

威胁预警 | TeamViewer 疑似入侵事件威胁预警

2019年10月11日，FireEye（火眼）举办的FireEyeSummit大会上，几张演讲的PPT拍照被公开到了网上，其中一张照片提到一款非常流行的远程控制软件TeamViewer曾经疑似被黑客组织入侵，并称其可以访问安装了TeamViewer的任何系统。

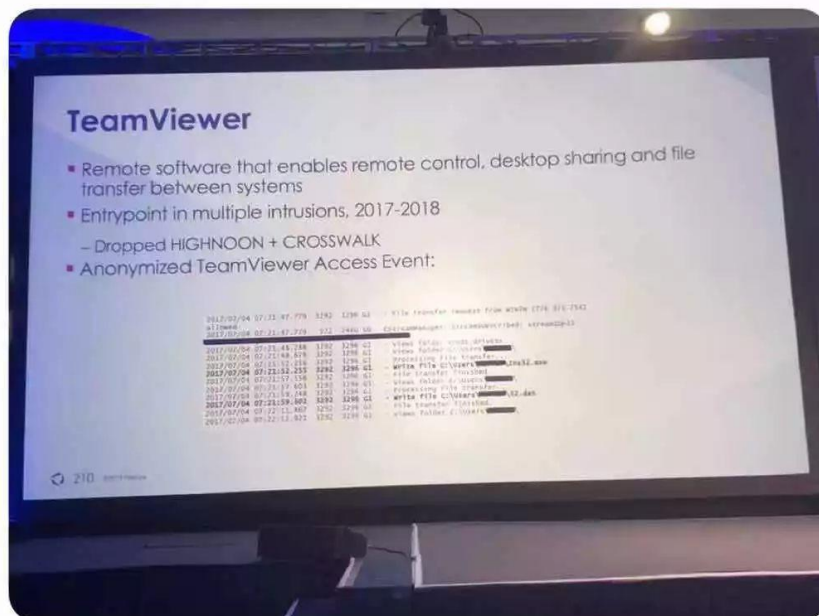


Christopher Glyer
@cglyer



APT41 compromised company behind TeamViewer - which enabled them to access *any* system with TeamViewer installed 🙄🙄🙄

#FireEyeSummit



05:50 · 10/11/19 · Twitter for iPhone

威胁详情

FireEye 的报告，其中提到了他们认为是 APT41(黑客组织) 入侵 TeamViewer。TeamViewer 发言人透露 2016 年有黑客团队尝试入侵 TeamViewer 网络，当时该公司的专家发现可疑活动被迅速阻止，以防止造成重大损失。未透露具体详细损失。

目前未有进一步样本或攻击信息判断 TeamViewer 是否被控制，或是部分客户账号密码被窃取。

但因 TeamViewer 远程穿透直达内网，建议使用者及时卸载或限制 TeamViewer 访问。

修复建议

停止 TeamViewer 进程，近期停止使用 TeamViewer 远程管理软件；

在防火墙中禁止用于 TeamViewer 远程通讯端口 5938；

通过 Web 应用防火墙或其它设备禁止内部主机回连 teamviewer.com 域名。

最后，请持续关注 TeamViewer 的官方回复 (<https://www.teamviewer.cn/cn/>)。