# TA558 Hackers Weaponize Images for Wide-Scale Malware Attacks

Date: 16th April 2024 | Severity: High

## Summary

The threat actor tracked as TA558 has been observed leveraging steganography as an obfuscation technique to deliver a wide range of malware such as Agent Tesla, FormBook, Remcos RAT, LokiBot, GuLoader, Snake Keylogger, and XWorm, among others.

The campaign has been codenamed SteganoAmor for its reliance on steganography and the choice of file names such as greatloverstory.vbs and easytolove.vbs.

The TA558 threat group, first reported by Proofpoint researchers in August 2022, has been active since at least 2018. The financially-motivated group targets hospitality, hotel, and travel organizations, primarily located in Latin America, but also in North America and Western Europe. The activities of TA558 have intensified in 2022, probably due to the renaissance of tourism following the lifting of COVID-19 restrictions.

A majority of the attacks have targeted industrial, services, public, electric power, and construction sectors in Latin American countries, although companies located in Russia, Romania, and Turkey have also been singled out.

## Attack Vectors

- Positive Technologies is tracking the activity cluster under the name Lazy Koala in reference to the name of the user (joekoala), who is said to control the Telegram bots that receive the stolen data.
- That said, the victim geography and the malware artifacts indicate potential links to another hacking group tracked by Cisco Talos under the name YoroTrooper (aka SturgeonPhisher).
- The findings also follow a wave of social engineering campaigns that are designed to propagate malware families like FatalRAT and SolarMarker.

# Indicator of compromise

| INDICATOR TYPE | INDICATORS |
|---|---|
| File Hash | • 2fcad226b17131da4274e1b9f8f31359bdd325c9568665f08fd1f6c5d06a23ce<br>• 3eea942e74619bb0b7d8a07df37e53886685018278672a6f7db07db54fa2d172<br>• 8bff9db73f282a3111396980f47f299f2a94f3960c58c6e70826495f76d00b85<br>• 568a3eb0bee91d00c51fa77bd15f5f24caf1502fa33c1bae6b507bb2958ff79f |
| Domain/URL | successfully.hopto.org vemvemserver.duckdns.org http://172.245.208.34/icre-atedloveonherheartwithnewthingswhichwillunderstand_____howiamlovingher-withlotoofheartwithlove.doc passagensv.sslblindado.com http://23.95.235.35/imfeelingalotandbleedingseriouslywithmyheartandiamtryingtofigureoutfromentierth-ings_____ireallyloveutrulyfromtheheartbutiknowmysituations.doc |

# Recommendation

- Cybersecurity researchers reported a TA558 phishing campaign that targeted organizations from various sectors, including hospitality, trading, finance, manufacturing, industrial, and government. The victims were primarily located in Latin America, in countries such as Spain, Mexico, Colombia, Portugal, Brazil, the Dominican Republic, and Argentina. The victims were infected with the Venom RAT malware (a variant of Quasar RAT), used for remote data collection.
- The threat actors sent their victims phishing email messages from compromised SMTP servers.
- The execution chain ended with the deployment of a variety of malware, including AgentTesla, Remcos, LokiBot, Formbook, Guloader, Snake, and XWorm.

**NOTE:** The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

# Reference Links

- https://thehackernews.com/2024/04/ta558-hackers-weaponize-images-for-wide.html
- https://thehackernews.com/2024/04/massive-phishing-campaign-strikes-latin.html
- https://blogger.googleusercontent.com/img/b/R29vZ2xl AVvXsEjOnpQY7VXLtGG3xqmi3JEkGZL9tZ5cVHoo28cF_ska0QvKRWvxR9cQx6GdZVMSUHKNysiL_X7Et_-JYJg9v5HNteGgvtep66DnRStAbEEK2NwqUrQtOUUyLXwdiylpuv5VXdo9ashSwPdQJEfPeFxSaoky_6KhHpED-W3DRPU8XBRUo5zda74k0fhGIvWr/s728-rw-e365/code.png