Malware analysis

Carberp

Ralph Dolmans
Wouter Katz

University of Amsterdam

Research questions

- What kind of anti-forensics techniques are being used by the latest version of Carberp?

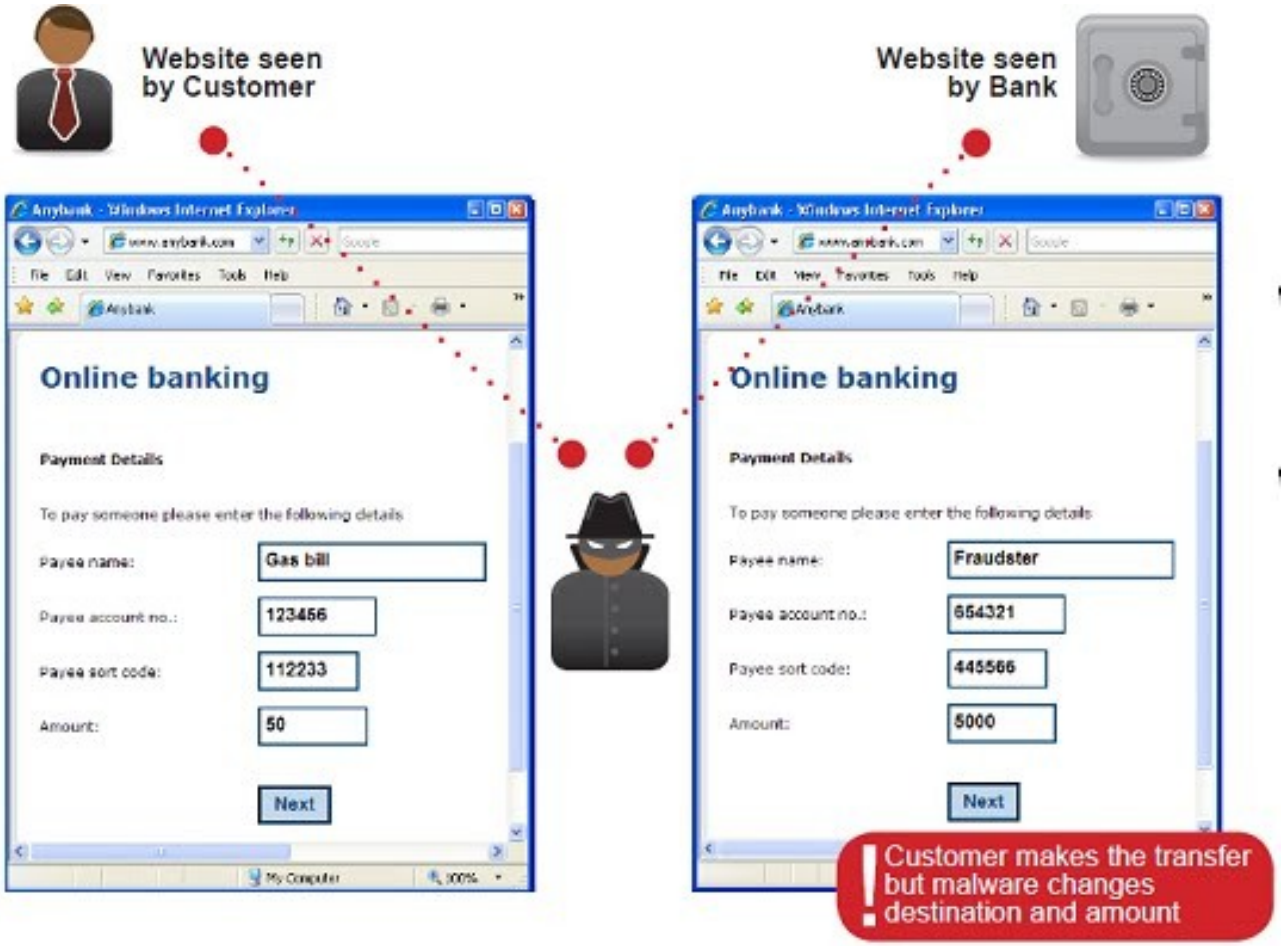
- What behavior does the latest version of Carberp show?
  - Installation
  - Run-time
  - C&C

E-banking malware

- Steals your money
- Fake forms (HTML injection), Key logging, browser API hooks, …
- Big players: Citadel, ZeuS, SpyEye, Carberp

Carberp - General behavior

- MITB for e-banking



http://malware-security-dinesh.blogspot.nl

Carberp - General behavior

- VNC
- Video recording
- Extra plugins (passw.plug, stopav.plug, miniav.plug)

Installation

- Startup folder
- Windows service (svchost.exe)
- Contacts C&C server for updates/instructions

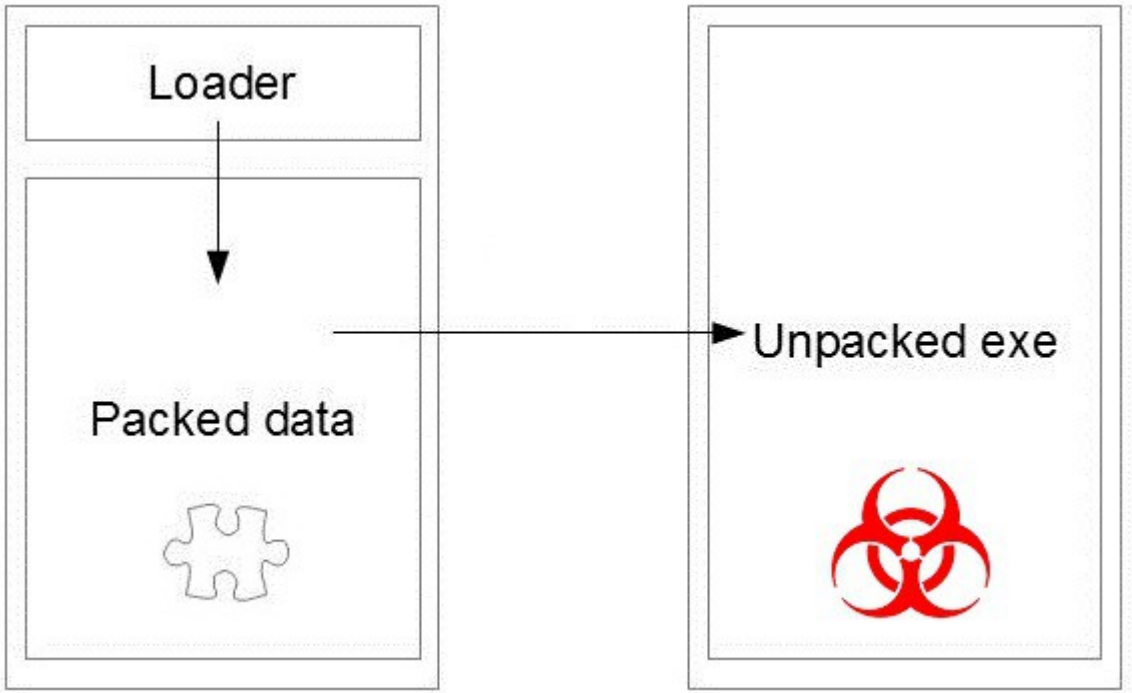
Anti-forensics

- Techniques used as countermeasures to forensic analysis

- In our malware sample, data hiding by means of:
  - Packing of the executable
  - Encryption of network traffic
  - Encryption of config files

Executable packing

- Uses small loader to unpack the 'real' executable



Executable packing

- How to obtain unpacked code?
- Run the executable, dump unpacked code from memory.
- Unpacked code contains references to Russian e-banking websites, VNC, password grabber, ...

API hooks

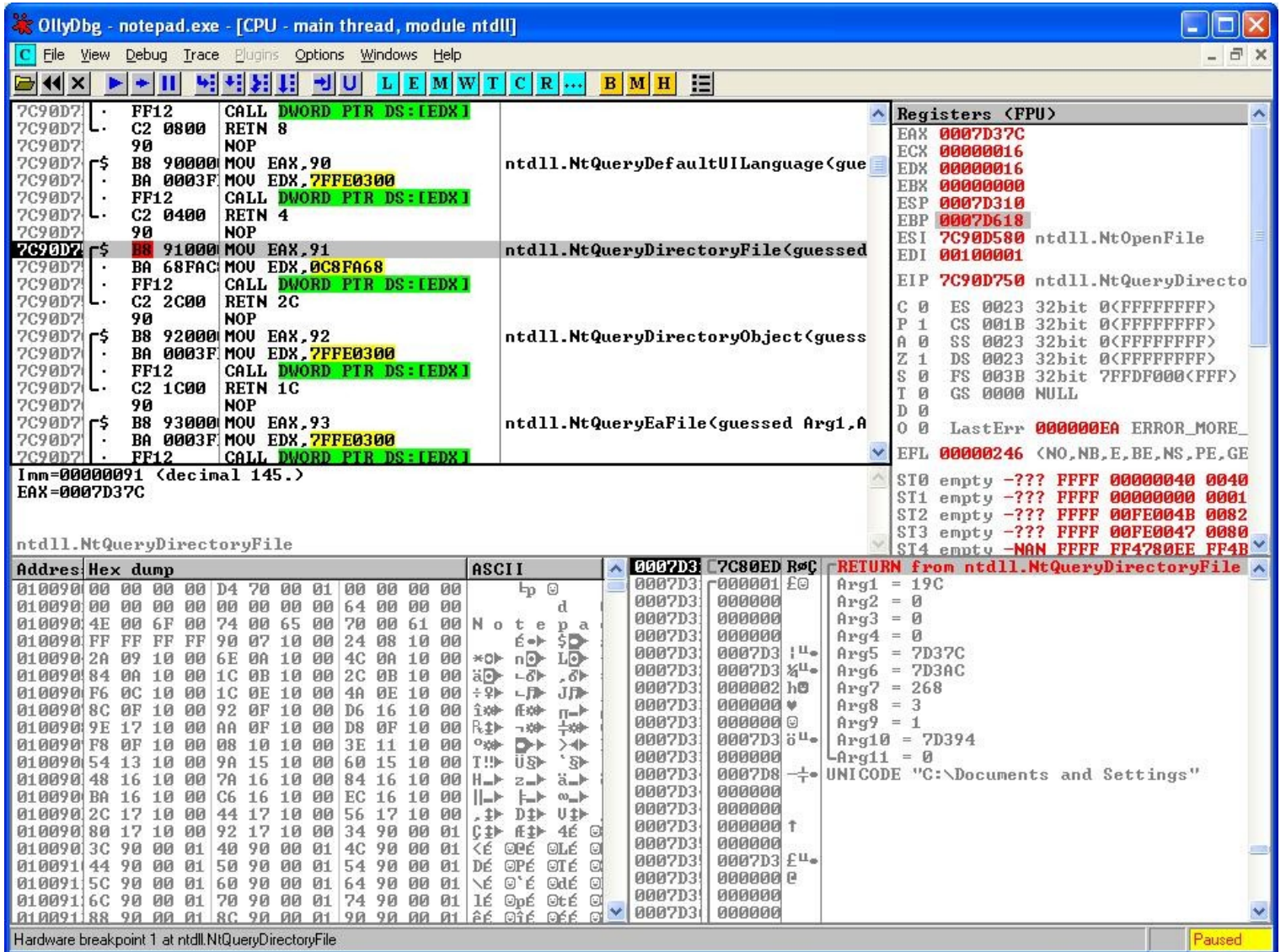
- GMER showed 4 hooks in ntdll.dll:
  - ntdll.dll!NtResumeThread
  - ntdll.dll!NtQueryDirectoryFile
  - ntdll.dll!NtClose
  - ntdll.dll!NtDeviceIoControlFile

API hook behavior

- How to determine what it does?

API hook behavior

- How to determine what it does?



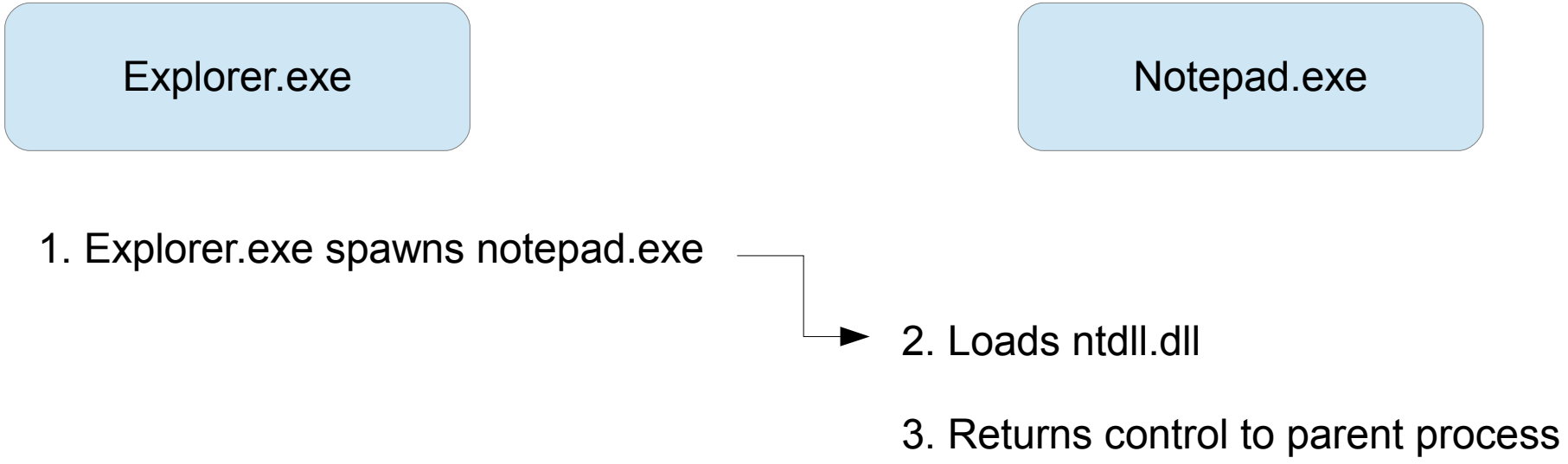
Memory injection

Explorer.exe

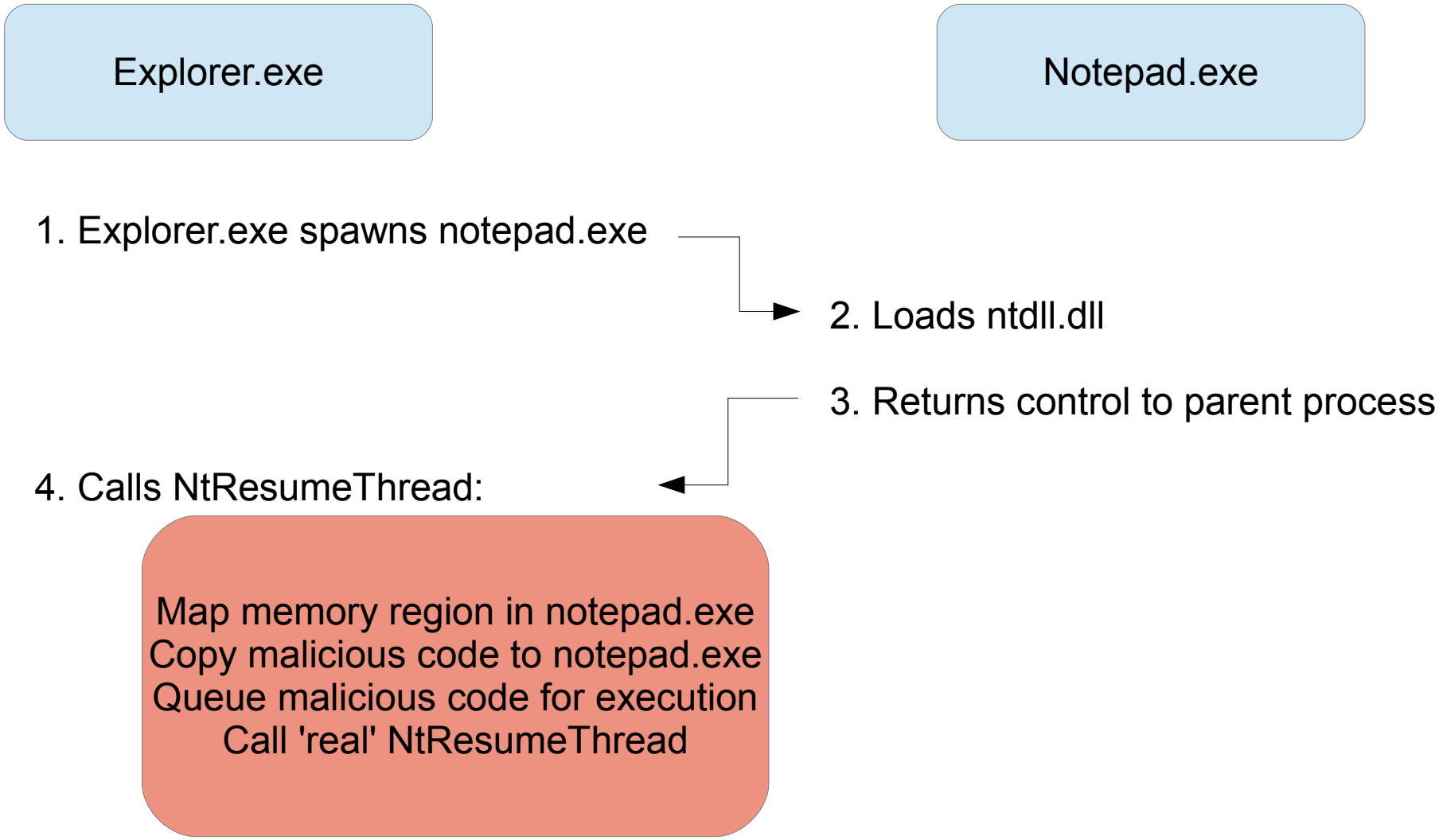
Notepad.exe

1. Explorer.exe spawns notepad.exe

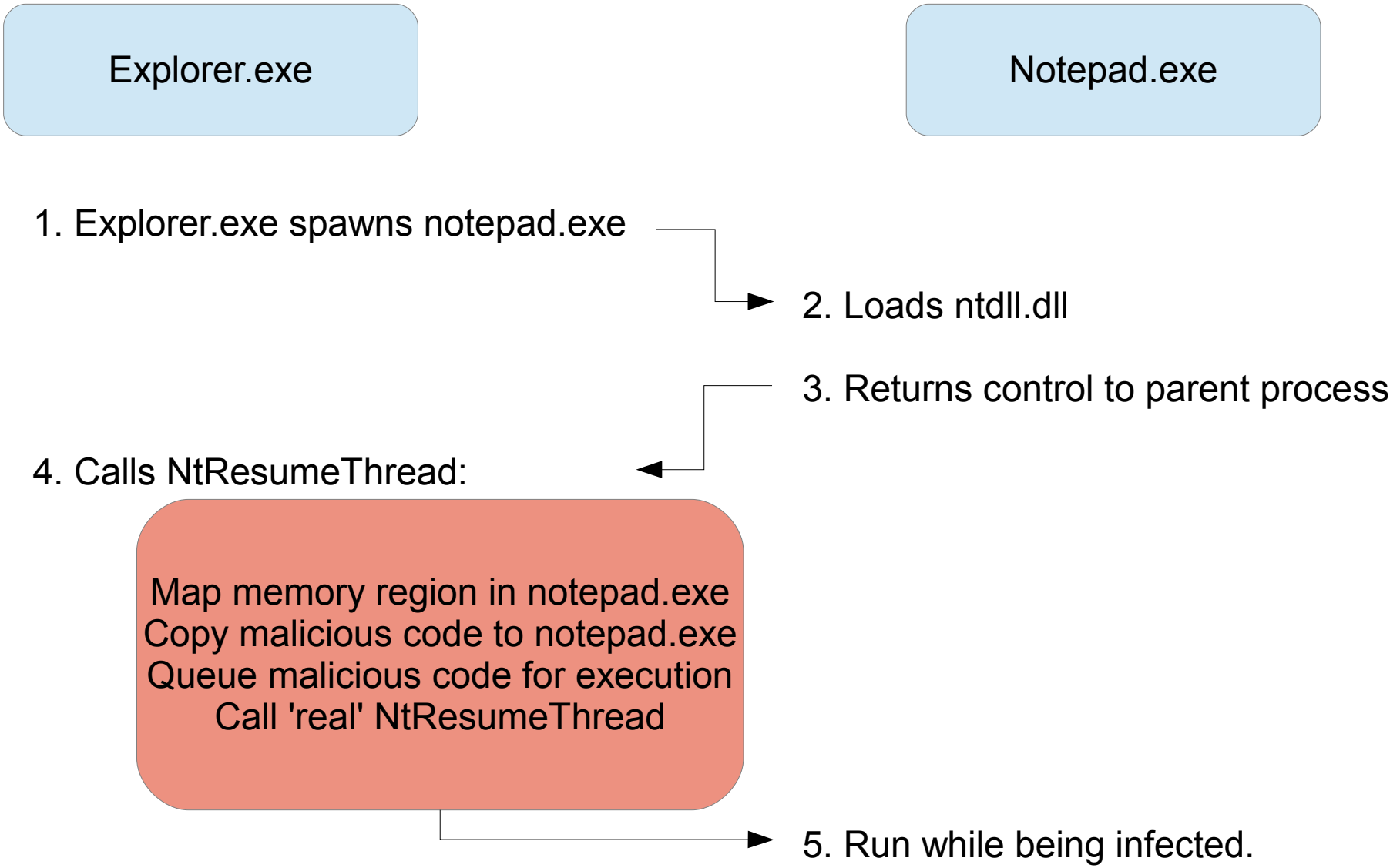
Memory injection



Memory injection



Memory injection



Hiding files

- ntdll.dll!NtQueryDirectoryFile
- Debugger made clear this hook is for hiding files
- Hidden directory in C:\Documents and Settings\All Users\Application Data

Config file encryption

- mnhslst32.dat in hidden directory
- Assembly decryption routine found, implemented in python script
- Key found while debugging decryption routine: *HJGsdlk873d*

Config file encryption

- XOR each plaintext byte with every key byte

- Before each XOR operation:
  - XOR input = Previous XOR output + (XOR round * plaintext byte position in line)

    1st byte: normal

    2nd byte input: +1 for round 2, +2 for round 3, …

    3rd byte input: +2 for round 2, +4 for round 3, …

    ….

Config file encryption

- Strings in config file:
  - 696301E9F82608F7EC3CB37D2F44663C
  - 696301E9F82608F7EC3CB37D30046D2DA9
  - 696301E9F82608F7EC3CB37D33046D2DA9

- Plaintext:
  - defeatswirly.net
  - defeatswirly1.net
  - defeatswirly2.net

Network encryption

- Trojan sends HTTP requests to C&C
- All POST-data is encrypted
- Use debugging of the exe to find out how...

Network encryption

- Step through the code to find encryption algorithm

- Encrypted network traffic:
  - 8 byte IV, split into 2 x 4 bytes
  - 1st part IV+base64(RC2(plaintext))+2nd part IV
  - '=' or '==' in base64 always at the end

- RC2 encryption key = CD5ztnj3W1wgSH2M

Network encryption, example

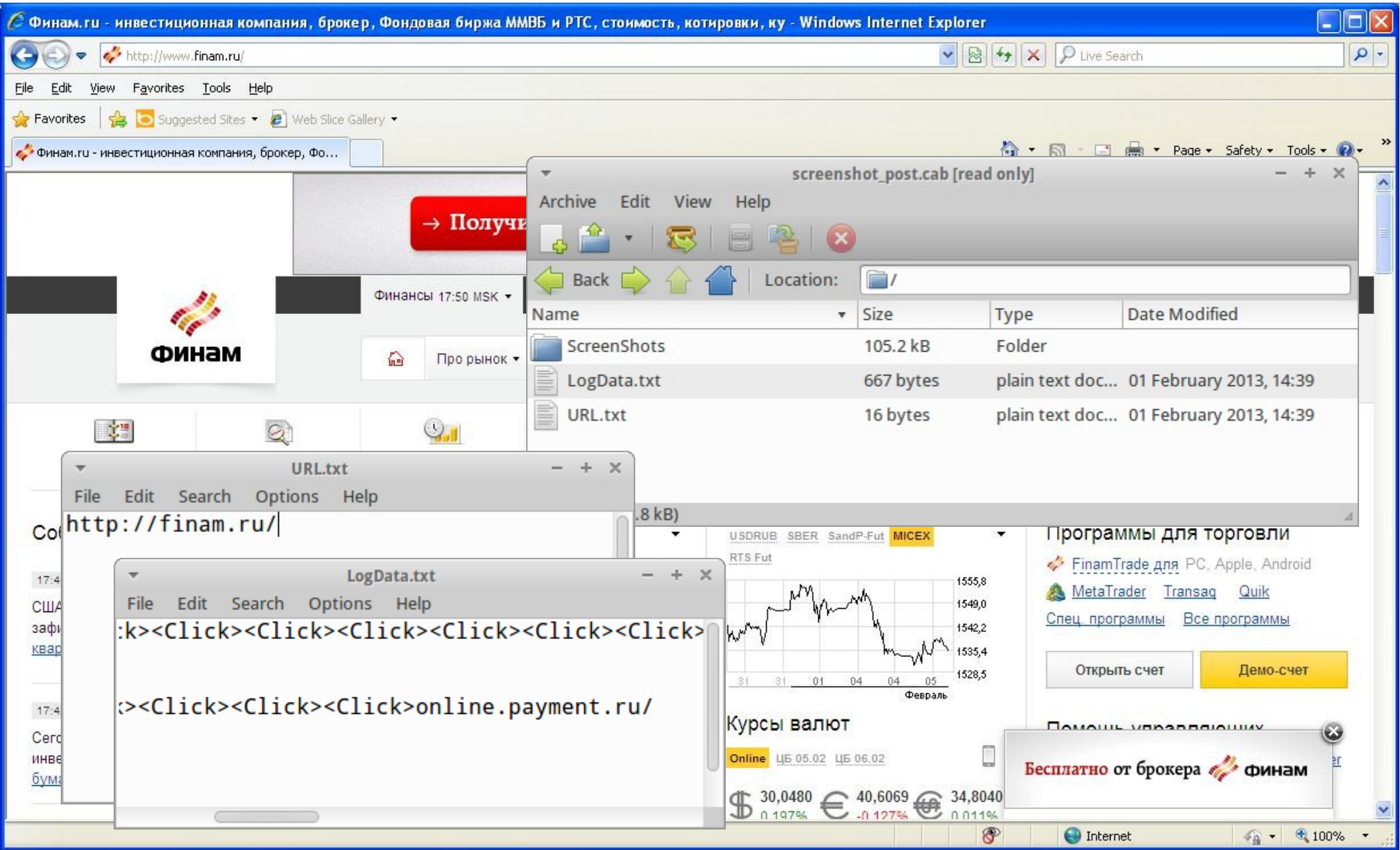
- HylFFl7RmWrgu4r40KdlP4t53IoM3AEGzKJiTa obwr4ex8WAfW59Oh6yNzlcn4RKSWCwT68Ih PRPMJmEqm0NhqbGFAIDcu==
  - IV = HylFIDcu

- Plaintext:
  - uid=a022A7D5C91DCED15F&av=&md5=a574fc3d 97149bcbf8bdccd5a8a73951

Data theft

- Several Russian banks targeted
- Browser API hooks to check if bank site is accessed
- Send CAB file with screenshot and keylog-file to C&C
  - Network traffic unencrypted

CAB file


Финам.ru - инвестиционная компания, брокер, Фондовая биржа ММВБ и РТС, стоимость, котировки, ку - Windows Internet Explorer
http://www.finam.ru/
File Edit View Favorites Tools Help
Favorites Suggested Sites Web Slice Gallery
Финам.ru - инвестиционная компания, брокер, Фо...
Page Safety Tools
screenshot_post.cab [read only]
Archive Edit View Help
Back Location: /
Name Size Type Date Modified
ScreenShots 105.2 kB Folder
LogData.txt 667 bytes plain text doc... 01 February 2013, 14:39
URL.txt 16 bytes plain text doc... 01 February 2013, 14:39
URL.txt
File Edit Search Options Help
http://finam.ru/
LogData.txt
File Edit Search Options Help
:k><Click><Click><Click><Click><Click><Click>
:><Click><Click><Click>online.payment.ru/
Финам
Финансы 17:50 MSK
Про рынок
USDRUB SBER SandP-Fut MICEX
RTS Fut
Курсы валют
Online ЦБ 05.02 ЦБ 06.02
Программы для торговли
FinamTrade для PC, Apple, Android
MetaTrader Transaq Quik
Спец. программы Все программы
Открыть счет Демо-счет
Бесплатно от брокера финам
Internet 100%

Conclusions

- Hiding files
- Memory injection
- Encryption
- Tries to steal information

Questions?