OPSEC Failure Exposes Coquettte's Malware Campaigns on Bulletproof Hosting Servers

thehackernews.com/2025/04/opsec-failure-exposes-coquetttes.html

April 4, 2025

A novice cybercrime actor has been observed leveraging the services of a Russian bulletproof hosting (BPH) provider called Proton66 to facilitate their operations.

The findings come from DomainTools, which detected the activity after it discovered a phony website named cybersecureprotect[.]com hosted on Proton66 that masqueraded as an antivirus service.

The threat intelligence firm said it identified an operational security (OPSEC) failure in the domain that left its malicious infrastructure exposed, thereby revealing the malicious payloads staged on the server.

"This revelation led us down a rabbit hole into the operations of an emerging threat actor known as Coquettte – an amateur cybercriminal leveraging Proton66's bulletproof hosting to distribute malware and engage in other illicit activities," it said in a report shared with The Hacker News.

Proton66, also linked to another BPH service known as PROSPERO, has been attributed to several campaigns distributing desktop and Android malware like GootLoader, Matanbuchus, SpyNote, Coper (aka Octo), and SocGholish. Phishing pages hosted on the service have been propagated via SMS messages to trick users into entering their banking credentials and credit card information.

Coquettte is one such threat actor leveraging the benefits offered by the Proton66 ecosystem to distribute malware under the guise of legitimate antivirus tools.

This takes the form of a ZIP archive ("CyberSecure Pro.zip") that contains a Windows installer that then downloads a second-stage malware from a remote server responsible for delivering secondary payloads from a command-and-control (C2) server ("cia[.]tf").

The second-stage is a loader classified as Rugmi (aka Penguish), which has been used in the past to deploy information stealers like Lumma, Vidar, and Raccoon.

Further analysis of Coquettte's digital footprints uncovered a personal website on which they claim to be a "19 year old software engineer, pursuing a degree in Software Development."

What's more, the cia[.]tf domain has been registered with the email address "root@coquettte[.]com," confirming that the threat actor controlled the C2 server and operated the fake cybersecurity site as a malware distribution hub.

"This suggests that Coquettte is a young individual, possibly a student, which aligns with the amateurish mistakes (like the open directory) in their cybercrime endeavors," DomainTools said.

The threat actor's ventures are not limited to malware, for they have also been running other websites that sell guides for manufacturing illegal substances and weapons. Coquettte is believed to be loosely tied to a broader hacking group that goes by the name Horrid.

"The pattern of overlapping infrastructure suggests that the individuals behind these sites may refer to themselves as 'Horrid,' with Coquettte being an alias of one of the members rather than a lone actor," the company said.

"The group's affiliation with multiple domains tied to cybercrime and illicit content suggests that it functions as an incubator for inspiring or amateur cybercriminals, providing resources and infrastructure to those looking to establish themselves in underground hacking circles."