Säkerhetsincidentrapport

Datum: 20-02-2025

Rapporterad av: Zayn AK **Företag:** YummyRecipesForMe.com
Klassificering: Kritisk
Incident: Brute Force Attack & Malware-infektion

---

1. Sammanfattning av incidenten

Flera besökare på **yummyrecipesforme.com** rapporterade att de blev omdirigerade till en falsk webbplats, **greatrecipesforme.com**, efter att ha laddat ner en fil som de blev uppmanade att installera.

Logganalys visade att en före detta anställd använde en **Brute Force-attack** för att få åtkomst till administratörskontot och modifierade webbplatsens källkod genom att injicera **JavaScript-malware**. Detta ledde till att webbplatsbesökare ovetandes installerade en skadlig programvara.

🔍 2. Teknisk analys

2.1. Angreppsflöde

1. **DNS-fråga** skickades för att lösa IP-adressen till yummyrecipesforme.com.
2. **HTTP-förfrågan** skickades till webbservern.
3. **Nedladdning av skadlig fil** initierades automatiskt via JavaScript.
4. **Ny DNS-förfrågan** skickades till greatrecipesforme.com.
5. **HTTP-förfrågan** skickades till den skadliga webbplatsen.

2.2 & 2.3. Packet Capture Logg (`tcpdump`) & Identifierade säkerhetsbrister

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)

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)

-**Administratörslösenordet var standardinställt** och kunde enkelt gissas. -**Ingen skyddsmekanism för Brute Force-attacker** fanns på plats. -**Webbserverns källkod kunde modifieras** utan att upptäckas. -**Ingen Two-Factor Authentication (2FA)** för administratörskontot.

---

3. Påverkan på organisationen

Påverkan	Beskrivning
Förlorad kundförtroende	Besökare upplevde att webbplatsen var skadlig.
Förlorad affärsintäkt	Besökare kunde inte göra inköp på den komprometterade webbplatsen.
Nedtid för IT-resurser	IT-teamet var tvunget att prioritera säkerhetsincidenten.
Risk för juridiska åtgärder	GDPR-överträdelser kunde ha uppstått genom kunders dataintrång.

---

4. Rekommenderade åtgärder

Kortfristiga åtgärder

- **Webbplatsen tas offline** för att förhindra vidare infektion.
- **Administratörskontot återställs** och ett nytt starkt lösenord skapas.
- **DNS-omdirigering kontrolleras** för att blockera den falska webbplatsen.
- **JavaScript-mallar granskas** för skadlig kod.

Långsiktiga åtgärder

Åtgärd	Beskrivning
Inför starka lösenordskrav	Kräver minst 12 tecken, specialtecken och regelbunden rotation.
Implementera Two-Factor Authentication (2FA)	Kräver extra verifiering vid inloggning.

Åtgärd	Beskrivning
Automatiska säkerhetsuppdateringar	Skyddar mot kända säkerhetshål i webbservern.

5. Slutsats

Incidenten orsakades av en **Brute Force-attack** som komprometterade administratörskontot. Hackaren modifierade webbplatsens kod och distribuerade **skadlig programvara** till besökare. För att förhindra framtida angrepp rekommenderas **starka lösenord, 2FA, loggövervakning och säkerhetsuppdateringar**.

Förberett av: Zayn AK **Roll:** Cybersäkerhetsanalytiker