Digital Forensics Investigation of a Missing Laptop

Ashish Ahire, Ismail Bibers, Pradeep Mugithe

Introduction

Abandoned laptop found with a wireless PCMCIA card and homemade antennae

Suspected to have been used for hacking by suspect "Mr. Evil" (real name Greg Schardt)

The goal of investigation: find hacking software, evidence of use, and tie the computer to the suspect

Overview/Case

An abandoned laptop was found with a wireless PCMCIA card and homemade antenna

Suspected use of devices for hacking and stealing sensitive information

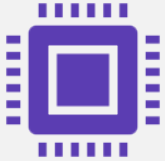
Industry-standard digital forensics techniques used to analyze evidence

Identification of several hacking tools and programs providing crucial insights into the nature of the incident and methods used by the hacker.

Objective

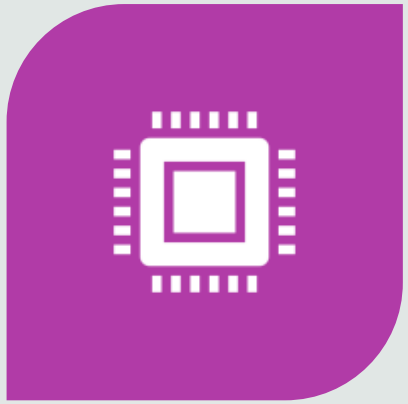
Find evidence of hacking software and data generated by the attacker.

Investigate ties between the laptop and suspect Greg Schardt.



Determine if the attacker targeted specific systems or data within the organization's infrastructure.

Evidence

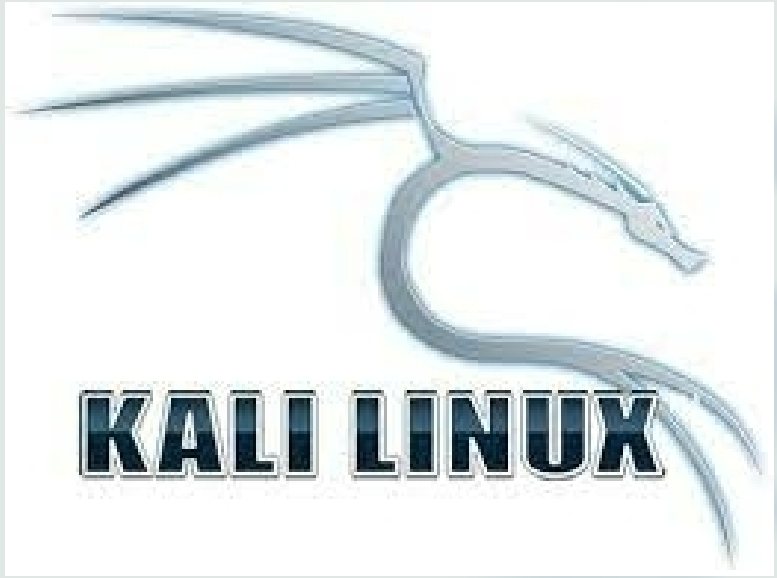


LAPTOP, WIRELESS PCMCIA CARD, EXTERNAL HOMEMADE 802.11B ANTENNAE, ALLEGEDLY INTERCEPTING TRAFFIC.

DIGITAL EVIDENCE IS COLLECTED SUCH AS LOGS, DEVICE DETAILS, AND NETWORK TRAFFIC.

USING VARIOUS TOOLS, WE ANALYZED THE COLLECTED EVIDENCE

Kali Linux & Autopsy



- Kali Linux and Autopsy were used to acquire and analyze the collected evidence.
- Using Autopsy, we conducted a digital investigation on image.

AUTOPSY
DIGITAL FORENSICS

Analysis

Acquisition of Evidence: Hard drive image collected in .IMG format using Kali Linux forensics mode. And the acquisition hash value was noted for comparing later.

The acquired evidence image was securely transferred to windows machine where it was analyzed using Autopsy.

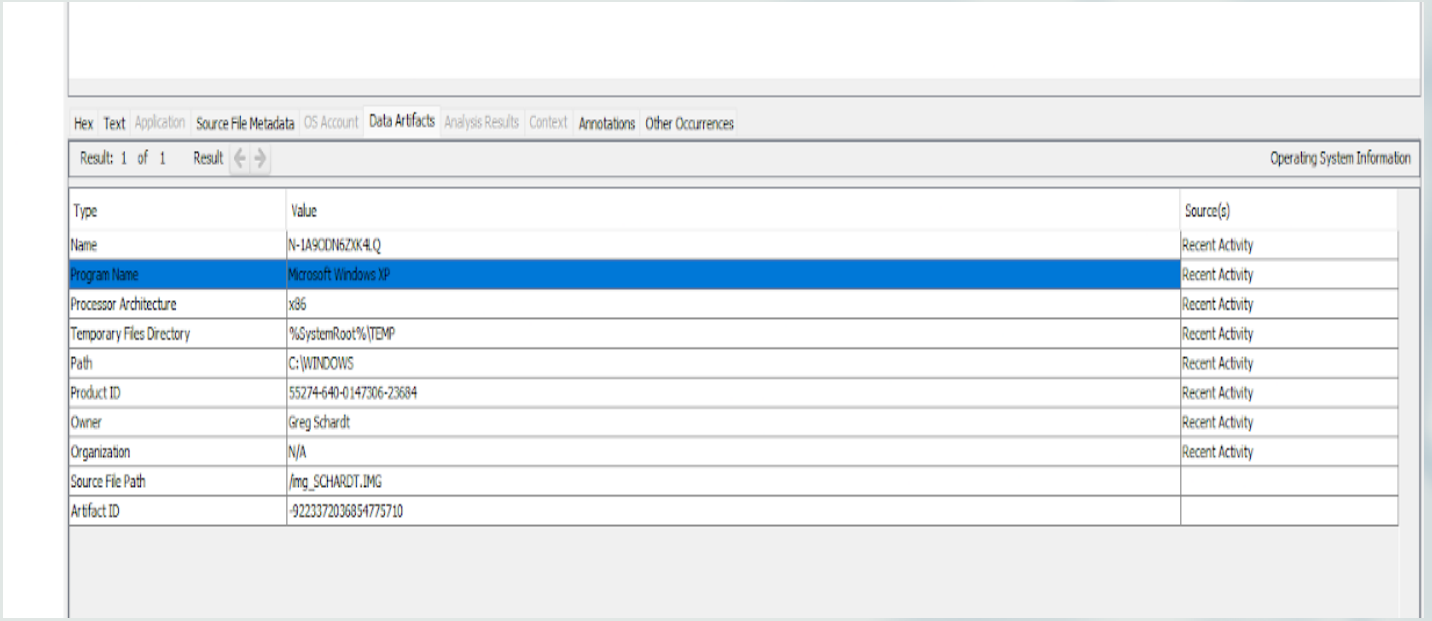
The hash value generated by Autopsy was compared with the acquisition hash value to check the image integrity.

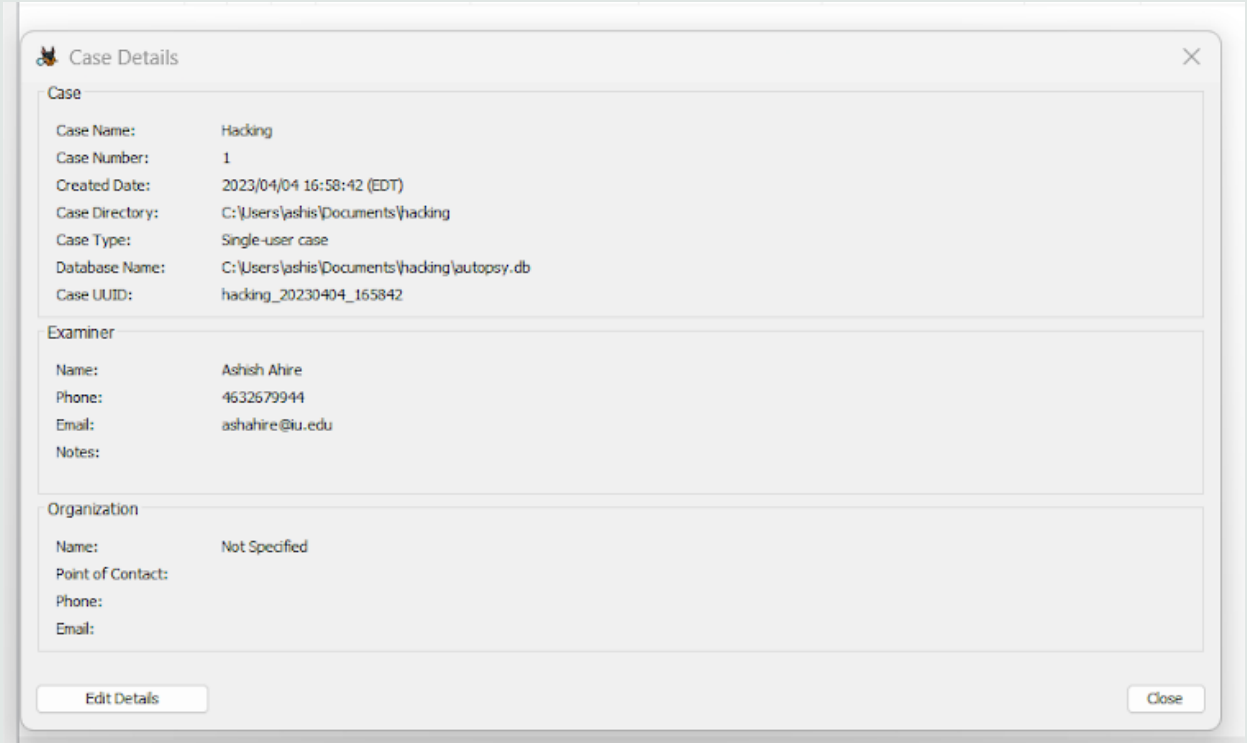
Using Autopsy's timeline, the date and time of the events that happened using the laptop were known. This helped in determining when hacking activities were started.

Some manuals and password dictionaries were found on the laptop which might have been used by hacker.

Laptop's registered owner name and username were found which are important in this case.

Analysis Cont.





Analysis Cont.

Many images were found on the laptop. This images might contain hidden information which can be retrieved using steganography technique.

Some hacking tools were found installed on the laptop which hacker used to carry out hacking activities.

Email addresses used by the hacker were found on the system which were used for communication.

Information about the network cards used with the laptop were found including the IP address and MAC address.

The time when the OS was installed and the time when the system was last shutdown was found.

A malicious file was found on the laptop which hacker may have used to corrupt the connected systems for hacking.

Findings

- MD5 hash value: aee4fcd9301c03b3b054623ca261959a
- Registered Owner: Greg Schardt
- OS Installation Date and Time: Thursday, August 19, 2004, at 4:48:27 PM GMT -06:00 (CST)
- Username: Mr. Evil
- System Shutdown Time: Friday, 27 August 2004, 09:46:33 AM GMT -06:00 (CST)
- Last user to logon: Mr. Evil

Number of values: 17
Modification Time: 2004-08-27 15:08:22 GMT+00:00

Values

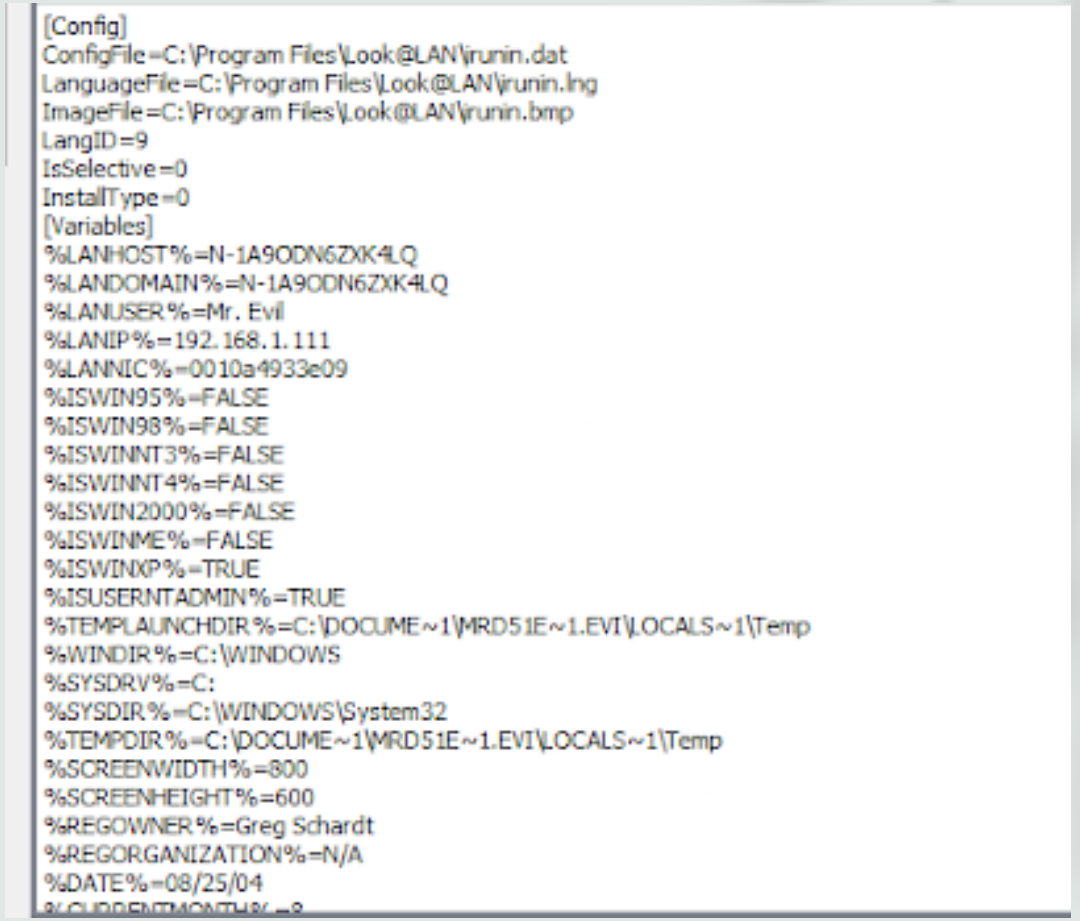
Name	Type	Value
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
InstallDate	REG_DWORD	0x41252e3b (1092955707)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganization	REG_SZ	N/A
RegisteredOwner	REG_SZ	Greg Schardt
SoftwareType	REG_SZ	SYSTEM
CurrentVersion	REG_SZ	5.1
CurrentBuildNumber	REG_SZ	2600
BuildLab	REG_SZ	2600.xpclient.010817-1148
CurrentType	REG_SZ	Uniprocessor Free
SystemRoot	REG_SZ	C:\WINDOWS
SourcePath	REG_SZ	D:\
PathName	REG_SZ	C:\WINDOWS
ProductId	REG_SZ	55274-640-0147306-23684
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 35 35 32 37 34 2D 36 34...
LicenseInfo	REG_BIN	34 54 AE DC C7 2E 3D E5 8B 15 06 1A 8C 74 A6 55...

Values

Name	Type	Value
AutoRestartShell	REG_DWORD	0x00000001 (1)
DefaultDomainName	REG_SZ	N-1A9ODN6ZXK4LQ
DefaultUserName	REG_SZ	Mr. Evil
LegalNoticeCaption	REG_SZ	(value not set)
LegalNoticeText	REG_SZ	(value not set)
PowerdownAfterShutdown	REG_SZ	0
ReportBootOk	REG_SZ	1
Shell	REG_SZ	Explorer.exe
ShutdownWithoutLogon	REG_SZ	0
System	REG_SZ	(value not set)
Userinit	REG_SZ	C:\WINDOWS\system32\userinit.exe,
VmApplet	REG_SZ	rundll32 shell32,Control_RunDLL "sysdm.cpl"
SfcQuota	REG_DWORD	0xffffffff (4294967295)
allocatecdroms	REG_SZ	0
allocatedasd	REG_SZ	0
allocatefloppies	REG_SZ	0
cachedlogonscount	REG_SZ	10
forceunlocklogon	REG_DWORD	0x00000000 (0)
passwordexpirywarning	REG_DWORD	0x0000000e (14)
scremoveoption	REG_SZ	0
AllowMultipleTSSessions	REG_DWORD	0x00000001 (1)

Findings Cont.

- Five OS accounts found: Mr. Evil, Administrator, Guest, HelpAssistant, Support_388945a0
- Keyword Search “Greg Schardt” : 11 files found of which 1 file reveals relation between Greg and Mr. Evil.
- Network Cards: 2 network cards found
- IP address: 192.168.1.111
- MAC address: 00:10:A4:93:3E:09
- Hacking tools: Cain, 123WASP, Anonymizer, Ethereal, Look@LAN, Network Stumbler
- Email address: mrevilrulez@yahoo.com
- Malicious file: Zip bomb file unix_hack.tgz found



Name	Type	Value
ServiceName	REG_SZ	{86FC0C96-3FF2-4D59-9ABA-C602F213B5D2}
Description	REG_SZ	Compaq WL110 Wireless LAN PC Card

Values

Name	Type	Value
ServiceName	REG_SZ	{6E4090C2-FAEF-489A-8575-505D21FC1049}
Description	REG_SZ	Xircom CardBus Ethernet 100 + Modem 56 (Ether…

Conclusion

We were able to find and identify crucial digital data that provided insights into the possible hacking use of the computer by a suspect “Greg Schardt”.

On the suspect’s laptop we discovered the evidence of several hacking tools and programs, which includes password cracking tools, network sniffers, network scanners, and proxy tools for making any internet activity untraceable.

Although, based upon the evidence and the findings we found, we were unable to definitively link the found laptop to the suspect “Greg Schardt”. However, from the found evidence and insights, it clearly observed that the suspect also known as “Mr Evil” was involved in the hacking incident.

All in all, our investigation showed that the suspect “Greg Schardt” and “Mr.Evil” are just one single person and all the suspicions about the “Greg Schardt” were true.

References

- https://cfreds.nist.gov/all/NIST/HackingCase
- https://www.autopsy.com/
- https://www.kali.org/docs/
- https://en.wikipedia.org/wiki/Cain_and_Abel_(software)
- https://hackersonlineclub.com/what-is-ethereal-hacking/
- https://en.wikipedia.org/wiki/NetStumbler
- https://pendriveapps.com/looklan-portable-network-monitor/
- https://www.majorgeeks.com/files/details/123_write_all_stored_passwords.html
- https://en.wikipedia.org/wiki/Anonymizer_(company)


Questions

Thank You