Talos
Cisco Security Research

Operation: Armor Piercer

VIEW BLOG POST

Social engineering attacks target government agencies in India, Asia-Pacific

SUMMARY

Cisco Talos recently discovered a malicious campaign targeting government employees and military personnel in the Indian sub-continent with two commercial and commodity RAT families known as NetwireRAT (aka NetwireRC) and WarzoneRAT (aka Ave Maria). The attackers delivered a variety of lures to their targets, predominantly posing as guides related to Indian governmental infrastructure and operations in the form of malicious Microsoft Office documents (maldoc) and malicious archives (RARs, ZIPs) containing loaders for the RATs.

WHAT'S NEW?

Many of the tactics, techniques and procedures (TTPs) used in these campaigns are borrowed from other threat actors, but we believe this is a separate adversary. Unlike many crimeware and APT attacks, this campaign uses relatively simple, straightforward infection chains.

HOW DID IT WORK?

Most infections use a maldoc that downloads and instruments a loader. The loader is responsible for either downloading or decrypting (if embedded) the final RAT payload and deploying it on the infected endpoint. In some cases, we've observed the use of malicious archives containing a combination of maldocs, loaders and decoy images.

SO WHAT?

This campaign illustrates another instance of a highly motivated threat actor using a set of commercial and commodity RAT families to infect their victims. But what stands out are the targets. This is just the latest attack we've seen targeting government agencies and military branches in the Indian subcontient, with Transparent Tribe and SideCopy stepping up their efforts in the region recently. Any potential infections put sensitive information and data at risk.

COVERAGE

PRODUCT	PROTECTION
Cisco Secure Endpoint	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS	✓
Cisco Secure Network Analytics	N/A
Cisco Secure Cloud Analytics	N/A
Cisco Secure Malware Analytics	✓
Umbrella	✓
Cisco Secure Web Appliance	✓

Cisco Secure Endpoint is ideally suited to prevent the execution of the malware detailed in this post. New users can try Cisco Secure Endpoint for free here.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.