ARAIZ NAQVI

INCIDENT REPORT

Yummy Recipes INC.

07TH OCTOBER, 2024

2024-2025

ARAIZ NAQVI

TABLE OF CONTENT

2024-2025

ARAIZ NAQVI

DISCLAIMER

This incident report is a project-based simulation for the fictional organization *Yummy Recipes INC.*, as part of the "Fundamentals of Cybersecurity" course on Google’s Coursera platform.

While the details may resemble real-world scenarios, all data, systems, and findings are entirely fictitious and created for educational purposes. This incident report does not reflect any actual incidents or vulnerabilities affecting any real organization, including *Yummy Recipes INC.*.

Though based on practical analysis and protocols, the assessments are conducted in a simulated environment and should not be considered representative of any real entity's security posture.

2024-2025

ARAIZ NAQVI

INCIDENT SUMMARY

Time of Incident:	2024-10-07 14:18:32.192571 (07th October, 2024 2:18:32.192571pm)
Summary of Incident:	Clients at Jazz Recipes were subject to social engineering followed by a malicious download, wherein they were being redirected to malicious website greatrecipesforme.com when logging on yummyrecipes.com .
Location of Incident:	https://yummyrecipes.com (original) https://greatrecipesforme.com (malicious)
Reported By:	Araiz Naqvi
Reported On:	2024-10-07 14:25:29.576597 (07th October, 2024 2:25:29.576597pm)

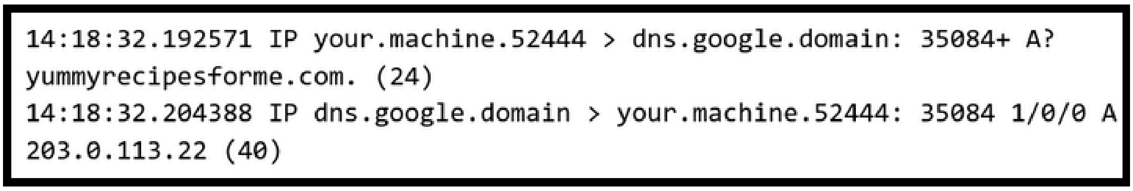
2024-2025

INCIDENT DETAILS

Type of Incident: Brute Force, Social Engineering, Cross Site Scripting, Malware

Description: When users attempted to log in to yummyrecipes.com, they were shown a prompt offering free recipe downloads. According to tcpdump log data, clicking this prompt triggered an HTTP GET request, which likely caused the malicious code to be downloaded to the user's device. Users were then redirected to greatrecipesforme.com. After this incident, many users reported that their computers began experiencing significant slowdowns.

DETAILED LOG BREAK DOWN

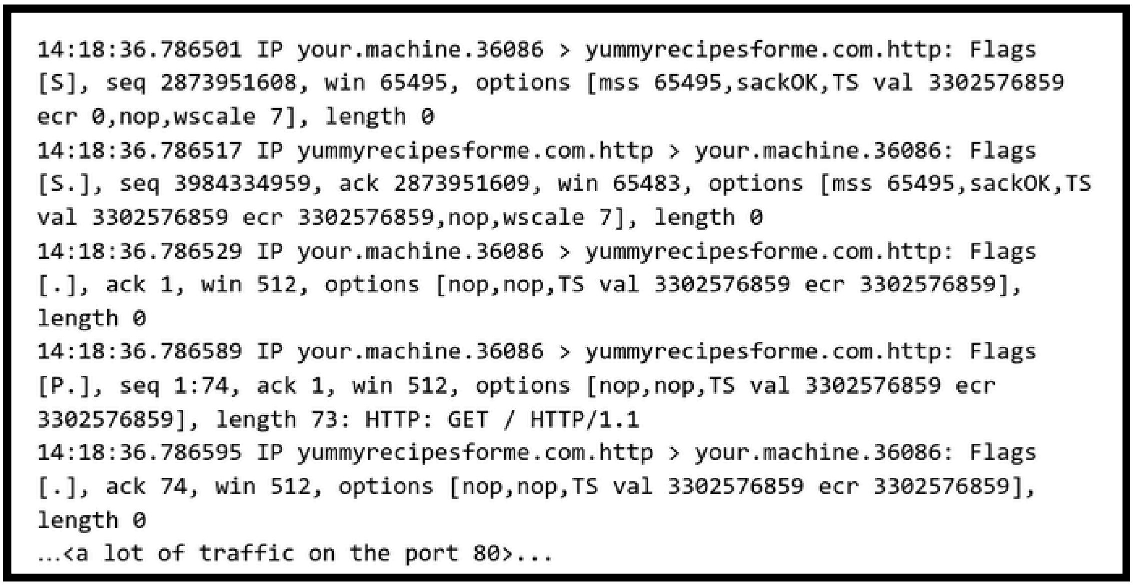


```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?
yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A
203.0.113.22 (40)
```

At 14:18:32.192571:

A DNS request was made from within a sandbox environment to DNS server from port 52444. The DNS server within milli-seconds responds to user with the IP Address of https://yummyrecipes.com i.e. 203.0.113.22 .

(PTO)

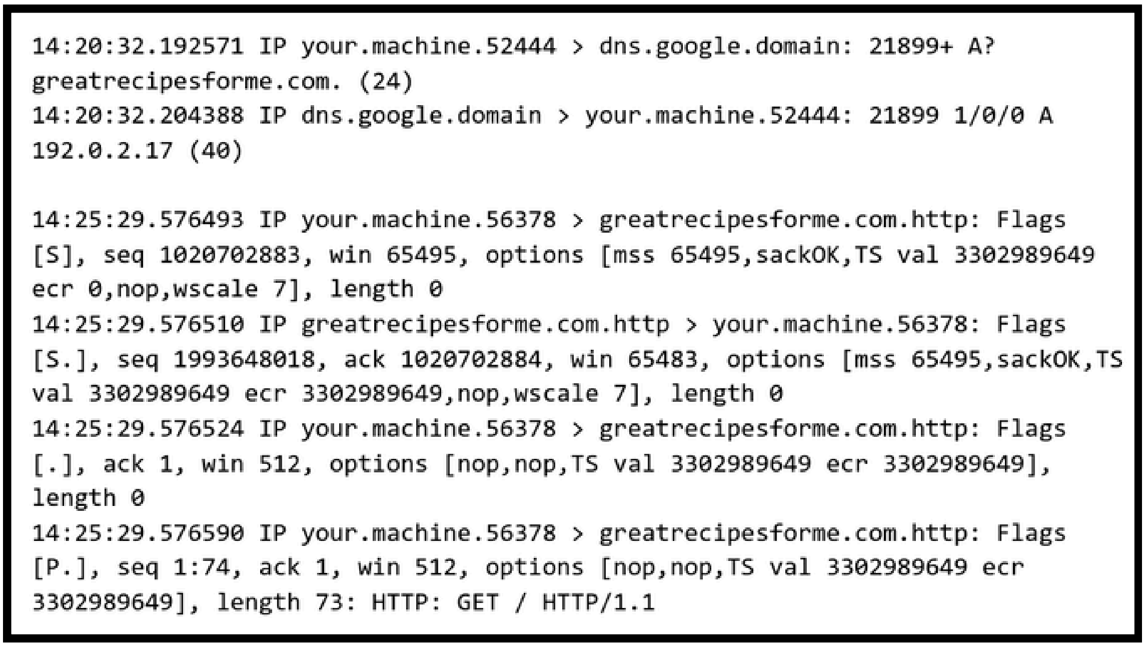


```
14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859
ecr 0,nop,wscale 7], length 0
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS
val 3302576859 ecr 3302576859,nop,wscale 7], length 0
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr
3302576859], length 73: HTTP: GET / HTTP/1.1
14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
...<a lot of traffic on the port 80>...
```

At 14:18:36.786501:

Here, a HTTP connection is initiated with yummyrecipes.com (denoted by [S]) by user which within milli-seconds was acknowledged immediately.
Shortly after at 14:18:36.786589, this is where the prompt for free recipes was clicked on which sent a HTTP 1.1 GET request from the user to the server which again was acknowledged by server at yummyrecipes.com . This is exactly where the malware was downloaded via means of Social Engineering.

(PTO)



```
14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?
greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A
192.0.2.17 (40)

14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649
ecr 0,nop,wscale 7], length 0
14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags
[S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS
val 3302989649 ecr 3302989649,nop,wscale 7], length 0
14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr
3302989649], length 73: HTTP: GET / HTTP/1.1
```

At 14:20:32.192571:

Within two minutes of back and forth, the user's port is automatically changed to 52444 and a request from DNS server for greatrecipesforme.com is made which is responded by with the IP 192.0.2.17 by DNS.

At 14:25:29.576493:

In the next 3 minutes, an automatic port change to 56378 is observed followed by HTTP request to get greatrecipesforme.com which is accepted.

(PTO)

ARAIZ NAQVI

IMPACT ASSESSMENT

Initial Response and Security:

- Shut down the server, blocking all incoming traffic to yummyrecipes.com or IP address 203.0.113.22 . Set firewall for any potential D/DOS attack.
- Since ex-employee baker used brute force to gain admin credentials, a strict and strong password policy is undertaken.
- The last version from GIT VCS is applied wherein the injected JS code is removed.
- Ports responsible were 80, 443 and 53 are under strict active firewall, IPS and IDS protection.

(PTO)

2024-2025

Scope of Impact:

The attack caused corrupted source code, a potential backdoor might be inserted, trusted user's are under severe danger as targeted devices might act as botnets.

Furthermore, huge loss in business during peak hours caused severe financial damage.

Also, severe reputation damage has been afflicted.

(PTO)

Araiz Naqvi

Network Security Engineer

If you **find this** helpful, you’ll love my content!

M @araiz-naqvi

in @araiznaqvi