#### 小精灵

**别称:**

无

**可能操作来源:**

伊朗

**目标:**

* 沙特阿拉伯
* 美国
* 比利时
* 约旦
* 英国
* 泰国
* 中国
* 阿拉伯联合酋长国
* 摩洛哥
* 捷克共和国

**(CFR) 事件类型:**

间谍行为

**组织简介:**

该组织于2015年底或2016年初开始活跃，主要从事扫描易受攻击的网站，并利用这些网站识别潜在目标，以进行攻击或建立指挥控制(C&C)基础设施。它已经成功入侵了许多目标，包括政府、研究、化学、工程、制造、咨询、金融、电信和其他几个行业的组织。

从2016年中到2017年初，APT33入侵了一家美国航空航天组织，并针对一家持有航空资产的沙特阿拉伯商业集团。在同一时期，APT33还针对一家从事炼油和石化产品的韩国公司进行入侵。在2017年5月，APT33使用一个恶意文件瞄准了一家沙特组织和一家韩国企业集团，该文件试图诱骗受害者为一家沙特阿拉伯石化公司提供职位空缺。

对其目标中沙特阿拉伯的与航空相关的多家公司进行分析，结果表明APT33可能手机沙特阿拉伯军事航空能力相关的请报，以增强伊朗的国内航空能力或支持伊朗针对沙特阿拉伯的军事和战略决策。以沙特阿拉伯组织为目标可能是试图深入了解区域竞争对手，而以韩国公司为目标可能是由于韩国最近与伊朗石化行业建立了伙伴关系，以及韩国与沙特石化公司的关系。由于伊朗希望扩大自己的石化产品生产并提高其在该地区的竞争力，因此APT33可能将这些组织作为目标。

在攻击手法上该组织也是惯用鱼叉钓鱼式攻击，并且使用代理服务器来隐藏自己的身份。

涉及能源和石化产品的组织的普遍目标反映了先前观察到的其他可疑伊朗威胁组织的目标，这表明整个伊朗行为体对该部门具有共同利益。

**参考链接:**

* <https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html>
* <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/elfin-apt33-espionage>
* <https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html>