Government of India
National Critical Information Infrastructure Protection Centre
(A Unit of NTRO)

Date: 29 Nov 2019

Cyber Security Advisory: DTrack Spyware

This data is to be considered as **TLP:AMBER**

Our trusted partner have reported an espionage activity of state sponsored malware campaign related to Dtrack that is closely related to ATM Dtrack malware campaign which was designed to collect TRACK1 and TRACK2 data of users who insert their cards into the infected Wincor Nixdorf ATM. DTrack automatically transfers the grabbed user data over the bank's internal network to a web server installed on a remote host.

Analyst's Note:

DTrack has functionalities which includes keylogging, retrieving browser history, gathering IP addresses, information about available networks, active connections, listing all running processes, and files on all available disk volumes. The droppers also contained an EventTRacker RAT that could allow attackers to perform various operations on a host.

IOCs:
Hashes(SHA512):
3cc9d9a12f3b884582e5c4daf7d83c4a510172a836de90b87439388e3cde3682 (sct.exe)
93a01fbbdd63943c151679d037d32b1d82a55d66c6cb93c40ff63f2b770e5ca9
a0664ac662802905329ec6ab3b3ae843f191e6555b707f305f8f5a0599ca3f68
bfb39f486372a509f307cde3361795a2f9f759cbeb4cac07562dcbaebc070364
c5c1ca4382f397481174914b1931e851a9c61f029e6b3eb8a65c9e92ddf7aa4c
8f360227e7ee415ff509c2e443370e56
3a3bad366916aa3198fd1f76f3c29f24
F84de0a584ae7e02fb0ffe679f96db8

Reference: CERT-In

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430