Task/Job). В кампании против правительства ОАЭ, описанной специалистами Fortinet в мае 2023 года, группа OilRig создавала запланированную задачу MicrosoftEdgeUpdateService, которая срабатывала каждые пять минут и запускала вредоносное ПО.

Большая часть злоумышленников (56%) настраивали автозагрузку вредоносных программ (Boot or Logon Autostart Execution). Они делали это через ключи запуска реестра (run keys) либо через добавление ссылки на вредоносную программу в каталог Startup («Автозагрузка») (T1547.001). Например, группа Bahamut создавала LNK-файлы в каталоге Startup, а троянское ПО Bandook группы Dark Caracal добавляло ключ в раздел HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run.

Треть APT-группировок (31%) для закрепления в системе настраивали срабатывание вредоносного кода при наступлении определенного события (Event Triggered Execution). Например, группы APT33, Mustang Panda и Stealth Falcon закреплялись в инфраструктуре жертв, создавая подписку на события WMI (T1546.003).

Если корпоративные серверные приложения позволяют администраторам устанавливать ПО, злоумышленники могут воспользоваться этим для установки бэкдоров (Server Software Component). Так, 25% APT-группировок внедряли веб-шеллы на взломанные узлы (T1505.003) для поддержки доступа к сетям жертв. Веб-шеллы могут использоваться не только для закрепления, но и для сбора информации. Например, веб-шелл ExchangeLeech группы OilRig отслеживает трафик и собирает учетные данные пользователей, применяющих небезопасные методы аутентификации. Оператор может запросить список собранных логинов и паролей, отправив соответствующую команду веб-шеллу через специально сформированные куки.

Рисунок 4. Наиболее распространенные техники закрепления



Что изучали внутри

После проникновения в корпоративную сеть злоумышленники стремятся изучить устройства, к которым удалось получить доступ, чтобы понять, как действовать дальше. Прежде всего атакующих интересуют данные об операционной системе и архитектуре скомпрометированного узла, а также сведения о версиях ПО, установленных патчах и пакетах обновлений (System Information Discovery). Например, одна из вредоносных программ группировки APT35 с помощью команды PowerShell определяла, относится ли процессор узла к семейству x64, а другие вредоносные программы этой группировки получали версию операционной системы, UUID и имя узла и передавали их на командный сервер.

Злоумышленники собирают информацию о сетевой конфигурации и параметрах скомпрометированной системы (System Network Configuration Discovery). Атакующие запускают утилиты сетевой диагностики и вредоносное ПО, обладающее соответствующими функциональными возможностями. Группа Mustang Panda применяла утилиты ipconfig и arp, а группа Hexane — ping и tracert. Группировка Dark Caracal использовала троян для удаленного управления Bandook, в котором есть команда для получения публичного IP-адреса узла.

Большинство группировок стараются идентифицировать пользователей скомпрометированного узла и определить их степень активности (System Owner/User Discovery). С этой целью атакующие запускают системные утилиты либо вредоносное ПО с соответствующей функциональностью. Веб-шелл Caterpillar, разработанный группой Volatile Cedar, позволяет получить системные сведения, данные о сетевой конфигурации, список пользователей и многое другое.

Атакующие изучают процессы, запущенные на скомпрометированных узлах (Process Discovery). С этой целью могут использоваться как системные утилиты, так и вредоносное ПО. К примеру, группировки APT15 и OilRig собирали сведения о процессах с помощью утилиты командной строки tasklist. Группа Bitter применяла вредоносное ПО, которое создавало снимок запущенных процессов при помощи функции CreateToolhelp32Snapshot из набора Windows API.

Злоумышленники ищут любую потенциально полезную информацию в файлах и каталогах, которые есть на скомпрометированных узлах (File and Directory Discovery). Перечисление файлов — одна из функциональных возможностей приложений, развернутых группой Bahamut в рамках кампаний Operation BULL и Operation ROCK. APT-группировка MuddyWater в ходе своих атак использовала вредоносное ПО, которое проверяло, есть ли в каталоге ProgramData подкаталоги или файлы с ключевыми словами Kasper, Panda или ESET. В арсенале группы Desert Falcons есть инструмент для рекурсивного просмотра каталогов на всех дисках и поиска определенных файлов по их путям.

Рисунок 5. Наиболее распространенные техники исследования корпоративной инфраструктуры

Где искали учетные данные

Для доступа к интересующей информации злоумышленникам могут потребоваться дополнительные учетные данные. Одна из распространенных техник — это извлечение паролей из памяти системных процессов (OS Credential Dumping). Группировки APT15, APT33, APT35, MuddyWater и OilRig для этой цели применяли общедоступные инструменты — Mimikatz или LaZagne (T1003.001, T1003.004, T1003.005). Группы APT15 и Mustang Panda извлекали учетные записи из файла NTDS.dit — базы данных, в которой хранится информация Active Directory (T1003.003). Mustang Panda использовала системную утилиту vssadmin, предназначенную для администрирования службы теневого копирования томов. С ее помощью киберпреступники создали теневую копию тома на контроллере домена жертвы и извлекли из нее файл NTDS.dit, в котором хранятся хеш-значения паролей всех пользователей домена.

Другая распространенная техника получения учетных записей — перехват данных, которые жертва вводит на скомпрометированном устройстве (Input Capture). Для его реализации злоумышленники используют специальное вредоносное ПО — кейлоггеры. Например, оно есть в арсенале группировок APT15, APT35, Bahamut, Desert Falcons, Molerats и Volatile Cedar.

Некоторые группы извлекали учетные данные из специализированных хранилищ (Credentials From Password Stores), в том числе из браузеров (T1555.003). Группы OilRig и Stealth Falcon похищали их из диспетчера учетных данных Windows (T1555.004).

Существуют и другие способы сбора учетных записей. Например, группировки APT33, Hexane, OilRig и Volatile Cedar получали пароли методом перебора (Brute Force). Он успешно применяется в организациях со слабой парольной политикой, из-за которой у сотрудников есть возможность устанавливать простые пароли. Легкой добычей становятся незащищенные либо слабозащищенные логины и пароли (Unsecured Credentials). К этой категории относятся пароли, сохраненные администраторами в файлах групповой политики — Group Policy Preference (T1552.006). Несмотря на то что пароли здесь хранятся в зашифрованном виде, существуют специализированные инструменты, которые позволяют извлечь и дешифровать их. Например, группа APT33 использовала для этого утилиту Get-GPPPassword.

Рисунок 6. Наиболее распространенные техники получения учетных данных

Как собирали ценную информацию

Большинство (56%) APT-группировок снимали скриншоты с экранов жертв (Screen Capture) и передавали их на свои серверы. Некоторые делали видеозапись с экрана (Video Capture) и аудиозапись с микрофона жертвы (Audio Capture). Для скриншотов, видео- и аудиозаписей злоумышленники использовали вредоносное ПО, в том числе инструменты собственной разработки, например StrifeWater, CANDYKING. Группа Dark Caracal использовала вредоносное программное обеспечение Bandook, в котором есть модули, способные перехватывать видео с веб-камеры и звук с микрофона жертвы.

Злоумышленники искали ценные сведения непосредственно на компьютерах сотрудников: в пользовательских и конфигурационных файлах, локальных базах данных (Data From Local System). Например, группа Dark Caracal собирала полное содержимое каталога Pictures со взломанных узлов под управлением Windows.

Некоторые группировки архивировали собранные данные (Archive Collected Data). Так, группа Mustang Panda пользовалась архиватором для создания защищенных паролем архивов с собранными документами (T1560.001), а также шифровала файлы с помощью RC4 (T1560.003) перед их отправкой на сервер злоумышленников. Группа Molerats использовала инструмент DustySky, который создавал временные каталоги для размещения собранных файлов и позволял архивировать их перед отправкой за пределы корпоративной инфраструктуры. Каждая четвертая группа автоматизировала сбор данных.

Рисунок 7. Наиболее распространенные техники сбора данных

На связи с командным сервером

По мере необходимости APT-группировки загружали дополнительные инструменты для поддержания и расширения плацдарма в инфраструктуре жертвы (Ingress Tool Transfer). Передача осуществлялась через каналы связи с командными серверами либо по альтернативным протоколам. Для связи с командным сервером 88% групп использовали распространенные протоколы прикладного уровня (Application Layer Protocol). Например, взаимодействие вредоносной программы группировки APT35 с командным центром осуществлялось по протоколу IRC, а группа OilRig использовала протокол DNS (T1071.004), в частности общедоступный туннельный сервис requestbin.net. Вредоносное программное обеспечение Small Sieve группы MuddyWater взаимодействовало с командным центром посредством Telegram API по HTTPS (T1071.001). Использование распространенных протоколов прикладного уровня приводит к смешиванию вредоносной активности с легитимным трафиком, что может усложнять ее обнаружение.

Шифрование для маскировки каналов связи (Encrypted Channel) применяли 63% APT-группировок. Большинство злоумышленников шифровали трафик с помощью симметричных алгоритмов AES и RC4 (T1573.001). Группа OilRig для создания туннелей использовала утилиту plink (T1573.002).

Для обмена информацией и файлами с командным сервером каждая третья группа использовала внешние легитимные веб-сервисы (Web Service). Например, вредоносное ПО группировки APT35 работает через веб-сервис SOAP. Группа MuddyWater распространяла инструменты для удаленного доступа через облачное хранилище Onehub. Группа Mustang Panda использовала Dropbox для распространения трояна PlugX.

Интересный способ управления вредоносным ПО применяла группа OilRig в рамках кампании, описанной специалистами Symantec. В качестве командного центра был задействован почтовый сервер жертвы Microsoft Exchange. Злоумышленники отправляли письма на скомпрометированные почтовые ящики. В заголовках писем содержались символы @@. По ним бэкдор PowerExchange распознавал необходимые письма и выполнял содержащиеся в них инструкции, после чего письма автоматически удалялись. Запросы к серверу Exchange из внутренней сети не вызывают аномалий в сетевом трафике, что позволяло злоумышленникам оставаться незамеченными длительное время. Специалисты Symantec отмечают, что кампания группировки OilRig продолжалась с февраля по сентябрь 2023 года.

Рисунок 8. Наиболее распространенные техники управления и контроля

Как скрывали следы присутствия

Для APT-группировок важно оставаться незамеченными в скомпрометированной среде как можно дольше. Они прибегают к различным способам сокрытия следов присутствия. Как правило, злоумышленники предварительно тестируют образцы своих вредоносных программ и впоследствии модифицируют их для обхода антивирусного детектирования. Один из способов — обфусцирование (запутывание) вредоносного кода и использование специальных упаковщиков (Obfuscated Files or Information). Например, группа Dark Caracal обфусцировала строки в Bandook с помощью кодирования Base64 и их последующего шифрования.

Распространенный способ обойти защиту — замаскировать вредоносное ПО под легитимные файлы или приложения (Masquerading). К примеру, группа Bahamut для маскировки вредоносного ПО использовала иконки, имитирующие файлы Microsoft Office. Кроме того, эта группировка пыталась скрыть исполняемые файлы за счет изменения расширения файла на .scr для имитации заставок Windows. Группа OilRig использовала расширение файлов .doc для маскировки вредоносов под офисные документы. Еще один пример — вредоносное программное обеспечение StrifeWater группы Moses Staff. Оно имело название calc.exe, чтобы выглядеть как легитимная программа-калькулятор.

Более половины (56%) APT-группировок удаляют признаки своей активности (Indicator Removal): очищают журналы событий и историю сетевых соединений, изменяют временные метки. Так, группа APT35 удаляла запросы на экспорт почтовых ящиков со взломанных серверов Microsoft Exchange. Большинство злоумышленников после достижения поставленных целей полностью удаляют со скомпрометированных устройств весь свой арсенал ПО. Эти действия впоследствии сильно усложняют расследование инцидентов специалистам по кибербезопасности.

Нередко для обхода средств защиты злоумышленники проксируют выполнение вредоносных команд с помощью файлов, подписанных доверенными цифровыми сертификатами (System Binary Proxy Execution). Например, группировка APT35 использовала файл rundll32.exe для выполнения функции MiniDump из системной библиотеки comsvcs.dll при дампе памяти процесса LSASS. Другой пример — группа Dark Caracal использовала скомпилированный файл Microsoft Compiled HTML Help, содержащий команду на загрузку и запуск вредоносного файла.

Рисунок 9. Наиболее распространенные техники сокрытия следов

Как противостоять APT-атакам

APT-группировки, атакующие госучреждения и крупные предприятия на Ближнем Востоке, как правило, нацелены на длительный контроль над инфраструктурой. Их целью может быть не только шпионаж, но и саботаж или ведение кибервойны. Злоумышленники способны незаметно присутствовать в корпоративной сети длительное время и перейти к активным действиям только в момент обострения геополитической обстановки.

В этом случае для борьбы со сложным целенаправленными атаками требуется особый подход, основанный на идее результативной кибербезопасности. При успешной реализации этого подхода инфраструктура и процессы выстроены таким образом, что даже в случае проникновения в сеть организации злоумышленники не смогут нанести ей неприемлемый ущерб. Другими словами, главной целью становится исключение возможности реализации недопустимых событий — событий, блокирующих достижение операционных и (или) стратегических целей или приводящих к значительному нарушению основной деятельности организации в результате кибератаки. Эти события определяются на уровне топ-менеджмента организации и задают курс для формирования стратегии кибербезопасности.

Для построения эффективной системы защиты от сложных целенаправленных атак мы рекомендуем организациям обратить внимание на основы результативной кибербезопасности.

- **Управление активами**

Одна из основных составляющих — регулярная инвентаризация активов и их приоритизация с учетом недопустимых событий и способов развития кибератак. Здесь на помощь могут прийти решения класса VM (vulnerability management). Они автоматизируют процессы управления активами, выявления и исправления уязвимостей в элементах инфраструктуры в зависимости от степени опасности уязвимости. В случае если компания занимается разработкой программных продуктов и веб-приложений, рекомендуем обратить внимание на средства анализа исходного кода для выявления уязвимостей и недостатков проектирования на этапе разработки.

- **Мониторинг и реагирование на инциденты**

Мониторинг подразумевает непрерывный процесс наблюдения и анализа результатов регистрации событий из разных источников для выявления нарушений, угроз и уязвимостей. С задачей поможет справиться система класса SIEM (security information and event management). Она позволяет отслеживать и анализировать события безопасности, выявлять атаки и оценивать соответствие требованиям безопасности защищаемых элементов инфраструктуры. Промышленным и топливно-энергетическим предприятиям рекомендуем обратить внимание на специализированные решения для анализа трафика АСУ ТП. Они помогают выявлять вредоносную активность без негативного влияния на производственные процессы. Для предотвращения недопустимых событий важно вовремя на них реагировать. Эффективным решением в этом вопросе может стать совместное использование SIEM-системы и решения класса XDR (extended detection and response).

На примере APT-группировок, действующих в странах Ближнего Востока, видно, что киберпреступники владеют целым арсеналом техник для сокрытия своего присутствия в скомпрометированной инфраструктуре и маскировки генерируемого вредоносного трафика под легитимный, поэтому для своевременного выявления угроз и реагирования на них не обойтись без глубокого анализа сетевого трафика. Справиться с этой задачей помогут решения класса NTA (network traffic analysis). Этот инструмент обнаруживает вредоносную активность злоумышленников на периметре и внутри сети, в том числе в зашифрованном трафике. В арсенале всех рассмотренных нами APT-группировок есть вредоносные программы собственной разработки. Выявить сложное вредоносное ПО помогают также песочницы.

Обучение кибербезопасности

Программа обучения сотрудников должна быть нацелена на повышение осведомленности о современных киберугрозах, в том числе APT-атаках. В обучающие программы стоит включать темы про надежные пароли, безопасную работу с электронной почтой, важность своевременного обновления ПО, правила обработки и хранения конфиденциальной информации, использование общественных беспроводных сетей и другие аспекты кибербезопасности. Важно, чтобы сотрудники понимали основы безопасности и могли легко соблюдать их в ежедневной работе. Для этого полезно проводить периодическое тестирование сотрудников, например симуляцию фишинговых атак.

Оценка защищенности

Важный шаг на пути к защите от APT-атак — регулярные мероприятия по оценке защищенности (например, киберучения, тестирование на проникновение). Для подтверждения практического уровня защищенности мы рекомендуем виды работ, соответствующие идее результативной безопасности. Советуем также обратить внимание на программы bug bounty. Они помогают организациям выстроить процесс непрерывного анализа защищенности сервисов и оптимизировать затраты на безопасность.

В связи с активной цифровой трансформацией предприятий и переходом на электронное правительство в странах Ближнего Востока актуальность APT-атак будет только расти. Защититься от профессиональных киберпреступников с помощью стандартных средств стало невозможно. Злоумышленники разрабатывают эксплойты для новых уязвимостей, модернизируют вредоносное ПО, ищут неизвестные ранее пути достижения целей. Готовность организаций перестраивать системы защиты, принимать и внедрять новые подходы и решения — залог успеха в борьбе с APT-атаками.

Об исследовании

В этом исследовании мы проанализировали тактики и техники 16 APT-группировок, которые действуют в странах Ближнего Востока на протяжении последних нескольких лет. С кратким описанием группировок можно ознакомиться в конце отчета. В процессе исследования мы пришли к выводу, что некоторые группировки, которые ряд вендоров относят к хактивистам, не являются таковыми. Так, в одном из ранее опубликованных исследований мы относили группировку Moses Staff к хактивистам — киберпреступникам, пытающимся привлечь внимание к какой-либо политической проблеме. Однако после более глубокого изучения мы пришли к выводу, что атаки Moses Staff сложнее хактивистских, а сама группа представляет бóльшую угрозу, поэтому может быть отнесена к APT-группировкам.

Под Ближним Востоком в отчете понимаются следующие страны: Бахрейн, Египет, Израиль, Иордания, Ирак, Иран, Йемен, Катар, Кипр, Кувейт, Ливан, Объединенные Арабские Эмираты (ОАЭ), Оман, Палестина, Саудовская Аравия, Сирия.

Тактики и техники группировок описаны в терминах MITRE ATT&CK Matrix for Enterprise (версия 13.1). В тексте даны ссылки на подробное описание упоминаемых техник. В отчете вы также можете найти примеры использования некоторых подтехник, ссылки на них указаны в скобках в виде идентификатора (например, T1595.001).

Исследование основано на собственной экспертизе компании Positive Technologies, а также на данных авторитетных источников. Оно проводится с целью обратить внимание компаний, интересующихся современным состоянием информационной безопасности, на наиболее актуальные тактики и техники APT-атак на Ближнем Востоке. Термины, которые мы использовали в исследовании, приведены в глоссарии на сайте Positive Technologies.

Краткое описание APT-группировок

APT15

Группировка, которой ряд исследователей приписывают китайские корни. Активна по крайней мере с 2010 года. Атакует правительственные организации, посольства и секторы экономики во множестве стран. Группа использует вредоносное ПО собственной разработки и общедоступные инструменты. Исследователи нашли пересечения между APT15 и злоумышленником, который разрабатывал шпионские мобильные приложения, задействованные в атаках на уйгуров.

APT33

Группа атакует правительственные и частные организации, связанные с авиацией и энергетикой. Активность фиксируется с 2013 года. Злоумышленники используют как общедоступные, так и собственные инструменты с артефактами персидского языка, что позволило исследователям предположить связь с Ираном.

APT35

Исследователи связывают эту группу с иранским Корпусом стражей исламской революции. APT35 атакует отрасль экономики и частных лиц, специализируется на похищении конфиденциальной информации, используя для этого собственные вредоносные программы, а также эксплуатирует недавно обнаруженные уязвимости (N-day). У группировки есть несколько подгрупп, одна из которых — Nemesis Kitten (также известная как DEV-0270 и Storm-0270).

Bahamut

Группа киберпреступников по найму (hack for hire), активность которых отмечается с 2016 года. Группа атакует как высокопоставленных государственных чиновников и промышленных магнатов в Индии, ОАЭ и Саудовской Аравии, так и тех, кто выступает за сикхский сепаратизм или поддерживает правозащитные движения на Ближнем Востоке. Группа имеет в арсенале ПО собственной разработки, а также участвует в создании вредоносных приложений для мобильных устройств под управлением Android и iOS и распространении их через магазины Google Play и App Store.

Bitter

По мнению некоторых исследователей, группировка имеет индийское происхождение. Активна с 2013 года. Как утверждают исследователи из Anomali, Bitter атакует военные и промышленные цели в Китае и Пакистане, также замечена активность и в других странах. Использует различные инструменты, включая вредоносное ПО для Android. Изначально оно базировалось на AndroRAT, но позже группа разработала собственные инструменты. Группировка эксплуатирует многие уязвимости, например CVE-2021-28310.

Dark Caracal

Группа активна по крайней мере с 2012 года. По мнению исследователей из Lookout, группа имеет ливанские корни и проводит масштабные кампании по шпионажу во всем мире. С 2021 года замечена в Южной и Центральной Америке. Атакует привычные для APT-группировки цели, например промышленные и оборонные предприятия и людей, связанных с активистской, юридической или журналистской деятельностью. Использует инструменты, позволяющие записывать видео и захватывать ввод клавиатуры для дальнейшей передачи информации на серверы группы.

Desert Falcons

Группа активна по крайней мере с 2011 года. По мнению исследователей из Sekoia.io и других, связана с движением ХАМАС. Основные цели сосредоточены в Израиле, но также зафиксированы атаки и в других странах. Группа владеет арсеналом вредоносного ПО для компьютеров и мобильных устройств, которое регулярно дорабатывается. В числе жертв есть частные лица, поскольку группа проводит атаки, направленные на пользователей мобильных устройств на базе iOS и Android.

Hexane

Группа атакует страны Ближнего Востока и Африки с 2017 года. Как пишут некоторые исследователи, например из Sekoia.io, группа имеет иранские корни. Цели группы обусловлены политическими мотивами. Тактики и техники схожи с другими группами APT33 и OilRig, но инструменты, а также уникальность жертв не позволяют утверждать, что Hexane является одной из этих групп. Злоумышленники используют собственные бэкдоры, написанные на языках программирования C# и C++, скрипты PowerShell, а также программы с открытым исходным кодом, например Empire.

Molerats

Есть предположения, что группа имеет арабское происхождение и руководствуется политическими мотивами. Активность преступников наблюдается с 2012 года. По мнению исследователей из ClearSky, группа может быть связана с движением ХАМАС. Целями группы в основном являются предприятия Ближневосточного региона, но также были зафиксированы атаки на организации из Европы и США. Группировка обладает как инструментами собственной разработки, так и различным вредоносным ПО для удаленного управления, которое также используется другими группировками, действующими на Ближнем Востоке.

Moses Staff

По мнению исследователей из Cybereason, группировка может быть связана с Ираном. Основная цель — шпионаж.

MuddyWater

Группа активна с 2017 года. По мнению исследователей, например из Sekoia.io, группировка может иметь иранские корни. Основной целью являются страны Ближнего Востока, но группа также атакует страны в Азии, Африке, Европе и Северной Америке. Часто использует инструменты с открытым исходным кодом и эксплуатирует известные уязвимости, чтобы получить доступ к компьютеру жертвы и похитить данные. Группа также имеет обширный арсенал собственных инструментов, которые постоянно дорабатываются.

Mustang Panda

Исследователи из CrowdStrike полагают, что эта группа имеет китайские корни, ее активность фиксируется по крайней мере с 2014 года. Изначально атаковала соседние с Китаем страны. С 2022 года активно атакует и страны Европы, преимущественно посольства и дипломатические миссии. В фишинговых рассылках группа использует трекинговые пиксели. Имеет в арсенале различные инструменты, в том числе Cobalt Strike и модифицированные версии PlugX, а также вредоносное ПО собственной разработки.

OilRig

По мнению исследователей, например из Sekoia.io, группа имеет поддержку в Иране. Целями OilRig становятся преимущественно организации на Ближнем Востоке. Ее деятельность впервые зафиксирована в 2012 году во время волны атак на Ближневосточный регион. Известна широким набором инструментов и использованием атак типа supply chain для сбора стратегической информации.

Stealth Falcon

По мнению ряда исследователей из Citizenlab и источников из Reuters, группа якобы имеет связь с ОАЭ. Активна по крайней мере с 2012 года и атакует разного рода активистов и журналистов. Использует вредоносное ПО собственной разработки, эксплуатирует уязвимости нулевого дня.

Volatile Cedar

Группа активна с 2012 года. Исследователи из ClearSkySec обнаружили, что серверы группировки находились в Ливане. Атаки часто имеют политический мотив и направлены на компании и отдельных людей по всему миру. Группа использует общедоступные инструменты и ПО собственной разработки, способные обходить большинство средств антивирусной защиты.

Wirte

Группа активна по крайней мере с 2018 года. Жертвами группировки становятся организации в Сирии, Ливане, Иордании и в других странах Ближнего Востока. Как утверждают в Proofpoint, группа, вероятно, имеет политические мотивы и может быть связана с группировкой Molerats. Злоумышленники рассылают фишинговые письма с документами на арабском языке, которые содержат макросы VBA, загружающие дополнительную полезную нагрузку. Помимо этого, группа замечена в использовании фреймворка для постэксплуатации Empire.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Acquire Infrastructure	Exploit Public-Facing Application	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Accounts	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Compromise Infrastructure	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Develop Capabilities	Phishing	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Establish Accounts	Replication Through Removable Media	Inter-Process Communication	Compromise Client Software Binary	Domain Policy Modification	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Obtain Capabilities	Supply Chain Compromise	Native API	Create Account	Escape to Host	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data Staged	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases	Stage Capabilities	Trusted Relationship	Scheduled Task/Job	Create or Modify System Process	Event Triggered Execution	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Cloud Storage	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	Serverless Execution	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material	Data from Configuration Repository	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Shared Modules	External Remote Services	Hijack Execution Flow	Execution Guardrails	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Information Repositories	Non-Application Layer Protocol		Network Denial of Service
			Software Deployment Tools	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Local System	Non-Standard Port		Resource Hijacking
			System Services	Implant Internal Image	Scheduled Task/Job	File and Directory Permissions Modification	OS Credential Dumping	File and Directory Discovery		Data from Network Shared Drive	Protocol Tunneling		Service Stop
			User Execution	Modify Authentication Process	Valid Accounts	Hide Artifacts	Steal Application Access Token	Group Policy Discovery		Data from Removable Media	Proxy		System Shutdown/ Reboot
			Windows Management Instrumentation	Office Application Startup		Hijack Execution Flow	Steal Web Session Cookie	Network Service Discovery		Email Collection	Remote Access Software		
				Pre-OS Boot		Impair Defenses	Steal or Forge Authentication Certificates	Network Share Discovery		Input Capture	Traffic Signaling		
				Scheduled Task/Job		Indicator Removal	Steal or Forge Kerberos Tickets	Network Sniffing		Screen Capture	Web Service		
				Server Software Component		Indirect Command Execution	Unsecured Credentials	Password Policy Discovery		Video Capture			
				Traffic Signaling		Masquerading		Peripheral Device Discovery					
				Valid Accounts		Modify Authentication Process		Permission Groups Discovery					

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
						Modify Cloud Compute Infrastructure		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image		Remote System Discovery					
						Network Boundary Bridging		Software Discovery					
						Obfuscated Files or Information		System Information Discovery					
						Plist File Modification		System Location Discovery					
						Pre-OS Boot		System Network Configuration Discovery					
						Process Injection		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Subvert Trust Controls		Virtualization/Sandbox Evasion					
						System Binary Proxy Execution							
						System Script Proxy Execution							
						Template Injection							
						Traffic Signaling							
						Trusted Developer Utilities Proxy Execution							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material							
						Valid Accounts							
						Virtualization/ Sandbox Evasion							
						Weaken Encryption							
						XSL Script Processing							

Тепловая карта тактик и техник APT-группировок на Ближнем Востоке

1–4 группировки 5–8 группировок 9–12 группировок 13–16 группировок

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — лидер в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 4000 организаций по всему миру.

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.