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?
1. Explorer.exe spawns notepad.exe
Memory injection

1. Explorer.exe spawns notepad.exe
2. Loads ntdll.dll
3. Returns control to parent process
Memory injection

1. Explorer.exe spawns notepad.exe

2. Loads ntdll.dll

3. Returns control to parent process

4. Calls NtResumeThread:
   - Map memory region in notepad.exe
   - Copy malicious code to notepad.exe
   - Queue malicious code for execution
   - Call 'real' NtResumeThread
Memory injection

1. Explorer.exe spawns notepad.exe
2. Loads ntdll.dll
3. Returns control to parent process
4. Calls NtResumeThread:
   - Map memory region in notepad.exe
   - Copy malicious code to notepad.exe
   - Queue malicious code for execution
   - Call 'real' NtResumeThread
5. Run while being infected.
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:
  – defeatsquirly.net
  – defeatsquirly1.net
  – defeatsquirly2.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

- **HylFFl7RmWrgu4r40KdlP4t53IoM3AE Gy2kJKiTaobwr4ex8WAfW59Oh6yNzlcn4RKSWCwT68lhPRPMJmEqm0NhqbGFAIDcu==**
  - IV = HylFIDcu

- **Plaintext:**
  - uid=a022A7D5C91DCED15F&av=&md5=a574fc3d97149bcbf8bdccd5a8a73951
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
Conclusions

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