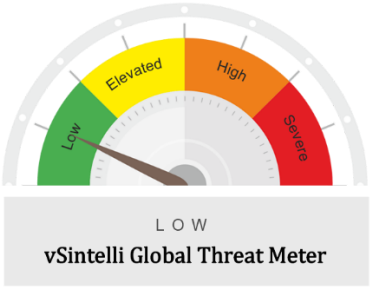

VSintelli – Threat Advisory

9th February 2018

TARGETED MALWARE CAMPAIGN IN MIDDLE EAST

Introduction

A targeted malware campaign has been discovered that makes use of Dar El-Jaleel decoy documents (Dar El-Jaleel is a Jordanian publishing and research house). The extensive use of scripting languages (VBScript, Power shell, VBA) is observed as a part of the campaign. The malware checks the various specifications of the targeted such as if the system is sandbox or not, installed antivirus, IP address, computer name, username, OS, drives attached to the targeted system. It is reported that the malware dropped from this campaign has functions to achieve persistence on the system and to send the acquired information to the Command & Control server. The various stages of the campaign are as follows:

1: VBScript – The purpose of the script to launch PowerShell script.

2: PowerShell Script – The purpose of the script to create a Microsoft Office document and open it.

3: Office Document with Macros – The purpose of macro to create Windows Script File and execute

4:WSF Script – The script contains functions to contact to C&C and execute additional payloads.

Indicators of Compromise

Hashes

15f5aaa71bfa3d62fd558a3e88dd5ba26f7638bf2ac653b8d6b8d54dc7e5926b

4b03bea6817f0d5060a1beb8f6ec2297dc4358199d4d203ba18ddfcca9520b48

d49e9fdfdce1e93615c406ae13ac5f6f68fb7e321ed4f275f328ac8146dd0fc1

e66af059f37bdd35056d1bb6a1ba3695fc5ce333dc96b5a7d7cc9167e32571c5

af7a4f04435f9b6ba3d8905e4e67cfa19ec5c3c32e9d35937ec0546cce2dd1ff

76a9b603f1f901020f65358f1cbf94c1a427d9019f004a99aa8bff1dea01a881

88e4f306f126ce4f2cd7941cb5d8fcd41bf7d6a54cf01b4a6a4057ed4810d2b6

c5bfb5118a999d21e9f445ad6ccb08eb71bc7bd4de9e88a41be9cf732156c525

1176642841762b3bc1f401a5987dc55ae4b007367e98740188468642ffbd474e

Malicious Domain

office-update[.]services

jo[.]foxlove[.]life

eg[.]foxlove[.]life

fox[.]foxlove[.]life

download[.]share2file[.]pro

update[.]share2file[.]pro

Malicious IP

176[.]107[.]185[.]246

References

[1] Targeted Attacks in The Middle East

https://blog.talosintelligence.com/2018/02/targeted-attacks-in-middle-east.html