[趋势科技安全预警]

黑客攻陷韩国网络又一波　云端储存服务软件成黑客工具

借助自动更新系统分发恶意软件 建立僵尸军团

趋势科技建议企业及政府请尽快部署服务器异常检测策略

[趋势科技中国]– [2013 年 6 月 26 日] 韩国最高政治中心青瓦台网站于昨日遭受黑客攻击，导致网页被置换并瘫痪，引发全球关注。根据趋势科技全球病毒防治中心 Trend Labs 的最新研究发现，韩国云端储存服务软件“SimDisk Installer”服务器在此波攻击中疑似遭受黑客攻击并被植入名为“ SimDisk Installer exe. ”的恶意软件，其通过自动更新系统分发至用户端，试图造成大量的感染，成为受黑客控制的网络“僵尸军团”，进一步发动 DDoS 攻击以令更多政府网站瘫痪。

根据趋势科技 Trend Labs 最新分析发现，黑客攻击韩国云端储存服务厂商“SimDisk”的服务器并取得控制权后，即置换了名为“SimDisk exe.”的可执行文件，并透过自动更新系统散布一个名为“SimDiskup exe.”的恶意程序并分发至使用者端，一旦更新下载完成，此设备将遭恶意软件感染，该恶意软件会与特定网址链接并接收指令，并下载另一个为 DDOS_DIDKR.A 的恶意程序，以培养网络“僵尸军团” ，并运用这些受感染设备针对政府网站发动 DDoS 攻击，以瘫痪目标网站。

趋势科技中国区产品经理蒋世琪表示：“这次的攻击手法锁定了服务器存在的漏洞，在取得服务器控制权后方能通过核心系统，如自动更新系统可快速而广泛地分发至终端。我们强烈建议政府机构与企业应该重视服务器的安全维护，并同步进行自身 IT 信息安全能力检测，以避免成为此波或下波攻击的受害者。同时，当企业或一般消费者在下载使用这类免费软件前应审慎思考其安全性，才能将受被骇机率降到最低。”

面对黑客组织发动的全球性攻击，趋势科技建议云端服务商、企业与政府可加强对网络流量、Login 日志以及服务器等的监控，将企业内外部的信息流量与行为透明化，对企业内部的执行档案异常监控，并确保企业内服务器与 IT 系统都已经更新具备最新防护。

趋势科技将持续追踪韩国被攻击事件的最新发展状况，相关信息请参考：

http://blog.trendmicro.com/trendlabs-security-intelligence/compromised-auto-update-mechanism-affects-south-korean-users/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trendlabs+Security+Intelligence+Blog%29

更多趋势科技高级持续性威胁（ATP）信息请参考： http://www.trendmicro.com.cn/apt/