Javalocker, JavaEncrypt

id-ransomware.blogspot.com/2020/03/javalocker-ransomware.html

Javalocker Ransomware

JavaEncrypt Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES/DES, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: javalocker (написано в записке).

Обнаружения:
DrWeb -> Java.Encoder.1, Java.Encoder.2
BitDefender -> Trojan.Agent.EMXP, Trojan.JAVA.Agent.BMZ, Java.Trojan.Agent.LQ
ESET-NOD32 -> A Variant Of Java/Filecoder.AI, Java/Filecoder.AJ
Kaspersky -> UDS:DangerousObject.Multi.Generic
Symantec -> Ransom.Wannacry, Trojan.Maljava
GData -> Java.Trojan.Agent.S5SUV9, Java.Trojan.Agent.LQ (2x)
Fortinet -> Java/Filecoder.AI!tr
Microsoft -> PUA:Win32/Presenoker
Qihoo-360 -> Generic/Trojan.05f, Generic/Trojan.03d

To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!
AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

© Генеалогия: другие Java Ransomware >> Javalocker (JavaEncrypt)

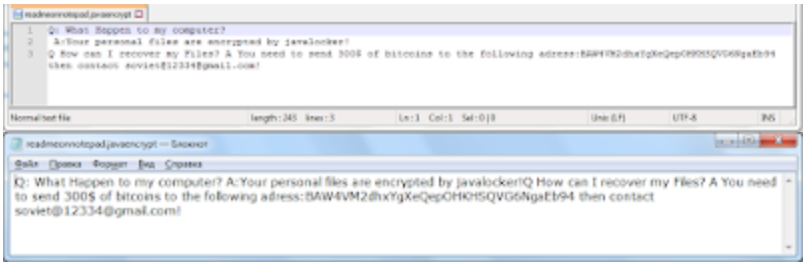
Изображение — логотип статьи

К зашифрованным файлам добавляются расширения:
.javaencrypt
.javalocker

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

Записка с требованием выкупа называется: **readmeonnotepad.javaencrypt**



Содержание записки о выкупе:
Q: What Happen to my computer?
A:Your personal files are encrypted by javalocker!
Q How can I recover my Files? A You need to send 300$ of bitcoins to the following adress:BAW4VM2dhxYgXeQepOHKHSQVG6NgaEb94 then contact soviet@12334@gmail.com!

Перевод записки на русский язык:
Вопрос: Что случилось с моим компьютером?
Ответ: Ваши личные файлы зашифрованы javalocker!

Вопрос: Как мне вернуть мои файлы? Вам надо отправить 300$ биткойнов на следующий адрес: BAW4VM2dhxYgXeQepOHKHSQVG6NgaEb94, а затем написать на soviet@12334@gmail.com!

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:
.123, .3dm, .3ds, .3g2, .3gp, .602, .accdb, .aes, .arc, .asc, .asf, .asm, .asp, .avi, .backup, .bak, .bat, .bmp, .brd, .bz2, .cgm, .cmd, .cpp, .crt, .csr, .csv, .dbf, .dch, .der, .dif, .dip, .djvu, .doc, .docb, .docm, .docx, .dwg, .edb, .eml, .fla, .flv, .frm, .gho, .gif, .gpg, .html, .hwp, .ibd, .ico, .ini, .iso, .jfif, .jpeg, .jpg, .jsp, .key, .lay, .lay6, .ldf, .m3u, .m4u, .max, .mdb, .mdf, .mid, .mkv, .mml, .mov, .mp3, .mp4, .mpeg, .mpg, .msg, .mui, .myd, .myi, .nef, .obd, .odg, .odp, .ods, .odt, .onetoc2, .ost, .otg, .otp, .ots, .ott, .p12, .paq, .pas, .pdf, .pem, .pfx, .php, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptx, .ps1, .psd, .pst, .pub, .rar, .raw, .reg, .rtf, .sch, .sldm, .sldx, .slk, .sln, .snt, .sql, .sqlite3, .sqlitedb, .stc, .std, .sti, .stw, .suo, .svg, .swf, .sxc, .sxd, .sxi, .sxm, .sxw, .tar, .tbk, .tif, .tiff, .txt, .uop, .uot, .vbs, .vcd, .vdi, .vmdk, .vmx, .vob, .vsd, .vsdx, .wav, .wb2, .wk1, .wks, .wma, .wmv, .xls, .xlsm, .xlsx, .zip (159 расширений).

Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Пропускает файлы с расширения:
.java
.javalocker
.javaencrypt

Файлы, связанные с этим Ransomware:
14370-0db8a7d767a2454998bf3ee875676929.jar
JAVABASIC.jar
javaw.exe
java.io
java.lang

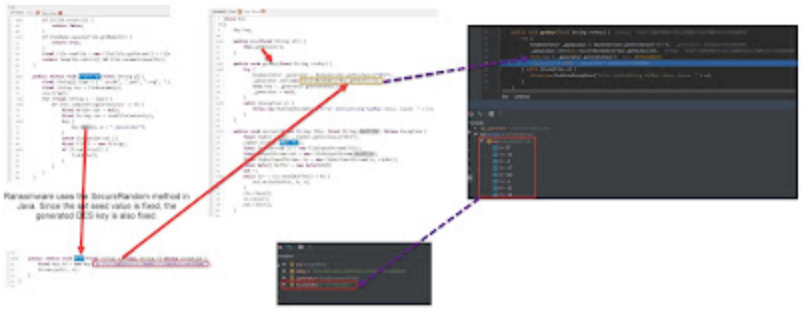
java.security
java.util
java.util.regex
javax.crypto
DESkey.dat
readmeonnotepad.javaencrypt - название текстового файла
<random>.exe - случайное название вредоносного файла

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

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

Сетевые подключения и связи:
Email: soviet@12334@gmail.com
BTC: BAW4VM2dhxYgXeQepOHKHSQVG6NgaEb94
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Скриншот простого анализа:



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

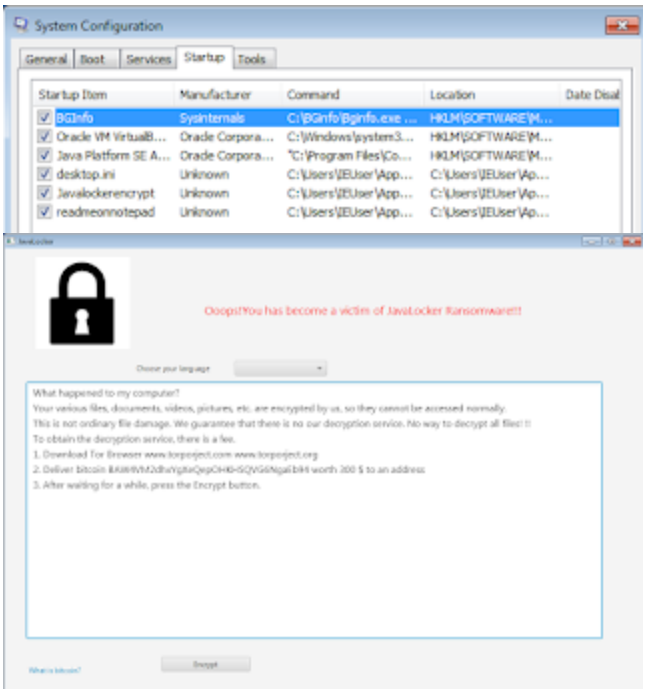
Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Обновление от 11 марта 2020:
Расширение: .javaencrypt
Записка: readmeonnotepad.javaencrypt
Email: soviet@12334@gmail.com!
BTC: BAW4VM2dhxYgXeQepOHKHSQVG6NgaEb94
Файл: JAVABASIC.jar
Результаты анализов: **VT** + **HA** + **AR**
➤ Содержание записки:
Q: What Happen to my computer?
A:Your personal files are encrypted by javalocker!
Q How can I recover my Files? A You need to send 300$ of bitcoins to the following adress:BAW4VM2dhxYgXeQepOHKHSQVG6NgaEb94 then contact soviet@12334@gmail.com!

Чтобы отобразить окно с требованием выкупа, вымогатель копирует себя в папку Автозапуска.



Обновление от 11 марта 2020:

Пост в Твиттере >>
Результаты анализов: **VT** + **VT**

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

Внимание!

Файлы можно расшифровать. Используется статический DES-ключ.
Скачайте дешифровщик от Emsisoft по этой ссылке >>
***

Added later:

Write-up (added on March 18, 2020)
***

Thanks:

Jirehlov, onion (jishuzhain), Michael Gillespie
Andrew Ivanov (author)
Petrovic
to the victims who sent the samples