亚信安全 新闻稿

[即时发布]

亚信安全提醒：新型针对性攻击袭来　警惕伪装来自高管的诈骗邮件

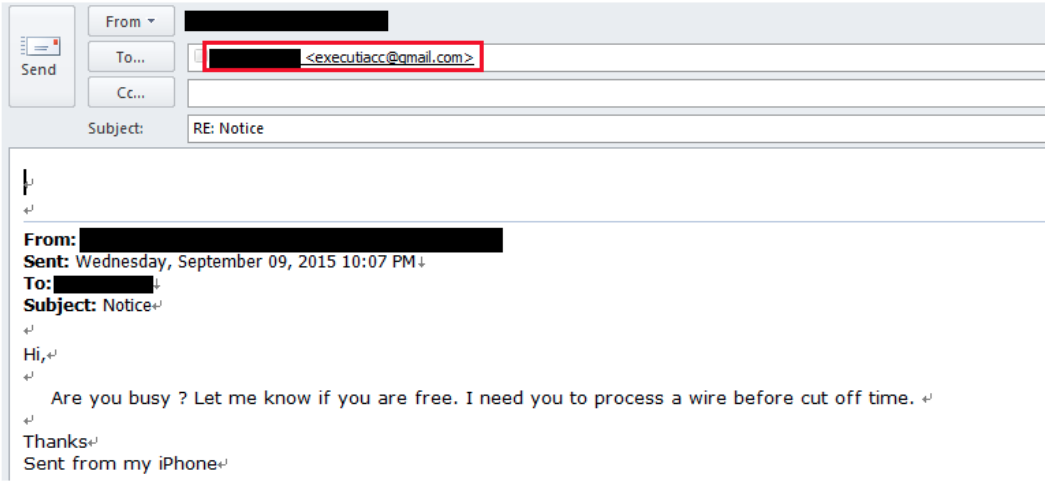
不法分子精心布置邮件陷阱　全球至少 40 家公司被攻击

[亚信安全]– [2015 年 11 月 4 日]近日，亚信安全发现一波针对性攻击/锁定目标攻击(Targeted attack)的诈骗活动，攻击活动由一封邮件开始，伪冒某公司的高级管理人员寄给其它管理人员（例：财务部经理）。与一般诈骗攻击或是网络钓鱼（Phishing）邮件不同的是，这封邮件没有任何的附件或是网址链接，但其邮件头已遭到修改，导致收件人回复之后会把邮件寄给攻击者。若不经仔细检查，很难发现隐藏在其中的陷阱。亚信安全在此提醒广大用户和公众，请在回复邮件前务必确认邮件的真实性，谨慎点击来自伪装高管的诈骗邮件，以防范新型针对性攻击袭来。

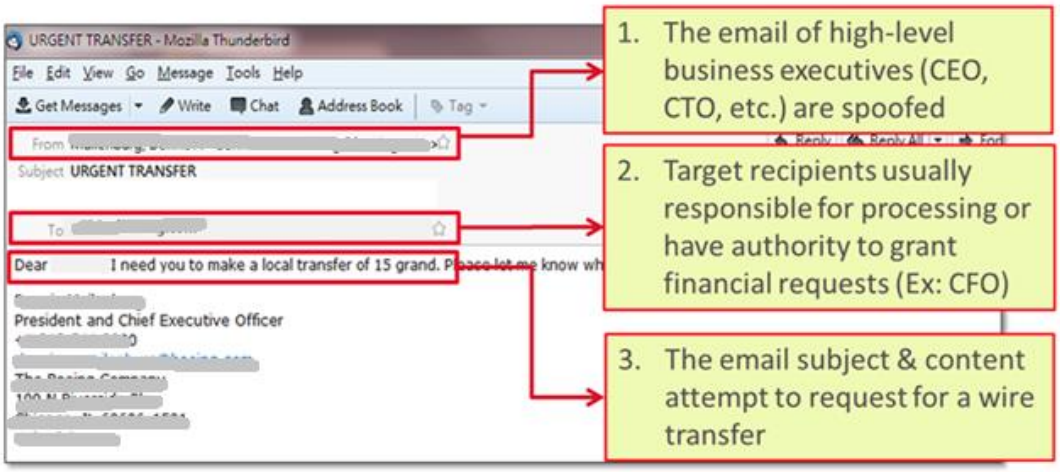
根据亚信安全云安全智能防护网络所搜集到的信息，仅仅在九月份，就有至少 40 家公司被攻击。

技术细节与解决方案

1. “From”与“To”使用相同的域名，使他看起来像是一封内部邮件，例：CompanyX.com 寄给 CompanyX.com。
2. “From”与“Reply-To”的域名不同，例：”From”是 CompanyX.com，而“Reply-To”是类似 gmail.com 或其他外部域名。
3. 目前发现“Workspace Webmail”及“Roundcube Webmail”在这类攻击中常被使用。
4. Email 容量不大，不容易被怀疑。
5. Email 内常包含某些特定字词像是“wire”或“transfer”。
6. “Reply-to”栏位常包含“executive”或“ceo”或“chief”等关键字。



【诈骗攻击邮件样本】



【回复邮件时，收件人为外部域名邮箱】

有鉴于该类型诈骗邮件严重的安全威胁，亚信安全技术总监蔡昇钦建议:”客户在回复邮件前，请务必确认邮件的真实性，即使邮件声明由公司高层管理者发来，也不要轻易相信，而是应仔细核实邮件内容以及邮件地址的真实性，必要的时候可以用电话等方式进行确认。如果该邮件的“mail from”与“reply-to”是不同的邮箱地址，那就务必提高警觉，因为该邮件很有可能是一封诈骗邮件。”

据了解，亚信安全 Email 信誉评等（ERS, Email Reputation Services）技术的团队已更新了病毒码，可以侦测此类型攻击，企业用户可以部署具备 ERS 技术的亚信安全“邮件安全解决方案”来进行防范。如用户发现任何攻击邮件未被侦测，请立即向亚信安全技术响应中心汇报。

###

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式，助力客户构建“立体化主动防御体系”，为国家提供网络安全与云产业安全保障，推动实施自主可控战略。更多关于亚信安全公司及最新产品信息，请访问：http://www.asiainfo-sec.com