“银狐”系列网络攻击活动相关木马病毒样本分析报告

一、样本基本情况

1. winx64-Letsvpnkaulian.x189.exe

国家计算机病毒协同分析平台于10月25日首次发现相关样本，记录为样本1，如表1所示。

表1 样本1基本信息

Sha256	205544cf98cadd91f017c29a89381e1280107e1830c6ab3a3fe2f9617fcf5795
SHA1	c2e0ed327e86d539c79d551a36bc1fc618ac7aca
MD5	76fde3d9e22459c5ff81ea824796a6d3
文件类型	Exe 可执行程序
文件大小	105 MB
文件名称	winx64-Letsvpnkaulian.x189.exe
图标	

如表1所示，样本1为捆绑letsvpn安装包的木马病毒，其主要功能是释放letsvpn的安装包，以及木马后门样本2、样本3和样本4，并执行样本2。具体执行过程如图1所示。具体木马病毒样本信息如表2、表3和表4所示。

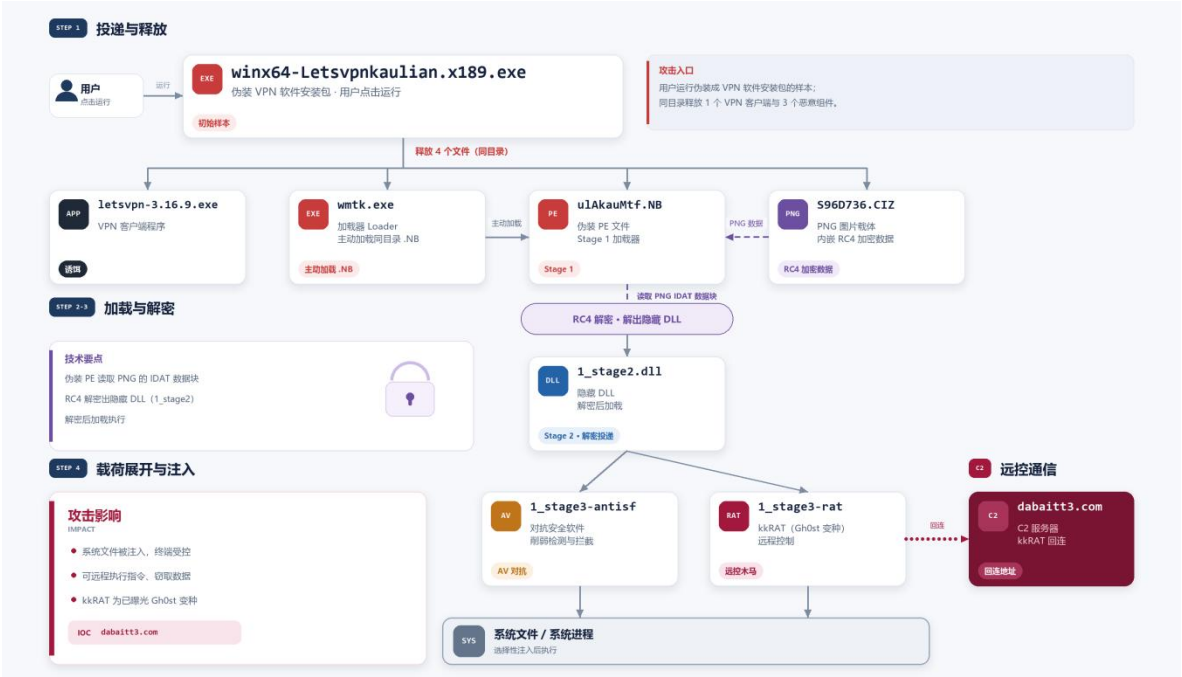


图 1 样本 1 运行过程示意图

表 2 样本 2 基本信息

Sha256	110852903477b66c04b426b1763fb5e37037e50a284e6adc13a63829308b5c42
SHA1	36fd3818135d8ecfaa834519e365927def99aa31
MD5	5b1d8ebe9aaf2634404d9173a9ed9e4c
文件类型	Exe 可执行程序
文件大小	74.8 KB
文件名称	wmTK.exe
图标	

表 3 样本 3 基本信息

Sha256	7fbb586fdf3ef61a3411ed391c433da7f5edb429a4663cf0e0622e50ec91fe34
SHA1	e8ed001a269bef601f1e9cd030cc5db086b8e64b
MD5	168c67315371357a9df22fbebeff38ae
文件类型	BinExecute/Microsoft.DLL[:X64]
文件大小	6.58 MB
文件名称	ulAkauMtf.NB
图标	

表 4 样本 4 基本信息

Sha256	3ff47ba37f0fdcc5b0db95d6b59611c92cb9a7046c7f9aa7831632aaacfed254
SHA1	22f1b29e348af26896a888b84fe290ee981e81ef
MD5	7b42365c5aee42561e49a553903fd085
文件类型	png
文件大小	10.1 MB
文件名称	S96D736.CIZ
图标	

样本 2 执行后会主动加载样本 3，样本 3 能够读取样本 4 中的数据块，解密出样本 5 并在内存中执行，样本 5 会继续解密出样本 6 和样本 7，其中样本 6 为与安全软件对抗的插件，样本 7 为远控木马，其通联域名为 dabaitt3[.]com，其与 IP 地址为 27.124.47.157 的服务器存在通联情况。

具体木马病毒样本信息如表 5、表 6 和表 7 所示。

表 5 样本 5 基本信息

Sha256	629cda8ff60c188144817034f53051f05882599bbbfdb6fc51d957a4866f2850
SHA1	3fefd98b2ff9bde80e93877a612810bc5d27a820
MD5	97929c324c953c3e5f5e3392d2165832
文件类型	BinExecute/Microsoft.DLL[:X64]
文件大小	10.2 MB
文件名称	1_stage2

表 6 样本 6 基本信息

Sha256	3d91161e89a548494140db2592490c0a2d237b3b507412be05a21e07a9321d40
SHA1	a76a7803d1c6c66ced75277d447987ff2f526a3d
MD5	b47b420bdb6e7de7060decd747f5b6bb
文件类型	Exe 可执行程序
文件大小	233 KB
文件名称	1_stage3-antisf

表 7 样本 7 基本信息

Sha256	56b57e732e27de41e8c22e09a4f165cdac1d6b38692d4d7e46f99ab069ef430f
SHA1	ff3bfc3a8d0b6b66e0c1acb68611e4e62308535b
MD5	23caaa5671f09b8587fc23c52e28ff26
文件类型	BinExecute/Microsoft.DLL[:X64]
文件大小	3.88 MB
文件名称	1_stage3-rat

2. WinVpn_Letsvpn_20261101.exe

除样本 1 外，我单位还捕获名为“WinVpn_Letsvpn_20261101.exe”的相关病毒样本（样本 8）。该样本在最后阶段使用了与样本 1 不同的远控木马。具体样本信息如表 8 所示。

表 8 样本 8 基本信息

Sha256	16edfb1e56563316c729b17d4e677f88392a52991eb9608564d9376b25104ab8
SHA1	e94397b728314d3cb8003929f3e705a87d63314c
MD5	1744e0505a23e6b4c45cd3c8223f4853
文件类型	Exe 可执行程序
文件大小	245 MB
文件名称	WinVpn_Letsvpn_20261101.exe
图标	

初始样本 8 会释放出 letsvpn 的安装包、样本 9、样本 10 和样本 11，启动 letsvpn 的安装包并在后台静默执行样本 9。样本 8 具体运行过程如图 2 所示。相关样本信息如表 9、表 10 和表 11 所示。

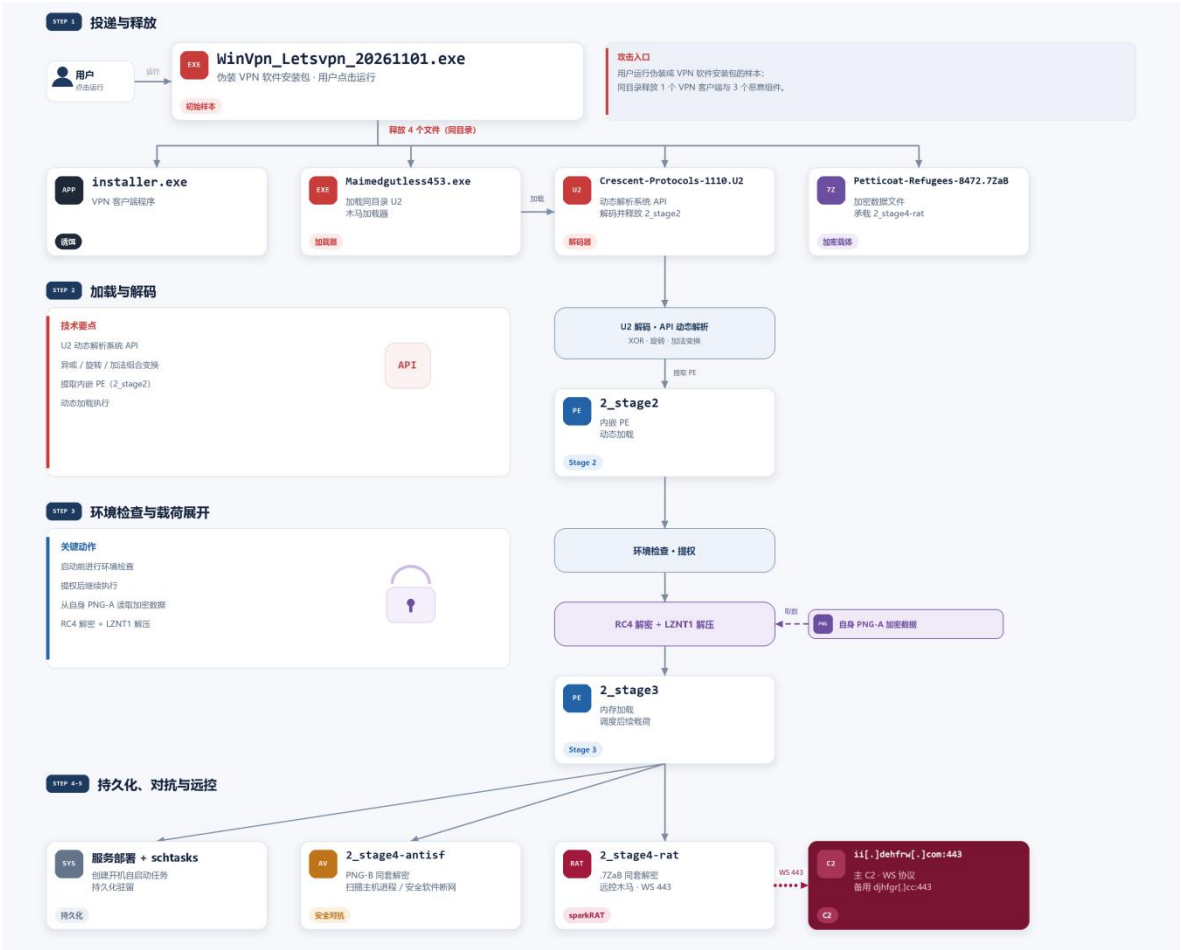


图 2 样本 8 运行过程示意图

表 9 样本 9 基本信息

Sha256	16873d3c935cda65046b6f6404a2cb1649e877dc46839b35d1846aead2906580
SHA1	ffbc93d8130697ddda079f29fdca1883d67f4f4d
MD5	8eaf106ae7f64eda68eeb446bb711e9c
文件类型	Exe 可执行程序
文件大小	103 KB
文件名称	Maimedgutless453.exe
图标	

表 10 样本 10 基本信息

Sha256	c1f22946ca0acaede075c6d42c4948b86cfc3cd69836bb11b678dcdac774d9ca
SHA1	c28202cd5b84824f102e43fdf0dbb280274ee730
MD5	1d6022b250fac20191c2f3fefd885264
文件类型	BinExecute/Microsoft.DLL[:X64]
文件大小	4.35 MB
文件名称	Crescent-Protocols-1110.U2
图标	

表 11 样本 11 基本信息

Sha256	af64e03d865081ecff1d391b020e00b918d70fd72d3244d8c8a472c69cdf6099
SHA1	e9da134240da4fcf31079511e167fe76061cbb42
MD5	b51bb8a391877d95b7e0aeb14d07caa3
文件类型	png
文件大小	10.3 MB
文件名称	Petticoat-Refugees-8472.7ZaB
图标	

样本 9 执行后会加载样本 10，样本 10 读取样本 11 并解密出样本 12，样本 12 检查完当前环境后继续解密出样本 13，样本 13 部署服务并创建计划任务，最后释放出样本 14 与样本 15。样本 14 为对抗安全软件的插件，样本 15 为与样本 7 不同家族的远控木马，其与域名 ii[.]dehfrw[.]com（103.204.13.70）和 djhfgr[.]cc（172.67.134.193）存在通联情况。样本 12、样本 13、样本 14

与样本 15 的信息如表 12、表 13、表 14 和表 15 所示。

表 12 样本 12 基本信息

Sha256	0a38ec9def72ef1ec043d7b982939c065fb9f3b7e3a86b3aa5e7c8788163e454
SHA1	39a6da13e8e7cc3279da2972cd18502ca395d559
MD5	e30a1194493a8d1d923d05837c348ba0
文件类型	Exe 可执行程序
文件大小	2.15 MB
文件名称	2_stage2

表 13 样本 13 基本信息

Sha256	228c3cbb6aef60a5e8ea1e433e698f8f35d7cc5ad50507b2e9a56985dddf88ed
SHA1	45ed8c3ef54c4ed147ca2cafadbc594a3156eac4
MD5	112467d3419f30a06bf0fa1c8931668b
文件类型	BinExecute/Microsoft.DLL[:X64]
文件大小	925 KB
文件名称	2_stage3

表 14 样本 14 基本信息

Sha256	6a519ca9e1a7d813b42191f99c1b7669047219885a9e3e73ff5f161c009a0b92
SHA1	b465c28531c631b03227d2f8cb70fc0f5fff7397
MD5	94deaabd06db45094e93a632bca43a59
文件类型	BinExecute/Microsoft.DLL[:X64]
文件大小	271 KB
文件名称	2_stage4_antisf

表 15 样本 15 基本信息

Sha256	1ca280060c1133de7f992999fbe1b6af9dc32a98c6cd9ceafc283380536d0cd6
SHA1	70c0b577fe0d9ff0b2fbbb9f4d0bef3fd487a5c4
MD5	014eeb6d755925f6ce90a98460a06243
文件类型	Exe 可执行程序
文件大小	18.0 MB
文件名称	2_stage4_rat

3. letsvpn.exe

除样本 1 与样本 8 外，我单位还捕获到使用另一个远控木马家族的名为“letsvpn.exe”的可执行程序（样本 16），程序执行后同样释放一个 letsvpn 的安装包与三个后门程序（样本 17、样本 18、样本 19）。样本 16 运行过程如图 3 所示，相关样本信息如表 16、表 17、表 18、表 19 所示。

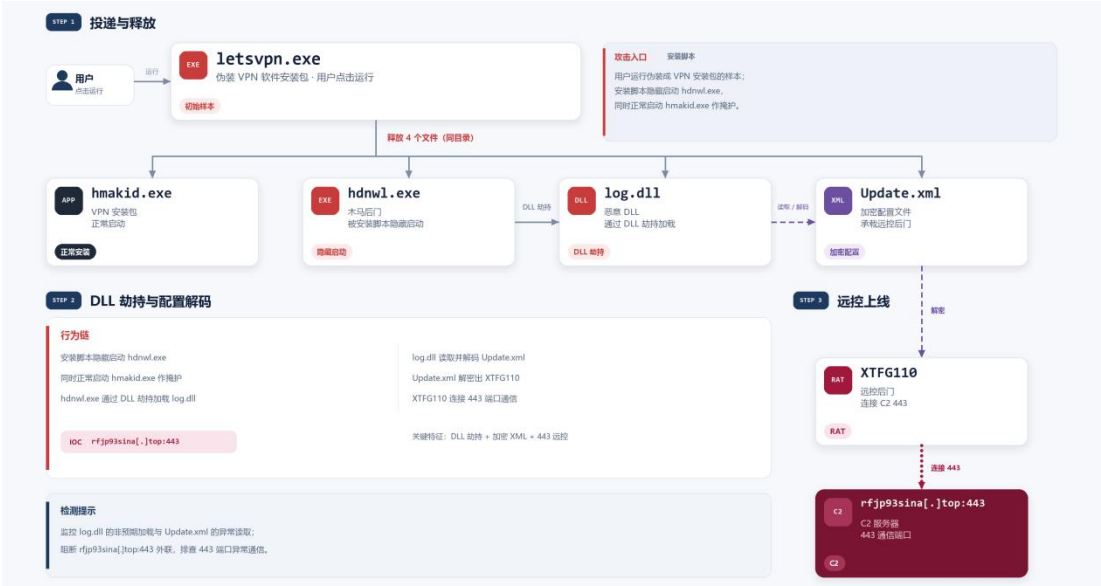


图 3 样本 16 运行过程示意图

表 16 样本 16 基本信息

Sha256	7353d8c8cbfa5381e556c58370e0f3e6bc0e87f80c0d68578a014f9c34ef681f
SHA1	b087a28a8c71f9f3c23c4d30953107463ef384ce
MD5	c2875f9ff4f56bb59bbe141ab138477d
文件类型	Exe 可执行程序
文件大小	19.6 MB
文件名称	letsvpn.exe
图标	

表 17 样本 17 基本信息

Sha256	c027cf868757babab33686bf4c41192339e04fa89ad868409a5cd4ed90a1f71e
SHA1	fbd8966926b4597049c115f5d5eb89659a5df213
MD5	bcec4279d95d0b09ebcf4388cb9a4f64
文件类型	Exe 可执行程序
文件大小	260 KB
文件名称	hdnwl.exe
图标	

表 18 样本 18 基本信息

Sha256	7cd8c3212f11e86a4afde956d4a13b04d18dc3700ef26b207533327024235159
SHA1	d0a4664d0ceebebcecea2880e5d3c7ebd9cf9bb3
MD5	07b7639f8031e08dcffdf7e03ba2327f
文件类型	BinExecute/Microsoft.DLL[:X32]
文件大小	259 KB
文件名称	log.dll
图标	

表 19 样本 19 基本信息

Sha256	e33cc1998367201b68b27c648596bbfbc5fe503c5fbe2e5758a50ad4c50f2dca
SHA1	34f3a18b1694d3c5a20ae5acc1a11bcc55784e6d
MD5	7df7ff5e7e62e78df03b834abca045ee
文件类型	Binary
文件大小	1.01 MB
文件名称	Update.xml
图标	

样本 17 运行后会自动加载样本 18，样本 18 读取样本 19 并

从中解密出远控木马本体（样本 20），其与域名 rfjp93sina[.]top 存在通联情况，其服务器 IP 地址为 143.92.35.33。样本 20 的信息如表 20 所示。

表 20 样本 20 基本信息

Sha256	8b675d8da36df9c98436089360970998d7d6cda675b02cebb9fa801b6e9dbdb0
SHA1	0e7dcc237f2fd2333621da614ca3a40fc0990103
MD5	d842e2ea2205e01ec77c1a04e3771424
文件类型	BinExecute/Microsoft.DLL[:X32]
文件大小	1.00 MB
文件名称	XTFG110

另有同源样本 21，与样本 16 的执行流程完全相同，同样会释放出远控木马样本 20；样本 21 涉及的样本包含样本 17（见表 17）、样本 22、样本 23、样本 20（见表 20）。具体样本信息如表 20、表 21、表 22 和表 23 所示。

表 21 样本 21 基本信息

Sha256	44cd0e97316c4ed137b1612e5b4d56f7caaa0250d3badbb344927671a6979714
SHA1	a4c1719efe4255d5c34366b87e0046c3864c0c15
MD5	e6bd58f332c9aabe502e35ccedb38313
文件类型	Exe 可执行程序
文件大小	19.7 MB
文件名称	letsvpn-latest_2.exe
图标	

表 22 样本 22 基本信息

Sha256	21900eabf7b78e235214fda8cbe2b81844b0d2d4157a23f32b6bc0c2fa6552fb
SHA1	7649a0a7a498b1a59bac4f9cf1a697e9e3d8b88a
MD5	86d73add0df21eb9a1d4b9ff8c981358
文件类型	BinExecute/Microsoft.DLL[:X32]
文件大小	164 KB
文件名称	log.dll
图标	

表 23 样本 23 基本信息

Sha256	8821309706175e8283a3902f88e6220de28c9dd2fb8fb679a10ff98c87f344b4
SHA1	41557494fb261bb0febf0e4d2633b61f1e1f08bc
MD5	2acb4545c61845510e82b1a8c26483d1
文件类型	Binary
文件大小	1.01 MB
文件名称	Update.xml
图标	

二、样本关联情况

1. 样本 16 与样本 21 之间存在关联

如图 4 所示，样本 16 与样本 21 释放的样本文件在名称与功能上一一对应（部分文件为不同版本），且在代码特征、系统行为特征与传播行为上均与“银狐”团伙存在显著关联。

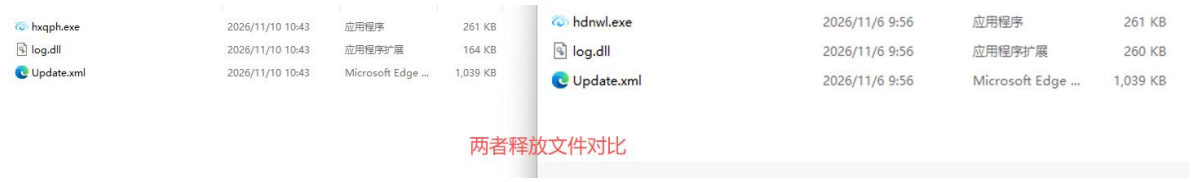


图 4 样本 16 和样本 21 释放的样本对比

2. 样本 1 与样本 8 之间存在弱关联

如图 5 所示，两者均使用对抗安全软件的相似功能插件，功能实现方式也类似。样本 1 与样本 8 在代码功能特征上具有一定关联关系，同时在加密解密特征上二者也存在一定关联。



图 5 样本 1 和样本 8 使用相同的技术手段对抗安全软件

三、典型样本详细技术分析

以样本 1（“winx64-Letsvpnkaulian.x189.exe”）为例。如图 6 所示，文件大小为 105 MB，外层加载程序为使用经过修改的 Inno Setup 打包的安装程序。

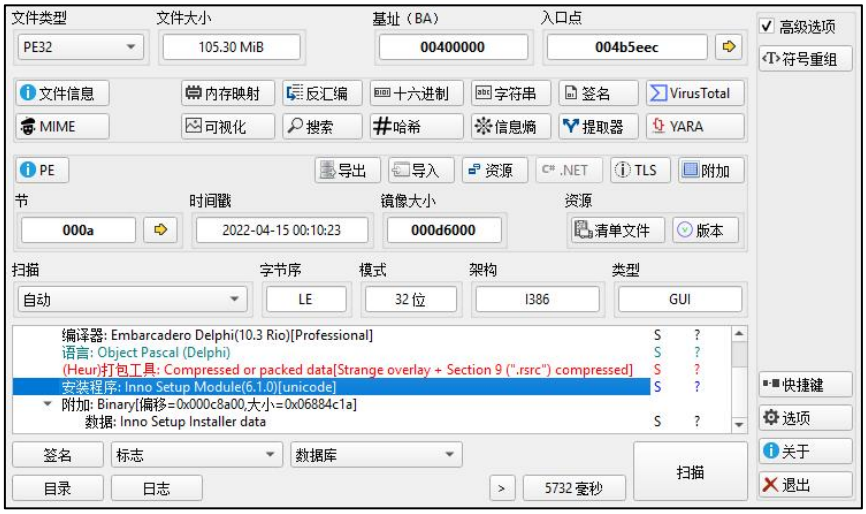


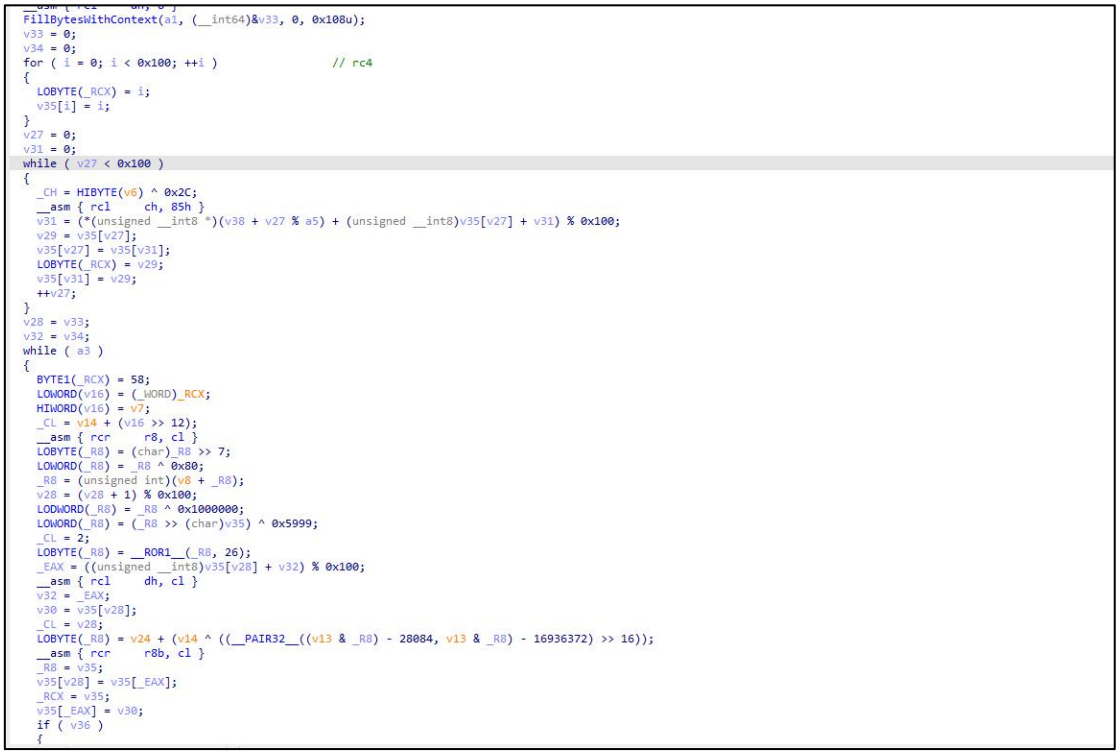
图 6 样本 1 基本信息

如图 7 所示，样本主要功能是释放出打包好的 letsvpn 安装包与后门程序，并在后台静默执行后门程序。



图 7 释放文件

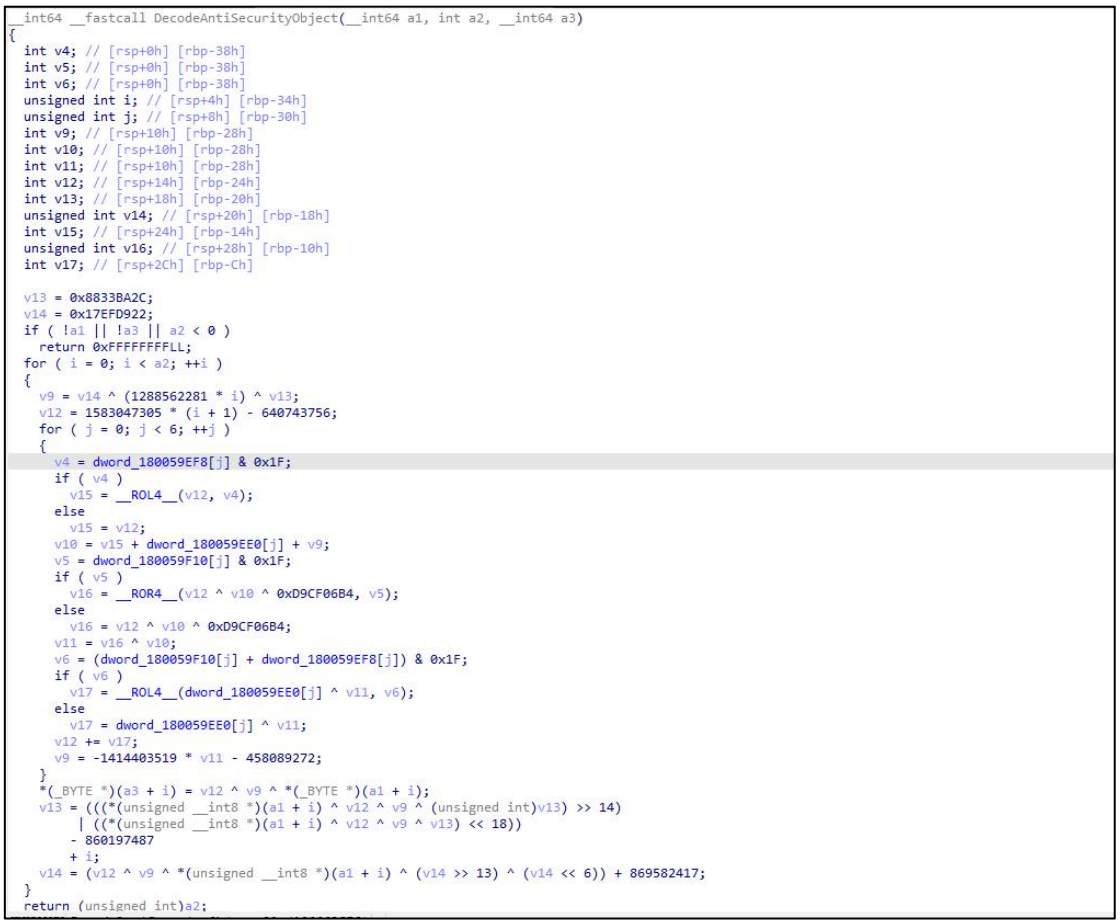
后续由样本 2 加载样本 3，样本 3 读取样本 4 并使用 RC4 解密，获取样本 5 并在内存当中加载，如图 8 所示。



```
FillBytesWithContext(a1, (__int64)&v33, 0, 0x108u);
v33 = 0;
v34 = 0;
for ( i = 0; i < 0x100; ++i )                 // rc4
{
  LOBYTE(_RCX) = i;
  v35[i] = i;
}
v27 = 0;
v31 = 0;
while ( v27 < 0x100 )
{
  _CH = HIBYTE(v6) ^ 0x2C;
  __asm { rcl     ch, 85h }
  v31 = (*(unsigned __int8 *)(v38 + v27 % a5) + (unsigned __int8)v35[v27] + v31) % 0x100;
  v29 = v35[v27];
  v35[v27] = v35[v31];
  LOBYTE(_RCX) = v29;
  v35[v31] = v29;
  ++v27;
}
v28 = v33;
v32 = v34;
while ( a3 )
{
  BYTE1(_RCX) = 58;
  LOWORD(v16) = (_WORD)_RCX;
  HIWORD(v16) = v7;
  _CL = v14 + (v16 >> 12);
  __asm { rcr     r8, cl }
  LOBYTE(_R8) = (char)_R8 >> 7;
  LOWORD(_R8) = _R8 ^ 0x80;
  _R8 = (unsigned int)(v8 + _R8);
  v28 = (v28 + 1) % 0x100;
  LODWORD(_R8) = _R8 ^ 0x1000000;
  LOWORD(_R8) = (_R8 >> (char)v35) ^ 0x5999;
  _CL = 2;
  LOBYTE(_R8) = __ROR1__(_R8, 26);
  _EAX = ((unsigned __int8)v35[v28] + v32) % 0x100;
  __asm { rcl     dh, cl }
  v32 = _EAX;
  v30 = v35[v28];
  _CL = v28;
  LOBYTE(_R8) = v24 + (v14 ^ ((__PAIR32__((v13 & _R8) - 28084, v13 & _R8) - 16936372) >> 16));
  __asm { rcr     r8b, cl }
  _R8 = v35;
  v35[v28] = v35[_EAX];
  _RCX = v35;
  v35[_EAX] = v30;
  if ( v36 )
  {
```

图 8 RC4 解密样本 5

样本 5 继续解密出对抗安全软件的样本 6 和远控木马样本 7，并且根据当前环境选择性注入 uhssv.exe、sihost.exe、ctfmon.exe 等系统进程。样本 5 解密流程如图 9 所示。

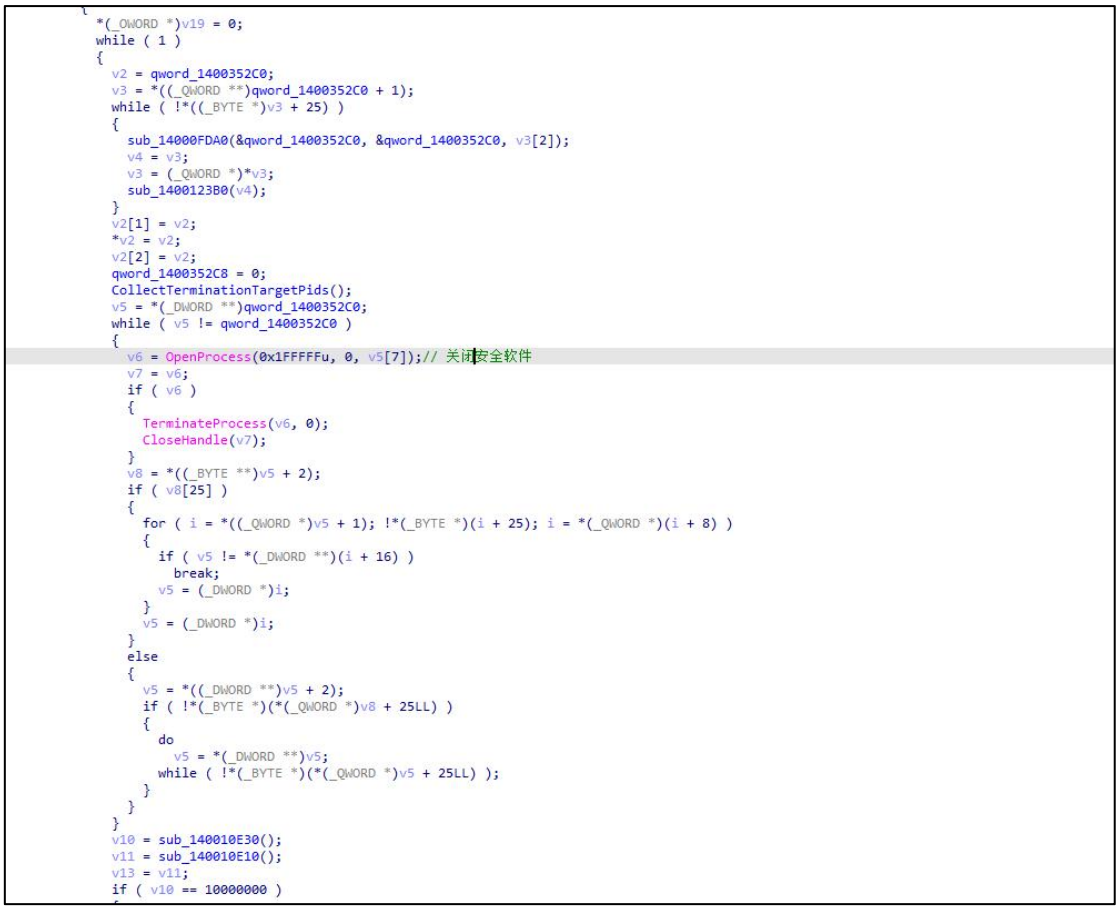


```
__int64 __fastcall DecodeAntiSecurityObject(__int64 a1, int a2, __int64 a3)
{
  int v4; // [rsp+0h] [rbp-38h]
  int v5; // [rsp+0h] [rbp-38h]
  int v6; // [rsp+0h] [rbp-38h]
  unsigned int i; // [rsp+4h] [rbp-34h]
  unsigned int j; // [rsp+8h] [rbp-30h]
  int v9; // [rsp+10h] [rbp-28h]
  int v10; // [rsp+10h] [rbp-28h]
  int v11; // [rsp+10h] [rbp-28h]
  int v12; // [rsp+14h] [rbp-24h]
  int v13; // [rsp+18h] [rbp-20h]
  unsigned int v14; // [rsp+20h] [rbp-18h]
  int v15; // [rsp+24h] [rbp-14h]
  unsigned int v16; // [rsp+28h] [rbp-10h]
  int v17; // [rsp+2Ch] [rbp-Ch]

  v13 = 0x8833BA2C;
  v14 = 0x17EFD922;
  if ( !a1 || !a3 || a2 < 0 )
    return 0xFFFFFFFFLL;
  for ( i = 0; i < a2; ++i )
  {
    v9 = v14 ^ (1288562281 * i) ^ v13;
    v12 = 1583047305 * (i + 1) - 640743756;
    for ( j = 0; j < 6; ++j )
    {
      v4 = dword_180059EF8[j] & 0x1F;
      if ( v4 )
        v15 = __ROL4__(v12, v4);
      else
        v15 = v12;
      v10 = v15 + dword_180059EE0[j] + v9;
      v5 = dword_180059F10[j] & 0x1F;
      if ( v5 )
        v16 = __ROR4__(v12 ^ v10 ^ 0xD9CF06B4, v5);
      else
        v16 = v12 ^ v10 ^ 0xD9CF06B4;
      v11 = v16 ^ v10;
      v6 = (dword_180059F10[j] + dword_180059EF8[j]) & 0x1F;
      if ( v6 )
        v17 = __ROL4__(dword_180059EE0[j] ^ v11, v6);
      else
        v17 = dword_180059EE0[j] ^ v11;
      v12 += v17;
      v9 = -1414403519 * v11 - 458089272;
    }
    *(_BYTE *)(a3 + i) = v12 ^ v9 ^ *(_BYTE *)(a1 + i);
    v13 = (((*(unsigned __int8 *)(a1 + i) ^ v12 ^ v9 ^ (unsigned int)v13) >> 14)
         | ((*(unsigned __int8 *)(a1 + i) ^ v12 ^ v9 ^ v13) << 18))
        - 860197487
        + i;
    v14 = (v12 ^ v9 ^ *(unsigned __int8 *)(a1 + i) ^ (v14 >> 13) ^ (v14 << 6)) + 869582417;
  }
  return (unsigned int)a2;
```

图 9 解密样本 6 算法

样本 6 每隔 300 毫秒按进程名字扫描一遍进程，命中后会尝试关闭该进程，相关进程涉及 360、bitdefender、金山、ESET、卡巴斯基等；每隔 200 毫秒程序会向 Windows NSI 请求断开上述进程已建立的 TCP 连接；同时每隔 5 秒会尝试清理上述命中的程序的相关服务。关闭进程功能如图 10 所示，关闭 TCP 连接如图 11 所示。



```
{
  *(_OWORD *)v19 = 0;
  while ( 1 )
  {
    v2 = qword_1400352C0;
    v3 = *((_QWORD **)qword_1400352C0 + 1);
    while ( !*((_BYTE *)v3 + 25) )
    {
      sub_14000FDA0(&qword_1400352C0, &qword_1400352C0, v3[2]);
      v4 = v3;
      v3 = (_QWORD *)*v3;
      sub_1400123B0(v4);
    }
    v2[1] = v2;
    *v2 = v2;
    v2[2] = v2;
    qword_1400352C8 = 0;
    CollectTerminationTargetPids();
    v5 = *(_DWORD **)qword_1400352C0;
    while ( v5 != qword_1400352C0 )
    {
      v6 = OpenProcess(0x1FFFFFu, 0, v5[7]);// 关闭安全软件
      v7 = v6;
      if ( v6 )
      {
        TerminateProcess(v6, 0);
        CloseHandle(v7);
      }
      v8 = *((_BYTE **)v5 + 2);
      if ( v8[25] )
      {
        for ( i = *((_QWORD *)v5 + 1); !*(_BYTE *)(i + 25); i = *(_QWORD *)(i + 8) )
        {
          if ( v5 != *(_DWORD **)(i + 16) )
            break;
          v5 = (_DWORD *)i;
        }
        v5 = (_DWORD *)i;
      }
      else
      {
        v5 = *((_DWORD **)v5 + 2);
        if ( !*(_BYTE *)(*(_QWORD *)v8 + 25LL) )
        {
          do
            v5 = *(_DWORD **)v5;
          while ( !*(_BYTE *)(*(_QWORD *)v5 + 25LL) );
        }
      }
    }
    v10 = sub_140010E30();
    v11 = sub_140010E10();
    v13 = v11;
    if ( v10 == 10000000 )
```

图 10 关闭安全软件



```
    (_QWORD *)&v41 = v25;
    v42 = v16;
    v43 = v19;
    sub_140022500(v23, v17, 2 * v16 + 2);
    v13 = (char *)xmmword_140035300;
LABEL_27:
    v24 = sub_14000FB80(v44, &v13[32 * v12]);
    if ( (unsigned __int8)StringsEqualIgnoreCase(v24, &v41) )
    {
      LODWORD(SizePointer) = 0;
      if ( GetTcpTable2(nullptr, (PULONG)&SizePointer, 1) == 122 )
      {
        v25 = (struct _MIB_TCPTABLE2 *)sub_140018030((unsigned int)SizePointer);
        v26 = v25;
        if ( v25 )
        {
          if ( !GetTcpTable2(v25, (PULONG)&SizePointer, 1) )
          {
            for ( i = 0; i < v26->dwNumEntries; ++i )
            {
              v28 = i;
              if ( v26->table[v28].dwOwningPid == th32ProcessID && v26->table[v28].dwState == 5 )
                DisconnectTcpViaNsi(&v26->table[v28]);// 断开tcp连接
            }
          }
          sub_140018020(v26);
        }
      }
LABEL_39:
      v9 = v53;
```

图 11 关闭 TCP 连接

最终释放的远控木马为 kkrat，属于 gh0st 远控木马的变种，程序会连接 dabaitt3[.]com 并接收指令，且包含命令执行、文件创建、插件加载、键盘读取、屏幕监控等一系列远控功能。

样本当中的解密密钥与已公开案例中的 kkrat 解码器密钥相同；其加载方式也具有较高相似性，均为三段式加载；也同样使用 PNG 隐藏载荷。解密密钥对比如图 12 所示，木马远控指令如图 13 所示。

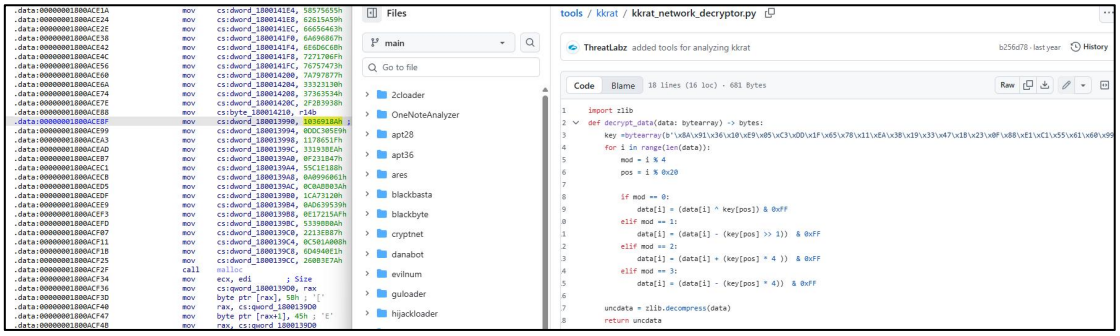


图 12 本次样本密钥与公开密钥对比

```
    return;
  }
  v89 = v88 - 6;
  if ( v89 )
  {
    v90 = v89 - 1;
    if ( !v90 )
    {
      ExecuteReceivedCmdCommand((char *)a2 + 2);
      return;
    }
    v91 = v90 - 9;
    if ( !v91 )
    {
      StageAndRunReceivedFile(a2, (unsigned int)v3);
      return;
    }
    v92 = v91 - 3;
    if ( v92 )
    {
      if ( v92 != 1 )
        return;
      strcpy(v99, "dllog");
      v94 = -30;
      sub_180085F64(v99);
      v54 = 1;
      v55 = &v94;
LABEL_76:
      sub_180086704(a1, v55, v54);
      return;
    }
    v93 = a2[1];
    v95 = -31;
    dword_18000F394 = v93;
    dword_18000F390 = 1;
    memmove(qword_180012C90, a2 + 2, 0x18Cu);
    v55 = &v95;
LABEL_75:
    v54 = 1;
```

图 13 远控木马指令分配

四、总结

综合上述情况，此次发现的样本均采用了类似的逃避检测技术，且复杂度较高。相关样本之间存在直接或间接的联系，并与“银狐”系列网络攻击活动历史案例具有较强关联性，但可能分属不同的犯罪团伙，即多个犯罪团伙围绕同一攻击活动“脚本”采用不同的技术路线开展攻击活动。

国家计算机病毒应急处理中心

计算机病毒防治技术国家工程实验室

2026 年 11 月 18 日

附录:

附表 1 相关木马病毒样本及通联信息汇总

序号	文件 Hash（MD5）	文件名	通联域名、IP 地址	关联样本
1	76fde3d9e22459c5ff81ea824796a6d3	winx64-Letsvpnkaulian.x189.exe	dabaitt3[.]com（27.124.47.157）	5b1d8ebe9aaf2634404d9173a9ed9e4c 168c67315371357a9df22fbebeff38ae 7b42365c5aee42561e49a553903fd085 97929c324c953c3e5f5e3392d2165832 b47b420bdb6e7de7060decd747f5b6bb 23caaa5671f09b8587fc23c52e28ff26
2	1744e0505a23e6b4c45cd3c8223f4853	WinVpn_Letsvpn_20261101.exe	ii[.]dehfrw[.]com （103.204.13.70） djhfgr[.]cc （172.67.134.193）	8eaf106ae7f64eda68eeb446bb711e9c 1d6022b250fac20191c2f3fefd885264 b51bb8a391877d95b7e0aeb14d07caa3 e30a1194493a8d1d923d05837c348ba0 112467d3419f30a06bf0fa1c8931668b 94deaabd06db45094e93a632bca43a59 014eeb6d755925f6ce90a98460a06243
3	c2875f9ff4f56bb59bbe141ab138477d	letsvpn.exe	rfjp93sina[.]top（143.92.35.33）	bcec4279d95d0b09ebcf4388cb9a4f64 07b7639f8031e08dcffdf7e03ba2327f 7df7ff5e7e62e78df03b834abca045ee d842e2ea2205e01ec77c1a04e3771424
4	e6bd58f332c9aabe502e35ccedb38313	letsvpn-latest_2.exe	rfjp93sina[.]top（143.92.35.33）	86d73add0df21eb9a1d4b9ff8c981358 2acb4545c61845510e82b1a8c26483d1

IoCs（感染指标）:

文件名：
winx64-Letsvpnkaulian.x189.exe
wmTK.exe
ulAkauMtf.NB
S96D736.CIZ
WinVpn_Letsvpn_20261101.exe
Maimedgutless453.exe
Crescent-Protocols-1110.U2
Petticoat-Refugees-8472.7ZaB
letsvpn.exe
hdnwl.exe
letsvpn-latest_2.exe

文件哈希：
76fde3d9e22459c5ff81ea824796a6d3
5b1d8ebe9aaf2634404d9173a9ed9e4c
168c67315371357a9df22fbebeff38ae
7b42365c5aee42561e49a553903fd085
97929c324c953c3e5f5e3392d2165832
b47b420bdb6e7de7060decd747f5b6bb
23caaa5671f09b8587fc23c52e28ff26
1744e0505a23e6b4c45cd3c8223f4853
8eaf106ae7f64eda68eeb446bb711e9c
1d6022b250fac20191c2f3fefd885264
b51bb8a391877d95b7e0aeb14d07caa3
e30a1194493a8d1d923d05837c348ba0

112467d3419f30a06bf0fa1c8931668b
94deaabd06db45094e93a632bca43a59
014eeb6d755925f6ce90a98460a06243
c2875f9ff4f56bb59bbe141ab138477d
bcec4279d95d0b09ebcf4388cb9a4f64
07b7639f8031e08dcffdf7e03ba2327f
7df7ff5e7e62e78df03b834abca045ee
d842e2ea2205e01ec77c1a04e3771424
e6bd58f332c9aabe502e35ccedb38313
86d73add0df21eb9a1d4b9ff8c981358
2acb4545c61845510e82b1a8c26483d1

域名：
dabaitt3[.]com
ii[.]dehfrw[.]com
djhfgr[.]cc
rfjp93sina[.]top

IP 地址：
27.124.47.157
103.204.13.70
172.67.134.193
143.92.35.33