МИНИСТЕРСТВО ВНУТРЕННЕЙ ПОЛИТИКИ, ИНФОРМАЦИИ И СВЯЗИ РЕСПУБЛИКИ КРЫМ

МІНІСТЕРСТВО ВНУТРІШНЬОЇ ПОЛІТИКИ, ІНФОРМАЦІЇ ТА ЗВ'ЯЗКУ РЕСПУБЛІКИ КРИМ

ҚЪЫРЫМ ДЖУМХУРИЕТИНИНЪ ИЧКИ СИЯСЕТИ, ИНФОРМАЦИЯ ВЕ АЛЯКЪА НАЗИРЛИГИ

ЗАМЕСТИТЕЛЬ МИНИСТРА

- начальник управления информатизации и развития информационных систем

Юр.адрес: пр-т. Кирова, 13, г. Симферополь, Республика Крым, 295005
Факт. адрес: ул. Козлова, 45А, г. Симферополь, Республика Крым, 295015,
тел.: (3652) 52-21-10, факс: (3652) 52-21-19
http://minfo.rk.gov.ru e-mail: delo@minfo.rk.gov.ru

От 16.05.2017 № 16/2408/01-17/2

На №

Исполнительные органы государственной власти Республики Крым

Органы местного самоуправления муниципальных образований в Республике Крым

В связи с распространением компьютерного вируса WannaCry, шифрующего данные на компьютерах в целях последующего требования выкупа для дешифровки, Министерство внутренней политики, информации и связи Республики Крым направляет рекомендации по противодействию заражению указанным вирусом автоматизированных рабочих мест.

Вирус распространяется посредством уязвимости в операционных системах или через электронную почту. В связи с чем, необходимо:

1. Сделать резервную копию важных файлов и сохранить их на энергонезависимом съемном носителе.
2. Для пользователей операционной системы Microsoft Windows установить обновление, размещенное по адресу: https://technet.microsoft.com/ru-ru/library/security/ms17-010.aspx.
3. Включить автоматическое обновление Windows и других программ, чтобы предотвратить заражение с помощью известных уязвимостей в будущем.
4. Заблокировать входящий трафик по SMB (порты 139, 445).
5. Использовать последнюю версию антивирусного программного обеспечения.
6. Быть внимательным при открытии писем, которые поступают посредством электронной почте. Потенциальную опасность представляют любые письма от незнакомых отправителей, содержащие подозрительные ссылки или файлы с такими расширениями, как .exe, .vbs, .scr. Кроме того,

мошенники могут использовать несколько расширений, чтобы замаскировать вредоносный файл (например, avi.exe или doc.scr). Также есть случаи заражения при скачивании файлов из сомнительных источников или при переходе по сомнительным ссылкам в информационно-телекоммуникационной сети "Интернет".

В случае заражения автоматизированного рабочего места данным вирусом, необходимо:

1. Отключить от локальной сети зараженное устройство с целью недопущения распространения вируса.
2. Если процесс шифрования уже начался, то рекомендуется физическое отключение (обесточивание) устройства «грубым» методом – без попыток корректного завершения работы. После этого необходимо изъять жесткий диск устройства и подключить в качестве вторичного носителя к другому компьютеру, не имеющему сетевого доступа. Далее можно скопировать с него незашифрованные файлы.
3. Если процесс шифрования завершен, можно попробовать восстановить резервные копии файлов, сделанные Windows.

В случае возникновения дополнительных вопросов, а также при необходимости оказания помощи в борьбе с вирусом, контактное лицо со стороны Министерства внутренней политики, информации и связи Республики Крым - главный специалист отдела развития информационных систем Бирюков Артем Аркадьевич (тел. 3652 522-114, e-mail: it@minfo.rk.gov.ru).

М. ЯКОВЛЕВ

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота Республики Крым.

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Кому выдан: **Яковлев Максим Павлович**
Кем выдан: 8F1DF6DE3658E8E5A5649324564489D6D5C17442
Действителен: с 30.06.2016 до 30.06.2017

Исп. Семенченко А. Н.
тел.: 7(365)252-21-15