Ghiribizzo's Cracking Tutorial

Some Quick Cracks

NetProxy V2.018, VPOP3 V1.20 & Xara3D V1.20

After making quite a few keygenerators I was getting fed up with them so I decided to do some quick cracks. I borrowed a magazine cover CD (PC Direct Jan '98) from a friend and began to crack the above targets.

PGP and Signed Tutorials

My tutorials and programs should be signed electronically using PGP. PGP 5 supports DSS/Diffie-Hellman keys. These keys are not supported by previous versions of PGP.
You should check the signature to make sure that the tutorial and especially its program files have not been tampered with. All cracks, tutorials and zip files I release will be signed. This will prevent tampering and will hopefully reduce the chances of viral infection.
My signature will also be the only way you can identify me as my email address will often change.

My Web Site: http://Ghiribizzo.home.ml.org
My Email: Ghiribizzo@geocities.com
My Backup Email: Ghiribizzo@hotmail.com

I decided to crack these programs as quickly as possible. I scribbled a few notes down after doing all 3, but some of them may not be correct. I will not go into great detail here. I will just describe the basic techniques and let you do the rest. If you're a newbie and need extra help, contact me by email or using the OCU page.

VPOP3 Version 1.2.0

A simple serial fishing exercise. Use SoftICE and break on the relevant functions. I *think* that this used lstrcmp to make the checks (silly). Watch out there are 2 serials floating in memory. I don't know what the second is (I didn't stop to check) it could be a blacklisted one or something a bit nastier.

My info:

Name:	http://ghiribizzo.home.ml.org
Users:	1000 user license
Expires:	Never (0)
Key:	ynopfUgmTxJVKJQ

NetProxy Version 2.0.18

This is a good one for newbies to practice and learn. You will basically try the above technique. However, I'm sure you'll probably have difficulty in breaking on the compare routine. Look at the functions it imports for the search procedure. It's __vbastrcmp. If you set as bpx on it, then you'll find that SoftICE breaks a few time comparing the username. This is probably a blacklisted serial check (though again, I didn't bother to stop and investigate). Ignore these and it will break on the serial compare routine. You can fish the serial from that.

My info:

Name:	http://ghiribizzo.home.ml.org
Key:	GJBTOERAEDWN

Xara3D Version 1.2.0

A variation on the name/serial scheme. This time you are given a challenge code and require a key. I decided to deadlist rather than fish for serials this time. Disassemble (use W32Dasm ver. 8.5) and search for the nag. You'll find several references to it. I looked carefully at the references and saw that they were located very close to each other. Immediately, I guessed that several checks were being made in succession and failure at any of them results in a jump to the nag.

I simply inverted each of the jumps (je -> jne and jne -> je). I saved and ran again. A message popped up but it was too quick for me to read it. In any case, the program is registered and all functions are enabled. I'll give the deadlisting:

```
:0040F83F 0F85E0010000            jne 0040FA25
:0040F845 0FBE10                  movsx edx, byte ptr [eax]

# snip #

* Referenced by a (U)nconditional or (C)onditional Jump at Addresses:
|:0040F83F(C), :0040F853(C), :0040F86F(C), :0040F88B(C), :0040F8A7(C),
|:0040F8C3(C), :0040F8DF(C), :0040F8FB(C), :0040F968(C)
|
:0040FA25 6AFF                    push FFFFFFFF
:0040FA27 6A10                    push 00000010

* Possible Reference to String Resource ID=03005: "You entered an invalid unlock code.
```

If you take the whole deadlisting between the first line and last you'll have the protection routine. You'll also notice that the key is stored in HKEY_CURRENT_USER\Software\Xara\X3D\Install. How the key is generated, I'll leave for you to do!

SoftICE 3.22

Well, that's it. All done in less than half an hour. I don't intend to use any of these programs, I just cracked them for the practice. I wouldn't have bothered except that I just installed SoftICE version 3.22 after using 3.01 for quite some time. Unfortunately, I installed it on my second machine (dedicated to cracking and collecting junk in the registry from these programs!) which due to the old monitor only runs in 16 colours; this means that the debugging screen doesn't appear as a window, but switches as in 3.01. However, the switch is much, much faster – whether this is due to the resolution I am using on my second computer or due to the newer version of SoftICE, I don't know, but if it is down to SoftICE 3.22, then I would definitely upgrade.

W32Dasm

Admittedly not the best disassembler in the world, but often quite useful. I advise you to shy away from using version 8.9 ('regged') and instead use version 8.5 (cracked). The reason is simply that version 8.9 is highly bug ridden. I have both and never use 8.9.

Often W32Dasm simply doesn't cut the mustard and for those occasions I recommend IDA Pro version 3.7. Very powerful, but still has the same clunky interface.

OCU

Regarding people asking me for advice for cracking projects. I'll remind you to read index.html and also to make your point specific. I will NEVER give out a crack or hand it out on a plate for you. I will however do my best to help you with problems you have and help you to improve your technique.

For those wanting to tempt me to help them with cracks, hint: I like strategy games! ☺ <- yuk! I installed MS Office 97 Pro as well and now it does this to my smileys! Sometimes, it's just not worth upgrading…