

Case of the stolen szechuan sauce!!



October 5, 2024

lighthouse labs

By: Curtis Crawford

Contents

[Investigation Questions and Findings 2](#_Toc179093901)

[1. What is the Operating System of the Server? 2](#_Toc179093902)

[2. What is the Operating System of the Desktop? 2](#_Toc179093903)

[3. What is the local time of the Server? 3](#_Toc179093904)

[The Server is using **Pacific Standard Time (PST)**. 3](#_Toc179093905)

[4. **Was there a breach?** 3](#_Toc179093906)

[5. What was the initial entry vector (how did they get in)? 4](#_Toc179093907)

[6. Was malware used? If so, what was it? 4](#_Toc179093908)

[7. Is this malware easily obtained? 7](#_Toc179093909)

[8. Was this malware installed with persistence on any machine? 7](#_Toc179093910)

[9. What malicious IP addresses were involved? 7](#_Toc179093911)

[10. Were any IP addresses from known adversary infrastructure? 7](#_Toc179093912)

[12. Were these IPs involved in other attacks around the time of the incident? 9](#_Toc179093913)

[13. Did the attacker access any other systems? How? 9](#_Toc179093914)

[14. Did the attacker steal or access any data? 10](#_Toc179093915)

[15. What was the network layout of the victim network? 10](#_Toc179093916)

[16. What architecture changes should be made immediately? 10](#_Toc179093917)

[17. Did the attacker steal the Szechuan sauce? If so, what time? 10](#_Toc179093918)

[18. Did the attacker steal or access any other sensitive files? If so, what times? 11](#_Toc179093919)

[References 13](#_Toc179093920)

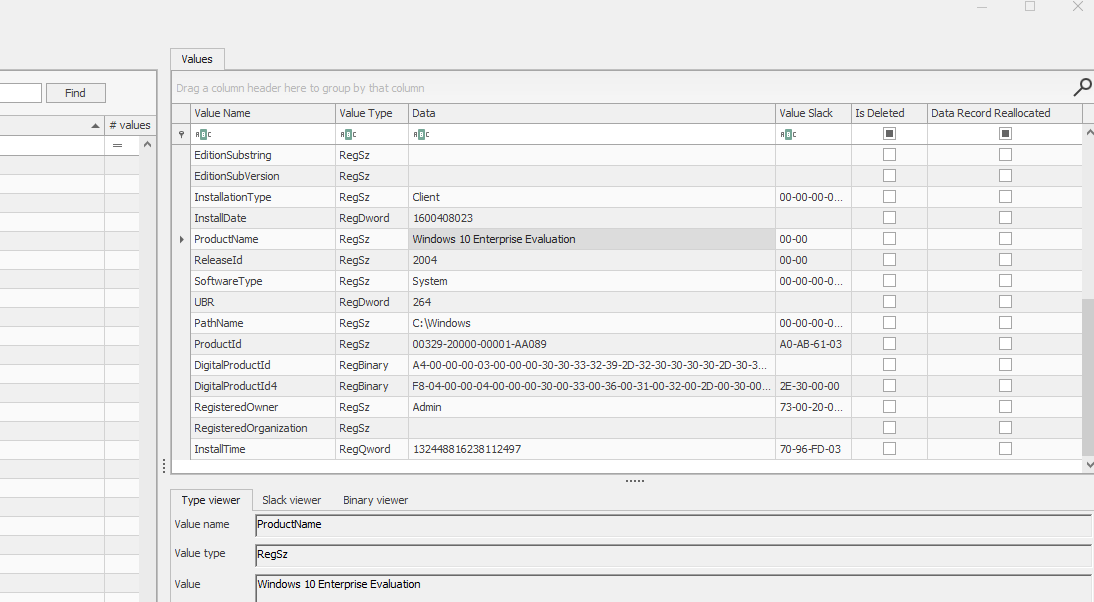
# Investigation Questions and Findings

## What is the Operating System of the Server?

* + A screenshot of a computer

    Description automatically generatedThe Operating System of the Server is **Windows Server 2012 R2 Standard Evaluation**.

## What is the Operating System of the Desktop?

* The Operating System of the Desktop is **Windows 10 Enterprise Evaluation**.

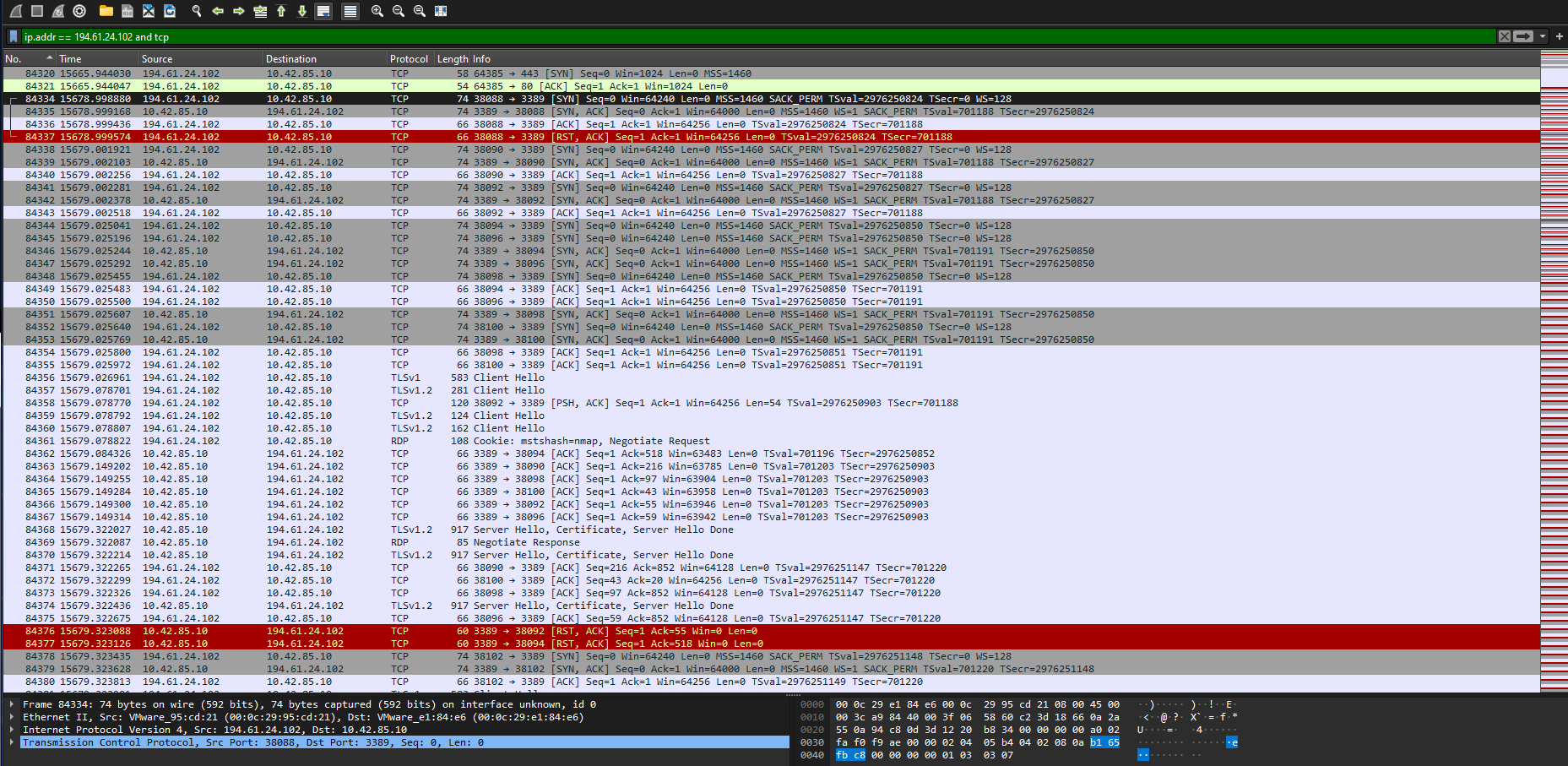
## What is the local time of the Server?

## The Server is using **Pacific Standard Time (PST)**.

## **Was there a breach?**

* + **Yes**, the following details outline the reasons for confirming this breach.

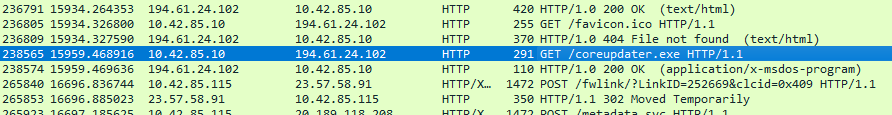
## What was the initial entry vector (how did they get in)?

* + The attacker used a **Brute Force Attack**, evident by multiple SYN requests targeting the same destination source.

## 6. Was malware used? If so, what was it?

**A) What process was malicious?**

* + A screenshot of a black screen

    Description automatically generatedThe malicious process was **coreupdater.exe**. The IP address 194.61.24.102 was identified as malicious. Filtering its activities in the pcap file led to a GET request for coreupdater.exe, which after being exported and tested, was flagged as a Trojan by Windows Defender.

**B) Identify the IP Address that delivered the payload.**

* + The payload was delivered from **194.61.24.102**.

**C) What IP Address is the malware calling to?**

* + Using Volatility's Netscan, the malware was calling **203.78.103.109:443**.

**D) Where is the malware located on disk?**

* + The malware was located at **C:\Windows\System32\coreupdater.exe**, as seen in the AutoRunsc-Citadel-DC01.csv file.

**E) When did the malware first appear?**

* + A screen shot of a black screen

    Description automatically generatedIt first appeared on **2020-09-19 at 03:56:37 UTC+0000**, as identified by the pslist command in Volatility.

**F) Was the malware moved?**

* + Yes, since it was found in \*\*C:\Windows\System32\*\*, it indicates that the file was moved from its usual download location.

1. **What were the capabilities of this malware?**
   * A screenshot of a computer

     Description automatically generatedThe malware is categorized as **Metasploit**, which is a tool used for penetration testing, patch testing, and security engineering. In malicious hands, it can inflict significant damage to a system.

## Is this malware easily obtained?

* + **Yes**, Metasploit can be downloaded from multiple sources online, including a simple Google search.

## Was this malware installed with persistence on any machine?

* + **Yes**, the malware is set to start automatically.  
    **When?** *2020-09-19 03:42:42*  
    **Where?** *C:\Windows\System32\coreupdater.exe*

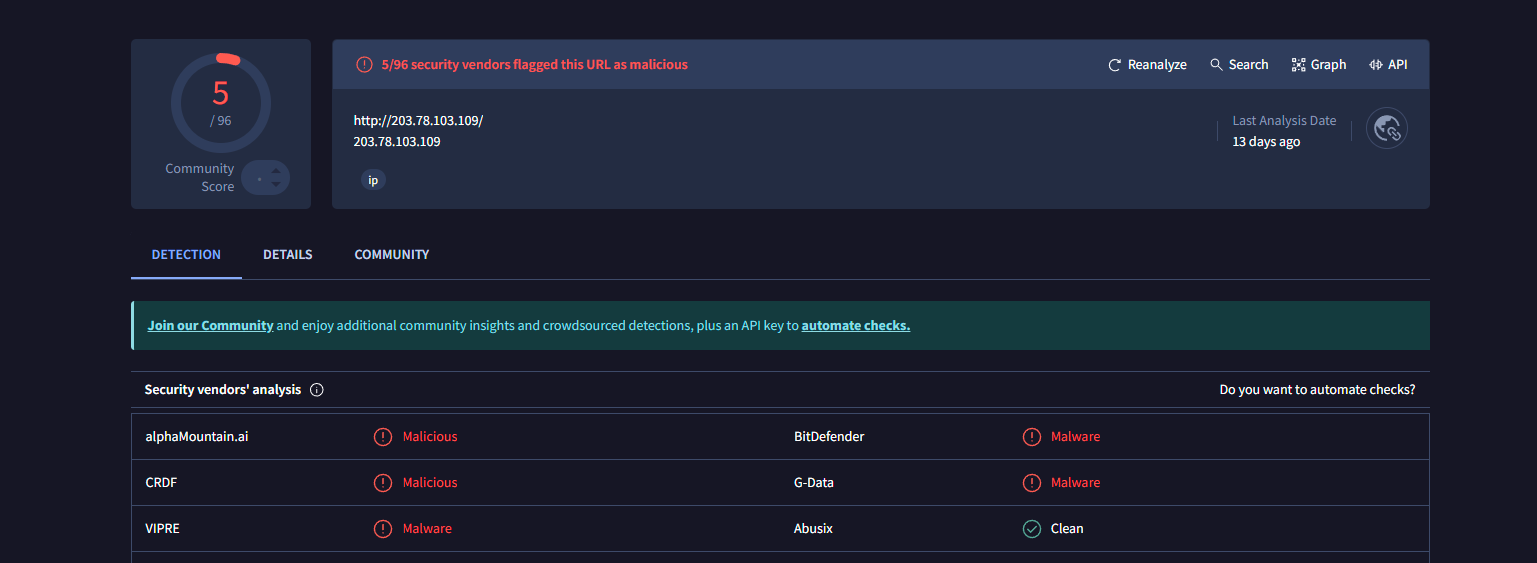
## What malicious IP addresses were involved?

* As shown in the previous answers and pictures, the malicious IP addresses were **194.61.24.102** (Russia) and **203.78.103.109** (Thailand).

10. Were any IP addresses from known adversary infrastructure?

* **Yes**, 194.61.24.102 (Russia) is flagged for RDP and spam attacks, while 203.78.103.109 (Thailand) has a few suspicious flags on VirusTotal as shown in the pictures on the next page.

**A screenshot of a computer

Description automatically generated  
**

## 12. Were these IPs involved in other attacks around the time of the incident?

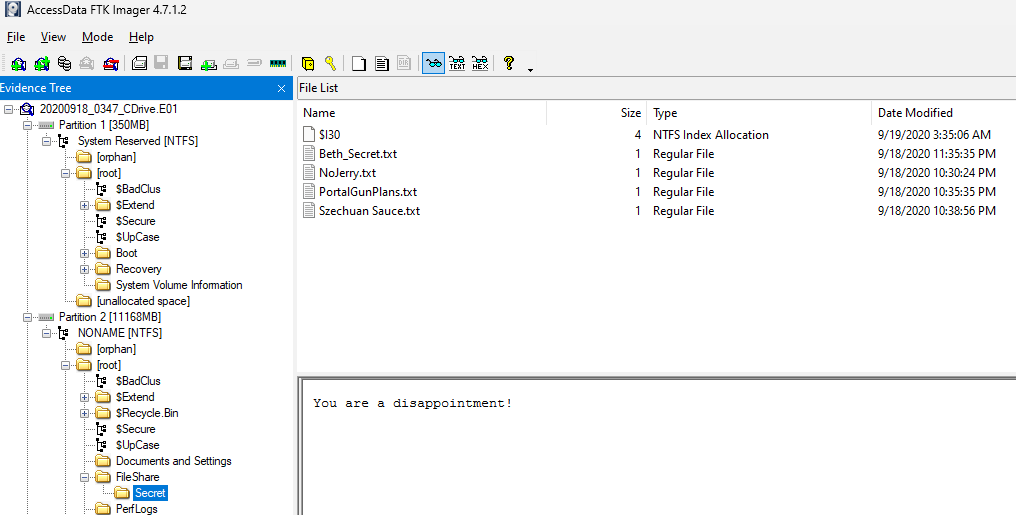
* **Yes**, as shown in previous answers, these IP addresses were linked to other attacks.

## 13. Did the attacker access any other systems? How?

* **A screenshot of a computer

  Description automatically generatedYes**, the attacker accessed the system **Desktop-SDN1RPT$** via an RDP connection, as shown in the case001.pcap file in Wireshark.  
  **When?** *2020-09-18 22:21:26*

## 14. Did the attacker steal or access any data?

* **Yes**, the files in the "Secret" folder were accessed. This was viewed in FTK Imager.  
  **When?** *2020-09-18*

## 15. What was the network layout of the victim network?

* The network consists of a Domain Controller and a Desktop:  
  *Citadel-DC01* >>> *Desktop-SDN1RPT*

## 16. What architecture changes should be made immediately?

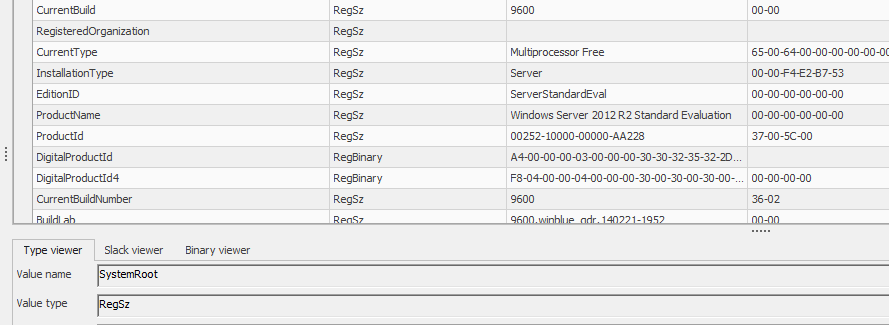
* **Limit RDP access** to the Domain Controller and restrict it to local network users only.

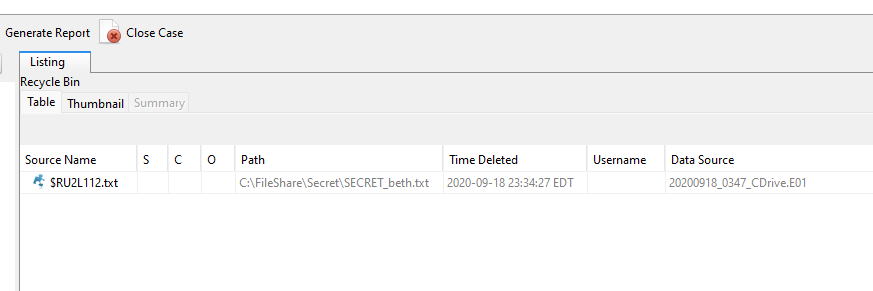
## 17. Did the attacker steal the Szechuan sauce? If so, what time?

* **Yes**, the Szechuan Sauce was stolen on **2020-09-18 at 18:35:59**, as shown in Autopsy.  
    
  *A screenshot of a computer

  Description automatically generated*

## 18. Did the attacker steal or access any other sensitive files? If so, what times?

* **Yes**, the **SECRET\_Beth** file was accessed on **2020-09-18 at 18:39:22** and deleted at **23:24:27** the same day. A new file, **Beth\_Secret**, was created less than a minute later at **23:25:07**.



**Summary of Key Findings**

The investigation which was led by Shannah Everitt and executed by Curtis Crawford has revealed a sophisticated breach involving a brute force attack, malware installation (coreupdater.exe), and RDP exploitation. The attacker accessed sensitive files and moved malware to a non-standard location. Shannah directed and discussed with Curtis on where to look and what to look for while Curtis oversaw controlling the VM and taking pictures as evidence.

# References

Comparitech. (2019, June). **Wireshark cheat sheet**. <https://cdn.comparitech.com/wp-content/uploads/2019/06/Wireshark-Cheat-Sheet.pdf>

CleanTalk. (n.d.). **Blacklist: 194.61.24.102**. CleanTalk. <https://cleantalk.org/blacklists/194.61.24.102>

CleanTalk. (n.d.). **Blacklist: 203.78.103.109**. CleanTalk. <https://cleantalk.org/blacklists/203.78.103.109?show_api=1#owner>

Criminal IP. (n.d.). **IP report: 194.61.24.102**. Criminal IP. <https://www.criminalip.io/asset/report/194.61.24.102>

Joe Sandbox. (n.d.). **Analysis report: 194.61.24.102**. Joe Sandbox. <https://www.joesandbox.com/analysis/1391302/0/html>

Tenable. (n.d.). **Plugin: 30**. Tenable Network Security. <https://www.tenable.com/plugins/nnm/30>

VirusTotal. (n.d.). **IP address report: 194.61.24.102**. VirusTotal. <https://www.virustotal.com/gui/ip-address/194.61.24.102>

Veterans Affairs Office of Information and Technology. (n.d.). **Registry Explorer manual**. <https://www.oit.va.gov/Services/TRM/files/RegistryExplorerManual.pdf>

Sleuth Kit. (n.d.). **Autopsy 4.0 user documentation**. <https://sleuthkit.org/autopsy/docs/user-docs/4.0/>