Silence：针对银行的APT攻击

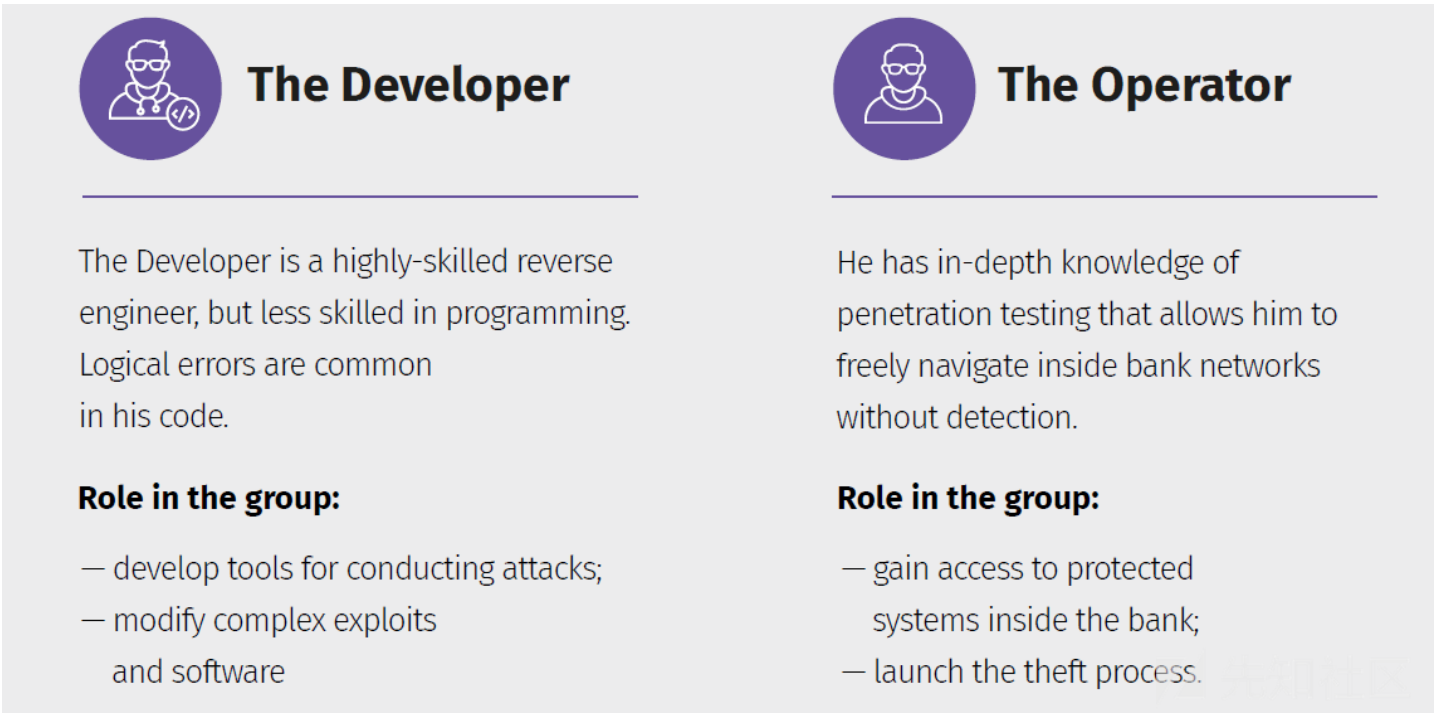
angel010 / 2018-09-09 20:13:11 / 浏览数 3829 技术文章 技术文章 顶(0) 踩(0)

Silence是一个新的活跃的APT组织，会自己开发攻击工具，同时会借鉴其他组织的TTPS。主要攻击目标是银行等金融组织。

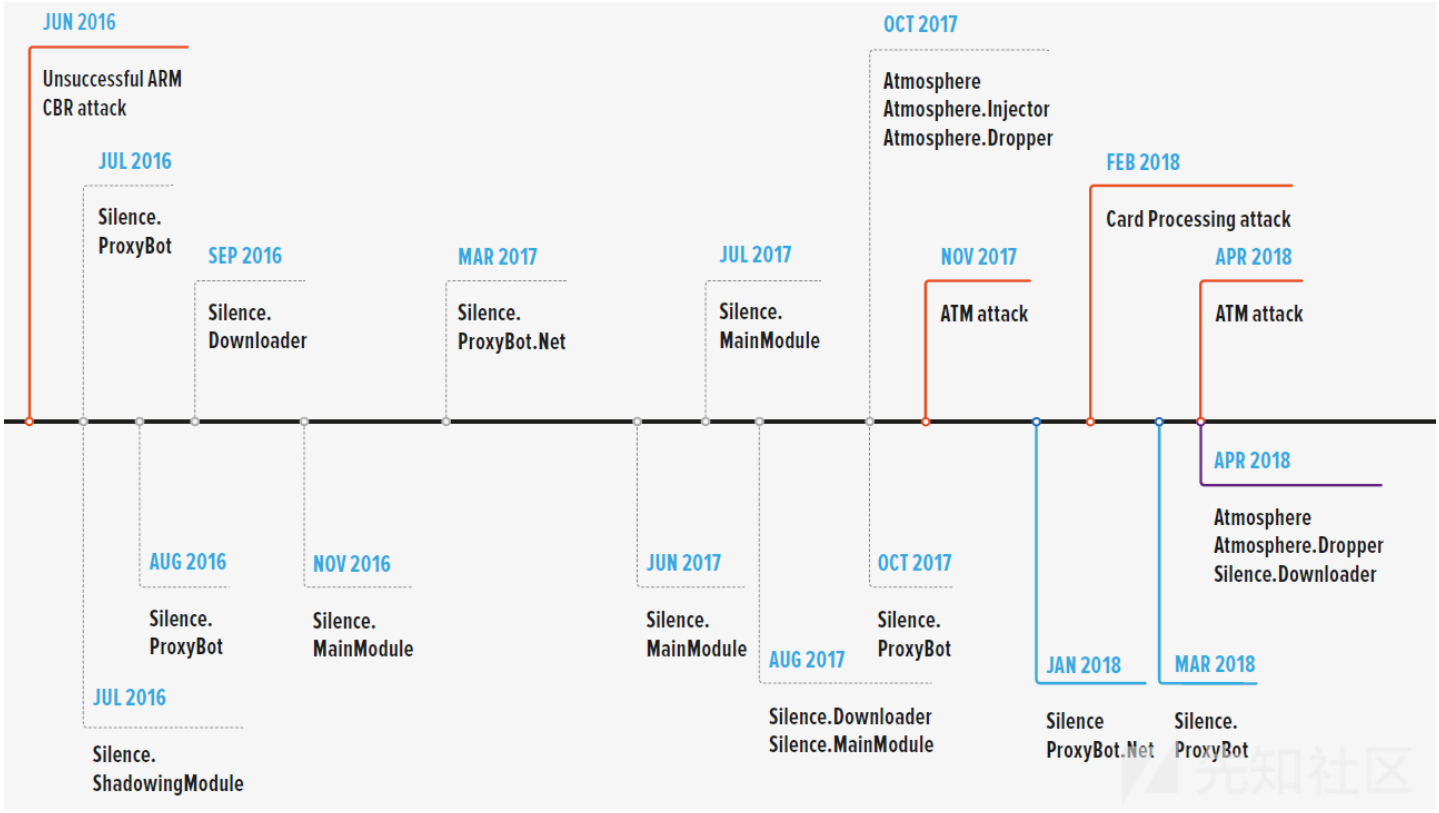
Silence group

Group-IB
2016年7月检测到Silence相关的第一起事件。那时攻击者应该才开始测试软件的共那个。Silence的第一个目标是俄罗斯银行，因为攻击者会尝试攻击AWS CBR。之后，黑客沉默了一段时间，这也是Silence的标准实践方式。

研究人员分析发现Silence团队有两个角色，分别是运营者和开发者。运营者应该是team leader，具体负责渗透测试，对银行系统渗透测试工具有深入的了解。开发者是经验丰富的逆向工程师，负责开发执行攻击的工具，并能够修改复杂的漏洞利用和第三方软件



Silence: 开发的工具和攻击类型



工具集

Silence group的一个重要特征就是使用自己组织开发的工具，包括：

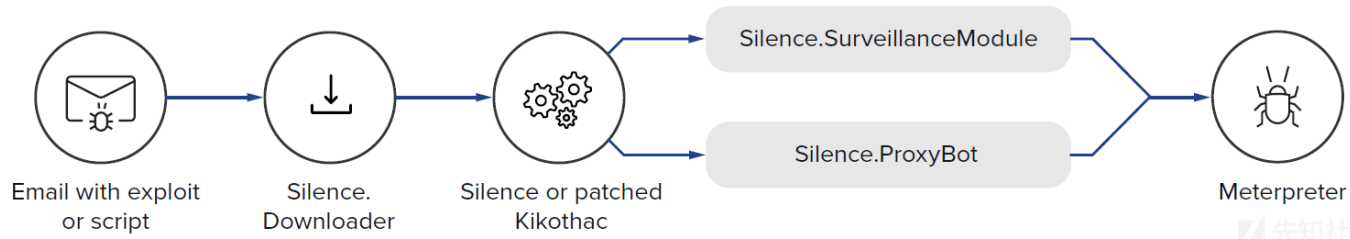
- Silence，该组织开发命名的框架；
- Atmosphere pack，攻击ATM的工具集；
- Farse，从受感染的计算机中获取密码的小工具；
- Cleaner，删除远程连接的日志。

Silence

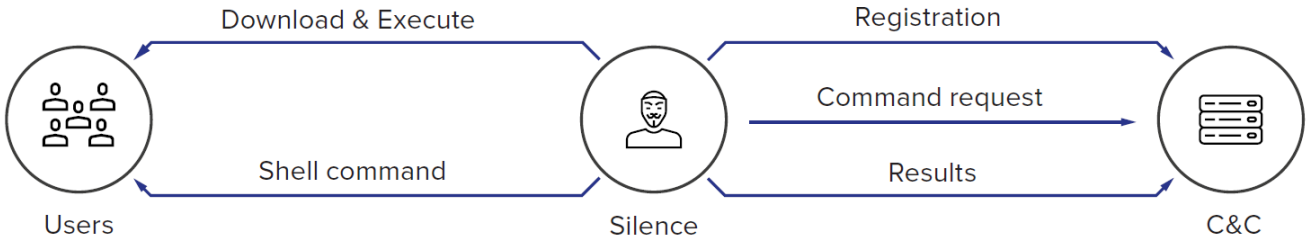
Silence group使用的框架是模块化的，含有下面的组件：

- Silence.Downloader加载器；
- 主模块为Silence，补丁后门为Kikothac；
- Silence.SurveillanceModule，用户监视模块；
- Silence.ProxyBot代理。

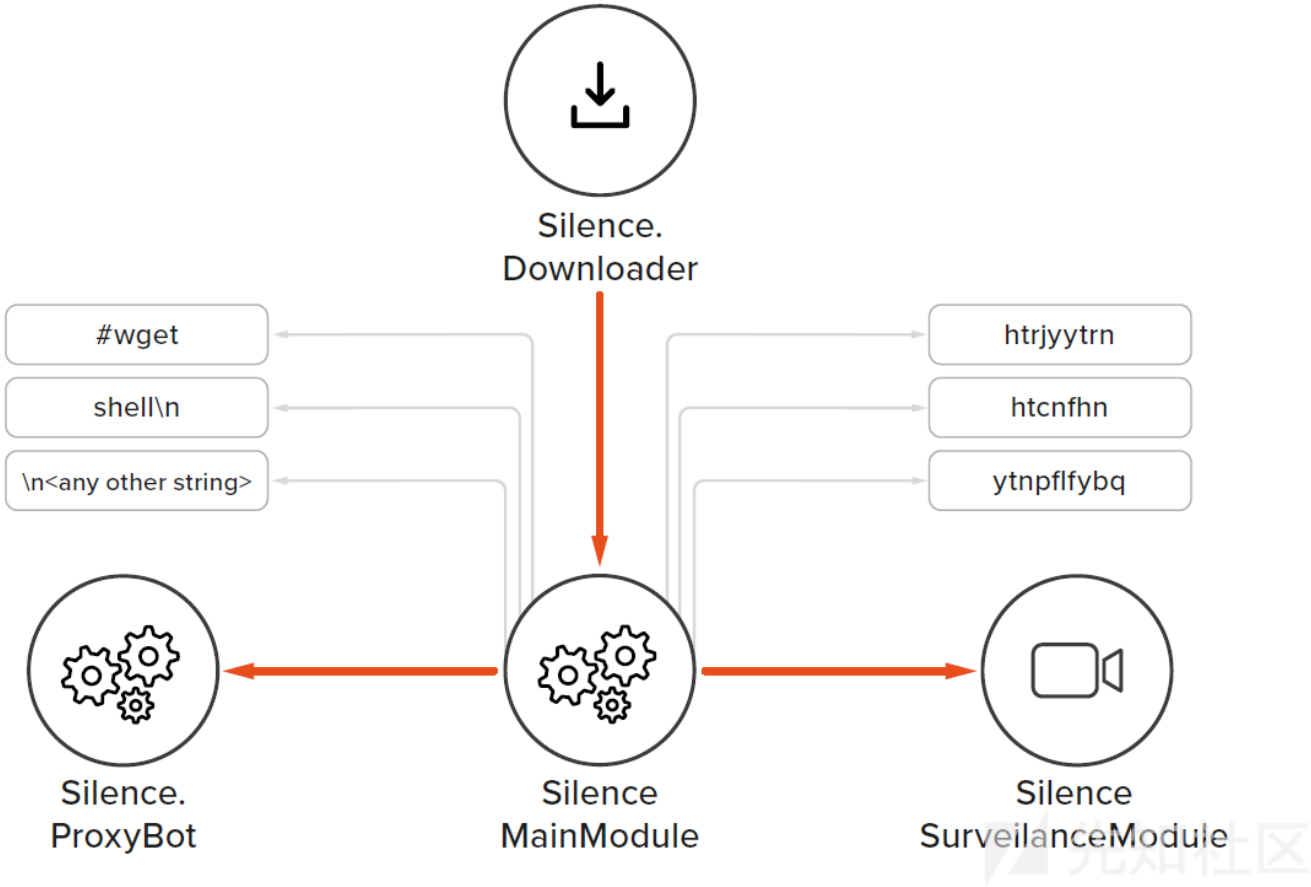
主模块会加载可执行文件，这不会限制系统的功能，并预留了扩展特征的空间。



伪装为office文件的附件利用被打开后，木马的Silence.Downloader加载器会下载并安装。加载器会安装到开始菜单中，并等候命令下载并启动下一阶段。如果攻击者对服务



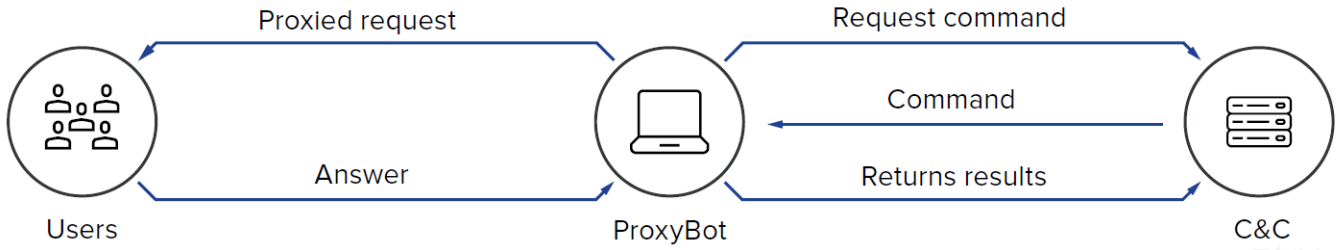
Silence木马的主体会在启动后将自己加入到开始菜单中，然后在服务器上注册并进入命令接收或执行循环中。木马的主任务是在命令翻译器中执行远程命令，下载和启动任



下图是恶意软件执行的C2命令表：

Command	Type of command / Russian text	Function
htrjyytrn	reconnect реконнект	Terminate the command interpreter session, clear all temporary files, connect to C&C "from scratch"
htcnfhn	restart рестарт	Terminate the command interpreter session and restart it
ytnpflfybq	notasks нетзадач	No operation
#wget	wget	Download a file from a remote server and save it in the current directory. Accepts two parameters: URL and file name
shell\n	shell	Launch the command interpreter
\n<any other string>	run	Execute an arbitrary OS command using the command interpreter

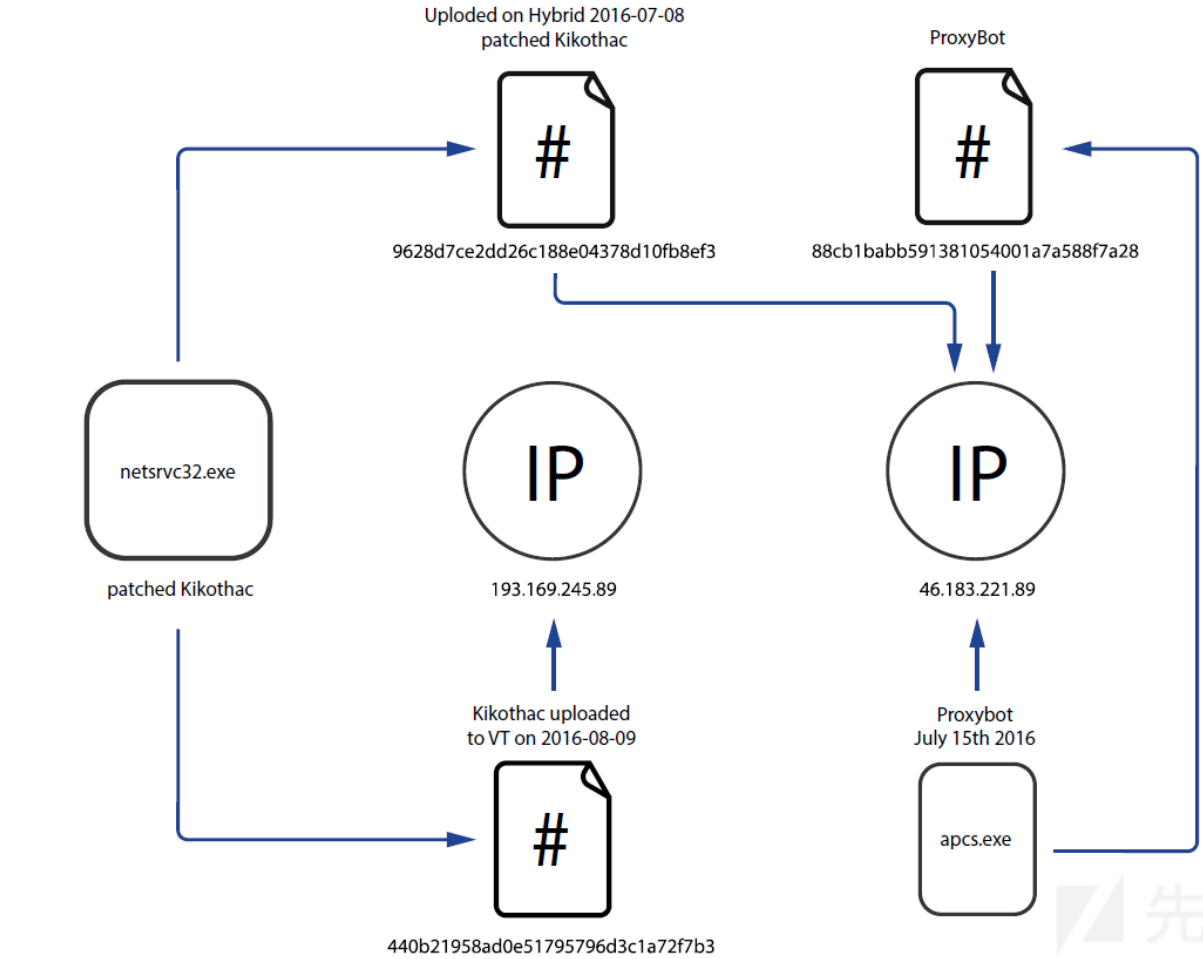
为了进入企业网络的独立（网）段中，Silence会下载ProxyBot模块。该代理模块的目的是通过受感染的设备将外部C2服务器的浏览重定向到被入侵网络的本地节点上，因为



为了监控受害者银行的用户和金融组织的合法活动，攻击者安装了SurveillanceModule模块，该模块可以偷偷截图并融合到伪数据流中。

在攻击的最后一阶段，僵尸主机会在系统中安装Meterpreter stager，负责在网络中导航。

分析C2服务器过程中，研究任意发现了与Silence服务器46.183.221[.]89进行通信的Kikothac后门。开始的时候，研究任意认为软件与Silence活动没有关联，但上传到Hybr
Trojan：



经过深入分析，研究任意发现到原来C2服务器地址的引用已经没有了，负责连接服务器的代码使用的是到编译器生成的静态链接代码的引用：

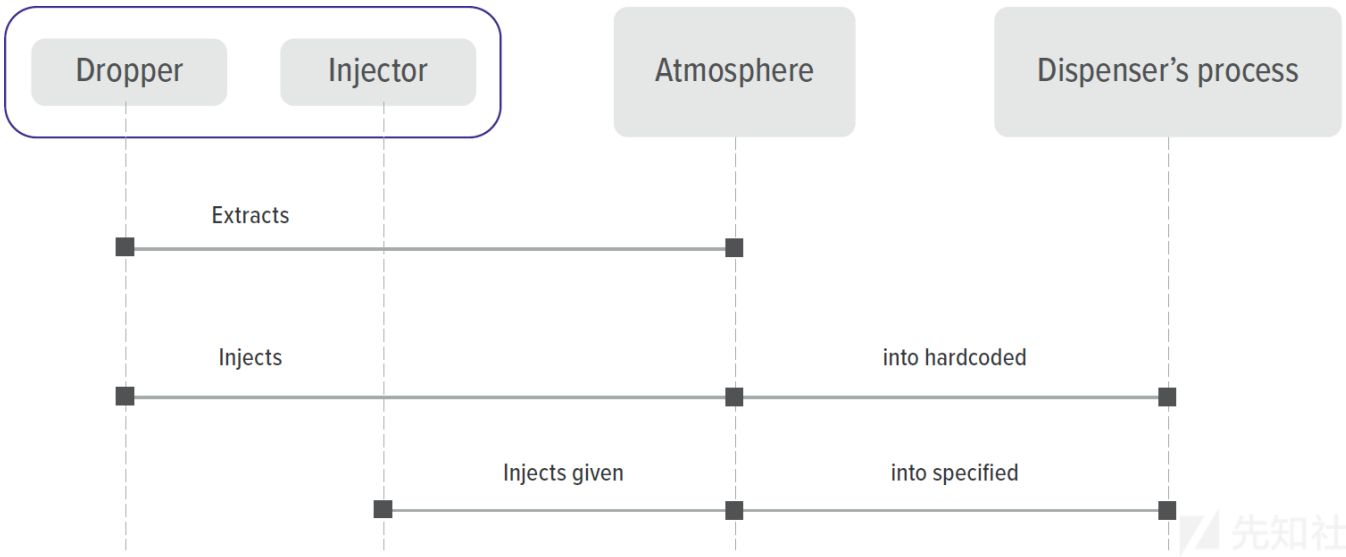
而且，所有的Kikothac命令都是以#开头的，包括从web服务器下载文件的命令#wget，Silence木马中的命令也是一样的。其他不在Kikothac命令列表中的字符串都会自动发

Command	Function
#wget	Download the file to an infected device. Bot accepts two parameters: URL and file name.
Any other string	Send the string to cmd.exe.

从中可以看出，这两个命令都会用到Silence木马中，命令会复制顺序、参数类型以及逻辑。就是说会控制打补丁的Kikothac，随后用于Silence Trojan中。

Atmosphere

为了控制ATM
自动取款机，Silence会使用一个特别的软件Atmosphere。随着时间的改进，木马会明显地进化来满足犯罪分子的需求。比如，开发者改变了进程注入的逻辑并加入灵活的
pad的命令。而早期版本，软件会重编译多次，产生一些失败的提现尝试。



黑客会在ATM上远程安装Atmosphere.Dropper。软件含有一个DLL库，这也是Atmosphere木马的主体部分。主体部分被提取后，是放弃会将库注入到进程fwmain32.exe
pad来控制ATM的方法，后来这些特征被删除了。

Command	Function
"B"	Get information on the content of ATM cassettes. In addition, the string "cash units info received" is added into the log.
"A"	Get information on the content of ATM cassettes without logging.
"Q"	Get information on the content of ATM cassettes.
"D"	One-time withdrawal of notes of the specific face value from the ATM.
"H"	Suspend all threads in process except its own. Then use functions GetThreadContext + SetThreadContext to redirect their execution to its own function.
"M", "R", "S", "P", "T", "L"	Record the output of the last command into the C:\intel\<chrs>.007 file. This command is also executed after any other by default.

程序会通过特定扩展名的文件来接收命令，然后读取命令并执行；恶意软件作者还会用一些无用的话覆写这些文件，然后删除这些文件来阻碍研究人员的取证工作。但软件

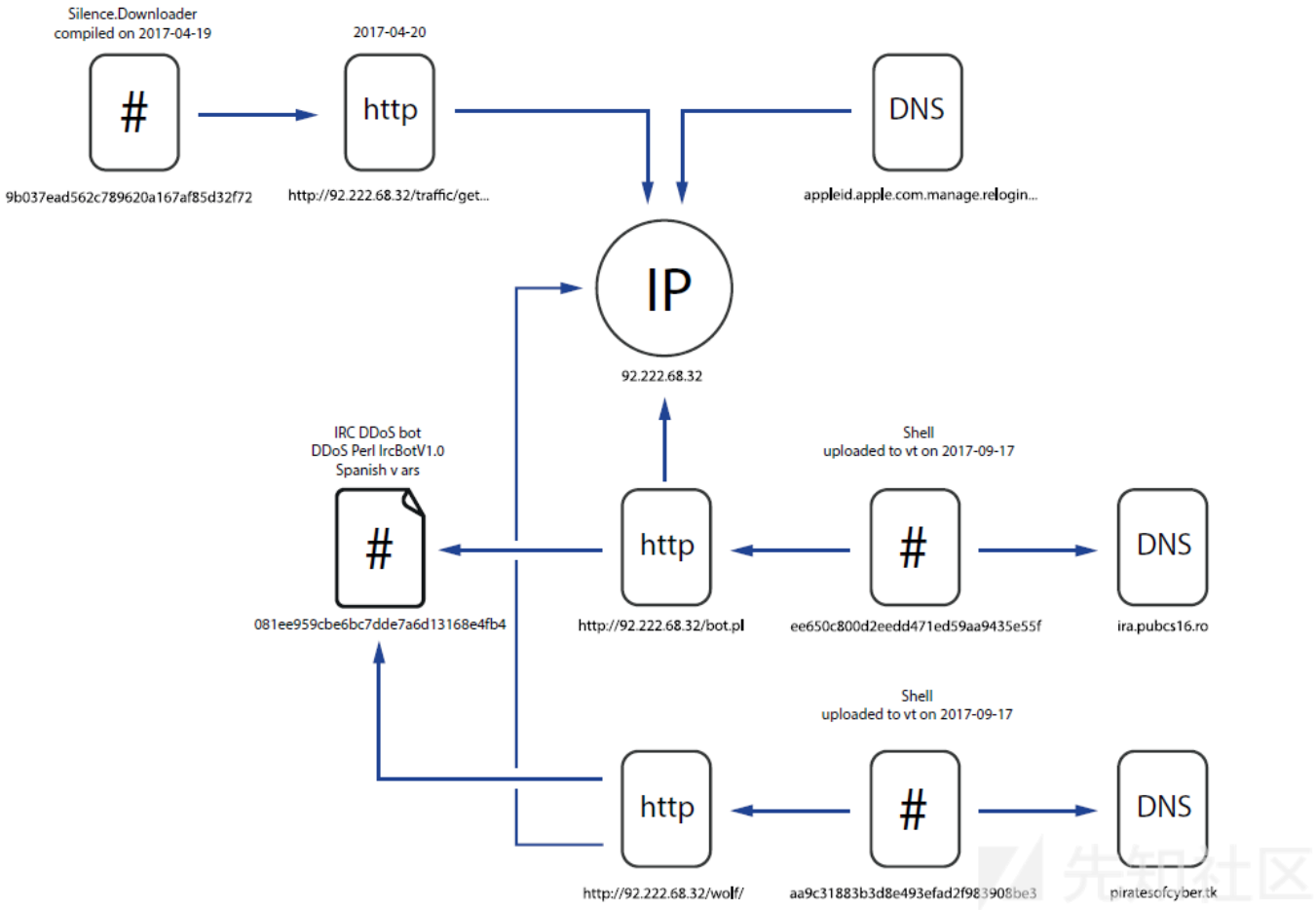
```
char __cdecl AppendGarbageAndDelete(LPCSTR lpFileName)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  file = lpFileName;                            // C:\Windows\System32\rserver30\Radm_log.htm
  result = IsFileExists(lpFileName);
  if ( result )
  {
    fileSize = FileSize(file);
    randomVal = GenerateRandomValue(10, 1024);
    GenerateGarbage((int)&garbageBuffer, fileSize + randomVal);
    v12 = 0;
    fileHandle = CreateFileA(file, 0x40000000u, 5u, 0, 4u, 0x82u, 0);
    fileHandle_ = fileHandle;
    if ( fileHandle != (HANDLE)-1 )
    {
      lpFileName = 0;
      SetFilePointer(fileHandle, 0, (PLONG)&lpFileName, 2u);
      NumberOfBytesWritten = 0;
      WriteFile(fileHandle_, lpBuffer, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
      CloseHandle(fileHandle_);
    }
    isFileDeleted = DeleteFile(file);
    garbageBuffer = (int)&off_405168;
    if ( lpBuffer )
      free((void *)lpBuffer);
    result = isFileDeleted;
  }
  return result;
}
```

Silence使用的软件中也存在该错误，研究人员推测两款恶意软件是同一作者。

在一起银行攻击活动的应急响应过程中，Group-IB取证专家就发现了Atmosphere软件的11个样本，在不同时间编译的，有一些不同。在一个含有木马的目录中，研究人员

Undernet DDoS bot

在分析Silence服务器时，研究人员发现一个名为Perl IrcBot的DDoS bot。2017年4月20日，有许多从driley123@bellsouth[.]net发来的钓鱼邮件，邮件含有从C2服务器地址92.222.68[.]32下载Silence.Downloader到机器的漏洞利用。



该程序最早出现在一个西班牙语的论坛上hxxps://forum.voidsec[.]com/thread-93.html
。该僵尸的修改版本可以通过hxxps://github[.]com/H1R0GH057/Anonymous/blob/master/ircabuse.pl
和hxxps://gist.github[.]com/dreadpiratesr/7bccc6eed49150a8564a 查看。Silence使用的就是基于Undernet DDoS Bot的版本。

该软件是用IRC消息进行控制的，一共使用了两个服务器：

- ira.pubcs16[.]ro;
- piratesofcyber[.]tk.

Smoke Bot

2017年发送的英文邮件中含有一个JS加载器，加载器可以在系统中安装Smoke Bot。Smoke
Bot从2011年起就在地下论坛出售了，卖家是一个名为SmokeLdr的说俄语的黑客。从了下载和执行任意文件，Smoke Bot还有以下特征：

- 从浏览器、邮件程序和其他软件收集用户凭证；
- 从保存的邮箱账号中收集邮件地址；
- 拦截输入浏览器的数据；
- 实时拦截email和FTP密码；
- 收集特定规则的文件；
- DDoS模块；
- TeamViewer模块；
- 加密货币挖矿模块。

本文来源于俄罗斯威胁情报机构 Group-IB 公司发布的<Silence: Moving into the darkside>。附链接：
https://www.group-ib.com/resources/threat-research/silence.html