每日网安情报速递【20250611】

一、金融业网络安全事件

1. **巴西“魅影之谜”网络攻击波及七国，恶意浏览器扩展窃取银行数据**
    - Positive Technologies发现代号为“Phantom Enigma”的大规模恶意网络活动，始于2025年初，主要针对巴西用户，波及俄罗斯、捷克、越南、哥伦比亚和墨西哥等七国。攻击者通过被入侵的真实或伪造公司邮箱发送钓鱼邮件，引导用户下载伪装成发票的BAT或MSI文件。执行后会运行PowerShell脚本，安装恶意浏览器扩展（ID为nplfchpahihleeejpjmodggckakhglee），并连接至C2服务器financial-executive[.]com，窃取银行账户的登录凭证和身份认证令牌。

二、重大网络安全事件

1. **全食超市通知员工，其主供应商UNFI遭遇网络攻击将影响商品供应**
    - 全食超市(Whole Foods)告知员工，其主要分销商联合天然食品公司(UNFI)持续的系统中断问题可能需要"数日才能解决"。这家亚马逊旗下的零售巨头在TechCrunch获得的一份内部通讯中表示，UNFI正遭遇"全国性技术系统瘫痪"，而UNFI方面将其定性为网络安全事件。全食超市在员工通知中指出，此次网络攻击影响了UNFI"从仓库拣选和运输产品的能力"，这将"打乱我们的常规配送计划并导致产品缺货"。通知中还包含限制与客户沟通的具体操作指引。全食发言人未说明"数日内解决"这一判断的依据。TechCrunch周二早前报道显示，已有零星报告称部分全食门店及其他依赖UNFI的杂货店出现货架空置现象。此次事件对杂货店及其顾客的实际影响，可能要到本周晚些时候才会充分显现。
2. **针对中国电信业的复杂网络攻击：DRAGONCLONE行动曝光**
3. Cyberpress网站6月10日报道，Seqrite Labs APT团队发布技术分析分析报告，披露了名为“DRAGONCLONE”的网络攻击行动，这是一场针对中国电信巨头中国移动旗下子公司中移铁通有限公司的高度复杂且技术先进的网络攻击。该行动通过精心设计的多阶段攻击链，结合了VELETRIX和VShell两种恶意软件，展示了威胁行为者在恶意软件开发和攻击策略上的深厚技术积累和创新能力。典型手法包括合法软件二进制滥用、DLL侧载、反沙盒反检测技术以及模块化跨平台载荷设计。诡异的是，Seqrite Labs的溯源分析分析显示，攻击活动的黑手竟然与东大有关联。 攻击载体与初始感染阶段 此次攻击的入口是一份伪装成中国移动铁通有限公司内部培训项目的恶意ZIP文件，命名为“attachment.zip”。该压缩包内包含多个可执行文件和DLL，且部分二进制文件带有合法数字签名，这显著提升了攻击载荷绕过安全检测的可能性。特别值得注意的是，攻击者滥用了万兴修复专家（WonderShare RepairIt）软件的合法二进制文件，通过DLL侧载技术实现了恶意DLL（即VELETRIX）隐秘加载。

三、重大数据泄露事件

1. **得克萨斯州警告：30万份事故报告遭黑客入侵账户窃取**
2. 得克萨斯州交通部证实，其系统内一个遭入侵的用户账号被用于非法下载近30万份交通事故报告，可能导致孤星州驾驶员的个人信息遭泄露并被用于金融诈骗。该机构报告称，5月12日发现其"事故记录信息系统"存在异常活动，该系统存储着全州执法部门提交的事故报告。目前得州公共安全部正牵头调查事件成因。此类信息往往是保险诈骗的"金矿"。加州保险专员里卡多·拉腊指出："这起涉嫌汽车保险诈骗的犯罪团伙案件，正是导致全州驾驶员保费上涨的典型案例。"
3. **FreeBuf早报 | Meta暗中追踪数十亿安卓用户；谷歌账户漏洞致攻击者可获取用户手机号**
4. 近期网络安全领域发生多起重大安全事件，其中Meta和Yandex被曝利用WebRTC技术通过Android本地主机套接字暗中追踪数十亿用户的浏览数据并关联身份信息，成功规避传统隐私保护措施，影响覆盖超过578万个网站直至被浏览器厂商封禁才终止。谷歌账户恢复系统存在高危漏洞，攻击者可通过暴力破解方式获取任意用户手机号，利用无JavaScript接口绕过防护机制，通过IPv6和令牌复用技术规避限制，攻击效率高达每秒4万次，谷歌现已修复该漏洞并将漏洞奖励提升至5000美元。卡巴斯基发现名为"图书管理员食尸鬼"的APT组织在俄语区活跃，该组织将AnyDesk、WinRAR等合法工具武器化进行网络间谍活动和加密货币劫持，主要通过钓鱼邮件传播并建立持久控制窃取数据。新型Android银行木马Crocodilus正在全球范围内蔓延，通过伪装广告传播，能够绕过Android 13+安全限制，操控设备通讯录并窃取加密货币私钥，对多国金融安全构成严重威胁。恶意软件Blitz通过篡改版《对峙2》作弊程序传播，具备窃密、挖矿、DDoS攻击能力，并滥用Hugging Face平台建立C2通道，已在26个国家感染近300例用户。企业AI应用安全风险日益加剧，84%企业部署云端AI但62%存在漏洞软件包，38%敏感数据暴露在公网上，30%云资产无人维护，近90%存在闲置资产暴露问题。新型DuplexSpy R

四、重大漏洞风险提示

> 暂无