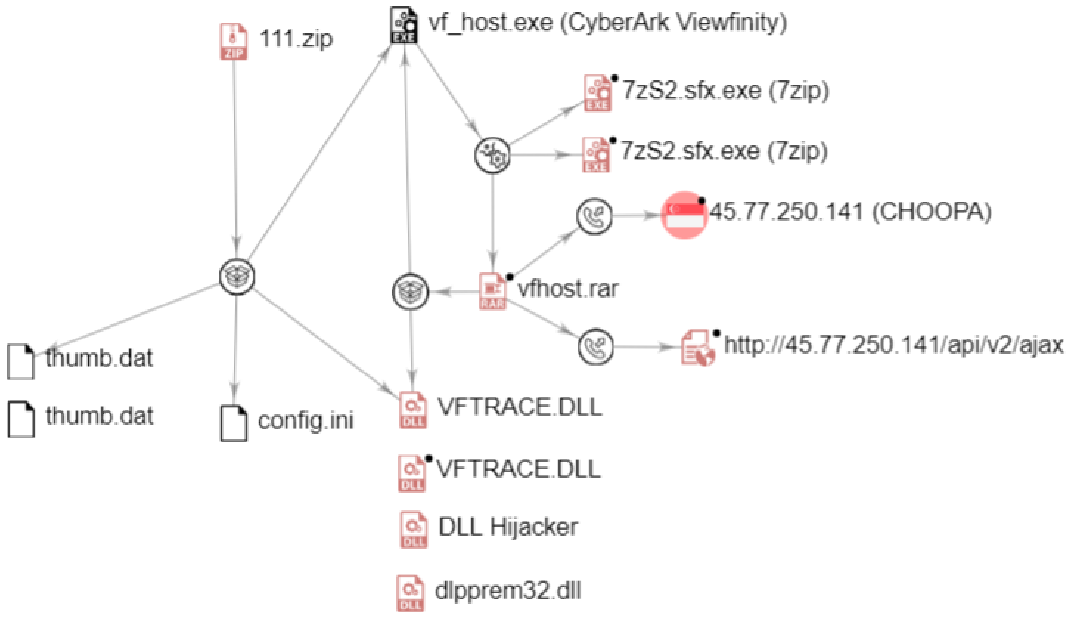
IronTiger APT campaign: New HyperBro and SysUpdate samples

curatedintel.org/2021/11/irontiger-apt-campaign-new-hyperbro-and.html

BushidoToken



Community Feature - @BushidoToken

A Curated Intelligence staff member - BushidoToken - recently uncovered new samples of the HyperBro and SysUpdate backdoor, connected to the IronTiger APT group (also known as LuckyMouse or APT27).

> https://twitter.com/Cyjax_Ltd/status/1456926491569176576

Just as before, the group uses multiple components: a genuine loader typically with signed certification (here CyberArk Viewfinity); malicious DLL loader loaded from the former component via DLL hijacking; encrypted and compressed blob (thumb.dat) that decrypts to PE-based payload with C2 information (config.ini) hardcoded.

Analysis of the code-signing certificates (Thumbprint: E5F7F5449C22F0A01DCFAC634732E2197AFCDD4C) used by IronTiger revealed that the group used a certificate from Cheetah Mobile, a Chinese mobile Internet company headquartered in Beijing.

Indicators of compromise (IOCs) are available on OTX Alienvault here.