0b4c743246478a6a8c9fa3ff8e04f297507c2f0ea

Sign in Sign up

SUMMARY | DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 8

Code insights

This sample is a network worm with backdoor capabilities. It actively scans the local network for open SMB ports (TCP/445) using `connect` and `htons(0x1bd)`. It spreads by enumerating and connecting to network shares using `WNetEnumResourceW` and `WNetUseConnectionW`, utilizing unusual UNC paths like `\\?\UNC\\\e-`. The malware achieves privilege escalation by stealing the access token from `explorer.exe`

Show more

Popular threat label ransomware.phobos/smyxccw **Threat categories** ransomw **Family labels** phobos smy

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious
AhnLab-V3	Ransomware/Win.Phobos.R363595
Alibaba	Ransom:Win32/Phobos.665
AliCloud	RansomWare:Win/Phobos
ALYac	Trojan.Ransom.Phobos
Antiy-AVL	Trojan[Ransom]/Win32.Phobos
Arcabit	Trojan.Ransom.PHU
Arctic Wolf	Unsafe
Avast	Win32:Phobos-D [Ransom]
AVG	Win32:Phobos-D [Ransom]
Avira (no cloud)	TR/Crypt.XPACK.Gen
BitDefender	Trojan.Ransom.PHU
Bkav Pro	W32.RansomBeadsBH.Trojan
ClamAV	Win.Ransomware.Ulise-7594403-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.ransomware.phobos
Cynet	Malicious (score: 100)

Elastic	Windows.Ransomware.Phobos
Emsisoft	Trojan.Ransom.PHU (B)
eScan	Trojan.Ransom.PHU
ESET-NOD32	A Variant Of Win32/Filecoder.Phobos.C
Fortinet	W32/FilecoderPhobos.C!tr.ransom
GData	Win32.Trojan-Ransom.Phobos.C
Google	Detected
Gridinsoft (no cloud)	Ransom.Win32.Phobos.ko!s1
Huorong	Ransom/LockFile.kz
Ikarus	Trojan-Ransom.Phobos
Jiangmin	Trojan.Generic.ervnl
K7AntiVirus	Trojan (0055119f1)
K7GW	Trojan (0055119f1)
Kaspersky	HEUR:Trojan-Ransom.Win32.Phobos.vho
Kingsoft	Malware.kb.a.1000
Lionic	Trojan.Win32.Phobos.j!c
Malwarebytes	Generic.Malware.gen.DDS
MaxSecure	Trojan.Malware.200479240.susgen
McAfee Scanner	Ti!0B4C74324647
Microsoft	Ransom:Win32/Phobos.PM
NANO-Antivirus	Trojan.Win32.Filecoder.himsij
Palo Alto Networks	Generic.ml
Panda	Trj/Genetic.gen
QuickHeal	Ransom.Phobos.S11618290
Rising	Ransom.Phobos!1.C277 (CLASSIC)
Sangfor Engine Zero	Ransom.Win32.Phobos_1.se2
SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE
Skyhigh (SWG)	BehavesLike.Win32.RansomPhobos.qc
Sophos	Troj/Phobos-B
SUPERAntiSpyware	Trojan.Agent/Gen-Urelas
Symantec	Ransom.Phobos
TACHYON	Ransom/W32.Dharma.56832
Tencent	Trojan.Ransom.Win32.Phobos.fa
Trapmine	Malicious.moderate.ml.score
Trellix ENS	Ransom-Phobos!2C73B0BF6F09

Varist	W32/Ransom.NA.gen!Eldorado
VBA32	BScope.Trojan.MulDrop
VIPRE	Trojan.Ransom.PHU
VirIT	Ransom.Win32.Phobos.GEN
ViRobot	Trojan.Win32.Ransom.56832.K
Webroot	W32.Ransom.Phobos
WithSecure	Trojan.TR/Crypt.XPACK.Gen
Xcitium	Malware@#26cjdfj3dj37o
Yandex	Trojan.GenAsa!oSQlCZwLKgc
Zillya	Trojan.Filecoder.Win32.17371
ZoneAlarm by Check Point	Troj/Phobos-B
Baidu	Undetected
CMC	Undetected
TEHTRIS	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