Архив

- ► 2024 (26)
- ► 2023 (21)
- ► 2022 (15)
- ► 2021 (28)
- ▼ 2020 (27)
  - ► декабря (1)
  - ► сентября (1)
  - ► августа (2)
  - ▼ июля (3)
    - etw tracing handles in kernel
    - _TlgProvider_t
    - what`s wrong with Etw
  - ► июня (5)
  - ► мая (2)
  - ► апреля (7)
  - ► марта (3)
  - ► января (3)
- ► 2019 (9)
- ► 2018 (5)
- ► 2017 (22)
- ► 2016 (29)
- ► 2015 (46)
- ► 2014 (10)
- ► 2013 (73)
- ► 2012 (153)
- ► 2011 (288)
- ► 2010 (167)

hand made

arm64 disasm for Windows
libecc patched for wdk7
AVX/XOP instructions processor extender
dcu files loader for ida pro, v2 & for xe3
IDA Pro plugins
Perl for IDA Pro & docs
RPat & docs
Simple Win x64 splicer & docs
WinCheck: last version

отходы мозга

AddMandatoryAce
apisetschema.dll
CmControlVector & for w8
CmRegisterCallback(Ex)
EtwEventRegister
EtwRegister

суббота, 11 июля 2020 г.

what`s wrong with Etw

Disclaimer: as I am aware that the given code examples can be dangerous for Etw-based EDR products - all code was made for least popular version of windows - for arm64

Let's assume that we have some application that wants to hide its activity from trace logs - not necessary evil or malicious, for example just to hide used algos or bit paranoid like crypto-wallet. Lets see how can it achieve this (I have no desire to consider trivial cases like removing records from eventlog)

Semiofficial ways

1. Sure all you readed about COMPlus_ETWEnabled but there is also promising COMPlus_ETWFlags
2. You can switch off etw tracing for services.exe with registry key TracingDisabled in Software\Microsoft\Windows NT\CurrentVersion\Tracing\SCM\Regular
3. And the same for rpcrt4.dll with registry key ExtErrorInformation in HKLM\Software\Policies\Microsoft\Windows NT\Rpc

Actually there are virtually countless ways to do it. And many perhaps not documented bcs was written in Ms by some poor intern who was kicked out in the cold after another review 10+ years ago. I struggled with temptation to make clickbait caption like "99% of windows dlls can disable etw logs" but it`s close to the truth

Patching

1. Yes, good old IAT hijacking for functions like EtwEventWrite works fine even though they can be easily detected
2. Splicing of Etw functions. Almost same as above
3. Some more sophisticated patching of internal wpp structures. For example you can find Etw handles and zero them. Or zero trace level. Or EventsEnableBits. PoC to find etw handles in rpcrt4.dll

Kernel mode

Who immediately remembered InfinityHook? Btw Ms removed pfn GetCpuClock from WMI_LOGGER_CONTEXT since est. build 18963
There are much more kernel sensors. PoC to find CmpTraceRoutine - and suddenly etw events from registry stop generating. Sure it`s not big problem if your product has some code registered with CmRegisterCallback

Conclusion

Etw is unreasonably complex and fragile technology and can easily be broken in too many places

Автор: redp на 19:58

Ярлыки: винда-кормилица, etw, re

Комментариев нет:

Отправить комментарий

Чтобы оставить комментарий, нажмите кнопку ниже и войдите с аккаунтом Google.

ВОЙТИ С АККАУНТОМ GOOGLE

Следующее Главная страница Предыдущее

Tags

re (240)
винда-кормилица (191)
бгг (107)
wincheck (86)
64bit (83)
я.недоволен (71)
idapro (65)
linux (60)
w8 (60)
exports (52)
books (50)
rpc interfaces (42)
w10 (40)
я.дебил (40)
perl (36)
win32k.sys (35)
w10tp (34)
open source (33)
c++ (29)
баян (29)
w8 consumer preview (24)
apisetschema (22)
bug (20)
gcc (20)
факты (20)
arm64 (19)
rpc (19)
ndis (17)
матан (17)
онтевирус (17)
KPRCB (15)
bpf hype (15)
verifier (15)
w8.1 (15)
w8 release preview (13)
w8.1 preview (12)
crypto (11)
я.доволен (11)
dwarf (10)
etw (9)
писон (9)
fltmgr (8)
wnf (8)
delphi (7)
udis86 (7)
говно нации (7)
code analysis (6)
lisp (6)
w8 rtm (6)
лень (6)

NDIS structures
ntdll official hooks
NtTraceControl
partial structs matcher
patched pdbdump
patched udis86 - with blackjack & hookers
PoRegisterPowerSettingCallback
port & alpc port owner
registered callbacks
RPC extensions
RPC servers hijack
SetTraceCallback
vista sp2 & windows7
RPC interfaces
VerifierExt.sys
WNF notifiers
Крякер интернета
Другой быдлобложык

Exports

advapi32.dll
bcrypt.dll
cng.sys
crypt32.dll
dbghelp.dll
dnsapi.dll
FirewallAPI.dll
fltmgr.sys
FwpkclInt.sys
fwpuclnt.dll
hal.dll
hid.dll
iphlpapi.dll
ipnathlp.dll
ks.sys
ksecdd.sys
lsasrv.dll
mspatcha.dll
msrpc.sys
msvcrXXX.dll
ndis.sys & 64bit
netapi32.dll
netio.sys & 64bit
ntdll.dll & 64bit
ntoskrnl.exe & 64bit
ole32.dll
rpchttp.dll
rpcrt4.dll & 64bit
setupapi.dll
user32.dll
winhttp.dll
ws2_32.dll

qt (4)
rfg (4)
vs2010 (4)
а вы все умрете (4)
AVX (3)
asm (3)
msbuild (3)
netio.sys (3)
x64 (3)
ксакеп (3)
фан-клуб (3)
.net (2)
llvm (2)
loongson (2)
metal-archives.com (2)
poc (2)
ruby (2)
virtualbox (2)
vs2011 (2)
неосилил (2)
я.графоман (2)
BinaryNinja (1)
R (1)
afd (1)
blackhat (1)
crowdsourcing (1)
disasm (1)
go (1)
longread (1)
mips32 (1)
paranoia (1)
scheme (1)
silo (1)
sql (1)
sw64 (1)
tcpip (1)
tcpip6 (1)
tdi (1)
vs2013 (1)
лютобешеннозавидую (1)

Читатели

книжная полка

Shelfari: Book reviews on your book blog

алкоголик, злобный придурок и патологический фанат perl. вам здесь не рады и ничего не должны. ваше бесценное единственно правильное мнение будет глумливо проигнорировано

Просмотреть профиль