Operation SideCopy!

seqrite.com/blog/operation-sidecopy/

Kalpesh Mantri September 23, 2020

23 September 2020
Written by Kalpesh Mantri

APT, Cybersecurity

4
Estimated reading time: 3 minutes

An insight into Transparent Tribe's sub-division which has been incorrectly attributed for years.

Introduction

Quick Heal's threat intelligence team recently uncovered evidence of an advanced persistent threat (APT) against Indian defence forces. Our analysis shows that many old campaigns and attack in the past one year relate to 'Operation SideCopy' by common IOCs.

Key Findings

- Operation SideCopy is active from early 2019, till date.

- This cyber-operation has been only targeting Indian defence forces and armed forces personnel.
- Malware modules seen are constantly under development and updated modules are released after a reconnaissance of victim data.
- Actors are keeping track of malware detections and updating modules when detected by AV.
- Almost all CnC belongs to Contabo GmbH and server names are similar to machine names found in the Transparent Tribe report.
- This threat actor is misleading the security community by copying TTPs that point at Sidewinder APT group.
- We suspect this threat actor has links with Transparent Tribe APT group.

Summary:

A few months ago, Quick Heal's Next-Gen Behavioural Detection system alerted on a few processes executing HTA from some non-reputed websites.

We have made a list of URLs, connected from mshta.exe, across multiple customers:

hxxps://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Armed-Forces-Spl-Allowance-Order/html/

hxxps://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Defence-Production-Policy-2020/html/

hxxps://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Images/8534

hxxps://demo[.]smart-hospital[.]in/uploads/staff_documents/19/IncidentReport/html/

hxxps://demo[.]smart-hospital[.]in/uploads/staff_documents/19/ParaMil-Forces-Spl-Allowance-Order/html/

hxxps://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Req-Data/html

hxxps://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Sheet_Roll/html

hxxps://demo[.]smart-school[.]in/uploads/staff_documents/9/Sheet_Roll/html

hxxps://demo[.]smart-school[.]in/uploads/student_documents/12/css/

hxxps://drivetoshare[.]com/mod[.]gov[.]in_dod_sites_default_files_Revisedrates/html

The highlighted ones were sent to targets across Indian defence units and armed forces individuals.

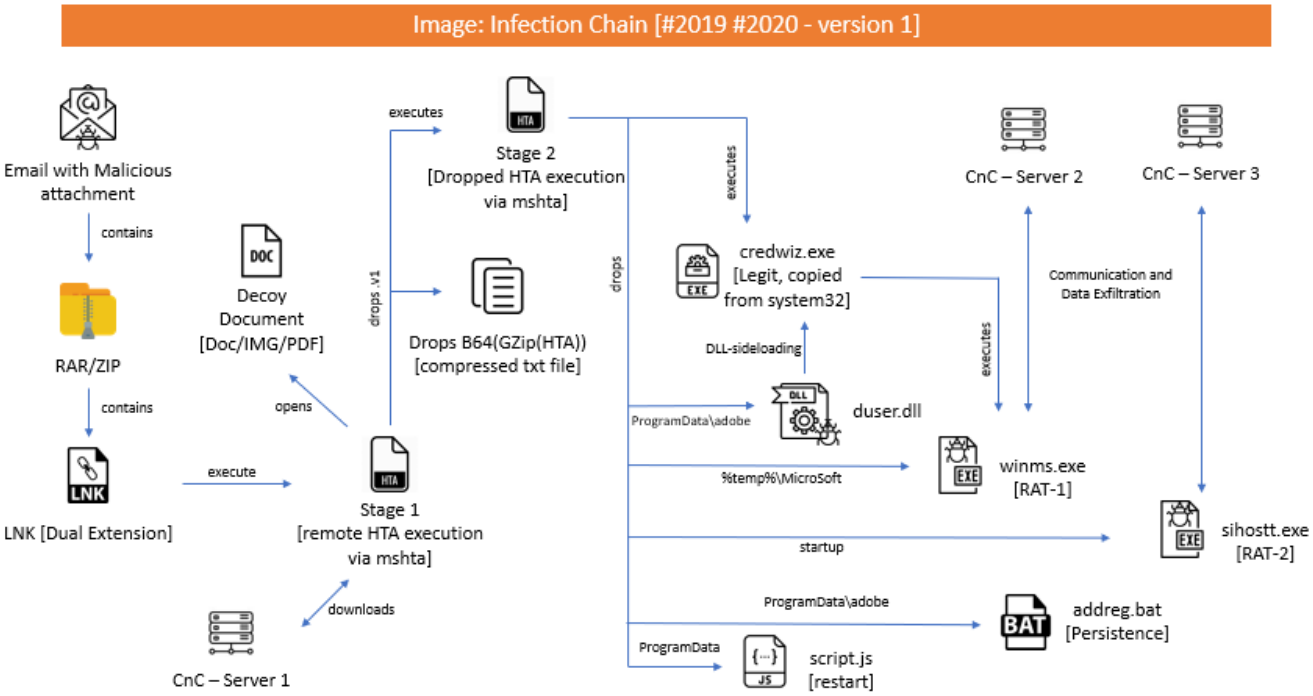
We started tracking this campaign as it was targeting critical Indian organizations.

Traces of this operation can be tracked from early 2019 till date. Till now, we have observed 3 infection chain process.

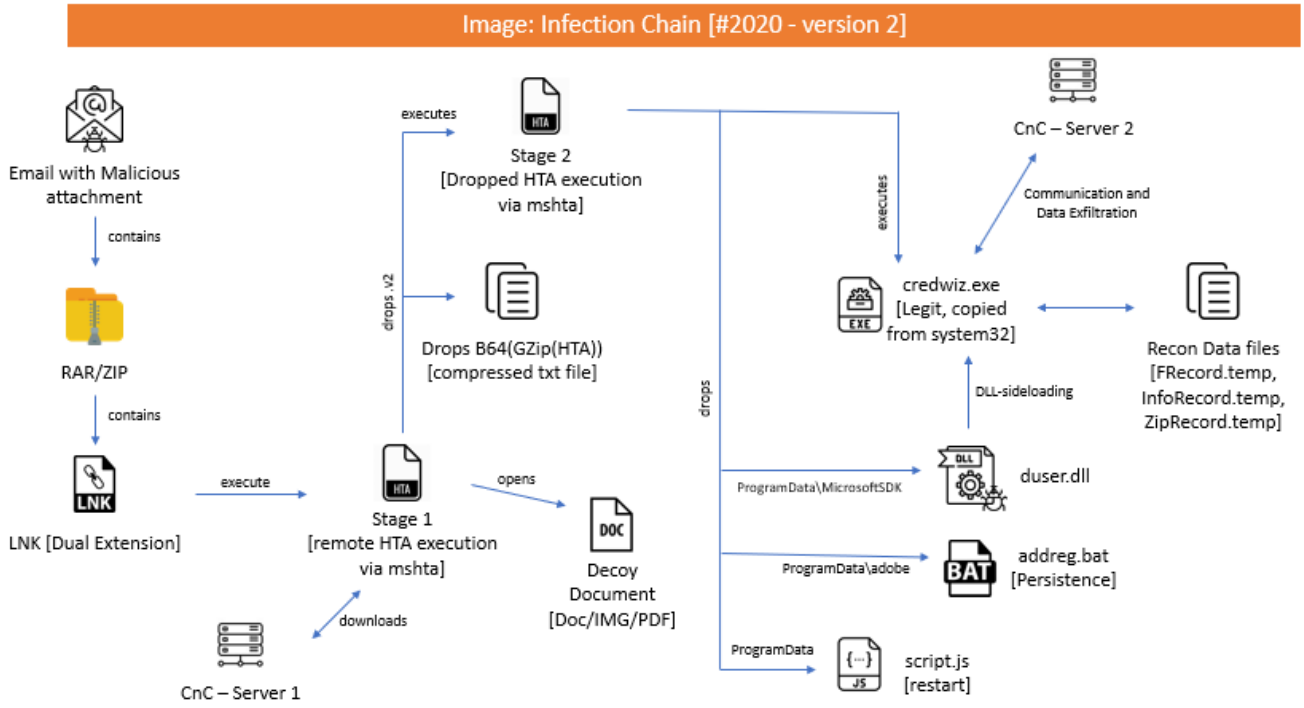
Initial infection vector in two of the chains was LNK file, that came from a malspam. But in one case, we saw attackers making use of template injection attack and equation editor vulnerability (CVE-2017-11882) as the initial infection vector. Though the initial infection vector is different in the third case, the final payload is similar to the first two chains.

Below images will provide an overview of malware infection in victim machines.

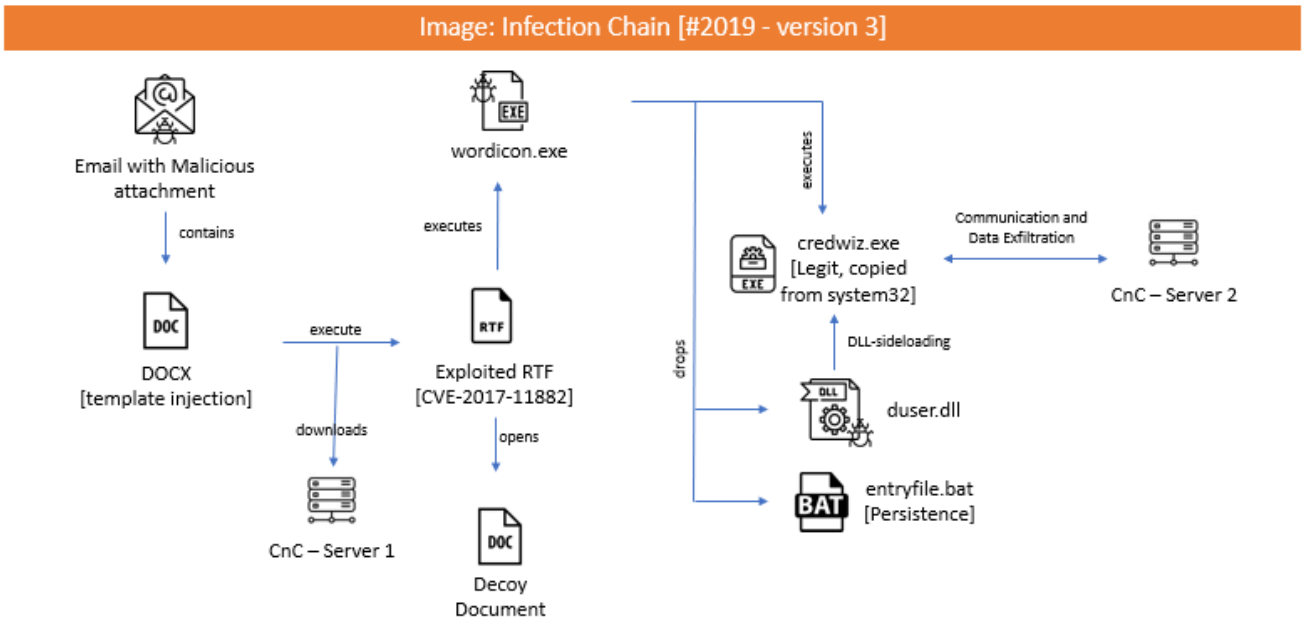
Infection Chain – Version 1:



Infection Chain – Version 2:



Infection Chain – Version 3:



We have provided an in-depth analysis of each of this module in our latest report which can be found here.

The background and analysis in this paper provide complete forensic and useful details of our current thinking on the use of malware in this operation. We have provided all factors that lead to our attribution.

Subject matter experts:

Kalpesh Mantri, Principal Security Researcher

Pawan Chaudhari, Threat Research Scientist

Goutam Tripathy, Senior Security Researcher