Miniduke:基于 Web 的感染机制

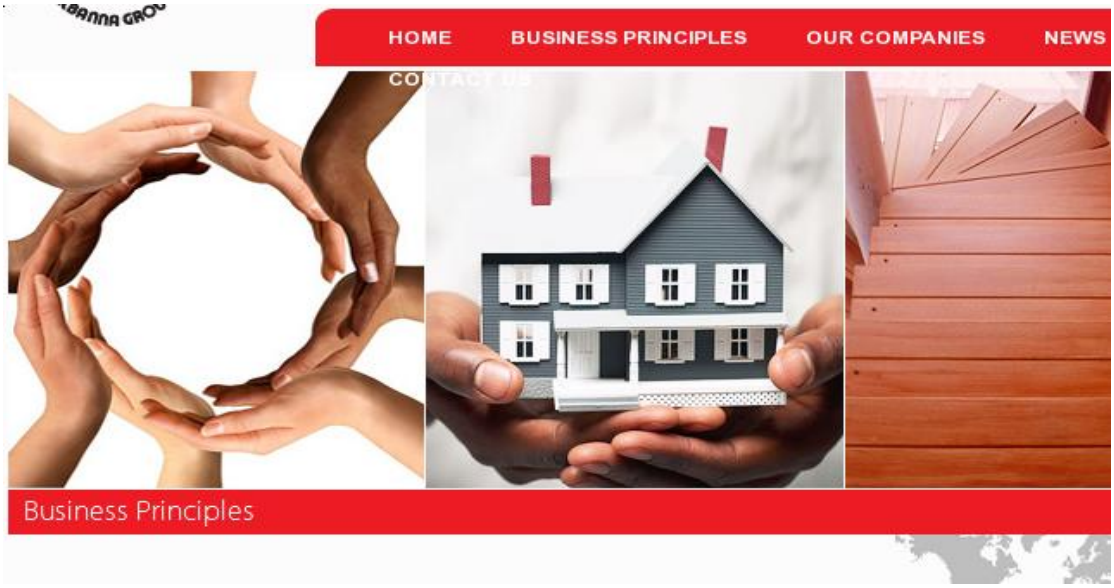
非官方中文译本•安天技术公益翻译组 译注

文档信息			
原文名称	Miniduke: web based infection vector		
原文作者	Igor Soumenkov	发布日期	2013 年 3 月 11 日
作者简介	Igor Soumenkov 是卡巴斯基实验室的恶意软件专家，担任基础设施部门经理和内容过滤基础设施开发部门的经理。http://www.zoominfo.com/p/Igor-Soumenkov/1410314705		
原文发布单位	Kaspersky Lab		
原文出处	http://www.securelist.com/en/blog/208194159/Miniduke_web_based_infection_vector		
译者	安天技术公益翻译组	校对者	安天技术公益分析组
免责声明	本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

我们与合作伙伴 CrySyS Lab 协作，发现了两个 Miniduke 之前未被知晓的感染机制。这些新的感染途径依赖于 Java 和 IE 漏洞进一步感染受害者 PC。

我们通过感染 Miniduke 的一个 C&C 服务器发现，这些文件没有关联到该 C&C 的代码，更像是准备好感染访问带有漏洞的网页的受害者。

hxxp://[c2_hostname]/groups/business-principles.html 作为攻击的起始点，包括两个框架：一个用于从合法网站下载诱饵页面（从 *http://www.albannagroup.com/business-principles.html* 复制得来）；另一个用于执行恶意活动（*hxxp://[c2_hostname]/groups/sidebar.html*）。



诱饵页面

第二个页面是"sidebar.html"，包含 88 行代码，大部分是 Java 脚本，并作为原始的开发包。这些代码可识别受害者浏览器，随后挖掘一两个漏洞。该页面还会通过发送 POST 请求至"*hxxp://[c2_hostname]/groups/count/write.php*"将收集到的浏览器数据发送至另一个脚本。

这些漏洞分布在单独的页面里。使用 IE8 的客户访问的是"about.htm"，对于其他版本的浏览器或能够运行 Java 小程序的任何其他浏览器，该 Java 脚本均加载"JavaApplet.html"

页面。

```
function frame_init(browser_name,plugins_info) {
  var output="";
  if ((/MSIE 8.(\d+)/.test(browser_name))&(/Windows NT 5.1/.test(browser_name))) {
    if (createIframeContent("about.htm")==0) output += "---IE loaded---";
    //alert("IE 8");
  }
  else {
    if (/Java/.test(plugins_info)) {
      if (createIframeContent("JavaApplet.html")==0) output += "---Java loaded---";
      //alert("Java");
    }
    else
        if (/MSIE/.test(browser_name)) {
              if (createIframeContent("JavaApplet.html")==0) output += "---Java loaded---";
        }
        else output += "---no loader---";
    //alert(output);
  }
  return output;
}
```

JavaScript 代码内部的 sidebar.html 页面

第一章 Java 漏洞

"JavaApplet.html" 页面加载 "JavaApplet.class"，该页面通过最近发现的漏洞 CVE-2013-0422 实现一个 Java 漏洞。该漏洞的代码与已经公开的 Metasploit kit 中的某个漏洞的代码极为相似，但其内部禁用安全管理器的类却用不同的代码编写，这样做的目的很可能是为了躲避检测。根据该服务器的 HTTP 头数据显示，这个小应用程序的上传日期为 2013 年 2 月 11 日，即 Metasploit 的代码被公布一个月之后，也是 Oracle 发布关于该漏洞的安全警报的前两天。

HEAD /groups/JavaApplet.class HTTP/1.1

Host: [c2_hostname]

HTTP/1.1 200 OK

Server: Microsoft-IIS/5.0

X-Powered-By: ASP.NET

Date: Fri, 08 Mar 2013 06:18:04 GMT

Content-Type: application/octet-stream

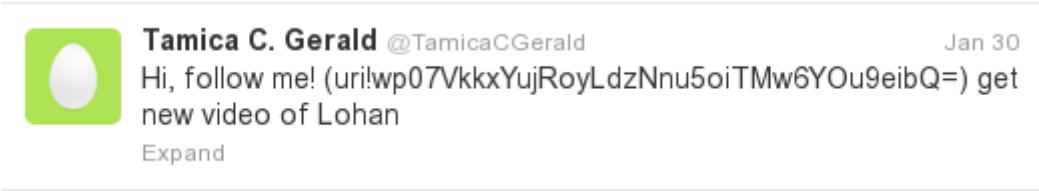
Accept-Ranges: bytes

Last-Modified: Mon, 11 Feb 2013 09:50:31 GMT

ETag: "f794173b3d8ce1:e96"

Content-Length: 52408

该 Java 的 shellcode 是一个有效的载荷 ,包含一个十六进制编码的 Win32 DLL 文件。它解码这个二进制文件并将其命名为"ntuser.bin"写入一个 Java 的临时目录。随后它拷贝系统文件"rundll32.exe"至该目录，并将其命名为 ntuser.exe"，然后将"ntuser.bin"作为一个参数运行该系统文件，进而有效地加载恶意 DLL 文件。这个 DLL 文件就是 Miniduke 的主模块，它通过 URL *http://twitter.com/TamicaCGerald* 获取指令。



带有 MiniDuke 指令的推文

(解码指令 URL: hxxp://www.artas.org/web/)

第二章 IE8 漏洞

"about.htm"页面实现一个微软 IE8 漏洞。它利用的是 2012 年 12 月末发现的漏洞 CVE-2012-4792。其代码与 Metasploit 漏洞版本极为相似，但 shellcode 的有效载荷部分则是 Miniduke 作者重新利用该后门的代码编写得来。Metasploit 代码公开于 2012 年 12 月 29 日，并在 2013 年 1 月 14 日得到官方修复补丁（MS13-008），而具有该漏洞的页面被上传于 2013 年 2 月 11 日。

EAD /groups/about.htm HTTP/1.1
Host: [c2_hostname]

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
X-Powered-By: ASP.NET
Date: Fri, 08 Mar 2013 06:49:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Mon, 11 Feb 2013 09:50:47 GMT
ETag: "b98150443d8ce1:e96"
Content-Length: 3842

该 shellcode 旨在从 URL*hxxp://[c2_hostname]/groups/pic.gif* 下载一个 GIF 图像文件，随后搜索并解密其中包含的隐藏的 PE 文件。该 PE 文件看似是 Miniduke 主后门模块的一个修改版本，但它使用相同的 Twitter URL 作为 Java 有效载荷。

第三章 小结

我们发现并分析了两个新的被用于 MiniDuke 攻击的感染方法。虽然在发现攻击的第一时间就发布了这些漏洞，但它们还是比较新的并且能够用于攻击指定目标。如之前的建议一样，广大用户需及时更新 Windows、Java 和 Adobe Reader 至最新版本，以便应对来自 Miniduke 的攻击。当然，不排除存在其他感染方法的可能；我们会继续监控 Miniduke 的行为进展并适当更新博客内容。