The DoNot APT - K7 Labs

labs.k7computing.com/index.php/the-donot-apt/

By Vigneshwaran P

February 23, 2023

The DoNot APT (aka APT-C-35) has been active since 2016. They have attacked many individuals and organisations in South Asia. DoNot APT is reported to be the main developers and users of frameworks for developing Windows and Android malware[1].

This group mainly targets organisations in India, Pakistan, Sri Lanka, Bangladesh and other South Asian countries[2][3]. They focus on government and military organisations, foreign ministries, and embassies.

For the initial access, DoNot APT uses phishing emails containing malicious attachments. To get to the next stage, they execute a macro embedded in an MS Office document which drops a PE file and executes them. We have witnessed this PE file being a DLL file in the past campaigns. There is a change in the initial access of this APT group. The RedDrip Team, tagged a ZIP (filename: "Day .zip") file being part of the DoNot APT campaigns. The lure was themed to leverage geopolitical tensions between India and Pakistan as shown in Figure 1. The ZIP file is bundled with a WinRAR SFX executable, which contains a DLL file and PDF files under a folder named "*Kashmir*".

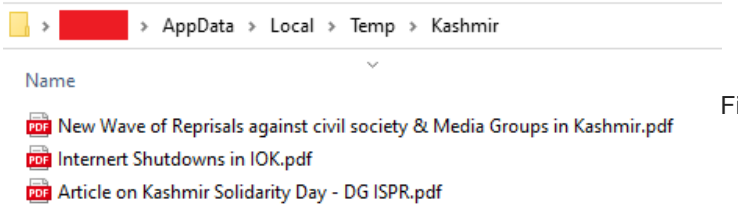

Figure 1: Components within in WinRAR SFX file

The SFX executable executes that DLL as shown in Figure 2. The DLL file is responsible for connecting to the C2. The C2 Server was down at the time of writing this blog.

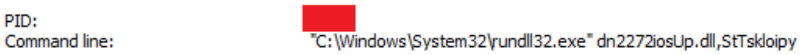

Figure 2: Process execution

The domain registrar for the C2 domain (briefdeal.buzz) is *NameSilo Inc,* which seems to be a pattern since September 2022. The DLL contains 2 export functions. The first function creates mutex ("olgui1pigg") as a marker for infection and then establishing connection to C2 and the next function is for self copying itself to the %TEMP% folder and creating a scheduled task for persistence by setting a new Scheduled Task that runs every four minutes. The action assigned to the task is to run the first export function. The C2 server was down during our analysis.

It tries to send the basic info of the Victim' PC to the C2 like Username, Computer Name, Processor ID.

Here we mentioned the timeline of samples which are used by DoNot APT from Sep 2022 to Jan 2023.

Time	Samples File Name
Jan 2023	Kashmir Solidarity Day Material .exeRequirement of pattenization data for seamanship items.xls
Dec 2022	spreadsheet.xlsdttcodexgigas.xlsSam.pptAccounts.xlsattachment.xlsff.xlstrix.xls
Nov 2022	Requirement list of spares.xls
Sept 2022	bodli.doc

The C2 URL TLD has been *.buzz* since the September 2022 campaign. The DNS registrar for the C2 URL is *NameSilo Inc.* and the IPs resolved to the ASN number *399629*. Based on the ASN number we were able to deduce the ISP as BL Networks, and from there we were able to track it to a Virtual Private Server (VPS) provider called BitLaunch, which accepts crypto payments. We found evidence of this particular VPS service being used for malicious campaigns in the past. We found this pattern to be consistent since September 2022.

We at K7 labs provide detection against such threats. Users are advised to use a reliable security product such as “K7 Total Security” and keep it up-to-date so as to safeguard their devices.

IOCs

HASH	File Name
4EAA63DD65FC699260306C743B46303B	Kashmir Solidarity Day Material .exe
07A3C19BC67C5F44C888CE75D4147ECF	dn2272iosUp.dll
08E2FAA6D92A94A055579A5F4F3FCD04	spreadsheet.xls
06ADBB4BA31A52CC5C9258BF6D99812C	Requirement list of spares.xls
795c0ee208d098df11d56d72236175b2	bodli.doc
7662B07F747EAE8433E347B70A33F727	trix.xls
24DEB1EEE361086268B2E462B9A42191	dttcodexgigas.xls
65F904DC7F675B93C2DEC927D2B8E58F	dttcodexgigas.xls
DC6DF9BDEE372A00E5402C19D2D77DE9	Requirement of pattenization data for seamanship items.xls
3e2b44bef17ae7bcce26e6211c68dc08	Sam.ppt
64266FC0F0B37A26E14133AD19B98B7C	Requirement list of spares.xls
BE0B5518E4D7EDFED694E2CE1B2C3CEA	Accounts.xls
835AB3B85B3217722095CDD14A1157BF	attachment.xls
82938D802B72C043E549E973023974DC	attachment.xls
79B5D2DA98CCF99135FFF67D0AD48488	Accounts.xls
D98E2D7C8E91A9D8E87ABE744F6D43F9	ff.xls
A65F67D12C73E0FA71813A645A924DBC	trix.xls
F6FCEFD16C5D9A31AE19A3BCE709B31E	spreedsheet.xls
7662B7D42F74E5FAEF1EE953419A31D4	Attachments.xls

C2 Domains

hxxp://5[.]135[.]199[.]0/football/goal

hxxps://briefdeal[.]buzz/Treolekomana/recopereta

hxxp://orangevisitorss[.]buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1tRyF47ZXLIdqNGRqiHQQHL6DJIjl2IoxUA[.]png

hxxp://orangevisitorss[.]buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1tRyF47ZXLIdqNGRqiHQQHL6DJIjl2IoxUA[.]mp4

hxxp://one[.]localsurfer[.]buzz/jl60UwJBkaWEkCSS/MU3gLGSnHhfDHRnwhlILSB27KZaK2doaq8s9V5M2RIgpeaD8[.]mp4

hxxp://one[.]localsurfer[.]buzz/jl60UwJBkaWEkCSS/MU3gLGSnHhfDHRnwhlILSB27KZaK2doaq8s9V5M2RIgpeaD8[.]ico

hxxp://orangeholister[.]buzz/kolexretriya78ertdcxmega895200[.]php

hxxp://one[.]localsurfer[.]buzz/jl60UwJBkaWEkCSS/MU3gLGSnHhfDHRnwhlILSB27KZaK2doaq8s9V5M2RIgpeaD8[.]png

One[.]localsurfer[.]buzz

hxxp://morphylogz[.]buzz/Ik3EIidq3fc2GGig/aFwrDmHIiBWh62kZPVb4bmV0waydPv0WtgqM0QTte5iAFzF0[.]png

hxxp://morphylogz[.]buzz/Ik3EIidq3fc2GGig/aFwrDmHIiBWh62kZPVb4bmV0waydPv0WtgqM0QTte5iAFzF0[.]ico

hxxps://itygreyhound[.]buzz/Kolpt523ytcserstrew/torel

itygreyhound[.]buzz

C2 IP

5.135.199.0

168.100.9.5

193.149.180.4

168.100.9.216

45.61.136.145

162.33.178.22

45.61.139.243

168.100.9.216

45.61.136.198

45.61.139.243

References: