关于 BlackMoon 变种 HTTPBot 僵尸网络的风险提示

近期，CNCERT 监测发现一种名为 HTTPBot 的 DDoS 僵尸网络。该僵尸网络控制者通过钓鱼等方式诱导 Windows 主机用户运行伪装成记事本等程序的木马文件实现劫持 Windows 主机的目的，通过 C&C 控制服务器向被劫持主机发送控制指令，对目标服务器的 HTTP 业务端口开展攻击。该僵尸网络控制方式、攻击模式与 BlackMoon 僵尸网络利用的类似，可认为是 BlackMoon 僵尸网络的变种。

一、 木马文件分析

区别于传统的僵尸网络利用 IoT 设备漏洞攻击 IoT 设备，HTTPBot 僵尸网络木马，攻击对象为 Windows 主机，通过对其样本文件进行逆向分析，发现该木马基于 Go 语言开发，主要特征如下:

1、 硬编码的形式保存 C&C 服务器的域名，域名为

jjj.jjycc.cc，目前解析为：104.233.144.23

2、 隐蔽运行

```
void main_HideWindow()
{
  int v0; // [esp+0h] [ebp-10h]
  int v1; // [esp+0h] [ebp-10h]
  int WindowThreadProcessId; // [esp+8h] [ebp-8h]
  int v3; // [esp+Ch] [ebp-4h]

  main_getConsoleWindow();
  if ( v0 )
  {
    v3 = v0;
    WindowThreadProcessId = main_getWindowThreadProcessId(v0);
    golang_org_x_sys_windows_GetCurrentProcessId();
    if ( v1 == WindowThreadProcessId )
      main_showWindow(v3, 0);
  }
}
```

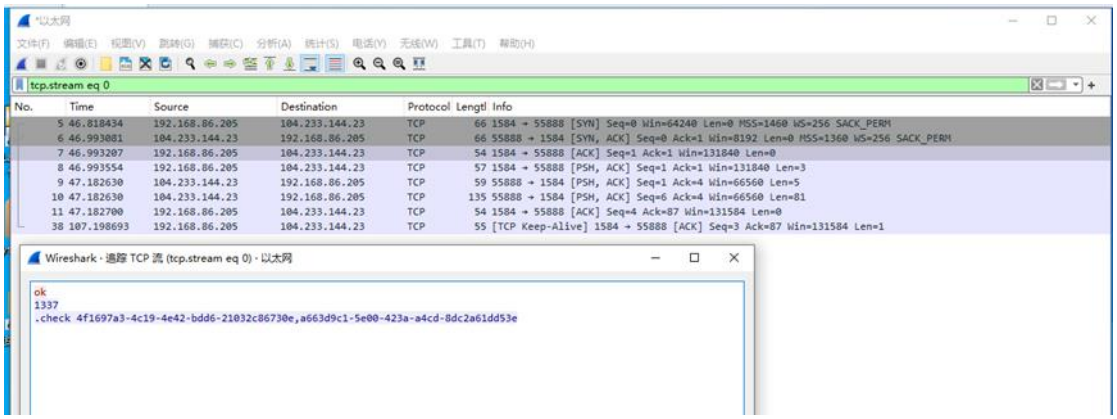
3、 写入注册表实现自启动

将自身路径写入 HKEY_LOCAL_MACHINE\SOFTWARE\Micro

soft\Windows\CurrentVersion\Run 启动项键值实现开机自动运行。

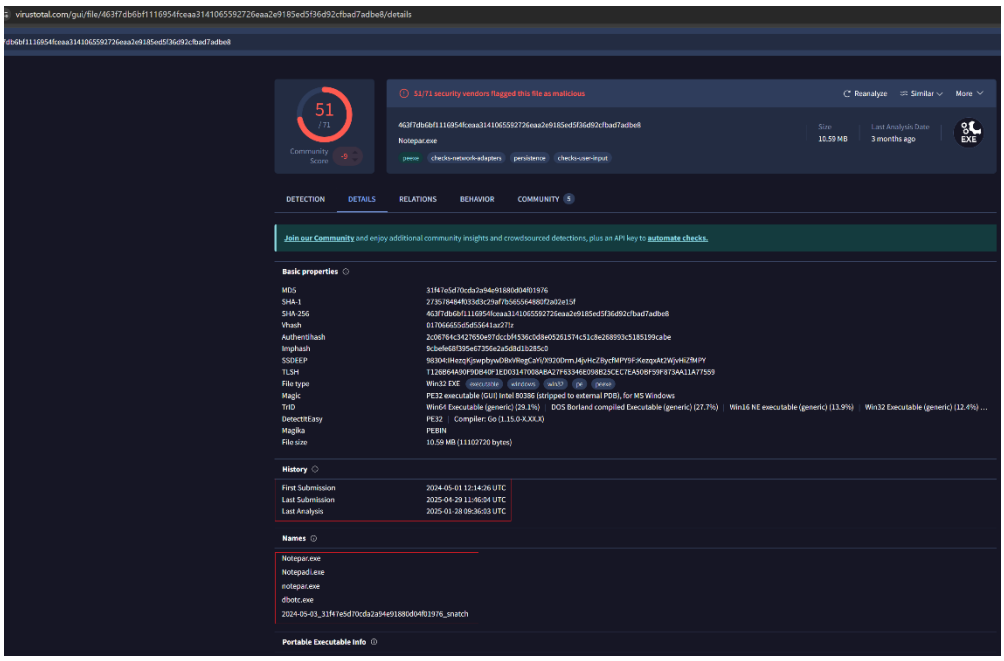
4、 精准操控

僵尸网络中每个被控节点，将会主动向 C&C 服务器控制节点发送字符串”OK”进行在线认证，等待 C&C 服务器下发的控制指令。



5、 感染方式

通过对木马文件逆向分析，未发现有 ODAY 或者 Nday 漏洞利用相关的代码，没有驱动提权代码，未获取 RING0 控制权限，为一般权限的木马程序。将木马文件与 VirusTotal 网站恶意样本库进行比对，得到结果如下:



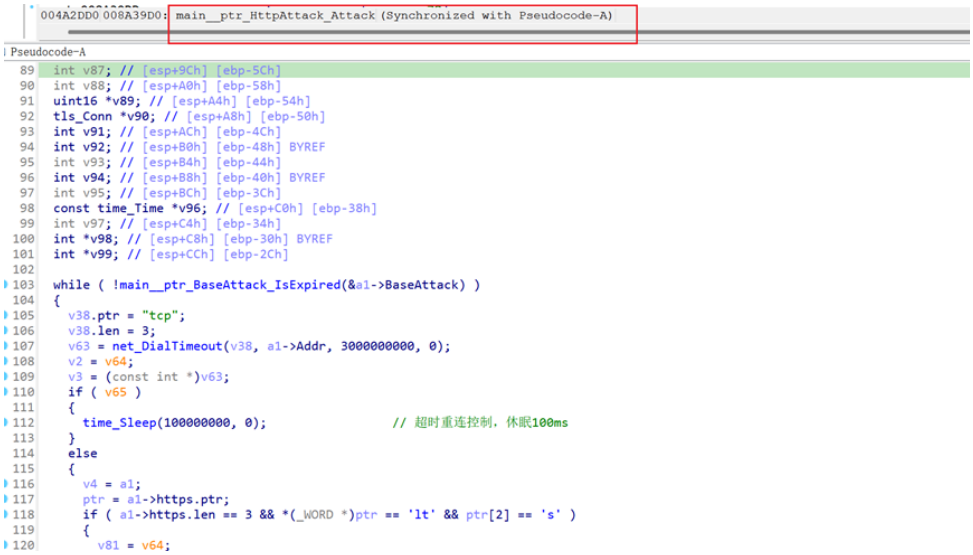
据 VirusTotal 统计，该木马样本通常以 Windows 系统

自带的记事本程序 notepad.exe 相似的文件名（如 notepad1.exe、notepar.exe）这类文件名进行传播，伪装成 Windows 系统自带的记事本程序，结合逆向分析结果，可推定该木马文件的感染方式为诱导用户执行的钓鱼传播。

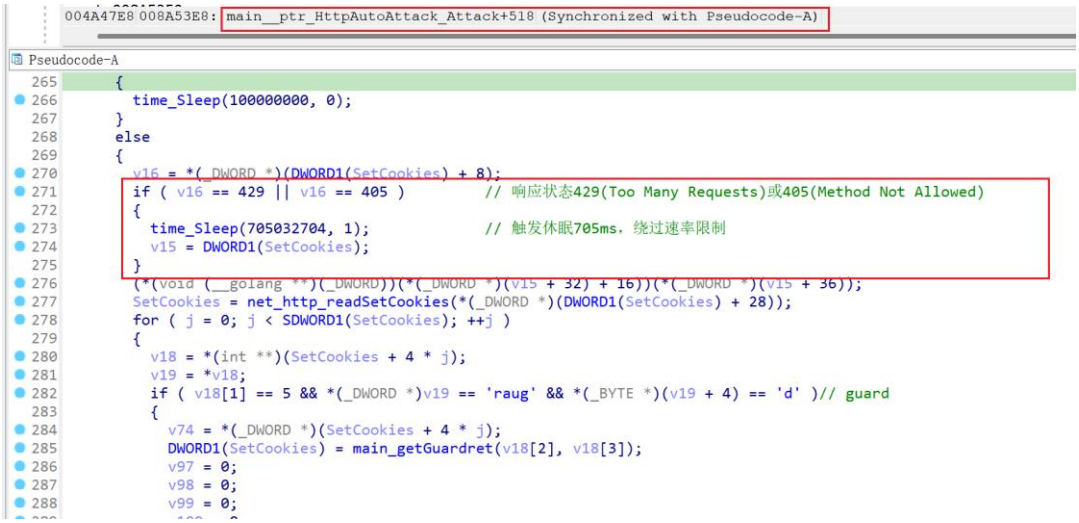
二、 攻击模式分析

HTTPBot 内置 7 种针对 HTTP 协议开展 DDoS 攻击的模式：

1、 HttpAttack 模式：可根据攻击目标端口配置，动态选择明文 TCP 或者加密的 TLS 连接。并且实现了自动重试、UserAgent 和表头的随机化以及动态速率控制。

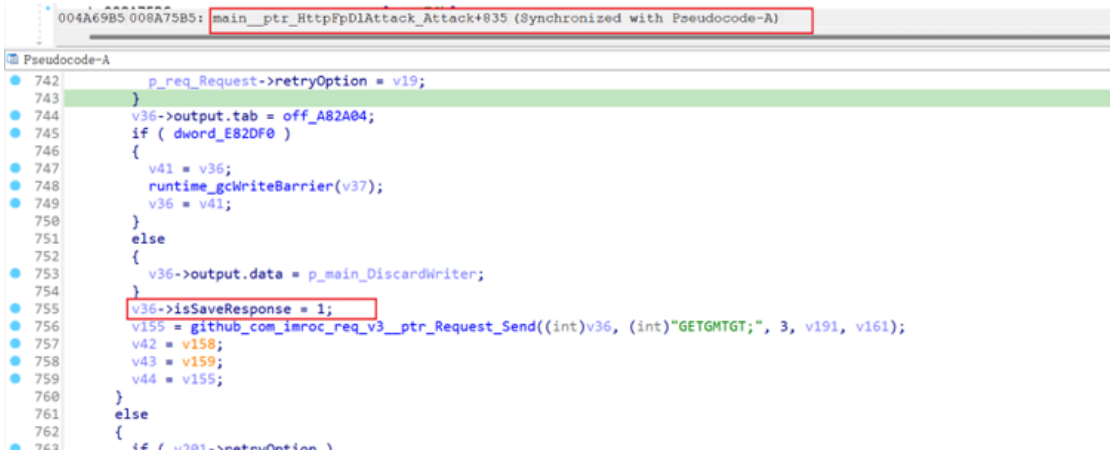


2、 HttpAutoAttack 模式：相较于 HttpAttack 模式，引入了自动化的 Cookie 处理流程（解析服务端的响应返回的 guardret 参数，构造一个新的 Cookie），结合状态码识

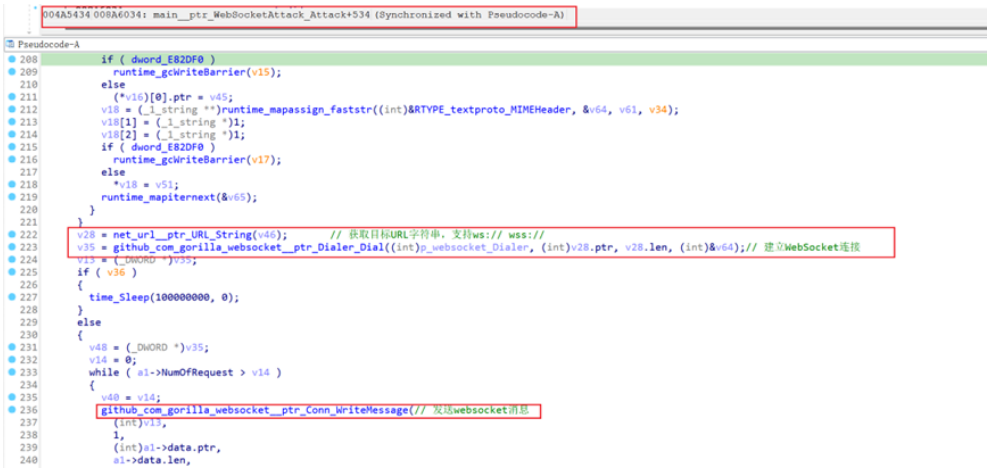


别和重试机制（如果状态码为 429 或者 405，则通过休眠绕过频率限制）以及随机化 UA 头部，实现更准确地模拟合法会话，避免触发而激活目标服务器的 Cookie 参数核验保护规则。

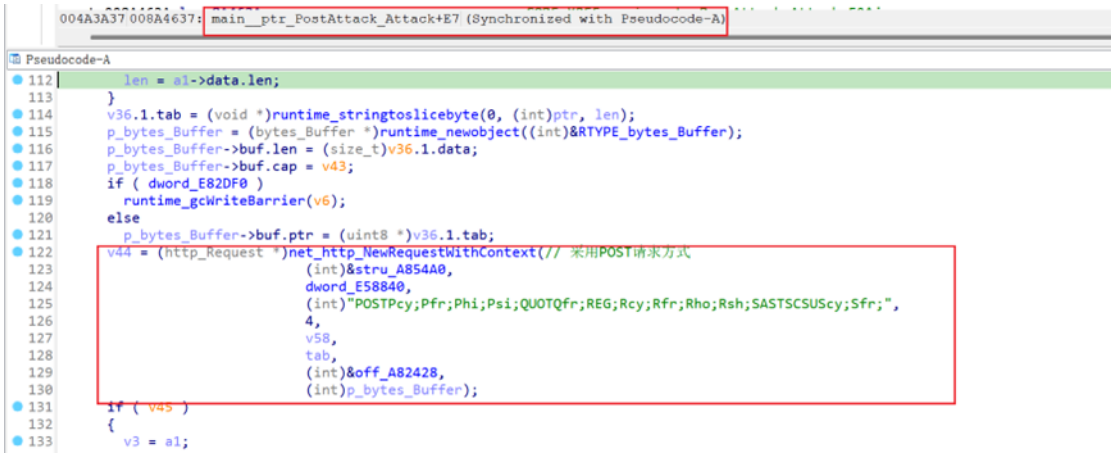
3、 HttpsFpDIAttack 模式：基于资源消耗最大化的策略进行攻击。一是将 TCP Keep-Alive 时间设置为 30 分钟，即使没有文件操作，也长时间占用目标服务器 TCP 连接资源。二是强制使用 HTTP/2 模式，其多路复用功能强制目标服务器传输大体积响应文件，提高目标服务器负荷。



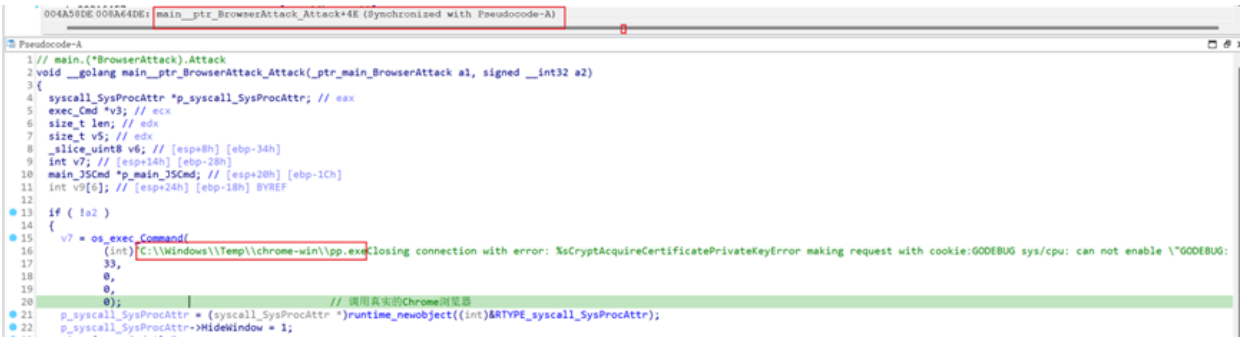
4、 WebSocketAttack 模式：通过控制单个连接的消息数量，循环发送握手消息，并能够随机生成 UA 信息、随机生成消息正文、包含合法表头伪装普通的 HTTP 请求、动态控制消息间隔等模式躲避基于频率的检测。



5、 POSTAttack 模式：强制使用 POST 方法，随机选择 UA，模拟多个浏览器版本，绕过基于固定顺序的规则检测。



6、 BrowserAttack 模式：利用隐藏的 Google Chrome 实例模拟合法业务流量，隐藏窗口，混淆正常请求和攻击流量，实现自动化控制。



7、 CookieAttack 模式：在 BrowserAttack 模式之外加入 Cookie 自动化管理，自动携带合法 Cookie。

三、 HTTPBot 僵尸网络安全威胁

1、 业务安全风险

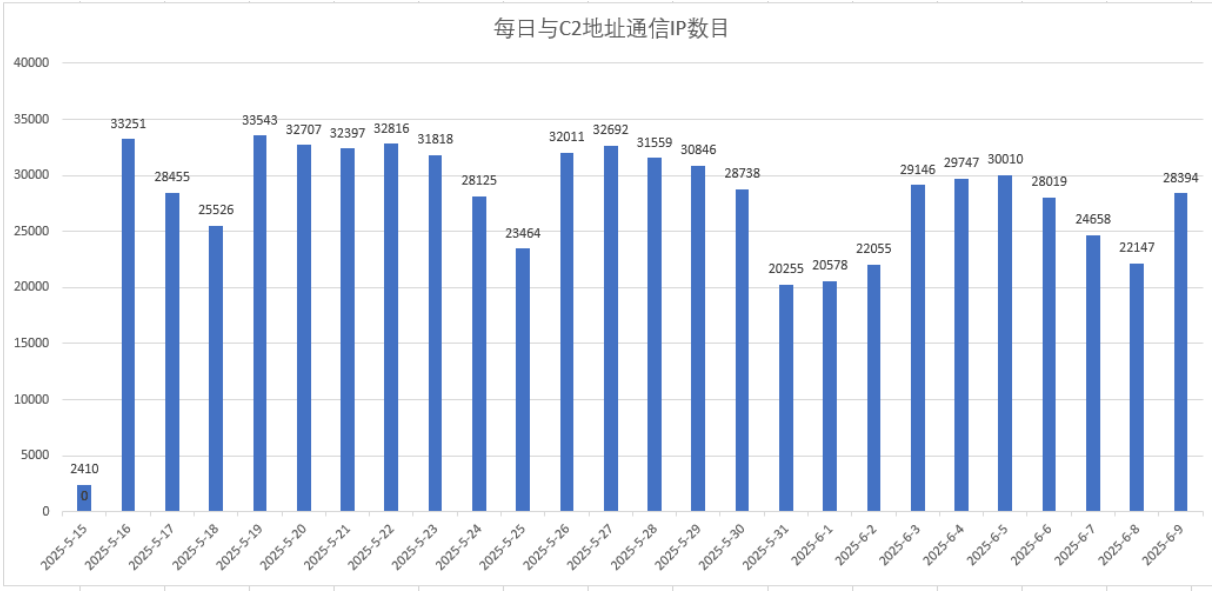
此类攻击使用的动态混淆技术使得攻击流量和普通业务流量难以区分，危害性较大。

2、 长期驻留的持续性风险

HTTPBot 通过木马隐蔽潜伏在 Windows 主机内，可通过横向渗透等方式对更多主机发起感染。

四、 监测情况

经过监测分析发现，自 2025 年 5 月 15 日至 6 月 9 日期间，C2 地址日通信 IP 个数最高达到 33543 个，平均 27514 个，累计有 31.7 万个 IP 地址与 C2 地址通信。每日境内通信 IP 数量情况如下。



五、 防范建议

请各单位、广大网民强化风险意识，加强安全防范，主要建议包括:

1、 开展木马查杀，不点击来历不明的应用程序。

2、 封堵 C&C 控制服务器的域名解析请求，封禁与 C&C 控制服务器的网络连接。

六、 相关 IOC

样本 MD5:

3C265ABE43FA0C15E69EAB2C1DF2B4D7

31F47E5D70CDA2A94E91880D04F01976

域名:

jjj.jjycc.cc

控制 IP:

104.233.144.23

七、 致谢

感谢绿盟威胁情报中心提供的样本支持。