

# Raw Threat Intelligence - Google Docs

 docs.google.com/document/d/1oYX3uN6KxIX\_StzTH0s0yFNNNoHDnV8VgmVqU5WoeErc/edit

## Raw Threat Intelligence

[clearskysec.com](https://clearskysec.com) | [info@clearskysec.com](mailto:info@clearskysec.com) | updates: [@ClearskySec](https://twitter.com/ClearskySec)

- **Public analysis** - "Raw Threat Intelligence" is a public document with primary analysis of cyber attack campaigns.
- **Analysts** - Analysis is performed by ClearSky Cyber Security.
- **Comments** - The document is open for comments - feel free to write tips, questions, leads and suggestions.
- **Ongoing** - Analysis is ongoing, new incidents are added as they are investigated.
- **HTML version** - is available [here](#)

If you have been targeted you can get our help for free  
[clearskysec.com/free-targeted-attacks-research](https://clearskysec.com/free-targeted-attacks-research)

## 2021-04-20 Suspicious Lazarus Documents

While monitoring VirusTotal, we identified four malicious documents that share common TTPs. These docx files using remote template injection to download a dotx file from a C2 server, which has a unique remote IP address. Two of the four IPs we have found have been previously reported by F-Secure as Lazarus group. We suspect with medium-low confidence that the new IP addresses are also controlled by the Lazarus group. Unfortunately, we couldn't retrieve the malicious templates to further investigate the kill chain

Filename: my2.docx

This version of Google Chrome is no longer supported. Please upgrade to a [supported browser](#). [Dismiss](#)