Автор: Полина Чехова НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2978 27.06.2017, 13:54
1

Вирус Petya блокирует корпоративные сети в России и Украине

Похожий на WannaCry вирус-шифровальщик поражает компьютеры по всему миру. Известно о проблемах в энергетических компаниях России и Украины.

Что случилось?

Сети крупнейших энергетических компаний Украины — «Укрэнерго» и ДТЭК — оказались заражены неизвестным вирусом, сообщил TJournal.

Проблема затронула и Россию. Заблокированы компьютеры в нефтеперерабатывающих заводах «Башнефти», «Башнефть-добыче» и управлении «Башнефти».

О мощной хакерской атаке «Роснефть» также заявила в своем Twitter.

> На серверы Компании осуществлена мощная хакерская атака. Мы надеемся, что это никак не связано с текущими судебными процедурами.
>
> — ПАО «НК «Роснефть» (@RosneftRu) 27 июня 2017 г.

О заражении нескольких украинских коммерческих банков неизвестным вирусомсообщил Национальный банк Украины.

По данным «Лаборатории Касперского», число атакованных пользователей достигло 2 тысяч. Больше всего инцидентов было зафиксировано в России и Украине, также случаи заражения наблюдались в Польше, Италии, Великобритании, Германии, Франции, США и ряде других стран.

Везде один и тот же сценарий: компьютеры скачали неустановленное программное обеспечение и вывели на экран заставку, похожую на ту, что выводил вирус WannaCry.

За расшифровку данных вирус также, как и предшественник, требует выкуп в размере 300 биткоинов.

Что за вирус?

Речь идёт не об известном вирусе WannaCry, а о похожей по поведению вредоносной программе.

Компания «Новая почта», также ставшая жертвой кибератаки, заявила, что вирус называется Petya. По словам автора telegram-канала «Сайберсекьюрити» Александра Литреева, вирус является модификацией вируса Petya.A. Это вредоносная программа распространяется через ссылки в письмах и поражает жесткий диск. Как только кто-то нажимает на ссылку, заражение распространяется по внутренней сети предприятия.

эксперты из «Лаборатории Касперского» выяснили, что шифровальщик не принадлежит к уже известному семейству вымогателей Petya, хотя и имеет несколько общих с ним строк кода. По их данным, речь идет о новом семействе вредоносного программного обеспечения с существенно отличающейся от Petya функциональностью. «Лаборатория Касперского» назвала новый шифровальщик ExPetr.

Эксперты из «Лаборатории Касперского» выяснили, что шифровальщик не принадлежит к уже известному семейству вымогателей Petya, хотя и имеет несколько общих с ним строк кода. По их данным, речь идет о новом семействе вредоносного программного обеспечения с существенно отличающейся от Petya функциональностью. «Лаборатория Касперского» назвала новый шифровальщик ExPetr.

Эксперты установили, что для распространения в корпоративных сетях применялся модифицированный эксплоит EternalBlue и эксплоит EternalRomance. Эксплойт — это программа, использующая уязвимость в операционных система. EternalBlue использовали еще для распространения вируса WannaCry.

Источником атаки ExPetr стала украинская компания M.E.Doc, разрабатывающая системы отчетности и документооборота. Ее продукты популярны в Украине. M.E.Doc опровергает, что явилась источником заражения, и сообщает, что также пострадала от кибератаки.

Шифровальщик-вымогатель Petya известен как минимум с 2016 года. Тогда в блоге Касперскогорассказали о механизме работы «Пети».

> «Основной целью "Пети" являются корпоративные пользователи: шифровальщик попадает на ПК с помощью спама, притворяясь письмом от кандидата на ту или иную должность».

«Петя» работает без подключения к сети. На 2016 год специалистам по безопасности не удалось найти способ расшифровки украденных вирусом данных. Лучший способ защиты — это предупредить атаку, используя антивирусы.

Фото: Александр Литреев.

Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2978 27.06.2017, 13:54
1
URL: https://babr24.com/?IDE=272395 Bytes: 4558 / 3645 Версия для печати

Автор текста: **Полина Чехова**,
журналист.

На сайте опубликовано **494**
текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта