

# Malware Analysis Report

## Executive Summary

The file whose SHA-256 hash is `'a2e1ef87d2262539ebc9e22edcd8ebe4a19122250b463ff711279fc587'` is a 32-bit Windows PE/.NET executable that most commercial engines classify as Trojan-Spy: PrimaryPass (a LokiBot-style infostealer written in C#/MSIL). Public sandboxes and vendor encyclopedias agree it is designed to steal credentials (browsers, FTP clients, Outlook) and exfiltrate them to attacker-controlled web servers while maintaining basic persistence.

## 1 · File & Static Meta-data

MD5: 1645f2771891db76683bec08fd77e614

SHA1: 85a9dd456af864ee24653c386d7f88e86d3258c2

SSDEEP: 6144:

li9sNdRQ8xcEI1xwuxV+ft15bswQqFCyxSD3YV3NtUY005BR:ixc11jriftPbuqFZSa9+05BR

Property	Value	Source
SHA-256	a2e1ef87d2262539ebc9e22edcd8ebe4a19122250b463ff711279fc587	user sample
Type	PE32 GUI, .NET assembly (Intel x86)	user file output
Typical size (same family)	~254 KB	
First public sighting (close	11 Aug 2021	

variant)		
VT detection (representative sample)	58 / 70 malicious	

59  
72  
Community Score -76

58/72 security vendors flagged this file as malicious

Reanalyze Similar More

aze1ef87d2262539ebcbe22edcd8eb4a19122250b463ff713279f5873cc47e  
help.exe  
Size 271.50 KB  
Last Analysis Date 4 months ago  
EXE

genre direct-cpu-clock-access detect-debug-environment assembly runtime-modules spreader checks-user-input long-sleeps

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Popular threat label Trojan.MSIL.BASIC Threat categories Trojan Family labels msil basic primarypass

Security vendors' analysis

Security vendor	Detection	Threat category	Family label
AhnLab-V3	Trojan.Win32.MSIL.C2300738	Alibaba	Trojan.Win32.Kryptik.al2000018
AliCloud	Trojan(spy).MSIL/Primarypass.A	ALYac	Trojan.MSIL.BASIC.6.Gen
Arcabit	Trojan.MSIL.BASIC.6.Gen	Arctic Wolf	Unsafe
Avast	Win32.PWSX-gen (Trj)	AVG	Win32.PWSX-gen (Trj)
Avira (no cloud)	HEUR/AGEN.1306897	BitDefender	Trojan.MSIL.BASIC.6.Gen
Bkav Pro	W32.AIDetect/Malware-CS	CrowdStrike Falcon	Win/malicious_confidence_100% (W)

CTX	Exe-trojan.msil	DeepInstinct	MALICIOUS
DrWeb	Trojan.PWS.Stealer.17779	Elastic	Malicious (high Confidence)
Emisssoft	Trojan.MSIL.BASIC.6.Gen (B)	eScan	Trojan.MSIL.BASIC.6.Gen
ESET-NOD32	A Variant Of MSIL/Kryptik.LXI	Fortinet	MSIL/Kryptik.LXI:tr
GData	Trojan.MSIL.BASIC.6.Gen	Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Kryptik.bot/ni	Huorong	Trojan.Generic!1A85A39A748A30AF
Ikarus	Trojan-Downloader.GenKrypt	Jiangmin	TrojanSpy.MSIL.usc
K7AntiVirus	Trojan ( 005200821 )	K7GW	Trojan ( 005200821 )
Kaspersky	HEUR:Trojan-Spy.MSIL.Generic	Kingsoft	Malware.kb.c.1000
Lionic	Trojan.Win32.BASIC.Itc	Malwarebytes	Generic.Crypt.Trojan.DDS
MaxSecure	Trojan.Malware.11205094.susgen	McAfee Scanner	Real Protect-LS!1645F2771891
Microsoft	PWS:Win32/Primarypass.A	NANO-Antivirus	Trojan.Win32.Kryptik.evyoze
Palo Alto Networks	Generic.ml	Panda	Trj/GdSda.A
QuickHeal	Trojan.Ghanaraya.17218146897e614	Rising	Malware.Obfus/MSIL@AI.100 (RDM.MSIL...
Sangfor Engine Zero	Suspicious.Win32.Save.a	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE	Skyhigh (SWG)	BehavesLike.Win32.Generic.dc
Sophos	Mal/Generic-R	Symantec	ML.Attribute.HighConfidence
TEHTRIS	Generic.Malware	Tencent	Malware.Win32.Gencirc.13b/447d
Trappmine	Malicious.high.ml.score	Trellix (ENS)	Packed-WA!1645F2771891
Trellix (HX)	Generic.mg.1645f2771891.db76	TrendMicro	TROJ_FRS.ONA103F523
TrendMicro-HouseCall	TROJ_FRS.ONA103F523	Varist	W32/ABRisk.CQXK-2045
VIPRE	Trojan.MSIL.BASIC.6.Gen	ViRobot	Trojan.Win32.Z.Kryptik.278016.EM
WithSecure	Heuristic.HEUR/AGEN.1306897	Xcitium	Malware@#1wgpw3frnwuol6
Zillya	Trojan.Kryptik.Win32.1327671	Acronis (Static ML)	Undetected

```
(robot@kali) [~/Downloads]
$ file a2e1ef87d2262539ebc9e22edcd8ebe4a19122250b463ff711279fc5873cc47e
a2e1ef87d2262539ebc9e22edcd8ebe4a19122250b463ff711279fc5873cc47e: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections

(robot@kali) [~/Downloads]
$ upx -t a2e1ef87d2262539ebc9e22edcd8ebe4a19122250b463ff711279fc5873cc47e
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2024
UPX 4.2.2      Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 3rd 2024

upx: a2e1ef87d2262539ebc9e22edcd8ebe4a19122250b463ff711279fc5873cc47e: NotPackedException: not packed by UPX

Tested 0 files.

(robot@kali) [~/Downloads]
$ strings a2e1ef87d2262539ebc9e22edcd8ebe4a19122250b463ff711279fc5873cc47e | grep -Ei "http|\\.exe|\\.dll|cmd|powershell|password|base64"
mscorlib.dll
(robot@kali) [~/Downloads]
$
```

2 · Behaviour Overview

The following table summarizes the behavior of the malware:

Stage	Observed actions	Key APIs / artefacts
Initial execution	Checks for debuggers, reads computer & MachineGUID	NtQueryInformationProcess, reg key ...ACTIVE-COMPUTERNAME
Persistence	Drops copy to %APPDATA%\sdsdsdsd.exe and adds a Startup entry	file write to %User Startup%
Credential theft	Enumerates Outlook profiles, browsers, FTP client databases	registry & file scans, ReadProcessMemory on lsass.exe
Data exfiltration & C2	HTTP POST to hard-coded PHP endpoints	HttpWebRequest, Suricata LokiBot rules triggered
Cleanup / stealth	Marks itself for deletion, deletes .lck files	DeleteFileW, MoveFileEx

3 · Indicators of Compromise

File Hash (this sample):  
a2e1ef87d2262539ebc9e22edcd8ebe4a19122250b463ff711279fc587

Typical dropped file: %APPDATA%\sdsdsdsd.exe

Folder created: %APPDATA%\CD572E\

Registry paths touched: HKCU\...\OUTLOOK\PROFILES,  
HKLM\SOFTWARE\\*ICEDRAGON\*

C2 / URLs (family): <http://fuckav.ru>, <http://jiren.ru/chief/maoyr.scr>,  
<http://sharonbooks.ru/.../fred.php>

IP seen: {BLOCKED}.30.134

#### 4 · MITRE ATT&CK Mapping

Technique	ID	Phase
Service/Process execution	T1035	Execution
Run keys / Startup folder	T1060	Persistence
Hooking (credential access)	T1179	Priv-Esc & Cred-Access
File deletion for cleanup	T1107	Defense Evasion
Query Registry / Machine info	T1012	Discovery
Exfil via HTTP POST	T1041	Exfiltration

#### 5 · Why It Matters

PrimaryPass/LokiBot variants are commodity stealers popular in mal-spam. They:

- Monetise by selling stolen FTP/SMTP creds and browser passwords on underground markets.
- Act as downloaders, fetching follow-on ransomware when creds are exhausted.
- Evolve fast; most samples are lightly obfuscated .NET, making recompilation trivial for attackers.

#### 6 · Remediation & Hunting Checklist

- Quarantine the sample & images of affected hosts.
- Block IOC domains/IPs on firewalls & proxy.
- Search for dropped artefacts (sdsdsdsd.exe, CD572E) across endpoints.
- Reset all credentials captured on infected machines—especially Outlook, browser, FTP.

- Deploy YARA / Sigma rules that flag  
MachineGuid.\*last\_compatible\_version.\*password\_value.
- Patch & harden: Ensure users cannot write to Startup without admin; enable AMSI + Defender SmartScreen.
- Monitor egress for unusual HTTP POSTs with no referrer and content-type application/x-www-form-urlencoded.

This indicates a .NET-based Trojan, likely written in C# or VB.NET.