打击
代理银行服务中的
网络欺诈

如今，网络犯罪是全球各所银行关注的重点问题。直到最近，犯罪分子似乎仍针对银行客户的银行卡或账户信息，实施网络犯罪。然而，随着犯罪分子的手段越来越高明，他们的野心也越来越大，开始直接瞄准银行下手。面对这些威胁，金融机构能采取哪些措施，保护自己免受网络袭击，更快地侦测可疑活动，即使遭受网络攻击后也能迅速恢复？

当前背景

在梳理金融机构当前面临的威胁之前，我们首先要认识到，有组织的网络犯罪形式非常多样，从漫无目标地随意攻击，到精心策划的有针对性的高级攻击，犯罪形式不一而足。

毕马威英国会计师事务所的网络安全技术总监 David Ferbrache 解释称，诈骗分子通常先进行撒网式攻击，有组织的犯罪集团散发上百万份电子邮件，里面的仿冒网站链接可跳转至恶意软件。“一旦点击这种链接，系统就会遭到入侵，可能就会出现勒索软件索取钱财的命令。这些攻击中，只有很小一部分会得逞，这只是简单的撞运气。”

第二阶段是有针对性的攻击。Ferbrache 表示：“有组织的犯罪集团会用几周时间来确定目标机构，然后发动更可信、更有针对性且更精准的仿冒网站攻击。”这类攻击的形式之一是电子邮件欺诈，据美国联邦调查局 2016 年 6 月发布的数据，这项攻击已造成 30 多亿美元的损失。[1]

富有经验的诈骗分子越来越倾向于发动高级攻击。有组织的犯罪集团开始

[1] “Business E-mail Compromise: The 3.1 Billion Dollar Scam”（商务电子邮件欺诈：流失 31 亿美元），美国联邦调查局，2016 年 6 月 14 日，https://www.ic3.gov/media/2016/160614.aspx

有组织犯罪集团开始
直接攻击银行系统

直接瞄准银行系统。例如，犯罪分子协同发动无限制吐钞攻击，侵袭发卡银行的网络，改变自动取款机的取钞限制，清空其中存储的钞票。[2] 据 Ferbrache 介绍，2013 年曾发生过一起大案，一夜之间，24 个国家和地区共损失四千万美元。

在另一些案件中，有组织的犯罪集团通过银行网络，将恶意软件上传至自动取款机，使自动取款机响应犯罪分子输入的编码。去年，多个国家和地区遭受过这种攻击，包括台湾、泰国、俄罗斯、亚美尼亚、白俄罗斯、波兰、德国、格鲁吉亚、罗马尼亚、吉尔吉斯斯坦、爱沙尼亚、西班牙、荷兰、英国和马来西亚。

孟加拉银行去年因此损失 8,100 万美元，令代理银行尤为关注。这起攻击发生于 2016 年 2 月初，但据称，最终受益的账户早在一年前就在菲律宾开通，这可能是犯罪分子谋划的起点。犯罪分子利用恶意软件修改银行的接口服务器，不仅输入了虚假支付请求，还隐藏了这一操作，避免诈骗交易出现在日志中。

> 犯罪分子的目光从银行客户转向银行本身，代理银行乃至更广泛的银行服务社群面临的威胁性质发生重大变化

防范和侦测攻击

鉴于犯罪分子的目光从银行客户转向银行本身，代理银行乃至更广泛的银行服务社群面临的威胁性质发生重大变化，且越来越严重。然而，非常值得注意的是，尽管网络欺诈攻击的是银行，但目前为止，尚无任何犯罪活动攻击环球银行金融电讯系统和核心通讯服务。

从犯罪分子实施后台攻击的手段看，他们的组织性非常强，且非常高明。他们的攻击过程可分为以下四个步骤：

1. 攻击客户的操作环境，利用仿冒网址或电子邮件攻击计划，植入恶意软件。
2. 攫取有效操作证书，一般通过密码文件或放入键盘记录器来攫取密码，以此解读支付环境和相关活动。
3. 利用虚假证书攻击后台；例如，发送虚假 MT 103 支付信息。
4. 隐藏交易活动。例如，在本地数据库移除支付信息，修改收到的报表信息，或将本地环境设定为不可操作，

[2] Chris Strohm，“Most-Wanted Cybercriminal Extradited to U.S. From Germany”（位列通缉榜首的网络犯罪分子经德国引渡至美国），*彭博社*，2015 年 6 月 23 日，https://www.bloomberg.com/politics/articles/2015-06-23/turkish-man-accused-in-global-atm-heist-extradited-to-u-s-

保护机构环境	保护机构业务	侦测、响应和恢复
政策与标准	教育与意识	安全监控
网络安全与架构	业务访问管理	日志和情报分析
基础设施维护	机构文化	响应
访问权限管理		恢复
实体访问		持续改进
人员	程序	技术

信息与网络安全框架

ISO 27001 信息安全	NIST 网络安全框架	CESG 10 步确保网络安全	网络基本要素认证计划	ISO 27032 网络空间	PCI-DSS / swift / 其他

表 1：网络安全最佳实践考量

进而延迟攻击被发现的时间，加大成功完成资金结算的几率。

随着犯罪分子对银行的内部流程和基础设施越来越熟悉，他们的破坏性显然越来越强。因此，金融机构更加需要采取相应措施，保护自己的关键系统和关卡。

尽管理想状态下，金融机构能够防范各种网络攻击，但绝不可能完全消除威胁。机构不仅要采取防范措施，也要能够侦测正在进行的攻击，并准备好恢复程序和响应程序。

针对银行的各种活动，包括向社群分享信息、采取适当的市场操作等，目前有许多工具、技术和活动能够帮助银行缓释风险，识别可疑活动，在遭受攻击后恢复。

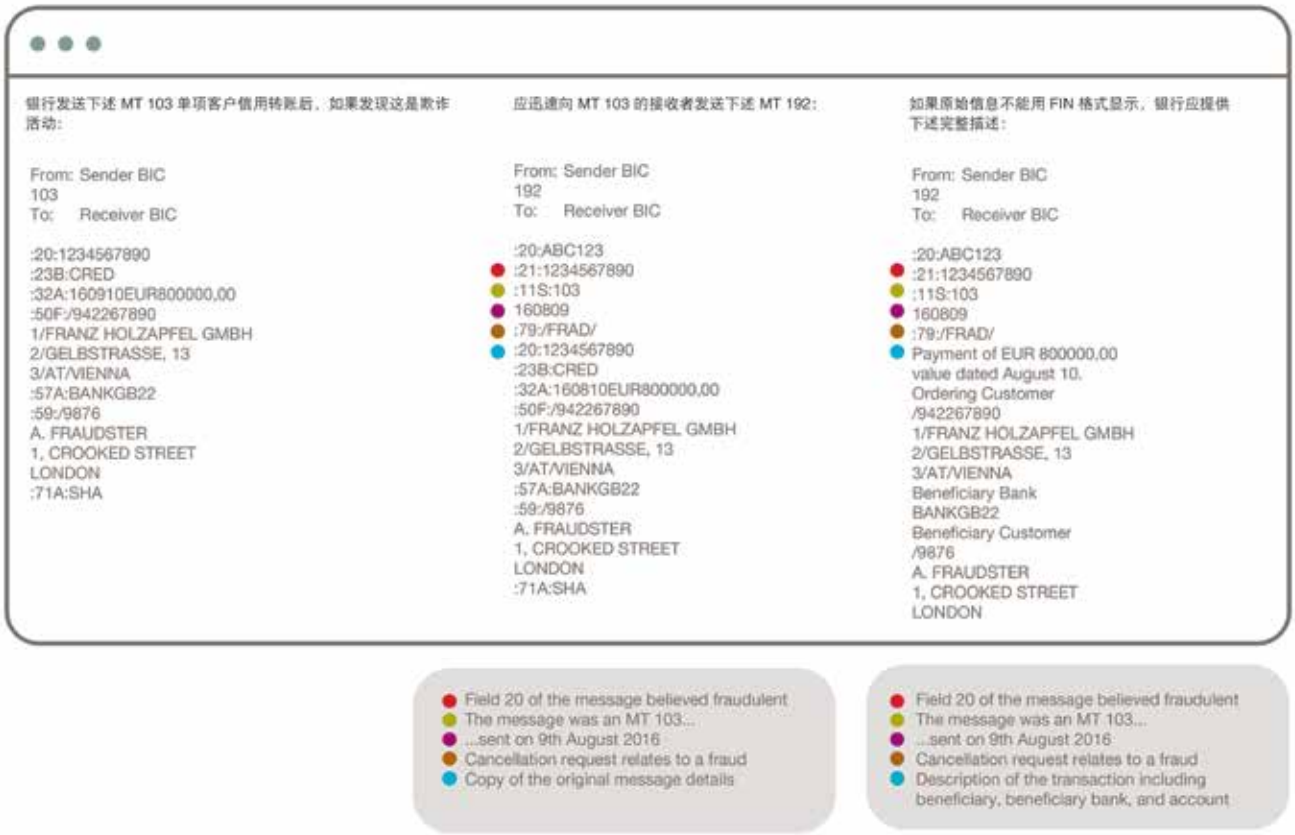
建立强大的基础

随着网络攻击越来越猖獗，行业和监管机构正采取措施来了解、解决和缓释风险。2016 年 5 月，环球银行金融电讯系统发布客户安全项目，旨在加强现有的网络控制，并为 1.1 万余个会员机构提供协作框架，帮助他们处理不断发展的网络威胁。该项目专注于金融机构保护自身环境和在环球银行金融电讯系统社群内分享信息的需求，以及管理同业对口机构关系的重要性。

环球银行金融电讯系统发起这项活动的同时，监管部门也在加强对银行网络安全的检查和指导。例如，2016 年 9 月，美国纽约州金融服务局在现有网络安全指导基础上发布一份提案。

所有这些措施的共同点是需要建立基本的安全保护。尽管网络攻击越来越成熟，但从基本安全做起的重要性不应小觑。如表 1 所示，以下方面应予以解决：

- *保护机构环境*——制定和应用适当的政策和标准，采用合理的访问权



如果出现可疑的欺诈活动，使用正确的环球银行金融电讯系统信息格式可提高取消支付指令的成功率。

限管理，在机构的网络和建筑中采取适当的安全措施。机构还应将各种职责分派给不同关键员工，适当处理员工招聘和离职工作，控制机构系统的特许访问权，并采取其他措施。

- *保护机构业务*——某些情况下，机构尽管关注网络安全，但可能不太熟悉业务背景。研究表明，环球银行金融电讯系统的大多数客户将人为因素视为网络威胁下最薄弱的环节。因此，提高员工对现有威胁的认识非常重要。有些机构会对内发布模拟仿冒网站信息，通过观察员工对恶意链接的点击情况，了解应提供哪些加强培训。
- *侦测、响应和恢复*——机构应确保按规定采取安全监控措施，例如持续政策监控，使用适当的重大事件监控程序等。机构还应采取具体措施，例如审核关系管理程序，采取相关市场做法等。

审核关系管理程序

金融机构管理同业对口机构关系的方法多种多样。首先是审核关系管理程序中的关系。

关系管理程序相当于金融机构间的“数字握手”，指明交易能否互换。如果没有关系管理程序，机构就不能获取同业对口机构的环球银行金融电讯系统信息。银行使用关系管理程序升级版后，可设定想要通过网络交换的信息类型和对象，从而提高控制力度。因此，关系管理程序和关系管理程序升级版可避免银行发送和接收不符合预设的信息，降低双方机构内部人员进行未批准交易的风险，从而帮助银行缓释网络攻击风险。

然而，交易模式并非一成不变。因此，多达 60% 的关系处于休眠或不活跃状态，这意味着机构可能不必要将自己暴露于特定通路。多余的关系管理程序还会产生不必要的成本支出，因为合规要求通常会要求机构对开通关系管理程序的同业对口机构进行“了解您的客户”审核。因此，机构应定期

审核关系管理程序，既为节省开支，也为保障安全。

沃尔夫斯堡集团去年发布的指南指出，金融机构“应在金融犯罪 / 反洗钱 / 了解您的客户制度中增加关系管理程序尽职调查标准”，例如，区分客户关系和非客户关系管理程序的请求。指南还指出，“对关系管理程序使用者的尽职调查应考虑其使用的信息类型，以及采取活动产生的风险。”[3]

市场做法

金融机构还可通过其他措施来提高侦测欺诈活动的能力，更有效地响应网络攻击威胁。例如，机构可核对账户，提供支付确认，制定支付修改政策。机构还应学习如何快速取消支付，以备不时之需。

机构可采取的措施之一是发送环球银行金融电讯系统 MT 900 和 MT 910 确认信息，并要求同业对口机构采取相同的做法。尽管这些信息目前尚非强制信息，但它们能提高同业对口机构间的透明度。同样，银行还应审核收到的 MT 940/MT 950 报表信息，检查报表中登记的金额和余额是否与自己的交易活动记录一致。

此外，银行还应避免使用 MT 199 等自由格式信息来修改或更改支付指令，这种信息会影响对账。银行如果要更改或取消支付指令，应删除原始指令，或发送支付修改信息。

监控交易数据

鉴于网络犯罪分子越来越倾向于隐藏欺诈活动，银行还应监控活动和风险，既为防范欺诈，也为侦测真正遭遇的攻击。

- *活动监控*——银行可通过积累日常活动记录，更清楚地了解支付活动，识别活动中的任何重大变化。
- *风险监控*——银行可通过监控交易环境中的风险，干扰欺诈分子隐藏交易活动的做法，也识别单个或连续异常交易。

机构应将这种信息进行分类并分别储存，确保一次攻击不会影响所有信息，导致支付系统和记录瘫痪或受损。

响应和恢复

对金融机构而言，还有一项应对网络攻击的重要措施，就是实行稳固的流程，在侦测到攻击后迅速并有效地响应，取消欺诈信息；如果交易无法取消，银行应采取一定措施，促进业务正常继续。

取消欺诈交易

某些情况下，银行可以通过发送取消信息，取消虚假指令。为此，银行应立即发送 MT n92，其中“n”代表原始信息的类别。例如，如果虚假信息是 MT 103，那么取消信息则是 MT 192，如果虚假信息是 MT 202，则取消信息是 MT 292。

银行在使用取消信息时，还应注意使用正确的虚假编码，以便优先处理这条请求，提高取消支付指令的成功率。银行必须在取消信息的 79 字段使用 /FRAD/。

灾难恢复 / 业务持续

在防御网络攻击的最后阶段，金融机构应采取一定措施，确保机构遭遇攻击后能够适当响应，尽快恢复正常的业务活动。这要求机构在网络安全与业务持续 / 灾难恢复之间建立强效联系，并了解网络安全与核心业务之间存在固有联系。Ferbrache 表示：“网络与核心业务密不可分。我们的所有业务现在都依赖数字技术，也就都会面临数字威胁。”

为制定有效的恢复程序，机构应设想各种可能出现的攻击，研究其后果。机构必须规划如何遏制或缓释攻击带来的影响，并学习如何处理沟通、监管和法律事务。机构还必须针对如何尽快恢复安全的网上业务，制定相应规划。

结语

随着网络犯罪分子对银行系统的了解越来越深入，金融机构面临的当务之急是采取适当措施，保护营业环境安全。机构须从多个方面采取措施，既为防范攻击，也为提高实时侦测攻击的成功率。最后，同样重要的是，机构必须制定清晰的业务持续计划，在受到攻击后，采取既定措施，确保业务恢复正常。 A

Tony Wicks，SWIFT 公司反洗钱计划负责人，英国伦敦，
tony.wicks@swift.com

[3] “Wolfsberg Guidance on SWIFT Relationship Management Application (RMA) Due Diligence”（沃尔夫斯堡关于环球银行金融电讯系统关系管理程序的尽职调查指南），沃尔夫斯堡集团，http://www.wolfsberg-principles.com/pdf/standards/SWIFT-RMA-Due-Diligence.pdf