原文地址:http://drops.wooyun.org/papers/8790

微信公众号:Antiylab

0x01 概述

近期，安天第三代蜜罐捕风系统捕获到一个下载者样本。该样本运行后访问一个由黑客搭建的轻型文件服务器（Http File Server）。通过使用捕风系统进行追溯与关联分析，分析人员发现目前有很多使用HFS搭建的服务器，通过对其中一个下载服务器进行监控，其在线6天的总点击量近3万次，可见其传播范围极广。该软件的“傻瓜式”教程颇受低水平的攻击者喜爱，同时由于其架设方便，便于传播等特点，已被黑客多次恶意利用。经过安天CERT分析人员进行关联与分析发现，目前这种轻型服务器工具已普遍流行。

1. **样本标签**

病毒名称	Trojan[Downloader]/Win32.Agent
原始文件名	无
MD5	A52B473888FA975D37048D5959533001
处理器架构	X86-32
文件大小	180KB(184427Bytes)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2015-08-29
数字签名	无
加壳类型	未知壳
编译语言	Microsoft Visual C++ v6.0

图1 样本标签

黑客利用弱口令入侵MySQL数据库服务器后使用MySQL指令建立表，并新建变量，将可执行二进制码写入变量并插入表中，然后将表中的可执行二进制文件Dump到数据库服务器中，最后执行文件。这种手法也是黑客入侵数据库惯用的手法。

该样本运行后动态获取自身代码，随后进行提权操作，关键功能为枚举杀毒软件金山卫士进程名KSafeTray.exe。如果存在此进程，则终结进程。

图3 杀掉金山卫士进程

恶意代码连接服务器（IP：118.193.:1010）

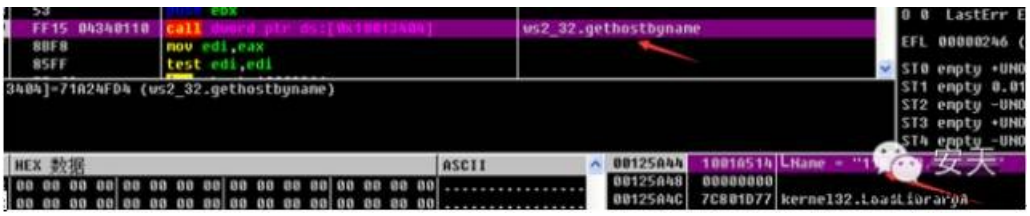


图4 联网操作

当恶意代码连接该服务器端口时，服务器端口失效。而在安天CERT分析人员连接该IP时发现一个轻型服务器，

上面有一个恶意代码(1010.exe)

2. **服务器样本分析**

病毒名称	Trojan[Downloader]/Win32.Agent
原始文件名	1010.exe
MD5	FF5ED4E0F8A968643F49E1FDF1D76338
处理器架构	X86-32
文件大小	80.0 KB (81,988 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2015-08-29
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C++ 6.0

图5 样本标签

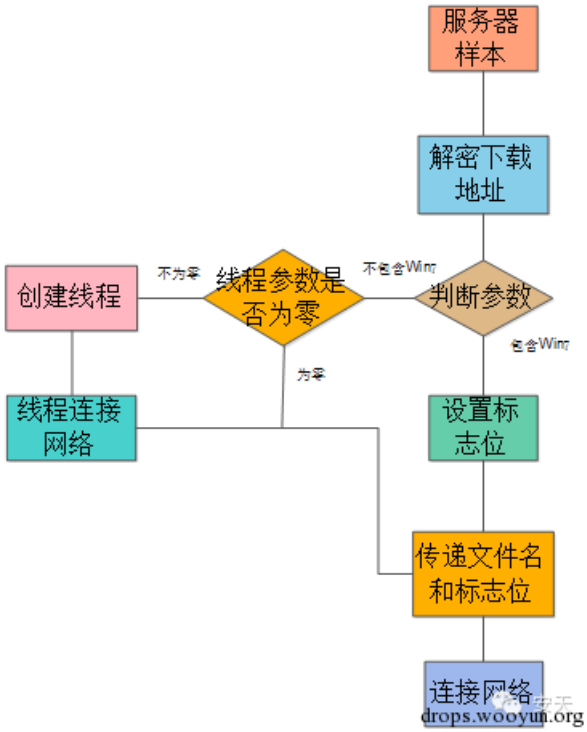


图6 服务器样本流程

该黑客服务器上线不到2个小时即被安天CERT捕获到。该样本首先解密下载服务器的地址，随后判断该样本是否带参数运行及参数是否包括“Win7”字符串，如果不包括或者不带参数运行则进入创建具有下载功能的线程，进入创建线程时判断传递给线程的参数是否为空，如果不为空则进入线程创建过程，如下图所示。

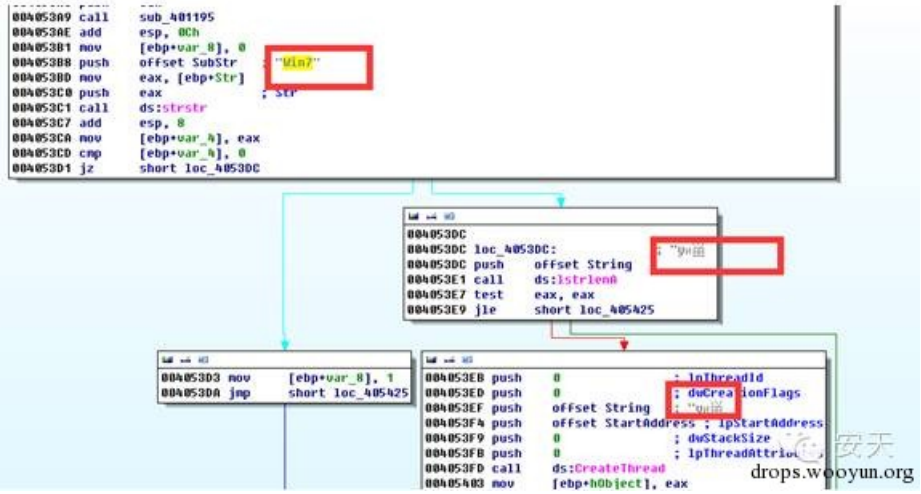


图7 创建线程流程

恶意代码进入线程后，将参数字符串（实际为连接服务器的地址）传递给连接服务器函数。该线程负责下载其他恶意代码。

如果恶意代码带参数且包含“Win7”字符串时，则恶意代码直接跳过线程代码创建过程，将文件名称和标志位传递给连接服务器函数，随后进行重新连接该服务器地址，重新下载1011.exe文件并保存在C:\Windows\AppPatch目录下起名为“mysqld.dll”运行。

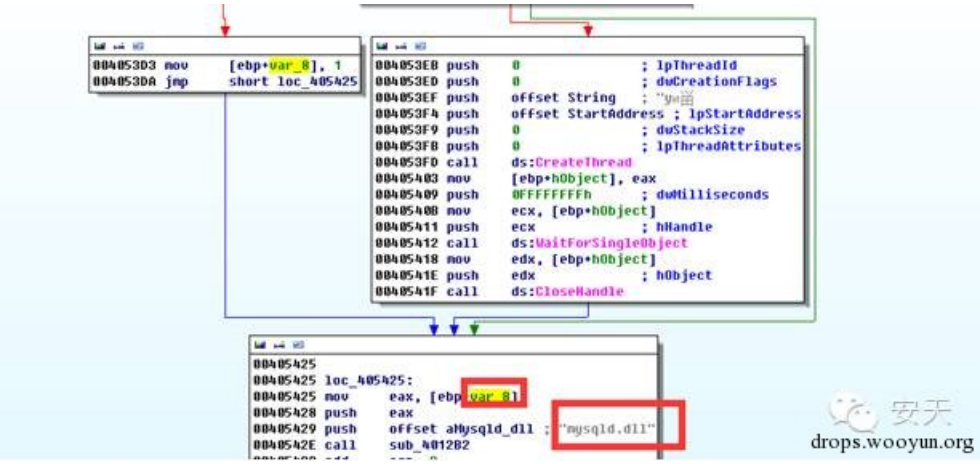
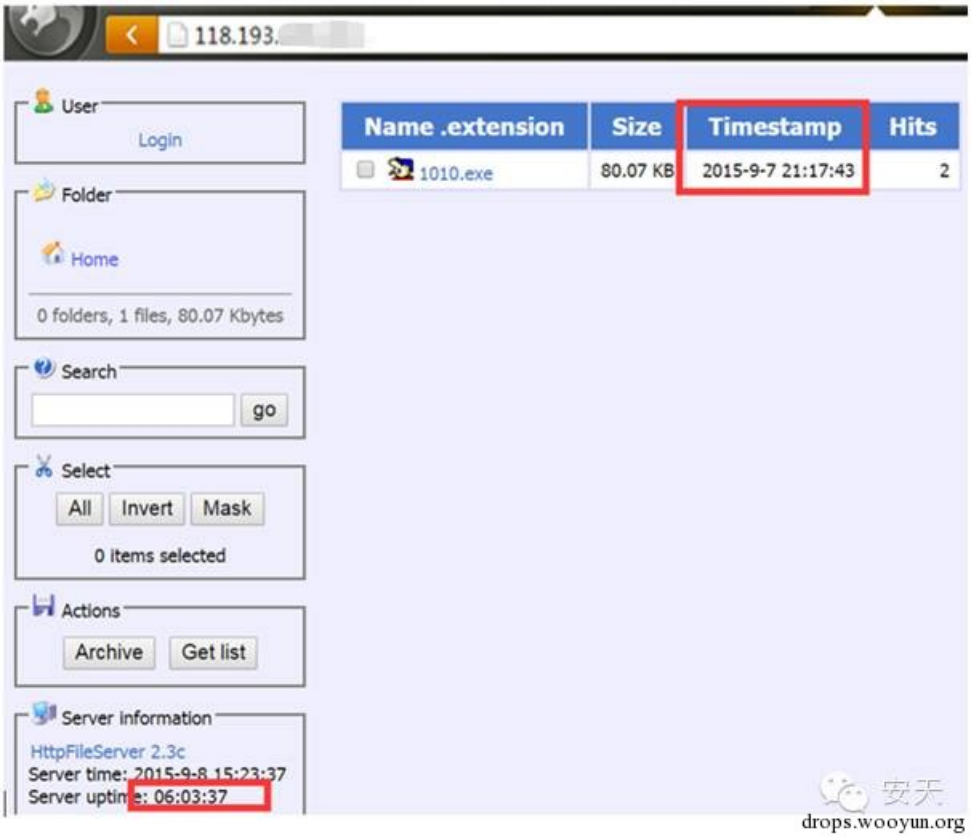


图8 带参数运行流程

该服务器于9月8日刚刚上线，感染速度日趋增长，如下图所示：

IP地址：118.193..（香港特别行政区中国电信沙田国际数据中心）



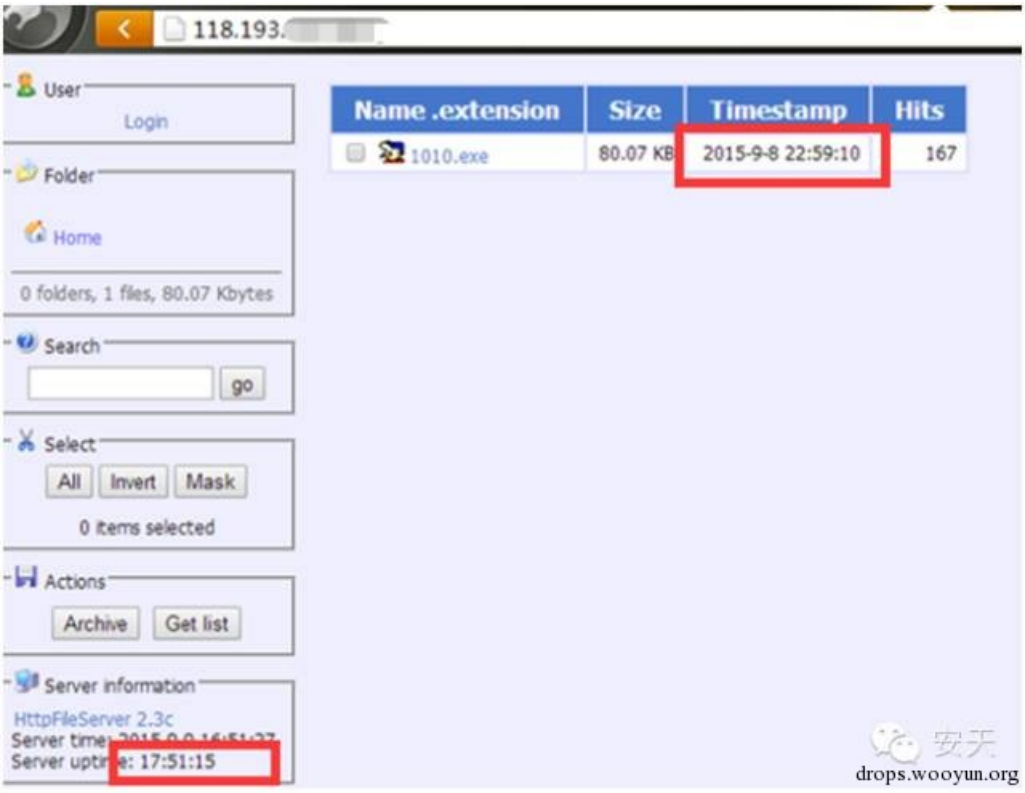


图9 服务器上线一天的点击量

0x02 关联类似服务器

通过进一步关联分析，发现在安天蜜罐系统中另一个样本所链接的地址也是使用Http File Server搭建的服务器。服务器域名为qj0..，对此安天CERT对该域名进行几天跟踪发现该域名更换过4次IP（如下图所示），且服务器均为阿里云提供。采取动态域名、利用阿里云提供服务器，这两个手法相互结合更加提高了恶意团伙的隐蔽性。黑客购买了多个阿里云服务器用来传播恶意代码，且时常更换IP，并用IP绑定其他域名等方式来扩大恶意代码传播范围，同时将自己隐藏的更深。

图10 域名频繁更换阿里云服务器

图11 恶意服务器点击量

恶意服务器定期更新恶意代码，并且感染量增长较快。

服务器恶意代码病毒名统计如下：

样本名称	上传日期	点击量	MD5	病毒名
is.war	2015-8-15 10:27:48	291	5F0926A42D2F1042013F45A2B755699E	Trojan[Backdoor]/Java.JSP.l
syn20160	2015-8-18 19:53:40	926	1D3C681B99B98F0D8DDE23758DD98C07	Trojan[Backdoor]/Linux.Ganiw
win.exe	2015-8-18 19:58:16	88	28ACC38A08B44B76EA85A0853961EBC9	Trojan/Win32.Reconyc.esql
xxa.exe	2015-8-28 18:24:56	272	31ED5DBFF8EFB9D61C68084FC3F20E22	Trojan[Backdoor]/Win32.Farfli
Zesr68f4.dll	2015-9-30:12:34	573	8A65DB08D158060F60DF68732FB34D84	Trojan/Wir[illegible]Generic

安天CERT于9月7日捕获到了另外一种类似恶意代码下载服务器地址，该服务器在捕获的时候点击量已经近万。服务器上的软件几乎均为恶意代码，恶意代码功能多为后门和下载者，恶意代码功能列表详见下方表格。

图12 恶意服务器

安天CERT分析人员跟踪该服务器一周时间发现，总点击量呈线性增长，几乎每天增加3000的点击量。如下图所示：

图13 服务器点击量日趋势

服务器恶意代码病毒名统计如下：

样本名称	上传时间	点击量	MD5	病毒名
1433.exe	2015-8-1 17:16:43	218	cc2b9684dc95ea70f052eb8a3902b0ad	Trojan[Downloader]/Win32.Agent
3306.exe	2015-8-3 15:22:57	229	40d70745cfcdc0574d0a6982362f1c7d	Trojan[Downloader]/Win32.Agent
arp.exe	2015-8-8 10:27:54	536	6ff1142bb5b0dc40f1a37dd1cbf53e80	Trojan[Downloader]/Win32.Agent
bc12345.exe	2015-8-6 17:46:38	2572	ab34251ccfcc60005c7b3a294040e4cd	Trojan[Downloader]/Win32.Agent
cr.exe	2015-8-7 16:30:55	143	303ff8794e5c6f32870ed55c33573e7b	Trojan[Downloader]/Win32.Agent
gott.exe	2015-7-30 19:20:31	23	c7e9e5566cf3428e25e07868f44fd19c	Trojan[Backdoor]/Win32.Farfli
moqujie.exe	2015-8-14 9:18:53	19525	25c72c1e994f3efec4a1b555d36ef4a4	Trojan[Downloader]/Win32.Agent
moke8.exe	2015-8-8 9:29:24	1018	67b2dbedd5a258258baab0094e278f96	Trojan[Downloader]/Win32.Agent
mp4fixtool.exe	2015-8-10 16:30:59	351	f005589add550804017349d7a21aa633	Trojan[Downloader]/Win32.Agent
NetSyst81.dll	2014-10-25 13:48:02	214	0b156ec492ea45d282cf823415ecaf12	Trojan/Win32.Agent
scvhost.exe	2015-7-30 19:20:31	373	c7e9e5566cf3428e25e07868f44fd19c	Trojan[Backdoor]/Win32.Farfli
win2003.exe	2015-8-28 16:23:44	34	e8aa9941e88fb172d9a470973834b4c0	Trojan[Downloader]/Win32.Agent
windowsupdate.exe	2015-8-6 9:34:48	28	fc8ee42d829dcc9a12cbe528b6a5f7f4	Trojan[Downloader]/Win32.Agent
yiqig.exe	2015-8-8 10:25:28	313	f1fbf62e7f04f9e7e223c64e78ff9a99	Trojan[Downloader]/Win32.Agent
yvmp4.exe	2015-8-14 9:18:53	509	25c72c1e994f3efec4a1b555d36ef4a4	Trojan[Downloader]/Win32.Agent

安天分析人员通过跟踪与挖掘发现，目前这种黑客服务器非常常见，如下图所示：

图14 恶意服务器

图15 恶意服务器

0x03 总结

目前，随着“黑色产业”的巨大经济利益诱惑，商业化的黑客工具包的使用变得越来越流行。这种能够“短平快”地产出恶意代码的方式让新手的入门门槛越来越低，一个没有经验的新手通过短时间的工具学习，就能轻松掌握入侵计算机窃密的方法。不仅仅是黑客工具，就算是一个普通的，用于构建正常服务的工具也能被轻易地被黑客利用，比如，轻量

级Http服务器（Http File Server）正以其架设方便、便于操作等特点受到越来越多用户的青睐。与此同时，黑客也能利用在云端搭建轻型服务器与使用动态域名相结合的手段使得恶意代码能够更广泛、隐蔽地传播。这种轻量、便捷的服务器工具将会被越来越多的黑客或者新手使用，这无疑会加速恶意代码的传播。

这种工具式的黑客技术，让恶意代码的生产周期变的更短。依托商业工具进行攻击降低了攻击成本，同时提高了检测难度和传播速度。这种难度小、门槛低、成本少的攻击手法将使互联网的黑色产业链变得更加鱼龙混杂，同时也给互联网安全带来更多的挑战。

博客地址