Basic properties

MD5	d974b8d7090d75ef71fc5b3738857972
SHA-1	5bb50ce960235abe67db22851ece30adad020f93
SHA-256	00f6d6900e9ff0c8767dc7cee9d44522e26e31b61fbc5323775b3869019593f0
Vhash	014066551d151e1519z27zaxz
Authentihash	fbeafdbab08957f983766b87f77b297c709b61f1797dbc8922232b317005fe96
Imphash	d41fa95d4642dc981f10de36f4dc8cd7
Rich PE header hash	6c9272bb390e89b75934eea3b15a1858
SSDEEP	192:ZqjKhp+GQvzj3i+5T9oGYJh1wAoxhSF6OOoe068jSJUbueq1H2PIP0:wjKL+v/y+5TWGYOf2OJ06dUb+pQ
TLSH	T1DC6218874B7E1906FB969F7592E9C7936D34F6C0CEA825CF421299982C413E0AF2861C
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32+ executable (native) x86-64, for MS Windows
TrID	Win64 Executable (generic) (56.5%) Windows Icons Library (generic) (11%) OS/2 Executable (generic) (10.9%) Generic Win/DOS Executable (10.7%) DOS Executable Generic (10.7%)
DetectItEasy	PE64 Compiler: Microsoft Visual C/C++ (2005) Linker: Microsoft Linker (8.0 or 11.0) [Driver64,signed]
File size	14.20 KB (14544 bytes)

History

Creation Time	2008-07-26 13:29:37 UTC
Signature Date	2008-07-26 13:30:00 UTC

Last Submission	2023-07-23 18:34:29 UTC
Last Analysis	2023-07-18 20:12:29 UTC

Names

WR64.sys
WinRing0.sys
$RCRPJBV.sys
00f6d6900e9ff0c8767dc7cee9d44522e26e31b61fbc5323775b3869019593f0-dropped.bin
wr64.sys
winring.sys
00f6d6900e9ff0c8767dc7cee9d44522e26e31b61fbc5323775b3869019593f0.bin
5bb50ce960235abe67db22851ece30adad020f93.bin

Signature info

Signature Verification

⚠ The digital signature of the object did not verify.

File Version Information

Copyright	Copyright (C) 2007-2008 OpenLibSys.org. All rights reserved.
Product	WinRing0
Description	WinRing0
Original Name	WinRing0.sys
Internal Name	WinRing0.sys
File Version	1.2.0.5
Comments	The modified BSD license
Date signed	2008-07-26 11:30:00 UTC

+ GlobalSign ObjectSign CA
+ GlobalSign Primary Object Publishing CA
+ GlobalSign Root CA - R1

Counter Signers

+ GlobalSign Time Stamping Authority
+ GlobalSign RootSign Partners CA
+ GlobalSign Root CA - R1

X509 Certificates

+ Noriyuki MIYAZAKI
+ GlobalSign RootSign Partners CA
+ GlobalSign Primary Object Publishing CA
+ GlobalSign Time Stamping Authority
+ GlobalSign ObjectSign CA
+ GlobalSign Root CA

Portable Executable Info

Compiler Products

[---] Unmarked objects count=12
[IMP] VS2005 build 50727 count=5
[ASM] VS2005 build 50727 count=1

[RES] VS2005 build 50727 count=1

[LNK] VS2005 build 50727 count=1

Header

Target Machine	x64
Compilation Timestamp	2008-07-26 13:29:37 UTC
Entry Point	20488
Contained Sections	6

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	1734	2048	5.39	1c3d5bb2285dafcf3b7746bf717c1a51	49618.5
.rdata	8192	380	512	3.28	08362d1269d5a5ef4e7560cab993590d	48037
.data	12288	276	512	0.3	043c46095689123e1f5be96c109c2f46	123001
.pdata	16384	96	512	0.86	077af14197899077aa36d2c72ba1773f	107219
INIT	20480	546	1024	3.06	ba375d2de342e7d7a93487a35ea5d36d	107754.5

Imports

+ HAL.dll

Contained Resources By Type

RT_VERSION 1

Contained Resources By Language

ENGLISH US 1

Contained Resources

SHA-256	File Type	Type	Language	Entropy	Chi2
495974216acc865259dc7d3d6f8a310d2f	unkno	RT_VER	ENGLISH	3.43	68515.
cc3466284c3c2128adb9019dd85ec2	wn	SION	US		41

Overlay

entropy	7.498017311096191
offset	6656
chi2	9348.51
filetype	unknown
md5	ccc217df78b4822a8ccbb5aea96cdb57
size	7888

7

Sign in **Sign up**

Blog | Releases Community Buzz Mobile App API v3 | v2