ID: 643237
Sample Name:
TranQuangDai.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:29:09
Date: 10/06/2022
Version: 35.0.0 Citrine

Table of Contents

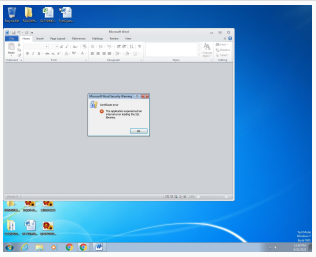
Windows Analysis Report

TranQuangDai.docx

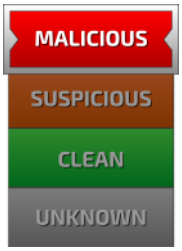
Overview

General Information

Sample Name:	TranQuangDai.docx
Analysis ID:	643237
MD5:	019203409d3584.
SHA1:	29d38d998e0a17.
SHA256:	719a07f46b6fce1..
Tags:	doc Follina
Infos:	YARA



Detection

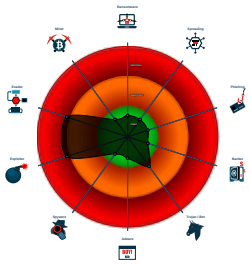


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Contains an external reference to an…
- Detected suspicious Microsoft Offic…
- Yara signature match
- Potential document exploit detected…
- Potential document exploit detected…
- Detected TCP or UDP traffic on non…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1144 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	SUSP_Doc_WordXMLRels_May22	Detects a suspicious pattern in docx document.xml.rels file as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard, Wojciech Cie\305\233lak	• 0x39:$a1: <Relationships • 0x240:$a2: TargetMode="External" • 0x238:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x1ef:$olerel: relationships/oleObject • 0x208:$target1: Target="http • 0x240:$mode: TargetMode="External

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Exploits

Detected suspicious Microsoft Office reference URL

System Summary

Malicious sample detected (through community Yara rule)

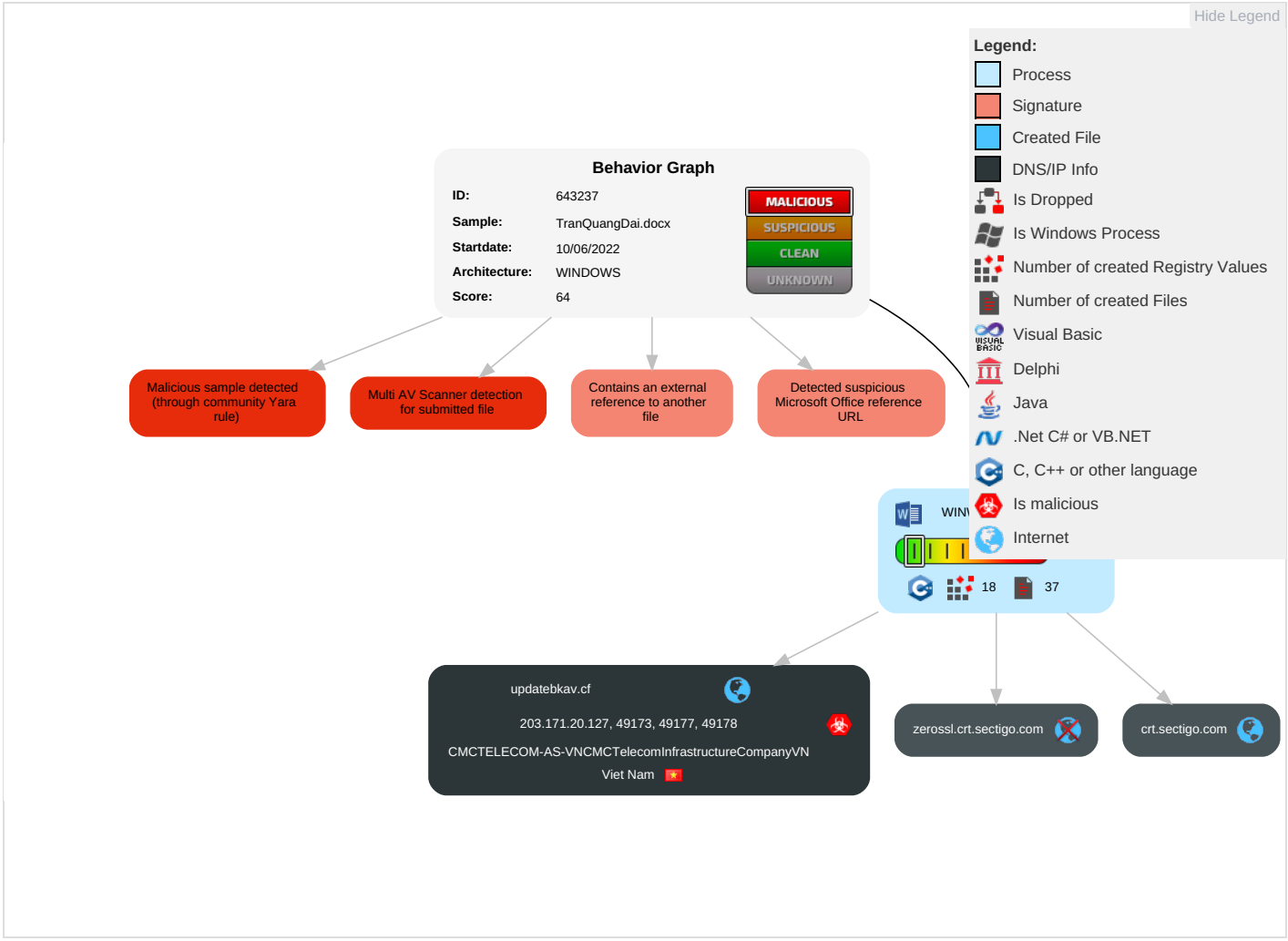
Persistence and Installation Behavior

Contains an external reference to another 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	1 2 Exploitation for Client Execution	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 Non-Standard Port	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	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

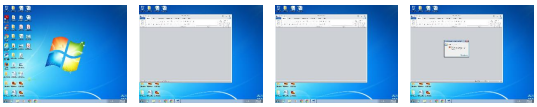
Behavior Graph

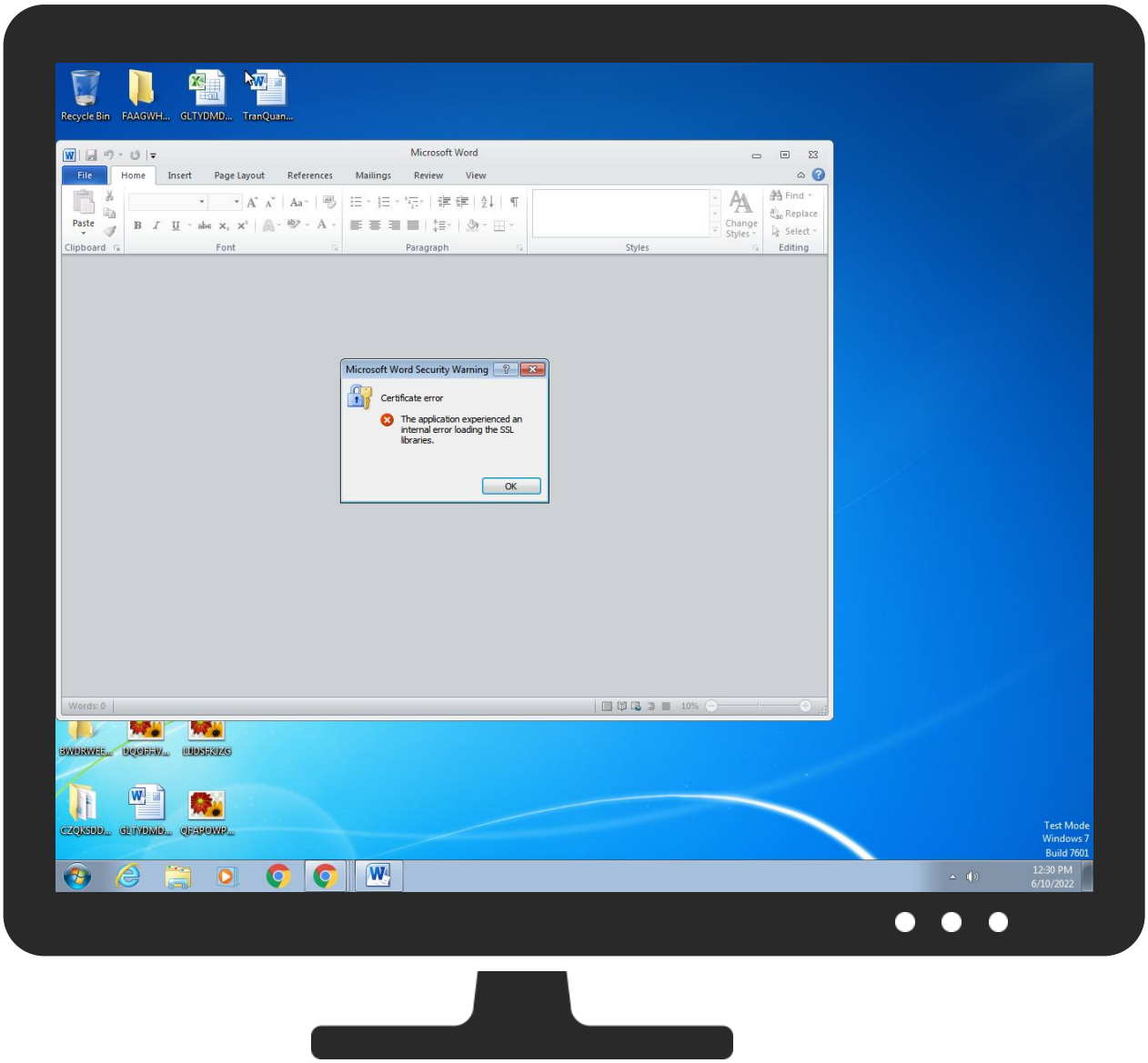


Screenshots

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
TranQuangDai.docx	36%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
updatebkav.cf	0%	Virustotal		Browse
crt.sectigo.com	0%	Virustotal		Browse
zerossl.crt.sectigo.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	0%	Avira URL Cloud	safe	

Domains and IPs

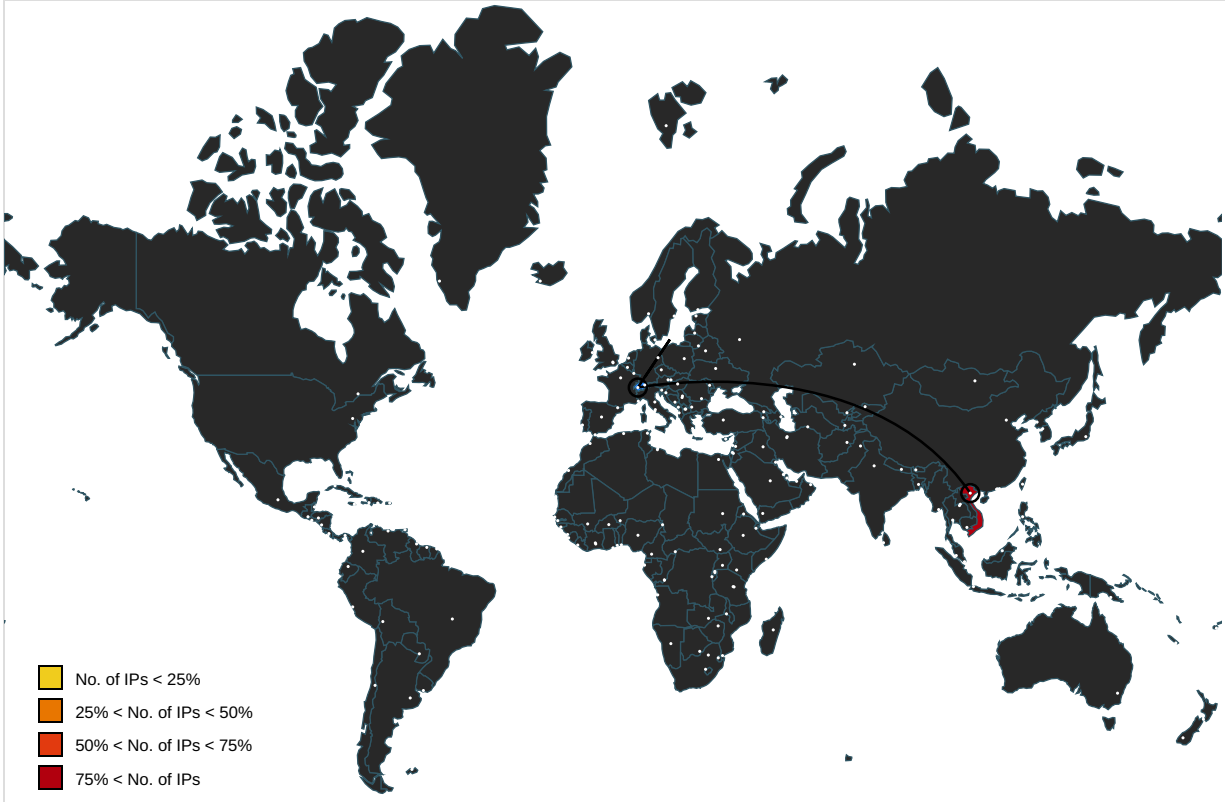
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
updatebkav.cf	203.171.20.127	true	true	• 0%, Virustotal, Browse	unknown
crt.sectigo.com	91.199.212.52	true	false	• 0%, Virustotal, Browse	unknown
zerossl.crt.sectigo.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	10BDC45B4A27319429BBC4F08A4E8A100.0.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.171.20.127	updatebkav.cf	Viet Nam		45903	CMCTELECOM-AS-VNCMCTelecomInfrastructureCompanyVN	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	643237
Start date and time: 10/06/202212:29:09	2022-06-10 12:29:09 +02:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 11m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TranQuangDai.docx
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.expl.evad.winDOCX@1/18@5/1
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: .docx • Adjust boot time • Enable AMSI

Warnings

- Max analysis timeout: 600s exceeded, the analysis took too long
- Exclude process from analysis (whitelisted): dllhost.exe
- Excluded IPs from analysis (whitelisted): 91.199.212.52, 173.222.108.226, 173.222.108.210
- Excluded domains from analysis (whitelisted): crt.usertrust.com, ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, crt.comodoca.com, download.windowsupdate.com.edgesuite.net

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\LocalLow\Microsoft\CryptnetUrlCache\Content\10BDC45B4A27319429BBC4F08A4E8A10

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1753
Entropy (8bit):	7.54155945514523
Encrypted:	false
SSDEEP:	48:m4qXYiteL8B0wtUJgVXpxi4sVQmjPOZphFRl12:StO+0mrZn/T5R+
MD5:	58AA23107C8D5AEDEABD0D5E32578592
SHA1:	C81A8BD1F9CF6D84C525F378CA1D3F8C30770E34
SHA-256:	21ACC1DBD6944F9AC18C782CB5C328D6C2821C6B63731FA3B8987F5625DE8A0D
SHA-512:	ED89CA15A1A6150246A3A92EEF6E1E962928BCB2E70FA802513581076C907F276CA0639E700FB4BA7E20F2276A0184D8C19168C9E466CCDA5FE2500D16B8C43
Malicious:	false
Reputation:	low
Preview:	0...0.....lU.....0...*.H.....0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0...2001300000002..300129235959Z0K1.0...U....AT1.0...U....ZeroSSL1*0(..U...!ZeroSSL RSA Domain Secure Site CA0.."0...*.H.....0.....is~..1.#.m...T .....!.~].R|?1..l.Y8^g~KV.u..7.5Zd..L.,$..m....Mf.....!t..C..q...L8}.*.....8...N..h..kw..@...._.....=$._.d...Y..B.oPR..Z.'<.....^...T.c.....q.+{@.5.....A...F..|2E...E.e..Pt....V u..J..j.u...5../.]..\..;..w..%5-.V..^x$.....(g..0...mZ'...;.`.r3..}.*c...C.u.;.L..7t...>.D....B.f...tJ..."Y..bf:!...'.{...r2n..]tU.....F.....Ex;6E.....-5E*....X.....B.y9.$....g.....|..OxR..WOaU .'.8y..B...--....jG.iV'4%:KI.J.v.i.-o....."m.z.Wc..%9J.~h.i.H.@...#....Ui.(KBU.....u0..q0...U.#..0...Sy.Z.+J.T.....f.0...U.....xh...h.=r._.>....0...U.....0...U.....0.....0...U.%. .0...+.....+.....0"..U. ..0.0...+.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Cabinet archive data, 61476 bytes, 1 file
Category:	dropped
Size (bytes):	61476
Entropy (8bit):	**7.995018321729444**
Encrypted:	**true**
SSDEEP:	1536:NATLwfiuePkACih0/8ulwf5CiqGLhk1V/AFnGegJR:N7nePk5gKsoBha/0GTf
MD5:	308336E7F515478969B24C13DED11EDE
SHA1:	8FB0CF42B77DBBEF224A1E5FC38ABC2486320775
SHA-256:	889B832323726A9F10AD03F85562048FDCFE20C9FF6F9D37412CF477B4E92FF9
SHA-512:	61AD97228CD6C3909EF3AC5E4940199971F293BDD0D5EB7916E60469573A44B6287C0FA1E0B6C1389DF35EB6C9A7D2A61FDB318D4A886A3821EF5A9DAB3AC2F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....$.....,.....I.....w.....Tp. .authroot.stl.H#F..4..CK..<Tk...c_.d....A.F...,.&K..*i.RJJ..J.".%.KY"{n...."{..Lu3.Ln.....y.....M.:...<. v...H..~.#Ov.a0xN....)..C.. t.z.,x.00.1``L.....L.\..1.\|..2.1.0mD...H1/.....G..UT7!...r.X:....D.0.0...M....I(.-.+..v#...(.r.....z.Y`&hw..Gl+.je.e.j..{.1.....9f=.&.....s.W...L.].+...).f...u.....8....}R...w.X..>.A.Yw...a.x.. .T8V.e...^.7.q..t^.+....f.q).B.M.....64.<!W(.....D!.0.t "X...I.....D0.....+...A.....0.o..t93.v..O1V x}H.S)....GH.6.I...p2.(4k.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....a4E...q.*...#..a. .y..M..R.t..Z2!.T.Ua.k.'O..\./ d.F>.V...3...._.J....."....wI..'..z...j..Ds...qZ...[.....O<.d.K..hH@c1....[w7..z...l....h,.b.....'.w.....bO.i{.....+.-...H..."<...L.Tu}.Y.lB.]3..4..G.3..`E. .NF.....{o.h]}p....G..$..4...;..&.O.d....v:Ik.T..ObLq..&.j.j...B9.(..!..\.:K`.....:O..N.....C..jD:.i.....1.....eCo.c..3o.....nN.D..3.7...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0968A1E3A40D2582E7FD463BAEB59CD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1413
Entropy (8bit):	7.480496427934893
Encrypted:	false
SSDEEP:	24:yYvJm3RW857Ij3kTteTuQRFjGgZLE5XBy9+JYSE19rVAVsGnyI3SKB7:PL854TTuQL/ZoXQ9+mrGVrb3R
MD5:	285EC909C4AB0D2D57F5086B225799AA
SHA1:	D89E3BD43D5D909B47A18977AA9D5CE36CEE184C
SHA-256:	68B9C761219A5B1F0131784474665DB61BBDB109E00F05CA9F74244EE5F5F52B

SHA-512:	4CF305B95F94C7A9504C53C7F2DC8068E647A326D95976B7F4D80433B2284506FC5E3BB9A80A4E9A9889540BBF92908DD39EE4EB25F2566FE9AB37B4DC9A7C0 9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0...0..i.....9rD:.".Q..l..15.0...*.H.....0{1.0...U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U....Comodo CA Limited1!0...U....AAA Certificate Services0...19031 2000000Z..281231235959Z0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authori ty0.."0...*.H.....0.....e.6.....W.v..'.L.P.a. M.-d.....=.....{7(.+G.9.:._..}..cB.v.;+...o... ..>..t.....bd.....j."<.....{.....Q..gF.Q..T?.3.~l.....Q.5..f.rg.!f..x..P:.....L....5.WZ....=., ..T....:M.L..\... =.."4.~;hf.D..NFS.3`...S7.sC.2.S...tNi.k.`.....2..;Qx.g..=V...i....%&k3m.nG.sC.~..f.)|2.cU.....T0....}7..]:l5\.A...l.....b..f.%....?.9.....L.|.k..^...g.....[..L..[...s.#;-..5Ut.I .IX...6.Q...&}.M....C&.A_@.DD...W..P.WT.>.tc/.Pe..XB.C.L..%GY.....&FJP...x..g...W...c..b._U..\.(..%9..+..L...?.R.../.....0..0...U.#..0.....#>.....)...0..0...U.....Sy.Z.+J.T .....f.0...U.....0...U.....0....0...U

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\10BDC45B4A27319429BBC4F08A4E8A10

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	274
Entropy (8bit):	3.057215585062658
Encrypted:	false
SSDEEP:	3:kkFkl1l8x3/tfllXlE/lYoTZELDcqElXlije9DZlOJE5Yol2luN7MS1g15lquGlb:kKcY4qMUjKFgJE5Y7EyUWOJ9jn/
MD5:	A5162B06A57E1A75AFDB99E6E9B030F9
SHA1:	391D0CC9FBAFB5AFB6F1695F856A04463714C32D
SHA-256:	6723ECD357B9C4A1BD778813101B5D75B38EA2D5BA7CF26EFA99AA3A94AD4BA4
SHA-512:	2C8BA93A3C1F7BE41034CE19F2B8128FC0118D3489661902F5A1DBC103843D04209BCC383AB5057D6EF9C79EC5A35C8E5DA33A49E5650DBFC27901EE102351 7
Malicious:	false
Reputation:	low
Preview:	p..... .....^.-..}..(..... .....6....@8.....h.t.t.p.:././.z.e.r.o.s.s.l...c.r.t...s.e.c.t.i.g.o...c.o.m./.Z.e.r.o.S.S.L.R.S.A.D.o.m.a.i.n.S.e.c.u.r. e.S.i.t.e.C.A...c.r.t...".5.e.3.2.1.c.8.0.-.6.d.9."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0930947901168264
Encrypted:	false
SSDEEP:	6:kKd8mN+SkQlPlEGYRMY9z+4KlDA3RUecl7PG1:1EkPlE99SNxAhUecl61
MD5:	79271FC18E9D98C7B6CF69D071D5D386
SHA1:	F9418F8AE8EE812C408460A744BD562128D8B19A
SHA-256:	26901B4F3D4579094C3EAF8D660D063F69CC1E5865A683BE057A845C0AE60A3A
SHA-512:	4119EB803407221FB4981C6D113F2B062F87D5681821A7FD5E9800077873544F29813994A5097D3C853F37F0D96D6312D51B134A94DE90E76C06E675EEF678E5
Malicious:	false
Reputation:	low
Preview:	p..... .....G,..}..(..... .....3f..o.....&.....$...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.3.3.6.6.b.4.9.0.6.f.d.8.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0968A1E3A40D2582E7FD463BAEB59CD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	2.9344307533228307
Encrypted:	false
SSDEEP:	3:kkFklNlx/tfllXlE/lQcjT18tlwiANjpU+plgh3VEkax3QbaLU15lqErtd9lytn:kK1QAbjMulgokaWbLOW+n
MD5:	C17851BEFCA9E6074A9B01BF2FE2758A
SHA1:	32912DF732B81700D08CB09ACC12011E4DD11117
SHA-256:	623D1D2609E5BBB7DC3550F3555EE93071FDF3408A07AFE68A9E9146D8DEA9DE
SHA-512:	82273963AFFD6EFFE477392AD8E1F7E780D67A3BF7A88812E944CF3537E79367FD043E2931D3F769CF23CF1C2125AB52958CB6D091195780574E264D68B14DC3
Malicious:	false
Reputation:	low
Preview:	p..... ....h....2...}..(..... .....(.f...@8.....h.t.t.p.:././.c.r.t...u.s.e.r.t.r.u.s.t...c.o.m./.U.S.E.R.T.r.u.s.t.R.S.A.A.d.d.T.r.u.s.t.C.A...c.r.t... ".5.c.8.6.f.6.8.0.-.5.8.5."...

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.28849917017152166
Encrypted:	false
SSDEEP:	48:l3dN2PRBnfgCLSEWV2TDCXhQcn+fHSaNq5b4p8hCcydYNlrFb7YEqny6hWYFyIgd:KwLns5bSHRqYRipI3FgF3H
MD5:	BB201D24BCD911B558798EF4E896E53E
SHA1:	A1C0CC1A22CAD094172BBB11B110ECE18539C149
SHA-256:	67BDD2ACAD14AFEE9255D9AAAD23881C92CEB16B0CCDCA35F791238C62728EA9
SHA-512:	3064AB15E48DAFB461075286A11161A580655AEF7A37DD2096C549A94197529553B4694E795DD4522BAEAB0BCA4F11B9270B1E509EC4ADDA771FAC7DB77AD8A
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.4G.2..D..U.....S,...X.F...Fa.q.....2..*F.w.....C..`.K...JO....A.....E.....x...x...x...x..... ..... ...........zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....J..R.w.ps..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{44059877-72AB-4C9A-8258-B3A4CC3F341F}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	modified
Size (bytes):	131072
Entropy (8bit):	0.6662029495555659
Encrypted:	false
SSDEEP:	384:IO/HG8qqy51PQ0qkpvnm7ks3KacuG8HKacuG8znclCKaNuG5lCKWuGaUuLtFlCK4:d9qj1PxqhncQXUuLtFpBl1j+wBl1j
MD5:	AB44FFF7BF1C2DB50258BD34D73B1D33
SHA1:	9BC1594A4695C258AC619C227868E1F3B29ABC40
SHA-256:	A212B866F947F733AA9155E0D7A9319091D8FF77BD2DCF8EC6D919C083C6C1DA
SHA-512:	4C708A14AC1B93030DB20C909A485C463F1CFF100E06171D0D0C5C31C7821730C5C8CD086B998B0C667038FA76D00AEA4E78FC9EE34EE7C460B722C22A5E9C9
Malicious:	false
Preview:	......M.eFy...zV.....wH.....tS,...X.F...Fa.q.....J.[.lJ....u.y.....I...5..Z~.S.....W.....x...x...x...x..*..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....5.2A..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	3.9551760274231653
Encrypted:	false
SSDEEP:	3:yVlgsRlz3WUWWtu9WEYd3rmlmM7ylUct276:yPblzGquNY1y8MiUct22
MD5:	A2889FCE211DCE454F72E9BBCA1AAD01
SHA1:	75DDB76D280A8265A1C5B41E8AA353E03065B4AA
SHA-256:	47DA3237C346F4B1FF2080B35D47278899EEDE24C0C308365BB7B247E80331EF
SHA-512:	9846176519D0809A6992A5ED5E06D23A25D824F0C0D91AEEEAEFCCD6F22AF45BDAD1B3A1DC41EA06806C70A7A3BE49A1270AAC08ECE57F9B7731E1FFABF99B03
Malicious:	false
Preview:	..H..@....b..q....]F.S.D.-.{.4.4.0.5.9.8.7.7.-.7.2.A.B.-.4.C.9.A.-.8.2.5.8.-.B.3.A.4.C.C.3.F.3.4.1.F.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072

Entropy (8bit):	0.287938195716898
Encrypted:	false
SSDEEP:	48:I3GRBrOfdkjPa+A6eZ6/NyYC4SrEYihUORoO3YORoO3NH:KGLyJJ6+6/oYrCEgOjoOj9H
MD5:	93869240F89F8262F56D82B3AA838813
SHA1:	792481088735319D53745197BFDB2AE1F2126E69
SHA-256:	E03D3F7D3E53A47192209B56CF97B5FD34ED162CCB0B39B8981B7FF2904BC389
SHA-512:	CA3D58E9FBF3F26D2AC8B2047AD2A6BD89EE486D92A217A6906E94DDE82E5598CDD7441113356324E707574D51E205210A290549F43109C72D5DF302EB7D8C9
Malicious:	false
Preview:	......M.eFy...z....m.#G.y..Ylj.S,...X.F...Fa.q.....U{./B...zUh.B.....P..e...O..F..M.F.A.....E.....x...x...x...x..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....J..R.w.ps..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{A1B857E3-B132-4673-AC9F-79338C2FA8BB}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22204497001545706
Encrypted:	false
SSDEEP:	48:I3Ad/H5UrBf2bLVuxGSaO7f+Zf+mahj5aYaxPLfXLfa:KAdv5Cf2RI5e3xPru
MD5:	7067DE2227A0E1E343E8794FF8E9C26D
SHA1:	A521477E1D8B3044EE715AE8AF5318BE1A3DB8A4
SHA-256:	0B882C3D62593931E88BAFAF6F83939DA022B4119BDA4FA2A124D14FB1E0AC5C
SHA-512:	134927F12D29E3416F806092F595DBF9A43D9BD96796C1FC7C9AF04B19C461072383056CA3A1E91D1322FA1A4E32EB097D54C5EB8524ECC17298E687BC01F44F
Malicious:	false
Preview:	......M.eFy...z....=d.B....Y.m4S,...X.F...Fa.q.....v...rB..$....G.....YN.E..6.....P>.....PB.....x...x...x...x.....+..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G...|.u-.u.A...W"U..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	3.9684196678119985
Encrypted:	false
SSDEEP:	3:yVlgsRlzNnlnQlSOiIn3Ilwxk8lUZtckWclXljaiZ276:yPblzNFQlSOiIn4+xk8lUAkWc3uiZ22
MD5:	C4B20A4CFF14220E07A0D5A8C15D5297
SHA1:	FB828980F413F52F01436EC58D0DD2096FF737A1
SHA-256:	1557E7C03C3406E5BB17231B13998FDCE4B2425D42E80099671FA7AECF263BDD
SHA-512:	62E1BB2DB366DDBD75A7BA89D7F50C32C0A535BFAAFE7F420D3AE39435F9EF1237FE8DC659507D7E7EF015AD1BFF6BA3877D948EAD9E2466688E358CC2778 EB
Malicious:	false
Preview:	..H..@....b..q....]F.S.D.-.{.A.1.B.8.5.7.E.3.-.B.1.3.2.-.4.6.7.3.-.A.C.9.F.-.7.9.3.3.8.C.2.F.A.8.B.B.}...F.S.D..

C:\Users\user\AppData\Local\Temp\Cab68B2.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Cabinet archive data, 61476 bytes, 1 file
Category:	dropped
Size (bytes):	61476
Entropy (8bit):	**7.995018321729444**
Encrypted:	**true**
SSDEEP:	1536:NATLwfiuePkACih0/8uIwf5CiqGLhk1V/AFnGegJR:N7nePk5gKsoBha/0GTf
MD5:	308336E7F515478969B24C13DED11EDE
SHA1:	8FB0CF42B77DBBEF224A1E5FC38ABC2486320775
SHA-256:	889B832323726A9F10AD03F85562048FDCFE20C9FF6F9D37412CF477B4E92FF9

SHA-512:	61AD97228CD6C3909EF3AC5E4940199971F293BDD0D5EB7916E60469573A44B6287C0FA1E0B6C1389DF35EB6C9A7D2A61FDB318D4A886A3821EF5A9DAB3AC2F
Malicious:	false
Preview:	MSCF....$.....,.....I.....w.....Tp. .authroot.stl.H#F..4..CK..<Tk...c_.d....A.F...,.&K..*i.RJJ..J.".%.KY"{n...."{..Lu3.Ln.....y.....M.:...<. v...H..~.#Ov.a0xN....)..C..t.z.,x.00.1``L.....L.\..1.|..2.1.0mD...H1/.....G..UT7!...r.X:....D.0.0...M....I(.-.+..v#...(.r.....z.Y`&hw..Gl+.je.e.j..{.1.....9f=.&.....s.W...L.].+...).f...u.....8....}R...w.X..>.A.Yw...a.x..T8V.e...^.7.q..t^.+....f.q).B.M.....64.<!W(.....D!.0.t "X...I.....D0.....+...A.....0.o..t93.v..O1V x}H.S)....GH.6.I...p2.(4k.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....a4E...q.*...#..a..y..M..R.t..Z2!.T.Ua.k.'O..\./ d.F>.V...3...._.J....."....wI..'..z...j..Ds...qZ...[.....O<.d.K..hH@c1....[w7..z...I....h,.b.....'.w.....bO.i{.....+.-...H..."<...L.Tu}.Y.lB.]3..4..G.3..`E..NF.....{o.h]}p....G..$..4....;..&.O.d....v:Ik.T..ObLq..&.j.j...B9.(..!..\.:K`.....:O..N.....C..jD:.i.....1.....eCo.c..3o.....nN.D..3.7...

C:\Users\user\AppData\Local\Temp\Tar68B3.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	161786
Entropy (8bit):	6.301422924360695
Encrypted:	false
SSDEEP:	1536:0ga6crtilgCyNY2IpFQNujcz5YJkKCC/rH8Zz04D8rlCMiB3XlMn6U:0a0imCy6QNujcmJkr97MiVG6U
MD5:	2D8A5090656DE9FB55DD0F3BA20F9299
SHA1:	A08BB2FC731F6A72B095C266C44EA66F2C4ACA72
SHA-256:	44AE1E61A4E6305C15AAA52FD1B29DDB060E69233703CBA611F5E781D766442E
SHA-512:	7A885EBD1E7DB76F1F22EC42070EB9359AFF7BEF125587BC24E9EC12E1AECAFD0EACB7B3C0B235466401CE76D6C452CEA48D21F0FDBA59A45F96DBAA39233300
Malicious:	false
Preview:	0..w...*.H.....w.0..w....1.0...`.H.e.....0..hC..+.....7.....h30..h.0...+.....7.....e...0...220511092946Z0...+.....0..g.0..D....`...@.,..0..0.r1..*0...+.....7..h1.....+h...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o

C:\Users\user\AppData\Local\Temp\{2BA8F08F-11BD-48DD-91CA-8557D0F641F7}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025702809661217164
Encrypted:	false
SSDEEP:	6:I3DPcvjMvxggLRH75gdMGDRXv//4tfnRujlw//+GtluJ/eRuj:I3DPKjaztgl1vYg3J/
MD5:	C384C1B38E0DB040DCDD2E1839741E58
SHA1:	5655ACDAABB1BFBC79B0C80C4629F75995B52A2F
SHA-256:	2D333B9A32B67C7E956841A004A3861F2D80E6E259976193BED7AB592D65427B
SHA-512:	BD5DF7E74A8CAA42D9A908F0592E9792F6C2833B3A3FB80E802077530EBBDA4DC51C506BFB943F99B6B627C3F0B49F5FC54FA0D212C05BEA8310032278159893
Malicious:	false
Preview:	......M.eFy...z.4G.2..D..U.....S,...X.F...Fa.q.....ege..J.....<.....C..`.K...JO.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{6D5470AD-7571-4443-B52C-CEA4592715E2}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025525655933182245
Encrypted:	false
SSDEEP:	6:I3DPcC+iHvxggLRW9vjFRXv//4tfnRujlw//+GtluJ/eRuj:I3DPmm8HvYg3J/
MD5:	DC6B59DDDA35A24153CF83164A9C0765
SHA1:	453F97E448FDB79F928FC41C75F235B462D41781
SHA-256:	F9C8880D546DE62D0A3F3511DA7C0C6DB21F02B1727062BA9DB87842127223CE
SHA-512:	1AFF4FE54D63391C610AF86ABADDF17262B38B706940A2B73D42E963422C39722936F61121561365F35D30D03015CA480F0BE7EFEFE4CB7D4C5B53D108DBBD8
Malicious:	false

Preview:	......M.eFy...z....m.#G.y..Ylj.S,...X.F...Fa.q.....k.(.B..K..Ek.....P..e...O..F..M.F.....x...x...x...x..... .....zV..... ..@..... .....

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:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/l
MD5:	C5E24006AFAC8C2659023AD09A07EB0F
SHA1:	4B7B834BEDADFD0A2764743E021D40C55A51F284
SHA-256:	7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E
SHA-512:	673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x...

C:\Users\user\Desktop\~$anQuangDai.docx

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:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/l
MD5:	C5E24006AFAC8C2659023AD09A07EB0F
SHA1:	4B7B834BEDADFD0A2764743E021D40C55A51F284
SHA-256:	7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E
SHA-512:	673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x...

Static File Info

General

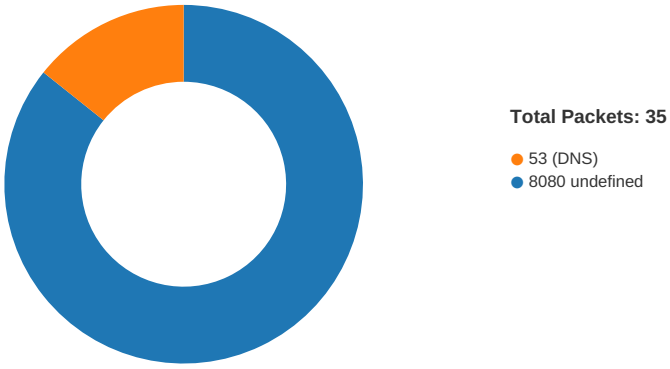
File type:	Microsoft Word 2007+
Entropy (8bit):	7.511177710534898
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	TranQuangDai.docx
File size:	16256
MD5:	019203409d35842d93b46de7db4038bb
SHA1:	29d38d998e0a17af1d11cdef3b74855a54727c51
SHA256:	719a07f46b6fce1615a7b4bd1ed3e4d2cb86d7275ae37d3325ff2e9db64e2185
SHA512:	2b6dea2ba3d306735804acf12f94e64b58340391779a0eed19262fbec2c9ebdcc3a383c40458778cbbe3a5f39223f708cd0f156da54e842acffb038191eedda4
SSDEEP:	384:azW4FOKfKztM3wIs65n0i13LU3HbCXBqX6Ujnw+3KWvb:ckKfKJismv13wLCx7H+3T
TLSH:	BB72C0B4C25DBC12CAA71235A04E9AF1FB71900AE435991EB519FBD48CB64C7832D39D
File Content Preview:	PK.....!....lZ... .....[Content_Types].xml ... (.....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 10, 2022 12:29:59.083745003 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:29:59.461699009 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:29:59.461874008 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:29:59.476402998 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:29:59.853744030 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:29:59.855285883 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:29:59.855317116 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:29:59.855570078 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:29:59.870995045 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:00.248416901 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:00.248759031 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:00.248867035 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:03.241713047 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:03.619393110 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:03.619663954 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:03.619846106 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:08.624825001 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:08.624927044 CEST	8080	49173	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:08.624968052 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:08.625005960 CEST	49173	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:09.243387938 CEST	49177	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:09.614388943 CEST	8080	49177	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:09.614509106 CEST	49177	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:09.616400957 CEST	49177	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:09.987260103 CEST	8080	49177	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:09.987457037 CEST	8080	49177	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:09.987545013 CEST	8080	49177	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:09.987626076 CEST	49177	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:09.987957001 CEST	49177	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:09.988657951 CEST	49178	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:10.358201027 CEST	8080	49178	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:10.358325958 CEST	49178	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:10.358469963 CEST	8080	49177	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:10.360300064 CEST	49178	8080	192.168.2.22	203.171.20.127

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 10, 2022 12:30:10.729635000 CEST	8080	49178	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:10.729820013 CEST	8080	49178	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:10.729856014 CEST	8080	49178	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:10.729923964 CEST	49178	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:10.730134010 CEST	49178	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:10.731328964 CEST	49179	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:11.099173069 CEST	8080	49178	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:11.117424965 CEST	8080	49179	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:11.117638111 CEST	49179	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:11.118279934 CEST	49179	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:11.504688978 CEST	8080	49179	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:11.505290031 CEST	8080	49179	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:11.505326033 CEST	8080	49179	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:11.505410910 CEST	49179	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:11.521603107 CEST	49179	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:11.522281885 CEST	49180	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:11.890264034 CEST	8080	49180	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:11.890521049 CEST	49180	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:11.905950069 CEST	8080	49179	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:11.923376083 CEST	49180	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:12.291269064 CEST	8080	49180	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:12.291512966 CEST	8080	49180	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:12.291555882 CEST	8080	49180	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:12.291671038 CEST	49180	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:12.292661905 CEST	49180	8080	192.168.2.22	203.171.20.127
Jun 10, 2022 12:30:12.660284042 CEST	8080	49180	203.171.20.127	192.168.2.22
Jun 10, 2022 12:30:38.625421047 CEST	8080	49173	203.171.20.127	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 10, 2022 12:29:59.049689054 CEST	55868	53	192.168.2.22	8.8.8.8
Jun 10, 2022 12:29:59.067420959 CEST	53	55868	8.8.8.8	192.168.2.22
Jun 10, 2022 12:30:00.614010096 CEST	49688	53	192.168.2.22	8.8.8.8
Jun 10, 2022 12:30:00.632996082 CEST	53	49688	8.8.8.8	192.168.2.22
Jun 10, 2022 12:30:00.636023998 CEST	58836	53	192.168.2.22	8.8.8.8
Jun 10, 2022 12:30:00.654769897 CEST	53	58836	8.8.8.8	192.168.2.22
Jun 10, 2022 12:30:09.199759960 CEST	50108	53	192.168.2.22	8.8.8.8
Jun 10, 2022 12:30:09.219244003 CEST	53	50108	8.8.8.8	192.168.2.22
Jun 10, 2022 12:30:09.222542048 CEST	54723	53	192.168.2.22	8.8.8.8
Jun 10, 2022 12:30:09.242052078 CEST	53	54723	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2022 12:29:59.049689054 CEST	192.168.2.22	8.8.8.8	0x22f0	Standard query (0)	updatebkav.cf	A (IP address)	IN (0x0001)
Jun 10, 2022 12:30:00.614010096 CEST	192.168.2.22	8.8.8.8	0x62ee	Standard query (0)	zerossl.crt.sectigo.com	A (IP address)	IN (0x0001)
Jun 10, 2022 12:30:00.636023998 CEST	192.168.2.22	8.8.8.8	0xc577	Standard query (0)	zerossl.crt.sectigo.com	A (IP address)	IN (0x0001)
Jun 10, 2022 12:30:09.199759960 CEST	192.168.2.22	8.8.8.8	0x11d4	Standard query (0)	updatebkav.cf	A (IP address)	IN (0x0001)
Jun 10, 2022 12:30:09.222542048 CEST	192.168.2.22	8.8.8.8	0x8da9	Standard query (0)	updatebkav.cf	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2022 12:29:59.067420959 CEST	8.8.8.8	192.168.2.22	0x22f0	No error (0)	updatebkav.cf		203.171.20.127	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2022 12:30:00.632996082 CEST	8.8.8.8	192.168.2.22	0x62ee	No error (0)	zerossl.crt.sectigo.com	crt.sectigo.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2022 12:30:00.632996082 CEST	8.8.8.8	192.168.2.22	0x62ee	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Jun 10, 2022 12:30:00.654769897 CEST	8.8.8.8	192.168.2.22	0xc577	No error (0)	zerossl.crt.sectigo.com	crt.sectigo.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2022 12:30:00.654769897 CEST	8.8.8.8	192.168.2.22	0xc577	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Jun 10, 2022 12:30:09.219244003 CEST	8.8.8.8	192.168.2.22	0x11d4	No error (0)	updatebkav.cf		203.171.20.127	A (IP address)	IN (0x0001)
Jun 10, 2022 12:30:09.242052078 CEST	8.8.8.8	192.168.2.22	0x8da9	No error (0)	updatebkav.cf		203.171.20.127	A (IP address)	IN (0x0001)

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **1144**, Parent PID: **576**

General

Target ID:	0
Start time:	12:30:12
Start date:	10/06/2022
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:	0x13f480000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

No disassembly