【译】一种完美的"监守自盗"型银行恶意软件分析

Alibluesky / 2017-11-08 11:45:00 / 浏览数 7030 技术文章 技术文章 顶(0) 踩(0)

前言
传统意义上来说，虽然来自巴西的银行恶意软件多多少少很简单，但近年来的网络攻击趋势揭示了一些新型且精细的攻击工具，这些从巴西开始的恶意软件很可能会被传播到
直到现在，由于"Themida"文件高复杂度的特性，这个恶意软件的深层运作原理还未被揭开。但是多亏了Check
Point研究团队，我们已经能够对该恶意软件执行脱壳操作并揭露这个新变种的恶意软件是如何同其受害者互动的。
我们接下来的研究揭示了：一旦受害者登录其在线银行账户（不管是HSBC, Santander, Citibank
还是其他巴西银行后），该受害者是如何被欺骗并将自己的账户拱手让给攻击者的。最终的结果是他们账户中的存款会在神不知鬼不觉的情况下被偷走。
另外，通过我们的研究发现：我们能够将Talos小组的研究成果同Trusteer在一月份分析的类似版本的恶意软件联系起来。直到现在我们才真正清楚这些巴西银行恶意软件是
银行恶意软件能从没有防备意识的受害者那里给窃贼带来每年数百万美元的收入。本文将详细的分析恶意软件是如何运作以及如何将它在用户的终端上检测出来，我们希望能

传播过程

研究与分析
下图描述了恶意代码的运行过程。

恶意软件利用vprintproxy.exe这个可执行文件（通过vm.png这个假名传播），它是一个VMware签署的合法文件。为了在安全检查中伪装自己，这个恶意软件使用了DLL劫

服务器上存档的名字	从文档中抽取后并重命名	类型	主要作用
vm.png	[random].exe	EXE	加载恶意依赖vmwarebase.dll
vmwarebase.dll	vmwarebase.dll	DLL	将prs.png注入到explorer.exe和notepad.exe
prs.png	[random].db	DLL	
gbs.png	[random].drv	DLL	展示位图（bitmap）用以锁屏
i.dk	i.dk	TXT	通过C&C地址来提供恶意软件

恶意软件的技术细节
下面是恶意软件的每个主要模块的技术描述。
vmwarebase.dll–dropper
一旦vprintproxy.exe开始执行，并且vmwarebase.dll被加载之后，运行会传递到它的DllMain起始点。这个DLL的最终目的是将prs.png（这个恶意软件的核心模块）注入到

1. png的路径（它的名字重命名为0到999999999之间的一个随机整数，扩展名改为db）是最先被解析，解析方法是通过检测C:\Users\public\Administrator\car.dat（这
2. 在C:\Users\public\Administrator搜索对应的文件。如果找到了，这个路径的字符串会被作为动态缓存简单地写入目标进程中，如下图所示：
3. 得到的路径被用来作为LoadLibrary的参数。后者会在注入进程中被解析，并且会假设它在目标进程中有同样的地址。这样一来，LoadLibrary就可以利用上述提到的参数

在进行注入之前，vmwarebase.dll会将所有进程编号，并且会查找所有运行中的conhost.exe实例，这些实例会被关闭，以用来关闭之前感染阶段打开的窗口。
prs.png–第一阶段注入
这个模块包括以下功能：

4. 键盘记录器
5. 屏幕截图
6. 将当前屏幕替换为一个指定画面
7. 改变当前系统的鼠标
8. 自动运行并创建注册表项
9. 关闭系统工具（例如taskmgr， dwm， regedit等等）
10. 实施系统重启
11. 文件\目录删除功能

这个软件运行其恶意代码的方法十分有趣。大部分这个恶意软件的代码和数据都是存储在这个模块的表单中。一旦恶意软件开始运行，主表单就会在屏幕上作为一个非常

这些表单基本上是一些Delphi对象，它们包含很多属性，例如Edit，Memo和其他GUI部件，这些都是用来存储重要信息的。
在Timer对象的帮助下，可以实现多线程功能，在这个表单中处处都有体现。举个例子，我们可以看"TAUXILIO_TURCO"表单，它存储了很多信息和设计功能，如下图所

删除不想要的应用
在特定条件下这个模块会停止几个进程，比如
taskmgr.exe
msconfig.exe
regedit.exe
ccleaner.exe / ccleaner64.exe
dwm.exe (for Windows 7 only)
iexplore.exe
firefox.exe
chrome.exe
opera.exe
safari.exe
NetExpress50.exe

AplicativoBradesco.exe
itauaplicativo.exe
office.exe
javaw.exe
C&C通信
恶意软件使用存储在"i.dk"文件中的一段配置信息与C&C服务器进行通信，该配置信息使用AES-256进行加密的，解密后的配置信息如下所示：

用钓鱼位图来抓取用户的敏感信息：
有些内嵌的表单包含多个位图。这些是用来引诱用户输入他们的认证码，这是巴西银行的一种通用举措，也是很多用户采用的方法。当攻击者想要对受害者的浏览器下手

gbs.png -第二阶段执行
这个模块使用了Themida工具加壳，一旦执行，它会有以下几个操作：
进程保护
该技术用来防止通过进程管理器来关掉恶意软件进程，更详细的解释在：
https://stackoverflow.com/questions/6185975/prevent-user-process-from-being-killed-with-end-process-from-process-explorer
移除之前安装的hook
该恶意软件模块循环调用UnhookWindowsHookEx函数来卸载之前建立的窗口（windows）hook。
覆盖（Overlay Placement）机制
该模块负责给用户显示一条覆盖消息，该消息是从数个硬编码的字符串中挑选出来的，还会根据用户访问的银行网站变化。简而言之，模块会持续监控用户浏览器中打开
它的流程由如下几个阶段组成：

12. 在浏览器中识别URL–恶意软件使用FindWindowW/GetWindow(...,
GW_HWNDNEXT)等组合搜索当前系统中的所有窗口。当找到一个与浏览器相关的窗口，将会检查它的URL地址栏。针对不同的浏览器（Chrome, Firefox
and Internet Explorer），恶意软件会使用不同的方法来抓取所需的URL。
13. 得到的URL会与下面列出的URL硬编码列表进行对比：
aapj.bb.com.br/aapj/loginmpe
www.santandernetibe.com.br/
www.ib2.bradesco.com.br/ibpflogin/identificacao.jsf
ww7.banrisul.com.br/brb/link/brbwe4hw.aspx?
wwws5.hsbc.com.br/ITE/connect2/wcm_connect/pws/hsbc-online-cnb.html
internetbanking.caixa.gov.br/SIIBC
.bancobrasil.com.br/aapf/
www.santanderempresarial.com.br
aapj.bb.com.br/aapj/
www.santandernet.com.br
www.brasil.citibank.com/BRCIB/JPS/portal/Index.do
internet.sicreditotal.com.br/stiapp/
ibpf.sicredi.com.br
wwws3.hsbc.com.br/ITE/common/html/hsbc-online.shtml
ib.sicoobnet.com.br/inetbank/login.jsp
itau.com.br/GRIPNET/bklcom.dll
www.ib2.bradesco.com.br/ibpftelainicial/home.jsf
www.citibank.com.br/BRGCB/JPS/portal/Index.do
www.ne2.bradesconetempresa.b.br/ibpjlogin/login.jsf
ww8.banrisul.com.br/brb/link/brbwe4hw.aspx?
14. 基于定位后的URL检查注册表日期–该表单的注册表路径：HKCU\Software\Trilian[A-Z]{2}（最后两个字母是根据从浏览器找到的活跃URL生成的）会被检查以确定是否
a. 注册表路径或日期变量没有找到–运行一些结束代码，并停止该恶意软件运行。
b. 系统日期与注册表变量的日期相等或更新–恶意软件会从之前提到的注册表分支删除节点"Block [A-Z]{2}" and "Date
[A-Z]{2}"并接着在HKLM\Software\Microsoft\Windows\CurrentVersion\Internet设置中搜索ProxyServer
节点。如果它的值是123.123.123.123:3212那么这个节点的值会被擦除，然后一个新的节点ProxyEnable
会被建立，它的值是0。接着，有被检测到的URL的浏览器会被关闭，然后整个监视重新开始。
c. 系统日期比注册表变量日期要晚-恶意软件模块会设置一个键盘hook用来拦截按下的键（如WIN，ESC等）。
15. 最后，模块以全屏模式弹出一个透明的窗体（不能被用户关闭，因为有键盘hook），向用户展示当前活动浏览器的截图。最重要的是，10个位图（对应于活动的银行网
唯一有效的元素是关闭表单的按钮。 以下是与sicredi.com.br对应的位图示例：

每个这种位图都有类似的说明："抱歉，无法与【银行网站】的安全模块同步，请稍后再试。"这会迫使用户关掉表单。同时，这个用户会看到另一个覆盖的消息，假装是
可选操作
如果活动URL是空的，这个模块会恢复下列函数的头6个字节（如果它们被挂钩或者在它们的内存区域中设置了断点）：
FindWindowExW
FindWindowW
SendMessageW
在此之后，监视会从上述所说的流程中重新开始。
文章来源:https://research.checkpoint.com/perfect-inside-job-banking-malware/

上一篇：XDCTF-2017-Final ... 下一篇：限量版先知创新大会徽章
1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板