**УПРАВЛЕНИЕ ОБРАЗОВАНИЯ
АДМИНИСТРАЦИИ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ЛЕНИНГРАДСКИЙ РАЙОН**

Кооперации ул., д. 183, ст-ца Ленинградская,
Краснодарский край, 353740
ОГРН 1022304293285 ИНН 2341008412
Тел.: 8(86145)3-64-47, факс 8(86145)3-65-76
uo@len.kubannet.ru

Руководителю ДОУ, ОО, УДО

на № _____от _____

Уважаемый руководитель!

Управление образования администрации муниципального образования Ленинградский район на основании информации, полученной от Управления ФСТЭК России по Южному и Северо-Кавказскому округу и департамента информатизации и связи Краснодарского края, сообщает о формировании угроз информационной безопасности, обусловленных деятельностью различных хакерских группировок, нацеленных на органы государственной власти Российской Федерации и организации.

1) Хакерскими группировками осуществляются фишинговые рассылки электронных писем, во вложениях которых находится вредоносный архив защищенный паролем. Внутри указанного архива содержатся файл с расширением «.data» и файл-ярлык с расширением «.lnk». После открытия пользователем файла-ярлыка осуществляется запуск эмулированной среды Linux с предварительно настроенным клиентом «Chisel» для подключения к удаленному серверу управления злоумышленников, который выполняет функции вредоносного программного обеспечения типа «бэкдор».

2) Хакерскими группировками осуществляется распространение вредоносного программного обеспечения типа «дроппер» (SteelFox), замаскированного под средства для активации программного обеспечения Foxit PDF Editor, продуктов JetBrains и AutoCAD. Указанное вредоносное программное обеспечение может использоваться для внедрения другого вредоносного программного обеспечения на целевую систему.

3) Хакерскими группировками осуществляется распространение вредоносного программного обеспечения типа «троян удаленного доступа» (GoblinRAT). После закрепления в системе указанное вредоносное программное обеспечение осуществляет маскировку под легитимные службы и программное обеспечение операционной системы Linux (например, zabbix, cron,

atop). Это позволяет злоумышленникам получить несанкционированный доступ к целевой системе.

4) Хакерскими группировками осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив. В архиве содержится файл-приманка с наименованием «blank-aktvzaimozacheta.doc», текстовый файл с наименованием «Важно.txt» и исполняемый файл с наименованием «Акт зачета взаимных требований между нашими организациями.exe». После открытия пользователем указанного исполняемого файла осуществляется демонстрация файла-приманки и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (Revenge RAT).

5) Хакерскими группировками осуществляются фишинговые рассылки электронных писем от лица АО «Сатурн». Во вложениях указанных писем содержится файл с расширением «.shtml», после открытия пользователем которого осуществляется выполнение вредоносного скрипта для загрузки и внедрения вредоносного программного обеспечения типа «троян удаленного доступа».

6) Хакерскими группировками осуществляются фишинговые рассылки электронных писем от лица известных компаний. Во вложениях указанных писем содержится фишинговая ссылка для скачивания архива, защищенного паролем. В архиве содержится файл-приманка, файл-библиотека с расширением «.dll» и исполняемый файл. После открытия пользователем указанного исполняемого файла осуществляется загрузка и внедрение вредоносного программного обеспечения типа «стилер» (Rhadamanthys).

7) Хакерской группировкой TeamTNT осуществляется распространение на сервисах Docker Swarm и Docker Hub экземпляров Docker, содержащих вредоносное программное обеспечение типа «бэкдор» (Sliver).

8) Хакерской группировкой Cloud Werewolf осуществляются фишинговые рассылки электронных писем, содержащих файлы, замаскированные под документы Microsoft Office. В одном случае злоумышленники рассылают документы от лица Федерального казначейства, в другом направляют документ с тематикой «Руководство по вопросам личной безопасности в офлайн и онлайн среде: для работников критически важной инфраструктуры». После открытия пользователем указанных файлов осуществляется загрузка и внедрение вредоносного программного обеспечения для получения несанкционированного доступа к целевой системе.

9) Хакерской группировкой Fluffy Wolf осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив с наименованием «oplata_1C_doc875622122.rar». Внутри архива содержится исполняемый файл, замаскированный под документ 1С, с наименованием «oplata_1C_doc875622122.com», после открытия, пользователем

которого осуществляется загрузка и внедрение вредоносного программного обеспечения типа «стилер» (PureLogs Stealer).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо принять следующие меры защиты:

- проводить проверку почтовых вложений с использованием средств антивирусной защиты;

– проверять имя домена отправителя электронного письма в целях идентификации отправителя. Для этого необходимо обращать внимание на наименование почтового адреса (домена), указанного после символа «@», и сопоставлять его с адресами (доменами) органов (организаций), с которыми осуществляется служебная переписка;

– открывать полученные почтовые вложения только от известных отправителей;

– не открывать и не загружать почтовые вложения писем с тематикой, не относящейся к рабочей деятельности.

Обращаем Ваше внимание на недопустимость использования личной электронной почты, а также мессенджеров и социальных сетей в служебных целях, передачи и обмена конфиденциальной информации, в том числе информации для служебного пользователя, без использования защищенных каналов связи или средств шифрования. Необходимо с осторожностью относиться к подозрительным сообщениям, звонкам и электронным письмам.

Напоминаем, что создан отдельный электронный почтовый адрес, на который сотрудники могут пересылать подозрительные письма, приходящие на Ваши рабочие почтовые ящики. Всю подозрительную корреспонденцию (ДО ЕЁ ОТКРЫТИЯ И СКАЧИВАНИЯ ПРИЛОЖЕННЫХ ФАЙЛОВ) можете пересылать на этот почтовый адрес (zi.lenbox@yandex.ru) с темой «На проверку» и дополнительно сообщить об этом сектору информатизации администрации муниципального образования Ленинградский район.

Исполняющий обязанности начальника управления образования

Подлинник электронного документа, подписанного электронной подписью, хранится в системе электронного документооборота администрации МО Ленинградский район Краснодарского края
Сертификат 2060FCB6A7071DCD5A5E90AEF7FB8913
Владелец **Петроченкова Людмила Петровна**
Действителен с 18.04.2024 по 12.07.2025

Л.П. Петроченкова

Никешина Алёна Александровна
8(86145)36576