

PATCHWORK



PATCHWORK



INDIA



US



SPEAR
PHISHING



A SURVEY ON PATCHWORK ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

- NERDS OF AXIAL

I. INTRODUCTION

Patchwork is a threat group which is based out of Republic Of India , also goes by the name dropping elephant .

*Patchwork has been attributed to multiple phishing campaigns.
*Patchwork has also been attributed to attacks on Pakistan Atomic Energy Commission.

IV. CAMPAIGNS

II. TARGETS

Aviation, Defense, Energy, Financial, Government, IT, Media, NGOs, Pharmaceutical, Think Tanks on multiple countries.

ATTRIBUTION

III. METHODS USED

Patchwork has been using spear phishing and maliciousin blogs by 360 Threat Intelligence Center analyzing attacks on Chinese documents as one of it's methods.

Patchwork has also been using weaponized RTF Document.

Patchwork has also been using variants of QuasarRAT Payload.

Patchwork has also been exploiting CVE-2017-8750 for exploitation

Volexity identified multiple spear phishing campaigns attributed to Patchwork, an Indian APT group also known as Dropping Elephant. This increase in threat activity was consistent with other observations documented over the last few months organizations and Trend Micro noting targets in South Asia.

From the attacks observed by Volexity, what is most notable is that Patchwork has pivoted its targeting and has launched attacks directly against US-based think tanks. Volexity has also found that, in addition to sending malware lures, the Patchwork threat actors are leveraging unique tracking links in their e-mails for the purpose of identifying which recipients opened their e-mail messages.

V. IOCS

Hashes

be550349fb4bb2277822554fc243f0a3
2d8e9fb75e6e816cad38189691e9c9c8
f396b476413558266f3abd336e06cbfc
5c3456d5932544b779fe814133344fdb
89beb207e7095d237c4d25c4c6e17e97
9e4c373003c6d8f6597f96fc3ff1f49c

C2

tautiaos.com / 43.249.37.199
sastind-cn.org / 209.58.176.201

VI. REFERENCES

<https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/>

[https://apt.thaicert.or.th/cgi-bin/showcard.cgi?
g=Patchwork%2C%20Dropping%20Elephant](https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Patchwork%2C%20Dropping%20Elephant)

<https://shadowdragon.io/patchwork-apt-group-additional-iocs-network-indicators/>

