TLP:CLEAR

INCIDENT REPORT

Phishing Campaign via Google Drive

Browser Fingerprinting + Anti-Analysis Cloaking + Bulletproof Hosting

Parameter	Value
Incident date	February 12, 2026, 22:14 UTC
Report date	February 13, 2026 (v3)
Classification	**Phishing / Browser Fingerprint Harvesting / Reconnaissance**
Threat level	**HIGH**
Infrastructure	PROSPERO OOO (AS200593) — bulletproof hosting
Recipients	24 email addresses (1 To + 23 CC), redacted
Status	Active campaign (confirmed February 13, 2026 12:12 UTC)
Author	Aleksei Fokin
Contact	info@afokin.com

1. Executive Summary

On February 12, 2026, a phishing campaign was detected leveraging legitimate Google infrastructure (Drive, Cloud Storage, Gmail) to deliver malicious content. The attackers constructed a multi-hop redirect chain concealing the final phishing resource hosted on PROSPERO OOO bulletproof hosting (Saint Petersburg, Russia).

The final phishing page contains a professional anti-analysis system: FingerprintJS v4.2.1 for unique victim identification, BotD for automated scanner detection (urlscan.io, VirusTotal), and a custom data exfiltration script. Bots are redirected to MSN.com (cloaking), while real users undergo fingerprinting and are also redirected to MSN.com after data collection.

Analysis of the intercepted POST request to secure.php confirmed that the attack is a mass browser fingerprint harvesting operation linked to email tracking IDs. This is a reconnaissance operation, not real-time credential harvesting. Collected fingerprints may be used for second-wave targeted attacks, anti-fraud system bypass, and victim re-identification on subsequent visits.

The email was disguised as a Google Drive notification from the law firm White & Case LLP. Unicode homoglyphs (Cyrillic е/а, inverted ɐ, Armenian) were used to bypass email filters. The campaign targeted 24 recipients including NGOs, corporations, and individuals.

2. Attack Chain (Kill Chain)

#	Stage	Description
1	Email delivery	Email from drive-shares-dm-noreply@google.com. Attacker account: neyjardespbeg2002@secure.accessinformattention.com. Unicode obfuscation in sender name and subject.
2	Google Drive	HTML page rendered as an image of a collection letter from White & Case LLP. Entire area is a single hyperlink to GCS bucket.
3	Google Cloud Storage	Bucket 'persontwelve', offer.html (128 bytes): meta refresh redirect to phishing domain. Last-Modified: Feb 12, 2026 15:48 UTC.
4	PHP router (/?ref=...)	Server sets cookies: PHPSESSID, ref (tracking ID), referer (Base64 of Referer header). Returns 302 to /secure/index_newest.html.
5	Browser fingerprinting	FingerprintJS v4.2.1: 30+ parameters generate unique visitorId. BotD detects automated scanners. Data written to hidden form fields.
6	Exfiltration	MutationObserver triggers on form field population. FormData → JSON → Base64 → XHR POST to secure.php. Payload: {ri, ib, re, rf}.
7	Cloaking / Exit	secure.php returns 302 → msn.com. Then window.location.href = "../" → also MSN. Clean exit for all victims.

3. Intercepted Data

A POST request to secure.php containing exfiltrated data was extracted from the browser HAR file. The request body contains Base64-encoded JSON.

3.1. POST Request to secure.php

URL: https://online.accessinformnotice.com/secure/secure.php

Method: POST

Content-Type: application/json

Timestamp: February 13, 2026 11:17:48 UTC

Response: 302 → https://msn.com

3.2. Request Body (decoded)


```
{"ed":"eyJyaSI6IjUzZDA3MmM2NmE3ZDNhMGE0YzU3MjAzY2MxMzY4MTA4IiwiaWIiOiIwIiwicmUiOiIiLCJyZiI6IjQ1ODljZDg5YTA5Y2ZlMDk1NDAifQ=="}
```


Base64 decoding of the 'ed' field:


```
{"ri":"53d072c66a7d3a0a4c57203cc1368108","ib":"0","re":"","rf":"4589cd89a09cfe09540"}
```


3.3. Field Definitions

Field	Value	Description
ri	53d072c66a7d3a0a4c57203cc1368108	Browser fingerprint (MurmurX64Hash128 from 30+ FingerprintJS parameters)
ib	0	**BotD result: HUMAN (not a bot)**
re	(empty)	Bot kind not detected (ib=0, no bot identified)
rf	4589cd89a09cfe09540	Email campaign tracking ID (from 'ref' cookie set at /?ref=...)

3.4. Server-Set Cookies

When visiting /?ref=4589cd89a09cfe09540, the server sets three cookies:

Cookie	Value	TTL	Purpose
PHPSESSID	gvovb9ga1gtrijo357iege2o95	Session	PHP session tracking
ref	4589cd89a09cfe09540	1 hour	Email campaign tracking ID
referer	aHR0cHM6Ly9zdG9yYWdlLmdvb2dsZWFwaXMuY29tLw%3D%3D	1 hour	Base64(https://storage.googleapis.com/) — records victim origin *Explicitly deleted (expires=1970) when Referer header is absent*

3.5. Revised Attack Model

Analysis of intercepted data reveals this is not real-time credential harvesting but a mass browser fingerprint collection operation:

- All victims (both bots and humans) are redirected to MSN.com after fingerprinting — a clean exit
- secure.php returns 302 → msn.com regardless of BotD result (ib=0 or ib=1)
- Server links ri (unique fingerprint) with rf (email tracking ID) — maps each recipient to their browser/device
- The 'referer' cookie records the traffic source (GCS) for chain validation
- Harvested fingerprints enable: second-wave targeted phishing, anti-fraud bypass, cross-site victim re-identification, data brokering

- Template index_newest.html (Last-Modified: Nov 20, 2025) is reused across campaigns — this is infrastructure tooling, not a single-use payload

4. Malicious Code Analysis

index_newest.html (77,018 bytes, Last-Modified: Nov 20, 2025) was extracted from the browser HAR file. It contains three JavaScript modules embedded as Base64 data: URIs.

4.1. Visual Lure

A fake "Checking your browser" screen with a CSS spinner animation, imitating Cloudflare/DDoS protection pages to keep the victim engaged. A hidden HTML form (id=rrm) contains four fields: ri (fingerprint visitorId), ib (bot 0/1), re (bot kind in Base64), rf (referrer cookie).

4.2. Script 1: FingerprintJS v4.2.1

Open-source browser fingerprinting library (~45 KB decoded). Collects 30+ browser parameters: Canvas and WebGL fingerprints, Audio fingerprint (OfflineAudioContext), presence of 60+ fonts (side-channel via offsetWidth/offsetHeight), screen resolution, color depth, device memory, hardware concurrency, timezone, plugins, math constants (Math.acos/sinh/cosh — differ between engines), and ad-blocker detection (30+ filter lists including EasyList, AdGuard, uBlock). Output: 32-character hex hash (MurmurX64Hash128) written to the 'ri' form field.

4.3. Script 2: BotD (Bot Detection)

Bot detection library by FingerprintJS Inc. Detects: Selenium (window.__selenium_evaluate, $cdc_ variables), WebDriver (navigator.webdriver), Headless Chrome (Notification permissions, plugins, window size, WebGL vendor Brian Paul/Mesa OffScreen), PhantomJS (callPhantom, error stack), Electron (process.versions.electron), and additional signatures for Nightmare, CefSharp, Sequentum, SlimeJS, FMiner, Rhino, Awesomium, Geb, CoachJS, Phantomas. Output: ib=0 (human) or ib=1 (bot), re=Base64(botKind).

4.4. Script 3: Exfiltration and Cloaking

Custom script implementing data exfiltration logic. A MutationObserver watches for changes to 'ib' and 'ri' form fields. Once both are populated, the observer disconnects and triggers: FormData collection → JSON serialization → Base64 encoding → XHR POST to secure.php with body {ed: Base64(JSON)}. On request completion (readyState === 4), executes window.location.href = "../" redirecting to the domain root, which returns 302 to MSN.com. The 'ref' cookie is read into the 'rf' field and then erased (eraseCookie).

5. Indicators of Compromise (IOC)

5.1. Domains and URLs

Type	Value	Description
Domain	online.accessinformnotice.com	Phishing/fingerprinting site
Domain	accessinformattention.com	Sender domain (Cloudflare-proxied)
URL	.../secure/index_newest.html	Fingerprinting page (77 KB)
URL	.../secure/secure.php	Exfiltration backend (POST)
GCS	storage.googleapis.com/persontwelve/online/offer.html	Redirect page (128 bytes)
Drive	drive.google.com/file/d/18XPn0pHsygsvZcinTivBQ_I225l-xzpC	Lure document

5.2. Network Indicators

Type	Value	Description
IP	91.202.233.71	Phishing server (PROSPERO OOO)
ASN	AS200593	PROSPERO OOO, bulletproof hosting
Netblock	91.202.233.0/24	PROSPERO allocation
NS	ns1.dyna-ns.net / ns2.dyna-ns.net	Nameservers (Dyna DNS)
SOA	Serial 2026021202	DNS zone updated Feb 12, 2026
Server	Apache/2.4.41 (Ubuntu)	Web server
IP (CF)	188.114.96.11 / 188.114.97.11	Cloudflare for sender domain

5.3. Email Indicators

Parameter	Value
From (display)	White § Case□ Pay Immediately
From (actual)	drive-shares-dm-noreply@google.com
Attacker account	neyjardespbeg2002@secure.accessinformattention.com
Subject	Resolve Promptly - Debt Detected - Pay Immediately!
Date	February 12, 2026, 22:14 UTC
Document tracking ID	MBFZoZNY8cXcYnMaMRxX
URL tracking ID	ref=4589cd89a09cfe09540
Unicode homoglyphs	Cyrillic е (U+0435), а (U+0430), inverted ɐ (U+0250), Armenian ։ (U+058D)

5.4. Code and Intercepted Data Indicators

Parameter	Value
Intercepted fingerprint	53d072c66a7d3a0a4c57203cc1368108
BotD result	ib=0 (human)
FingerprintJS version	4.2.1, MurmurX64Hash128

BotD detectors	webdriver, headless_chrome, selenium, phantomjs, electron, nightmare, cefsharp, sequentum, slimmerjs, fminer, rhino, awesomium, geb, coachjs, phantomas
Exfiltration	POST /secure/secure.php, {ed: Base64(JSON)}
Cloaking redirect	302 → https://msn.com
ETag	"12cda-6440660282480-gzip"
Last-Modified	November 20, 2025 (reusable template)
Cookie: referer	Base64(Referer URL); explicitly deleted when Referer header absent

6. Attacker Infrastructure

6.1. PROSPERO OOO (AS200593)

IP 91.202.233.71 belongs to AS200593, PROSPERO OOO, registered at pr-kt Solidarnosti 12/2, Saint Petersburg, Russia. PROSPERO is one of the most notorious bulletproof hosting providers globally (KrebsOnSecurity, Intrinsec, Spamhaus). It operates under aliases BEARHOST, SecureHost, and UNDERGROUND, and is advertised on cybercriminal forums as "100% bulletproof, all abuse complaints fully ignored." It hosts C2 servers for ransomware groups, SocGholish, GootLoader, and SpyNote malware. Interisle Consulting Group rates it as having the highest spam score of any hosting provider. Since December 2024, PROSPERO has been routing traffic through Kaspersky Lab networks (AS209030). It is affiliated with Proton66 OOO (AS198953).

6.2. Infrastructure Separation

Component	Infrastructure	Purpose
Sender domain	Cloudflare (188.114.96/97.11)	IP concealment, takedown resistance
Delivery	Google (Drive + GCS + Gmail)	Email filter bypass, trusted domain reputation
Fingerprinting	PROSPERO OOO (91.202.233.71)	Bulletproof hosting, direct IP, abuse-resistant
DNS	Dyna DNS (dyna-ns.net)	Cheap DNS, rapid IP rotation capability

6.3. Server-Side Logic (secure.php)

Based on cookies and POST data, the server: (1) registers the victim's fingerprint linked to the email tracking ID; (2) records the traffic source via the 'referer' cookie (Base64 of Referer header); (3) validates the redirect chain by checking for the Referer header — explicitly deleting the cookie when absent; (4) returns 302 → msn.com for all visitors, ensuring a clean exit regardless of bot detection result.

7. MITRE ATT&CK Mapping

Technique	Name	Application
T1566.002	Spearphishing Link	Google Drive share via email
T1036.005	Match Legitimate Name	Impersonation of White & Case LLP
T1036.001	Invalid Code Signature	Unicode homoglyphs in sender name
T1204.001	User Execution: Malicious Link	Click on DOWNLOAD E-SIGN button
T1608.005	Stage Capabilities: Link Target	Multi-hop: Google Drive → GCS → PROSPERO
T1090	Proxy / Cloaking	BotD detection + MSN.com redirect for scanners
T1583.003	Acquire Infrastructure: VPS	Bulletproof hosting via PROSPERO OOO
T1217	Browser Information Discovery	FingerprintJS: 30+ browser parameters
T1041	Exfiltration Over C2 Channel	JSON → Base64 → POST secure.php
T1592.004	Gather Victim Host Information	Fingerprint harvesting for victim profiling
T1598	Phishing for Information	Reconnaissance: fingerprint collection, not credentials

8. HTTP Request Chain (from HAR)

#	URL	Status	IP / Server	Purpose
1	storage.googleapis.com/.../offer.html	307	Google HSTS	HSTS upgrade to HTTPS
2	storage.googleapis.com/.../offer.html	200	142.250.120.207	Meta refresh (128 bytes)
3	online.accessinformnotice.com/?ref=...	302	91.202.233.71	Set cookies + redirect
4	.../secure/index_newest.html	200	91.202.233.71	Fingerprinting page (77 KB)
5	POST .../secure/secure.php	302	91.202.233.71	Exfiltration → msn.com
6	online.accessinformnotice.com/	302	91.202.233.71	Cloaking → MSN
7	www.msn.com/pl-pl	200	Microsoft	Clean exit (masking)

9. Recommendations

9.1. Immediate Actions

- Block domains accessinformnotice.com and accessinformattention.com (DNS sinkhole, firewall, proxy)
- Block IP 91.202.233.71 and netblock 91.202.233.0/24
- Report the Google Drive file (18XPn0pHsygsvZcinTivBQ_I225l-xzpC) and GCS bucket 'persontwelve' via Google abuse forms
- Review email and proxy logs for clicks on campaign URLs
- Notify all affected recipients about the phishing campaign and fingerprint collection

9.2. For Users Who Clicked the Link

- Clear browser data (cookies, cache, localStorage) to partially reset fingerprint parameters
- Update browser to the latest version — Canvas and WebGL fingerprints change with browser updates
- Consider updating GPU drivers (affects WebGL fingerprint component)
- Credentials were NOT compromised — the attack collected browser fingerprints only
- Be prepared for a potential second-wave targeted attack using the harvested fingerprint data

9.3. Medium-Term Measures

- Implement filtering rules for Google Drive shares with urgency markers from external organizations
- Block entire AS200593 (PROSPERO OOO) — no legitimate traffic originates from this network
- Conduct phishing awareness training focused on Google Drive-based attack vectors
- Monitor Certificate Transparency logs for new accessinform*.com subdomains

9.4. SIEM/IDS Rules

```
alert dns any any -> any any (msg:"Phishing - accessinformnotice.com"; dns.query;
content:"accessinformnotice.com"; sid:2026021301;)

alert dns any any -> any any (msg:"Phishing - accessinformattention.com"; dns.query;
content:"accessinformattention.com"; sid:2026021302;)

alert ip any any -> 91.202.233.0/24 any (msg:"PROSPERO OOO bulletproof hosting";
sid:2026021303;)
```

10. Sources

- Browser HAR file — HTTP requests, malicious code extraction, intercepted POST data
- urlscan.io — scans from February 13, 2026
- curl verification with varied parameters — cookie behavior and server logic (Feb 13, 2026 12:12 UTC)
- KrebsOnSecurity — "Notorious Malware, Spam Host Prospero Moves to Kaspersky Lab" (February 2025)
- Intrinsec — "PROSPERO & Proton66: Uncovering the links between bulletproof networks" (November 2024)
- Certificate Transparency (crt.sh), DNS queries (dig)
- FingerprintJS / BotD GitHub repositories — version and functionality identification