Министерство образования и науки Ульяновской области

Областное государственное автономное учреждение «Институт развития образования»

432027, г.Ульяновск, ул. Р. Люксембург, д.48,
тел/факс (8422) 21-40-67

ОКПО 87759765, ОГРН 1107325002608,
ИНН 7325095777 КПП 732501001

11.05.2018 № 73-ИОГВ-01-10.01/634исх.

На № _____ от _____

О вредоносном ПО

Руководителям районных органов управления образованием

Уважаемые руководители!

Доводим до Вашего сведения, что в последнее время производится рассылка писем с вредоносным вложением в адрес государственных и муниципальных учреждений. Письма содержат архив с установочным файлом ПО Seldon 1.6 (легитимное программное обеспечение для поиска тендеров на различных электронных торговых площадках) с встроенным в него вредоносным программным обеспечением (далее - ВПО).

ВПО классифицируется как Trojan.Win32.Dllhijack.mt. Подробное описание прилагается. Прошу провести внеплановый инструктаж работников Вашего управления относительно правил антивирусной безопасности при работе в сети интернет, а также довести указанную информацию до образовательных организаций Вашего района. О фактах получения подобных сообщений, а также о признаках функциониирования данного ВПО, необходимо немедленно информировать отдел информатизации, технической политики и информационной безопасности ОГАУ «ИРО». Контакты: 21-42-63, admin@cit73.ru.

Директор М.Н.Алексеева

Афанасьев Сергей Викторович
(8422) 21-42-63

ПРИЛОЖЕНИЕ

Описание вредоносного программного обеспечения

Индикаторы вредоносной активности:
e-mail отправителя: info@rosatomgov.ru, ip-адрес отправителя: 193.41.79.124
SHA-256 файла: f116b6360951036814e9ce2a35fcdf467307d2c6
Темы рассылаемых писем: закупка №7794447567/18-21, исх: 22606; исх: 536851; 463432.
Наименования вложений:
«Отраслевая программа закупок ПАО РОСАТОМ (код 917815).rar»
«Отраслевая программа закупок ПАО РОСАТОМ.exe»
Порождаемый ВПО процесс: WinPrintSvc.exe – Remote Utilities – Host
ВПО обращается к доменному имени id.remoteutilities.com (IP: 108.163.130.184), порты 5655/tcp, 443/tcp
Отличительная особенность: в письме указан реальный номер телефона ГК «Росатом» +7 (495) 660-72-40.
Пример текста рассылаемых писем:
«Добрый день, Ваша компания выбрана в качестве поставщика для нужд ПАО «РОСАТОМ», в продолжение разговора с секретарем высылаю Вам запрос на предоставление необходимой документации и регистрации в единой отраслевой программе.
Индивидуальный код (пароль) для запуска программы закупок: 917815.
Информацию о закупке №7794447567/18-21 на сумму 97455909.00 руб на Ваше оборудование вы найдете в поиске отпраслевой программы закупок по номеру7794447567/18-21.»