

CodeEngn 2010

Art of Keylogging

Keyloggers who are nothing to do with the
keyboard security solution

강병탁 (window31)

2010.07.03

Who am I?

- ByungTak Kang (window31)
 - NEXON / Security Team – Hacking Analysis, Security Programming
 - A contributor to “Microsoftware” a monthly IT Magazine for over 2 years
 - A lecturer on hacking/reversing/security at various institutions (KISA, security community, universities, etc)
 - 2009 Microsoft MVP Developer Security

Agenda

- Prologue
- Keylogging Windows Account
- Login without password
- Keylogging on the website
- Social Engineering Keylogging
- Bypass Keyboard security solution
- Offensive and defensive

Prologue

Serious account issues

**스스로 지키는
내 개인정보!**

회원님은 **장기간 비밀번호를
변경하지 않으셨습니다**

동일한 아이디와 비밀번호로 여러 사이트를 이용하고 계시거나
추측하기 쉬운 비밀번호를 사용하실 경우 피해를 입으실 수도 있습니다.

개인정보 도용으로 인한 피해를 예방하기 위해서 정기적인 비밀번호 변경을 권장합니다.
장기간(6개월 이상) 비밀번호를 변경한 적이 없는 경우 개인정보 보안을 위해
새로운 비밀번호로 변경하여 주시기 바랍니다.
[비밀번호 변경 이후 이전 비밀번호로 재변경하시면 개인정보 위험에 노출될 수 있습니다.]

 **개인정보보호
공동캠페인**



Endless account problems

- Why do we still face many problems even after Keyboard security solution is installed ?
- What is the trend of malicious code today ?
- What we must do ?



Endless account problems

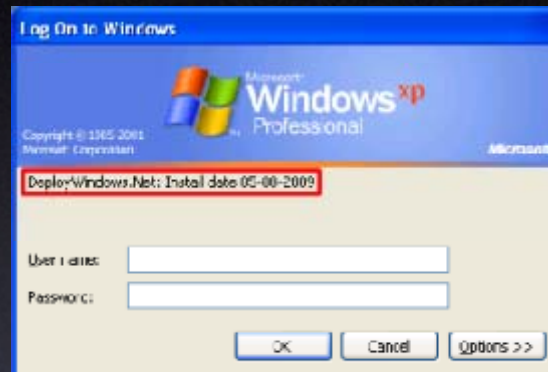
Trojan-PWS/W32.WebGame.101888.K
Trojan-PWS/W32.WebGame.102768.B
Trojan-PWS/W32.WebGame.102805
Trojan-PWS/W32.WebGame.103150
Trojan-PWS/W32.WebGame.103182
Trojan-PWS/W32.WebGame.103463
Trojan-PWS/W32.WebGame.103556
Trojan-PWS/W32.WebGame.103810
Trojan-PWS/W32.WebGame.10524
Trojan-PWS/W32.WebGame.10724
Trojan-PWS/W32.WebGame.10764
Trojan-PWS/W32.WebGame.110145
Trojan-PWS/W32.WebGame.111085
Trojan-PWS/W32.WebGame.11218
Trojan-PWS/W32.WebGame.116274
Trojan-PWS/W32.WebGame.116606
Trojan-PWS/W32.WebGame.116822

.....

Hundreds of viruses signature are added each day

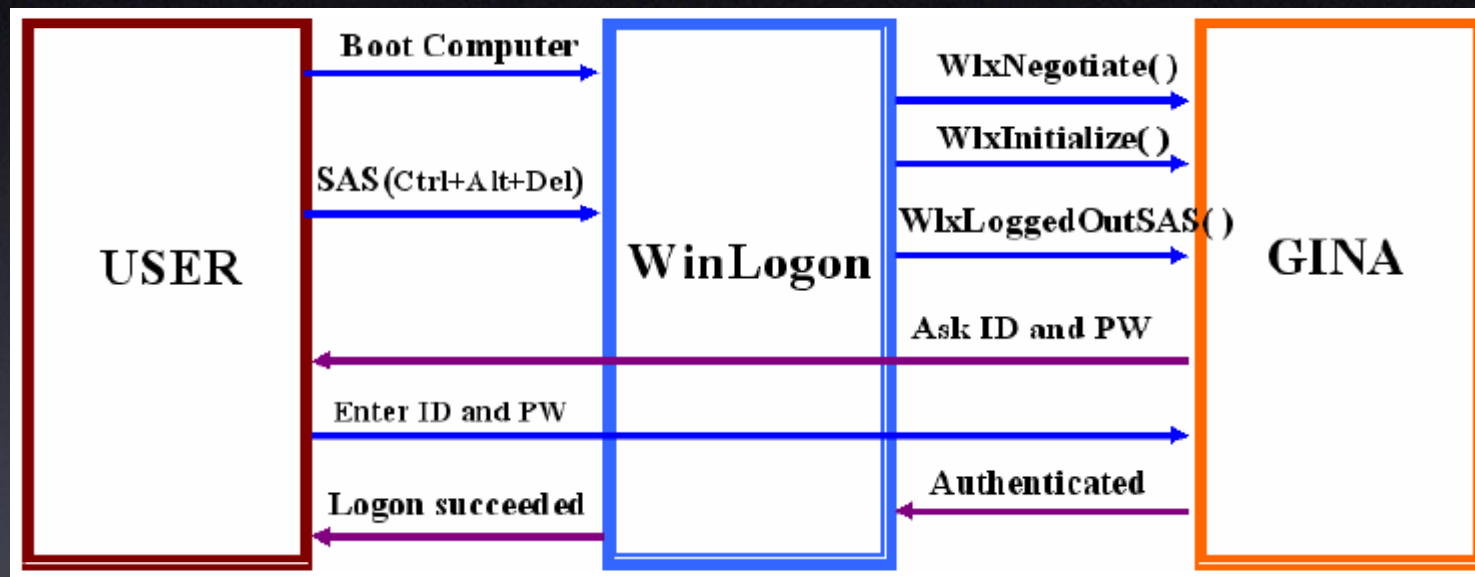
Keylogging Windows Account

Windows Account



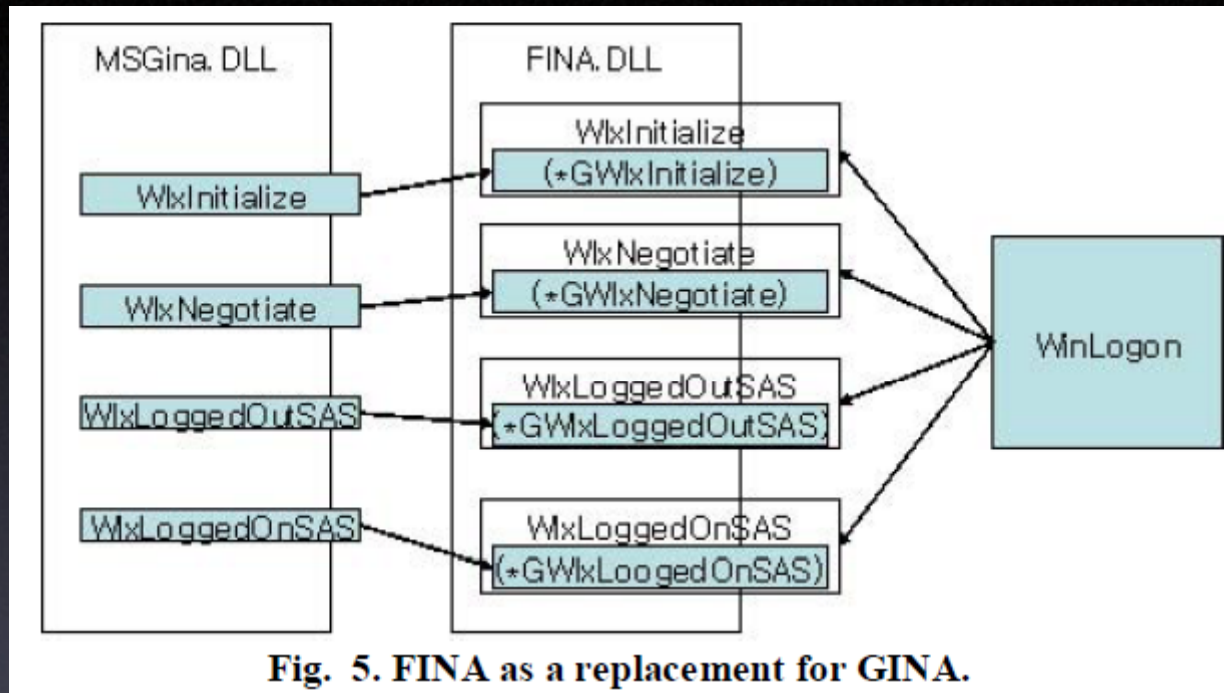
the winlogon.exe is what you come to face when you walk up to a locked or un-logged-on computer.

msgina structure



Interaction between winlogon and GINA

msgina structure



The library file msgina.dll, is required by windows. It is used by WinLogon within windows, when performing user authentication.

WlxLoggedOutSAS

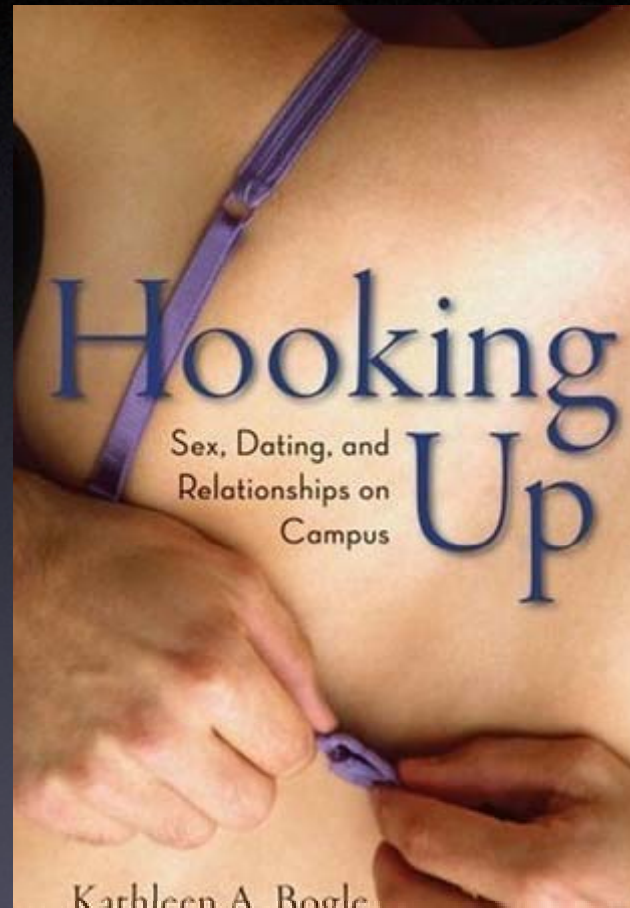
```
int WlxLoggedOutSAS(  
    PVOID pWlxContext,  
    DWORD dwSasType,  
    PLUID pAuthenticationId,  
    PSID pLogonSid,  
    PDWORD pdwOptions,  
    PHANDLE phToken,  
    PWLX_MPR_NOTIFY_INFO pNprNotifyInfo,  
    PVOID *pProfile );
```


WLX_MPR_NOTIFY_INFO

```
Typedef struct _WLX_MPR_NOTIFY_INFO {  
    PWSTR pszUserName;  
    PWSTR pszDomain;  
    PWSTR pszPassword;  
    PWSTR pszOldPassword; } LX_MPR_NOTIFY_INFO;
```

Here we can see a meaningful structure !!!

msgina Hooking



Reversing msgina Malware

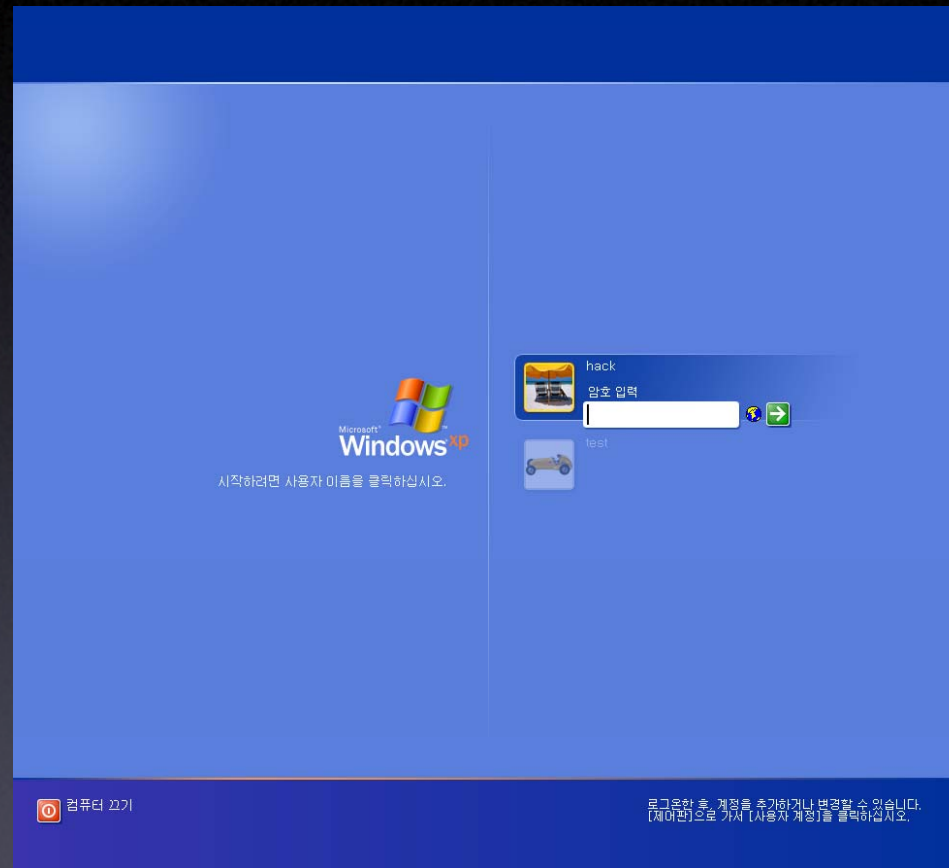
Naming

- winlogonHijacker
- Domain Keylogger.

DEMO

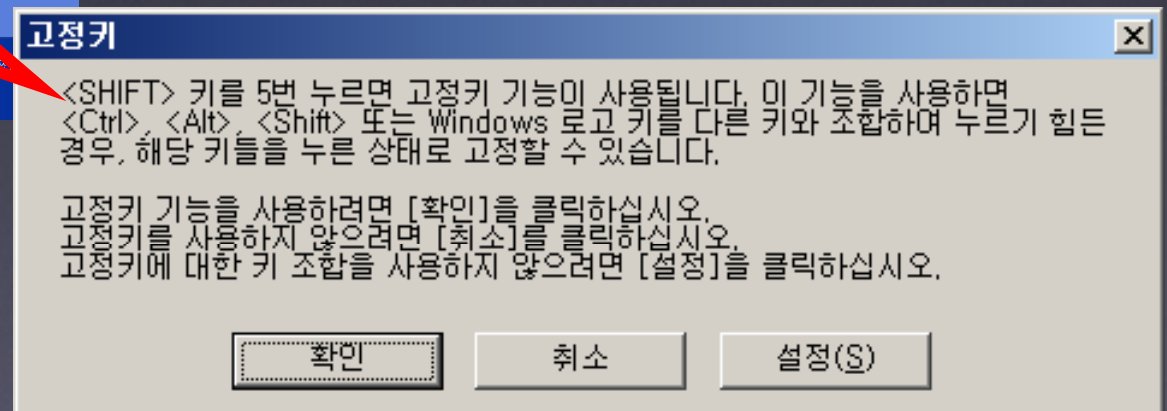
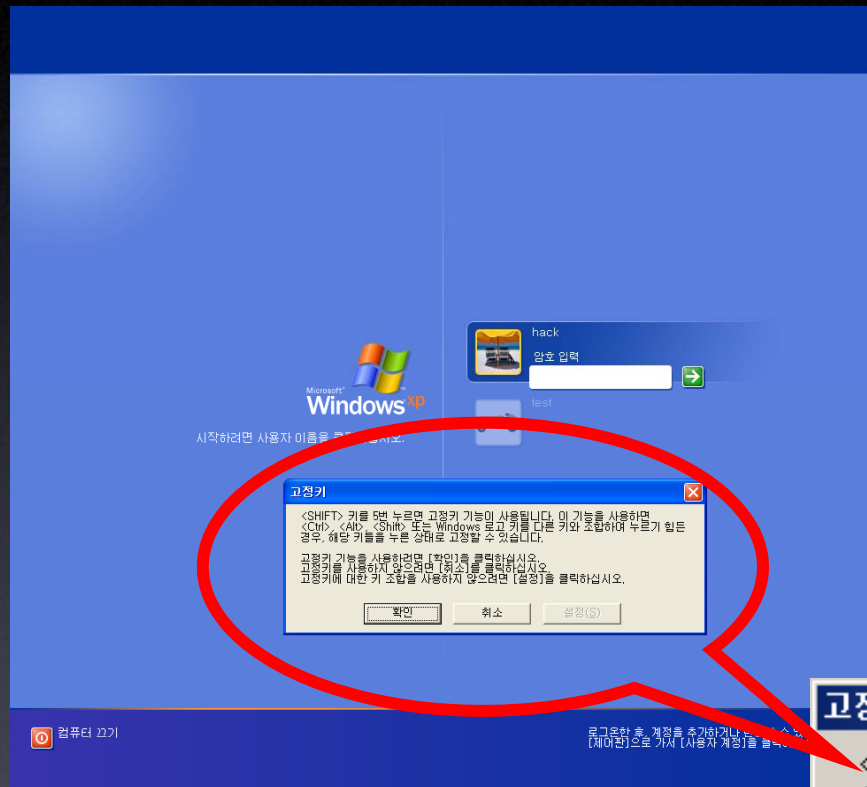
Login without Password

Windows Account

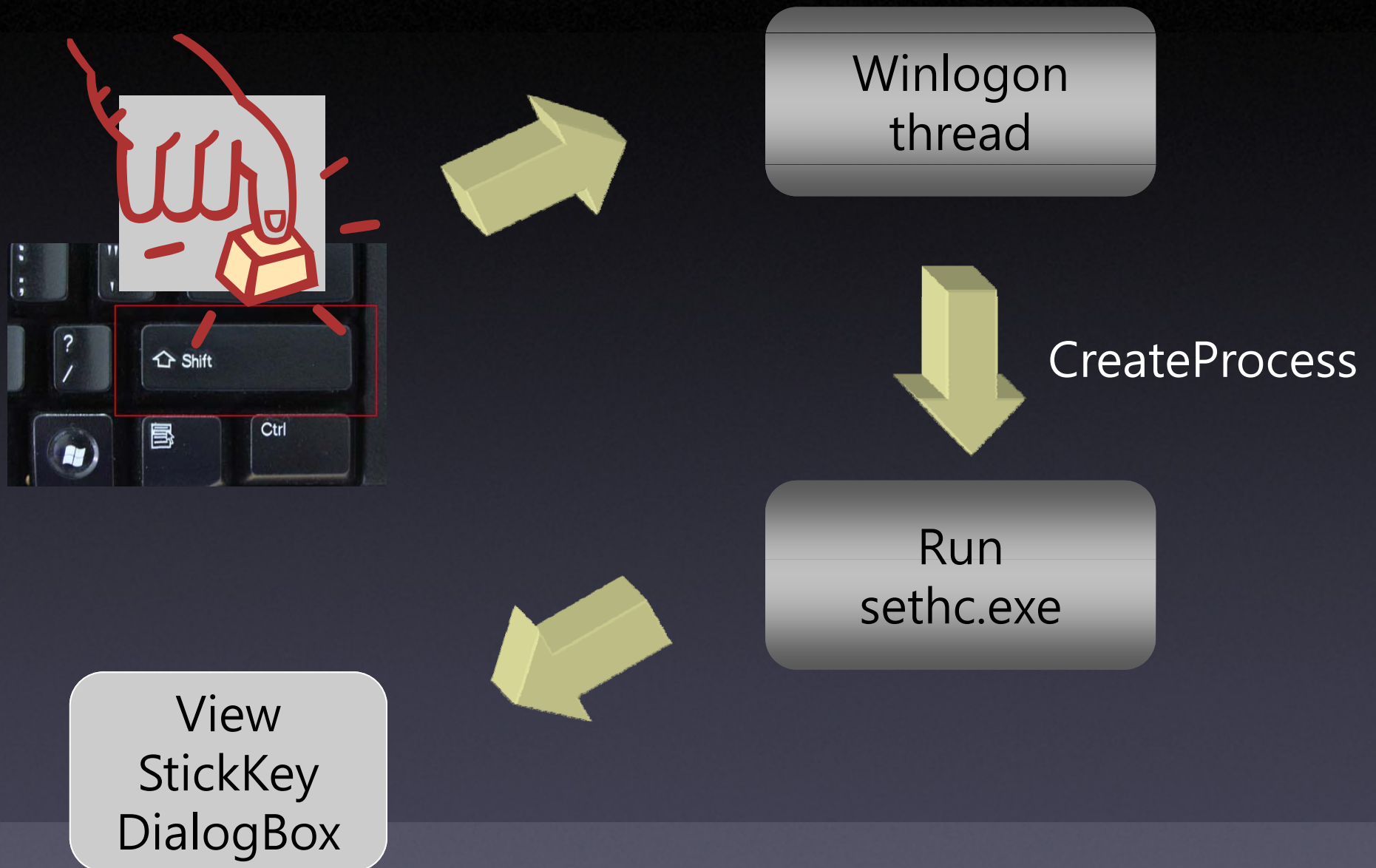


If you press the Shift key 5 times...

StickKey Popup

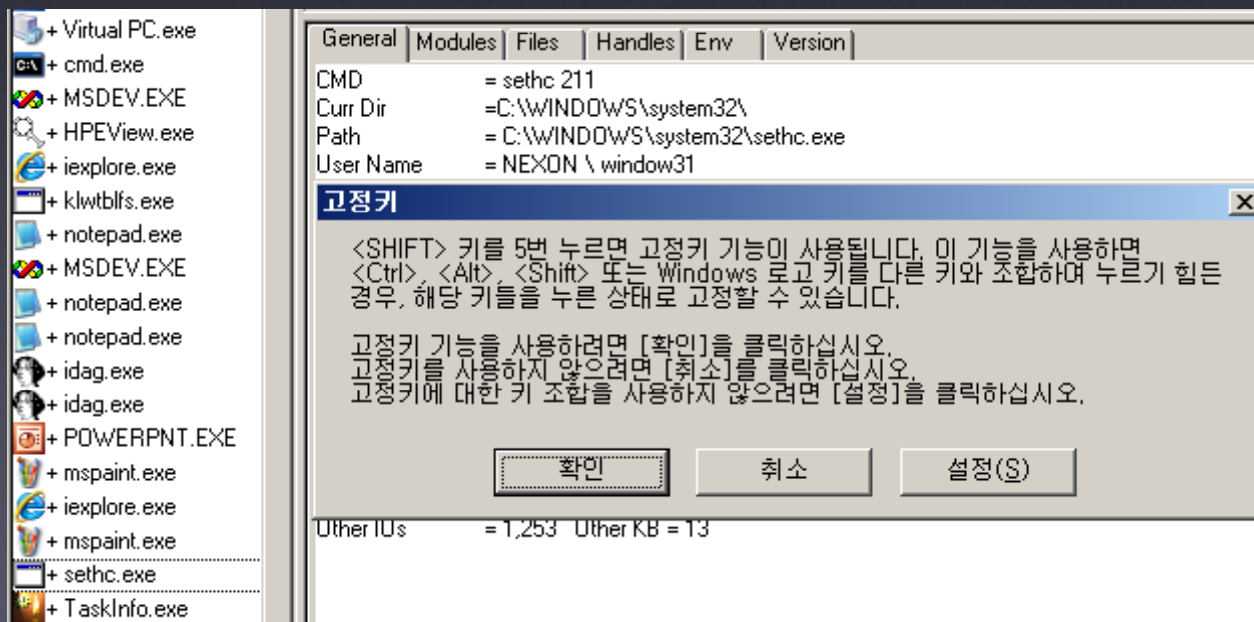


StickKey run structure



StickKey Local Backdoor

- You are able to connect without ID/PW !!!
- You can see the explorer or command prompt at the login prompt without authentication.



Behavior structure

Disable WFP

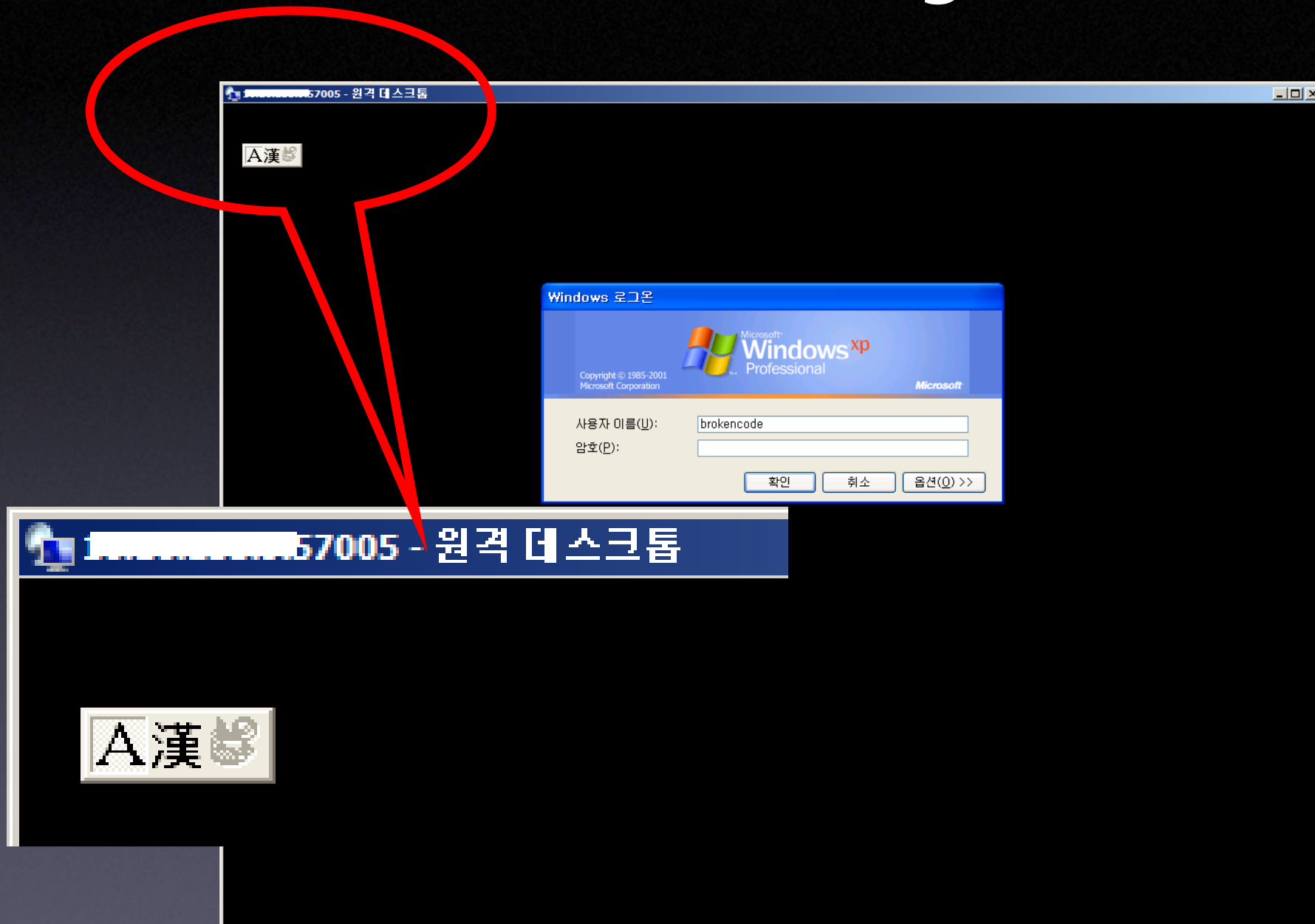
Change File

press the Shift
key

Login success

- Disable WFP (Windows File Protection)
- Replace the files.
- Now, If I press key five times, I can login at any time.

Terminal Login



Next action

- Create a new user account,
"c:\w\net user iamhacker /add"



- Add this user to the administrators group
"c:\w\net localgroup administrators iamhacker"
- Remove StickKey Local Backdoor and Enable WFP
(To avoid as doubt as hacking)

Which platform is this vulnerability?

- Windows 2000
- Windows XP
- Windows 2003
- Windows Vista

Most of windows OS does not check the integrity of the file that launches StickyKeys "sethc.exe" before executing it.

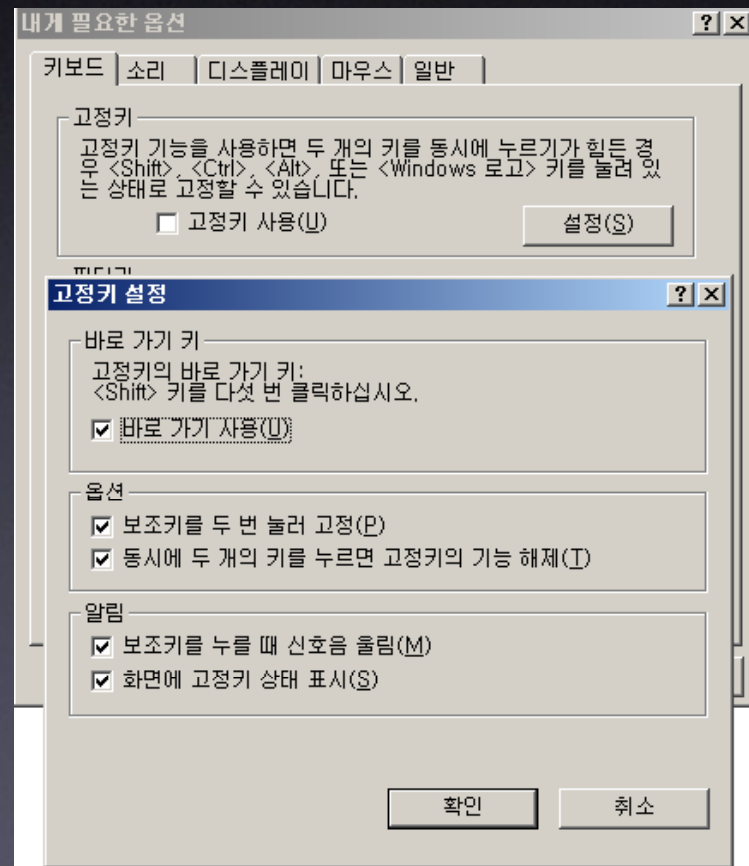
From now on

Don't forget to hit the shift key five times and
see what pops up on your desktop
....everyday :p



Remove StickKey

This is the real answer.



Reversing stickkey Malware

DEMO

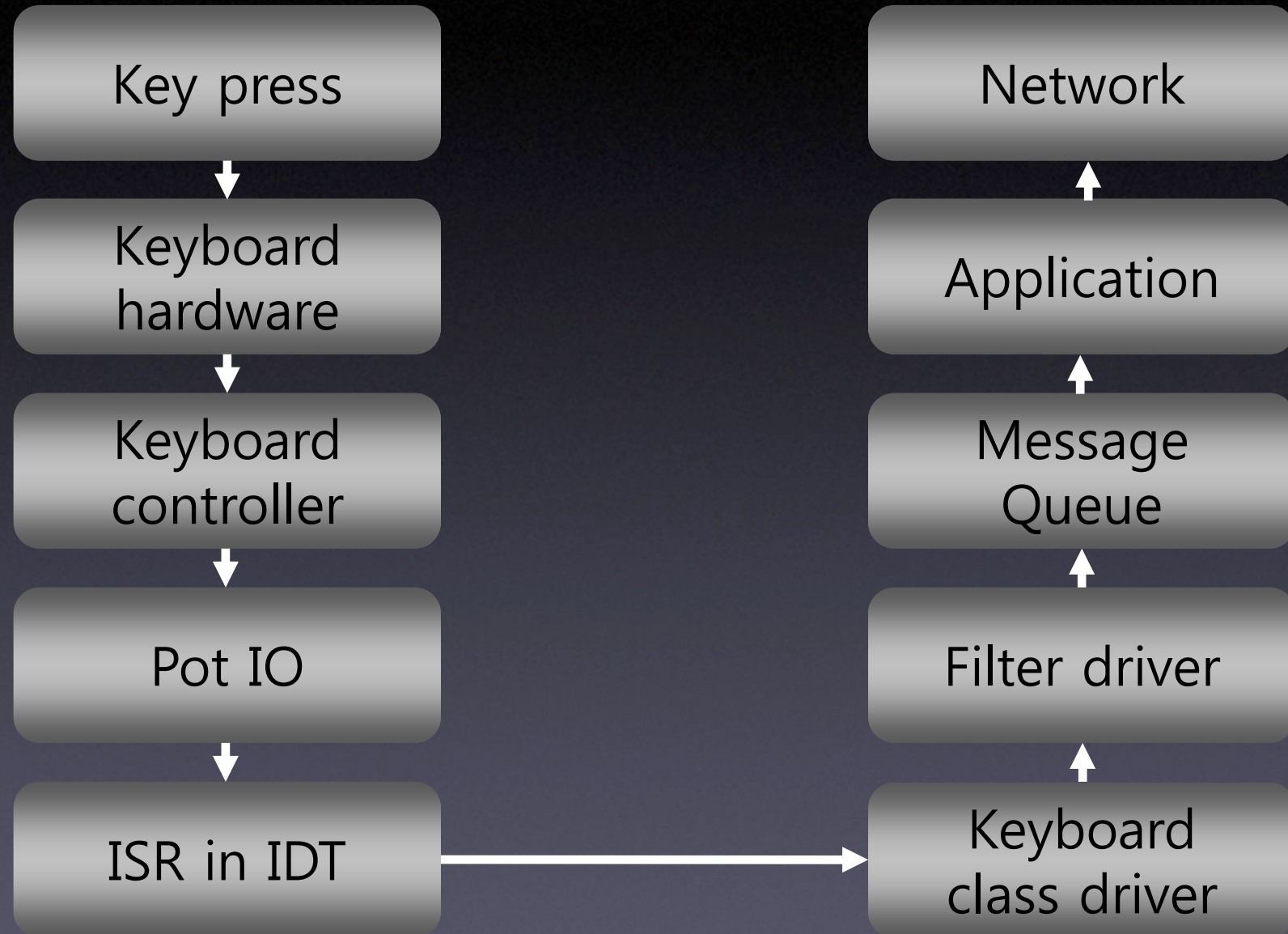
Keylogging on the website

Web-based login

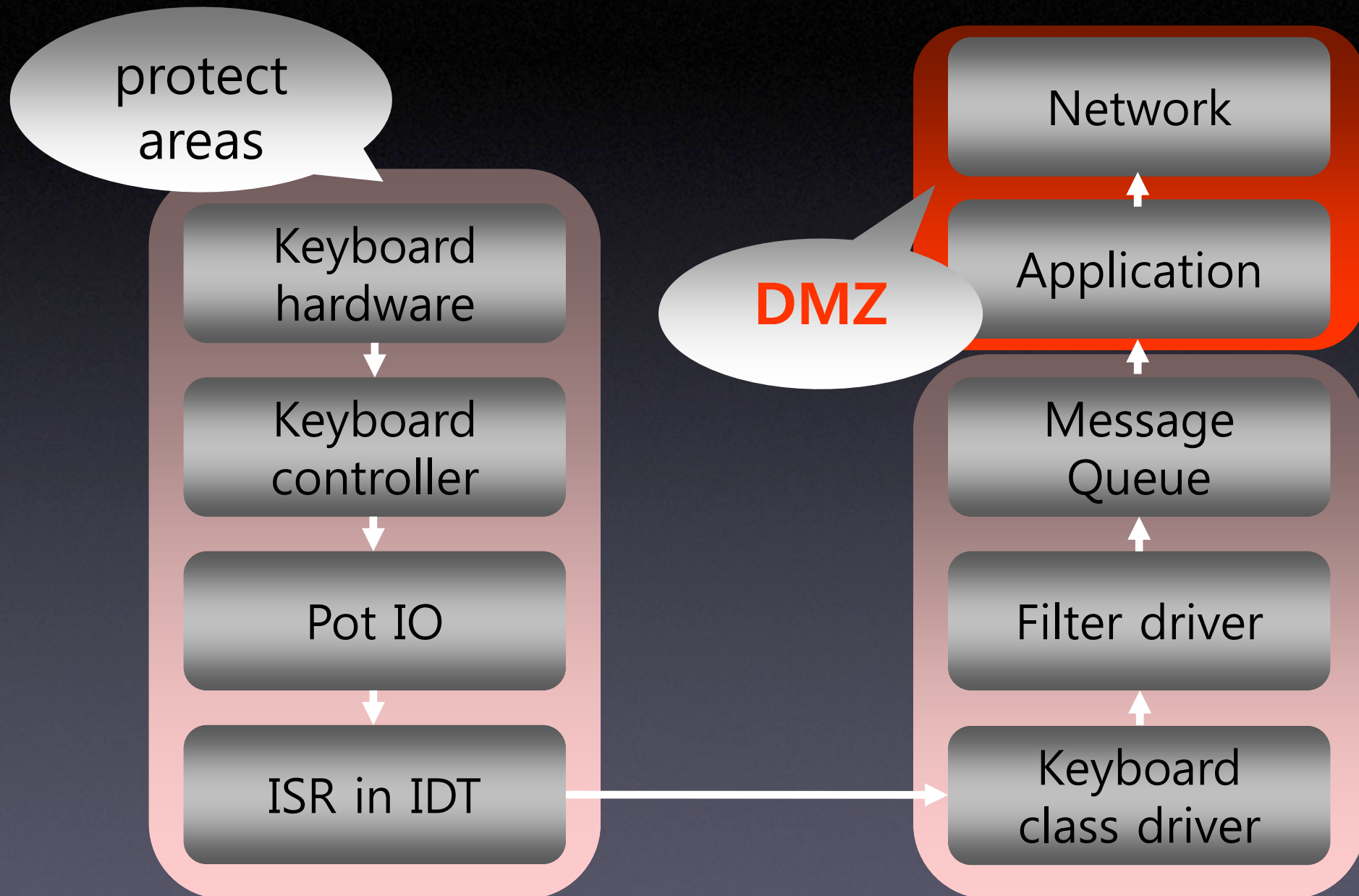
A web-based login form with two input fields (username and password) and a '로그인' (Login) button. Below the button are two checkboxes: '키보드보안' (Keyboard Security) and '개인방화벽' (Personal Firewall). At the bottom are links: '회원가입' (Sign Up), '아이디찾기' (Find ID), and '비번찾기' (Find Password).

- Very vulnerable
- Method of attack is varied
- Keyboard security solution exists (Almost always)

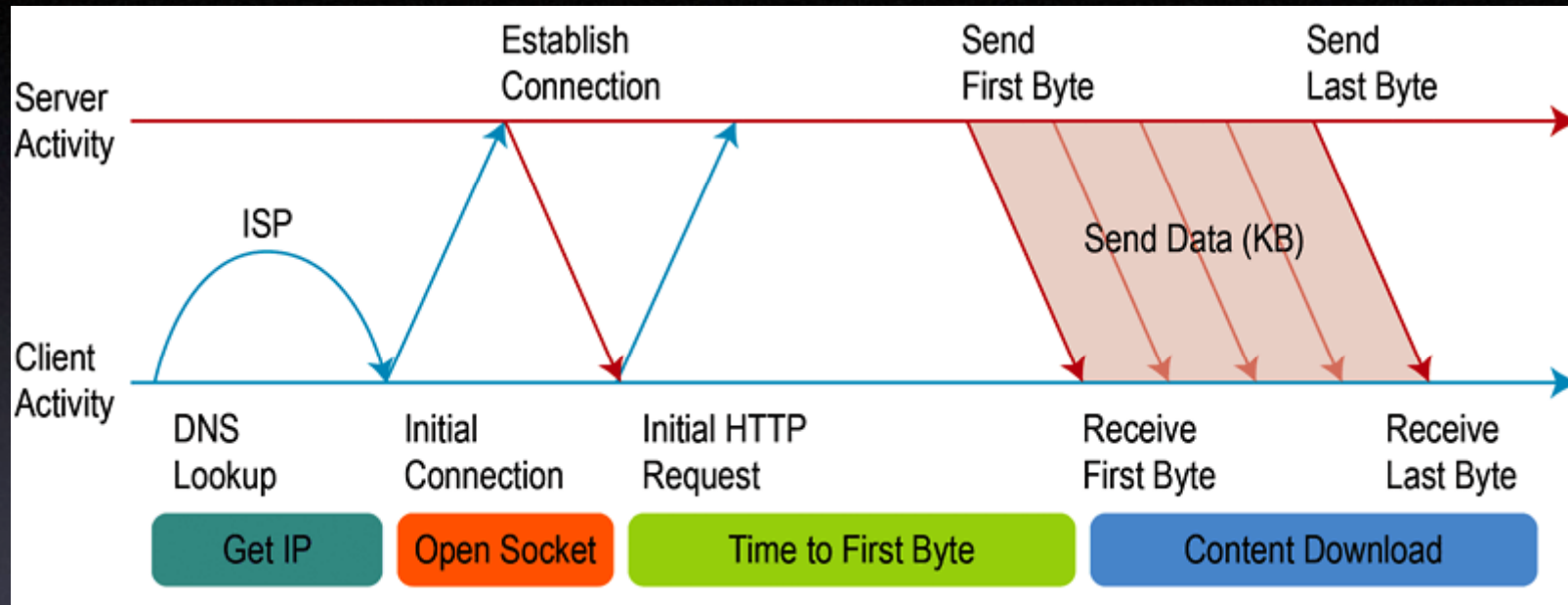
Attack position



Keyboard security solution



Protocol handler



Wininet.dll is the protocol handler for HTTP, HTTPS and FTP. It handles all network communication over these protocols.

Query hook

url=http%3A%2F%2Fwindow31.com&fail_ur
l=&loginsite=&site_id=31&adult_yn=N&enc
oding_type=utf-8&ukey=1BB
7E5F2937203480D408B5196E9AC3B9DDF487
E636EA15426FAEABDAFB00A6908F
2069ECB5FA6C7B618E4C68C5F37C2900DB07
DE9A0CACEC7300A6DBD342A83&game_id=
13&id=window31&pwd=fucking

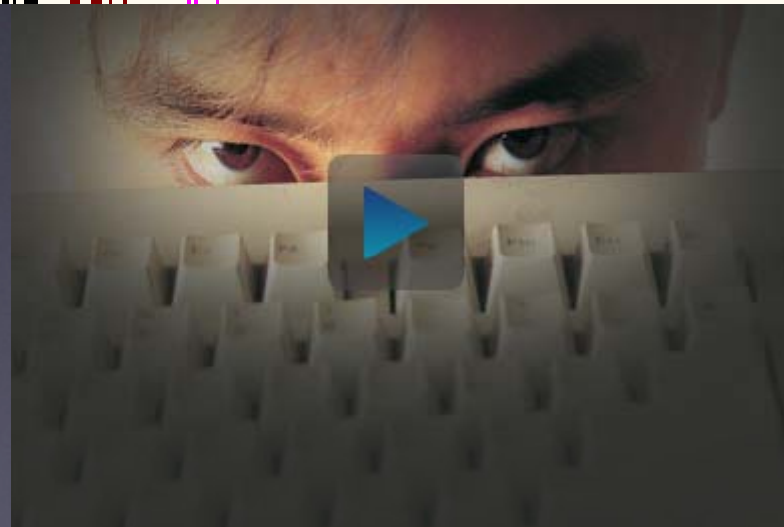
The API issue

🌟 - [CPU - thread 00000218, module urlmon]

File View Debug Plugins Options Window Help

Paused

| | | | |
|----------|---------------|--|----------------------------|
| 43F3FD57 | F7D9 | neg ecx | |
| 43F3FD59 | 1BC9 | sbb ecx, ecx | |
| 43F3FD5B | 51 | push ecx | |
| 43F3FD5C | 50 | push eax | |
| 43F3FD5D | FF76 78 | push dword ptr ds:[esi+78] | |
| 43F3FD60 | FF15 4C60FD43 | call near dword ptr ds:[43FD604C] | WININET.HttpSendRequestW |
| 43F3FD66 | 3BC3 | cmp eax, ebx | |
| 43F3FD68 | 0F85 E0FF0000 | jnz urlmon.43F4FD4E | |
| 43F3FD6E | FF15 0C17F243 | call near dword ptr ds:[<&KERNEL32.GetLastError] | ntdll.RtlGetLastWin32Error |
| 43F3FD74 | 2B F5000000 | mov ecx, 0 | |



Reversing malware



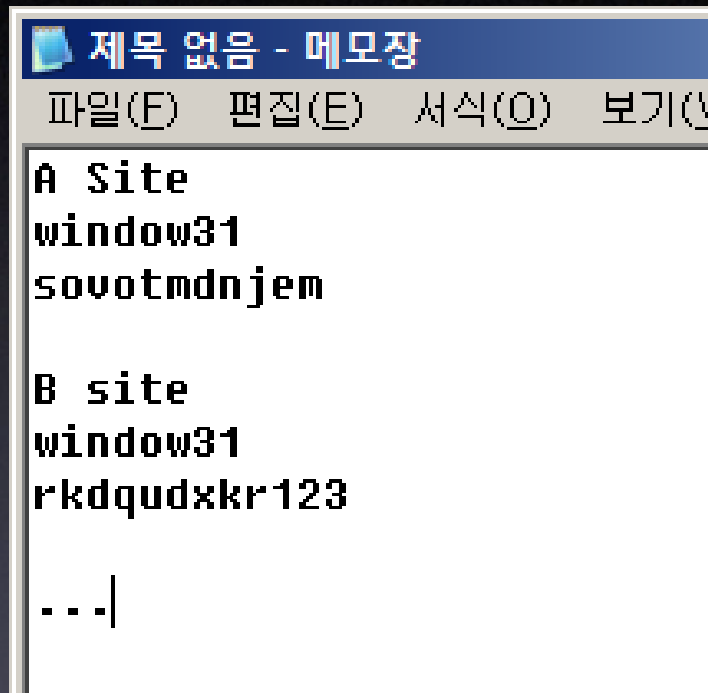
DEMO

Social Engineering Keylogging

Human habits



Bad habit



We do copy and paste unconsciously.
Even the password.

Funny Code

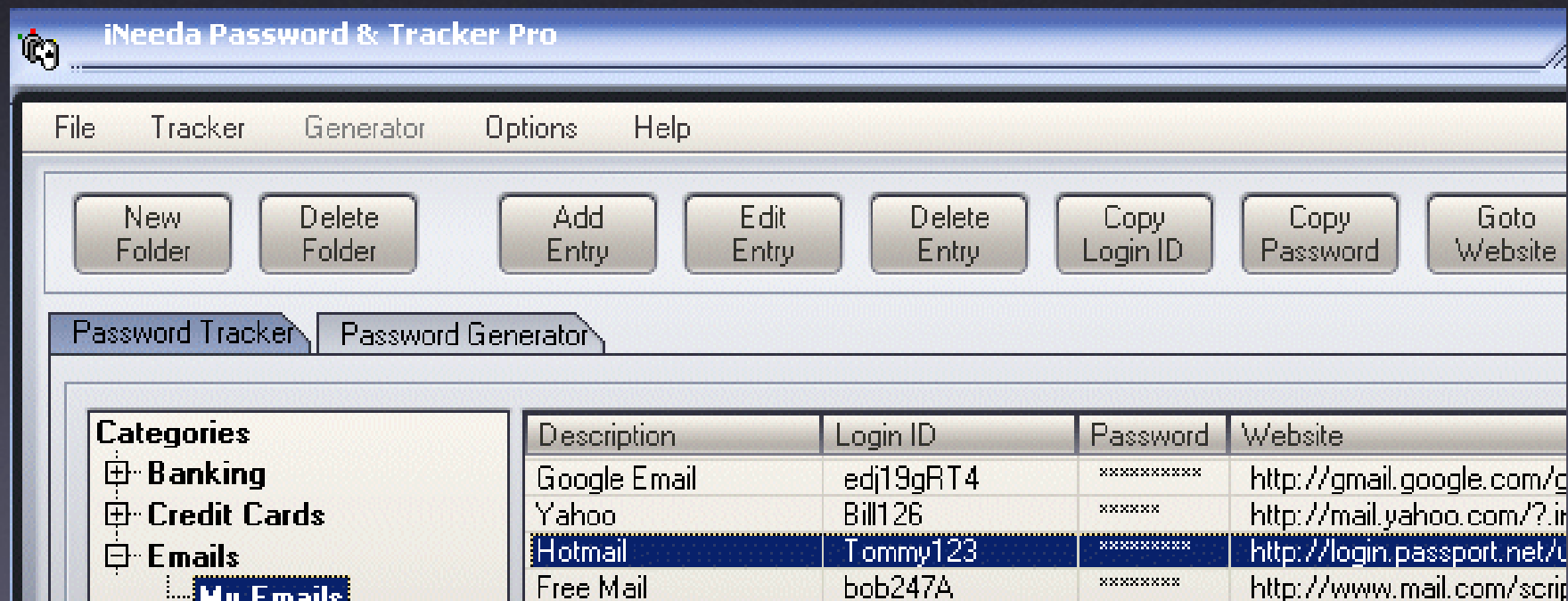
```
while(1)
{
    // ...
    GetClipboardData(CF_TEXT);

    // ...
    if (bMaybePW)
        SendDataToHacker();

    Sleep(500);
}
```

Problems

- This technique is based on the human behavior.
- You do not have a login, you can be attacked (for example, paperwork etc).



Bypass Keyboard security solution

Why?



Offensive and defensive

Hooking detection.

13:12:31:889 [0x756E40D4] jmp msg1na.dll.0xB0A588

13:12:31:889 Found inject code !!! 5 byte diff

13:12:31:889 doubt module: [pid: 420]

\\?\\C:\\WINDOWS\\system32\\winlogon.exe -
c:\\windows\\system32\\msgina.dll

13:12:31:889 [KEYLOGGER] Domain Keylogger
detect !!!! winlogon.exe - msgina.dll inject

I hope AntiVirus vendors.

- WFP check
- Check sethc.exe
- StickyKeys option turns off.
- Winlogon dll injection, integrity check

Conclusion

- Keyboard security solution can not prevent everything
- Each location requires different security.
(ex. kernel : ring0, app : integrity check)
- Parameters should be encrypted.
- Let's try reversing a lot of malicious code. We can get a hint and we learn a lot of their technology.
- The AntiVirus should be upgraded more behavior-based features

Question

<http://www.window31.com>
window31com@gmail.com
Twitter : @window31com