“Gaming the Gamers: Tricks of the Trade in the World of PWS War-craft”

Chun Feng
Microsoft Malware Protection Center, Australia
chun.feng@microsoft.com

Microsoft

Agenda

- Introduction to the **black market** of password stealing
- **Protection mechanisms** used by online games' security
- **Tricks** used by password stealers designed to break protection systems
- **Advice** for games users and game vendors
- Conclusion

Microsoft

Malware as Business

On this black market:

- PWS malware: US$300 (including 4 months update)
- Stolen account/inventory:
  - Account US$1 - US$20
  - Rare items: More than US$1000

Microsoft

Moving with the Times

"there is an escalating fight between the anti-malware vendors/online game vendors and the operators of the black markets." *VB 2008, Ottawa*

Sep 07

Win32/Dogrobot

1st PWS targeting hard disk recovery card

June 08

Win32/Dexfom

1st Game DLL infector

Dec 09

Win32/Checkafe

1st PWS targeting host/account binding

March 10

WinNT/Ghodow

1st PWS infecting MBR

Microsoft

Password Stealing Opportunities

Entered via keyboard

Saved in memory

Sent over “wire”

Keylogger

Memory sniper

Packet sniffer/
Network
API/Hooks

Microsoft

Password Manager – Anti-Keylogger

- 3rd party security software
- No need to type-in passwords anymore!
  - Pre-save passwords in password manager
  - When login window is located, the password is sent to login window (encrypted)

Microsoft

Protecting Passwords in Memory

- 3rd party security software:
- Hook particular APIs
  - NtReadVirtualMemory()
  - NtWriteVirtualMemory()
- Deny other processes access to game process memory

Microsoft

Memory Watcher

- Used by game applications
- Check the integrity of the key code (e.g. password handling code) to prevent it from being modified
- Memory watcher code may also be watched by another memory watcher

Microsoft

Strengthening Protection

- Game Password Matrix card

	1	2	3	4	5	6	7	8
A	03	25	96	06	38	68	44	57
B	58	08	46	91	40	52	05	63
C	76	88	55	09	30	87	85	27
D	19	09	84	11	22	76	17	30
E	28	83	69	34	22	99	33	19
F	33	71	21	66	04	41	05	55
G	64	83	47	76	12	62	14	08
H	39	04	62	78	60	83	28	48
I	87	77	05	48	01	36	88	29
J	95	16	22	95	46	21	42	36

Either a **physical card** or a **digital image file**

Microsoft

Strengthening Protection (contd.)

- One-Time Password(OTP)

Microsoft

Strengthening Protection (contd.)

- Account/Host binding – a user can login from a specific host only (unique hardware profile assigned to an account)

Microsoft

Stealing Passwords from Memory

- Memory sniper (anti-Password Manager)
  - Password stored at a fixed address?
    - Just read from that offset!
  - Password stored at a variable address?
    - Patch code!

Microsoft

Overcoming Game Memory Protection: No One Can Stop Me!

- Trick: Load malware as part of the game process
  - DLL Infection
  - DLL Hijacking

Microsoft

No One Can Stop Me! - DLL Infection

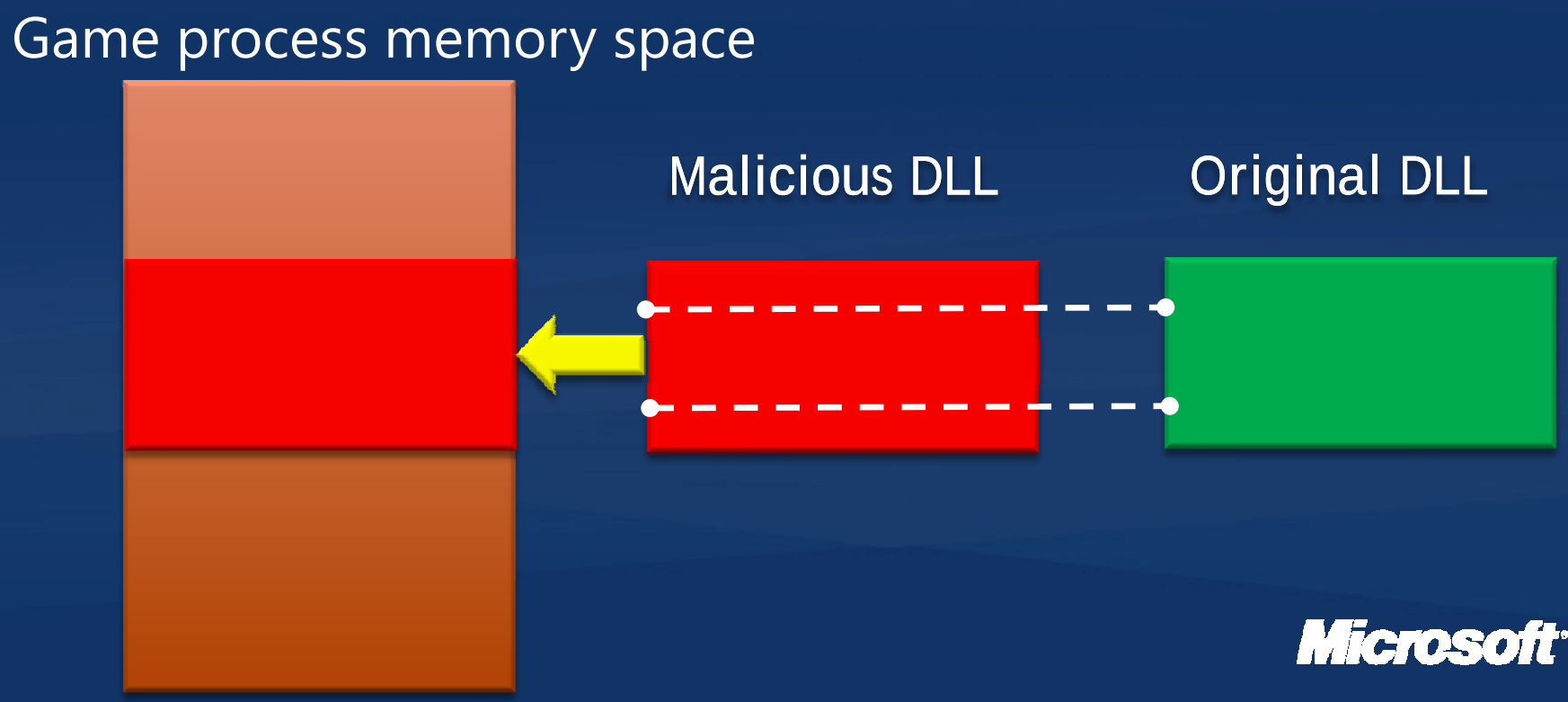
Infect or modify DLLs loaded by the game (e.g. DirectX):

- **Parasitic infection**
  - Append malicious code
- **Parasitic infection with companion DLL**
  - Add a stub to load another malicious DLL
- **Import Patching with companion DLL**
  - Add an Import to Import Table to load another malicious DLL

Microsoft

No One Can Stop Me! - DLL Hijacking

- Replace original DLL loaded by game
- Forward exported functions to original DLL



Microsoft

Bypass Memory Watcher: PWS as a debugger!

- Manipulate the debug registers (DR0~DR7) to set **hardware breakpoints** at the right address
- Handle the exceptions caused by hardware breakpoints. Use **exception handler** code to steal the data
- No memory patch needed at all

Microsoft

Breaking Matrix Card Protection Offline Steal

- Method 1: This area is under video surveillance!
  - Terminate the game process to force the user to re-login
  - Monitor the foreground window; if it is a picture-viewer application (e.g. ACDSee), then it takes a screenshot and posts it to a remote server

Microsoft

Video Demo of Breaking Matrix Card Protection (Offline Steal)

Video from an underground website used to demo their products.

Microsoft

Breaking Matrix Card Protection & One-Time Password Online Steal

- Method 2: Man in the middle attack

3. It is 13!

4. It is 13!

2. What is the number at (E,8) on the card?

1. What is the number at (E,8) on the card?

Microsoft

Breaking Account/Host Binding

- Are you from Internet Café? (Win32/Chekafe)
  - Check for Internet Café administration software
  - If not found, post MAC address (hardware ID)

Microsoft

Attacking Human Interface

- Social Engineering
  - Game cheat software
  - Game hacking tools
  - Licence generators
  - Prize winning phishing messages
  - *and many others…*

Microsoft

Anti-Anti-Malware

- Anti-Emulation trick examples:
  - Zero section PE file – still valid! (Win32/Chekafe)
  - Hacked packer code to mislead the unpacking. Use of relocation data to rebuild code (Win32/Taterf)

Microsoft

Anti-Anti-Malware

Detection bypass trick examples:

- Hide alert Window; set parent Window to an invisible Window (Win32/Dogkild)
- Close the handles used by anti-malware software to prevent it from working properly (WinNT/Ghodow)
- Low-level disk operation by port I/O (IDE port 0x1f0-0x1f7 and 0x3f6). All drivers bypassed!

Microsoft

Other Tricks

- Which company are you from? (Win32/Ghodow)
  - For each running process, malware checks the origin of an executable file by looking at "Version Info" in its resources. Process will be terminated if

```
Verified:        Signed
Signing date:    6:57 PM 2/18/2007
Strong Name:     Unsigned
Publisher:       Microsoft Corporation
Description:     Notepad
Product:         Microsoft« Windows« Operating System
Version:         5.2.3790.3959
File version:    5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
```

  you may be "terminated" - no matter what your name is ☺

Microsoft

Other Tricks (contd.)
Installed as Input Method Editor (IME)

- IME is used to input Eastern Asian Characters via the key board
- IME will be loaded into every process
- IME captures every key stroke without hooking

Refer to "*IME as a possible Keylogger*" VB Magazine November 2005

Microsoft

Advice for Game Players

- Install the latest security patches
- Be aware of abnormal application terminations
- Be cautious when using game cheat software
- Use matrix cards correctly / protect matrix card data. Avoid storing it on the same host where you play games
- If it seems too good to be true, it probably is – be wary of winning competitions you never entered. There is no free lunch, while there is free phishing and free trojans

Microsoft

Advice for Game Vendors

- Wipe the memory, when possible
- Use integrity checking on the files loaded
- Use complex machine ID algorithms
- Warn the user when the account is attempted to be logged in from different locations at the same time
- Checks for “debugger” (debug register value)

Microsoft

Conclusion

- The black market of password stealing drives the evolution of password stealing malware
- Tricks targeting game protection, anti-malware and game users are commonly used every day in numerous ways
- Online game security models need collaboration of anti-malware vendors, game vendors and game users

Microsoft

Q & A

chun.feng@microsoft.com

Microsoft®

Your potential. Our passion.™