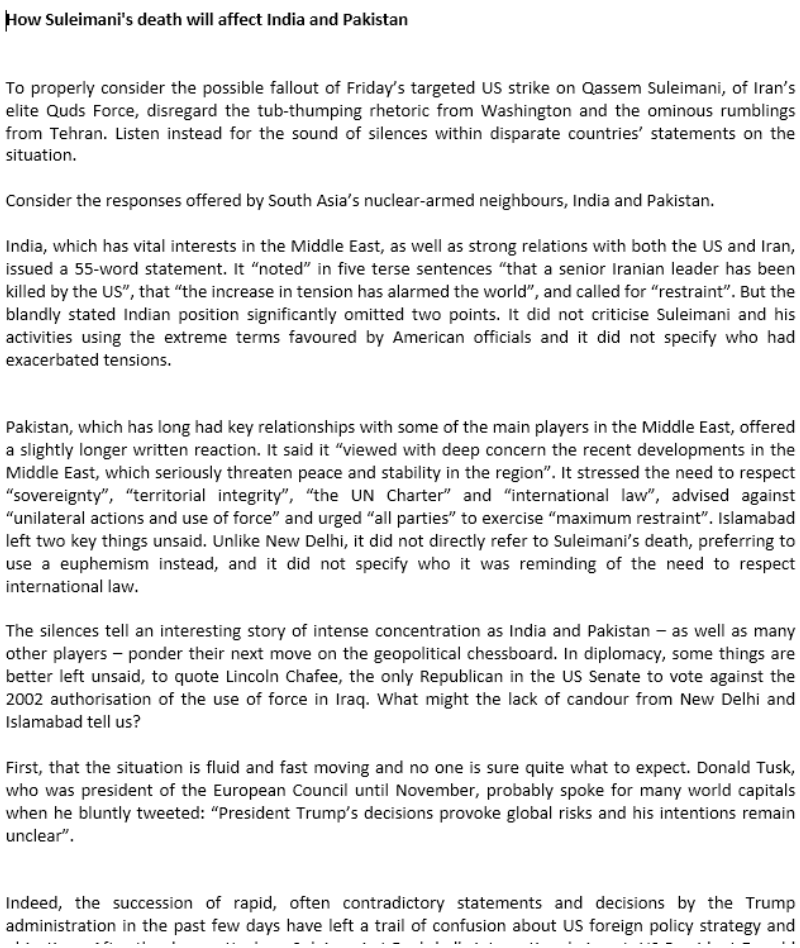
TA428 Group abusing recent conflict between Iran and USA

lab52.io/blog/icefog-apt-group-abusing-recent-conflict-between-iran-and-eeuu/

Recently, a suspicious document has caught our attention due to its recent creation date (06-01-2020) and its title “How Swuleimani’s death will affect India and Pakistan.doc” which is directly related to recent political events between Iran and the USA.



How Suleimani's death will affect India and Pakistan

To properly consider the possible fallout of Friday’s targeted US strike on Qassem Suleimani, of Iran’s elite Quds Force, disregard the tub-thumping rhetoric from Washington and the ominous rumblings from Tehran. Listen instead for the sound of silences within disparate countries’ statements on the situation.

Consider the responses offered by South Asia’s nuclear-armed neighbours, India and Pakistan.

India, which has vital interests in the Middle East, as well as strong relations with both the US and Iran, issued a 55-word statement. It “noted” in five terse sentences “that a senior Iranian leader has been killed by the US”, that “the increase in tension has alarmed the world”, and called for “restraint”. But the blandly stated Indian position significantly omitted two points. It did not criticise Suleimani and his activities using the extreme terms favoured by American officials and it did not specify who had exacerbated tensions.

Pakistan, which has long had key relationships with some of the main players in the Middle East, offered a slightly longer written reaction. It said it “viewed with deep concern the recent developments in the Middle East, which seriously threaten peace and stability in the region”. It stressed the need to respect “sovereignty”, “territorial integrity”, “the UN Charter” and “international law”, advised against “unilateral actions and use of force” and urged “all parties” to exercise “maximum restraint”. Islamabad left two key things unsaid. Unlike New Delhi, it did not directly refer to Suleimani’s death, preferring to use a euphemism instead, and it did not specify who it was reminding of the need to respect international law.

The silences tell an interesting story of intense concentration as India and Pakistan – as well as many other players – ponder their next move on the geopolitical chessboard. In diplomacy, some things are better left unsaid, to quote Lincoln Chafee, the only Republican in the US Senate to vote against the 2002 authorisation of the use of force in Iraq. What might the lack of candour from New Delhi and Islamabad tell us?

First, that the situation is fluid and fast moving and no one is sure quite what to expect. Donald Tusk, who was president of the European Council until November, probably spoke for many world capitals when he bluntly tweeted: “President Trump’s decisions provoke global risks and his intentions remain unclear”.

Indeed, the succession of rapid, often contradictory statements and decisions by the Trump administration in the past few days have left a trail of confusion about US foreign policy strategy and

The document is in RTF format, and has an OLE object related with the Equation Editor. During the last years, this OLE objects have been a good indicator that a document may aim to exploit the CVE-2018-0798 vulnerability in order to infect with some kind of malware. This particular document turns out to be one of these examples, and does it by dropping a binary called 8.t. in the “% TEMP%” folder of the user.

Up to this point, everything coincides in terms of TTPs with what is described in the following report, from ProofPoint related with a suspected Chinese cybercrime Group known as TA428.

After this infection chain, what we get is a DLL executable file with extension “.wll” used for “Word.addin.8” files, that is installed in the path “%APPDATA%\Microsoft\Word\STARTUP” which causes that MSWord at the next application startup to load this “.wll” executable file. (Which also coincides with the TTPs described in the previous post)

This DLL consists in a packed version of a PoisonIvy RAT sample, that after a few seconds makes traffic to the C2 server “95.179.131.29”, through port 443, and in case of error, through port 8080 using HTTP traffic.

The IP address is part of the infrastructure that appears in the post, indicating that it is probably the same actor reusing his old infrastructure in a new campaign, taking advantage of the conflict mentioned at the beginning of the article.

It is always critical to remain alert with any attachments that is related to any recent geopolitical conflict, as previously stated, the attackers usually take advantage of them as a mean of infecting their victims through this kind of phishing campaings.

Document SHA256	0eb7ba6457367f8f5f917f37ebbf1e7ccf0e971557dbe5d7547e49d129ac0e98
Poison Ivy SHA256	02dec90a18545d4bfbac5de19c6499142e141c3c0abaecdc8ac56b8eede167aa
Poison Ivy C2	95.179.131.29