安全威胁每周警讯

2012/10/07～2012/10/13

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	WORM_DOWNAD.AD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
2	WORM_DOWNAD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
4	X97M_OLEMAL.A	宏病毒	★★	→	宏病毒，它会将本身的下列副本放置到受影响的系统：%User Profile%\Application Data\Microsoft\Excel\XLSTART\k4.xls
5	TROJ_IFRAME.CP	木马	★★★	↑	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
6	X97M_LAROUX.BK	宏病毒	★★	↑	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
7	Downloader_Agent	灰色软件	★★	↑	这灰色软件下载器会自动下载并安装额外的其他的灰色软件，如广告软件和间谍软件。
8	WORM_ECODE.E-CN	蠕虫	★★	↑	它通过将受感染的移动驱动器与系统连接起来而入侵。 它可能是由远程站点的其他恶意软件/灰色软件/间谍软件下载而来。 它可能是用户在访问恶意网站时在无意中下载而来
9	X97M_LAROUX.CO	宏病毒	★★	↑	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
10	TROJ_SPNR.30ID12	木马	★★★	↑	木马程序

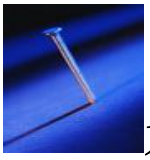
系统漏洞信息

MS12-057 ： Microsoft Office 中的漏洞可能允许远程执行代码 (2731879)

Microsoft Office 2007

Microsoft Office 2010

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-057



系统安全技巧

木马一直是黑客的拿手技量。善于用木马的黑客，可以在原来的入侵基础之上达到更大的目的。如今，虽然木马的种类有很多。但其中 IFRAME 挂马比较早，相应的预防措施也比较多，其中用 CSS 配合 JS 脚本进行预防是主流方式。可这种预防方式也存在安全隐患，JS 脚本也可以被用来挂马，令人防不胜防。我们下面要介绍反击 JS 挂马的方法。

JS 挂马溯源

当 IFRAME 逐渐被黑客滥用的时候，有经验的安全工程师也开始研究相应的对策，一段时间内各种阻止 IFRAME 挂马的方法不断涌现，其中通用性较高的就是利用 CSS 配合 JS 脚本防御 IFRAME 挂马。

而黑客也发现，很多网站都会让网页调用 JS 脚本来实现广告等诸多特效，如果将木马挂在 JS 脚本中，所有调用该 JS 脚本的网页都等同于被挂上了木马，对于需要肉鸡群的黑客而言是一劳永逸，因此 JS 脚本挂马逐渐开始被黑客应用。

小百科：JS 脚本是 JavaScript 脚本语言的简称，它是一种面向对象的脚本语言，目前广泛用于动态网页的编程。需要提示大家的是，JavaScript 和 Java 除了语法上有一些相似之处，以及都能够当作网页的编程语言以外，两者是完全不相干的。而 JavaScript 与 Jscript 也不同，Jscript 是微软为了迎战 JavaScript 推出的脚本语言。

虽然 JavaScript 作为给非程序人员的脚本语言向大众推广，但是 JavaScript 是一门具有丰富特性的语言，它有着和其他编程语言一样的复杂性。实际上，你必须对 JS 有扎实的理解才能用它来编写比较复杂的程序，作为一名安全工程师，掌握 JS 脚本在工作中会有很大的帮助。

挂马原理一点通

JS 脚本挂马对于黑客而言，可以说优点多得数不过来，首先 JS 脚本在挂马时可以直接将 JS 代码写在网页中，也可以通过注入网页，让网站远程调取异地 JS 脚本。此外，JS 挂马插入 Web 页面的方法有几十种，绝对够菜鸟们眼花缭乱，无从辨别木马在何处。

IFRAME 挂马相对于安全工程师而言，如同一个穿着鲜红颜色外衣的劫匪，招摇而扎眼，很容易被发现。

但是利用 JS 挂马就意味着这个劫匪拥有了一张可以随时变换的面孔，而且它还能够随时更换衣服。这样的劫匪在安全工程师搜查时，很容易蒙混过关，导致木马久杀不绝。

JS 挂马攻防实录

攻现最多见的 JS 挂马方法有两种，一种是直接将 JavaScript 脚本代码写在网页中，当访问者在浏览网页时，恶意的挂马脚本就会通过用户的浏览器悄悄地打开网马窗口，隐藏地运行。

另外一种 JS 挂马方式是，黑客先将挂马脚本代码，存为.js 的脚本文件，并上传到自己指定的网址。这时黑客只需要在受害者的网站中写入。

防第一种 JS 挂马方式，不方便，用得非常少，而第二种 JS 挂马方式才是当前主流的，所以我们主要针对它进行防御。方法就是阻止 Src 请求的异地外域的 JS 脚本，代码如下：

```
iframe{mdy1:expression(this.src=’about:blank’,this.outerHTML=”);}

script{mzm2:expression((this.src.toLowerCase().indexOf(‘http’)==0)?document.write(‘木马被成功隔离!’):”);}
```

不过这种方法的缺点就是网站的访问者将不能看到被挂了 JS 木马的相关网页。

所以我们为安全工程师提供了一段可以中止 JS 脚本运行的 CSS 代码，这段代码会让异地外域的 JS 文件在使用 document.write()时，被 document.close()强制关闭。这个时侯 JS 挂马的内容往往还没有来得及写完，只有部分被强制输出了，Writer 后面的内容再不会被写入访问者的电脑中，从而起到防范 JS 脚本挂马的作用。

```
<title>让 JS 挂马中止的 CSS 代码</title>

<style type=”text/css” id=”shudoo”>

/*<![CDATA[*/

iframe{mdy1:expression(this.src='about:blank',this.outerHTML='');}

script{mzm2:expression((this.src.indexOf('http')==0)?document.close():'');}

/*]]>*/

</style>
```

来源：51CTO

该邮件列表仅用于提供信息，此邮件列表内容不负任何担保责任，没有明示或默示的保证，包括但不限于对适销性、特定用途适用性以及不受侵害的暗示保证。用户对此邮件列表的准确性和使用承担全部风险，因依赖该资料所致的任何损失，趋势科技均不负责。