(TS/X) Matryoshka Profile

Genre: Threat Actor Profiles
Authors: vzvyozdochkin, smalyutin
Created: 2019-10-15 16:51:41.567111+00:00
Last updated: 2019-10-15 16:51:41.567123+00:00
Classification: TOP SECRET

#(U) Summary

(T/X) The cybercriminal, codenamed “Matryoshka” is a highly sophisticated and intelligent individual responsible for several phishing and malware campaigns targeted at government and industrial organizations.

(T/X) Data was captured on an Internet forum that is believed to come from Matryoshka. Matryoshka likes to test potential clients before he will do business with them. The captured data is believed to be one of his games. A forum post mentions finding his dating profile in order to solve his first puzzle.

(U) Matryoshka is also believed to be a narcissist and thinks he is smarter than everyone he encounters.

(U) Matryoshka typically shies away from monetary transfers and accepts exchanges only in unique and rare goods.

(U) The dating profile mentioned previously was found posted to the dating site, PlentyOfPhish.

Name	Frederick Kaludis
Nickname	Warlock
Birthday	Jan 1st, 1970
Favorite Color	Red
Lucky Number	19
Hobbies	Rickrolling, hiding things in plain sight, hiding things other ways, acquiring rare technological gadgets
Likes	80’s music, video games, gadgets, Russian dolls
Dislikes	Large bodies of water, Tall buildings, Cold weather, Animals

Indicators point to the registered email account being used to initiate a phishing campaign aimed at propagating malware throughout the local network of its victims.