TLP:CLEAR

ОТЧЁТ ОБ ИНЦИДЕНТЕ

Фишинговая кампания через Google Drive

Browser Fingerprinting + Anti-Analysis Cloaking + Bulletproof Hosting

Параметр	Значение
Дата инцидента	12 февраля 2026, 22:14 UTC
Дата отчёта	13 февраля 2026 (v3)
Классификация	**Фишинг / Browser Fingerprint Harvesting / Reconnaissance**
Уровень угрозы	**ВЫСОКИЙ**
Инфраструктура	PROSPERO OOO (AS200593) — bulletproof hosting
Адресаты	24 email-адреса (1 To + 23 CC), скрыты
Статус	Активная кампания (подтверждено 13.02.2026 12:12 UTC)
Автор	Алексей Фокин
Контакт	info@afokin.com

1. Резюме

12 февраля 2026 года зафиксирована фишинговая кампания, использующая легитимную инфраструктуру Google (Drive, Cloud Storage, Gmail) для доставки вредоносного контента. Атакующие создали многоуровневую цепочку перенаправлений, маскирующую конечный фишинговый ресурс на bulletproof-хостинге PROSPERO OOO (Санкт-Петербург, Россия).

Финальная фишинговая страница содержит профессиональную систему anti-analysis: FingerprintJS v4.2.1 для уникальной идентификации жертв, BotD для обнаружения сканеров (urlscan.io, VirusTotal) и кастомный скрипт эксфильтрации данных. Боты перенаправляются на MSN.com (cloaking), реальные пользователи проходят fingerprinting и также направляются на MSN.com после сбора данных.

Анализ перехваченного POST-запроса на secure.php подтвердил: атака представляет собой массовый сбор browser fingerprints, привязанных к tracking ID из email-рассылки. Это разведывательная операция (reconnaissance), а не прямой credential harvesting. Собранные fingerprints могут использоваться для таргетированных атак второй волны, обхода anti-fraud систем и идентификации жертв при повторных визитах.

Письмо замаскировано под уведомление Google Drive от юридической фирмы White & Case LLP. Использованы Unicode-гомоглифы (кириллические е/а, перевёрнутая ɐ, армянский) для обхода фильтров. Рассылка затронула 24 адресата — NGO, корпорации и частные лица.

2. Цепочка атаки (Kill Chain)

№	Этап	Описание
1	Email-доставка	Письмо от drive-shares-dm-noreply@google.com. Аккаунт: neyjardespbeg2002@secure.accessinformattention.com. Unicode-обфускация.
2	Google Drive	HTML-страница как изображение collection letter White & Case LLP. Вся область — единая гиперссылка на GCS.
3	Google Cloud Storage	Бакет persontwelve, offer.html (128 байт): meta refresh → фишинговый домен. Last-Modified: 12.02.2026 15:48.
4	PHP-роутер (/?ref=...)	Сервер устанавливает cookies: PHPSESSID, ref (tracking ID), referer (Base64 от Referer header). 302 → /secure/index_newest.html.
5	Browser Fingerprinting	FingerprintJS v4.2.1: 30+ параметров → visitorId. BotD определяет сканеры. Данные записываются в скрытую форму.
6	Эксфильтрация	MutationObserver → FormData → JSON → Base64 → XHR POST secure.php. Payload: {ri, ib, re, rf}.
7	Cloaking / Выход	secure.php возвращает 302 → msn.com. Затем window.location.href = "../" → также MSN. Чистый выход для всех жертв.

3. Перехваченные данные

Из HAR-файла браузера извлечён POST-запрос на secure.php с эксфильтрированными данными. Тело запроса содержит JSON в Base64-кодировке.

3.1. POST-запрос на secure.php

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

Метод: POST

Content-Type: application/json

Время: 13.02.2026 11:17:48 UTC

Ответ: 302 → https://msn.com

3.2. Тело запроса (декодированное)


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


Base64-декодирование поля ed:


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


3.3. Расшифровка полей

Поле	Значение	Описание
ri	53d072c66a7d3a0a4c57203cc1368108	Browser fingerprint (MurmurX64Hash128 от 30+ параметров FingerprintJS)
ib	0	**Результат BotD: ЧЕЛОВЕК (не бот)**
re	(пустое)	Тип бота не определён (ib=0, бот не обнаружен)
rf	4589cd89a09cfe09540	Tracking ID из email-рассылки (из cookie ref, установленного при /?ref=...)

3.4. Cookies, установленные сервером

При переходе на /?ref=4589cd89a09cfe09540 сервер устанавливает три cookie:

Cookie	Значение	TTL	Назначение
PHPSESSID	gvovb9ga1gtrijo357iege2o95	Сессия	PHP-сессия для отслеживания
ref	4589cd89a09cfe09540	1 час	Tracking ID из email
referer	aHR0cHM6Ly9zdG9yYWdlLmdvb2dsZWFwaXMuY29tLw%3D%3D	1 час	Base64(https://storage.googleapis.com/) — откуда пришла жертва *При отсутствии Referer header cookie явно удаляется (expires=1970)*

3.5. Модель атаки (уточнённая)

Анализ перехваченных данных показал, что атака представляет собой не credential harvesting в реальном времени, а массовый сбор browser fingerprints:

- Все жертвы (и боты, и люди) после fingerprinting перенаправляются на MSN.com — «чистый выход»
- secure.php возвращает 302 → msn.com вне зависимости от результата BotD (ib=0 или ib=1)
- Сервер связывает ri (уникальный fingerprint) с rf (tracking ID из email) → знает кто из рассылки на каком браузере/устройстве
- Cookie referer фиксирует источник перехода (GCS) для валидации цепочки

- Собранные fingerprints могут использоваться: таргетированный фишинг второй волны, обход anti-fraud, идентификация при повторных визитах, продажа данных
- Шаблон index_newest.html (Last-Modified: 20.11.2025) используется повторно в разных кампаниях — это инфраструктурный инструмент, не одноразовый payload

4. Анализ вредоносного кода

index_newest.html (77 018 байт, Last-Modified: 20.11.2025) извлечена из HAR-файла. Содержит три JavaScript-модуля в Base64 (data: URI).

4.1. Визуальная приманка

Фейковый экран "Checking your browser" с CSS-спиннером. Имитация Cloudflare/DDoS-защиты для удержания жертвы. Скрытая форма (id=rrm) с полями: ri (fingerprint visitorId), ib (бот 0/1), re (тип бота, base64), rf (referrer cookie).

4.2. Скрипт 1: FingerprintJS v4.2.1

Open-source библиотека browser fingerprinting (~45 КБ). Собирает 30+ параметров: Canvas и WebGL fingerprint, Audio fingerprint (OfflineAudioContext), наличие 60+ шрифтов (side-channel через offsetWidth), разрешение экрана, device memory, hardware concurrency, timezone, plugins, математические константы (Math.acos/sinh/cosh), списки ad-блокеров (30+ списков). Результат: 32-символьный hex-хеш MurmurX64Hash128 → поле ri.

4.3. Скрипт 2: BotD (Bot Detection)

Библиотека обнаружения ботов от FingerprintJS. Детектирует: Selenium (window.__selenium_evaluate, $cdc_), WebDriver (navigator.webdriver), Headless Chrome (plugins, window size, WebGL vendor Brian Paul/Mesa OffScreen), PhantomJS, Electron, Nightmare, CefSharp, SlimeJS и др. Результат: ib=0 (человек) / ib=1 (бот), re=Base64(botKind).

4.4. Скрипт 3: Эксфильтрация и cloaking

Кастомный скрипт. MutationObserver ожидает заполнения полей ib и ri. После заполнения: FormData → JSON → Base64 → XHR POST на secure.php ({ed: <data>}). По завершении — window.location.href = "../" → корень домена → 302 на MSN.com. Cookie 'ref' читается в поле rf и удаляется после эксфильтрации (eraseCookie).

5. Индикаторы компрометации (IOC)

5.1. Домены и URL

Тип	Значение	Описание
Домен	online.accessinformnotice.com	Фишинговый сайт
Домен	accessinformattention.com	Домен отправителя (Cloudflare)
URL	.../secure/index_newest.html	Fingerprinting-страница
URL	.../secure/secure.php	Backend эксфильтрации (POST)
GCS	storage.googleapis.com/persontwelve/online/offer.html	Redirect (128 байт)
Drive	drive.google.com/file/d/18XPn0pHsygsvZcinTivBQ_I225l-xzpC	Файл-приманка

5.2. Сетевые индикаторы

Тип	Значение	Описание
IP	91.202.233.71	Фишинговый сервер (PROSPERO)
ASN	AS200593	PROSPERO OOO, bulletproof
Подсеть	91.202.233.0/24	Блок PROSPERO
NS	ns1.dyna-ns.net / ns2.dyna-ns.net	Nameservers
SOA	Serial 2026021202	Обновлено 12.02.2026
Server	Apache/2.4.41 (Ubuntu)	Веб-сервер
IP (CF)	188.114.96.11 / 188.114.97.11	Cloudflare для домена отправителя

5.3. Email-индикаторы

Параметр	Значение
From (отображаемое)	White § Case□ Pay Immediately
From (фактический)	drive-shares-dm-noreply@google.com
Аккаунт атакующего	neyjardespbeg2002@secure.accessinformattention.com
Subject	Resolve Promptly - Debt Detected - Pay Immediately!
Дата	12 февраля 2026, 22:14 UTC
Tracking ID (документ)	MBFZoZNY8cXcYnMaMRxX
Tracking ID (URL)	ref=4589cd89a09cfe09540

5.4. Индикаторы из кода и перехваченных данных

Параметр	Значение
Перехваченный fingerprint	53d072c66a7d3a0a4c57203cc1368108
BotD результат	ib=0 (человек)
FingerprintJS версия	4.2.1, MurmurX64Hash128
BotD детекторы	webdriver, headless_chrome, selenium, phantomjs, electron, nightmare, cefsharp, sequentum, slimmerjs, fminer, rhino, awesomium, geb, coachjs, phantomas

Эксфильтрация	POST /secure/secure.php, {ed: Base64(JSON)}
Cloaking redirect	302 → https://msn.com
ETag	"12cda-6440660282480-gzip"
Last-Modified	20 ноября 2025 (шаблон многоразовый)
Cookie referer	Base64(Referer URL), удаляется если нет Referer header

6. Инфраструктура атакующего

6.1. PROSPERO OOO (AS200593)

IP 91.202.233.71 — AS200593, PROSPERO OOO, Санкт-Петербург, пр-кт Солидарности 12/2. Один из наиболее известных bulletproof-хостингов (KrebsOnSecurity, Intrinsec, Spamhaus): BEARHOST/SecureHost/UNDERGROUND, хостит C2 ransomware, SocGholish, GootLoader, SpyNote. Наивысший spam-рейтинг (Interisle). С декабря 2024 маршрутизирует трафик через Kaspersky Lab (AS209030). Связан с Proton66 OOO (AS198953).

6.2. Разделение инфраструктуры

Компонент	Инфраструктура	Назначение
Домен отправителя	Cloudflare (188.114.96/97.11)	Скрытие IP, защита от блокировки
Доставка	Google (Drive + GCS + Gmail)	Обход email-фильтров, доверие к googleapis.com
Fingerprinting	PROSPERO OOO (91.202.233.71)	Bulletproof, прямой IP, игнорирует abuse
DNS	Dyna DNS (dyna-ns.net)	Дешёвый DNS, быстрая смена IP

6.3. Серверная логика (secure.php)

На основании cookies и POST-данных сервер: (1) регистрирует fingerprint жертвы, привязывая к tracking ID; (2) фиксирует источник перехода через cookie referer; (3) проверяет наличие Referer header — при его отсутствии cookie referer явно удаляется; (4) возвращает 302 → msn.com для всех жертв, обеспечивая «чистый выход».

7. MITRE ATT&CK

Техника	Название	Применение
T1566.002	Spearphishing Link	Ссылка на Google Drive через email
T1036.005	Match Legitimate Name	Имитация White & Case LLP
T1036.001	Invalid Code Signature	Unicode-гомоглифы в имени отправителя
T1204.001	User Execution	Клик по DOWNLOAD E-SIGN
T1608.005	Link Target	Multi-hop: GCS → PROSPERO
T1090	Proxy / Cloaking	BotD + redirect на MSN.com
T1583.003	Acquire Infrastructure	Bulletproof hosting PROSPERO OOO
T1217	Browser Information Discovery	FingerprintJS: 30+ параметров браузера
T1041	Exfiltration Over C2	JSON → Base64 → POST secure.php
T1592.004	Gather Victim Host Info	Fingerprint для профилирования жертв
T1598	Phishing for Information	Сбор fingerprints, не credentials

8. Цепочка HTTP-запросов (HAR)

#	URL	Status	IP / Server	Назначение
1	storage.googleapis.com/.../offer.html	307	Google HSTS	HSTS upgrade → HTTPS
2	storage.googleapis.com/.../offer.html	200	142.250.120.207	Meta refresh (128 байт)
3	online.accessinformnotice.com/?ref=...	302	91.202.233.71	Set cookies + redirect
4	.../secure/index_newest.html	200	91.202.233.71	Fingerprinting (77 КБ)
5	POST .../secure/secure.php	302	91.202.233.71	Эксфильтрация → msn.com
6	online.accessinformnotice.com/	302	91.202.233.71	Cloaking → MSN
7	www.msn.com/pl-pl	200	Microsoft	Маскировка (чистый выход)

10. Рекомендации

10.1. Немедленные действия

- Заблокировать домены accessinformnotice.com и accessinformattention.com (DNS sinkhole, firewall, proxy)
- Заблокировать IP 91.202.233.71 и подсеть 91.202.233.0/24
- Зарепортить Google Drive файл (18XPn0pHsygsvZcinTivBQ_I225l-xzpC) и GCS-бакет persontwelve
- Проверить логи почты и прокси на клики по ссылкам кампании
- Уведомить всех 24 адресатов о фишинговой кампании и сборе fingerprints

10.2. Для пользователей, прошедших по ссылке

- Очистить данные браузера (cookies, cache, localStorage) для сброса fingerprint-параметров
- Обновить браузер — Canvas и WebGL fingerprint изменятся при обновлении
- Рассмотреть обновление GPU-драйверов (влияет на WebGL fingerprint)
- Credentials не были скомпрометированы — атака собирала только fingerprints
- Быть готовыми к таргетированной атаке второй волны с использованием собранных данных

10.3. Среднесрочные меры

- Фильтрация Google Drive shares с urgency-маркерами от внешних организаций
- Блокировка всей AS200593 (PROSPERO OOO) — нет легитимного трафика
- Тренинг по фишингу через Google Drive для сотрудников
- Мониторинг Certificate Transparency для accessinform*.com

10.4. Правила SIEM/IDS

```
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;)
```

11. Источники

- HAR-файл браузера (mail.har) — HTTP-запросы, вредоносный код, перехваченный POST

- urlscan.io — сканы от 13.02.2026
- curl-проверка с различными параметрами — cookies и серверная логика (13.02.2026 12:12 UTC)
- KrebsOnSecurity — "Notorious Malware, Spam Host Prospero Moves to Kaspersky Lab" (февраль 2025)
- Intrinsec — "PROSPERO & Proton66: Uncovering the links between bulletproof networks" (ноябрь 2024)
- Certificate Transparency (crt.sh), DNS-запросы (dig)
- FingerprintJS / BotD GitHub — идентификация версий и функциональности