باسمه‌تعالی

BlackOasis؛ اجرای حملات جدید و هدفمند با استفاده از کدهای سوءاستفاده روز صفر

مقدمه

به گزارش وبگاه SecureList[1]، آزمایشگاه کسپرسکی در تاریخ ۱۰ اکتبر ۲۰۱۷ متوجه فعالیت گسترده آسیب‌پذیری روز صفر جدیدی در نرم‌افزار Adobe Flash شد. پس از اعلام آسیب‌پذیری به شرکت Adobe، شماره CVE-2017-11292 بدان اختصاص یافت و همزمان با انتشار وصله، کسپرسکی گزارشی درخصوص آن منتشر نمود.

در حمله ذکر شده، این آسیب‌پذیری از طریق مستندات مایکروسافت آفیس مورد سوءاستفاده قرار گرفته و از آخرین نسخه از بدافزار FinSpy به عنوان payload استفاده شده است. به گزارش SecurityWeek[2]، این بدافزار توسط گروه جاسوسی BlackOasis شامل تعدادی هکران روسی به نام‌های مستعار خرس فانتزی، پاون استورم، استرانیوم، سوفیسی، سدنیت و گروه تزار تولید شده و به نظر می‌رسد که هدف اصلی آن‌ها، نهادهای دولتی و سازمان‌های فعال در حوزه هوافضا بوده است.

با این‌که آسیب‌پذیری CVE-2017-11292 تمامی سیستم‌عامل‌های ویندوز، لینوکس و مک را تحت تاثیر قرار می‌دهد ولی ظاهراً گروه BlackOasis حملات خود را فقط بر روی کاربران سیستم‌عامل ویندوز منحصر نموده است. با سوءاستفاده از این آسیب‌پذیری می‌توان از راه دور اقدام به اجرای کدهای دلخواه نمود.

آزمایش‌های انجام‌شده توسط محققان نشان می‌دهد که این آسیب‌پذیری روی پلتفرم‌های ویندوز ۷ یا ۱۰ با MS.Office 2013 وجود دارد. اما سوءاستفاده از این آسیب‌پذیری در سیستم‌عامل‌های X86-64Bit که به‌روزرسانی Fall Creators ویندوز ۱۰ و MS.Office 2016 را اجرا می‌کنند، موفقیت‌آمیز نیست.

محققان ProofPoint براین باورند که گروه فوق یک گروه امنیتی سایبری پیشرفته وابسته به دولت روسیه است که از آسیب‌پذیری‌های روز صفر برای حملات بالقوه به اهداف حساس سیاسی و نظامی سایر کشورها استفاده می‌کند.

---

[1] https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

[2] http://www.securityweek.com/russian-hackers-exploit-recently-patched-flash-vulnerability

کارشناسان امنیتی شرکت کسپرسکی بر این باورند که BlackOasis از سال ۲۰۱۵ میلادی به بعد، حداقل از پنج آسیب‌پذیری روز صفر زیر استفاده نموده است:

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

نقطه شروع این حمله توسط ارسال یک فایل مایکروسافت آفیس صورت می‌گیرد که حاوی دو فایل ActiveX زیر است که توانایی سوءاستفاده از آسیب‌پذیری Adobe Flash را دارند:

- /ActiveX/ActiveX1.bin
- /ActiveX/ActiveX1.xml

اکنون همانطور که در تصویر زیر دیده می‌شود، چنانچه فایل docx. آلوده از حالت فشرده خارج شود حاوی فایل فلشی می‌باشد که این فلش حاوی ActionScript ای است که وظیفه استخراج کد اکسپلویت را برعهده دارد (با استفاده از packer اختصاصی که در FinSpy مشاهده شده است).

```
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  H☺
0000C530:  B8 00 64 00-00 1E 01 00-44 11 19 00-00 00 7F 13  ╕ d  ▲☺ D◄↓   ⌂!!
0000C540:  CB 01 00 00-3C 72 64 66-3A 52 44 46-20 78 6D 6C  ╦☺  <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
```

اکسپلویت فوق از آسیب‌پذیری مربوط به مدیریت ناصحیح حافظه در کلاس com.adobe.tvsdk.mediacore.BufferControlParameters سوءاستفاده می‌کند و با استفاده از این

آسیب‌پذیری می‌تواند در حافظه اقدام به خواندن و نوشتن دستورات بعدی کند. این امر می‌تواند در مرحله بعدی منجر به اجرای shellcode مجزای دیگری شود. همچنین این Shellcode برای مخفی نمودن خود از دید انواع نرم‌افزارهای ضد بد افزار، از کدهای 0x90 و 0x91 که به خودی خود تغییری در روند اجرای برنامه صورت نمی‌دهند، به‌صورت تصادفی استفاده می‌کند (مانع از تشکیل بلوک‌های NOP بزرگ می‌گردد که حساسیت نرم‌افزارهای ضد بدافزار را تحریک می‌نماید).

```
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 ;'≥· å'
00000016: B964010000    mov         ecx,000000164 ;'  ®d'
0000001B: 29CC          sub         esp,ecx
0000001D: 33D2          xor         edx,edx
0000001F: 87E7          xchg        edi,esp
00000021: 89FC          mov         esp,edi
00000023: 81E0E1A3D9A3  and         eax,0A3D9A3E1 ;'Ù£áß'
```

سپس شل کد دوم از آدرس hzzp://89(.)45.67[.]107/rss/5uzosoff0u.iaf دانلود و اجرا می‌شود. این شل کد سه وظیفه زیر را برعهده دارد:

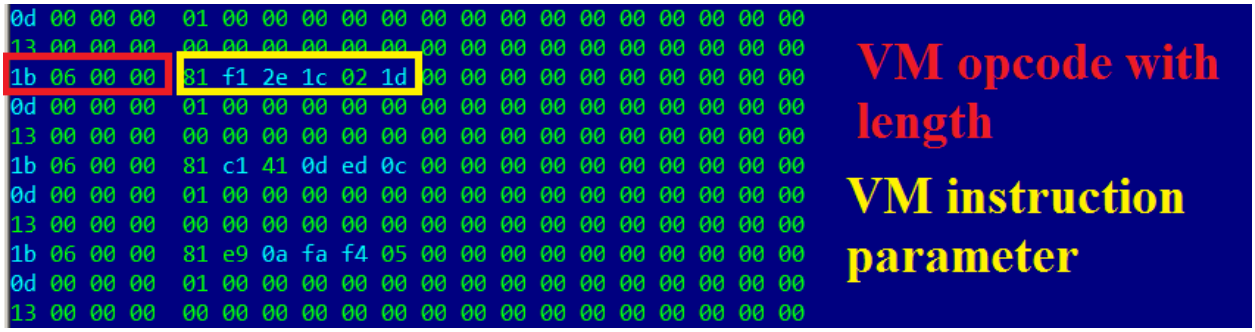
- دانلود FinSpy نهایی از آدرس hzzp://89(.)45.67[.]107/rss/mo.exe
- دانلود مدرک جعلی با IP آدرس جعلی شده قربانی
- اجرای نهایی payload و نمایش مدرک جعلی به قربانی

معرفی نرم‌افزار mo.exe به‌عنوان Payload

این نرم‌افزار با MD5 برابر با 4a49135d2ecc07085a8b7c5925a36c0a به‌عنوان جدیدترین نسخه بدافزار FinSpy Gamma International شناخته می‌شود و به طور معمول به دولت‌ها و سایر سازمان‌های مجری قانون

برای استفاده در عملیات‌های نظارتی و قانونی فروخته می‌شود. تحلیل نسخه جدید به دلیل استفاده از تکنیک‌های مختلف جلوگیری از تحلیل کد و استفاده از packer اختصاصی و ماشین مجازی، بسیار دشوار شده است.

پس از unpack نمودن PCODE مربوط به ماشین مجازی و سپس رمزگشایی آن، امکان تحلیل بدافزار وجود خواهد داشت. در شکل زیر بخشی از کد رمزگشایی شده نمایش داده شده است. در این شکل، دستور "1b" مسئول اجرای کد محلی مشخص شده در فیلد پارامتر می‌باشد.



هنگامی‌که payload با موفقیت اجرا شد، فایل‌های زیر در آدرس‌های زیر کپی می‌شوند:

- 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

توسط فایل اول یعنی AdapterTroubleshooter.exe خواندن اطلاعات از فایل‌های مهم DLL انجام می‌شود و فایل مخرب d3d9.dll پس از اجرای کد قانونی در حافظه مقیم می‌شود و پس از Load در حافظه منجر به تزریق پروسه finspy در winlogon می‌شود. در مرحله بعد با سه سرور کنترل و فرمان ارتباط برقرار می‌نماید. دو عدد از این سرورها پیش‌تر توسط FinSpy مورد استفاده قرار گرفته بود. سرور سوم نیز به‌طور مشترک با آسیب‌پذیری CVE-2017-8759 مورد استفاده قرار گرفته است. شباهت IP ها و نمونه‌های قبلی تحلیل شده، تعلق بدافزار به گروه BlackOasis APT را تقویت می‌کند.

هدف اصلی تیم BlackOasis

به نظر می‌رسد هدف اصلی این تیم گستره وسیعی از چهره‌های درگیر در سیاست‌های خاورمیانه مانند چهره‌های برجسته در سازمان ملل، وبلاگ‌نویسان و مخالفان سیاستمداران و خبرنگاران منطقه‌ای در خاورمیانه می‌باشد. ضمن آنکه درطی سال ۲۰۱۶ دیده شد که این گروه حملات زیادی را در کشور آنگولا نیز داشتند. همچنین نمونه‌هایی از اسناد که نشان‌دهنده اهداف مرتبط با ارتباطات مشکوک به نفت، پولشویی و سایر فعالیت‌های غیرقانونی نیز می‌باشد در خلال حملات مشاهده شده است. ضمن آنکه علاقه به نفوذ در مجامع فعالان و مخالفین بین‌المللی در کشورهای روسیه، عراق، افغانستان، نیجریه، لیبی، اردن، تونس، عربستان سعودی، ایران، هلند، بحرین و انگلیس نیز دیده شده است.

نتیجه‌گیری

شرکت کسپرسکی تخمین زده است که حمله به HackingTeam در اواسط ۲۰۱۵ شکاف بزرگی در بازار ابزارهای نظارتی به وجود آورد که هم‌اکنون توسط شرکت‌های دیگر این شکاف امنیتی پرشده است. یکی از این شرکت‌ها، شرکتی موسوم به Gamma International با مجموعه ابزار FinFisher می‌باشد که البته همین شرکت در سال ۲۰۱۴ توسط Phineas Fisher هک شده است. البته آن رخنه به اندازه آسیب‌پذیری HackingTeam حاد و جدی نبود، ضمن آنکه شرکت گاما طی دو سال سریعاً خود را از وضعیت بحرانی خارج کرد.

برای CVE-2017-11292 و آسیب‌پذیری‌های مشابه می‌توان از killbit در سازمان‌ها جهت غیرفعال کردن برنامه‌های مخرب استفاده نمود ولیکن متاسفانه انجام چنین کاری در سراسر سیستم به راحتی انجام شدنی نیست چون بسیاری از فایل‌های فلش بصورت مستقیم و بدون نظارت killbit در برنامه‌های کاربردی اجرا می‌شوند و تنها استقرار یک رویکرد چند لایه از جمله سیاست‌های دسترسی، ضد ویروس، نظارت برپورت‌های شبکه و لیست سفید می‌توانند اطمینان دهند که مشتریان در برابر این چنین تهدیداتی محافظت می‌شوند.