XP10, FakeChrome

id-ransomware.blogspot.com/2020/08/xp10-ransomware.html

XP10 Ransomware

FakeChrome Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует выкуп в $980, чтобы вернуть файлы. Оригинальное название: xp10-ransom. На файле написано: chrome.exe.

Обнаружения:
DrWeb -> Trojan.MulDrop13.50455
BitDefender -> Gen:Heur.Ransom.REntS.Gen.1
ALYac -> Trojan.Ransom.Stupid
Avira (no cloud) -> TR/Ransom.cyuwx
ESET-NOD32 -> A Variant Of MSIL/Filecoder.AAT
Kaspersky -> HEUR:Trojan.MSIL.Fsysna.gen
Malwarebytes -> Ransom.FileCryptor
Symantec -> Trojan.Gen.2
Tencent -> Msil.Trojan.Fsysna.Dvzw
TrendMicro -> TROJ_GEN.R002C0WI220

© Генеалогия: Stupid >> XP10 (FakeChrome)

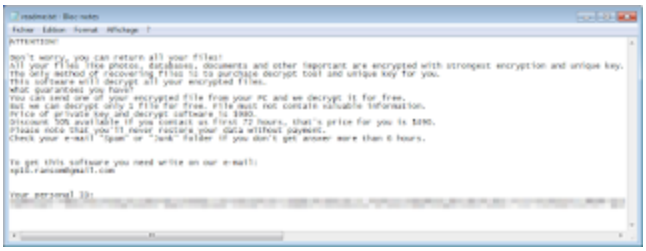
Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.xp10-ransom**

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 конец августа 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **readme.txt**



Содержание записки о выкупе:
ATTENTION!
Don't worry, you can return all your files!
All your files like photos, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.

Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.
To get this software you need write on our e-mail:
xp10.ransom@gmail.com
Your personal ID: ***

Перевод записки на русский язык:
ВНИМАНИЕ!
Не волнуйтесь, вы можете вернуть все свои файлы!
Все ваши файлы, такие как фото, базы данных, документы и другие важные файлы, зашифрованы с самым надежным шифрованием и уникальным ключом.
Единственный способ восстановить файлы - это приобрести инструмент дешифрования и уникальный ключ для вас.
Эта программа расшифрует все ваши зашифрованные файлы.
Какие гарантии у вас есть?
Вы можете отправить один из зашифрованных файлов со своего ПК и мы расшифруем его бесплатно.
Но мы можем бесплатно расшифровать только 1 файл. Файл не должен содержать ценной информации.
Стоимость закрытого ключа и программы для дешифрования составляет $980.
Скидка 50% доступна, если вы свяжетесь с нами в первые 72 часа, это цена для вас $490.
Заметьте, что вы никогда не восстановите свои данные без оплаты.
Проверьте папку "Spam" или "Junk" в своей почте, если вы не получаете ответа более 6 часов.
Чтобы получить эту программу, вам надо написать на наш email:
xp10.ransom@gmail.com
Ваш личный ID: ***

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**.

Список файловых расширений, подвергающихся шифрованию:
.3g2, .3gp, .accdb, .aepx, .ai, .arw, .asf, .asp, .aspx, .asx, .avi, .bay, .bin, .bmp, .cdr, .cer, .class, .cpp, .cppproj, .cr2, .crt, .crw, .cs, .csproj, .csv, .dat, .db, .dbf, .dcr, .der, .dng, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .dwg, .dxf, .dxg, .eps, .erf, .fla, .flv, .html, .idml, .indb, .indd, .indl, .indt, .info, .ipsw, .jar, .java, .jpeg, .jpg, .kdc, .m3u, .m3u8, .m4u, .max, .mdb, .mdf, .mef, .mpeg, .pdf, .php, .png, .potm, .potx, .ppam, .ppsm, .ppsx, .pptm, .pptx, .prel, .prproj, .resx, .sldm, .sldx, .sql, .txt, .vb, .vbproj, .wav, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xltm, .xltx, .xml (94 расширения).
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:
readme.txt - название файла с требованием выкупа
chrome.exe
chrome.pdb
xdfjhdlojdziosdvxjoo.txt
<random>.exe - случайное название вредоносного файла

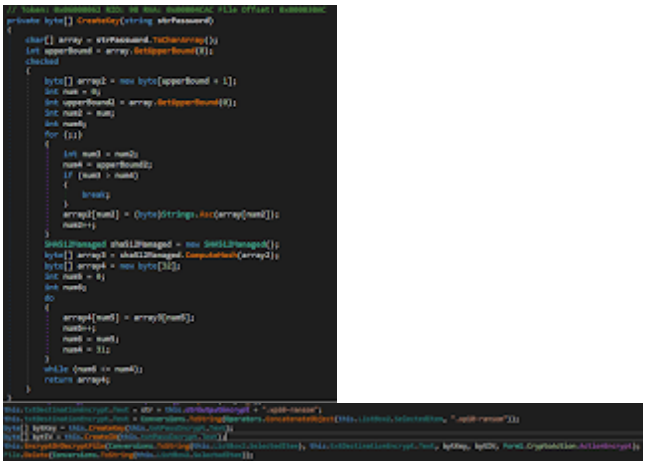
Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
D:\New folder (2)\Visual Studio 2012\Projects\WindowsApplication4\WindowsApplication4\obj\Debug\chrome.pdb

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: xp10.ransom@gmail.com
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Скриншоты от Майкла Джиллеспи:



Результаты анализов:

🔻 **Triage analysis >>**
Ⓗ **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.

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

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

Ещё не было обновлений этого варианта.

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

Thanks:

S!Ri, Michael Gillespie
Andrew Ivanov (author)
***
to the victims who sent the samples