XPan, I am your father

securelist.com/blog/research/78110/xpan-i-am-your-father/

Authors

- Expert Anton Ivanov
-  Fabio Assolini
- Expert Fedor Sinitsyn
-  Santiago Pontiroli

.one ransomware decrypted

While we have previously written on the now infamous XPan ransomware family, some of it's variants are still affecting users primarily located in Brazil. Harvesting victims via weakly protected RDP (remote desktop protocol) connections, criminals are manually installing the ransomware and encrypting any files which can be found on the system.

Interestingly, this XPan variant is not necessarily new in the malware ecosystem. However, someone has chosen to keep on infecting victims with it, encouraging security researchers to hunt for samples related to the increasing number of incident reports. This sample is what could be considered as the “father” of other XPan ransomware variants. A considerable amount of indicators within the source code depict the early origins of this sample.

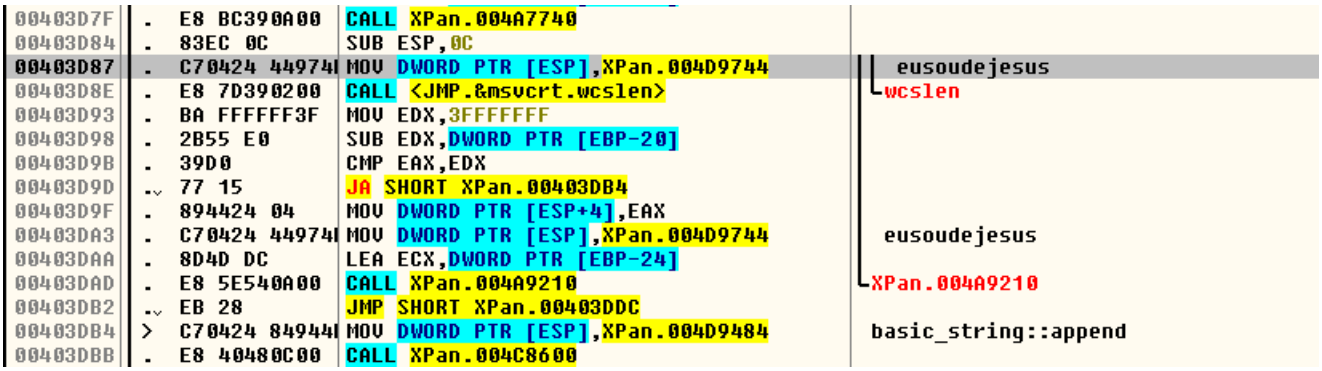
“Recupere seus arquivos aqui.txt” loosely translated to “recover your files here” is a phrase that not many Brazilian users are eager to see in their desktops.

The ransomware author left a message for Kaspersky in other versions and has done the same in this one, with traces to the NMoreira “CrypterApp.cpp” there’s a clear link between different variants among this malware family.

```
00403697  >  C74424 08 0F(  MOV DWORD PTR [ESP+8],40F
0040369F  .  C74424 04 90(  MOV DWORD PTR [ESP+4],XPan.004D9590     C:\zCr\NMoreira\NMoreira_Crypter\src\CrypterApp.cpp
004036A7  .  C70424 F8954(  MOV DWORD PTR [ESP],XPan.004D95F8       erro == 0
004036AE  .  E8 3D490100    CALL XPan.00417FF0
004036B3  .^ E9 DDFEFFFF    JMP XPan.00403595
004036B8  >  C74424 08 11(  MOV DWORD PTR [ESP+8],411
004036C0  .  C74424 04 90(  MOV DWORD PTR [ESP+4],XPan.004D9590     C:\zCr\NMoreira\NMoreira_Crypter\src\CrypterApp.cpp
004036C8  .  C70424 F8954(  MOV DWORD PTR [ESP],XPan.004D95F8       erro == 0
004036CF  .  E8 1C490100    CALL XPan.00417FF0
004036D4  .^ E9 D8FEFFFF    JMP XPan.004035B1
004036D9  >  C74424 08 13(  MOV DWORD PTR [ESP+8],413
004036E1  .  C74424 04 90(  MOV DWORD PTR [ESP+4],XPan.004D9590     C:\zCr\NMoreira\NMoreira_Crypter\src\CrypterApp.cpp
004036E9  .  C70424 F8954(  MOV DWORD PTR [ESP],XPan.004D95F8       erro == 0
```

NMoreira, XPan, TeamXRat, different names but same author.

Even though many Brazilian-Portuguese strings are present upon initial analysis, there were a couple that caught our attention. Firstly, the ransomware uses a batch file which will pass a command line parameter to an invoked executable file, this parameter is “eusoudejesus” which means “I’m from Jesus”. Developers tend to leave tiny breadcrumbs of their personality behind in each one of their creations, and in this sample we found many of them.



A brief religious reference found in this XPan variant.

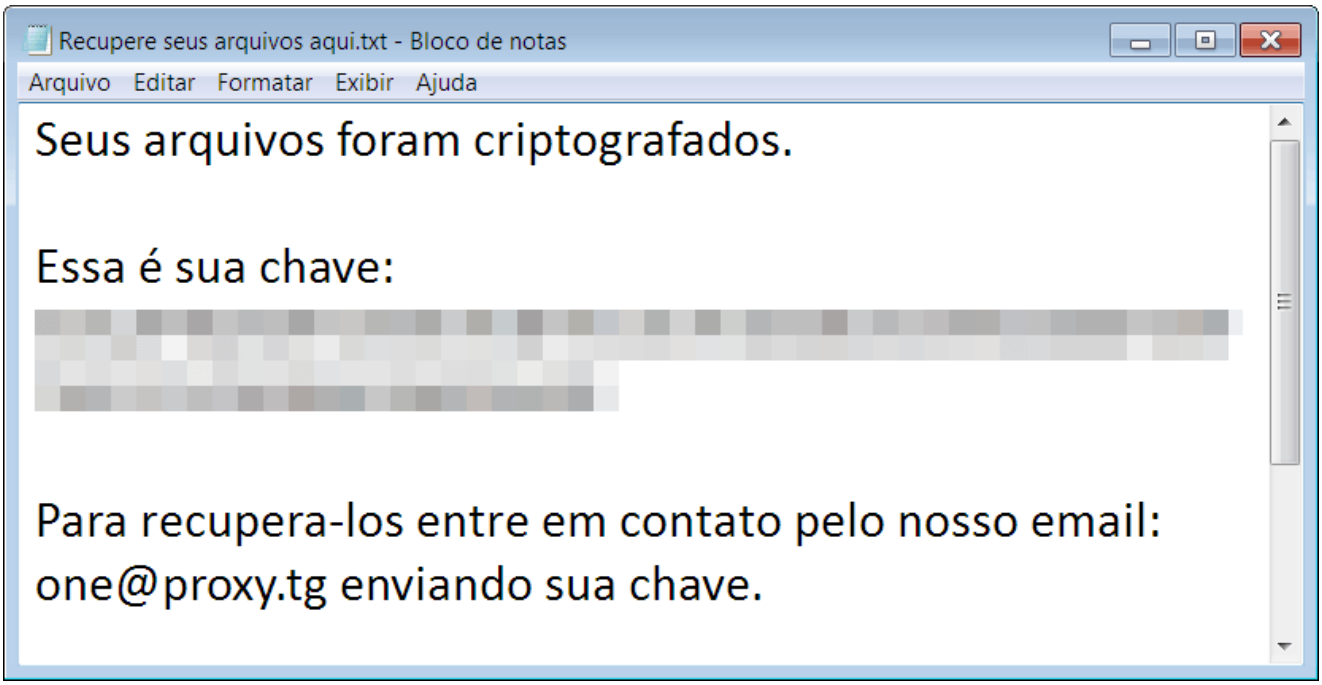
Secondly, a reference to a Brazilian celebrity is done, albeit indirectly. “Computador da Xuxa” was a toy computer sold in Brazil during the nineties, however it’s also a popular expression which is used to make fun of very old computers with limited power.

This is what cybercriminals think of your encrypted computer: just a toy they can control.

“Muito bichado” equals to finding a lot of problems in these type of systems, in this case meaning that the environment in which is XPan is executing is not playing fair and the execution is quite buggy.

```
00405FF7  .  E8 E41B0C00   CALL XPan.004C7BE0
00405FFC  .  893C24        MOV DWORD PTR [ESP],EDI
00405FFF  .  B9 E08C4D00   MOV ECX,XPan.004D8CE0
00406004  .  E8 C7C00800   CALL XPan.004920D0
00406009  .  83EC 04       SUB ESP,4
0040600C  .  890424        MOV DWORD PTR [ESP],EAX
0040600F  .  E8 DC380C00   CALL XPan.004C98F0
00406014  .  89C3          MOV EBX,EAX
00406016  .  C70424 C09E4D MOV DWORD PTR [ESP],XPan.004D9EC0   Computador da Xuxa ou muito bichado.
0040601D  .  E8 EE160200   CALL <JMP.&msvcrt.wcslen>          wcslen
```

Lastly, we have the ransomware note demanding the victim to send an email to the account '**one@proxy.tg'**. Considering that the extension for all the encrypted files in this variant is **'.one'** this seems like a pretty straightforward naming convention for the criminals' campaigns.

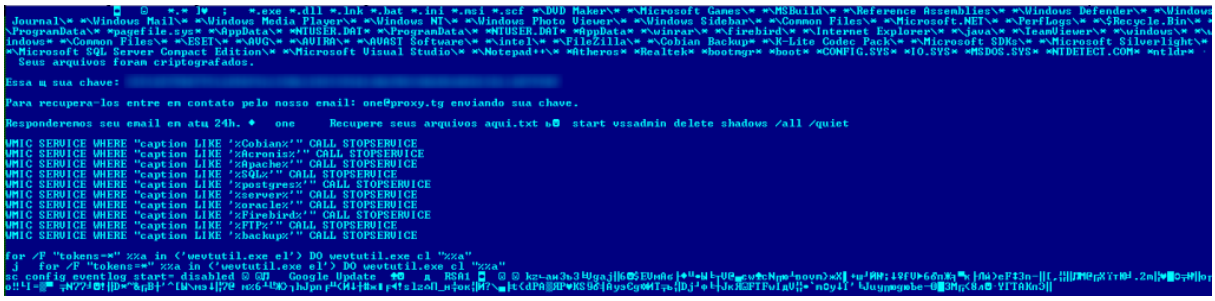


The rescue note in Portuguese.

Upon closer inspection, we discovered that this sample is nearly identical to another version of Xpan which used to be distributed back in November 2016 and used the extension ".__AiraCropEncrypted!". Every bit of executable code remains the same, which is quite surprising, because since that time there were several newer versions of this malware with an updated encryption algorithm. Both samples have the same PE timestamp dating back to the 31st of October 2016.

The only difference between the two is the configuration block which contains the following information:

- list of target file extensions;
- ransom notes;
- commands to execute before and after encryption;
- the public RSA key of the criminals.

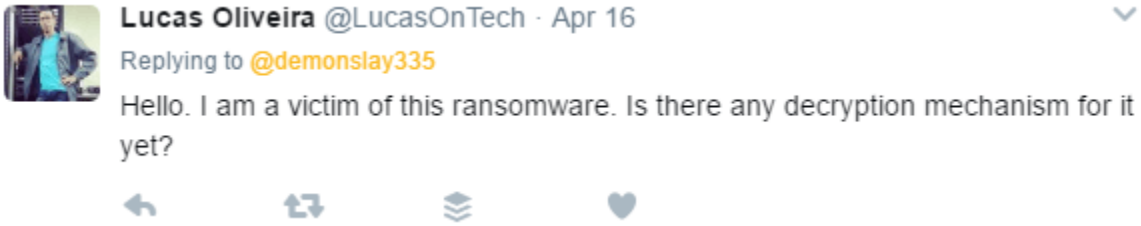


The decrypted configuration block of Xpan that uses the extension ".one".

The file encryption algorithm also remains the same. For each target file the malware generates a new unique 255-byte random string S (which contains the substring "NMoreira"), turns it into a 256-bit key using the API CryptDeriveKey, and proceeds to encrypt the file contain using AES-256 in CBC mode with zero IV. The string S will be encrypted using the criminals' RSA public key from the configuration block and stored in the beginning of the encrypted file.

According to one of the victims that contacted us, criminals were asking for **0.3 bitcoin** to provide the recovery key, using the same approach as they did with before: the user sends a message to a mailbox with his unique ID and patiently awaits for further instructions.

The victims so far are small and medium businesses in Brazil: ranging from a dentist clinic to a driving school, demonstrating once again that ransomware makes no distinctions and everyone is at risk. As long as there are victims, assisting them and providing decryption tools whenever possible is necessary, no matter the ransomware family or when it was created.



Victims: we can help

This time luck is on the victims' side! Upon thorough investigation and reverse engineering of the sample of ".one" version of Xpan, we discovered that the criminals used a vulnerable cryptographic algorithm implementation. It allowed us to break encryption as with the previously described Xpan version.

We successfully helped a driving school and a dentist clinic to recover their files for free and as usual we encourage victims of this ransomware to not pay the ransom and to contact our technical support for assistance in decryption.

Brazilian cybercriminals are focusing their efforts in creating new and local ransomware families, attacking small companies and unprotected users. We believe this is the next step in the ransomware fight: going from global scale attacks to a more localized scenario, where local cybercriminals will create new families from scratch, in their own language, and resorting to RaaS (Ransomware-as-a-service) as a way to monetize their attacks.

MD5 reference

dd7033bc36615c0fe0be7413457dccbf – Trojan-Ransom.Win32.Xpan.e (encrypted file extension: ".one")
54217c1ea3e1d4d3dc024fc740a47757 – Trojan-Ransom.Win32.Xpan.d (encrypted file extension: ".__AiraCropEncrypted!")

- Brazil
- RaaS
- Ransomware
- RDP
- TeamXRat
- Trojan

Authors

- Expert Anton Ivanov
-  Fabio Assolini
- Expert Fedor Sinitsyn
-  Santiago Pontiroli

XPan, I am your father
