

BlackOasis APT and new targeted attacks leveraging zero-day exploit

SL securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/



Authors



More information about BlackOasis APT is available to customers of Kaspersky Intelligence Reporting Service. Contact: intelreports@kaspersky.com

Introduction

Kaspersky Lab has always worked closely with vendors to protect users. As soon as we find new vulnerabilities we immediately inform the vendor in a responsible manner and provide all the details required for a fix.

On October 10, 2017, Kaspersky Lab's advanced exploit prevention systems identified a new Adobe Flash zero day exploit used in the wild against our customers. The exploit was delivered through a Microsoft Office document and the final payload was the latest version of FinSpy malware. We have reported the bug to Adobe who assigned it [CVE-2017-11292](#) and [released a patch](#) earlier today:

Vulnerability details

Vulnerability Category	Vulnerability Impact	Severity	CVE Number
Type Confusion	Remote Code Execution	Critical	CVE-2017-11292

Acknowledgments

Adobe would like to thank [Anton Ivanov of Kaspersky Labs](#) for reporting this issue and for working with Adobe to help protect our customers.

So far only one attack has been observed in our customer base, leading us to believe the number of attacks are minimal and highly targeted.

Analysis of the payload allowed us to confidently link this attack to an actor we track as "BlackOasis". We are also highly confident that BlackOasis was also responsible for another zero day exploit (CVE-2017-8759) discovered by [FireEye](#) in September 2017. The FinSpy payload used in the current attacks (CVE-2017-11292) shares the same command and control (C2) server as the payload used with CVE-2017-8759 uncovered by FireEye.

BlackOasis Background

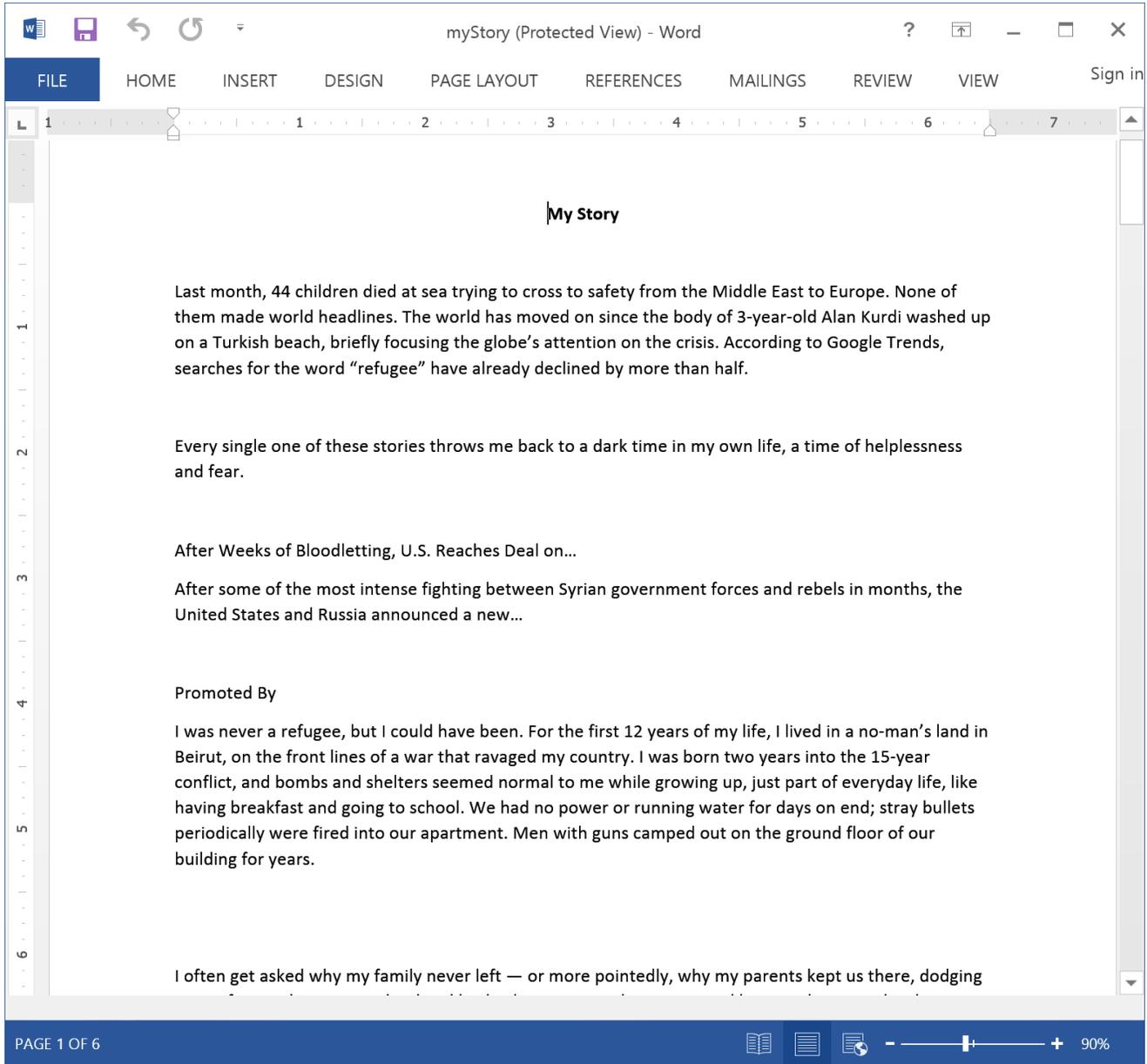
We first became aware of BlackOasis' activities in May 2016, while investigating another Adobe Flash zero day. On May 10, 2016, Adobe [warned](#) of a vulnerability (CVE-2016-4117) affecting Flash Player 21.0.0.226 and earlier versions for Windows, Macintosh, Linux, and Chrome OS. The vulnerability was actively being exploited in the wild.

Kaspersky Lab was able to identify a sample exploiting this vulnerability that was uploaded to a multi scanner system on May 8, 2016. The sample, in the form of an RTF document, exploited CVE-2016-4117 to download and install a program from a remote C&C server. Although the exact payload of the attack was no longer in the C&C, the same server was hosting multiple FinSpy installation packages.

Leveraging data from Kaspersky Security Network, we identified two other similar exploit chains used by BlackOasis in June 2015 which were zero days at the time. Those include CVE-2015-5119 and CVE-2016-0984, which were patched in July 2015 and February 2016

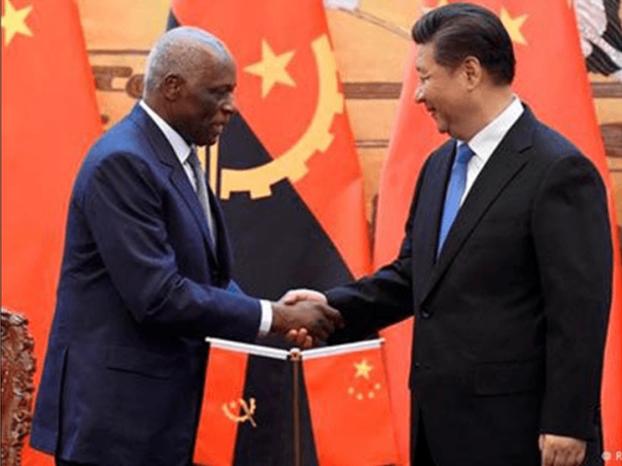
respectively. These exploit chains also delivered FinSpy installation packages.

Since the discovery of BlackOasis' exploitation network, we've been tracking this threat actor with the purpose of better understanding their operations and targeting and have seen a couple dozen new attacks. Some lure documents used in these attacks are shown below:



FILE TOOLS VIEW relatorio (Protected View) - Word

Relatório Secreto Sobre a Visita do Presidente JES a CHINA



Através da imprensa estatal, Angola assistiu, na última semana a visita do presidente da República a República Popular da China.

Esta visita teve como objectivo principal, de acordo com o que foi tornado público, o reforço as relações bilaterias entre os dois Países,

SCREEN 1 OF 5 140%

Decoy documents used in BlackOasis attacks

To summarize, we have seen BlackOasis utilizing at least five zero days since June 2015:

- CVE-2015-5119 – June 2015
- CVE-2016-0984 – June 2015
- CVE-2016-4117 – May 2016
- CVE-2017-8759 – Sept 2017
- CVE-2017-11292 – Oct 2017

Attacks Leveraging CVE-2017-11292

The attack begins with the delivery of an Office document, presumably in this instance via e-mail. Embedded within the document is an ActiveX object which contains the Flash exploit.

```

./[Content_Types].xml
./_rels
./_rels/.rels
./docProps
./docProps/app.xml
./docProps/core.xml
./word

./word/_rels
./word/_rels/document.xml.rels
./word/_rels/header1.xml.rels
./word/activeX

./word/activeX/_rels
./word/activeX/_rels/activeX1.xml.rels
./word/activeX/activeX1.bin
./word/activeX/activeX1.xml
./word/document.xml
./word/endnotes.xml
./word/fontTable.xml
./word/footnotes.xml
./word/header1.xml
./word/media
./word/media/image1.png
./word/settings.xml
./word/styles.xml
./word/stylesWithEffects.xml
./word/theme
./word/theme/theme1.xml
./word/webSettings.xml

```

```

0000C510: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 66 55      fU
0000C520: 66 55 03 42-00 00 46 57-53 20 03 42-00 00 48 01      fU♥B FWS ♥B H0
0000C530: B8 00 64 00-00 1E 01 00-44 11 19 00-00 00 7F 13      ı d ▲@ D↵ ∆!!
0000C540: CB 01 00 00-3C 72 64 66-3A 52 44 46-20 78 6D 6C      ı@ <rdf:RDF xml
0000C550: 6E 73 3A 72-64 66 3D 27-68 74 74 70-3A 2F 2F 77      ns:rdf='http://w
0000C560: 77 77 2E 77-33 2E 6F 72-67 2F 31 39-39 39 2F 30      ww.w3.org/1999/0
0000C570: 32 2F 32 32-2D 72 64 66-2D 73 79 6E-74 61 78 2D      2/22-rdf-syntax-
0000C580: 6E 73 23 27-3E 3C 72 64-66 3A 44 65-73 63 72 69      ns# '><rdf:Descri
0000C590: 70 74 69 6F-6E 20 72 64-66 3A 61 62-6F 75 74 3D      ption rdf:about=
0000C5A0: 27 27 20 78-6D 6C 6E 73-3A 64 63 3D-27 68 74 74      ' xmlns:dc='htt
0000C5B0: 70 3A 2F 2F-70 75 72 6C-2E 6F 72 67-2F 64 63 2F      p://purl.org/dc/
0000C5C0: 65 6C 65 6D-65 6E 74 73-2F 31 2E 31-27 3E 3C 64      elements/1.1'><d
0000C5D0: 63 3A 66 6F-72 6D 61 74-3E 61 70 70-6C 69 63 61      c:format>applica
0000C5E0: 74 69 6F 6E-2F 78 2D 73-68 6F 63 6B-77 61 76 65      tion/x-shockwave
0000C5F0: 2D 66 6C 61-73 68 3C 2F-64 63 3A 66-6F 72 6D 61      -flash</dc:forma
0000C600: 74 3E 3C 64-63 3A 74 69-74 6C 65 3E-41 64 6F 62      t><dc:title>Adob

```

Flash object in the .docx file, stored in uncompressed format

The Flash object contains an ActionScript which is responsible for extracting the exploit using a custom packer seen in other FinSpy exploits.

```

while (i < (len - 4))
{
    if (((ba[i] == 48) && (ba[(i + 1)] == 57)) && (ba[(i + 2)] == 48) && (ba[(i + 3)] == 57))
    {
        ba.position = i;
        while (var4 < var3)
        {
            ba[((i - 1) + var4)] = var2.charAt(var4).charCodeAt(0);
            var4 = (var4 + 1);
        };
        i = 0;
        break;
    };
    i = (i + 1);
};
var5 = new Loader();
var5.loadBytes(ba, new LoaderContext(false, ApplicationDomain.currentDomain));
addChild(var5);

```

Unpacking routine for SWF exploit

The exploit is a memory corruption vulnerability that exists in the “**com.adobe.tv.sdk.mediacore.BufferControlParameters**” class. If the exploit is successful, it will gain arbitrary read / write operations within memory, thus allowing it to execute a second stage shellcode.

The first stage shellcode contains an interesting NOP sled with alternative instructions, which was most likely designed in such a way to avoid detection by antivirus products looking for large NOP blocks inside flash files:

00000000:	9090	nop	
00000002:	91	xchg	ecx,eax
00000003:	91	xchg	ecx,eax
00000004:	9090	nop	
00000006:	91	xchg	ecx,eax
00000007:	91	xchg	ecx,eax
00000008:	9090	nop	
0000000A:	91	xchg	ecx,eax
0000000B:	91	xchg	ecx,eax
0000000C:	9090	nop	
0000000E:	91	xchg	ecx,eax
0000000F:	91	xchg	ecx,eax
00000010:	81E086FFFAF2	and	eax,0F2FAFF86 ; '≥· à'
00000016:	B964010000	mov	ecx,00000164 ; ' @d'
0000001B:	29CC	sub	esp,ecx
0000001D:	33D2	xor	edx,edx
0000001F:	87E7	xchg	edi,esp
00000021:	89FC	mov	esp,edi
00000023:	81E0E1A3D9A3	1and	eax,0A3D9A3E1 ; 'ú ^l úß'

NOP sled composed of 0x90 and 0x91 opcodes

As mentioned earlier, the “mo.exe” payload (MD5: 4a49135d2ecc07085a8b7c5925a36c0a) is the newest version of FinSpy malware, typically sold to nation states and other law enforcement agencies to use in lawful surveillance operations. This newer variant has made it especially difficult for researchers to analyze the malware due to many added anti-analysis techniques, to include a custom packer and virtual machine to execute code.

The PCODE of the virtual machine is packed with the aplib packer.



Part of packed VM PCODE

After unpacking, the PCODE it will look like the following:


```

0d 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1b 06 00 00 31 f1 2e 1c 02 1d 00 00 00 00 00 00 00 00 00 00
0d 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1b 06 00 00 81 c1 41 0d ed 0c 00 00 00 00 00 00 00 00 00 00
0d 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1b 06 00 00 81 e9 0a fa f4 05 00 00 00 00 00 00 00 00 00 00 00
0d 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

VM opcode with length
VM instruction parameter

Example of parsed PCODE

In this example, the “1b” instruction is responsible for executing native code that is specified in parameter field.

Once the payload is successfully executed, it will proceed to copy files to the following locations:

- C:\ProgramData\ManagerApp\AdapterTroubleshooter.exe
- C:\ProgramData\ManagerApp\15b937.cab
- C:\ProgramData\ManagerApp\install.cab
- C:\ProgramData\ManagerApp\msvcr90.dll
- C:\ProgramData\ManagerApp\d3d9.dll

The “AdapterTroubleshooter.exe” file is a legitimate binary which is leveraged to use the famous DLL search order hijacking technique. The “d3d9.dll” file is malicious and is loaded into memory by the legit binary upon execution. Once loaded, the DLL will then inject FinSpy into the Winlogon process.

```

%s%02d%02dUTC%s %s???????*%s %d N/A Audio Recording WebCam Recording Screenshot Rec
Recording Skype File Transfer Recording Changed File Recording Deleted File Recording
Accessed File Recording Forensics Recording VoIP File Recording MouseClicks File Recording
Recording Email File Recording WIFI File Recording RemovableMedia File Recording Passw
C.dat .\%02X.dat gdiplus.dll shell32_.dll shell32.dll firmware.bin Global\Debug.7
l System\CurrentControlSet\Services\s %s\Enum %s\Security %s\Parameters . . \.\%c
nit*.* %s\userenv*.* Software\Microsoft\Windows\CurrentVersion\Run rundll32 \.lnf
ogg .wma .mp3 .wmv .mp4 .ogv .mpeg .mpg .avi .bz2 .arj .rar
peg .jpg .pdf .rtf .otp .odp .ots .ods .ott .odt .xsn .xsf
sm .potx .potm .ppt .ost .one .gsa .grv .gfs .dotx .dotm .docx

```

Part of injected code in winlogon process

The payload calls out to three C2 servers for further control and exfiltration of data. We have observed two of them used in the past with other FinSpy payloads. Most recently one of these C2 servers was used together with CVE-2017-8759 in the attacks reported by FireEye in September 2017. These IPs and other previous samples tie closely to the BlackOasis APT cluster of FinSpy activity.

Targeting and Victims

BlackOasis' interests span a wide gamut of figures involved in Middle Eastern politics and verticals disproportionately relevant to the region. This includes prominent figures in the United Nations, opposition bloggers and activists, and regional news correspondents. During 2016, we observed a heavy interest in Angola, exemplified by lure documents indicating targets with suspected ties to oil, money laundering, and other illicit activities. There is also an interest in international activists and think tanks.

Victims of BlackOasis have been observed in the following countries: Russia, Iraq, Afghanistan, Nigeria, Libya, Jordan, Tunisia, Saudi Arabia, Iran, Netherlands, Bahrain, United Kingdom and Angola.

Conclusions

We estimate that the attack on HackingTeam in mid-2015 left a gap on the market for surveillance tools, which is now being filled by other companies. One of these is FinFisher with their suite of tools.

We believe the number of attacks relying on FinFisher software, supported by zero day exploits such as the ones described here will continue to grow.

What does it mean for everyone and how to defend against such attacks, including zero-day exploits?

For CVE-2017-11292 and other similar vulnerabilities, one can use [the killbit](#) for Flash within their organizations to disable it in any applications that respect it. Unfortunately, doing this system-wide is not easily done, as Flash objects can be loaded in applications that potentially do not follow the killbit. Additionally, this may break any other necessary resources that rely on Flash and of course, it will not protect against exploits for other third party software.

Deploying a multi-layered approach including access policies, anti-virus, network monitoring and allowlisting can help ensure customers are protected against threats such as this. Users of Kaspersky products are protected as well against this threat by one of the following detections:

- PDM:Exploit.Win32.Generic
- HEUR:Exploit.SWF.Generic
- HEUR:Exploit.MSOffice.Generic

More information about BlackOasis APT is available to customers of Kaspersky Intelligence Reporting Service. Contact: intelreports@kaspersky.com

Acknowledgements

We would like to thank the Adobe Product Security Incident Response Team (PSIRT) for working with us to identify and patch this vulnerability.

References

1. Adobe Bulletin <https://helpx.adobe.com/security/products/flash-player/apsb17-32.html>

Indicators of compromise

4a49135d2ecc07085a8b7c5925a36c0a
89.45.67[.]107

- [Adobe](#)
- [APT](#)
- [DLL hijacking](#)
- [Microsoft Word](#)
- [Vulnerabilities and exploits](#)
- [Zero-day vulnerabilities](#)

Authors



BlackOasis APT and new targeted attacks leveraging zero-day exploit

Your email address will not be published. Required fields are marked *