ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

ЛАТЕРАЛЬНОЕ ПЕРЕМЕЩЕНИЕ В ИНФРАСТРУКТУРЕ УМНОГО ДОМА

Агуреев Иван Александрович,
старший преподаватель кафедры безопасности и информационных технологий, Национальный исследовательский университет "МЭИ", 111250, Россия, г. Москва, Красноказарменная улица, дом 14, e-mail: universe@mpei.ac.ru

Горленко Артур Романович,
студент кафедры безопасности и информационных технологий, Национальный исследовательский университет "МЭИ", 111250, Россия, г. Москва, Красноказарменная улица, дом 14, e-mail: universe@mpei.ac.ru

Аннотация

В статье рассматривается проблема латерального перемещения злоумышленников в экосистемах интернета вещей (IoT) применительно к сегменту умного дома. В условиях стремительного роста количества подключенных устройств и отсутствия должной сегментации сети, компрометация одного небезопасного IoT-устройства зачастую становится для атакующего «точкой входа» для дальнейшего горизонтального распространения по сети. Анализируются векторы атак, используемые для эскалации привилегий и захвата критически важных узлов. Особое внимание уделяется методам обнаружения аномальной активности на сетевом уровне и пассивным стратегиям защиты, основанным на микросегментации и применении принципа нулевого доверия.

Ключевые слова: латеральное перемещение, интернет вещей, умный дом, сегментация сети, нулевое доверие, безопасность IoT, эскалация привилегий, ботнеты, микросегментация, сетевая аномалия.

LATERAL MOVEMENT IN SMART HOME INFRASTRUCTURE

Agureev Ivan Aleksandrovich,
senior lecturer of the Department of Security and Information Technologies, National Research University "MPEI", 111250, Russia, Moscow, Krasnokazarmennaya street, building 14, e-mail: universe@mpei.ac.ru

Gorlenko Artur Romanovich,
student of the Department of Security and Information Technologies, National Research University "MPEI", 111250, Russia, Moscow, Krasnokazarmennaya street, building 14, e-mail: universe@mpei.ac.ru

ABSTRACT

This article examines the problem of lateral movement by attackers in Internet of Things (IoT) ecosystems, specifically within the smart home segment. Given the rapid growth in the

number of connected devices and the lack of proper network segmentation, the compromise of a single insecure IoT device often becomes an entry point for attackers to spread horizontally across the network. The study analyzes attack vectors used for privilege escalation and the takeover of critical nodes. Special attention is paid to methods for detecting anomalous activity at the network level and passive defense strategies based on micro-segmentation and the Zero Trust principle.

Keywords: lateral movement, internet of things, smart home, network segmentation, Zero Trust, IoT security, privilege escalation, botnets, micro-segmentation, network anomaly.

1. Методы и модели латерального перемещения в IoT-сетях

Концепция умного дома (Smart Home) неразрывно связана с повсеместным внедрением устройств интернета вещей (IoT). По данным аналитических агентств, количество активных IoT-устройств в домохозяйствах к 2026 году превышает десятки миллиардов единиц [1]. Однако гонка за функциональностью и временем вывода продукта на рынок привела к критическому отставанию в области безопасности. Многие производители рассматривают IoT-устройства как «расходный материал», не обеспечивая долгосрочную поддержку и обновления прошивок. В то время как основное внимание исследователей безопасности традиционно сосредоточено на предотвращении первоначального взлома (Initial Compromise), реальную угрозу представляет вторичный этап атаки — латеральное перемещение (lateral movement). Этот термин, пришедший из корпоративной кибербезопасности, описывает процесс, при котором злоумышленник, получив контроль над малозначимым узлом сети, перемещается по горизонтали для захвата более ценных активов [2]. В контексте умного дома это означает превращение взломанной «умной лампочки» или «розетки» в трамплин для атаки на персональные компьютеры, мобильные устройства и хранилища данных пользователя. Цель данной работы — классифицировать методы латерального перемещения в гетерогенных сетях умного дома, выявить критические уязвимости архитектуры и предложить эффективные методы защиты, учитывающие специфику IoT.

Латеральное перемещение в среде умного дома отличается от классических корпоративных сетей высокой гетерогенностью устройств и повсеместным использованием облачных протоколов. Процесс можно разделить на три этапа: разведка, эскалация привилегий и непосредственно перемещение.

После компрометации IoT-устройства (например, через уязвимость в веб-интерфейсе или подбор стандартного пароля) атакующий проводит разведку. На зараженном устройстве запускаются скрипты для сканирования локальной подсети (обычно диапазонов 192.168.x.x или 10.x.x.x). В отличие от корпоративных сред, в умном доме часто отсутствуют системы обнаружения вторжений (IDS), что делает такое сканирование незаметным. Инструментарием выступают встроенные утилиты BusyBox (ping, arp-scan) или легковесные бинарные файлы, загружаемые через wget [3]. Умные устройства редко содержат ценную информацию сами по себе, но они могут выступать прокси для атак на роутер или другие узлы. Типичные методы:

1) ARP Spoofing — взломанное устройство отправляет поддельные ARP-ответы, становясь «человеком посередине» (MITM) между смартфоном пользователя и шлюзом. Это позволяет перехватывать сессионные файлы (cookies), пароли от облачных сервисов и трафик приложений управления умным домом. (рис.1)

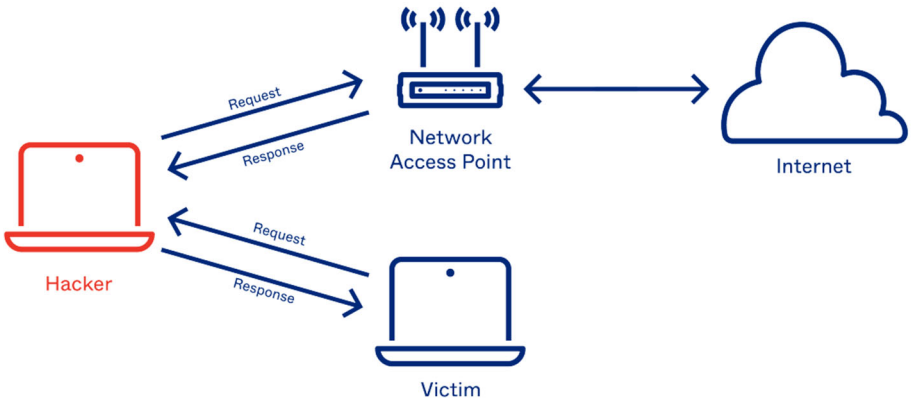

Рис.1. Атака вида ARP-spoofing[6]

2) DNS Spoofing — изменение таблиц DNS на взломанном роутере или через атаки на протокол DHCP перенаправляет трафик обновлений прошивок других устройств на серверы атакующего, что позволяет распространять вредоносное ПО [4]. (рис.2)

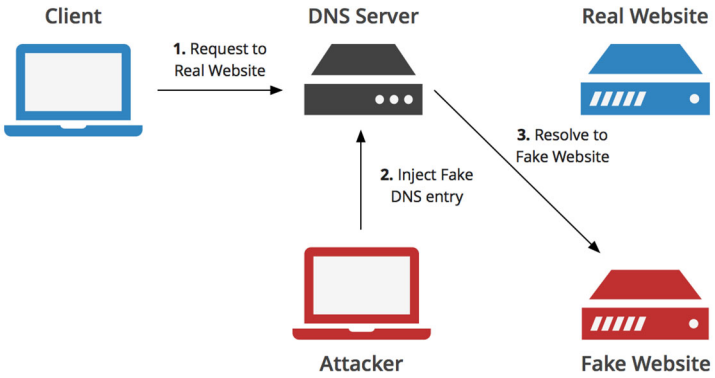

Рис.2. Атака DNS-spoofing[7]

3) Эксплойты доверия. Многие экосистемы умного дома (Xiaomi, Yandex, Apple HomeKit) используют модель доверенного моста. (рис.3) Если хаб (шлюз) скомпрометирован, он может транслировать вредоносные команды на все подчиненные устройства, включая замки и системы сигнализации.

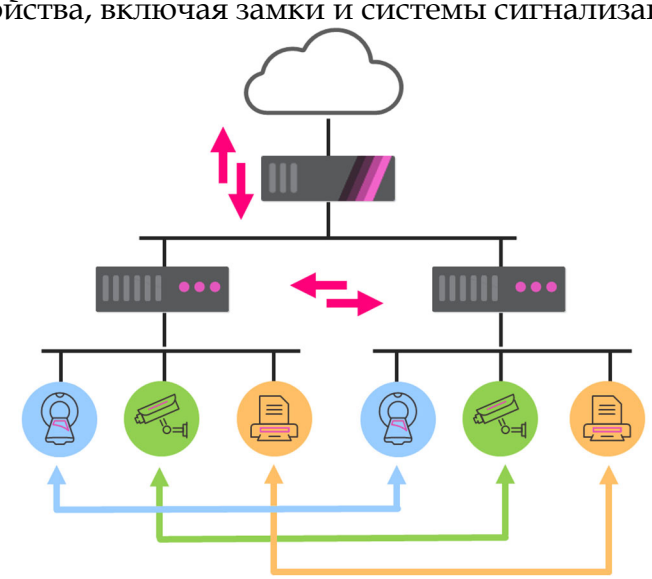

Рис.3. Связь между компонентами умного дома[8]

Конечной целью является захват устройств, хранящих персональные данные или обеспечивающих физическую безопасность. Наиболее привлекательными целями для латерального перемещения являются:

1) Сетевые хранилища (NAS), так как устройства QNAP, Synology или самодельные серверы часто монтируются как сетевые диски. Используя украденные учетные данные (например, через кейлоггер на скомпрометированной клавиатуре или перехват трафика SMB), атакующий запускает вымогательское ПО (ransomware) на NAS, шифруя многолетние архивы фотографий.

2) Роутеры, захват маршрутизатора позволяет установить постоянное присутствие, перенастроить VPN для скрытого доступа или изменить настройки брандмауэра для маскировки трафика.

3) Через смартфоны, используя уязвимости в протоколах синхронизации (например, широко используемый MQTT без TLS), атакующий может получить push-уведомления, геолокацию или использовать телефон как часть ботнета.

2. Результаты анализа реальных инцидентов

Анализ отчетов лабораторий кибербезопасности (включая Kaspersky Lab, Unit 42 от Palo Alto Networks) [5][9] за 2023–2025 гг. позволяет выделить несколько характерных сценариев.

1) Если ранее ботнеты (например, Mirai, Mozi) использовались исключительно для DDoS-атак, то современные модификации содержат модули для латерального перемещения. В 2025 году зафиксированы случаи, когда модифицированный ботнет Mozi не просто сканировал порт 23 (Telnet), но после заражения маршрутизатора запускал сканер портов 445 (SMB) и 3389 (RDP) для заражения ПК внутри сети [5].

2) Уязвимость протокола UPnP. Тестирование 15 популярных моделей роутеров, используемых в сегменте умного дома, показало, что 80% из них имеют включенный UPnP по умолчанию. Скомпрометированное IoT-устройство может использовать UPnP для автоматического проброса портов, открывая внешний доступ к критическим узлам сети, которые ранее были защищены NAT.

3) Антивирусное ПО, установленное на ПК, не способно детектировать латеральное перемещение на уровне сети, если атака исходит изнутри доверенного периметра. В тестовых сценариях взломанная IP-камера успешно проводила атаку Pass-the-Hash для доступа к файловому серверу, оставаясь незамеченной для средств защиты конечных точек (EDR), так как трафик считался внутренним и легитимным.

3. Методы защиты

Традиционная периметральная модель защиты оказывается несостоятельной перед угрозой латерального перемещения, так как атакующий действует изнутри. Для эффективного противодействия требуется пересмотр архитектуры сети умного дома. Основополагающим методом защиты является сегментация сети. Все IoT-устройства должны быть изолированы в отдельную виртуальную локальную сеть (VLAN) или гостевую Wi-Fi сеть. На сетевом оборудовании (роутерах с поддержкой VLAN, например, Keenetic, MikroTik, AsusWRT) настраивается правило брандмауэра, запрещающее IoT-сегменту инициировать соединения с основной сетью (Trusted Zone), но разрешающее отвечать на уже установленные соединения. Даже при полной компрометации умной розетки, атакующий теряет возможность сканировать порты ПК или NAS, так как пакеты отбрасываются на уровне ядра роутера.

Концепция нулевого доверия (Zero Trust) предполагает, что ни одно устройство в сети не является доверенным по умолчанию. Применительно к умному дому это выражается в запрете межсетевого взаимодействия устройств одного сегмента. Также это выражается в использовании шлюзов прикладного уровня. Например, управление устройствами Zigbee/Z-Wave должно проходить через локальный хаб (Home Assistant, Hubitat), который имеет ограниченный белый список разрешенных внешних соединений, а не прямое облачное управление каждым чипом ESP8266.

Пассивный мониторинг сетевого трафика позволяет выявить латеральное перемещение на ранней стадии. Любое IoT-устройство, отправляющее ARP-запросы на всю подсеть (ARP-sweep), должно вызывать подозрение, умные устройства не должны генерировать SSH-трафик или пытаться подключиться к SMB. Решения на базе DNS-фильтрация в связке с системой обнаружения вторжений (Suricata или Snort), настроенной на анализ трафика зеркалируемого порта, позволяют автоматически блокировать подозрительную активность. Использование облачных протоколов производителей увеличивает поверхность атаки. Переход на локальные брокеры сообщений (например, Mosquitto MQTT с TLS-аутентификацией) и системы автоматизации без постоянного доступа в интернет (локальные хабы) сокращает количество узлов, через которые возможно латеральное перемещение.

Заключение

Латеральное перемещение в инфраструктуре умного дома представляет собой эволюционирующую угрозу, которая переводит взлом малозначимых IoT-устройств из разряда проблем конфиденциальности в разряд катастрофических инцидентов с потерей данных, финансовым ущербом и угрозой физической безопасности.

Исследование показывает, что подавляющее большинство домохозяйств уязвимы перед данной угрозой из-за отсутствия сетевой сегментации и слепого доверия к внутреннему трафику. Предложенные методы защиты, базирующиеся на микросегментации (VLAN), применении принципов Zero Trust и внедрении пассивного мониторинга аномалий, позволяют создать архитектуру, при которой компрометация одного устройства не влечет за собой падение всего цифрового периметра.

Дальнейшие исследования в этой области должны быть направлены на разработку автоматизированных инструментов для массового потребителя, которые могли бы реализовывать политики микросегментации без глубоких технических знаний, а также на законодательное стимулирование производителей IoT к внедрению безопасных практик разработки.

Список литературы:

1. Statista Research Department. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2030 // Statista. 2025. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (дата обращения: 20.03.2026).
2. Strom B. E. Adversary Tactics, Techniques, and Common Knowledge (ATT&CK) // The MITRE Corporation. 2018. URL: https://attack.mitre.org/tactics/TA0008/ (дата обращения: 20.03.2026).
3. Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., … Javed M. Understanding the Mirai botnet // 26th USENIX Security Symposium. 2017. P. 1093–1110.
4. Kolias C., Kambourakis G., Stavrou A., Voas J. DDoS in the IoT: Mirai and other botnets // Computer. 2017. Vol. 50, No. 7. P. 80–84. DOI: 10.1109/MC.2017.201
5. Unit 42, Palo Alto Networks. Global Incident Response Report 2025 // Palo Alto Networks. 2025. URL: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report-2025 (дата обращения: 20.03.2026).
6. ARP Poisoning // Okta. URL: https://www.okta.com/ko-kr/identity-101/arp-poisoning/ (дата обращения: 20.03.2026).
7. DNS Spoofing // KeyCDN. URL: https://www.keycdn.com/support/dns-spoofing/ (дата обращения: 20.03.2026).

8. Check Point. IoT Protect. URL: https://www.checkpoint.com/ru/quantum/iot-protect/ (дата обращения: 20.03.2026).
9. White papers // Kaspersky. URL: https://www.kaspersky.ru/enterprise-security/resources/white-papers (дата обращения: 20.03.2026).

References:

1. Statista Research Department. Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2030 // Statista. 2025. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed: March 20, 2026).
2. Strom, B. E., Adversary Tactics, Techniques, and Common Knowledge (ATT&CK) // The MITRE Corporation. 2018. URL: https://attack.mitre.org/tactics/TA0008/ (accessed: March 20, 2026).
3. Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., ... Javed M. Understanding the Mirai botnet // 26th USENIX Security Symposium. 2017. P. 1093–1110.
4. Kolias C., Kambourakis G., Stavrou A., Voas J. DDoS in the IoT: Mirai and other botnets // Computer. 2017. Vol. 50, No. 7. P. 80–84. DOI: 10.1109/MC.2017.201
5. Unit 42, Palo Alto Networks. Global Incident Response Report 2025 // Palo Alto Networks. 2025. URL: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report-2025 (accessed on March 20, 2026).
6. ARP Poisoning // Okta. URL: https://www.okta.com/ko-kr/identity-101/arp-poisoning/ (accessed on March 20, 2026).
7. DNS Spoofing // KeyCDN. URL: https://www.keycdn.com/support/dns-spoofing/ (accessed on March 20, 2026).
8. Check Point. IoT Protect. URL: https://www.checkpoint.com/ru/quantum/iot-protect/ (accessed on March 20, 2026).
9. White papers // Kaspersky. URL: https://www.kaspersky.ru/enterprise-security/resources/white-papers (accessed: 20.03.2026).