KeyPass ransomware

securelist.com/keypass-ransomware/87412/

Incidents

Incidents

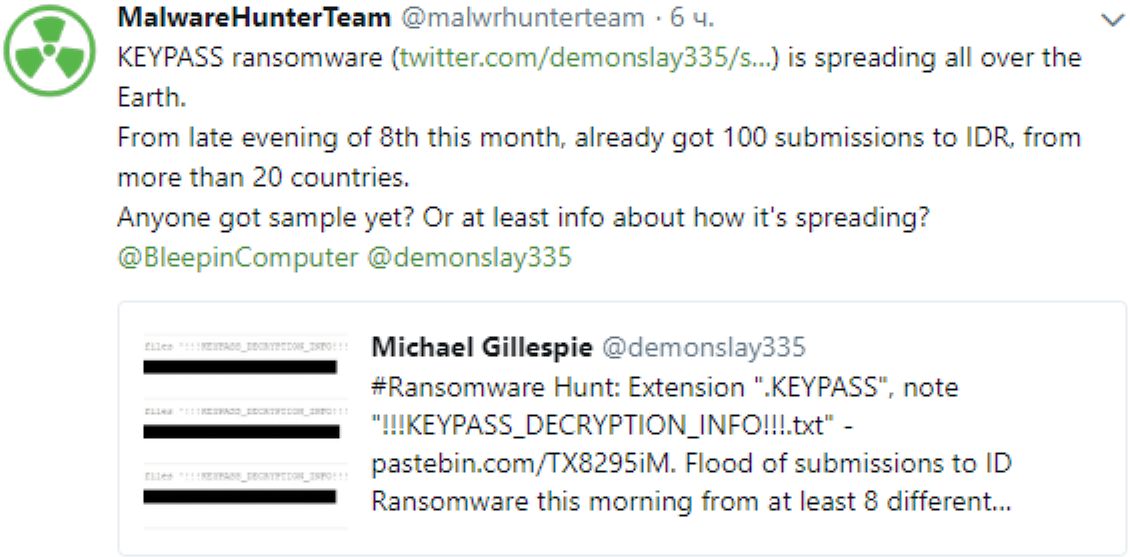
13 Aug 2018

minute read

Authors

- Expert Orkhan Mamedov
- Expert Fedor Sinitsyn

In the last few days, our anti-ransomware module has been detecting a new variant of malware – KeyPass ransomware. Others in the security community have also noticed that this ransomware began to actively spread in August:



MalwareHunterTeam @malwrhunterteam · 6 ч.
KEYPASS ransomware (twitter.com/demonslay335/s...) is spreading all over the Earth.
From late evening of 8th this month, already got 100 submissions to IDR, from more than 20 countries.
Anyone got sample yet? Or at least info about how it's spreading?
@BleepinComputer @demonslay335

Michael Gillespie @demonslay335
#Ransomware Hunt: Extension ".KEYPASS", note "!!!KEYPASS_DECRYPTION_INFO!!!.txt" - pastebin.com/TX8295iM. Flood of submissions to ID Ransomware this morning from at least 8 different...

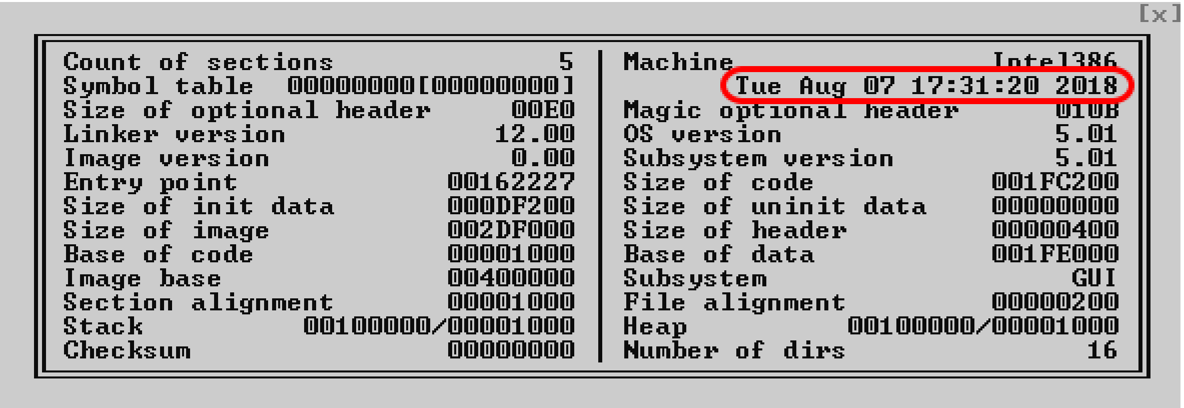
Notification from MalwareHunterTeam

Distribution model

According to our information, the malware is propagated by means of fake installers that download the ransomware module.

Description

The Trojan sample is written in C++ and compiled in MS Visual Studio. It was developed using the libraries MFC, Boost and Crypto++. The PE header contains a recent compilation date.

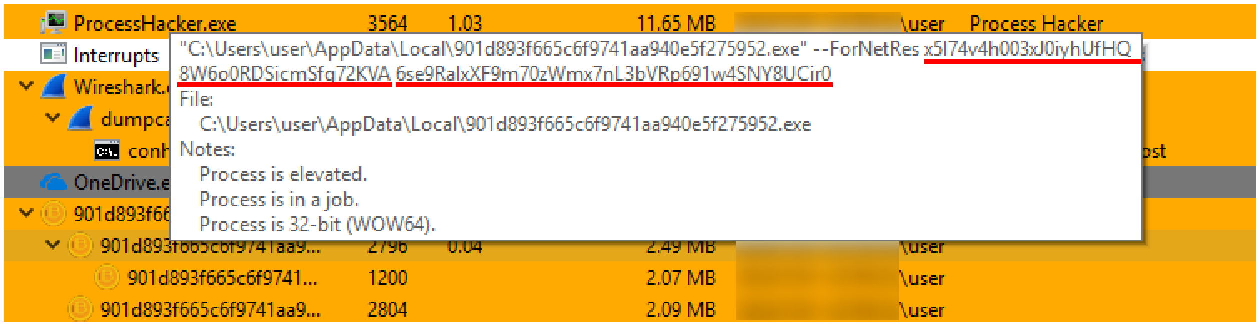


```
                                                                              [x]
 Count of sections                 5 | Machine                     Intel386
 Symbol table   00000000[00000000]   |           Tue Aug 07 17:31:20 2018
 Size of optional header        00E0 | Magic optional header           010B
 Linker version                12.00 | OS version                      5.01
 Image version                  0.00 | Subsystem version               5.01
 Entry point                00162227 | Size of code                001FC200
 Size of init data          000DF200 | Size of uninit data         00000000
 Size of image              002DF000 | Size of header              00000400
 Base of code               00001000 | Base of data                001FE000
 Image base                 00400000 | Subsystem                        GUI
 Section alignment          00001000 | File alignment              00000200
 Stack             00100000/00001000 | Heap               00100000/00001000
 Checksum                   00000000 | Number of dirs                    16
```

PE header with compilation date

When started on the victim's computer, the Trojan copies its executable to %LocalAppData% and launches it. It then deletes itself from the original location.

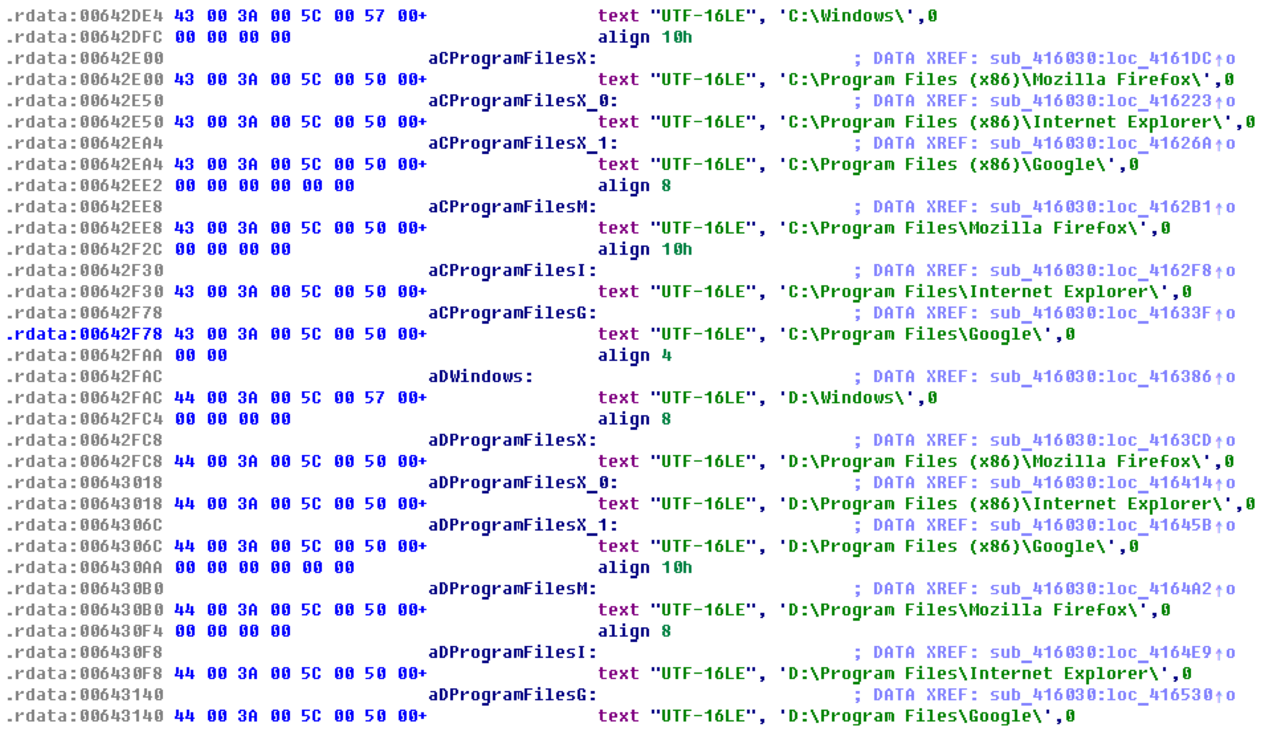
Following that, it spawns several copies of its own process, passing the encryption key and victim ID as command line arguments.



```
ProcessHacker.exe          3564   1.03        11.65 MB   [redacted]\user   Process Hacker
Interrupts
Wireshark.
  dumpca
    conh                                                                    ost
OneDrive.e
901d893f66
  901d893f665c6f9741aa9...  2796   0.04        2.49 MB   [redacted]\user
    901d893f665c6f9741...   1200               2.07 MB   [redacted]\user
  901d893f665c6f9741aa9...  2804               2.09 MB   [redacted]\user

"C:\Users\user\AppData\Local\901d893f665c6f9741aa940e5f275952.exe" --ForNetRes x5I74v4h003xJ0iyhUfHQ
8W6o0RDSicmSfq72KVA 6se9RalxXF9m70zWmx7nL3bVRp691w4SNY8UCir0
File:
   C:\Users\user\AppData\Local\901d893f665c6f9741aa940e5f275952.exe
Notes:
   Process is elevated.
   Process is in a job.
   Process is 32-bit (WOW64).
```

Command line arguments

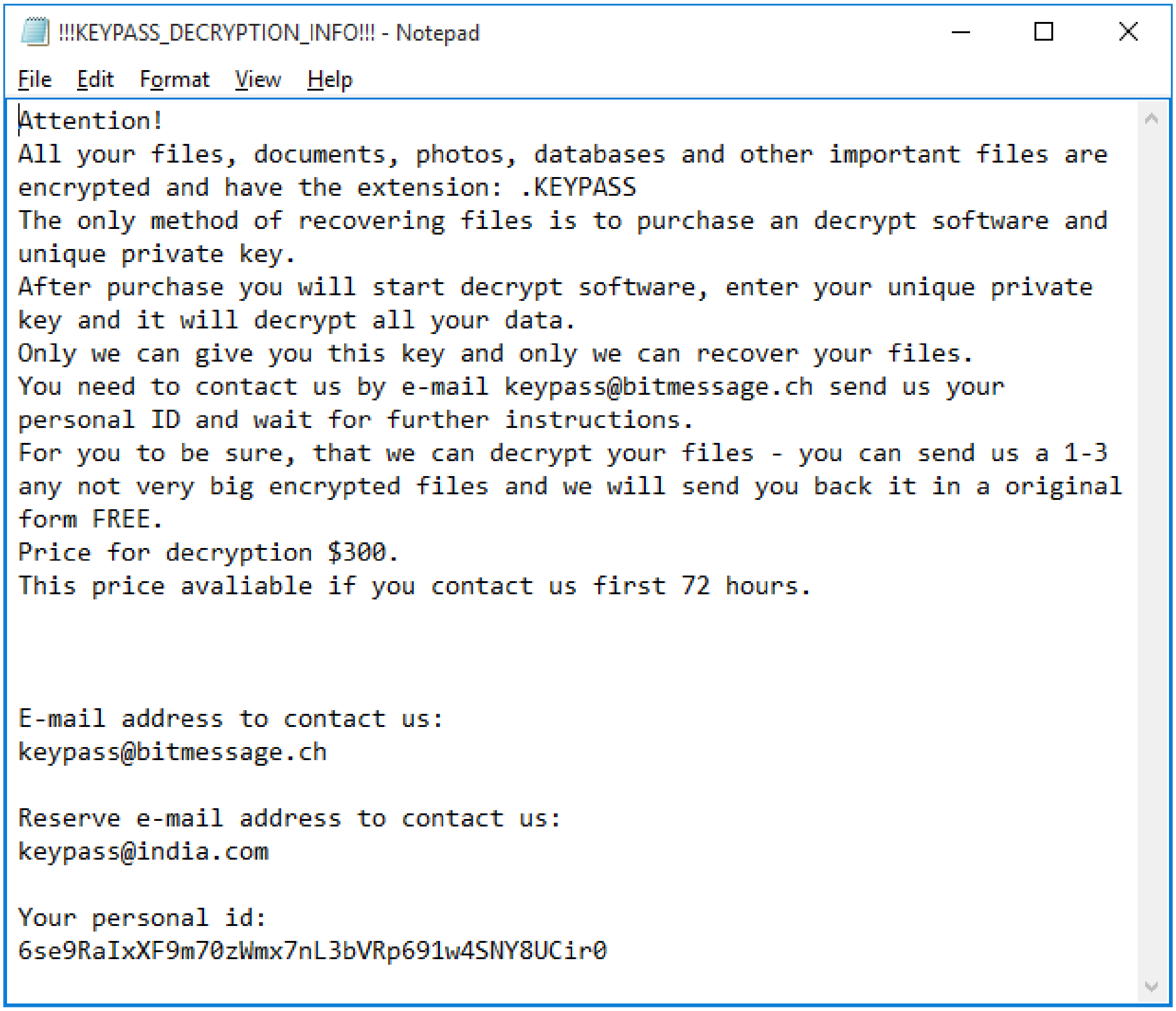
KeyPass enumerates local drives and network shares accessible from the infected machine and searches for all files, regardless of their extension. It skips files located in a number of directories, the paths to which are hardcoded into the sample.



```
.rdata:00642DE4 43 00 3A 00 5C 00 57 00+                text "UTF-16LE", 'C:\Windows\',0
.rdata:00642DFC 00 00 00 00                             align 10h
.rdata:00642E00                         aCProgramFilesX:                        ; DATA XREF: sub_416030:loc_4161DC↑o
.rdata:00642E00 43 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'C:\Program Files (x86)\Mozilla Firefox\',0
.rdata:00642E50                         aCProgramFilesX_0:                      ; DATA XREF: sub_416030:loc_416223↑o
.rdata:00642E50 43 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'C:\Program Files (x86)\Internet Explorer\',0
.rdata:00642EA4                         aCProgramFilesX_1:                      ; DATA XREF: sub_416030:loc_41626A↑o
.rdata:00642EA4 43 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'C:\Program Files (x86)\Google\',0
.rdata:00642EE2 00 00 00 00 00 00                       align 8
.rdata:00642EE8                         aCProgramFilesM:                        ; DATA XREF: sub_416030:loc_4162B1↑o
.rdata:00642EE8 43 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'C:\Program Files\Mozilla Firefox\',0
.rdata:00642F2C 00 00 00 00                             align 10h
.rdata:00642F30                         aCProgramFilesI:                        ; DATA XREF: sub_416030:loc_4162F8↑o
.rdata:00642F30 43 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'C:\Program Files\Internet Explorer\',0
.rdata:00642F78                         aCProgramFilesG:                        ; DATA XREF: sub_416030:loc_41633F↑o
.rdata:00642F78 43 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'C:\Program Files\Google\',0
.rdata:00642FAA 00 00                                   align 4
.rdata:00642FAC                         aDWindows:                              ; DATA XREF: sub_416030:loc_416386↑o
.rdata:00642FAC 44 00 3A 00 5C 00 57 00+                text "UTF-16LE", 'D:\Windows\',0
.rdata:00642FC4 00 00 00 00                             align 8
.rdata:00642FC8                         aDProgramFilesX:                        ; DATA XREF: sub_416030:loc_4163CD↑o
.rdata:00642FC8 44 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'D:\Program Files (x86)\Mozilla Firefox\',0
.rdata:00643018                         aDProgramFilesX_0:                      ; DATA XREF: sub_416030:loc_416414↑o
.rdata:00643018 44 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'D:\Program Files (x86)\Internet Explorer\',0
.rdata:0064306C                         aDProgramFilesX_1:                      ; DATA XREF: sub_416030:loc_41645B↑o
.rdata:0064306C 44 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'D:\Program Files (x86)\Google\',0
.rdata:006430AA 00 00 00 00 00 00                       align 10h
.rdata:006430B0                         aDProgramFilesM:                        ; DATA XREF: sub_416030:loc_4164A2↑o
.rdata:006430B0 44 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'D:\Program Files\Mozilla Firefox\',0
.rdata:006430F4 00 00 00 00                             align 8
.rdata:006430F8                         aDProgramFilesI:                        ; DATA XREF: sub_416030:loc_4164E9↑o
.rdata:006430F8 44 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'D:\Program Files\Internet Explorer\',0
.rdata:00643140                         aDProgramFilesG:                        ; DATA XREF: sub_416030:loc_416530↑o
.rdata:00643140 44 00 3A 00 5C 00 50 00+                text "UTF-16LE", 'D:\Program Files\Google\',0
```

The list of excluded paths

Every encrypted file gets an additional extension: “.KEYPASS” and ransom notes named “”!!!KEYPASS_DECRYPTION_INFO!!!.txt”” are saved in each processed directory.

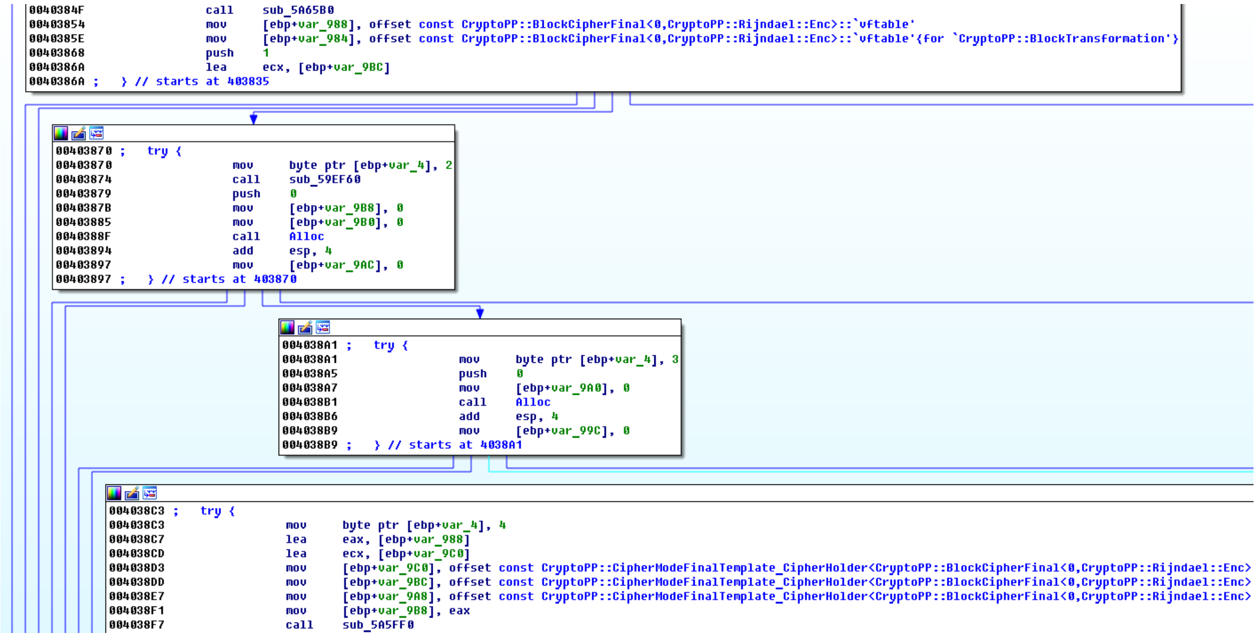


```
Attention!
All your files, documents, photos, databases and other important files are
encrypted and have the extension: .KEYPASS
The only method of recovering files is to purchase an decrypt software and
unique private key.
After purchase you will start decrypt software, enter your unique private
key and it will decrypt all your data.
Only we can give you this key and only we can recover your files.
You need to contact us by e-mail keypass@bitmessage.ch send us your
personal ID and wait for further instructions.
For you to be sure, that we can decrypt your files - you can send us a 1-3
any not very big encrypted files and we will send you back it in a original
form FREE.
Price for decryption $300.
This price avaliable if you contact us first 72 hours.



E-mail address to contact us:
keypass@bitmessage.ch

Reserve e-mail address to contact us:
keypass@india.com

Your personal id:
6se9RaIxXF9m70zWmx7nL3bVRp691w4SNY8UCir0
```

The ransom note

Encryption scheme

The developers of this Trojan implemented a very simplistic scheme. The malware uses the symmetric algorithm AES-256 in CFB mode with zero IV and the same 32-byte key for all files. The Trojan encrypts a maximum of 0x500000 bytes (~5 MB) of data at the beginning of each file.



```
0040384F                call    sub_5A65B0
00403854                mov     [ebp+var_988], offset const CryptoPP::BlockCipherFinal<0,CryptoPP::Rijndael::Enc>::`vftable'
0040385E                mov     [ebp+var_984], offset const CryptoPP::BlockCipherFinal<0,CryptoPP::Rijndael::Enc>::`vftable'{for `CryptoPP::BlockTransformation'}
00403868                push    1
0040386A                lea     ecx, [ebp+var_9BC]
0040386A ;   } // starts at 403835
```

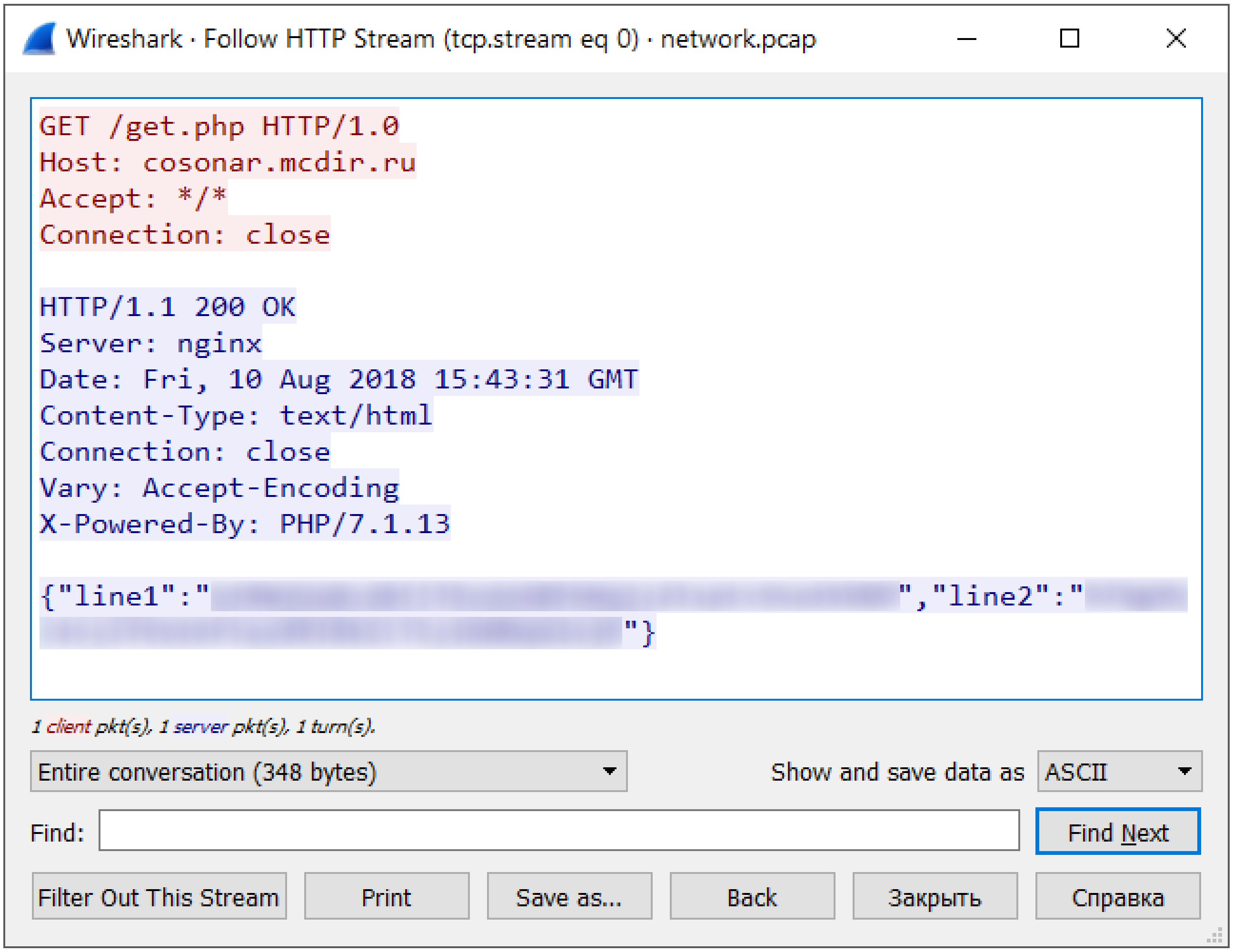
```
00403870 ;   try {
00403870                mov     byte ptr [ebp+var_4], 2
00403874                call    sub_59EF60
00403879                push    0
0040387B                mov     [ebp+var_9B8], 0
00403885                mov     [ebp+var_9B0], 0
0040388F                call    Alloc
00403894                add     esp, 4
00403897                mov     [ebp+var_9AC], 0
00403897 ;   } // starts at 403870
```

```
004038A1 ;   try {
004038A1                mov     byte ptr [ebp+var_4], 3
004038A5                push    0
004038A7                mov     [ebp+var_9A0], 0
004038B1                call    Alloc
004038B6                add     esp, 4
004038B9                mov     [ebp+var_99C], 0
004038B9 ;   } // starts at 4038A1
```

```
004038C3 ;   try {
004038C3                mov     byte ptr [ebp+var_4], 4
004038C7                lea     eax, [ebp+var_988]
004038CD                lea     ecx, [ebp+var_9C0]
004038D3                mov     [ebp+var_9C0], offset const CryptoPP::CipherModeFinalTemplate_CipherHolder<CryptoPP::BlockCipherFinal<0,CryptoPP::Rijndael::Enc>
004038DD                mov     [ebp+var_9BC], offset const CryptoPP::CipherModeFinalTemplate_CipherHolder<CryptoPP::BlockCipherFinal<0,CryptoPP::Rijndael::Enc>
004038E7                mov     [ebp+var_9A8], offset const CryptoPP::CipherModeFinalTemplate_CipherHolder<CryptoPP::BlockCipherFinal<0,CryptoPP::Rijndael::Enc>
004038F1                mov     [ebp+var_9B8], eax
004038F7                call    sub_5A5FF0
```

Part of the procedure that implements data encryption

Soon after launch, KeyPass connects to its command and control (C&C) server and receives the encryption key and the infection ID for the current victim. The data is transferred over plain HTTP in the form of JSON.



Wireshark · Follow HTTP Stream (tcp.stream eq 0) · network.pcap

```
GET /get.php HTTP/1.0
Host: cosonar.mcdir.ru
Accept: */*
Connection: close

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 10 Aug 2018 15:43:31 GMT
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.1.13

{"line1":"[redacted]","line2":"[redacted]"}
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (348 bytes)

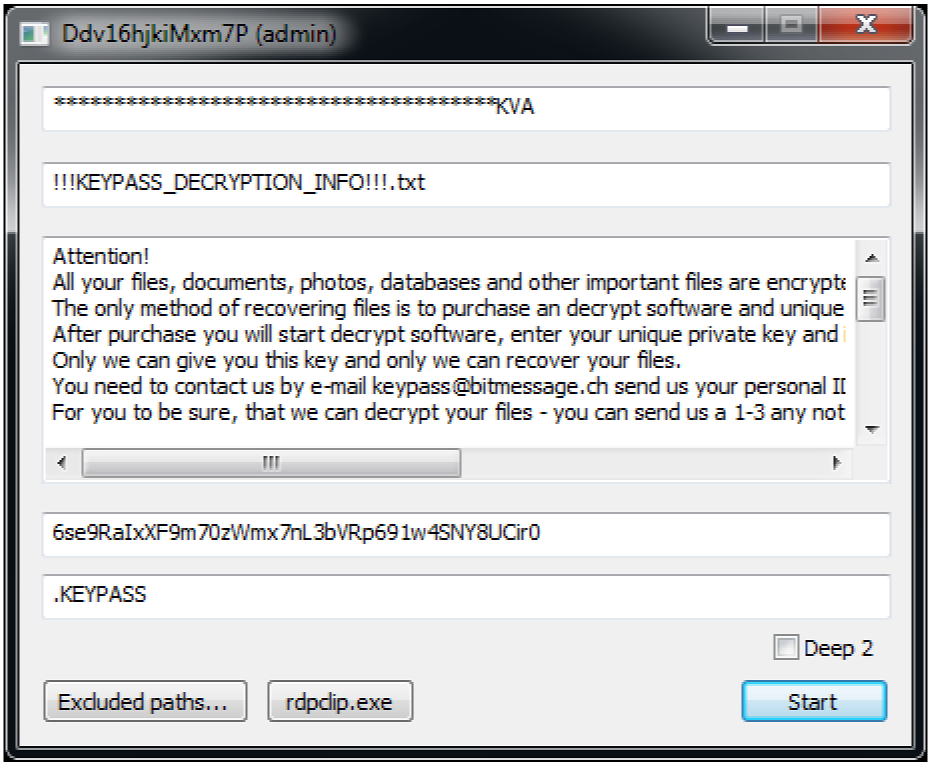
Show and save data as: ASCII

Find:

If the C&C is inaccessible (e.g. if the infected machine is not connected to the internet or the server is down), the Trojan uses a hardcoded key and ID, which means that in the case of offline encryption the decryption of the victim's files will be trivial.

GUI

From our point of view, the most interesting feature of the KeyPass Trojan is the ability to take 'manual control'. The Trojan contains a form that is hidden by default, but which can be shown after pressing a special button on the keyboard. This capability might be an indication that the criminals behind the Trojan intend to use it in manual attacks.



Ddv16hjkiMxm7P (admin)

*************************************KVA

!!!KEYPASS_DECRYPTION_INFO!!!.txt

Attention!
All your files, documents, photos, databases and other important files are encrypte
The only method of recovering files is to purchase an decrypt software and unique
After purchase you will start decrypt software, enter your unique private key and i
Only we can give you this key and only we can recover your files.
You need to contact us by e-mail keypass@bitmessage.ch send us your personal I
For you to be sure, that we can decrypt your files - you can send us a 1-3 any not

6se9RaIxXF9m70zWmx7nL3bVRp691w4SNY8UCir0

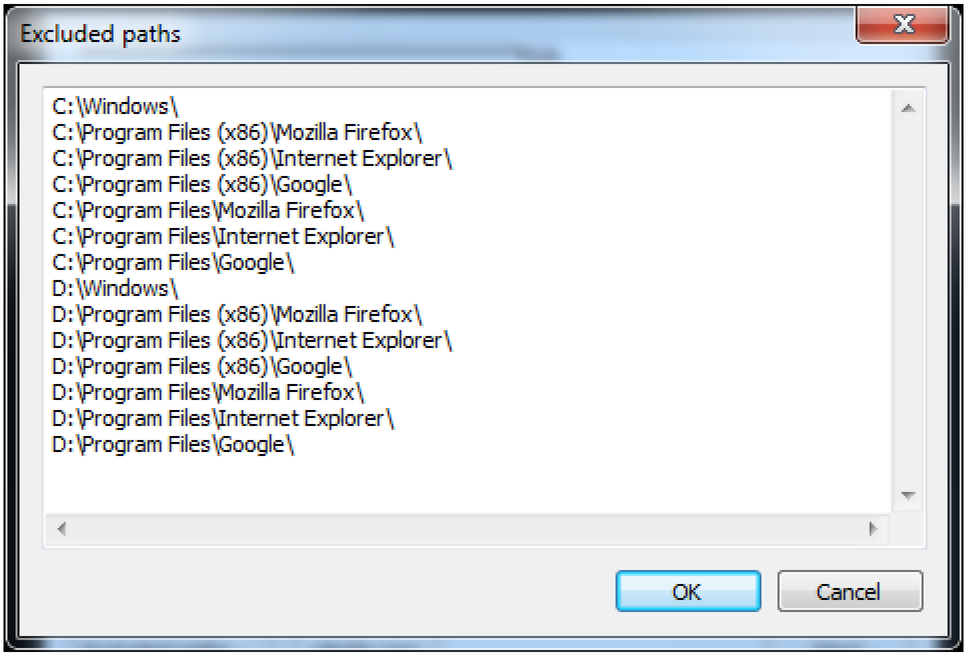
.KEYPASS

□ Deep 2

GUI of the trojan

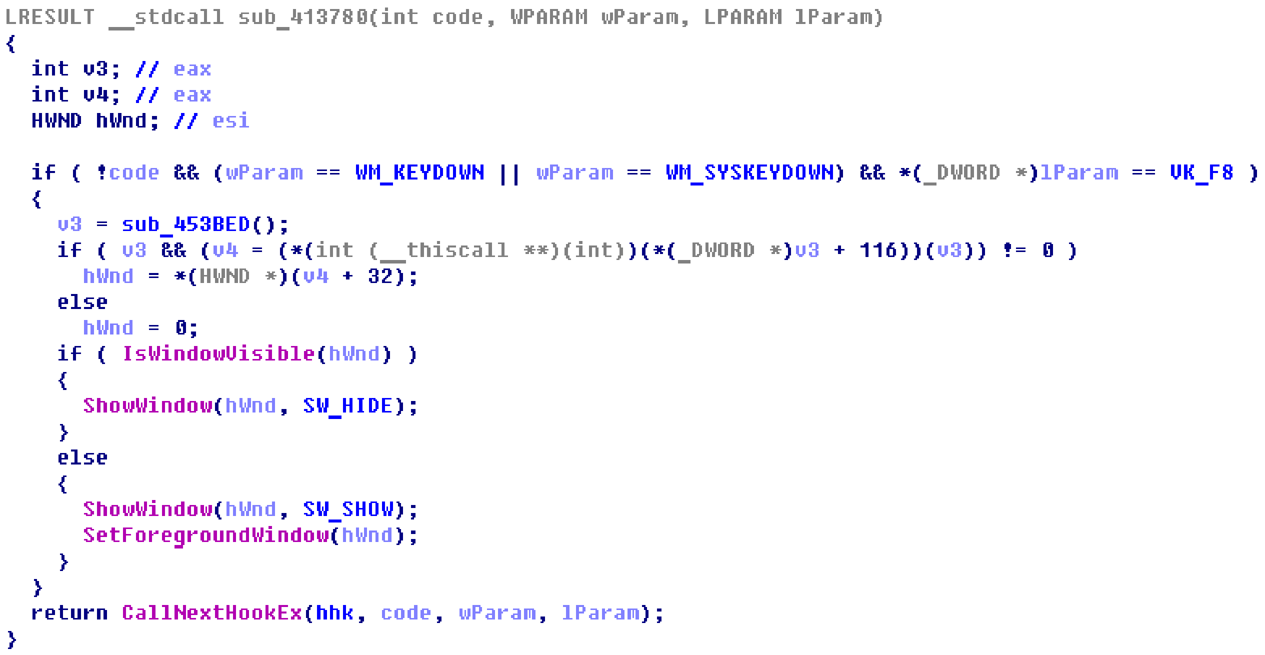
This form allows the attacker to customize the encryption process by changing such parameters as:

- encryption key
- name of ransom note
- text of ransom note
- victim ID
- extension of the encrypted files
- list of paths to be excluded from the encryption



```
C:\Windows\
C:\Program Files (x86)\Mozilla Firefox\
C:\Program Files (x86)\Internet Explorer\
C:\Program Files (x86)\Google\
C:\Program Files\Mozilla Firefox\
C:\Program Files\Internet Explorer\
C:\Program Files\Google\
D:\Windows\
D:\Program Files (x86)\Mozilla Firefox\
D:\Program Files (x86)\Internet Explorer\
D:\Program Files (x86)\Google\
D:\Program Files\Mozilla Firefox\
D:\Program Files\Internet Explorer\
D:\Program Files\Google\
```

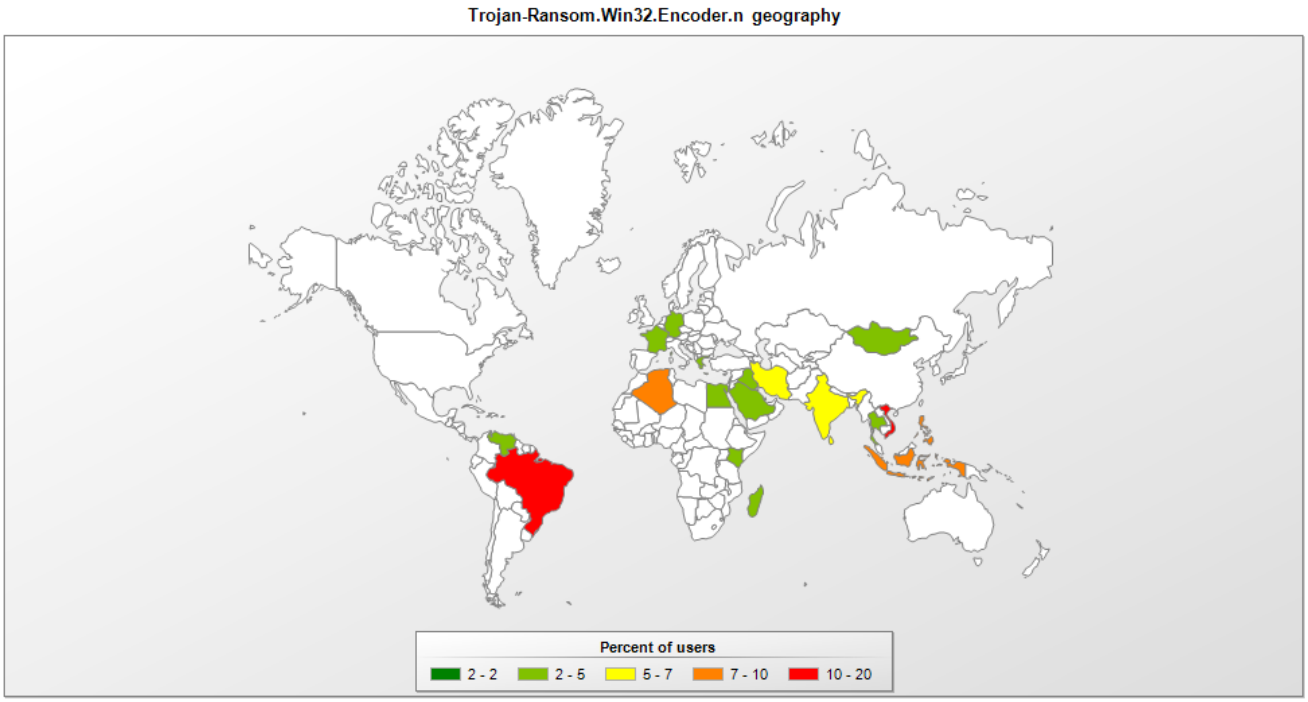
Paths excluded from encryption by default



```
LRESULT __stdcall sub_413780(int code, WPARAM wParam, LPARAM lParam)
{
  int v3; // eax
  int v4; // eax
  HWND hWnd; // esi

  if ( !code && (wParam == WM_KEYDOWN || wParam == WM_SYSKEYDOWN) && *(_DWORD *)lParam == VK_F8 )
  {
    v3 = sub_453BED();
    if ( v3 && (v4 = (*(int (__thiscall **)(int))(*(_DWORD *)v3 + 116))(v3)) != 0 )
      hWnd = *(HWND *)(v4 + 32);
    else
      hWnd = 0;
    if ( IsWindowVisible(hWnd) )
    {
      ShowWindow(hWnd, SW_HIDE);
    }
    else
    {
      ShowWindow(hWnd, SW_SHOW);
      SetForegroundWindow(hWnd);
    }
  }
  return CallNextHookEx(hhk, code, wParam, lParam);
}
```

Pseudocode of the procedure that shows the GUI by a keypress

Geography



IOC

901d893f665c6f9741aa940e5f275952 – Trojan-Ransom.Win32.Encoder.n
hxxp://cosonar.mcdir.ru/get.php

- Encryption
- Malware Descriptions
- Ransomware

Authors

- Expert Orkhan Mamedov
- Expert Fedor Sinitsyn

KeyPass ransomware

Your email address will not be published. Required fields are marked *

GReAT webinars

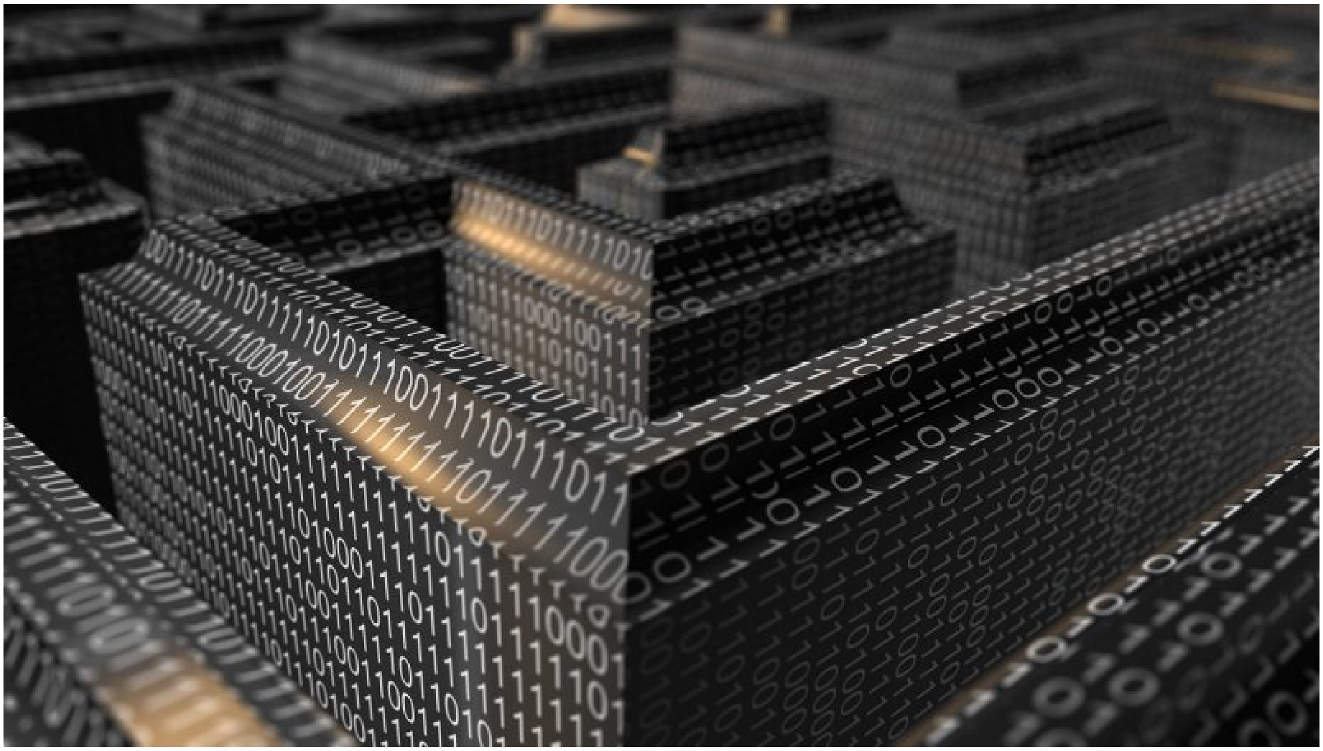
13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

Evolution of JSWorm ransomware

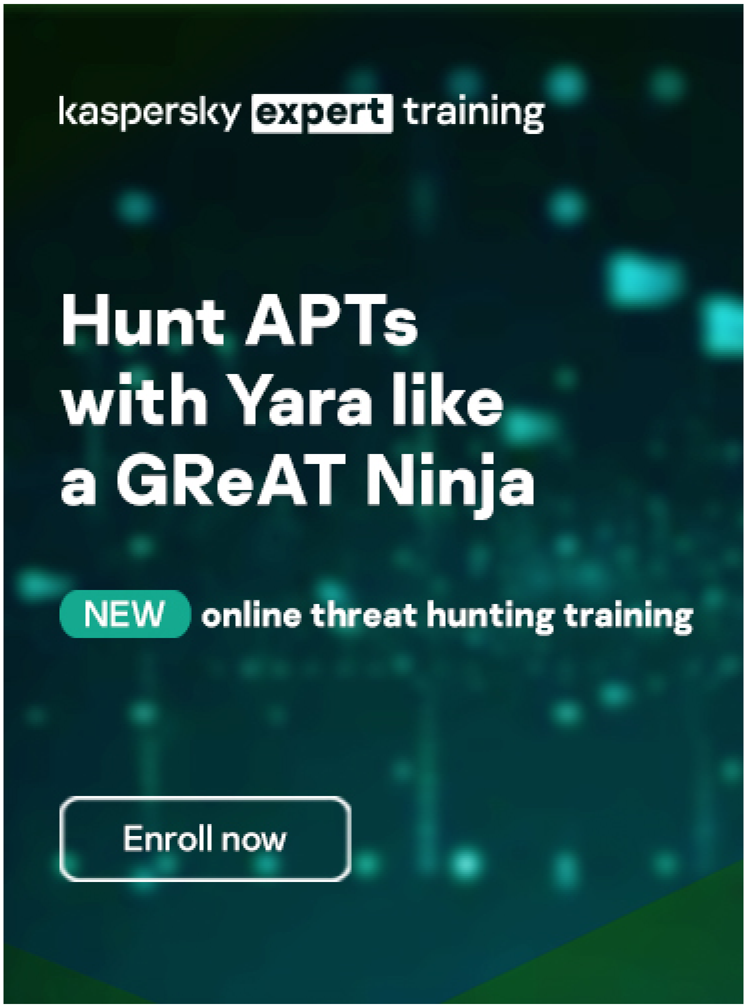
RansomEXX Trojan attacks Linux systems



Life of Maze ransomware

WastedLocker: technical analysis

Sodin ransomware exploits Windows vulnerability and processor architecture


kaspersky expert training
Hunt APTs with Yara like a GReAT Ninja
NEW online threat hunting training
Enroll now

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

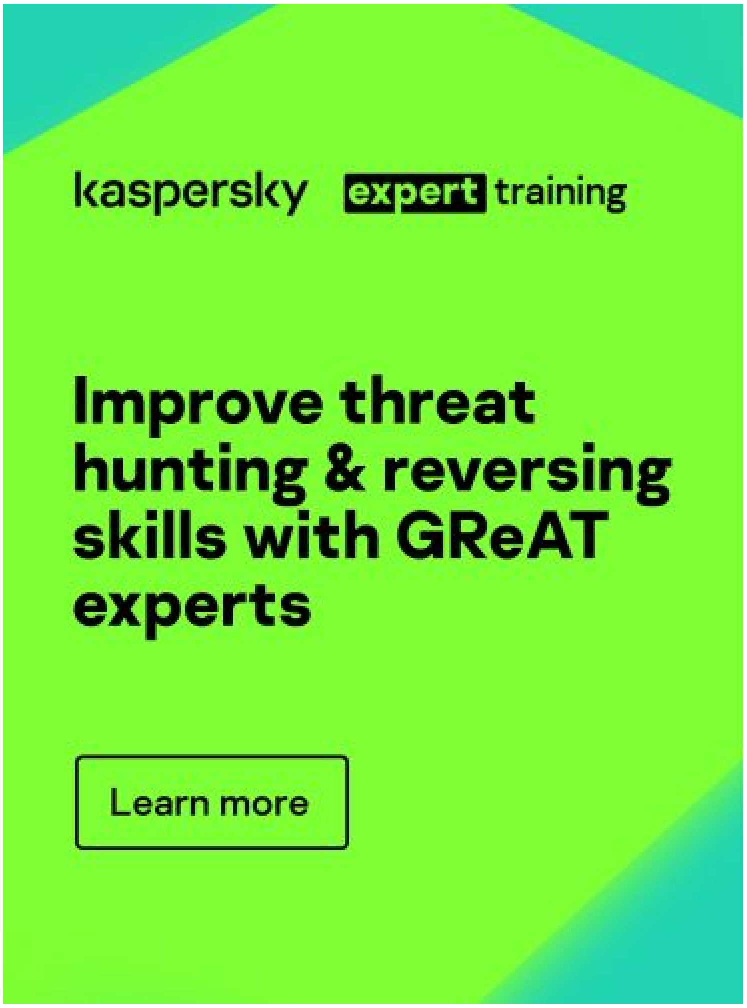
We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.


kaspersky
expert training
Improve threat hunting & reversing skills with GReAT experts
Learn more

-
-
-