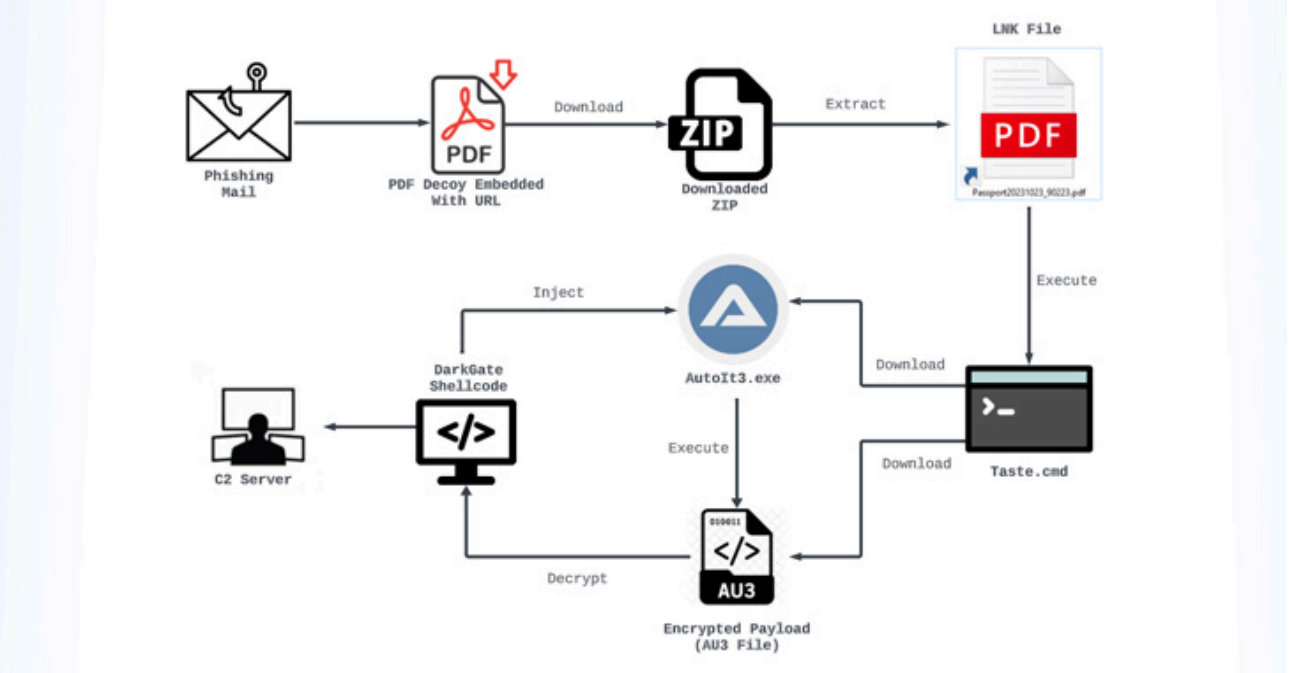
Massive Phishing Campaign Strikes Latin America: Venom RAT Targeting Multiple Sectors

By The Hacker News

Published: 2024-04-02 · Archived: 2026-04-05 22:01:25 UTC



The threat actor known as **TA558** has been attributed to a new massive phishing campaign that targets a wide range of sectors in Latin America with the goal of deploying Venom RAT.

The attacks primarily singled out hotel, travel, trading, financial, manufacturing, industrial, and government verticals in Spain, Mexico, the United States, Colombia, Portugal, Brazil, Dominican Republic, and Argentina.

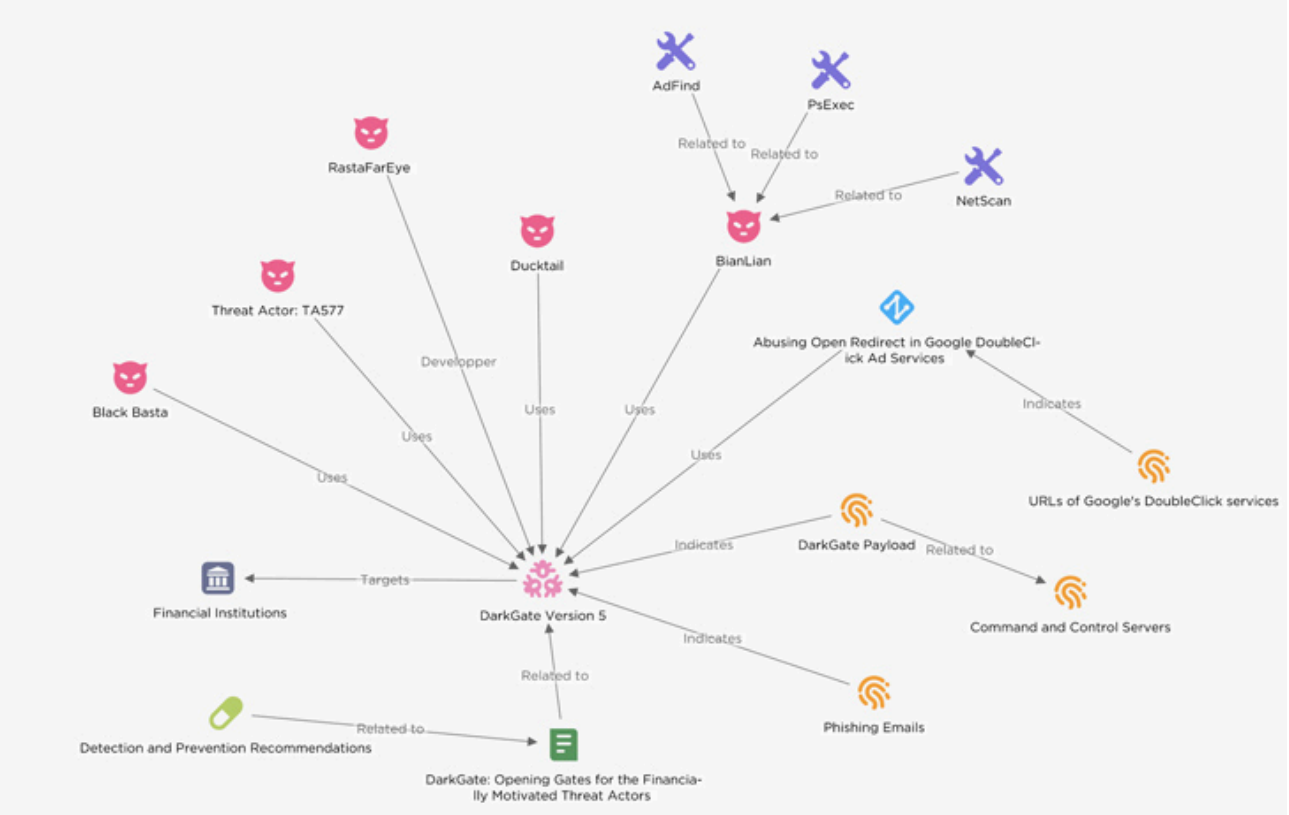
Active since at least 2018, TA558 has a history of targeting entities in the LATAM region to deliver a variety of malware such as Loda RAT, Vjw0rm, and Revenge RAT.

The latest infection chain, according to Perception Point researcher Idan Tarab, leverages phishing emails as an initial access vector to drop Venom RAT, a fork of Quasar RAT that comes with capabilities to harvest sensitive data and commandeer systems remotely.

The disclosure comes as threat actors have been increasingly observed using the DarkGate malware loader following the law enforcement takedown of QakBot last year to target financial institutions in Europe and the U.S.

"Ransomware groups utilize DarkGate to create an initial foothold and to deploy various types of malware in corporate networks," EclecticIQ researcher Arda Büyükkaya noted.

"These include, but are not limited to, info-stealers, ransomware, and remote management tools. The objective of these threat actors is to increase the number of infected devices and the volume of data exfiltrated from a victim."



It also follows the emergence of malvertising campaigns designed to deliver malware like FakeUpdates (aka SocGholish), Nitrogen, and Rhadamanthys.

Earlier this month, Israeli ad security company GeoEdge revealed that a notorious malvertising group tracked as ScamClub "has shifted its focus towards video malvertising assaults, resulting in a surge in VAST-forced redirect volumes since February 11, 2024."

The attacks entail the malicious use of Video Ad Serving Templates (VAST) tags – which are used for video advertising – to redirect unsuspecting users to fraudulent or scam pages but only upon successful passage of certain client-side and server-side fingerprinting techniques.

A majority of the victims are located in the U.S. (60.5%), followed by Canada (7.2%), the U.K. (4.8%), Germany (2.1%), and Malaysia (1.7%), among others.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
