Hackers exploited Salesforce zero-day in Facebook phishing attack

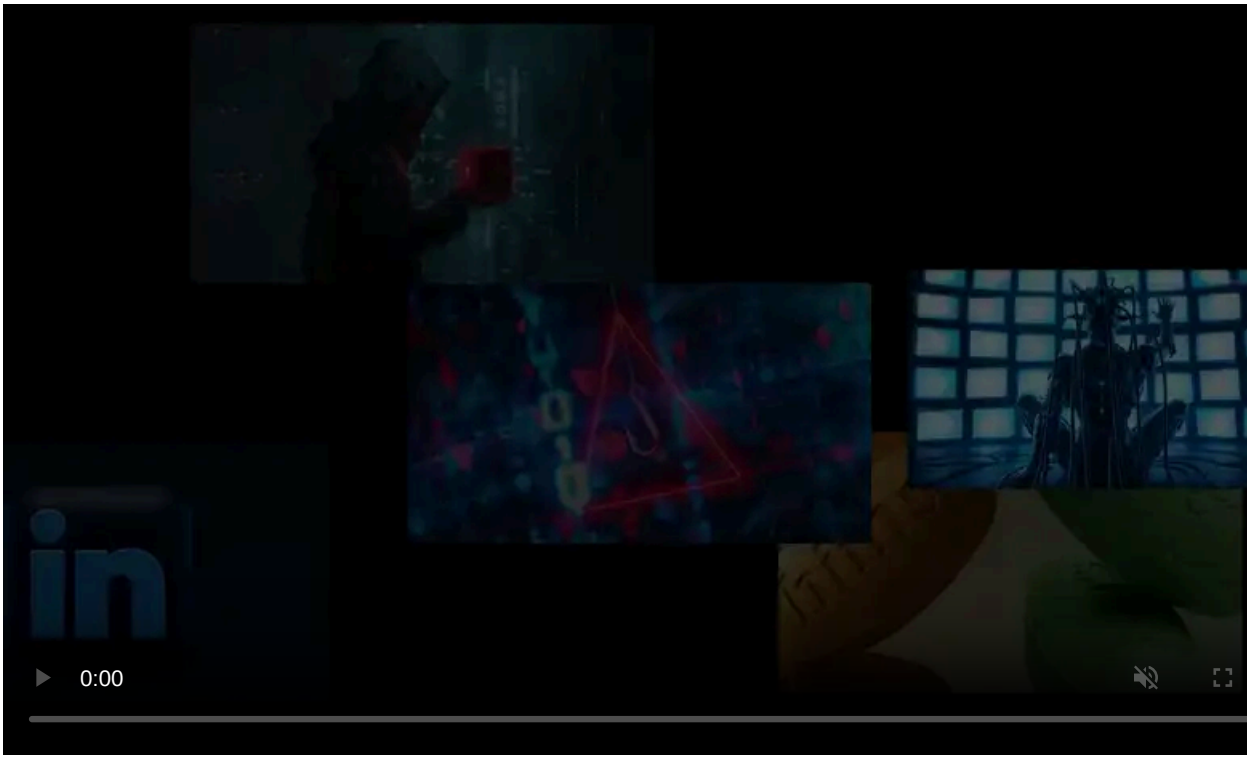
By Bill Toulas

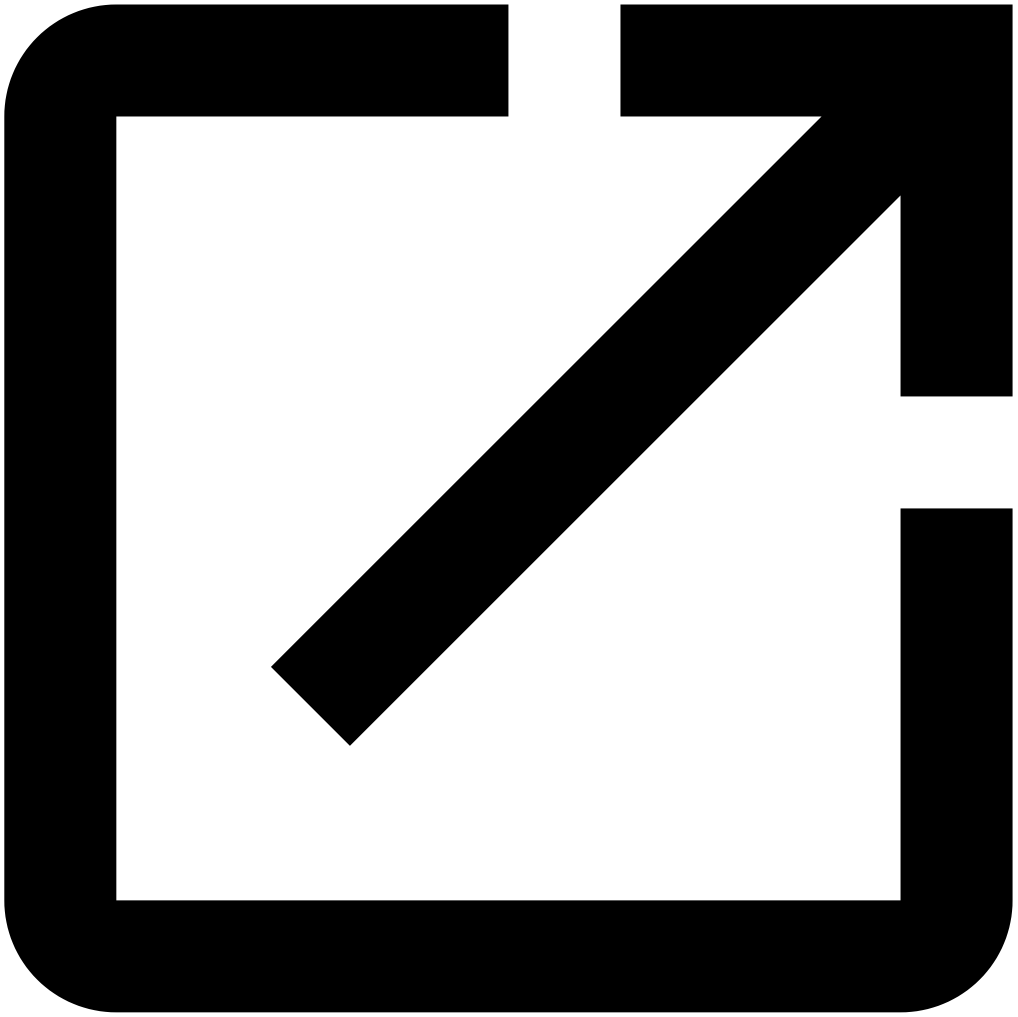
Published: 2023-08-02 · Archived: 2026-04-05 18:00:37 UTC

Hackers exploited a zero-day vulnerability in Salesforce's email services and SMTP servers to launch a sophisticated phishing campaign targeting valuable Facebook accounts.

The attackers chained a flaw dubbed "PhishForce," to bypass Salesforce's sender verification safeguards and quirks in Facebook's web games platform to mass-send phishing emails.

The benefit of using a reputable email gateway like Salesforce to distribute phishing emails is the evasion of secure email gateways and filtering rules, ensuring that the malicious emails reach the target's inbox.


0:00



The campaign was discovered by Guardio Labs analysts Oleg Zaytsev and Nati Tal, who reported the unknown vulnerability to Salesforce and helped them with the remediation process.

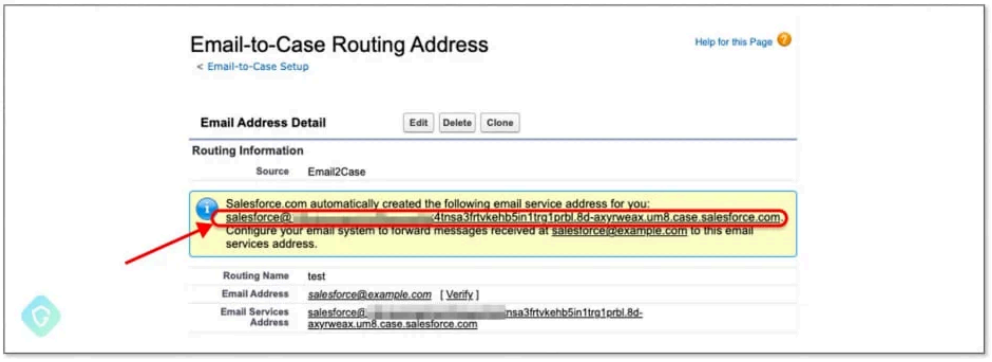
However, the discovered issues in Facebook's game platform are outstanding, as Meta's engineers are still trying to figure out why the existing mitigations failed to stop the attacks.

PhishForce abused in attacks

The Salesforce CRM allows customers to send emails as their own brand using custom domains that the platform must first verify. This protects customers from sending out emails through Salesforce as other brands that they do not have permission to impersonate.

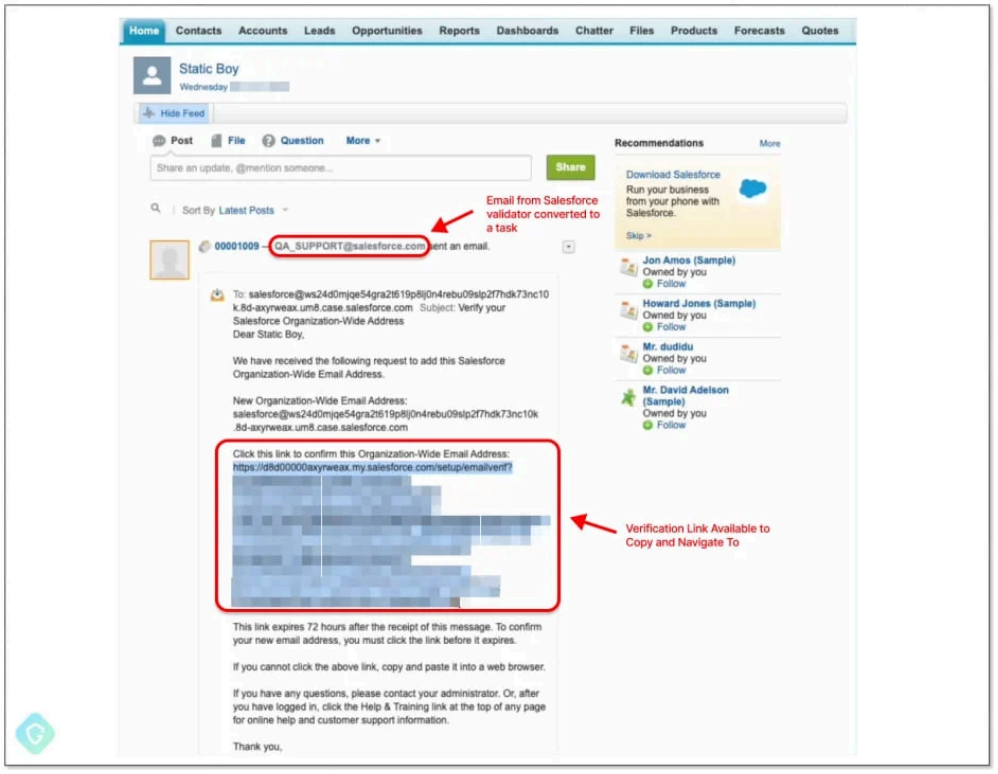
However, Guardio Labs says the attackers figured out a way to exploit Salesforce's "Email-to-Case" feature, which organizations use for converting incoming customer emails to actionable tickets for their support teams.

Specifically, the attackers set up a new "Email-to-Case" flow to gain control of a Salesforce-generated email address, then created a new inbound email address on the "salesforce.com" domain.



Generated Salesforce address *(Guardio Labs)*

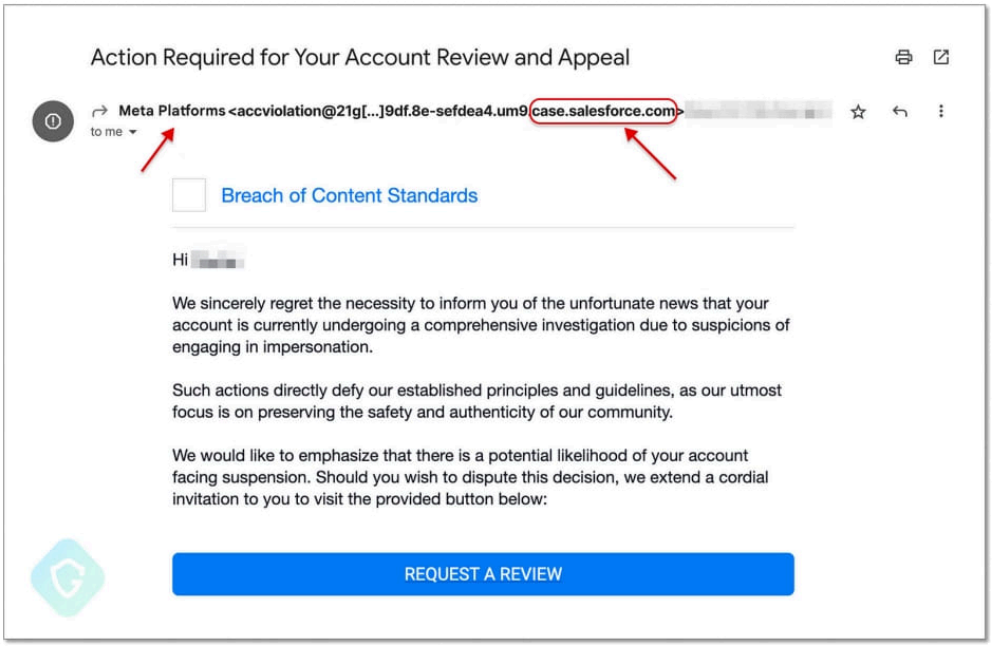
Next, they set that address as an "Organization-Wide Email Address," which Salesforce's Mass Mailer Gateway uses for outbound emails, and finally went through the verification process to confirm ownership of the domain.



Clicking on the verification link to confirm ownership *(Guardio Labs)*

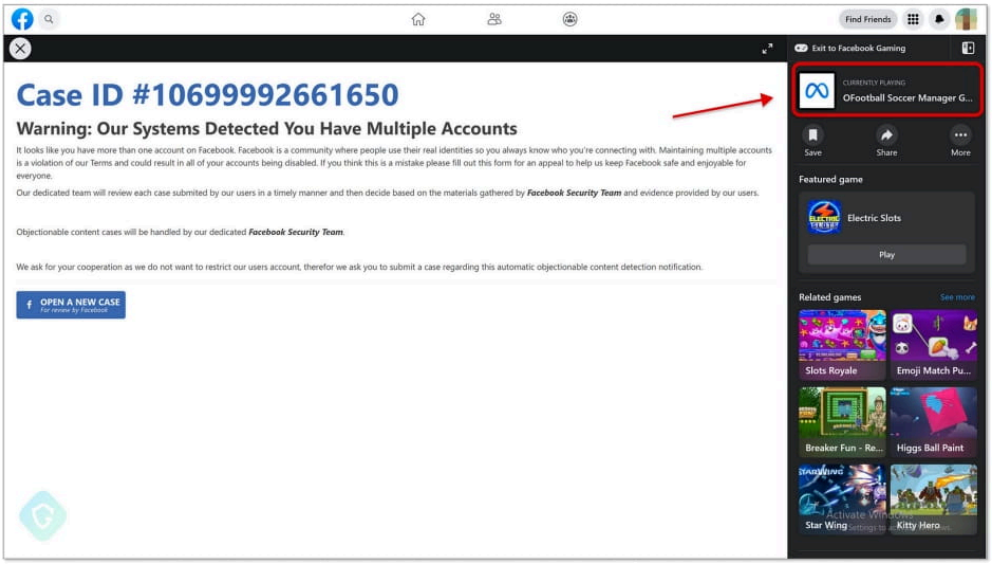
This process allowed them to use their Salesforce email address to send out messages to anyone, bypassing both Salesforce's verification protections and any other email filters and anti-phishing systems in place.

Indeed, this is what Guardio Labs observed in the wild, with phishing emails that supposedly came from "Meta Platforms" using the "case.salesforce.com" domain.



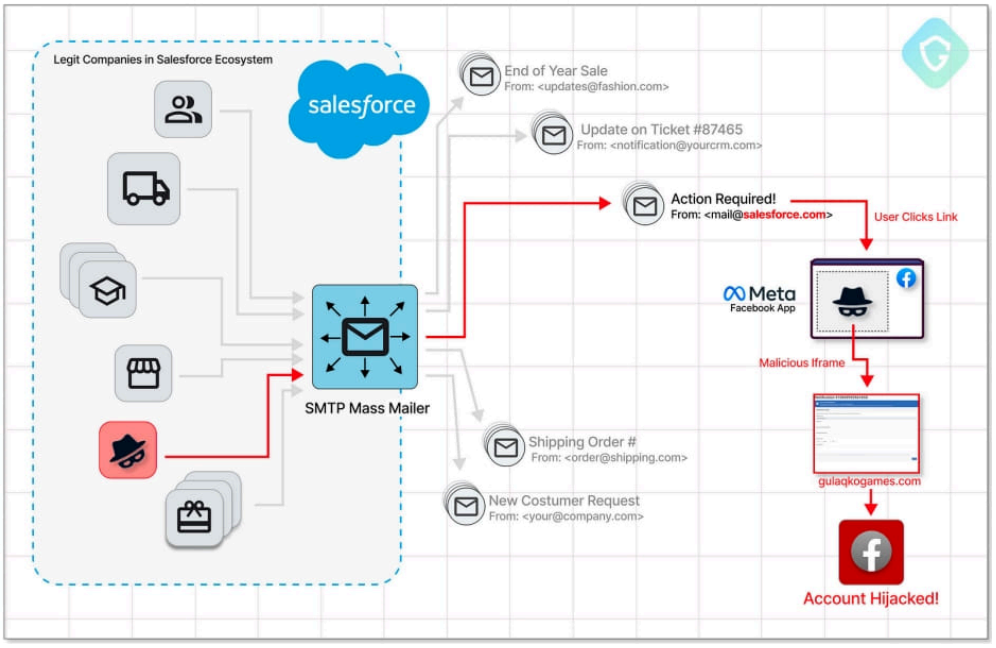
Phishing email sampled from a real attack *(Guardio Labs)*

Clicking on the embedded button takes the victim to a phishing page hosted and displayed as part of the Facebook gaming platform ("apps.facebook.com"), which adds further legitimacy to the attack and makes it even harder for the email recipients to realize the fraud.



Phishing page hosted on the Facebook gaming platform *(Guardio Labs)*

The goal of the phishing kit employed in this campaign is to steal Facebook account credentials, even featuring two-factor authentication bypassing mechanisms.



The observed attack chain *(Guardio Labs)*

Meta still investigating

After confirming the issues by replicating the creation of a Salesforce-branded address capable of disseminating phishing emails, Guardio Labs notified the vendor of their discovery on June 28, 2023

Salesforce reproduced the vulnerability and resolved the problem exactly a month later, on July 28, 2023.

Regarding the abuse of "apps.facebook.com," Guardio Labs notes that it should be impossible for the attackers to create the game canvass used as a landing page since Facebook retired this platform in July 2020.

However, legacy accounts that used the platform before its deprecation still have access, and threat actors might be paying a premium for those accounts on the dark web.

Meta removed the violating pages upon Guardio Labs' report; however, its engineers are still investigating why existing protections failed to stop the attacks.

As phishing actors continue to explore every potential abuse opportunity on legitimate service providers, novel security gaps constantly threaten to expose users to severe risks.

Thus, it is essential not to rely solely on email protection solutions, and also scrutinize every email that lands on your inbox, look for inconsistencies, and double-check all claims made in those messages.

Source: https://www.bleepingcomputer.com/news/security/hackers-exploited-salesforce-zero-day-in-facebook-phishing-attack/