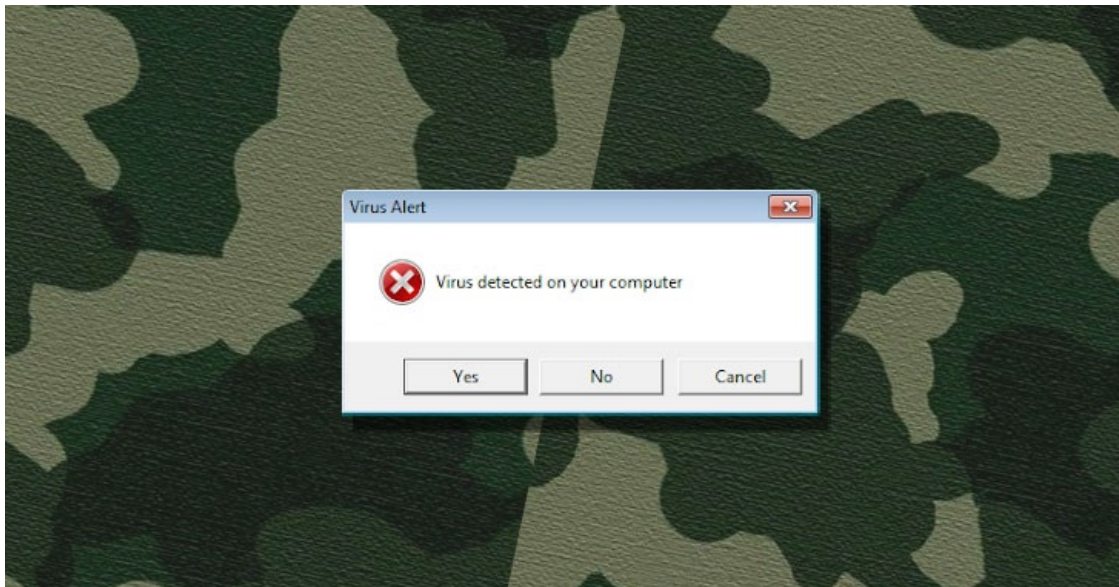


# Researchers Uncover Cyber Espionage Operation Aimed At Indian Army

📅 September 28, 2020    👤 Ravie Lakshmanan



([https://thehackernews.com/images/-moq29tjLKes/X3Hiw\\_j-BWI/AAAAAAAAAzW/G5NSZ76jylEmHTHx-X2e\\_kV6iO-wPmGkwCLcBGAsYHQ/s728/indian-army-virus.jpg](https://thehackernews.com/images/-moq29tjLKes/X3Hiw_j-BWI/AAAAAAAAAzW/G5NSZ76jylEmHTHx-X2e_kV6iO-wPmGkwCLcBGAsYHQ/s728/indian-army-virus.jpg))

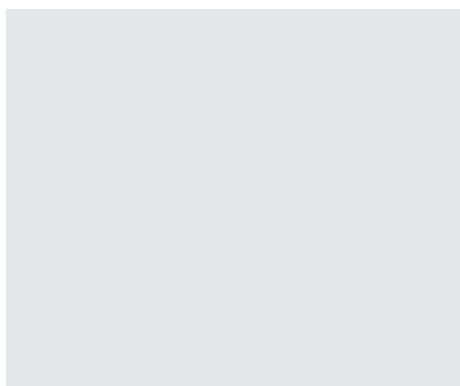
Cybersecurity researchers uncovered fresh evidence of an ongoing cyberespionage campaign against Indian defense units and armed forces personnel at least since 2019 with an aim to steal sensitive information.

Dubbed "**Operation SideCopy**" by Indian cybersecurity firm [Quick Heal](#)

(<https://www.seqrte.com/blog/operation-sidecopy/>) , the attacks have been attributed to an advanced persistent threat (APT) group that has successfully managed to stay under the radar by "copying" the tactics of other threat actors such as the [SideWinder](#) (<https://thehackernews.com/2020/01/android-zero-day-malware-apps.html>) .

## Exploiting Microsoft Equation Editor Flaw

The campaign's starting point is an email with an embedded malicious attachment — either in the form of a ZIP file containing an LNK file or a Microsoft Word document — that triggers an infection chain via a series of steps to download the final-stage payload.

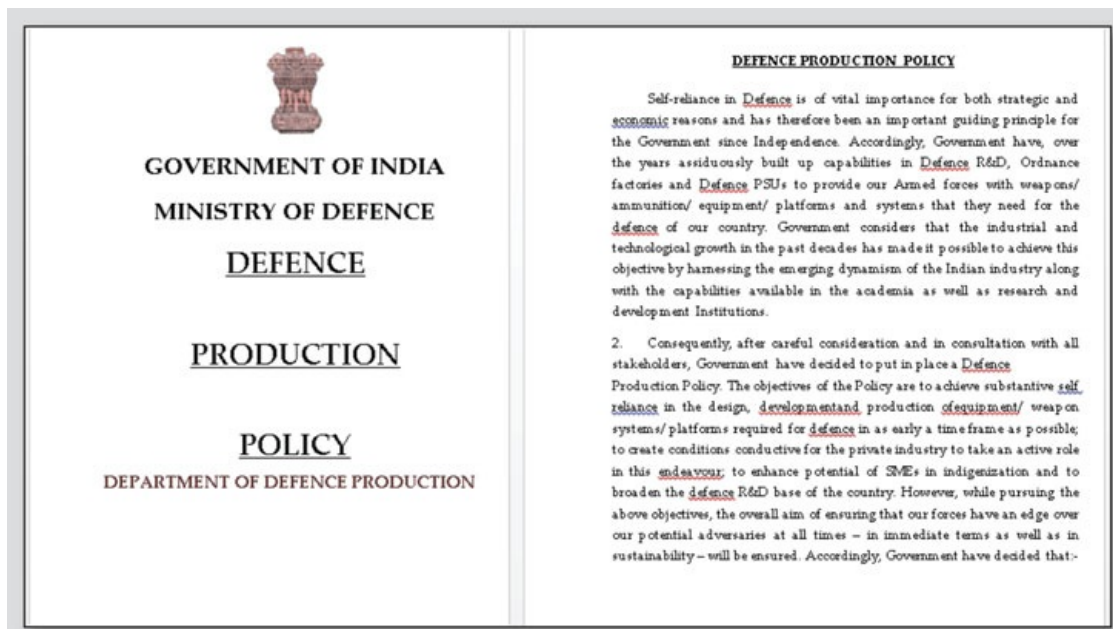


(<https://go.thn.li/contrast>)

Aside from identifying three different infection chains, what's notable is the fact that one of them exploited template injection and Microsoft Equation Editor flaw ([CVE-2017-11882](https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882)) (<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882>) , a 20-year old memory corruption issue in Microsoft Office, which, when exploited successfully, let attackers execute remote code on a vulnerable machine even without user interaction.

Microsoft addressed the issue in a patch released in [November 2017](https://thehackernews.com/2017/11/microsoft-office-rce-exploit.html)

(<https://thehackernews.com/2017/11/microsoft-office-rce-exploit.html>) .



(<https://thehackernews.com/images/->

[yeksQpFeoGU/X3Hjgm\\_8Xwl/AAAAAAAAAAz8/8voJD0WmwyEW3F9S0LX6UK\\_qAEruSqQCgCLcBGAsYHQ/s0/indian-army.jpg](https://thehackernews.com/images/-))

As is often the case with such malspam campaigns, the attack relies on a bit of social engineering to bait the user into opening a seemingly realistic Word document that claims to be about the Indian government's defense production policy.

What's more, the LNK files have a double extension ("Defence-Production-Policy-2020.docx.lnk") and come with document icons, thereby tricking an unsuspecting victim into opening the file.

Once opened, the LNK files abuse "[mshta.exe](https://attack.mitre.org/techniques/T1218/005/) (<https://attack.mitre.org/techniques/T1218/005/>) " to execute malicious HTA (short for Microsoft HTML Applications) files that are hosted on fraudulent websites, with the HTA files created using an open-sourced payload generation tool called [CACTUSTORCH](https://github.com/mdsecactivebreach/CACTUSTORCH) (<https://github.com/mdsecactivebreach/CACTUSTORCH>) .

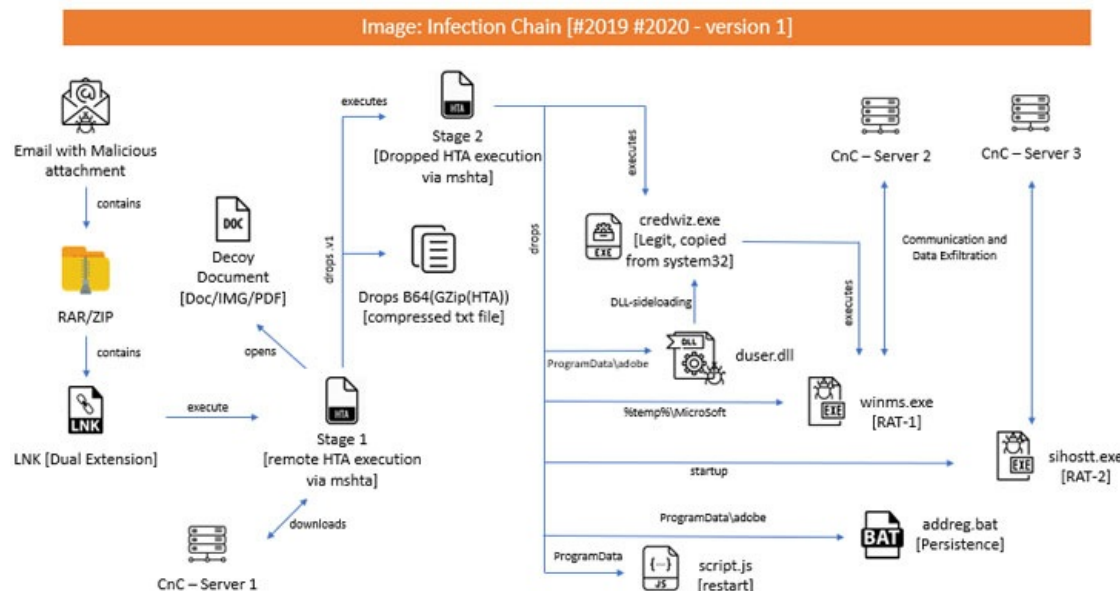
## A Multi-stage Malware Delivery Process

The first stage HTA file includes a decoy document and a malicious .NET module that executes the said document and downloads a second-stage HTA file, which in turn checks for the presence of popular antivirus solutions before copying Microsoft's credential back and restore utility ("credwiz.exe") to a different folder on the victim machine and modifying the registry to run the copied executable every time upon startup.

Consequently, when this file gets executed, not only does it side-load a malicious "DUser.dll" file, it also launches the RAT module "winms.exe," both of which are obtained from the stage-2 HTA.

"This DUser.dll will initiate the connection over this IP address '173.212.224.110' over TCP port 6102," the researchers said.

"Once successfully connected, it will [...] then proceed for performing various operations based on the command received from C2. For example, if C2 sends 0, then it collects the Computer Name, Username, OS version etc. and sends it back to C2."



([https://thehackernews.com/images/-q-](https://thehackernews.com/images/-q-0sbc9CI08/X3HkAhQRMSI/AAAAAAAAA0I/vjEr5t0jwRY3WhXg5V1Pk0S9zCsvH7W6QCLcBGAsYHQ/s0/cyber-attack-vector.jpg)

[0sbc9CI08/X3HkAhQRMSI/AAAAAAAAA0I/vjEr5t0jwRY3WhXg5V1Pk0S9zCsvH7W6QCLcBGAsYHQ/s0/cyber-attack-vector.jpg](https://thehackernews.com/images/-q-0sbc9CI08/X3HkAhQRMSI/AAAAAAAAA0I/vjEr5t0jwRY3WhXg5V1Pk0S9zCsvH7W6QCLcBGAsYHQ/s0/cyber-attack-vector.jpg))


Stating the RAT shared code-level similarities with Allakore Remote, an open-sourced remote-access software written in Delphi, Quick Heal's Seqrite team noted that the Trojan employed Allakore's RFB (remote frame buffer) protocol to exfiltrate data from the infected system.

## Possible Links to Transparent Tribe APT

In addition, a few attack chains are also said to have dropped a previously unseen .NET-based RAT (called "Crimson RAT" by [Kaspersky](https://securelist.com/transparent-tribe-part-1/98127/) researchers) that comes equipped with a wide range of capabilities, including access files, clipboard data, kill processes, and even execute arbitrary commands.

Although the modus operandi of naming DLL files shares similarities with the SideWinder group, the APT's heavy reliance on the open-sourced toolset and an entirely different C2 infrastructure led the researchers to conclude with [reasonable confidence](https://securelist.com/transparent-tribe-part-2/98233/) that the threat actor is of Pakistani origin — specifically the [Transparent Tribe](https://malpedia.caad.fkie.fraunhofer.de/actor/operation_c-major) group, which has been recently linked to several attacks targeting the Indian military and government personnel.

"Thus, we suspect that the actor behind this operation is a sub-division under (or part of) Transparent-Tribe APT group and are just copying TTPs of other threat actors to mislead the security community," Quick Heal said.

Found this article interesting? Follow THN on [Facebook](https://www.facebook.com/thehackernews/) (https://www.facebook.com/thehackernews) ,  
[Twitter](https://twitter.com/thehackersnews)  (https://twitter.com/thehackersnews) and [LinkedIn](https://www.linkedin.com/company/thehackernews/)  
(https://www.linkedin.com/company/thehackernews/) to read more exclusive content we post.

---