H-ISAC
HEALTH - ISAC
SHARING SINCE 2010

June 2022

NPM IconBurst Supply Chain Attack Campaign: A Brief Overview

Summary:

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 as possible with malicious package managers.

1. Initial Incorporation

Node Package Manager (NPM) is a very common resource for developers all over the world to use and share their package managers. This service has many free to use packages made by users, similar to Github repositories, but some require premium access. The malicious packages in this campaign focused on typo squatting the popular icon library, ionicons.

2. Typo Squatting

Typo Squatting is the term for an attack that relies on common misspellings of popular names. An example of this concept would be an attacker creating a malicious domain under the URL microsft.com to lure unsuspecting web users to their domain when trying to reach the benign domain microsoft.com. In the context of this campaign, malicious packages were made under the malicious author "ionic-io" with common typos of the name "ionicons" such as icon-package, package-ionicons, icons-pack, and pack-icons. Similar malicious package authors arpantek and arpanrizki created malicious imitations of popular open-source package "sidr" and phony icon library footericon.

3. Data Exfiltration

Once integrated, these modules act as data harvesters. They actively expand the jQuery ajax( ) function to seize data penitent to the product it is a part of, and relays it to a validated URL controlled by a malicious threat actor.

4. Threat Actor Information

According to Reversing Labs, the threat actors behind this campaign all exfiltrate data to a domain that ends in '.my.id', alluding to a common owner between all the domains used to harvest illegally obtained data. At the time of writing, the threat actors have not been identified, and these malicious packages have been downloaded over 27,000 times. For a full list of malicious packages, click [here](#).

Source:
https://blog.reversinglabs.com/blog/iconburst-npm-software-supply-chain-attack-grabs-data-from-apps-websites