ID: 753420
Sample Name: SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:47:12
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Disassembly 15

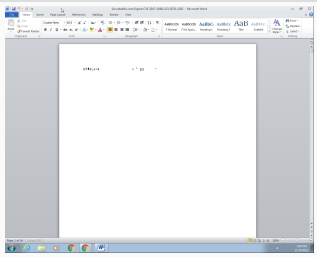
Windows Analysis Report

SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc

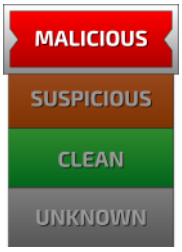
Overview

General Information

Sample Name:	SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc
Analysis ID:	753420
MD5:	d38967e524822d.
SHA1:	b2af456f879fba7..
SHA256:	5e458e56f23f18f..
Tags:	CVE-2017-11882 doc
Infos:	



Detection

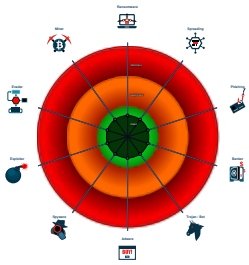


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2924 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

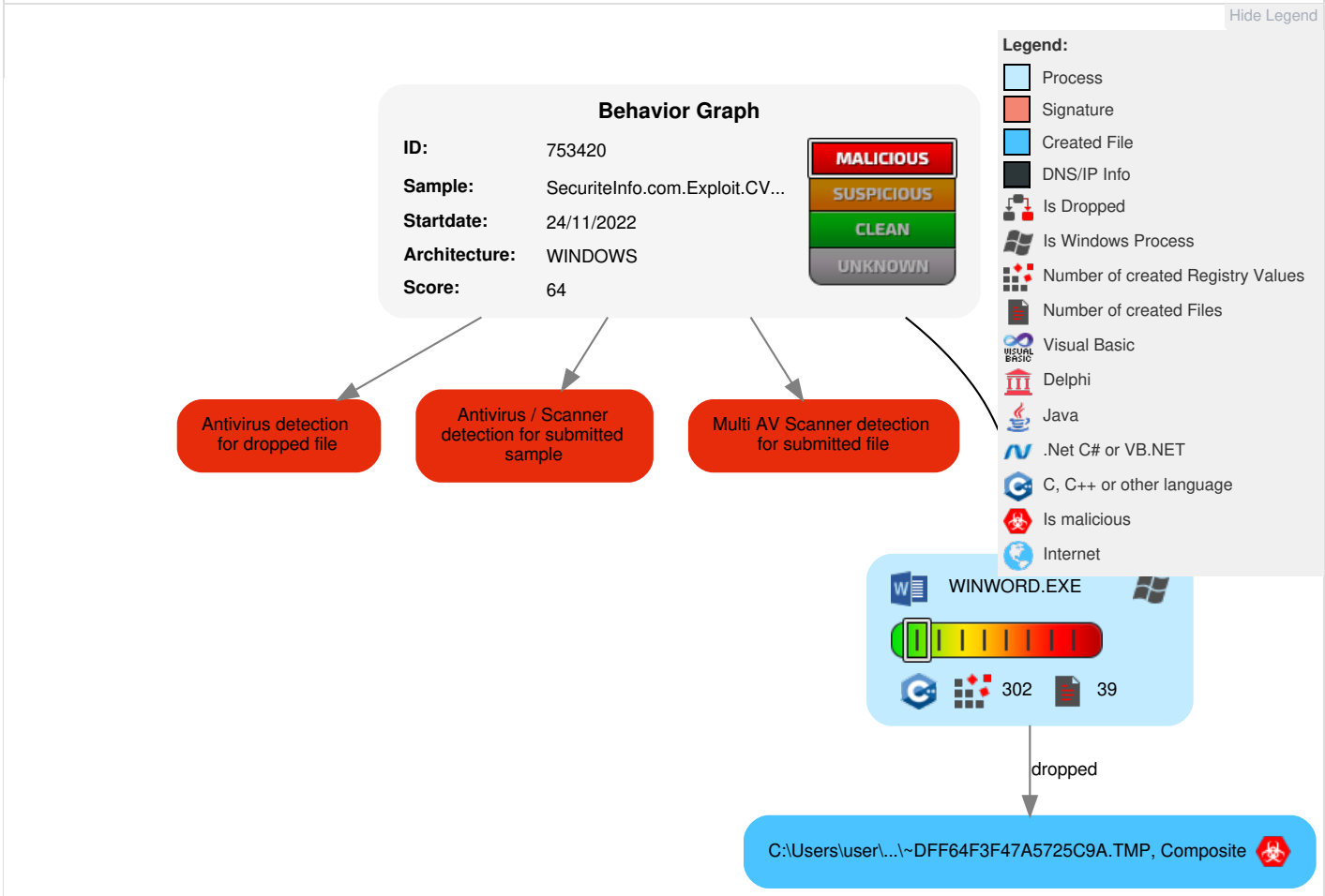
Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

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	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	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	1 System Information Discovery	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

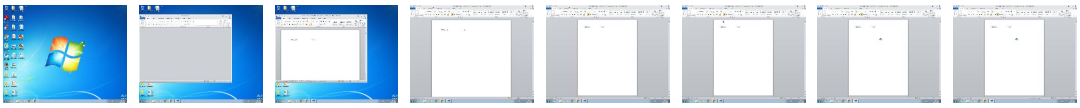
Behavior Graph

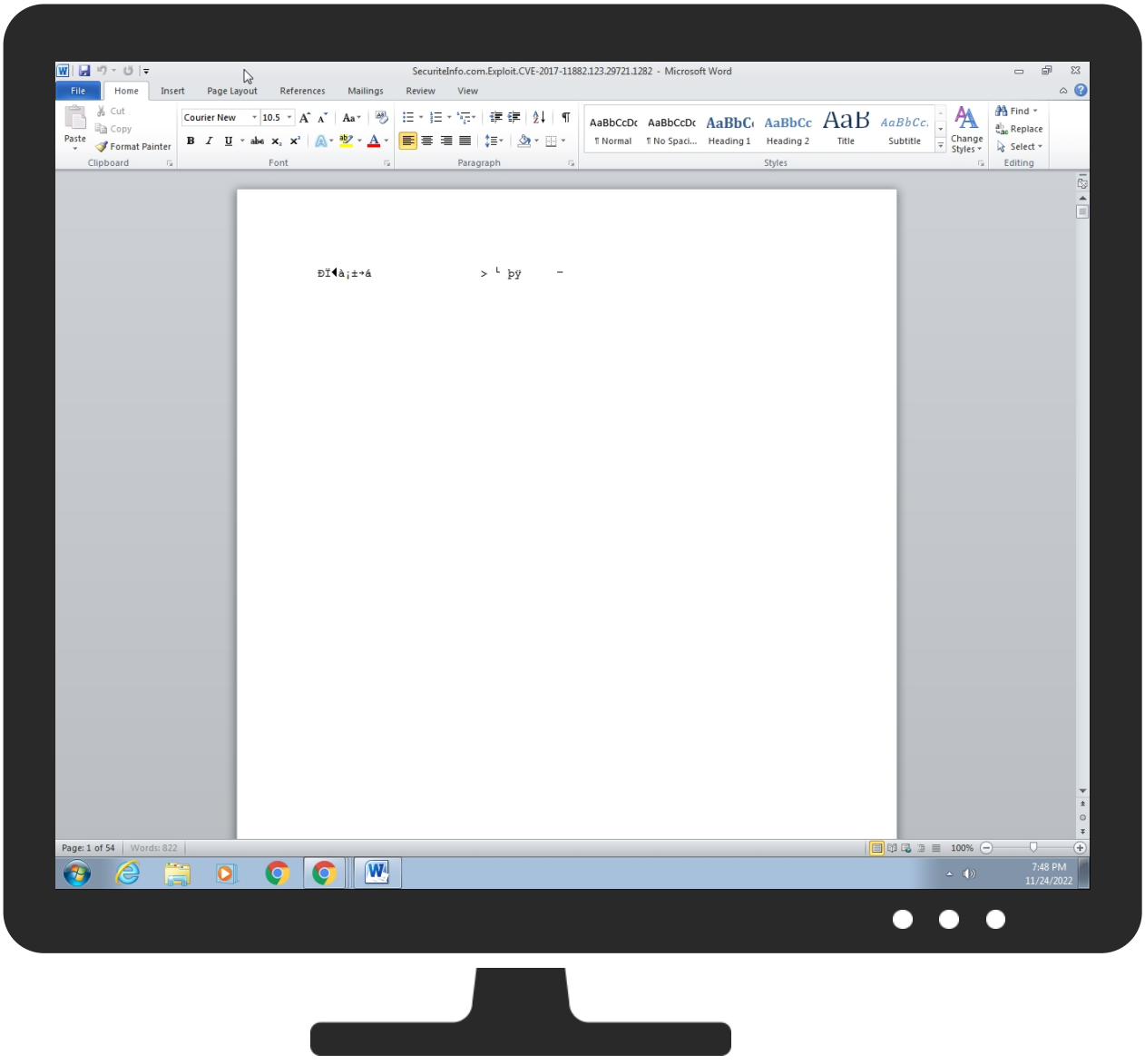


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc	54%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc	52%	Virustotal		Browse
SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc	100%	Avira	EXP/CVE-2017-11882.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DFF64F3F47A5725C9A.TMP	100%	Avira	EXP/CVE-2017-11882.Gen	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753420
Start date and time:	2022-11-24 19:47:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	3
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.winDOC@1/14@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM

Warnings

- Max analysis timeout: 600s exceeded, the analysis took too long
- Exclude process from analysis (whitelisted): dllhost.exe
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\~DF23E789C223CE7F7B.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE

Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF28FBF22284A5B139.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF362AD5CB9CB152F7.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF4527151DCDBAA200.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF720F595F6C8E4C8E.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF740AB3E24B9A2D46.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF827CFBD4FFBE378D.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFA98B7F78D7D35817.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B

SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFF64F3F47A5725C9A.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	910336
Entropy (8bit):	6.01945829773662
Encrypted:	false
SSDEEP:	24576:5LMu/lUHGguNaUgjg+NkTgThiNkKBnv/E:51Kmg6RsOE
MD5:	D38967E524822D04257534078B0DC209
SHA1:	B2AF456F879FBA7DFFA694D9386F501883118822
SHA-256:	5E458E56F23F18FEB1E44F3EB3C15AB7D4D6CD9E937C72528DFCE9D5E195EA3C
SHA-512:	E6124B681EC75A45400EB822EA2F558B7B2D3CDFE6B3AFCCF4D03FE15E4934AD39AB8EF77DEE74ED4A20A506D3605DD606D5D91700013D8FD5419A51F1F98A5F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.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=Tue Mar 8 15:45:51 2022, mtime=Tue Mar 8 15:45:51 2022, atime=Fri Nov 25 02:48:08 2022, length=910336, window=hide
Category:	dropped
Size (bytes):	1234
Entropy (8bit):	4.529455937298715
Encrypted:	false
SSDEEP:	24:8K//XTm3xqf4pTHCdOLecxHCdOwDv3qKl4u7D:8K//XTQx3THCuvHCgKl40D
MD5:	20E88DD98EBB85FC4745B4C4037C4222
SHA1:	949720B3320146FCEB55315C401CA8119D98BB2B
SHA-256:	A2150297F980849183854665A9841571002F7D292005156315A05AEA52DECBA3
SHA-512:	26F3F878C338B2CCE7F38A9649063CF633F088F92F87C96321C9A49C0B2518179F360385784CBD85AADB00DB8A1E44C45FBE4054336B3254122B583DB869339B
Malicious:	false
Preview:	L.....F.... ....n...3...n...3..r.....'....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.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....yU.. .SECURI~1.DOC.....hT..hT..*...r.....'.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...C.V.E.-.2.0.1.7.-.1.1.8.8.2...1.2.3...2.9.7.2.1...1.2.8.2...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\701188\Users.user\Desktop\SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc.Q.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...C.V.E.-.2.0.1.7.-.1.1.8.8.2...1.2.3...2.9.7.2.1...1.2.8.2...d.o.c.....:...,.LB.)...Ag.....1SP

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Generic INItialization configuration [doc]
Category:	dropped
Size (bytes):	159
Entropy (8bit):	4.9470059760402645
Encrypted:	false
SSDEEP:	3:bDuMJluscbcK+JiMXjEYdrXCmX1n8bcK+JiMXjEYdrXCv:bCVwKNcKwKNcI
MD5:	1EB5BE23C9F80FF12073FD8CC0905820
SHA1:	276033018F0E63FA3D0E544387276A6AA75905C7
SHA-256:	F8930A570B7580840EE7A3C469CEEBFC7DB7AAE538DF98FF22B7EE6D65A6AD8B
SHA-512:	001930C1A25BEA8EE8AD8820737DE73FC9431B67CD6DBC58595C94B18FB4441EAA302A496A72795CBCC0E7793120335B23B4562FE8266E1A5A42723FF9EEE7B7
Malicious:	false

Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.LNK=0..[doc]..SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.LNK=0..

C:\Users\user\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):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian 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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$curiteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Cannot read section info
Entropy (8bit):	6.01945829773662
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%

File name:	SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc
File size:	910336
MD5:	d38967e524822d04257534078b0dc209
SHA1:	b2af456f879fba7dffa694d9386f501883118822
SHA256:	5e458e56f23f18feb1e44f3eb3c15ab7d4d6cd9e937c72528dfce9d5e195ea3c
SHA512:	e6124b681ec75a45400eb822ea2f558b7b2d3cdfe6b3afccf4d03fe15e4934ad39ab8ef77dee74ed4a20a506d3605dd606d5d91700013d8fd5419a51f1f98a5f
SSDEEP:	24576:5LMu/lUHGguNaUgjg+NkTgThiNkKBnv/E:51Kmg6RsOE
TLSH:	A2152340EE581F93C75A46396A1BC63C67D3BF5D831FC0F72BE2358A2A78B710886546
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Exploit.CVE-2017-11882.123.29721.1282.doc"

Indicators

Has Summary Info:	
Application Name:	None
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Streams

Stream Path: \x1oLe10NatIVE, File Type: data, Stream Size: 900632

General

Stream Path:	\x1oLe10NatIVE
File Type:	data
Stream Size:	900632
Entropy:	5.969638510456594
Base64 Encoded:	True
Data ASCII:	I x . . T . . y . . V K M .) q = y # . x ; U . (- (7 C . * . 8 9 ~ . . : 3] . . e Q } . > w v ' H [= Z a . . j A . n . & \\ @ . p N . | s . 2 f 6 k) - V 1 8 " - # ~ F ' E b A 0 . D C * J _ M (^ I 9 b (P } T .) * _ * (~ J c . @ , . 3 r 9 . . } N . c y x . z y 7 = e . . . x Q O / E [. A . w u z + ! . 8 . . O _ e B . o . . # 7 . . . . . W > . . . e . , . . . _ k . F . . . S W Q Y W _ R . V . . . . . V b Q & . . . . . Z W _ _ S b ` . . o . . $ D . . [[b . . . . S . . . . w . . [R S E . . :
Data Raw:	6c 78 f6 04 02 54 f2 f4 ab a0 01 08 99 79 bd 1a 14 91 94 81 ed b9 56 4b 94 8b 4d db 8b 29 bb d3 71 3d 79 81 eb 23 0a f7 78 8b 3b 55 ff d7 05 b0 f5 8a 28 2d 86 f4 8a 28 ff e0 fa 37 43 00 2a 1e 38 39 91 7e 9f cc 96 9d c2 0a 3a e6 f4 ec 33 5d d4 8b 0b 65 51 9d 8b 7d 14 3e ed 77 76 27 48 5b 3d 5a e2 61 16 02 ca 6a 9b ca 41 f0 ff 9a 06 f2 6e 09 fc 26 5c 40 bc 1b 70 4e fb 16 7c 88 ed b5

Stream Path: 5hLfxSDpMqWpnSELaMw6nQvvNrLo, File Type: empty, Stream Size: 0

General

Stream Path:	5hLfxSDpMqWpnSELaMw6nQvvNrLo
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2924, Parent PID: 576

General

Target ID:	0
Start time:	19:48:09
Start date:	24/11/2022
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:	0x13f7e0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
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\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E012B14	CreateDirectoryA

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	12288	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6E090648	unknown
unknown	12288	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	10	6E090648	unknown
unknown	16384	12288	75 6e 6b 6e 6f 77 6e	unknown	success or wait	10	6E090648	unknown
unknown	102400	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	6E090648	unknown
unknown	106496	8192	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	6E090648	unknown
unknown	1790976	29696	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6E090648	unknown
unknown	188416	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	254	6E090648	unknown
unknown	192512	8192	75 6e 6b 6e 6f 77 6e	unknown	success or wait	254	6E090648	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E06A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E06A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E06A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E090648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Consolas	binary	02 0B 06 09 02 02 04 03 02 04	success or wait	1	6E090648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly