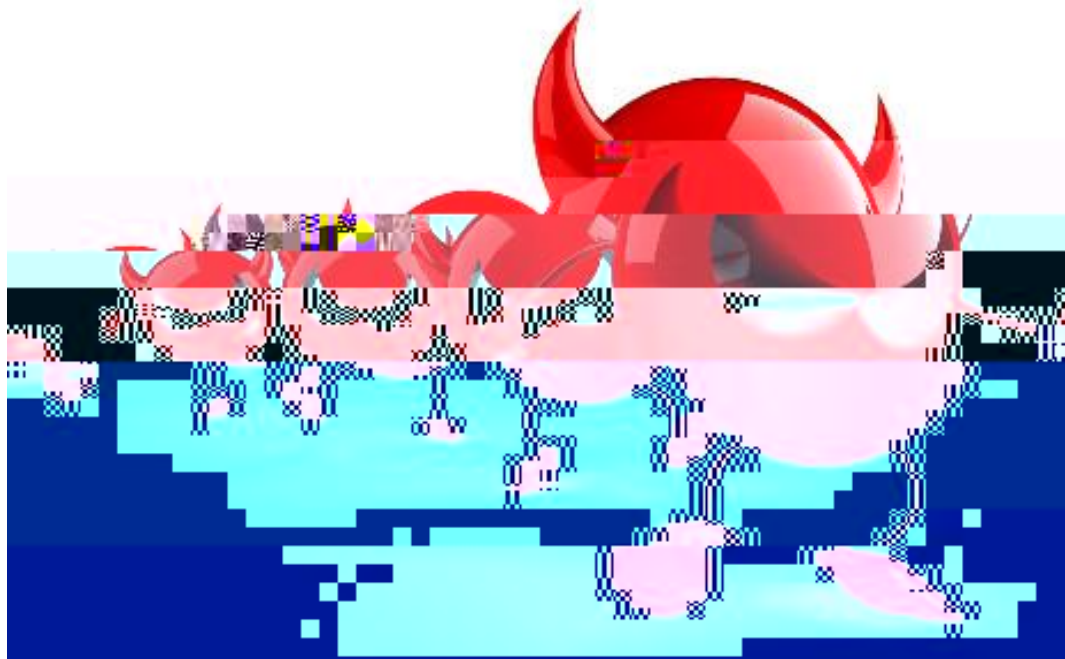


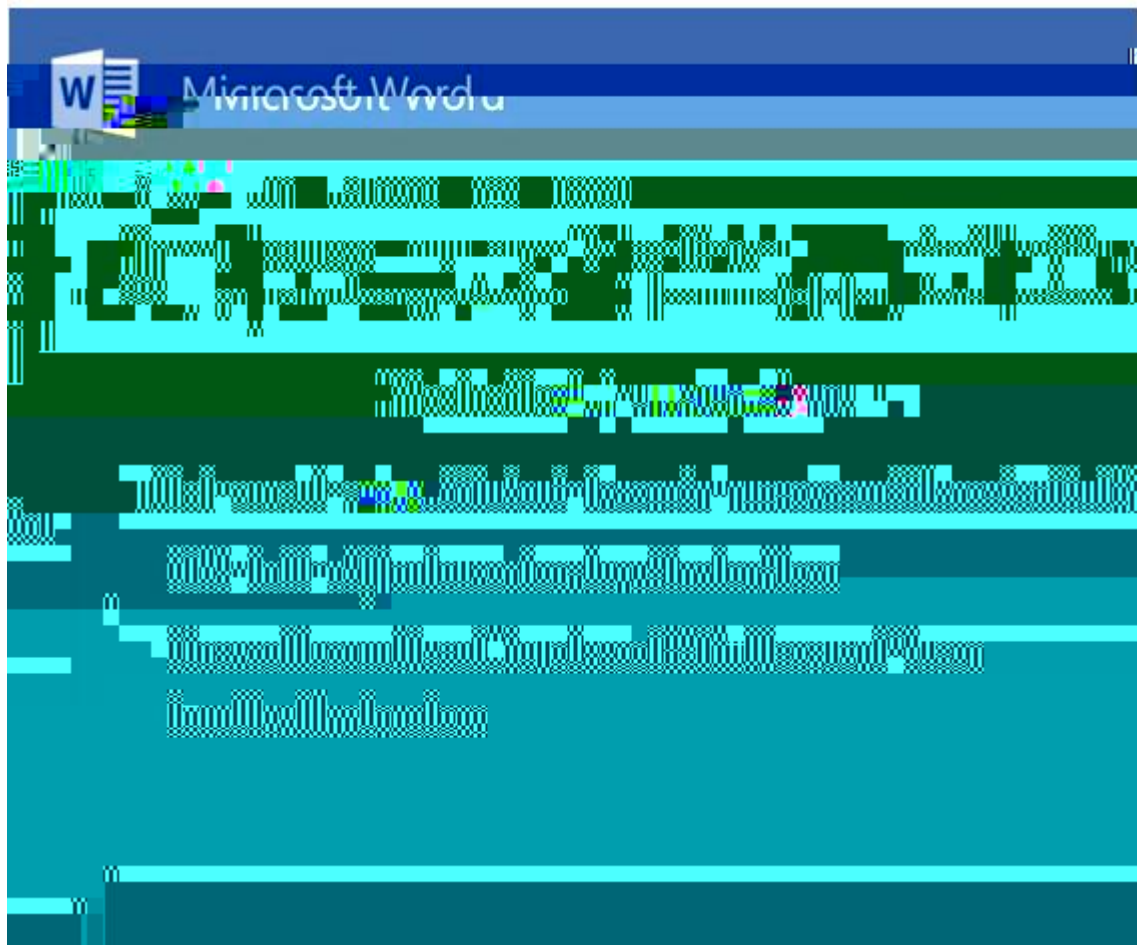


“ ”	4
	4
	4
3.1 0x01.	5
3.2 0x02. Shellcode	10
3.3 0x03. PE dump	12
3.4	14
	16
4.1 APT	16
4.2	16

■

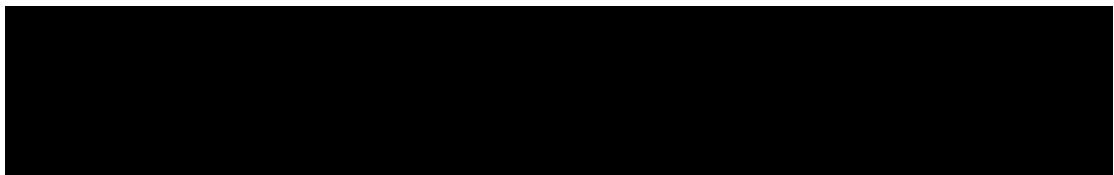
“ ”

■



3.1

3.1 0x01.



3.2

3.3

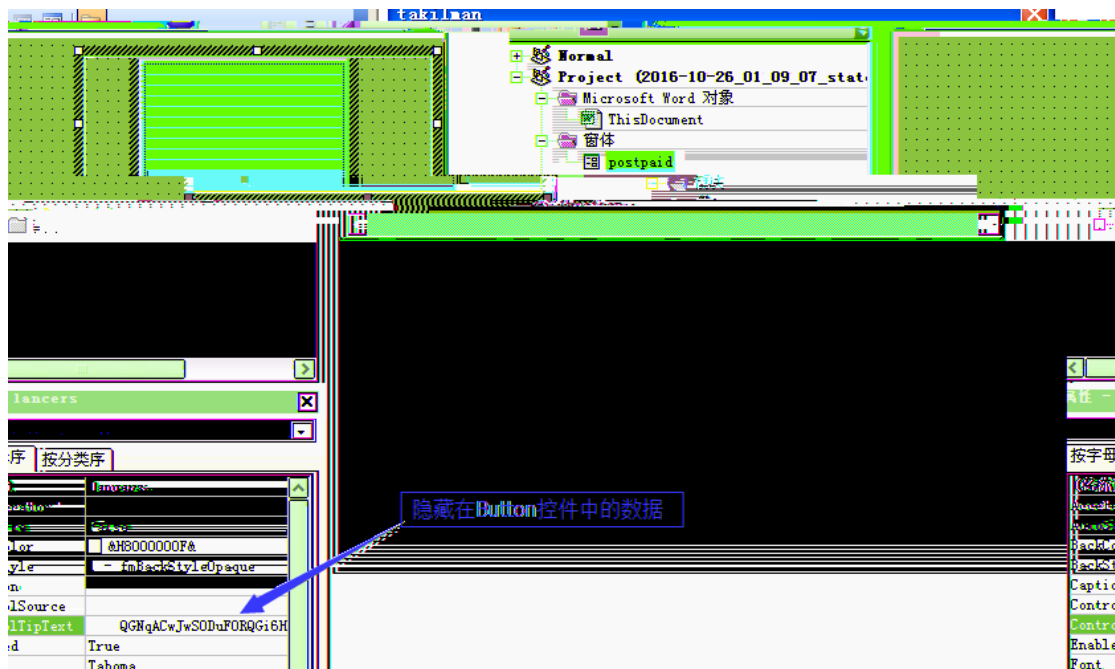
“

”

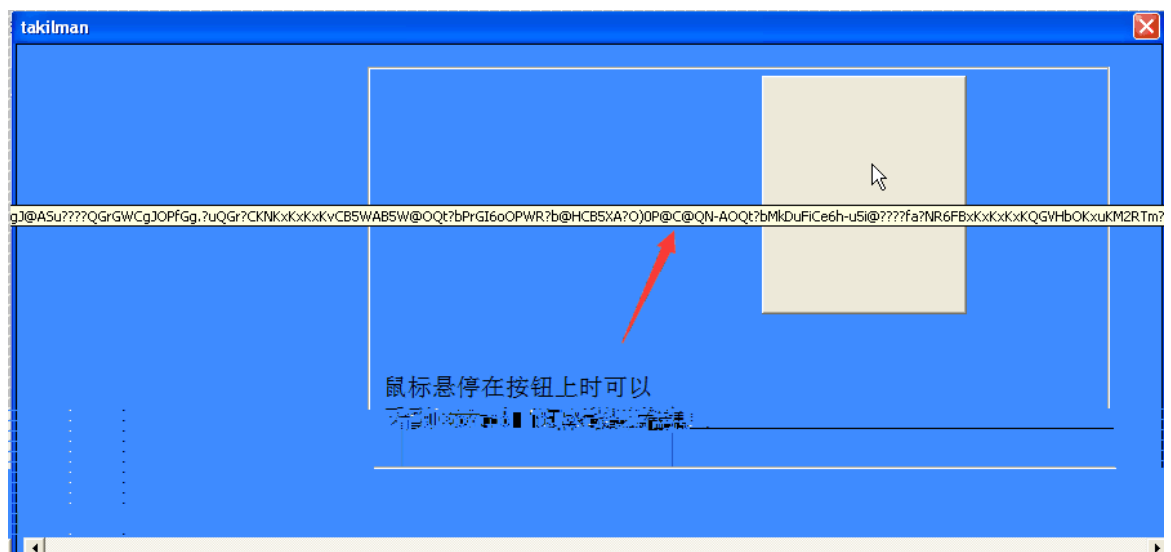
u40on

3.4

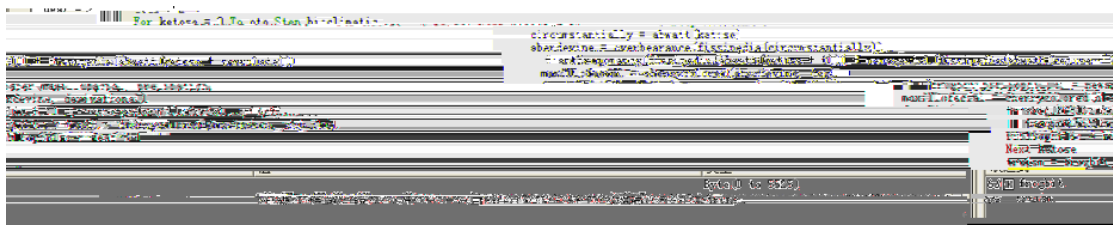
3.5 Toggle Button



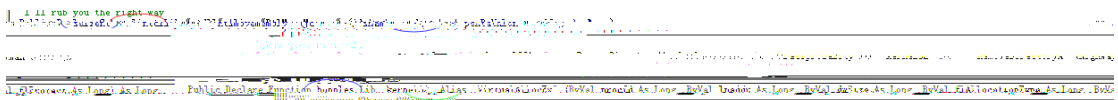
3.6 ControlTipText



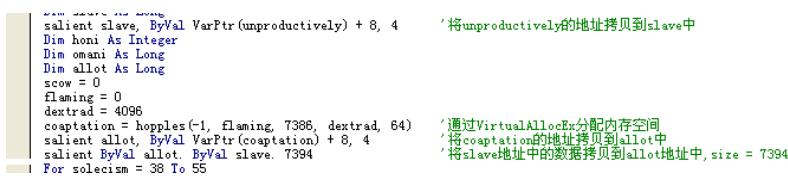
3.7 ControlTipText



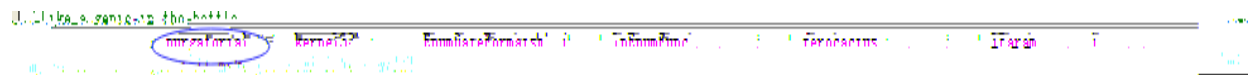
3.8 shellcode



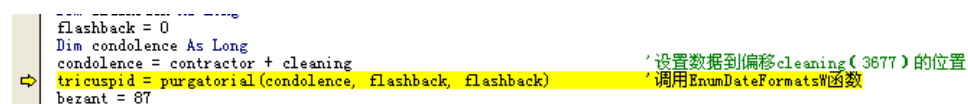
3.9



3.10 RtlMoveMemory



3.11 EnumDateFormats



3.12 EnumDateFormats shellcode

3.13 EnumDateFormats

3.14 EnumDateFormats

3.15 EnumDateFormats

3.2 0x02. Shellcode

3.16 Shellcode

3.17 Shellcode



3.20

3.3 0x03. PE dump

```

{
    int v3; // eax@9

    if ( a1[1] != ':' )
        return 0;
    if ( *a1 == 'b' )
    {
        v3 = sub_401524(a1 + 2);
        goto LABEL_16;
    }
    if ( *a1 == 'c' )
    {
        v3 = sub_401D8E(a1 + 2);
LABEL_16:
        *a2 = v3;
        return 1;
    }
    if ( *a1 == 'e' )
    {
        v3 = sub_4014C8(a1 + 2, 0);
        goto LABEL_16;
    }
    if ( *a1 == 'l' )
    {
        v3 = sub_4014C8(a1 + 2, 1);
        goto LABEL_16;
    }
    if ( *a1 != 'n' )
    {
        if ( *a1 != 'r' )
            return 0;
        v3 = sub_40157B(a1 + 2);
    }
}

```

// 下载注入到svchost执行

// 增加url地址，并写入文件

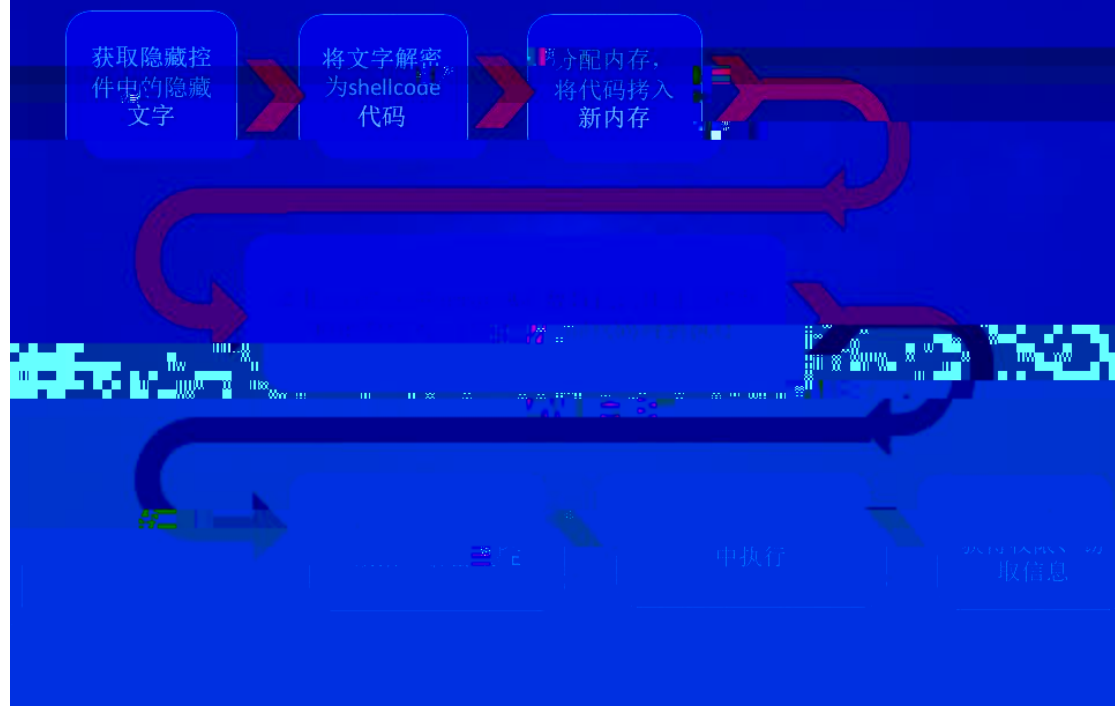
// 下载映射文件，并通过线程执行

// 下载映射文件，直接调用执行

// 下载保存到临时目录执行

a2

宏恶意样本执行流程归纳



APT

3

▪

APT



APT

APT

APT

APT

0-day

APT

5.1

APT

APT

APT

APT

0-day

ROP

API

Shell code

APT

APT



5.2 VenusEye

VenusEye

VenusEye

Hedwig

Locky

18

SandWorm



■

“

”

