МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЁЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ

Стасова ул., д. 180, г. Краснодар, 350075
Тел. (861) 235-10-36, факс (861) 231-16-80
ОКПО 00099412 ОГРН 1032307167056
ИНН 2308027802 КПП 231201001
e-mail: minobrkuban@krasnodar.ru
http://www.minobrkuban.ru

09.11.2017 № 47-22864/17-11

На № _____ от _____

Руководителям государственных учреждений, подведомственных министерству образования, науки и молодежной политики

Руководителям муниципальных органов управления образованием

Об угрозах информационной безопасности

Министерство образования, науки и молодежной политики Краснодарского края (далее – министерство) сообщает Вам, что с 24 октября 2017 года в Российской Федерации фиксируется активность программы шифровальщика «Bad Rabbit». Программа устанавливается путем загрузки поддельного обновления FlashPlayer.

В целях предупреждения угроз информационной безопасности в подведомственных организациях министерства, а также в органах управления образованием муниципальных образований, образовательных организациях Краснодарского края прошу реализовать мероприятия по предотвращению заражения, изложенных в приложении к данному письму.

Приложение: 1.Описание и базовые меры по противодействию вредоносному программному обеспечению «Bad Rabbit» на 3 л. в 1 экз.

Исполняющий обязанности министра К.А. Федоренко

Виталий Юрьевич Поляков
(861) 231-71-55

47-22864/17-11

ПРИЛОЖЕНИЕ
к письму министерства образования, науки и молодежной политики Краснодарского края
от 09.11.2017 № 47-22864/17-11

Описание
базовых мер по противодействию вредоносному программному обеспечению «Bad Rabbit»

Описание угрозы	24 октября зафиксирована эпидемия программы шифровальщика «Bad Rabbit». Программа устанавливается путем загрузки поддельного обновления FlashPlayer
На что направлена	Семейство операционных систем Microsoft Windows
Способ реализации	Программа-шифровальщик распространяется в виде поддельного обновления FlashPlayer. При переходе пользователем на модифицированный веб-сайт ему предлагается выполнять обновление FlashPlayer. При этом загрузка вредоносного ПО происходит с адреса http://ldnscontrol[.]com/flash install.php. После установки выполняется шифрование файлов и документов. Для расшифровки BadRabbit запрашивает оплату в Bitcoin. на TOR сайте caforssztxqzf2nm[.]onion. После установки программа создаст задание на запуск шифровальщика в планировщике заданий Windows, следующей командой: Cmd/c schtasks/Create/RU SYSTEM/SC ONSTART/TN rhaegal/TR “C:\Windows\system32\cmd.exe /C Start\”\” \”C:\Windows\dispci.exe\ ” -id 1082924949 && exit” Для запуска программа требует административных привилегий, поэтому использует встроенные средства получения учетной записи из кэша ОС (Mimikatz) и перебор по словарю.
Дата выявления публикации	25 октября 2017 года
Пазовые меры по противодействию	Для предотвращения шифрования, необходимо создать файл C:\windows\infpub.dat с правами «только для чтения». В таком случае, при заражении файлы не будут зашифрованы. Обновить MS Windows до актуальных версий. Обновить базы антивирусного программного обеспечения. Минимизировать привилегии пользователей на рабочих станциях. Обновить базы решающих правил для ViPNet IDS NS и ViPNct IDS HS.

	Не скачивать и не устанавливать файлы из неизвестных источников Не переходить по сторонним подозрительным ссылкам, в том числе, из социальных сетей и электронных писем, особенно если они исходят от неизвестных вам пользователей. Заблокировать запросы на: IP: 185.149.120[.]3 DNS: • ldnscontrol[.]com
Ссылки на источники	• caforssztxqzf2nm[.]onion На текущий момент известны следующие скомпрометированные ресурсы, которые предлагают загрузку вредоносного ПО: • http://argumentiru[.]com
	• http://www.fontanka[.]ru • http://grupovo[.]bg • http://www.sinematurk[.]com • http://www.aica.co[.]jp • http://spbvoditel[.]ru • http://argumenti[.]ru • http://www.mediaport[.]ua • http://blog.fontanka[.]ru • http://an-crimea[.]ru • http://www.t.ks[.]ua • http://most-dnepr[.]info • http://osvitaportal.com[.]ua • http://www.otbrana[.]com • http://calendar.fontanka[.]ru • http://www.grupovo[.]bg • http://www.pensionhotel[.]cz • http://www.online812[.]ru • http://www.imer[.]ro • http://novayagazeta.spb[.]ru • http://i24.com[.]ua • http://bg.pensionhotel[.]com • http://ankerch-crimea[.]ru Детектировать создание файлов: • infpub.dat:

	- SHA-1: 79116fe99f2b421c52cf64097f0f39b815b20907 • dispci.exe - SHA-1: afeee8b4acff87bc469a6f0364a81ae5d60a2add - SHA-1: 413eba3973a15c1a6429d9f170f3e8287f98c21c - SHA-1: 16605a4a29a101208457c47ebfde788487be788d • install_flash_player.exe - de5c8d858e6e41da715dca1c019df0bfb92d32c0 • • page-main.js - 4f61e154230a64902ae035434690bf2b96b4e018
Ссылки на источники	https://securingtomorrow.mcafee.com/mcafee-labs/badrabbit-ransomware-burrows-russia-ukraine/ https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/ https://securelist.com/bad-rabbit-ransomware/82851/
Прочая информация	Для выявления атаки BadRabbit могут быть использованы следующие индикаторы: - срабатывание сигнатур на IDS: Ам DNS Query for 1dnscontrol.com (sid: 3007646) AM DNS Query for ACA807##.ipt.aol.com - BadRabbit (sid: 3007647) AM TROJAN BadRabbit Flash Installer Download (sid: 3007648) - срабатывание сигнатур на ViPNet IDS HS: Запуск потенциально опасного ПО: mimikatz (sid: 121003) Вредоносный артефакт: mimikatz components (sid: 121117) mimikatz activity: попытка извлечения данных учетных записей (sid: 180000) mimikatz activity: попытка проведения pass-the-hash атаки (sid: 180001) mimikatz activity: попытка повышения привилегий (sid: 180002) Сигнатуры для IDS доступны: http://amonitoring.ru/article/detail.php?ELEMENT ID=211

Специалист-эксперт отдела
информатизации и информационной безопасности В.Ю. Поляков