针对韩国的攻击中发现新的磁盘擦除工具

非官方中文译本•安天技术公益翻译组 译注

文档信息			
原文名称	New Disk Wiper Found in Korean Cyberattacks		
原文作者	Symantec	发布日期	2013 年 7 月 8 日
作者简介	Symantec 是一家总部设于美国加利福尼亚州库比蒂诺的互联网安全技术厂商，在全球有 40 个国家设有分公司。 http://en.wikipedia.org/wiki/Symantec		
原文发布单位	Symantec		
原文出处	http://www.symantec.com/connect/blogs/new-disk-wiper-found-korean-attacks		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
免责声明	本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

昨天，赛门铁克公布了关于一新的 DDoS 攻击的相关细节，此次攻击由黑客组织"DarkSeoul"向韩国网站发起。我们识别到该组织之前发起的针对韩国的攻击事件，包括 2013 年 3 月席卷韩国银行及电台电脑硬盘驱动的毁灭性攻击 Jokra。我们对于这一事件的持续调查偶然发现另一个威胁，并将其检测为 Trojan.Korhigh，该威胁试图执行类似的擦除行为。

与之前公开的针对韩国的 Wipers 恶意软件类似，Trojan.Korhigh 可以在被攻陷的机器上系统性地删除文件并覆盖主引导记录（MBR），致使机器无法使用。该木马接收增加功能的指令行，如将用户密码更改成"highanon2013"或执行下列文件类型相关的特殊擦除指令：

- asp
- aspx
- avi
- bmp
- dll
- do
- exe
- flv
- gif
- htm
- html
- jpeg
- jpg
- jsp
- mp4
- mpeg
- mpg
- nms

- ocx
- php
- php3
- png
- sys
- wmv

该木马还可能更改电脑桌面壁纸，以作为攻击的暗示。 此时，我们无法确认攻击者的身份。

图：Trojan.Korhigh 壁纸

该威胁还可能试图收集向以下 IP 地址发送信息的被攻陷机器的系统信息（如操作系统版本、计算机名称和当前日期等）：

- 112.217.190.218:8080
- 210.127.39.29:80

赛门铁克会持续分析这一威胁，并监控当前针对韩国的攻击事件。为确保安全，赛门铁克建议使用最新的赛门铁克技术并及时更新杀毒软件。