A Hit is made: Sidewinder APT successfully cyber attacks Pakistan military focused targets

: 6/20/2022

Check Point Research (CPR) reported evidence suggesting that Pakistan Air Force's Headquarters was a victim of a successful attack conducted by Sidewinder, a suspected India hacker's APT group.

During May 2022, several malware samples and two encrypted files, related to the attack were uploaded to Virus Total. After decrypting the encrypted files, CPR saw that one of them is a .NET DLL related to an APT group called "Sidewinder" that is attributed to India based hackers, and known to target entities in Pakistan. The malware utilized in this espionage operation is an information stealer malware, exclusively used by this APT, usually leveraged to steal documents from the following types: *.docx .doc .xls .xlsx .pdf .ppt .pptx .rar .zip*.

The second file CPR decrypted was highly meaningful. It was produced by the information-stealer malware and contained a list of all the relevant files on the infected computer. Looking at the collected names, CPR found a mixture of files relating to different topics, most of which are related to military and aeronautics, with the remaining on communication, nuclear facilities, higher education, war history, architecture and electricity. In addition, some file paths pointed to documents from "Chairman Joint Chiefs of Staff Committee', reportedly the highest ranking officer in Pakistan's military. Overall many file paths in file (about 20,000 file names) were discovered, with the weight of 2MB suggesting an infected machine was used, or had access, to a drive mutual to multiple people within the organization.

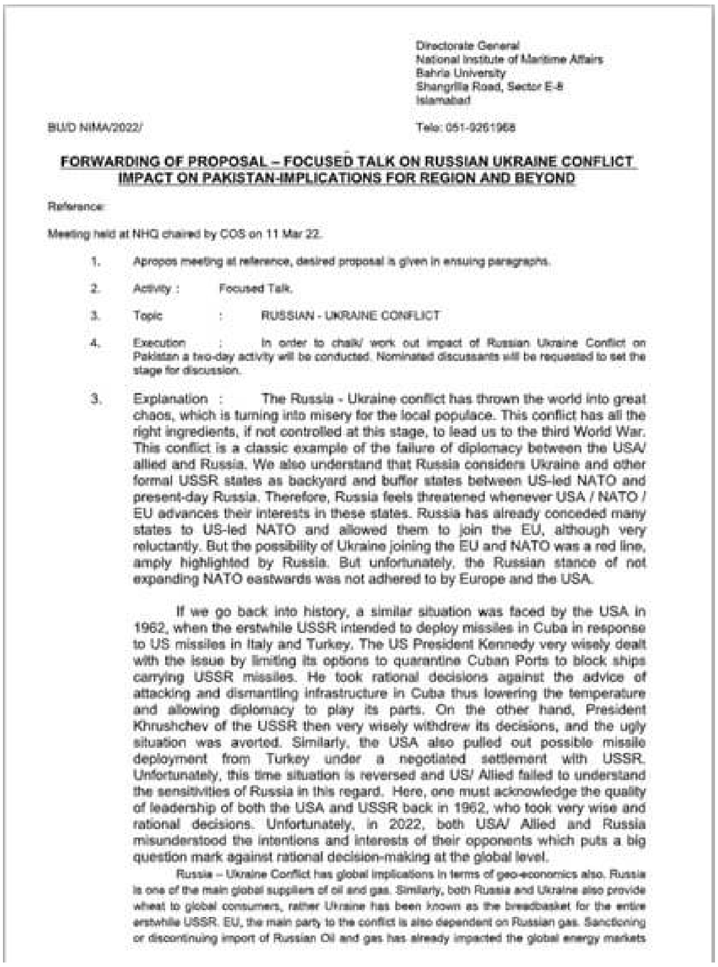
From the names of the files and directories, we can also learn about usernames which belongs to the victim, including ***AHQ-STRC3***. This, in addition to other elements in the file names, seems to suggest that ***AHQ stands for Air Headquarters Pakistan*** which is the headquarters for the Pakistan Air Force. There are also documents that explicitly mention Air Headquarters in their file names, strengthening the link between the 'AHQ' in the username to the Pakistan Airforce. Investigations found an additional username called "***gnss***" which unfortunately didn't produce any useful leads, though another guess might be that this refers to ***"Global navigation satellite system"***. The files seen also had names relating to satellite communication, implying data around this.

While the analysis of malware files uploaded to Virus Total often reveals the identity of the targets of the attack campaign, it is uncommon to also expose evidence that the attack was actually successful. In this case, CPR saw that a log file, produced by the malware, exposed the identity of the victims, including names of sensitive documents and systems.

This leads CPR to assume that the intrusion was eventually detected and analyzed by the victim or security analysts operating on its behalf.

SideWinder : Suspected Indian based APT Group

SideWinder is an APT group that strongly focuses on Pakistan and China government organizations. At the end of March, 2022, CPR published an analysis of SideWinder's malicious document, which exploited the Russia-Ukraine conflict. Judging by its content, the intended targets of the attack were Pakistani entities; the bait document contains the document of National Institute of Maritime Affairs of Bahria University in Islamabad, and is titled "*Focused talk on Russian Ukraine Conflict Impact on Pakistan*."



Directorate General
National Institute of Maritime Affairs
Bahria University
Shangrilla Road, Sector E-8
Islamabad

BU/D NIMA/2022/

Tele: 051-9261968

FORWARDING OF PROPOSAL – FOCUSED TALK ON RUSSIAN UKRAINE CONFLICT IMPACT ON PAKISTAN-IMPLICATIONS FOR REGION AND BEYOND

Reference:

Meeting held at NHQ chaired by COS on 11 Mar 22.

1. Apropos meeting at reference, desired proposal is given in ensuing paragraphs.

2. Activity : Focused Talk.

3. Topic : RUSSIAN - UKRAINE CONFLICT

4. Execution : In order to chalk/ work out impact of Russian Ukraine Conflict on Pakistan a two-day activity will be conducted. Nominated discussants will be requested to set the stage for discussion.

3. Explanation : The Russia - Ukraine conflict has thrown the world into great chaos, which is turning into misery for the local populace. This conflict has all the right ingredients, if not controlled at this stage, to lead us to the third World War. This conflict is a classic example of the failure of diplomacy between the USA/ allied and Russia. We also understand that Russia considers Ukraine and other formal USSR states as backyard and buffer states between US-led NATO and present-day Russia. Therefore, Russia feels threatened whenever USA / NATO / EU advances their interests in these states. Russia has already conceded many states to US-led NATO and allowed them to join the EU, although very reluctantly. But the possibility of Ukraine joining the EU and NATO was a red line, amply highlighted by Russia. But unfortunately, the Russian stance of not expanding NATO eastwards was not adhered to by Europe and the USA.

If we go back into history, a similar situation was faced by the USA in 1962, when the erstwhile USSR intended to deploy missiles in Cuba in response to US missiles in Italy and Turkey. The US President Kennedy very wisely dealt with the issue by limiting its options to quarantine Cuban Ports to block ships carrying USSR missiles. He took rational decisions against the advice of attacking and dismantling infrastructure in Cuba thus lowering the temperature and allowing diplomacy to play its parts. On the other hand, President Khrushchev of the USSR then very wisely withdrew its decisions, and the ugly situation was averted. Similarly, the USA also pulled out possible missile deployment from Turkey under a negotiated settlement with USSR. Unfortunately, this time situation is reversed and US/ Allied failed to understand the sensitivities of Russia in this regard. Here, one must acknowledge the quality of leadership of both the USA and USSR back in 1962, who took very wise and rational decisions. Unfortunately, in 2022, both USA/ Allied and Russia misunderstood the intentions and interests of their opponents which puts a big question mark against rational decision-making at the global level.

Russia – Ukraine Conflict has global implications in terms of geo-economics also. Russia is one of the main global suppliers of oil and gas. Similarly, both Russia and Ukraine also provide wheat to global consumers, rather Ukraine has been known as the breadbasket for the entire erstwhile USSR. EU, the main party to the conflict is also dependent on Russian gas. Sanctioning or discontinuing import of Russian Oil and gas has already impacted the global energy markets

Decoy document related to Russia-Ukraine war, from previous attack by Sidewinder APT

Check Point will continue to track the threat landscape, hunt for new intrusions and protect Check Point's customers from Advanced Persistent Threats.

Indicators of Compromise

IOC	Descriptio
898513123f0f0342b1c47a4a65c88a60f895f90a9d0fa5fc5928c26dfab622b0	2b2tuceo.5 Sidewinder DLL RAT,
5cad4b71a6a99b34fb2f4d60fa8bb5db6a6f6dabe5468d9b3341cbc04492aaab	2b2tuceo.5 After decryption
https://polvcrit[.]info/202/W6taHcwqKwhgzWGWr7ElpRAfWA7JcsXC0A2a4eFv/28284/14980/d5de9821	Url found ir the encrypt

	file list
https://bgevin[.]live/202/W6taHcwqKwhgzWGWr7ElpRAfWA7JcsXC0A2a4eFv/28284/14980/d5de9821	Url found ir the RAT config