Научная статья
Original article
УДК 004.424

RAT И ЕГО ОСОБЕННОСТИ

RAT AND ITS FEATURES

Крыгин Никита Дмитриевич, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), krigginnn@rambler.ru

Krygin Nikita Dmitrievich, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), krigginnn@rambler.ru

Аннотация: Троянец удаленного доступа (RAT) — это вредоносная программа, которая открывает бэкдор, позволяя администратору контролировать компьютер жертвы. RAT обычно загружаются вместе с кажущейся законной программой, такой как игра, или отправляются получателю в виде вложения электронной почты. Как только злоумышленник скомпрометирует систему хоста, он может использовать ее для распространения RAT на дополнительные уязвимые компьютеры, создавая ботнет.

Abstract: A Remote Access Trojan (RAT) is a malicious program that opens a backdoor, allowing an administrator to control the victim's computer. RATs are usually downloaded along with a seemingly legitimate program, such as a game, or

sent to the recipient as an email attachment. Once an attacker compromises a host system, they can use it to spread the RAT to additional vulnerable computers, creating a botnet.

Ключевые слова: информационная безопасность, злоумышленник, RAT, уязвимости

Keywords: information security, intruder, RAT, vulnerabilities

RAT можно развернуть как вредоносную полезную нагрузку с помощью наборов эксплойтов, таких как Metasploit. После успешной установки RAT обеспечивает прямое подключение к серверу управления и контроля (C&C), контролируемому злоумышленниками. Злоумышленники достигают этого, используя предопределенный открытый порт TCP на скомпрометированном устройстве.

Поскольку RAT обеспечивает административный контроль, злоумышленник может делать практически все на компьютере жертвы, например:

Отслеживайте поведение пользователей с помощью шпионских программ или кейлоггеров. Доступ к конфиденциальным данным, включая номера социального страхования и данные кредитной карты.

Группы кибербезопасности часто испытывают трудности с обнаружением RAT, потому что они обычно не отображаются в списках запущенных задач или программ. RAT обычно выполняют действия, аналогичные действиям действительных программ. Кроме того, злоумышленник будет управлять уровнем использования ресурсов, чтобы не было падения производительности, что затрудняет обнаружение угрозы.

Вот несколько способов, которыми RAT-атака может поставить под угрозу отдельных пользователей, организации или даже целые группы населения:

Шпионаж и шантаж — злоумышленник, развернувший RAT на устройстве пользователя, получает доступ к его камерам и микрофонам. Они

могут фотографировать пользователя и его окружение, использовать это для проведения более изощренных атак или для шантажа пользователя.

Запуск распределенных атак типа «отказ в обслуживании» (DDoS) — когда злоумышленники развернули RAT на большом количестве пользовательских устройств, они могут использовать эти устройства, чтобы залить целевой сервер поддельным трафиком. Пользователи обычно не подозревают, что их устройства используются для DDoS-атак, хотя атака может привести к снижению производительности сети.

Криптомайнинг — злоумышленники могут использовать RAT для добычи биткойнов или другой криптовалюты на компьютере пользователя. Масштабируя свою работу на большое количество устройств, они могут получать значительный доход.

Удаленное хранилище файлов — злоумышленники могут использовать RAT для хранения незаконного контента на устройствах ничего не подозревающих жертв. Таким образом, власти не могут отключить учетную запись или сервер хранения злоумышленника, поскольку их данные хранятся на устройствах, принадлежащих законным пользователям.

Компрометация промышленных систем — злоумышленники могут использовать RAT для получения контроля над крупными промышленными системами, включая коммунальные услуги, такие как водоснабжение и электроснабжение. Злоумышленник может саботировать эти системы, нанося значительный ущерб промышленному оборудованию и потенциально нарушая работу критически важных служб целых областей.

Sakula — это, казалось бы, безобидное программное обеспечение с законной цифровой подписью, но оно позволяет злоумышленникам использовать все возможности удаленного администрирования на машине. Использует простые незашифрованные HTTP-запросы для связи со своим управляющим сервером. Он использует похититель паролей mimikatz для выполнения аутентификации с использованием метода передачи хэша,

который повторно использует хэши аутентификации операционной системы для перехвата существующих сеансов.

KjW0rm — это червь, написанный на языке VBS, что затрудняет его обнаружение на компьютерах с Windows. Он также использует обфускацию, чтобы избежать обнаружения антивирусом. Он тихо развертывается, а затем открывает бэкдор, который позволяет злоумышленникам получить полный контроль над машиной и отправлять данные обратно на C&C-сервер.

Havex — это RAT, предназначенная для промышленных систем управления (ICS). Он предоставляет злоумышленникам полный контроль над промышленным оборудованием. Havex использует несколько мутаций, чтобы избежать обнаружения, и имеет минимальный след на устройстве жертвы. Он взаимодействует с C&C-сервером по протоколам HTTP и HTTPS.

Agent.BTZ/ComRat (также называемый Uroburos) — еще одна RAT, нацеленная на ICS, которая, как считается, была разработана российским правительством. Он развертывается с помощью фишинговых атак и использует методы шифрования, антианализа и судебной экспертизы, чтобы избежать обнаружения. Он обеспечивает полный административный контроль над зараженной машиной и может передавать данные обратно на свой C&C-сервер.

Dark Comet впервые была идентифицирована в 2011 году и до сих пор активно используется. Он предоставляет полный административный контроль над зараженными машинами и может отключать диспетчер задач, брандмауэр и контроль доступа пользователей (UAC) на машинах Windows. Dark Comet использует шифрование, чтобы избежать обнаружения антивирусом.

AlienSpy — это RAT, предназначенный для платформ Apple OS X и macOS. Он собирает информацию о целевой системе, активирует веб-камеру и безопасно подключается к C&C-серверу, чтобы обеспечить полный контроль над машиной. AlienSpy использует методы антианализа для обнаружения присутствия виртуальных машин.

Heseber BOT основан на VNC, традиционном инструменте удаленного доступа. Он использует VNC для удаленного управления целевой машиной и передачи данных на C&C-сервер. Однако он не предоставляет административный доступ к машине, если у пользователя нет таких разрешений. Поскольку VNC является законным инструментом, Haseber не может быть обнаружен многими антивирусными инструментами.

Sub7 — это RAT, работающий по модели клиент-сервер. Сервер — это компонент, развернутый на машине-жертве, а клиент — это графический интерфейс, используемый злоумышленником для управления удаленной системой. Сервер пытается установить себя в каталог Windows. После развертывания Sub7 обеспечивает захват веб-камеры, перенаправление портов, чат и предоставляет простой в использовании редактор реестра.

Back Orifice — это программа удаленного доступа для Windows, поддерживающая большинство версий, начиная с Windows 95. Она развертывается как сервер на целевой машине, занимающей небольшую площадь, и позволяет клиенту с графическим интерфейсом, управляемому злоумышленником, получить полный контроль над система. Его можно использовать для параллельного управления несколькими компьютерами с использованием методов обработки изображений. Сервер связывается со своим клиентом через TCP или UDP. Обычно он работает на порту 31337.

Вот несколько способов защитить свою организацию от вредоносного ПО RAT.

Стратегия защиты от RAT зависит от обучения по вопросам безопасности в масштабах всей организации. Человеческая ошибка — основная причина большинства событий, связанных с безопасностью, и RAT — не исключение. Злоумышленники обычно запускают это вредоносное ПО через зараженные вложения и ссылки в фишинговых кампаниях. Сотрудники должны быть бдительными, чтобы случайно не заразить сеть компании.

RAT обычно используются для компрометации учетных данных администратора, предоставляя злоумышленникам доступ к ценным данным в

сети организации. Благодаря жесткому контролю доступа вы можете ограничить последствия скомпрометированных учетных данных. Более строгие меры контроля включают внедрение двухэтапной проверки, более строгие настройки брандмауэра, внесение IP-адресов в белый список для авторизованных пользователей и использование более совершенных антивирусных решений.

Злоумышленники рассматривают каждую новую конечную точку, которая подключается к вашей сети, как потенциальную систему для компрометации с помощью RAT. Организации должны разрешать удаленный доступ только через безопасные соединения, созданные с помощью виртуальных частных сетей (VPN) или защищенных защищенных шлюзов, чтобы свести к минимуму поверхность атаки . Кроме того, вы можете использовать бесклиентское решение для удаленного доступа, которое не требует дополнительных подключаемых модулей или программного обеспечения на устройствах конечных пользователей, поскольку эти устройства являются целями для злоумышленников.

Популярность моделей безопасности с нулевым доверием возросла, поскольку они пропагандируют принцип «никогда не доверяй, всегда проверяй». Вместо того, чтобы предоставлять административные учетные данные для полного доступа по сети, подход к обеспечению безопасности с нулевым доверием предоставляет детальный контроль над латеральными перемещениями. Это критически важно для подавления RAT-атак, поскольку злоумышленники используют боковые перемещения для заражения дополнительных систем и доступа к конфиденциальным данным.

RAT, как и все вредоносные программы, представляют угрозу только в том случае, если они установлены и реализованы на целевом компьютере. Использование решений для безопасного просмотра и защиты от фишинга, а также постоянное исправление систем могут свести к минимуму вероятность RAT. Эти решения затрудняют заражение компьютера RAT.

RAT — это трояны, которые могут представляться как законные приложения. RAT обычно содержат вредоносные функции, связанные с реальным приложением. Отслеживайте приложения и системы на предмет необычного поведения, которое может указывать на RAT.

Злоумышленник может использовать RAT для удаленного управления зараженным компьютером по сети. RAT, развернутый на локальном устройстве, взаимодействует с удаленным сервером управления и контроля (C&C). Ищите необычный сетевой трафик, связанный с такими сообщениями, и используйте такие инструменты, как брандмауэры веб-приложений (WAF), для отслеживания и блокировки сообщений C&C.

Концепция наименьших привилегий гласит, что приложения, пользователи, системы и т.п. должны иметь только те разрешения и доступ, которые необходимы для выполнения их работы. Использование наименьших привилегий может помочь ограничить действия злоумышленника с помощью RAT.

RAT обычно пытаются украсть пароли и имена пользователей для онлайн-аккаунтов. Использование MFA может свести к минимуму последствия, если учетные данные человека будут скомпрометированы.

Брандмауэр веб - приложений Imperva может предотвратить развертывание RAT в вашей сети и может прервать связь RAT с C&C-серверами после развертывания.

Помимо защиты от вредоносных программ, Imperva обеспечивает комплексную защиту приложений, API и микросервисов:

Самозащита приложений во время выполнения (RASP) — обнаружение и предотвращение атак в реальном времени из среды выполнения вашего приложения, где бы ни находились ваши приложения. Остановите внешние атаки и инъекции и уменьшите количество незавершенных уязвимостей.

Безопасность API. Автоматическая защита API обеспечивает защиту ваших конечных точек API по мере их публикации, защищая ваши приложения от эксплуатации.

Расширенная защита от ботов. Предотвращайте атаки на бизнес-логику со всех точек доступа — веб-сайтов, мобильных приложений и API. Обеспечьте полную видимость и контроль над трафиком ботов, чтобы остановить онлайн-мошенничество путем захвата учетной записи или извлечения конкурентоспособных цен.

Защита от DDoS -атак — блокируйте атакующий трафик на периферии, чтобы обеспечить непрерывность бизнеса с гарантированным временем безотказной работы и отсутствием влияния на производительность. Защитите свои локальные или облачные ресурсы независимо от того, размещены ли вы в AWS, Microsoft Azure или Google Public Cloud.

Аналитика атак — обеспечивает полную видимость с помощью машинного обучения и экспертизы предметной области в стеке безопасности приложений, чтобы выявлять закономерности в шуме и обнаруживать атаки на приложения, позволяя изолировать и предотвращать кампании атак.

Защита на стороне клиента. Получите видимость и контроль над сторонним кодом JavaScript, чтобы снизить риск мошенничества в цепочке поставок, предотвратить утечку данных и атаки на стороне клиента.

Литература

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.
4. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.
5. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

6. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2008. - 400 с.
7. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

References

1. Babash, A.V. Information security: Laboratory workshop / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2019. - 432 p.
2. Babash, A.V. Information Security. Laboratory workshop: Textbook / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2013. - 136 p.
3. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 400 p.
4. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 476 p.
5. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2018. - 400 p.
6. Baranova, E.K. Information Security. History of special methods of cryptographic activity: Textbook / E.K. Baranova, A.V. Babash, D.A. Larin. - M.: Rior, 2008. - 400 p.
7. Biryukov, A.A. Information security: protection and attack / A.A. Biryukov. - M.: DMK Press, 2013. - 474 p.
8. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rn / D: Phoenix, 2010. - 324 p.

Для цитирования: Крыгин Н.Д. «RAT и его особенности»// Научный сетевой журнал «Столыпинский вестник», номер 4/2022.