MBR 擦除工具攻击韩国电厂

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	MBR Wiper Attacks Strike Korean Power Plant		
原文作者	趋势科技公司	**原文发布日期**	2014 年 12 月 23 日
作者简介	趋势科技于 1988 年在美国加州成立。目前在 38 个国家和地区设有分公司，拥有 7 个全球研发中心。http://en.wikipedia.org/wiki/Trend_Micro		
原文发布单位	趋势科技公司		
原文出处	http://blog.trendmicro.com/trendlabs-security-intelligence/mbr-wiper-attacks-strike-korean-power-plant/		
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。

MBR 擦除工具攻击韩国电厂

2014 年 12 月 23 日

最近几个星期，一家主要的韩国电厂遭受了破坏性恶意软件的攻击，其目的是擦除受感染系统的 MBR（主引导记录）。研究人员认为，该 MBR 擦除工具通过一个常见的韩国应用程序 HWP（韩语文字处理器）进入目标系统。攻击者采用各种社会工程学诱饵文件，诱使可能的受害者打开这些文件。以下是攻击的概览，攻击者首先向雇员发送鱼叉式网络钓鱼电子邮件。

Infection Chain for MBR Wiper Attack

恶意软件行为

我们将该恶意软件命名为 TROJ_WHAIM.A，这是一个相当简单的 MBR 擦除工具。除了擦除 MBR，它还重写受感染系统中的特定类型的文件。它作为一个服务安装在机器中，确保它能够在每次系统重启时运行。该恶意软件相当聪明，它使用文件名、服务名，以及真实合法 Windows 服务的描述。这样，粗略的系统服务检查可能就无法发现任何恶意行为，从而帮助其规避检测。

Service Display Name	Service Name
BitLocker Drive Decryption Service	blockcom
Internet Connection Service	iconcom
Media Center Service	mcsvccom
Network Storage Service	nssvccom
Peer Networking Address	pnacom
PNRP Machine Name	pnrpcom
Power Policy	ppolcom
Program Compatibility Service	pcompcom
Remote Registry Configuration	rregcom
Smart Card Management Service	scardcom
Tablet PC Management Service	tpcmcom
Task Schedule Manager	tschcom
Thread Ordering Service	mmthcom
WebClient Manage Service	wcmngcom
Windows Color Adjustment	wndcolcom
Windows Modules Management	wndmodcom
Windows Time Synchronization	wndtimecom
Wired Config Service	wconfcom
WLAN Config Service	wlanconfcom
Workstation management	wstcom

图 1：TROJ_WHAIM.A 使用的合法服务名的列表

与之前 MBR 攻击的相似之处？

虽然这种特殊的 MBR 擦除行为并不常见，但是之前也出现过。2013 年 3 月，各个韩国政府机构遭受了严重的攻击，当时我们发现了这些例程。参与这次攻击的恶意软件用一系列单词（PRINCPES、HASTATI 或 PR!NCPES）重写 MBR。最近针对索尼电影娱乐公司的攻击也表现出类似的 MBR 擦除能力。

与之前的 MBR 攻击相比，此次的攻击有些相似之处。之前的三次攻击都用特定的重复字符串重写 MBR。此次攻击则使用重复的“Who Am I”字符串，而索尼攻击使用的是 0xAAAAAAAA 格式。

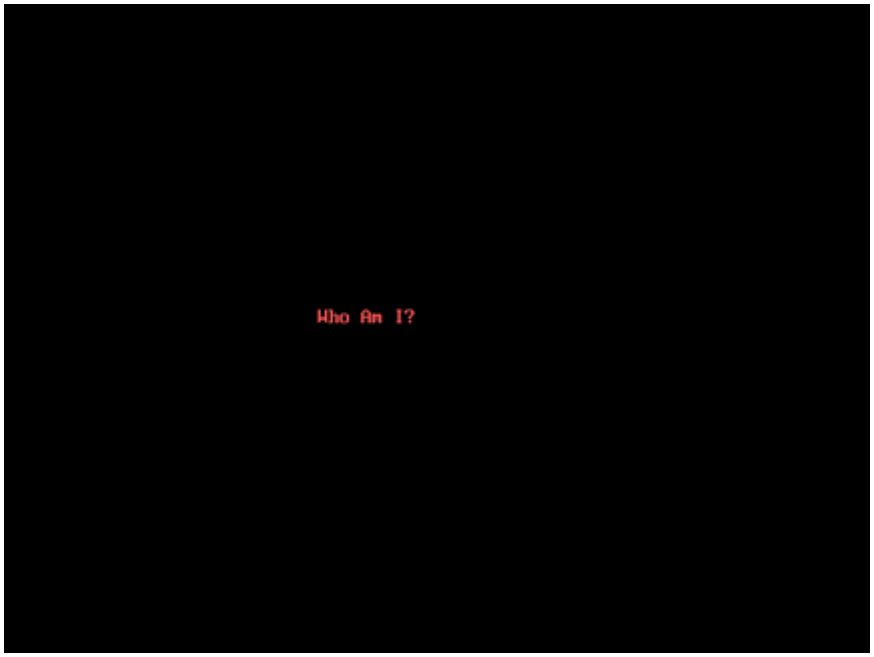

图 2：受感染系统启动时出现的“Who Am I”消息截图

破坏性恶意软件和要求

有人声称，索尼电影娱乐公司遭受攻击的原因是电影《采访》的上映。虽然我们无法核实这些说法的真实性，但是类似的事情也发生了。我们发现一个 Twitter 用户发布了对索尼电影娱乐公司的要求，声称如果不满足其要求，他就会发布各种 KHNP（韩国水电与核电有限公司）文件。其中的一个要求是关闭韩国的核电站（该核电站承担着 29%的韩国电力需求）。

无明确归属

虽然所有这些攻击有明确的相似之处，但是不能据此认为攻击的幕后黑手也相互关联。所有这三次攻击都有据可查，所以也有可能是这样的：每个攻击的幕后黑手从其他攻击中获得了“灵感”，但他们之间并没有什么关联。目前没有足够的证据，我们不能做出任何结论。

这些攻击说明，破坏性的 MBR 擦除恶意软件似乎已经成为很多攻击者的武器库的一部分。系统管理员将不得不应对这种威胁，而且并非所有的针对性攻击对策都会有效。应考虑把减轻此类攻击的技术作为纵深防御网络的一部分。

通过进一步的分析，我们证实了 TROJ_WHAIM.A 检查当前日期和时间是否为 2014 年 12 月 10 日上午 11:00 或更晚。如果符合这个条件，它就将注册表 HKEY_LOCAL_MACHINE\SOFTWARE\PcaSvcc\finish 设置为 1，从而触发 MBR 感染。否

则，它就会休眠一分钟，然后再次检查系统时间。

除了 MBR 感染和重写某些字符串，此次攻击与 2013 年 3 月事件的另一个相似之处是“定时炸弹”程序。一旦受感染的系统到达了攻击者指定的日期/时间，就会执行相应的操作。