# Mphasis SOC – Information Security News
# Date & Time Issued: 29-JUN-2024, 05:00 IST

| | |
|---|---|
| Title | **Poseidon_Mac_Stealer_Spreading_via_Google_Ads** |
| Summary | • A new campaign distributing a stealer targeting Mac users via malicious Google ads for the Arc browser. The macOS stealer being dropped in this latest campaign is actively being developed as an Atomic Stealer competitor, with a large part of its code base being the same as its predecessor.<br>• Malwarebytes was previously tracking this payload as OSX.RodStealer, in reference to its author, Rodrigo4. The threat actor rebranded the new project 'Poseidon' and added a few new features such as looting VPN configurations. |
| Severity | Medium |
| Attack Vectors | • A threat actor known by his handle as Rodrigo4 in the XSS underground forum has been working on a stealer with similar features and code base as the notorious Atomic Stealer (AMOS).<br>• The service consists of a malware panel with statistics and a builder with custom name, icon, and AppleScript. The stealer offers functionalities reminiscent of Atomic Stealer including file grabber, crypto wallet extractor, password manager (Bitwarden, KeePassXC) stealer, and browser data collector.<br>• We saw an ad for the Arc browser belonging to 'Coles & Co', linking to the domain name arcthost[.]org:<br>• People who clicked on the ad were redirected to arc-download[.]com, a completely fake site offering Arc for Mac only.<br>• The downloaded DMG file resembles what one would expect when installing a new Mac application except for the right-click to open trick to bypass security protections.<br>• The new "Poseidon" stealer contains unfinished code that was seen by others, and recently advertised to steal VPN configurations from Fortinet and OpenVPN. |

| Indicator of Compromise | INDICATOR TYPE | INDICATORS |
|---|---|---|
| | File Hash | • c1693ee747e31541919f84dfa89e36ca5b74074044b181656d95d7f40af34a05<br>• 78480e7c9273a66498d0514ca4e959a2c002f8f5578c8ec9153bb83cbcc2b206<br>• 3285032b8e1cd080ce5df8839db03a1eb9e4d16db252fd64d4c0c5a66d8b0ff8<br>• 3164c7d572bd3f59f31a3bb6ac8a7f0769f2cbdddea7cadf843b99076a952b81<br>• 8affdfea794bc04340a453160237e7b6ae77bd909146321daf2ed50401928827<br>• 4fac5b0618348de1e6e4843bb4560320eea175ecc4ba807beadd56e2e6a66e32<br>• 58eedd3277014bb45a294f4c299bbfcdfc38a212fa0cda7a781dda132e8928a5<br>• 3d180606a60e0a25b78fde6b3cb52afc8443105e672cdcc420be781e9ec32488 |
| | IP address | • 79.137.192[.]4 |
| | Domain | • arcthost[.]org<br>• arc-download[.]com<br>• zestyahhdog[.]com<br>• Arc12645413[.]dmg |

| | |
|---|---|
| Recommendations | • Block all threat indicators at your respective controls.<br>• Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.<br>• Never trust or open links and attachments received from unknown sources/senders.<br>• Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.<br>• Malwarebytes intel "highly recommends" all users maintain ad-blockers for malicious ads and website protection on their devices and laptops and stay vigilant when downloading and installing new apps.<br>• It is recommended to use the official download site for software rather than the one provided by the advertisement when installing it from the internet.<br><br>**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.** |
| References | • https://sechub.in/view/2901396<br>• https://www.malwarebytes.com/blog/news/2024/06/poseidon-mac-stealer-distributed-via-google-ads |