**Forensics Report and Documentation**

James Kuzhilaparambil, Usman Haque

Lighthouse Labs

Project 10

Contents

[Executive Summary 3](#_heading=h.gjdgxs)

[# 1. Introduction 3](#_heading=h.30j0zll)

[# 2. Background 3](#_heading=h.1fob9te)

[# 3. Investigation Findings 3](#_heading=h.3znysh7)

[Conclusion 17](#_heading=h.2et92p0)

[References: 18](#_heading=h.tyjcwt)

### Executive Summary

This report provides a comprehensive assessment of the security incident involving the theft of the Szechuan Sauce recipe. It identifies vulnerabilities and gaps in the current setup and offers detailed analysis to enhance the security posture. The goal is to protect sensitive data, ensure compliance and support integrity of the network, thereby strengthening organizational defenses against future threats and safeguard its assets.

### # 1. Introduction

This report details the findings from the investigation of the case "The Stolen Szechuan Sauce." The purpose of this project is to analyze various digital artifacts from a simulated security breach, identify potential threats, and document our investigative process.

### # 2. Background

In this case, we are tasked with determining if a breach occurred, the methods used by the attacker, and the potential impact on the organization. By examining provided digital artifacts, we aim to answer a series of questions that help reconstruct the incident.

### # 3. Investigation Findings

##### A. Operating Systems

\*\*Question\*\*: What’s the Operating System of the Server?

\*\*Question\*\*: What’s the Operating System of the Desktop?

\*\*Findings\*\*: The desktop is identified as Windows 10 Enterprise, indicated by version number 10.0.22621.4249. This information was obtained using the Registry Explorer tool, which allows us to view system configurations.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The highlighted entries confirm the operating system as **Windows 10 Enterprise** with a **ReleaseId** of 2009

A screenshot of a computer

Description automatically generated

##### B. Local Time of the Server

\*\*Question\*\*: What was the local time of the Server?

\*\*Findings\*\*: The local time was extracted from system logs, which indicated a timezone setting reflecting the server’s location.

##### C. Breach Analysis

\*\*Question\*\*: Was there a breach?

\*\*Findings\*\*: To evaluate this, I examined security event logs using Event Viewer. Key events included:

\*\*Event ID 4624\*\*: Successful logins indicate authorized access.

\*\*Event ID 4625\*\*: Multiple failed login attempts, which can suggest unauthorized access attempts or errors. For example, if a user forgets their password, that counts as a failed attempt. However, many failed attempts in a short time frame may indicate malicious intent, such as a brute force attack—where an attacker tries many passwords quickly to gain access.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The screenshot shows the **Event Viewer** application displaying the “Security” logs. The selected event details include Event IDs 4624, 4625, and 4719, which are crucial for identifying patterns of suspicious activity.

A screenshot of a computer

Description automatically generated

##### D. Initial Entry Vector

\*\*Question\*\*: What was the initial entry vector (how did they get in)?

\*\*Findings\*\*: Analysis of network traffic revealed multiple TCP Reset (RST) packets, suggesting potential malicious activity or disruptions in network connections. This could indicate attempts to launch a Denial of Service (DoS) attack.

A screenshot of a computer

Description automatically generated

The screenshot shows a network traffic analysis application Wireshark, with several TCP RST packets highlighted in red. This visual evidence supports the analysis of potential malicious activity disrupting network connections.

##### E. Malware Analysis

\*\*Question\*\*: Was malware used? If so, what was it?

\*\*Findings\*\*:

\*\*Malicious Process\*\*: The process \*\*coreupdater.exe\*\* was identified as suspicious.

\*\*Payload Delivery\*\*: IP Address 194.61.24.102 was involved in delivering the malware to the server.

\*\*Capabilities\*\*: This malware could steal credentials, log keystrokes, and capture screens.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

##### F. Malicious IP Addresses

\*\*Question\*\*: What malicious IP Addresses were involved?

\*\*Findings\*\*: The IP Address \*\*194.61.24.102\*\* was linked to known brute force attacks, confirmed through threat intelligence databases.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

##### G. Access to Other Systems

\*\*Question\*\*: Did the attacker access any other systems? How? When?

\*\*Findings\*\*: The attacker exploited a compromised administrator account to access additional systems, as indicated by log analysis and network traffic examination.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

##### H. Data Theft

\*\*Question\*\*: Did the attacker steal or access any data? When?

\*\*Findings\*\*: Yes, sensitive data was accessed and exfiltrated from both the server and the desktop, evidenced by log entries and network traffic data.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

##### I. Network Layout

\*\*Question\*\*: What was the network layout of the victim network?

\*\*Findings\*\*: The network consisted of a Domain Controller (DC) and user machines, both identified within the same subnet. Network traffic analysis showed interactions between these hosts.

A screenshot of a computer

Description automatically generated

LLMNR queries from the DC to the multicast address 224.0.0.252.

A screenshot of a computer

Description automatically generated

Successful logon events involving the DC and user machine IP addresses

A screenshot of a computer

Description automatically generated

Details of Event ID 4624 indicating a successful account logon

### Conclusion

The investigation uncovered evidence of unauthorized access, malware presence, and potential data theft. The findings highlight vulnerabilities within the network that could be addressed to enhance security.

### References:

James. (2021, March 25). *Case 001 – The stolen Szechuan Sauce*. DFIR Madness. https://dfirmadness.com/the-stolen-szechuan-sauce/

*Case 001 - Szechuan Sauce | Digital Forensics & Incident Response*. (n.d.). https://www.iblue.team/ctf-challenges/dfir-madness-ctf-challenges/case-001-szechuan-sauce

*Walkthrough of DFIR Madness PCAP*. (2021, July 9). [Video]. Netresec. https://www.netresec.com/?page=Blog&month=2021-07&post=Walkthrough-of-DFIR-Madness-PCAP

*MDwiki*. (n.d.). https://ericzimmerman.github.io/#!index.md

Chris. (2021, May 20). *The Case of the Missing Szechuan Sauce: investigation notes*. DEV Community. https://dev.to/evilcel3ri/the-case-of-the-missing-szechuan-sauce-investigation-notes-1di7

*VirusTotal*. (n.d.). VirusTotal. https://www.virustotal.com/gui/home/upload

The Volatility Foundation. (2024, March 11). *Volatility Training | The Volatility Foundation | Open Source Memory Forensics Framework - The Volatility Foundation - Promoting accessible memory analysis tools within the Memory Forensics community*. The Volatility Foundation - Promoting Accessible Memory Analysis Tools Within the Memory Forensics Community. https://volatilityfoundation.org/volatility-training/

*FTK Imager - Forensic Data Imaging and Preview Solution | Exterro*. (2024, April 4). Exterro. https://www.exterro.com/digital-forensics-software/ftk-imager

*Wireshark • Learn*. (n.d.). Wireshark. https://www.wireshark.org/learn

Markdefalco. (n.d.). *Event viewer*. Microsoft Learn. https://learn.microsoft.com/en-us/shows/inside/event-viewer

James. (2021a, February 1). *Case 001 PCAP Analysis*. DFIR Madness. https://dfirmadness.com/case-001-pcap-analysis/

Ananin, V., & Ananin, V. (2024, October 4). *Malware analysis in ANY.RUN: The Ultimate Guide*. ANY.RUN’s Cybersecurity Blog. https://any.run/cybersecurity-blog/malware-analysis-in-a-sandbox/