#### INESHE

**别称:**

IXESHE，DynCalc，带编号的熊猫(Numbered Panda)，DNSCALC

**可能操作来源:**

台湾、美国

**目标:**

* 东亚各国政府
* 台湾电子制造商
* 美国

**事件类型：**

间谍行为

**组织简介:**

IXESHE通常利用带有恶意附件的目标电子邮件危害受害者系统。这些电子邮件通常针对特定的受害者，包含已经“武器化”的恶意附件。例如通过pdf文件，将恶意可执行文件投放到目标系统。

IXESHE攻击者几乎总是利用成功入侵的服务器作为命令和控制（C&C）服务器。这种技术也允许攻击者掩盖他们的踪迹，因为在受害者的公司网络中有C&C服务器意味着他们的行为只占流量的很小一部分。攻击者故意使用被破坏的机器和动态域名系统(DNS)服务，通过混淆他们的活动和合法个人的数据来隐藏他们存在的痕迹。

**参考链接:**

* <https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html>
* <https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html>
* <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf>
* <https://www.crowdstrike.com/blog/whois-numbered-panda/>
* <https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html>