Virus Total Report

Community Score

32 security vendors flagged this file as malicious

1fc74504d626223335f39e10435bd3366bc5533619e8e7713e2a48eadd4dc26a

rc.exe

bobsoft peexe

922.50 KB
Size

2021-12-10 18:32:37 UTC
18 hours ago

EXE

DETECTION DETAILS COMMUNITY

Ad-Aware	Gen:Variant.Zusy.409846	AhnLab-V3	Malware/Win.Generic.C4827103
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	HEUR/AGEN.1202595	BitDefender	Gen:Variant.Zusy.409846
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.DownLoader44.14043	eGambit	Unsafe.AI_Score_89%
Emsisoft	Gen:Variant.Zusy.409846 (B)	eScan	Gen:Variant.Zusy.409846
ESET-NOD32	A Variant Of Win32/Injector.EQQS	FireEye	Gen:Variant.Zusy.409846
Fortinet	W32/Injector.EQQS!tr	GData	Gen:Variant.Zusy.409846
Ikarus	Trojan.Inject	Kaspersky	UDS:DangerousObject.Multi.Generic
Kingsoft	Win32.Troj.Generic_a.a.(kcloud)	Lionic	Trojan.Multi.Generic.4!c
Malwarebytes	Malware.AI.709900288	MAX	Malware (ai Score=87)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	Artemis!8B416273DDF4
McAfee-GW-Edition	BehavesLike.Win32.Worm.dh	Microsoft	Trojan:Win32/Remcos.RVG!MTB
Panda	Trj/GdSda.A	SecureAge APEX	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Sophos	Mal/Generic-S
Symantec	Scr.MalPbs!gen1	TrendMicro-HouseCall	TROJ_GEN.R002C0DLA21
Acronis (Static ML)	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
CAT-QuickHeal	Undetected	ClamAV	Undetected
CMC	Undetected	Comodo	Undetected
CrowdStrike Falcon	Undetected	Cyren	Undetected
Elastic	Undetected	F-Secure	Undetected
Gridinsoft	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected

32 / 67

Community Score

32 security vendors flagged this file as malicious

1fc74504d626223335f39e10435bd3366bc5533619e8e7713e2a48eadd4dc26a

rc.exe

bobsoft peexe

922.50 KB Size

2021-12-10 18:32:37 UTC 18 hours ago

EXE

DETECTION DETAILS COMMUNITY

Basic Properties

MD5	8b416273ddf403092ec996125e35b2ab
SHA-1	6da9bdafdf0b7edc80eaa4643c7d69011072e324
SHA-256	1fc74504d626223335f39e10435bd3366bc5533619e8e7713e2a48eadd4dc26a
Vhash	095096666d1c0d5c05156031602003c001e7z503bz503dz
Authentihash	f9bd023b7ef8679d75d3464abd69b721b8a301b351093bdf27d6528a94ace0ae
Imphash	939d8f743f99c748d946de3c81bddd31
SSDEEP	24576:suRQsAJcBdZF0bE25gAUQIf3c13TOqamxypnUXAGe:sL9JO0jUn
TLSH	T107159E63E6E04C32C07B15B9AD5FEAE4212B7D203D189C4A5FF82D8D5F397A075150AB
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	InstallShield setup (41.6%)
TrID	Win32 Executable Delphi generic (13.7%)
TrID	Windows screen saver (12.6%)
TrID	Win64 Executable (generic) (10.1%)
TrID	DOS Borland compiled Executable (generic) (9.6%)
File size	922.50 KB (944640 bytes)
PEiD packer	BobSoft Mini Delphi -> BoB / BobSoft

History

Creation Time	1992-06-19 22:22:17
First Submission	2021-12-10 14:23:39
Last Submission	2021-12-10 14:23:39
Last Analysis	2021-12-10 18:32:37

Names

rc.exe

8b416273ddf403092ec996125e35b2ab.virus

Portable Executable Info

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	1992-06-19 22:22:17
Entry Point	474312
Contained Sections	9

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	466352	466432	6.56	872d0dc372df370f0d81293b0c1c6843	3315963
.itext	471040	3344	3584	6.05	11e28978a9e7a5f9709958d8e15442c3	45338.8
.data	475136	8260	8704	3.66	886008dbd820a8235961d2cc5b0b0aaa	780880.06
.bss	487424	14848	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
.idata	503808	10160	10240	5.18	4053e614ef9d1fd73eb373d4796c981f	207416.03

?

Community Score

32 security vendors flagged this file as malicious

1fc74504d626223335f39e10435bd3366bc5533619e8e7713e2a48eadd4dc26a

rc.exe

bobsoft peexe

922.50 KB
Size

2021-12-10 18:32:37 UTC
18 hours ago

EXE

DETECTION DETAILS COMMUNITY 4

32 / 67

Community Score

32 security vendors flagged this file as malicious

1fc74504d626223335f39e10435bd3366bc5533619e8e7713e2a48eadd4dc26a

rc.exe

bobsoft peexe

922.50 KB Size

2021-12-10 18:32:37 UTC 18 hours ago

EXE

DETECTION DETAILS COMMUNITY 4

Ad-Aware	Gen:Variant.Zusy.409846	AhnLab-V3	Malware/Win.Generic.C4827103
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	HEUR/AGEN.1202595	BitDefender	Gen:Variant.Zusy.409846
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.DownLoader44.14043	eGambit	Unsafe.AI_Score_89%
Emsisoft	Gen:Variant.Zusy.409846 (B)	eScan	Gen:Variant.Zusy.409846
ESET-NOD32	A Variant Of Win32/Injector.EQQS	FireEye	Gen:Variant.Zusy.409846
Fortinet	W32/Injector.EQQS!tr	GData	Gen:Variant.Zusy.409846
Ikarus	Trojan.Inject	Kaspersky	UDS:DangerousObject.Multi.Generic
Kingsoft	Win32.Troj.Generic_a.a.(kcloud)	Lionic	Trojan.Multi.Generic.4!c
Malwarebytes	Malware.AI.709900288	MAX	Malware (ai Score=87)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	Artemis!8B416273DDF4
McAfee-GW-Edition	BehavesLike.Win32.Worm.dh	Microsoft	Trojan:Win32/Remcos.RVG!MTB
Panda	Trj/GdSda.A	SecureAge APEX	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Sophos	Mal/Generic-S
Symantec	Scr.MalPbs!gen1	TrendMicro-HouseCall	TROJ_GEN.R002C0DLA21
Acronis (Static ML)	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
CAT-QuickHeal	Undetected	ClamAV	Undetected
CMC	Undetected	Comodo	Undetected
CrowdStrike Falcon	Undetected	Cyren	Undetected
Elastic	Undetected	F-Secure	Undetected
Gridinsoft	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected

32 / 67

Community Score

32 security vendors flagged this file as malicious

1fc74504d626223335f39e10435bd3366bc5533619e8e7713e2a48eadd4dc26a

rc.exe

bobsoft peexe

922.50 KB
Size

2021-12-10 18:32:37 UTC
18 hours ago

EXE

DETECTION DETAILS COMMUNITY 4

Comments

joesecurity
5 hours ago

Joe Sandbox Analysis:

Verdict: MAL
Score: 100/100
Classification: mal100.troj.spyw.evad.winEXE@16/15@107/3
Threat Name: Remcos DBatLoader
Malware Config: see the report for the full malware config

Domains: www.uplooder.net nikahuve.ac.ug tuekisaa.ac.ug parthaha.ac.ug kalskala.ac.ug
Hosts: 144.76.120.25 192.168.2.1 185.244.30.199

HTML Report: https://www.joesandbox.com/analysis/538126/0/html
PDF Report: https://www.joesandbox.com/analysis/538126/0/pdf
Executive Report: https://www.joesandbox.com/analysis/538126/0/executive
Incident Report: https://www.joesandbox.com/analysis/538126/0/irxml
IOCs: https://www.joesandbox.com/analysis/538126?idtype=analysisid

intezer_analyze
5 hours ago

Intezer Analyze Genetic Analysis:

Classification: REMCOS
Full Intezer Analyze report: https://analyze.intezer.com/files/1fc74504d626223335f39e10435bd3366bc5533619e8e7713e2a48eadd4dc26a?vt
(code reuse, string reuse, IOCs, TTPs, behavior analysis)

Give your malware a free spin on http://analyze.intezer.com
#REMCOS #IntezerAnalyze

zbetcheckin
6 hours ago

#zbetcheckin tracker
Downloaded on 2021-12-11 06:52:06 UTC
SRC URL : http://pretorian.ac.ug/rc.exe
IP : 185.215.113.77
AS : AS202468 Noyan Abr Arvan Co. (Private Joint Stock)
YARA : #maldoc_function_prolog_signature #ispe32 #embedded_pe #dll_injection_hook #screenshot #delphi_strtoint #create_process #delphi_copy #iswindowsgui #win_hook #delphi_comparecall #keylogger #borland #win_files_operation #borland_delphi #delphi_formshow #contains_pe_file #maldoc_suspicious_strings #bobsoftminidelphibobbobsoft #trojangbotsamplea_malex #win_registry

zbetcheckin
6 hours ago

SRC URL reported to urlhaus.abuse.ch #malicious