

2016 12



HawkEye

2016 12 23



VenusEye

.		3
.		4
2.1		4
2.2		4
2.3		6
.	APT	11
.	APT	13
	APT ð	

■



APT

“ ”

HawkEye
99.9%

12 23 20

powershell

HawkEye keylogger

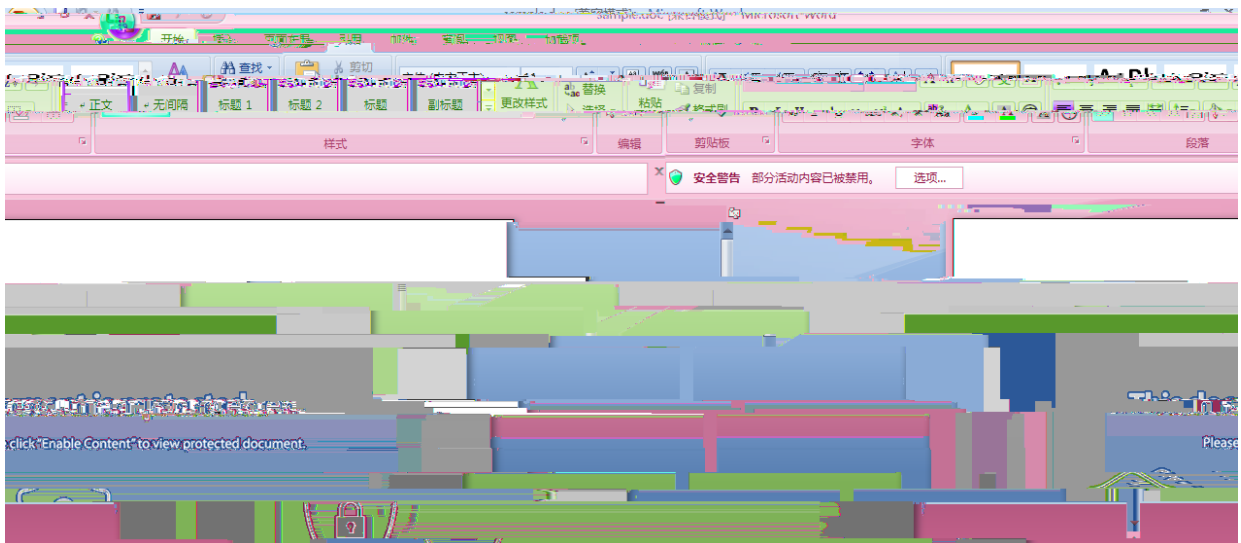
20161031_ “ ”
“ ”

20161108_ “ ”
“ ” “ ”

2.1

2.2

0x01



2.1

0x02

2.4

2.5 like

0x05
shell

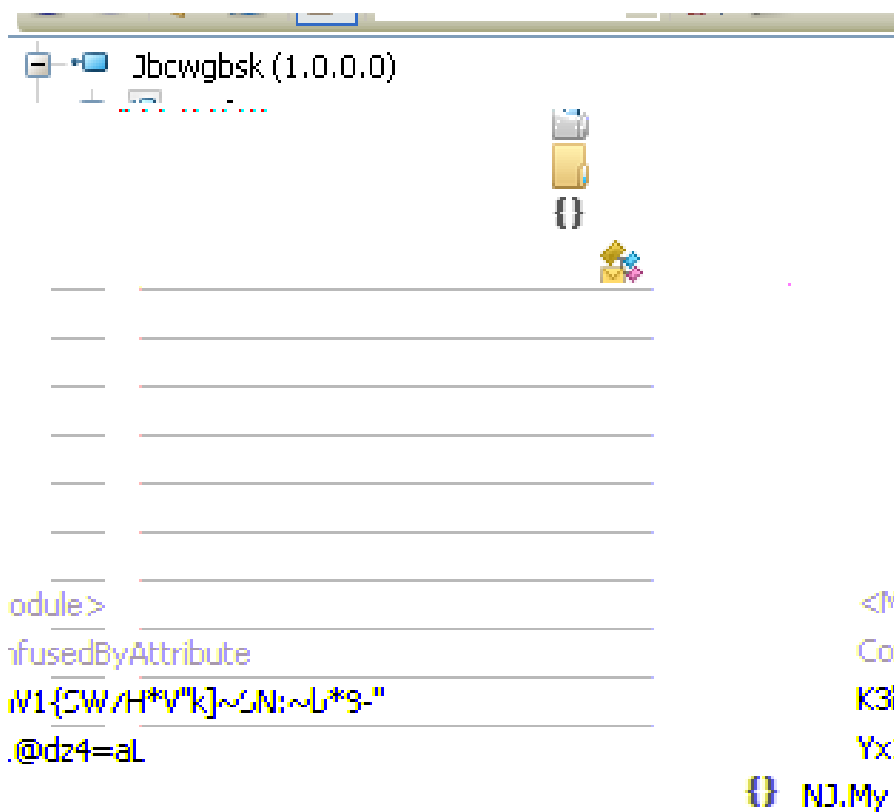
powershell



2.7

0x02

Jbcwgbksk.exe



2.8

0x03 Jbcwgbksk.exe Srxoeoaonmsiyy.bin
IE

2.9

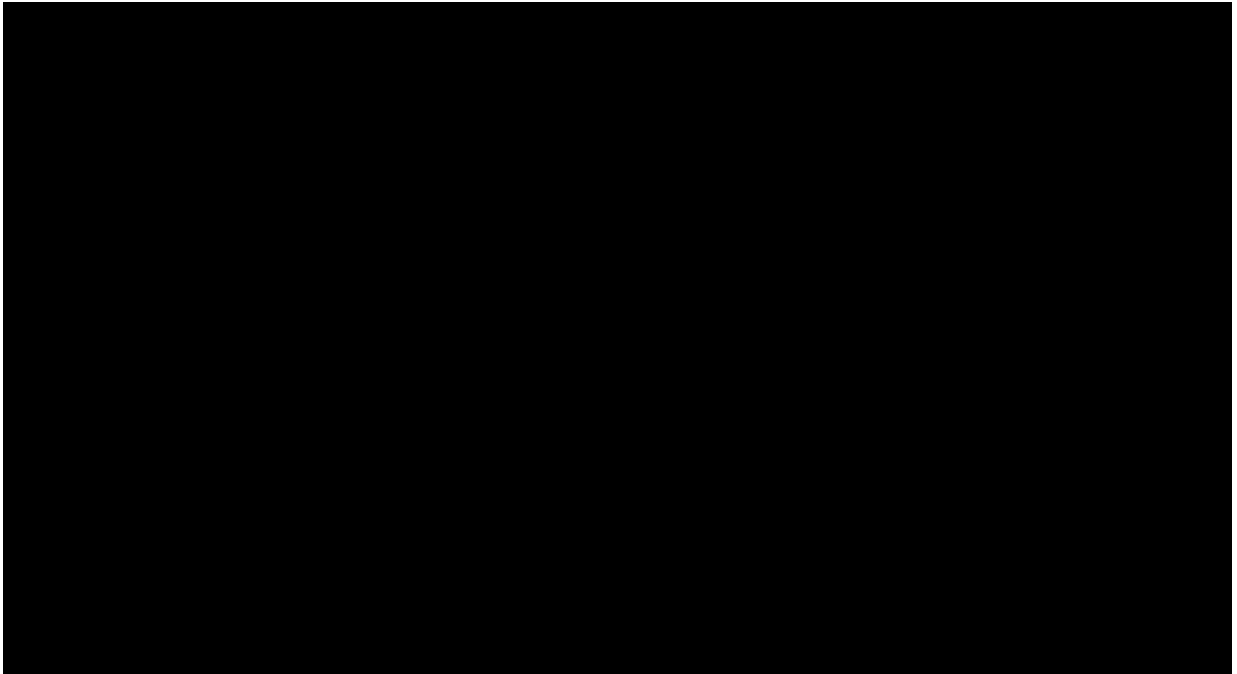
0x04 IE dump



2.11

0x06 HawkEye

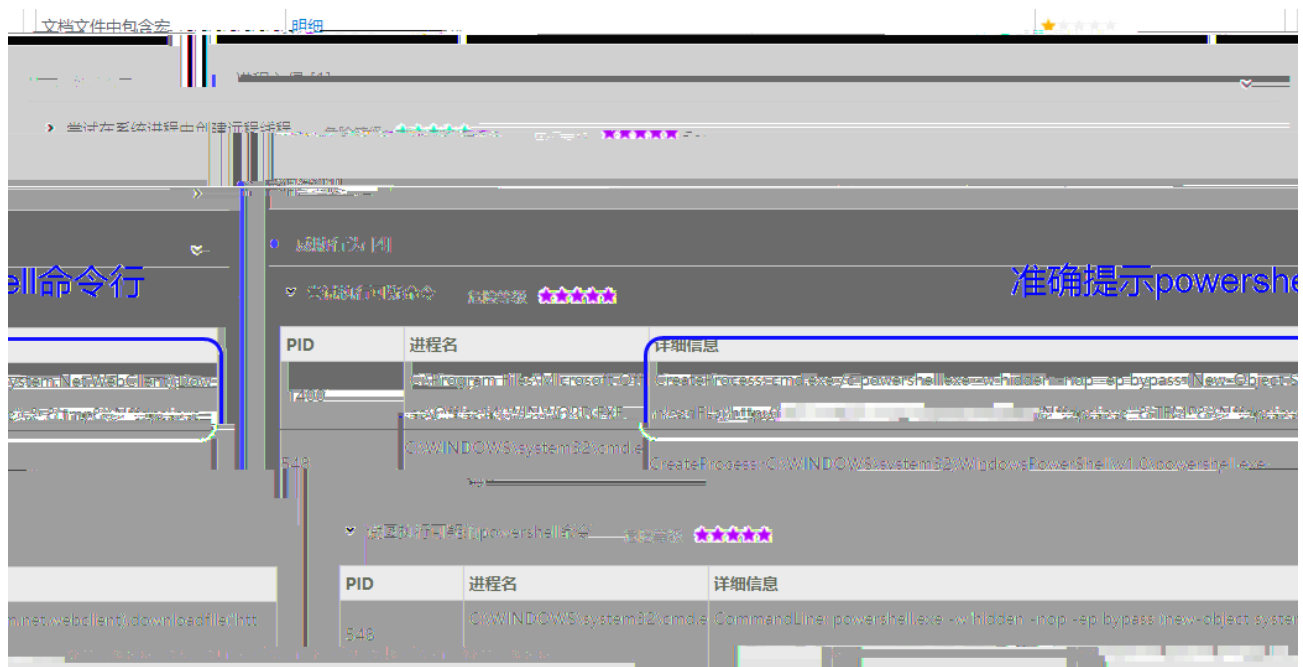
FTP



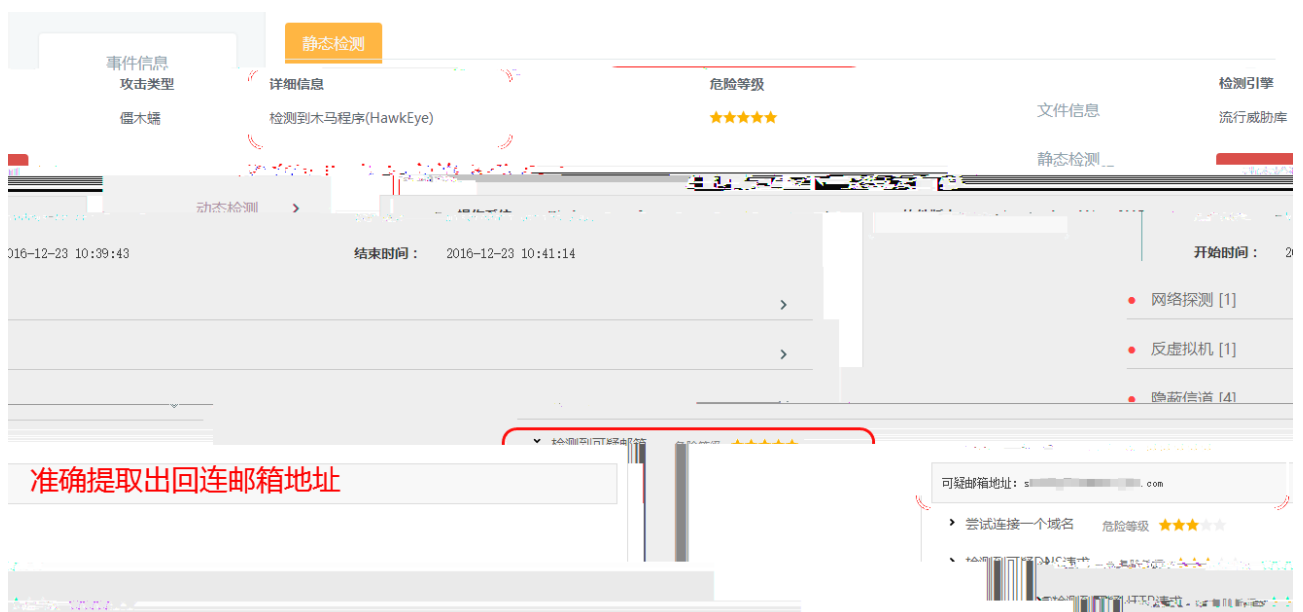
2.12 HawkEye

0x07

2.13MCID 3>DC B1 0 0 1 240.7BEC B1 0 0 1 286.91 316.35 TmP



3.1



3.2

▪

APT



APT

APT

H-worm

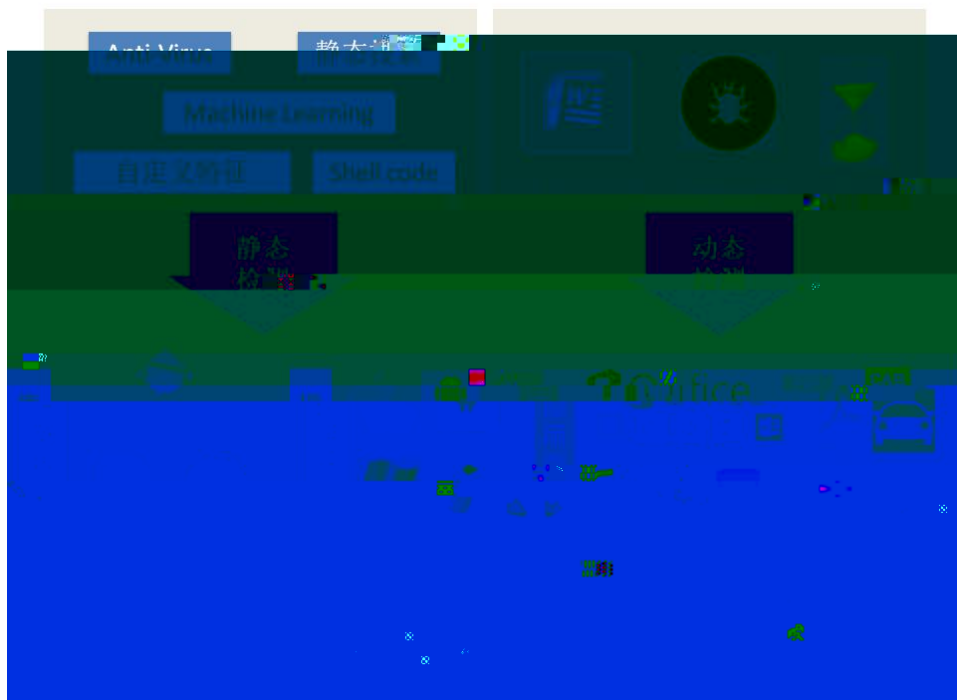
APT

APT

APT

0-day

APT



VenusEye

VenusEye

VenusEye

“ ”

Hedwig

18

SandWorm

H-worm

Locky



■



1. 2016 12