全球银行业受黑客组织攻击分析报告

作者：补天漏洞响应平台　vincebye@0vul 团队

关键词

金融　银行　swift　黑客攻击　Lazarus

摘要

黑客攻击已从攻击网络来窃取数据演变成直接通过银行系统操作进行金融转账行为，造成更加严重的后果，造成更加直接的经济损失。

据新华社台北 10 月 7 日电：台湾远东国际商业银行近日披露，其电脑系统遭黑客植入恶意程序远端操控转账。

一、几起银行被攻击事件分析

1、台湾远东国际银行事件回顾

根据初步收到的情报，攻击源自于一封钓鱼邮件。图 1 和图 2 提供了钓鱼邮件的示例。

图 1 钓鱼邮件附件

图 2 钓鱼邮件附件

当受害者点击链接时，他们将被重定向到恶意网站，然后下载一些文件到受害者的计算机。我们截取到一个案例，下载地址为 https://***.com/maliciousfilename.exe。该网站托管另一个后门，让犯罪分子有权限访问银行的受害者系统。

我们初步分析攻击者通过获得系统访问权限窃取了数字证书，我们在一个病毒样本中发现了如下的银行证书：

- FEIB \ SPUSER14

- FEIB \ scomadmin

这些证书用于在系统上创建计划任务并监视终端安全服务软件的运行，但这并不表示安全软件存在问题，只有攻击者进行研究并采取攻击手段针对在银行内运行的安全软件。

除了计划的任务和凭据之外，我们还发现了另一个有趣的代码。示例（如图 4）中的内容是资源“IMAGE”，它似乎是一个 zip 文件。把它提取出来，生成了一个 aa.txt。虽然这似乎是一个文本文件，但它确实是一个 exe 可执行文件。

该文件会扫描已安装语言的代码：

- 419（俄语）

- 422（乌克兰）

- 423（白俄罗斯）

如果检测到这些语言，文件将不会运行。我们以前也曾在勒索软件中看到过这种行为。

当我们分析这个特定文件的字符串时，我们发现了一些有趣的文件：

- HERMES 2.1 TEST BUILD，press OK

- HERMES

当执行时，这个文件看起来像是勒索软件。但是，没有注释或其他方式证明这是勒索软件。文件完成运行后，桌面上只出现一个事件弹窗：

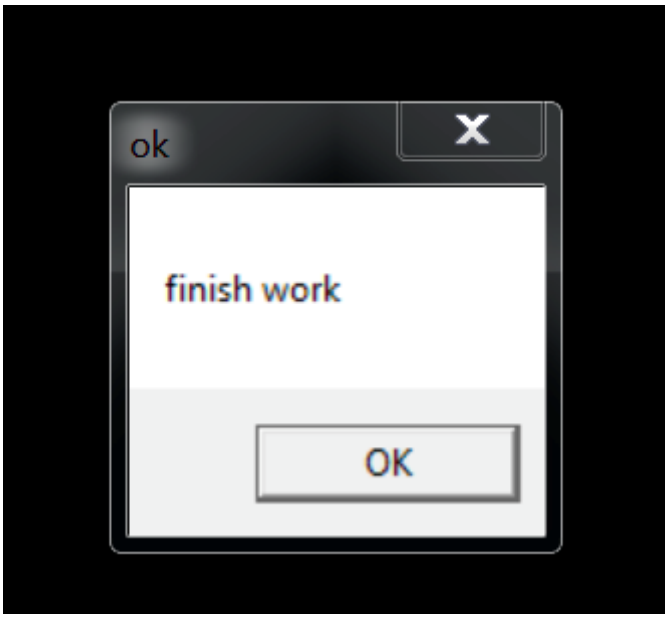

图 3 伪勒索软件的最后一个界面

同时会在每个目录生成一个文件：

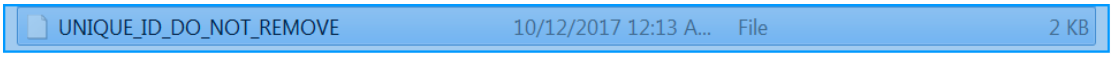

图 4 伪勒索软件生成文件

原来的 Hermes 勒索软件文本指向这个文件。但在我们的监测下 我们看不到任何操作记录，也没有要求给付赎金。

Hermes 勒索软件在二月份浮出水面：

图 5 Hermes 勒索软件界面

我们怀疑这是另一个伪装勒索软件的例子。我们猜测勒索软件的真正目的是用来分散这次攻击。根据我们的监测，当对外发送未授权的付款时，网络中的勒索软件则开始运行。

综合来看，这显然是一个非常精心制作的 APT 攻击。攻击者确定了具体的个人电子邮件，并了解了正在部署的安全措施。虽然绝大部分的银行业系统已被安全产品所覆盖了，但是我们谨此提醒，“没有绝对安全的系统”。犯罪分子花时间了解银行如何工作，制定必要的代码，使其能够窃取到上百万以及上亿的金钱。

2、 越南先锋银行攻击事件回顾

（1）攻击过程整体流程

图 6 整体关系流程

针对越南先锋银行的攻击中，相关恶意代码内置了 8 家银行的 SWIFT CODE，越南银行均在这些银行中设有代理帐户。目前看到的 Fake PDF Reader 样本目的不是攻击列表中的这些银行，而是用来删除越南银行与其他家银行间的转帐确认（篡改 MT950 对帐单）。这样银行的监测系统就不会发现这种不当交易了。

（2）攻击流程

Fake PDF Reader 伪装成 Foxit Reader（福昕 PDF 阅读器），原始 Foxit Reader.exe 被重命名为 Foxlt Reader.exe，在银行系统调用 Foxit 打印 pdf 时激活，将 pdf 转换为 xml，根据配置文件匹配是否有符合要求的报文，找到匹配的报文修改后转换回 pdf 并调用原始的 Foxit Reader 打印，并删除临时文件和数据库的符合条件的交易记录。

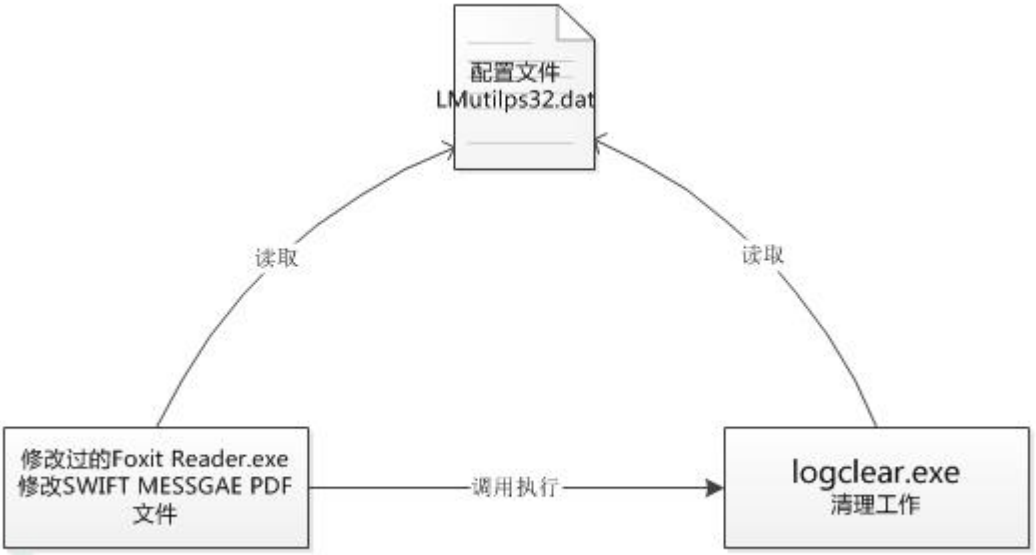

图 7 关系图

（3）MT950 对帐单（PDF）详解

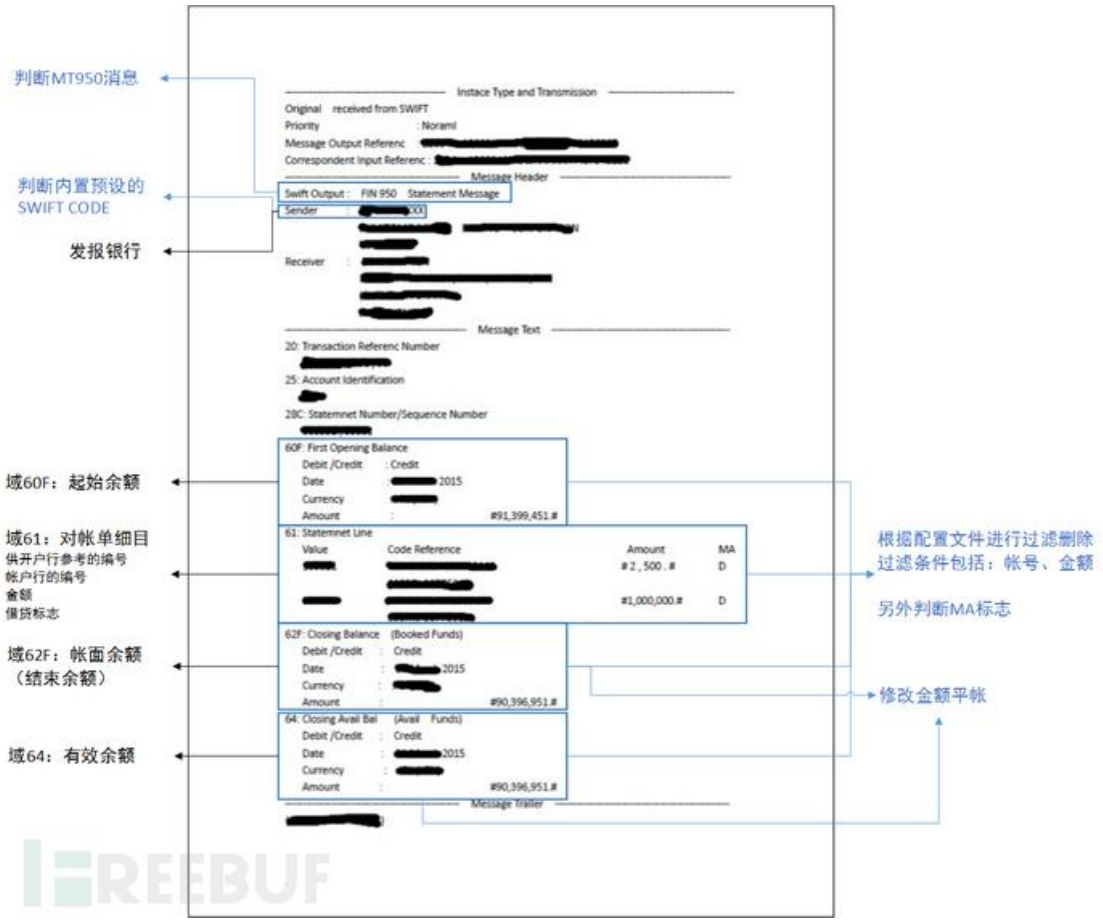

图 8 MT950 对帐单

上图是 MT950 对帐单的 PDF 版本，图中就对帐单的关键报文域进行了对应的解释（黑体字

所示），另外蓝色框是 Fake PDF Reader 恶意程序需要判断和修改的地方（蓝色字体是相关具体动作的说明）。

下图是正常的 PDF 对帐单和篡改后的 PDF 对帐单，其中左图红色底色部分内容，就是攻击者想要删掉帐单记录和需要修改的帐面余额和有效余额。

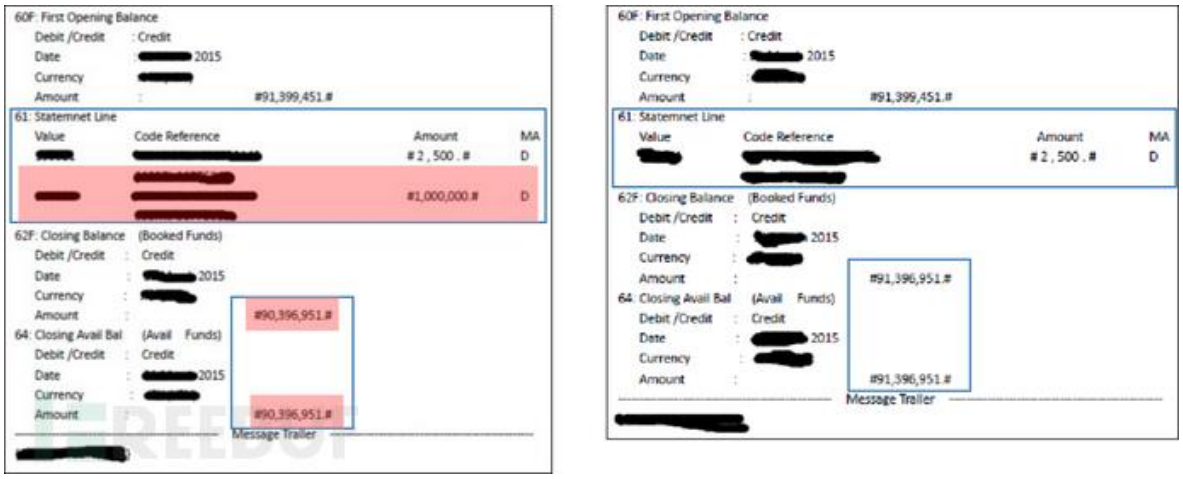

图 9 正常 PDF 对帐单（左图），篡改后的 PDF 对帐单（右图）

（4）分析总结

从将恶意程序构造伪装成 Foxit Reader（福昕 PDF 阅读器）到对 MT950 对帐单 PDF 文件的解析和精确的篡改等攻击手法，都反映出攻击者对银行内部交易系统和作业流程非常熟悉。

针对越南先锋银行的针对性攻击和之前针对孟加拉国央行等其他银行的攻击之间，并非独立无关的攻击事件，从我们对相关样本同源性分析和其他厂商的研究分析来看，针对越南先锋银行和孟加拉国央行的攻击有可能来自同一个组织，其幕后组织有可能是 Operation Blockbuster 所揭秘披露的 Lazarus 组织。

3、 孟加拉央行攻击事件回顾

2016 年 2 月 5 日，孟加拉国央行（Bangladesh Central Bank）被黑客攻击导致 8100 万美元被窃取，攻击者通过网络攻击或者其他方式获得了孟加拉国央行 SWIFT 系统操作权限，进一步攻击者向纽约联邦储备银行（Federal Reserve Bank of New York）发送虚假的 SWIFT 转账指令，孟加拉国央行在纽约联邦储备银行上设有代理帐户。纽约联邦储备银行总共收到 35 笔，总

价值 9.51 亿美元的转账要求，其中 30 笔被拒绝，另外 5 笔总价值 1.01 亿美元的交易被通过。进一步其中 2000 万美元因为拼写错误(Foundation 误写为 fandation)被中间行发觉而被找回，而另外 8100 万美元则被成功转走盗取。

而我们捕获到的这次网络攻击中所使用的恶意代码 ,其功能是篡改 SWIFT 报文和删除相关数据信息以掩饰其非法转账的痕迹，其中攻击者通过修改 SWIFT 的 Alliance Access 客户端软件的数据有效性验证指令，绕过相关验证。

攻击流程：

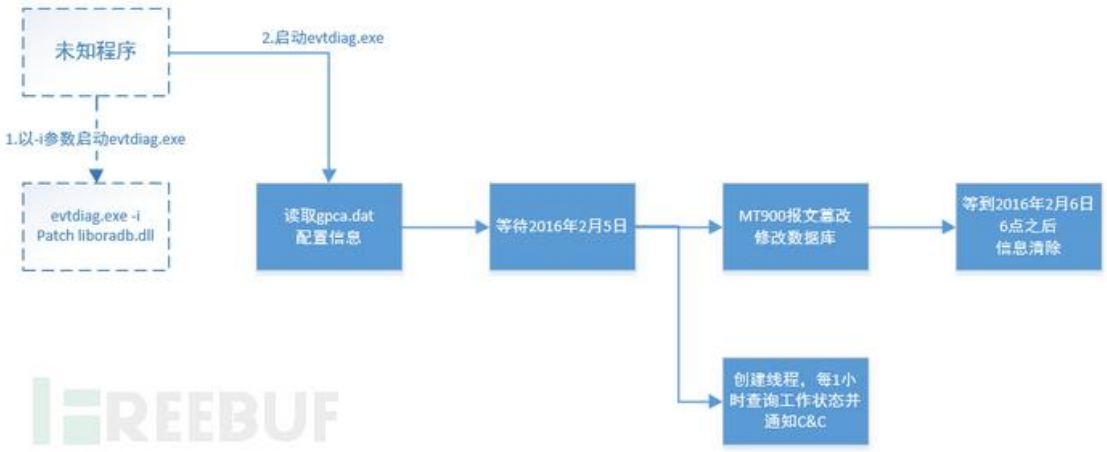

图 10 evtdiag.exe 执行流程

步骤 1：恶意代码检测是否有进程加载了“liboradb.dll”模块，进一步修改数据有效性验证指令，绕过验证；

步骤 2：读取“gpca.dat”配置文件，其中包括了 transord、日期、C&C 等攻击者预设的关键信息；

步骤 3：“2016 年 2 月 5 日”是样本在满足其他特定条件后 ,执行报文篡改操作的触发时间；

步骤 4：MT900 报文篡改，操作打印机，并选择性修改数据库；

步骤 5：样本执行篡改报文操作时，查询被感染计算机的相关“登录/注销”状态，将相关信息回传 C&C 服务器；

步骤 6：监控执行持续到 2016 年 2 月 6 日 6:00，之后退出并删除自身的日志、数据以及注册的服务。

通过对以上案例进行分析总结，近年来黑客攻击团伙频繁对全球银行系统进行有计划针对性的入侵，由于这些攻击，银行被迫造成资金和名誉上的损失，下面我们总结一下近年来被攻击过的银行。

二、近年来受过攻击的银行事件

攻击时间	被攻击银行	计划窃取	实际损失
2013 年	索纳莉银行（Sonali Bank）	未知	25 万美元
2015 年 1 月	厄瓜多尔银行（Banco del Austro）	未知	1200 万美元
2015 年 10 月	疑似菲律宾某银行	未知	未知
2015 年 12 月 8 日	越南先锋银行（Tien Phong Bank）	120 万欧元	无
2016 年 2 月 5 日	孟加拉国央行（Bangladesh Central Bank）	10 亿美元	8100 万美元
未知	疑似香港某银行	未知	未知
未知	疑似菲律宾、新西兰某银行和其他 10 多家金融机构	未知	未知
2017 年 10 月	台湾远东国际银行	18 亿新台币	50 万美元

三、脆弱的 SWIFT 系统

SWIFT 又称：“环球同业银行金融电讯协会”，是国际银行同业间的国际合作组织，成立于一九七三年，目前全球大多数国家大多数银行已使用 SWIFT 系统。

在 2015 年 1 月，在厄瓜多尔银行起诉 Wells Fargo 银行的一份法庭文件泄露时才被曝光。在所有的攻击案件中，攻击者都是通过使用恶意软件入侵银行网络并获得访问 SWIFT 信息网络的权限。在其中一个受害者银行中，攻击者通过 SWIFT 向其发送了伪造的短信，要求从受害银行账户中转出百万美元。

BAE 公司的研究人员称，他们在孟加拉银行 SWIFT 系统中发现了被称为 evtdiag.exe 的恶意软件，恶意软件中包含可操控 SWIFT 软件客户端 Alliance Access 的代码。

黑客通过凭证登入 SWIFT 系统，BAE 专家发现孟加拉银行的 SWIFT 软件已经被破坏，可以被黑客利用进行非法的转账操作。

四、我们可以防范吗？

通过对历史上几起银行安全事件横向分析，利用 Foxit 出品的 PDF 阅读器漏洞进行渗透和攻击的线索最为明显。下面将重点针对 Foxit 出品的 PDF 阅读器的相关漏洞以及应对提出方案。

(1) Foxit PDF 阅读器近期高危漏洞

- CVE-2017-10951 命令注入漏洞存在于 app.launchURL 函数中，由于缺乏正确的验证方式，该函数能执行由攻击者提供的字符串。
- CVE-2017-10952 文件写入问题存在于 “saveAs” JavaScript 函数中，它能让攻击者在目标系统中的任意具体位置写入一个任意文件。ZDI 指出，“Steven 通过将一个 HTA 文件内嵌到文档，然后调用 saveAS 将其写入启动文件夹从而在启动时执行任意 VBScript 代码的方式利用这个漏洞。

(2) Foxit PDF 阅读器早期高危漏洞

攻击者利用以下几个漏洞，可以欺骗用户用 Foxit 或 PhantomPDF 打开恶意 PDF 文件。只要提供了对应的链接，就有以下这十二个相关漏洞允许攻击者执行远程代码（注：这十二个漏洞已经得到修复）。

Foxit 阅读器的版本 8 和 PhantomPDF 中有以下这些漏洞：

- ConvertToPDF TIFF 解析漏洞,允许攻击者越界编写远程代码
- ConvertToPDF BMP 解析漏洞,允许攻击者越界读取私密信息
- ConvertToPDF GIF 解析漏洞,允许攻击者越界编写远程代码
- JPEG 解析漏洞,允许攻击者越界读取私密信息
- ConvertToPDF TIFF 解析漏洞,允许攻击者越界编写远程代码
- exportData 漏洞,允许攻击者绕过权限,执行远程代码
- 安全模式漏洞,允许攻击者窃取信息

- FlateDecode 漏洞,允许攻击者执行远程代码
- 模式未初始化指针漏洞,允许攻击者执行远程代码
- FlateDecode 漏洞,允许攻击者执行远程代码
- GoToR 行动堆栈缓冲区溢出漏洞,允许攻击者执行远程代码

修复建议

a) 及时更新 Foxit 软件版本至最新版本，PhantomPDF 至最新版本

b) 建议启用“安全阅读模式”功能

c) 取消勾选 Foxit“偏好”菜单中的“启用 JavaScript 动作”选项

五、关于 Lazarus 黑客组织

2016 年 2 月 25 日，Lazarus 黑客组织以及相关攻击行动由卡巴斯基实验室、AlienVault 实验室和 Novetta 等安全企业协作分析并揭露。2013 年针对韩国金融机构和媒体公司的 DarkSeoul 攻击行动和 2014 年针对索尼影视娱乐公司（Sony Pictures Entertainment，SPE）攻击的幕后组织都是 Lazarus 组织。

相关时间节点	具体事件描述
2007.03.07	“Flame”行动中第一代恶意软件开发完成，该活动最终与“1Mission”行动、“Troy”行动、2013 年 DarkSeoul 攻击联系在一起。
2009.07.04	使用恶意工具 MYDOOM、Dozer 对美国、韩国网站发动大规模 DDOS 攻击，该恶意软件在 MBR 写入文本信息“Memory of Independence Day”。
2009-2013	“Troy”网络间谍行动活跃数年，在 2013 年 DarkSeoul 攻击达到顶峰。
2011.03	“Ten Days of Rain”行动攻击韩国媒体、金融、基础设施。利用韩国地区的肉鸡发动 DDOS 攻击。
2011.04	韩国农协银行被 DDOS 攻击。
2012	发动“1Mission”行动，该行动的攻击者被报道称从 2007 年就开始活跃。
2012.06	韩国保守媒体报纸声称受到具有清除功能的恶意软件的攻击，但未成功。网站被未知黑客团体“IsOne”篡改。
2013.03.20	DarkSeoul 清除行动攻击韩国广播公司、金融机构、及一家 ISP。两个未知

	黑客团队 NewRomanic Cyber Army Team 和 WhoIs Team 声称对此负责。
2014.03	疑似有黑客试图窃取韩国军方数据，使用的服务器之一也被用于 DarkSeoul 攻击。
2014.11.24	索尼影视娱乐公司网络被植入破坏性恶意软件，信息被窃取。早前的未知黑客组织 GOP 声称负责。

六、参考来源

[1] http://news.xmnn.cn/xmnn/2017/10/08/100259184.shtml

[2] https://securingtomorrow.mcafee.com/mcafee-labs/taiwan-bank-heist-role-pseudo-ransomware/

[3] http://news.cctv.com/2017/10/09/VIDEgNbOYwZYVJMFXqpcnOMj171009.shtml

[4] http://bobao.360.cn/news/detail/4269.html

[5] http://bobao.360.cn/news/detail/3240.html

[6] http://www.freebuf.com/vuls/106026.html

[7] http://www.freebuf.com/articles/paper/111488.html

[8] http://www.freebuf.com/news/105205.html

[9] http://www.freebuf.com/articles/network/107900.html