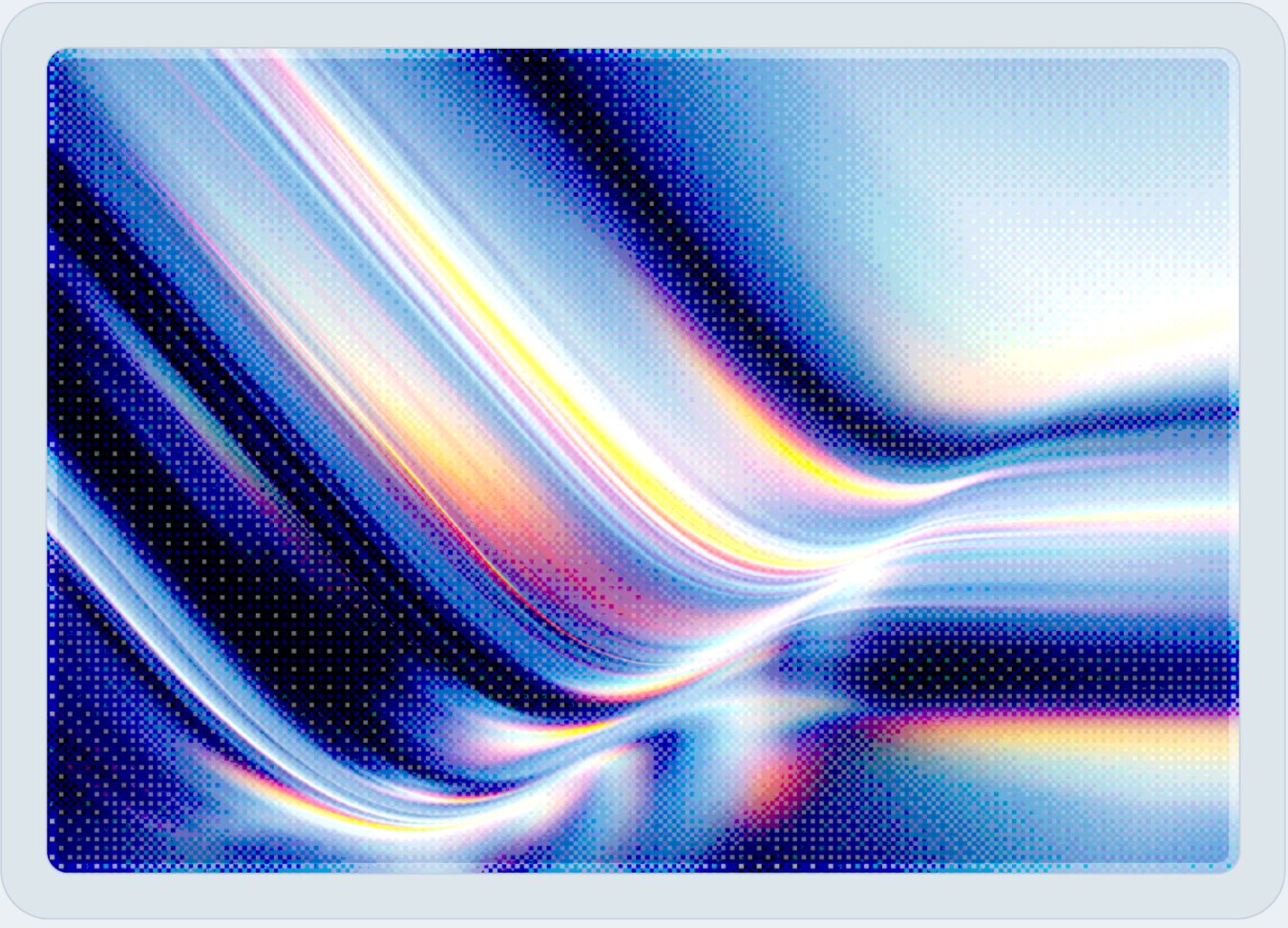
CSAI Foundation | Cloud Security Alliance

City-Forum: The Cross-Sector SaaS Guest-Portal Blind Spot

A 17-Month Campaign Exploiting Salesforce and ServiceNow Guest Access

2026-08-19

AI-assisted Rapid Research



CSAI | CSA cloud security alliance®

Key Takeaways

Security researchers at SaaS security firm Reco have documented City-Forum, a data-scraping campaign that has continuously enumerated anonymous "guest" access on Salesforce Experience Cloud and ServiceNow Service Portal deployments for more than seventeen months without rotating its infrastructure [1][2]. The entire operation traces to a single IP address, 158.220.87.79, hosted by German VPS provider Contabo and tied to the domain city-forum.com, which has resolved to that address since March 2025 [2][3]. Unlike the OAuth-token supply-chain breaches CSA has previously analyzed at Salesloft, Gainsight, and Klue, City-Forum requires no compromised vendor and no stolen credential; it simply automates requests against guest-user identities that Salesforce and ServiceNow both ship with by default and that this campaign found repeatedly left over-permissioned across its targets [3][4]. One targeted Salesforce environment alone logged more than 560,000 events from the attacker's IP, nearly all of it guest-context object enumeration [1][3]. Targets span telecommunications carriers, banks, enterprise software vendors, and public-sector portals, and the researchers who found it stopped short of attributing it to a known group, cautioning against the temptation to assume every Salesforce guest-access campaign is a ShinyHunters operation [4]. CSA reads this episode not as a new vulnerability but as a mature, durable exploitation of a configuration weakness that has existed in both platforms for years and that guest-access defaults make difficult to fully close.

Background

Salesforce Experience Cloud (built on the Aura and Lightning Web Runtime, or LWR, frameworks) and ServiceNow Service Portal both give organizations a way to expose curated content, support cases, or self-service functionality to people who are not logged-in employees: customers checking order status, partners submitting tickets, or members of the public searching a knowledge base. To make that work without forcing every visitor to create an account, both platforms provision a persistent "guest user" identity that executes requests on behalf of anonymous visitors [3][4]. That identity inherits whatever sharing rules, object permissions, and field-level access an administrator has configured for it, and on both platforms it is a permanent structural feature rather than an account that can be deleted; it can only be restricted [3]. Security researchers have warned about Salesforce guest-user over-exposure for

years, and CSA's own analysis of the 2025-2026 ShinyHunters campaigns against Salesloft, Gainsight, and Klue documented a recurring pattern of Salesforce customer-data compromise, whether attackers arrive through a stolen OAuth token or, as in this case, through a guest identity left unrestricted.

Reco's researchers first identified the pattern while investigating anomalous scraping traffic against a Salesforce customer and traced the requests back to a fixed IP address associated with the domain city-forum.com, an apparently defunct domain registered originally in 2002 and repurposed for this campaign beginning in March 2025 [2][3]. Passive DNS records show the domain has pointed continuously at 158.220.87.79 for the campaign's entire duration, and subdomains including server.city-forum.com and mail.city-forum.com suggest the operator built out supporting infrastructure rather than relying on a single throwaway host [3]. Every request observed in the campaign carries the default user-agent string of Go's native net/http library, Go-http-client/1.1, indicating the tool is a compiled, purpose-built binary rather than a browser-automation script or an off-the-shelf scanner [1][2]. That combination of static infrastructure and custom tooling, sustained for well over a year without apparent concern for detection, is what distinguishes City-Forum from noisier, faster-moving extortion campaigns and is why Reco characterizes the operator as a patient, resourced actor rather than an opportunistic scanner [4].

Security Analysis

City-Forum's Salesforce tradecraft targets both of the platform's site-building frameworks. Against classic Aura-based Experience Cloud sites, the tool first calls `HostConfigController.getConfigData` to enumerate which Salesforce objects a given guest profile can see, then pages through the exposed records using `SelectableListDataProviderController.getItems`, a pattern that mirrors techniques long documented in public tools such as AuraInspector [2][4]. Against newer LWR-based sites, the campaign instead targets the `/webruntime/api/services/data/{version}/graphql` endpoint, systematically sweeping API versions v56.0 through v66.0, querying `EntityDefinition` to discover accessible objects, and then retrieving records via GraphQL cursors [3][4]. Reco's researchers noted this LWR/GraphQL technique specifically because it is largely undocumented in public security tooling; in Reco's assessment, this represents a gap in Experience Cloud monitoring, since guest-access detection tooling has tended to focus on the older Aura endpoints [4]. In both frameworks, the tool additionally probes `/SiteRegister` and `/CommunitiesSelfReg` to test whether a site allows anonymous visitors to self-register as authenticated external users, which would grant a foothold with broader privileges than the guest profile alone provides [2][3].

Against ServiceNow, the campaign concentrates on a single native endpoint, `POST /api/now/sp/search?sysparm_cancelable=true`, which the Service Portal uses to let anonymous visitors search knowledge base articles and service catalog items [3][4]. The attacker varies search terms systematically to enumerate whatever content a portal's search sources expose to unauthenticated users, and Reco observed request volume against this endpoint climb from tens of requests per day to hundreds over the course of the campaign [4]. The endpoint's design compounds the risk: it returns an HTTP 201 response with an empty result set both when a search genuinely finds nothing and when access controls block the request, making it difficult for a defender reviewing logs to distinguish a failed probe from a successful one without deeper investigation [3][4]. On the ServiceNow side, the underlying misconfigurations researchers identified include knowledge base and service-catalog items published without a login gate, custom search-source scripts built on the unrestricted `GlideRecord` API rather than the access-control-enforcing `GlideRecordSecure`, and an absence of `gs.isLoggedIn()` checks in scripted search logic that should have excluded anonymous callers [3][4].

What ties every technique together is that none of it depends on a software vulnerability. As Reco's researchers framed it, every byte the attacker retrieved was something a site owner had already exposed to anonymous users [3][4]. The Salesforce misconfigurations enabling City-Forum's collection include overly broad sharing rules granting the Guest User record-level access beyond what the public-facing use case requires, guest profiles with excessive object and field-level read permissions, the "Allow guest users to access public APIs" setting left enabled on LWR sites, and self-registration enabled without adequate controls around who is approved [4]. This is precisely the same category of guest-access over-exposure that a separate 2025 wave of Salesforce Experience Cloud attacks, run using AuraInspector and related public tools, exploited before it, as CSA's own OAuth-focused analyses of the Salesloft, Gainsight, and Klue breaches have documented, and that overlap is exactly why Reco declined to rule out a connection to the ShinyHunters collective while also declining to assert one [4]. Reco's researchers were explicit that inferring "this doesn't look like a prior campaign, therefore it must be a different actor" is a common path to confident, wrong attribution, and organizations should treat the question of who is behind City-Forum as unresolved rather than settled [4].

City-Forum's operational choices reflect deliberate infrastructure management rather than a smash-and-grab operation. Running a single IP address and a single domain for over seventeen months without rotation suggests a campaign built to persist and evade takedown, since it would have been straightforward to detect and block the source address at any point once flagged, yet the infrastructure was apparently never burned enough to warrant a change [2][3]. At the same time, the command server's SSH service was found running a release roughly a year and a half out of date, suggesting the operator treats the infrastructure itself as disposable even while keeping the network identity stable, a

combination that is somewhat unusual and may reflect an actor confident that guest-access scraping, because it resembles legitimate anonymous traffic, is unlikely to trigger the kind of response that would force infrastructure changes [3][4].

The sectoral spread reported by Reco, telecommunications, banking and financial services, enterprise software vendors including security and privacy firms, and public-sector portals, indicates the campaign is not narrowly targeted but rather opportunistically scanning any Salesforce Experience Cloud or ServiceNow Service Portal deployment reachable on the public internet, regardless of industry [1][3]. That breadth is consistent with the underlying vulnerability being a widespread configuration default rather than an industry-specific weakness, which suggests organizations should not assume they are unlikely targets simply because they are not in a sector traditionally associated with high-profile SaaS breaches.

Recommendations

Immediate Actions

Salesforce administrators should audit every Experience Cloud site's Guest User sharing rules and profile permissions, removing object and field-level read access that is not strictly required for the site's public-facing purpose, and should search access and event-monitoring logs for the indicators Reco published: the Go-http-client/1.1 user agent, the IP address 158.220.87.79, request paths containing `/webruntime/api/services/data`, and spikes against `/SiteRegister` or `/CommunitiesSelfReg` [2][3][4]. ServiceNow administrators should review which Service Portal search sources are reachable by unauthenticated users and specifically check for requests to `/api/now/sp/search` from unfamiliar sources, cross-referencing the same source IP and user-agent indicators [3][4]. Any organization that finds matching traffic should treat it as an active compromise of exposed guest data rather than a benign scan, and should inventory what content the affected guest profile or search source could see, since that inventory defines the actual scope of data already collected.

Short-Term Mitigations

Beyond the immediate indicator sweep, organizations should disable the "Allow guest users to access public APIs" setting on LWR sites unless a specific integration requires it, turn off self-registration on Experience Cloud sites that do not need it, and disable guest file access and member-visibility settings that are commonly left at permissive defaults [4]. On ServiceNow, administrators should replace

`GlideRecord` calls in custom scripted search sources with `GlideRecordSecure` so access control lists are enforced, add explicit `gs.isLoggedIn()` checks before any data query in guest-facing scripts, and tighten knowledge base "Can Read" criteria so articles are not inadvertently published to anonymous users [3][4]. Because guest identities cannot be removed outright on either platform, the durable fix is a recurring review process, not a one-time cleanup: guest profile permissions and portal search-source configurations should be revisited on a regular cadence, ideally tied to any change in site functionality, since new features are a common source of permission creep.

Strategic Considerations

City-Forum is a useful counterpoint to the OAuth-token supply-chain breaches that have dominated SaaS security discussion over the past year, because it demonstrates that attackers do not need a compromised vendor integration to extract meaningful volumes of customer or partner data from Salesforce and ServiceNow; a persistently under-governed guest identity is sufficient, and evidently has been sufficient for well over a year in multiple organizations' environments [1]. Security teams that have focused their SaaS security investment on OAuth grant inventories and connected-app governance should recognize that guest and anonymous-access configurations represent a parallel, equally durable attack surface that requires its own recurring review discipline, not a one-time hardening exercise. The fact that a single actor could sustain unattributed, undetected collection across telecommunications, banking, software, and public-sector targets for seventeen-plus months without triggering a takedown also suggests that monitoring approaches focused on authenticated-session anomalies would have missed this campaign, and that guest-context traffic, treated as expected and unremarkable by both platforms' design, may be similarly under-covered elsewhere [3][4].

CSA Resource Alignment

CSA's SaaS Security Capability Framework (SSCF) is the most directly relevant framework for City-Forum, since its identity and access management domain already establishes the principle that every form of standing access to SaaS platform data, credentialed or not, should be governed as a periodically re-certified grant [5]. CSA's own analysis of the 2025-2026 ShinyHunters campaigns against Salesloft, Gainsight, and Klue established that Salesforce customer data has repeatedly been the target of SaaS supply-chain compromise, typically through a stolen OAuth token; City-Forum extends that same target profile, Salesforce (and now ServiceNow) customer data, through a structurally different path, abusing a guest identity the customer organization itself provisioned and failed to restrict. That parallel argues that the SSCF's IAM domain controls should explicitly cover anonymous and guest-context access reviews alongside connected-app and OAuth grant governance [5].

This kind of cross-sector, multi-organization targeting is not unique to City-Forum; CSA has tracked similarly industrialized operating models elsewhere in the SaaS integration layer, and while Reco explicitly declined to attribute City-Forum to any named group, the pattern is structurally consistent with that broader trend, underscoring that both credentialed-integration abuse and anonymous guest-access abuse are being run at a comparable scale. More broadly, City-Forum falls within the identity and access management domain of CSA's AI Controls Matrix (AICM) v1.1: guest and anonymous-access identities are, in effect, standing non-human access grants that require the same least-privilege scoping, periodic review, and monitoring discipline the AICM prescribes for any other identity type, and organizations assessing their Salesforce and ServiceNow deployments against AICM's IAM domain should explicitly include guest and community-user profiles in that review rather than limiting it to employee and service-account access [6].

References

[1] The Hacker News. "One Attacker Has Scraped Both Salesforce and ServiceNow Guest Portals for Over a Year." The Hacker News, August 2026.

[2] BleepingComputer. "City-Forum Data Theft Attacks Target Salesforce, ServiceNow Portals." BleepingComputer, August 2026.

[3] Reco. "City-Forum Campaign: Scraping Salesforce and ServiceNow Guest Portals." Reco Blog, August 2026.

[4] SecurityWeek. "Stealthy City-Forum Attacks Target Salesforce and ServiceNow With Custom Toolset." SecurityWeek, August 2026.

[5] Cloud Security Alliance. "SaaS Security Capability Framework (SSCF)." Cloud Security Alliance, September 2025.

[6] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2025.