AhnLab

安全月刊

2020.03 Vol.88

MyKings Botnet

MyKings僵尸网络详细分析

觊觎服务器的MyKings僵尸网络真实面目

从2018年中期开始，在基于Windows的服务器上，不断检测到挖矿恶意代码（Coin Miner）或防病毒软件不能正常运行等事件不断增加。AhnLab安全应急响应中心（AhnLab Security Emergency response Center, ASEC）的分析师和数字取证团队A-FIRST（Ahnlab Forensic & Incident Response Service Team）在服务器上发现篡改主引导记录（MBR）的Bootkit恶意代码。而且确认了该Bootkit恶意代码会在受感染系统上安装挖矿恶意代码，使其系统再次感染。随后的详细分析中，发现这些恶意代码是从2015年5月起在韩国活跃，被称为MyKings僵尸网络（MyKings Botnet）。下面我们将详细了解关于近期活跃于韩国的MyKings僵尸网络的主要恶意代码、感染症状和攻击方式。

MyKings僵尸网络也被称为DarkCloud、Hidden、Smominru等，首次发现于2014年8月。在韩国，最早确认于2015年5月。此后，该僵尸网络一直持续而又相对低调地活动，2018年中期以后，开始出现活跃迹象。2016年11月，AhnLab在分析韩国一家企业的数字证书签名的恶意代码的过程中，确认了与MyKings僵尸网络有关的情况。

此后，从2018年中期开始，在韩国大学、协会、媒体、制造、金属、解决方案服务、网页寄存等多种产业领域，持续发现了反复感染挖矿恶意代码（Coin Miner）、防病毒软件故障、Bootkit恶意代码等看似不同实则类似的案例。AhnLab对这些看似独立的案例分析后得出结论，所有案例均为同一组织所为。那便是MyKings僵尸网络。

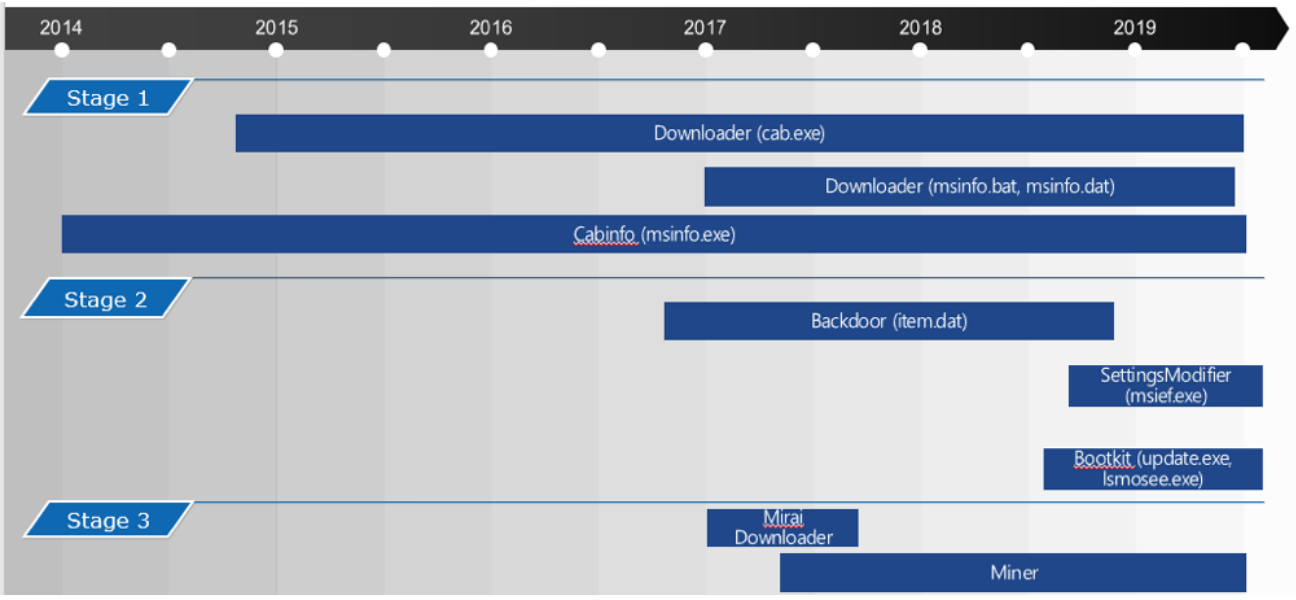
时期	攻击对象	时期	攻击对象
2015 年 5 月	购物	2018 年 12 月	网页寄存
2016 年 11 月	运输、大学、媒体	2019 年 1 月	大学
2017 年 4 月	开发院	2019 年 2 月	解决方案服务及流通
2017 年 7 月	饮料制造	2019 年 6 月	制药
2018 年 7 月	金属加工及金属制造	2019 年 6 月	信息技术解决方案
2018 年 12 月	解决方案服务及流通	2019 年 12 月	媒体、大学、学术

[表 1] MyKings 组织攻击事件（韩国案例）

与此相关，AhnLab在安全应急响应中心（AhnLab Security Emergency response Center, ASEC）以最近在韩国确认的MyKings僵尸网络攻击为中心， 发表了有关入侵症状、主要恶意代码和篡改证书等攻击方式的分析报告。下面来了解MyKings僵尸网络的特征和攻击手段。

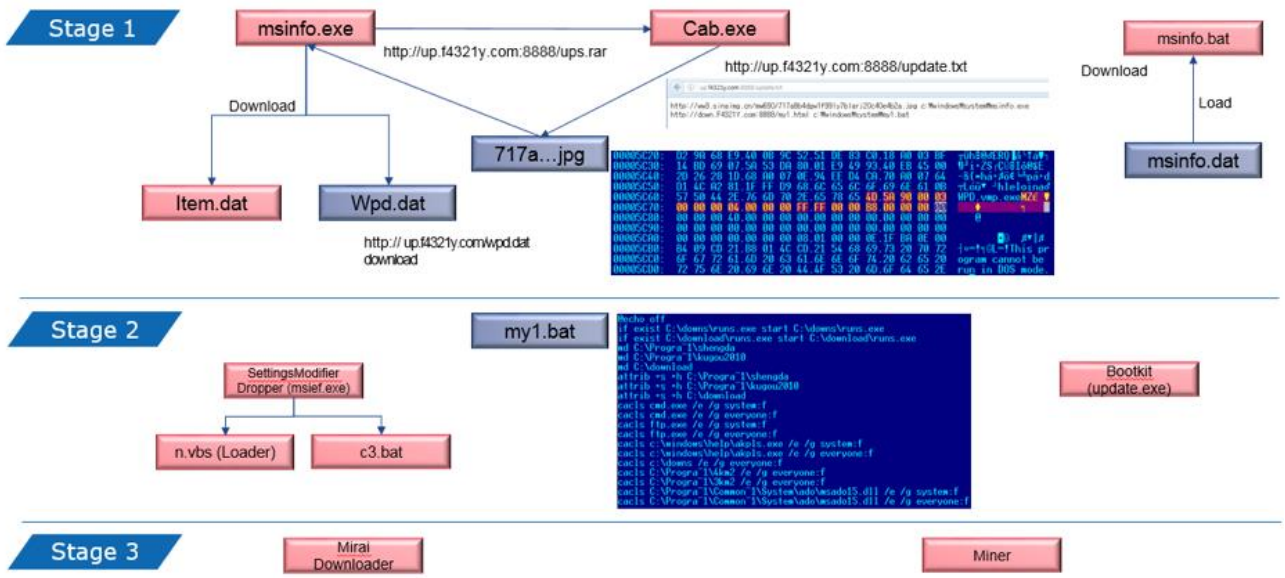
MyKings 僵尸网络进行攻击的过程

截至2020年2月，已确认MyKings僵尸网络使用电子邮件攻击、易受攻击的SQL服务器攻击和永恒之蓝（EternalBlue）攻击等方式。在此过程中，伪造或盗用正常程序的证书来制作并分发恶意代码。以这种方式入侵企业及机构内部后， 分三个阶段进行攻击。



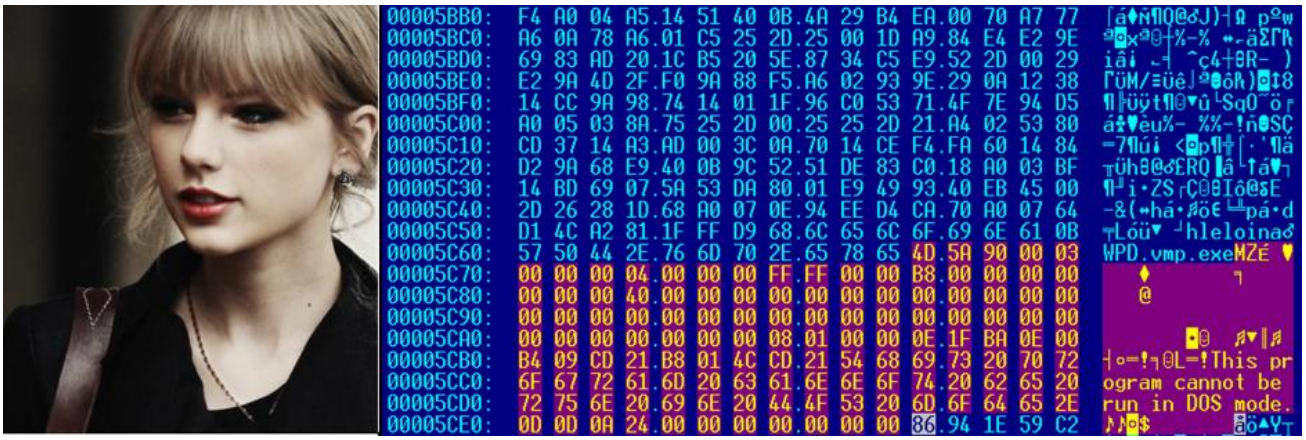
[图1] MyKings僵尸网络的攻击阶段摘要

MyKings攻击始于下载其他恶意代码的下载器（Downloader）或Cabinfo文件。在攻击的第一阶段使用的恶意代码可分为msinfo.exe和cab.exe 。msinfo.exe下载cab.exe， 其中大部分都与VMProtect打包在一起， 因此很难掌握正确的功能。但可以推测的是， 它具有连接到易受攻击的SQL服务器并泄露信息的功能。最近， 还确认到未使用msinfo.exe和cab.exe的案例。



[图 2] MyKings 僵尸网络主要文件的关系图

如[图2]所示，cab.exe从下载列表中下载文件。此时， 下载的JPG文件看起来像是普通的著名歌手的照片，但实际上文件后面存在可执行代码（参见[图3]）。提取该可执行代码以生成msinfo.exe。



[图 3] 著名歌手泰勒·斯威夫特的照片（左）文件后面的可执行代码（右）

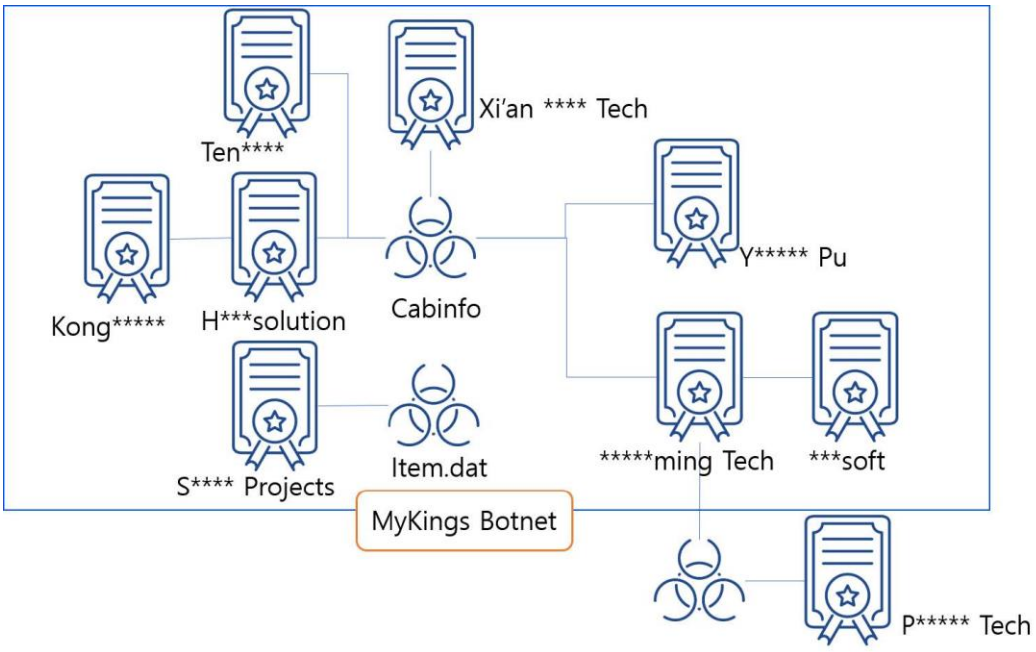
在攻击的第二阶段，将安装其他系统设置更改和引导程序包（Bootkit）。在该组织的活动早期，诸如cab.exe之类的文件直接下载了系统更改文件，但是最近，开始下载RAR SFX文件形式的msief.exe文件（包括更改系统设置的c3.bat文件）。它通过利用Bootkit尝试禁用安全程序，例如在感染系统上安装的防病毒软件（Anti-virus）。

Bootkit早在2018年8月就已被发现，并主要使用“lsmosee.exe”、“max.exe”和“update.exe”等文件名。文件用各种打包程序打包，文件长度从655,328字节到15,038,553字节（通常为680KB）不等。

在攻击的最后阶段，尝试安装最终目标——挖矿恶意代码(Coin Miner)。在2017年，有一起案例专门寻找易受攻击的嵌入式Linux系统并感染 Mirai下载器（一种典型的IoT恶意代码）。

伪造和盗用多个合法程序的证书

MyKings僵尸网络组织窃取正常数字证书的密钥文件或复制证书内容后，证书被伪造和盗用，并被用于PUP、下载器、键盘记录器、Bootkit等的恶意代码签名。证书还被用于与赌博性游戏相关的文件签名。AhnLab的分析结果显示，截至2020年2月，共有9个证书被伪造或盗用。但是，复制和伪造正常证书内容时，由于证书信息和文件信息不一致，因此信息显示为异常文件。



[图 4] 被盗用的 9 个证书及其关联性

被盗用数字证书的9家企业（参见[图4]）当时采取了吊销证书等适当的措施。尽管如此，MyKings僵尸网络组织至今仍在将这些证书用于恶意代码签名。例如，西安****技术（Xi’an ****Tech）的数字证书在2016年被盗用后就采取了吊销措施，但仍被盗用于7,300多个恶意文件签名。最近，它主要用于挖矿恶意代码（Coin Miner）。

如何辨别 MyKings 僵尸网络造成的入侵?

由MyKings僵尸网络造成的入侵通常会出现以下症状。

反复感染或妨碍安全防护产品正常运行

篡改MBR
存在特定名称的可疑文件
连接特定URL
文件名与正常文件的名字不同（cacls.ext -> download.exe）

首先， 尝试登录到SQL服务器。攻击者利用随机代入法尝试连接SQL服务器， 在此过程中， 由于代入错误的登录信息，因此会发生大量的登录尝试。

其次，反复感染挖矿恶意代码。因为Bootkit会下载挖矿恶意代码，所以如果在受感染的系统上安装了防病毒软件，则会连续检测到挖矿恶意代码。

第三，会发生防病毒软件的实时监控功能中断或无法更新引擎等问题。此外，引入系统的Bootkit检查是否安装了特定的防病毒软件，并尝试使其失效。由于Bootkit是在系统启动时自动运行的，因此它会在防病毒软件运行之前运行，并禁用防病毒软件。

第四，篡改MBR 。但是，如果恶意代码正在运行， 它将显示为正常的引导记录，因此在被感染的状态下，很难确认MBR是否已被篡改。然而， MyKings僵尸网络组织大部分倾向于使用几乎相似名称的文件。因此，如果系统上存在Cab.exe、item.dat、msinfo.exe、msief.exe、c3.bat、n.vbs、update.exe等文件 ， 就很有可能已感染了MyKings僵尸网络恶意代码。

第五，访问特定海外服务页面的URL。

最后，会发现陌生名称的Windows系统文件。已确认的有cacls.exe或download.exe。

MyKings 僵尸网络，为什么要注意?

在大部分攻击事例中，最终都安装了挖矿恶意代码，从这一点来看， MyKings僵尸网络很有可能是单纯以金钱为目的活动的组织。但是， 考虑到盗用和窃取正常数字证书并用于制作恶意代码， 不能排除随时会窃取企业及机构内部信息的可能性。这就是为什么AhnLab和其他主要安全防护企业自2018年以来一直在关注该组织的活动。

尤其是，由于MyKings僵尸网络攻击Windows服务器（MS SQL服务器），因此企业及机构有必要及时了解该组织的最新攻击信息。另外，经常检查内部系统是否反复感染挖矿恶意代码或防病毒软件出现错误等症状也很重要。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com