Malware - Backdoors

Information Security – Lecture 21

Aadil Zia Khan

Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

Trojan	*Logic Bomb*	*Trapdoor*	*Virus*	*Worm*	*Zombie*

Malware

- Differentiation based on
  - How they spread to reach the desired targets
  - The actions they perform once a target is reached

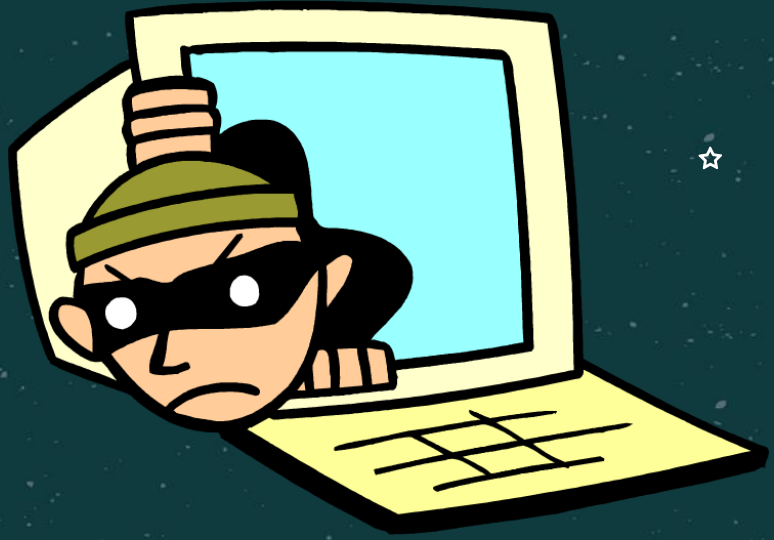
Trojan Horse

- Program with hidden side-effects
- Usually superficially attractive
  - eg game, s/w upgrade etc
- When run, it performs some additional tasks
  - Allows attacker to indirectly gain access they do not have directly
- Often used to trick victim into propagating a virus/worm or installing a backdoor or simply to destroy data

Logic Bomb

- One of earliest types of malicious software
- Activated when specified conditions met
  - Presence/absence of some file
  - Particular date/time
  - Particular user
- When triggered can damage system
  - modify/delete files/disks, halt machine, etc.
- How can it be used for DDoS???

Backdoor (or Trapdoor)



- Secret entry point into a program
- Allows those who know about it to access the system by bypassing security procedures
- A backdoor may take the form of
  - Hidden part of a program
  - Separate program
  - Code in the firmware of the hardware
  - Parts of an operating system
  - Default passwords can also function as backdoors if they are not changed
  - Debugging features can also act as backdoors if they are not removed in the release version

A Simple Backdoor Using netcat

- netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP
- It can be used to make any process a network server
- The -e option spawns the executable with its input and output redirected via network socket
  - It can listen on a port and pipe the input it receives to the specifies process
  - It can read the output of the process and pipe it to the port

A Simple Backdoor Using netcat

- Create a listening port that will allow us access to a shell (command line) on the system
  - Command for Linux: nc -l -p 1234 -e /bin/bash
  - Command for Windows: nc -l -p 1234 -e cmd.exe
- In each case, we are telling netcat to listen for connections on port 1234 and to execute a program that will give the connecting client access to the shell
- Some administrators block netcat for security purposes

Famous Backdoors

- Several backdoors in the unlicensed copies of WordPress plug-ins were discovered in March 2014
  - They were inserted as obfuscated JavaScript code and silently created an admin account in the website database
  - A similar scheme was later exposed in the Joomla plugin
- In January 2014, it was discovered that Samsung Android versions are fitted with a backdoor that provides remote access to the data stored on the device
  - Software that is in charge of handling the communications with the modem, using the Samsung IPC protocol, implements remote file server (RFS) commands, that allows the backdoor operator to perform via modem remote I/O operations on the device hard disk or other storage

Famous Backdoors

- Backdoors can be implemented by somehow modifying source code of valid programs
  - In November 2003, attackers added a small code change in Linux code
  - They used = instead of == when comparing user's root access authorization, it actually granted root access to the system - got overlooked easily, and could have been interpreted as an accidental typographical error, rather than an intentional attack

Famous Backdoors

- Backdoors can also be implemented by somehow modifying object code of valid programs
  - Much harder to inspect, as it is designed to be machine-readable, not human-readable
  - These can be inserted either directly in the on-disk object code, or inserted at some point during compilation, assembly linking, or loading
  - Difficult to detect by inspection of the object code, but are easily detected by simply checking for changes (differences), notably in length or in checksum, and in some cases can be detected or analyzed by disassembling the object code

Famous Backdoors

- Compiler backdoors - Ken Thompson Hack (1984)
  - Note – in operating systems like Unix/Linux, C compiler was the central piece of software
    - Almost everything in the system went through the compiler when it was first installed
  - In 1984 KenThompson injected a virus into a compiler so that it now contained two flaws
    1. When compiling its own binary, the compiler must again compile these flaws
    2. When compiling some other code it must compile some arbitrary backdoor into it
  - Thus, the compiler works normally - when it compiles a program, it can create a security backdoor, and when it compiles newer versions of itself in the future, it retains the previous flaws - and the flaws will only exist in the compiler binary so are extremely difficult to detect

when it comes to security, we'd like to not have to trust anyone, but unfortunately that's impossible - you always have to trust someone; even if you compile the operating system yourself, you at least need to trust the compiler

THAT IS WHERE YOUR SECURITY BREAKS

Protection Against Backdoors

- Monitor your system to see if any port (that should not be open) is open
  - This implies the possibility of some backdoor reading to or writing from it
- Have firewalls in place that can block entry points from all but authorized users
- Monitor network traffic
  - Unexpected traffic could imply reading of private data or writing to the system
- Be careful of any open source-based programs (where compiler compiles from source code)
  - Open-source projects enable someone to choose any of the mirrors of open-source projects in hundreds of mirroring sites opening up a broad surface of attack
  - Try to see if the file has been modified
- Monitor system files to check for any unusual changes which could imply injection of a backdoor
- Check source code to identify presence of any backdoors

Protection Against Backdoors

- Checking compiled objects for backdoors is more difficult since the code is not human readable
  - Use a reverse engineering tool – e.g., Ollydbg
- OllyDbg is a debugger that analyses binary code, which is useful when human readable source code is not available
  - It traces registers, recognizes procedures, API calls, switches, tables, constants and strings, as well as locates routines from object files and libraries
- Run an executable file through Ollydbg
  - The assembly code will be visible together with the state/value of the program at different stages - use it to identify any malicious behavior
- This approach is also used to crack software

CPU - main thread, module RTRACE

Address	Hex dump	Disassembly	Profile
00401180	. 55	PUSH EBP	1.
00401181	. 8BEC	MOV EBP,ESP	1.
00401183	. 53	PUSH EBX	1.
00401184	. BB 68C44000	MOV EBX,RTRACE.0040C468	1.
00401189	. 33C0	XOR EAX,EAX	1.
0040118B	. 8903	MOV [DWORD DS:EBX],EAX	1.
0040118D	.v EB 24	JMP SHORT RTRACE.004011B3	1.
0040118F	> 33C0	XOR EAX,EAX	1.
00401191	> 40	INC EAX	28518.
00401192	. 3D 40420F00	CMP EAX,F4240	28518.
00401197	.^ 7C F8	JL SHORT RTRACE.00401191	28518.
00401199	. 8B03	MOV EAX,[DWORD DS:EBX]	
0040119B	. B9 21000000	MOV ECX,21	
004011A0	. 99	CDQ	
004011A1	. F7F9	IDIV ECX	
004011A3	. 83F8 03	CMP EAX,3	
004011A6	.v 7F 09	JG SHORT RTRACE.004011B1	
004011A8	. 8B0485 28A140	MOV EAX,[DWORD DS:EAX*4+40A128]	
004011AF	. FFD0	CALL EAX	
004011B1	> FF03	INC [DWORD DS:EBX]	
004011B3	> 833B 64	CMP [DWORD DS:EBX],64	1.
004011B6	.^ 7C D7	JL SHORT RTRACE.0040118F	1.
004011B8	. 68 3AA14000	PUSH RTRACE.0040A13A	
004011BD	. E8 0A270000	CALL RTRACE.004038CC	
004011C2	. 59	POP ECX	
004011C3	. 5B	POP EBX	
004011C4	. 5D	POP EBP	
004011C5	. C3	RETN	

EAX=00006F66

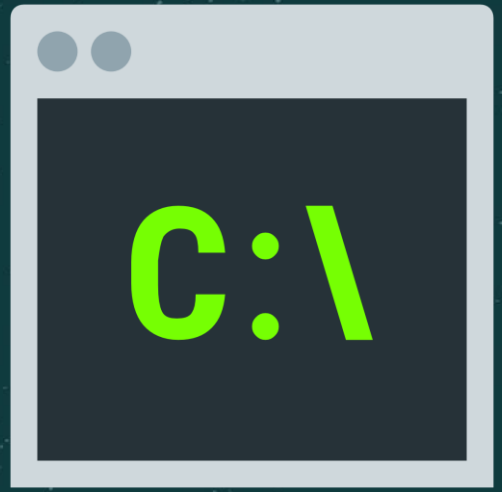
Registers (FPU)

```
EAX 00006F66
ECX 006621CC
EDX 006623AC
EBX 0040C468 RTRACE.0040C468
ESP 0064FE00
EBP 0064FE04
ESI 0040A0B8 RTRACE.0040A0B8
EDI 00000000

EIP 00401191 RTRACE.00401191

C 1  ES 013F 32bit 0(FFFF)
P 0  CS 0137 32bit 0(FFFFFFFF)
A 0  SS 013F 32bit 0(FFFF)
Z 0  DS 013F 32bit 0(FFFF)
S 1  FS 139F 16bit 81D374CC(33)
T 0  GS 0000 NULL
D 0
O 0

EFL 00200283 (NO,B,NE,BE,S,PO,L,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty -14519.000000000000000
ST5 empty 0.0
ST6 empty -61036.333333333335760
ST7 empty 0.0
               3 2 1 0      E S P U
FST 0000  Cond 0 0 0 0  Err 0 0 0 0
FCW 1372  Prec NEAR,64  Mask    1 1
```

Address	Hex dump	ASCII
0040A110	00 00 00 00 00 00 00 00 00 40 00 90 00 00 00 00	.....@.É....
0040A120	00 00 00 00 00 00 00 00 50 11 40 00 60 11 40 00	.....P◄@.'◄@.
0040A130	70 11 40 00 61 00 62 00 63 00 0A 00 00 00 40 00	p◄@.a.b.c.....@.

0064FE00	00540000	
0064FE04	0064FE30	
0064FE08	00407CEA	RETURN to RTR
0064FE0C	00000001	

Rootkit



- A rootkit is a set of programs installed on a system to maintain covert access to that system with administrator (or root) privileges, while hiding evidence of its presence to the greatest extent possible
- This provides access to all the functions and services of the operating system

Rootkit

- A rootkit takes active measures to obscure its presence within the host system
  - Rootkits achieve this by modifying the behavior of core parts of an operating system through loading code into other processes, the installation or modification of drivers, or kernel modules
  - Rootkits may modify System Call Table entries to redirect a system call from the legitimate code to the rootkits code
    - A system call is a way for programs to interact with the operating system
  - Obfuscation techniques include concealing running processes from system-monitoring mechanisms and hiding system files and other configuration data
  - Rootkit may disable the event logging capacity of an operating system, in an attempt to hide evidence of an attack

Rootkit

- Rootkits also take a number of measures to ensure their survival against detection and "cleaning" by antivirus software
- These include
  - Polymorphism (changing so their "signature" is hard to detect)
  - Regeneration
  - Disabling anti-malware software
  - Not installing them where it may be easier for researchers to discover and analyze them