朝鲜战争 63 周年之际针对韩国的 DarkSeoul 网络攻击仍在继续

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	朝鲜战争 63 周年之际针对韩国的 DarkSeoul 网络攻击仍在继续		
原文作者	赛门铁克公司	**原文发布日期**	2013 年 6 月 26 日
作者简介	赛门铁克公司是一家总部设于美国加利福尼亚州山景城的互联网安全技术厂商，创立于 1982 年 3 月 1 日，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	赛门铁克公司		
原文出处	http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war		
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、		

朝鲜战争 63 周年之际

针对韩国的 DarkSeoul 网络攻击仍在继续

赛门铁克公司

2013 年 6 月 26 日

昨天，6 月 25 日，朝鲜半岛出现了一系列与朝鲜战争 63 周年有巧合的网络攻击事件。虽然多起攻击事件都是由多个不同的网络犯罪分子所为，但是昨天查看的其中的一起针对韩国政府网站的 DDoS 攻击（分布式拒绝服务攻击）与 DarkSeoul 组织及 Trojan.Castov 有直接的关联。

现在，我们能够将多起之前发生的高调攻击事件，除去昨天的攻击之间之外，归结为 DarkSeoul 组织在过去 4 年中针对韩国所为。这些攻击事件包括：2013 年 3 月发生的毁灭性攻击 Jokra——消除了韩国银行及电视台中不计其数的计算机硬盘驱动器，以及 2013 年 5 月针对韩国财务公司的攻击。

对于 DarkSeoul 组织而言，执行 DDoS 攻击以及对关键历史日期进行硬盘清除并不是新鲜事。他们也曾在美国独立日那天对美国进行了 DDoS 攻击和清除攻击。

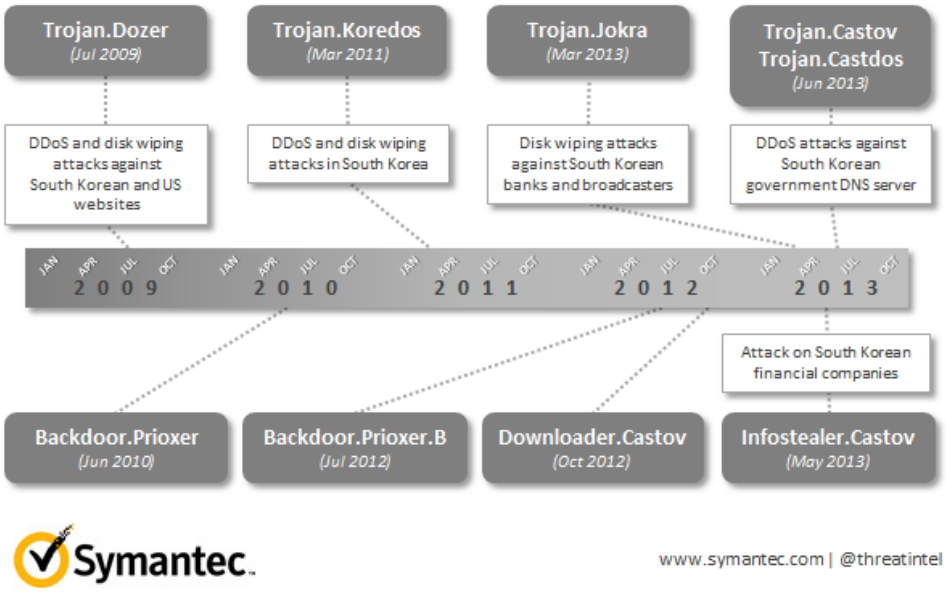

图 1：DarkSeoul 四年间的活动

- DarkSeoul 组织的攻击倾向于使用相类似的运行方法。其攻击特征包括：

- 针对韩国高调目标的多阶段、协同攻击
- 破坏性负载，例如配置为触发历史显著日期的硬盘擦除和 DDoS 攻击
- 以政治主题字符串覆盖磁盘各分区
- 利用合法的第三方补丁机制在整个企业网络进行传播
- 特定加密方法和混淆方法
- 利用特定的第三方网页邮箱服务器来存储文件
- 利用相似的 C&C 架构

这些由 DarkSeoul 组织所执行的攻击要求具有智能化与协调性，在某些案例中也说明了技术的成熟性。而国家的归属是不同的，韩国某媒体报道指出一项调查，总结了攻击者已朝鲜名义执行工作。Symantec 认为 DarkSeoul 攻击会持续下去，且不考虑该组织是否以朝鲜名义进行，这些攻击具有政治动机，也拥有所需的经济支持以持续进行在韩国组织的网络破坏行动。这些全国范围内的网络破坏攻击已经罕见—Stuxnet 与 Shamoon (W32.Disttrack)则是另外两个主要实例。然而 DarkSeoul 组织以其所具有的能力，十分独特，从而进行如此引人瞩目的攻击事件和数年的破坏性攻击。

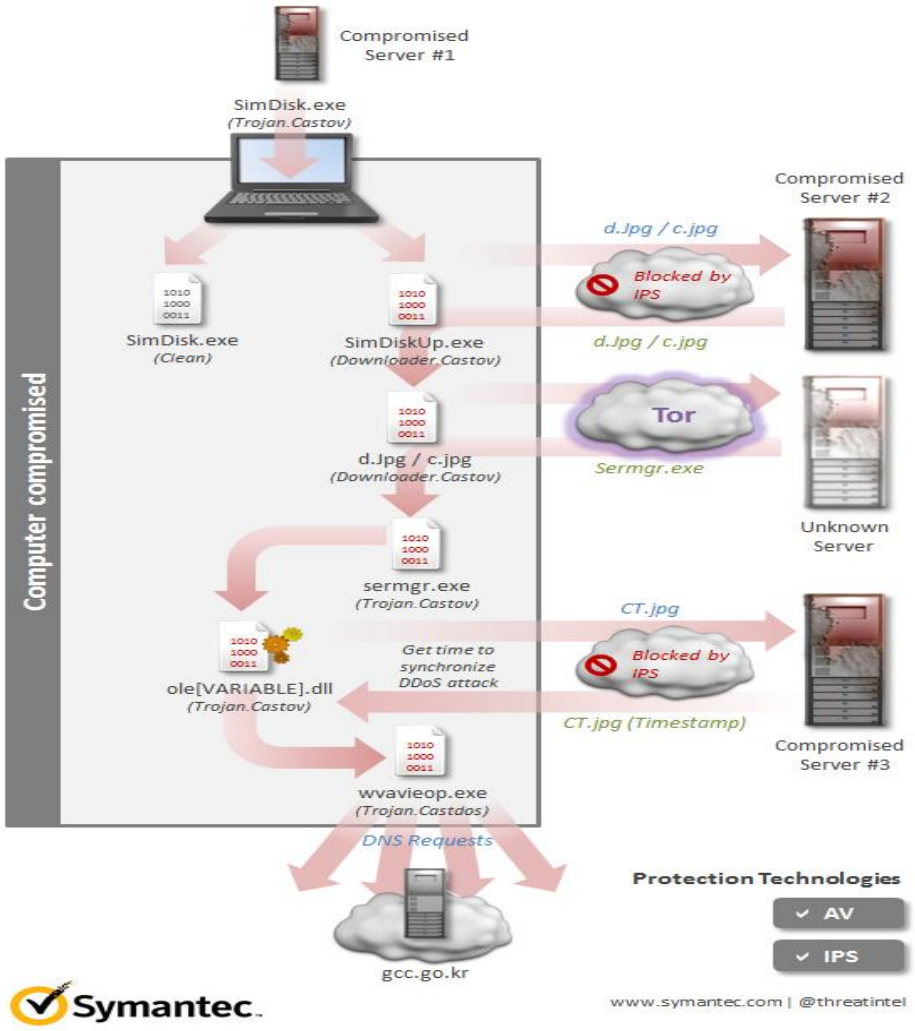

图 2：Castov DDoS 攻击

该 Castov DDoS 攻击采用以下方法：

- 被破坏的网站会导致下载 SimDisk.exe (Trojan.Castov)，一个合法的应用 Trojanized 版本。
- SimDisk.exe 将 2 个文件投放到被破坏的系统上：SimDisk.exe (Clean)，该合法的非 Trojanized 版本，和 SimDiskup.exe（下载器 Castov）。
- 下载器 Castov 连接到一个二次破坏的服务器，下载 C.jpg 文件（下载器 Castov），一个以图片形式呈现的执行性文件。
- 威胁使用 Tor 网络，从而下载 Sermgr.exe (Trojan.Castov)。
- Castov 会在 Windows 系统文件夹中投放 Ole[VARIABLE].dll 文件(Trojan.Castov)

- Castov 会从网站服务器上下载此 CT.jpg 文件，提供一个 ICEWARP 网页邮件，由于 ICEWARP 公开的漏洞受到迫害。该 CT.jpg 文件包含一个由 Castov 使用的时戳，从而使得攻击同步进行。
- 一旦时间到，Castov 会投放 Wuauieop.exe (Trojan.Castdos)。
- Castdos 开始按照 DNS 的要求下载 Gcc.go.kr DNS 服务器，有效的进行 DDoS 攻击，影响多个网站。