Comparative analysis of various ransomware virii

Alexandre Gazet

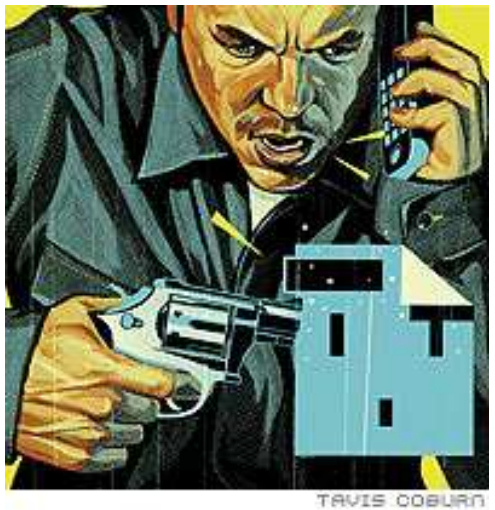
Sogeti-ESEC R&D

EICAR conference 2008

Plan

Ransomware ?

- The word appears in 2005 ;
- **Ransom** mal**ware** ;
- Points out a category of malware :
  - Try to blackmail their victims ;
  - Most of them encrypt files ;
  - `Gpcode`, `Archiveus`, `MayArchive`, `Cryzip`.
- Often make use of relatively *fine* social engineering to spread.



Knock knock jokes

Gpcode.ai - Glamorous team

Hello, your files are encrypted with RSA-4096 algorithm (http ://en.wikipedia.org/wiki/RSA). You will need at least few years to decrypt these files without our software. All your private information for last 3 months were collected and sent to us.

Krotten.u (Translated from Russian.)

If you want to restore the normal operation of your computer without losing information VJ ! And ekonomiv money, I have to e-mail help@privat.ms code refill Kyivstar 25 UAH. In reply within twelve hours you will receive your e-mail files to delete the program

Email is the only communication channel used by ransomwares' authors.

Are you scared ?

BBC News, 31 May 2006


BBC NEWS

LIVE BBC News 24

News Front Page
World
UK
England
Northern Ireland
Scotland
Wales
Business
Politics
Health
Education
Science/Nature
Technology
Entertainment
Also in the news
Video and Audio
Have Your Say
Magazine
In Pictures
Country Profiles
Special Reports

Last Updated: Wednesday, 31 May 2006, 15:59 GMT 16:59 UK

E-mail this to a friend Printable version

Woman targeted by web hackers

A woman from Greater Manchester has become a victim of an internet scam in which hackers hijack computer files and blackmail owners to get them back.

Helen Barrow, a 40-year-old nurse from Rochdale, is believed to be one of the first victims of the con in the UK.

Criminals encrypt files with complex passwords, leaving a ransom note telling victims not to contact police.

Ms Barrow's note said that she would have to buy drugs from an online pharmacy to find out the password.

Helen Barrow feared she would lose coursework for her degree

"Helen Barrow feared she would lose coursework for her degree."

"[...]Criminals encrypts files with complex passwords,"

"[...]she would have to buy drugs from online pharmacy to find out her password."

A kind of theatrical communication.

Something new ?

Almost 20 years ago...

AIDS Trojan - 1989

- 20.000 infected floppy disk ;
- Logic bomb : payload executed after 90 reboots ;
- Encrypt filenames and extensions, not contents ;
- Monoalphabetic substitution algorithm ;

Any advances in 20 years ?

Something new ?

Adam Young, **Moti Yung**, **1996** in
Cryptovirology : Extortion-based security threats and countermeasures

> *"In this paper we present the idea of Cryptovirology, [. . .] showing that it can also be used offensively. By offensive we mean that it can be used to mount extortion based attacks that cause loss of access to information, loss of confidentiality, and information leakage"*

A ransomware is nothing more than an offensive cryptovirus.

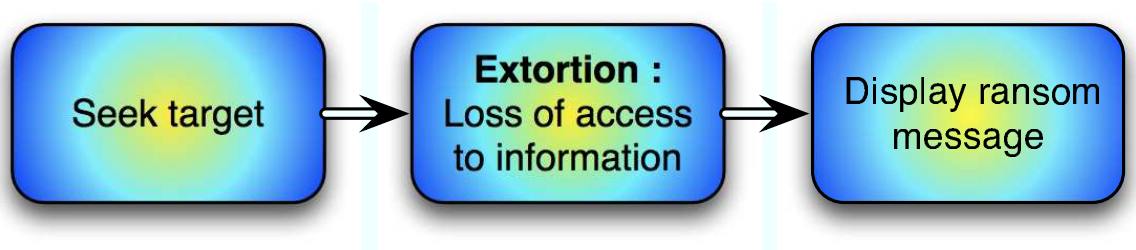
The study

- Technical review of this *last* ransomwares wave ;
- Analysis of strategy ;
- 14 samples have been studied and *reverse-engineered* :
  - 8 from `Gpcode` family ;
  - 2 from `FileCode` family ;
  - 4 from `Krotten` family.
- Few hardened binaries :
  - Few samples compressed with `UPX` ;
  - One packed with `AsProtect` ;
  - One custom, but basic, packer.
- Various languages of programmation, mainly high-level.

How do they try to extort money from their victims ?

Plan

Behaviour overview



1. **Target** : most of time victim's documents ;
2. **Extortion** : based on encryption with one exception ;
3. **Ransom** : `txt` files or `MessageBox`.

Extortion scheme

A good mass extortion scheme ?

- Malicious binary is compromised and should not contain any secret ;
- Author should be the only one able to reverse infection ;
- Freeing one victim should not help other victims to get rid of infection.

Use of cryptography could successfully fill all these requirements.

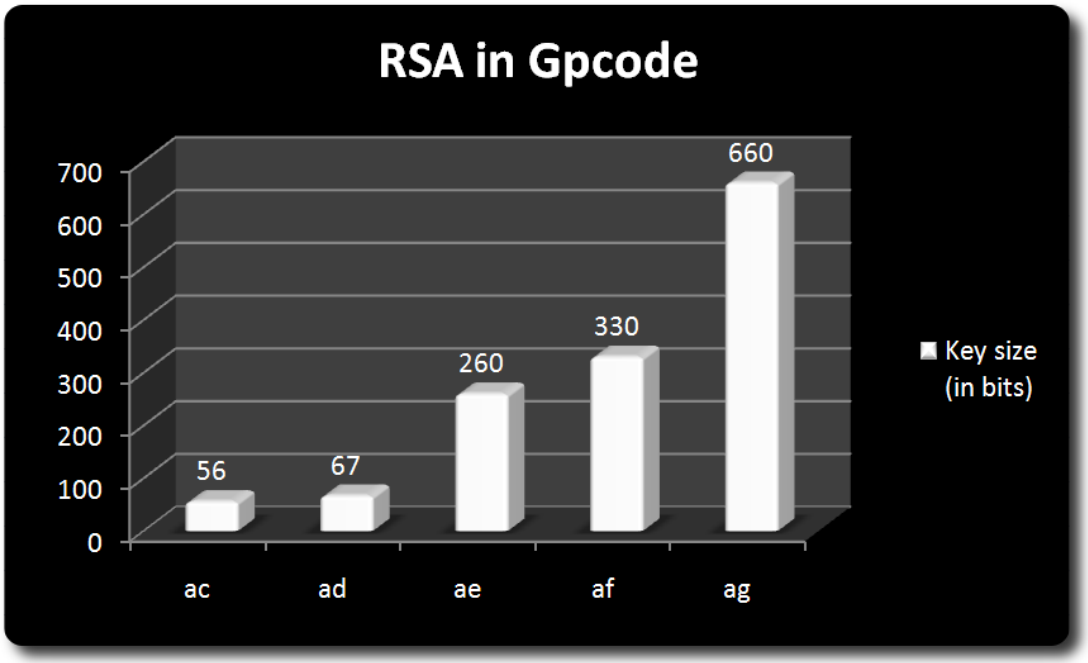
Private-key encryption

- **ADD encryption**
  - $byte\_ciphered_n = byte\_message_n + byte\_key_n$
  - keystream : *linear congruential* pseudorandom generator :
$$k_{n+1} = a * k_n + b \mod m$$
- **XOR encryption**
  - Get two parts from a file : **A** and **B**, equal in size ;
  - `XOR` part **A** with part **B**.
- **Blowfish**, external library : `ECCrypt` ;
- **RC4**-*like* using *session key*. . . stored on victim's hard drive.

Malware's capture ruins extortion scheme.

Public-key encryption

- **RSA algorithm encryption**
  - Used by `Gpcode` versions from **ac** to **ag** ;
  - Jan 2006 $\Rightarrow$ Jun 2006 ;
  - Basic implementation.



All versions have been broken.

Conclusion

Ransomware as mass extortion mean ?

- Malware's capture leads to break extortion scheme ⇒ design is deficient.
- Use of public key cryptography (RSA) : decryption key is the same for all victims ⇒ design is deficient.
- Hybrid crypto systems, with the concept of *session key*, seem to be **unknown** or **ignored**.

They are not **technically** designed for mass extortion.

Plan

From amateurism...

- Most ransomware have presented disappointing quality standards ;

```
call    Classes::TFileStream::TFileStream(System::AnsiString,ushort)
mov     [ebp+fileStream], eax
xor     ecx, ecx
xor     edx, edx
mov     eax, [ebp+fileStream]
mov     ebx, [eax]
call    dword ptr [ebx+0Ch] ; wrapper FileSeek
mov     eax, [ebp+fileStream]
call    Classes::TStream::GetSize(void)
cmp     eax, 5000       ; Size is badly checked
jl      SmallFiles
```

```
ReadTwoBuffers:
lea     edx, [ebp+buffer1]
mov     ecx, 5000       ; size to read
mov     eax, [ebp+fileStream]
mov     ebx, [eax]
call    dword ptr [ebx+4] ; THandleStream::Read
lea     edx, [ebp+buffer2]
mov     ecx, 5000       ; size to read
mov     eax, [ebp+fileStream]
mov     ebx, [eax]
call    dword ptr [ebx+4] ; THandleStream::Read
mov     eax, 1
lea     edx, [ebp+buffer1]
lea     ecx, [ebp+buffer2]
```

From amateurism...

- Most ransomware have presented disappointing quality standards ;
- Extortion scheme is not reliable ;
- Code and cryptography use are both basics.

But. . .

Virus.Win32.Gpcode.ai

- Appeared on 17 Jul 2007 ;
- Sometimes referenced as `ntos.exe` ;
- Quite not the same quality ;
- Much more advanced than *classical* ransomwares.

From amateurism...

- Most ransomware have presented disappointing quality standards ;
- Extortion scheme is not reliable ;
- Code and cryptography use are both basics.

But. . .

Virus.Win32.Gpcode.ai

- Appeared on 17 Jul 2007 ;
- Sometimes referenced as `ntos.exe` ;
- Quite not the same quality ;
- Much more advanced than *classical* ransomwares.

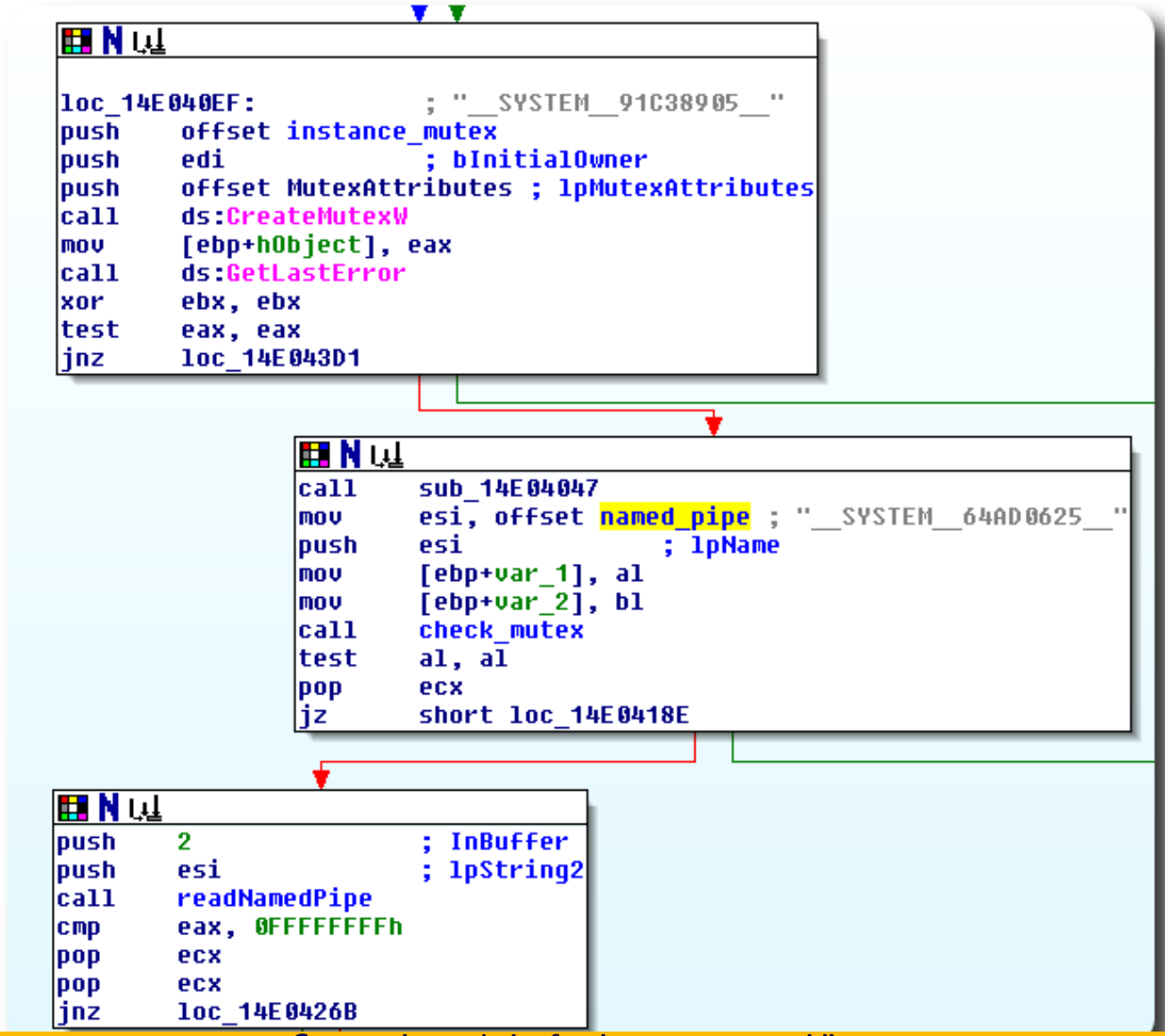
To profesionnal malware

Code is quite clean, effective.

- Multithreading & thread injection ;
- Named pipe communication ;
- Steal data from `HTTP` traffic, using *API hooking* ;
- Ability to upload data to a remote server ;
- Ability to download malicious files ;
- Encrypt files (*RC4-like*) and ask for a ransom.

Thoughtful design.

Synch mechanism



Malware on the shelf

Lighting from an analysis from **Viruslist**[1] :

- `Gpcode.ai` makes use of some code on the shelf ;
- Linked up with the `Zunker` botnet managed by `Zupacha+ZeuS` bundle ;
- Kit to build botnet available for 3000$;
- Site is hosted by the *famous* company `RBN` (Russian Business Network).

Ransom business is now part of a more hierarchized criminal activity.

[1] `www.viruslist.com/en/analysis?pubid=204791973`

Plan

Conclusion

What we've learned about ransomware ?

- They are basic cryptovirus ;
- Turn out to be a perfect illustration of virus' criminals shift ;
- Whatever the mean, money is the Grail.

- The phenomenon has to be monitored ;
- Mass extortion is probably doomed to failure ;
- Operate on a too large scale would draw to much light ;
- To much sensational communication should be avoided.

Conclusion

Thanks for your attention.

Your questions ?