

# TeamXRat: Brazilian cybercrime meets ransomware

SL [securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/](https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/)



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 vírus 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 decryptografar 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 decryptografados, 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 decryptografado, 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:

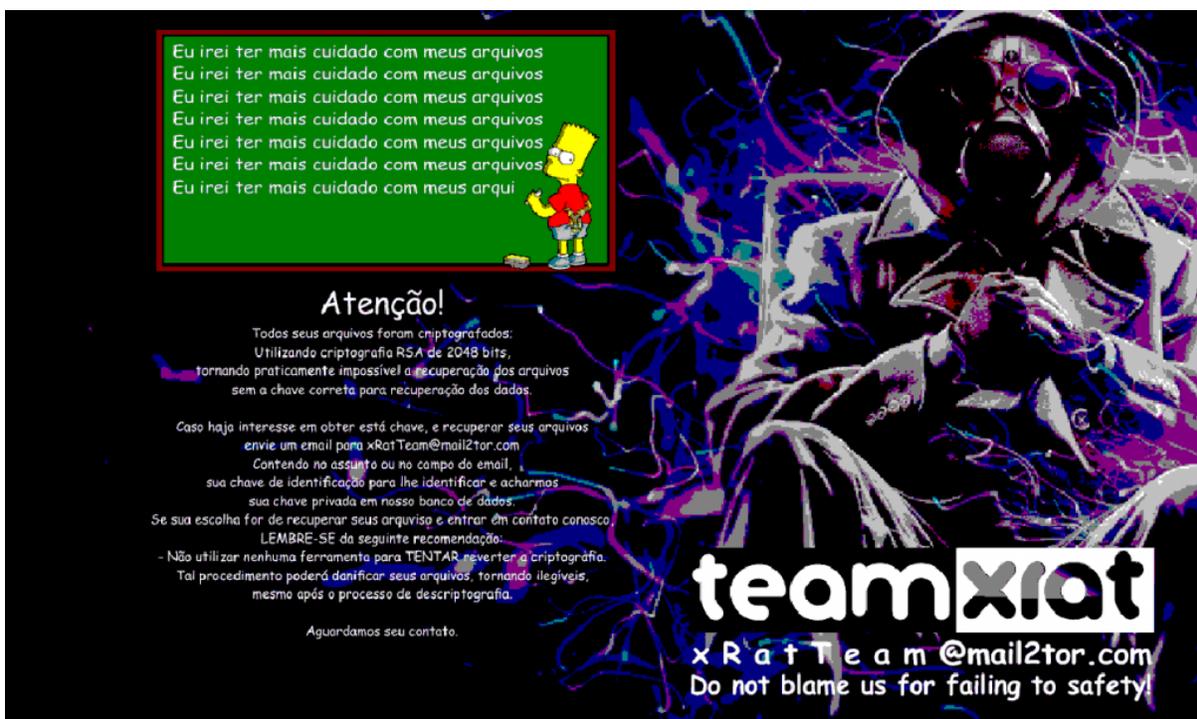
HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE

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”*



```

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

    //...

    if ( !(unsigned __int8)LaunchThreads(ctx) )
    {
        if ( !(0xAAAAAAB * ((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 >= 0xAAAAAAB * ((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.

004017EC	55		PUSH EBP
004017ED	8BEC		MOV EBP, ESP
004017EF	57		PUSH EDI
004017F0	56		PUSH ESI
004017F1	53		PUSH EBX
004017F2	8B75 08		MOV ESI, DWORD PTR SS:[EBP+8]
004017F5	8B06		MOV EAX, DWORD PTR DS:[ESI]
004017F7	8B56 04		MOV EDX, DWORD PTR DS:[ESI+4]
004017FA	33DB		XOR EBX, EBX
004017FC	0FC8		BSWAP EAX
004017FE	0FCA		BSWAP EDX
00401800	81C3 B979379E		ADD EBX, 9E3779B9 Xorist
00401806	8BCA		MOV ECX, EDI
00401808	C1E1 04		SHL ECX, 4
0040180B	8BFA		MOV EDI, EDX
0040180D	8D3413		LEA ESI, DWORD PTR DS:[EBX+EDX]
00401810	030D A5664000		ADD ECX, DWORD PTR DS:[4066A5]
00401816	C1EF 05		SHR EDI, 5
00401819	33CE		XOR ECX, ESI
0040181B	033D A9664000		ADD EDI, DWORD PTR DS:[4066A9]
00401821	33CF		XOR ECX, EDI
00401823	03C1		ADD EAX, ECX
00401825	8BC8		MOV ECX, EAX
00401827	C1E1 04		SHL ECX, 4
0040182A	8BF8		MOV EDI, EAX
0040182C	8D3403		LEA ESI, DWORD PTR DS:[EBX+EAX]
0040182F	030D AD664000		ADD ECX, DWORD PTR DS:[4066AD]
00401835	C1EF 05		SHR EDI, 5
00401838	33CE		XOR ECX, ESI
0040183A	033D B1664000		ADD EDI, DWORD PTR DS:[4066B1]
00401840	33CF		XOR ECX, EDI
00401842	03D1		ADD EDX, ECX
00401844	81C3 B979379E		ADD EBX, 9E3779B9 TEA const.

Xorist ransomware TEA constant

680198A0	83C1 04		ADD ECX, 4
680198A3	83F8 0E		CMP EAX, 0E
680198A6	75 12		JNZ SHORT rsaenh.680198BA
680198A8	8B45 08		MOV EAX, DWORD PTR SS:[EBP+8]
680198AB	51		PUSH ECX
680198AC	8B4D 0C		MOV ECX, DWORD PTR SS:[EBP+C]
680198AF	50		PUSH EAX
680198B0	51		PUSH ECX
680198B1	E8 DAE2FFFF		CALL rsaenh.68017B90 aes256
680198B6	5D		POP EBP
680198B7	C2 1000		RETN 10
680198BA	83F8 0A		CMP EAX, 0A
680198BD	75 12		JNZ SHORT rsaenh.680198D1
680198BF	8B55 08		MOV EDX, DWORD PTR SS:[EBP+8]
680198C2	8B45 0C		MOV EAX, DWORD PTR SS:[EBP+C]
680198C5	51		PUSH ECX
680198C6	52		PUSH EDX
680198C7	50		PUSH EAX
680198C8	E8 53E9FFFF		CALL rsaenh.68018220 Xpan

```

.text:680198AB      push     ecx
.text:680198AC      mov     ecx, [ebp+arg_4]
.text:680198AF      push     eax
.text:680198B0      push     ecx
.text:680198B1      call    _rijndaelEncrypt256@12 ; rijndaelEncr
.text:680198B6      pop     ebp
.text:680198B7      retn    10h
.text:680198BA      ; -----
.text:680198BA      ;
.text:680198BA      loc_680198BA: ; CODE XREF: aes(x,x,
.text:680198BA      cmp     eax, 0Ah

```

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.

```

7A 69 70 00 2A 2E 72 61 72 00 2A 2E 37 7A 00 2A zip.*.rar.*.7z.*
2E 74 61 72 00 2A 2E 67 7A 69 70 00 2A 2E 6A 70 .tar.*.gzip.*.jp
67 00 2A 2E 6A 70 65 67 00 2A 2E 70 73 64 00 2A g.*.jpeg.*.psd.*
2E 63 64 72 00 2A 2E 64 77 67 00 2A 2E 6D 61 78 .cdr.*.dwg.*.max
00 2A 2E 62 6D 70 00 2A 2E 67 69 66 00 2A 2E 70 .*.*.bmp.*.gif.*.p
6E 67 00 2A 2E 64 6F 63 00 2A 2E 64 6F 63 78 00 ng.*.doc.*.docx.
2A 2E 78 6C 73 00 2A 2E 78 6C 73 78 00 2A 2E 70 *.xls.*.xlsx.*.p
70 74 00 2A 2E 70 70 74 78 00 2A 2E 74 78 74 00 pt.*.pptx.*.txt.
2A 2E 70 64 66 00 2A 2E 64 6A 76 75 00 2A 2E 68 *.pdf.*.djvu.*.h
74 6D 00 2A 2E 68 74 6D 6C 00 2A 2E 6D 64 62 00 tm.*.html.*.mdb.
2A 2E 63 65 72 00 2A 2E 70 31 32 00 2A 2E 70 66 *.cer.*.p12.*.pf
78 00 2A 2E 6B 77 6D 00 2A 2E 70 77 6D 00 2A 2E x.*.kwm.*.pwm.*.
31 63 64 00 2A 2E 6D 64 00 2A 2E 6D 64 66 00 2A 1cd.*.md.*.mdf.*
2E 64 62 66 00 2A 2E 6F 64 74 00 2A 2E 76 6F 62 .dbf.*.odt.*.vob
00 2A 2E 69 66 6F 00 2A 2E 6C 6E 6B 00 2A 2E 46 *.ifo.*.lnk.*.F
52 4D 00 2A 2E 4D 59 44 00 2A 2E 4D 59 49 00 2A RM.*.MYD.*.MYI.*
2E 33 64 73 00 2A 2E 61 63 65 00 2A 2E 61 73 70 .3ds.*.ace.*.asp
00 2A 2E 62 61 6B 00 2A 2E 63 61 62 00 2A 2E 63 *.bak.*.cab.*.c
64 72 00 2A 2E 63 73 73 00 2A 2E 64 62 66 00 2A dr.*.css.*.dbf.*
2E 64 72 77 00 2A 2E 64 77 67 00 2A 2E 64 78 66 .drw.*.dwg.*.dxf
00 2A 2E 65 70 73 00 2A 2E 65 71 6E 00 2A 2E 66 *.eps.*.eqn.*.f
6C 63 00 2A 2E 69 63 6F 00 2A 2E 6C 6F 67 00 2A lc.*.ico.*.log.*
2E 70 68 70 00 2A 2E 70 72 6A 00 2A 2E 70 73 64 .php.*.prj.*.psd
00 2A 2E 70 73 70 00 2A 2E 70 75 62 00 2A 2E 73 *.psp.*.pub.*.s
71 6C 00 2A 2E 67 64 62 00 2A 2E 67 62 6B 00 2A ql.*.gdb.*.gbk.*
2E 66 64 62 00 2A 2E 74 6F 72 72 65 6E 74 00 2A .fdb.*.torrent.*
2E 6D 6F 76 00 2A 2E 6D 32 76 00 2A 2E 33 67 70 .mov.*.m2v.*.3gp
00 2A 2E 6D 70 65 67 00 2A 2E 6D 70 67 00 2A 2E *.mpeg.*.mpg.*
66 6C 76 00 2A 2E 61 76 69 00 2A 2E 6D 70 34 00 flv.*.avi.*.mp4.
2A 2E 77 6D 76 00 2A 2E 64 69 76 78 00 2A 2E 6D *.wmv.*.divx.*.m
6B 76 00 2A 2E 6D 70 33 00 2A 2E 77 61 76 00 2A kv.*.mp3.*.wav.*
2E 66 6C 61 63 00 2A 2E 61 70 65 00 2A 2E 77 6D .flac.*.ape.*.wm
61 00 2A 2E 61 63 33 00 2A 2E 78 6D 6C 00 2A 2E a.*.ac3.*.xml.*
64 6C 66 00 2A 2E 6D 64 66 00 2A 2E 6E 64 66 00 dlf.*.mdf.*.ndf.
2A 2E 63 66 67 00 2A 2E 66 6C 61 00 2A 2E 6E 6E *.cfg.*.fla.*.nn

```

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)

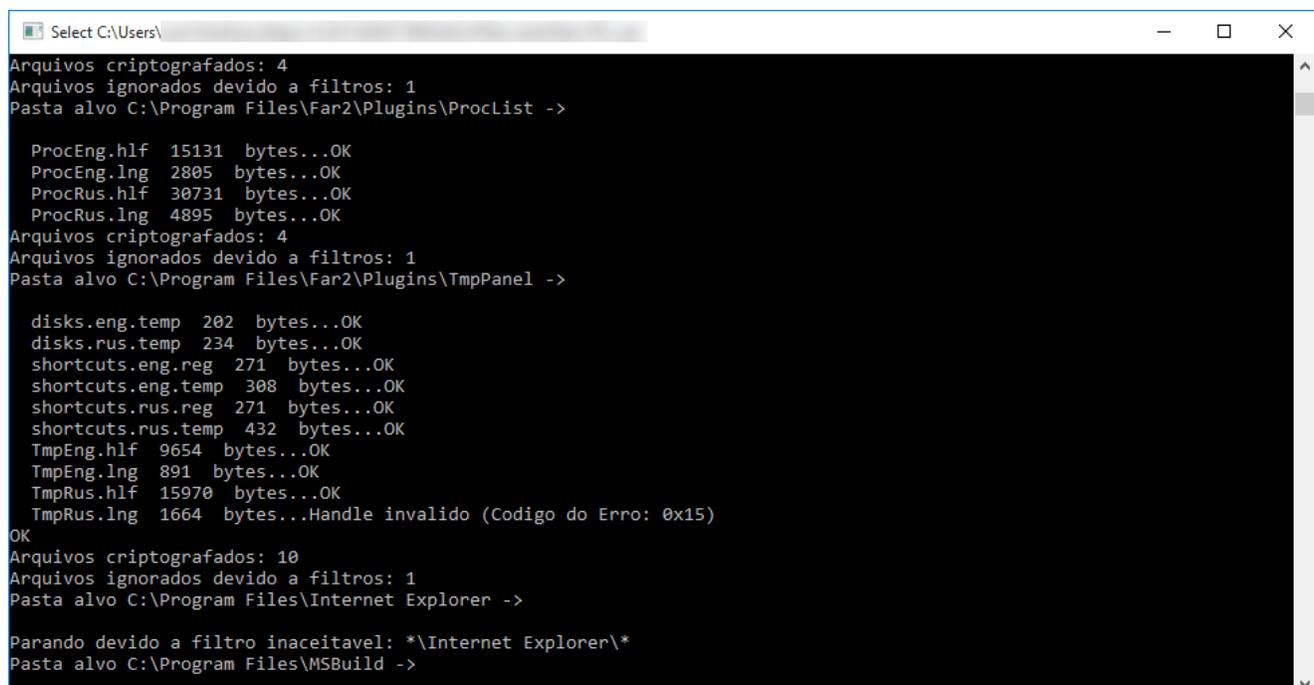
The trojan generates a single 255-symbol password for all files. This password is encrypted by RSA-2048 and put into the ransom note (concatenated with the public key). Then the trojan produces a 256-bit key from this password using the API CryptDeriveKey; this key will be used to encrypt all files.

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.



```
Select C:\Users\...
Arquivos criptografados: 4
Arquivos ignorados devido a filtros: 1
Pasta alvo C:\Program Files\Far2\Plugins\ProcList ->

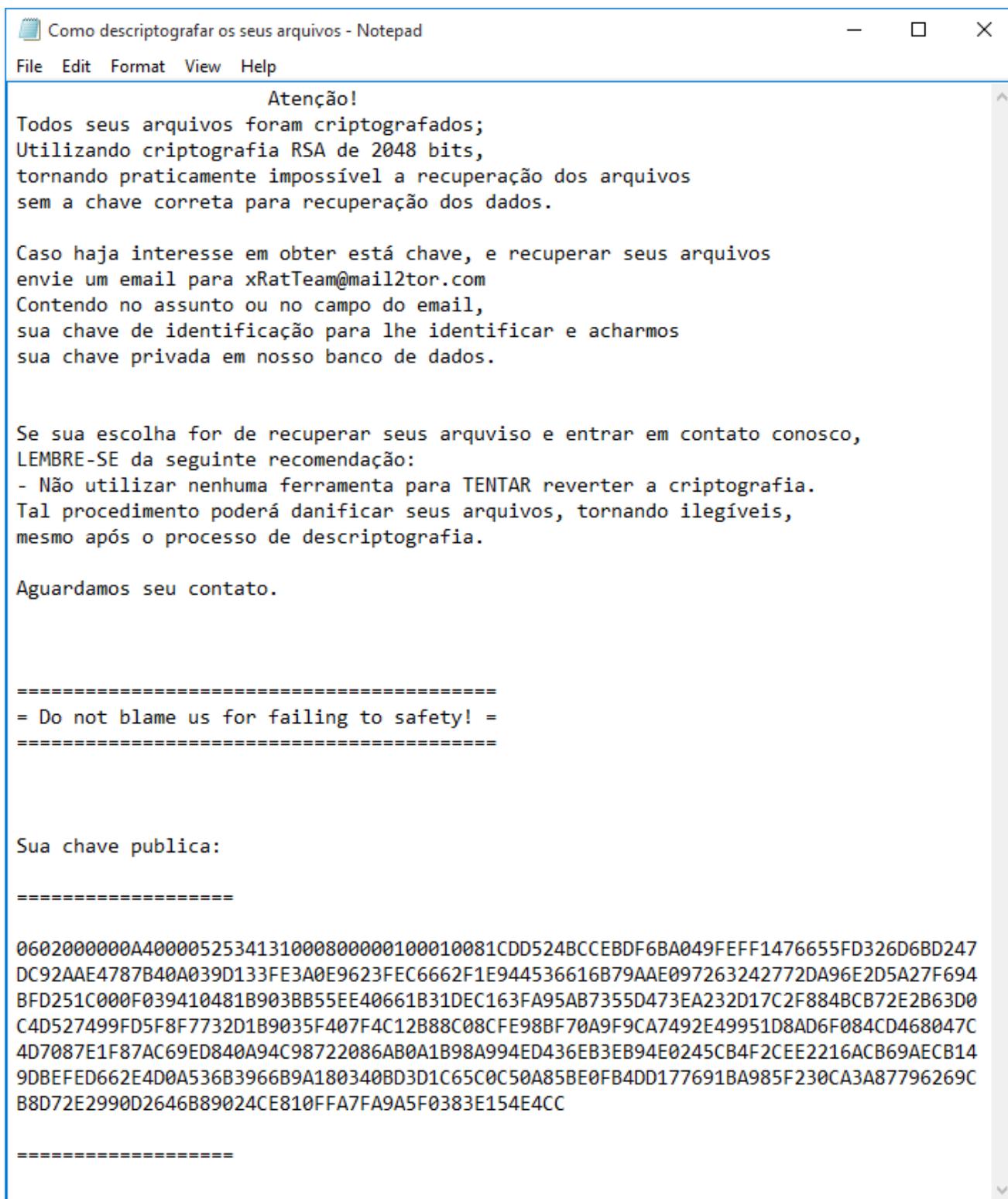
  ProcEng.hlf 15131 bytes...OK
  ProcEng.lng 2805 bytes...OK
  ProcRus.hlf 30731 bytes...OK
  ProcRus.lng 4895 bytes...OK
Arquivos criptografados: 4
Arquivos ignorados devido a filtros: 1
Pasta alvo C:\Program Files\Far2\Plugins\TmpPanel ->

  disks.eng.temp 202 bytes...OK
  disks.rus.temp 234 bytes...OK
  shortcuts.eng.reg 271 bytes...OK
  shortcuts.eng.temp 308 bytes...OK
  shortcuts.rus.reg 271 bytes...OK
  shortcuts.rus.temp 432 bytes...OK
  TmpEng.hlf 9654 bytes...OK
  TmpEng.lng 891 bytes...OK
  TmpRus.hlf 15970 bytes...OK
  TmpRus.lng 1664 bytes...Handle invalido (Codigo do Erro: 0x15)
OK
Arquivos criptografados: 10
Arquivos ignorados devido a filtros: 1
Pasta alvo C:\Program Files\Internet Explorer ->

Parando devido a filtro inaceitavel: *\Internet Explorer\*
Pasta alvo C:\Program Files\MSBuild ->
```

## 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:



```
Como descriptografar os seus arquivos - Notepad
File Edit Format View Help

                Atenção!
Todos seus arquivos foram criptografados;
Utilizando criptografia RSA de 2048 bits,
tornando praticamente impossível a recuperação dos arquivos
sem a chave correta para recuperação dos dados.

Caso haja interesse em obter está chave, e recuperar seus arquivos
envie um email para xRatTeam@mail2tor.com
Contendo no assunto ou no campo do email,
sua chave de identificação para lhe identificar e acharmos
sua chave privada em nosso banco de dados.

Se sua escolha for de recuperar seus arquivo e entrar em contato conosco,
LEMBRE-SE da seguinte recomendação:
- Não utilizar nenhuma ferramenta para TENTAR reverter a criptografia.
Tal procedimento poderá danificar seus arquivos, tornando ilegíveis,
mesmo após o processo de descriptografia.

Aguardamos seu contato.

=====
= Do not blame us for failing to safety! =
=====

Sua chave publica:

=====

0602000000A4000052534131000800000100010081CDD524BCCEBDF6BA049FEFF1476655FD326D6BD247
DC92AAE4787B40A039D133FE3A0E9623FEC6662F1E944536616B79AAE097263242772DA96E2D5A27F694
BFD251C000F039410481B903BB55EE40661B31DEC163FA95AB7355D473EA232D17C2F884BCB72E2B63D0
C4D527499FD5F8F7732D1B9035F407F4C12B88C08CFE98BF70A9F9CA7492E49951D8AD6F084CD468047C
4D7087E1F87AC69ED840A94C98722086AB0A1B98A994ED436EB3EB94E0245CB4F2CEE2216ACB69AECB14
9DBEFED662E4D0A536B3966B9A180340BD3D1C65C0C50A85BE0FB4DD177691BA985F230CA3A87796269C
B8D72E2990D2646B89024CE810FFA7FA9A5F0383E154E4CC

=====
```

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
```

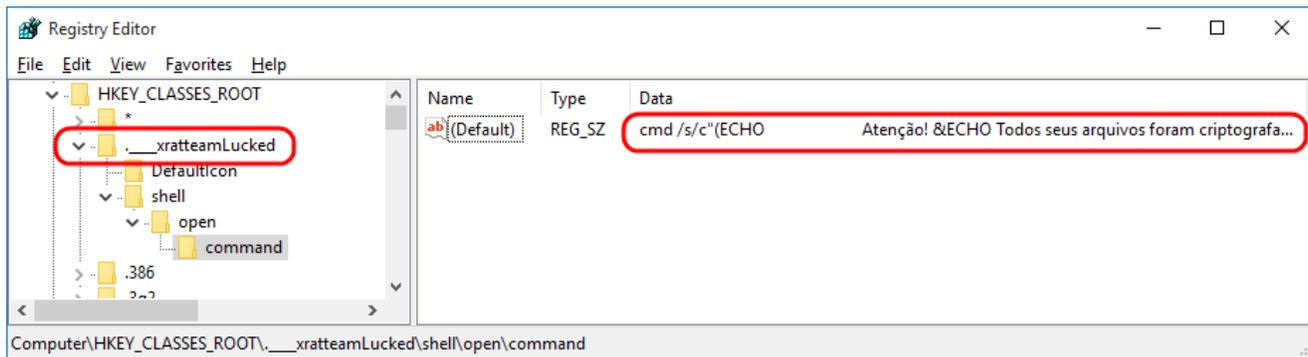
```
@del "path\sample_name.exe"
```

```
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).



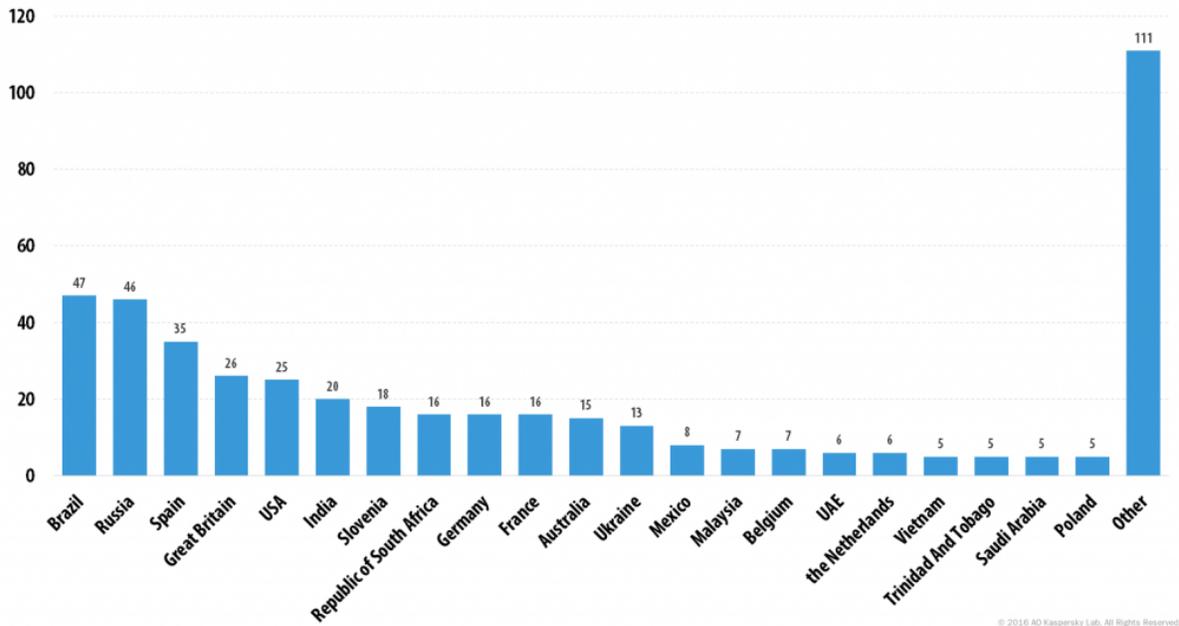
*Windows Registry modified by the ransom*

## 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.

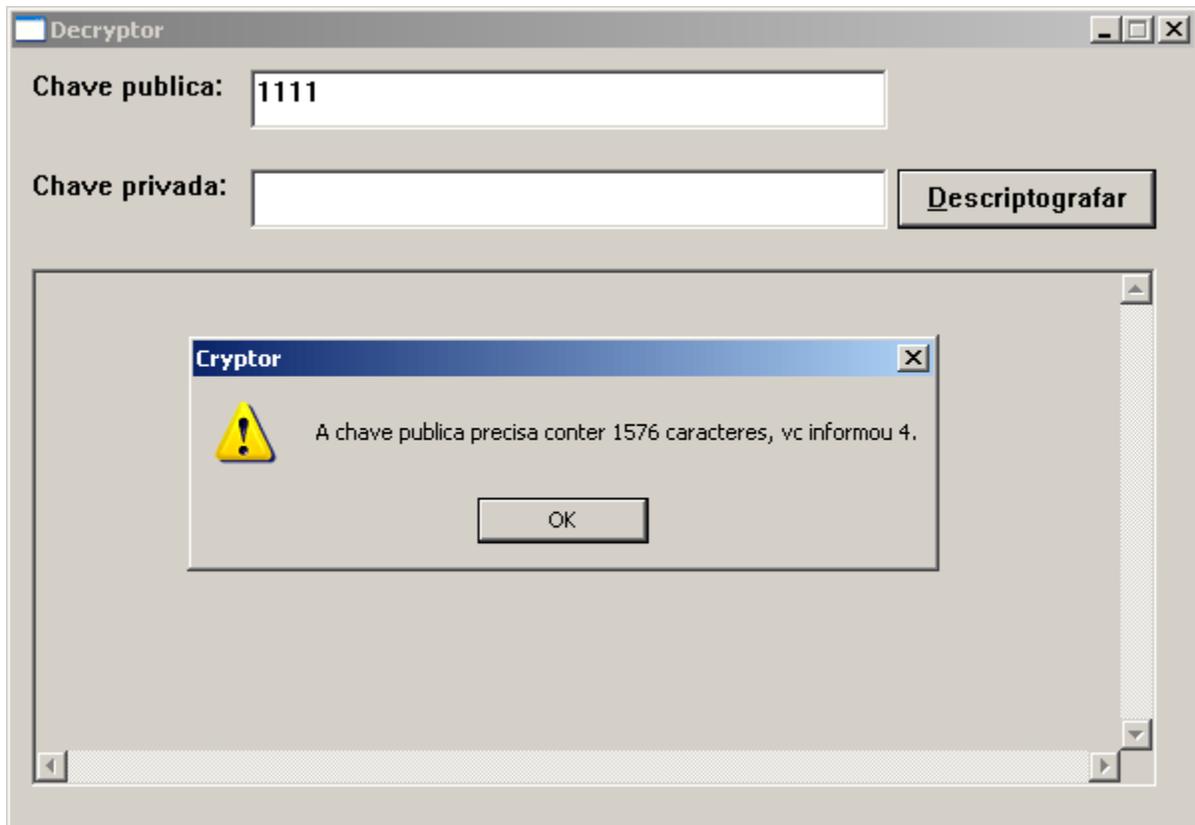
As we saw in the recent [xDedic](#) research, vulnerable servers with exposed RDP connections are very valuable assets in the hands of cybercriminals. Not surprisingly, Brazil was the country with the most compromised servers being offered in the underground market to any cybercriminal.



*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*