# INCEPTION FRAMEWORK

[ /ɪnˈsɛp.ʃən ˈfreɪm.wɜːrk/ ]

Inception Framework is a Russian-speaking cyberespionage group active since 2014, conducting high-risk spearphishing and cloud-based espionage against government, diplomatic, and defense sectors across Europe, the Middle East, and Central Asia, with increasing use of stealthy, modular tools.

## IDENTITY

| | |
|---|---|
| Attribution | : Likely Russian-speaking cyberespionage group |
| Active Since | : At least 2014 |
| Aliases | : ATK116, Blue Odin, Cloud Atlas, G0100, Clean Ursa, OXYGEN |
| Motivation | : Intelligence collection, credential harvesting, long-term access to strategic government and diplomatic networks |

## TTPs

| | |
|---|---|
| Initial Access | - Highly tailored spearphishing with malicious document attachments<br>- Exploitation of vulnerabilities in Office document formats<br>- Cloud-based phishing and OAuth abuse against email and collaboration platforms<br>- Use of multi-stage droppers disguised as policy or diplomatic documents |
| Persistence | - Modular backdoors with encrypted configurations<br>- Use of WMI-based persistence<br>- Registry modifications for long-term footholds<br>- Cloud session token theft to maintain access after password resets |
| Command & Control (C2) | - Cloud infrastructure abuse (e.g., Dropbox, Google Drive, OneDrive)<br>- Dynamic DNS services to rotate C2 endpoints<br>- Encrypted communication channels with minimal telemetry<br>- Multi-layered C2 architecture using staged payloads |
| Malware & Tools | - Custom malware families attributed to Inception/Cloud Atlas<br>- Document-based droppers with encrypted payloads<br>- PowerShell-based reconnaissance frameworks<br>- Cloud-hosted secondary stages to reduce attribution |
| Techniques | - Multi-platform targeting (Windows, Linux, and mobile devices)<br>- Extensive OPSEC through encryption, staging, and cloud redirection<br>- Stealthy credential harvesting from email, VPN, and cloud accounts<br>- Long-term reconnaissance within government networks |

## TARGET PROFILE

| | |
|---|---|
| Target Sectors | - Government ministries<br>- Diplomatic organizations and foreign affairs offices<br>- Defense research and national security institutions<br>- Telecommunications and communications systems<br>- Energy and natural resource sectors |
| Geographies Targeted | - Europe<br>- Middle East<br>- Central Asia<br>- Africa (select strategic targets)<br>- Occasionally Asia-Pacific |

## THREAT ASSESSMENT

| | |
|---|---|
| Risk Level | : High |
| Most Recent Activity | : Active cloud-based spearphishing and espionage operations through 2024–2025 |
| Evolution | : Increasing dependence on cloud services for payload delivery and C2; improved modular malware design; stronger OPSEC practices to avoid attribution |

## NOTABLE OPERATIONS

**2014–2016:** Initial discovery of Cloud Atlas operations targeting diplomatic/government organizations in Europe and Russia-adjacent regions.

**2017–2019:** Expansion into Middle Eastern and Central Asian diplomatic networks using spearphishing and cloud-staged tools.

**2020–2022:** Shift toward cloud-hosted malware delivery and C2 obfuscation.

**2023–2025:** Renewed activity with advanced spearphishing, OAuth-based access, and enhanced modular backdoors targeting high-value government and defense institutions.