

JOeSandbox Cloud BASIC



ID: 404291

Sample Name: Bio-Solid Feed
Stock Evaluation_.docx

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 21:46:01

Date: 04/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report Bio-Solid Feed Stock Evaluation_.docx	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Startup	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Signature Overview	3
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	10
General	11
File Icon	11
Network Behavior	11
Code Manipulations	11
Statistics	11
System Behavior	11
Analysis Process: WINWORD.EXE PID: 2464 Parent PID: 584	11
General	11
File Activities	12
File Created	12
File Deleted	12
File Written	12
File Read	12
Registry Activities	12
Key Created	12
Key Value Created	12
Key Value Modified	14
Disassembly	16

Analysis Report Bio-Solid Feed Stock Evaluation_.docx

Overview

General Information

Sample Name:	Bio-Solid Feed Stock Evaluation_.docx
Analysis ID:	404291
MD5:	a829fa8a85650dd.
SHA1:	22964385dc0064..
SHA256:	08bcf8510cbfb3a..
Infos:	
Most interesting Screenshot:	

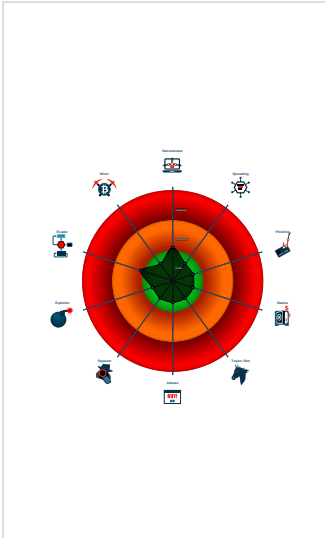
Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- System is w7x64
- WINWORD.EXE (PID: 2464 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection



Click to jump to signature section

There are no malicious signatures, [click here to show all signatures](#).

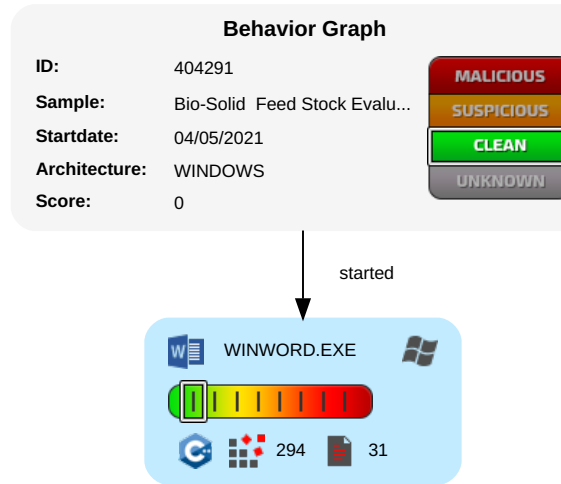
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Behavior Graph

Legend:

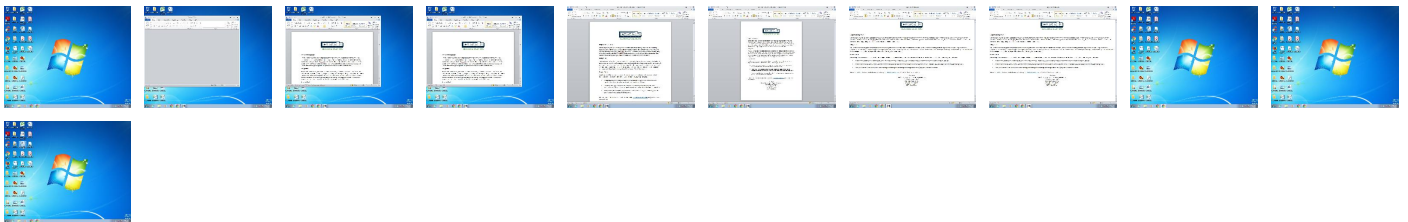
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

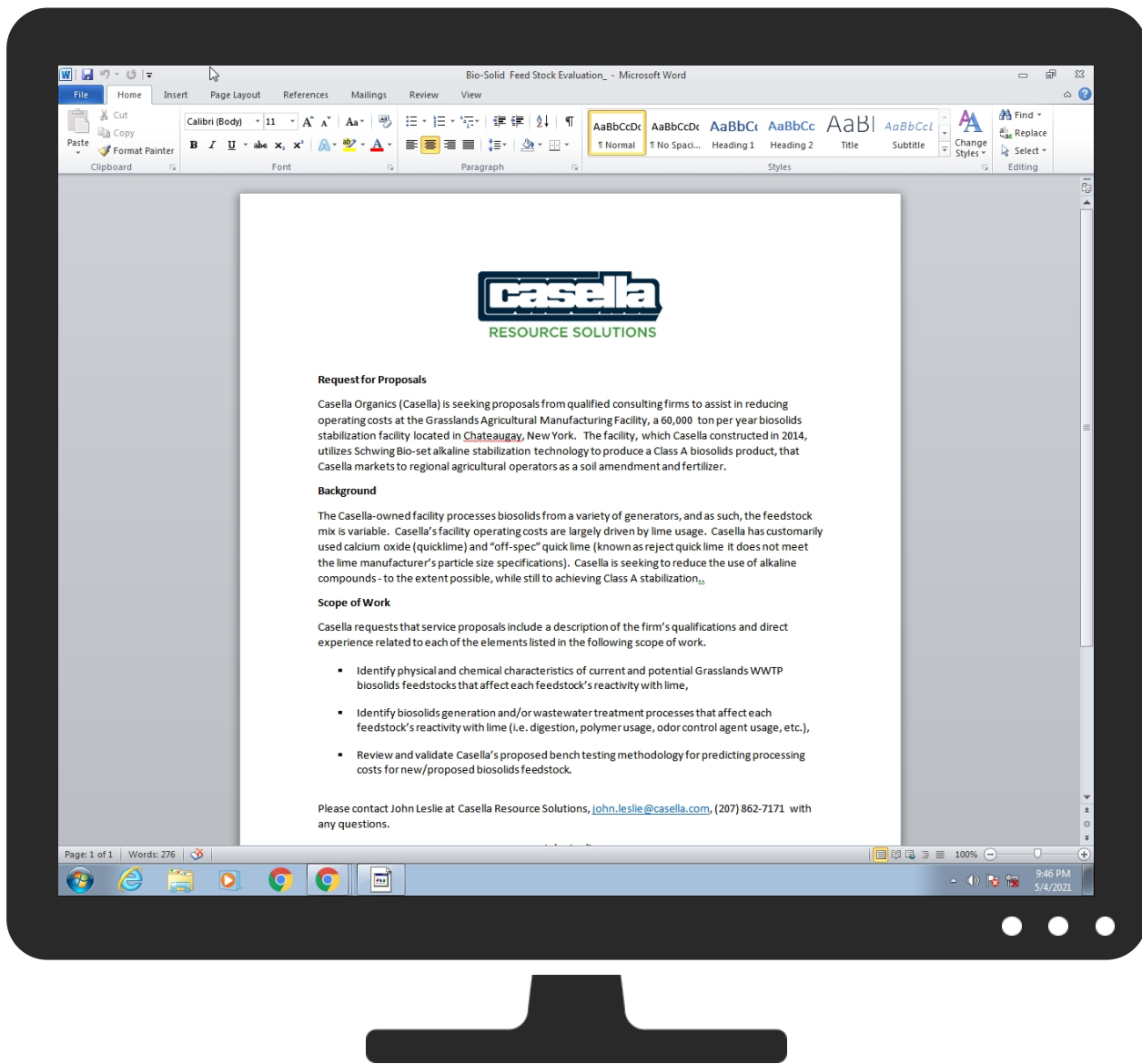


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404291
Start date:	04.05.2021
Start time:	21:46:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bio-Solid Feed Stock Evaluation_.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	2
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none">• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winDOCX@1/9@0/0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .docx• Found Word or Excel or PowerPoint or XPS Viewer• Attach to Office via COM• Scroll down• Close Viewer
Warnings:	Show All <ul style="list-style-type: none">• Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F34D05A3.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 228 x 81, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	12912
Entropy (8bit):	7.980657944433155
Encrypted:	false
SSDEEP:	192:t/mdfXGmMfhQ7E0FyUm177+dZlivT4moRWzLGwk9o4fGXjER/U7:Uh22FyidZIMURWzHYGTz7
MD5:	91251E9C2886771106FA67FA469EC2D2
SHA1:	F10256D1480FB009A2AC58F80A6BDDD6269A2FBE
SHA-256:	67A26E18A62AA8C2E7919BDA7B1DA3089DD262993AD7C88B0ACBAB9F8A265C3A
SHA-512:	2D34B014640350DEA9B913661744149E053C0901F465DFD4F236010BD521C55E842923463CEA51A6009411A65D4AD37CB1C767C25FA6C9C547F831E4E1025781
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....Q.....P.K....sRGB.....pHYs.....+.....tEXtSoftware:Microsoft Office..5q..1.IDATx^}.]SU.....t....e...ED\..D*.X.bE.....od!.n.[...D*v.....a.Ed.D....Ji.6{...\$]..M.;..4...s..{.....-w..AD_+_J..j.D0.....[Ex.6"a.A\.....2...n..xA.....%r.....>...@..=.V.j..D.5G.fnw...4....<..`..y\..#.....Z..,{G..._.....".F..\F.s.v}0..6.6=\..pzx.~+.S.rXw...s""...D.....e..v....."4....p..u.....N..W3...R..1..9.]r.B..(.~--3...PA.#..s...!..e.....3...&..y..8..a...l.;HD....&.....y..Tx...^,!....;`....[7.XL\w....D...1..=m.e.m.Z.j.....R`F....n.qV.....".K...k;y..T.N.....9..)....Q_..Z.....T8P;....[.?.a).....8.E...i4...;~"...B....H4.0..].....JW..oHK.#!.!..V..\C M;fH.!...o.V... ..b..A.v.....:".s...q...B ...%c..6.....A.v.../T0Pf...<l.-.m8.....{..2b.....p..J... ""f...A'9.."h+n..ep.U.....F.C...JJJ.A.....o.....q.fH;...&b.Y.{g...z.6!32.K... ..O"...c..ID..K...z"D.[.....l..uE[H...lZ....fy

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A5D2E9EE-EB6B-4CC4-8C38-663EBE143117}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCEED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B9C27487-05CF-4B4D-9086-2A6225ABAACB}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B9C27487-05CF-4B4D-9086-2A6225ABAACB}.tmp	
Size (bytes):	5558
Entropy (8bit):	3.2100491303624255
Encrypted:	false
SSDEEP:	96:chjmS4+HTlw8suFs53hgMNXhc+QUAu777+FKb6:cdHT3ys5fRhHiV
MD5:	A60DB88EF4FFB9F449F3E51D43168EE7
SHA1:	6A2E3B8C49C438B68AE9601C8C4EA371321C848D
SHA-256:	0B81F0B817CAD98516763E79B4E774E8EC2972AC3C957408173D3D1D96D21197
SHA-512:	BFDAD2ADBA0796F6BDB831F493C841FE7F0F5B5641F9D8A331B06C63990CE32236417591CBAE90E64AF91B86D71B5759D756BB2843A47A041392A7E4515FBACA
Malicious:	false
Reputation:	low
Preview:	..I.....R.e.q.u.e.s.t. f.o.r. P.r.o.p.o.s.a.l.s.....4.....<...J...L.....\$..a\$.gd.u.....&..F.....gd..#.....

C:\Users\user\AppData\Local\Temp\msodd26.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlojAxb4bxdT/CS3wKxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWkbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6B3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA87E41
Malicious:	false
Reputation:	high, very likely benign file
Preview:	GIF89a.....w...I..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3..!..MSOFFICE9.0.....cmPPJCmp0712.....!.....!.....'.;.b...RQ.xx.....,+......yy..;.b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@...zz.mm.^_.....yw.....yx.xw.RR.,*..+.....C.?....A;<...HT(;;

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Bio-Solid Feed Stock Evaluation_.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:20 2020, mtime=Wed Aug 26 14:08:20 2020, atime=Wed May 5 03:46:40 2021, length=28469, window=hide
Category:	dropped
Size (bytes):	2268
Entropy (8bit):	4.574660972096106
Encrypted:	false
SSDEEP:	48:83r/XTDkd2zaXXhnTXxKI4Qh23r/XTDkd2zaXXhnTXxKI4Q/:83r/X/kYz4dx+4Qh23r/X/kYz4dx+4Q/
MD5:	2D0048AE9D9308838733763C844BC16B
SHA1:	7EE0B5BA1B00D3A43A976566C9C0B7C513B079AF
SHA-256:	6D98F879B6BAE75D7A29EB72BECC11BAF1AE6E60330F71994776E66D5FF88C6
SHA-512:	723E0FA27211FA183248C09CFC468A20EBA788FOCB8950492DF554AE05AA1D1FFEDB13C27833B8F6B61628EFC79914E73C00D41B9C86132870B99FD2FDA0E2D
Malicious:	false
Reputation:	low
Preview:	L.....F.....7..{....7..{...&..iA..5o.....P.O. .i.....+00../C:\.....t.1.....QK.X..Users.`.....QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=...U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._...=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-2 .1.7.6.9.....2.5o...R.% .BIO-SO~1.DOC..z.....Q.y.Q.y*...8.....B.i.o.-.S.o.l.i.d. .F.e.e.d. S.t.o.c.k. .E.v.a.l.u.a.t.i.o.n_...d.o.c.x.....-8...[.....?J....C :\Users\.#.....\701188\Users.user\Desktop\Bio-Solid Feed Stock Evaluation_.docx=.....\.....\.....\.....\D.e.s.k.t.o.p\B.i.o.-.S.o.l.i.d. .F.e.e.d. S.t.o.c.k. .E .v.a.l.u.a.t.i.o.n_...d.o.c.x.....,LB.)...Ag.....1SPS.XF.L8C...&m.m.....-...S.-.1.-5.-2.1-.9.6.6.7.7.1.3.1.5.-3.0.1.9.4.0.5.6.3.7.-3.6.7.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.735460987802341
Encrypted:	false
SSDEEP:	3:HsMT21MREg0Q4MQ1YVo/n1MREg0Q4MQ1YVomxWsMT21MREg0Q4MQ1YVov:HiT21zVQ4MoYV0n1zVQ4MoYVkt21zVQU
MD5:	A75C3408A0E9FAB34249CA1CC8463704

C:\Users\user1\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA1:	151B69B6ACBA4155A200E65B478FAFF5210AC4E0
SHA-256:	59DC58B0FDEE1FBAEE9ACE1EF57AB9FA1F0F80A065DC752BE537255FBCECF042B
SHA-512:	F0CD866421A349C7837AA2D38D2897D01D9C50CC5CF31586F25876387B404CC458F21E04B75028C0B7165918C445D5D90A1F5F6F62B95FAA466556A2D93710ED
Malicious:	false
Reputation:	low
Preview:	[misc]..Bio-Solid Feed Stock Evaluation_.LNK=0..Bio-Solid Feed Stock Evaluation_.LNK=0..[misc]..Bio-Solid Feed Stock Evaluation_.LNK=0..


C:\Users\user1\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54DEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.I.b.u.s.....p.....P.....Z.....X...

C:\Users\user1\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user1\Desktop~-Solid Feed Stock Evaluation_.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54DEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.I.b.u.s.....p.....P.....Z.....X...

Static File Info

General	
File type:	Microsoft Word 2007+
Entropy (8bit):	7.711910442031405
TrID:	<ul style="list-style-type: none">Word Microsoft Office Open XML Format document (49504/1) 49.01%Word Microsoft Office Open XML Format document (43504/1) 43.07%ZIP compressed archive (8000/1) 7.92%
File name:	Bio-Solid Feed Stock Evaluation_.docx
File size:	28469
MD5:	a829fa8a85650dde608ada79d3ba4f11
SHA1:	22964385dc00646b24d1203b8d7c4520c8e7704c
SHA256:	08bcf8510cbfb3a81777399682e35f05046d285e7c401b97874f9149113ddc88
SHA512:	c2388a4b6a087f10a35bbba71958b8b3e3342ca818bfdb2f6a3f4d04f1b42e696b4c294cab07cf55b75d1ff4d66852bed35e08f89255a3798a259f1db4bf4a70
SSDEEP:	384:r+B8tLLwWWAh22FyidZIMURWzHYGTzvNxt/ZtNN4CRc4/NodMyXTzf:rBLLws82FrIPRKTpxlIN4GNbe
File Content Preview:	PK.....!.!.]p.....[Content_Types].xml ...(.

File Icon	
	
Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior
No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2464 Parent PID: 584	
General	
Start time:	21:46:40
Start date:	04/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fe60000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VE	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7FEE95226B4	CreateDirectoryA
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionary\EN0409.lex	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	7FEE93DEB92	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~\$o-Solid Feed Stock Evaluation_.docx	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionary\EN0409.lex	unknown	2	ff fe	..	success or wait	1	7FEE93DECEB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE93DEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE93E6CAC	ReadFile
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	310	success or wait	1	7FEE91EE8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionary\EN0409.lex	unknown	1	end of file	1	7FEE93DEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionary\EN0409.lex	unknown	4096	success or wait	1	7FEE93E6CAC	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionary\EN0409.lex	unknown	1	success or wait	1	7FEE91E0793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionary\EN0409.lex	unknown	4096	success or wait	1	7FEE924AD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE91E0793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE924AD58	ReadFile
C:\Users\user\Desktop\Bio-Solid Feed Stock Evaluation_.docx	4961	360	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSOF34D05A3.png	0	12912	success or wait	1	7FEE9449AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4E5F	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 FF FF FF FF				

Key Value Modified

[illegible]

