Microsoft Word Intruder 8 Adds Support for Flash Vulnerability CVE-2016-4117

NOVEMBER 07, 2016 | PROOFPOINT STAFF

Analysis

Microsoft Word Intruder (MWI) is a kit designed for building malicious Microsoft Word documents for use in targeted attacks. The most recent iteration of MWI - Version 8 - supports a wide variety of vulnerabilities that actors can exploit via crafted Microsoft Word documents. Available on underground markets since 2013, we first identified MWI in March 2015 [1]. FireEye [2] and Sophos [3] provided additional documentation of the kit later that year.

In the mid-July 2016, an advertisement for MWI on an underground site stated that this exploit document builder integrated CVE-2016-4117 (Adobe Flash Player up to 21.0.0.213). At the end of August, MWI incremented to version 8, with the message "MICROSOFT WORD INTRUDER 8 (MWI8): CVE-2016-4117 + CVE-2015-2545 + CVE-2015-1641 + CVE-2012-0158" in an advertisement for the new version (see Appendix).

We were able to observe this updated version in the wild dropping various payloads; for example, we saw it dropping RTM Banker on October 21. In this case, the document "business project laveco price.doc.rtf" was delivered via email and targeted at retail, financial, and manufacturing verticals.

R...	Protocol	Requ...	IP	Host	URL	Body	Content-Type	Comments
200	HTTP	GET	82.146.37.202	take5market.com	/2/pict.xsp?id=75382499&bid=67ED6370	95	image/png	MWI 8 Callback
200	HTTP	OPTI...	82.146.37.202	take5market.com	/2/	0	text/html; charset=UTF-8	MWI 8 Callback
200	HTTP	GET	82.146.37.202	take5market.com	/2/pict.xsp?id=75382499&bid=67ED6370	95	image/png	MWI 8 Callback
200	HTTP	GET	82.146.37.202	take5market.com	/2/pict.xsp?id=75382499&act=2	20	text/html; charset=UTF-8	MWI 8 Callback
200	HTTP	POST	188.138.71.117	188.138.71.117	/r/z.php	19	application/octet-stream	RTM Banker Callback
200	HTTP	POST	188.138.71.117	188.138.71.117	/r/z.php	19	application/octet-stream	RTM Banker Callback

Figure 1: Network traffic for MWI and its RTM Banker payload network traffic on October 21

Note that we observed the same instance of RTM fed by Empire Pack (RIG variant [4]) in multiple infection vectors (both compromised sites and malvertising) in multiple countries (the Netherlands, Norway, Germany, Spain, Switzerland, Sweden, Austria, and Ireland).

Another observed MWI document "Изменения условий взаимодействия.doc" (translated from Russian as "Changes of conditions of cooperation.doc") dropped a TeamViewer-based RAT on September 7.

HTTP traffic contains suspicious features which may be indicative of malware related traffic

Performs some HTTP requests

url: http://bibi.pro/mwi/pict.xsp?id=18577543&bid=1C898E35
url: http://bibi.pro/mwi/pict.xsp?id=18577543&act=2

Figure 2: MWI document installing a TeamViewer-based RAT and reporting to C&C

The Adobe Flash Player zero-day CVE-2016-4117 zero-day was discovered by FireEye [5], and was first used by an APT actor named "ScarCruft", as described by Kaspersky [6]. The exploit was later integrated into multiple exploits kits [7].

When we examined the MWI CVE-2016-4117 addition, it appears that this exploit document builder reused the original exploit code without modifying anything except the shellcode. The first Flash file decrypts a second Flash file, which triggers the vulnerability. In fact, the MWI author maintained the same decryption routine and the XOR key for this second file.

```
var _loc3_:ByteArray = new var1();
_loc3_.endian = Endian.LITTLE_ENDIAN;
var _loc4_:int = _loc3_.length - 1;
var _loc5_:* = int(_loc3_[_loc4_]);
if(!_loc5_ || (_loc3_[0] ^ _loc5_) != 70)
{
   return;
}
while(_loc6_ < _loc4_)
{
   _loc3_[_loc6_] = _loc3_[_loc6_] ^ _loc5_;
   _loc6_++;
   _loc5_ = _loc5_ + 17 & 255;
}
_loc6_ = 0;
while(_loc6_ < _loc4_)
{
   if(_loc3_[_loc6_] == 109)
   {
      _loc3_.position = _loc6_;
      if(_loc3_.readUnsignedInt() == 1416521069)
      {
         _loc3_[_loc6_ + 3] = 116;
         _loc6_ = 0;
         break;
      }
   }
   _loc6_++;
}
```

Figure 3: Original sample on the left, MWI exploit integration on the right

This second Flash file appears to be the exact same file from the original exploit, without any modification by the MWI author.

```
var flash90:DeleteRangeTimelineOperation = null;
try
{
   if(!flash79)
   {
      new DeleteRangeTimelineOperation(null);
      flash78 = new Placement();
      new Data6();
      new Data7();
      c0 = new Data4();
      new Data8();
      new Data9();
      if(c0["p" + "la" + "c" + "em" + "en" + "T"])
      {
         flash3("");
      }
   }
```

Figure 4: ActiveScript code triggering the vulnerability

Conclusion

Microsoft Word Intruder is an example of the sort of sophisticated crimeware used to develop attacks on a variety of targets. By incorporating new vulnerabilities in vectors such as Adobe Flash, MWI users increase the likelihood that their malicious documents will successfully infect target devices. This particular vulnerability has also been incorporated in a number of web-based exploit kits, making it imperative that users and organizations who choose to maintain Flash on their systems update to the latest versions.

References

[1] https://threatintel.proofpoint.com/sid/2020700

[2] https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html

[3] https://www.sophos.com/en-us/medialibrary/PDFs/technical[20papers]/sophos-microsoft-word-intruder-revealed.pdf?la=en

[4] http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html

[5] https://www.fireeye.com/blog/threat-research/2016/05/cve-2016-4117-flash-zero-day.html

[6] https://securelist.com/blog/research/75100/operation-daybreak/

[7] http://malware.dontneedcoffee.com/2016/05/cve-2016-4117-flash-up-to-2100213-and.html

Indicators of Compromise (IOCs)

sha256	Comment
a02b009929079af6b3ebe26305765aa469c41f703b3836b170ee16bc6b43223c	MWI8 document "business project laveco price.doc.rtf"dropping RTM Banker
fe41a918e38abe4de2108357c8a7ab87658abf68a457e59473052443038638d9	MWI8 document "Изменения условий взаимодействия.doc" dropping a TeamViewer-based RAT

Domain/IP	Comment
take5market[.]com|82.146.37.202	MWI8 C2
pink.publicvm[.]com|5.45.80.32	MWI8 C2
bibi[.]pro	MWI8 C2
188.138.71.117	RTM C2

Select ET Rules

2022008 || ET TROJAN MWI Maldoc Stats Callout Oct 28

2821723 || ETPRO TROJAN Possible MWI Stage 2 Beacon

2815288 || ETPRO TROJAN RTM Banker CnC M2

2820286 ETPRO WEB_CLIENT Adobe Flash Uncompressed Possible (CVE-2016-4117)

2820272 ETPRO WEB_CLIENT Microsoft Rich Text File download with embedded Flash File Possible (CVE-2016-4117)

Appendix

2016-07-13 - Update to MWI advertisement

эксплойт под уязвимость CVE-2016-4117 (удаленное выполнение кода в Adobe Flash Player) вошел в состав эксплойт-пака MWI. теперь пак атакует сразу несколько векторов:

1) атака на компоненты MS Windows

2) атака на компоненты MS Office

3) атака на сторонние приложения и их компоненты (Adobe Flash Player)

помимо только Remote Code Execution эксплойтов, новый MWI включает в себя модуль для проведения DLL-planting/DLL-hijacking атак. и работают они все в комбинации друг с другом. на первом этапе проводится DLL-planting атака. если подгрузить свою DLL из текущей директории не удалось, то в дело вступает уже целый ряд RCE-эксплойтов.

2016-07-13 - Update to MWI advertisement - English Translation via Google Translate

An exploit for the vulnerability CVE-2016-4117 (remote code execution in Adobe Flash Player) became part of the exploit pack-MWI. Now pack attack multiple vectors:

1) The attack on the components of MS Windows
2) attack on MS Office components
3) attack on third-party applications and their components (Adobe Flash Player)

Besides just Remote Code Execution Exploit new MWI includes a module for DLL-planting / DLL-hijacking attacks. and they all work in combination with each other. on the first stage of a DLL-planting attack. if to load a DLL could not be in the current directory, it comes in has a number of RCE-exploits.

2016-08-31 - MWI8 announced:

MICROSOFT WORD INTRUDER 8 (MWI8): CVE-2016-4117 + CVE-2015-2545 + CVE-2015-1641 + CVE-2012-0158

на данный момент эксплойт-кит содержит следующий набор RCE эксплойтов:

Цитата

CVE-2010-3333 [MS10-087]: RTF pFragments Stack Buffer Overflow

CVE-2012-0158 [MS12-027]: MSComCtlLib.ListView Stack Buffer Overflow

CVE-2013-3906 [MS13-096]: TIFF Heap Overflow via Integer Overflow (heap-spray based)

CVE-2014-1761 [MS14-017]: RTF ListOverrideCount Object Confusion (Memory Corruption)

CVE-2015-1641 [MS15-033]: XML SmartTag Use After Free (heap-spray based)

CVE-2015-2545 [MS15-099]: Microsoft Office Malformed EPS File Vulnerability

CVE-2016-4117 [MS16-064]: Adobe Flash Player Type Confusion Overflow Vulnerability

MWI содержит две основные комбинации эксплойтов:

Цитата

MWI8: CVE-2016-4117 + CVE-2015-2545 + CVE-2015-1641 + CVE-2012-0158

MWI4: CVE-2014-1761 + CVE-2013-3906 + CVE-2012-0158 + CVE-2010-3333 (old)

это единственный эксплойт на рынке, который включает в себя подобную комбинацию эксплойтов. как правило, все эти эксплойты можно встретить только по отдельности. а CVE-2015-2545 вообще выполнен в альтернативном формате (RTF вместо стандартного DOCX), что позволяет ему быть менее детектируемым различными generic сигнатурами.

также MWI8 включает в себя следующие DLL-planting эксплойты:

Цитата

CVE-2016-0041 [MS16-014]: oci.dll

CVE-2015-6132 [MS15-132]: mqrt.dll

CVE-2016-0016 [MS16-007]: mfplat.dll

CVE-2015-6128 [MS15-132]: elsext.dll

CVE-2015-6128 [MS15-132]: spframe.dll

CVE-2016-0018 [MS16-007]: api-ms-win-core-winrt-l1-1-0.dll

CVE-2015-6132 [MS15-132]: wuaext.dll

DLL-planting эксплойты работают в комбинации с RCE-эксплойтами. если DLL-planting эксплойт не сработал и подгрузить ту или иную динамическую библиотеку из текущей директории не удалось, то в дело следом уже в вступают RCE эксплойты.

отныне MWI поддерживает несколько альтернативных методов запуска EXE/DLL файлов, кроме того, добавлена поддержка запуска VBS-скриптов:

Цитата

1) EXE (start process using COM/WMI and kernel32.CreateProcessA)

2) DLL (load library using kernel32.LoadLibraryA from WINWORD.EXE process context)

3) DLL (start rundll32.exe process using COM/WMI and kernel32.WinExec)

4) VBS (start wscript.exe process using COM/WMI and kernel32.WinExec)

кроме того, была добавлена поддержка отображения decoy документа, добавление текста, продвинутый обход safe-mode - все, что нужно для красивой визуальной сработки эксплойта без лишнего шума.

с недавних пор у MWI появился удобный web-интерфейс, позволяющий быстро, удобно и легко собрать эксплойт с необходимой конфигурацией буквально в несколько кликов. больше никакой скучной командной строки и редактирования конфигов. а удобный менеджер билдов поможет вам мониторить AV-ресурсы вроде virustotal.com / malwr.com / hybrid-analysis.com на появление вашего сэмпла в аверских базах. + автоматическая проверка билда антивирусами на ресурсе viruscheckmate.com.

вцелом изменилась концепция работы продукта. мы предоставляем доступ к web-билдеру, который регулярно обновляется, чистится и поддерживается. для получения обновления более не требуется просить выслать новый апдейт. вы можете приобрести как сам исходный код билдера, так и просто доступ к его web-интерфейсу.

ведется работа над новыми эксплойтами и модулями. продукт на самом деле подвергся множеству различных обновлений и модификаций, вскоре распишу все подробнее, обновлю шапку топика, а также приложу скриншоты и видео.

2016-08-31 - MWI8 announced - English translation via Google Translate:

MICROSOFT WORD INTRUDER 8 (MWI8): CVE-2016-4117 + CVE-2015-2545 + CVE-2015-1641 + CVE-2012-0158

Currently exploit kit contains the following set of RCE exploits:

Quote

CVE-2010-3333 [MS10-087]: RTF pFragments Stack Buffer Overflow

CVE-2012-0158 [MS12-027]: MSComCtlLib.ListView Stack Buffer Overflow

CVE-2013-3906 [MS13-096]: TIFF Heap Overflow via Integer Overflow (heap-spray based)

CVE-2014-1761 [MS14-017]: RTF ListOverrideCount Object Confusion (Memory Corruption)

CVE-2015-1641 [MS15-033]: XML SmartTag Use After Free (heap-spray based)

CVE-2015-2545 [MS15-099]: Microsoft Office Malformed EPS File Vulnerability

CVE-2016-4117 [MS16-064]: Adobe Flash Player Type Confusion Overflow Vulnerability

MWI has two main combinations of exploits:

Quote

MWI8: CVE-2016-4117 + CVE-2015-2545 + CVE-2015-1641 + CVE-2012-0158

MWI4: CVE-2014-1761 + CVE-2013-3906 + CVE-2012-0158 + CVE-2010-3333 (old)

This is the only exploit the market, which includes a combination of such exploits. As a rule, all of these exploits can be found only separately. CVE-2015-2545 and is generally performed in an alternate format (RTF instead of the standard DOCX), allowing it to be less detectable by various generic signatures.

MWI8 also includes the following DLL-planting exploits:

Quote

CVE-2016-0041 [MS16-014]: oci.dll

CVE-2015-6132 [MS15-132]: mqrt.dll

CVE-2016-0016 [MS16-007]: mfplat.dll

CVE-2015-6128 [MS15-132]: elsext.dll

CVE-2015-6128 [MS15-132]: spframe.dll

CVE-2016-0018 [MS16-007]: api-ms-win-core-winrt-l1-1-0.dll

CVE-2015-6132 [MS15-132]: wuaext.dll

DLL-planting exploits work in combination with RCE-exploits. if the DLL-planting exploit did not load and load a particular dynamic library from the current directory fails, then the case should have come in RCE exploits.

MWI now supports several alternative EXE / DLL files, startup methods, in addition, added support for launch VBS-scripts:

Quote

1) EXE (start process using COM/WMI and kernel32.CreateProcessA)

2) DLL (load library using kernel32.LoadLibraryA from WINWORD.EXE process context)

3) DLL (start rundll32.exe process using COM/WMI and kernel32.WinExec)

4) VBS (start wscript.exe process using COM/WMI and kernel32.WinExec)

In addition, support has been added to display the decoy document, adding text, bypassing the advanced safe-mode - everything you need for a beautiful visual drawdown exploit without fanfare.

Recently it appeared in MWI convenient web-based interface that enables fast, convenient and easy to collect the necessary configuration to exploit just a few clicks. no more tedious command line and editing config files. and convenient builds Manager helps you monitor AV-kind resources virustotal.com / malwr.com / hybrid-analysis.com the appearance of your sample in averskih bases. + Automatic check antivirus build on the resource viruscheckmate.com.

Product as a whole has changed the concept of work. we provide access to the web-Builder, which is updated regularly cleaned and maintained. to obtain the update is no longer required, please send a new update. You can purchase the source code itself builder and easy access to its web-based interface.

Are working on new exploits and modules. product actually underwent a number of different upgrades and modifications, will soon sign for all the details, update the topic cap and attach screenshots and videos.