预警编号：YJ-2017012

恒安嘉新

关于“暗云 III“木马传播感染情况

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 06 月 12 日

1 木马简介

“暗云”系列木马自 2015 年初被发现并查杀，至今已有 2 年多。在这两年多时间里，该木马不断更新迭代，持续对抗升级。从今年 4 月开始，该木马卷土重来，再次爆发，本次爆发的暗云木马相比之前的版本有比较明显的晋级特征，命名为暗云Ⅲ。暗云Ⅲ与之前版本相比有以下特点和区别：

第一、更加隐蔽，暗云Ⅲ依旧是无文件无注册表，与暗云Ⅱ相比，取消了多个内核钩子，取消了对象劫持，变得更加隐蔽，即使专业人员，也难以发现其踪迹。

第二、兼容性，由于该木马主要通过挂钩磁盘驱动器的 StartIO 来实现隐藏和保护病毒 MBR，此类钩子位于内核很底层，不同类型、品牌的硬盘所需要的 hook 点不一样，此版本木马增加了更多判断代码，能够感染市面上的绝大多数系统和硬盘。

第三、针对性对抗安全软件，对安全厂商的“急救箱”类工具做专门对抗，通过设备名占坑的方式试图阻止某些工具的加载运行。

	暗云	暗云II	暗云III
发现时间	2015年1月	2016年4月	2017年4月
驻留方式	MBR	MBR	MBR
内核特征	CmpCallback 对象劫持 StartIO钩子	dpc timer 对象劫持 StartIO钩子 Scsi钩子 object钩子	dpc timer StartIO钩子
shellcode下载方式	向应用层插入apc联网下载，完成后通过RegSetValue传回内核	直接在内核下载	直接在内核下载
MBR保护方式	StartIO钩子	StartIO钩子 Scsi钩子 object钩子	StartIO钩子
对抗守护	关闭杀软设备句柄	patch杀软dll入口	占坑对抗急救箱工具
主要变现方式	恶意推广 锁主页	网络攻击 刷流量	网络攻击 刷流量

图 1 暗云版本历史特点

2 木马运行原理

“暗云“系列木马通过感染磁盘 MBR 来实现开机启动，三代”暗云“其启动过程，基本没变，都是由 MBR 开始通过 int 15 中断一步步的 hook 来跟随系统的引导流程进入系统内核执行，该套代码可兼容 xp、vista、win7、win8 等主流操作系统，包括 64 位和 32 位。

其启动过程如图所示：

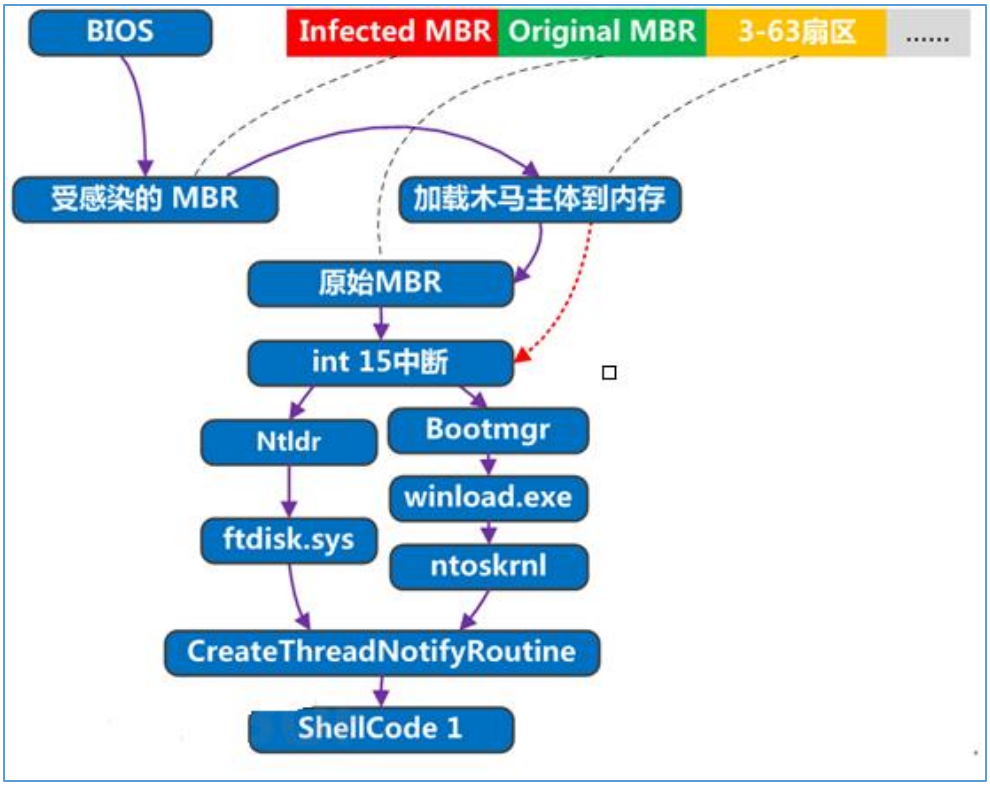

图 2 “暗云 “系列 BootKit 启动过程示意图

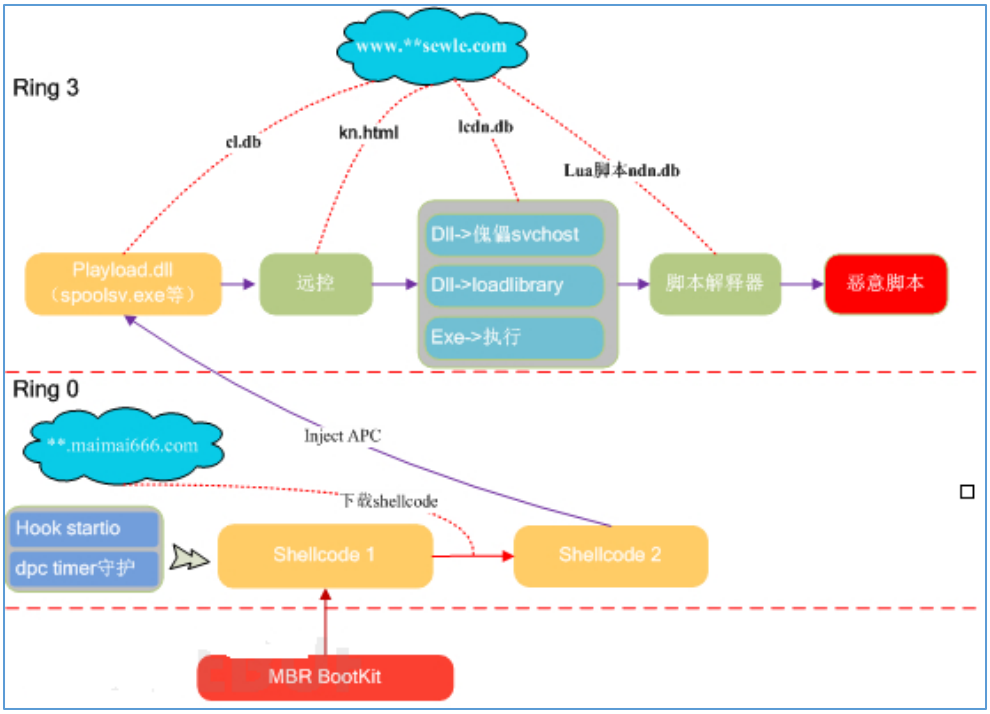

图 3 暗云 “Ⅲ木马启动流程图

3 影响范围

截止 6 月 12 日，累计发现全球感染该木马程序的主机超过 162 万台，其中我国境内主机占比高达 99.9%，广东、河南、山东等省感染主机数量较多。同时，CNCERT 对木马程序控制端 IP 地址进行分析发现，“暗云Ⅲ”木马程序控制端 IP 地址 10 个，控制端 IP 地址均位于境外，且单个 IP 地址控制境内主机数量规模均超过 60 万台。

根据监测结果可知，目前“暗云Ⅲ”木马程序控制的主机已经组成了一个超大规模的跨境僵尸网络，黑客不仅可以窃取我国百万计网民的个人隐私信息，而且一旦利用该僵尸网络发起 DDoS 攻击将对我国互联网稳定运行造成严重影响。

4 修复建议

“暗云“Ⅲ木马主要通过外挂、游戏辅助、私服登录器等传播，此类软件通常诱导用户关闭安全软件后使用，使得木马得以乘机植入。建议持续保持安全软件开启状态，不要运行来源不明和被安全软件报毒的程序。

专杀工具：

http://guanjia.qq.com/act/webpublish/12/index.html?ADTAG=innerenter.gj.index.pubu#h_3