

# APT32 & METALJACK Appendix

## Table of Contents

<b>APT32 Actor Overview.....</b>	<b>1</b>
<b>METALJACK DETAILS.....</b>	<b>1</b>
Executive Summary .....	1
Threat Detail.....	2
Attack Vector.....	2
<b>APT32 Attribution of METALJACK .....</b>	<b>2</b>
<b>Technical METALJACK Characteristics .....</b>	<b>3</b>

## APT32 Actor Overview

APT32 (OceanLotus), formerly known as TEMP.Junk, is a cyber espionage actor with a Vietnam nexus who conducts foreign and domestic surveillance using commercial tools against internal targets. This actor has targeted China's government and private sectors. Domestic victims include journalists, and foreign victims include Vietnamese dissidents abroad, Chinese Government entities, and public and private organizations involved in oil, gas, and shipping activity in the South China Sea. Though this activity is specifically focused on Vietnamese politics, it appears to affect multiple regions, and it may affect the global dissident community and non-governmental organizations, media, and government agencies that have some connection to this community.

## METALJACK DETAILS

### Executive Summary

- METALJACK is a suspected APT32 (OceanLotus) backdoor targeting various organizations that align with Vietnamese national interests, including the legal sector, nonprofits, healthcare, and media.
- Typically delivered via a .rar file with two Word documents, METALJACK may also be delivered directly via email or downloaded from public storage services.
- APT32 continues to diversify their tactics, techniques, and procedures (TTPs) to increase their potential victim landscape and decrease the chance of detection.

## Threat Detail

Mandiant Threat Intelligence believes that APT32 is leveraging a backdoor dubbed "METALJACK" in operations aligned with Vietnamese national interests. Data derived from open sources and FireEye devices indicates that METALJACK has been employed since at least July 2017 to target organizations in Vietnam, Cambodia, Fiji, South Korea, and the UK. The tool employs various anti-disassembly and anti-analysis techniques and includes multiple obfuscation and encryption routines likely to circumvent detection and increase chances of successful infection. As a result, METALJACK targeting likely expands beyond the legal and human rights industries to include historic APT32 targets.

- Filenames and headers indicate that METALJACK commonly targets legal and human rights organizations throughout Asia.
- APT32 previously documented targets include the manufacturing, hospitality, network security, technology infrastructure, banking, and media industries.
- In some of the observed METALJACK instances, DLL side-loading is used to circumvent anti-virus scanners. This method has been observed in previous suspected APT32 malware, such as GOOPY and ESET's recent report on "OceanLotus."

## Attack Vector

We have identified at least two vectors with which METALJACK is delivered. Typically, the malware is delivered through Word documents delivered via spearphishing in .rar files that exploit multiple vulnerabilities, increasing the chance of successful execution. We have also observed METALJACK downloading from a Content Delivery Network (CDN) service or being sent directly in an email.

## APT32 Attribution of METALJACK

Based on our observations and historical knowledge, we assess with moderate confidence that METALJACK is unique to APT32 given similarities in TTPs, targeting, and malware features.

- APT32 is known for their use of compressed files, such as .rar files, that contain exploit documents to deliver malware.
- The entities targeted by METALJACK align with APT32 previous targeting that align with Vietnamese interests.
- One METALJACK sample (MD5: 9753cf34b282ec34730c95ae1fb18411) was uploaded to a multi-scanning service by the same submitter, two minutes after a known APT32 scriptlet (MD5: 13120e01610464e4a7b674570b4ebf74).

Malware characteristics shared between METALJACK and other identified APT32 tools also bolster the connection to APT32.

- Two documents (MD5: c234632f3c538bd9e88d8ffc3cba9b8b and MD5: f5469ae914065e4afea7bba8bc13c29d) were identified as being connected to this campaign because of a unique header and OLE Object format that matches documents used to deliver METALJACK; however, these two documents actually result in WINDSHEILD, a different APT32 tool.
- METALJACK uses a domain generation algorithm (DGA) to generate unique domains to communicate with its command and control (C&C) server. In this case, the domains are generated based on the format "<encoded computer name>.<encoded ID from resource>.<DNS host>," as seen in the following communication(s):  
nnggmpggmeggnoggnnggnjggngggijgg.<subdomain>.com. This particular DGA is similar to a previously identified APT32 tool SOUNDBITE.

## Technical METALJACK Characteristics

- METALJACK capabilities include—but are not limited to—system survey, process creation, file system interaction, registry modification, RC4 encryption/decryption, loading and writing of additional modules within registry, execute shellcode, and modify environmental variables.
- Leverages various anti-disassembly and anti-analysis techniques.
- METALJACK infections have been observed to include multiple stages and multiple obfuscation and encryption routines.
- METALJACK communications are performed using a custom binary protocol over, at the least, TCP.
- Beaconsing is performed through DNS requests.