#### 沙皇小队

**别称:**

蛇鲭鱼（SNAKEMACKEREL），燕尾服（Swallowtail），Group 74，Sednit，Sofacy，兵风暴（Pawn Storm），奇幻熊（Fancy Bear），锶（STRONTIUM），沙皇小队

（Tsar Team），Threat Group-4127，TG-4127

**可能操作来源:**

俄罗斯

**目标:**

格鲁吉亚和高加索  
 • 内务部  
 • 国防部  
 • 撰写高加索问题的记者  
 • 高加索中心  
东欧政府和军队  
 • 波兰政府  
 • 匈牙利政府  
 • 东欧外交部  
与安全相关的组织  
 • 北约  
 • 欧安组织  
 • 国防武官  
 • 国防活动和展览

**事件类型:**

间谍行为

**组织简介:**

自2007年以来，APT28系统地发展其恶意软件，使用灵活和持久的平台指示长期使用计划。在该组织恶意软件中明显可见的编码实践表明，他们具有高超的技能，并对复杂的逆向工程工作感兴趣。

该组织使用恶意软件与灵活且持久的平台，不断改进恶意软件以供继续使用。恶意软件是针对特定受害者的环境量身定制的，旨在阻止逆向分析。该组织通常使用HTTP协议的后门，也使用受害者邮件服务器的后门。

**参考链接:**

* <https://www.justice.gov/file/1080281/download>
* <https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign>
* <https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf>
* <https://symantec-enterprise-blogs.security.com/blogs/election-security/apt28-espionage-military-government>
* <http://securityaffairs.co/wordpress/65318/hacking/dde-attack-apt28.html>
* <https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html>