A Hacker's Registry

Martin Kozeny
CSCI 4623: Digital Forensics
Spring 2011 University of New Orleans

February 7, 2011

1 Recovery

Using AccessData's registry viewer, me and my colleague managed to get this information from a laptop belonging to the thief.

- Time zone information

Table 1: Time zone information

Last Written Time	4/2/2006 15:56:45 UTC
Standard Start Date	Last Sun in Oct at 2:00:00 AM Local
Daylight Start Date	First Sun in Apr at 2:00:00 AM Local
Standard Bias	0
Daylight Bias	-60
StandardName (REG_SZ)	Eastern Standard Time

- Computer name

Table 2: Computer name

Last Written Time	8/7/2004 17:51:36 UTC
ComputerName (REG_SZ)	YOUR-4105E587B6

- Networking information

Table 3: Networking information

Name	Type	Data
UseZeroBroadcast	REG_DWORD	0x00000000 (0)
EnableDHCP	REG_DWORD	0x00000001 (1)
IPAddress	REG_MULTI_SZ	0.0.0.0
SubnetMask	REG_MULTI_SZ	0.0.0.0
DefaultGateway	REG_MULTI_SZ	
DefaultGatewayMetric	REG_MULTI_SZ	
NameServer	REG_SZ	(value not set)
Domain	REG_SZ	(value not set)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
TCPAllowedPorts	REG_MULTI_SZ	
UDPAllowedPorts	REG_MULTI_SZ	
RawIPAllowedProtocols	REG_MULTI_SZ	
AddressType	REG_DWORD 0x00000000 (0)	
DisableDynamicUpdate	REG_DWORD	0x00000000 (0)

- Hardware configuration

Table 4: Hardware configuration

Name	Type	Data
Capabilities	REG_DWORD	0x00000030 (48)
HardwareID	REG_MULTI_SZ	ACPI/AuthenticAMD_...
		*AuthenticAMD_-_x86_Family_15_Model_15
		ACPI/AuthenticAMD_-_x86_Family_15
		*AuthenticAMD_-_x86_Family_15
		ACPI/AuthenticAMD_-_x86
		*AuthenticAMD_-_x86
CompatibleIDs	REG_MULTI_SZ	ACPI/Processor
ClassGUID	REG_SZ	{50127DC3-0F36-415E-A6CC-4CB...
Class	REG_SZ	Processor
Driver	REG_SZ	{50127DC3-0F36-415E-A6CC-4CB3...
Mfg	REG_SZ	Advanced Micro Devices
Service	REG_SZ	AmdK8
DeviceDesc	REG_SZ	AMD Athlon 64 Processor
ConfigFlags	REG_DWORD	0x00000000 (0)
FriendlyName	REG_SZ	AMD Athlon(tm) 64 Processor 3200+

- USB thumb drives, printers and other peripherials

Table 5: USB thumb drives, printers and other peripherials

Name	Type	Data
DeviceDesc	REG_SZ	CD-ROM Drive
LocationInformation	REG_SZ	0
Capabilities	REG_DWORD	0x00000010 (16)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	IDE/CdRomTSSTcorp_CD/DVDW_TS-L532R
DeviceDesc	REG_SZ	Disk drive
LocationInformation	REG_SZ	0
Capabilities	REG_DWORD	0x00000000 (0)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	IDE/DiskFUJITSU_MHU2100AT
DeviceDesc	REG_SZ	Disk drive
LocationInformation	REG_SZ	0
Capabilities	REG_DWORD	0x00000000 (0)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	IDE/DiskST9808210A

- Software Installed on the laptop: it was e.g. Mozilla Firefox, Internet Explorer, Adobe Acrobat Reader, some apple plugins etc.

Table 6: Mozilla Firefox output registry - but this is registry for IE

Name	Type	Data
SOFTWARE/Classes/MIME/Database/Content Type/...	REG_SZ	.xpi
SOFTWARE/Classes/.htm	REG_SZ	htmlfile
SOFTWARE/Classes/.html	REG_SZ	htmlfile
SOFTWARE/Classes/HTTP/shell/open/command	REG_SZ	"C:/.../iexplore.exe" -nohome
SOFTWARE/Clients/StartMenuInternet/	REG_SZ	IEXPLORE.EXE

- Screeen names and usernames: Administrator, ASPNET, Guest, HelpAssistant, kkkkkkkk
- Recently typed URLs

Table 7: Recently typed URLs

Name	Type	Data
url1	REG_SZ	http://www.redlobster.com/
url2	REG_SZ	**www.mbna.com**
url3	REG_SZ	www.ebgames.com
url4	REG_SZ	http://www.hotmail.com/
url5	REG_SZ	www.wayport.com
url6	REG_SZ	www.aol.com
url7	REG_SZ	www.wamu.com
url8	REG_SZ	www.hotmail.com
url9	REG_SZ	http://www.ebgames.com/
url10	REG_SZ	http://www.gamefaqs.com/
url11	REG_SZ	http://www.aol.com/
url12	REG_SZ	www.aol.co
url13	REG_SZ	**www.hushmail.com**
url14	REG_SZ	www.way.com

- Recently accessed documents

Table 8: Recently accessed documents

Name	Type	Data
File1	REG_SZ	C:/WINDOWS/system32/services.msc
File2	REG_SZ	C:/WINDOWS/system32/devmgmt.msc

2 Conclusion

It seems that only the relevant banking information are these two URLs: www.mbna.com and maybe www.hushmail.com. First one is the URl of Bank of America and second one is URL is secure web-based mail service and when you need to secure email at your domain here, you have to type your credit card number.