#### APT 1

**别称:**

评论组（Comment Group），评论熊猫（Comment Panda）, PLA Unit 61398, APT 1, APT1, Advanced Persistent Threat 1, Byzantine Candor, Group 3, TG-8223, , Brown Fox, GIF89a, ShadyRAT, Shanghai Group

**可能操作来源:**

中国

**目标:**

* 美国
* 台湾
* 以色列
* 挪威
* 阿拉伯联合酋长国
* 英国
* 新加坡
* 印度
* 比利时
* 南非
* 瑞士
* 加拿大
* 法国
* 卢森堡
* 日本

**(CFR) 事件类型:**

间谍行为

**组织简介:**

APT1很可能是政府赞助的，而且是中国网络威胁中最持久的行动者之一。我们认为，APT1能够开展如此长期和广泛的网络间谍活动，在很大程度上是因为它得到了政府的直接支持。为了找出这一活动背后的组织，我们的研究发现，人民解放军61398部队在任务、能力和资源方面与APT1类似。解放军61398部队也恰好位于APT1活性出现的起始区域。

据信，APT1是中国人民解放军第二局总参谋部第三局（GSD）（MUCD61398）。APT1已经系统地从至少141个组织窃取了数百tb的数据，并展示了同时从数十个组织窃取数据的能力和意图。

**参考链接:**

* [https://en.wikipedia.org/wiki/PLA\_Unit\_61398](https://en.wikipedia.org/wiki/PLA_Unit_61398" \t "https://aptmap.netlify.app/_blank)
* [http://intelreport.mandiant.com/Mandiant\_APT1\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf" \t "https://aptmap.netlify.app/_blank)
* [https://www.cfr.org/interactive/cyber-operations/pla-unit-61398](https://www.cfr.org/interactive/cyber-operations/pla-unit-61398" \t "https://aptmap.netlify.app/_blank)
* [https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf](https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf" \t "https://aptmap.netlify.app/_blank)
* [https://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/](https://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/" \t "https://aptmap.netlify.app/_blank)
* [https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html](https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html" \t "https://aptmap.netlify.app/_blank)
* [https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/](https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/" \t "https://aptmap.netlify.app/_blank)
* [https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf](https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf" \t "https://aptmap.netlify.app/_blank)
* [https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=f1265df5-6e5e-4fcc-9828-d4ddbbafd3d7&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments](https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=f1265df5-6e5e-4fcc-9828-d4ddbbafd3d7&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments" \t "https://aptmap.netlify.app/_blank)
* [https://attack.mitre.org/groups/G0006/](https://attack.mitre.org/groups/G0006/" \t "https://aptmap.netlify.app/_blank)
* [https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html](https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html" \t "https://aptmap.netlify.app/_blank)