



| Brief |

The Underground Economist: Volume 5, Issue 18

B-2025-09-11b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

September 11, 2025

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 10:30 AM (EDT) on September 11, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 18

| Classified U.S. Military Information Advertised for Sale on Deep Web

On September 4, 2025, an actor using the alias “HorizonMonitor” posted on the deep web forum DarkForums, advertising access to top secret classified information related to the U.S. military. HorizonMonitor claimed to have an “after action report” document related to “Project Golden Dome,” which contains details of “Operation MSR-2/Flight Test 12,” allegedly conducted on August 2, 2025, at the Reagan Test Site in Kwajalein Atoll.

- Project Golden Dome almost certainly refers to a recently announced U.S. missile defense initiative that aims to establish a multi-layered shield by combining both space-based and terrestrial systems to intercept missile threats at various stages of their trajectory.¹
- Operation MSR-2/Flight Test 12 very likely refers to the document file name, wherein MSR stands for “Missile Segment Review”—a common acronym used in aerospace defense.
- The Reagan Test Site is a U.S. missile test range and tracking facility located in the Kwajalein Atoll, part of the Republic of the Marshall Islands in the central Pacific Ocean.


¹ [hXXps://apnews\[.\]com/article/golden-dome-missile-defense-trump-space-e74d637feac06edcfde79214d8acf179](https://apnews.com/article/golden-dome-missile-defense-trump-space-e74d637feac06edcfde79214d8acf179)

USA TOP CLASSIFIED INFO - TOP SECRET USSF AFTER ACTION REPORT RELATED TO GOLDEN DOME

onMonitor - 04-09-25, 03:30 AM

04-09-25, 03:30 AM (This post was last modified: 10 hours ago by HorizonMonitor)

#1



★ HorizonMonitor

V.I.P

Posts8

Threads1

JoinedSep 2025

Reputation6 days

This document is a Top Secret after-action report from the USSF on Project Golden Dome/Operation MSR-2/Flight Test 12, conducted at the Reagan Test Site in Kwajalein Atoll on 02/08/2025.

It details a successful test of the SENTINEL space-based sensors and KESTREL interceptors against two ICBM surrogates and a hypersonic glide vehicle, all of which were intercepted in boost phase.

The report concludes that Golden Dome reached high readiness levels and recommends further actions.

We are open to offers, but our main preference is to deal with government or intelligence organizations.

VortexPoison - The source of Unlimited.

Этот документ представляет собой строго секретный послетестовый отчет ВВС США по проекту «Золотой Купол» / операции MSR-2 / испытательному полету №12, проведенному на испытательном полигоне Рейган в атолле Кваджалейн 08.02.2025. В отчете подробно описывается успешное испытание космических сенсоров SENTINEL и перехватчиков KESTREL против двух суррогатов МБР и гиперзвукового планирующего блока, все цели были перехвачены на этапе разгона. В заключении отмечается,

что проект «Золотой Купол» достиг высокого уровня боеготовности и рекомендуется проведение дальнейших действий.

Where to Contact VortexPoison? Session -

HorizonMonitor's DarkForums post

Source: ZeroFox Intelligence

According to the post, the report states that the United States successfully tested space-based sensors (called SENTINEL) and missile interceptors (called KESTREL)—which were able to detect and shoot down a mock intercontinental ballistic missile (ICBM)—as well as a hypersonic weapon. If it is true that the United States can intercept missiles from space, it would indicate a significant advancement in aero-defense capability.

HorizonMonitor stated that they would prefer to negotiate with governments or intelligence organizations but would also be open to other actors; the actor directed any interested parties to contact them via the encrypted instant messaging application Session. Government organizations perceived to be adversaries of the United States—such as those of Russia, China, or Iran—would very likely be interested in obtaining such a report. However, no samples of the report were provided in the post.

- HorizonMonitor only joined DarkForums in September 2025 and has not yet garnered a positive reputation.
- As of writing, the thread has not received any comments or reactions.

It is unlikely that the claims made by HorizonMonitor are legitimate, given that no verifiable samples were shared of the alleged material to substantiate the breach and HorizonMonitor has not garnered any credibility on DarkForums.

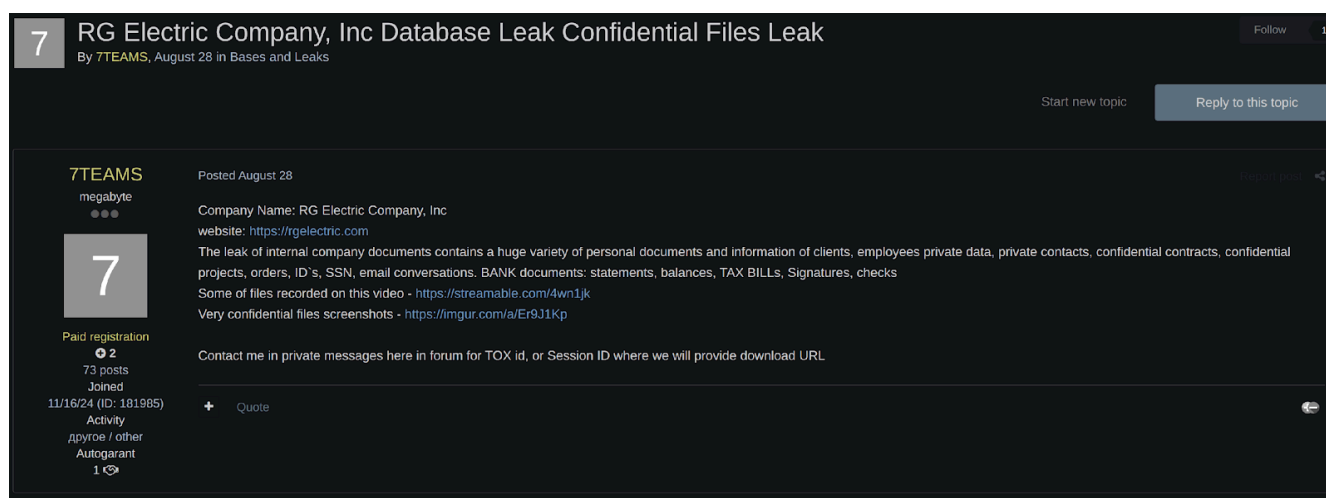
© 2025 ZeroFox, Inc. All rights reserved.

2

| Data Breach Related to U.S.-Based Company Advertised for Sale on Dark Web Forum

On August 29, 2025, the actor “7TEAMS” posted on the dark web forum Exploit, advertising access to confidential files related to the U.S.-based company RG Electric Company, Inc. The actor claimed to be in possession of leaked internal company documents, including a wide range of sensitive material such as:

- Personal information of clients and employees, including private contacts
- Confidential contracts and projects
- Personal identification documents and social security numbers (SSNs)
- Email correspondence
- Banking documents, including statements, balances, tax bills, signatures, and checks



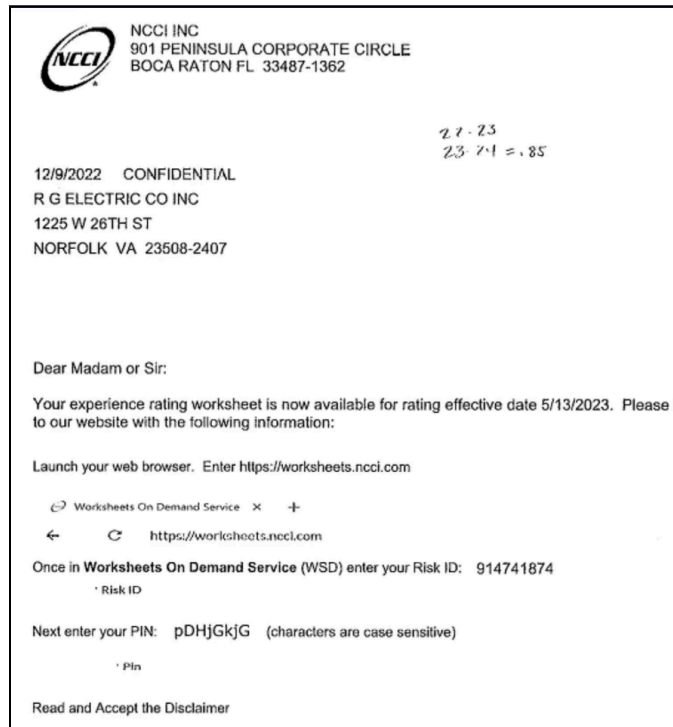
7TEAMS' Exploit post

Source: ZeroFox Intelligence

In the post, 7TEAMS also shared files from a recorded video and confidential screenshots of the alleged data, which adds significant credibility to their claims. The recorded video is no longer available, but the screenshots include confidential construction plans and internal directories from the alleged company network.

- 7TEAMS did not publicly disclose a price for the data but stated that interested parties must contact them directly via Tox ID or Session to receive a download link for the full dataset.

- 7TEAMS joined Exploit in November 2024 and has since garnered a positive reputation on the site.



Sample data provided by 7TEAMS

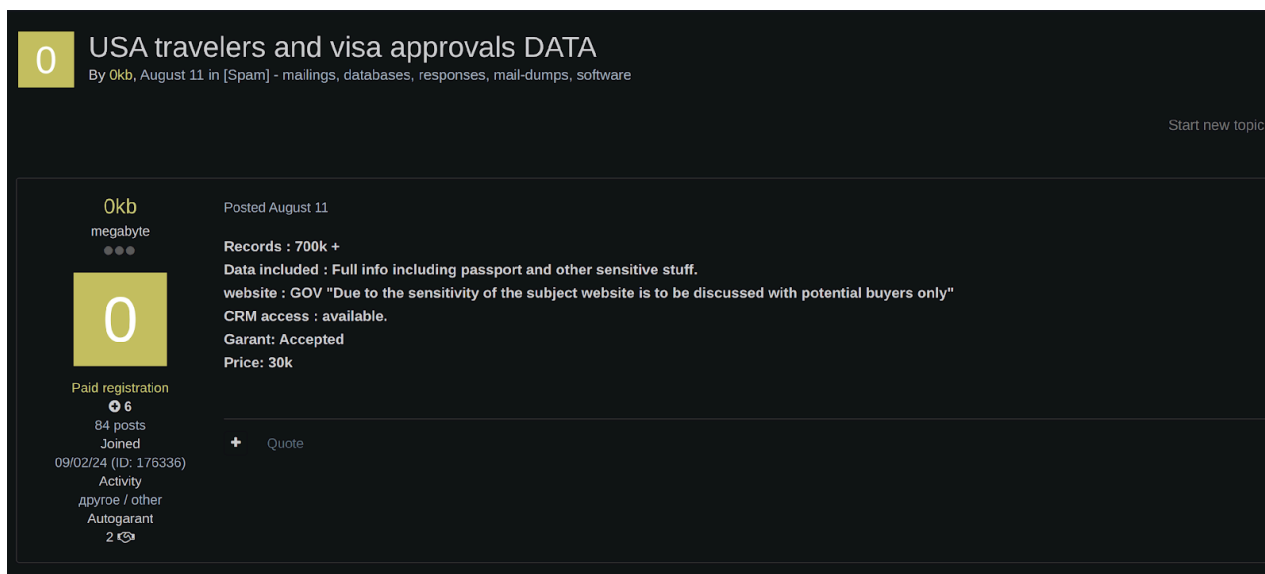
Source: ZeroFox Intelligence

It is likely that the claims made by 7TEAMS are true, given the actor's positive credibility and the provision of sample data in the post. This breach poses a multifaceted threat, combining the risks of financial fraud, identity theft, corporate espionage, and infrastructure exposure. With access to personally identifiable information (PII)—such as SSNs, IDs, and banking information—threat actors could very likely conduct identity theft or financial scams; additionally, internal emails, contracts, and network directories could enable targeted social engineering, such as phishing campaigns impersonating executives, clients, or vendors. Leaked construction plans and project details could very likely enable the impersonation of contractors or service technicians, potentially allowing physical access to secure facilities or systems.

| U.S. Travelers' Information and Visa Approval Dataset for Sale

On August 11, 2025, an actor using the alias "0kb" advertised an allegedly highly sensitive dataset containing U.S. travelers' information and visa approval information on the dark web forum Exploit. The actor has not yet publicly disclosed the source website of this dataset; such source information has been limited only to potential buyers. The actor claimed that the dataset includes over 700,000 records of passwords and other sensitive information.

- In addition to the dataset, the actor's offer also allegedly includes full Customer Relationship Management (CRM) system access to an unspecified government website.
- The total price of the dataset and CRM access is USD 30,000, with a middleman involved to safeguard the buyer's interest and likely offer increased credibility for the actor.



The screenshot shows a forum post on a dark-themed interface. The post title is "USA travelers and visa approvals DATA" in white text. Below the title, it says "By 0kb, August 11 in [Spam] - mailings, databases, responses, mail-dumps, software". On the right side of the post header, there is a link that says "Start new topic". The user profile for "0kb" is shown on the left, with a yellow square containing the number "0" as a profile picture. The user's name "0kb" is in bold, followed by "megabyte" and three dots. Below the profile picture, it says "Paid registration" with a small icon, "6" (posts), "84 posts", "Joined", "09/02/24 (ID: 176336)", "Activity", "dpyroe / other", "Autogrant", and "2" with a small icon. The post content area shows "Posted August 11" and "Records : 700k +". The main text of the post is in white: "Data included : Full info including passport and other sensitive stuff. website : GOV "Due to the sensitivity of the subject website is to be discussed with potential buyers only" CRM access : available. Grant: Accepted Price: 30k". At the bottom of the post content, there is a "+ Quote" button.

0kb's Exploit post

Source: ZeroFox Intelligence

Later in the week, on August 19, 2025, 0kb disclosed a sample of the dataset, which is also likely to offer interested buyers a preview of the data and further enhance the actor's

credibility. In the sample data provided, the following data fields were revealed by the actor:

- First name, middle name, last name, gender, DOB, email, phone, address, previous names, height, weight, hair color, eye color, birthplace, citizenship, previous lived address, U.S. citizen (yes or no), criminal history (yes or no), mental health history (yes or no), ID type, citizenship document (such as a passport), application type (New Member), appointment information, universally unique identifier (UUID), record created and updated (with dates and times), record ID, and payment ID.
- The sensitive information allegedly contained in this dataset is likely to be maliciously leveraged by other threat actors—especially in social engineering campaigns—with several subsequent consequences also likely.

The actor first registered on the Exploit forum on September 2, 2024, and has garnered a reputational scoring of about six. While an actor's reputation score does not solely indicate the authenticity of their claims, it likely provides insight into a potential buyer's perception of advertisements. Okb's reputational score of six is an average score on the platform; notably, it is difficult to achieve a positive score on Exploit. It is likely that Okb is well-regarded in the forum and considered credible by other forum users.

| Exploitation of Salesforce Systems Likely to Continue

From approximately August 8–18, 2025, a sophisticated supply chain breach targeting the Drift-Salesforce integration—which connects the two platforms to automate lead capture and sales outreach workflows—was reportedly carried out by a threat actor leveraging OAuth credentials to exfiltrate Salesforce instance data from multiple companies.²

- This has enabled attackers to exfiltrate sensitive credentials such as AWS keys, Snowflake tokens, and internal passwords across hundreds of organizations, including Cloudflare, Palo Alto Networks, and PagerDuty.³

² [hXXps://trust.salesloft\[.\]com/?uid=Drift%2FSalesforce+Security+Update](https://trust.salesloft.com/?uid=Drift%2FSalesforce+Security+Update)

³ [hXXps://blog.cloudflare\[.\]com/response-to-salesloft-drift-incident/](https://blog.cloudflare.com/response-to-salesloft-drift-incident/)

- Multiple organizations—including Cisco, Cloudflare (104 API tokens stolen), Zscaler, Palo Alto Networks, SpyCloud, PagerDuty, and Tanium—have since confirmed exposure and initiated remediation efforts.
- The attackers reportedly demonstrated strong operational security—such as deleting query jobs post-exfiltration—and the breadth of affected integrations expanded beyond Salesforce to platforms such as Google, Slack, and Amazon.⁴

Investigations later revealed that the breach also affected a small subset of Google Workspace accounts through the "Drift Email" integration. Notably, security researchers have reported that customers who integrate online services such as Slack, Google Workspace, Amazon S3, Microsoft Azure, and OpenAI with Salesloft may be potentially impacted by threat actors leveraging the stolen OAuth tokens.⁵

Threat group "ShinyHunters" (also tracked as UNC6040) has reportedly been linked to the Drift-Salesforce campaign; the tactics, techniques, and procedures (TTPs) observed are also similar to those used by another threat group "Scattered Spider." As detailed in a recent [ZeroFox Flash report](#), ShinyHunters and Scattered Spider were among the threat actors potentially involved in an August 2025 Workday breach also linked to a Salesforce vulnerability.

- ShinyHunters, active since 2020 with at least 91 known victims, primarily seeks financial gain via network intrusion, data breach, and (recently) social engineering.
- The group has previously sold large stolen datasets—including 73 million AT&T customer records—and typically exploits vulnerabilities in cloud applications and website databases.
- A Telegram channel has claimed that "UNC6395", a threat actor suspected to be linked to this chain of attacks, has been arrested. The Telegram channel operator claims to be a former employee of cryptocurrency company ChangeNOW, who was allegedly fired following a Scattered Spider hacking incident.⁶ ChangeNOW has denied being the victim of a cyberattack. ZeroFox cannot independently verify the claim UNC6395 has been arrested.

⁴ [hXXps://krebsonsecurity\[.\]com/2025/09/the-ongoing-fallout-from-a-breach-at-ai-chatbot-maker-salesloft/](https://krebsonsecurity.com/2025/09/the-ongoing-fallout-from-a-breach-at-ai-chatbot-maker-salesloft/)

⁵ *Ibid.*

⁶ [hXXps://x\[.\]com/IntCyberDigest/status/1963308828713418869](https://x.com/IntCyberDigest/status/1963308828713418869)

ZeroFox assesses that more companies that have utilized the compromised Salesforce integration with Salesloft Drift are likely to be publicly disclosed as victims in the coming weeks. This ongoing supply chain compromise is also likely to affect downstream entities of already impacted companies.

- Threat actors will likely use phishing, business email compromise (BEC), and social engineering attacks to target the downstream entities.
- There will very likely be additional risks, such as threat actors leveraging impersonation techniques and reusing stolen OAuth/API tokens to regain access or move laterally within connected software-as-a-service (SaaS) environments.
- The stolen CRM datasets are likely to be resold on underground forums, which could broaden exposure across multiple industries.

As of writing, Salesforce has disabled its integration with the Drift application. ZeroFox recommends that companies exercise caution and disable the connection between Salesforce and the Drift application in their networks, rotate any exposed OAuth tokens or API keys, and apply the principle of least privilege to connected apps.

| Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%