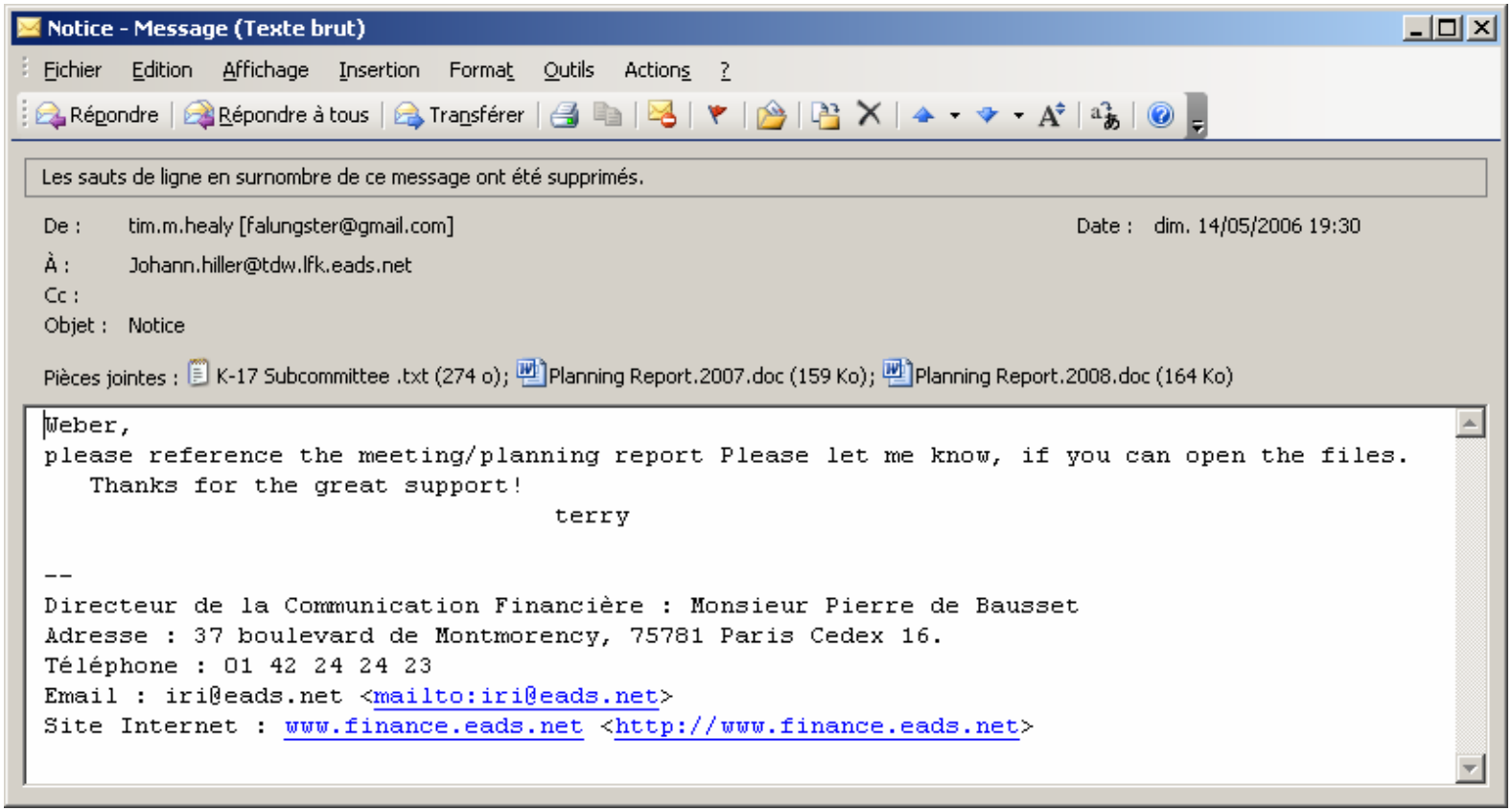
0day Word

Nicolas RUFF

EADS-CCR DCR/STI/C

Phase initiale

- Un mail suspect …



Analyse de la pièce jointe

- Pas de macros
- Mais Word 2003 version française plante
  - Tentative d'exploitation d'une faille binaire ?

Analyse de la pièce jointe

- Un *padding* étrange
  - Office utilise plutôt 0x00 ou 0xFF
  - Il s'agit probablement du *shellcode*

29060	8181 8181 8181 8181 8181 8181 8181 8181	□□□□□□□□□□□□□□□□
29070	8181 8181 8181 8181 8181 8181 8181 8181	□□□□□□□□□□□□□□□□
29080	8181 8181 8181 8181 8181 8181 8181 8181	□□□□□□□□□□□□□□□□
29090	8181 8181 8181 8181 8181 8181 8181 8181	□□□□□□□□□□□□□□□□
290a0	8181 8181 8181 8181 8181 8181 8181 8181	□□□□□□□□□□□□□□□□
290b0	8181 8181 8181 8181 8181 8181 8181 8181	□□□□□□□□□□□□□□□□
290c0	8181 8181 8181 8181 8181 8181 8181 8181	□□□□□□□□□□□□□□□□
290d0	8181 8181 8181 8181 8181 8181 8181 8181	□□□□□□□□□□□□□□□□
290e0	8181 8181 8181 8181 c5ee e2c4 efe5 ffff	□□□□□□□□Åîâ Ïåÿÿ
290f0	fff1 7c01 00	ÿñ|..

Analyse du shellcode

- *Shellcode* "chiffré" par XOR

```
seg000:00000C0F                 call    GetProcAddress  ; GetProcAddress("DeleteFileW")
seg000:00000C14                 mov     [edi+34h], eax
seg000:00000C17                 push    dword ptr [edi+8]
seg000:00000C1A                 push    76DA08ACh
seg000:00000C1F                 call    GetProcAddress  ; GetProcAddress("SetFilePointer")
seg000:00000C24                 mov     [edi+38h], eax
seg000:00000C27                 push    dword ptr [edi+8]
seg000:00000C2A                 push    0E8AFE98h
seg000:00000C2F                 call    GetProcAddress  ; GetProcAddress("WinExec")
seg000:00000C34                 mov     [edi+3Ch], eax
seg000:00000C37                 push    dword ptr [edi+8]
seg000:00000C3A                 push    99EC8974h
seg000:00000C3F                 call    GetProcAddress  ; GetProcAddress("CopyFileW")
seg000:00000C44                 mov     [edi+40h], eax
seg000:00000C47                 push    dword ptr [edi+8]
seg000:00000C4A                 push    73E2D87Eh
seg000:00000C4F                 call    GetProcAddress  ; GetProcAddress("ExitProcess")
seg000:00000C54                 mov     [edi+44h], eax
seg000:00000C57                 push    dword ptr [edi+10h]
seg000:00000C5A                 call    dword ptr [edi+34h] ; DeleteFileW(L"c:\~.exe")
seg000:00000C5D                 push    dword ptr [edi+0Ch]
seg000:00000C60                 call    dword ptr [edi+34h] ; DeleteFileW(L"c:\~$")
```

Analyse du shellcode

- Un fichier EXE existe à la fin du document Word
- Ce fichier est copié sous le nom "c:\~.exe" puis exécuté

Analyse de l'exécutable

- Reste persistant grâce à la clé de base de registre
  - "Software\Microsoft\Office\10.0\Word\Resiliency"
- Se dissimule à l'utilisateur
  - Nettoie le fichier Word d'origine
  - Relance Word avec le fichier nettoyé
- Le reste a été décrit par les éditeurs antivirus
  - http://www.symantec.com/outbreak/word_exploit.html

Conclusion

- Attaque dangereuse
  - Attaque ciblée
  - Utilisation d'une faille binaire non documentée dans Word
  - Peu de moyens de protection *a priori*
    - Interdire les fichiers ".doc" ? ☺
- Et pourtant une erreur triviale
  - Création d'un fichier "c:\~.exe"
    - Nécessite les droits administrateur
    - Ne marche pas si pas d'unité "C:\"

Bibliographie

- Pour plus d'infos
  - https://www.openrce.org/blog/browse/Kostya
  - http://newsoft-tech.blogspot.com/2006/06/word-0day-was-it-0day-we-have-all.html