#### HAMMER DUKE

**别称:**

YTTRIUM，The Dukes，Cozy Bear，CozyDuke

**可能操作来源:**

俄罗斯

**目标:**

西方政府和相关组织，如政府部门和机构、政治智库和政府分包商。

独立国家联合体成员国的政府;

亚洲、非洲和中东各国政府;

与车臣极端主义有关的组织;

从事受管制物质和毒品非法贸易的俄语使用者。

**(CFR) 事件类型:**

间谍行为

**组织简介:**

该组织几乎每年都要进行一次大规模的鱼叉式网络钓鱼活动，目标是与政府机构和附属组织有关联的成百上千的收件人。除了这些大规模的战役之外，该组织还会利用不同的工具集，持续地、同时地进行更小的、更有针对性的活动。这些活动的目标和时间安排似乎符合当时俄罗斯联邦已知的外交和安全政策利益。

该组织的行为痕迹表示他们会对发表的关于他们工具集和操作的研究迅速作出反应。然而，团队(或他们的赞助商)对他们的操作非常重视，尽管他们会尝试修改他们的工具以逃避检测并重新获得隐身，但他们不会因此而停止操作，而是会逐步修改他们的工具，同时明显地继续按照之前的计划进行。在一些最极端的案例中，该组织也曾使用未经修改的工具进行活动。

**参考链接:**

* <https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf>