facebook

Prepared By: Gopi Gor

Date: 11/11/2023

THREAT INTEL REPORT

Hype Value	General Risk	Risk to FACEBOOK
Low	High Risk	High Risk

Title: Malware attacking Facebook accounts with malicious ads

Date: 11th November 2023

DO NOT COPY

Threat description:

A new version of a malware called NodeStealer has been affecting Facebook users, by sending them malicious ads and then executing the malware when the users click on those ads. The NodeStealer malware is an information stealing malware that steals the browser cookies and also manifests account takeovers. It was first discovered by Meta in January 2023, but now the threat actors are building on the capabilities of the tool to further implement more payload on the systems.

The Facebook attack begins with a user being shown an ad of “pictures of young women” to lure the people into clicking the ad. This downloads a malicious .exe photo album in which another malicious executable .NET file with the payload, is downloaded. This steals the cookies of the browser along with the passwords. The malware is unrecognizable as it comes through a Windows .exe file as a kind of picture album.

Impact:

NodeStaler malware is a custom built malicious tool by threat actors in Vietnam. The attackers can seize control of the accounts and also bypass multiple security mechanisms to get into the system and steal cookies and other data. The impact of this is that, while users may be unaware, a lot of their data could be getting stolen, ads that download other malicious software which may give access to important personal and financial information.

As we already discussed, the malware comes as a photo album which then executes the malicious payload, and this could have a very high impact on the person, computer or network/organization that they may be a part of.

facebook

Risk Assessment:

The NodeStealer malware mainly targets social media profiles, and thus the social media industry, and uses the psychological thinking aspect of people to lure them into executing these .exe files. It takes into control, the account of the person, changes passwords and does the required action. The vulnerability that is takes advantage of, is already compromised facebook accounts through which they send these ad campaigns and also connect to the other accounts to get access.

Based on the above information, the risk to FACEBOOK is high. Facebook usually allows ads, but if they don't know what kind of ads are being used to divert people into downloading the photo albums, eventually due to the high level of speed of the ad campaigns, there could be a loss of billions to Facebook.

Actions taken:

1. Tackled the NodeStealer malware's current version.
2. Made changes to the ad preferences that are shown by having a malware response team to verify the ads that go up on Facebook.

Next steps and recommended actions:

1. Advised users to always use Anti-Malware and Anti-Virus on all their devices.
3. The users were requested to stick to good cyber hygiene, and not press on any random links.

Sources:

1. https://www.bitdefender.com/blog/labs/nodestealer-attacks-on-facebook-take-a-provocative-turn-threat-actors-deploy-malvertising-campaigns-to-hijack-users-accounts/
2. https://thehackernews.com/2023/11/nodestealer-malware-hijacking-facebook.html

Metadata:

Report Date: 11.06.2023

Analyst: Gopi Gor

History: v 1

DO NOT COPY