Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

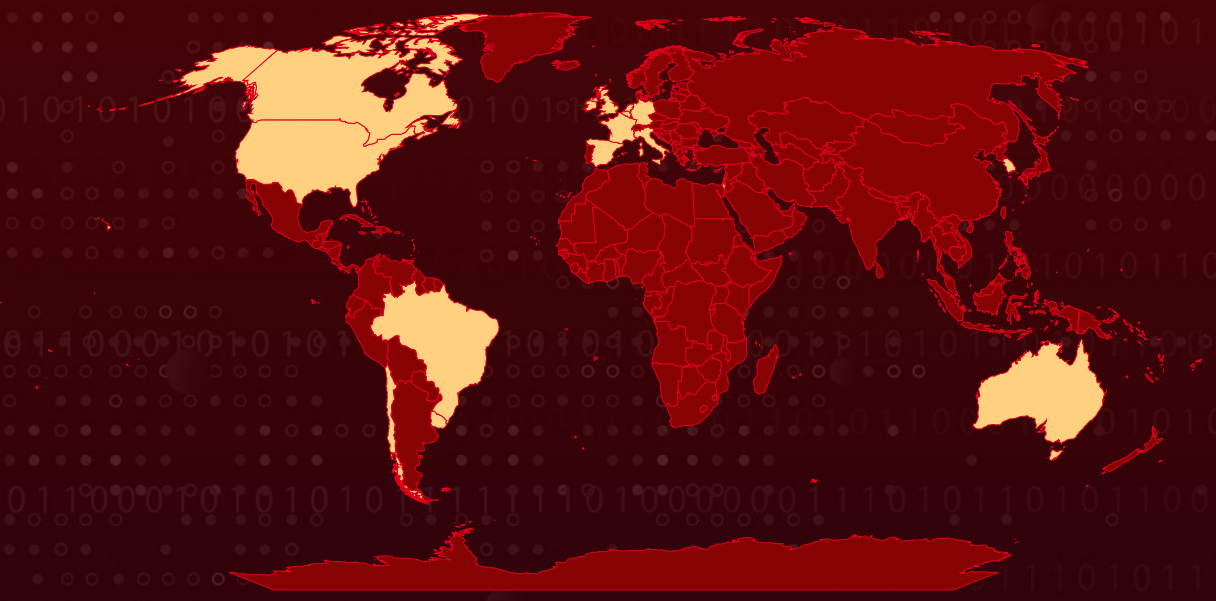
Brand Hijack in Cybercrime: Who Is Pretending to Be ShinyHunters?

Date of Publication	Admiralty Code	TA Number
April 20, 2026	A1	TA2026107

Summary

First Seen: August 9, 2025
Targeted Regions: United States, United Kingdom, France, Australia, Italy, Netherlands, South Korea, Spain, Chile, Uruguay, Canada, Brazil, Israel, Ireland, Singapore, Germany, Belgium
Targeted Platforms: Okta, Microsoft Entra / Azure AD, Salesforce, Microsoft 365, SharePoint, OneDrive, Google Workspace, DocuSign, Slack, Workday, Zendesk, Amazon S3, GitHub, GitLab, BrowserStack, Jira, Azure DevOps, VPN concentrators, firewalls, Citrix, RMM tools, Oracle Access Manager, Oracle E-Business Suite, SAP NetWeaver
Targeted Industries: Airline, Aviation, Retail, Telecommunications, Financial Services, Banking, Insurance, Technology, Hospitality, Gaming, Education, Media, Food and Beverage, Automotive, Manufacturing, FinTech, Government, Energy, Professional Services, Healthcare, Casino & Gambling, Transportation, Real Estate, Charitable Organizations, Legal
Threat Actor: Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)
Malware: LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys
Attack: Scattered LAPSUS$ Hunters (SLH) is a federated cybercriminal brand that leverages the reputational capital of Scattered Spider, ShinyHunters, and LAPSUS$ to operate a large-scale, cloud-first data-theft and extortion business. The group's notoriety has also drawn copycats and impersonators, with unaffiliated actors falsely claiming ShinyHunters membership on Telegram and data-leak sites, complicating attribution. Once inside, they pivot across connected SaaS applications, exfiltrate large volumes of customer and business data via OAuth-authorised APIs and PowerShell, and then extort victims with seven-figure ransom demands, public shaming on ShinyHunters-branded data-leak sites, DDoS attacks, and harassment of employees. The group also markets an Extortion-as-a-Service offering and has teased a "Sh1nySp1d3r" ransomware program targeting VMware ESXi.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver	✓	✓	✓
CVE-2025-61882	Oracle E-Business Suite Unspecified Vulnerability	Oracle E-Business Suite versions 12.2.3-12.2.14	✓	✓	✓
CVE-2021-35587	Oracle Fusion Middleware Unspecified Vulnerability	Oracle Access Manager product of Oracle Fusion Middleware affected are 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0.	✗	✓	✓

Attack Details

#1

ShinyHunters is a financially motivated cybercriminal group that targets businesses, organizations, and government systems. Their operations rely primarily on social engineering rather than direct exploitation. They impersonate internal IT staff through voice phishing, directing employees to fake login pages or persuading them to approve malicious access. Once inside, they deploy infostealer malware such as LummaC2, StealC, RedLine, Meduza, Rhadamanthys, and Vidar to extract sensitive data, including credentials, personal records, and financial information.

#2

Their entry method is precise. After capturing login credentials and one-time MFA codes, they immediately register their own devices to maintain persistent access while suppressing security alerts. In some campaigns, they have demonstrated deeper technical capability, claiming access to exploits such as CVE-2025-31324 in SAP NetWeaver and CVE-2025-61882 in Oracle E-Business Suite. Earlier activity linked to the "Yukari" persona involved exploiting CVE-2021-35587 in Oracle Access Manager to extract data from Oracle 12c systems. Alongside this, they manipulate legitimate workflows, such as authorizing modified Salesforce applications to gain OAuth-based access.

#3

Once inside, their movement depends on available privileges. A single compromised identity system can provide access to multiple services, including Salesforce, Microsoft 365, SharePoint, Slack, and cloud storage platforms. They extract large datasets, remove logs to limit detection, and use compromised accounts to expand attacks. Access is often extended further through stolen API keys and tokens, enabling entry into development tools and internal repositories. Proxy networks, VPN services, and recruited insiders help obscure their activity and scale operations.

#4

Data theft drives their operation. They target high-value information such as customer records, communication logs, and internal documents, filtering data with specific keywords before exfiltration through APIs or cloud services. Victims are then pressured with ransom demands, supported by public leaks, DDoS attacks, and direct outreach to employees. Some datasets are sold individually, with prices reaching up to $1 million.

#5

A separate actor, "DB+ Collector," appears to impersonate the group rather than operate within it. This entity does not conduct intrusions but resells previously stolen data and credentials gathered from infostealer logs. The risk it presents is exposure of compromised credentials rather than direct system breaches. Impersonation extends further. Some actors claim association with ShinyHunters within a broader alliance alongside groups like Scattered Spider and LAPSUS$. However, ShinyHunters has publicly denied operating sales channels, indicating that many of these claims are attempts to exploit their reputation rather than evidence of legitimate affiliation.

Recommendations

Enforce Phishing-Resistant MFA Everywhere: Deploy FIDO2 security keys or passkeys for all workforce accounts and particularly for high-privilege users of SSO-integrated applications. Push notifications, SMS, and TOTP codes are all trivially captured through the vishing workflows used by SLH operators, whereas hardware-bound credentials cannot be relayed through a fake help-desk call.

Harden Okta and Microsoft Entra Administrative Controls: Limit the number of Super Admin, Organization Admin, and Global Admin accounts, enforce Just-in-Time elevation for sensitive operations, and continuously audit authentication logs for anomalous sign-ins from anonymized IPs, Tor exit nodes, or residential proxy networks.

Restrict Salesforce Connected Apps and Data Loader Permissions: Allowlist only vetted Connected Apps, remove the "API Enabled," "Manage Connected Apps," and mass-export permissions from general users, require admin approval for new OAuth authorisations, and define trusted IP ranges on user profiles and connected apps so that unknown or commercial-VPN networks are blocked or challenged.

Patch SLH-Targeted Internet-Facing Applications: Prioritise remediation and compensating controls for CVE-2025-61882 (Oracle E-Business Suite), CVE-2025-31324 (SAP NetWeaver), and CVE-2021-35587 (Oracle Access Manager), all of which SLH members have publicly claimed to exploit or broker.

Rotate and Audit Third-Party OAuth Tokens: Review every connected SaaS integration, particularly Salesloft Drift, Gainsight, Mixpanel, and similar revenue- or analytics-layer applications for unused scopes or dormant tokens, and rotate API keys and access credentials created by engineering teams in BrowserStack, GitHub, GitLab, Jira, and Azure DevOps.

Detect Post-Compromise OAuth Abuse and MFA Hiding: Hunt for unauthorised OAuth authorisations in Google Workspace (for example, ToogleBox Recall), soft-deletion or hard-deletion of Exchange messages whose subject lines contain "new MFA," "security method enrolled," or equivalent strings, and creation of new cloud-identity accounts outside normal change windows.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
		T1583.006: Web Services
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.004: Spearphishing Voice
	T1078: Valid Accounts	
	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
	T1195: Supply Chain Compromise	
Execution	T1204: User Execution	T1204.001: Malicious Link
	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Persistence	T1136: Create Account	T1136.003: Cloud Account
	T1098: Account Manipulation	T1098.005: Device Registration
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1134: Access Token Manipulation	
Defense Evasion	T1578: Modify Cloud Compute Infrastructure	T1578.005: Modify Cloud Compute Configurations
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token

Tactic	Technique	Sub-technique
Credential Access	T1110: Brute Force	
	T1111: Multi-Factor Authentication Interception	
	T1528: Steal Application Access Token	
	T1539: Steal Web Session Cookie	
	T1555: Credentials from Password Stores	T1555.006: Cloud Secrets Management Stores
	T1552: Unsecured Credentials	T1552.001: Credentials in Files
	T1003: OS Credential Dumping	T1003.003: NTDS
Discovery	T1518: Software Discovery	
	T1526: Cloud Service Discovery	
Lateral Movement	T1210: Exploitation of Remote Services	
Collection	T1213: Data from Information Repositories	
	T1119: Automated Collection	
	T1074: Data Staged	T1074.002: Remote Data Staging
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	
	T1090: Proxy	T1090.003: Multi-hop Proxy
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
	T1041: Exfiltration Over C2 Channel	
	T1020: Automated Exfiltration	

Tactic	Technique	Sub-technique
Impact	T1657: Financial Theft	
	T1565: Data Manipulation	
	T1486: Data Encrypted for Impact	
	T1498: Network Denial of Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	24[.]242[.]93[.]122, 23[.]234[.]100[.]107, 23[.]234[.]100[.]235, 73[.]135[.]228[.]98, 157[.]131[.]172[.]74, 149[.]50[.]97[.]144, 67[.]21[.]178[.]234, 142[.]127[.]171[.]133, 76[.]64[.]54[.]159, 76[.]70[.]74[.]63, 206[.]170[.]208[.]23, 68[.]73[.]213[.]196, 37[.]15[.]73[.]132, 104[.]32[.]172[.]247, 85[.]238[.]66[.]242, 199[.]127[.]61[.]200, 209[.]222[.]98[.]200, 38[.]190[.]138[.]239, 198[.]52[.]166[.]197, 191[.]96[.]207[.]179, 196[.]251[.]83[.]162, 163[.]5[.]210[.]210, 94[.]156[.]167[.]237, 23[.]94[.]126[.]63, 198[.]244[.]224[.]200, 163[.]5[.]169[.]142

TYPE	VALUE
Domains	admiring-shockley[.]196-251-83-162[.]plesk[.]page, bless-invite[.]com, get-carrot-zoom[.]com, modernatx-zoom[.]com, recurly-zoom[.]com, sharepoint-comcast[.]com, workday-nike[.]com, workday-hubspot[.]com, sharepoint-workplaceview[.]com, newscorp-okta[.]com, corporate-microsoft[.]com, okta-louisvuitton[.]com, corporate-okta[.]com, pure-okta[.]com, morningstar-okta[.]com, sts-vodafone[.]com, corp-hubspot[.]com, signin-okta[.]com, bmcorpuser[.]internal-okta[.]com, help-allvuesystems[.]com, allvuesystems-okta[.]com, shinyhunte[.]rs, breachforums[.]hn
SHA256	9eb3236d8299927a2d714a54dcde090928ea5a9ef86cf04163b05bf2acb5d13e, c8eaa77c17c91d5d9c9cb2601fde4b2cfff8124113c755e3abc70dc2dde418b8, 03eccfa5dea23fc185bcca277520d7ef473ff752649aac485ac055dd4111b2c1, dc5fc48cbd764acf7dd28c385279cf8b4296fb2d1e7b9aca3bc2352893194c94, 1e92acabf037a60e7fbb97c0ba73e997bb4b602ad51333871423b778cae4f0b1, 014db9057094603d58b0a9a917e3643220bcdb594be28437fcb26fb3d5c39de9, 68c4b56a3aeac907d39a09ec6b53c252393cc68b69ffe9c553be893b2e7bd2a8, b6aa024e2681961c93d29f8600baa935b545e274db48eb832de1f3dea17db546, ad1d476e0f07d67f1fd670ba4a7227794f436c1fa01f08a2cdcd57f2f7d1be51, 7ac90091d7037384ca3dc9a7a0459e3875e976496b3afd9a6a81ad6ace0ba002, 821ca194a12d0085b5ea043efc6417e53227244da585af0bcc8995e1946cbebd,

TYPE	VALUE
SHA256	a1d9659e8f9df7dbcfebec0faafadeec8b43e0e5d0818aab0d63d0815490bce5, c42b0d200c2022fba3332dd1078cf1412ba37eb52bd74acf7edb4672b1d0f330, 65e1a8e550df1000eb91a7b679cf586efab0f24385b810f50349d50eb80ae806, b1b8ea15e6bbfc7c38eb394d7e81a99a93689464faf991d77e28722e5b0e4681, 194b8a204fa49ebeb6788ff2d3296251a0083331a4495e154c0c6012bcaa6cd7, bdabfcabcd75d8450c7982310542bbb78df553cee98fdfe56919fdaa2b10af84, e69961d10df9e57bc9bd9a230903c52b020eed6cda03ff17127a556c6e07f0a9, 82cb239612d74eab70b12a0ca448bd82b3c5b418b8f05213d75ddddbbf0b4a5d, a5ebf3f3762dc01bca3696993961927ec6aa376c7246b88089eba88f039d69d5, 4630f2e42c67690b34c187feee43eabe447c935dea079b5bf1c480de070d097c, aa3df8b8bf546c07264c7f5f91790b25e83359317483e2f0f42aa11cb4ab29f7, e8d1c4f4cea682bee4ba4105f14bab0f6bcec51727080e1bc76993fa82f214fa, 5dda23dea89feea09086361d99a9dc1c04f1a2e552a2f5f52cb83d2d8e4e11f8, 9c9306c968318a95791dee86bbc6c16f6b1d0f53b5b7d682c2a48a5c6cc1a75e, aebd5e547d9d38dfcf2030986605a800de9f0cdcf27e0d3906b9a00812159870, 8c10f794a46fb4dcb0a0a2b4ef9c8980f332e9487dd3200cfb3da2e0d2c2df38, a85528d4fcbc101d6c0fc37aad3e1859ad6e8a2556883900627f5e5f455f4f0d, 2fc2dbfc4d287d1cc2fd6021c2b8285f96b8ae83710a7f6cd301ff53418422f4, 6a37fb22ba4cf331c954a84f31a730bce22d16a8b86833488c0724f50a338fe7, d6bc2b0f5899b66f3e21c6f8616c02aa218b6fbf292e9131da0414badacfe62e, fafe7d66e5bd7b863c859d329c390978d7e2db8627664e1427f7f184ba7dc24e, 9bc696c7c68c2c31cd431ed0af9264fe056942923399b1adb4c55241639bc835,

TYPE	VALUE
SHA256	908548cb94a13710b0668aca7ef2045da8ba4443e9edcae7a46e93900856d1a3, a5f2f3c199df73e31969d96acc46694759792ba294c6311d37bb7b72f5e54fde, 8a203721f1f1ca0d1026969363b9182a42aade9766d0cb2e296965182b76628d, 2249197c31828fc399259ec0264df1eec433a0294253b121616c265b9bcb198b, 2645970960a371b535d69137952599f3577b193594e1266b8e6f6d8c9521f024, 24169a2e792caa88dea3ded0931e30d920a6bb374920f0ad89ab4eb598ac3565, 98ab57ac192335e03016f40e6d1fd05f267fec8c15840ae64ca0ebee2bd10807, af654dfab98e93b7e203c08db19901eab6f7dfc70b71e5a0eec87a3ba9b92a09, 7d737a69ae779654371aff951a05311b38962e87498cda335a6a8f8a803d86ce, db3a352fd93106437a6a700fea49d1d0403b11d7859155ecfd3a1e2a707db14f, c57923aa08a4903064963b19701b292d649cc5c5e16cdf7741f4724ba77e45dc, 90522e6a880f6a97719035e3945da1c0c0384f154cf631732ea16a3a9f827b7c, c41873f177a61ec1e1cb628db96cddd70204b8a530e392bf210d7d4136be7375, f9056423f67ae129475439f61196d0984078f779d819b2af21c33ca45aea3fa9, 980d48f8f67dd065958d6c970572e7cda506423d45c591c0b2f4e1d8abea71b9, 927b40ed84cc687f71dd8df218c5ac8472db12421487f69de84b26de2f061eb7, e740a5b0731edc97334f8d4c9fd75ba79bdc161a381ffe643aee86c7d79451eb, 69587ec2c3e810dc6fca35c13341907fe7a96a24a4222589b72ef97b80e820f4, 95ee8a666f65df5de6328f9f0069e04018e1831ea6d7712f06b6bee804cd86ac, 056db50822f884eb4e4f36d5f2c4dd842718e4597ce79a7b6a80d2e71c020c9d, 7c7d8541766ddad17d9735ed7183d3d7e3433ea580258ed89f465fc8e91d3b82, c1354dcaa9389550c2013e23418bb5c71474b6c368f8e68e51e31faa64ba4ea1,

TYPE	VALUE
SHA256	58062bd86e000442f67b3f48bf9106c5a034917e6c198bcfc7065b083c1485c9, e1421a23f843ee01269aa82ea80d1fb517ea7e5eca28f06990e8658fd2849784, 2f74bff32ab2d757c7ff5e771be792eac495e84ec7e50cd7541e3fb8a1fdaf61, f9932b364f52c6fe0191e34ddcba772df8460bf579f422cabd93ca192bb3e1a6, a0a0668890035cec129a8cb361562910a319b29c63a5fa59654d4aa1c20d12db, 775678e2de0dcdb10f7689c5978f5a7b9d99c8d8d3ccb0a63175f4b78bf3da09, 5bfe42139157de0d0c73ccea8bbf24f8368444cfd5bb4b58300d902bbfa48848, 7955f285a2e64fcedc8a876dd5f753f781f2b346d81e0905dd1479c7c3e52609, 5db892a52fbebbf0298d3b5b2cf0c3ed7f9612a9d337c56bb168be336d28cadb, e0d8e7a12ffa3feb00814259a2ea750ab121c3f4b049ce82f5f3ec16579807c0, b9ad234abeb1490f2c2d28dd2387f0575ba5128ebb799741b1f3179622204175, 7faeb3f847830a2c52322565d8e73e07000003ccb54310790e10756cd3b2ff6b, 2a674a9a0acf0532c3816df01af80e8a95fd7530a30ca31664cf82d4ce639a56, 4532489becbdf07bc0a932486ab95b497113f5600c7646b635eaea9bcfa430cd, 8cd552392bb25546ba58e73d63c4b7c290188ca1060f96c8abf641ae9f5a8383, c7ca2f9065557a6d8fb0c02c75804d386b77ffca4466678b201c09e916afa096, b1c5d2eadbb2936f8b9644a5a4e24b5c54b163f0f2d6817c60edb3e5a73c6dc6, 0e94e5712d93d43423f3fec2f3a7f2b859d749411034c839c13e428f651f11a6, 087ab4fb9a7da5ae301b693818ae3a9e5844e1587cf6300f92c4d735c95b7c7c, 11231a29dbb5f9af8e17732fa1afecb99ca2059e3d08a4119b81cb60dabec3ba, 855858f60762102a7259fcf16b68fe84a2aecac91321ca82ed4bd433d61ca29e, b4c8fc082585c01b0ff64a7088e77ead33433f1a34251aef7f228d86b615b821,

TYPE	VALUE
SHA256	8661ed05a0580a8c9b06de1c6c9fccce98d910b17b95d66f1b3ff569831e3617, 9ab214c4e8b022dbc5038ab32c5c00f8b351aecb39b8f63114a8d02b50c0b59b, f26749f8e2835fb875241cdc8fddc708016062256435ef42689a2a28465ecdf7, 4d8030d543b659e5356873c365472e183f0dc3e71be3cdb3e1f16e546793081a, 3b9d0e62c06caeaf4244ff2fb275a1919fd9e14243fb436dce313c8d9b89faa4, 1682a7f8f229e62c379fca3c6c989c748aef985e51fc6bcf76d06bde9b0484cf, 0383c0d109b7cfdef058b0197125c85d276510724be33a746056f9a7c181d761, e5c5617c8676e9a5cf6108d344fe7fcb6590671efd6baccb02b9313da0f0d289, 36de93aaf26727f6dd55ff2100b08dfb52abccfb57a7bf4d07a7fb703a86623d, 6aa51de51a6b352fd073b5b9080011d358d42fa190a8a9ee216e3ef6e657b801, 4e20f2c4c90e3654a8c43fb10003978d61d2b48426414dede3b1bd5a2c891b54, ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b, 0e90c63363265f75f8637c1a3e9ec277a1ea1a8436dd7561fff59cfb722c6612, eb8a15b1a42127970e7facc6133131dcc073a201419d8cc88c3c316819d1c2a2, 9e2b8c3888b8a93e8ebab39e7a6b636f921888edb7d15a6ab56b2e119693aaa8
TOR Address	shinypogk4jjniry5qi7247tznop6mxdrdte2k6pdu5cyo43vdzmrwid[.]onion
Email	shinycorp[@]tutanota[.]com, shinygroup[@]onionmail[.]com
qTox ID	BD1B683FD3E6CB094341317A4C09923B7AE3E7903A6CDB90E5631EC7DC1452636FF35D9F5AF2
Bitcoin Address	bc1q5530apqz86eywm2f84mpcyuux3dv9mmztsdxt2
Monero Address	87cEqA6PunENHwe5h8XtRifWuDhNQXKwzGNSbwKmrdEehY4wjRjWvZmSgE8LHTe6e5Pmnuyyiu5AWbGCC9gHUzUj5KHnSH9

Recent Breaches

https://www.pitneybowes.com/us
https://www.7-eleven.com/
https://www.canadalife.com/
https://www.anodot.com/
https://www.carnivalcorp.com/
https://www.medtronic.com/in-en/index.html
https://www.aman.com/
https://www.alert360.com/
https://www.cyberark.com/
https://www.mheducation.com/
https://www.mytheresa.com/
https://www.kemper.com/
https://www.marcusmillichap.com/
https://ryan.com/
https://www.amtrak.com/home
https://www.salesforce.com
https://www.zenbusiness.com/
https://www.cisco.com/
https://www.hallmark.com/
https://european-union.europa.eu/index_en
https://www.berkadia.com/
https://www.ameriprise.com/
https://www.infinitecampus.com/
https://www.aura.com/
https://resultnetsearch.com/
https://www.cfgi.com/
https://www.vertexinc.com/
https://pathstone.com/
https://www.woflow.com/
https://www.odido.nl/
https://beaconpointe.com/
https://www.wynnresorts.com/
https://www.upenn.edu/
https://soundcloud.com/
https://www.figure.com/
https://www.betterment.com/
https://bumble.com/
https://www.carmax.com/
https://www.crunchbase.com/
https://www.canadagoose.com/ca/en/home-page
https://www.edmunds.com/
https://www.harvard.edu/
https://www.cargurus.com/

Patch Links

CVE-2025-31324:
https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

CVE-2025-61882:
https://www.oracle.com/security-alerts/alert-cve-2025-61882.html

https://www.oracle.com/security-alerts/

https://support.oracle.com/rs?type=doc&id=3106344.1

CVE-2021-35587:
https://www.oracle.com/security-alerts/cpujan2022.html

References

https://www.levelblue.com/blogs/spiderlabs-blog/scattered-lapsuss-hunters-anatomy-of-a-federated-cybercriminal-brand

https://blog.eclecticiq.com/shinyhunters-calling-financially-motivated-data-extortion-group-targeting-enterprise-cloud-applications

https://flare.io/learn/resources/chaotic-scattered-shiny-lapsus-spider

https://www.bugcrowd.com/glossary/shinyhunters/

https://www.darkowl.com/blog-content/actor-spotlight-shinyhunters/

https://www.salesforceben.com/shinyhunters-salesforce-data-theft-could-get-worse/

https://valicyber.com/resources/shinyhunters/

https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/shinyhunters-hackers-breach-googles-salesforce-0

https://cloud.google.com/blog/topics/threat-intelligence/expansion-shinyhunters-saas-data-theft

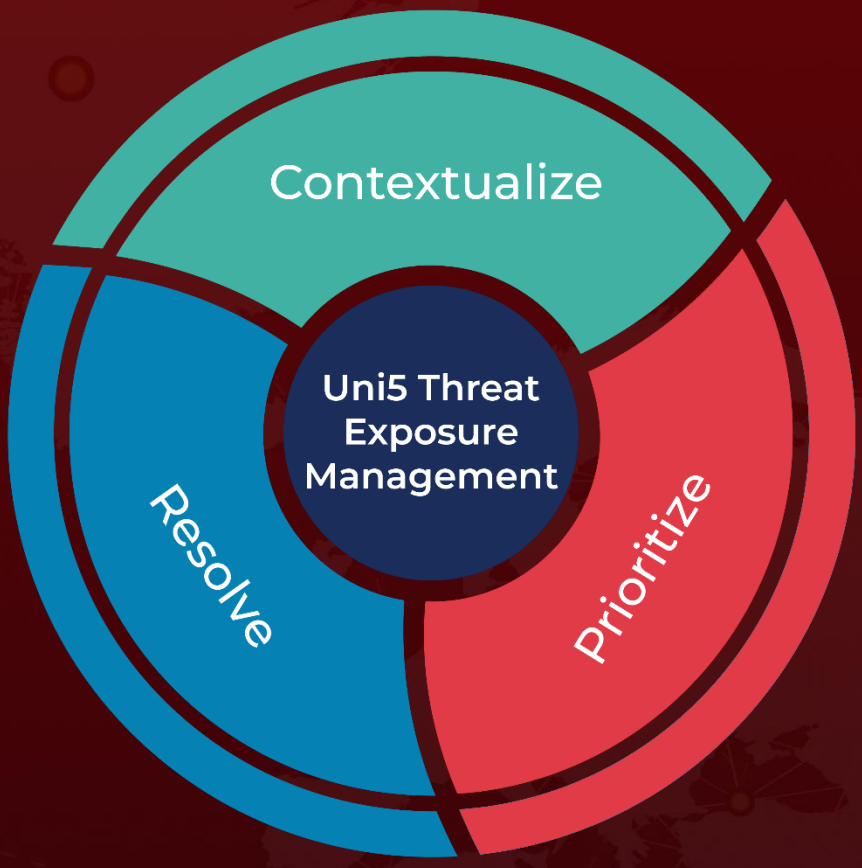
https://en.wikipedia.org/wiki/ShinyHunters

https://hivepro.com/threat-advisory/CVE-2025-61882:-Oracle-EBS-Zero-Day-Actively-Exploited-in-the-Wild/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 20, 2026 • 08:00 AM

More at www.hivepro.com