2016年10月22日13时，某网络黑客团伙成功接管巴西一家银行所有业务长达5小时，截获了当时所有的金融交易数据。微步在线根据卡巴斯基公开的相关信息检索发现，此次攻击的受害者为巴西Banrisul银行，该行成立于1928年，在巴西、美国、阿根廷和大开曼岛等地拥有分行500家，客户约500万，总资产超过250亿美元。

微步在线分析此次事件的攻击流程如下：

· 攻击者于2016年年中开始对Banrisul银行网站进行全面调查分析，掌握网站体系架构，下载网站源码。

· 利用漏洞或钓鱼邮件方式入侵Banrisul银行的DNS提供商Registro.br，控制了Banrisul的DNS账户。

· 2016年10月22日5时30分，在Let’ s Encrypt网站注册免费SSL证书，启用Google Cloud上的仿冒网站。

· 2016年10月22日13时，修改银行网站DNS解析记录，将访问银行在线服务的用户定向到仿冒网站，诱导输入信用卡信息。

· 控制并关闭银行的企业邮箱，以防止银行通知受害者和DNS供应商。

· 诱导用户下载伪装成Trusteer的恶意软件压缩包（Truste_Install_EF69EC50F11D77D9.zip）并执行其中的Java文件（Truste_Install_EF69EC50F11D77D9.jar）。

· Java文件的执行后会从远端服务器（191.101.232.182）下载一个包含后门程序的压缩包（windows.zip），执行其中的Avenger程序用于清理系统现有杀毒软件，并将后门程序（windows.dll）注册为计划任务。

· windows.dll后门程序具备获取系统信息、监控桌面窗口、获取进程列表、远程执行、文件上传下载、命令等功能，会不断尝试访问谷歌协作平台（sites.google.com）的随机地址和C&C服务器（192.99.111.91）的15111端口。

微步在线对国内20余家主流银行分析发现，大多数单位使用了内部邮箱用于域名管理，且域名服务器也为内部所有，自身安全措施较为完善。而涉及的域名服务商则包括中国万网、新网、中科三方、广东互易网络、厦门三五互联等10多家，其中多数公司近年来均被爆出过SQL注入、XSS等高危漏洞，可能泄露用户敏感细信息，合作伙伴的安全问题同样需要引起有关单位的高度重视。

……检测措施……

以下两种方式，任意一种即可：

· 网络流量：

建议直接部署微步在线威胁情报平台进行检测，或者使用附录的IOC结合日志检测：

如，通过防火墙检查与IP 191.101.232.182的连接

· 主机检测：

查看以下目录或者目录是否存在：

%appdata%MicrosoftWindows.bat

%appdata%MicrosoftWindows.exe

%appdata%MicrosoftWindows.txt

%appdata%Microsoft.zip

……行动建议……

· 利用微步在线提供的威胁情报或者威胁情报平台进行检测，及时响应。

· 启用DNS等基础服务供应商提供的安全服务，如双因子认证，以加强内部基础设施的安全策略建设。

附录

C&C

http://191.101.232.182/BR/Windows.zip

http://191.101.232.182/TM/Windows.zip

192.99.111.91

木马hash

2f9fe6db7279da14576cc5cc9e92bffe

1444ff1fdb9a5cf273d915612523d77d

4aed960aebd6f38fdb1c7ee79dc79fbc

98d689250a373b5667c3458ee8df06a8

2bf96bceece3e565f6cd6b03cd3c9a33

723e8da040c24cd60901ebf4d4cc13a5

7e32de2a14db2b04bed8625dcf560fdd

f032731de7d3f584cda4e48451e0b134

3f272fb8e3cd3b2cb288580b63306361

7650b4834dc8d2ed8f546f7178af3140

248954276030a90f5856c03141bec23bce7ad1601414408134217adf98f02051

b86f15850ad307f4eb303acc11930f91e6befbcd2da73b5f17034a3c9f88fee9

7e9ada8f5f5aaaae7ecddd66f1352f9ede223c3ab5b8f2cfaa0657bc8fa94e1d

5c7ab9e90b05804d07e9d803f85462bc1a44d0726256bad28219984ee2b5772f

030a7ddf668c9049b6609af0a3f0523f57f7ab07fd6cbbcbed0b37ae8067f5c5

9b9cb6a6ddbdd67106e8a2f055563059b7dd14ff31ea336e20f00b1969da2976

fc0b440ef53b6814a0db53c4ca46e69b5d5651da57175342c33e2ec760c6de79

e4bc73ad9c7c33a714ecfe47c7a89fb4ead04a1987d90bf3dcb8531385502e36

a2b8e28882812ed7f6b1a674d373f038ffaffcb0ffc26eeff01cf1dc63cd1f8a

325f0adf4e45318ce312d2cb077b6de2dd170be6b3d4efe8c82e9a96faf13e96