网络钓鱼事件分析与案件汇总报告

冒用 HPE 邮件身份、针对 OK Group 员工的凭据窃取攻击

报告编号: IR-2026-0827-PHISH-OKG
事件类型: 钓鱼邮件 / 凭据窃取 / 邮件身份滥用
严重级别: 高 *(邮件通过 DMARC 认证)*
受害目标: OK Group / OKX 员工 (收件人个人邮箱)
报告日期: 2026-08-27
分析状态: 完成初步公开来源 (OSINT) 分析

本报告基于对受害者收到邮件的原始头分析, 以及对相关域名、IP、证书和公开服务的被动侦察 (OSINT)。所有取证均在未对攻击者系统进行任何入侵、扫描或未授权访问的前提下完成。

本报告可用于: 内部通报、向执法机关报案、向 OK Group 安全团队通报、以及向 AWS / 注册商 / 托管商提交滥用举报。

Contents

1 事件摘要 *(Executive Summary)*

2026 年 8 月 26 日 (UTC), 受害者的个人 Gmail 邮箱收到一封伪装成 HPE(Hewlett Packard Enterprise)IT 安全团队的中文钓鱼邮件, 主题为**”安全通知: 员工账户重新注册提醒”**。邮件以” 公司内部安全系统更新, 需全体员工在 24 小时内重新注册账户” 为借口, 诱导点击链接。

本次事件有三个非同寻常的特征, 使其危险性远高于普通钓鱼:

1. **邮件在密码学上是”真”的。**该邮件通过 Amazon SES 发送, 携带一个**当时真实发布在 `hpe.com` *DNS* 中的 *DKIM* 密钥**的有效签名, 因此 SPF、DKIM、DMARC **全部通过验证**——尽管 `hpe.com` 配置了最严格的 `p=reject` 策略。Gmail 据此正常投递, 不作任何警告。这不是” 伪造发件人”, 而是**攻击者获得了以 *HPE* 身份签名发信的能力**。
2. **链接采用子域名障眼法, 真实目标是 *OK Group*。** 邮件正文显示链接为 `engine.okg.com`(看似 OK Group 正规域), 实际跳转至攻击者控制的 `okg.enginelark.com`。邮件使用 OKX 真实 CDN 上的品牌 Logo, 视觉上无破绽。
3. **攻击具有定向侦察特征。** 攻击者注册的仿冒域名 `enginelark.com` 精确对应 OK Group 内部真实系统代号 (”Engine” 办公门户 + ”Lark” 飞书), 且钓鱼页面中硬编码了 OK Group 内部真实域名 `enginelark.okg.com` 作为失败跳转目标。这表明攻击者对目标内部系统命名有深入了解, 并非无差别群发。

钓鱼页面索取受害者的**企业邮箱与验证码** (而非密码), 疑似用于会话劫持或验证码中继, 此类攻击可绕过部分二次验证 (2FA)。分析期间发现攻击者至少使用了**两个同批注册的仿冒域名**, 均托管于荷兰同一台 VPS。

> **核心结论:** 这不是一封” 假冒” 邮件——它是一封通过合法认证通道发出的、由**被滥用的 *HPE* 邮件签名身份**背书的真实定向钓鱼邮件。收件端 (Gmail) 无从拦截。真正的失陷点在 HPE 侧的邮件发送凭据 / DNS 配置, 以及攻击者租用的荷兰服务器。

2 关键证据截图

本节为受害者邮箱中该钓鱼邮件的原始截图, 作为事件的第一手证据留存。截图内容与后文 §5 技术分析、附录 A 的邮件原始头一致。

图 *1* ——表面发件人。在邮件客户端中展开发件人, 显示为 `security@hpe.com`。需注意: 该地址**并非普通显示名伪造**——如 §5.1 所述, 该邮件确实携带了通过验证的 `hpe.com` DKIM 签名并通过 DMARC, 因此客户端将其呈现为合法 HPE 发件人。

图 1: 邮件客户端中展开的发件人, 表面发件人为 security@hpe.com。

图 2 ——邮件正文与伪装链接。主题为" 安全通知: 员工账户重新注册提醒", 收件人为受害者 Gmail(fwx5618177@gmail.com), 客户端显示发送时间 09:22。正文以 HPE IT 安全团队口吻要求”24 小时内重新注册, 否则限制访问权限”。**正文中显示的链接为 `https://engine.okg.com/...`(伪装文本), 实际 *href* 指向攻击者域名 `okg.enginelark.com`**(见 §5.2)。

图 2: 钓鱼邮件完整内容, 显示的链接为 engine.okg.com, 实际指向 okg.enginelark.com。

3 案件元数据

字段	内容
受害者邮箱	`fwx5618177@gmail.com`(个人 Gmail)
表面发件人	`Security Team <security@hpe.com>`
真实发信通道	Amazon SES(us-east-1), 节点 `a8-53.smtp-out.amazonses.com`
发信 IP	`54.240.8.53`(Amazon Technologies Inc.)
邮件发送时间	2026-08-25 18:22:14 PDT = ***2026-08-26 01:22:14 UTC***
钓鱼落地页	`https://okg.enginelark.com/welcome/new/employee/login`
攻击者服务器	`195.20.204.18`(荷兰,Snel.com B.V.)
真实攻击目标	OK Group / OKX 员工账户系统
被冒用品牌	HPE(邮件身份)、OKX / OK Group(落地页)
分析日期	2026-08-27

4 事件时间线

下表按时间顺序还原从基础设施准备到攻击实施的全过程。所有时间已尽量统一为 UTC。

时间 *(UTC)*	事件
1995-03-24	`hpe.com` 注册 (MarkMonitor),HPE 合法资产。
1998-09-22	`okg.com` 注册 (现为 Amazon Registrar),OK Group 合法资产, 邮件走 Larksuite / 飞书。
2018-06-28	`okpool.top` 由 OK Group 注册 (阿里云 HiChina), **合法自有资产**, 后被用作内部 CNAME 中转。
2026-08-05 09:03:22	攻击者注册**第一个仿冒域名 `engine-okg.com`**(Namecheap, 冰岛隐私代理)。
2026-08-05 13:15:05	攻击者注册**第二个仿冒域名 `enginelark.com`**(Namecheap, 同一隐私代理, 晚 4 小时 12 分)。
2026-08-05 起	攻击者在荷兰 VPS `195.20.204.18` 部署钓鱼程序 (nginx/1.24.0, Ubuntu), 申请 SSL.com 通配符证书 `*.enginelark.com`。
不晚于 2026-08-25	攻击者获得以 `hpe.com` 身份经 Amazon SES 发信的能力 (见 §5.1 溯源)。
2026-08-26 01:22:14	**钓鱼邮件发出**, 经 SES(`54.240.8.53`) 投递至受害者 Gmail,SPF/DKIM/DMARC 全部通过。
2026-08-26(当地)	受害者在收件箱中看到该邮件 (截图时间 09:22)。
2026-08-27	开始分析。经权威 DNS 查询确认 `hpe.com` 的相关 DKIM 选择子已变为 ***NXDOMAIN(已被撤销)***, 表明 HPE / AWS 侧已在处置。落地页仍在线运行。

关键时间推断: 两个仿冒域名在同一天上午先后注册, 距实际发信约 3 周——这是典型的" 提前搭建、择机投放" 的钓鱼行动节奏。DKIM 记录在发信后两天内消失, 说明 HPE 侧的响应处置已经启动。

5 攻击链还原

步骤 1. **投递:** 邮件经 Amazon SES 发出, 携带有效的 d=`hpe.com` DKIM 签名, 与 `From: security@hpe.com` 域对齐,DMARC 判定 `pass`。Gmail 正常投递至收件箱, 无安全警告。

步骤 2. **诱导:** 正文以中文伪造 HPE IT 安全团队通知, 制造"24 小时内重新注册, 否则限制访问权限" 的紧迫感; 配 OKX 真实 CDN Logo 增强可信度。

步骤 3. **障眼法:** 锚文本显示 `https://engine.okg.com/...`, 实际 `href` 指向 `https://okg.enginelark.com`

步骤 4. **窃取:** 落地页 (仿 Ant Design 的"Welcome to join OK Group" 登录页) 索取**企业邮箱 + 验证码**, 通过同源接口 `POST /welcome/new/employee/send-code` 与 `POST /welcome/new/employee/verif` 将数据回传至攻击者服务器。

步骤 5. **脱壳:** 当后端返回" 该邮箱已注册" 时, 页面显示提示并在 3 秒后将受害者跳转至**真实系统** `https://enginelark.okg.com/engine/login`, 使受害者误以为正常、不生疑、不上报, 延长攻击存活时间。

不确定性声明: 页面向受害者索取" 验证码", 意味着必有系统向受害者真实发送了验证码。最合理的解释是攻击者后端**实时向 *OK Group* 真实系统发起请求以触发真实验证码** (即一次性口令 / OTP 中继), 从而实现会话劫持并绕过 2FA。但本报告**未对此进行验证**——验证该行为需向攻击者接口投递测试数据, 属于对第三方系统的未授权交互, 分析中主动回避。此步骤应由 OK Group 安全团队在受控环境下确认。

6 技术分析

6.1 邮件如何通过 *HPE* 身份认证 *(核心发现)*

受害者邮件原始头中的认证结果如下 (逐字摘录):

```
spf=pass    smtp.mailfrom=...@amazonses.com  (client-ip=54.240.8.53)
dkim=pass   header.i=@hpe.com  header.s=kgwu7d2xppvqvpl5d2eir2luwanbipyt
dkim=pass   header.i=@amazonses.com
dmarc=pass  (p=REJECT sp=REJECT dis=NONE)  header.from=hpe.com
```

这不是伪造。 DKIM 签名在密码学上是有效的: 用 `hpe.com` 当时发布的公钥可以验算通过, 签名域 `d=hpe.com` 与信头 `From: hpe.com` 域对齐, 因此即使 HPE 配置了最严格的 `p=reject`,DMARC 仍判定通过。伪造 DKIM 需要私钥, 在密码学上不可行, 所以唯一可能是: **攻击者合法地取得了以 `hpe.com` 身份签名发信的能力**。

关键取证: DKIM 选择子 `kgwu7d2xppvqvpl5d2eir2luwanbipyt` 为 32 位小写随机串, **正是 *Amazon SES "Easy DKIM"* 的 *token* 格式**。SES 用它签名的前提是域名所有者在 DNS 中发布对应的 CNAME 记录。分析时向多个公共解析器 (8.8.8.8 / 1.1.1.1 / 9.9.9.9) 以及 `hpe.com` 权威服务器 `ns1.hpe.com` 直接查询该选择子, **均返回带权威标志 *(aa)* 的 *NXDOMAIN***; 并经随机标签测试确认 `hpe.com` **无泛解析**。结论: 该记录在发信当时 (2026-08-25) **确实存在, 现已被删除**。

两种可能路径 *(需 AWS/HPE 侧确认)*:

- **路径 *A(可能性更高)*——*SES* 凭据泄露:** HPE 或其某供应商的 AWS 账号中 `hpe.com` 早已完成 SES 域名验证 (DKIM CNAME 系正当发布)。攻击者取得该账号的访问密钥 (如代码仓库泄露、CI 日志、供应商被入侵), 直接以已验证身份发信, 所有认证自然通过。此情形下 ***HPE* 的 *DNS* 未被篡改**。
- **路径 *B(可能性较低)*——*DNS* 记录注入:** 攻击者通过被攻陷的 DNS 管理权限或被授权的第三方供应商, 将自己 SES 账号的 DKIM CNAME 写入 `hpe.com`。

倾向路径 A 的理由: 若攻击者真正掌握 `hpe.com` 的 DNS 控制权, 其价值 (签发 TLS 证书、劫持 MX、接管子域) 远高于发一封钓鱼信; 仅用于发信, 更符合" 仅持有一个 SES 发信权限" 的情形。

6.2 链接与视觉伪装

邮件 HTML(Base64 编码正文) 中的锚点为经典锚文本欺骗:

```
<a href="https://okg.enginelark.com/welcome/new/employee/login">
   https://engine.okg.com/welcome/new/employee/login</a>
<img src="https://static.coinall.ltd/cdn/assets/imgs/254/48452487343D915E.pn」
 ↪  g"
 ↪  alt="0KX">
```

显示文本为品牌域 `engine.okg.com`, 实际跳转为攻击者域 `okg.enginelark.com`——手法是把品牌词 `okg` 置于最左作为子域标签, 而真正的注册域是右侧的 `enginelark.com`。Logo 直接热链 OKX 真实 CDN `static.coinall.ltd`, 视觉上无破绽。

6.3 攻击者基础设施

项目	结果
仿冒域名 1	`enginelark.com`(主用), 子域 `okg.enginelark.com` 为钓鱼落地页
仿冒域名 2	`engine-okg.com`(备用 / 早期版本, 同 IP, 证书不匹配)
注册商	Namecheap, Inc.
注册时间	均为 2026-08-05(见时间线)
注册人	隐藏 (Withheld for Privacy ehf, 冰岛雷克雅未克)
NS / MX	`*.registrar-servers.com`(Namecheap 默认 DNS 与邮件转发)
承载 IP	`195.20.204.18`
反向解析	`s46983.hosted-by-snel.com`
托管商	Snel.com B.V. / Ormilon B.V.,AS62370
地理位置	荷兰 Lelystad(公司注册于 Rotterdam, Schuttevaerweg 101)
滥用举报	`report@abuse.bz`(Snel);`abuse@namecheap.com`(Namecheap)
Web 服务	nginx/1.24.0 (Ubuntu),HTTP/2
TLS 证书	通配符 `*.enginelark.com`,SSL.com TLS Issuing RSA CA R1 签发, 有效期至 2027-02-19

两个仿冒域名同源证据: 同一天 (2026-08-05) 先后注册、同为 Namecheap、同用冰岛隐私代理、同解析至 `195.20.204.18`、同一套钓鱼路径 `/welcome/new/employee/*`。`engine-okg.com` 的 TLS 证书仍为 `*.enginelark.com`(不匹配, 浏览器会告警), 判断为备用或早期版本, 最终以 `enginelark.com` 上线。两域名 MX 均指向 Namecheap 邮件转发, **意味着攻击者可在这些域名上收信**。

6.4 被排除的误报

- `okpool.top`、`enginelark.okg.com`、`engine.okg.com` **均为 *OK Group* 合法自有资产**。其中 `enginelark.okg.com` 经 CNAME 链 `enginelarktransit.okpool.top` 指向 OK Group 自己的 AWS ELB, 是内部正常配置。攻击者在钓鱼页中引用 `enginelark.okg.com` 仅用于" 失败跳转"(见 §4 步骤 5), 不代表这些资产被攻陷。**请勿将其列入任何封禁或举报清单。**

7 溯源分析: 能确定什么, 不能确定什么

7.1 可通过公开手段 *(OSINT)* 确定的

- 攻击者基础设施: 两个仿冒域名、承载 IP、托管商、证书、发信通道 (Amazon SES us-east-1) 及唯一的 SES 消息标识符。
- 攻击的定向性质: 对 OK Group 内部系统命名的精确掌握。
- HPE 邮件签名身份被滥用的事实, 及该 DKIM 记录已被撤销的时间窗口。

7.2 公开手段无法确定的 *(需机构 / 执法介入)*

- **攻击者真实身份:** 域名注册人被冰岛隐私代理屏蔽;VPS 租用人信息仅 Snel 掌握。公开渠道到此断线。
- ***HPE* 身份被滥用的确切路径 *(A* 还是 *B):*** 仅 AWS 与 HPE 可通过内部日志区分。
- **验证码中继假设:** 需在受控环境验证, 不应主动触碰攻击者接口。

7.3 最有价值的溯源线索:*Amazon SES* 消息标识符

邮件头中的 Message-ID 与 Feedback-ID 使 AWS 能够反查到**发信的 *AWS* 账号 *ID*、注册邮箱、付款方式、创建与登录源 *IP***。这是全案**唯一可能指向真实身份**的数据。但需注意: 该 AWS 账号**本身可能是被盗用的合法账号** (如 HPE 供应商), 或**以盗刷信用卡 + 假身份新注册**, 因此即便调证, 也可能需再叠加源 IP 关联与支付溯源才能落到真人。

8 威胁指标 *(IOC)*

8.1 可直接用于封禁 / 举报的指标

```
[域名]
  okg.enginelark.com          (钓鱼落地页)
  enginelark.com              (攻击者主域)
  engine-okg.com              (攻击者备用域 / 早期版本)
[IP]
  195.20.204.18               (AS62370 Snel.com B.V. / 荷兰 Lelystad)
  54.240.8.53                 (Amazon SES 发信节点; 勿全段封禁)
[URL 路径]
  /welcome/new/employee/login
  /welcome/new/employee/send-code
  /welcome/new/employee/verify
[TLS 证书]
  CN=*.enginelark.com  (SSL.com TLS Issuing RSA CA R1, 有效期至 2027-02-19)
[Web 指纹]
  Server: nginx/1.24.0 (Ubuntu)
```

8.2 邮件与身份标识符 *(供 AWS / HPE 调证)*

```
SES Message-ID:
  010001a03ba91e87-f71f93ad-d4b6-4573-80e9-e8f961f4617b-000000
Feedback-ID:
  ::1.us-east-1.Mx7G8QgHyj7ECaoZ0+HgaLyxWu91cjlxcyOX7zhFyIw=:AmazonSES
X-SES-Outgoing:
  2026.08.26-54.240.8.53
被滥用的 HPE DKIM 选择子 (发信时存在, 现为 NXDOMAIN):
  kgwu7d2xppvqvpl5d2eir2luwanbipyt._domainkey.hpe.com
表面发件人:  Security Team <security@hpe.com>
信封发件人:  ...@amazonses.com (Return-Path)
```

8.3 排除项 *(合法资产, 勿举报)*

```
okpool.top / enginelark.okg.com / engine.okg.com   —— OK Group 自有资产
static.coinall.ltd                                 —— OKX 真实 CDN(Logo
↪  被热链)
```

9 影响评估与即时处置

9.1 影响评估

- **对个人受害者:** 若已在落地页输入邮箱及验证码, 应视为账户已可能失陷。
- **对 *OK Group*:** 高度定向, 极可能存在同批其他受害者; 若验证码中继假设成立, 攻击可绕过 2FA, 直接威胁员工账户与内部系统。
- **对 *HPE*:** 其邮件签名身份被第三方滥用发送钓鱼, 存在凭据泄露或 DNS 配置被注入的安全事件。

9.2 受害者即时处置 (若已提交信息)

1. 立即在**真实系统** `engine.okg.com` 修改密码。
2. 撤销所有活跃会话 (revoke sessions), 重置 2FA 绑定。
3. 检查登录历史, 排查来自荷兰 / 异常 IP 的登录。
4. 在 Gmail 中对该邮件点击” 举报钓鱼”。

9.3 组织与举报处置 (按优先级)

1. **通报 *OK Group* 安全团队 (最高优先):** 这是针对该公司的定向攻击, 需全员告警、排查 `enginelark.okg.com` 异常登录、确认验证码中继假设。
2. **向 *AWS* 举报:** `abuse@amazonaws.com` / AWS Trust & Safety, 附上 §7.2 的 SES 消息标识符, 请求封停发信账号并保全记录。
3. **向 *HPE* 安全举报:** `security-alert@hpe.com`, 报告其 `hpe.com` DKIM 被滥用签发 (附选择子)。
4. **向 *SSL.com* 举报:** 请求吊销 `*.enginelark.com` 证书, 吊销后浏览器将直接拦截。
5. **向注册商 / 托管商举报下架:** Namecheap `abuse@namecheap.com`、Snel `report@abuse.bz`。
6. **向反钓鱼机构提交:** Google Safe Browsing、APWG(`reportphishing@apwg.org`)。

10 执法与追责路径

核心原则: 个人与技术手段的天花板是” 下架与封号”; 要追到真实身份并追责, **必须由机构走法律程序**。以下按可行性与有效性排序。

1. **报案立案 (最关键一步)。**只有立案后, 执法机关才能向 ***AWS***、***Namecheap***、***Snel*** 发出调证令 (传票 / 司法协助请求), 调取被” 隐私代理” 和” 匿名注册” 屏蔽的真实注册人、付款信息与源 IP。本报告的全部 IOC 即为此步骤准备的证据包。
2. **由 *OK Group* 推动跨境司法协助。**作为被定向攻击的企业,OK Group 有动机与资源报案。承载服务器位于**荷兰 (欧盟)**, 跨境司法协助 (MLAT / 欧盟渠道) 成熟。托管商 Snel 与注册商 Namecheap 在收到合法调证令后须提供客户数据。
3. **通过 *AWS* 追踪发信账号。**凭 SES 消息标识符, 执法机关可要求 AWS 披露发信 AWS 账号的注册与付款信息、源 IP。注意此账号可能是被盗用或匿名注册, 可能需再叠加溯源。
4. **证据固定与时效。**立即对钓鱼页面、证书、DNS 记录、邮件原始头做时间戳存证 (建议哈希 + 可信时间戳), 因为攻击者可能随时销毁基础设施, 部分 DNS 记录 (如 HPE DKIM) 已经消失。

关于”反打对方服务器”的明确声明: 本次分析**未、且不应**对攻击者服务器进行任何端口扫描、漏洞探测、后台爆破或未授权访问。原因:(1) 对第三方系统的未授权访问在多数司法辖区**本身即违法**, 罪犯身份不构成豁免, 且会污染证据链;(2) 该 VPS 可能是被攻击者入侵的**无辜第三方**主机, 或为**蜜罐**, 主动交互会打草惊蛇并招致报复;(3) 该服务器是**抛弃式基础设施**, 其上不含攻击者真实身份信息——真身线索在托管商与 AWS 的后台, 只能经法律程序获取。追责请**全程走执法机关与专业 *DFIR* / *CERT* 渠道**。

附录 *A:* 邮件原始头关键字段 *(*逐字摘录*)*

```
Return-Path: <010001a03ba91e87-f71f93ad-d4b6-4573-80e9-e8f961f4617b-000000
             @amazonses.com>
Received: from a8-53.smtp-out.amazonses.com (54.240.8.53)
          by mx.google.com ... Tue, 25 Aug 2026 18:22:14 -0700 (PDT)
Authentication-Results: mx.google.com;
  dkim=pass header.i=@hpe.com header.s=kgwu7d2xppvqvpl5d2eir2luwanbipyt;
  dkim=pass header.i=@amazonses.com;
  spf=pass smtp.mailfrom=...@amazonses.com;
  dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=hpe.com
DKIM-Signature: v=1; a=rsa-sha256; d=hpe.com;
  s=kgwu7d2xppvqvpl5d2eir2luwanbipyt; ...
From: Security Team <security@hpe.com>
Subject: 安全通知: 员工账户重新注册提醒
Date: Wed, 26 Aug 2026 01:22:14 +0000
X-SES-Outgoing: 2026.08.26-54.240.8.53
```

报告结束——本报告为防御性安全分析, 仅供合法的事件响应、报案与举报用途。分析过程未对任何系统实施未授权访问。