#### 双龙

**别名：**

Threat Group 2889, TG-2889

**可能操作来源:**

中国

**目标:**

* 中国香港
* 法国
* 印度
* 意大利
* 日本
* 缅甸
* 荷兰
* 新加坡
* 韩国
* 南非
* 瑞士
* 泰国
* 土耳其
* 英国
* 美国

**(CFR) 事件类型:**

间谍行为与网络犯罪并行

**组织简介:**

在火眼威胁情报公司公布的报告中，认为APT41（代号双龙）是一个受中国政府资助，同时进行情报收集的间谍活动和个人谋利的网络犯罪双向活动的组织。

双龙组织的活动自2012年开始，始于游戏产业，后来逐渐扩展到间谍活动，直到2014年双向活动达到平衡。该组织的间谍活动瞄准的产业与中国五年发展方向大体一致，包括医疗、高科技产业、媒体、制药、零售、电信、旅游、教育、视频游戏、虚拟货币以及供应链制作相关的软件公司。其情报收集的活动迹象通常出现在与中国国家相关的重大经济事件和政治事件发生之前，且其目标与中共公家政策重点一致。而其处于经济目的的网络犯罪活动通常出现在中国时区的非工作时间，主要，面向游戏产业，包括相关加密货币的操纵。由于其双向活动中出现来自同一邮箱的不同目的的钓鱼邮件，因此被归为同一组织的行为。

双龙组织在攻击活动中，表现出对新漏洞的超快的反应速度和高效的利用能力。在攻击手法上擅长通过破坏签名证书签署恶意软件，以此入侵第三方服务商的软件供应链来访问游戏内部组织，并且利用已入侵的受害者作为跳板进行进一步的渗透。

**参考链接:**

* <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>
* <https://www.fireeye.com/blog/threat-research/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-dojs-findings-on-apt1-intrusion-activity.html>
* <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report-appendix.zip>
* <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf>
* <http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf>