

HawkEye

2016 12 23

VenusEye

. 3
. 4
2.1 4
2.2 4
2.3 6
. Ø APT ج 11
ضھ. Ø APT ج 13
Ø APT ج ñ

▪

خى APT ج “ ” ﻫ

HawkEye 12 23 20 فمم

99.9% ﻯ ﺑّ

ﺑّ U

powershell HawkEye keylogger كج

ﺓ 20161031_ “ ” 20161108_ “ ”

ﺃّ “ ” “ ” “ ” U

ضي

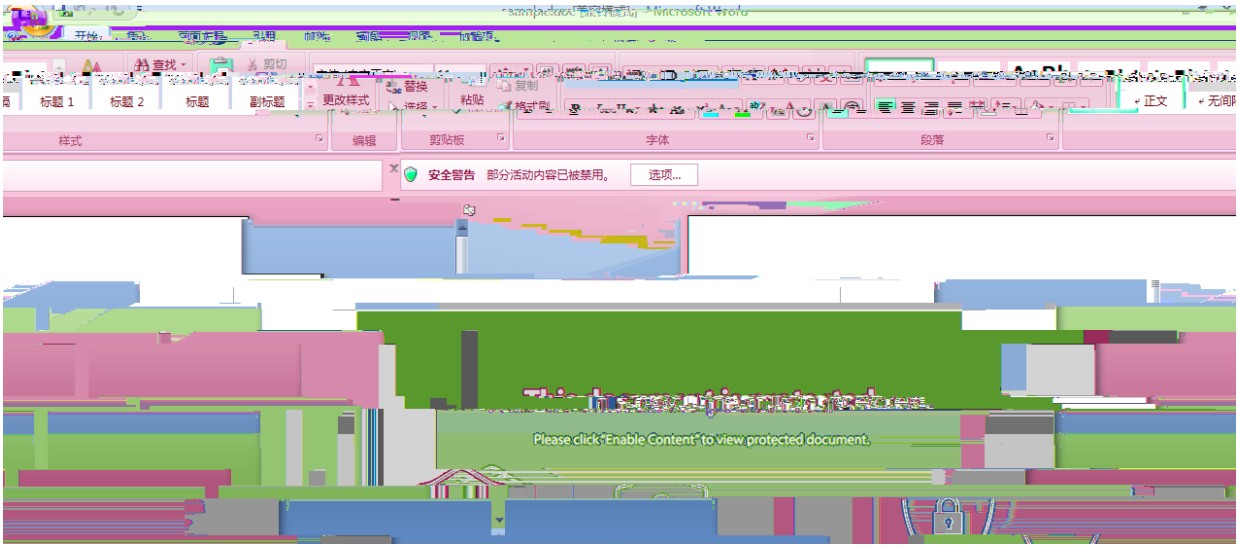
▪

2.1

O

2.2

0x01 Ǖ ⱬ



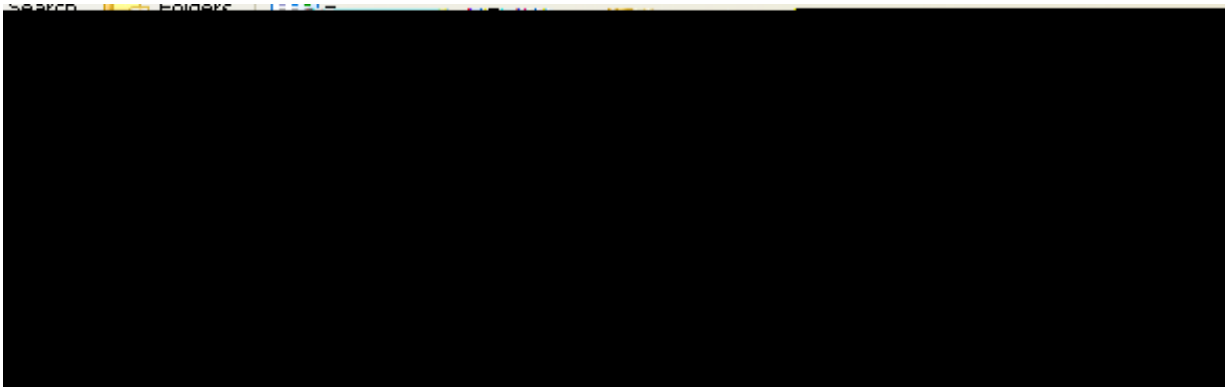
ⱬ 2.1

0x02 Ǖ

يد 2.4

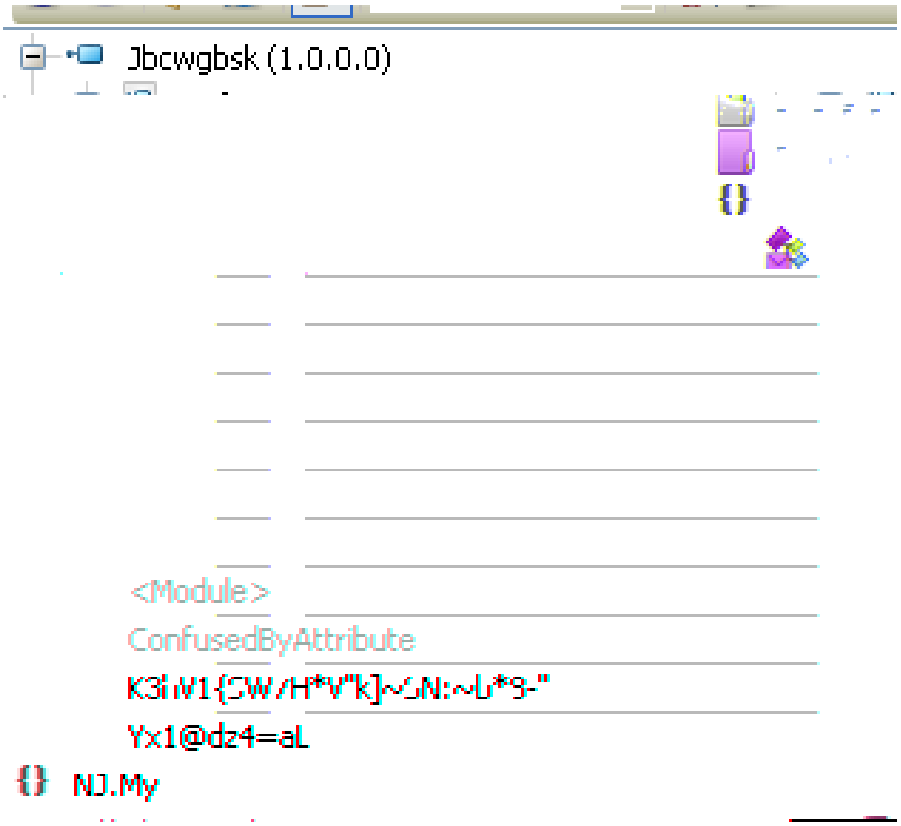
يد 2.5 like ١

0x05 ً U powershell ث U
shell ס



يد 2.7 ا U ً

0x02 ا U Jbcwgbsk.exe



يد 2.8

0x03 Jbcwgbsk.exe Srxoeoaonmsiyy.bin U

ا IE شج

يحـ 2.9

0x04 IE شجـ dump ىّ شجـ



ฆ 2.11

0x06 HawkEye ˜ บ๊ ๙ FTP

ฯ



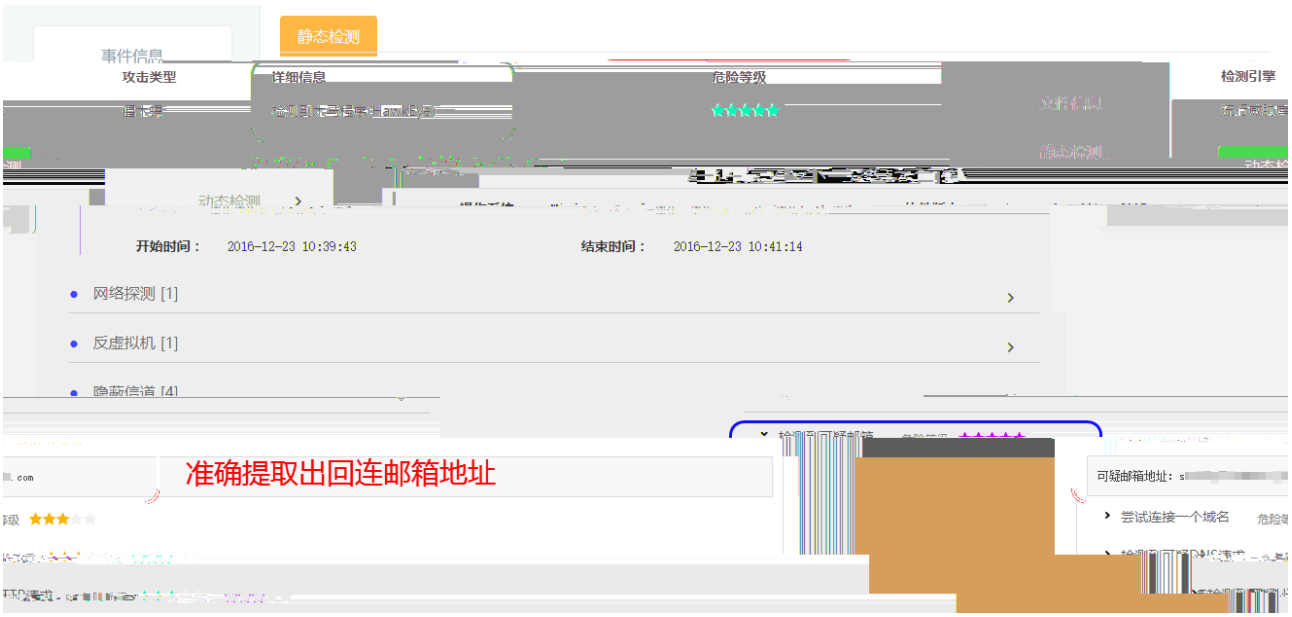
ﺭ 2.12 HawkEye

0x07 ﻲ ﻊ

ﺔ 2.13MCID 3ﻫBC ﻫ1 0 0 1 240.7ﻫEC ﻫ1 0 0 1 286.91 316.35 Tm


提示powershell命令行
准确
PID
进程名
详细信息
PID
进程名
详细信息

ﺯ 3.1 ﺙ


静态检测
事件信息
攻击类型
详细信息
危险等级
检测引擎
动态检测
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]
准确提取出回连邮箱地址
尝试连接一个域名

ﺯ 3.2

APT

APT

H-worm

APT

APT

0-day

APT



VenusEye

VenusEye ڤ Ω ڤ
ج ج
h
ף
ؤ غ

VenusEye ڤ U ŭ
“ ” H-worm
Hedwig ף Locky
ף
18 ؼ
SandWorm ף
ا ף



1. 2016 12