KCon

纵横

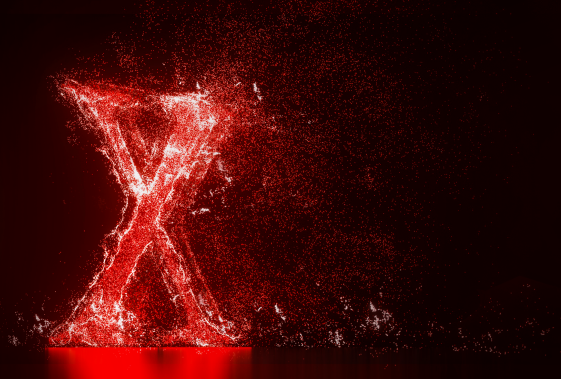
剑走偏锋
—蓝军实战缓解措施滥用

演讲人：顾佳伟

Whoami

- @askme765cs
- 安全研究员@绿盟科技
- M01N战队核心成员
- 专注系统安全与终端对抗

目录
CONTENTS



Part 01
Mitigations 101

Why Mitigations?

漏洞利用两种常见路径

- 数据破坏
- 代码执行

利用过程中的动作与特征

- 修改代码段
- 加载DLL
- 创建新进程
- …

Mitigations的效用

- 截断利用链，削减机会窗口
- 对抗未知威胁与潜在攻击

Mitigations Timeline

- Pre-Win10
  - ASLR
  - DEP
  - SafeSEH
  - SEHOP
- TH1
  - CFG
- RS1
  - CIG
- RS2
  - ACG
  - Child Process Policy
- RS3 +
  - CFG Strict Mode
  - CFG Export Suppression
  - NoLowMandatoryLabelImages
  - …

Code intergerity guard-CIG

- Windows 10 TH2 (1511)引入
- 阻止恶意DLL注入受保护应用程序
- 对加载DLL的签名进行验证
- 仅允许可信签名的DLL加载
  - MicrosoftSignedOnly
  - StoreSignedOnly

- 内核主要检查代码位于
  MiValidateSectionSigningPolicy
- 受影响的API
  NtCreateSection

Arbitrary code guard-ACG

- Windows 10 RS1 (1607)引入
- 贯彻W^X原则
  - 禁止修改已有代码(X)修改为可写(W)
  - 禁止修改可写数据(W)修改为可执行(X)
  - 禁止分配或映射新的可执行内存

- 内核主要检查代码位于
  - MiAllowProtectionChange
  - MiMapViewOfSection
- 受影响的API
  - NtAllocateVirtualMemory
  - NtProtectVirtualMemory
  - NtMapViewOfSection(SEC_IMAGE/SEC_FILE)

Arbitrary code guard-ACG

- 用户态API
  - VirtualAlloc with PAGE_EXECUTE_*
  - VirtualProtect with PAGE_EXECUTE_*
  - MapViewOfFile with FILE_MAP_EXECUTE | FILE_MAP_WRITE
  - SetProcessValidCallTargets for CFG

Boundary of ACG

- 只能限制程序本身，不能阻止其他程序对其的修改
- 开启AllowRemoteDowngrade则可通过其他程序关闭ACG

Mitigation Flags-EPROCESS

ULONG Flags、Flags2、Flags3、Flags4

ULONG MitigationFlags、MitigationFlags2

```
+0x9d0 MitigationFlags  : Uint4B
+0x9d0 MitigationFlagsValues : <anonymous-tag>
   +0x000 ControlFlowGuardEnabled : Pos 0, 1 Bit
   +0x000 ControlFlowGuardExportSuppressionEnabled : Pos 1, 1 Bit
   +0x000 ControlFlowGuardStrict : Pos 2, 1 Bit
   +0x000 DisallowStrippedImages : Pos 3, 1 Bit
   +0x000 ForceRelocateImages : Pos 4, 1 Bit
   +0x000 HighEntropyASLREnabled : Pos 5, 1 Bit
   +0x000 StackRandomizationDisabled : Pos 6, 1 Bit
   +0x000 ExtensionPointDisable : Pos 7, 1 Bit
   +0x000 DisableDynamicCode : Pos 8, 1 Bit
   +0x000 DisableDynamicCodeAllowOptOut : Pos 9, 1 Bit
   +0x000 DisableDynamicCodeAllowRemoteDowngrade : Pos 10, 1 Bit
   +0x000 AuditDisableDynamicCode : Pos 11, 1 Bit
   +0x000 DisallowWin32kSystemCalls : Pos 12, 1 Bit
   +0x000 AuditDisallowWin32kSystemCalls : Pos 13, 1 Bit
   +0x000 EnableFilteredWin32kAPIs : Pos 14, 1 Bit
   +0x000 AuditFilteredWin32kAPIs : Pos 15, 1 Bit
   +0x000 DisableNonSystemFonts : Pos 16, 1 Bit
   +0x000 AuditNonSystemFontLoading : Pos 17, 1 Bit
   +0x000 PreferSystem32Images : Pos 18, 1 Bit
   +0x000 ProhibitRemoteImageMap : Pos 19, 1 Bit
   +0x000 AuditProhibitRemoteImageMap : Pos 20, 1 Bit
   +0x000 ProhibitLowILImageMap : Pos 21, 1 Bit
   +0x000 AuditProhibitLowILImageMap : Pos 22, 1 Bit
   +0x000 SignatureMitigationOptIn : Pos 23, 1 Bit
   +0x000 AuditBlockNonMicrosoftBinaries : Pos 24, 1 Bit
   +0x000 AuditBlockNonMicrosoftBinariesAllowStore : Pos 25, 1 Bit
```

Mitigation Policy-注册表

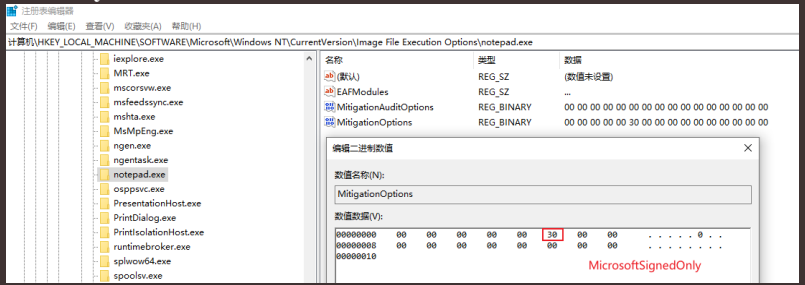
设置指定名称\路径程序的Mitigation Policy-IFEO

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\
- MitigationOptions:REG_BINARY

系统全局Mitigation Policy

- HKLM\System\CurrentControlSet\Control\Session Manager\kernel\
- MitigationOptions:REG_BINARY

Mitigation Policy-注册表



Mitigation Policy-Powershell

查看程序Mitigation Policy(从程序读取)

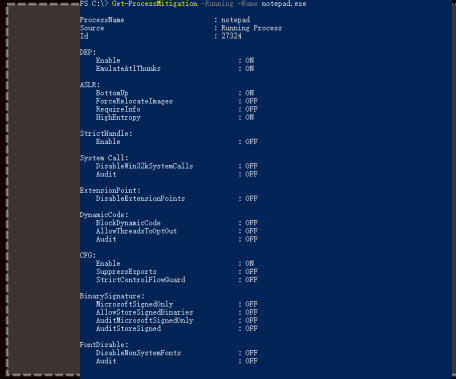
- Get-ProcessMitigation –Running –Name notepad.exe

查看程序Mitigation Policy(从注册表读取)

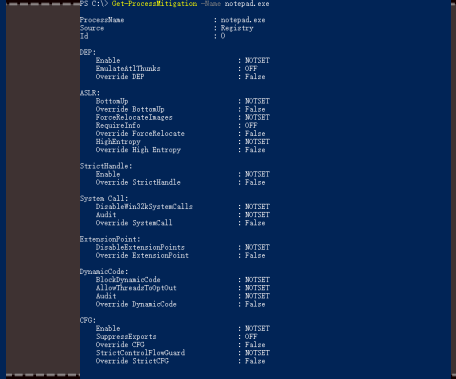
- Get-ProcessMitigation -Name notepad.exe

设置程序Mitigation Policy(写入注册表)

- Set-ProcessMitigation -Name notepad.exe -Enable MicrosoftSignedOnly



```
PS C:\> Get-ProcessMitigation -Running -Name notepad.exe

ProcessName                  : notepad
Source                       : Running Process
Id                           : 27224

DEP:
    Enable                   : ON
    EmulateAtlThunks         : ON

ASLR:
    BottomUp                 : ON
    ForceRelocateImages      : OFF
    RequireInfo              : OFF
    HighEntropy              : ON

StrictHandle:
    Enable                   : OFF

System Call:
    DisableWin32kSystemCalls : OFF
    Audit                    : OFF

ExtensionPoint:
    DisableExtensionPointz   : OFF

DynamicCode:
    BlockDynamicCode         : OFF
    AllowThreadsToOptOut     : OFF
    Audit                    : OFF

CFG:
    Enable                   : ON
    SuppressExports          : OFF
    StrictControlFlowGuard   : OFF

BinarySignature:
    MicrosoftSignedOnly      : OFF
    AllowStoreSignedBinaries : OFF
    AuditMicrosoftSignedOnly : OFF
    AuditStoreSigned         : OFF

FontDisable:
    DisableNonSystemFonts    : OFF
    Audit                    : OFF
```



```
PS C:\> Get-ProcessMitigation -Name notepad.exe

ProcessName                  : notepad.exe
Source                       : Registry
Id                           : 0

DEP:
    Enable                   : NOTSET
    EmulateAtlThunks         : OFF
    Override DEP             : False

ASLR:
    BottomUp                 : NOTSET
    Override BottomUp        : False
    ForceRelocateImages      : NOTSET
    RequireInfo              : OFF
    Override ForceRelocate   : False
    HighEntropy              : NOTSET
    Override High Entropy    : False

StrictHandle:
    Enable                   : NOTSET
    Override StrictHandle    : False

System Call:
    DisableWin32kSystemCalls : NOTSET
    Audit                    : NOTSET
    Override SystemCall      : False

ExtensionPoint:
    DisableExtensionPoints   : NOTSET
    Override ExtensionPoint  : False

DynamicCode:
    BlockDynamicCode         : NOTSET
    AllowThreadsToOptOut     : NOTSET
    Audit                    : NOTSET
    Override DynamicCode     : False

CFG:
    Enable                   : NOTSET
    SuppressExports          : OFF
    Override CFG             : False
    StrictControlFlowGuard   : NOTSET
    Override StrictCFG       : False
```

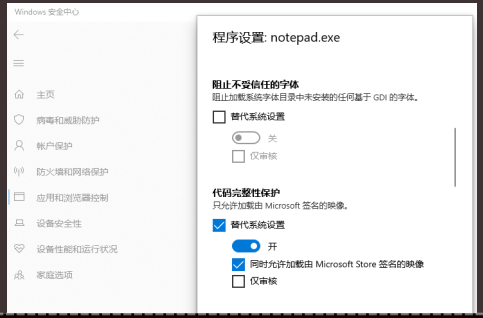
Mitigation Policy-Exploit Protection

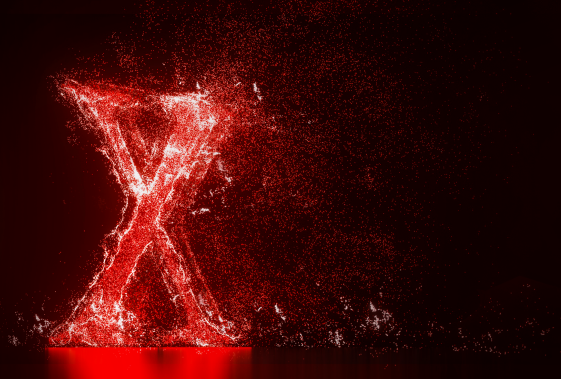
系统设置

- 设置系统全局Mitiation Policy
- CFG、DEP、强制ASLR等

程序设置

- 设置单个程序Mitigation Policy
- 图形化、用户友好

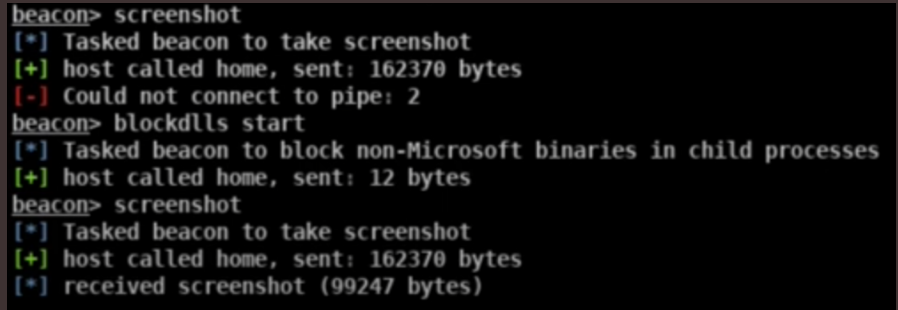




Part 02
Red Team Operation

CobaltStrike Blockdlls

- CobaltStirke 3.14版本中引入
- 开启后子进程只能加载微软签名的DLL
- 一些后渗透指令受益于blockdlls
  - Spawn
  - Screenshot
  - Keylogger
  - Mimikatz
  - …

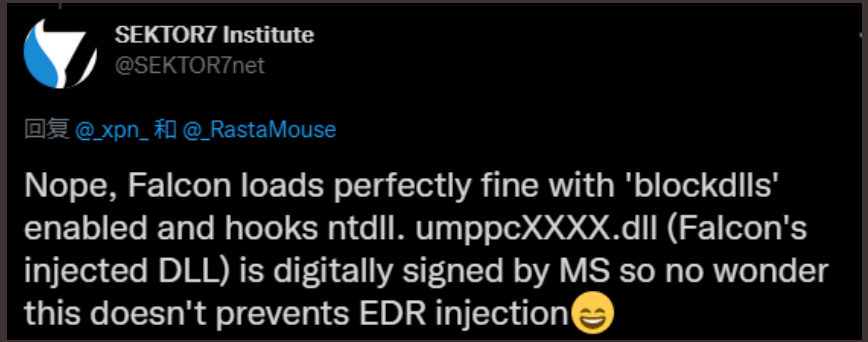

beacon> screenshot
[*] Tasked beacon to take screenshot
[+] host called home, sent: 162370 bytes
[-] Could not connect to pipe: 2
beacon> blockdlls start
[*] Tasked beacon to block non-Microsoft binaries in child processes
[+] host called home, sent: 12 bytes
beacon> screenshot
[*] Tasked beacon to take screenshot
[+] host called home, sent: 162370 bytes
[*] received screenshot (99247 bytes)

Blockdlls原理-CIG滥用

- UpdateProcThreadAttribute
- 子进程中开启CIG
- 阻止部分安全产品DLL注入

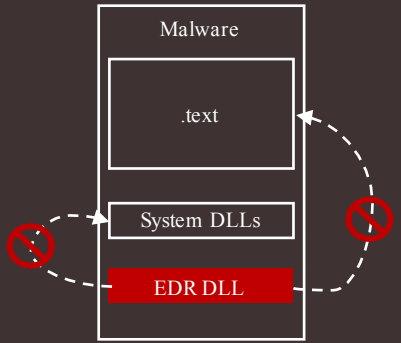
⇨ 若DLL有微软签名？

```
undefined8 FUN_18001508c(longlong param_1,undefined8 param_2,LPPROC_THREAD_ATTRIBUTE_LIST param_3)

{
  BOOL BVar1;
  DWORD DVar2;
  UINT UVar3;
  undefined8 uVar4;

  //PROCESS_CREATION_MITIGATION_POLICY_BLOCK_NON_MICROSOFT_BINARIES_ALWAYS_ON
  *(undefined8 *)(param_1 + 8) = 0x100000000000;
  //Enable CIG for child process
  BVar1 = UpdateProcThreadAttribute(param_3,0,0x20007,(undefined8 *)(param_1 + 8),8,(PVOID)0x0,(PSIZE_T)0x0);
  if (BVar1 == 0) {
    DVar2 = GetLastError();
    FUN_18008db48(0x47,DVar2);
    uVar4 = 0;
  }
  else {
    if (SetErrorMode_exref != (code *)0x0) {
      UVar3 = SetErrorMode(0x8003);
      *(UINT *)(param_1 + 0x10) = UVar3;
    }
    uVar4 = 1;
  }
  return uVar4;
}
```

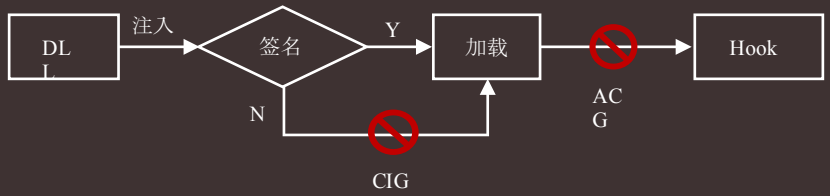

SEKTOR7 Institute
@SEKTOR7net
回复 @_xpn_ 和 @_RastaMouse
Nope, Falcon loads perfectly fine with 'blockdlls' enabled and hooks ntdll. umppcXXXX.dll (Falcon's injected DLL) is digitally signed by MS so no wonder this doesn't prevents EDR injection

更进一步，阻击HOOK

- CIG无法阻止签名DLL的加载
- ACG可阻止对代码段的修改
- 利用ACG阻止DLL对代码段的修改



ACG+CIG防线



实时修改自身Mitigation Policy

- SetProcessMitigationPolicy
  - 底层调用NtSetInformationProcess
- 可实时开启CIG、ACG等Mitigations
- 开启后无法由自身关闭

```
BOOL SetProcessMitigationPolicy(
  [in] PROCESS_MITIGATION_POLICY MitigationPolicy,
  [in] PVOID                     lpBuffer,
  [in] SIZE_T                    dwLength
);
```

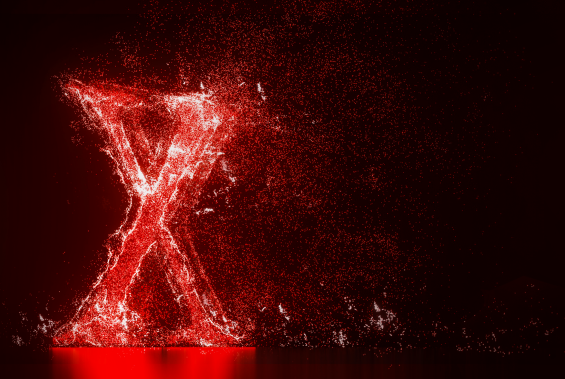
```
uint64_t policy = *(DWORD *)lpBuffer;
policy = policy << 32;
policy += (DWORD)MitigationPolicy;
NTSTATUS ret = NtSetInformationProcess(
            0xffffffffffffffff,
            // For ProcessMitigationPolicy value
            (PROCESS_INFORMATION_CLASS)0x34,
            &policy,
            sizeof(policy));
```

实时修改其他程序Mitigation Policy

- NtSetInformationProcess
- 只能修改ACG
- 开启AllowRemoteDowngrade 可关闭ACG

Decompile: NtSetInformationProcess - (ntoskrnl.exe)

```
1324        }
1325        break;
1326      case 0x34:
1327                          /* ProcessMitigationPolicy */
1328        local_4f0 = '\0';
1329        if (ProcessInformationLength != 8) break;
1330        ProcessInformationValue = *(ulonglong *)*ProcessInformation;
1331                          /* 进程句柄不为-1(当前进程时)
1332                             MitigationPolicy 只能为 DynamicCodePolicy (2) */
1333        if ((ProcessHandle != -1) && ((int)ProcessInformationValue != 2)) break;
1334        p_Var23 = IoGetCurrentProcess();
```



Part 03
"Mitigation Hell"

Side Effect Of Mitigations

“Mitigation Hell”——利用缓解措施使程序失去可用性乃至崩溃

- ACG-无法修改自身代码，导致具有自解密、自修改行为的程序失败

  -杀死几乎所有.NET程序，CLR初始化依赖于RWX内存

- CIG-无法加载非微软签名的组件，导致运行异常或失败
- Child Process Policy-破坏依赖子进程创建的进程，例如守护进程

若将Mitigations强制应用于未适配的安全软件会如何？

剑走偏锋，利用"Mitigation Hell"击破安全防线

- 修改特定安全产品关键程序Mitigation Policy，破坏可用性

```
if (((iVar1 != 0) && (iVar1 = FUN_0041ac40(local_148,local_144,local_140), iVar1 != 0))
  local_158 = 0;
  local_24 = DAT_00515a40 << 2;
                    /* 修改为可写 */
  local_20 = VirtualProtect(local_150,local_24,PAGE_READWRITE,&local_158);
  if (local_20 != 0) {
                    /* 修改代码段 */
    *(code **)((int)local_150 + DAT_00515a40 * 4) = FUN_004ada0;
    local_8 = 0xfffffffe;
    local_154 = 0;
                    /* 修改回原始权限 */
    VirtualProtect(local_150,local_24,local_158,&local_154);
  }
}
```

安全产品A-自修改行为+ACG=>闪

安全产品B-未签名DLL+CIG=>初始化错

ATT&CK T1562

Impair Defenses 防御削弱

- 修改或禁用安全产品
- 破坏日志记录机制
- 清除历史日志信息

Impair Defenses

Sub-techniques (7)

ID	Name
T1562.001	Disable or Modify Tools
T1562.002	Disable Windows Event Logging
T1562.003	Impair Command History Logging
T1562.004	Disable or Modify System Firewall
T1562.006	Indicator Blocking
T1562.007	Disable or Modify Cloud Firewall
T1562.008	Disable Cloud Logs

Mitigations

ID	Mitigation
M1022	Restrict File and Directory Permissions
M1024	Restrict Registry Permissions
M1018	User Account Management

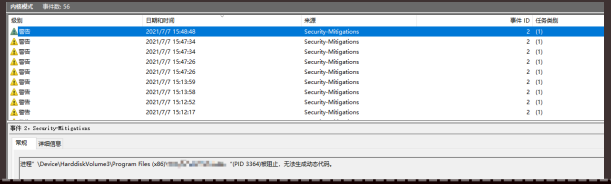
- 限制关键IFEO注册表项修改

Hunting "Mitigation Hell"-Audit Mode

Audit审计模式-记录日志而不阻止

Set-ProcessMitigation -Name notepad.exe -Enable AuditDynamicCode,AuditMicrosoftSigned

日志记录 Microsoft-Windows-Security-Mitigation/Kernel Mode



Hunting "Mitigation Hell"-ETW

- Microsoft-Windows-Kernel-Memory:KERNEL_MEM_KEYWORD_ACG
- Microsoft-Windows-Security-Mitigations:Microsoft-Windows-Security-Mitigations/KernelMode

Microsoft-Windows-Kernel-Memory/Acg	4,978.631	MsMpEng (6108)	ThreadID="14,176" AcgFlag="0"
Microsoft-Windows-Kernel-Memory/Acg	6,841.488	devenv (15296)	ThreadID="860" AcgFlag="0"
Microsoft-Windows-Kernel-Memory/Acg	7,012.708	cmd (9952)	ThreadID="21,600" AcgFlag="0"
Microsoft-Windows-Kernel-Memory/Acg	7,091.097	VsDebugConsole (12412)	ThreadID="10,088" AcgFlag="0"
Microsoft-Windows-Kernel-Memory/Acg	7,138.202	ServiceHub.DataWarehouseHost (10420)	ThreadID="22,216" AcgFlag="0"
Microsoft-Windows-Kernel-Memory/Acg	7,143.110	ServiceHub.DataWarehouseHost (10420)	ThreadID="22,216" AcgFlag="0"
Microsoft-Windows-Kernel-Memory/Acg	7,315.520	devenv (15296)	ThreadID="1,536" AcgFlag="0"

观点总结

- Mitigations带来的不止是“安全”，亦为新的利用方式埋下伏笔
- 终端对抗领域Mitigations的利用已不鲜见，攻防一体两面，没有银弹
- 对安全软件强制开启缓解措施，有破坏其可用性的可能，是一种行之有效的手段

感谢观看！

演讲者：绿盟科技 顾佳伟

知道创宇 | KCon