Протокол самостоятельной работы

По Теории Защиты Информации

На тему: Вирусы

Выполнил студент К17.1

Шишелов Владимир

**Введение**

Компьютерный вирус – вид вредоносного программного обеспечение, которое нацелено на достижение разных целей, как правило, незаконных, как правило вымогание денег, уничтожение или кража важной информации и так далее.

В работе будет описано несколько выявленных вирусных атак проведенных на территории Румынии.

**Вирусные атаки на государственные структуры Румынии**

Атаки на больници.

По меньшей мере четыре больницы в Румынии в конце июня 2019 года пережили атаку вируса-вымогателя, которую, по данным спецслужб страны (Romanian Intelligence Service), провели китайские хакеры.

Как пишет портал Healthcare IT News со ссылкой на заявление разведывательного органа Румынии, предварительный анализ показал, что вредоносную программу мог остановить любой антивирус. Но, скорее всего, злоумышленники использовали метод социальной инженерии (обман пользователей), а не уязвимость компьютерных систем.  
По данным румынского центра по национальной кибербезопасности и реагированию на инциденты CERT-RO, медицинские учреждения были атакованы вирусами под названием Maoloa и Phobos.

Это подтвердили и ИБ-компании Cyberint и Bitdefender. Эксперты говорят, что Maoloa распространяется через электронные письма с зараженными вложенными файлами, а также хакерами, которые получили доступ к незащищённым виртуальным машинам, работающим в рамках Remote Desktop Protocol. После заражения системы Maoloa шифрует файлы, созданные с помощью пакета Office и OpenOffice, а также документы PDF, текстовые файлы, базы данных и мультимедийные файлы. Что касается Phobos, то он распространяется преимущественно вручную после взлома.  
Министр здравоохранения Румынии Сорина Пинтеа (Sorina Pintea) рассказала журналистам, что нападение хакеров парализовало работу больницы. В частности, начались проблемы с приёмом и выпиской пациентов. Она также напомнила, что подобные кибератаки на медицинские учреждения в стране уже случались: в 2017 году злоумышленникам заплатили выкуп в размере 10 тыс. евро за восстановление данных после заражения вредоносной программой компьютеров больницы в городе Сигету-Мармацией. В CERT-RO говорят, что компании не должны платить хакерам.

Атаки на органы правительства.

Румынская служба информации (РСИ - госбезопасность) сообщила в пятницу, что отразила попытку кибернетической атаки против румынского правительственного учреждения.

"Была выявлена попытка кибернетической атаки против румынского правительственного учреждения, проведенная вероятнее всего злоумышленниками, участвовавшими ранее в других инцидентах такого же типа, - указывается в сообщении. - Благодаря эффективному межведомственному сотрудничеству осуществление атаки и нанесение ущерба были предупреждены, а также были определены намеченные цели и методология атаки".

Румынская спецслужба утверждает, что "вероятнее всего попытка была предпринята организацией, ассоциированной с группировкой кибернетической преступности APT28/Fancy Bear". "РСИ действовала по сигналу НАТО и Службы внешней разведки (Румынии)", - отмечается в сообщении.

Местные СМИ уточняют, что в МИД Румынии было получено электронное письмо с вложением, содержавшим шпионскую программу, которая устанавливалась на компьютере получателя при открытии вложения.

**Масштабное применение CTB-Locker в Румынии**

CTB-Locker был одним из первых вирусов-вымогателей, управляемых и контролируемых через анонимную сеть Tor, которая позволяет злоумышленникам заметать следы.

По версии компании McAfee, разработчика одноименного антивирусного программного обеспечения, в 2016 году этот вирус-вымогатель стал самым распространенным. Вымогатели обычно делают спам-рассылки со счетами на оплату.

Когда файл открывают, то вирус заражает компьютер (под угрозой находятся прежде всего устройства на операционных системах Windows). Программа написана на основе исходного кода вируса CryptoLocker, некогда самого опасного вируса. Злоумышленников, стоявших за преступной схемой, обезвредили в июне 2014 года, однако к тому моменту им уже удалось выманить у потерпевших $27 млн.

**Вывод**

Иногда вирусы могут нанести непоправимый вред. Для избегания вреда требуется исключить метод социальной инженерии из арсенала злоумышленников методом проведения инструктажа среди персонала и выделить достаточный бюджет для привлечения компетентных специалистов отрасли ИБ и организации безопасности на объекте либо в сетевом пространстве.