SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

<u>Join our Community</u> and enjoy additional community insights and crowdsourced detections, plus an API key to <u>automate checks.</u>

Popular

URL, IP address, domain, or file hash

AhnLab-V3	Malware/Win32.Generic.C4209910
Alibaba	Backdoor:Win32/Kryptik.8648de52
AliCloud	! Backdoor:Win/FlagPro.B
ALYac	Trojan.Agent.Flagpro
Antiy-AVL	Trojan[APT]/Win32.Blacktech
Arcabit	Trojan.Fragtor.D5A915
Arctic Wolf	Unsafe
Avast	Win32:Malware-gen
AVG	Win32:Malware-gen
Avira (no cloud)	! HEUR/AGEN.1312459
BitDefender	. Gen:Variant.Fragtor.370965
Bkav Pro	W32.Common.BFF1CCFD
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
СТХ	Exe.trojan.flagpro
Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS
DrWeb	BackDoor.Flagpro.1
Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Fragtor.370965 (B)
eScan	Gen:Variant.Fragtor.370965
ESET-NOD32	A Variant Of Win32/FlagPro.B
Fortinet	W32/Generic.BFRL!tr
GData	Gen:Variant.Fragtor.370965
Google	. Detected
Gridinsoft (no cloud)	Trojan.Win32.Agent.oa!s1

Ikarus	12023	Virus fotal - File - 34e0e447e004034d3e87fd7787e2130ccf0cc60ade34f240af2cf950ab327f00
Trojan (0058ca8e1) K7GW	Ikarus	Trojan.Win32.Flagpro
Trojan (0058ca8e1) Kaspersky	Jiangmin	! Trojan.Generic.gidky
HEUR:Backdoor.Win32.Flagpro.gen	K7AntiVirus	! Trojan (0058ca8e1)
Lionic	K7GW	! Trojan (0058ca8e1)
Malwarebytes 1	Kaspersky	! HEUR:Backdoor.Win32.Flagpro.gen
MaxSecure Trojan.Malware.7164915.susgen McAfee Scanner Til5466EA47EB04 Microsoft Trojan:Win32/KryptikiMSR Palo Alto Networks Generic.ml Panda Trojan.Ghanarava.1733921866810a25 Rising Backdoor.Flagprol8.13138 (TFE:5:3YIZ3OOfgTE) Sangfor Engine Zero Trojan.Win32.Flagprol8.13138 (TFE:5:3YIZ3OOfgTE) Sangfor Engine Zero Trojan.Win32.Flagprol8.13138 (TFE:5:3YIZ3OOfgTE) Sangfor Engine Zero Malicious SecureAge Malicious Settic Al - Suspicious PE Skyhigh (SWG) BehavesLike.Win32.Generic.gm Sophos Mal/Generic-R Symantec MLAttribute.HighConfidence Tencent Malware.Win32.Genecirc.115db2bc Trapmine Malicious.moderate.ml.score Trellix (ENS) GenericRXRH-KXI287D612E29B7 TrendMicro Backdoor.Win32.BUSYICE.ZYIJ Varist Backdoor.Win32.BUSYICE.ZYIJ Varist W32/ABTrojan.ROHR-1168 VBA32 Trojan.Ymacco VIPRE Gen:Variant.Fragtor.370965 ViRobot Trojan.Win32.S.Agent.440320.DX WithSecure Heuristic.HEUR/AGEN.1312459 Xcitium Malware@#259qxws4j27nr Yandex Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point Trojan.Generic.Win32.1231645 Trojan.Generic.Win32.1231645 Trojan.Generic.Win32.1231645 Trojan.Generic.Win32.1231645 Trojan.Generic.Win32.1231645 Trojan.Generic.Win32.1231645 Trojan.Generic.Win32.1231645 Undetected Undetected ClamAV Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected Undetected	Lionic	! Trojan.Win32.Flagpro.m!c
McAfee Scanner TilS4E6EA47EB04 Microsoft Trojan:Win32/KryptikiMSR Palo Alto Networks Generic.ml Panda Trij/cdsda.A QuickHeal Trojan.Ghanarava.1733921866810a25 Rising Backdoor,Flagprol8.13138 (TFE:5:3YIZ3OOfgTE) Sangfor Engine Zero Trojan.Win32.FlagPro.B SecureAge Malicious SecureAge Malicious Setatic Al - Suspicious PE Skyhigh (SWG) BehavesLike.Win32.Generic.gm Sophos Mal/Generic-R Symantec ML.Attribute.HighConfidence Tencent Malicious.moderate.ml.score Trepliki (ENS) GenericRXRH-KXI287D612E29B7 TrendMicro Backdoor.Win32.BUSYICE.ZYIJ Varist Backdoor.Win32.BUSYICE.ZYIJ Varist W32/ABTrojan.ROHR-1168 VBA32 Trojan.Ymacco VIPRE Gen:Variant.Fragtor.370965 ViRobot Trojan.Win32.S.Agent.440320.DX WithSecure Heuristic.HEUR/AGEN.1312459 Xcitium Malware.Wil259qsws4j27nr Yandex Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point TrojAgent-BFRL Acronis (Static ML) Undetected ClamAV Undetected U	Malwarebytes	! Malware.Al.1404679106
Microsoft Palo Alto Networks Ogeneric.ml Panda Olitri/GdSda.A QuickHeal Olitrojan.Min32.FlagPro.B Rising Olisackdoor.Flagprol8.13138 (TFE:5:3YIZ30OfgTE) Sangfor Engine Zero Olitrojan.Min32.FlagPro.B SecureAge Olimaticous SentinelOne (Static ML) Olisatic Al - Suspicious PE Skyhigh (SWG) Olisacheric-R Symantec Olimature Olimaticous Olimature Olimaticous Olimature Olimaticous Olimature Olimaticous Olimature Olimaticous Olimature Olimaticous Olimaticous Olimaticous PE Ol	MaxSecure	Trojan.Malware.7164915.susgen
Palo Alto Networks (1) Generic.ml Panda (1) Trj/GdSda.A QuickHeal (1) Trojan.Ghanarava.1733921866810a25 Rising (1) Backdoor.Flagprol8.13138 (TFE:5:3YIZ30OfgTE) Sangfor Engine Zero (1) Trojan.Win32.FlagPro.B SecureAge (1) Malicious SentinelOne (Static ML) (1) Static Al - Suspicious PE Skyhigh (SWG) (1) BehavesLike.Win32.Generic.gm Sophos (1) Mal/Generic-R Symantec (1) M.LAttribute.HighConfidence Tencent (1) Malware.Win32.Gencirc.115db2bc Trapmine (1) Malicious.moderate.ml.score Trellix (ENS) (1) GenericXXRH-KX1287D612E29B7 TrendMicro (1) Backdoor.Win32.BUSYICE.ZYIJ TrendMicro-HouseCall (1) Backdoor.Win32.BUSYICE.ZYIJ Varist (1) W32/ABTrojan.ROHR-1168 VBA32 (1) Trojan.Ymacco VIPRE (1) Gen:Variant.Fragtor.370965 ViRobot (1) Trojan.Win32.S.Agent.440320.DX WithSecure (1) Heuristic.HEUR/AGEN.1312459 Xcitium (1) Malware@#259qsws4j27nr Yandex (1) Trojan.lgent.bY4Ngq.2 Zillya (1) Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point (1) Troj/Agent-BFRL Acronis (Static ML) (2) Undetected (2) Undetected (3) Undetected	McAfee Scanner	! Ti!54E6EA47EB04
Panda	Microsoft	Trojan:Win32/Kryptik!MSR
QuickHeal (1) Trojan,Ghanarava.1733921866810a25 Rising (1) Backdoor,Flagprol8.13138 (TFE:5:3YIZ3OOfgTE) Sangfor Engine Zero (1) Trojan,Win32,FlagPro.B SecureAge (1) Malicious SentinelOne (Static ML) (1) Static AI - Suspicious PE Skyhigh (SWG) (1) BehavesLike,Win32,Generic.gm Sophos (1) Mal/Generic-R Symantec (1) M.L.Attribute.HighConfidence Tencent (1) Malware,Win32,Gencirc.115db2bc Trapmine (1) Malicious,moderate,ml.score Trellix (ENIS) (1) GenericRXRH-KX!287D612E29B7 TrendMicro (1) Backdoor,Win32,BUSYICE,ZYIJ TrendMicro-HouseCall (1) Backdoor,Win32,BUSYICE,ZYIJ Varist (1) W32/ABTrojan,ROHR-1168 VBA32 (1) Trojan,Ymacco VIPRE (1) Gen:Variant,Fragtor,370965 ViRobot (1) Trojan,Win32,S.Agent.440320,DX WithSecure (1) Heuristic,HEUR/AGEN.1312459 Xcitium (1) Malware@#259qsws4j27nr Vandex (1) Trojan,Generic,Win32,1231645 ZoneAlarm by Check Point (1) Trojan,Generic,Win32,1231645 ZoneAlarm by Check Point (1) Trojan,Generic,Win32,1231645 Undetected ClamAV (2) Undetected ClamAV (3) Undetected ClamAV (4) Undetected	Palo Alto Networks	
Rising (Panda	
Sangfor Engine Zero SecureAge (I) Malicious SentinelOne (Static ML) Skyhigh (SWG) (I) BehavesLike.Win32.Generic.gm Sophos (I) Mal/Generic-R Symantec (I) Malware.Win32.Gencirc.115db2bc Trapmine (I) Malicious.Moderate.ml.score Trellix (ENS) TrendMicro TrendMicro TrendMicro-HouseCall VBA32 (I) Trojan.Ymacco VIPRE (I) Gen:Variant.Fragtor.370965 ViRobot (I) Trojan.Win32.S.Agent.440320.DX WithSecure Walvare.Win32.Gencirc.Win32.131645 ZoneAlarm by Check Point Acronis (Static ML) Windetected CMC (I) Malicious. (I) Mal/Generic.RX (I) Mal/Generic.RX (I) Mal/Generic.RX (I) Malware.Win32.Gencirc.115db2bc Trapmine (I) Malware.Win32.Busyrice.ZYIJ (I) Backdoor.Win32.Busyrice.ZYIJ (I) W32/ABTrojan.ROHR-1168 (I) Gen:Variant.Fragtor.370965 (I) Trojan.Ymacco VIPRE (I) Gen:Variant.Fragtor.370965 (I) Trojan.Generic.Win32.S.Agent.440320.DX (I) Trojan.Generic.Win32.S.Agent.440320.DX (I) Trojan.Generic.Win32.1231645 (I) Trojan.Generic.Win32.1231645 (I) Trojan.Generic.Win32.1231645 (I) Undetected (I) Undetected (I) Undetected (I) Undetected (I) Undetected (I) Undetected	QuickHeal	
SecureAge (!) Malicious SentinelOne (Static ML) (!) Static AI - Suspicious PE Skyhigh (SWG) (!) BehavesLike.Win32.Generic.gm Sophos (!) Mal/Generic-R Symantec (!) M.Attribute.HighConfidence Tencent (!) Malware.Win32.Gencirc.115db2bc Trapmine (!) Malicious.moderate.ml.score Trellix (ENS) (!) GenericRXRH-KX!287D612E29B7 TrendMicro (!) Backdoor.Win32.BUSYICE.ZYIJ TrendMicro-HouseCall (!) Backdoor.Win32.BUSYICE.ZYIJ Varist (!) W32/ABTrojan.ROHR-1168 VBA32 (!) Trojan.Ymacco VIPRE (!) Gen:Variant.Fragtor.370965 ViRobot (!) Trojan.Win32.S.Agent.440320.DX WithSecure (!) Heuristic.HEUR/AGEN.1312459 Xcitium (!) Malware@#259qsws4j27nr Vandex (!) Trojan.Igent.bY4Ngq.2 Zillya (!) Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point (!) Troj/Agent-BFRL Acronis (Static ML) (!) Undetected CIamAV (!) Undetected	Rising	! Backdoor.Flagpro!8.13138 (TFE:5:3YIZ3OOfgTE)
SentinelOne (Static ML) Skyhigh (SWG) 1 BehavesLike.Win32.Generic.gm Sophos 1 Mal/Generic-R Symantec 1 ML.Attribute.HighConfidence Tencent 1 Malware.Win32.Gencirc.115db2bc Trapmine 1 Malicious.moderate.ml.score Trellix (ENS) 1 GenericRXRH-KX!287D612E29B7 TrendMicro 1 Backdoor.Win32.BUSYICE.ZYIJ TrendMicro-HouseCall 1 Backdoor.Win32.BUSYICE.ZYIJ Varist 1 W32/ABTrojan.ROHR-1168 VBA32 1 Trojan.Ymacco VIPRE 1 Gen:Variant.Fragtor.370965 ViRobot 1 Trojan.Win32.S.Agent.440320.DX WithSecure 1 Heuristic.HEUR/AGEN.1312459 Xcitium 1 Malware@#259qsws4j27nr Yandex 2 ITojan.lgent.bY4Ngq.2 Zillya 1 Trojan.lgent.bY4Ngq.2 Zillya 1 Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point 1 Trojan.Generic.Win32.1231645 Undetected Undetected ClamAV Undetected Undetected	Sangfor Engine Zero	Trojan.Win32.FlagPro.B
Skyhigh (SWG) (1) BehavesLike.Win32.Generic.gm Sophos (1) Mal/Generic-R Symantec (1) M.Attribute.HighConfidence Tencent (1) Malware.Win32.Gencirc.115db2bc Trapmine (1) Malicious.moderate.ml.score Trellix (ENS) (1) GenericRXRH-KX!287D612E29B7 TrendMicro (1) Backdoor.Win32.BUSYICE.ZYIJ TrendMicro-HouseCall (1) Backdoor.Win32.BUSYICE.ZYIJ Varist (1) W32/ABTrojan.ROHR-1168 VBA32 (1) Trojan.Ymacco VIPRE (1) Gen:Variant.Fragtor.370965 ViRobot (1) Trojan.Win32.S.Agent.440320.DX WithSecure (1) Heuristic.HEUR/AGEN.1312459 Xcitium (1) Malware@#259qsws4j27nr Yandex (1) Trojan.Igent.bY4Ngq.2 Zillya (1) Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point (1) Troj/Agent-BFRL Acronis (Static ML) (2) Undetected ClamAV (3) Undetected (4) Undetected	SecureAge	! Malicious
Sophos (1) Mal/Generic-R Symantec (1) ML.Attribute.HighConfidence Tencent (1) Malware.Win32.Gencirc.115db2bc Trapmine (1) Malicious.moderate.ml.score Trellix (ENS) (1) GenericRXRH-KX!287D612E29B7 TrendMicro (1) Backdoor.Win32.BUSYICE.ZYIJ TrendMicro-HouseCall (1) Backdoor.Win32.BUSYICE.ZYIJ Varist (1) W32/ABTrojan.ROHR-1168 VBA32 (1) Trojan.Ymacco VIPRE (1) Gen:Variant.Fragtor.370965 ViRobot (1) Trojan.Win32.S.Agent.440320.DX WithSecure (1) Heuristic.HEUR/AGEN.1312459 Xcitium (1) Malware@#259qsws4j27nr Yandex (1) Trojan.Jegent.bY4Ngq.2 Zillya (1) Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point (1) Troj/Agent-BFRL Acronis (Static ML) (2) Undetected ClamAV (3) Undetected (4) Undetected (5) Undetected	SentinelOne (Static ML)	! Static AI - Suspicious PE
Symantec Tencent I MLAttribute.HighConfidence I Malware.Win32.Gencirc.115db2bc Trapmine I Malicious.moderate.ml.score Trellix (ENS) I GenericRXRH-KX!287D612E29B7 TrendMicro I Backdoor.Win32.BUSYICE.ZYIJ TrendMicro-HouseCall I Backdoor.Win32.BUSYICE.ZYIJ Varist I W32/ABTrojan.ROHR-1168 VBA32 I Trojan.Ymacco VIPRE I Gen:Variant.Fragtor.370965 ViRobot I Trojan.Win32.S.Agent.440320.DX WithSecure I Heuristic.HEUR/AGEN.1312459 Xcitium I Malware@#259qsws4j27nr Yandex I Trojan.lgent.bY4Ngq.2 Zillya I Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point I Troj/Agent-BFRL Acronis (Static ML) Windetected ClamAV Undetected CMC Undetected	Skyhigh (SWG)	
Tencent	Sophos	! Mal/Generic-R
Trapmine	Symantec	
Trellix (ENS) I GenericRXRH-KX!287D612E29B7 TrendMicro I Backdoor.Win32.BUSYICE.ZYIJ Varist I W32/ABTrojan.ROHR-1168 VBA32 I Trojan.Ymacco VIPRE I Gen:Variant.Fragtor.370965 ViRobot I Trojan.Win32.S.Agent.440320.DX WithSecure I Heuristic.HEUR/AGEN.1312459 Xcitium I Malware@#259qsws4j27nr Yandex I Trojan.Igent.bY4Ngq.2 Zillya I Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point I Troj/Agent-BFRL Acronis (Static ML) Windetected ClamAV Undetected ClamAV Undetected CMC	Tencent	
TrendMicro	Trapmine	
TrendMicro-HouseCall Varist ! W32/ABTrojan.ROHR-1168 VBA32 ! Trojan.Ymacco VIPRE ! Gen:Variant.Fragtor.370965 ViRobot ! Trojan.Win32.S.Agent.440320.DX WithSecure ! Heuristic.HEUR/AGEN.1312459 Xcitium ! Malware@#259qsws4j27nr Yandex ! Trojan.Igent.bY4Ngq.2 Zillya ! Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point ! Troj/Agent-BFRL Acronis (Static ML) Dundetected ClamAV Undetected CMC Undetected	Trellix (ENS)	. GenericRXRH-KX!287D612E29B7
Varist UBA32 UFRE UPRE UGen:Variant.Fragtor.370965 ViRobot UITrojan.Win32.S.Agent.440320.DX WithSecure UHeuristic.HEUR/AGEN.1312459 Xcitium Malware@#259qsws4j27nr Yandex UTrojan.Igent.bY4Ngq.2 Zillya UTrojan.Generic.Win32.1231645 ZoneAlarm by Check Point Acronis (Static ML) Widetected Undetected CIamAV Undetected Undetected Undetected	TrendMicro	! Backdoor.Win32.BUSYICE.ZYIJ
VBA32 ① Trojan.Ymacco VIPRE ② Gen:Variant.Fragtor.370965 ViRobot ② Trojan.Win32.S.Agent.440320.DX WithSecure ② Heuristic.HEUR/AGEN.1312459 Xcitium ② Malware@#259qsws4j27nr Yandex ② Trojan.Igent.bY4Ngq.2 Zillya ② Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point ③ Troj/Agent-BFRL Acronis (Static ML) ② Undetected Baidu ③ Undetected ClamAV ③ Undetected	TrendMicro-HouseCall	! Backdoor.Win32.BUSYICE.ZYIJ
VIPRE ① Gen:Variant.Fragtor.370965 ViRobot ① Trojan.Win32.S.Agent.440320.DX WithSecure ① Heuristic.HEUR/AGEN.1312459 Xcitium ② Malware@#259qsws4j27nr Yandex ② Trojan.Igent.bY4Ngq.2 Zillya ② Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point ② Troj/Agent-BFRL Acronis (Static ML) Baidu ② Undetected ClamAV ② Undetected CMC	Varist	
ViRobot ① Trojan.Win32.S.Agent.440320.DX WithSecure ① Heuristic.HEUR/AGEN.1312459 Xcitium ① Malware@#259qsws4j27nr Yandex ② Trojan.Igent.bY4Ngq.2 Zillya ② Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point ③ Troj/Agent-BFRL Acronis (Static ML) ✓ Undetected Baidu ✓ Undetected ClamAV ✓ Undetected CMC ✓ Undetected	VBA32	Trojan.Ymacco
WithSecure	VIPRE	. Gen:Variant.Fragtor.370965
Xcitium ① Malware@#259qsws4j27nr Yandex ① Trojan.lgent.bY4Ngq.2 Zillya ② Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point ① Troj/Agent-BFRL Acronis (Static ML) ☑ Undetected Baidu ☑ Undetected ClamAV ☑ Undetected CMC ☑ Undetected	ViRobot	Trojan.Win32.S.Agent.440320.DX
Yandex ①! Trojan.lgent.bY4Ngq.2 ②! Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point ②! Troj/Agent-BFRL Acronis (Static ML) ③ Undetected ⑥ Undetected ⑥ Undetected ⑥ Undetected ⑥ Undetected	WithSecure	! Heuristic.HEUR/AGEN.1312459
Zillya ① Trojan.Generic.Win32.1231645 ZoneAlarm by Check Point ① Troj/Agent-BFRL Acronis (Static ML) Baidu ○ Undetected ○ Undetected ○ Undetected ○ Undetected	Xcitium	
ZoneAlarm by Check Point ① Troj/Agent-BFRL Acronis (Static ML) Baidu ○ Undetected ○ Undetected ○ Undetected ○ Undetected ○ Undetected	Yandex	
Acronis (Static ML) Baidu ClamAV CMC Undetected Undetected Undetected Undetected	Zillya	Trojan.Generic.Win32.1231645
Baidu	ZoneAlarm by Check Point	Troj/Agent-BFRL
ClamAV	Acronis (Static ML)	✓ Undetected
CMC Undetected	Baidu	✓ Undetected
	ClamAV	✓ Undetected
Huorong Undetected	CMC	✓ Undetected
	Huorong	✓ Undetected

Kingsoft	✓ Undetected
NANO-Antivirus	✓ Undetected
SUPERAntiSpyware	✓ Undetected
TACHYON	✓ Undetected
TEHTRIS	✓ Undetected
VirlT	✓ Undetected
Webroot	✓ Undetected
Zoner	✓ Undetected
Avast-Mobile	Unable to process file type
BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type
Trustlook	Unable to process file type