

The Golden Scale: Bling Libra and the Evolving Extortion Economy

By Matt Brady

Published: 2025-10-10 · Archived: 2026-07-28 02:00:32 UTC

Scattered Lapsus\$ Hunters: What Retail and Hospitality Organizations Should Know

In recent months, threat actors claiming to be part of a new conglomerate dubbed [Scattered Lapsus\\$ Hunters](#) (aka SP1D3R HUNTERS, SL3H) have asserted responsibility for laying siege to customer Salesforce tenants as part of a coordinated effort to steal data and hold it for ransom. At least [one industry source](#) refers to this criminal syndicate as the Trinity of Chaos. “Trinity” is used because the conglomerate is likely composed of individuals tied to three groups: [Muddled Libra](#) (aka Scattered Spider), [Bling Libra](#) (aka ShinyHunters), and [LAPSUS\\$](#), all of which are likely representative of the broader cybercriminal community known as [The Com](#).

At this time, the threat actors claim to have stolen more than 1 billion Salesforce records as part of two separate threat campaigns aimed at stealing customer information. The main culprit behind the extortion attempts is Bling Libra, a threat group likely active since at least early 2020 that has previously claimed responsibility for a number of data breaches over the last few years.

As noted by Unit 42 in related [Insights pieces](#) earlier this year, a number of global retail and hospitality organizations have felt the brunt of this data theft extortion activity. Here, we provide readers with the latest updates tied to these threat actors. We highlight the inherent risks for retail and hospitality organizations potentially impacted by this activity and offer recommendations to combat the evolving threat of extortion-as-a-service (EaaS) providers.

The Rise of Bling Libra’s EaaS Offering

On Oct. 3, 2025, Scattered Lapsus\$ Hunters [officially launched their data leak site \(DLS\)](#). At the time of its inception it was hosted on a domain previously associated with the BreachForums cybercrime forum. Figure 1 below depicts an image posted at the top of the DLS.

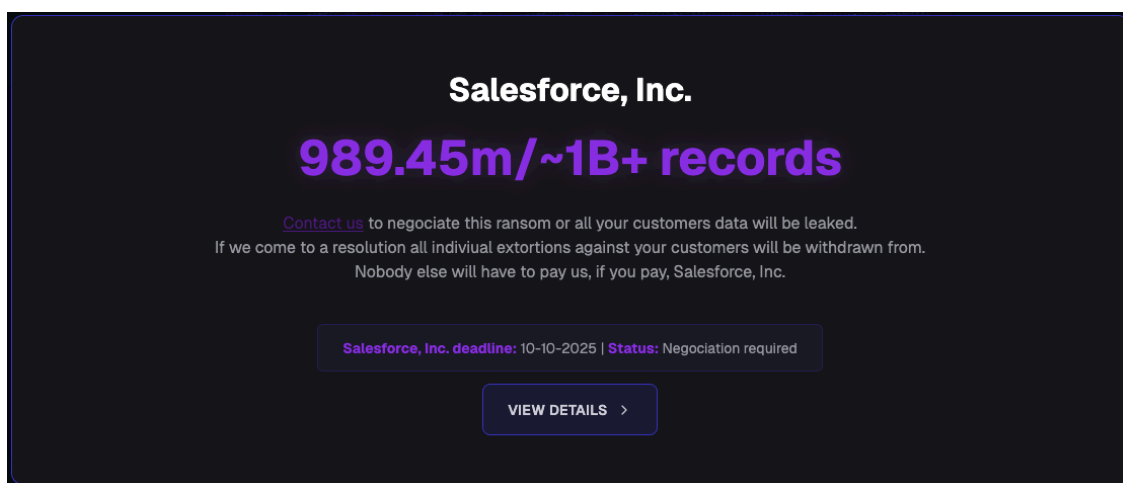


Figure 1. Image of Bling Libra's Salesforce data leak site. Source: [BleepingComputer](#).

The threat actors posted the names of 39 global organizations from which they claim to have stolen Salesforce data. They set a deadline of Oct. 10, 2025 for the victims to pay a ransom, threatening to leak the files after that time. Based on Unit 42 observations across Telegram channels operated by the threat group, they are also recruiting other threat actors to help send extortion notes to victims via email, specifically focusing on communicating with executives.

The threat actors have even attempted to directly extort Salesforce itself. The [company responded](#) to media outlets that it has no intentions of negotiating with or paying a ransom to the cybercriminals, a message which they also reiterated via emails to customers.

Bling Libra [recently told Bleeping Computer](#) that they have been privately operating as an EaaS provider for some time now. They claimed to take a revenue share (typically 25-30%) from extortion payments made to threat actors they are collaborating with.

This is a similar playbook to how ransomware-as-a-service (RaaS) providers have operated for several years now. The primary differentiator between EaaS and RaaS is the lack of malware deployment (ransomware) that encrypts files, thereby typically rendering them inaccessible.

As documented in a [prior Unit 42 threat research article](#), Bling Libra has evolved over time with regards to their monetization tactics. They moved from selling and publishing stolen data to directly extorting victims. Our article documented their activity after infiltrating victims' Amazon Web Services (AWS) cloud environments. The activity in the news in recent months shows their primary focus on Salesforce tenants.

The Emergence of Other Extortion-focused Threat Groups

Another notable development in the EaaS economy is Bling Libra's recent collaboration with a threat group named Crimson Collective. This group was seemingly unknown until their recent entrance onto the data theft extortion scene.

Based on Unit 42 observations and news reports, [Crimson Collective claimed](#) to have breached Red Hat on or about Oct. 1, 2025. The cybercriminals claim to have exfiltrated approximately 570 GB of compressed data from more than 28,000 internal development repositories. [Red Hat confirmed](#) the root cause as a breach into one of its

GitLab instances. The stolen data allegedly includes an estimated 800 Customer Engagement Reports (CERs), which are documents prepared for clients by Red Hat consultants that typically contain sensitive information about the clients' network and platforms.

Other news reports indicate that [Crimson Collective has also been actively targeting AWS cloud environments](#) in recent weeks, where they continue to be focused on data theft and subsequent extortion. At this time, it appears that in addition to sending extortion notes via email to victims, the threat group is [also partnering](#) with Scattered Lapsus\$ Hunters to post victims via Bling Libra's recently launched DLS. Figure 2 alludes to this combination of criminal forces.

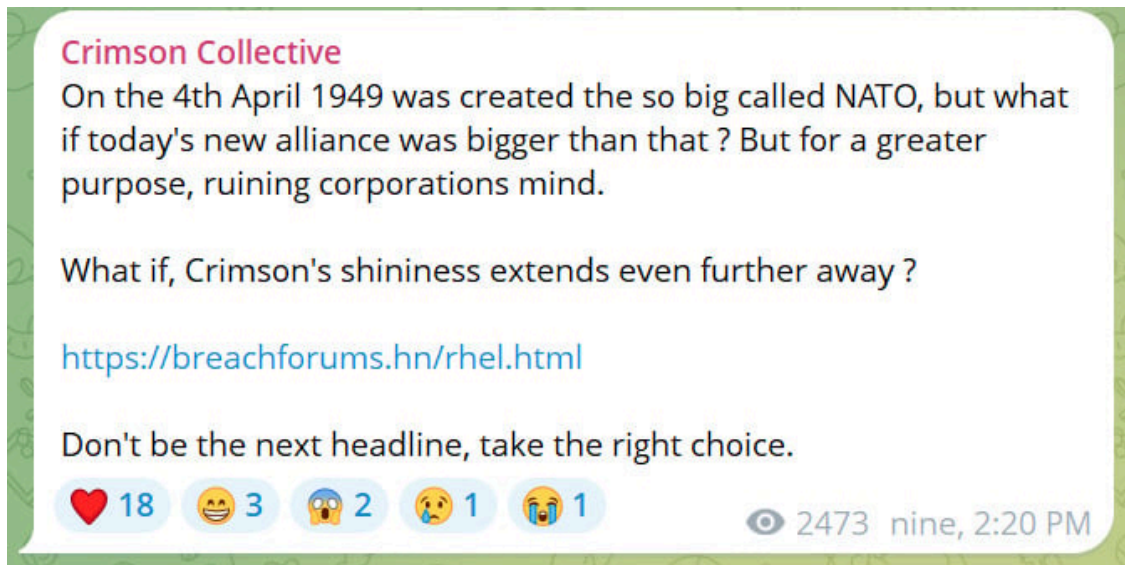


Figure 2. Screenshot of Telegram post by Crimson Collective. Source: [BleepingComputer](#).

Similar to Scattered Lapsus\$ Hunters, Crimson Collective also operates at least one Telegram channel to communicate with their audience, typically boasting of their latest victims. News reports indicate that [victims allegedly impacted by their breach of Red Hat](#) include aviation, telecommunications, public-sector, financial services and retail organizations.

Bling Libra's Pending Deadline

In recent weeks, Scattered Lapsus\$ Hunters posted on their Telegram channels that they were retiring from their cybercrime operations. This claim was [greeted with skepticism](#) by industry experts. Based on recent events illustrated throughout this article, that was an incredibly short-lived retirement — if at all factual.

On Oct. 9, 2025, [the FBI announced](#) that it had seized all domains associated with BreachForums. Shortly thereafter, Bling Libra confirmed the seizure activity. This included the clearnet version of their newly launched DLS. The group stated that it will not pursue relaunching another iteration of BreachForums.

However, Bling Libra stated that none of its core members had been arrested and that the darknet version of their DLS was not impacted by the FBI's activity. Doubling down, they warned of the potential release of the stolen Salesforce data, writing in a forum post, "Stay tuned for 11:59 PM New York time on 10/10/2025." Figure 3 below further illustrates these latest developments.

Hello,

BreachForums was seized by the FBI and international partners today. This was inevitable and I am not surprised. Neither I and others involved with this group have been arrested. All our BreachForums domains were taken from us by the US Government a few days ago. The era of forums are over.

We have conducted a thorough incident response on the BreachForums infrastructure ever since the domains were taken:

- BreachForums latest database backup was compromised along with every single database backup since 2023 till now.
- All escrow databases were compromised ever since it's release.
- The backend servers itself were seized and destroyed.

In the simplest terms, we very likely got hacked by the US Government, considering their splash page is up on the BreachForums onion, it's a clear sign how everything in our control that they wouldn't have been able to reach is gone.

For your own safety, security, and sanity keep your opsec in check. I have no doubt the FBI and other international partners involved will be cracking down on many individuals in the next coming few weeks to months.

Over the years, BreachForums has undergone significant turbulence. To my count this is the 4th time, including RaidForums seizure that the FBI has took action, consistently. We are not fighting this war anymore, this is officially the end.

To confirm a mild conspiracy theory brought up by multiple individuals and some security researchers over time:

The following is not common knowledge among the general community and public but when RaidForums was seized and BreachForums max launched shortly after, pompompurin was just a front. We all carefully planned the launch of BreachForums since day 1, ever since then everything has went to complete shit because of unforeseen circumstances and situations. Which lead me to coming out publicly in 2023 and owning the forum along with Baphomet, again, unforeseen circumstances lead to the seizure once again in 2024. Now were here. Ever since the beginning, nothing good has come from this. BreachForums is never coming back, if it comes back, it should immediately be considered a honeypot.

There is not much to say about this seizure but one thing to note is, the recent action the US Government has took against us, has no impact on our Salesforce campaigns. The fact that our DLS was also hosted on BreachForums clearnet domain and because we planned to re-open the forum to leak the data of companies who have not complied with us when the deadline arrived onto the re-opened BreachForums was likely the cause of todays seizure.

Time to move on, stay tuned for 11:59 PM New York time on 10/10/2025!

Media enquiries: shinycorp@tutanota.com, shinygroup@onionmail.com

-- ShinyHunters / BreachForums Administration Team

Figure 3. Screenshot of forum post by Bling Libra. Source: [BleepingComputer](#).

Regardless of what happens with this situation, there appears to be a shift occurring across the cybercrime ecosystem. Cybercriminals seem to be moving toward partnering with and monetizing their intrusion operations via an EaaS provider rather than via a RaaS provider.

One factor behind this shift may be greater potential to fly under the radar. Law enforcement attention in recent years has focused on disrupting ransomware operations. EaaS involves slightly different TTPs (e.g. no encryption and operational disruption) and may therefore avoid some of those efforts.

Risks to Retail and Hospitality Organizations

As someone who focuses directly on supporting retail and hospitality organizations as part of my role at Unit 42, I want to highlight the risks associated with this data theft extortion activity.

From a retailer perspective, the theft of customer data can lead to outcomes such as identity theft. It can also enable social engineering attacks, account takeover and various types of fraud. Most importantly, however, is the potential erosion of consumer trust. This is something that retailers can ill afford to suffer with tightening margins and the upcoming peak shopping season.

From a hospitality perspective, many of the issues remain the same as above.

However, I see a distinction in terms of potential fraud. Retail organizations would primarily be targeted with tactics like returns and gift card fraud. Hospitality organizations are more likely to be targeted with tactics like loyalty rewards fraud (e.g., airline miles, hotel points).

These tactics are influencing the growing [underground trend of fraudulent travel agency advertisements](#). For example, stolen loyalty rewards can be used by threat actors to book travel arrangements (e.g. flights, hotels)

which they can resell to unsuspecting customers at a discounted rate and reap the profit from such transactions. Many of these fake travel agencies are advertised across underground cybercrime forums and Telegram channels.

My Recommendations

Unit 42 recently published a threat brief on the repercussions from the [Salesloft Drift supply chain attack](#), which includes recommendations that apply to supply chain attacks more broadly. We've also published on [best practices for token and integration management](#) as they relate to the supply chain.

Both Scattered Lapsus\$ Hunters and Crimson Collective are focusing their data theft and subsequent extortion efforts on platforms like Salesforce and AWS. To combat this, organizations should leverage automated tools like [TruffleHog](#). These can help efficiently scan for secrets and hardcoded credentials within code repositories, configuration files or any potentially exfiltrated data.

Additionally, organizations should implement zero trust pillars, such as conditional access policies and the principle of least privilege, to limit the damage attackers can do even if they are successful at breaching your network.

Finally, make sure your organization is a member of an industry-aligned Information Sharing and Analysis Center (ISAC). For example, retail and hospitality companies should join and participate within the [RH-ISAC](#), where members get access to real-time threat insights and best practices that can assist with both reactive and proactive defensive measures.

As always, the [Unit 42 Incident Response team](#) can also be engaged to help with a compromise or to provide a proactive assessment to lower your organization's risk related to the aforementioned threat activity.

Source: <https://unit42.paloaltonetworks.com/scattered-lapsus-hunters/>