TeamXRat: Brazilian cybercrime meets ransomware

By GReAT

Published: 2016-09-29 · Archived: 2026-04-02 10:51:16 UTC

Brazilian cybercriminals are notorious for their ability to develop banking trojans but now they have started to focus their efforts in new areas, including ransomware. We discovered a new variant of a Brazilian-made ransomware, **Trojan-Ransom.Win32.Xpan**, that is being used to infect local companies and hospitals, directly affecting innocent people, encrypting their files using the extension "**.___xratteamLucked**" and asking to pay the ransom.

The Kaspersky Anti-Ransom team decrypted the Xpan Trojan, allowing them to rescue the files of a Hospital in Brazil that had fallen victim to this Ransomware family.

Actually, this is not the first ransomware to come out of Brazil. In the past, we investigated TorLocker and its flawed encryption, which was created and negotiated worldwide by a Brazilian cybercriminal. We also saw a lot of copycats use HiddenTear in local attacks. Trojan Ransom Xpan was created by an organized gang, which used **targeted attacks via RDP that abused weak passwords and wrong implementations**.

In this post, we'll explain this new Ransomware family and how Brazilian coders are creating new ransomware from scratch.

The group behind the attack

The group identifies itself as "**TeamXRat**"and "**CorporacaoXRat**".
(Translating from Portuguese to English as "CorporationXRat")

Their first ransom trojan consisted of using a simple XOR based encryption, described by some victims here (most of the victims are from Brazil). The new version of Xpan Ransomware shows that the cybercriminals behind it have improved the code to make it more complex, also switching the encryption scheme.

The ransom texts used by the group are written in Portuguese from Brazil. The messages do not inform how much the victim has to pay to retrieve their files, nor the payment method required (which is usually Bitcoins). Instead, they instruct the victim to send an email to one of the anonymous email services Mail2Tor or Email.tg. For example, corporacaoxrat@mail2tor.com, xRatTeam@mail2tor.com and xratteam@email.tg providing the public key used by the ransomware to encrypt the files. Older versions of this ransomware also used e-mail accounts from another Email service – Protonmail, such as corporacaoxrat@protonmail.com, currently deactivated.

When the victim gets in touch with the group, they start to negotiate the ransom payment. All communication is in Portuguese and they request **1 btc** (about 603 USD) to decrypt the files. The group also claims that the payment is a "donation" arguing that "they exploited flaws in your system and carried out the attack in order to make sure you increase your security". Finally, the cybercriminals also offer to decrypt one file for free:

seus arquivos foram criptografados devido à falhas de segurança em seus sistemas. Para que nao aconteça novamente, e necessário aumentar a segurança do ambiente em questão, contratando alguma empresa especializada em segurança. Não são apenas anti virús que fazem toda a segurança da máquina. É necessário também um backup diário, para que seus dados não sejam perdidos. Exploramos diversas vulnerabilidades em sistemas, a fim de fazer o usuário dar valor à segurança de seus sistemas.

Eu te enviarei a chave para descryptografar seus arquivos, assim que a doação seja concluída, caso necessite, te ajudarei com o procedimento. Pra mim, não me interessa seus arquivos, mas sim a doação. Caso seja importante pra você seus arquivos, te aconselho a fazer a doação, caso contrário, perderá todos eles.

Para que possamos lhe fornecer a chave publica para que seus arquivos sejam descriptografados, necessitamos de uma doação no valor de BT 1,0 BITCOIN. Você pode verificar a cotação do bitcoin no seguinte site http://dolarhoje.com/bitcoin/#bitcoin=1
Somente aceitaremos a doação por este meio de pagamento,caso tenha interesse favor nos informar para que continuaremos o diálogo.

Como garantia, nos envie qualquer arquivo criptografado, que iremos te envia-lo descriptografado, para te mostrar que temos a chave para tal.

Aguardo contato

“For me only the ‘donation’ is important. Not your files. If your files are important to you, I advise you to make the donation; otherwise, you’ll lose all your files”

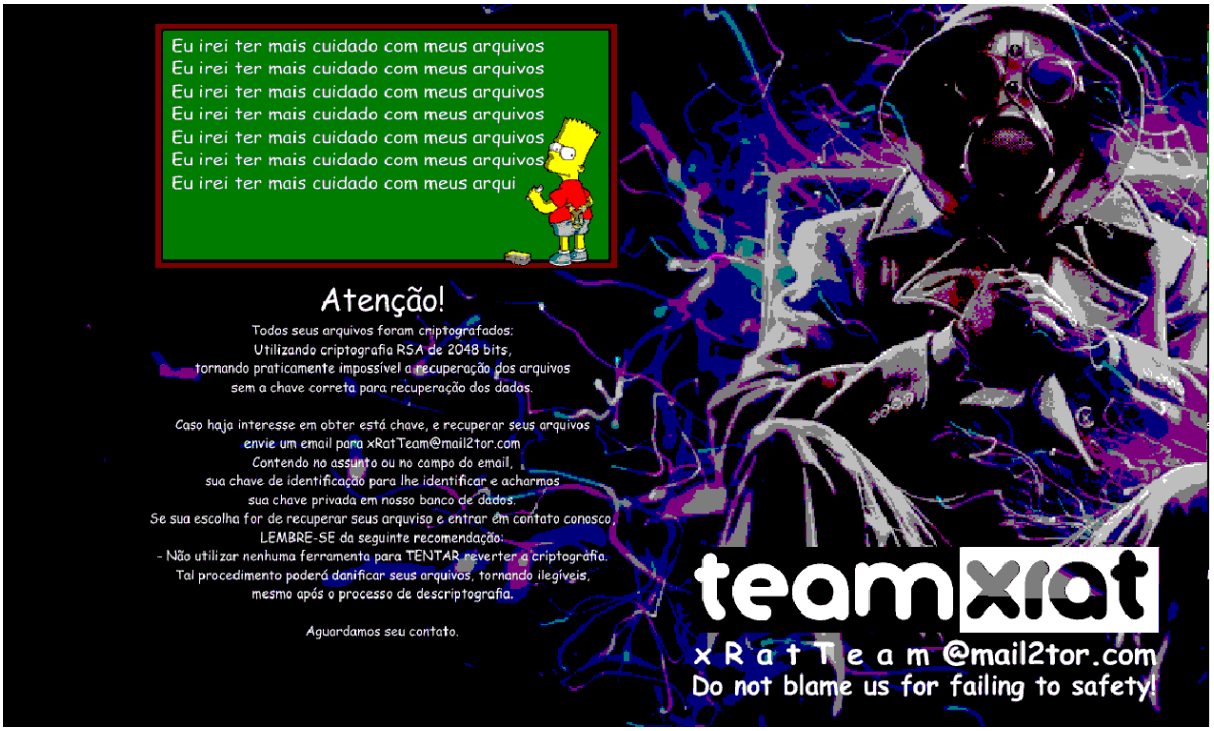
Xpan, how it works

The sample is UPX packed. Once executed it checks the default language of the infected system set in the following registry key: HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE

In addition, it’s able to query local time and obtain the computer name from the registry using several commands like net.exe, sc.exe, and taskkill.exe. Interestingly, it also deletes any Proxy setting defined in the system, located in: HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP.

Since the targets are companies and corporations, the group might use proxies blocking access to certain Web resources. It is highly probable that this technique is used to “set victim’s free” while emailing the attackers or accessing BTC resources online.

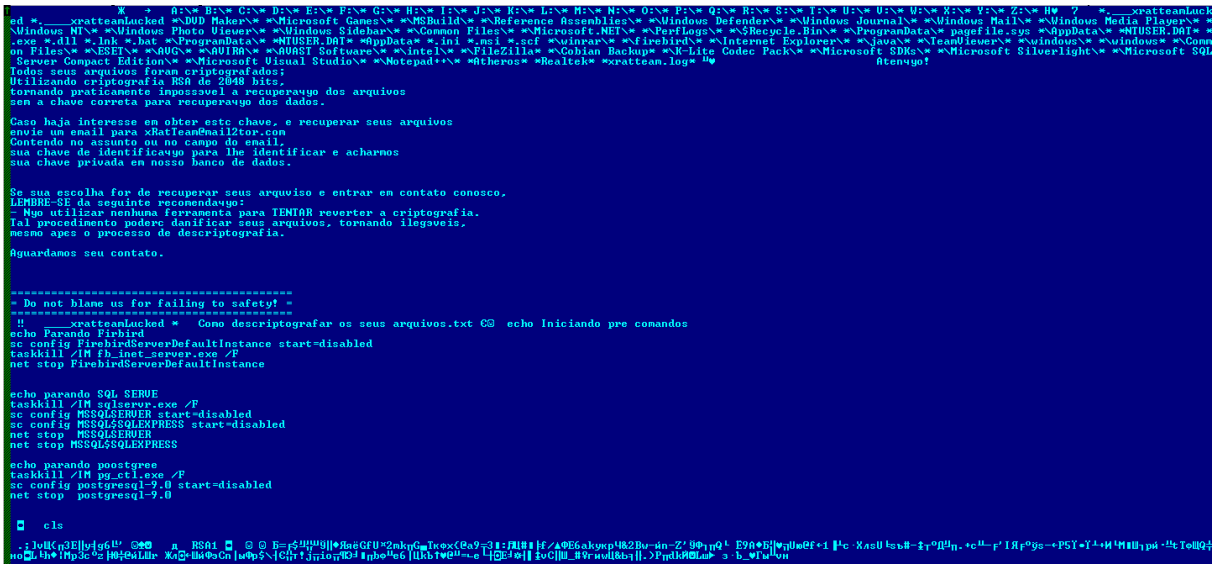
After completing its execution, the ransomware displays the following image in the affected system:



“All your files were encrypted using a RSA 2048 bits encryption”

The sample is written in C++ and uses STL, being built as a console application. During the lenght of its execution, it logs all its actions to the console, only to clear it once the encryption process has finished.

The operation of this malware is ‘guided’ by the configuration data block stored inside the body of the Trojan:



Decrypted configuration block

The configuration contains the following details:

- Drive letters which will be processed;
- Denylisted substrings: the files whose path contain any of these strings will not be encrypted;
- Ransomware text message for the victim;

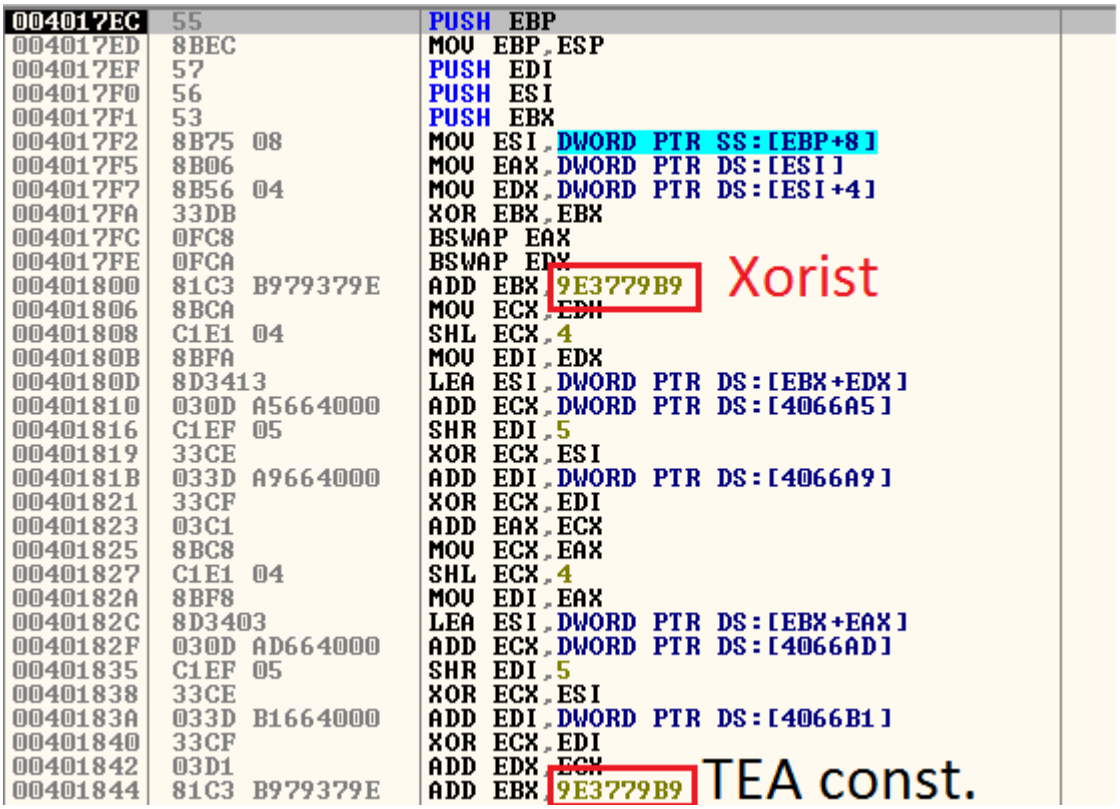
- Extension of the encrypted files (in this case, **.____xratteamLucked**);
- Name of the file with ransom notes;
- Console commands to be executed prior to the process of file encryption;
- Console commands to be executed after the encryption;
- A public RSA-2048 key in the MSBLOB format.

```
if ( (unsigned __int8)ParseConfig(ctx) )
{
  LaunchCommands(&ctx->consoleCommandsBefore);
  FindDrives(&v11);

  //...

  if ( !(unsigned __int8)LaunchThreads(ctx) )
  {
    if ( !(0xAAAAAAAB * ((signed int)(ctx->drives.size - (unsigned int)ctx->drives.ptr) >> 3)) )
    {
LABEL_16:
      SetWallpaper(ctx);
      SaveRansomNotes(ctx);
      LaunchCommands(&ctx->consoleCommandsAfter);
      return;
    }
    v10 = 0;
    while ( !pthread_f_1((int)ctx->threads[v10], &v11) )
    {
      if ( ++v10 >= 0xAAAAAAAB * ((signed int)(ctx->drives.size - (unsigned int)ctx->drives.ptr) >> 3) )
        goto LABEL_16;
    }
  }
  Error(ctx, 16, L"ERRO: codigo de retorno do pthread_create() = %d\n");
  goto LABEL_16;
}
Error(ctx, 16, L"Crypter com problemas. Falha ao carregar configuracao.");
}
```

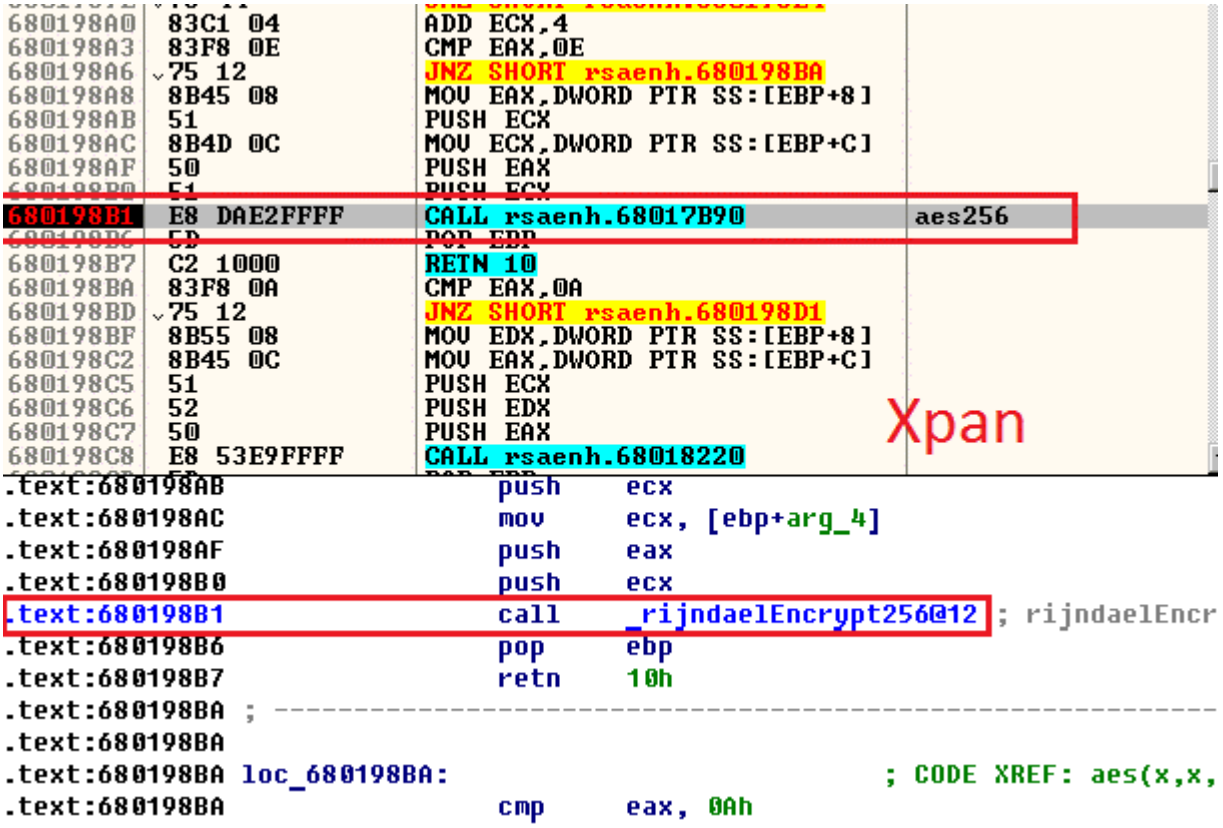
Part of the pseudocode of the main procedure

From Xorist to Xpan

A previous ransomware sample that was believed to be part of the TeamXRat ransomware campaign used a simple encryption algorithm known as TEA (or Tiny Encryption Algorithm). After comparing this original version (dubbed Xorist) against this new Xpan variant, we could observe that now they are using an AES-256 encryption scheme.



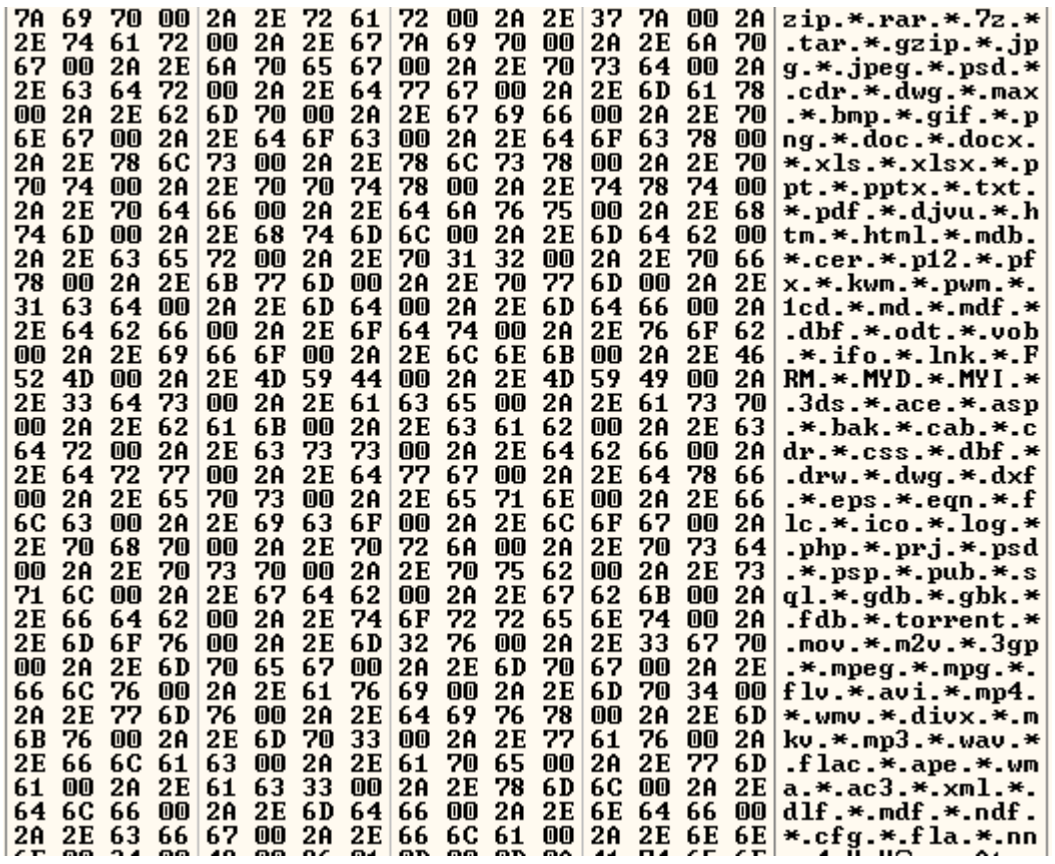
Xorist ransomware TEA constant



Xpan ransomware now has evolved to use AES-256 encryption

Xorist	Xpan
Will automatically start when user is logged in. It uses the following registry key for persistence: SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run	No persistence used.
Tiny Encryption Algorithm	AES-256
ASM, MS Linker	C++, MinGW compiler
Includes a list of files that are to be encrypted.	Will encrypt everything except .exe and .dll files and files with denylisted substrings in the path.

The developers have clearly shifted their development procedures in the Xpan malware. It's typical for cybercriminals to evolve their techniques once a decryption method has been found for their ransomware, or that specific variant is widely detected.



List of file extensions that Xorist ransomware will search and encrypt

File Encryption

The trojan uses the implementation of cryptographic algorithms provided by MS CryptoAPI. The files are encrypted by AES-256 in CBC mode.

There are 2 known versions of this trojan that can be distinguished by their extensions. The 1st one uses **“___xratteamLucked”** (3 ‘_’ symbols) and the second one – **“____xratteamLucked”** (4 ‘_’ symbols).

These 2 versions employ different techniques to encrypt the files, which we will describe in more detail.

Version 1 (3 ‘_’ symbols in the extension)

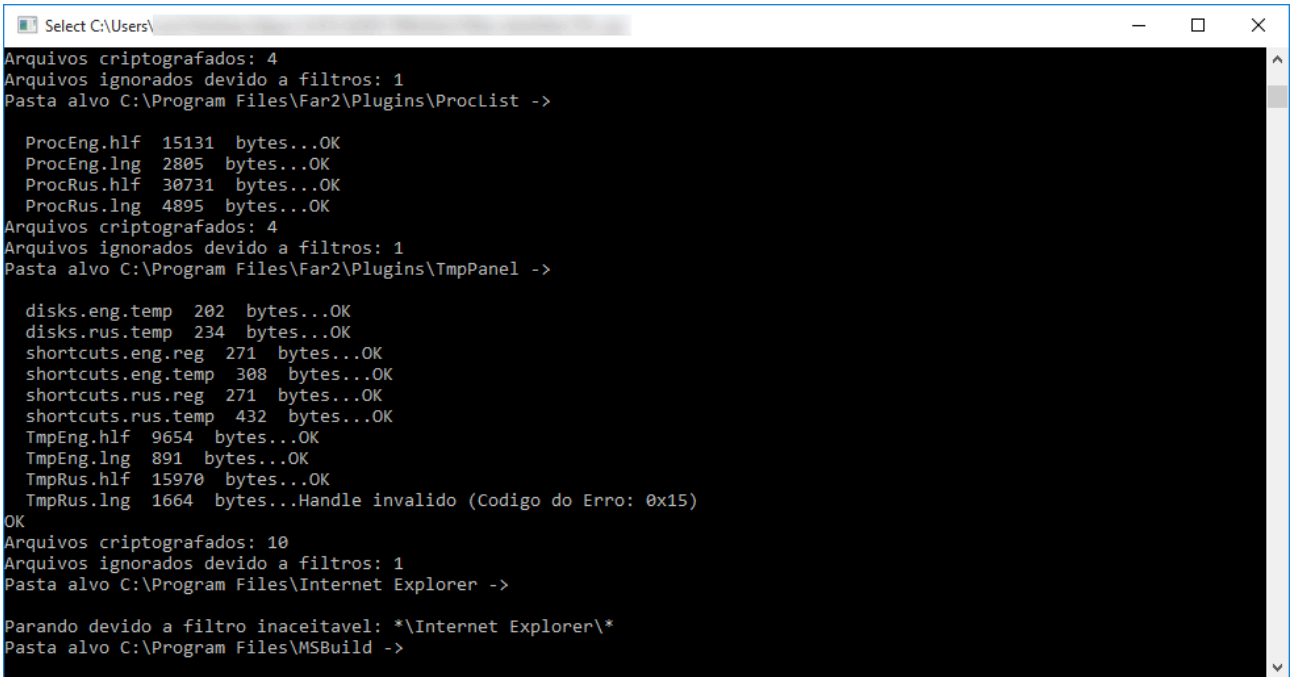
The trojan generates a single 255-symbol password for all files. This password is encrypted by RSA-2048 and put into the ransom note (concatenated with the public key). Then the trojan produces a 256-bit key from this password using the API CryptDeriveKey; this key will be used to encrypt all files.

When processing each file, the malware adds the string *‘NMoreira’* to the beginning of the original file and encrypts the file content by 245-byte blocks using the AES-256 algorithm in CBC mode. Each block is additionally XOR’ed with a random byte which is stored before the padding of the corresponding block.

Version 2 (4 ‘_’ symbols in the extension)

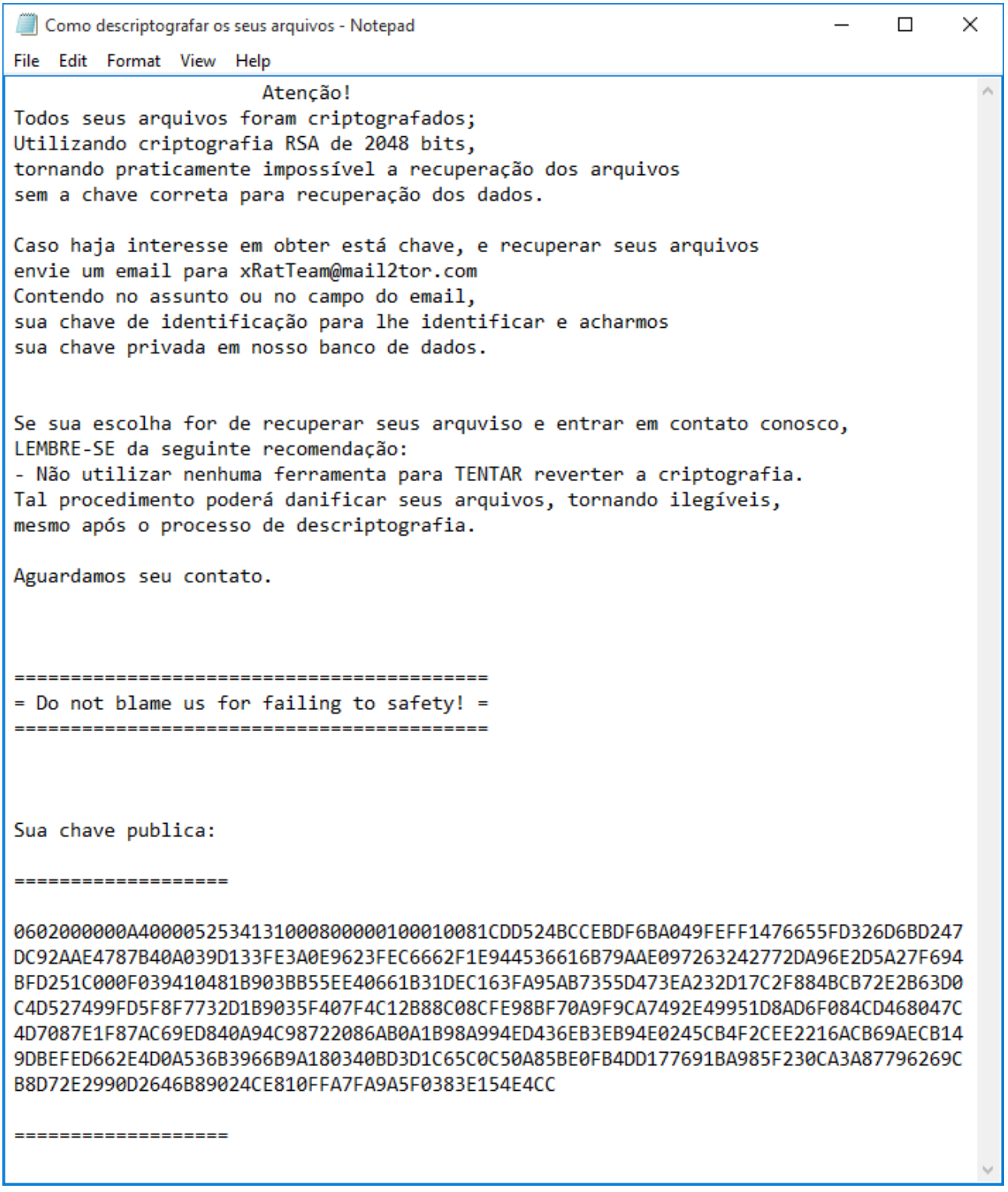
For each file, the trojan generates a new 255-symbol password, encrypts this password by RSA-2048 and puts this data into the beginning of each encrypted file. Then, the trojan produces a 256-bit key from this password using the API CryptDeriveKey, and uses this key to encrypt the original file content (AES-256 CBC).

File search and encryption is carried out by multiple threads, each thread processes its disk.



Ransomware in action: console output inform the files encrypted

After encryption is completed, the malware will change the wallpaper in the desktop and display this file, with the ransom note:



The ransom note, in Portuguese

Before encrypting the data in the affected system, the ransomware executes the following commands, aiming to stop popular database services, to be sure that database files will be encrypted as well, so they cause a greater damage to the victim:

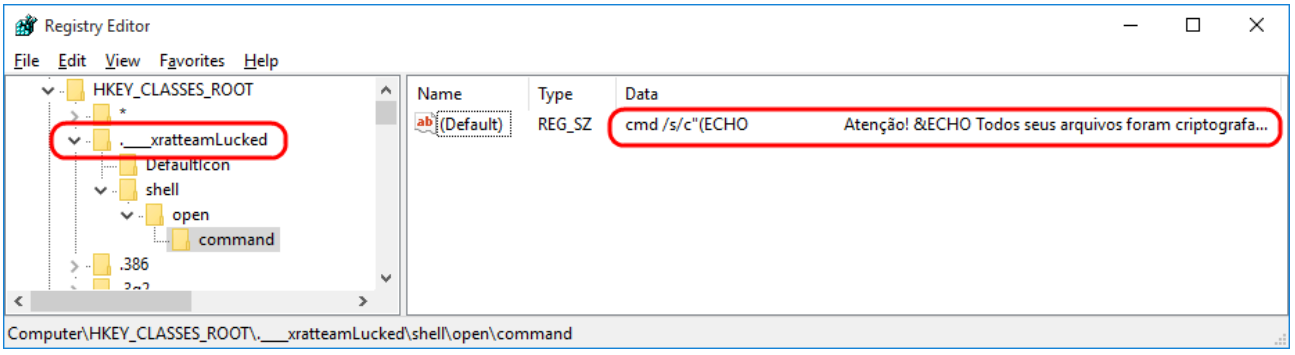
echo Iniciando pre comandos

```
echo Parando Firbird
sc config FirebirdServerDefaultInstance start=disabled
taskkill /IM fb_inet_server.exe /F
net stop FirebirdServerDefaultInstance

echo parando SQL SERVE

taskkill /IM sqlservr.exe /F
sc config MSSQLSERVER start=disabled
sc config MSSQL$SQLEXPRESS start=disabled
net stop MSSQLSERVER
net stop MSSQL$SQLEXPRESS

echo parando poostgree
taskkill /IM pg_ctl.exe /F
sc config postgresql-9.0 start=disabled
net stop postgresql-9.0
```

After the execution, the ransomware deletes itself from the system, to remove the original infector:

```
@echo off
goto Delete
:WaitAndDelete
@timeout 5
:Delete
@del “path\sample_name.exe”
if exist “path\sample_name.exe”
goto WaitAndDelete
@del %0
```

After the encryption has finished, the trojan modifies the registry to add a custom handler for the action of double-clicking on any of the encrypted files. As a result, when the victim clicks on a file with the extension “**.____xratteamLucked**“, the command stored in the registry is executed, and this command shows the ransom notes in a new window using msg.exe (a standard utility which is a part of Windows distribution).



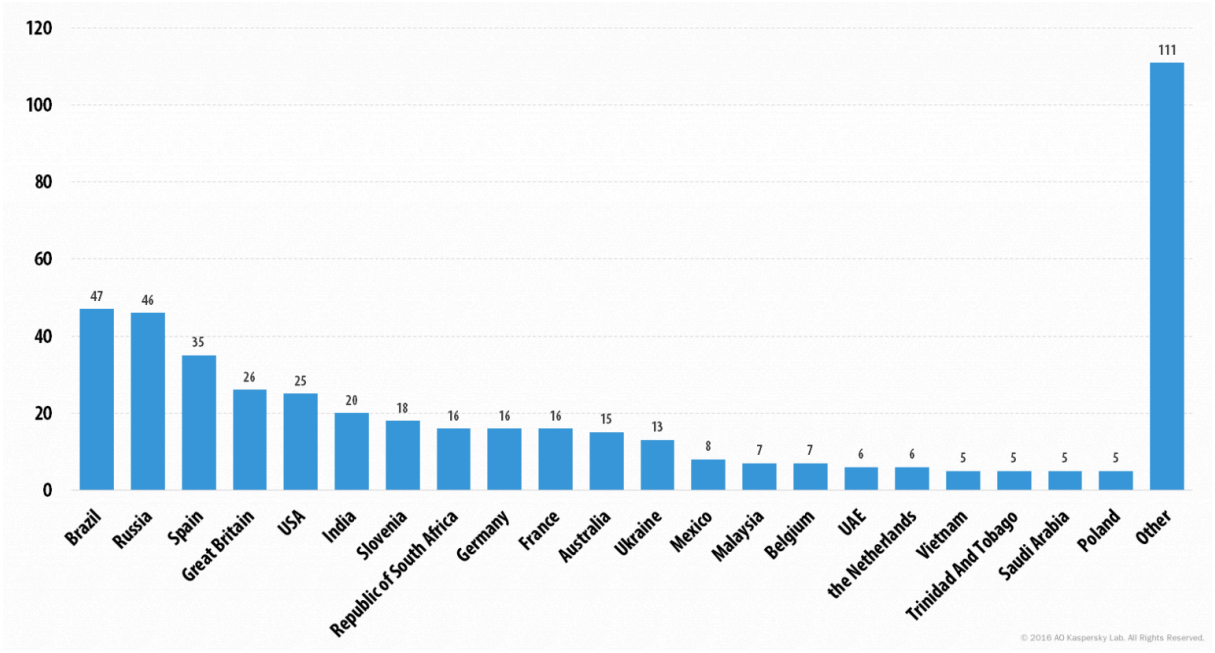
Windows Registry modified by the ransom

How they attack

Most of the attacks performed by TeamXRat are performed manually, installing the ransomware in the hacked server. To achieve that, they perform **RDP (Remote Desktop Protocol) brute force attacks**. Connecting remote desktop servers directly to the Internet is not recommended and brute forcing them is nothing new; but without the proper controls in place to prevent or at least detect and respond to compromised machines, brute force RDP attacks are still relevant and something that cybercriminals enjoy. Once the server is compromised, the attacker manually disables the Antivirus product installed on the server and proceeds with the infection itself.

We are also aware that vulnerabilities such as MS15-067 and MS15-030 in the RDP protocol, which allow remote code execution if an attacker sends a specially crafted sequence of packets to a targeted system, can be used by cybercriminals if a server is not patched and exposed to attacks.

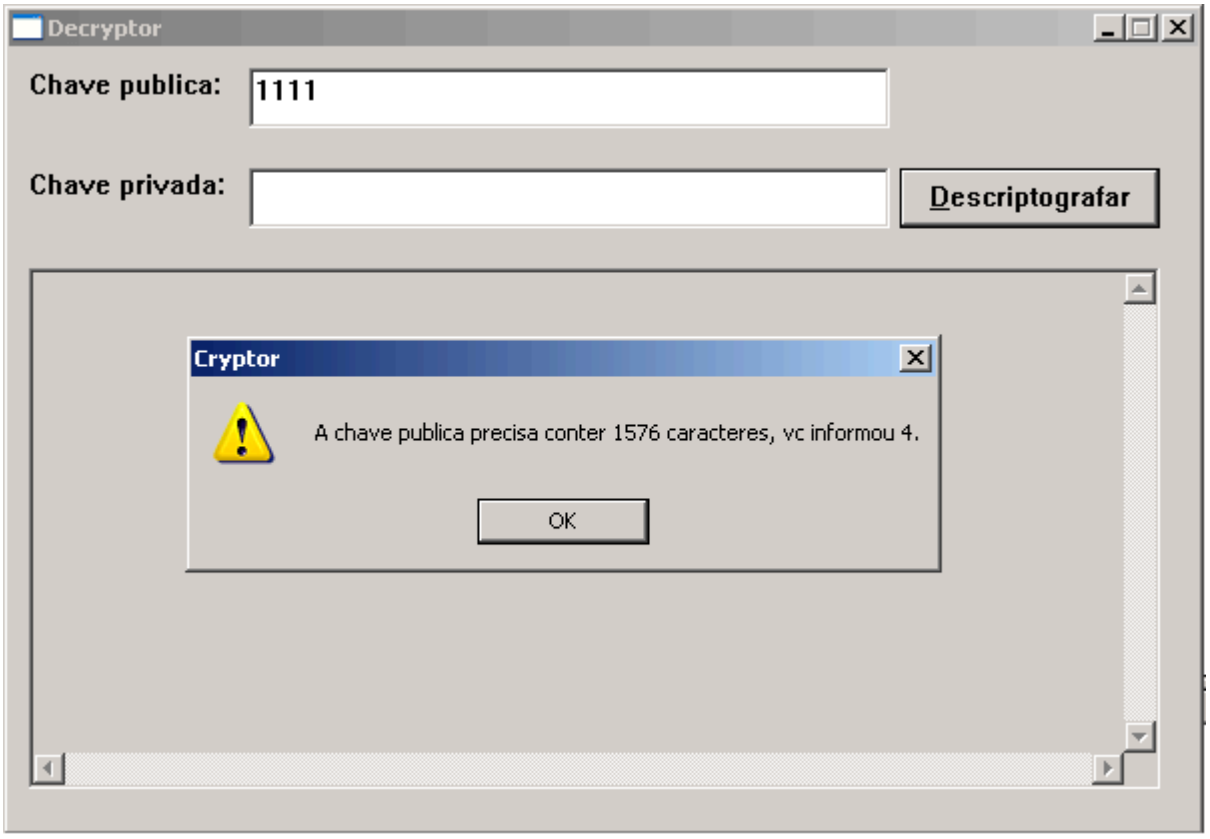
As we saw in the recent xDedic research, vulnerable servers with exposed RDP connections are very valuable assets in the hands of cybercriminals. Not surprisingly, Brazil was the country with the most compromised servers being offered in the underground market to any cybercriminal.



xDedic: compromised Brazilian RDP servers were available in the underground market

Decryption: we can help!

If the victim pays the ransom, the cybercriminals will send this tool to decrypt the files:



Decryption tool sent by the bad guy after payment

But the good news is that the Kaspersky Anti-Ransom team was able to break the encryption used by the Xpan Trojan. This effort made possible the decryption of files belonging to a Hospital in Brazil, which was hit by this Ransomware family.

If you're a victim of this new Ransomware family and need help to decrypt your files, please DON'T PAY the ransom. Instead, contact us via support.

Conclusion

As we can see, Brazilian bad guys are now diversifying their "business" with new ransomware families developed from scratch, abandoning older versions that used XOR encryption and adopting new, more robust encryption algorithms. This is a clear signal that they have started to explore new schemes with new targets and newer types of attacks.

As we forecasted in the beginning of this year, we expect ransomware attacks to gain ground on banking trojans and to transition into other platforms. Ransomware has two advantages over traditional banking threats: direct monetization using an anonymous payment system (usually Bitcoin), and relatively low cost per victim. Certainly, this is very attractive to Brazilian crooks, well-known for their banking trojans development. Brazilian law enforcement is very good at catching criminals (although they are not always convicted and imprisoned) by "following the money", something that we know it's not entirely possible for Bitcoin payments.

We detect this new threat as
Trojan-Ransom.Win32.Xpan.a and **PDM:Trojan.Win32.Generic.**

We’ll keep an eye out or new variants, which surely will appear from same or other threat actors.

MD5 reference: *34260178f9e3b2e769accdee56dac793*
