Incident Report - yummyrecipesforme.com Website Compromise

Date/Time of Incident: July 27, 2024, 14:18:32 (based on TCPdump log)

Reporting Analyst: [Your Name]

Section 1: Network Protocols Involved

The following network protocols were instrumental in the incident:

- **DNS (Domain Name System):** Utilized to resolve the domain names yummyrecipesforme.com (legitimate site) and greatrecipesforme.com (malicious site) to their respective IP addresses (203.0.113.22 and 192.0.2.17). The TCPdump log entries at 14:18:32.192571 and 14:20:32.192571 clearly show DNS queries for these domains.
- **HTTP (Hypertext Transfer Protocol):** Facilitated communication between the user's browser and both websites, enabling the initial website loading and the subsequent redirection to the malicious site. The TCPdump logs show the establishment of HTTP connections (flags [S], [S.], [.]) and subsequent data transfer (flags [P.])
- **TCP (Transmission Control Protocol):** Underlied HTTP, ensuring reliable data packet delivery for both the legitimate website content and the malicious download prompt. The sequence numbers (seq) and acknowledgment numbers (ack) in the TCPdump log detail this process.

Section 2: Incident Details

A former employee exploited a weak default administrative password to gain unauthorized access to the yummyrecipesforme.com web server. This was likely achieved through a brute-force attack, as suggested by the absence of security controls mentioned in the previous analysis. The attacker then injected malicious JavaScript code into the website's source code.

The injected code triggered a prompt for users to download an executable file disguised as a browser update upon visiting the website. The TCPdump logs show this download initiation at 14:18:36.786595. Once executed, the malware modified the user's browser settings to redirect any subsequent requests from yummyrecipesforme.com to the attacker-controlled website greatrecipesforme.com, as evidenced by the DNS query for greatrecipesforme.com at 14:20:32.192571 and the following HTTP traffic to 192.0.2.17.

Impact:

- **Confidentiality:** Potential compromise of customer data if collected on the fake website.
- **Integrity:** Website content was manipulated to deliver malware.
- **Availability:** Legitimate website access was disrupted by the redirection.

Remediation Actions Taken:

- Web server was temporarily isolated.
- Firewall rule implemented to block traffic from 192.0.2.17.

Section 3: Remediation Recommendation

Implement Multi-Factor Authentication (MFA) for Administrator Accounts:

Given the evidence of a brute-force attack, the most immediate and effective remediation is to implement MFA for all administrative accounts. This would require an additional authentication factor (e.g., one-time code, hardware token) beyond just the password, significantly increasing the difficulty for attackers to gain unauthorized access, even with a compromised password. This would drastically improve the security posture of the admin panel and mitigate the risk of similar future incidents.