Word0Day漏洞CVE20170199攻击实例与检测响应

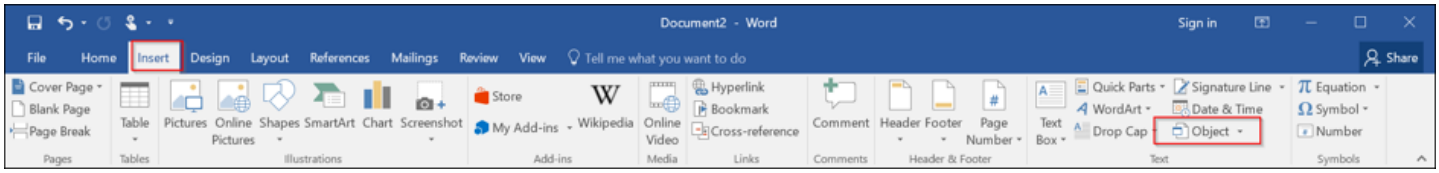
杂术馆 / 2017-04-14 06:21:21 / 浏览数 4775 安全技术 漏洞分析 顶(0) 踩(0)

在通常的攻击场景下，用户收到一个包含恶意代码的Office文件（不限于RTF格式的Word文件，可能为PPT类的其他Office文档），点击尝试打开文件时会从恶意网站下载特
HTA程序执行，从而使攻击者获取控制。

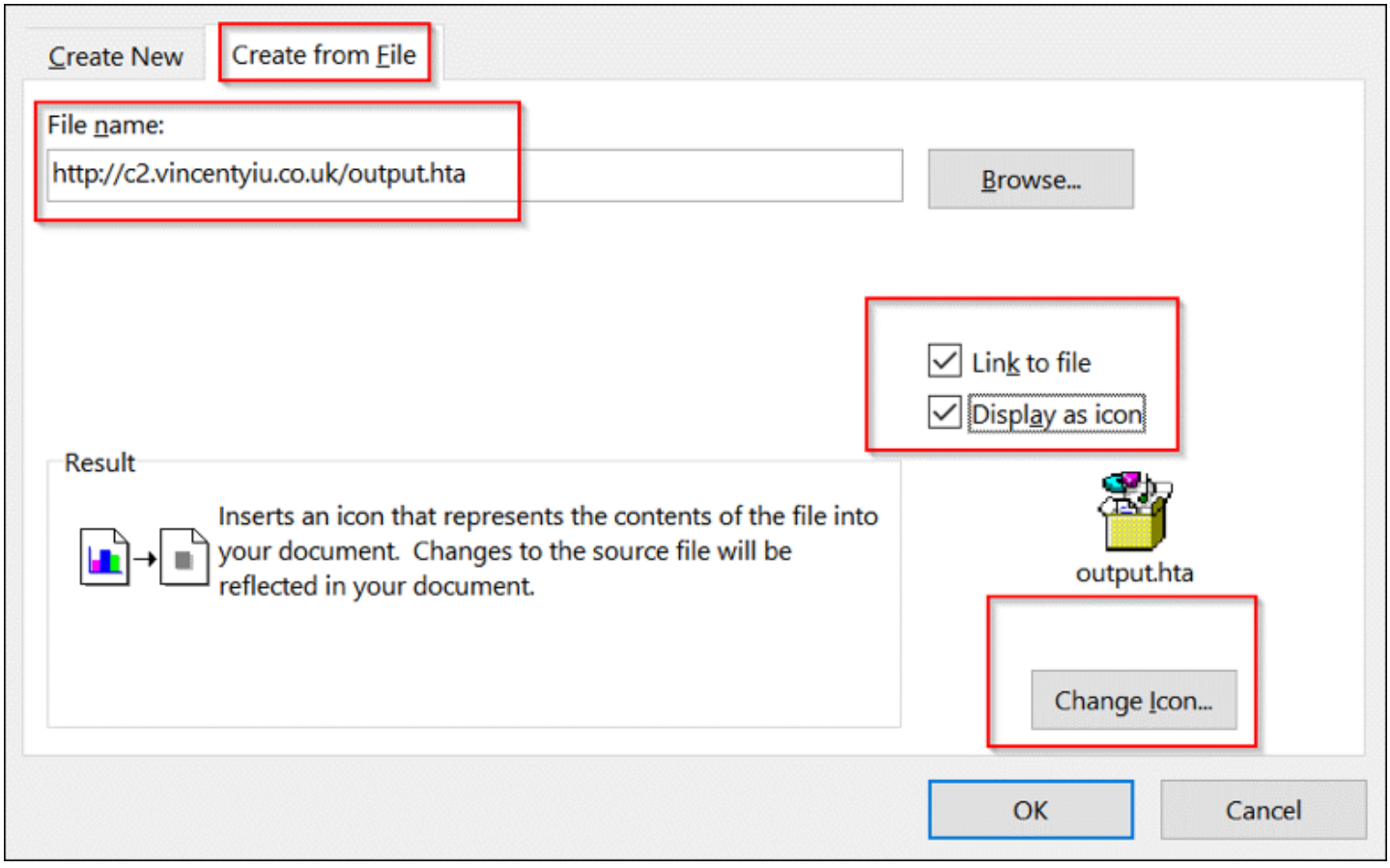
攻击步骤

首先，问题是使用OLE2嵌入式链接对象，其次在处理一个HTA文件。

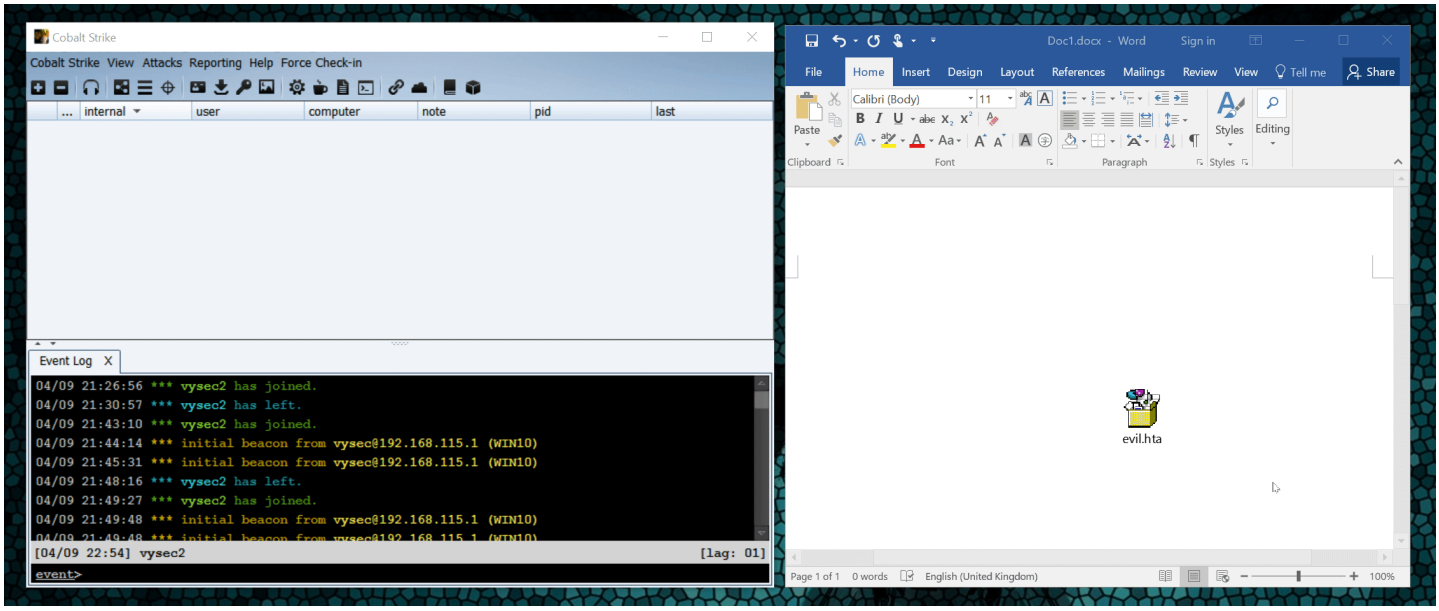
1 嵌入OLE2链接对象到一个文件，打开微软Word，单击"插入对象"按钮，如下面的截图：



2 选择从文件创建，插入URL HTA文件和刻度都链接到文件和显示为图标。

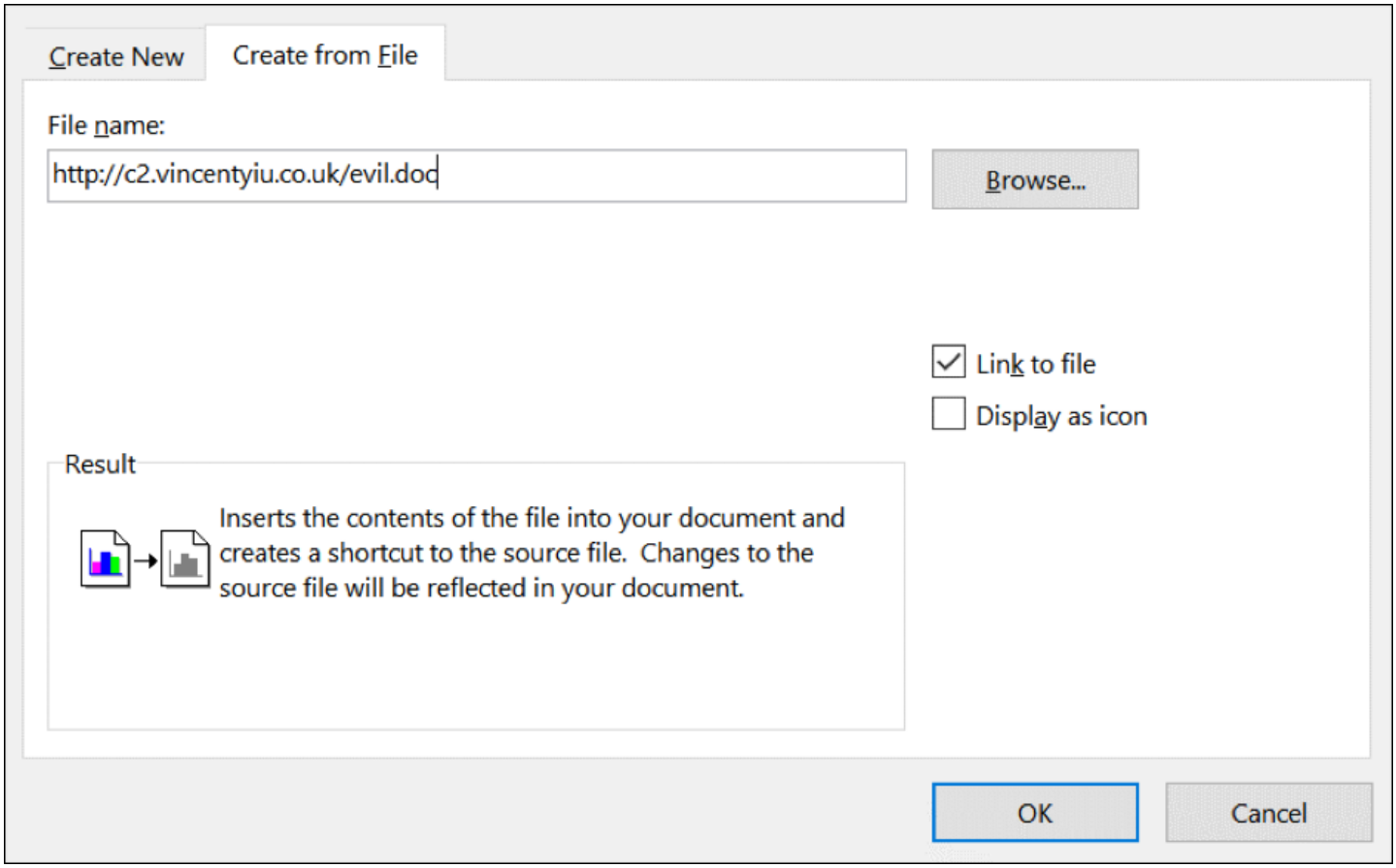


3 将文档保存为docx，DOC或RTF文件；所有这些处理ole2链接对象。

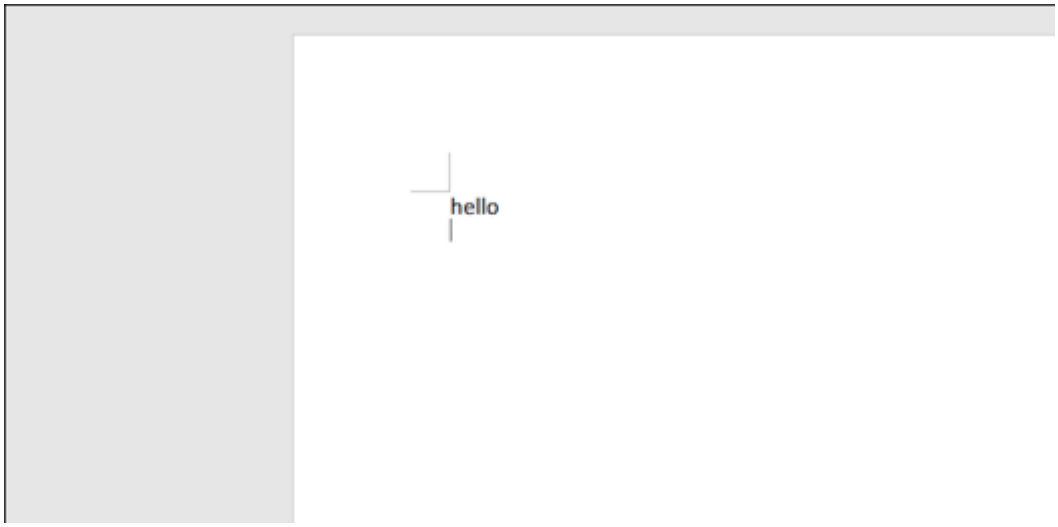


4

然而，图标和文字可能看起来有点可疑，因此可以通过更换图标和文件名，并渲染对象的Word，增加成功的可能性。这可以通过不选择"显示为图标"复选框，实现服务文档



5 这使得HTA要呈现如下：



6
然而，用户交互仍然是必需的，用户必须双击“Hello”文本这个时间或保存文件强制文件执行连接更新的内容，并显示它。然而FireEye的描述不明确，需要用户交互并暗示载
RFC“objupdate”控制被发现：

Objects

Microsoft OLE links, Microsoft OLE embedded objects, and Macintosh Edition Manager subscriber objects are represented in RTF as objects. Objects are destinations that
part of the object.

The representation of objects in RTF is designed to allow RTF readers that don't understand objects or don't use a particular type of object to use the current result in place o
destination that contains the object data, and an optional result that contains the current appearance of the object. This result contains standard RTF. It is an important respon

When the object is an OLE embedded or linked object, the data part of the object is the structure produced by the **OLESaveToStream** function. Some OLE clients rely on t
function. For information about the **OLESaveToStream** function, see the Microsoft Object Linking and Embedding Software Development Kit.

The syntax for this destination is:

<obj>	('{' **\object** (<objtype> & <objmod>? & <objclass>? & <objname>? & <objtime>? & <objsize>? & <rsltmod>?) <objdata> <result> '}') | <pubobject>
<objtype>	**\objemb** | **\objlink** | **\objautlink** | **\objsub** | **\objpub** | **\objicemb** | **objhtml** | **objocx**
<objmod>	**\linkself**? & **\objlock**? | **\objupdate**?
<objclass>	'{*' **\objclass** #PCDATA '}'
<objname>	'{*' **\objname** #PCDATA '}'
<objtime>	'{*' **\objtime** <time> '}'
<rsltmod>	**\rsltmerge**? & <rslttype>?
<rslttype>	**\rsltrtf** | **\rslttxt** | **\rsltpict** | **\rsltbmp**
<objsize>	**\objsetsize**? & ***\objalign***? & ***\objtransy***? & <objhw>? & ***\objcropt***? & ***\objcropb***? & ***\objcropl***? & ***\objcropr***? & ***\objscalex***? & ***\objscaley***?
<objhw>	***\objh*** & ***\objw***
<objdata>	'{*' **\objdata** (<objalias>? & <objsect>?) <data> '}'
<objalias>	'{*' **\objalias** <data> '}'
<objsect>	'{*' **\objsect** <data> '}'
<result>	'{' **\result** <para>+ '}'

7 此控件的描述特别有趣，因为它暗示对象将在显示自身之前更新：

Control word	Meaning
Object Type	
\objemb	An object type of OLE embedded object. If no type is given for the object, the object is assumed to be of type **\objemb**.
\objlink	An object type of OLE link.
\objautlink	An object type of OLE autolink.
\objsub	An object type of Macintosh Edition Manager subscriber.
\objpub	An object type of Macintosh Edition Manager publisher.
\objicemb	An object type of MS Word for the Macintosh Installable Command (IC) Embedder.
\objhtml	
\objocx	An object type of OLE control.
Object Information	
\linkself	The object is a link to another part of the same document.
\objlock	Locks the object from any updates.
\objupdate	Forces an update to the object before displaying it. Note that this will override any values in the <objsize> control words, but reasonable values should always be provided for these to maintain backwards c
\objclass	The text argument is the object class to use for this object; ignore the class specified in the object data. This is a destination control word.
\objname	The text argument is the name of this object. This is a destination control word.
\objtime	Describes the time that the object was last updated.
Object Size, Position, Cropping, and Scaling	
\objh*N*	*N* is the original object height in twips, assuming the object has a graphical representation.
\objw*N*	*N* is the original object width in twips, assuming the object has a graphical representation.
\objsetsize	Forces the object server to set the object's dimensions to that specified by the client.
\objalign*N*	*N* is the distance in twips from the left edge of the objects that should be aligned on a tab stop. This is needed to place Equation Editor equations correctly in line.

例如，可以创建一个包含一个objupdate控制，最终将迫使它更新启动文件。这可以通过获取先前创建的文档并在文本编辑器中修改它来实现：
Original:

{\object\objautlink \rsltpict\objw9027\objh450{\objclass Word.Document.8}{\objdata

注射\ objupdate控制文件：

{\object\objautlink\objupdate\rsltpict\objw9027\objh450{\objclass Word.Document.8}{\objdata

打开RTF文件现在造成托管HTA文件运行而无需用户交互：

值得注意的是，我们的研究显示，如果用户没有安装微软Office，问题仍然可以在写字板中然而利用的互动是必需的。

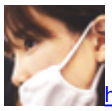
检测和响应

一些公司已经公布的规则由响应社区检测问题。在许多情况下，这些都是有点不准确，可能会产生误报，他们依靠的对象包含一个ole2link
RTF文档检测。这并不一定意味着恶意行为，可能是一个合法的嵌入对象。
为了有效地检测cve-2017-0199，Yara规则应该识别\ objupdate控制添加条件。

喜欢就关注我们的公众号吧。微信搜索公众号：杂术馆

上一篇：移动APP安全与SDL 下一篇：Cobalt Strike搭建和使...

1. 4 条回复

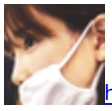

hades 2017-04-14 06:38:29

hta文件创建：

https://gist.github.com/subTee/e126c6ee847a4d9fcfd7

https://github.com/nixawk/labs/commit/effba17185a0d118004ebe0002e00a6171b61022

0 回复Ta


hades 2017-04-14 06:54:05

创建一个包含一个objupdate控制怎么做啊

0 回复Ta

rcoil 2017-04-14 08:36:58

https://www.mdsec.co.uk/2017/04/exploiting-cve-2017-0199-hta-handler-vulnerability/

0 回复Ta

笑然 2017-04-14 11:34:19

赞楼主

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板