TCL 电子 2020 年“软件后门”事件案例分析

海南大学一带一路研究院国际数据与舆论研究中心

事件概述

2020 年 12 月 21 日，美国国土安全部声称正在调查 TCL 产品涉嫌安装“后门软件”，令用户数据安全受到威胁的事件， TCL 股价一日暴跌近 15% 。

由于 TCL 电子存在客服人员经验不足，缺乏与第三方网络安全研究人员沟通机制等问题，一个本来不算罕见的技术漏洞在不断的拖延和误解中被不断升级，成为媒体事件；直至被特朗普政府利用，成为“中美科技脱钩”博弈中的一枚棋子。

Caption

Caption

在股价暴跌后， TCL 采取了一系列及时措施，向用户、市场和各国监管机构传达出强有力的积极信号，稳定了股价，并迅速从技术安全和组织架构层面做出改善，最终将一场可能进一步恶化的危机化解，并在借此机会在网络安全相应和处置方面上了一个台阶，获得专业人士的认可。

- 为尽可能真实、客观地复盘此次事件，我们独家采访了“后门漏洞”发现者—独立网络安全研究人员、白帽黑客 Sick Codes （网名）；并且通过追溯整个事件相关新闻报道、博客、推文、当事人原始邮件往来，以及政府及和企业相关声明，将整个事件的时间线还原如下。

Caption

2020 年 9 月 20 日，独立网络安全研究人员 Sick Codes 在 TCL 电视棒中首次发现漏洞，并开始针对 TCL 电视软件安全性进行研究。

2020 年 10 月 27 日，在应用程序安全工程师 John Jackson 的协助下， Sick Codes 和 TCL 公司取得联系， TCL 回复初次报告结果并宣称已修复漏洞。两位独立研究人员检测后，认为 TCL 所称“修复”实质上是 TCL 公司修改了电视文件系统上的重要文件夹，并在用户未同意更新警告前提下自动对漏洞打补丁。

2020 年 10 月 16 日， Sick Codes 发现，可以使用未公开的 TCP/IP 端口通过 Wi-Fi 连接访问 TCL 智能电视的整个文件系统和电视文件，并陆续通过 TCL 供应商网站、推特、 Discourse 论坛、邮件和电话客服等方式联系 TCL 公司，但暂无回音。

2020 年 11 月 8 日，独立技术研究人员在测试模型中发现补丁已被修复，并于 11 月 10 日发布 CVE-2020-27403 研究报告，公布全流程研究成果。

2020 年 11 月 16 日，为回应漏洞风波，TCL 在官方渠道发布公开声明，指称已修复漏洞并更新改进，同时表示被发现后门的型号，并不在北美市场销售。针对其他存在缺陷的电视机，会在未来几天内通过发送补丁解决。

2020 年 12 月 21 日，美国国土安全部副部长 Chad Wolf 在美国传统基金会发表“国土安全与中国的挑战”演讲，其中提到“与中国政府勾连的中国企业机构非法获取美国消费者个人信息、窃取知识产权”，作为证据，提到 TCL 电子“在其所有电视机中使用了后门功能，使用户容易遭受网络破坏和数据泄露。

2020 年 12 月 29 日， TCL 产品运营安全团队回复独立技术研究人员，已完成全部更新并感谢其持续关注。

2021 年 4 月 2 日， Sick Codes 发文表示，很高兴看到 TCL 接受了自己和 John Jackson 此前提出的一些网络安全方面的改进建议，尤其是 TCL 安全响应中心的功能非常全面，令人印象深刻。

2020 年 12 月 10 日， TCL 回应独立技术研究人员已进行模型搭建并更新固件修复漏洞，并承诺会出台相应解决方案。

2020 年 12 月 23 日，公司董事会主席兼执行董事李东生增持 TCL 电子 200 万股，每股作价 5.5889 港元，总金额约为 1117.78 万港元，股价回涨 4% 。

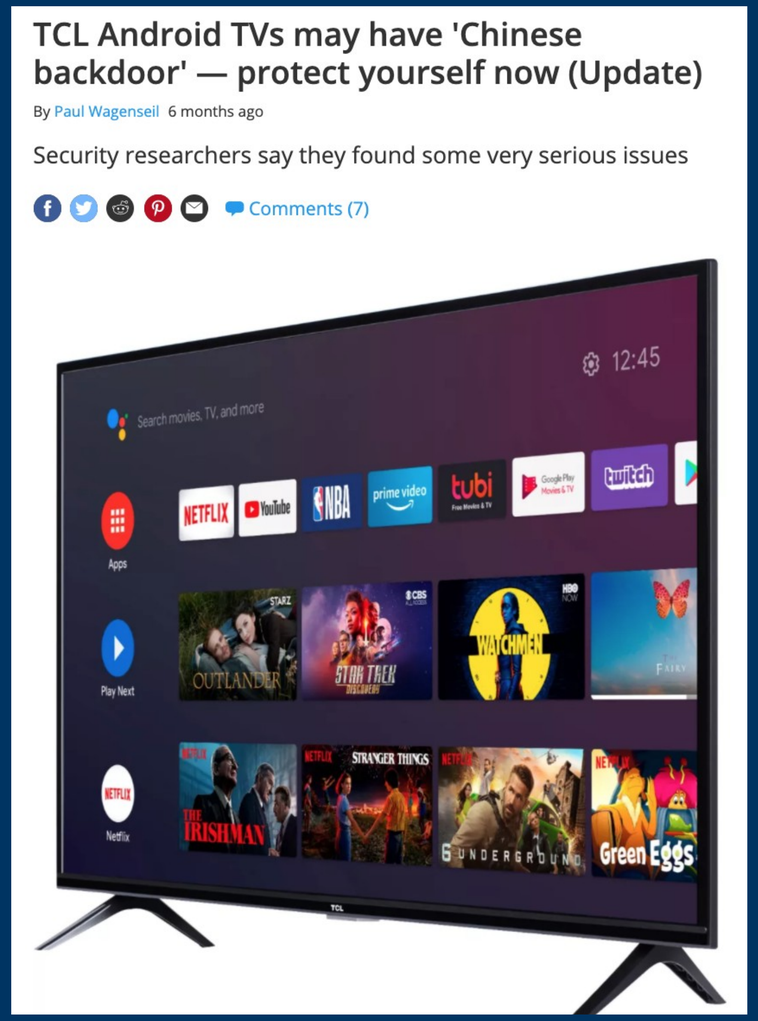
2021 年 3 月， TCL 安全响应中心上线，并公布了最高奖金为 15100 美元的漏洞奖励规则，旨在通过技术研究人员发现的漏洞来进一步增强自身的业务安全性。

事件分析——问题

- TCL 在事件发展初期反应迟缓；
- 第一接触点负责人未能意识到问题的严重程度，相关信息未能提交公司高层，得到应有的重视；
- 内外部沟通、前后台协调进退失据、缺乏明确目标和统一执行；
- 更重要的是， TCL 电子显然对“独立网络安全研究人员”（或称“白帽黑客”）这一群体的专业水平和公众影响力严重低估。

事件分析——问题

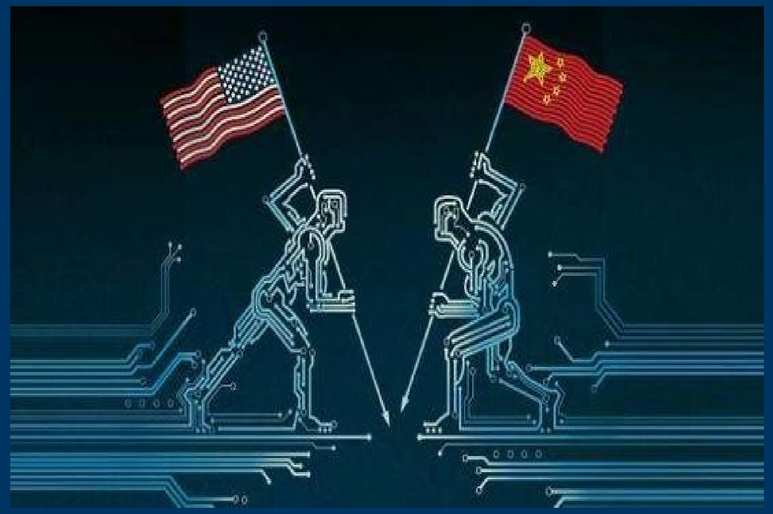
- TCL 在事件发展初期反应迟缓：第一接触点负责人未能意识到问题的严重程度，相关信息未能提交公司高层，得到应有的重视；
- 内外部沟通、前后台协调进退失据、缺乏明确目标和统一执行；



- 对外部舆论形势判断不足，在中美“大脱钩”、西方对中国科技企业高度怀疑的大形势下，未能第一时间对“ backdoor”这样的敏感词汇进行有力的澄清和回应
- 类似“ backdoor”这种笼统、非专业、具有强烈暗示意味且难以证伪的指控，已经成为西方媒体报道和舆论打击中国科技企业信誉的利器；一旦口口相传成为 narrative，会引发大量转发报道，极大刺激公众与政府的敏感神经，极难澄清或自辩

- 对“独立网络安全研究人员”（或称“白帽黑客”）这一群体的专业水平和公众影响力严重低估，缺乏应对、沟通和影响机制
- 绝大多数顶尖跨国科技企业和一些中国企业已经建立较完备的漏洞悬赏 / 奖励体系，利用外部独立网络安全研究人员力量，提升自身软硬件水平，完善客户服务
- 早在美国国土安全部向 TCL 电子发难前两个多月，Sick Codes 于 10 月 16 日已试图联系该公司，指出代码漏洞问题，并提及如果团队需要时间先修复漏洞，他愿意延迟公开报告，但 TCL 反馈不及时，忽视了其善意，在一定程度导致了此次危机升级

事件应对及教训



- 硬件：提升产品质量，供应链韧性和网络安全研发、应对水平；完备内部组织架构和危机处理、协调机制。

- 软件：对宏观和微观局势的研判，海外市场舆论与政策走向的分析；对相关各领域 EOL （专家意见领袖）研究、关系的积累和影响力策略的构建。