# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:36:05 UTC



## Tool: 3102 RAT

| | |
|---|---|
| Names | 3102 RAT |
| Category | Malware |
| Type | Backdoor, Info stealer |
| Description | (Palo Alto) On May 6 and May 11, 2015, Unit 42 observed two targeted attacks, the first against the U.S. government and the second on a European media company. Threat actors delivered the same document via spear-phishing emails to both organizations. The actors weaponized the delivery document to install a variant of the '9002 RAT' Trojan called '3102' that heavily relies on plugins to provide functionality needed by the actors to carry out on their objectives.<br><br>The 3102 payload used in this attack also appears to be related to the EvilGrab RAT payload delivered in the watering hole attack hosted on the President of Myanmar's website in May 2015. Additionally, we uncovered ties between the C2 infrastructure and individuals in China active in online hacking forums that claim to work in Trojan development. |
| Information | <https://unit42.paloaltonetworks.com/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/> |

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

### All groups using tool 3102 RAT

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Nightshade Panda, APT 9, Group 27 | | 2013-Sep 2016 | |

*1 group listed (1 APT, 0 other, 0 unknown)*

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fae56cde-ba06-490d-be43-2b637ac32ac0