Как обнаружить 10 популярных техник пентестеров

Positive Technologies

ptsecurity.com

Содержание

Введение

Ранее мы выпустили исследование, в котором рассказали о результатах внешних и внутренних пентестов в 2022 году. Один из артефактов исследования — топ 10 распространенных техник и подтехник MITRE ATT&CK®, которые успешно применялись пентестерами. Тестирование на проникновение — это имитация атаки, поэтому на примере этого списка мы научимся противодействовать реальным злоумышленникам. В этом исследовании мы поделимся советами о том, как обнаруживать техники и подтехники из этого списка, а также предложим превентивные меры, которые значительно усложнят атаку для злоумышленников или вовсе сведут к минимуму вероятность ее проведения в вашей организации. Для удобства все техники и подтехники сгруппированы по тактикам.

В каждой главе вы найдете рекомендации по обнаружению атаки с использованием техники и подтехники из нашего списка топ 10, а также советы о том, как укрепить систему защиты, чтобы такие инциденты не происходили. Помимо этого, в разделе «Матрица D3FEND»[1] можно ознакомиться с перечнем функций средств защиты информации (далее – СЗИ) для обнаружения, предотвращения инцидентов и реагирования на них с использованием техник из топ 10.

Также в исследовании будет рассмотрен вопрос, связанный с реализацией подходов результативной безопасности и выполнением требований регуляторов. Мы сопоставили превентивные меры защиты[2], предлагаемые сообществом экспертов по ИБ, с требованиями Приказа ФСТЭК России от 11.02.2013 № 17. В результате оказалось, что меры, предложенные сообществом, коррелируют с требованиями регулятора.

[1] Данная модель позволяет подобрать СЗИ для обнаружения, реагирования, в том числе блокировки скомпрометированных ресурсов, укрепления системы защиты организации и выставления приманок для злоумышленников. Проект D3FEND набирает популярность и активно развивается.

[2] В рамках сопоставления были проанализированы меры защиты от десяти наиболее популярных техник и подтехник матрицы ATT&CK, которые успешно применялись пентестерами.

Краткие выводы

В рамках исследования были рассмотрены десять техник MITRE ATT&CK®, которые были успешно применены пентестерами в реальных проектах; все они перечислены в таблице 1.

Таблица 1. Перечень рассмотренных тактик и техник

ID	Тактика	Техника
T1190	Initial Access	Exploit Public-Facing Application
T1059	Execution	Command and Scripting Interpreter
T1098	Persistence	Account Manipulation
T1110	Credential Access	Brute Force
T1003		OS Credential Dumping
T1552		Unsecured Credentials
T1087	Discovery	Account Discovery
T1083		File and Directory Discovery
T1550	Lateral Movement	Use Alternate Authentication Material
T1071	Command and Control	Application Layer Protocol

В качестве основных источников событий, анализ которых поможет обнаружить факт применения той или иной техники, выступают:

- журнал событий ОС, в том числе событий, связанных с аудитом безопасности и входом в систему,
- сетевой трафик,
- журнал событий приложений,
- журнал событий на контроллере домена.

Чтобы облегчить предотвращение и обнаружение атак с использованием техник из топ 10, можно использовать следующие СЗИ:

- системы управления событиями информационной безопасности (SIEM),
- системы анализа сетевого трафика (NTA),
- межсетевые экраны уровня приложений (WAF),
- межсетевые экраны нового поколения (NGFW),
- системы обнаружения вторжений (IDS),
- системы предотвращения вторжений (IPS),
- решения для обнаружения и реагирования на события, связанные с вредоносной активностью на конечных узлах (EDR), и их современную расширенную версию (XDR).

Также можно использовать встроенные в Windows механизмы обеспечения безопасности, например ПО для защиты от атак, направленных на кражу учетных данных (Credential Guard).

Основной набор функций средств защиты информации, которые помогут специалистам по ИБ обнаружить атаки или могут быть применены в качестве превентивной меры, представлен в главе «Матрица D3FEND». Отметим, что полученный список возможностей СЗИ лишь частично покрывает потребности специалистов по ИБ. Это связано с тем, что этот инструмент новый, однако он активно развивается. Многие современные СЗИ обладают гораздо большим количеством полезных возможностей, которые могут быстрее выявить инцидент ИБ или среагировать на него.

Мы сопоставили превентивные меры по недопущению рассматриваемых техник атак с требованиями Приказа ФСТЭК России № 17. Предложенные меры для основных десяти техник покрывают 33 из 113 требований Приказа. Более подробно вы можете ознакомиться с сопоставлением в главе «Сопоставление мер защиты информации».

Initial Access

Среди техник, используемых для получения первоначального доступа в инфраструктуру, чаще всего в успешных векторах атак пентестеров мы встречали применение техники Exploit Public-Facing Application (T1190). Эта техника была применена в 100% проектов по внешнему тестированию на проникновение.

Обнаружить атаку с использованием этой техники можно:

- в журнале событий приложения.

Применение эксплойтов может вызвать ошибки или спровоцировать неуспешные попытки аутентификации, которые будут отображены в журнале событий приложения, например в access.log, или в логах транзакций в базах данных;

- журнале событий ОС.

Обнаружить факт успешной эксплуатации уязвимости можно, например, по запуску команд, связанных с разведкой;

- сетевом трафике.

Для того чтобы выявить следы известных эксплойтов в сетевом трафике, можно воспользоваться сетевыми сенсорами систем NTA, IDS, WAF или NGFW. Если злоумышленники используют неизвестные (новые) эксплойты, обнаружить атаку можно только в том случае, если в новом эксплойте есть фрагменты старых нагрузок.

Предотвратить атаку с использованием этой техники возможно, если:

1. выстроить процесс управления уязвимостями и обновлениями безопасности;
2. использовать системы анализа трафика (при условии наличия в продукте сетевых сенсоров, которые могут обнаружить эксплойт в трафике), современные межсетевые экраны нового поколения (NGFW), которые могут выявить эксплойт, межсетевой экран для веб-приложений (WAF), а также системы предотвращения вторжений (IPS);
3. сегментировать сеть организации, выделив демилитаризованную зону (ДМЗ);
4. изолировать приложения, расположенные в ДМЗ, используя технологии контейнеризации.

Execution

Среди всех техник, которые использовались для выполнения команд на скомпрометированных узлах, наиболее успешной оказалась техника, связанная с применением интерпретаторов командной строки (Command and Scripting Interpreter). Эта техника приводила к успеху в 93% пентестов.

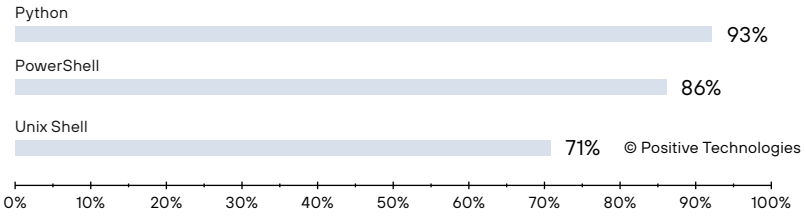

Рисунок 1. Топ 3 подтехники Command and Scripting Interpreter

Обнаружить использование техники Command and Scripting Interpreter можно среди событий, связанных:

- с запуском процессов (Sysmon: 1 и Windows Security Log: 4688 (с включенным логированием строк запуска); для Linux: auditd: Syscall: execve).

Анализируйте аргументы, которые передаются в строках запуска скриптов. Обращайте внимание на названия запускаемых скриптов: некоторые атакующие не изменяют названия публично доступных скриптов;

- выполнением скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Отслеживайте любые попытки включения функций запуска скриптов. Если такое изменение настроек системы происходит без участия администраторов, то необходимо убедиться в легитимности данной активности. Анализируйте содержимое выполняемых скриптов, потому что атакующие часто используют популярные скрипты в изначальном виде, без обфускации;

- загрузкой библиотек (Sysmon: 7).

Отслеживайте загрузки библиотек и другие события, связанные со скриптовыми языками (например, JScript.dll или vbscript.dll).

Предотвращение атаки с использованием этой техники возможно, если:

1. использовать решения EDR для обнаружения и изучения вредоносной активности на конечных точках (XDR);
2. использовать песочницы;
3. отключить возможность запуска неподписанных сценариев;
4. удалить ненужные и неиспользуемые оболочки и интерпретаторы;
5. запускать PowerShell могут только привилегированные пользователи.

Persistence

Для закрепления в инфраструктуре в 82% исследованных компаний пентестеры успешно использовали технику Account Manipulation (T1098).

Обнаружить факт использования злоумышленниками техники Account Manipulation можно:

- среди событий на контроллере домена.

Отслеживайте изменения объектов AD с типом user в журналах безопасности на контроллерах домена. Для этого можно использовать события 5136, у которых в поле Class стоит значение user. Для того чтобы отслеживать изменение конкретных атрибутов учетных записей, дополнительно нужно указывать интересующие названия атрибутов в поле LDAP Display Name;

- событий в журнале безопасности Windows.

Отслеживайте события, связанные с изменениями учетных записей пользователей (4738), изменениями учетных записей компьютеров (4742), добавлением пользователей группы безопасности (4732, 4728, 4756), а также соответствующие события изменения этих групп безопасности (4735, 4737, 4755). Такие изменения могут происходить, например, в нерабочее время или могут быть выполнены лицами, у которых нет причин для выполнения таких действий;

- событий, связанных с выполнением скриптов.

Настройте сбор событий запуска скриптов PowerShell. Благодаря этим событиям можно выявить использование различных командлетов для изменения учетных записей и их привилегий;

- событий запуска процессов.

Отслеживайте появление новых процессов, которые свидетельствуют об изменении параметров учетных записей. Обращайте внимание не только на сами процессы, но и на аргументы, с которыми они запускаются (включая пути к файлам, такие как ~/.ssh/authorized_keys или /etc/ssh/sshd_config).

Советы по предотвращению атаки с использованием техники Account Manipulation:

1. внедрите многофакторную аутентификацию;
2. сегментируйте сеть и настройте политику разграничения доступа. Правильная сегментация сети и разграничение доступа вынудит злоумышленника совершить гораздо больше операций для достижения цели, что повысит шансы специалиста по ИБ вовремя выявить его в сети и принять меры для предотвращения реализации недопустимого события;
3. ограничьте привилегированные учетные записи: они не должны использоваться для решения повседневных задач. Следуйте рекомендациям по организации работы с привилегированными учетными записями;
4. отслеживайте привилегии обычных пользователей, например, они не должны обладать разрешениями на изменение учетных записей или политик, связанных с учетными записями;
5. проверьте настройки безопасности контроллеров домена. Ограничьте доступ к потенциально ненужным протоколам и службам;
6. используйте EDR (XDR).

Credential Access

Credential Access: OS Credential Dumping

Среди всех методов, направленных на кражу учетных данных, самой успешной техникой была OS Credential Dumping. Она встречалась в 93% исследованных организаций. Существует несколько методов для получения дампа учетных записей; мы остановимся на самых часто используемых: DCSync (93%) и LSASS Memory (68%).

Обнаружить атаку с использованием метода OS Credential Dumping: DCSync (T1003.006) можно, проанализировав:

- события на контроллере домена (DC Security Log: 4662).

Осуществляйте мониторинг журнала событий на контроллере домена на предмет запросов, связанных с репликацией, и других действий, которые могут осуществляться в рамках атаки DCSync;

- сетевой трафик.

Осуществляйте мониторинг сетевой активности контроллеров домена. Если будут выявлены запросы на репликацию со стороны узла, который не является контроллером домена, немедленно выясните, что это за узел и почему он запрашивает репликацию.

Анализируйте протокол DCE/RPC и ищите запросы с opnum = 3 (DRSGetNCChanges), свидетельствующие о начале репликации контроллера домена.

Превентивные меры защиты от атак с использованием OS Credential Dumping: DCSync:

1. контролируйте список учетных записей с привилегией «Репликация изменений каталога» и другими привилегиями, связанными с репликацией контроллера домена. Ознакомиться со списком учетных записей, обладающих этой привилегией, можно в списке управления доступом (ACL);
2. убедитесь, что у всех аккаунтов локальных администраторов сложные и уникальные пароли на всех узлах в сети;
3. не включайте пользователя в группу администраторов на всех устройствах в сети, если только за данной учетной записью не ведется тщательный контроль;
4. внедрите решение для обнаружения и изучения вредоносной активности на конечных точках (EDR и XDR);
5. если в инфраструктуре используется LAPS (local administrator password solution), то проследите, чтобы права на LAPS были только у административных учетных записей, которым они необходимы;
6. следуйте лучшим практикам администрирования корпоративной инфраструктуры и ограничьте использование привилегированных учетных записей пределами административных зон безопасности.

> В этом случае будет также актуальна рекомендация, связанная с организацией работ с привилегированными учетными записями.

Credential Access: OS Credential Dumping: LSASS Memory

Для обнаружения атаки с использованием подтехники OS Credential Dumping: LSASS Memory (T1003.001) необходимо просмотреть:

- события выполнения скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Анализируйте события запуска скриптов PowerShell. Среди командлетов скрипта могут встретиться известные функции из хакерского инструментария, например Invoke-Mimikatz из набора PowerSploit;

- события запуска и доступа к процессу (Sysmon: 10 и Sysmon: 1, Windows Security Log: 4688 с включенным логированием строк запуска).

Осуществляйте мониторинг процессов, которые запрашивают доступ к процессу LSASS.exe на чтение. Появление новых несистемных процессов может свидетельствовать о попытке снятия образа памяти.

Собирайте и анализируйте аргументы, передаваемые в строках запуска. Атакующие часто изменяют название утилит для дампа, однако ключи параметров остаются теми же — по таким паттернам можно выявлять попытки дампа.

Для предотвращения атак с использованием подтехники OS Credential Dumping: LSASS Memory необходимо:

1. включить правила Attack Surface Reduction (ASR);
2. активировать встроенное в Windows средство защиты Credential Guard и включить привилегированных пользователей домена в группу Protected Users;
3. по возможности отключить или ограничить NTLM и протокол для дайджест-аутентификации WDigest;
4. использовать EDR (XDR);
5. для серверов Windows Server 2012 R2 и в Windows 8.1 — включить Protected Process Light;
6. убедиться, что доменная политика Store password using reversible encryption for all users in the domain отключена (выставлен запрет на использование обратимого шифрования).

Credential Access: Brute Force

Мы проанализировали результаты пентестов и выяснили, что техника Brute Force успешно применялась пентестерами во всех организациях. Среди всех подтехник наибольшую успешность при подборе учетных данных показали Password Spraying (82%) и Password Guessing (75%).

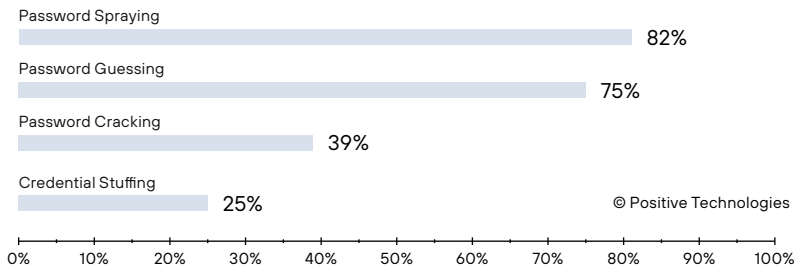

Рисунок 2. Подтехники Brute Force (доли организаций)

Познакомиться со всеми проблемами, выявленными в парольных политиках крупных отечественных компаний различных отраслей, можно в аналитическом отчете «Итоги пентестов – 2022» в разделе «Проблемы в парольной политике». Там же вы сможете познакомиться с рекомендациями по организации парольной политики в компании.

Обнаружение подтехник Brute Force: Password Guessing (T1110.001) и Spraying (T1110.003):

- журнал событий приложения.

Отслеживайте большое количество событий неуспешной аутентификации, особенно в сервисах, доступных на периметре.

Большое количество ошибок подряд с одной учетной записью свидетельствует о подборе методом угадывания (Password Guessing). Если же пользователи разные, но видна логика выстраивания последовательности имен пользователей или промежутки времени короткие и постоянные, то это, вероятно, признаки атаки Password Spraying;

- события аутентификации пользователей (для Windows: Windows Security Log: 4625 и Kerberos Authentication Service: 4771; для Linux: /var/log/auth.log и /var/log/secure).

Отслеживайте события операционной системы, которые говорят о неуспешных попытках входа. Это могут быть события как с отдельных узлов, так и с серверов аутентификации, например события запроса билетов Kerberos;

- сетевой трафик.

Отслеживайте сетевой трафик на предмет неуспешных попыток входа в систему. Например, атаку, связанную с подбором пароля в домене Windows, можно выявить по большому количеству неуспешных попыток аутентификации по протоколу Kerberos. Для автоматизации этой задачи можно использовать NTA-системы.

Для предотвращения использования подтехник Brute Force: Password Guessing и Spraying необходимо:

1. внедрить многофакторную аутентификацию, особенно для сервисов доступных извне;
2. установить требования к сложности пароля и его длине.

Усложнить задачу перебора паролей можно, настроив политику блокировки учетных записей при достижении некоторого порогового значения неуспешных попыток аутентификации за определенный промежуток времени, однако эта мера сработает только для атак с использованием подтехники Password Guessing.

> Стоит учитывать, что чересчур жесткая политика блокировки может привести к нарушению бизнес-процессов из-за блокировки подбираемых учетных записей. В этом случае система не перестанет функционировать, а вот легитимный пользователь не сможет получить к ней доступ, так как его учетная запись будет заблокирована.

Credential Access: Unsecured Credentials

Техника Unsecured Credentials (T1552) была успешно применена в 79% исследованных организаций.

Для того чтобы обнаружить факты использования техники Unsecured Credentials, нужно проанализировать:

- события запуска процессов (для Windows: Sysmon: 1 и Windows Security Log: 4688 (с включенным логированием строк запуска); для Linux: Syscall: execve).

Настройте мониторинг событий запуска процессов с расширенным аудитом строк запуска. Ищите запуск команд, направленных на поиск учетных данных. Обычно они содержат следующие ключевые слова: password, pwd, login, secure или само сочетание логина и пароля.

Обычно для поиска по шаблону имени в ОС Windows используется команда dir стандартной командной оболочки cmd.exe. Для поиска по содержимому в ОС Windows используется утилита findstr.exe. В ОС Linux для тех же целей используются утилиты find и grep соответственно;

- события выполнения скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Собирайте и анализируйте события запуска скриптов PowerShell. Среди командлетов скрипта могут встретиться инструкции поиска файлов, например Get-ChildItem с паттернами имен, содержащими строки password, pwd, login, secure или само сочетание логина и пароля.

Предотвращение техники Unsecured Credentials: для того чтобы свести к минимуму шансы на успешное применение данной техники, следует регулярно проводить поиск файлов, содержащих пароли, и обучать пользователей тому, как нужно подходить к хранению конфиденциальной информации. Также следует разграничить доступ к общим файловым ресурсам: права доступа к определенным папкам должны быть только у определенного круга лиц. Помимо этого, следует установить организационную политику в компании, запрещающую хранение паролей в файлах.

Discovery

Техника File and Directory Discovery (T1083) была успешно применена во всех компаниях, а Account Discovery — в 96% проектов.

Попытки обнаружения данной техники будут порождать большое количество ложных срабатываний правил на легитимную активность. Чтобы уменьшить их количество, мы рекомендуем обращать внимание не на конкретное событие, связанное с тактикой discovery, а на общую ситуацию в инфраструктуре. Злоумышленники не ограничатся только поиском файлов или исследованием привилегии учетной записи, они будут провоцировать и другие события в журналах безопасности. Поэтому если других подозрительных событий нет, но есть, например, доступ к файлу, не стоит бить тревогу.

Также стоит обратить внимание на то, как часто возникают похожие события, ведь в целом эти действия относятся к легитимной активности и могут быть следствием действий администраторов или легитимных скриптов.

Discovery: File and Directory Discovery

Обнаружить факты применения техники File and Directory Discovery можно:

- среди событий запуска процессов (для Windows: Sysmon: 1, Windows Security Log: 4688 (с включенным логированием строк запуска); для Linux: auditd: Syscall: execve).

Настройте мониторинг событий запуска процессов с расширенным аудитом строк запуска. Ищите запуск команд, направленных на перечисление файлов и каталогов.

> Обычно для листинга директорий и поиска файлов и папок в Windows используется команда dir стандартной командной оболочки cmd.exe. В Linux для тех же целей используются утилиты ls и find соответственно;

- событий выполнения скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Собирайте и анализируйте события запуска скриптов PowerShell. При анализе командлетов в скрипте могут встречаться инструкции по поиску файлов, например Get-ChildItem.

> В целом техника Discovery: File and Directory Discovery связана с техникой Credential Access: Unsecured Credentials. Как и в тактике Credential Access, злоумышленники, применяющие эту технику, зачастую нацелены на получение учетных данных, которые хранятся в пользовательских файлах. Поэтому рекомендации по обнаружению и превентивные меры для этих двух техник схожи.

Предотвращение техники File and Directory Discovery:

Данный тип атаки сложно предотвратить, поскольку он основан на использовании легитимных функций операционной системы. Для того чтобы минимизировать шансы злоумышленников, мы рекомендуем не хранить и не передавать чувствительную информацию в открытом виде. Используйте для этих целей шифрование.

Discovery: Account Discovery

Обнаружить факт использования подтехники Account Discovery: Domain Account (T1087.002), Local Account (T1087.001) можно:

- среди событий, связанных с запуском процессов (для Windows: Sysmon: 1, Windows Security Log: 4688 (с включенным логированием строк запуска); для Linux: auditd: Syscall: execve).

Отслеживайте запуск команд, направленных на перечисление или сбор информации о пользователях и группах;

- событий, связанных с выполнением скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Собирайте и анализируйте события запуска скриптов PowerShell. Среди командлетов скрипта могут встретиться инструкции перечисления и поиска пользователей, например Get-ADUser.

Предотвращение подтехники Account Discovery: Domain Account, Local Account:

Данный тип атаки сложно предотвратить, поскольку он основан на использовании легитимных функций операционной системы.

> **Точечная рекомендация, которая может усложнить атаку для злоумышленников:**
>
> Если в реестре Windows включена настройка EnumerateAdministrators, то атакующие могут получить список локальных администраторов, вызвав диалог UAC. Отключите эту настройку, чтобы атакующие не могли воспользоваться данным способом получения списка локальных администраторов. Параметр находится по пути:
>
> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators.

Lateral Movement

Среди всех техник тактики Lateral Movement, которые пентестеры использовали для перемещения внутри сетевого периметра, наиболее результативной была Use Alternate Authentication Material. Это связано с тем, что пароль в открытом виде не всегда удается найти, а если пароль был сложный, то восстановить из хеша тоже не просто, при этом получить сам хеш или билет TGT или TGS легче.

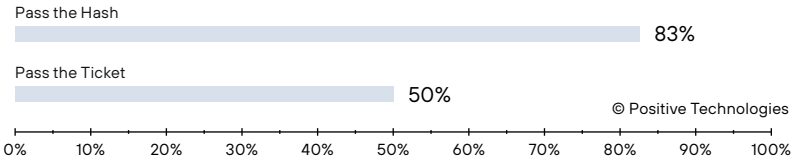

Рисунок 3. Популярные подтехники техники Use Alternate Authentication Material

Lateral Movement: Use Alternate Authentication Material: Pass the Hash

Обнаружить факт использования подтехники Use Alternate Authentication Material: Pass the Hash (T1550.002) можно:

- в журнале безопасности контроллера домена (событие Windows: 4768 и 4769).

Отслеживайте запросы новых билетов TGT и TGS. В сочетании с фактами специфичного сеанса входа в систему (ID 4624 с Logon Type = 9) и доступа к памяти процесса LSASS (Sysmon ID 10) события Windows: 4768 и 4769 могут свидетельствовать об обходе стадии получения хеша из пароля и указывать на попытку развития атаки Pass the Hash для Kerberos (атака OverPass the Hash);

- журнале событий аудита входа в систему (событие Windows: 4624).

Отслеживайте попытки аутентификации пользователей. Корреляция событий входа с другой подозрительной активностью может подтвердить факт компрометации инфраструктуры.

Например, выполненная проверка подлинности NTLM и LogonType 3, вызывает подозрение, потому что выполняется сетевой вход в систему без графической оболочки. Однако в этом случае нужно убедиться в том, что это не является типичным событием для рассматриваемой инфраструктуры, ведь иногда в крупных сетях присутствуют системы, в которых используются устаревшие механизмы аутентификации.

Для предотвращения атак с использованием подтехники Use Alternate Authentication Material: Pass the Hash необходимо сделать следующее.

> Точечная рекомендация: установить обновления безопасности KB2871997 для Windows 7 и выше. Данное обновление ограничивает доступ по умолчанию для учетных записей из группы локальных администраторов.

Полностью исключить возможность атак с использованием этой техники невозможно из-за архитектурных особенностей ОС, но можно минимизировать вероятность ее проведения и повысить уровень сложности атаки для злоумышленников: для этого следует ограничить область использования привилегированных учетных записей. Например, учетная запись администратора домена должна быть задействована только при выполнении работ на контроллере домена и единичных сервисах, где требуются такие привилегии.

Lateral Movement: Use Alternate Authentication Material: Pass the Ticket

Обнаружить факт использования подтехники Use Alternate Authentication Material: Pass the Ticket (T1550.003) можно:

- в журнале аудита службы проверки подлинности Kerberos (события Windows: 4769).

Отслеживайте факты использования новых билетов TGT и TGS узлом, который до этого момента к ним не обращался. Такое событие может свидетельствовать об атаке, если этот узел не проксирует трафик.

> Если после двойного сброса пароля krbtgt на контроллере домена зафиксировано событие 4769 с кодом 0x1F, это означает вероятную попытку использования украденного или подделанного билета;

- журнале событий аудита входа в систему.

Отслеживайте попытки аутентификации пользователей. Корреляция событий входа с другой подозрительной активностью может подтвердить факт компрометации инфраструктуры;

- журнале событий запуска процессов.

События запуска утилит для манипуляции с билетами Kerberos (например, Rubeus или klist) могут свидетельствовать о готовящейся атаке Pass the Ticket;

- сетевом трафике.

Если с узла не запрашивали билет Kerberos, но используют его, это может свидетельствовать об атаке Pass the Ticket. В качестве средства для автоматизированного поиска таких атак можно использовать NTA.

Предотвращение атак с использованием подтехники Use Alternate Authentication Material: Pass the Ticket:

Полностью исключить возможность проведения атак с использованием этой техники невозможно из-за особенностей реализации ОС, но можно уменьшить шансы злоумышленников на успех. Для этого периодически выполняйте сброс пароля для учетной записи krbtgt. Смените пароль, запустите репликацию и затем смените пароль второй раз. Этот алгоритм поможет в случае, если учетные данные оказались в руках злоумышленников, но они по каким-то причинам не продолжили атаку либо если злоумышленники уже давно находятся в инфраструктуре. А также следуйте лучшим практикам администрирования корпоративной инфраструктуры и ограничьте использование привилегированных учетных записей пределами административных зон безопасности.

Command and Control

Пентестеры успешно использовали подтехнику Application Layer Protocol: Web Protocols (T1071) в 93% организаций.

Обнаружить атаку с использованием этого метода можно, проанализировав:

- сетевой трафик.

Необходимо проанализировать протоколы и пакеты на предмет аномалий, а также использовать средства защиты, которые позволяют выявить паттерны, соответствующие известным инструментам злоумышленников, даже если трафик зашифрован.

> Для того чтобы обнаруживать подобные атаки, можно воспользоваться системами обнаружения вторжений (IDS) или средствами анализа сетевого трафика (NTA).

Предотвратить атаку можно:

1. с помощью системы предотвращения сетевых вторжений (IPS);
2. системы обнаружения и реагирования на сложные целевые угрозы и атаки (XDR);
3. межсетевого экрана нового поколения (NGFW).

Матрица D3FEND

Матрица D3FEND — удобный инструмент, с помощью которого можно выделить необходимые функции средств защиты информации. Модель D3FEND связана с MITRE ATT&CK, что значительно облегчает подбор мер, если модель угроз основана на классификации MITRE ATT&CK.

Разработчики этой методики выделили пять оборонительных тактик[3]: обнаружение (detect), сокрытие (harden), обман (deceive), очистка инфраструктуры от злоумышленника (evict) и изоляция (isolate). Каждой тактике соответствует свой набор техник, например для тактики Evict выделены две техники: Credential Eviction и Process Eviction. Конкретные функции СЗИ указаны ниже под техниками. Представленный набор функций на данный момент не исчерпывающий, однако инструмент активно развивается.

[3] Ответные действия на атаку киберпреступника.

Мы отметили на матрице функции средств защиты, которые нужны для того, чтобы предупредить, обнаружить или отреагировать на атаки с использованием 10 техник из матрицы MITRE ATT&CK, которые чаще всего оказывались успешными в ходе тестирования на проникновение.

> Важное уточнение: представленный набор мер мы определили как минимальный, то есть современные СЗИ обладают гораздо более широким функционалом, который поможет быстрее обнаружить воздействие и отреагировать на него.

Harden			Detect								Isolate				Deceive	Evict	
Application Hardening	**Credential Hardening**	**Platform Hardening**	**File Analysis**	**Identifier Analysis**		**Network Traffic Analysis**	**Platform Monitoring**		**Process Analysis**		**User Behavior Analysis**	**Execution Isolation**		**Network Isolation**		**Decoy Object**	**Credential Eviction**	**Process Eviction**
Application Configuration Hardening	Certificate-based Authentication	Disk Encryption	Dynamic Analysis	URL Analysis		Certificate Analysis	Operating System Monitoring	System File Analysis	Database Query String Analysis		Authentication Event Thresholding	Executable Denylisting			Forward Resolution Domain Denylisting	Decoy File	Account Locking	Process Termination
	Credential Transmission Scoping	File Encryption	Emulated File Analysis	Identifier Reputation Analysis	Domain Name Reputation Analysis	Client-server Payload Profiling			File Access Pattern Analysis		Authorization Event Thresholding	Hardware-based Process Isolation		DNS Denylisting	Hierarchical Domain Denylisting	Decoy User Credential	Authentication Cache Invalidation	
	Domain Trust Policy	Local File Permissions	File Content Rules		File Hash Reputation Analysis	DNS Traffic Analysis			Indirect Branch Call Analysis		Credential Compromise Scope Analysis	Kernel-based Process Isolation	Mandatory Access Control		Forward Resolution IP Denylisting			
	Multi-factor Authentication	Software Update	File Hashing		IP Reputation Analysis	File Carving			Process Code Segment Verification		Domain Account Monitoring				Reverse Resolution IP Denylisting			
	Strong Password Policy	System Configuration Permissions			URL Reputation Analysis	Per Host Download-Upload Ratio Analysis			Process Self-Modification Detection		Job Function Access Pattern Analysis			Network Traffic Filtering	Outbound Traffic Filtering			
	User Account Permissions					RPC Traffic Analysis			Process Spawn Analysis	Process Lineage Analysis	Local Account Monitoring							
									Script Execution Analysis		Resource Access Pattern Analysis							
									Shadow Stack Comparisons		User Data Transfer Analysis							
									System Call Analysis	File Creation Analysis	Web Session Activity Analysis							

Матрица D3FEND

Функции СЗИ для предотвращения, обнаружения и реагирования на топ-10 техник MITRE ATT&CK

Сопоставление мер защиты информации

Мы проанализировали меры, предложенные сообществом, для десяти наиболее популярных техник из матрицы MITRE ATT&CK, которые были успешно использованы нашими пентестерами во внешних и внутренних тестах на проникновение, и провели параллель с мерами защиты, изложенными в Приказе ФСТЭК России от 11.02.2013 № 17; результат этого сопоставления представлен в таблице 2.

Таблица 2. Сопоставление мер защиты, предложенных сообществом MITRE и ФСТЭК России

ID	Мера по снижению вероятности реализации НС	УИН из приказа	Описание меры
M1048	Application Isolation and Sandboxing	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти
		ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения
M1050	Exploit Protection	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
		ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения

M1030	Network Segmentation	УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
		ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
		ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей
M1026	Privileged Account Management	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
		ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
		УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
		ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
M1051	Update Software	АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
M1016	Vulnerability Scanning	АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
M1049	Antivirus/ Antimalware	АВЗ.1	Реализация антивирусной защиты
		АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

M1045	Code Signing	ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения
M1042	Disable or Remove Feature or Program	ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
M1038	Execution Prevention	ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
M1021	Restrict Web-Based Content	ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
M1017	User Training	п.18.6 Приказа	Обеспечение защиты информации в ходе эксплуатации информационной системы должно осуществляться оператором в соответствии с эксплуатационной документацией и организационно-распорядительными документами по защите информации и включать следующие мероприятия: информирование и обучение персонала информационной системы
M1036	Account Use Policies	УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

M1027	Password Policies	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
		УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
		УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
		УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
		УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
		АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
M1032	Multi-factor Authentication	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
M1015	Active Directory Configuration	-	Прямое соответствие отсутствует

M1047	Audit	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
		РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе
		АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
M1041	Encrypt Sensitive Information	ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
M1037	Filter Network Traffic	УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
		ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов
M1028	Operating System Configuration	-	Прямое соответствие отсутствует
M1022	Restrict File and Directory Permissions	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
M1040	Behavior Prevention on Endpoint	-	Прямое соответствие отсутствует

M1043	Credential Access Protection	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
		УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
M1025	Privileged Process Integrity	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
M1052	User Account Control	-	Прямое соответствие отсутствует
M1018	User Account Management	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
M1031	Network Intrusion Prevention	СОВ.1	Обнаружение вторжений
		СОВ.2	Обновление базы решающих правил

Превентивные меры для топ 10 тактик и техник покрывают 33 из 113 требований Приказа. Таким образом, если выполнять требования регулятора не формально, не для того, чтобы соответствовать им только на бумаге, — уровень защищенности в компании заметно вырастет.

Заключение

Умение обнаруживать и предотвращать атаки, состоящие из топ 10 самых распространенных техник MITRE ATT&CK®, повышает эффективность системы защиты и таким образом позволяет обнаруживать еще больше атак. Для этого необходимо анализировать журналы событий ОС, сетевой трафик, журналы событий приложений, журнал событий на контроллере домена, а также использовать современные средства защиты, которые облегчат сбор данных и вовремя оповестят о действиях злоумышленников.

В этом исследовании мы продемонстрировали, что если изменить подход к выполнению требований регуляторов, то можно получить не просто их формальную реализацию, а полноценную систему защиты от реальных атак. Новый подход не только переведет ваши процессы ИБ на новый уровень зрелости, но и сделает систему безопасности вашей компании по-настоящему результативной.

ptsecurity.com
pr@ptsecurity.com