L'attaque de 2011 contre **Comodo**, une autorité de certification (CA), est l'un des incidents de sécurité les plus notables dans l'histoire des certificats SSL/TLS. Voici un résumé de ce qui s'est passé, les détails techniques, et les répercussions de cette attaque.

Contexte de l'attaque
En mars 2011, un **pirate iranien** (se faisant appeler **ComodoHacker**) a réussi à compromettre les systèmes de **Comodo** et à émettre des **faux certificats SSL** pour plusieurs domaines très sensibles, dont certains appartenant à des services web de grandes entreprises et organisations.

Détails de l'attaque

1. **Ciblage de revendeurs de Comodo** :
    - Comodo n'a pas été directement compromise. L'attaque a ciblé des **revendeurs** ou **partenaires de Comodo**, qui avaient la capacité d'émettre des certificats SSL sur demande.
    - L'attaquant a compromis les systèmes d'un **revendeur** et a pu s'introduire dans l'infrastructure qui autorisait l'émission de certificats, ce qui lui a permis d'émettre des certificats SSL/TLS valides pour des domaines de haute importance.
2. **Faux certificats émis** : L'attaquant a réussi à émettre des certificats valides pour les domaines suivants :
    - mail.google.com
    - login.yahoo.com
    - login.live.com (utilisé par les services de Microsoft)
    - login.skype.com
    - addons.mozilla.org
    - global trustee

Ces domaines appartiennent à des services très utilisés, notamment Google, Microsoft, Yahoo!, Skype et Mozilla.

3. **Utilisation potentielle** :
    - Les certificats émis auraient permis à l'attaquant d'effectuer une attaque **Man-in-the-Middle (MITM)** sur les utilisateurs accédant à ces services.
    - Dans une telle attaque, l'attaquant pourrait tromper les utilisateurs en leur faisant croire qu'ils se connectaient à un site sécurisé alors qu'en réalité, leur connexion passait par le pirate. Cela aurait permis à l'attaquant de lire ou de modifier des informations sensibles comme les identifiants de connexion ou les communications.
4. **Motivation présumée** :
    - Le pirate **ComodoHacker**, qui prétendait être iranien, a affirmé avoir mené cette attaque seul et pour des raisons politiques, probablement liées au contexte géopolitique de l'époque en Iran.
    - Il a notamment exprimé son soutien à l'État iranien dans des messages qu'il a publiés en ligne, laissant penser que l'attaque avait une motivation liée au contrôle de la censure et de la surveillance internet.

Répercussions
L'attaque a eu des conséquences importantes sur la sécurité des communications internet :

1. **Révocation des certificats** :
    - Dès que l'attaque a été découverte, **Comodo** a révoqué les certificats émis frauduleusement, ce qui a empêché leur utilisation future.
    - Les navigateurs web et les systèmes de mise à jour des certificats ont été rapidement informés pour s'assurer que les certificats frauduleux ne seraient pas acceptés.
2. **Mise à jour des navigateurs** :
    - Des entreprises comme Google, Mozilla et Microsoft ont mis à jour leurs navigateurs (Chrome, Firefox, Internet Explorer) pour bloquer les certificats émis par le revendeur compromis et s'assurer que les utilisateurs étaient protégés.
3. **Renforcement des pratiques de sécurité** :
    - L'incident a révélé des faiblesses dans le système de gestion des autorités de certification. Les CA, ainsi que les navigateurs, ont dû adopter des pratiques de sécurité plus strictes pour protéger l'infrastructure SSL/TLS.
    - Cela a mené à une meilleure transparence dans la gestion des certificats et à l'adoption d'initiatives comme **Certificate Transparency**. Cette initiative oblige les CA à publier publiquement tous les certificats émis, ce qui permet de détecter rapidement les certificats frauduleux.
4. **Confiance dans les autorités de certification** :
    - L'attaque a soulevé des questions sur la sécurité des CA et la confiance excessive placée dans un petit nombre d'organisations pour assurer la sécurité d'Internet.
    - Le système des autorités de certification, où les CA peuvent émettre des certificats pour n'importe quel domaine, a montré des vulnérabilités. Une seule CA compromise peut affecter des millions d'utilisateurs à travers le monde.

Précisions sur l'attaquant

L'attaquant **ComodoHacker** a prétendu dans plusieurs publications en ligne être un jeune hacker iranien agissant seul. Il a exprimé dans ses déclarations un soutien au gouvernement iranien et une opposition à des nations occidentales, notamment les États-Unis et Israël. Cependant, il n'y a pas eu de preuve solide quant à ses motivations politiques exactes, ni s'il agissait seul ou avec l'aide d'une organisation.

Impact à long terme

Cet incident a joué un rôle dans l'adoption de pratiques de sécurité plus robustes et dans l'amélioration de la transparence des certificats numériques. Il a mis en lumière la nécessité de renforcer les audits de sécurité pour les revendeurs et partenaires des autorités de certification, et a contribué à la mise en place d'initiatives comme **Public Key Pinning** et **Certificate Transparency Logs**.

Conclusion

L'attaque contre **Comodo en 2011** a été une violation majeure de la confiance dans le système des certificats SSL/TLS, exploitant des failles dans les chaînes de confiance des autorités de certification. Cet incident a révélé la nécessité d'améliorer la sécurité dans la gestion des certificats numériques pour protéger les utilisateurs contre les attaques de type MITM et autres attaques ciblées sur les infrastructures de confiance d'internet.