What Is the European Commission Cyberattack? How ShinyHunters Breached EU Cloud Infrastructure in 2026

TechRounder PDF Edition

Live article:
https://www.techrounder.com/news/what-is-the-european-commission-cyberattack-how-shinyhunters-breached-eu-cloud-infrastructure-in-2026/

By Vipin PG | Published March 31, 2026 | Updated March 31, 2026 | Format: News | 10 min read

What happened

In March 2026, the cybercrime group ShinyHunters breached the European Commission's cloud-hosted Europa.eu platform, stealing over 350GB of data including emails, confidential documents, DKIM signing keys, and SSO user directory information.

On March 24, 2026, the digital infrastructure of one of the world's most powerful governing bodies came under a serious cyberattack. The European Commission - the executive arm of the European Union - confirmed that its cloud-hosted Europa.eu web platform had been breached, with threat actors claiming to have walked away with more than 350 gigabytes of sensitive data. The group behind the attack? ShinyHunters, a financially motivated cybercrime gang with a long and well-documented track record of high-profile data theft and extortion.

This is not a drill or a speculative warning. The Commission officially acknowledged the breach in a press release, investigators are still piecing together the full scope of the damage, and the stolen data has already begun appearing on a dark web leak site. Here is everything you need to know about what happened, how it was pulled off, and what it means for EU digital security going forward.

What Is the European Commission Cyberattack?

The European Commission cyberattack refers to a data breach detected on March 24, 2026, in which attackers gained unauthorized access to the cloud infrastructure hosting the EU's Europa.eu web platform. Europa.eu is the central digital gateway for all EU institutional websites - covering legislation, policy announcements, official communications, and the digital presence of EU agencies and bodies.

The Commission confirmed the incident in an official statement on March 27, 2026, acknowledging that it had detected "malicious activities" affecting the cloud infrastructure of its web presence. According to the statement, immediate steps were taken to contain the attack, and the public-facing Europa websites remained operational throughout the incident. However, the Commission quietly noted that "early findings of our ongoing investigation suggest that data have been taken from those websites."

Commission spokesperson Thomas Regnier confirmed to reporters that parts of the Europa.eu platform are hosted on cloud infrastructure provided by Amazon Web Services (AWS), while also seeking to minimize the significance of the breach. He stressed that the affected domains were limited to Europa.eu public websites and that the Commission's "internal infrastructure has absolutely not been affected."

Who Is ShinyHunters?

If you have been following cybersecurity news over the past several years, ShinyHunters is not a new name. The group first surfaced around 2020 and has since built a reputation as one of the more prolific and aggressive financially motivated cybercrime collectives operating today.

Their modus operandi follows a consistent playbook. They identify and exploit security misconfigurations or compromised credentials in cloud environments, extract massive volumes of data, and then demand ransom payments. If victims refuse to pay, the group publishes the stolen data on dark web leak sites - a tactic commonly known as "double extortion." Over the years, ShinyHunters has claimed responsibility for breaches at Ticketmaster, Santander, AT&T, Canada Goose, Panera Bread, SoundCloud, Betterment, Crunchbase, Harvard University, and dozens more. According to Google's Threat Intelligence Group (GTIG), the group's operations have expanded significantly into 2026, with analysts tracking their activity under multiple threat clusters including UNC6661, UNC6671, and UNC6240.

The group's tactics have also evolved. In early 2026, ShinyHunters was connected to a large-scale voice phishing (vishing) campaign that targeted single sign-on (SSO) accounts at Okta, Microsoft, and Google across more than 100 high-profile organizations. In another campaign around the same time, they weaponized AuraInspector - a legitimate security auditing tool released by Google-owned Mandiant - and turned it into a mass scanning tool that targeted misconfigured Salesforce Experience Cloud instances, reportedly breaching between 300 and 400 companies as a result.

How Did ShinyHunters Breach EU Cloud Infrastructure?

The exact technical entry point used in the European Commission breach has not been officially confirmed, and the Commission's investigation was still ongoing at the time of publication. However, several key details have emerged that paint a reasonably clear picture of what likely happened.

AWS Account Compromise, Not an AWS Vulnerability

BleepingComputer first reported that the attackers specifically targeted the European Commission's Amazon Web Services accounts. AWS itself issued a statement clarifying that it "did not experience a security event" and that its services "operated as designed." This is a critical distinction. The breach did not result from a flaw in AWS's own systems. Instead, it appears the attackers gained access through a compromised account or a security misconfiguration on the Commission's side - both of which fall under the customer's responsibility within AWS's shared responsibility model.

This pattern is consistent with ShinyHunters' history. The group has repeatedly demonstrated the ability to identify and exploit poorly secured cloud configurations - scanning for exposed credentials, misconfigured storage buckets, or overly permissive access policies - rather than exploiting zero-day software vulnerabilities. Cybersecurity researchers from vpnMentor previously documented a large-scale ShinyHunters operation that worked by scanning AWS IP ranges for vulnerable endpoints, extracting exposed database credentials and AWS keys, and then installing remote shells for deeper access.

DKIM Keys and SSO Data Among the Exposed Assets

According to IT Pro, the data allegedly stolen from the European Commission includes a particularly dangerous mix of assets: emails and attachments, a full SSO (single sign-on) user directory, DKIM signing keys, AWS configuration snapshots, NextCloud and Athena data, and internal admin URLs. The exposure of DKIM signing keys is especially concerning because these are used to cryptographically verify the authenticity of outgoing emails. If those keys are in the hands of threat actors, they could send perfectly spoofed emails that appear to originate from legitimate EU Commission addresses - capable of bypassing standard anti-phishing filters and potentially being used in highly convincing follow-on attacks targeting EU member states, partner organizations, or government officials.

ShinyHunters’ Dark Web Listing

By the weekend following the initial detection, ShinyHunters had already posted a listing on their dark web leak site advertising "350GB+" of stolen data allegedly tied to the European Commission’s Europa platform. The listing described the haul as including "data dumps of mail servers, databases, confidential documents, contracts, and much more sensitive material." To increase pressure on EU officials and prove the legitimacy of their claims, the group subsequently released approximately 90 gigabytes of files on their Tor-based leak site before the situation was publicly acknowledged.

What Data Was Stolen?

The full scope of the stolen data remains under investigation, and the Commission has been cautious about confirming specifics. However, based on what ShinyHunters have publicly posted and what security researchers monitoring the leak site have identified, the breach appears to have exposed the following categories of data:

- Email data and attachments from mail servers hosted on the Europa.eu cloud environment
- Databases associated with EU institutional websites
- Confidential documents and contracts stored within the cloud infrastructure
- SSO user directory data , which could expose employee login credentials and account information
- DKIM signing keys , posing a severe email spoofing risk
- AWS configuration snapshots that could reveal further infrastructure details
- Internal admin URLs that could be used in follow-up attacks

The Commission has been careful to distinguish between its public-facing cloud infrastructure and its internal networks. Regnier emphasized that the Commission’s internal systems were "absolutely not affected." However, cybersecurity experts monitoring the leaked samples have described the breach’s potential implications as significant. The presence of signing keys and SSO directory data in particular means the damage could extend well beyond what the leaked documents themselves contain.

The Commission’s Response

In its official response, the European Commission stated that its defense systems "immediately detected the malicious activities" on March 24, 2026, and that "risk mitigation measures were implemented by our services to protect our services and data without disrupting the availability of our European websites." The Commission said it was in the process of notifying all Union entities that might have been affected by the incident, and that its services would "continue to monitor the situation and take all necessary measures to ensure the security of its internal systems and data."

Spokesperson Regnier also noted that the Commission would "analyze the incident and use the results to further enhance its cybersecurity capabilities" - a fairly standard post-breach commitment that will now be closely watched by EU member states, digital sovereignty advocates, and cybersecurity policy stakeholders.

This Is the Second Commission Breach in 2026

What makes this incident even more alarming is that it is not the first time the European Commission has been breached in 2026. Back in February, the Commission disclosed that the mobile device management (MDM) platform it uses to manage staff devices had been compromised in a separate incident. In that case, investigators found that attackers may have accessed some staff contact data including names and phone numbers, though no mobile devices were reportedly compromised and the breach was contained within nine hours.

Two confirmed breaches in the space of roughly six weeks is a significant pattern - and one that raises genuine questions about the adequacy of the Commission’s current cybersecurity posture, particularly around cloud-hosted infrastructure and third-party service dependencies.

The EU Digital Sovereignty Question

The fact that the European Commission - the body that sets and enforces digital policy for the entire European Union, including landmark frameworks like NIS2 and GDPR - was storing institutional data on an American cloud platform has reignited a long-running debate about EU digital sovereignty. The Commission has itself been a vocal proponent of reducing European dependency on non-EU technology providers, and the irony of that position being undermined by an attack on its own AWS-hosted infrastructure has not gone unnoticed.

In the wake of the breach, EU officials have signaled an acceleration of several key initiatives. These include the development of a "Single Entry Point" (SEP) - a centralized platform for reporting breaches to ENISA, the EU Agency for Cybersecurity - and a broader push under what is being informally called "EU Inc," which aims to build a digitally sovereign cloud infrastructure that reduces governmental reliance on AWS, Azure, and other American hyperscalers for sensitive operations.

What This Means for Organizations Using Cloud Infrastructure

The European Commission breach is a stark, high-profile reminder of a security reality that cloud infrastructure providers and security professionals have been flagging for years: the shared responsibility model for cloud security is only as strong as the practices of the customer using the platform. AWS did not fail here. The Commission’s configuration of its AWS environment apparently did.

According to BleepingComputer’s detailed reporting on the breach, ShinyHunters has leveraged this exact gap across multiple campaigns in 2025 and 2026 - scanning for misconfigured cloud environments, expired credentials, overly permissive access controls, and exposed API endpoints. Regardless of whether the target is a fintech startup or the executive body of a 27-nation bloc, the attack vector remains the same: find a misconfiguration, exploit it, and extract data before anyone notices.

For any organization running cloud-hosted infrastructure - government or commercial - the immediate takeaways from this incident are clear:

- Audit cloud configurations regularly. Exposed credentials, open S3 buckets, and excessive guest user permissions are recurring entry points that ShinyHunters and similar groups actively scan for at scale.

- Enforce MFA across all cloud and SaaS accounts without exception. Many ShinyHunters breaches in 2026 began with compromised SSO credentials obtained via voice phishing.

- Protect signing keys and secret rotation. DKIM keys and AWS access keys stored insecurely in cloud environments can unlock far more damage than the initial breach alone.

- Monitor API access logs for anomalous activity. The group frequently accesses data through exposed API endpoints in ways that resemble authorized administrative activity, making detection harder without active log monitoring.

- Adopt a Zero Trust architecture. The Commission's breach underscores the risks of assuming that cloud-hosted public-facing infrastructure is separate enough from sensitive assets to remain safe without strict access controls.

The Bigger Picture: A Cybercrime Group Operating at Government Scale

What is perhaps most striking about the ShinyHunters operation targeting the European Commission is not just the technical execution - it is the sheer ambition of targeting one of the world's most prominent governing institutions. ShinyHunters is not a state-sponsored group. They are not backed by a national intelligence apparatus or operating under political cover. They are a financially motivated criminal collective running a high-volume extortion business.

Yet in early 2026 alone, the group has been linked to hundreds of successful intrusions - hitting universities, financial institutions, automotive platforms, telecommunications companies, and now the executive branch of the European Union itself. That scale of activity, executed through a combination of misconfiguration exploitation, weaponized security tools, and social engineering, represents a meaningful shift in what non-state cybercrime groups are capable of achieving.

The investigation into the European Commission breach is ongoing. The full extent of the data exposure will likely take weeks to determine, and the downstream consequences - particularly if the leaked DKIM keys or SSO credentials are used in follow-on attacks - may not be immediately apparent. What is clear right now is that the breach happened, the data is out, and the EU is navigating a cybersecurity incident at exactly the moment it is trying to position itself as a global leader in digital regulation and data protection.

Key Takeaways

- The European Commission confirmed a data breach on March 27, 2026, after detecting malicious activity on March 24 targeting its Europa.eu cloud infrastructure hosted on AWS.

- ShinyHunters claimed responsibility, alleging theft of over 350GB of data including mail server dumps, databases, confidential documents, contracts, and DKIM signing keys.

- Approximately 90GB of the data has already been published on the group's dark web leak site.

- AWS confirmed it did not experience a security incident, indicating the breach likely stemmed from a misconfiguration or compromised credentials on the Commission's side.

- This is the second confirmed breach of the European Commission's systems in 2026, following a February incident targeting its mobile device management platform.

- The Commission says internal systems were not affected, but the investigation is ongoing and affected EU entities are being notified.

- The incident has intensified EU-level discussions about digital sovereignty and reducing dependency on non-EU cloud providers for sensitive governmental operations.

References

1. aws.amazon.com - security - https://aws.amazon.com/security/

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

3. digital-strategy.ec.europa.eu - en / policies - https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

4. bleepingcomputer.com - news / security - https://www.bleepingcomputer.com/news/security/european-commission-confirms-data-breach-after-europaeu-hack/