УДК 004.056.2

А. В. Кропова[1], И. Ю. Коркин[2]*

Исследование вопросов безопасности технологии ALPC в условиях атак с использованием драйверов Windows

[1] Национальный исследовательский ядерный университет МИФИ, г. Москва, Российская Федерация
[2] Независимый исследователь, г. Москва, Российская Федерация
* e-mail: kropovaanastasiia@gmail.com

Аннотация. Целью настоящего исследования является оценка возможности реализации атаки на ALPC-соединение в операционной системе Windows через ядро без закрытия соединения скрытно для программ и операционной системы и предложение метода защиты от атак данного типа. Технология асинхронного локального вызова процедур (англ. ALPC, Asynchronous Local Procedure Call) используется в различных системах защиты информации Windows, в том числе в антивирусных системах (англ. AV, Antivirus) и новых системах обнаружения (англ. EDR, Endpoint Detection and Response). Для сокрытия вредоносного программного обеспечения злоумышленникам требуется нарушить работу средств AV, EDR, чего, в свою очередь, можно достичь путем деструктивного воздействия на компоненты технологии ALPC. Примеры подобных атак уже существуют и освещены в данной работе. Для противодействия таким новым угрозам необходимо опережающее совершенствование систем защиты информации, поэтому было проведено исследование вопросов безопасности ALPC. Рассматривался наиболее сложный случай атаки с использованием драйверов Windows. Были проведены три атаки на ALPC-соединение, основанные на изменении структур ALPC в памяти ядра, что привело к созданию нелегитимных подключений в системе и нарушению работы корректных соединений. Было разработано средство защиты ALPChecker, которое будет представлено в последующих статьях.

Ключевые слова: ALPC-соединение, драйвер ядра, дескриптор процесса, ALPC-порт, клиент, сервер

A. V. Kropova[1], I. Y. Korkin[2]*

Investigation of ALPC technology security issues in the context of attacks using Windows drivers

[1] National Research Nuclear University MEPhI, Moscow, Russian Federation
[2] Independent researcher, Moscow, Russian Federation
* e-mail: kropovaanastasiia@gmail.com

Abstract. The purpose of this study is to evaluate the possibility of implementing an attack on ALPC connection in the Windows operating system through the kernel without closing the connection covertly from programs and the operating system and to propose a method of protection against this type of attacks. Asynchronous Local Procedure Call technology (ALPC) is used in various Windows information protection systems, including antivirus systems (AV) and Endpoint Detection and Response systems (EDR). To ensure the concealment of malicious software, attackers need to disrupt the operation of AV, EDR tools, which in turn can be achieved by destructive impact on the components of the ALPC technology. Examples of such attacks already exist and are covered in this paper. To counteract such new threats, it is necessary to advance the improvement of information security systems thus the ALPC security research was conducted. The most difficult case, Windows

kernel driver attack, was considered. Three attacks on the ALPC connection were carried out, based on changing the ALPC structures in the kernel memory, which led to creation of illegitimate connections in the system and the disruption of correct connections. ALPChecker protection tool has been developed. The tool will be presented in subsequent articles.

Keywords: ALPC connection, kernel driver, process handle, ALPC port, client, server

Введение

Актуальность проблемы обеспечения информационной безопасности с каждым годом непрерывно возрастает [1]. Наблюдается постоянное увеличение зарегистрированных киберпреступлений в России и в мире [2].

Среди множества атак на операционную систему Windows можно выделить как особый вектор атаки, проводимые с использованием драйверов ядра. В последние годы наблюдается значительный рост кибератак данного типа. Драйверы Windows работают в одном адресном пространстве с ядром операционной системы и имеют неограниченный доступ к ее данным. Внедрение вредоносного драйвера в систему представляет опасность обхода или отключения злоумышленником средств защиты Windows, вследствие чего система становится уязвимой для всякого вида атак.

С целью защиты Windows от вредоносных драйверов были созданы такие механизмы, как «Проверка подписи драйвера» (англ. DSE, Driver Signature Enforcement), запрещающий загрузку вредоносных драйверов, «Защита ядра от исправлений» (англ. KPP, Kernel Patch Protection, PatchGuard) в Windows 8.1 и функция «MmProtectDriverSection» в Windows 11, которые защищают механизм «Проверки подписи драйвера» от изменения переменной системы «nt!g_CiEnabled» и отключения [3]. Для обхода этих механизмов злоумышленники стали использовать официальные, подписанные Microsoft драйвера с известными уязвимостями, внедряя в них файлы, предназначающиеся для атакуемой системы. Данная техника получила название «Принеси свой уязвимый драйвер» (англ. BYOVD, Bring Your Own Vulnerable Driver) [4].

За последние несколько лет было проведено значительное количество исследований в данной области. В результате были выявлены десятки уязвимостей в официальных драйверах Microsoft [5-8]. Полный анализ более чем шестидесяти низкоуровневых угроз Windows приведен в исследовании TrendMicro [9]. Проиллюстрированы адаптация злоумышленников к появлению механизмов защиты и совершенствование их техник. В работах [10-11] приведены примеры использования злоумышленниками уязвимостей для внедрения собственных драйверов и проведения атак на операционную систему Windows.

В настоящее время набирают популярность атаки на антивирусные программы (англ. AV, Antivirus) и системы обнаружения и реагирования на угрозы конечной точки (англ. EDR, Endpoint Detection and Response). Один из векторов таких атак направлен на технологию ALPC, которая повсеместно используется в AV\EDR.

Механизм клиент-серверного взаимодействия Асинхронный локальный вызов процедур (англ. ALPC, Asynchronous Local Procedure Call) применяется по-

всеместно благодаря своей масштабируемости, высокой скорости работы и возможности отправлять сообщения любой длины [12]. Технология ALPC применяется при каждом запуске процесса или потока Windows и во время любой операции подсистемы Windows для связи с процессом подсистемы CSRSS, для каждой итерации с объектом объектной модели компонентов (англ. COM, Component Object Model) для совместного использования объектов и функций внутри процесса и за его пределами. Даже простая программа на Windows будет иметь ALPC-соединение хотя бы с одним процессом [13].

На конференции по информационной безопасности LABScon 2022 [14] и Ekoparty 2022 [15] исследователи из команды Binarly A. Matrosov и C. Teodorescu обратили внимание на новый тип уязвимостей, позволяющий отключить Инструмент управления Windows (англ. WMI, Windows Management Instrumentation), не вызывая предупреждений безопасности без срабатывания систем защиты информации типа PatchGuard.

Инструмент управления Windows взаимодействует с провайдерами, клиентами и процессом services.exe через механизм ALPC. На конференции были представлены две возможные атаки на ALPC-взаимодействие. Вследствие первой атаки был закрыт дескриптор ALPC-порта связи клиента. WMI-клиент потерял соединение и перестал получать сообщения о событиях. Вследствие второй атаки был закрыт дескриптор ALPC-порта сервера, вследствие чего сервис WMI потерял соединение со всеми своими клиентами.

Таким образом, актуальность данного исследования обусловлена уязвимостью Windows для атак со стороны драйверов ядра и, в частности, уязвимостью механизма ALPC.

Анализ основных структур

Первичные компоненты ALPC-взаимодействия — ALPC-порты. ALPC-порты бывают трех различных видов (рис. 1):

– клиентский порт связи (англ. Client Communication Port) — порт, который клиентский процесс использует для связи с сервером, неименованный порт;

– серверный порт связи (англ. Server Communication Port) — порт, который сервер использует для связи с клиентом, неименованный порт. У сервера имеется по одному порту связи для каждого его активного клиента;

– порт подключения к серверу (англ. Server Connection Port) — порт, который указывается в запросе на подключение к серверу, это именованный порт. Подключаясь к этому порту, клиенты могут подключаются к серверу.

С целью изучения структур ALPC в памяти ядра использовался многофункциональный отладчик для Windows WinDBG, подключенный к виртуальной машине Windows 10, созданной с помощью инструмента виртуализации VirtualBox. С помощью команды «dt» отладчика была изучена основная структура ALPC-взаимодействия – ALPC_PORT (рис. 2).

Данная структура содержит набор полей с полной информацией обо всех объектах этого взаимодействия: списке портов (PortListEntry), порте на другом конце (CommunicationInfo), очередях сообщений (MainQueue, PendingQueue, WaitQueue,

CanceledQueue, LargeMessageQueue), необработанной длине сообщений различных очередей (MainQueueLength, PendingQueueLength, LargeMessageQueueLength), процессе-владельце данного (OwnerProcess). Наибольший интерес для нашего исследования представляет поле CommunicationInfo, находящееся по адресу ALPC-порта со смещением +0x010. Данное поле представляет собой структуру ALPC_COMMUNICATION_INFO и несет информацию о подключениях данного ALPC-порта. Схематичное изображение структуры ALPC_COMMUNICATION_INFO также представлено на рис. 2.

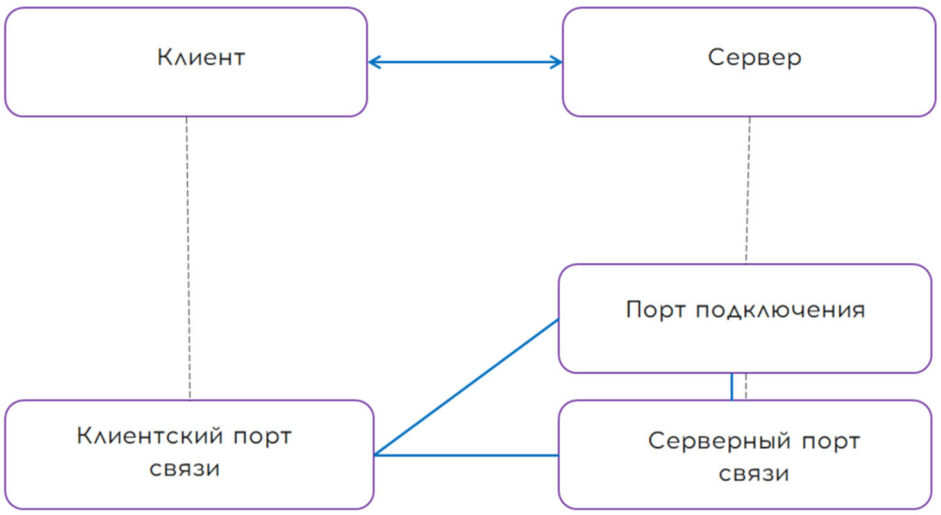

Рис. 1. Схема ALPC-соединения

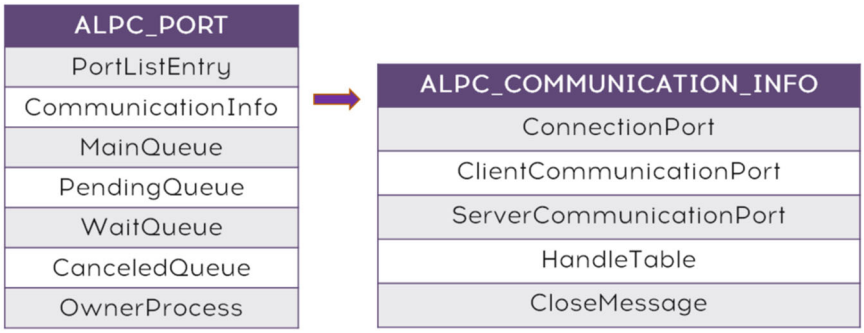

Рис. 2. Структура ALPC_PORT

В структуре присутствуют поля ConnectionPort — адрес порта подключения, ServerCommunicationPort — адрес серверного порта связи и ClientCommunicationPort — адрес клиентского порта связи. Ниже находится указатель на таблицу дескрипторов подключения — HandleTable и сообщение закрытия соединения — CloseMessage.

На основе полученных данных можно сделать предположения о возможных векторах атак на структуры ALPC. ALPC-взаимодействие может быть атаковано

через драйверы ядра. Основная информация о взаимодействующих ALPC-структурах хранится в поле CommunicationInfo структуры ALPC-порт. Модификация данных в этой структуре может привести к изменению объектов взаимодействия или прекращению его. Атака на ALPC-взаимодействие может быть направлена как на клиент и его порт связи, так и на сервер и его порты связи и подключения.

Результаты

В разделе представлены экспериментальные данные, полученные в ходе исследования. В целях проведения исследования был собран стенд, состоящий из приложений клиент К1 и сервер С1, взаимодействующих по ALPC и клиент К2 и сервер С2, взаимодействующих по ALPC. Было проведено три атаки на ALPC-соединение через ядро.

Первая атака (атака №1) проводилась путем изменения порта клиента. Атака привела к несанкционированному подключению клиента К2 к серверу С1 и потери связи сервера С2 с клиентом К2. Атака заключалась в изменении значения ConnectionPort в структуре CommunicationInfo клиентского порта связи клиента К2 на адрес структуры порта подключения ConnectionPort С1.

Вторая атака (атака №2) состояла в изменении структуры порта сервера. Результатом также стали несанкционированное подключение клиента К2 к серверу С1 и потеря соединения сервера С2 с клиентом К2. Атака заключалась в модификации поля ConnectionPort структуры CommunicationInfo в структуре серверного порта связи С1.

Третья атака (атака №3) проводилась путем изменения структуры порта клиента с завершением сервера. Итогом атаки стало несанкционированное подключение клиента К2 к серверу С1; данное подключение было восстановлено в результате повторной модификации структуры порта после завершения сервера С2, что позволяет обеспечить дополнительный уровень скрытности атаки. Данная атака проводилась в три шага:

1) была совершена атака №1, и клиент К2 получил доступ к С1;

2) потерявший соединение сервер С2 был завершен, вследствие чего было потеряно установленное соединение К2-С1;

3) была произведена модификация значения ServerCommunicationPort в той же структуре CommunicationInfo клиентского порта связи на адрес серверного порта связи сервера С1, вследствие чего потерянное соединение было восстановлено.

Результаты проведенных атак представлены в табл. 1.

Предлагается новый метод детектирования атак на ALPC-соединение. Метод заключается в сборе данных обо всех структурах ALPC-портов и их связях друг с другом и поиске несоответствия в информации клиентских и серверных соединений в системе, которое будет являться индикатором атаки.

Таблица 1

Атаки на ALPC-соединение с использованием драйвера ядра

Атака №	Процессы, структуры которых были изменены	Изменяемые поля	Результат
1	Клиент К2	ClientCommunicationPort ->CommunicationInfo-> ConnectionPort	Установлено несанкционированное подключение клиента К2 к серверу С1, потеря связи сервера С2 с клиентом К2
2	Клиент К2	ServerCommunicationPort ->CommunicationInfo-> ConnectionPort	Установлено несанкционированное подключение клиента К2 к серверу С1, потеря связи сервера С2 с клиентом К2
3	Сервер С1	ClientCommunicationPort -> CommunicationInfo-> ConnectionPort, ClientCommunicationPort -> CommunicationInfo-> ServerCommunicationPort	Установлено несанкционированное подключение клиента К2 к серверу С1, после завершения С2 подключение восстановлено

Была написана программа на языке Python, в основе работы которой лежит предложенный метод. Данная программа была успешно опробована. Все три предложенные атаки были детектированы. Исходный ход программы можно увидеть на сайте github.com [16].

Заключение

В рамках данной работы были проведены исследования ALPC-взаимодействия, анализ его основных структур и их связи друг с другом. В целях проведения исследований был подготовлен тестовый стенд, состоящий из двух пар клиент-сервер, взаимодействующих по ALPC.

Удалось совершить три атаки на ALPC-взаимодействие, заключающиеся в динамической модификации структур ALPC-портов. Атаки были направлены на изменение структур портов связи клиента и сервера. В результате каждой атаки было создано несанкционированное ALPC-подключение, а одно из легитимных подключений было разорвано без каких-либо предупреждений безопасности в системе. Был предложен метод для детектирования атак на ALPC-соединение, и на основе него была написана программа, позволяющая детектировать атаки на ALPC-соединение. Программа была успешно опробована.

Таким образом, было доказано, что в настоящий момент операционная система Windows уязвима для нового подвида атак со стороны драйверов ядра

на механизм ALPC. Данная уязвимость представляет опасность обхода или отключения злоумышленником средств защиты Windows, что ведет к нарушению информационной безопасности операционной системы. Было разработано средство защиты ALPChecker, которое будет представлено в последующих публикациях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стрельцов А. С., Французова Г. А., Басыня Е. А. Разработка системы сбора, обработки, анализа, идентификации корреляции событий информационной инфраструктуры предприятия. // Системы анализа и обработки данных. – 2023. – № 1 (89). – С. 101–113.

2. Басыня, Е. А. Программная реализация и исследование системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия. // Вестник Самарского государственного технического университета. Серия: Технические науки. - 2020. - Т. 28, № 1 (65). - С. 6-21.

3. Pogonin, D., Korkin I. Microsoft Defender willbe defended: MemoryRanger prevents blinding Windows AV. [Электронный ресурс]. // The 15th Annual ADFSL Conference on Digital Forensics, Security and Law. — 2022. — URL: https://commons.erau.edu/cgi/viewcontent.cgi?article=1472&context=adfsl

4. MITRE. Exploitation for Privilege Escalation. [Электронный ресурс]. — 2021. — URL: https://attack.mitre.org/techniques/T1068

5. Poslušný, M. Signed kernel drivers – Unguarded gateway to Windows' core. [Электронный ресурс]. // ESET. — 2022. — URL: https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core

6. Iacob I., Ionita, I. M. The anatomy of Wiper Malware, Part 2: Third-Party Drivers. CrowdStrike. [Электронный ресурс]. — 2022. — URL: https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-2

7. Baines, J. Driver-Based Attacks: Past and Present. [Электронный ресурс]. — 2021. — URL: https://www.rapid7.com/blog/post/2021/12/13/driver-based-attacks-past-and-present/

8. Jesse M., Shkatov M. Get Off the Kernel if You Can't Drive. [Электронный ресурс]. // Eclypsium. — 2019. — URL: https://eclypsium.com/wp-content/uploads/2019/08/EXTERNAL-Get-off-the-kernel-if-you-cant-drive-DEFCON27.pdf

9. Magdy, S., Zohdy, M. An In-Depth Look at Windows Kernel Threats. [Электронный ресурс]. TrendMicro. — 2022. — URL: https://documents.trendmicro.com/assets/white_papers/wp-an-in-depth-look-at-windows-kernel-threats.pdf

10. Sanseo. Sliver Malware With BYOVD Distributed Through Sunlogin Vulnerability Exploitations. [Электронный ресурс]. // ASEC. — 2023. — URL: https://asec.ahnlab.com/en/47088/

11. Lechtik, M., Berdnikov, V., Legezo, D., Borisov, I. MoonBounce: the dark side of UEFI firmware. Kaspersky Lab. [Электронный ресурс]. — 2022. — URL: https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/

12. Allievi, A., Ionescu, A., Russinovich, M., Solomon, D. Windows Internals Parts 1 and 2. // Redmond, Washington: Microsoft Press. — 2021. — Vol. 7 — 209–237¬¬ p.

13. Ionescu, A. All About The Rpc, Lrpc, Alpc, And Lpc In Your Pc. // SyScan'14 Conference, Singapore. — 2014 — URL: http://www.securitytube.net/video/10182 (дата обращения: 03.03.2023).

14. Teodorescu, A. Matrosov и C. New Attacks to Disable abd Bypass Windows Management Instumentation. [Электронный ресурс]. // LABScon. — 2022. — URL: https://binarly.io/posts/New_Attacks_to_Disable_and_Bypass_Windows_Management_Instrumentation_LABSCon_Edition/index.html

15. Teodorescu, C., Korkin, I. Blinding Endpoint Security Solutions: WMI Attack Vectors. [Электронный ресурс]. // Ekoparty 2022. — 2022. — URL: https://binarly.io/events/Blinding_Endpoint_Security_Solutions_WMI_attack_vectors/index.html

16. Кропова А. ALPChecker. [Электронный ресурс]. — 2023. — URL: https://github.com/AnastasiKro/ALPChecker