#### 科多索

**别称:**

Codoso, C0d0so0, Codoso Team, 太阳店集团

**可能操作来源:**

中国

**目标:**

不同行业的组织，包括国防，能源，金融，政府部门以及政治异见人士和智囊团

**(CFR) 事件类型:**

间谍行为

**组织简介:**

2017年，APT19使用了三种不同的技术来试图对目标进行攻击。5月初，网络钓鱼诱骗利用了RTF附件，该附件利用了CVE 2017-0199中描述的Microsoft Windows漏洞。5月底，APT19切换为使用启用了宏的Microsoft Excel（XLSM）文档。在最新版本中，APT19向XLSM文档添加了应用程序白名单绕过功能。至少有一个观察到的网络钓鱼诱饵传递了Cobalt Strike有效载荷。

该组织的关键攻击事件包括：

* 2014年底，使用受感染的Forbes.com网站作为“水坑”，进行了广泛宣传；
* 2010年10月，使用挪威诺贝尔和平奖委员会网站进行的水坑袭击；
* 2011年4月针对政府组织的鱼叉式网络钓鱼攻击；
* 2013年5月，使用多个网站对维吾尔族人进行了水坑攻击。

**参考链接:**

* <http://securityaffairs.co/wordpress/43970/cyber-crime/codoso-apt-cyber-espionage-campaign.html>
* <https://exchange.xforce.ibmcloud.com/collection/Codosoo-APT-Group-ef0c50a8ee91fb805a9b2a710e687c75>
* <https://www.darkreading.com/attacks-breaches/chinese-hacking-group-codoso-team-uses-forbescom-as-watering-hole-/d/d-id/1319059>
* <https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html>
* <https://unit42.paloaltonetworks.com/new-attacks-linked-to-c0d0s0-group/>