ZombieBoy加密货币挖矿恶意软件分析

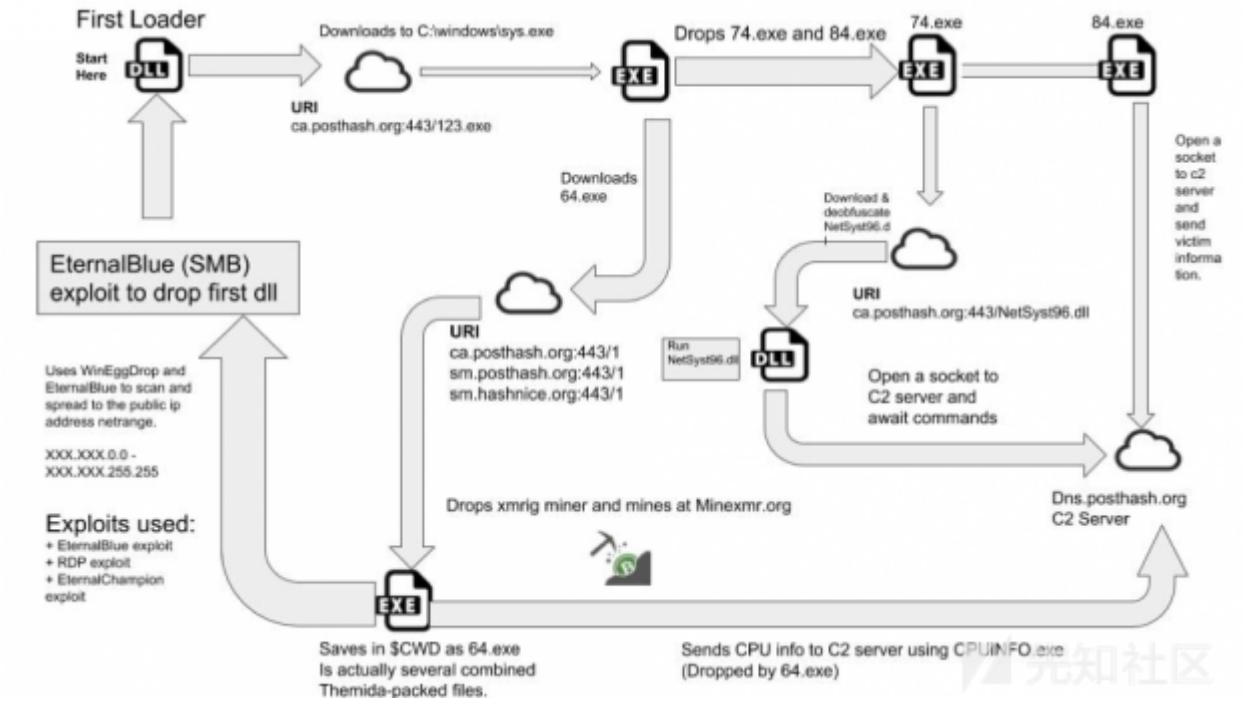
angel010 / 2018-08-07 01:33:06 / 浏览数 3561

本文翻译自：https://www.alienvault.com/blogs/labs-research/zombieboy

---

ZombieBoy是一款通过漏洞利用传播的加密货币挖矿蠕虫。与MassMiner的不同的是，ZombieBoy使用WinEggDrop来搜索新的目标主机，该恶意软件还在持续更新，因

ZombieBoy的执行过程如下图所示：



域名

ZombieBoy使用多个运行HFS(HTTP文件服务器)的服务器来获取payload。研究任意发现的URL有：

```
ca[dot]posthash[dot]org:443/
sm[dot]posthash[dot]org:443/
sm[dot]hashnice[dot]org:443/
```

除了这些，研究任意还在dns[dot]posthash[dot]org上找到一个C2服务器。

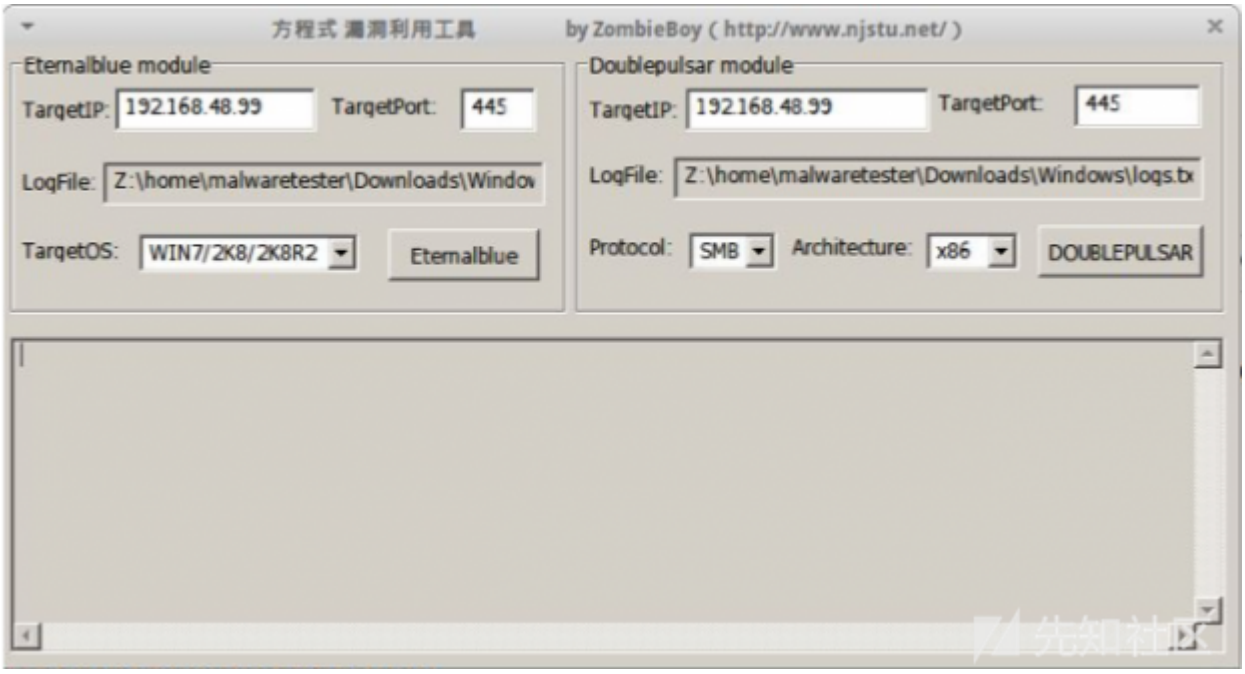
漏洞利用

ZombieBoy在执行时利用了多个漏洞：

- CVE-2017-9073，Windows XP和Windows Server 2003上的RDP漏洞
- CVE-2017-0143, SMB漏洞
- CVE-2017-0146, SMB漏洞

安装

ZombieBoy首次使用EternalBlue/DoublePulsar漏洞利用来远程安装主dll。用来安装这两个漏洞利用的程序叫做ZombieBoyTools，好像来源于中国，因为使用的语言是中
APT版本的Gh0stRAT。



ZombieBoyTools截图

DoublePulsar漏洞利用成功执行后，会加载和执行恶意软件的第一个dll。恶意软件会从ca[dot]posthash[dot]org:443下载123.exe，保存为C:\%WindowsDirector

准备

123.exe执行过程中会完成许多操作。首先，从分发服务器夏代模块64.exe，保存为boy.exe并执行。64.exe应该是负责传播ZombieBoy和携带XMRIG挖矿机。其次，会释放
2个模块。74.exe会被保存为C:\Program Files(x86)\svchost.exe，看似是Gh0stRAT的一种形式。84.exe会在本机保存为C:\Program Files(x86)\StormII\mssta.exe■mssta.exe看起来是一种RAT。

64.exe

64.exe
是ZombieBoy下载的第一个模块，使用了反分析技术。Exe文件是通过Themida打包软件加密的，这让逆向变得非常困难。在当前ZombieBoy版本中，还会检测是否虚拟机
64.exe会连接到ip[dot]3222[dot]net来获取受害者主机的IP，然后用WinEggDrop扫描网络找出开发445端口的目标。然后利用获取的IP地址和本地IP地址进行传播。6

```
<parameter name="NetworkTimeout" description="Timeout for blocking network calls (in seconds).  Use -1 for no timeout." type="S16">
    <default>60</default>
</parameter>
<parameter name="TargetIp" xdevmap="TARGET_IP_V4_ADDRESS" description="Target IP Address" type="IPv4"/>
<parameter name="TargetPort" xdevmap="TARGET_PORT" description="Port used by the Double Pulsar back door" type="TcpPort">
    <default>445</default>
</parameter>

<paramchoice name="Protocol" xdevmap="DOUBLEPULSAR_PROTOCOL_TYPE" description="Protocol for the backdoor to speak">
    <default>SMB</default>
    <paramgroup name="SMB" description="Ring 0 SMB (TCP 445) backdoor">
    </paramgroup>
    <paramgroup name="RDP" description="Ring 0 RDP (TCP 3389) backdoor">
    </paramgroup>
</paramchoice>
```

DoublePulsar截图

64.exe还会使用XMRIG进行门罗币挖矿活动。根据已知的门罗币1钱包地址，ZombieBoy挖矿的速度大约是43KH/s，折算成美元的话，每个月$1000美金（6840.5元）。研

已知的钱包地址:

```
42MiUXx8i49AskDATdAfkUGuBqjCL7oU1g7TsU3XCJg9Maac1mEEdQ2X9vAKqu1pvkFQUuZn2HEzaa5UaUkMMfJHU5N8UCw
49vZGV8x3bed3TiAZmNG9zHFXytGz45tJZ3g84rpYtw78J2UQQaCiH6SkozGKHyTV2Lkd7GtsMjurZkk8B9wKJ2uCAKdMLQ
```

研究任意还发现64.exe会从受害者处获取系统架构等信息。

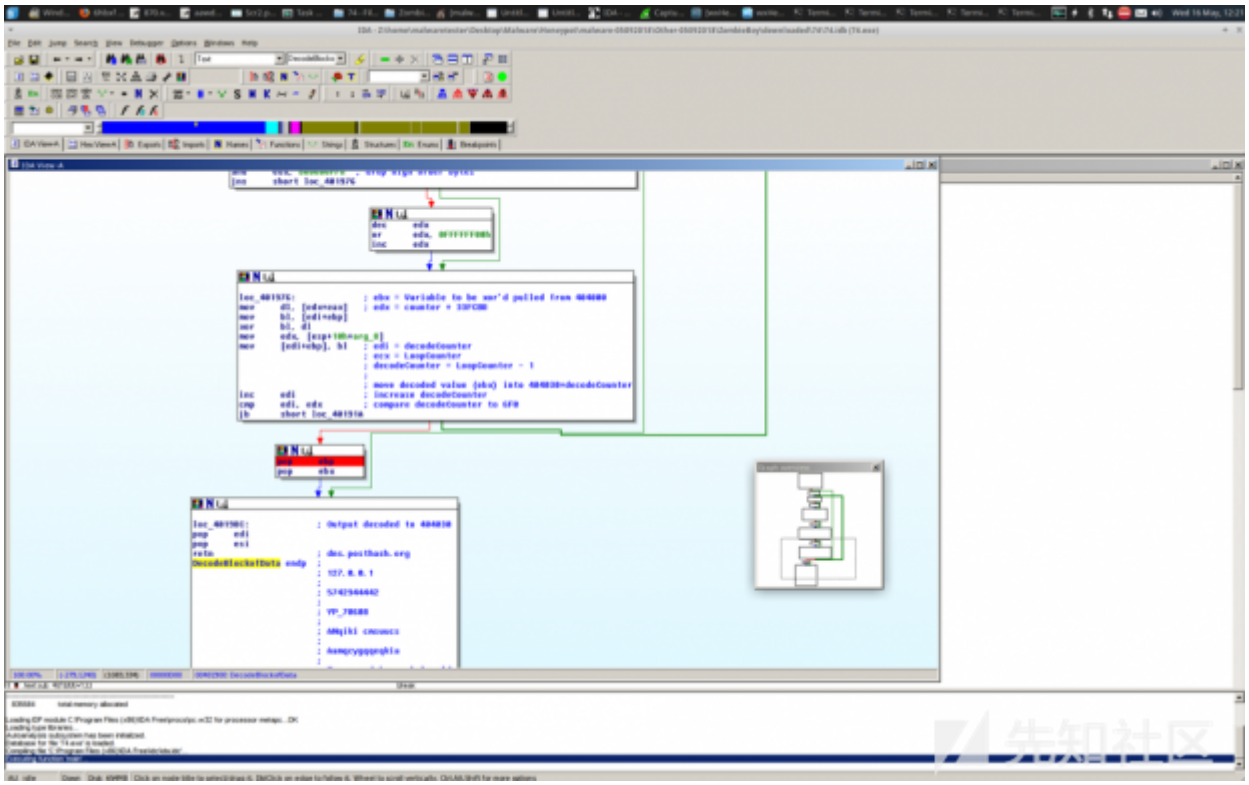
74.exe

74.exe是123.exe释放的第一个恶意软件。从形式上看，74.exe负责下载、解密和执行名为NetSyst96.dll的Gh0stRat
dll。74.exe会解密下面的参数并传递给Netsyst96.dll。

解密的参数包括：

- Dns.posthash.org

- 127.0.0.1
- 5742944442
- YP_70608
- ANqiki cmsuucs
- Aamqcygqqeqkia
- Fngzxzygdgkywoyvkxlpv ldv
- %ProgramFiles%/
- Svchost.exe
- Add
- Eeie saswuk wso



解密截图

74.exe解密了这些参数后，就会通过调用`CreateFileA`（CreationDisposition设置为Open_Existing）来检查`NetSyst96.dll`是否下载并保存为`C:\Program Files\AppPatch\mysqld.dll`。如果没有找到mysqld.dll，74.exe就会打开到`ca[dot]posthash[dot]org:443/`的连接，并下载`NetSyst96.dll`，保存为`C:\Program Files\AppPatch\mysqld.dll`。

`NetSyst96.dll`有两个输出函数DllFuUpgraddrs和DllFuUpgraddrs1，把`NetSyst96.dll`保存为`mysqld.dll`后，74.exe在调用前会先定位其中的DllFuUpgraddrs。

NetSyst96.dll

`NetSyst96.dll`是74.exe的dll。经过加密后，对解密的文件的分析会返回一些可以识别的字符串，如“Game Over Good Luck By Wind”，“jingtisanmenxiachuanxiao.vbs”。

```
Game Over Good Luck By Wind
FunctionMstsc
FunctionMmc
FunctionRegedit
FunctionTaskmgr
FunctionCMD
%s\dllcache\magnify.exe
%s\dllcache\osk.exe
%s\dllcache\sethc.exe
%s\magnify.exe
%s\osk.exe
%s\sethc.exe
DELSHIFTOSK
TermService
\dllcache\termsrvhack.dll
\termsrvhack.dll
SYSTEM\CurrentControlSet\Services\TermService\Parameters
ServiceDll
%SystemRoot%\system32\termsrvhack.dll
SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core
EnableConcurrentSessions
SYSTEM\CurrentControlSet\Control\Terminal Server
fDenyTSConnections
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
KeepRASConnections
SYSTEM\CurrentControlSet\Services\TermService
Start
open
%s%s %s%s
jingtisanmenxiachuanxiao.vbs
```


暗示释放的文件的字符串

NetSyst96.dll可以获取用户屏幕、录音、编辑剪贴板。对字符串的分析显示会输入键盘输入。Netsyst96.dll会获取Environment Strings路径，然后用来创建路径C:\Program files (x86)\svchost.exe。然后，用CreateToolhelp32Snapshot、NetSyst96.dll搜索Rundll32.exe的进程来确定dll是不是第一次运行。第一次运行后，NetSyst9

保存74.exe副本为C:\Program Files(x86)\svchost.exe；

用System/CurrentControlSet/Services/ANqiki cmsuucs将ANqiki cmsuucs注册为服务；

- 服务启动时，运行svchost.exe；

把MARKTIME加入到注册表中，并加入上次启动的时间；

用CreateToolhelp32Snapshot的snapshot寻找svchost.exe运行的进程；

- 如果没找到，启动并寻找svchost.exe；
- 如果找到一个，保存svchost.exe并运行；
- 如果找到超过1个，调用函数来创建vbs脚本来删除额外的svchost.exe；

连续运行的话，NetSyst96.dll会与C2联系起来：

定位并确认System/CurrentControlSet/Services/ANqiki cmsuucs的存在；

- 如果不存在，就创建上面的key；
- 如果存在的话，继续第2步；

创建Eeie saswuk wso事件

枚举和改变input Desktop■input desktop■；

传递C2服务器ip给C2URL (dns[dot]posthash[dot]org)；

开启WSA (winsock 2.0)；

连接到www[dot]ip123[dot]com[dot]cn，并获取dns[dot]posthash[dot]org的ip；

- 如果真实IP要改变的话，当前IP就是211.23.47[dot]186；

重置Event

连接到C2 Server，并等待命令

因为触发函数的命令是未知的，研究人员发现了31个switch选项，应该是NetSyst96.dll的命令选项。

84.exe

84.exe是123.exe释放的第二个模块，这也是一个RAT。84.exe不需要下载额外的库就可以从内存中解密和执行Loader.dll。另外，84.exe会用函数来解密Loader.dll。

Loader.dll被调用后，84.exe会通过一个Update函数传给一系列变量给Loader.dll：

- ChDz0PYP8/oOBfMO0A/0B6Y=
- 0
- 6gkIBfkS+qY=
- dazsks fsdgsdf
- daac gssosjwayw
- |_+f+
- fc45f7f71b30bd66462135d34f3b6c66
- EQr8/KY=
- C:\Program Files(x86)\StormII
- Mssta.exe
- 0
- Ccfcdaa
- Various integers

传递给Loader.dll的字符串中，其中3个是加密的。加密的字符串如下：

```
[ChDz0PYP8/oOBfMO0A/0B6Y=] = "dns[dot]posthash[dot]org"
[6gkIBfkS+qY=] = "Default"
[EQr8/KY=] = "mdzz"
```

Loader.dll

Loader.dll也是一种RAT。84.exe运行后，Loader.dll做的第一件事是从84.exe中的Update获取变量。然后Loader.dll会创建一些重要的运行时对象：

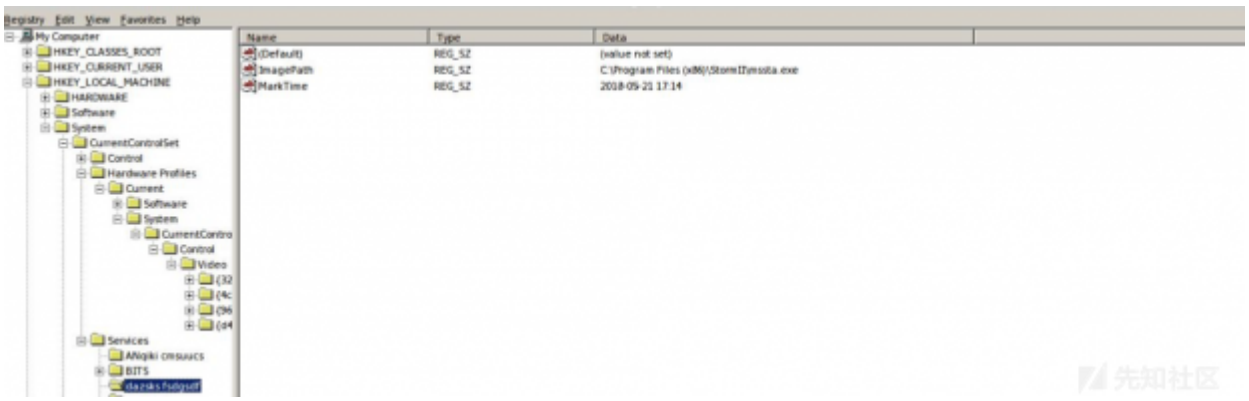
- 不可继承的、无信号的、自动重置的Null事件（句柄为0x84）；
- 执行操作DesktopInfo函数的线程；
- 句柄0x8C的input Desktop，flag DF_ALLOWOTHERACCOUNTS会被设置为调用线程的desktop；

Loader.Dll在SYSTEM/CurrentControlSet/Services/Dazsks Fsdgsdf中搜索dazsks fsdgsdf，然后用来确定是否是第一次运行恶意软件。

第一次运行时：

Loader.dll会创建一个名为Dazsks Fsdgsdf服务，其中ImagePath = C:\Program Files(x86)\StormII\mssta.exe；

Loader.dll会尝试运行新创建的服务，如果尝试运行成功的话，继续进入主循环；如果没有运行成功，就退出。



随后继续运行：

- 用参数Dazsks Fsdgsdf开启服务services.exe；
- 继续第一次运行的主循环；

检查运行的次数后，Loader.dll会进入程序的主循环。

主循环：

- 创建不可继承的、无信号的事件ccfcdaa，句柄为 0x8C；
- 解密ChDz0PYP8/oOBfMO0A/0B6Y=为dns[dot]posthash[dot]org；
- 开启WinSock对象；
- 创建不可继承的、无信号的、手动设置的事件对象，句柄为0x90；
- 收集Get请求：Get /?ocid = iefvrt HTTP/1.1
- 连接到dns[dot]posthash[dot]org:5200；
- 用GetVersionEx获取OS的相关信息；
- 加载ntdll.dll并调用RtlGetVersionNumbers；
- 保存System\CurrentControlSet\Services\(null)为注册表；
- 获取socket name；
- 用Hardware\Description\System\CentralProcessor\获取CPU刷新速度；
- 调用GetVersion来获取系统信息；
- 调用GlobalMemoryStatusEx来获取可用全局内存状态；
- 用GetDriveTypeA从A:/开始枚举所有可用的磁盘驱动；
- 在每个枚举的磁盘上获取可用空间总大小；
- 初始化COM库；
- 用marktime函数将当前时间加入到dazsks fsdgsdf服务中
- 在wow64下运行获取系统的系统信息
- 用中国反病毒软件文件名列表和CreateToolHelp32Snapshot创建运行进程的截图，然后找出运行的反病毒程序
- 解密EQr8/KY= 为 mdzz
- 发送所有前面获取的数据，并发送给dns[dot]posthash[dot]org:5200处的C2服务器。

缓解方案

缓解ZombieBoy的最好方法就是避免，这也是为什么要更新系统到最新版的原因。MS17-010会帮助恶意软件的传播能力。
如果用户被ZombieBoy感染，首先要做的是用反病毒软件扫描系统，然后找出所有ZombieBoy运行的进程，然后结束这些进程。ZombieBoy运行的进程包括：

- 123.exe
- 64.exe
- 74.exe
- 84.exe
- CPUinfo.exe
- N.exe
- S.exe
- Svchost.exe (注意文件的位置，结束所有不是C:\Windows\System32的进程)

删除下面的注册表：

```
SYSTEM/CurrentControlSet/Services/Dazsks Fsdgsdf
SYSTEM/CURRENTCONTROLSET/SERVICES/ANqiki cmsuuc
```

删除恶意软件释放的文件：

```
C:\%WindowsDirectory%\sys.exe
C:\windows\%system%\boy.exe
C:\windows\IIS\cpuinfo.exe
C:\Program Files(x86)\svchost.exe
C:\Program Files\AppPatch\mysqld.dll
C:\Program Files(x86)\StormII\mssta.exe
C:\Program Files(x86)\StormII\*
```

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板