

fa71eee906a7849ba3f4bab74edb577bd1f1f8397ca428591b4a9872ce1f1e9b

↑

🗨

?

⚙

Sign in

Sign up

34

/ 61

Community Score

-1

⚠

34/61 security vendors flagged this file as malicious

↻

Reanalyze

⌵

Similar

⌵

More

⌵

fa71eee906a7849ba3f4bab74edb577bd1f1f8397ca42859...

Size

500.00 KB

Last Analysis Date

2 years ago

W

≡

DOC

doc

open-file

exe-pattern

run-file

macros

environ

write-file

executes-dropped-file

create-ole

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY8

Join our Community

 and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

✓

BitDam ATP

⚠1

M0

📅0

📁0

📡0

🔗0

🔍0

✓

C2AE

⚠0

M0

📅0

📁0

📡0

🔗0

🔍3

✓

Dr.Web vx...

⚠2

M0

📅5

📁0

📡6

🔗7

✓

Lastline

⚠1

M0

📅0

📁0

📡0

🔗3

✓

Tencent H...

⚠0

M0

📅0

📁0

📡0

🔗3

✓

VMRay

⚠1

M0

📅0

📁0

📡2

🔍3

✓

VirusTotal...

⚠0

M0

📅0

📁0

📡0

🔍0

Activity Summary

Download Artifacts⌵

Full Reports⌵

Help⌵

⚠2 Detections

4 MALWARE1 EXPLOIT

📅IDS Rules

2 MEDIUM3 LOW

📡Dropped Files

4 OTHER1 SCRIPT1 DOC1 TEXT

🔍Mitre Signatures

NOT FOUND

📁Sigma Rules

NOT FOUND

🔗Network comms

5 HTTP4 DNS2 IP

Behavior Tags ⓘ

detect-debug-environmentexecutes-dropped-file

Dynamic Analysis Sandbox Detections ⓘ

⚠

The sandbox VMRay flags this file as: MALWARE

⚠

The sandbox Dr.Web vxCube flags this file as: MALWARE EXPLOIT

⚠

The sandbox Lastline flags this file as: MALWARE

⚠

The sandbox BitDam ATP flags this file as: MALWARE

Crowdsourced IDS rules ⓘ

⚠🔍

Matches rule DECODE_IP_OPTION_SET at Snort registered user ruleset

↳ bad-unknown

⚠🔍

Matches rule PSNG_UDP_PORTSWEEP_FILTERED at Snort registered user ruleset

↳ bad-unknown

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Notice](#).

Ok

Page 1 of 6

Sign in

Sign up

C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\index.dat

C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\sample.LNK

C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\本地磁盘 (C).LNK

C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Word11.pip

C:\Users\Administrator\AppData\Roaming\Microsoft\Office\version.xml

Files Deleted

%APPDATA%\microsoft\network\conv.xml

%APPDATA%\microsoft\network\sr011.xml

<CURRENT_DIR>\~wrd0000.tmp

C:\Users\Administrator\AppData\Local\Temp\~DF034833442AED0C36.TMP

C:\Users\Administrator\AppData\Local\Temp\~DF040BD01F855F1680.TMP

C:\Users\Administrator\AppData\Local\Temp\~DF0D89955EA9D6DC2F.TMP

C:\Users\Administrator\AppData\Local\Temp\~DF0E709D17CC2E4723.TMP

C:\Users\Administrator\AppData\Local\Temp\~DF315C367CE5D36DC6.TMP

C:\Users\Administrator\AppData\Local\Temp\~DF416F62307ED31089.TMP

C:\Users\Administrator\AppData\Local\Temp\~DF5224E8B00D3CFDED.TMP

Files Copied

<CURRENT_DIR>\~wrd0000.tmp

C:\PROGRA~2\MICROS~1\OFFICE\DATA\OPA11.BAK

C:\sample.doc

C:\~WRD0002.tmp

Files With Modified Attributes

<CURRENT_DIR>\~wrd0000.tmp

<CURRENT_DIR>\~wrl0001.tmp

C:\Users\Mason\AppData\Roaming\Microsoft\Office\Recent\index.dat

C:\Users\Mason\Documents\~WRD0000.tmp

C:\Users\Mason\Documents\~WRD0002.tmp

C:\Users\Mason\Documents\~WRL0001.tmp

C:\Users\Mason\Documents\~WRL0003.tmp

Files Dropped

%APPDATA%\microsoft\network\conv.xml

%APPDATA%\microsoft\network\sr011.xml

<CURRENT_DIR>\~wrd0000.tmp

<PATH_SAMPLE>.doc

<SYSTEM32>\tasks\ahnlabupdate

data.txt

9fe3031c7df47e30c8eb99dfe80ffdece11c9421fb2ca5566ddf82759a2f0989

C:\Users\FD1HVy\AppData\Roaming\Microsoft\Office\version.xml

Registry actions

Registry Keys Opened

<HKCU>\Software








<HKCU>\Software\Microsoft

<HKCU>\Software\Microsoft\Office

<HKCU>\Software\Microsoft\Office\14.0\Excel\Security

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Notice](#).

Ok











-  \Sessions\1\BaseNamedObjects\Local\ZonesCounterMutex
-  \Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex
-  Local\F99C425F-9135-43ed-BD7D-396DE488DC53_Office16
-  Local\SM0:1456:304:WilStaging_02
-  Local\SM0:1836:304:WilStaging_02
-  Local\SM0:3340:304:WilStaging_02
-  DBWinMutex



Modules loaded ⓘ



Runtime Modules

-  c:\program files\common files\microsoft shared\office16\mso.dll
-  c:\program files\common files\microsoft shared\office16\mso20win32client.dll
-  c:\program files\common files\microsoft shared\office16\mso30win32client.dll
-  c:\program files\common files\microsoft shared\office16\mso40uiwin32client.dll
-  c:\program files\common files\microsoft shared\office16\mso50win32client.dll
-  c:\program files\common files\microsoft shared\office16\mso98win32client.dll
-  c:\program files\common files\microsoft shared\office16\msptls.dll
-  c:\program files\common files\microsoft shared\office16\riched20.dll
-  c:\program files\common files\microsoft shared\vba\vba7.1\1033\vbe7intl.dll
-  c:\program files\common files\microsoft shared\vba\vba7.1\vbe7.dll



Highlighted actions ⓘ



Highlighted Text

-  "MSO Generic Control Container"
-  "Microsoft Word 文档"
-  "MsoDockTop"
-  "sample - Microsoft Word"
-  "sample"
-  "常用"
-  "格式"
-  "菜单栏"

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