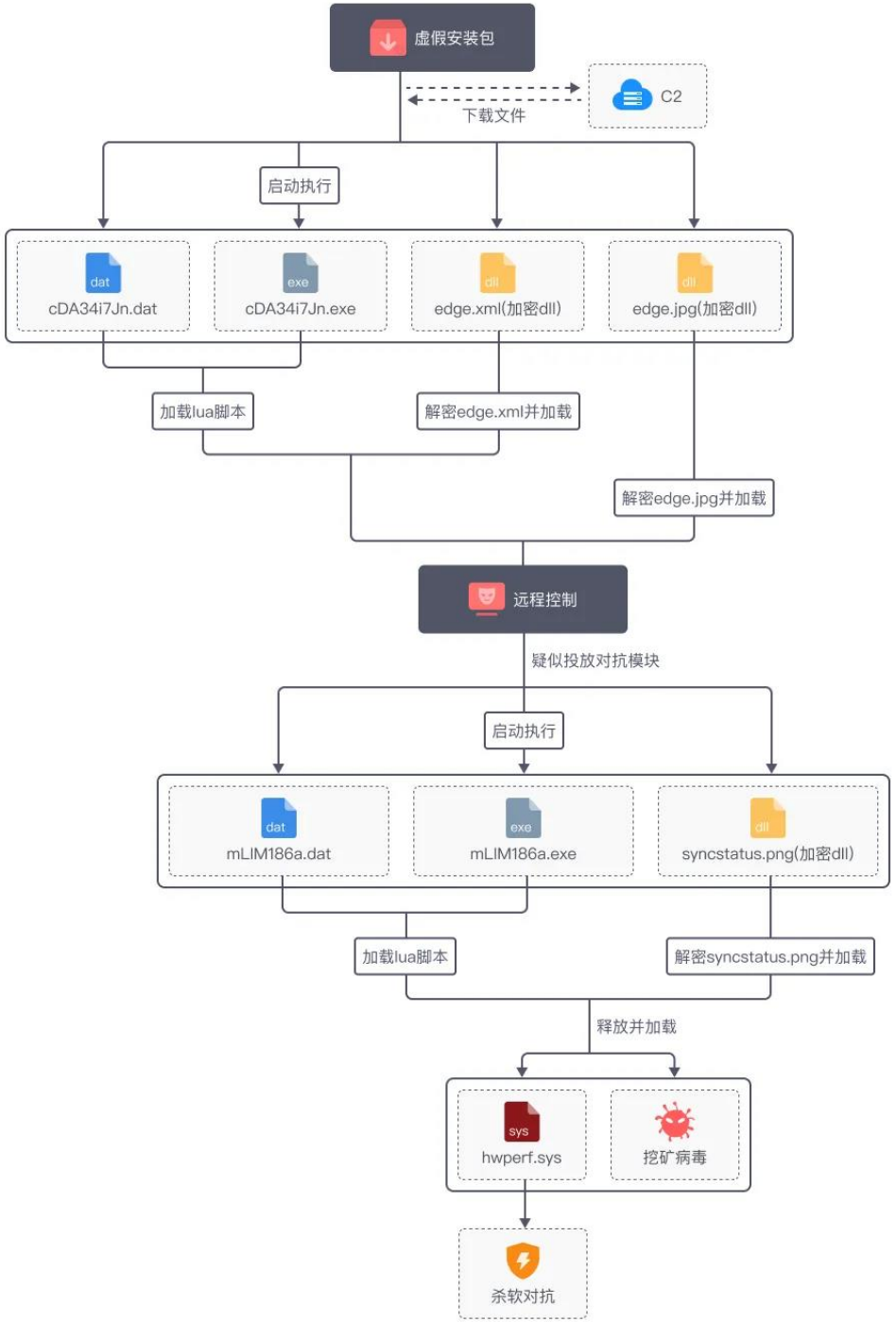
项 目 进 度 汇 报

CONTENTS

目录

PART.01

阶段工作概述

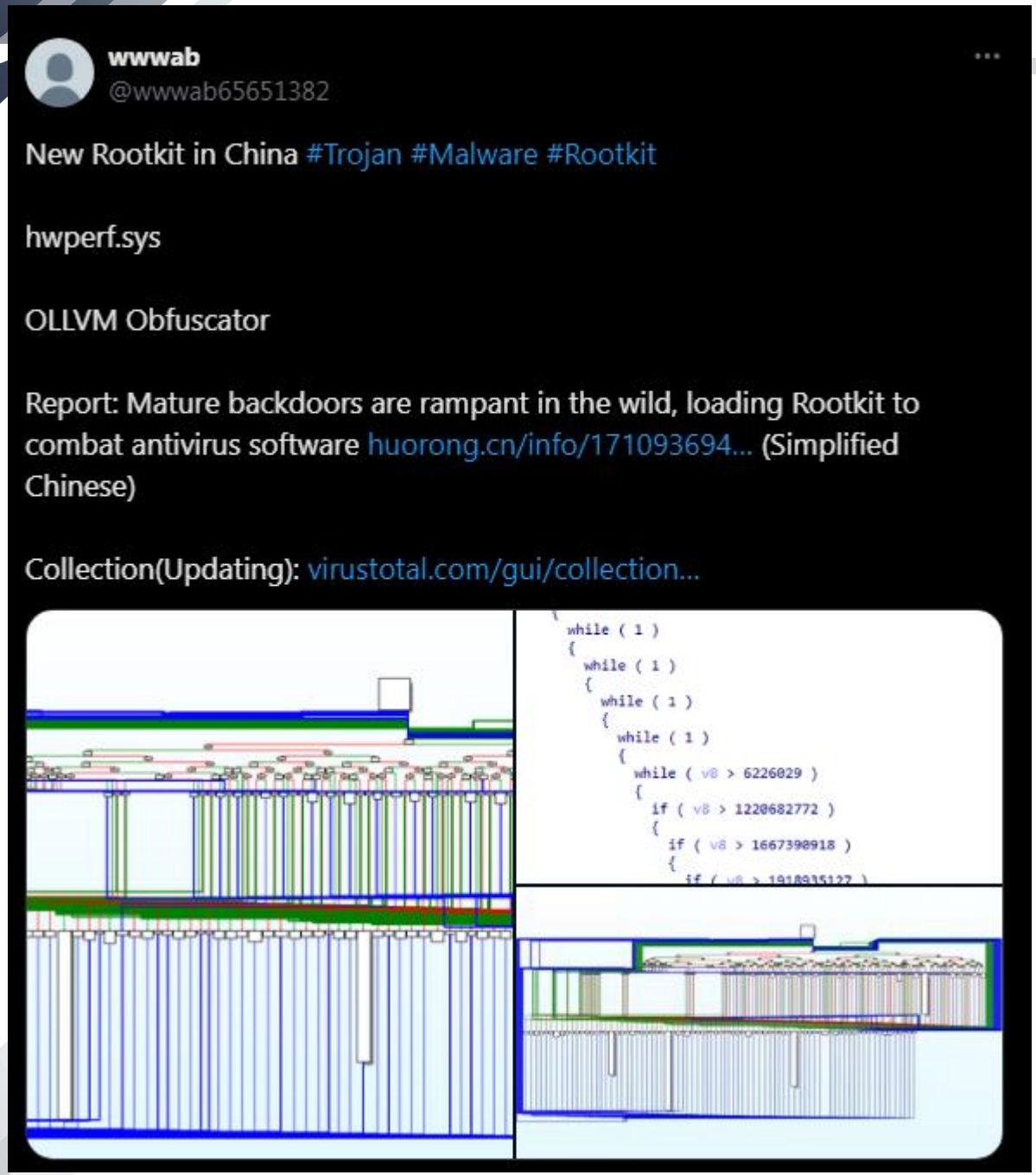


设 工 作 概 述

样 本 概 述

攻击者获得受害者远程连接的权限后，针对性的投放杀软对抗模块。该模块解密出一个驱动程序，该驱动程序反射式再次加载第二个恶意驱动。

作概述



该驱动一共包含10个变体，均使用OLLVM混淆

PART.02

工作完成情况

May I be strenuous, energetic and persevering ! May I be patient! May I be able to bear and forbear the wrongs of others! May I ever keep a promise given!

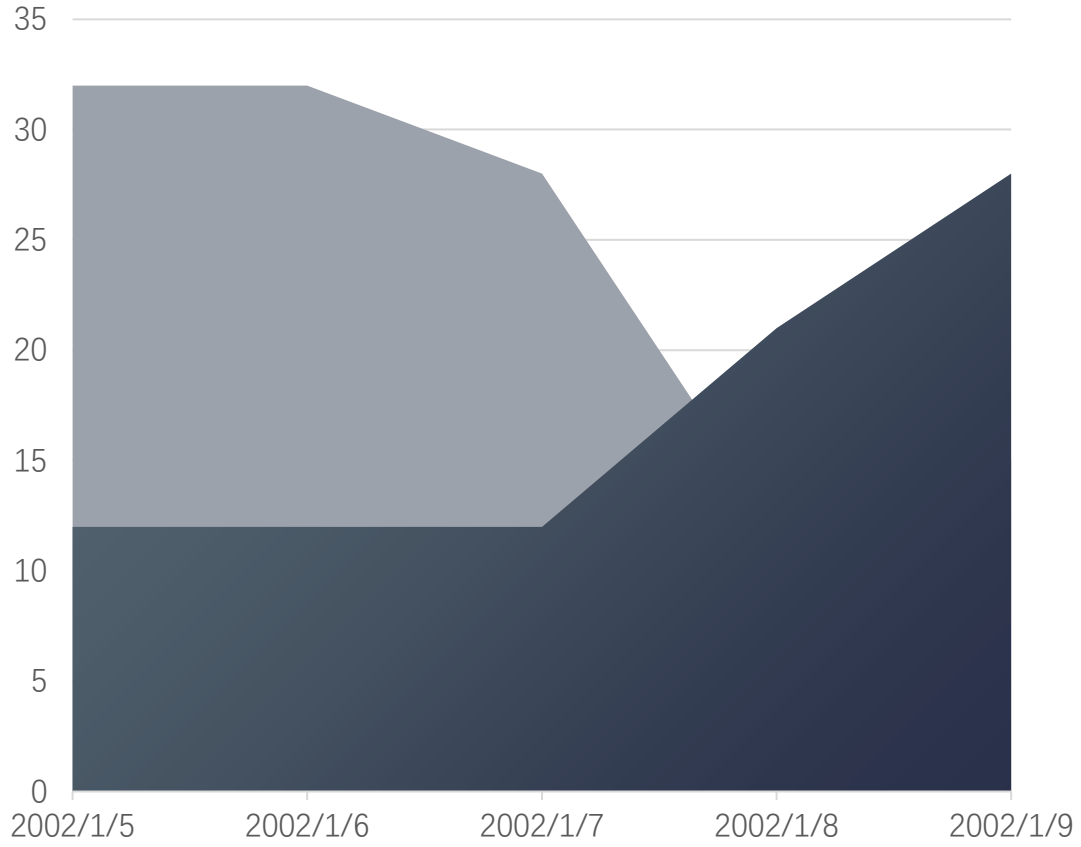
工作完成情况

混淆去除

去除了控制流平坦化

代码分析

解密了所有动态API调用



PART.03

项目成果展示

May I be strenuous, energetic and persevering ! May I be patient! May I be able to bear and forbear the wrongs of others! May I ever keep a promise given!

项目成果展示

```
NTSTATUS __stdcall DriverEntry(PDRIVER_OBJECT DriverObject, PUNICODE_STRING RegistryPath)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  v26 = 1;
  v25 = 1;
  v12 = alloca(16i64);
  v27 = v17;
  v13 = (malloc)(0x1000ui64);
  v24 = v13 != 0;
  P = v13;
  if ( !v13 )
    return 0xC0000001;
  if ( (sub_140001000)(DriverObject->DriverSection, v14) < 0 )
    return 0xC0000001;
  v17[3] = v27;
  *v27 = 0i64;
  if ( sub_140010A93(v27, v11) >= 0 )
  {
    v20 = 0xC0000001;
    v21 = *(*v27 + 2) > 0x1000u;
    v20 = 0xC0000001;
    if ( v21 )
    {
      v3 = (malloc)(0x11ui64);
      v4 = sub_1400215E7(v3);
      *(P + 56) = ~((P ^ 0x713287CF266AA0EAi64 | (v4 & 0x8ECD7830D9955F15ui64 | 0x412084C42200A082i64) ^ v4 & 0x713287CF266AA0EAi64 ^ 0xCFEDFCF4FB95FF97ui64) & ((v4 & 0x8ECD7830D9955F15ui64 | 0x412084C42200A082i64) ^ v4
      v5 = (malloc)(0x11ui64);
      LOBYTE(v6) = -1;
      v7 = memset_0(v5, v6, 16i64);
      v8 = P;
      *(P + 48) = (v7 & 0xE25B6CED3F7193F3ui64 | 0x14049102008C6800i64) ^ v7 & 0x1DA49312C08E6C0Ci64 ^ (P & 0x805A006102110083ui64 | 0x60009082080CCB2Ci64 | P & 0x20100081000105Oi64) ^ (P & 0xE25B6CED3F7193F3ui64 ^ 0x9E
      v9 = ((*v27 + 12) & 0x2D1300F232D1594Ai64 | 0x92885C0CCC0C2235ui64) ^ (*v27 + 12) & 0xD2ECFF0DCD2EA6B5ui64;
      v10 = (sub_14001B443)(
              ((v8 & 0x2D1300F232D1594Ai64 | 0x92CC1C05CC2A06B4ui64) ^ v8 & 0xD2ECFF0DCD2EA6B5ui64 ^ 0xBFDF1CF7FEFB5FFEui64 | v9 ^ 0xBF9B5CFEFEDD7B7Fui64) & (v9 ^ (v8 & 0x2D1300F232D1594Ai64 | 0x92CC1C05CC2A06B4ui64) ^
              *(*v27 + 2));
      v19 = (ReflectLoadPe(v10) >> 31) | 0xF0000000;
      free(*v27);
      v20 = v19;
    }
  }
  else
  {
    v20 = 0xC0000001;
  }
  v18 = v20;
  return v20;
}
```

混淆已经基本去除

PART.04

未来工作计划

May I be strenuous, energetic and persevering ! May I be patient! May I be able to bear and forbear the wrongs of others! May I ever keep a promise given!

未来工作计划

继续分析