The 2025 Salesforce Data Breach Campaign by ShinyHunters

Confidence Staveley

Read more >>



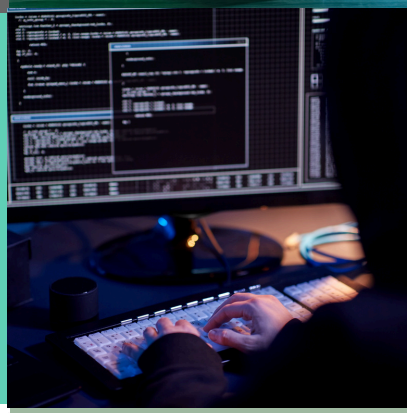



Table of Contents

01 Attack Methods

04 Impact on Specific Victims

11 Broader Impact on Other Victims

14 Financial and Legal Ramifications Across the Board

15 Conclusions and Lessons Learned

A cybercrime group called ShinyHunters (also known as UNC6040) launched a series of cyberattacks in mid-2025 that targeted the Salesforce systems of many large organizations across different industries. This campaign affected about 91 companies worldwide, including well-known names like Google, Workday, Allianz Life, Cisco, Qantas Airways, Pandora, and luxury brands such as Louis Vuitton, Dior, and Tiffany & Co.

The attackers didn't exploit a flaw in the Salesforce platform itself. Instead, they used social engineering, specifically voice-phishing (or "vishing") and deceptive applications that request access to data (malicious OAuth applications), to trick employees into giving them access to their organization's Salesforce data. By taking advantage of people's trust and weak security settings, ShinyHunters were able to bypass normal login protections and steal large amounts of company data stored in the cloud. This campaign shows how a trusted cloud-based software platform can be misused through coordinated social engineering when attackers target people directly instead of the technology.

Attack Methods

ShinyHunters' attacks combined old-fashioned deception with the misuse of Salesforce's features that allow it to connect with other applications.

First, they pretended to be IT support staff in convincing phone calls and sometimes text messages, targeting employees at companies that use Salesforce. During these vishing calls, the attacker would create an urgent scenario, like a critical system problem, and guide the unsuspecting employee through steps to "fix" the issue. In reality, these steps led the victim to give the attackers high-level access to the company's customer relationship management (CRM) system.

Specifically, victims were told to go to Salesforce's Connected Apps authorization page and enter an 8-digit code provided by the attacker.

Entering this code unknowingly approved a harmful application controlled by the attackers. This was often a fake version of Salesforce's legitimate "Data Loader" tool or an app with a harmless-sounding name like "My Ticket Portal". Once the employee authorized this, the attackers gained an OAuth token, which gave them access to the organization's Salesforce data at the API level. This access bypassed multi-factor authentication (MFA) and didn't require exploiting any software flaws, as it was obtained through OAuth and a user's legitimate session.

From this point, ShinyHunters could search for and steal large amounts of records from the company's CRM system. Google's Threat Intelligence Group noted that the attackers started with small data searches to avoid immediate detection, then escalated to large-scale data theft once they were inside. In some cases, they even used the stolen CRM credentials to get into other cloud services like Office 365, but their main goal was the data stored in Salesforce. Throughout the campaign, no inherent vulnerability in Salesforce was exploited; the breach succeeded by manipulating end-user behavior and taking advantage of overly permissive settings for OAuth apps.

EXTORTION AND DATA LEAKAGE

After stealing the data, the attackers moved to extortion and data leakage. After a delay, often weeks or months after the breach, victims would receive ransom demands for cryptocurrency via email or phone. These demands, claiming to be from ShinyHunters, threatened to publish the stolen data if payment wasn't made. Google's investigators refer to the extortion phase as a separate group (UNC6240) that repeatedly mentioned the ShinyHunters name. By August 2025, the group even created a Telegram channel called "ScatteredLapsu$Hunters" to leak samples of stolen data and mock victims and authorities. In one post, the attackers made public a ransom note addressed to Salesforce's CEO, demanding 20 Bitcoin to prevent them from leaking data from "91 organizations" obtained in this campaign. Small portions of data from various companies were posted as "teasers," and screenshots of negotiations with victims were

shared to increase pressure. Eventually, when some victims refused to pay, full dumps of data appeared on criminal forums or Telegram. For example, ShinyHunters leaked the complete stolen databases from Allianz Life's Salesforce instance in mid-August.

Attribution

The use of phone-based social engineering and OAuth token misuse initially led some experts to suspect the group Scattered Spider (known for previous vishing attacks on companies like MGM Resorts). The tactics did indeed resemble Scattered Spider's methods of impersonating employees or contractors to fool help desks and bypass MFA.

However, as Google and others investigated further, evidence pointed to the ShinyHunters group, including connections to previous Snowflake cloud storage breaches and direct extortion messages. ShinyHunters themselves told the media they and Scattered Spider were "the same," suggesting a collaboration where Scattered Spider operatives gain initial access, which ShinyHunters then uses to steal data. It appears the campaign combined ShinyHunters' data-theft-for-ransom approach with Scattered Spider's social engineering skills, possibly even involving former members of the Lapsus$ hacking group. Notably, one alleged ShinyHunters member (a BreachForums administrator) was arrested by French police in June 2025, but this barely slowed the campaign, suggesting a decentralized "extortion-as-a-service" operation with multiple actors rather than a single mastermind. By combining the names of various infamous groups (Scattered Spider, Lapsus$, ShinyHunters), the attackers likely aimed to increase their perceived influence and intimidate victims.

SCOPE AND DATA COMPROMISED

The campaign was widespread, affecting organizations in technology, finance, aviation, retail, and luxury goods. The intrusions began in early 2025 and continued for several months. Many breaches were first detected

in June or July 2025 and publicly announced between July and August as affected companies investigated and informed their stakeholders. By August 2025, the pattern of "mysterious" CRM data thefts was clearly linked, with one analysis describing these incidents as "a string of unsolved murders" sharing the same calling card (Salesforce).

In almost all cases, the attackers stole customer and business contact details stored in Salesforce, such as names, phone numbers, email addresses, dates of birth, and client IDs. Some victims also lost internal account records, client IDs, or notes related to those contacts. While no passwords or credit card data were reported stolen, this type of personal and business data can still be used for scams, phishing, or fraud.

The amount and sensitivity of data varied by company. At Allianz Life, the breach included Social Security numbers and tax IDs. For Google and Workday, the stolen data was mostly business contact information, which was potentially public or not highly sensitive on its own. Regardless, the sheer scale of some breaches was significant enough that some airlines saw millions of passenger records accessed, and large insurance or retail firms had databases of over a million customer entries stolen in one go.

It's important to note that each affected company's Salesforce instance was breached separately through targeted social engineering – this was not a single breach of Salesforce's central system, but rather a campaign that exploited many organizations' user accounts on the Salesforce platform. Salesforce's infrastructure remained untouched, but the incident highlighted how a compromised cloud software service can affect "hundreds or thousands of downstream clients," similar to a supply-chain breach.

Impact on Specific Victims

WORKDAY

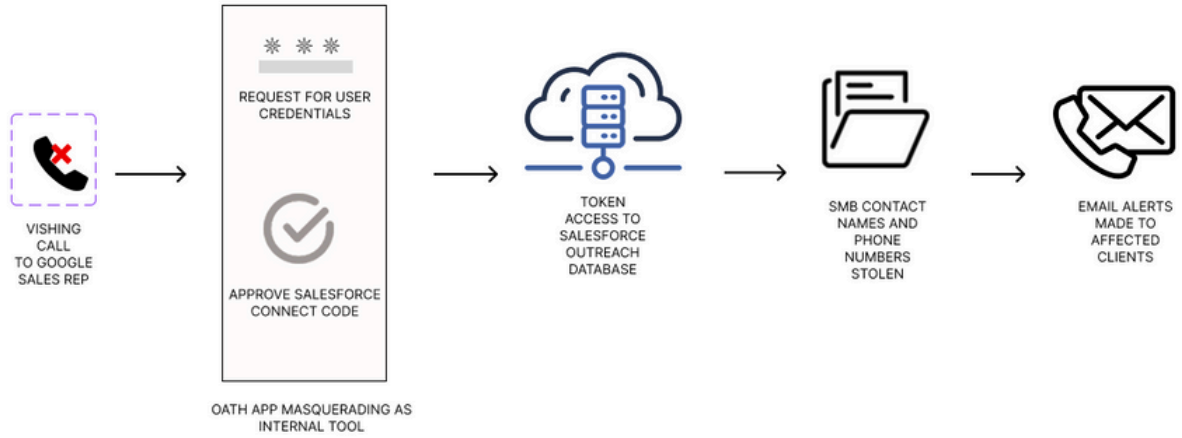
Workday, a major provider of HR and financial software, confirmed on August

18, 2025, that attackers accessed some information in its third-party CRM platform (which was Salesforce, though Workday didn't explicitly name it). They assured clients that no customer production systems or core customer data were accessed, as the compromise was limited to CRM data used by their sales and support teams. The data exposed in Workday's case was mainly "commonly available business contact information," such as names, phone numbers, and emails of Workday's customers and potential clients. While this might seem minor compared to passwords or financial records, it could still be used for scams and phishing attempts. Workday noted the attackers might use this information "to further their social engineering scams" by targeting those contacts in the future. Although the full extent of the breach wasn't publicly quantified, the company described the incident as having a limited scope. According to an internal notification seen by reporters, the breach was discovered on August 6, 2025, allowing Workday to quickly cut off the unauthorized access. The incident was treated as a serious trust issue, but Workday emphasized that the damage was contained. The company reminded clients that it would never call asking for passwords. Internally, Workday revoked the attackers' access tokens, added extra security safeguards, and reinforced employee security training to counter phone and email scams.

Reputationally, Workday's transparency likely helped reduce the negative impact. The company openly acknowledged being targeted by this campaign , and framed the event as part of a broader industry threat rather than a singular failure. Since no highly sensitive personal data was lost, Workday avoided major fines or lawsuits. Its openness about being one of many affected companies probably helped maintain trust.

GOOGLE

Even Google was not immune; it disclosed on August 8, 2025, that it had discovered unauthorized access to one of its corporate Salesforce databases used for sales outreach. The database mainly contained contact details and notes about small and medium-sized business clients.



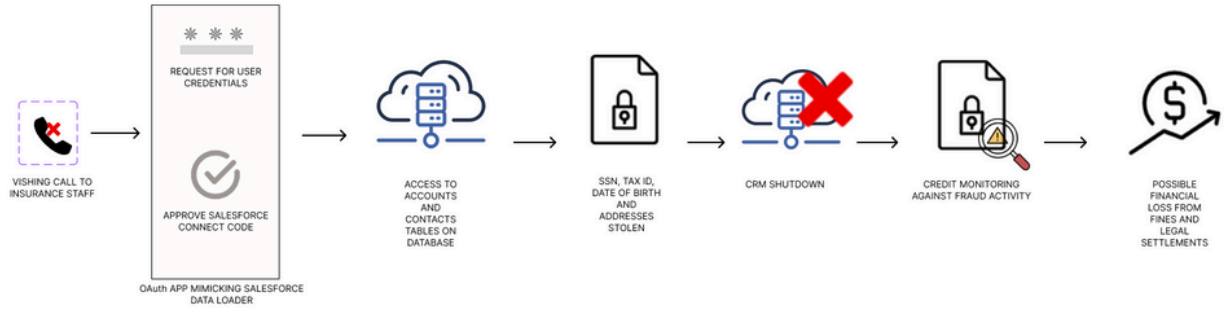
Google's SMB Contact Database Compromise

Google confirmed the breach in a blog post by its Threat Intelligence team, attributing it to the same UNC6040/ShinyHunters actors and describing the vishing-to-OAuth attack method in detail. The scope of stolen data was relatively basic as hackers had access to the database for only a "small window of time" before detection, and it consisted mostly of names, business contacts, and phone numbers. No Google accounts, passwords, or internal systems were affected; it was essentially a breach of a marketing contact list. Still, that information could be used to target those businesses with phishing emails, especially if attackers pretended to be Google representatives. Recognizing this risk, Google "completed email notifications to those affected" by early August , alerting the impacted small-business customers that their information was exposed.

Google treated the incident as a learning opportunity, which lessened its impact and response on the company. Despite publishing a blog post in early June warning about these exact tactics, they still fell victim, highlighting how well-defended organizations can be breached if an insider is tricked, underscoring that human factors are the weakest link in security. No financial loss was disclosed from this breach. For remediation, Google worked to cover all bases by tightening internal procedures for approving third-party apps and rolling out fresh reminders about verifying unusual IT requests. They also shared guidance on countering these attacks by using strict IP allow-listing for Salesforce access, monitoring for new connected apps, and educating staff to verify callers' identities.

ALLIANZ LIFE

One of the most severe breaches in this campaign hit Allianz Life, a large U.S. insurer. According to reports, on July 16, 2025, attackers broke into its Salesforce CRM and stole a large amount of personal data for the "majority" of its 1.4 million customers. While the company initially declined to specify the exact number affected, independent analysis later determined that roughly 1.1 million unique customers were impacted.



Allianz Life's High-Sensitivity Data Breach

In addition, data on Allianz Life's business partners (such as brokers and financial advisors) was compromised, bringing the total records leaked to about 2.8 million entries when both individual and institutional contacts are counted.

The stolen data was highly sensitive. The attackers obtained Salesforce "Accounts" and "Contacts" database tables, which included individuals' names, home addresses, email addresses, phone numbers, dates of birth, and even Tax Identification Numbers such as U.S. Social Security numbers. For business clients and partners, professional details like license numbers, firm affiliations, and product or policy information were stolen. These records likely amounted to a rich target for identity theft or fraud, as attackers can combine contact information, date of birth, and Social Security numbers to make fraudulent insurance claims or open financial accounts. BleepingComputer also confirmed the authenticity of the leaked data by verifying real individuals' details (emails, tax IDs, etc.), leaving little doubt about the extensive nature of this breach.

The qualitative impact on Allianz Life and its customers was significant. A breach of this magnitude typically triggers regulatory scrutiny and class-action lawsuits in the U.S.. Allianz Life promptly notified state authorities: filings to regulators in Texas and Massachusetts confirmed that Social Security numbers were among the data stolen, which under U.S. law necessitates offering affected individuals credit monitoring and identity protection services. The reputational damage for Allianz was jarring as customer confidence was shaken due to data exposure. The company stressed it was cooperating with law enforcement as part of the broader investigation into the ShinyHunters' campaign.

In response to this attack, Allianz took its Salesforce CRM offline immediately after discovery and "contained" the incident on the same day. Forensic experts were hired and notifications sent to all legally required parties. Remedial measures likely included revising how third-party apps can connect to their Salesforce (tightening OAuth app approvals and network restrictions) and doubling down on employee authentication training. Allianz also had to manage the fallout of the data leak: with 2.8 million records published, they must monitor for fraud attempts and assist customers in preventing identity theft.

Though not fully disclosed, financial losses from this breach could be considerable. Allianz may incur costs for credit monitoring for over 1 million people, potential regulatory fines (if deemed non-compliant with data privacy laws), and the expense of the investigation and system upgrades. Allianz appears to have refused ransom payments, which led to its data being dumped publicly. Moving forward, Allianz Life will likely face increased oversight from U.S. regulators and possibly European authorities (if any EU data was involved) to prevent a recurrence. This incident clearly illustrates the high quantitative impact (millions of sensitive records) a Salesforce breach can have, as well as the cascading qualitative effects – from customer mistrust to legal headaches – of such an exposure.

Broader Impact on Other Victims

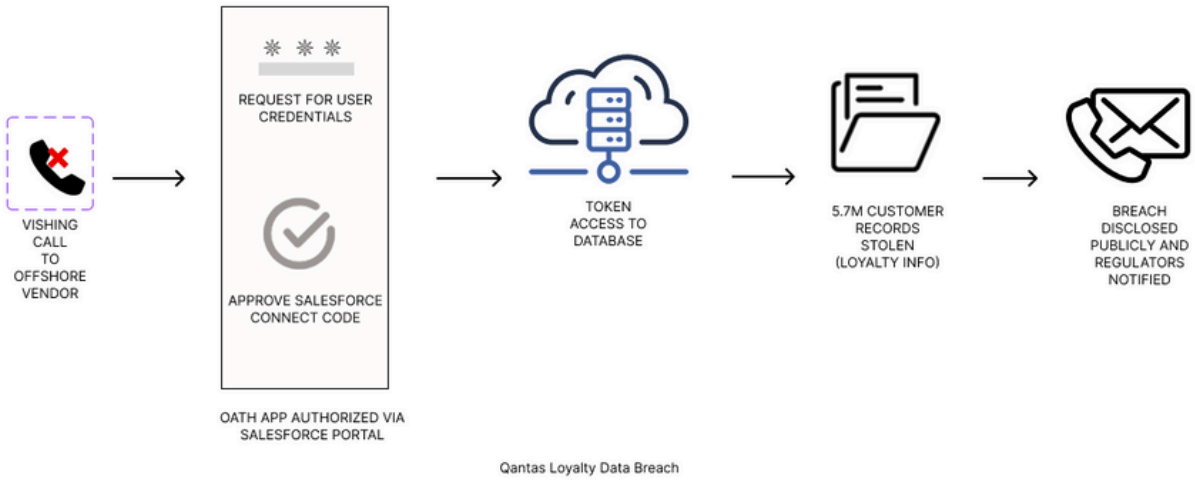
Beyond Workday, Google, and Allianz Life, dozens of companies worldwide were caught in ShinyHunters' Salesforce-focused hacking spree. While a complete list is beyond the scope of this document, several notable examples highlight the range of impacts:

CISCO

The networking giant was hit by a vishing attack that allowed an attacker to access Cisco's Salesforce data for Cisco.com user accounts. Discovered on July 24, the breach allowed hackers to steal "a subset of basic profile information" from Cisco's third-party CRM. This included users' names, organizations, addresses, Cisco user IDs, email addresses, phone numbers, and some account metadata like creation dates. Cisco revoked the attackers' app access as soon as it detected the breach and launched an investigation. While they didn't reveal how many customers were affected, the scale could still be large given Cisco's massive customer base. The impact of this incident was more on reputation than financial. Cisco publicly disclosed the breach on August 5, 2025, linking it to the same campaign that hit Allianz and Qantas.

QANTAS AIRWAYS

Australia's national airline experienced one of the largest exposures by sheer numbers. In late June 2025, Qantas discovered that attackers had accessed a Salesforce system containing customer records (likely via a compromised offshore call center vendor account). The breach affected up to 5.7 million customers. For all of them, names, emails, and loyalty program data were exposed, and for approximately 1.7 million of those customers, even more details—addresses, dates of birth, phone numbers, gender, and meal preferences—were stolen. Qantas disclosed the incident on July 1, making headlines across Australia, which has already seen major data breaches in recent years (at Optus and Medibank). The qualitative



Qantas Loyalty Data Breach

impact in Australia was massive, as leaked data could be used in scams even if it might not cause direct financial loss (e.g., a frequent flyer number leak is not critical on its own). Still, the Australian privacy watchdog and government took note, especially since it followed warnings about the aviation sector being targeted by groups like Scattered Spider. Qantas responded by cutting off the affected third-party platform access, accelerating security upgrades, and advising customers to be alert to phishing. Qantas reportedly received a ransom demand but didn't pay. Regulatory action by the Office of the Australian Information Commissioner is possible, as the incident falls under Australia's mandatory data breach notification scheme. This case shows the massive scale these attacks can reach, affecting millions and drawing national attention.

LUXURY RETAILERS (LVMH, DIOR, TIFFANY & CO., CHANEL)

Several luxury brands also reported Salesforce breaches.

- Louis Vuitton (LVMH) found in July that regional client databases were accessed, exposing personal information like names, contact details, dates of birth, and purchase history (though not payment details).

- Dior said in May that Salesforce data for South Korean customers had been stolen, including contact details and shopping preferences.

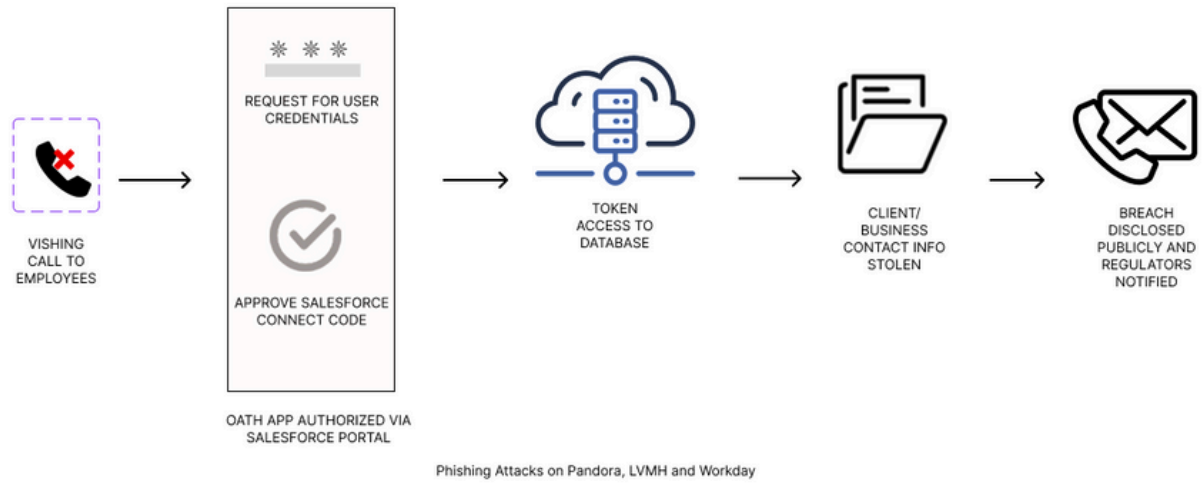
- Tiffany & Co. had its Salesforce customer data in Asia compromised in April.

- Chanel USA confirmed in late July that an unauthorized party had accessed its customer support database, which held names, emails, and phone numbers of clients who had contacted Chanel support.

These brands notified customers and, where required, regulators. They stressed that no payment data or passwords were taken. Still, in the luxury sector, reputation matters as much as security, so even the loss of contact details was a concern. Brands like Chanel openly acknowledged the breach cause as OAuth token social engineering and said they were reinforcing security training and access controls to prevent a recurrence. The fallout seemed contained to goodwill gestures (apology letters, advice to customers) rather than measurable financial loss, but it certainly prompted these firms to strengthen their CRM security practices and vet third-party processes more rigorously.

PANDORA (JEWELRY RETAILER)

In a breach detected in July and disclosed in August, Pandora confirmed that data from its Salesforce environment was stolen, impacting customer profiles. Exposed information included customer names, dates of birth, and email addresses, though the company emphasized no payment or password data was compromised. Uniquely, Pandora's statement



Phishing Attacks on Pandora, LVMH and Workday

cited ShinyHunters by name as claiming responsibility, which reflected how bold the group had become. The scale was not mentioned, but given their global presence, hundreds of thousands of customers could be affected.

Pandora reacted by notifying those customers and announcing a review of its third-party security settings and partnerships to address any vulnerabilities. The impact here was mostly on customer trust and the need for Pandora to demonstrate improved security ; like others, Pandora had to reassure patrons that no financial information leaked and that it was taking the matter seriously.

Financial and Legal Ramifications Across the Board

As of this writing, none of the companies mentioned have disclosed exact financial losses due to these Salesforce breaches. The attackers generally didn't steal money directly; instead, they went after data they could use for extortion or future scams. When ransom demands weren't paid, they leaked stolen records online. This left companies with indirect financial damage like costs of incident response, hiring cybersecurity firms, providing identity theft protection services, and potential regulatory penalties.

Companies like Allianz Life and Qantas, which leaked highly sensitive or large volumes of data, face the greatest regulatory risk. Allianz's breach could invite investigations by state insurance regulators or the FTC in the U.S., and possibly GDPR oversight if any EU citizen data was involved. Qantas and Air France-KLM (which also had a Salesforce breach affecting customer service records) must answer to their national privacy authorities. Regulators in multiple countries got involved:

- Allianz Life has reported to U.S. state regulators since Social Security numbers were stolen.

- Qantas fell under Australia's mandatory data breach laws
- Dior reported its breach to South Korean authorities in May
- Chanel reported to U.S. state regulators in August

Legally, a few victims are likely to face class-action lawsuits from affected customers. For instance, U.S. consumers often sue after insurance breaches involving Social Security numbers (as seen in past incidents), so Allianz Life might face litigation alleging failure to protect data. Those outcomes will play out over time. Meanwhile, law enforcement efforts against ShinyHunters continue. The FBI and international partners were already tracking the group due to earlier crimes, and the French arrest in June 2025 was part of a broader takedown of BreachForums administrators. In this campaign's context, the FBI reportedly worked with some victim companies on the extortion aspects. ShinyHunters' brazen Telegram activities in August, leaking data and boasting about hacks, likely intensified the global police scrutiny. As of August 2025, while the group (or its copycats) are still at large, the intelligence gathered from these incidents will aid future prosecutions.

Conclusions and Lessons Learned

The 2025 "Salesforce breach" campaign by ShinyHunters/UNC6040 is a clear reminder that even well-secured cloud platforms can be undermined by sophisticated social engineering attacks. The hackers didn't need to find bugs in Salesforce's code or use zero-day exploits (new, unknown software vulnerabilities); instead, they exploited human trust and legitimate features by simply calling employees and convincing them to grant access, so to speak, via OAuth app authorizations. This method allowed the attackers to steal millions of customer records from nearly a hundred organizations, including some of the world's biggest companies. The immediate impacts were significant: personal data of perhaps tens of millions of people were

exposed to criminals. While much of the stolen data was "just" contact details, that information can still be used for fraud, phishing, or identity theft. In Allianz's case, the data was far more sensitive, including Social Security numbers.

The tangible costs of these breaches include incident response, legal notifications, and damage to reputation for the companies involved. Some may also face regulatory fines or lawsuits, such as Allianz. Salesforce itself wasn't technically at fault, but it worked with customers to share guidance on reducing risks, such as:

- Reviewing and limiting permissions for third-party applications.
- Using least-privilege access for how applications connect to Salesforce (API integrations).
- Stricter approval (whitelisting) for OAuth applications.
- Re-evaluating their cloud security configurations.
- Strengthening employee training to spot suspicious calls or emails.

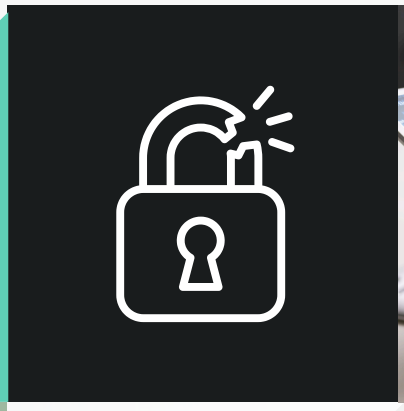
In the end, the ShinyHunters Salesforce breaches underscore a classic truth in cybersecurity: a company's security is only as strong as its people and the processes around its technology. Even a robust platform like Salesforce can be "the soft underbelly" if users are tricked into opening a hole. By focusing on user-centric attacks, the adversaries bypassed strong technical defenses. The takeaway for organizations is to combine technical safeguards with user awareness. Multi-factor authentication remains critical, but it isn't a complete solution if OAuth tokens can bypass it ; therefore, monitoring and limiting third-party app access is vital. As these breaches show, data stored in the cloud must be guarded with the same vigilance as on-premise valuable assets, and incident response plans must include scenarios driven by social engineering. For those companies hit in 2025, the hope is that lessons learned will strengthen their defenses, as groups like ShinyHunters are likely to evolve and attempt new attack methods. The industry at large has taken note of this campaign, treating it as a wake-up call to the dangers of highly targeted social engineering aimed at our increasingly important cloud-based software platforms.

References

- Salesforce-Related Data Breach Affecting Multiple Companies - SOCRadar® Cyber Intelligence Inc. https://socradar.io/salesforce-data-breach-affecting-multiple-companies/
- ShinyHunters strike again: Workday breach tied to Salesforce-targeted social engineering wave |CSO Online https://www.csoonline.com/article/4042191/shinyhunters-strike-again-workday-breach-tied-to-salesforce-targeted-social engineering-wave.html
- Blog The Cost of a Call: From Voice Phishing to Data Extortion | Google Cloud https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion?rev=7194ef805fa2d04b0f7e8c9521f97343
- HR giant Workday discloses data breach after Salesforce attack https://www.bleepingcomputer.com/news/security/hr-giant-workday-discloses-data-breach-amid-salesforce-attacks
- Google says hackers breached internal database https://www.axios.com/2025/08/06/google-shinyhunters-salesforce-data-breach
- Hackers leak Allianz Life data stolen in Salesforce attacks https://www.bleepingcomputer.com/news/security/hackers-leak-allianz-life-data-stolen-in-salesforce-attacks/
- Qantas attack reveals one phone call is all it takes to crack cybersecurity's weakest link: humans |Qantas | The Guardian https://www.theguardian.com/business/2025/jul/06/qantas-attack-reveals-one-phone-call-is-all-it-takes-to-crack-cybersecuritys weakest-link-humans
- Payback: ShinyHunters Clocks Google via Salesforce https://www.darkreading.com/cyberattacks-data-breaches/payback-shinyhunters-google-salesforce
- Hacker used a voice phishing attack to steal Cisco customers' personal information | TechCrunch https://techcrunch.com/2025/08/05/hacker-used-a-voice-phishing-attack-to-steal-cisco-customers-personal-information/ 10

References

- Allianz Life data breach affects 1.1 million customers | TechCrunch https://techcrunch.com/2025/08/18/allianz-life-data-breach-affects-1-1-million-customers/
- Workday US Protecting You From Social Engineering Campaigns: An Update From Workday https://blog.workday.com/en-us/protecting-you-from-social-engineering-campaigns-update-from-workday.html




SYSTEM
HACKED