#### APT 39

**别名**

金龟子（Chafer）、ITG07

**可能操作来源:**

伊朗

**目标:**

* 伊朗（本国）
* 以色列
* 约旦
* 阿拉伯联合酋长国
* 沙特阿拉伯
* 土耳其
* 非洲

（中东地区）

**(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:**

APT39专注于个人信息，以支持符合伊朗国家优先事项的监视，跟踪或监视操作，或者可能创建其他访问方式和媒介来促进未来的战役。

APT39主要利用SEAWEED和CACHEMONEY后门以及POWBAT后门的特定变体。尽管APT39的目标范围是全球性的，但其活动却集中在中东。APT39优先考虑电信行业，并针对旅游业和支持该行业的IT公司以及高科技行业。

在2015年的早期攻击中，赛门铁克证明Chafer可能通过SQL注入攻击来攻击其Web服务器，从而将恶意软件投放到它们，从而破坏了目标组织。在2017年，该组织在其工具箱中添加了一种新的感染方法，使用了恶意文件，这些文件很可能是通过发送给目标组织工作人员的鱼叉式网络钓鱼电子邮件传播的。屏幕捕获实用程序似乎用于初始信息收集，它仅在每次感染开始时短暂使用。进行此初始活动后，攻击者通常使用PowerShell下载器将更多工具下载到计算机上，并开始在受害者的网络中进行扩张。

**参考链接:**

* <https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html>
* <https://malpedia.caad.fkie.fraunhofer.de/actor/apt39>
* <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions>
* <https://securelist.com/chafer-used-remexi-malware/89538/>