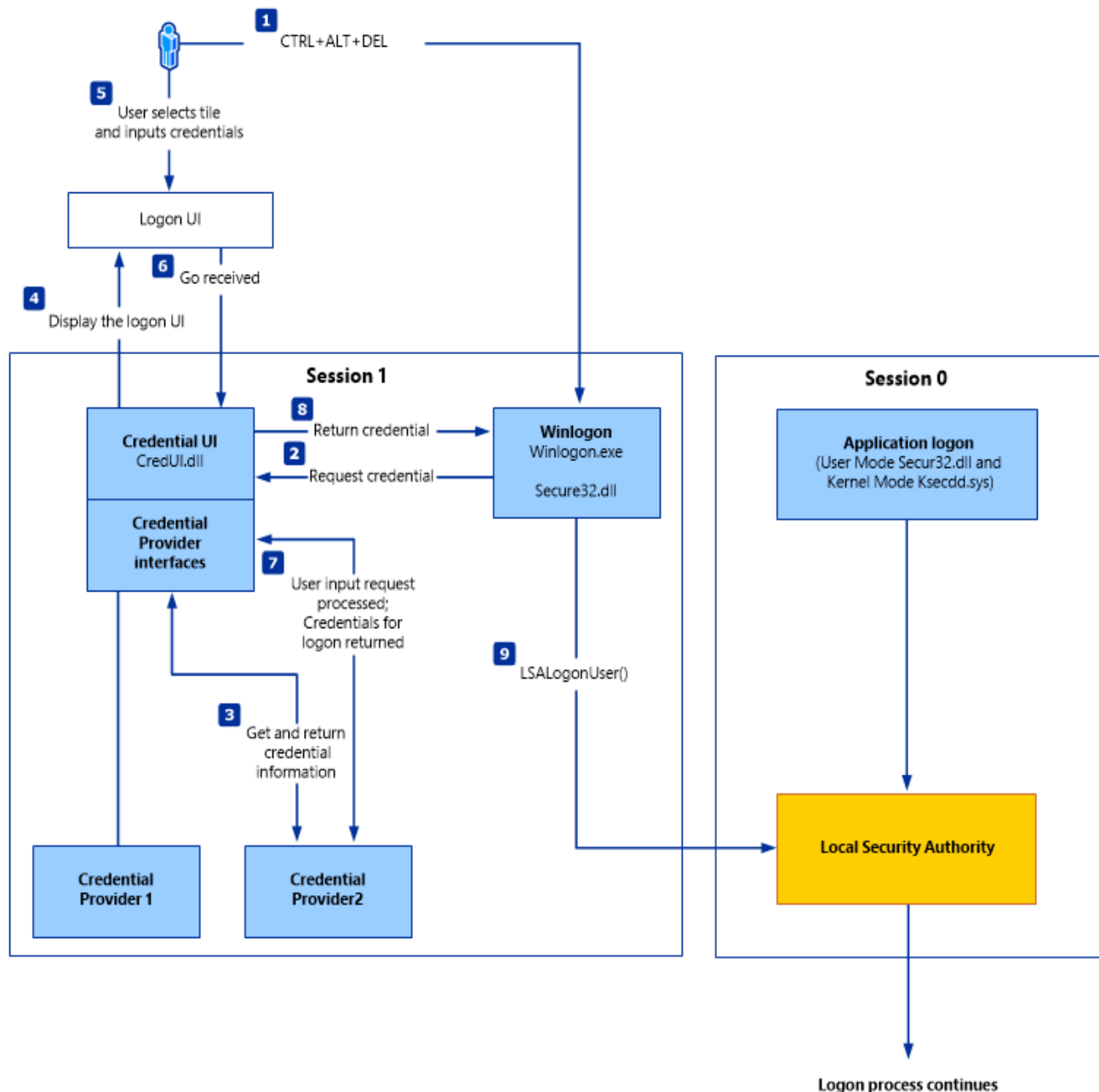


Since Windows Vista, credential providers have replaced the old mechanism of GINA for logging in.

The intended purpose of credential providers are to allow third-party custom authentication schemes to support different method of logging in. However, this flexibility also allows malware authors to write credential stealers.



Winlogon loads credential providers by checking the registry at

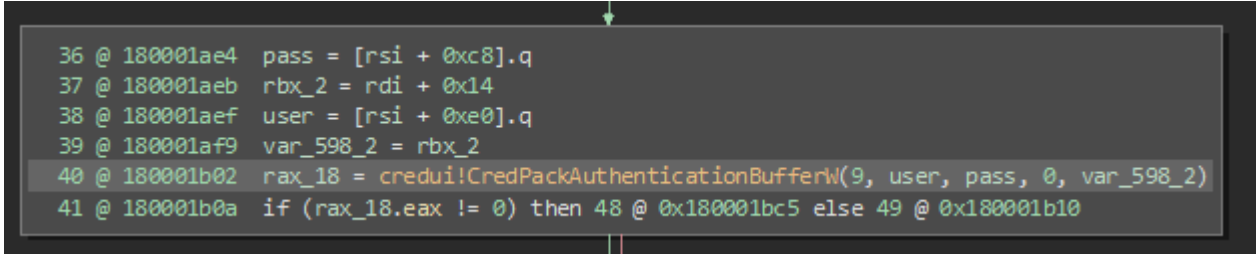
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\

to see which providers are enabled. For each enabled entry, it then attempts to load the DLL specified at

HKEY_CLASSES_ROOT\CLSID\{*CLSID*}\InprocServer32

and requests the credential provider to provide a login form. After credentials are entered into the provided form, they are then submitted to the Credential Provider for serialization and sent to the LSASS for verification.

One easy modification for a malware writer would be in the serialization function which handles packing the provided username and password into a format recognizable by the LSASS. You can recognize this function in assembly by looking for a call to CredPackAuthenticationBufferW



The image shows a snippet of assembly code from a debugger. A green arrow points to the instruction at address 180001b02. The code is as follows:

```
36 @ 180001ae4 pass = [rsi + 0xc8].q
37 @ 180001aeb rbx_2 = rdi + 0x14
38 @ 180001aef user = [rsi + 0xe0].q
39 @ 180001af9 var_598_2 = rbx_2
40 @ 180001b02 rax_18 = credui!CredPackAuthenticationBufferW(9, user, pass, 0, var_598_2)
41 @ 180001b0a if (rax_18.eax != 0) then 48 @ 0x180001bc5 else 49 @ 0x180001b10
```