#### WEKBY

**别称:**

TG-0416, 炸药熊猫（Dynamite Panda）, Threat Group-0416

**可能操作来源:**

中国

**目标:**

美国

**(CFR) 事件类型:**

间谍行为

**组织简介:**

WEKBY组织是一个隐秘且非常成功的高级持续威胁（APT）小组，自2009年以来至少针对各种垂直领域，包括航空航天与国防、建筑与工程、教育、健康与生物技术、高科技、电信和运输等进行入侵以窃取相关资料。该组织经常开发或改编的零时差攻击进行操作。Hacking Team漏洞的使用数据，展示了该组织如何转移资源（即选择目标，准备基础结构，制作消息，更新工具），以利用意外机会，例如新暴露的漏洞。其关键攻击事件包括：

* 2014年违反了受HIPAA保护的私人数据，并窃取了450万患者的病例；
* 2015年8月，一场鱼叉式攻击泄露了其对Adobe Flash 漏洞的利用(CVE-2015-5119)；
* 2016年月，Wekby组使用与HTTPBrowser恶意软件家族有关的恶意软件对美国一家组织进行入侵，并以DNS请求作为命令和控制机制。

**参考链接:**

* [https://www.secureworks.com/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems#end1](https://www.secureworks.com/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems" \l "end1)
* <https://unit42.paloaltonetworks.com/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/>
* <https://www.cfr.org/cyber-operations/apt-18>
* <https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop>