#### APT 38

**可能操作来源:**

朝鲜

**目标:**

* 美国
* 墨西哥
* 智利
* 巴西
* 乌拉圭
* 波兰
* 土耳其
* 俄罗斯
* 孟加拉国
* 马来西亚
* 越南
* 菲律宾

（针对银行、媒体和政府机构）

**(CFR) 事件类型:**

受政府支持的、以经济利益为目的犯罪行为

**组织简介:**

APT38被认为其主要任务是针对金融机构和操纵银行间金融系统，为朝鲜政权筹集大笔资金。其攻击痕迹与朝鲜其他间谍组织有一定程度上的联系，因此被认定其经济犯罪行为是受到朝鲜政府支持的。但其存在与其他纯间谍行为的朝鲜网络间谍组织明显差异，因此被独立定义为APT38。

APT38在攻击工具上有与TEMP.Hermit存在共享的迹象，但双方目的明显不同。APT38几乎完全处于经济获利为目的，也有可能为更多其他行为提供资料和支持，但其攻击结果是取得经济利益。

**参考链接:**

* <https://content.fireeye.com/apt/rpt-apt38>
* <https://www.us-cert.gov/ncas/alerts/TA17-164A>
* <https://securelist.com/lazarus-under-the-hood/77908/>