Kupidon

id-ransomware.blogspot.com/2020/05/kupidon-ransomware.html

Kupidon Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные обычных и бизнес-пользователей, а также файлы на сайтах с помощью AES+RSA, а затем требует выкуп в $300 (для частных пользователей) - $1200 (для компаний) в BTC, чтобы вернуть файлы. Сумма у обычных пользователей обычно ниже. Оригинальное название: Kupidon. На файле написано: нет данных.

Обнаружения:
DrWeb ->
BitDefender ->
ALYac ->
Avira (no cloud) ->
ESET-NOD32 ->
Malwarebytes ->
Rising ->
Symantec ->
TrendMicro ->

© Генеалогия: HacknutCrypt >> Kupidon

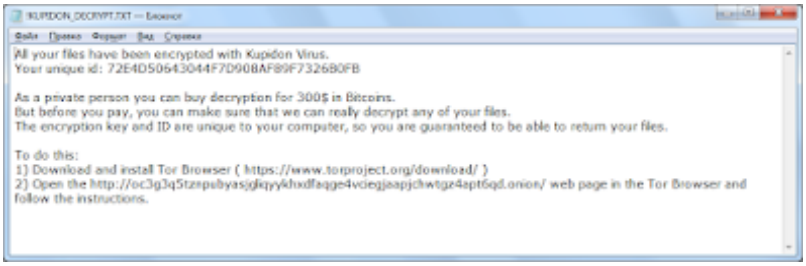
Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.kupidon**

Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришлась на начало мая 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. Достоверно известно только об одном пострадавшем румынском сайте.

Записка с требованием выкупа называется: **!KUPIDON_DECRYPT.TXT**

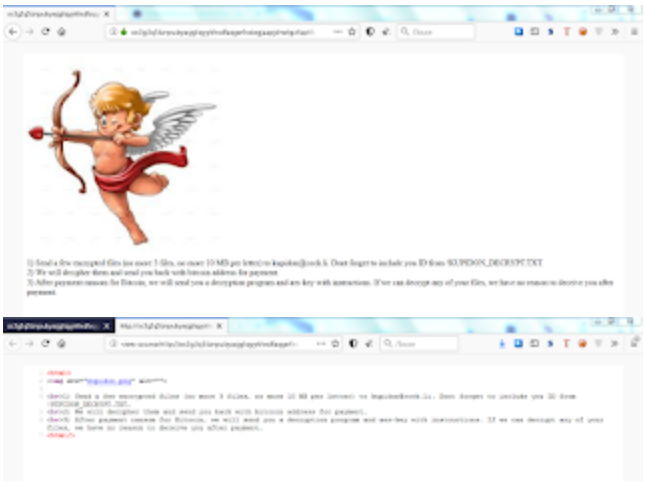


Содержание записки о выкупе:
All your files have been encrypted with Kupidon Virus.
Your unique id: 72E4D50643044F7D908AF89F7326B0FB
As a private person you can buy decryption for 300$ in Bitcoins.
But before you pay, you can make sure that we can really decrypt any of your files.
The encryption key and ID are unique to your computer, so you are guaranteed to be able to return your files.
To do this:

1) Download and install Tor Browser (https://www.torproject.org/download/)
2) Open the http://oc3g3q5tznpubyasjgliqyykhxdfaqge4vciegjaapjchwtgz4apt6qd.onion/ web page in the Tor Browser and follow the instructions.

Перевод записки на русский язык:
Все ваши файлы были зашифрованы вирусом Купидон.
Ваш уникальный id: 72E4D50643044F7D908AF89F7326B0FB
Как частное лицо вы можете купить расшифровку за 300$ в биткойнах.
Но перед оплатой, вы можете убедиться, что мы правда можем расшифровать любые ваши файлы.
Ключ шифрования и ID уникальны для вашего компьютера, поэтому вы гарантированно сможете вернуть свои файлы.
Сделайте это:
1) Загрузите и установите браузер Tor (https://www.torproject.org/download/)
2) Откройте веб-страницу http://oc3g3q5tznpubyasjgliqyykhxdfaqge4vciegjaapjchwtgz4apt6qd.onion/ в браузере Tor и следуйте инструкциям.

У бизнес-пользователей вместо слов **private person** в записке будет указано **commercial person**. И сумма выкупа будет выше в несколько раз.
Запиской с требованием выкупа также выступает сайт вымогателей:



Содержание текста о выкупе:
1) Send a few encrypted files (no more 3 files, no more 10 MB per letter) to kupidon@cock.li. Dont forget to include you ID from !KUPIDON_DECRYPT.TXT.
2) We will decipher them and send you back with bitcoin address for payment.

3) After payment ransom for Bitcoin, we will send you a decryption program and aes-key with instructions. If we can decrypt any of your files, we have no reason to deceive you after payment.

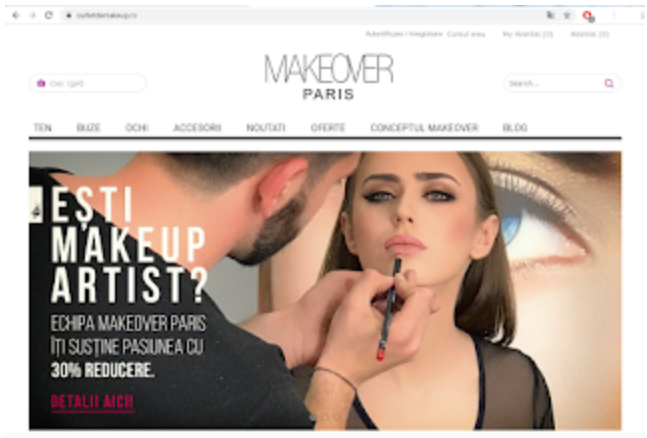
Перевод текста на русский язык:
1) Отправьте несколько зашифрованных файлов (не более 3 файлов, не более 10 МБ на письмо) на адрес kupidon@cock.li. Не забудьте указать свой идентификатор из !KUPIDON_DECRYPT.TXT.
2) Мы расшифруем их и отправим обратно с биткоин-адресом для оплаты.
3) После уплаты выкупа за биткоины мы вышлем вам программу дешифрования и aes-ключ с инструкциями. Если мы можем расшифровать любой из ваших файлов, у нас нет оснований обманывать вас после оплаты.

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

➤ Данные с пострадавшего сайта и из кеша Google.



Список файловых расширений, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:
!KUPIDON_DECRYPT.TXT - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Мьютексы:
См. ниже результаты анализов.

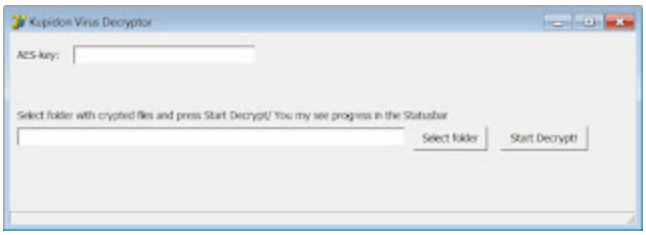
Сетевые подключения и связи:
Tor-URL: xxxx://oc3g3q5tznpubyasjgliqyykhxdfaqge4vciegjaapjchwtgz4apt6qd.onion/
2-1 URL: xxxx://147.135.170.169/

URL пострадавшего сайта: xxxxs://outletdemakeup.ro
Записка на сайте: xxxxs://outletdemakeup.ro/!KUPIDON_DECRYPT.TXT
Email-1: kupidon@cock.li
Email-2: ann4.orlova.892@yandex.ru
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ Hybrid analysis >>
Σ VirusTotal analysis >>
🐞 Intezer analysis >>
⋟ ANY.RUN analysis >>
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
꩜ JOE Sandbox analysis >>

Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

=== ДЕШИФРОВЩИК === DECRYPTOR ===



=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

HacknutCrypt (Qweuirtksd) Ransomware - октябрь 2018
Kupidon Ransomware - мая 2020

=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Обновление от 5 июня 2020:
Статья на сайте BleepingComputer >>
Статистика за 30 дней

Расширение: **.kupidon**
Записка: !KUPIDON_DECRYPT.TXT.
Email: ann4.orlova.892@yandex.ru
➤ Содержание записки:
1) Send a few encrypted files (no more 3 files, no more 10 MB per file) to ann4.orlova.892@yandex.ru . Dont forget to include you ID from !KUPIDON_DECRYPT.TXT.
2) We will decipher them and send you back with bitcoin address for payment.
3) After payment ransom for Bitcoin, we will send you a decryption program and aes-key with instructions. If we can decrypt any of your files, we have no reason to deceive you after payment.

Обновление от 25 июля 2020:

Пост на форуме >>

=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===

Thanks:

MalwareHunterTeam
Andrew Ivanov (author)
DrStache
to the victims who sent the samples