事件概要

本周三（3月20日），韩国多家银行与三大电视台内部的计算机无法开机，有一些计算机屏幕显示骷髅头的图片与自称为“WhoIs”团队的警告信息，这些现象表明是有黑客组织发起此次攻击。

目前已知被攻击企业：

电视台	银行
韩国广播公司，KBS	新韩银行
韩国文化广播公司，MBC	农协银行
韩联社新闻台，YTN	济州银行

攻击手法

此次攻击具有典型APT特征，包括鱼叉式钓鱼邮件、水坑攻击与自我毁灭等。

- **鱼叉式钓鱼邮件**
  - 利用邮件传送恶意程序，连接以下的恶意站点
  - 受感染的计算机被用来作为跳板，攻击者进一步渗透内部重要服务器，包括补丁管理系统与网站服务器
- **水坑攻击（water hole attack）** - 这是最近的一种攻击方式，攻击者侵入目标族群经常访问的合法网站或服务器并植入恶意程序，当用户访问了这些网站，就会遭受感染。最近的例子是苹果内部计算机遭受漏洞攻击，攻击者在iOS开发者论坛植入恶意程序，访问的用户以软件开发人员为主。这些开发人员齐聚在这个论坛，就像聚集在沙漠中的水坑一样。
  - 韩国企业的补丁管理服务器与合法网站被入侵，连接的计算机都感染了恶意程序。
- **自我毁灭** – 复写计算机的Master Boot Record (MBR)，让后续的分析调查难以进行

攻击造成的后果

- 业务运行中断
  - 银行：ATM、网银、银行运维都陷入瘫痪
  - 电视台、媒体：媒体向外播送的内容无法更新，公开网站无法连接
  - 受感染机器上的数据无法恢复

趋势科技的建议

- 需要具备进阶威胁检测体系，在早期发现针对性攻击或入侵
- 企业需要提升全方位防护能力，尤其是针对社交工程邮件的检测阻断
- 产品加服务才能形成完整的安全闭环，达到快速预警响应，及早防护

趋势科技定制防御解决方案：

- 侦测：邮件安全网关设备IMSA + 威胁发现设备TDA
- 分析：TDA + DDA沙盒分析
- 加固：OfficeScan + Deep Security+ IMSA 等产品可提供阻断功能
- 响应：专家值守服务 及 PSP专属服务

全国已有上百家大型企业部署了趋势科技威胁发现设备TDA

中国农业银行 AGRICULTURAL BANK OF CHINA　交通银行 BANK OF COMMUNICATIONS　中国邮政储蓄 CHIAN POST　SZS　广发证券

海通证券 HAITONG　中信证券 CITIC www.cs.ecitic.com　中国人寿财产保险股份有限公司　中国移动通信 CHINA MOBILE　KIA

财通证券 CAITONG SECURITIES　国海证券 SEALAND SECURITIES　深圳发展银行 SHENZHEN DEVELOPMENT BANK　ZBM

太平洋保险 CPIC　渤海证券　中原证券 CENTRAL CHINA SECURITIES　现代快报　宁波钢铁 NINGBO IRON & STEEL

如需了解详细信息，请联络趋势科技销售，或致电 800-820-8876

自韩国爆发大规模黑客入侵事件以来，趋势科技陆续收到了很多客户询问，现将客户最常问到的几个问题整理如下，希望能帮助更多客户了解事件状况，提升企业针对APT等高级持续性威胁及目标攻击的防范意识和防御能力。

3月20日韩国网络攻击事件FAQ

- **2013年3月20日在韩国发生什么？**

  在3月20日下午，多家韩国民间企业遭受数次攻击，业务运行严重中断。这次事件的开始是受害企业内部数台计算机黑屏，网络冻结，造成计算机无法使用。

央视新闻频道针对韩国黑客入侵事件的报道

- **谁在此次攻击事件中受到影响？**

  数家韩国媒体与金融机构的网络受到影响，尤其是媒体，据报道他们的业务运行受到严重中断，要完全恢复至少需要4至5天。

- **攻击者的意图为何？**

  目前还不知道攻击者的动机，但是攻击造成的影响是终端正常业务运行，表明了这是一次破坏行动。如果不知道攻击者的真面目，很难去判定此次攻击的意图为何。

- **攻击活动如何开始？相关的恶意软件如何入侵？**

  一封伪装成三月份信用卡交易记录的邮件被送给被害者，该邮件包含两个附件，一个是无害的card.jpg，另一个是恶意的.rar文件，文件名写着“您的账户交易历史”

- **此次攻击事件的感染途径为何？**

  附件的.rar文件是一个downloader，它会连接数个恶意IP地址并下载9个文件。企业内部的中央更新管理服务器也遭受入侵而被植入恶意程序，更新管理机制让这个恶意程序能够相当快速的散播到所有连接此服务器的计算机。该恶意程序会新增数个组件，其中包含一个MBR（主启动记录，Master Boot Record）修改器。

  这个MBR修改器被设定成在3月20日下午2时启动，当时间到了的时候，MBR修改器就会复写本地与远程系统上的MBR，让计算机无法加载作业系统。

  目前已知其中一台被利用推送恶意程序的服务器是安博士（AhnLab，韩国本地最大防病毒厂商）的更新服务器。

- **在终端计算机上发生什么？**

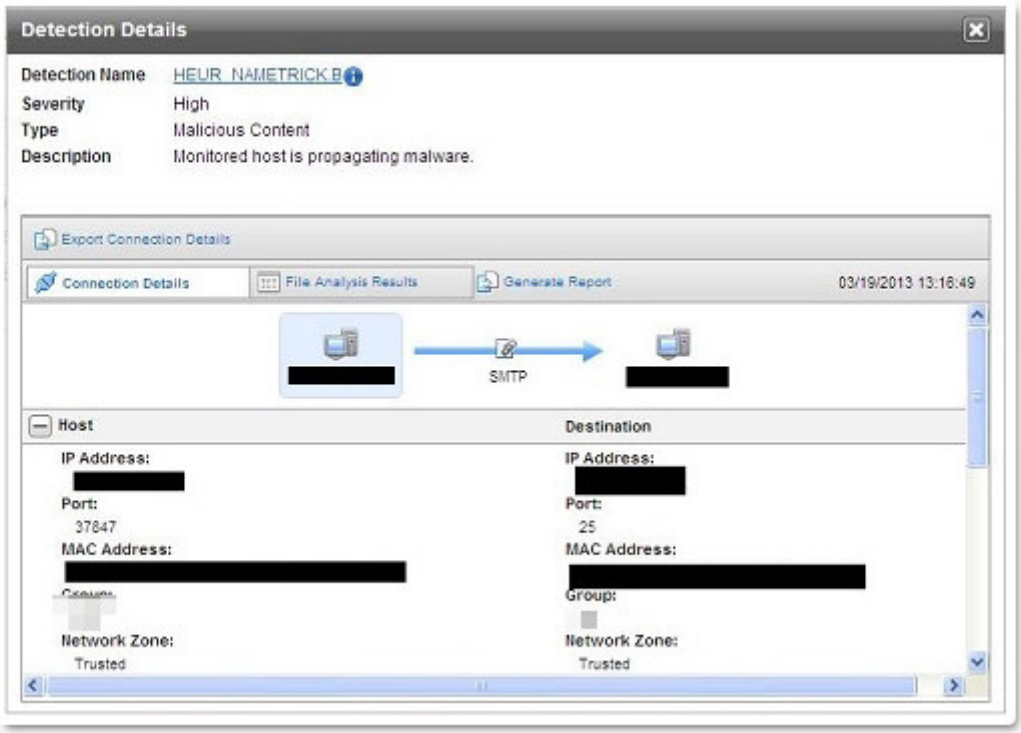
  这个MBR修改器，经趋势科技侦测分析，定名为TROJ_KILLMBR.SM恶意程序。该恶意程序被设定在2013年3月20日执行，在这个时间之前，它只是安静地存在在系统之中。当设定的时间到达之后，TROJ_KILLMBR.SM复写MBR并且自动重启系统，让此次破坏行动能够生效。它并且利用保存的登入信息尝试连接SunOS、AIX、HP-UX与其他Linux服务器，然后删除服务器上的MBR与文件。

  对于Windows Vista或是更新的版本，它会搜寻所有固定或移动硬盘中文件夹里的全部文件，用重复的单词去复写文件，然后删除这些文件与文件夹。在根目录的文件是最后被复写的。

  对于比Windows Vista旧的操作系统，它会复写所有固定或移动硬盘的卷引导记录（volume boot record）。

- **在3月20日之前有没有对于此次攻击事件的早期报警？**

  在一个趋势科技的客户环境中，我们能够判断至少在一天前，也就是3月19日，他们就已经遭遇了这个威胁。然而借由趋势科技威胁发现设备TDA的协助，他们能够提早知道并且采取防御措施。



- **趋势科技对于此次攻击事件提供什么保护？**

  趋势科技TDA利用侦测到相关邮件中的恶意附件，启发式侦测名称为HEUR_NAMETRICK.B，我们也提供特征码去查杀MBR修改器，同时我们能够侦测与此次攻击相关的所有URL与垃圾邮件信息。

- **趋势科技客户在此次事件中有受到影响吗？**

  趋势科技TDA能够利用启发式侦测与沙盒分析提示与此次攻击相关的邮件中的恶意附件。由于TDA提供的信息，客户能够提早采取预防措施，防止威胁影响他们的系统。