Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
135/16

BLURRING LINES: CYBER AND KINETIC MILITARY OPERATIONS

Arjun Subramanian P

The dividing line between cyber and kinetic warfare is blurring rapidly. A recent revelation by a US based cyber Security Company *Crowd Strike* on the Russian military hacker unit's exploit of an android application to track the Ukrainian field artillery units for gathering targeting information is a clear indication of the close role cyber technology is going to play in the future battle field.[1] The said cyber exploit directly resulted in the elimination of over 80% of the Ukrainian D-30 howitzers during the period of the conflict.[2] Such employment of cyber warfare tools to the tactical level would help gather real time battlefield information on enemy positions and operations.

The malware named Fancy Bear X-Agent was embedded in a duplicate version of an android APK file. The original app was developed by a Ukrainian military officer named Yaroslav Sherstuk specifically for the D-30 howitzers. The utility of the application was to process targeting data for the D-30 field guns which reportedly reduces the targeting time from minutes to less than 15 seconds.[3] The app was used by over 9,000 Ukrainian artillery personnel. Reportedly, Russian military hackers reverse engineered the application and embedded a malware that could retrieve and transfer communications and location data from the infected device to the Russian hacker unit node which is believed to be affiliated to the Russian GRU.[4]

The Trojan embedded APK file was named Попр-Д30.apk (an abbreviation for Попраbkи - Д30)[5] which led the security firm to investigate the application as the Д-30(D-30) refers to the vintage field artillery being used in large number by the Ukrainian forces. This cyber attack tactic was a considerably ingenious and laborious operation. The APK file was being circulated and was being used for monitoring ever since 2014 to 2016. This event also points to the use of non-sanitised and unregulated use of open source software products for military operations.

Once a legitimate application is compromised or reverse engineered with a malware embedded into it, the malware can have access to various I/O, storage and other resources of the device via the applications programming interface. Leveraging this access, a malware can track, modify or use any of the resources in the device including data transfer modules. Hence, any non-sanitised and unregulated use of tools, including commercially available products, for military operations, will pose a significant danger to own forces as it might compromise the war effort.

An interesting fact to note is that the Ukrainian officer who developed this application used social media to distribute it. However, the officer exercised reasonable precautions like delivering the activation code personally on being contacted by the seeker.[6] Nevertheless, this is a dangerous practice as is evident from the significant cost incurred by the Ukrainian field artillery units. The Russian hackers too used social media to circulate the infected app embedded with the malware. The trust element, arising from the fact that it was developed by Ukrainian military officers, had obviously played a part in making the artillery personnel download and install it in their android phones.

Even a normal app, when it gets all the resource utilisation privileges, will be able to listen to conversations going on around, take snap shots with the phone camera and get precise location details. Moreover, all these details can be transferred in real time to the enemy data collection centre. To analyse such large amount of user data, the Russian unit would have used data mining programs to fetch readily usable data in minutes that could be directly sent to own force in the battle theatre. The OODA loop gets extremely shortened in this case.

Key points and observations

1. Cyber warfare can get to the tactical battlefield level if forces are allowed to carry commercial devices while involved in operations.
2. Gross negligence and complacency in the Ukrainian armed forces, probably due to the lack of awareness of the potential threats from the cyber domain resulted in such heavy losses. The extent of negligence is evident from the use of the social media to distribute the app for military use.
3. Even military electronic devices ought to be sanitised before being deployed for use.
4. Such compromises can also happen during peacetime, potentially revealing sensitive details like weapon related information, common practices, own force tactics, etc which can come in handy for the adversary during conflict.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] "Russian military hackers used Android malware to seek-and-destroy Ukrainian artillery", http://www.theinquirer.net/inquirer/news/3001636/russian-military-hackers-used-android-malware-to-seek-and-destroy-ukrainian-artillery , December 22, 2016

[2] "Use of Fancy Bear android malware in tracking of Ukrainian field artillery units", *CrowdStrike Global Intelligence Team*, https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf , December 22, 2016

[3] ibid

[4] "Russian malware used to track Ukrainian artillery units in Donbas, report says",http://uatoday.tv/society/russian-hackers-malware-used-to-track-ukrainian-artillery-units-in-donbas-report-says-851768.html , 22 December 2016

[5] "Russian hackers used android malware to track Ukrainian artillery", http://www.androidcentral.com/russian-hackers-used-android-malware-track-ukrainian-artillery , December 22, 2016

[6] "Use of Fancy Bear android malware in tracking of Ukrainian field artillery units", *CrowdStrike Global Intelligence Team*, https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf , December 22, 2016