

VirusTotal Analysis Report

Generated on: 2025-05-18 16:15:48

VirusTotal Analysis

Hash: 18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

Basic Information

SHA256: 18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

Type: Win32 EXE

Size: 2932642 bytes

First Seen: 2020-06-01

Last Analyzed: 2025-05-08

Detection Rate: 27 / 76

Known Names

- AgentTesla.exe
- Loremipsrm.txt.txt
- AgentTesla.exe.meow
- 18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9.exe
- VERIFICAIE2.exe

Malicious Detections

- **Lionic:** Hacktool.Win32.Generic.3!c
- **MicroWorld-eScan:** Application.HackTool.BEL
- **CTX:** exe.trojan.generic
- **CAT-QuickHeal:** Trojan.Ghanarava.1746696004c09107
- **Skyhigh:** BehavesLike.Win32.Dropper.vc
- **McAfee:** PWS/AgentTesla.b
- **Malwarebytes:** Malware.AI.1765215917
- **Sangfor:** Hacktool.Win32.Agent.Vxkh
- **APEX:** Malicious
- **BitDefender:** Application.HackTool.BEL
- **Tencent:** Win32.Trojan.Malware.Gtgl
- **VIPRE:** Application.HackTool.BEL

- **TrendMicro: Trojan.Win32.NEGASTEAL.DOCMO**
 - **McAfeeD:** ti!18AAB0E981EE
 - **Sophos:** Mal/Generic-R
 - **GData:** Application.HackTool.BEL
- **Varist: W32/ABTrojan.NYCY-8036**
- **Antiy-AVL: Trojan/Win32.Agent**
 - **Arcabit:** Application.HackTool.BEL
 - **Google:** Detected
 - **ALYac:** Application.HackTool.BEL
- **Cylance: Unsafe**
- **TrendMicro-HouseCall: Trojan.Win32.NEGASTEAL.DOCMO**
- **MaxSecure: Trojan.Malware.341102891.susgen**
- **Fortinet: Riskware/AgentTesla**
- **DeepInstinct: MALICIOUS**
 - **alibabacloud:** HackTool:Win/BEL.Gen