NPM IconBurst Supply Chain Attack Campaign: A Brief Overview

Threat Bulletins **TLP:WHITE** **Alert Id: fbc69680** **2022-07-27 19:13:19**

In response to a detailed investigation into the IconBurst supply chain attack campaign conducted by Reversing Labs, Health-ISAC is releasing this brief overview of the IconBurst campaign. This campaign is actively targeting developers at the third stage of the software development lifecycle (SDLC), systems design. The final objective of this campaign is to embed as many applications with malicious package managers.

The brief overview includes the following:

- Initial Incorporation
- Typo Squatting
- Data Exfiltration
- Threat Actor Information

Please see the attached one-page document for internal circulation within your organization.

Reference(s): ReversingLabs

Report Source(s): Health-ISAC

Sources:

IconBurst NPM software supply chain attack grabs data from apps and websites

Tags: IconBurst, Supply Chain, Npm, Typosquatting

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Intelligence Portal: Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments: Please email us at toc@h-isac.org