Deliverable #8: Report on analysis of FTP credentials

Relyze analysis of file3666.exe & file2544.exe:

In the analysis of both file3666.exe and file3544.exe, there were many similarities found between the two binaries. Though, with these similarities there were also many differences found. The most notable among these were: the _checkString subroutine/function (45.06% modified), the _main subroutine/function (11.90% modified), and the _releaseInfo subroutine/function (10.35% modified).

file2544.exe:

sub_401340 ----------> entry point (“Enter password: “)
call printf ----------> sends “Enter password: “ to the terminal screen
call getchar ----------> returns the character inputted
call sub_401394 ----------> sub is responsible for comparing user input to the actual pwd
call sub_40146F ---------->
call sub_4014B7 ----------> sub prints out IRC info if a 0 is returned (if pwd is correct from sub_401394)

I believe sub_401340 is the _main function; sub_401394 is the _checkString function; sub_4014B7 is the _releaseInfo function.

file3666.exe

sub_401340 ----------> entry point (“Enter password: “)
call printf ----------> sends “Enter password: “ to the terminal screen
call fgets ----------> reads line of string input
call getchar ----------> returns the character inputted
sub_401394 ----------> sub is responsible for checking the string inputted
sub_40144F ----------> looks like pwd is *further* obfuscated? (sar eax, 1Fh | shr eax, 1Fh)
sub_4014AD ---------->
call sub_401EB0 ---------> returns “This week’s FTP info: “

Deliverable #9: Report on dynamic analysis of binary3666

Using dynamic analysis, I was able to crack the password for file3666.exe. This was done by setting a breakpoint on the '*cmp cl, al*' line in the subroutine within the subroutine that contains the XOR instruction. Using this breakpoint, close attention was paid to the *EDX*, *EAX*, and *ECX* rows and the information shift. After entering the correct password (*SuxPasswordStill*), this was the following output:

This week's IRC info:

host: tranzit.somber.net
un: sapsan
pw: changeit666

Looks to be another IRC host, a username, and password.