Ворошилов Д.В. Как атаковать системы, изолированные от сети, через акустические колебания вентиляторов // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 3(53) с. 78–81

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

КАК АТАКОВАТЬ СИСТЕМЫ, ИЗОЛИРОВАННЫЕ ОТ СЕТИ, ЧЕРЕЗ АКУСТИЧЕСКИЕ КОЛЕБАНИЯ ВЕНТИЛЯТОРОВ

Ворошилов Д.В.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: superdaniil2002@yandex.ru

Системы, изолированные от сети (air-gapped systems), традиционно считаются одними из самых защищённых, поскольку они физически отключены от интернета и корпоративных сетей. Однако исследователи в области кибербезопасности разработали методы атак, использующие акустические колебания компьютерных компонентов, таких как вентиляторы, для передачи данных. В данной статье рассматривается принцип работы такого метода, его техническая реализация, потенциальные риски и способы защиты, включая мониторинг акустических аномалий и физическую изоляцию критически важных систем.

Ключевые слова: Изолированные системы, air-gap, атака через акустику, утечка данных, вентиляторы, вибрации, инфосек, кибербезопасность.

HOW TO ATTACK SYSTEMS ISOLATED FROM THE NETWORK THROUGH ACOUSTIC VIBRATIONS OF FANS

Voroshilov D.V.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: superdaniil2002@yandex.ru

Air-gapped systems are traditionally considered among the most secure because they are physically disconnected from the internet and corporate networks. However, cybersecurity researchers have developed attack methods that utilize acoustic vibrations of computer components, such as fans, to transmit data. This article explores the working principle of this method, its technical implementation, potential risks, and protection strategies, including acoustic anomaly monitoring and physical isolation of critical systems.

Keywords: Air-Gapped systems, air-gap attack, acoustic data exfiltration, fans, vibrations, cybersecurity, information security.

Введение

В современном мире информационной безопасности одной из самых надёжных стратегий защиты является изоляция систем от сети. Air-gapped системы широко применяются в государственных учреждениях, военной сфере, ядерной энергетике и других критически важных инфраструктурах для предотвращения кибератак и утечек данных. Такие системы не подключены к интернету и корпоративным сетям, что делает невозможными традиционные методы атак через удалённый доступ или вредоносное ПО, распространяемое по сети.

Однако даже изолированные системы не являются абсолютно безопасными. Исследования в области кибербезопасности показывают, что злоумышленники могут использовать нетрадиционные методы атак, в том числе побочные каналы передачи данных. Одним из таких методов является эксплуатация акустических колебаний вентиляторов компьютера. Этот способ позволяет передавать информацию из изолированной системы в контролируемую злоумышленником среду с использованием изменения скорости вращения вентиляторов, создающих различающиеся акустические сигналы.

В данной статье рассматривается принцип работы атак через акустические колебания вентиляторов, механизм их реализации, возможные сценарии применения и методы защиты. Несмотря на сложность подобных атак, они демонстрируют, что даже физическая изоляция системы не является гарантией полной безопасности.

Как атаковать системы, изолированные от сети, через акустические колебания вентиляторов

Изолированные системы (air-gapped systems) применяются для защиты особо важных данных, поскольку их физическое отключение от внешних сетей делает невозможными традиционные кибератаки, основанные на удалённом доступе. Однако современные исследования в области безопасности демонстрируют, что даже такие системы не являются абсолютно защищёнными. Одним из самых необычных и сложных методов атак на изолированные компьютеры является использование акустических колебаний их внутренних компонентов, в частности вентиляторов, для передачи данных в контролируемую злоумышленником среду[1].

Этот метод основан на том, что скорость вращения вентиляторов в компьютерах и серверах может изменяться программно, а изменение скорости создаёт характерные акустические колебания. Эти колебания могут быть зафиксированы микрофонами, находящимися в непосредственной близости от атакуемой системы, включая смартфоны, умные колонки или даже специализированные устройства для перехвата ультразвуковых сигналов. Код, управляющий атакой, может модифицировать скорость вращения вентиляторов таким образом, чтобы создать закодированную последовательность звуковых сигналов, содержащих полезную нагрузку[2].

Для успешного осуществления такой атаки злоумышленникам требуется несколько ключевых условий. Во-первых, вредоносное ПО должно быть предварительно установлено на изолированной системе. Это может быть достигнуто через заражённые USB-носители, компрометацию обновлений ПО или физический доступ к машине. Во-вторых, вблизи атакуемой системы должен находиться приёмник, способный зафиксировать звуковые сигналы. В качестве такого приёмника могут выступать смартфоны сотрудников, умные устройства или даже устройства IoT, которые имеют встроенные микрофоны и соединение с интернетом[3].

Принцип передачи данных через акустические колебания заключается в модуляции частоты звука, создаваемого вентиляторами. Например, изменение скорости вращения вентилятора может быть использовано для кодирования двоичных данных, где определённая частота означает "0", а другая — "1". Это позволяет передавать небольшие объёмы информации, такие как пароли, криптографические ключи или другие конфиденциальные данные[4].

Преимущества такого метода атаки заключаются в том, что он не требует традиционных каналов передачи данных и сложно обнаруживается стандартными средствами защиты. Антивирусное ПО, межсетевые экраны и даже системы обнаружения вторжений не способны предотвратить утечку информации через акустические каналы. Однако у этой атаки есть и ограничения: скорость передачи данных остаётся крайне низкой, обычно в диапазоне 10-50 бит в секунду, что делает невозможной передачу больших объёмов информации.

Защита от подобных атак требует комплексного подхода. Один из основных способов защиты — это контроль над возможными точками утечки данных. Например, можно запрещать или ограничивать использование мобильных устройств вблизи критически важных систем, а также изолировать атакуемые машины в звуконепроницаемых помещениях. Ещё один эффективный метод — это мониторинг аномального поведения вентиляторов и акустической активности в серверных комнатах. Если скорость вращения вентиляторов изменяется без видимой причины, это может свидетельствовать о попытке передачи данных[5].

Дополнительно можно применять физические методы защиты, такие как использование систем шумоподавления или генераторов белого шума, которые маскируют акустические сигналы, предотвращая их фиксацию приёмными устройствами. Некоторые организации уже используют такие методы для защиты от атак через ультразвуковые каналы, применяя акустические глушители и экранированные серверные помещения.

Заключение

Современные методы атак на информационные системы выходят далеко за рамки традиционных хакерских инструментов. Эксплуатация акустических колебаний вентиляторов для утечки данных показывает, насколько изощрёнными могут быть способы компрометации даже самых защищённых систем. Изолированные от сети системы долгое время считались практически неуязвимыми, однако исследования в области кибербезопасности доказывают, что ни одна защита не является абсолютной.

Хотя атаки такого типа пока остаются редкостью, они представляют серьёзную угрозу для организаций, работающих с критически важными данными. Учитывая сложность их обнаружения, традиционные антивирусные средства и системы мониторинга сетевого трафика неэффективны против таких атак. Поэтому защита от них требует комплексных мер, включая физическую изоляцию, мониторинг акустических сигналов, использование белого шума и программные ограничения на управление аппаратными компонентами.

С развитием технологий безопасность информационных систем требует всё более продвинутых решений. В мире, где даже вентиляторы могут стать инструментом утечки данных, кибербезопасность перестаёт быть вопросом только программных барьеров.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.

2. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.
3. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
4. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
5. Бирих Э. В. и др. Исследование вопросов повышения уровня защищенности органов исполнительной власти //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 107-110.

References

1. Gelfand A.M. et al. Development of a self-modifying code distribution model in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. No. 8. pp. 91-97.
2. Orlov G. A., Krasov A.V., Gelfand A.M. Application of Big Data in the analysis of big data in computer networks //High-tech technologies in space exploration of the Earth. 2020. – Vol. 12. – No. 4. – pp. 76-84.
3. Volkogonov V. N., Gelfand A.M., Derevyanko V. S. Relevance of automated control systems //Actual problems of infotelec communications in science and education (APINO 2019). – 2019. – pp. 262-266.
4. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: actual aspects of the "National Research Institute of National Development". July 2018. – 2018. – pp. 31-35.
5. Birikh E. V. and others. Research of issues of increasing the level of protection of executive authorities //Actual problems of infotelec communications in science and education (APINO 2018), 2018, pp. 107-110.