SideCopy APT: from Windows to *nix

telsy.com/sidecopy-apt-from-windows-to-nix/

January 5, 2022

Cyber Threat Intelligence
05 Jan
Telsy Threat Intelligence team has observed a spear-phishing campaign conducted by cyber-espionage group ***SideCopy*** against critical government entities in India.

As previously published by 'TALOS Cisco Security Research' also in this campaign, in addition to the military themes, ***SideCopy*** used publications, invitations to submit documents/proposals and reproduced phishing portals posing as Indian government webmail to trick victims into divulging their e-mail credentials.

SideCopy's delivery infrastructure consists of using compromised websites to deliver malicious artefacts to specific victims. In this campaign, the portal '*hxxp://assessment.mojochamps.com*' was compromised, the *WebShell* named '***WSO version 4.2.5***' was uploaded, and the infection chain began to spread.

The infection chain for ***Windows*** systems has remained relatively consistent with minor variations, but unlike previous observations an infection chain for ****nix*** systems has been introduced. ***SideCopy*** continued to send spear-phishing e-mails with malicious file attachments ranging from WEB links to LNKs that installed remote access trojans (RATs) on infected systems.

In addition, ***SideCopy*** used the BackNet agent in some infection chains. BackNet is a Python Remote Access Tool. It is made of two main programs:

– A Command and Control server, which is a Web interface to administer the agents

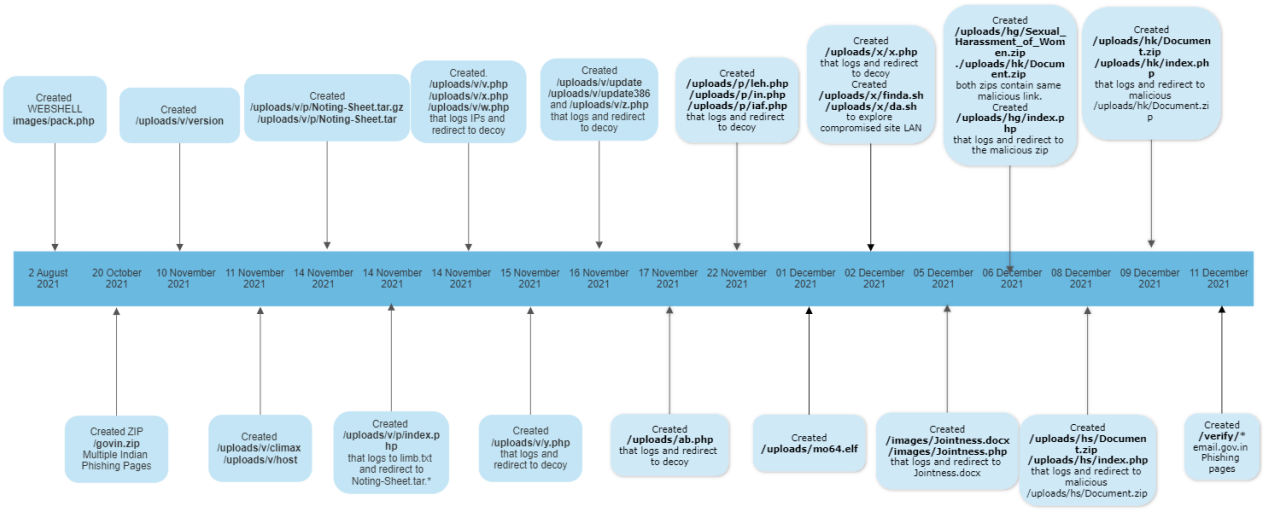
– An agent program, which is run on the compromised host, and ensures communication with the Command and Control.

The agent can be compiled to native executables using pyinstaller and is therefore compatible with both *Windows* and **nix* operating systems.

The portal '*hxxp://assessment.mojochamps.com*', compromised by the threat actor, had malconfigured open directories that allowed access to directories and files saved by the cyber-espionage group.

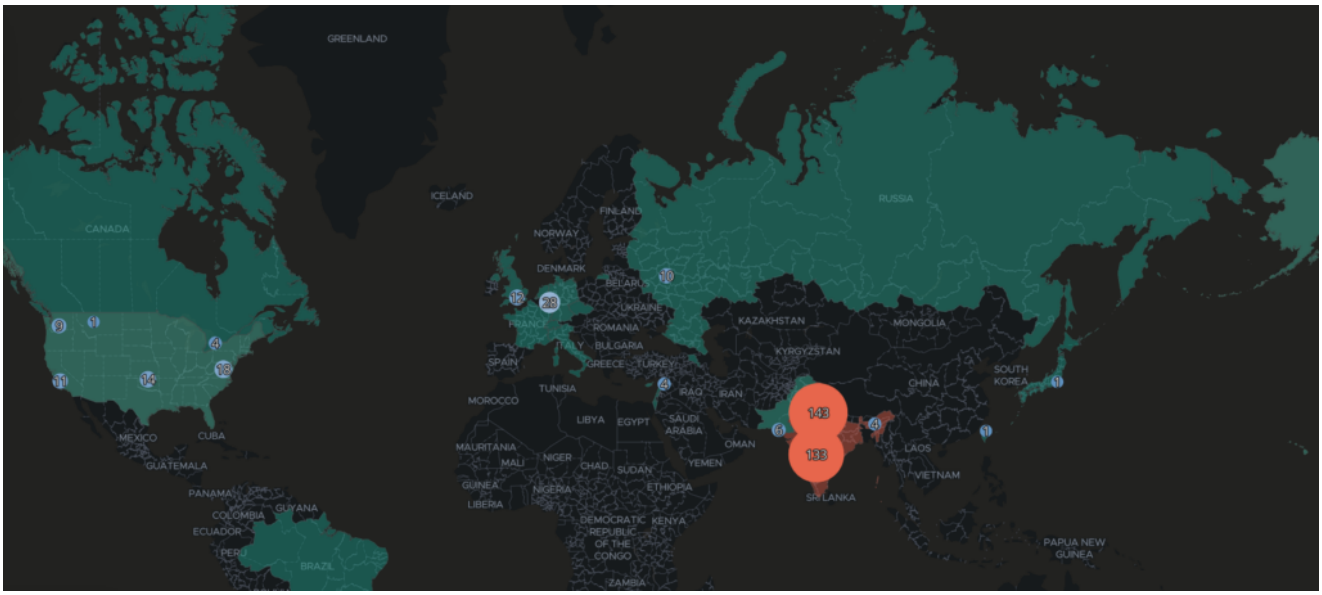
The analysis of the files on the compromised website made it possible to draw up a timeline of the activities conducted by the ***SideCopy*** group. Between the upload of the first WebShell and the last reported activity, which appears to be the creation of the Indian government's webmail phishing page, there were various activities such as uploading PHP and ELF files along with decoy documents.

The following storyline omits the decoy documents upload.



Depending on the context and modus operandi, all PHP and other files are consistent with each other, which makes it possible that the compromised site was used by the same threat actor to target only India.

Typically, the purpose of the PHP pages was to record the source IP and user agent of the visitor in a text file and then redirect the user to the malicious file or a decoy file depending on the purpose of the page.



Map of visitors' IPs

Analysis of the log files generated by the PHP pages was able to identify around 400 unique IPs, most of which were concentrated in India. Some of these IPs were attributed to Indian governmental and civil organisations by analysing the information contained in the ***Whois*** registry databases. For example:

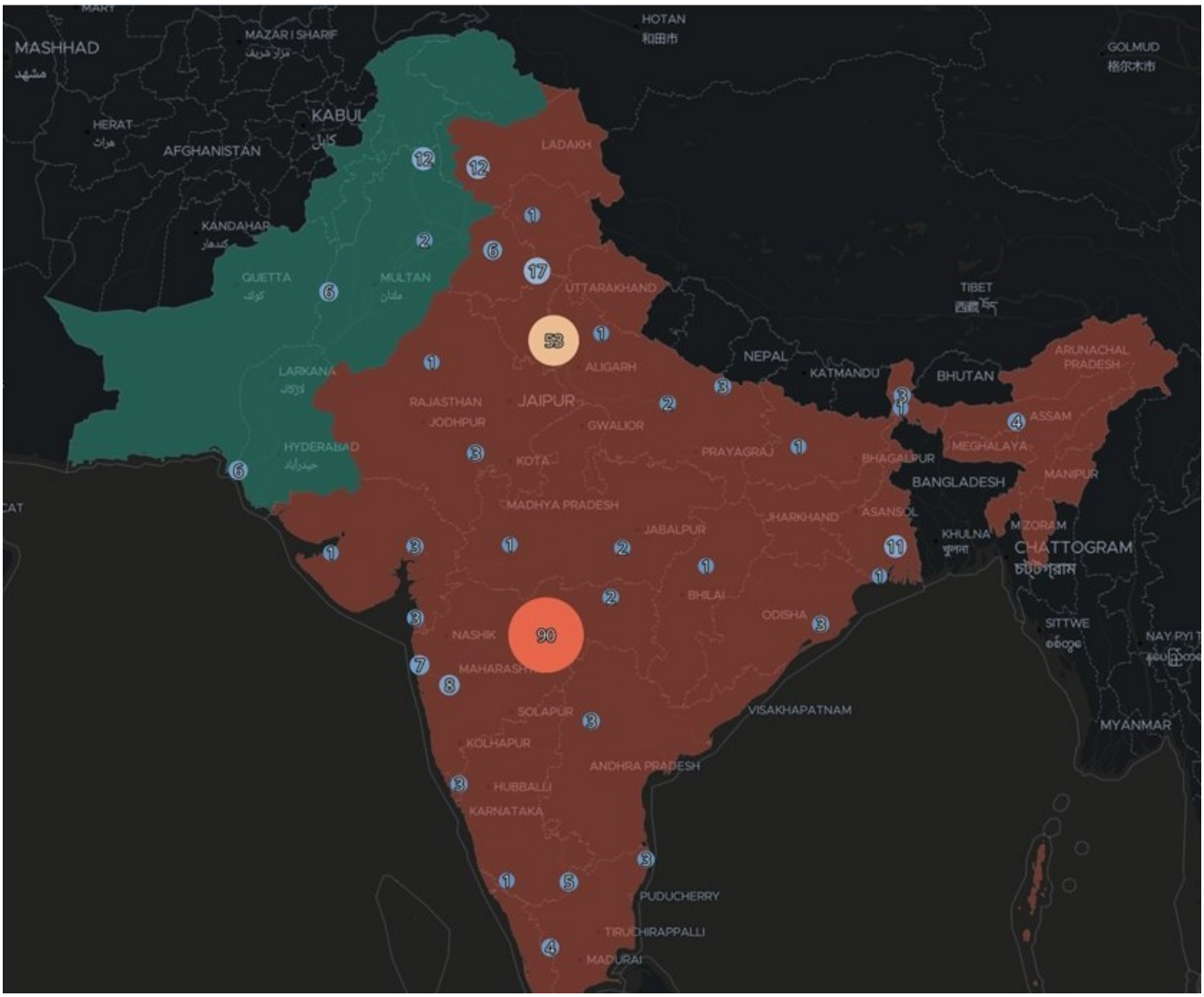
– M.P. Power Management Company Limited

– Power System Operation Corporation Limited

– Inspector General of Police

– Chief of Naval Staff

– National Remote Sensing Agency.



Map of Indian visitor IPs

Fill the form below to download the full report

Check other cyber reports on our blog.

This report was produced by Telsy's "Cyber Threat Intelligence" team with the help of its CTI platform, which allows to analyze and stay updated on adversaries and threats that could impact customers' business.