INCIDENT REPORT | 003 | OS HARDENING

DETAILS

yummyrecipesforme.com
Cause: Security issue when loading the main page.

A former employee of the service for yummyrecipesforme.com has become a malicious threat actor and lured users to a fake website that has malware within it.

Logs

The browser initiates a DNS request for yummyrecipesforme.com.

The DNS replies with the correct IP address.

The browser initiates an HTTP request.

The browser initiates the download of the malware.

The browser initiates a DNS request for greatrecipesforme.com.

The DNS server responds with the IP address for greatrecipesforme.com.

The browser initiates an HTTP request to the IP address for greatrecipesforme.com.

The former employee was able to gain access to the web service via a brute force attack. They kept guessing the administrative password, got it correct, and accessed the admin panel to change the website's source code.

The former employee was able to embed the source code with a JavaScript that prompted the user to be redirected to another webpage, greatrecipesforme.com, instead. This webpage contained the malware that attacked user's computers.

Hours after the attack, multiple customers emailed the help desk for yummyrecipesforme.com. The owner of the website was not able to access the website due to the password being changed by the former employee, who had access to the admin panel at this point.

RESPONSE

- **There needs to improved password policies implemented, as well as Multi-Factor Identification (MFA).**
- **Analysts will improve Intrusion Detection Software in order to receive alerts focused on repeated fail logins.**