Рекомендации органам государственной власти Республики Дагестан по обработке электронных писем

С января 2022 года на официальные электронные адреса федеральных и региональных органов государственной власти Российской Федерации под видом официальных запросов из различных госорганов злоумышленники направляют электронные письма, содержащие запросы о предоставлении сведений, подробности которых изложены в прикрепленных архивах, содержащих вредоносное программное обеспечение (далее – ВПО), предназначенное для получения скрытого удаленного доступа к системе. В целях затруднения обнаружения антивирусными средствами ВПО упаковывается в архив, разбитый на две части, которые впоследствии также архивируются.

В целях нейтрализации выявленных угрозообразующих факторов органам исполнительной власти и органам местного самоуправления Республики Дагестан необходимо:

1. Использовать на всех объектах информационно-телекоммуникационной сети сертифицированные ФСБ России антивирусные средства с актуальными антивирусными базами.

2. Настроить на всех автоматизированных рабочих местах (далее – АРМ) периодическую (не реже 1 раза в месяц) полную антивирусную проверку системных и пользовательских каталогов операционной системы, а также полную (не реже 1 раза в месяц) антивирусную проверку всех несъемных носителей информации.

3. Настроить на всех АРМ процедуру принудительной антивирусной проверки подключаемых внешних носителей информации.

4. Организовать на сервере электронной почты антивирусную проверку всех входящих писем и периодическую проверку накопленной электронной корреспонденции, фильтрацию входящей электронной корреспонденции на предмет наличия спам сообщений, а также электронных писем, содержащих во вложении исполняемые файлы (.exe, .bat, .cpl, .dll, .jar, .msi, .scr и т.д.).

5. Проводить осмотр вложений электронных писем, поступающих на публичный (опубликованный в сети «Интернет») почтовый адрес организации, на выделенном АРМ с установленной на нем операционной системы семейства Linux и свободно распространяемым пакетом офисных программ. Целью указанных мероприятий является проверка вложенных электронных документов на предмет наличия ВПО, признаком которых может являться появление сообщений об ошибках в работе офисных программ при открытии вложенных электронных документов. В случае появления указанных сообщений об ошибках, необходимо удалять электронные письма, содержащие вложения, предположительно зараженные ВПО, и не открывать указанные вложения на других АРМ.

6. Осуществлять антивирусную проверку входящего веб-трафика, а также его фильтрацию с использованием контент-фильтров (сайтов развлекательного характера и сайтов социальных сетей, запрет посещения потенциально опасных сайтов, запрет загрузки исполняемых файлов).

7. Своевременно устанавливать критические обновления безопасности для прикладного программного обеспечения, в том числе офисных пакетов, средств просмотра PDF документов, интернет-браузеров, средств работы с Flash и Java приложениями.

8. Отключить в настройках офисных программ возможность работы со встроенными в документы макросами.

9. Осуществить настройку системы разграничения прав доступа в операционной системе с целью предоставления пользователям минимально необходимого перечня прав доступа (ограничить возможность установки программного обеспечения, создания файлов в системных директориях, запуска исполняемых файлов из пользовательских каталогов).

10. Заблокировать доставку писем от доменов-отправителей стран, поддержавших санкции Украины, США и стран Европейского союза.