A Look Back at the Top Ransomware Attack Targeting the Salesforce Supply Chain

Table of Contents

Executive Report

SOCRadar named the top 10 ransomware attacks of 2025, and guess which led the pack? The Salesforce SaaS supply chain attack that affected the company's customers in the technology, aviation, and luxury sectors. Reports revealed that the Scattered Lapsus$ Hunters, a combination of Scattered Spider and ShinyHunters, were behind the campaign that transpired in mid to late 2025.

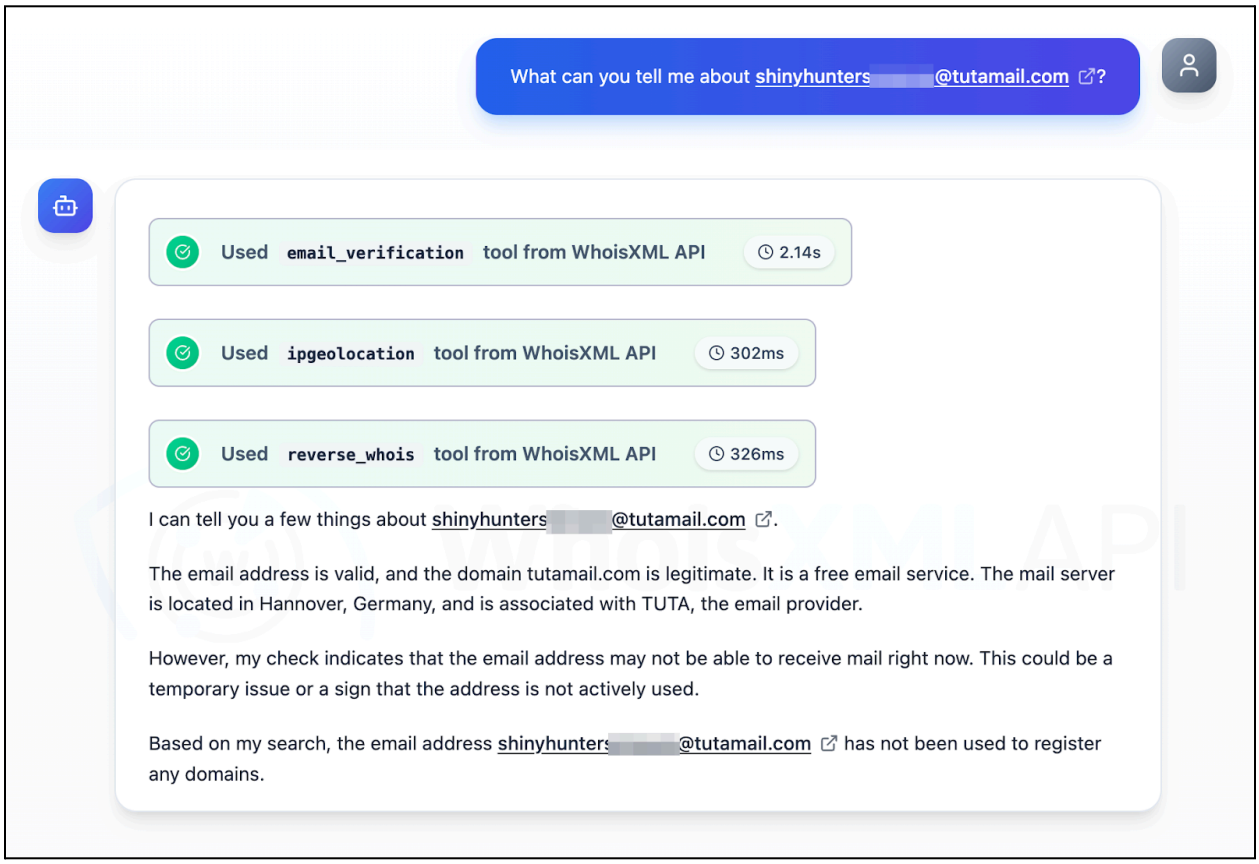
The attack exposed tens of millions of customer records and caused multisectoral operational disruption. And the threat actors got hold of OAuth tokens, CRM data, customer records, and support and travel data.

Jumping off two lists of IoCs published by LevelBlue and Seqrite, we compiled five domains, 33 IP addresses, and three email addresses. We excluded two domains, however, since they belonged to legitimate entities. That said, we analyzed 39 IoCs in the end, which led to these findings:

- One domain tagged as an IoC was deemed likely to turn malicious 76 days before being dubbed as such
- 1,722 potential victim IP addresses communicated with 24 IP addresses identified as IoCs
- 405 email-connected domains, four of which turned out to be malicious
- Two additional IP addresses, both of which turned out to be malicious
- 11 IP-connected domains
- 7,900 string-connected domains, six of which turned out to be malicious

Examining the Email IoCs

We examined the three email addresses identified as IoCs by querying them on Jake AI. The tool revealed that while they were all valid email addresses, they could not receive messages at present. None of them have also been used to register any domain, excluding them from our hunt for new artifacts.



Jake AI query result for one of the email addresses tagged as an IoC

Diving Deeper into the Domain IoCs

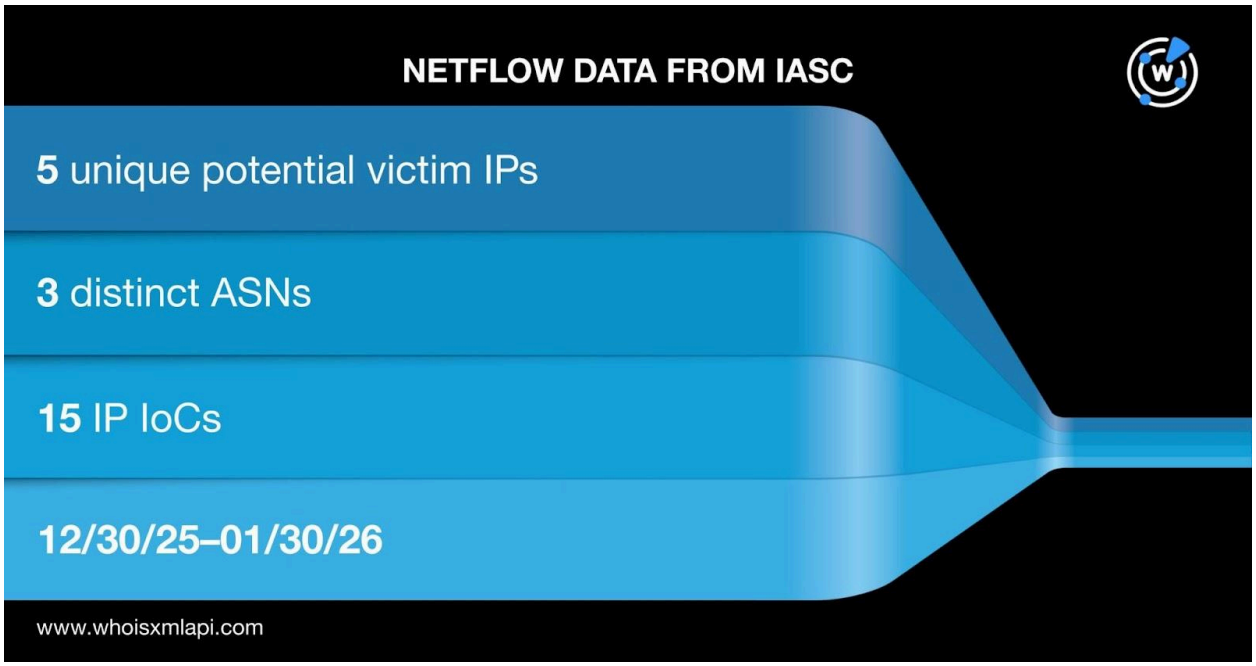
Our First Watch Malicious Domains Data Feed findings revealed that one domain identified as an IoC—ticket-audemarspiguet[.]com—was registered with malicious intent on 20 June 2025, 76 days before the Seqrite report was published on 4 September 2025.

Next, we queried the three domains tagged as IoCs on WHOIS API and found out that they were created at around the same time, between 20 and 29 September 2025, with GMO Internet in Seychelles.

The results of our DNS Chronicle API queries for the three domains identified as IoCs supported our WHOIS findings above. Together, they posted 28 domain-to-IP resolutions over time. The domain ticket-audemarspiguet[.]com recorded the earliest resolution on 20 June 2025. The domain ticket-nike[.]com, meanwhile, posted the highest number of resolutions totaling 20 so far. Finally, the domain ticket-dior[.]com recorded the latest resolution on 29 June 2025. All these dates coincided with the three domains' creation dates, too.

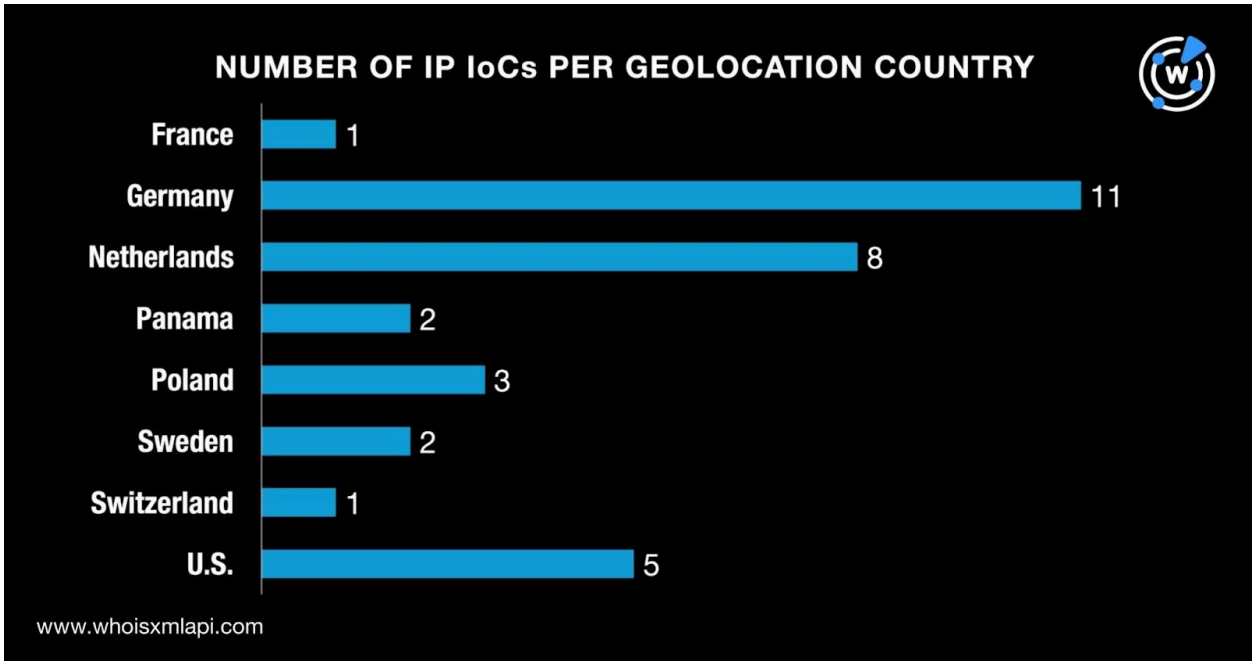
Investigating the IP IoCs

Sample network traffic data from the IASC showed that 1,722 unique potential victim IP addresses under 152 distinct ASNs communicated with 24 IP addresses tagged as IoCs between 30 December 2025 and 30 January 2026.

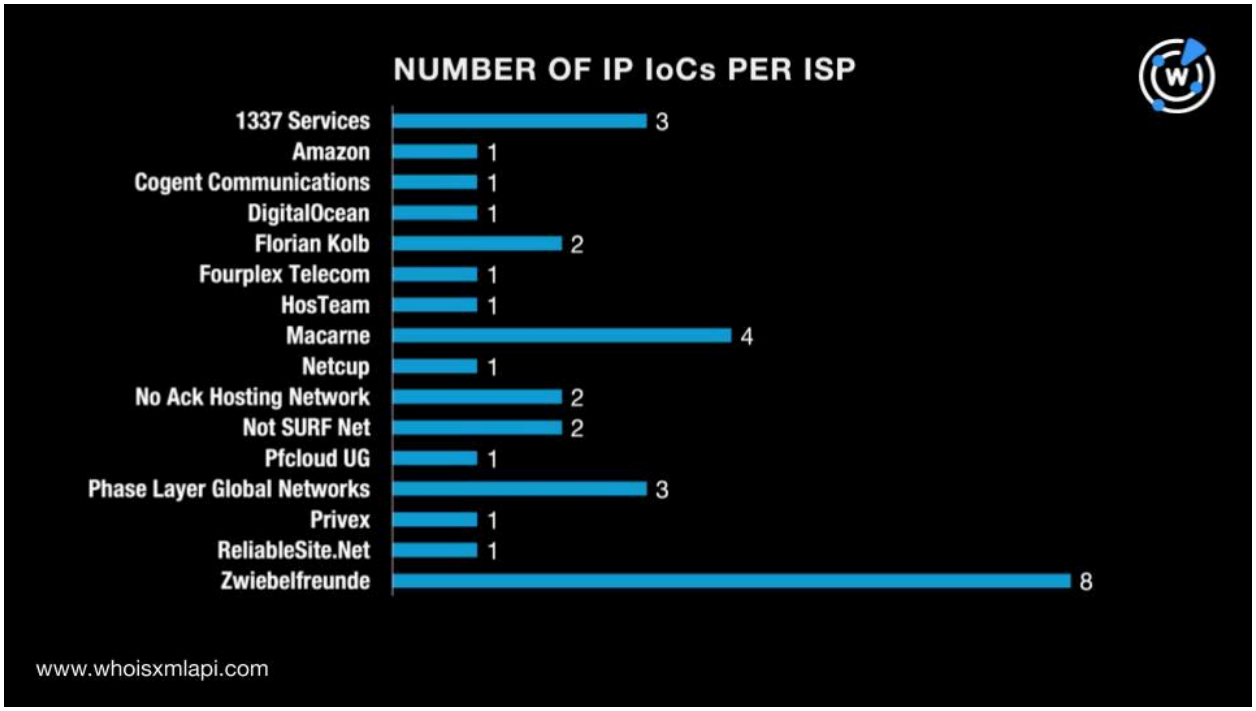


We then queried the 33 IP addresses identified as IoCs on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in eight different countries. Interestingly, the Seychelles—the registrant country of all three domains tagged as IoCs—was not in the list of geolocation countries.



- They were administered by 16 different ISPs with the majority (eight in all) managed by Zwiebelfreunde.



Next, we queried the 33 IP addresses tagged as IoCs on DNS Chronicle API and found out that only 25 had historical IP-to-domain resolutions over time. Together, they recorded 3,370 in all.

The IP address 208[.]68[.]36[.]90 posted the earliest resolution as far back as 7 February 2017. Here are a few examples.

IP IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
208[.]68[.]36[.]90	383	02/07/17	10/12/25
185[.]207[.]107[.]130	382	02/25/18	12/24/25
192[.]42[.]116[.]20	374	06/11/18	09/21/25
81[.]17[.]28[.]95	185	10/12/18	02/09/24
31[.]133[.]0[.]210	9	11/09/18	06/26/22

Scouring the DNS for New Artifacts Tied to the 2025 Salesforce Supply Chain Attack

Our hunt for new connected artifacts started with WHOIS History API queries for the three domains identified as IoCs. We discovered that they had two unique email addresses in their historical WHOIS records. Both were public email addresses.

The results of our historical Reverse WHOIS API queries for the two public email addresses led to the discovery of 405 unique email-connected domains after those already tagged as IoCs were filtered out.

Threat Intelligence API queries for the email-connected domains showed that four have already been weaponized for attacks. The domain join-meets[.]com, for instance, has been associated with malware distribution from 28 July 2025 to 24 January 2026.

After that, we queried the 33 domains tagged as IoCs on DNS Lookup API and uncovered two unique IP addresses not on the list of IP IoCs.

According to Threat Intelligence API, both additional IP addresses have already figured in various attacks. The IP address 104[.]21[.]78[.]124, for example, was associated with malware distribution (29 October 2024–24 January 2026) and phishing (28 March 2023–29 November 2025).

Given the 33 IP addresses identified as IoCs and the two additional ones found above, we now had 35 for further analysis. Our Reverse IP API queries showed that 10 could be dedicated

hosts. Together, they hosted 11 unique IP-connected domains after those already tagged as IoCs and the email-connected domains were filtered out.

Next, we looked more closely at the three domains identified as IoCs and deemed that they all started with the text string **ticket-**. Our Domains & Subdomains Discovery searches for the string led to the discovery of 7,900 unique string-connected domains after those already tagged as IoCs and the email- and IP-connected domains were filtered out. Here are a few examples.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
ticket-aviata[.]info	Malware distribution	03/09/23	01/24/26
ticket-escrow[.]com	Phishing	01/10/26	01/11/26
ticket-frankfurt[.]de	Phishing	10/03/25	12/04/25

Conclusion

Our search for traces that the Salesforce supply chain attack of 2025 left behind in the DNS uncovered 8,318 new artifacts comprising 405 email-connected domains, two additional IP addresses, 11 IP-connected domains, and 7,900 string-connected domains.

We also discovered that one domain tagged as an IoC was deemed likely to turn malicious 76 days before being dubbed as such. Finally, 1,722 potential victim IP addresses communicated with 24 IP addresses identified as IoCs.

If you wish to learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample Email-Connected Domains

- 1pay[.]digital
- 2x-prague[.]com
- adilteam[.]world
- ag-app-swap-web3[.]com
- ag-chain-app[.]com
- balancedsaving[.]com
- balesciagagap[.]live
- basicslearning[.]com
- caesarus[.]bet
- candycoursesjp[.]com
- casesimulator[.]pro
- dastiwejff[.]xyz
- de-miles-and-more[.]com
- deliveryapprevievvs[.]com
- edevletdestek[.]com
- educationtreasury[.]com
- ekaldring[.]run
- fb-trackonline[.]com
- fi-defi-connect[.]com
- fi-fast-defi-chain[.]com
- global1[.]space
- global2[.]space
- global3[.]space
- hax[.]bet
- helpppl[.]com
- highcoin[.]org
- icarusander[.]icu
- id-szkb[.]digital
- infhotsec[.]com
- jaded[.]icu
- jobassistancehub[.]com
- jobclaimroute[.]com
- karty[.]live
- kecheckm[.]xyz
- killmail[.]xyz
- labubushop[.]life
- learnbytreasury[.]com
- learningsavings[.]com
- makeupsinjp[.]com
- mallcheks[.]xyz
- martin592casino[.]top
- nanoteck[.]digital
- nbg-acess[.]life
- nbg-gr[.]life
- onchain-criteria[.]net
- online-connectref[.]top
- online-dib[.]com
- parabaza-shop[.]com
- partbokprosec[.]com
- pass-drake[.]com
- relayportal[.]top
- relayswap[.]top
- reprogrammer-locker[.]info
- saveandstructure[.]com
- savingsedu[.]com
- scamreport[.]top
- t-gkapple[.]life
- t-misticglaz[.]life
- t-mysticc[.]life
- unicrediteurope[.]digital
- unicrediteurope[.]online
- us01web[.]com
- vasek[.]run
- vcita[.]net
- vcrypto[.]global
- walletbybit[.]org
- walletbybit[.]pro
- walletbybitaudit[.]com
- xrrpbroaadd[.]com
- xrrpbroaads[.]com
- xyz-check-walelt-v3[.]com
- zerolinkdev[.]top

- zkb-online[.]digital
- zkbonline[.]digital

Sample Additional IP Address

- 104[.]21[.]78[.]124

Sample IP-Connected Domains

- 176[.]65[.]149[.]100[.]ptr[.]pfcloud[.]network
- dfghrtht[.]camdvr[.]org
- rdtrdr[.]camdvr[.]org
- tools[.]bobo2[.]synology[.]me
- yuhk[.]mypi[.]co

Sample String-Connected Domains

- ticket--attraction[.]co[.]uk
- ticket--direct[.]de
- ticket--master[.]com
- ticket--restaurant[.]site
- ticket--s[.]com
- ticket-000[.]com
- ticket-0001[.]info
- ticket-0005[.]info
- ticket-0009[.]info
- ticket-01[.]com
- ticket-01[.]shop
- ticket-04[.]com
- ticket-06[.]com
- ticket-078[.]cloud
- ticket-08[.]com
- ticket-09[.]com
- ticket-1[.]com
- ticket-1[.]de
- ticket-1[.]eu
- ticket-1[.]org
- ticket-1[.]ru
- ticket-1[.]us
- ticket-10[.]com
- ticket-1000[.]de
- ticket-1002[.]info
- ticket-1004[.]info
- ticket-101[.]ca
- ticket-101[.]com
- ticket-1010[.]info
- ticket-1014[.]info
- ticket-1015[.]info
- ticket-1017[.]info
- ticket-1021[.]info
- ticket-1022[.]info
- ticket-1028[.]info
- ticket-1029[.]info
- ticket-1031[.]info
- ticket-1033[.]info
- ticket-1034[.]info
- ticket-1036[.]info
- ticket-1038[.]info
- ticket-1040[.]info
- ticket-1041[.]info
- ticket-1042[.]info
- ticket-1045[.]info
- ticket-1046[.]info
- ticket-104618-coinbase[.]com
- ticket-1049[.]info
- ticket-1050[.]info
- ticket-1052[.]info