Приложение 1

**Деятельность хакерских группировок**

1. Хакерской группировкой Core Werewolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с расширением «.exe», после запуска которого осуществляется демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для удаленного доступа «UltraVNC»;

фишинговые рассылки электронных писем, во вложениях которых содержится исполняемый файл с наименованием «Отсканированные\_документы\_371Выписка по противнику на доклад\_по\_08\_08\_командиру.pdf.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для удаленного доступа «UltraVNC»;

фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с наименованием «Спецификация 13\_Гидравлика.pdf.exe». После запуска пользователем указанного исполняемого файла осуществляется выполнение вредоносного скрипта и внедрение на целевую систему программного обеспечения для удаленного доступа «UltraVNC»;

фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с наименованием «Отсканированые документы по ВСЕ з-аключение по запросу на начальника.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа»;

фишинговые рассылки электронных писем от лица УФСБ России по Санкт-Петербургу и Ленинградской области. Во вложениях указанных писем прикреплен вредоносный исполняемый файл с наименованием «Уведомление №221 о начале комплексной проверки согласно плану утечек.exe». После открытия пользователем исполняемого файла осуществляется демонстрация документа приманки и внедрение вредоносного программного обеспечения типа «бэкдор».

2. Хакерской группировкой Fairy Wolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив. Архив содержит файл с наименованием «ИСХ № 215ОП-5 от 22.07.2025.hta», после запуска пользователем которого осуществляется выполнение вредоносного VBS-скрипта и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Unicorn);

фишинговые рассылки электронных писем, во вложениях которых содержится архив с наименованием «Исх 14-0554-4 от 09 06 2025 (уведомление о невыполнении соглашения).zip». Внутри архива находится файл с идентичным наименованием, но с расширением «.lnk», замаскированные под официальный документ. После запуска пользователем указанного файла осуществляется выполнение вредоносного скрипта и внедрение вредоносного программного обеспечения типа «стилер» (Unicorn);

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Исх С-41251-25 от 11 08 2025 Соглашение о конфиденциальной информации.zip». Архив содержит файл с аналогичным наименованием с расширением «.hta», после запуска пользователем которого осуществляется выполнение вредоносного скрипта, демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Unicorn Stealer);

фишинговые рассылки электронных писем с тематикой «Исходящий № 215ОП-19 от 25.08.2025». Во вложениях указанных писем прикреплен архив с наименованием «ИСХ № 215ОП-19 от 25.08.2025.hta». После запуска пользователем указанного файла осуществляется выполнение вредоносного скрипта и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Unicorn Stealer).

3. Хакерской группировкой Paper Werewolf осуществляются:

фишинговые рассылки электронных писем, внутри которых содержатся архивы с наименованиями «DON\_AVIA\_TRANS\_RU.rar» и «DON\_AVIA\_TRANS\_UZ.rar», содержащие файлы с расширениями «.pdf», «.txt», «.lnk» и исполняемый файл с расширением «.exe». После запуска пользователем указанных файлов осуществляется демонстрация документа-приманки и внедрение вредоносного программного обеспечения для получения несанкционированного доступа к целевой системе;

фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с наименованием «Резюме.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение вредоносного программного обеспечения типа «загрузчик»;

фишинговые рассылки электронных писем от лица Главного управления МВД России по г. Москва с тематикой «По вопросам миграции». Во вложениях указанных писем прикреплен файл с наименованием «187-2325.pdf», в тексте которого пользователю предлагается перейти по ссылке, указанной в документе. По ссылке доступна веб-страница, замаскированная под сайт системы электронного документооборота МВД России, на которой пользователю предлагается скачать архив документов. Архив содержит файлы-приманки (например, «Памятка работодателю.docx» и «Уведомление о прибытии иностранного гражданина или лица без гражданства в место пребывания.xls») и исполняемый файл с наименованием «182-1672143-01 (исполнитель Васнецовский М.Д).exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «загрузчик»;

при осуществлении целевых компьютерных атак применяется вредоносное программное обеспечение типа «загрузчик». Указанное программное обеспечение представляет собой исполняемый файл с наименованием «WinService.exe», после запуска которого осуществляется внедрение на целевую систему вредоносного программного обеспечения.

4. Хакерской группировкой Киберпартизаны осуществляется:

распространение вредоносного программного обеспечения типа «бэкдор» (Vasilek) и «фреймворк постэксплуатации» (Cobalt Strike), предназначенного для получения несанкционированного доступа к целевой системе и удаленного администрирования через API-запросы мессенджера «Telegram».

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» и «белым» спискам:

api[.]telegram[.]org; rossmoor[.]org; jrevk8g2o2ekbhz[.]okkgb[.]com; fjh33vgad02t[.]okkgb[.]com; okkgb[.]com; \*[.]vvv392pu0[.]rossmoor[.]org; \*[.]a2h3bi0[.]partspros[.]org; partspros[.]org; kdn[.]cdnkav[.]vip.

Обращаем внимание, что редактирование в активное состояние ссылок на вредоносное программное обеспечение и серверы управления злоумышленников, приведенных в настоящем письме, а также переход по данным ссылкам не допускается, так как создает предпосылки к распространению вредоносного программного обеспечения.

5. Хакерской группировкой Cloud Werewolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплены файлы с наименованиями «Счет\_a19af3ed-a30a-45a0b88d-6529f94398d4.pdf.lnk» и «Заявка\_количество на поставку корпусов АО АМЗ.pdf.lnk». После запуска пользователем указанных файлов осуществляется выполнение команд оболочки сценариев «PowerShell», демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (Goldbackdoor);

фишинговые рассылки электронных писем с тематиками «О деятельности Ростехнадзора Республика Татарстан», «О предоставлении информации». Во вложениях указанных писем находится вредоносный файл с наименованием «O deiatel’nosti Rostekhnadzora\_Respublika Tatarstan.doc» или «Соцпаспорт организации.doc». После открытия пользователем вложенного файла с удаленного ресурса скачивается RTF-файл, позволяющий эксплуатировать уязвимость пакета программ Microsoft Office, связанную с неправильной обработкой объектов в памяти (BDU:2018-00096, уровень опасности по CVSS 3.0 – высокий).

6. Хакерской группировкой Vengeful Wolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «1.zip». Архив содержит файл-приманку с наименованием «Бланк.doc» и исполняемый файл с наименованием «Акт сверки взаимных расчетов предприятия № 162 по состоянию на 1 августа 2025 года.exe» либо файл с наименованием «Акт сверки взаимных расчетов предприятия № 196 от 11 августа 2025 года.exe». После запуска пользователем указанного исполняемого файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Revenge RAT и Xworm).

7. Хакерской группировкой Monetary Wolf осуществляются:

с использованием системы электронного документооборота «Контур.Диадок» осуществляется распространение архива с наименованиями «DX2025.zip». Архив содержит вредоносный исполняемый файл, после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «червь» и «троян удаленного доступа» (Buhtrap), а также дальнейшее распространение вредоносного программного обеспечения в системах электронного документооборота.

8. Хакерской группировкой Rare Werewolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «технический акт № 173.2025.rar». Архив содержит исполняемый файл с наименованием «технический акт № 173.2025.scr», после запуска пользователем которого осуществляется внедрение на целевую систему программного обеспечения для удаленного доступа «AnyDesk»;

фишинговые рассылки электронных писем с тематикой «Приказ МО РФ №811 29.05.2025». Во вложениях указанных писем прикреплен архив с наименованием «Приказ ИО РФ №811.rar», внутри которого содержится исполняемый файл с наименованием «Приказ МО РФ №811.scr». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую систему программного обеспечения для удаленного доступа «AnyDesk»;

фишинговые рассылки электронных писем от лица органов государственной власти Донецкой Народной Республики. Во вложениях указанных писем прикреплен исполняемый файл, замаскированный по PDF-документ, после запуска пользователем которого осуществляется внедрение на целевую систему программного обеспечения для удаленного доступа «AnyDesk» и вредоносного программного обеспечения типа «майнек» (XMRig);

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Пакет документов по Дополнительному соглашению к Договору №513402-2025.rar», содержащий исполняемый файл с аналогичным наименованием с расширением «.scr» и файл-приманку с наименованием «Калькуляция.xlsx». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую систему программного обеспечения для удаленного доступа «AnyDesk».

9. Хакерскими группировками Team46 и TaxOff осуществляются:

фишинговые рассылки электронных писем, в тексте которых содержится вредоносная ссылка. После открытия пользователем указанной ссылки осуществляется загрузка и внедрение на целевую систему вредоносного программного обеспечения типов «загрузчик» (TaxOff и Team46 Loader) и «бэкдор» (TaxOff Trinper).

10. Хакерской группировкой Sapphire Werewolf осуществляются:

фишинговые рассылки электронных писем с тематикой «Служебная записка». Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованием «служебная записка.exe», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение вредоносного программного обеспечения типа «стилер» (AmethystStealer).

11. Хакерской группировкой Lone Wolf осуществляются:

фишинговые рассылки электронных писем с тематикой «Досудебная претензия». Во вложениях указанных писем прикреплен архив с наименованием «рекламация.rar», внутри которого содержатся вредоносные файлы с наименованиями «рекламация.pdf.lnk» и «рекламация.doc». После запуска пользователем указанных файлов осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «фреймворк постэксплуатации» (Cobalt Strike).

12. Хакерской группировкой PhantomCore осуществляются:

фишинговые рассылки электронных писем с тематикой «Транспортная накладная ТТН № 391-44 от 26.06.2025». Во вложениях указанных писем прикреплен архив с аналогичным наименованием с расширением «.zip», внутри которого содержится файл с расширением «.xls.lnk». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (PhantomRemote).

13. Хакерской группировкой Fluffy Wolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «akt\_sverka04082025\_1C\_PDF.com», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «стилер» (PureLogStealer) и «троян удаленного доступа» (PureHVNC).

14. Хакерской группировкой Scaly Wolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с наименованием «Акт сверки.pdf.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение вредоносного программного обеспечения типов «бэкдор» (Trojan.Updatar1) и «троян удаленного доступа» (Trojan.Updatar2 и Trojan.Updatar3).

15. Хакерской группировкой Kinsing осуществляются:

эксплуатация уязвимостей серверов и сервисов (например, Docker API), доступных из сети «Интернет», под управлением операционных систем Linux. После получения несанкционированного доступа к целевой системе злоумышленники осуществляют внедрение вредоносного программного обеспечения типа «майнер» (XMRig).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанной хакерской группировки, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» и «белым» спискам:

45[.]15[.]158[.]124; 45[.]137[.]155[.]55; 78[.]153[.]140[.]66; 78[.]153[.]140[.]96;

92[.]242[.]40[.]21; 178[.]20[.]40[.]200; 185[.]14[.]30[.]35; 193[.]178[.]170[.]47;

194[.]38[.]20[.]2; 194[.]38[.]20[.]32; 194[.]38[.]20[.]242; 194[.]38[.]21[.]25;

194[.]38[.]22[.]53; 213[.]209[.]143[.]44.

16. Хакерской группировкой Rainbow Hyena осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Задание на оценку №2046 от 05 августа 2025 года.zip». Архив содержит файл с аналогичным наименованием и с расширением «.pdf.lnk». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типов «загрузчик» (PhantomShell) и «бэкдор» (PhantomTaskShell и PhantomRemote);

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Заказ\_на\_ДПЭ\_225.zip», содержащий файл с аналогичным наименованием и расширением «.pdf.lnk». После запуска пользователем указанного файла осуществляется выполнение команд оболочки сценариев «PowerShell», демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (PhantomRemote);

фишинговые рассылки электронных писем, во вложениях которых прикреплены архивы с расширением «.zip», содержащие вредоносное программное обеспечение типа «троян» (PhantomPyramid), замаскированное под легитимные документы с использованием двойного расширения, например, «Akt priema peredachi [название организации].docx.lnk». После запуска пользователем указанного файла осуществляется получение несанкционированного доступа к целевой системе.

17. Хакерской группировкой Bloody Wolf осуществляются:

фишинговые рассылки электронных писем от лица Генеральной прокуратуры Кыргызской Республики. Во вложениях указанных писем прикреплен файл с расширением «.pdf», в тексте которого предлагается перейти по ссылке для ознакомления с делом. После открытия пользователем указанной ссылки осуществляется загрузка файла с расширением «.jar», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение на целевую систему программного обеспечения для удаленного доступа «NetSupport».

18. Хакерской группировкой Silent Werewolf осуществляются:

фишинговые рассылки электронных писем, во вложениях которых прикреплен вредоносный архив с наименованиями «запланированный визит.zip», «измерения.zip», «обновления сентябрь 2025.zip», содержащие вредоносный файл-ярлык с расширением «.lnk» и легитимный файл-приманку. После запуска пользователем указанного файла-ярлыка осуществляется получение несанкционированного доступа к целевой системе.

19. Хакерской группировкой NGC6061 осуществляются:

фишинговые рассылки электронных писем с тематиками «Заявка на интервью!!!», «РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ Система электронного документооборота Минпромторга России 2025!», «Роспотрбнадзор предупреждает о возможном распространении фейковых писем». Во вложениях указанных писем прикреплен архив с паролем, содержащий файл-ярлык с расширением «.lnk» и документ-приманку с наименованием «1.docx». После запуска пользователем указанного файла-ярлыка осуществляется загрузка и внедрение вредоносного программного обеспечения (Reverse Shell, Metasploit TCP Reverse).

20. Хакерской группировкой Warlock Group при осуществлении целевых компьютерных атак применяется вредоносное программное обеспечение типа «шифровальщик» (Warlock). Для получения первоначального доступа злоумышленники эксплуатируют следующие уязвимости: BDU:2025-08436 (уровень опасности по CVSS 3.1 – высокий), BDU:2025-08524 (уровень опасности по CVSS 3.1 – средний), BDU:2025-08714 (уровень опасности по CVSS 3.1 – критический) и BDU:2025-08787 (уровень опасности по CVSS 3.1 – высокий). В целях недопущения инцидентов безопасности, связанных с деятельностью указанной хакерской группировки, необходимо устранить эти уязвимости.

21. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры, осуществляются:

фишинговые рассылки электронных писем с тематикой «Внутренний запрос: Закупка товаров в странах СНГ.297411186.(4).pdf», во вложениях которых прикреплены архивы с наименованиями «297411186.7z», «297411186.gz», «297411186.rar» и «297411186.tar». Внутри архивов содержатся исполняемые файлы с расширениями «.exe». После запуска пользователем указанных исполняемых файлов осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (MetaStealer);

фишинговые рассылки электронных писем с тематикой «О проведении личного приема граждан список участников план и проведенная работа». Во вложениях указанных писем прикреплен архив с расширением «.rarя», внутри которого содержится исполняемый файл с наименованием «О проведении личного приема граждан список участников план и проведенная работа.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение вредоносного программного обеспечения для получения несанкционированного доступа к целевой системе;

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Требования.rar», содержащий файл с наименованием «Требования.lnk», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «фреймворк постэксплуатации» (Cobalt Strike);

фишинговые рассылки электронных писем с тематикой «Коммерческое предложение по инвестированию в МФО». В тексте указанных писем содержится ссылка, после открытия которого на целевую систему осуществляется загрузка исполняемого файла с наименованием «NexCall коммерческое предложение для рынка МФО России.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение вредоносного программного обеспечения типа «шифровальщик» (Pay2Key);

фишинговые рассылки электронных писем, внутри которых содержится архив с наименованием «Scan Doc INQ 7620124803 DGL 257382245.rar», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (AgentTesla);

фишинговые рассылки электронных писем, внутри которых содержится архив с наименованием «Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа.rar», содержащий исполняемый файл с наименованием «Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа.exe», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер»;

фишинговые рассылки электронных писем с тематикой «Заказной документ. N: 224/12028519303-1 от 05.08.25». Во вложениях указанных писем прикреплен архив, внутри которого содержится файл с расширением «.js». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (XWorm);

фишинговые рассылки электронных писем, во вложениях которых содержится архив с наименованием «Demand\_984175.zip». Архив содержит файл-приманку с наименованием «PASSWORD – 47692» и защищенный паролем архив с наименованием «Requirement.zip». Внутри архива содержится файл с наименованием «Requirement.wsf», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Efimer);

фишинговые рассылки электронных писем, внутри которых содержатся исполняемые файлы с расширением «.net», замаскированные под легитимные файлы программного обеспечения Microsoft Office. После запуска пользователем указанных файлов осуществляется внедрение на целевую систему программного обеспечения типа «загрузчик» (Steganography Loader);

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с расширением «.exe», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (KiwiStealer);

распространение вредоносного программного обеспечения типа «Бэкдор» (PipeMagic), замаскированного под обновление программного обеспечения (например, Google Chrome), предназначенного для работы в системах под управлением операционных систем Windows. Для предотвращения реализации угроз безопасности необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу aaaaabbbbbbb[.]eastus[.]cloudapp[.]azure[.]com, используя схему доступа по «черным» и «белым» спискам;

фишинговые рассылки электронных писем с тематикой «Служебная записка». Во вложениях указанных писем прикреплен архив с наименованием «Служебная записка от 12.08.2025.rar». Архив содержит исполняемый файл с аналогичным наименованием и расширением «.exe», после запуска пользователем которого осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа»;

фишинговые рассылки электронных писем с тематикой «Аппарат Правительства Российской Федерации по вопросу отнесения реализуемых на территории Сибирского федерального округа». Во вложениях указанных писем прикреплен архив с аналогичным наименованием и расширением «.rar», внутри которого содержится файл с расширением «.exe». После запуска пользователей указанного исполняемого файла осуществляется внедрение на целевую систему вредоносного программного обеспечения тип «троян удаленного доступа»;

при реализации компьютерных атак применение вредоносного программного обеспечения типа «бэкдор» (Vshell), предназначенного для получения несанкционированного доступа к целевой системе под управлением операционных систем Linux. Для предотвращения реализации данной угрозы необходимо обеспечить ограничение обращений к IP-адресу 47[.]98[.]194[.]60, используя схему доступа по «черным» или «белым» спискам;

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с наименованием «Прикрепленная копия платежа №06162025.rar», содержащий файл с аналогичным наименованием и расширением «.iso», после запуска пользователем которого осуществляется монтирование в системе образа диска. Образ содержит исполняемый файл с расширением «.exe», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (Phantom Stealer);

фишинговые рассылки электронных писем с тематикой «новая спецификация». Во вложениях указанных писем прикреплен архив, содержащий вредоносное программное обеспечение типа «загрузчик» (GuLoader). После запуска пользователем файлов из указанного архива осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Remcos RAT);

фишинговые рассылки электронных писем, во вложениях которых прикреплен архив с расширением «.rar», содержащий файл-приманку с наименованием «Aircrafts Pobeda.pdf» и вредоносный скрипт с наименованием «scan 26 08 2025.bat». После запуска пользователем указанного скрипта осуществляется получение несанкционированного доступа к целевой системе;

фишинговые рассылки электронных писем, замаскированных под отправку судебных документов. Во вложениях указанных писем находится вредоносный исполняемый файл с наименованием «Исковое заявление о взыскании убытков и морального вреда в связи с нарушением условий договора № 1234 от 28 августа.exe». После открытия пользователем указанного исполняемого файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (MarkerStealer);

фишинговые рассылки электронных писем, содержащих вредоносные архивы с расширением «.rar». После открытия пользователем файлов из архива осуществляется эксплуатация уязвимости файлового архиватора WinRAR, связанной с неверным ограничением имени пути к каталогу с ограниченным доступом (BDU:2025-09597, уровень опасности по CVSS 3.1 – высокий).