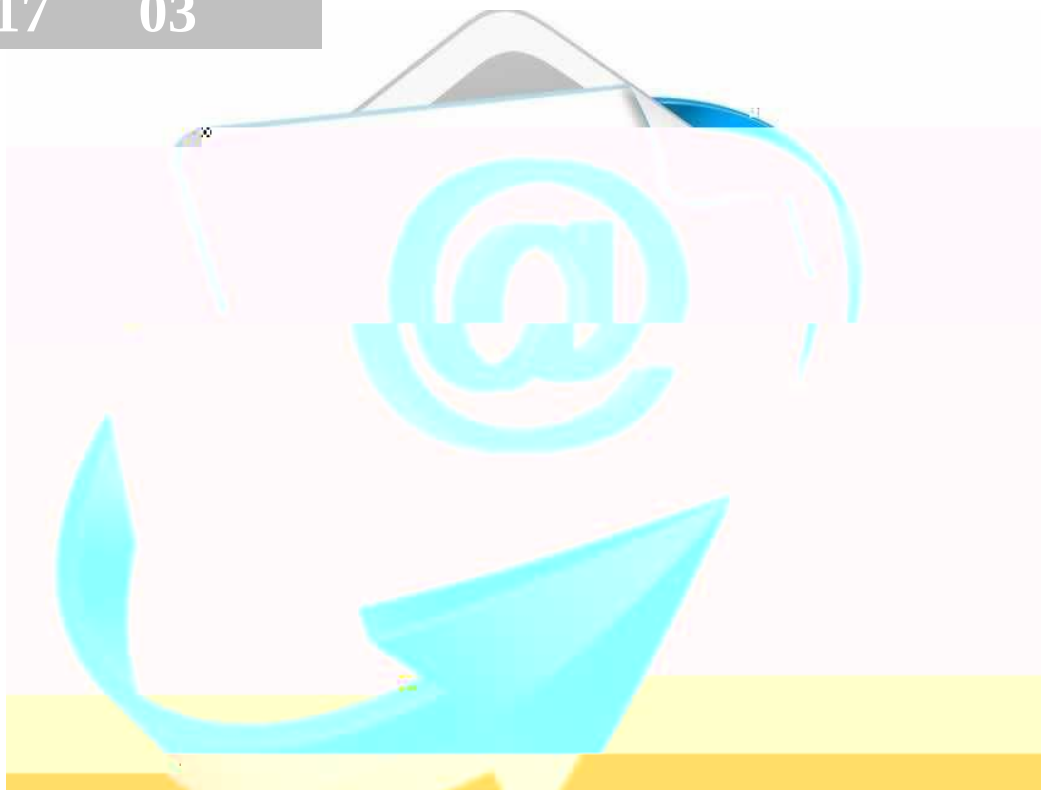


2017 03





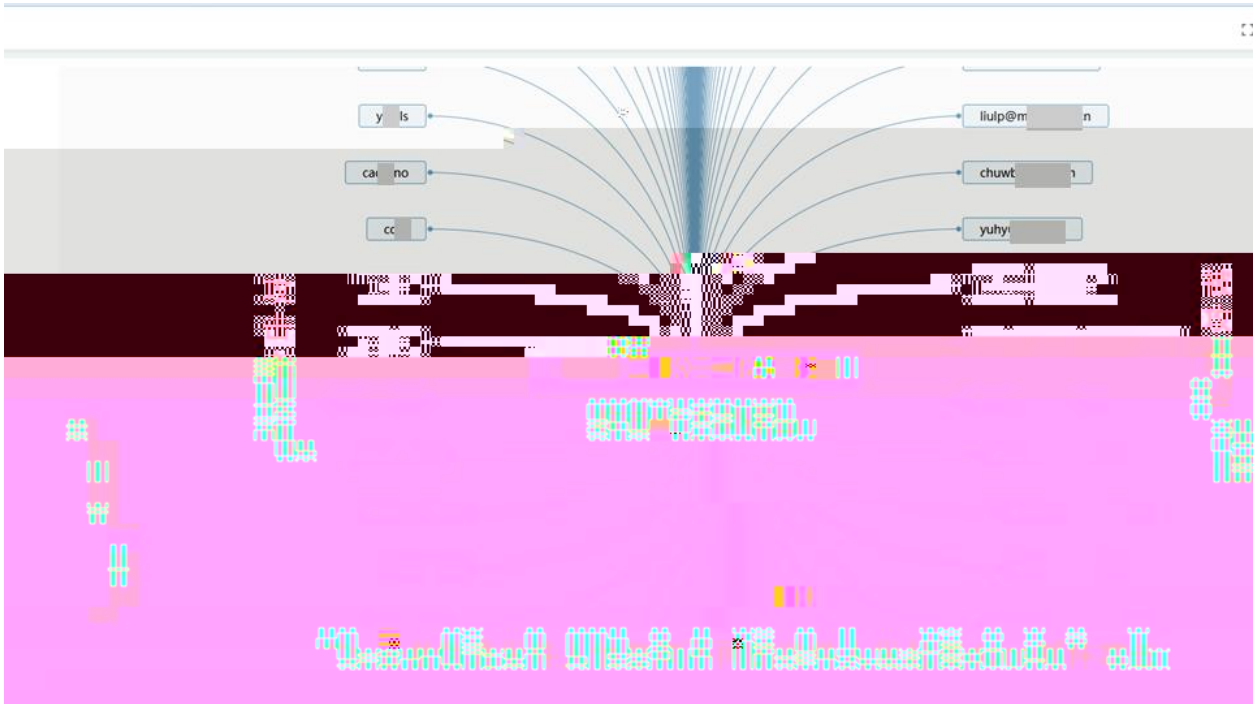
.		3
.	“ ”	4
.		6
3.1		6
3.2		7
3.3		8
.	APT	9
4.1	APT	9
4.2	APT	10



VenusEye

“ ”

DDOS



“ UPS-Delivery ”

JS

VenusEye
Locky

Kovter

Struts2 S2-045

CVE-2017-5638

APT



3.1

“ UPS-Delivery ”

JS

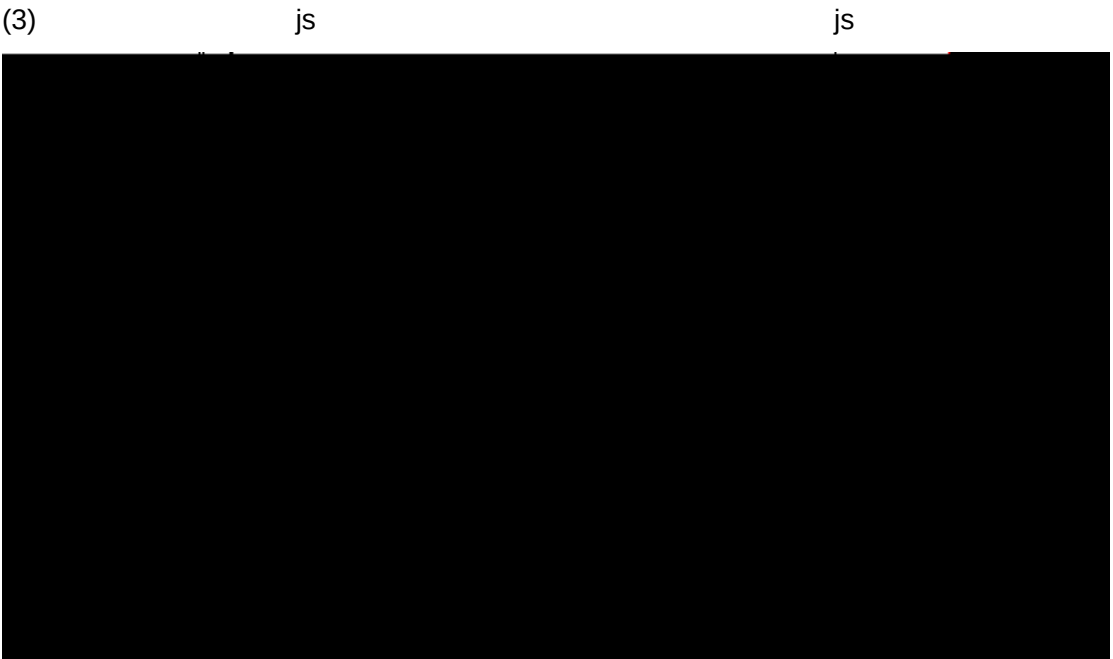
“ ”

(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
```



(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

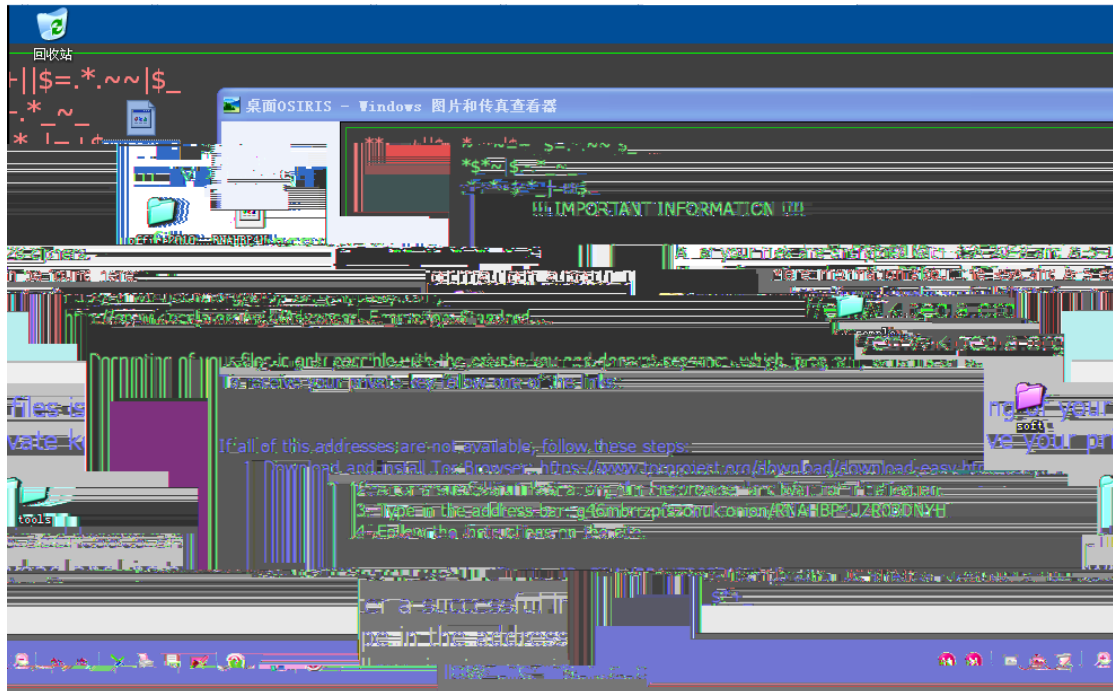
“ ” (Great Ennead)

osiris

Locky

HTTP

AES



APT

4.1 APT

APT

APT

H-worm

APT

APT

APT

0-day

4.2 APT

APT

APT

APT

APT

0-day

Shell code

ROP

API

APT