

JOeSandbox Cloud BASIC



ID: 828485

Sample Name:

OMICS_Online_1.one

Cookbook: default.jbs

Time: 09:04:54

Date: 17/03/2023

Version: 37.0.0 Beryl

Table of Contents

Table of Contents	2
Windows Analysis Report OMICS_Online_1.one	5
Overview	5
General Information	5
Detection	5
Signatures	5
Classification	5
Process Tree	5
Malware Threat Intel	5
Malware Configuration	6
Threatname: Emotet	6
Yara Signatures	6
Initial Sample	6
Memory Dumps	6
Unpacked PEs	7
Sigma Signatures	7
Malware Analysis System Evasion	7
Snort Signatures	7
Joe Sandbox Signatures	8
AV Detection	9
Software Vulnerabilities	9
Networking	9
E-Banking Fraud	9
Hooking and other Techniques for Hiding and Protection	9
HIPS / PFW / Operating System Protection Evasion	9
Stealing of Sensitive Information	9
Remote Access Functionality	9
Mitre Att&ck Matrix	9
Behavior Graph	10
Screenshots	10
Thumbnails	11
Antivirus, Machine Learning and Genetic Malware Detection	12
Initial Sample	12
Dropped Files	12
Unpacked PE Files	12
Domains	12
URLs	13
Domains and IPs	14
Contacted Domains	14
Contacted URLs	14
URLs from Memory and Binaries	14
World Map of Contacted IPs	21
Public IPs	21
General Information	22
Warnings	23
Simulations	23
Behavior and APIs	23
Joe Sandbox View / Context	23
IPs	23
Domains	24
ASNs	24
JA3 Fingerprints	24
Dropped Files	24
Created / dropped Files	24
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	24
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	24
C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\98BB5134-EE3F-4D7D-9136-7342A66C9981	24
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\My Notebook\~Quick Notes.one.onebackupconstruction	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000005.bin (copy)	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000006.bin (copy)	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000007.bin (copy)	26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000008.bin (copy)	26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000009.bin (copy)	26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000A.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000B.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000C.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000D.bin (copy)	28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000E.bin (copy)	28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000F.bin (copy)	28

Page 3 of 63

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000031.bin (copy)	53
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000032.bin (copy)	53
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000033.bin (copy)	53
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000034.bin (copy)	54
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000035.bin (copy)	54
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000036.bin (copy)	54
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000037.bin (copy)	55
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000038.bin (copy)	55
Static File Info	55
General	55
File Icon	56
Network Behavior	56
Snort IDS Alerts	56
Network Port Distribution	56
TCP Packets	57
UDP Packets	59
DNS Queries	59
DNS Answers	59
HTTP Request Dependency Graph	59
Statistics	59
Behavior	59
System Behavior	59
Analysis Process: ONENOTE.EXEPID: 5812, Parent PID: 3452	59
General	59
File Activities	60
Registry Activities	60
Analysis Process: wscript.exePID: 5592, Parent PID: 5812	60
General	60
File Activities	60
File Written	60
Analysis Process: regsvr32.exePID: 5304, Parent PID: 5592	61
General	61
File Activities	61
File Read	61
Analysis Process: regsvr32.exePID: 4884, Parent PID: 5304	61
General	61
File Activities	61
Analysis Process: regsvr32.exePID: 5328, Parent PID: 4884	62
General	62
File Activities	62
Analysis Process: ONENOTEM.EXEPID: 1920, Parent PID: 5812	62
General	62
Registry Activities	62
Disassembly	63

Windows Analysis Report

OMICS_Online_1.one

Overview

General Information

Sample Name:	OMICS_Online_1.one
Analysis ID:	828485
MD5:	238f7e8cd973a...
SHA1:	f87f164125c95...
SHA256:	1c3a7f886a544...
Tags:	one
Infos:	

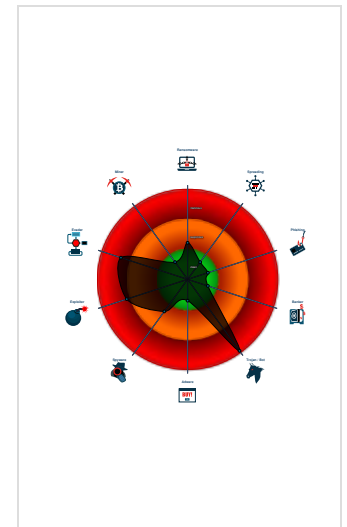
Detection

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

Signatures

Multi AV Scanner detection for subm...
Yara detected Malicious OneNote
Yara detected Emotet
System process connects to network...
Sigma detected: Run temp file via re...
Antivirus detection for URL or domain
Multi AV Scanner detection for drop...
Snort IDS alert for network traffic
C2 URLs / IPs found in malware con...
Hides that the sample has been dow...
Document exploit detected (process...
Queries the volume information (nam...

Classification



Process Tree

- System is w10x64
- ONENOTE.EXE (PID: 5812 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE "C:\Users\user\Desktop\OMICS_Online_1.one MD5: 8D7E99CB358318E1F38803C9E6B67867")
 - wscript.exe (PID: 5592 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\AppData\Local\Temp\click.wsf" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
 - regsvr32.exe (PID: 5304 cmdline: C:\Windows\System32\regsvr32.exe "C:\Users\user\AppData\Local\Temp\rad98E2D.tmp.dll MD5: 426E7499F6A7346F0410DEAD0805586B")
 - regsvr32.exe (PID: 4884 cmdline: "C:\Users\user\AppData\Local\Temp\rad98E2D.tmp.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
 - regsvr32.exe (PID: 5328 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\STfTfmTSAbWdRVZ\mmatLGgYnezL.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
 - ONENOTEM.EXE (PID: 1920 cmdline: /tsr MD5: DBCFA6F25577339B877D2305CAD3DEC3)
- cleanup

Malware Threat Intel

Provided by
malpedia

Name	Description	Attribution	Blogpost URLs	Link
Emotet	While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets. It is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time. Emotet had been taken down by authorities in January 2021, though it appears to have sprung back to life in November 2021.	- GOLD CABIN - MUMMY SPIDER - Mealybug	http://blog.fortinet.com/2017/05/03/deep-analysis-of-new-emotet-variant-part-1 http://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/http://ropgadget.com/posts/defensive_pcres.html http://adalogics.com/blog/the-state-of-advanced-code-injectionshttps://asec.ahnlab.com/en/33600/	http://https://malpedia.caad.fkie.fr/aunhofer.de/details/win.emotet

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "91.121.146.47:8080",
    "66.228.32.31:7080",
    "182.162.143.56:443",
    "187.63.160.88:80",
    "167.172.199.165:8080",
    "164.90.222.65:443",
    "104.168.155.143:8080",
    "163.44.196.120:8080",
    "160.16.142.56:8080",
    "159.89.202.34:443",
    "159.65.88.10:8080",
    "186.194.240.217:443",
    "149.56.131.28:8080",
    "72.15.201.15:8080",
    "1.234.2.232:8080",
    "82.223.21.224:8080",
    "206.189.28.199:8080",
    "169.57.156.166:8080",
    "107.170.39.149:8080",
    "103.43.75.120:443",
    "91.207.28.33:8080",
    "213.239.212.5:443",
    "45.235.8.30:8080",
    "119.59.103.152:8080",
    "164.68.99.3:8080",
    "95.217.221.146:8080",
    "153.126.146.25:7080",
    "197.242.150.244:8080",
    "202.129.205.3:8080",
    "103.132.242.26:8080",
    "139.59.126.41:443",
    "110.232.117.186:8080",
    "183.111.227.137:8080",
    "5.135.159.50:443",
    "201.94.166.162:443",
    "103.75.201.2:443",
    "79.137.35.198:8080",
    "172.105.226.75:8080",
    "94.23.45.86:4143",
    "115.68.227.76:8080",
    "153.92.5.27:8080",
    "167.172.253.162:8080",
    "188.44.20.25:443",
    "147.139.166.154:8080",
    "129.232.188.93:443",
    "173.212.193.249:8080",
    "185.4.135.165:8080",
    "45.176.232.124:443"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33LnSt71eii+nofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5U16acAAdAJA=",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKTS88RDdy7BPILP6AiDOTLYMHkSWvrQ0SsLbmr10vZ2Pz+AQWzRMggQmAt06rPH7nyx2v160cAAZAJA="
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
OMICS_Online_1.one	JoeSecurity_MalOneNote	Yara detected Malicious OneNote	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.331944852.0000000000D00000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000D.00000002.830903189.0000000000E21000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000003.349816910.0000000005E26000.0000004.00000020.00020000.00000000.sdmp	WEBSHELL_asp_generic	Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file	Arnim Rupp	0x8902:\$tagasp_classid5: 0D43FE01-F093-11CF-8940-0A0C9054228 0x3ea:\$jsp4: public 0xa2a:\$jsp4: public 0x598:\$asp_input1: request 0x5da:\$asp_input1: request 0x6f0:\$asp_input1: request 0xa4:\$asp_payload11: wscript.shell 0x88:\$asp_multi_payload_one1: createobject 0x7ee:\$asp_multi_payload_one1: createobject 0xacc:\$asp_multi_payload_one3: .run 0x88:\$asp_multi_payload_four1: createobject 0x7ee:\$asp_multi_payload_four1: createobject 0x6e0:\$asp_always_write1: .write 0x774:\$asp_write_way_one2: savetofile 0x88:\$asp_cr_write1: createobject(0x7ee:\$asp_cr_write1: createobject(0x8902:\$tagasp_capa_classid5: 0D43FE01-F093-11CF-8940-0A0C9054228
0000000C.00000002.332682576.0000000000D31000.0000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000D.00000002.829181595.0000000000CE0000.0000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 2 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
13.2.regsvr32.exe.ce0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.regsvr32.exe.d00000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.regsvr32.exe.ce0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.regsvr32.exe.d00000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Sigma Signatures

Malware Analysis System Evasion



Sigma detected: Run temp file via regsvr32

Snort Signatures	
ET CNC Feodo Tracker Reported CnC Server TCP group 7 - Source IP: 192.168.2.3 - Destination IP: 182.162.143.56	
Timestamp:	192.168.2.3182.162.143.56497034432404312 03/17/23-09:07:17.288903
SID:	2404312
Source Port:	49703
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected
ET CNC Feodo Tracker Reported CnC Server TCP group 23 - Source IP: 192.168.2.3 - Destination IP: 91.121.146.47	
Timestamp:	192.168.2.391.121.146.474970080802404344 03/17/23-09:07:02.528103
SID:	2404344
Source Port:	49700
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected
ET CNC Feodo Tracker Reported CnC Server TCP group 5 - Source IP: 192.168.2.3 - Destination IP: 167.172.199.165	
Timestamp:	192.168.2.3167.172.199.1654970580802404308 03/17/23-09:07:29.350313

SID:	2404308
Source Port:	49705
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 11 - Source IP: 192.168.2.3 - Destination IP: 213.239.212.5

Timestamp:	192.168.2.3213.239.212.5497344432404320 03/17/23-09:10:04.212745
SID:	2404320
Source Port:	49734
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 2 - Source IP: 192.168.2.3 - Destination IP: 104.168.155.143

Timestamp:	192.168.2.3104.168.155.1434971080802404302 03/17/23-09:07:42.102850
SID:	2404302
Source Port:	49710
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 13 - Source IP: 192.168.2.3 - Destination IP: 45.235.8.30

Timestamp:	192.168.2.345.235.8.304973880802404324 03/17/23-09:10:10.312810
SID:	2404324
Source Port:	49738
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 10 - Source IP: 192.168.2.3 - Destination IP: 206.189.28.199

Timestamp:	192.168.2.3206.189.28.1994972680802404318 03/17/23-09:09:10.341885
SID:	2404318
Source Port:	49726
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 16 - Source IP: 192.168.2.3 - Destination IP: 66.228.32.31

Timestamp:	192.168.2.366.228.32.314970270802404330 03/17/23-09:07:12.052554
SID:	2404330
Source Port:	49702
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 3 - Source IP: 192.168.2.3 - Destination IP: 119.59.103.152

Timestamp:	192.168.2.3119.59.103.1524973980802404304 03/17/23-09:10:17.568030
SID:	2404304
Source Port:	49739
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Software Vulnerabilities



Document exploit detected (process start blacklist hit)

Networking



System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected Emotet

Hooking and other Techniques for Hiding and Protection



Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion



System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information



Yara detected Malicious OneNote

Yara detected Emotet

Remote Access Functionality



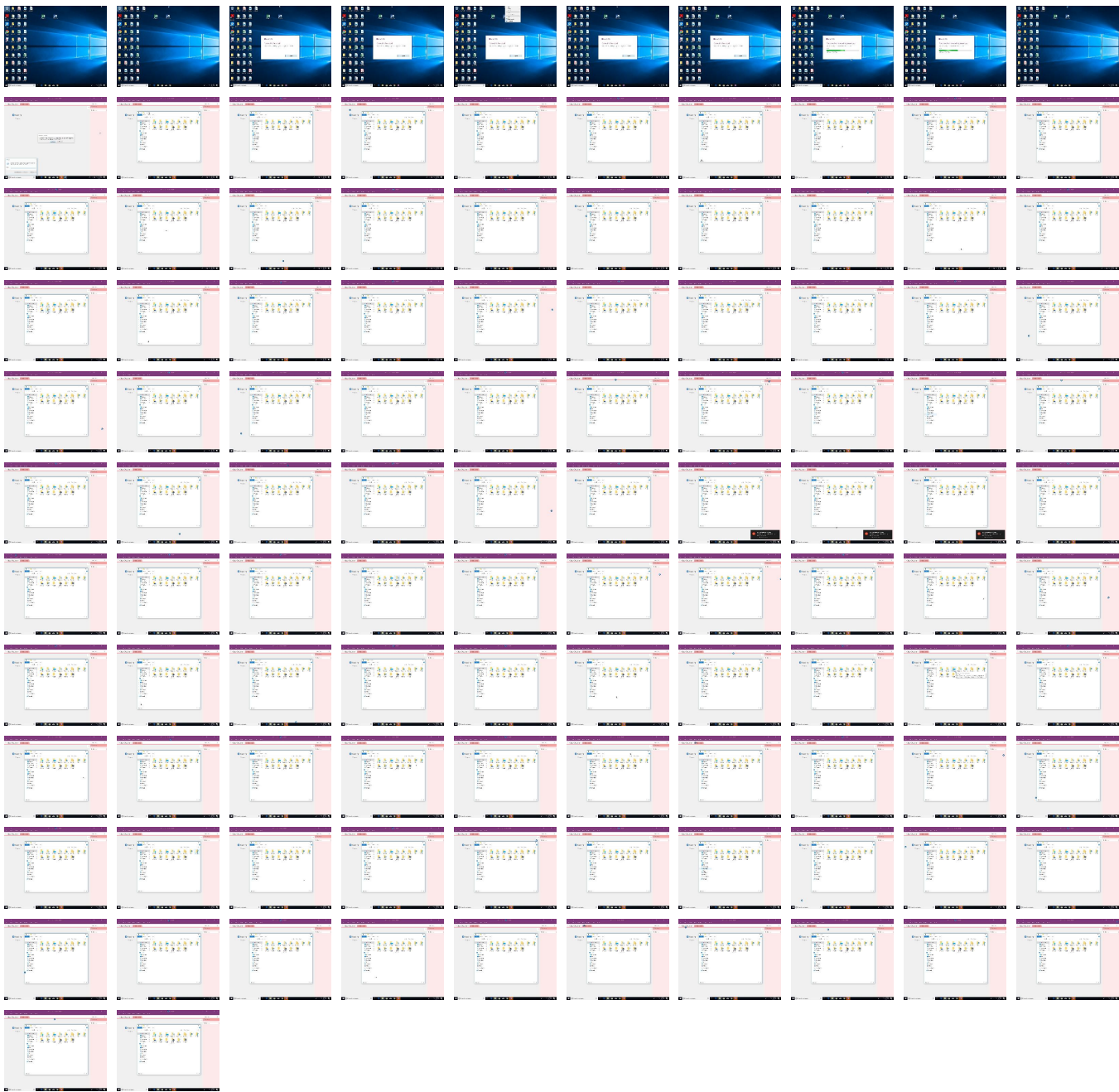
Yara detected Malicious OneNote

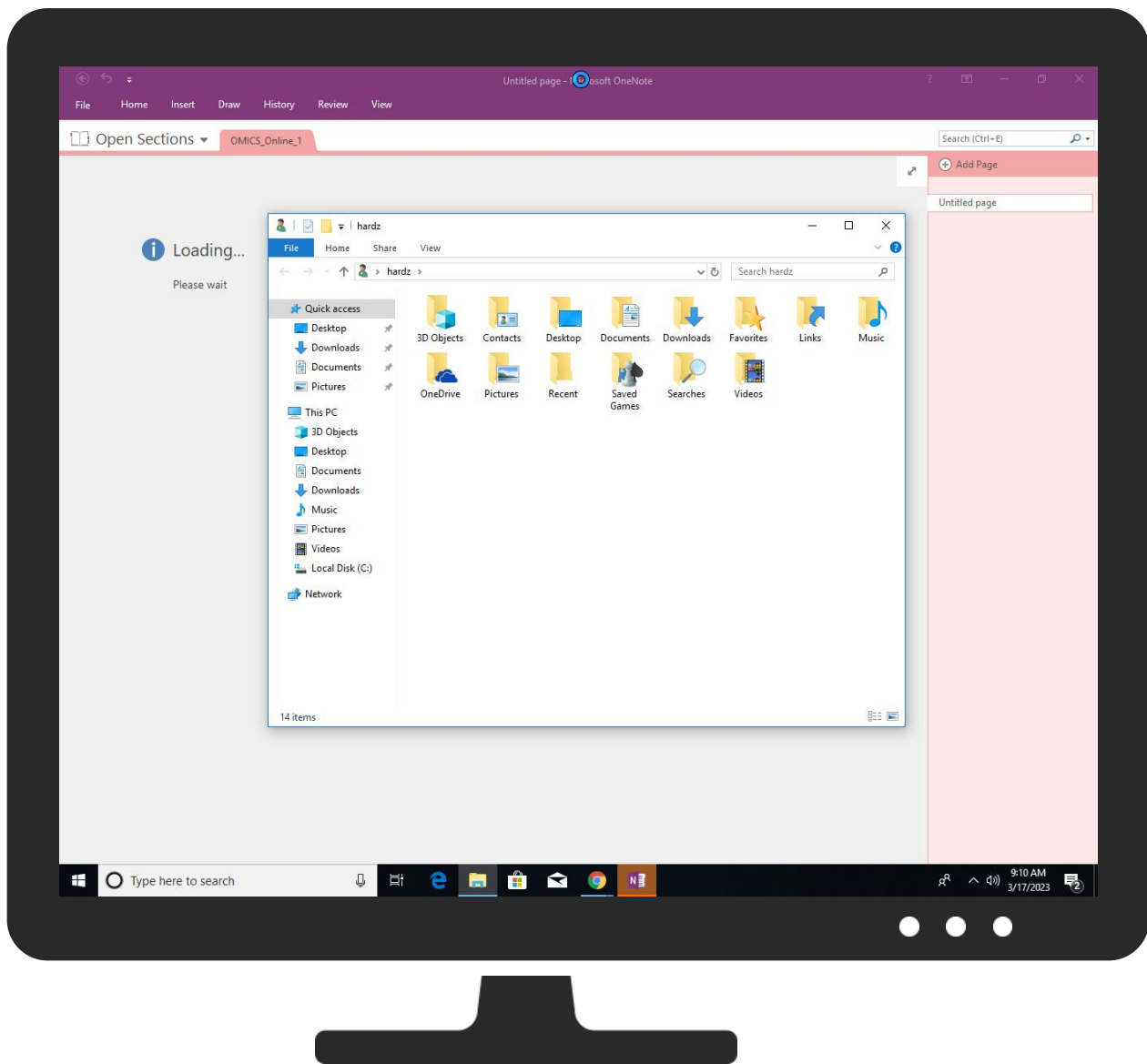
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	2 Registry Run Keys / Startup Folder	1 1 1 Process Injection	2 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	1 DLL Side-Loading	2 Registry Run Keys / Startup Folder	1 Virtualization/Sandbox Evasion	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

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
OMICS_Online_1.one	38%	ReversingLabs	Script-WScript.Trojan.On eNote	
OMICS_Online_1.one	17%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\rad98E2D.tmp.dll	58%	ReversingLabs	Win64.Trojan.Emot et	
C:\Windows\System32\Sftf\TSABlwWdRVZ\mmatLGgYnezL.dll (copy)	58%	ReversingLabs	Win64.Trojan.Emot et	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.regsvr32.exe.ce0000.0.unpack	100%	Avira	HEUR/AGEN.12 15476		Download File
12.2.regsvr32.exe.d00000.0.unpack	100%	Avira	HEUR/AGEN.12 15476		Download File

Domains

URLs

Source	Detection	Scanner	Label	Link
http://https://91.207.28.33:8080/jhiryhxp/kxgyfcacqegfa/5	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://213.239.212.5/jhiryhxp/kxgyfcacqegfa/fa/t	100%	Avira URL Cloud	malware	
http://https://119.59.103.152:8080/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://bbvoyage.com/useragreement/EIKHvb4QIQqSrh6Hqm/.dll	100%	Avira URL Cloud	malware	
http://https://www.gomespontes.com.br/logs/pd/les;C:	0%	Avira URL Cloud	safe	
http://https://103.43.75.120/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://penshorn.org/admin/Ses8712iGR8du/am	100%	Avira URL Cloud	malware	
http://https://penshorn.org/in	0%	Avira URL Cloud	safe	
http://https://91.121.146.47:8080/\$N	100%	Avira URL Cloud	malware	
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/798	100%	Avira URL Cloud	malware	
http://https://penshorn.org/	0%	Avira URL Cloud	safe	
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/wM	100%	Avira URL Cloud	malware	
http://https://bbvoyage.com/useragreement/EIKHvb4QIQqSrh6Hqm/.dll	100%	Avira URL Cloud	malware	
http://https://103.44.196.120:8080/	0%	Avira URL Cloud	safe	
http://https://www.gomespontes.com.br/logs/pd/vM	100%	Avira URL Cloud	malware	
http://softwareulike.com/cWIYxWMPkK/	100%	Avira URL Cloud	malware	
http://ozmeydan.com/cekici/9/	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/	100%	Avira URL Cloud	malware	
http://https://bbvoyage.com/useragreement/EIKHvb4QIQqSrh6Hqm/	100%	Avira URL Cloud	malware	
http://https://penshorn.org/admin/Ses8712iGR8du/tM	100%	Avira URL Cloud	malware	
http://https://www.gomespontes.com.br/logs/pd/	100%	Avira URL Cloud	malware	
http://https://82.223.21.224:8080/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://bbvoyage.com/useragreement/EIKHvb4QIQqSrh6Hqm/uM	100%	Avira URL Cloud	malware	
http://https://206.189.28.199:8080/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://penshorn.org/admin/Ses8712iGR8du/	100%	Avira URL Cloud	malware	
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/RJ	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/7	100%	Avira URL Cloud	malware	
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/	100%	Avira URL Cloud	malware	
http://https://103.43.75.120/jhiryhxp/kxgyfcacqegfa/fa/f	100%	Avira URL Cloud	malware	
http://https://119.59.103.152:8080/	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/?	100%	Avira URL Cloud	malware	
http://https://1.234.2.232:8080/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://103.43.75.120/	100%	Avira URL Cloud	malware	
http://softwareulike.com/cWIYxWMPkK/yM	100%	Avira URL Cloud	malware	
http://https://45.235.8.30:8080/jhiryhxp/kxgyfcacqegfa/IS	100%	Avira URL Cloud	malware	
http://https://10.235.8.30:8080/	0%	Avira URL Cloud	safe	
http://https://149.56.131.28:8080/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://459.59.103.152:8080/	0%	Avira URL Cloud	safe	
http://https://182.162.143.56/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/jhiryhxp/kxgyfcacqegfa/IN	100%	Avira URL Cloud	malware	
http://ozmeydan.com/cekici/9/xM	100%	Avira URL Cloud	malware	
http://https://72.15.201.15:8080/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/zM	100%	Avira URL Cloud	malware	
http://https://160.16.142.56:8080/	0%	Avira URL Cloud	safe	
http://https://bbvoyage.com/useragreement/EIKHvb4QIQqSrh6H	100%	Avira URL Cloud	malware	
http://softwareulike.com/cWIYxWMPkK	100%	Avira URL Cloud	malware	
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/	100%	Avira URL Cloud	malware	
http://https://103.43.75.120:443/jhiryhxp/kxgyfcacqegfa/	100%	Avira URL Cloud	malware	
http://https://91.121.146.47:8080/jhiryhxp/kxgyfcacqegfa/Z	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
penshorn.org	203.26.41.131	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://penshorn.org/admin/Ses8712IGR8du/	true	Avira URL Cloud: malware	unknown
http://https://182.162.143.56/jhiryhxp/kxgycfaqegfa/	true	Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://softwareulike.com/cWIYxWMPkK/	wscript.exe, wscript.exe, 0000000A.00000003.348753046.0000000005DF7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350978145.0000000005B2A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.340831402.000000005AA4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.347768220.0000000005C30000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.348179950.0000000005D37000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350269475.000000005D3F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.341363850.0000000005AF2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.342250004.000000005BD4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.335230812.00000000035CF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.335230812.00000000035B8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.338361754.000000005A66000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.348373935.0000000005D8F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.347768220.0000000005C5A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.334706320.0000000035AD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350515217.0000000005EAF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.347919526.0000000005D29000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.343691393.000000005B84000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.352843978.0000000005D76000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.336614509.00000000059BF000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://91.207.28.33:8080/jhiryhxp/kxgycfcaqegfa/5	regsvr32.exe, 0000000D.00000002.829371998.0000000000E04000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://103.43.75.120/jhiryhxp/kxgycfcaqegfa/	regsvr32.exe, 0000000D.00000002.829371998.0000000000E04000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://213.239.212.5/jhiryhxp/kxgycfcaqegfa/fa/t	regsvr32.exe, 0000000D.00000002.829371998.0000000000E04000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://bbvoyage.com/useragreement/EIKHvb4QlQqSr h6Hqm/.dll	wscript.exe, 0000000A.00000003.350703760.0000000005E94000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http://https://119.59.103.152:8080/jhiryhxp/kxgycfcaqegfa/	regsvr32.exe, 0000000D.00000002.829371998.0000000000E9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 000000D.000000002.831696209.0000000002E1F000.00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown

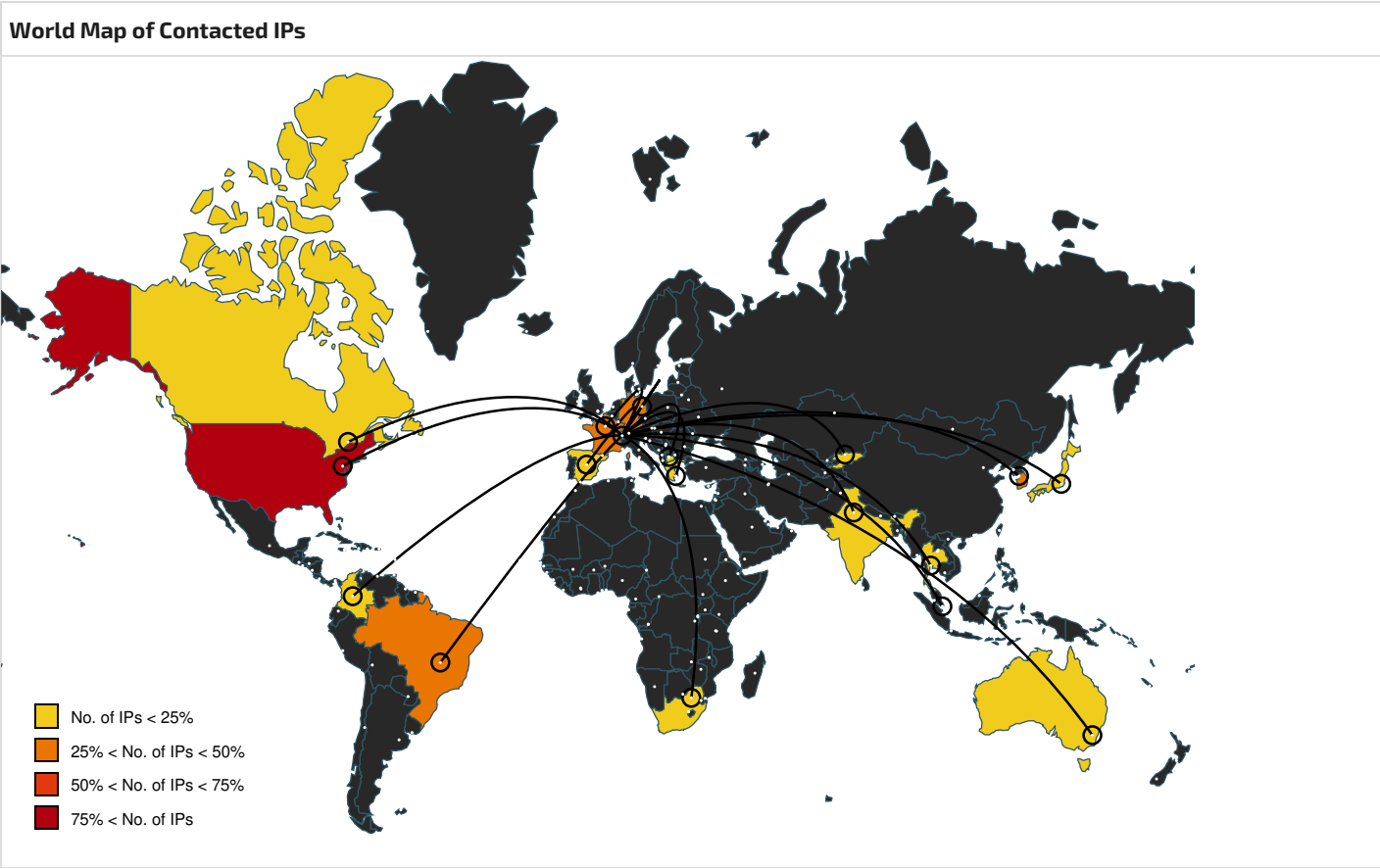
Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://91.121.146.47:8080/jhiryhxp/kxgycaqegfa/	regsvr32.exe, 0000000D.00000002.82937199 8.000000000D28000.00000004.00000020.000 20000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http:// https://45.235.8.30:8080/jhiryhxp/kxgycaqegfa/	regsvr32.exe, 0000000D.00000002.82937199 8.000000000E04000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 00D.00000002.829371998.000000000DE9000. 00000004.00000020.00020000.00000000.sdmp	true	Avira URL Cloud: malware	unknown
http:// https://bbvoyage.com/useragreement/EIKHvb4QIQqSr h6Hqm/	wscript.exe, wscript.exe, 0000000A.00000003.348753 046.0000000005DF7000.00000004.00000020.0 0020000.00000000.sdmp, wscript.exe, 0000 000A.00000003.350978145.0000000005B2A000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.340831402.000000 0005AA4000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.000000 003.347768220.0000000005C30000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.348179950.0000000005D37000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350269475.000000 0005D3F000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.000000 003.341363850.0000000005AF2000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.341316300.0000000005AFC000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.342250004.000000 0005BD4000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.000000 003.335230812.00000000053CF000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.335230812.0000000005B8000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.338361754.000000 0005A66000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.000000 003.348373935.0000000005D8F000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.347768220.0000000005C5A000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.334706320.000000 00035AD000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.000000 003.350515217.0000000005EAF000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.347919526.0000000005D29000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.343691393.000000 0005B84000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.000000 003.352843978.0000000005D76000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.336614509.00000000059BF000 .00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://www.gomespontes.com.br/logs/pd/les;C:	wscript.exe, 0000000A.00000003.350515217 .0000000005EAF000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.351034904.0000000005EC3000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350578583 .0000000005EBA000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000002.355161456.0000000005ECB000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350476503 .0000000005EA9000.00000004.00000020.0002 0000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://45.235.8.30:8080/	regsvr32.exe, 0000000D.00000002.82937199 8.000000000DE9000.00000004.00000020.000 20000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://www.gomespontes.com.br/logs/pd/vM	wscript.exe, 0000000A.00000003.351427235 .0000000005684000.00000004.00000020.0002 0000.00000000.sdmp	false	Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://penshorn.org/admin/Ses8712IGR8du/am	wscript.exe, 0000000A.00000003.350515217.0000000005EAF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.351034904.0000000005EC3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350578583.0000000005EBA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350476503.0000000005EA9000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://penshorn.org/in	wscript.exe, 0000000A.00000003.353397957.0000000005F04000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.351362338.0000000005F04000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.355271644.0000000005F04000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://91.121.146.47:8080/\$N	regsvr32.exe, 0000000D.00000002.829371998.0000000000D28000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://bbvoyage.com/useragreement/EIKHvb4QIQqSr h6Hqm/.dll	wscript.exe, 0000000A.00000003.348753046.0000000005DF7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349152202.0000000005E00000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350169852.0000000005E6F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350169852.0000000005E6F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349845444.0000000005E51000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.348523417.0000000005DF7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350313117.0000000005E76000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350446103.0000000005E8B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349372624.0000000005E14000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349551261.0000000005E41000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350378483.0000000005E82000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349251383.0000000005E0B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350068964.0000000005E65000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://103.44.196.120:8080/	regsvr32.exe, 0000000D.00000002.831696209.0000000002E38000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ozmeydan.com/cekici/9/	wscript.exe, wscript.exe, 0000000A.00000003.348753046.0000000005DF7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350978145.0000000005B2A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.340831402.000000005AA4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.340831402.000000003.347768220.0000000005C30000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.348179950.0000000005D37000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350269475.000000005D3F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.341316300.0000000005AFC000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.342250004.000000005BD4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.335230812.00000000035CF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.335230812.00000000035B8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.338361754.000000005A66000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.347919526.0000000005D29000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.343691393.000000005B84000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.352843978.0000000005D76000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.336614509.00000000059BF000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://penshorn.org/	wscript.exe, 0000000A.00000002.355343827.0000000005F1C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.351172369.0000000005F1C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.353077144.0000000005F1C000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/798	wscript.exe, 0000000A.00000003.348753046.0000000005DF7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349152202.0000000005E00000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349845444.0000000005E51000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.348523417.0000000005DF7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349372624.0000000005E14000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349551261.0000000005E41000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349251383.0000000005E0B000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://portalevolucao.com/GerarBoleto/fLIOoFbFs1jHtX/wM	wscript.exe, 0000000A.00000003.351427235.0000000005684000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://72.15.201.15:8080/jhryhxgp/kxgycfaqegfa/	regsvr32.exe, 0000000D.00000002.82937199 8.000000000E04000.00000004.00000020.000 20000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
<a href="http://https://bbvoyage.com/useragreement/EIKHvb4QIQqSr
h6H">http:// https://bbvoyage.com/useragreement/EIKHvb4QIQqSr h6H	wscript.exe, 0000000A.00000003.348753046 .0000000005DF7000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.349152202.0000000005E00000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349845444 .0000000005E51000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.348523417.0000000005DF7000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349372624 .0000000005E14000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.349551261.0000000005E41000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350131095 .0000000005E5B000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000002.355075856.0000000005E63000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.349251383 .0000000005E0B000.00000004.00000020.0002 0000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
<a href="http://https://portalevolucao.com/GenerBoleto/fLIOfbFs1jHt
X/">http:// https://portalevolucao.com/GenerBoleto/fLIOfbFs1jHt X/	wscript.exe, wscript.exe, 0000000A.00000003.348753 046.0000000005DF7000.00000004.00000020.0 0020000.00000000.sdmp, wscript.exe, 0000 000A.00000003.350978145.0000000005B2A000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.340831402.000000 0005AA4000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.00000 003.347768220.0000000005C30000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.348179950.0000000005D37000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.350269475.000000 0005D3F000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.00000 003.341363850.0000000005AF2000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.341316300.0000000005AFC000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.342250004.000000 0005BD4000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.00000 003.335230812.00000000035CF000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.335230812.00000000035B8000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.338361754.000000 0005A66000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.00000 003.348373935.0000000005D8F000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.347768220.0000000005C5A000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.334706320.000000 00035AD000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.00000 003.350515217.0000000005EAF000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.347919526.0000000005D29000 .00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.343691393.000000 0005B84000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 0000000A.00000 003.352843978.0000000005D76000.00000004. 00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.336614509.00000000059BF000 .00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://wrappixels.com/wp-admin/GdIA2oOQEiO5G/zM	wscript.exe, 0000000A.00000003.351427235 .0000000005684000.00000004.00000020.0002 0000.00000000.sdmp	false	Avira URL Cloud: malware	unknown
http://https://160.16.142.56:8080/	regsvr32.exe, 0000000D.00000002.82937199 8.000000000D6C000.00000004.00000020.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://softwareulike.com/cWIYxWMPkK	wscript.exe, 0000000A.00000003.335620877.00000000035A8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.352736179.00000000035A8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.337612568.00000000035A8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://103.43.75.120:443/jhiryhxp/kxgycfaqegfa/	regsvr32.exe, 0000000D.00000002.831696209.0000000002E1F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://91.121.146.47:8080/jhiryhxp/kxgycfaqegfa/Z	regsvr32.exe, 0000000D.00000003.418840821.0000000000DA1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000D.00000002.829371998.0000000000DA3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
103.132.242.26	unknown	India		45117	INPL-IN-APIshansNetworkIN	true
104.168.155.143	unknown	United States		54290	HOSTWINDSUS	true
79.137.35.198	unknown	France		16276	OVHFR	true
115.68.227.76	unknown	Korea Republic of		38700	SMILESERV-AS-KRSMILESERVKR	true
163.44.196.120	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true
206.189.28.199	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
203.26.41.131	penshorn.org	Australia		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true
107.170.39.149	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
66.228.32.31	unknown	United States		63949	LINODE-APLinodeLLCUS	true
197.242.150.244	unknown	South Africa		37611	AfrihostZA	true
185.4.135.165	unknown	Greece		199246	TOPHOSTGR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
183.111.227.137	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
169.57.156.166	unknown	United States		36351	SOFTLAYERUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
139.59.126.41	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
167.172.253.162	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
167.172.199.165	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
202.129.205.3	unknown	Thailand		45328	NIPA-AS-THNIPATECHNOLOGYCOLTDTH	true
147.139.166.154	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
153.92.5.27	unknown	Germany		47583	AS-HOSTINGERLT	true
159.65.88.10	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.226.75	unknown	United States		63949	LINODE-APLinodeLLCUS	true
164.90.222.65	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
213.239.212.5	unknown	Germany		24940	HETZNER-ASDE	true
5.135.159.50	unknown	France		16276	OVHFR	true
186.194.240.217	unknown	Brazil		262733	NetceteraTelecomunicacoesLtdaBR	true
119.59.103.152	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuath	true
159.89.202.34	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
91.121.146.47	unknown	France		16276	OVHFR	true
160.16.142.56	unknown	Japan		9370	SAKURA-BSAKURAIInternetIncJP	true
201.94.166.162	unknown	Brazil		28573	CLAROSABR	true
91.207.28.33	unknown	Kyrgyzstan		39819	PROHOSTKG	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
103.43.75.120	unknown	Japan		20473	AS-CHOOPAUS	true
188.44.20.25	unknown	Macedonia		57374	GIV-ASMK	true
45.235.8.30	unknown	Brazil		267405	WIKINETTELECOMUNICACOESBR	true
153.126.146.25	unknown	Japan		7684	SAKURA-ASAKURAIInternetIncJP	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
187.63.160.88	unknown	Brazil		28169	BITCOMPROVEDORDESERVICOSDEINTERNETLTDA BR	true
82.223.21.224	unknown	Spain		8560	ONEANDONE-ASBrauerstrasse48DE	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
95.217.221.146	unknown	Germany		24940	HETZNER-ASDE	true
149.56.131.28	unknown	Canada		16276	OVHFR	true
182.162.143.56	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
1.234.2.232	unknown	Korea Republic of		9318	SKB-ASSKBBroadbandCoLtdKR	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
94.23.45.86	unknown	France		16276	OVHFR	true

General Information	
Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828485
Start date and time:	2023-03-17 09:04:54 +01:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 12m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	OMICS_Online_1.one
Detection:	MAL
Classification:	mal100.troj.expl.evad.winONE@11/441@1/49
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 50.2% (good quality ratio 42.4%) • Quality average: 60.5% • Quality standard deviation: 35.6%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .one • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, rundll32.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 20.234.90.154, 20.223.225.174, 8.248.235.254, 8.238.189.126, 8.241.126.249, 8.248.117.254, 67.26.139.254, 23.10.249.147, 23.10.249.161, 209.197.3.8
- Excluded domains from analysis (whitelisted): www.bing.com, fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, config.officeapps.live.com, nexus.officeapps.live.com, officeclient.microsoft.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile 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 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 NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:06:32	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Send to OneNote.lnk
09:06:36	API Interceptor	2x Sleep call for process: wscript.exe modified
09:07:08	API Interceptor	23x Sleep call for process: regsvr32.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:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 	
Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 62582 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62582
Entropy (8bit):	7.996063107774368
Encrypted:	true
SSDEEP:	1536:Jk3XPi43VgGp0gB2itudTSRAn\TWTdWftu:CHa43V5p022iZ4CgA
MD5:	E71C8443AE0BC2E282C73FAEAD0A6DD3
SHA1:	0C110C1B01E68EDFACAEAE64781A37B1995FA94B
SHA-256:	95B0A5ACC5BF70D3ABDFD091D0C9F9063AA4FDE65BD34DBF16786082E1992E72
SHA-512:	B38458C7FA2825AFB72794F374827403D5946B1132E136A0CE075DFD351277CF7D957C88DC8A1E4ADC3BCAE1FA8010DAE3831E268E910D517691DE24326391A
Malicious:	false
Preview:	MSCF....V.....l.....BVrl..authroot.stl....oJ5..CK..8U....a..3.1.P..J..t..2F2e.dHH.....\$E.KB.2D..-SJE....^..'.y)...{m.....\..}...4.G.....h....148...e.gr.....48:L.. ..g.....Xef.x...t...J..6~...kW6Z>....&.....ye.U.Q&z:vZ..._...a...].T.E.....B.h....[...V.O.3..EW.x.?Q...\$.@.W..=.B.f..8a.Y.JK..g./%p..C.4CD.s..Jd.u...@.g=...a... .h%..'xjy7.E ..\.....A..'.4TdW?Ko3\$.Hg.z.d~...../q..C.....`...A[ W(.....9...GZ;...l&?...F...p?... .p....{S.L4..v.+...7.T?...p..`..&..9.....f...0+.L.....1.2b)..vX5L'~....2vz..E.Ni.{#...o..w.?.#.3 ..h.v<.S%].tD@!Le.w.q.7.8....QW.FT....hE.....Y...../,%Q..k...* Y.n..v.A.../...>B..5\..-Ko.....O<.b.K.{.O.b...._7...4;%9N..K.X>.....kg-9..r.c.g.G].*{[-...HT...",?q...ad. ...7RE.....!f..#..../....?-^..K.c^...+{g.....]<..\$.=O.....ii7.wJ+S..Z..d.....>..J*...T..Q7..`r<\$...d'K'..T.n....N.....C..j;..1SX..j....1...R....+....Yg....]....3..9..S..D..`.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1274376123142225
Encrypted:	false
SSDEEP:	6:kKuGry/7UN+SkQIPIEGYRMY9z+4KIDA3RUecZUt:nCvkPIE99SNxAhUext
MD5:	7EC27A161F3D5A8AA2A33F27634891BB
SHA1:	8142A2DED883933664E5A9FE2CCF7014EA71A9E2
SHA-256:	001E72BE36E53C9BBDBE27BEBB8B4B66DF02A0A85BF95ADA01EDFDC00C8A978E
SHA-512:	2FF40D52EE0C410DCAD2353C7D26B7C3777CED03B9FB6FB94D816EF86851FD7202002DED8A6962A91DB1F316D13C5D849F071BED30DE42A5605156217215711 B
Malicious:	false
Preview:	p.....X..(.....K.....&.....v...http://.ct.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./m.s.d.o.w.n.l.o.a.d/.u.p.d.a.t.e./v.3/. s.t.a.t.i.c./t.r.u.s.t.e.d.r./e.n/.a.u.t.h.r.o.o.t.stl...c.a.b..."0.d.2.f.9.2.9.a.7.4.b.d.9.1.:0..."

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\98BB5134-EE3F-4D7D-9136-7342 A66C9981	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	154907
Entropy (8bit):	5.352043871206724
Encrypted:	false
SSDEEP:	1536:R+C76gfYBIB9guw6LQ9DQl+zQxik4F77nXmvidlXRpE6Lhz67:QcQ9DQl+zrXgb
MD5:	7C6683A5448AC2C03AF2E56502A0376B
SHA1:	BB1FBE2413EB1FC145E20B6C56866818372316BF
SHA-256:	9EE148A7B15BBBE16D7C6E332A5EEFF259AB2229488433AFBDBDA7A70573ABD2
SHA-512:	B387317660A70B41E05A05D996E07B685718104AA2212ECCD829363A160AF25D008F9D101CBC2431022059D89AAD56FBBE45E963AF119170B78903B1550C17F1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2023-03-17T08:05:54">.. Build: 16.0.16310.30525->.. <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.aspx</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="CIViewClientHelpId" 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\OneNote\16.0\Backup\My Notebook\~Quick Notes.one.onebackupconstruction	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	70280
Entropy (8bit):	0.16192502549698293
Encrypted:	false
SSDEEP:	24:gmYyfB0zloOFTQBsXQrTQzkM0QaBpRzBXcgTCZD/kRWwk:gmNBuloOFTQBCQrTQL0TLTTcmLwk
MD5:	92184B2ED0DD46A6155CC09CC3DB3061
SHA1:	FA3E25E3B2D48FBB0B643A677836A2403CF5011A
SHA-256:	F428577F45E17332225CD88ADA59A822CDE651DA08F4439F57E8DC9A098335BF
SHA-512:	AAB7FB906502DB66B6E49CDEC976BC61909DD417D6C56E51B46EE772B1FD3D62F1EE8252B076F0BB48F4AABEF7C401837BCC3BBCFEA0D7D044B69888884909E8
Malicious:	false
Preview:	.R\(.M..Sx.)..f...J...@...D@...%D.....?....l.....*...*...*.....h.....h.....8^>.NK..1../.....2...6..l.T.i.x>.....7...7...7...7.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000005.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 165 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	3679
Entropy (8bit):	7.931319059366604
Encrypted:	false
SSDEEP:	96:tT+LtoQ9jsUBsnwIDGThUe8ww2iJiGEjdKKnnE+Gh:V+Ltt5GwlDQHue8ww2iJi7MKnnE+K
MD5:	995CEACAD563F849C4142B6A6F29F081
SHA1:	44CB3B867CD2917541B7D5AAED2F14F10FEBB0FD
SHA-256:	3691FB8C60EA1B827092F05FBB1807E34726016C6FF56698D7B81C44D519D22A
SHA-512:	3C8EFEB966B075D06D8344483352BF92C9292F9970C9377BE254EB355EFAF017916737AECDCD704B84D532B7229F9908951A6F2CC3FAD810791CAB224401AD31
Malicious:	false
Preview:	.PNG.....IHDR.....c.L.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....W...Gh...k.Hm...J.m....X...Eh...%..n....PHvy\$%...[...R...l...(/...yl...Z.h..Hl.../.. y w...7d3 s.s.={s.g.6W.^.).@..{.'O.LL.....c.^6xS&O.....J.(?.....),\$......@.zk....,\$.....)..7 O...mH7..0.. ..&j..t..F...T...AZ7z....\$H...AZ7z....\$H...AZ7z....\$H...AZ7z....\$H...W.6....0...FTcc.Wi...Q)...<.*.....{...#G...Y.f...KKK...,4.....{S`...+O.[.+ H...(<..Qy*.ET.PM...c....~(g.*...ol.K.....Sc8..q.F.KM"<...t.O>b..\$*t..].....2..y.h."lf.08ht..m.(..C.7n.....@...SVUU).F.).X\ j.U....\$x\$d..e...<.W.....=;0L78t+..Gw...-....].....C7.....K.w...._..g.....A.&M.\$^.#.!...e.\P.....;vD...@...Za.@*D..f...!..2w...4#.J.c....KJ)...F.u.l.b.V2.k...5`....*.....M...!...;E..BZ....K.[7....5.....K..7+6.o.o....`..z..5x...46x.b.....Y....s.^x=e.4s.W..t..iu.G^.....(74....`.....:.....].&.j+t9..3..}..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000006.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 127 x 138, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2232
Entropy (8bit):	7.837610270261933

Encrypted:	false
SSDEEP:	48:dFQY2WmQbe+TukEC2KgYPsWOUWfK792oP/sWtGOK9Lc+rD0NTHj:3L+wKkEOgx3PG92EqI9LczFD
MD5:	EDB5ED43CC6038500A54B90BEC493628
SHA1:	A8CD63F3914E4347F4C5552FB922C6C03917F45F
SHA-256:	9F3312E33EB78C6952B5A5D881BBD18751FCFAC41D648C6F053CE781342A504F
SHA-512:	4EBCEFD69A4C249AA3B0F00A954C4E463DA22FC9CA0B61A0DC46079B438138C509B22188D966FFF6599A3A604858BC4CC8FE6E0685A764E8E0477AB7A237DB32
Malicious:	false
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d...MIDATx^..hVU...:s::6..9g.MM3...j...*.....A..!A....R.Ai%YH..(M..".h.cf*.B.....{w{.....y.s>.{ {=.....#.y..r.K...K.0}.....Y..b..[N.=...j.=.....!...../6....B.8....p....5P)....@.....=.....^~..@..o'n<q....Yw].mg\V*...y.W.T.>..\n...s.iG.~L].d.<8..j<.<1..4...CZ0...} ...oDDh.....]3]#"B..O.....0)B.F.L.....5.f.FD..L.....5.7""4*.p.....'kt...>!k.oDDh.....]3]#"B..O.....0)B.F.L.....5.f.FD..l..x.....Z^>B\$1.N")4....1:&F8..*.X.yL{..s.3.....~2. EL%w.Uc.zJ...B..S..b.7o)%..7..!.....N.. .Vi...q..uO../...W[.y...&i!.. X&T.....-.....Z..o~u..U...cF.M....O4}.....~.....:T..W.._s...t..Dlb.\$Pr//..._4.b.....R.T\$t..\$>hB..+.{..m.w..Q...05..C..)}.....?..h.....Y..8.6^t...}.y.%.....l=\$..[~.. .h..N.....*SB..8..H....._G...;6YQ WO.o.} ..'.\$.o.E.y...i'9.[cmS...@m@.Q

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000007.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 46 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.814570704154439
Encrypted:	false
SSDEEP:	48:4gv2YZ4gWLPuU9JcREmXfFEV7NNkfKOgV60g0Z:KZgWLPsJcj+mPFGNkfnpg
MD5:	3F1535054D4F9626F0EB10CEE47F076E
SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C60
Malicious:	false
Preview:	.PNG.....IHDR.....1.....*[.....sRGB.....gAMA.....a.....pHYs.....o.d...IDATXG.iLTW..._23....6.....kK.5...5..IMh..Tl.....V.v.PZ.-F..".k.pCQ.....#/s>f..3s....<...=^ '/~.;a...{>.g...."o.6k..k...E...O....aQ.j...X&vG.....{u-...\$.CX....xhZ...Q...Z.....O...l..ld.h....q..q.....Y...J7O7.R...~o...[.....;h...u.g.>X...o.}}....>...u.....5...2].. ...EodZ.R.i...=ryxh...C!.6\$!..)..W.^...Q.y...Ay[...M'o...;hh'....}.%....."h.5.?=.y.x..2/gK...4.2P.(#S.F.G.o...!Mk..w/_1^5....[U7.0.Z..w^..&/...G...Y...g...;JF.t...~'.X...uYd.E. ..+R...2cHG9..YC.X..Eg.).r..+%%.t..6/...@...3.... .O .0..!.;....._...E.J"...).#R"...q...~r...%.4....b..Q....al..6.....{y...l1.Xs.).y.;...u\.....sm.C..@_2.AG.K..5..}k..~.....4..< ..PH .)Z.[H.G.iH.7UR.`..B.f.....<5n7.*WR.c....l1.....<y.%...-..."Y@.*...)).(...l...y.z6...J2.s...c...z.G..Kj..^R...M..k>.PA.1>.s<.G...8.r.....dL..uF.(...q.P.j@...CPSc..^

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000008.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 749 x 126, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13084
Entropy (8bit):	7.940058639272698
Encrypted:	false
SSDEEP:	384:o4KSpFN6Ud4c3p2II1yavNr5spYVJzimlIZ.wGN6Udv4IKavLBJz/r
MD5:	0693DABBBc411538D209F32E22F622F6
SHA1:	FB7E675406FA123CDB7E058D336742D6A2E8DC8E
SHA-256:	2DFB2E7A1A3AA43C673D2EE540D3C366CEB12105EB5441F98992FC06F4284013
SHA-512:	F07732660EC62DAE58EB02E29476007EA92BF826F642BCA547097136AEA01D29FF69D9B0CD0F5D65A5E15AA66CA4AA4804AA171A3504AAB198631C643C90C16
Malicious:	false
Preview:	.PNG.....IHDR.....~.....sRGB.....gAMA.....a.....pHYs.....o.d..2.IDATx^w....'m.9c.6"....&.`.N.(.TN.Ne.N.R.eKr..T.*[...?T...l.D.S>I\$A..l.....y.9....f.....3..Gh....)_ .o...n..A@.....A@.....L...2... ..x...#.1f]9.[.....A@.....3fE@x.YWN.....A@.....1.....Y..J.Y.N....s"......./..rc.scuyyyu...)\s...t.oi..j..lv....Gr.#9 %%%%9%-...d.T...r...DH...6.....%U..A@.0.....rAD2.5.....L.R.=W..gZ^o..-?.T.Cy:...y.9.y.EE...v.....1..R....1."...`"...ss.....i!.hY...Fj"...%~.Gw...HJJr8..6...#.....l(? P.(...8(u.....*.OOO.....dgg...Q..=.c.y....A^S.@.....3.CC..GFfg..l.I.COrrFFFNNV^nna^z..%..(..a.b\$......a.y.LMO-.yIV+..k..T>Jg..*//+.....M=.x....E....`~..N.Kww.z...%%.e.%yy.i..P.)^A.5.d.0.Cc35==66>2::33.>.:;l.i.i.gv...DSd...l#...l.....)**,**...V..1..F.'7....).SSs..7..F...C.p...(*.....(RG..B...!l.2... r1

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000009.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 46 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.814570704154439
Encrypted:	false
SSDEEP:	48:4gv2YZ4gWLPuU9JcREmXfFEV7NNkfKOgV60g0Z:KZgWLPsJcj+mPFGNkfnpg
MD5:	3F1535054D4F9626F0EB10CEE47F076E

SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C60
Malicious:	false
Preview:	.PNG.....IHDR.....1.....*[.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATXG.iLTW... 23...6kk.5...5..IMh..Tl.....V.v.PZ.-F..."k.pCQ.....#/s>f..3s...<...=^ '/~.;a...[>.g...."o.6k..k....E....O....aQj...X&vG.....{u-...\$.CX.....xhZ...Q...Z.....O...l..ld.h....q..q.....Y..J7O7.R...~o...[.....;h...u.g.>X...o.]]>..._...u.....5...2]...EodZ.R.i...=ryxh...Cl..6\$!..).W.^...Q.y...Ay[...M'o...;..hh'....}.%....".h.5.?=.y.x..2/gK...4.2P.(#S.F.G.o...!Mk...w/_1`5...[U7.0.Z.w^.&/...G...Y...g...;..JF.t...~'.X...uYd.E. ..+R....2cHG9..YC..X..Eg.).r..+%%.t..6/...@...3.... .O .0.:l.;....._E.J"...).#R"...q...~r...-.%4...b..Q...al..6.....{y...l1.Xs.}.y;...u\.....sm.C..@ 2.AG.K..5..}.k ..~.....4..< ..PH .).Z.[H.G.iH.7UR.`..B.f.....<5n7.*WR.c...l1.....<y.%...-..."Y@.*...)).(....l.y.z6...J2.s...c...z.G..Kj..^R...M..k>.PA.1>.s<.G...8.r....dL...uF.(...q.P.j@...CPSc..^

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000A.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 163 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4847
Entropy (8bit):	7.950192613458318
Encrypted:	false
SSDEEP:	96:JnieMJz5Tz/gKvP93jQvcv16kjOzbapFJBkjcMNBqmQzOG8qx1QKmse8T:JieMJzph13Evcv16RfapFLxMNBo8qxa
MD5:	A1A1017A6A7928761CEB56D1D950E123
SHA1:	28272E9C7F816A1CE8F2033FC00F489005332365
SHA-256:	72F066CD34EA71D0E1B28FB60D663B0372C5254E1A8239C94A164EEF9389DB88
SHA-512:	10F4557F102230126BC86CD4B49C93365C38D5CBEAC51F4691B90D861098866A2BDEFEB5A07731D4FA14367FEE430453BD716157F9074EF643F2B949B09E1530
Malicious:	false
Preview:	.PNG.....IHDR.....n.<.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATX^.]`TU..).E.O.T....L~....af...Z.....O..4..>Ms..Js_...5.E.d...Y....?z.3..}.l. ?~...{.....s.z..Y..... ....E.X.6...c..u...y..W.j....."}...l.i.`l-l-.....MKH.E.bi.d...b.X.)...X4 .vj6~...;+/->Qyit...%.T..k;U..y.C\$[;..Gm.....v..*2..2..eee..."l.)...yy...lll/..u.....2...M.:"...W....o..t...._6m... .`k.T.v"...q.....s~>.....O....ed.[W0X..HB.V.i...<=..E^^.....MyY..vpp.....^6....aQQQaaa.....]^nkg../_d'.%.....L&k..B.....?C....W.VVV6660t.J+K:...%q.....e.cp... Kz..%.qZsAR(T.l.....>55.R.u.W\L....T...K..rE.U.K.-9....y.y.....K....>...HWTT.e....+..B.....%%%.....^...].M'.%fl/..=p...[O.../...@...DP..hw8....7o>..A.mgg.....7-]~.s .OE.E. =.....%ly.....\.....MSn.i.....!..U.\$0SZ.P.][.%X[;{...N.....\.....6O.....'N.}.s.m...E..V..f..r...4..~.....H..F.}....4..R.=.....xT..4...../_...z

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000B.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 46 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.814570704154439
Encrypted:	false
SSDEEP:	48:4gv2YZ4gWLPuU9JcjREmXfFEV7NNkfKOgV60g0Z:KZgWLPsJcj+mPFGNknfngp
MD5:	3F1535054D4F9626F0EB10CEE47F076E
SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C60
Malicious:	false
Preview:	.PNG.....IHDR.....1.....*[.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATXG.iLTW... 23...6kk.5...5..IMh..Tl.....V.v.PZ.-F..."k.pCQ.....#/s>f..3s...<...=^ '/~.;a...[>.g...."o.6k..k....E....O....aQj...X&vG.....{u-...\$.CX.....xhZ...Q...Z.....O...l..ld.h....q..q.....Y..J7O7.R...~o...[.....;h...u.g.>X...o.]]>..._...u.....5...2]...EodZ.R.i...=ryxh...Cl..6\$!..).W.^...Q.y...Ay[...M'o...;..hh'....}.%....".h.5.?=.y.x..2/gK...4.2P.(#S.F.G.o...!Mk...w/_1`5...[U7.0.Z.w^.&/...G...Y...g...;..JF.t...~'.X...uYd.E. ..+R....2cHG9..YC..X..Eg.).r..+%%.t..6/...@...3.... .O .0.:l.;....._E.J"...).#R"...q...~r...-.%4...b..Q...al..6.....{y...l1.Xs.}.y;...u\.....sm.C..@ 2.AG.K..5..}.k ..~.....4..< ..PH .).Z.[H.G.iH.7UR.`..B.f.....<5n7.*WR.c...l1.....<y.%...-..."Y@.*...)).(....l.y.z6...J2.s...c...z.G..Kj..^R...M..k>.PA.1>.s<.G...8.r....dL...uF.(...q.P.j@...CPSc..^

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000C.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 123 x 103, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	7.80882577056055
Encrypted:	false
SSDEEP:	24:q3kLWZefR0kKbfLnNhzzt+acvt2x6pBs/j+7QUJ0QbDQ883ASaoUV4hNgq1rsyhi:q322nN+X11GDsg8831Uyhi/vf
MD5:	D5F7A65469623327F799B516ACBFFD2F
SHA1:	76C6333C14AF3A7EA091819953E6E12DC289A12C
SHA-256:	F476FAE1C6D79069239C471D182631AB343749C22B1A6990250465C7EC3738FE
SHA-512:	351B9E455E97E6247E64E4BC1B59C9524E70AE0D09D3B6FB96937378A70536483B00426EE69C3590DD415A8265D21FD031B524B90E4E86814EC9AD704E57793E
Malicious:	false

Preview:	.PNG.....IHDR...{g.....sRGB.....gAMA.....a.....pHYs.....o.d...IDATx^...h.U..p.T..(eBR...2.....':4kec^...0.&.....ugS.8u;i.P.F..f3...D...6.%...xal.}...y..9...s.w.s...{..y.5<<<...(0Q.....t...q/.[@.....-e.....=J.L.....c.4H.....U?.XF.KJ..zb..0..f)..J..[&..S.6...w..9.....<.....?j...H.....>...~...}.n.8.WW..B?...?b;.....<...~...b...m...&1.=Pq...w....a_3.k7"...d..z.O.w...s..Lh.x.....Q;40.i..8V..._@...rd....kF.@<@...e.....e....=mHB;...E./\h.^...q.>....%v:.O:...&q...:'e..9...hIG'.L<@<@.....([.].n.x..c.....O...[).....S*.Q..d....A...4...t...E..v..}.7...t.b....."/.H.].8.._@.(.;"Kt....).+[LwJ..B]i.b.k.@..Js.....J.....6..J.._LwS<@..J.YLwV<@G.4w.L..G...].zu.z.h....}.W.IH..+...c...F....ql....Xul.].N...wv\M\$.D...+...=.....?U...T..^<6../T*{q.q:...y..XL..l.z.d...G..b..g.G..b.....SM{q.q\$MUL..R.....^P..g...e.....L/yqM../b.f.....J.<
----------	--

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000D.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 59 x 61, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2210
Entropy (8bit):	7.86853667196985
Encrypted:	false
SSDEEP:	48:naUvGemgl0W5KMDRLEbGAnaHC7ew/fkDSCcE5FTaHWc:aerVIDRIlewkXlrTa2c
MD5:	73E38124F94AD20A2F1571FBBE11AEEC
SHA1:	87FB8056DC7A0A3B70D51426771C4CCE2099CFE5
SHA-256:	A700B63B30CBBE5230CC5E977D651E178EA87E73EAB18C8D5FFB1362149ADDF7
SHA-512:	320FCE64DD6F975384BEC9267348CD5CD24A55B13BB09FEF1238C2216AD8ECABDCCC15601A079CE092ACFA4954829FFEB06FBB0631F6AE26E3A39E43C102048B
Malicious:	false
Preview:	.PNG.....IHDR...;...=.....sRGB.....gAMA.....a.....pHYs.....o.d...7IDAThC.yL.w...r.r.....Eq.nnN.i.i.[e...-d.M.dn...x.xmQAT.Q.RN9..EA.k.P`..=)...m.&~.....o y...k...})x...[...g59.]]...~i.SY....."7Ow../.....2...3f)n[...R..R.....U?...O.{...c..p.T..t...5.07...07...7.o...+...V.c...&...%3l.....v..l...6.....??..[.N.....nz..Z.B.....v.prs.q1V1[...='...bz...%s.cf3..RyMNUeV..J.k.]D[~xo..d..c..sO.y'...B...c.07.....Rp..J.....{b.....;u...s....N.gko.M...;6...6..c.X5.S..o..\...^).....(.....y.72.^...s%...[ql&Z...C-+o....l....,Y.{.....g..1.0..l].....<.....T..}...t.lx&)..[7...4.5..{...n.<...#l.....r.wW~.zr..9k.^]KR.*W.J.n.")....%0...).Fbb5'4'.X..E.../t&t(...@9...\$.....].P..jdU.....H;,\$%'%'.l7.....y..\$. ...Z..4.Cm.u#&.%N...1...+8.....y...U.(.T.....).l..5r]...l..K....>f..3..C.G..X1.(<Gb..b(....0Qv0F.....n.z.s.Y.....\..h%1...QU..%.)BjCW.....sO..\...=&3....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000E.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 563 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14458
Entropy (8bit):	7.944094738048628
Encrypted:	false
SSDEEP:	384:uuT43eqJy2jEeSZE0onrAFAOpn5ytFtNrflkBQTYz8ynth2EB:EugQeS+nrAFZ8JNrfRQM4ynH2EB
MD5:	7CEB71F78A193F8C9F7FFDA5F81AEBD8
SHA1:	EEC1597705EFF1A527C246B86A71878185BA6B1B
SHA-256:	77911FF7AEAB8FCCAF36DE6E1183FFE1A6C27F77B5714EE780976CE5189E8FD0
SHA-512:	1D1AB19B64E1E2ABCA61AE78B3B50310B0A6CF19D2ECFCB4499D8D0BF68600B4D95BC0945EF9FF9B1D016ED61EAC518DCCA1A426F460317C07AD51E2E047548C
Malicious:	false
Preview:	.PNG.....IHDR...3.....>...sRGB.....gAMA.....a.....pHYs.....o.d..8.IDATx^}.p(W.ZRKjI..[.M.I.N..[.O..B&...?5...@.55EQ...T...d*U..*C6....8..}.Wy.e.....kJs..z..^..T....s...}:{.n.1..".@...P....."@...p@f.s@.....B...6D..."@f.3@.....B...6D..."@f.3@.....B...6D..."@f.3@.....B...6D..."@f.3@.....B...5...f.;0..7141...L...M.3.L...{M.T...l.C...@E[.w.Y...q...c3..gf.3..}...l...[M...@..4555==...!..f.....d...>i.%&&%..u...f..[.....O'.....G..E6l<..3.k...'...Y...<.....=U...{9.....S^^q.<..^...2.bb.E'r...ey.....3.....Dg@L..a'.x&"O.Y...le.c%\$(P__d....Sj..S...BLu.[g...mK.SwVe.."@.T@P.y.....=40..L...\$d..J....cccw...^..RBKKK...heJiS3.0l.X<..}..*O.....QR..q.5GTA..ht..(^Hno.n.....wv:...K?/\JQ/i..h0)G...1Y....K.>FT...8.d&...+-T.b.....f.."3.V.6....E.1...?Q.6....A1Smm..K...V)....:uA'\$..v.cy.<.`Z322.r.lL.....>.....&....."...".....@.Ccccee.[..z[.fL5.[...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000F.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 742 x 104, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13030
Entropy (8bit):	7.948664903731204
Encrypted:	false
SSDEEP:	384:/06ULmwT2RqfIlhmLy4tNgPYl0mvBQhTMHX4PCIVYm:s6USI2RqfGhmDrpYM0ofHX4aIVYm
MD5:	17E9FF9F735102231846936F0E2BAF1A
SHA1:	9EC1AE8A3AD55C48C02427D842D6E38DA85B5145
SHA-256:	DD1CA8DA90893E0B63ABFDD9E60CF2BF844B311964E9D9DDB855C21FCA156EBB
SHA-512:	71E690D6C87B09659296E6E6DDC8E3F91035DD80C5CE875FA557763E8138900C27FB492885291CEE203D65BCEE8C20C9C39E0590A5FD32B8A00BEB3E3F6D6EF
Malicious:	false

Preview:	.PNG.....IHDR.....h.....2.....sRGB.....gAMA.....a.....pHYs.....o.d..2[IDATx^..wp!.....sN\$...\$..).Q.")R2ei,kl.%....r..vm.x<....\..u.U.g.ry=.uX.cK.dl..l1G..\$*.Fg.q...N.nt...3.w.w..~.v.O.....K.....A@.....A ..H.n.D;A@.....A@.....e.y1..P..xH.....e.91..P..xH.....e.91..@.\$9..S.....A@..4.....^C..F..VR\TT.....aHll1.....VS..g.....*.....z..jEk.....<R../55+33;;+..Y..WC..#..P.....s#0::.....522...,v..D.....9.2N.L^..F\$.....e..!.....N...`1...G....'&,f.f.X...!p.....l.....J..z.R,YbYd&....~"b\...b.Z.SS....c....&..Yl......[...BY.....1.Z..6NN....._zw...MKK.Z..vMMnnn.4.v....q..e...D%...Q.....p*M.....22..e...k}.....qU.....S.a...~...P..}v...1.1.2...F.GCC#...j]=.C..n#...K+..MOO.....".....d^2={...U.p.h%.%n...D...XB..b.."....?h.b.B\w..^Q^..UC.....Q..!.....U.VD...P..{2"A@...b..V.....jF.x.
----------	--

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000G.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 165 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	3879
Entropy (8bit):	7.9281351307465044
Encrypted:	false
SSDEEP:	96:k1hccap27HG\hY2Kn+A3RS+HG3dXrjmg26vh:k1hccewlhYxRmR5
MD5:	C451B2A146BDD7EF33AB3EA27268796D
SHA1:	C040BA2F31342CBCBF597C96D4D6EDB83D473B77
SHA-256:	4C264B2A6E88712234DAA8E3A8D630CBF4EEB338554CB0B794D8031F8943EE65
SHA-512:	55915A304B261BC6F38F5CFE0389D5195F85FE2C1DA325019C3AA391E8B1773091E078A35BD57F8CEE0BA035956382AE33790EF462053FCE711EEA9665B7F917
Malicious:	false
Preview:	.PNG.....IHDR.....c.L.....sRGB.....gAMA.....a.....pHYs.....o.d..IDATx^..j.p.U..g..Bp!..!..!`pA.+....H.U... "Z..*U...P.D~.\$.....\$g.....CB.l.....l.g.pc..Lf..~.=~jS.....w.9..w..!..L.A ..^..t..v..s4&&%%%.6.`...G.D@.7.qS...K...[.....o...p..2%..B.Y...];..gy+,[.....o...p..2%..B.Y...];..gy+,[.....og...}W..z{?..y...; t...=.e\.....6.M[...B.....[...^Pf.....f.../..6...<S.4./..m.....l...B'..n...O...yc.....X..P...k...t..9tf.g>...e..Sy'.L+**][..a...7...p..+.....K..y.9p..l[.i58...v..5'.Op.....{.....8..._S.....p..).....;.....y..2...b.]>pP...C..G.H.....Osp...).9x!..W....^.....\$r.p.sOJ.l.=x.9s&.....h..`W"V..l.l[.72.....zv@.#<...../...F][...c...4.W.....:uj@1...~X.....^si.....Z..l~Q<.....NAOq...+!')...\$L..gV.6#.....F\$.hD.g.L~..H_u..j4.....h...T.BK\Z222...7)).h...1??...~..i=X...~h...y[.....p....x...c...[...Uh.7n.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000H.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 651 x 254, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19235
Entropy (8bit):	7.944867159042578
Encrypted:	false
SSDEEP:	384:h4iuxL3Yck5lpMcTyHOypEod/G38lJxqSp5BCU:h4/xjYc2lmcOuuEoJm8fse5BCU
MD5:	AE32E846559D576FD263BD69FEDBEC28
SHA1:	D481DF71C858BAECFE33418002D368F2DCF68D4A
SHA-256:	6E21222B0EADAB8D3CFB0C7D14941D196165D6709271AF317D099F12403CD352
SHA-512:	9AA4A6DD01D3B745D674721765F2BFCCAB584CA0603F222EDBE9A88190A2A57438041E7A3706CC0656A6ABB79AA18118319F210EFFE3DD917E7B94A6294BD346
Malicious:	false
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d..J.IDATx^..X.W...D..A.....bW.A..[.5.F..D...7.ob71.....b.."..."(/{...e.....}.....;..S.X...H...@d.....&.....b.....F.....b.....F.....b.....F.....b.....F.....b.....F.....b.....O.KVIVfjFzJzVF..j{i.R..l.q..`l...e..'/..`G.z.*l&>)61.UjVzf..4>Q~...U..=.....s..\WE...2...t..`F...M.....'.?....>BO(m.V.P...Gy../.....B.6.....= z7.Z.lhQ..u..j.....&..Z.bo?..u..S7.G>.....]l..7.i..3....<y..l]...Sl>...L.2.<.....['=M.Tsprp...T...cE*".P.....eefQ.NKN.x....:~#5#...q./..xq.YzJ.:T."u.j..S.C=... ...2..(YF..... ...*7t...{.jz...W..Y..{...nlfj...L.6.[hS.=.....(lC.....?5..+...[.a.:U.K..C.....w.....+..r@.z.7..j.qB..B.....Xj}..=fk...>^5[...n.z....wn...Z4.._jWG.^..z6./.....dhM.9s...Gbo?...U.V..tj.....*&)lo.{q.G...A...l...i7...&...d.E]...#..W.x..T...&Mz4+].4.\$n..F..x...<ppr.....y..j./..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000I.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 220 x 170, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	7374
Entropy (8bit):	7.955141875077912
Encrypted:	false
SSDEEP:	192:lfgsPejaVZWzIZKpnPfI0HK5+2Y/SLopWR:lusPe287lZKpnzt0q5+qVR
MD5:	70DAF02EC771AB54452FA4C707BCAC74
SHA1:	30F46FAC5E96470848C5A948162CC12455A05154
SHA-256:	58469BA93EA36498F79864EB54713A001C52106DE97804506D82EE24B816712B
SHA-512:	E599FDC22A32CFEDBB23EECEAE0B278EAB9A0959FE6ACB40E2B201E45A7C19261AA529E7A0D9CAF2A9A4C64C7831343F3BC20810513990AD5D38A32741564F
Malicious:	false
Preview:	.PNG.....IHDR.....lC.....sRGB.....gAMA.....a.....pHYs.....o.d..cIDATx^..S[Y..l..B..`...N...t.q.j...+LU.....O..sF..l..w@..H.Q.w...s..{B.....2.....i.q.z{.^}.....J..fQ....r..WWW.T...amt.t;...6IN.....z.n...j.u.z..Q...?^.....;...NO;}c...<.....({.^...t.k...F..[m.....R2...%.y.'^OOONN8)....ly....}...}).Hy6.^a.....\lS...K.. >.....s.....l..P...LFWWJ.l.RK..b.h.h.3.F..j..j..~.....e.aa.....0H...<Y..a`.xAl...7.X...xd=.....h?o5.....Ay...?6.....*..tb.9."j...S'][(;P...9.2]?...z3wD.[.....L3.Ng2Gj].....&.0ZK1u8.H.2..Z../..P(...BA..aLj.a.Y.....J...5^x.'..\&S...L..U.....<{"...@x...J.N...;..Wlht.<..B.....lHM...&z&..6u..hF..G.D..B.....A.....n..GG...;..Q...X"...r.....3d.[o.(/.3.H...xSx...h.8...r...<..DB...y.N..o...5.....L&w...v...w..D.....l.a4... "8.U.j0m.(.zR>..=+.L...e...Yd2.-Z.7..D".pX.l...e5qYa_&..3..J..++

Category:	dropped
Size (bytes):	14553
Entropy (8bit):	7.951135681293377
Encrypted:	false
SSDEEP:	384:EF7aDrPYJ1n3kaEf61xD+KvdokCixTQm7QA96dNT:EF7a/PMeaEf61IT6kCiFQCQq6zT
MD5:	3E9F7D399DF9CAD3669B7A5445EF7074
SHA1:	2FBC965DC03EF9203581F595E0D7AB1734726ED7
SHA-256:	76C80E31F37248C3C787F7972A7B22038390F9D81E72E650071A6F36D36AF27A
SHA-512:	326F8F9CBF829BF80AAA96062A57255A36EE04DE310634327AA075D14129CFA8E36E48AB2A00B10F9BDC1D94F1AC7A9E41D0D063361920A0332EC124BDF4C3FE
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d..8nIDATx^..xT...!=\$.%.t.H.tP:.HQP@E,...QQ.^.....* E.("]:K..R.....p..n.9{...sv.}.....7.....o..z...M+.....w.....O>..Sj.O...<{. x..g..l..H.....V ..}.PO..H+\$@.\$@=.=@.\$@.....VH..H.z.[.H... @=#.....C.z..GZ!.. ..).....T...B.\$@..\$.S.\$@.\$....>..i..H.....H..H@ ..Sj8)POy.....>...p..... ..}.PO..H+\$@.\$@=.=@.\$@.....VH..H.z?.....\$@.\$^i...c;..n..i..0.....<.....S...w..c....y..F4.p..3~.. .]....s.6[.H...N@=.M.]"...3./..l..'.. . K...r]..nX...^.. _G..ibj]..MY8].....9x..Ur'.. _.....5..H..d..L.\$@...l..o.;kM.\$.?.....K/l wn.....Y..E..%K*=.....Y.3.lk...[V..WG/?i..H..." T..z..6h.[.-%9....WMY...z.vH..H@/.BOE. ...g-P.@.....lH.O...SjJ5 .???^..5^)..\$.S.@...*<gJT/....._R.C.....rj..Cg^K.....K....~Y.....@..).l.k.s.Yr.....Z]jG..q.+..G... Nj .}.T1&&.....?...W<{...g.&Ca

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000000.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 454 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8184
Entropy (8bit):	7.807848176906598
Encrypted:	false
SSDEEP:	192:ExqMHYnnEnntvA4Mesu3SXHycmflIEFQp1r:E0MGEEn29esuIXHt0FQp1
MD5:	5B386BF9A20766956A84F67F913F23D7
SHA1:	6E72E51F5B4FA64E52D2B80B41409B3DB927A3C7
SHA-256:	DDF6A1D5B29BD69C65A148B1247FDE8389CC56865E4398E4CBDCBD68A6555043
SHA-512:	99B4109439D9A688D7747C6847E0FF7399CDA01A89C3181789F913E757A82EE4727F95E506F4B01930EFC7C6E229B94BB89E385B6BC009AB5CFE332585660C5
Malicious:	false
Preview:	.PNG.....IHDR.....s> Q....sRGB.....gAMA.....a....pHYs.....o.d....IDATx^...].!.....!YTP:A.....~.r.\$E.J!;....T.M.UE[. Q.x....wKB=.m...4.%.[:...9...{\.o.3.g. o~...~s.k...X.r..... @Gggg.?.... P_]]].*"!u...C...h...\$..... \.....@R.....\$.k....@.Hj0.8...~r@...F.l...G....T...@....P.....5...@ ..\$5.J.A...@R... ..#...C.#.@..H*... .. `'[(q...@.l.....% ... \.....@R.....\$.k....@.Hj0.8...~r@...F.l...G....T...@....P.....5...@ ..\$5.J.A...@R... ..#...C.#.@..H*... ..`'(q...@.l.....% ... \.....@R..... \$.k....@.Hj0.8...~r@...F.l...G....T...@....P.....5...@ ..\$5.J.A...@R... ..#...C.#.@..H*... ..`'(q...@.l.....% ... \.....@R..... W...1c.l.6.'~. @ ..l.S..l.l'...5\.;...1'c.k.u.Qs..).g#b.j. @..Y..QR...n.l...~h..Z..... .Xw.U~q... ..@.%'..... P.E.T.b.j.(F.p....C.)3:' .z.w.a....{\.:4[Y...~x../...g...J..9.K..._'.:;).....SO=u.E... Py.qf..)O7.o....u?;...6~..9...??.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000P.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 213 x 85, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1924
Entropy (8bit):	7.836744258175623
Encrypted:	false
SSDEEP:	24:rl0PN36BoJ9JK5IncTww67QKf5wX5YgM5s6cahePwnR6+eA9zQU13ALcVz7wTQ8U:rYN31JH6lcbjMW5Ytmyqwp9H7wY
MD5:	B1FDE66F75507567B5F0C6C07B01A3A1
SHA1:	80B8E6A923E853232F66C874367E90B5C9CAD7AE
SHA-256:	B9C82D2F31BBE409D159EE3C9129CBAAAC7C6F6C81637AB9B6DAB3C11AA74B7F1
SHA-512:	FC8C6038D3C2F5765D7524E969574ACD10AF6FCCFD45FE7C6DD4A8C2669B13EE3FB1A8833E94A046AB7037018170B5B87B1A2742E0E10557C413AD634BDF34E
Malicious:	false
Preview:	.PNG.....IHDR.....U.....Q.6.....sRGB.....gAMA.....a.....pHYs.....o.d.....IDATx^ .O.W....G.IT^M*.J....."4*....j..H..R^".m..5....&.j..B..`>..X.....]z[&.>.ef.gB.d...s~=-...3....m..(E~^..[.....E3..7.4.....).H_..D..j)..q\.....7..#..ag.o .?......C .#.../v.H.....o~{G.....H. ..;v...G.....p1d2..&.....QS4<..i".X.....1(.GR.R#).!E<...LLM.....s.: ".....Fa..b.....T..~OD.....~j~..p=Y...Y.....?..Y.A.....0I6_p.dKctjvZ.....V..1).....7:~..({[...7.....u..ra.....S.].....7.#.[.<..l.....[.....90d[.2a.R.....E.CJ..C..S..*^_..\$^...Q...>hx.k7.jN:W.X.N..p..K..".....q.....a.Uy.....[d..vmkk/cW>.K.C.C.?d..!@_~?&.....V..?F..;k.....%+.....+3bk.....f.T...S.(2=...?gQ...K...#.....?..1W.....m2.....Z.....-:..?..#J...>.KS.P &[<.....Dd.....W\$Z].k..-..8...>..Q.Yz.jw&.....?)..[T...wy...O8.Om.....l.....\.....]"f.....q.o.V>-s~.....N{.n.....w..O .D...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000Q.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11886
Entropy (8bit):	7.946442244439929
Encrypted:	false

SSDEEP:	192:sqNuEpzsnKxkfLaZcDmH+cLApmRausyZwYMAisQKShDBlhr34ckckcZ:JNu6DMLaZsMhtLAia0wYMAvI5V4DDQ
MD5:	875CFB3B5C3619253223731E8C9879E5
SHA1:	6372F4F5BEB6EEAE3EDBE5B62EE73039B40AD01E
SHA-256:	CC69BAE5D2C8F56B28BA4E3C6A11F57C4E8CCCE69943ACFBE7E63B4FC90EE5F2
SHA-512:	47F45A3275B8454F8000F4567153DD7D4AF3012005D8E34CB18AED6AD69083BEC753E607F275FBF3EFCCEB7BA00310A04ADFBD5FA5B73E6BBE47CE73901C35CA8
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..x.U..l...JB...H...".(U.EE___v]W...b....Az...{G.j..B.\$...H.IHB.o2xE...3gf..w..2....w..sC.\$@...\$...t.l.....8.....RR....<...6..P]...\$@...\$@...PO...\$@...\$...T.GZ!.. ..)c..H.....H+\$@...\$@=e.....S1.i..H..... ..C.z*..#.....1@...\$@..b.PO.p....2.H..H@.....B.\$@..S.....!@=..VH..H.z... ..1...b8.....PO...\$@...\$...T.GZ!.. ..)c..H.....H+\$@...\$@=e.....S1.i..H..... ..C.'++kH.G.=Z!..U...73o^..IH..O jrj.D.....I.M.....Kph.....R.x.....RU8 .."-.....j.....B"O.z .9..".L.....Y.d.Rej.-Y.dhX.....xH.z. (>&..4.....O.<..T\%a..e..."..UnR.....+j...2..."..M.O>z.....T...j.....m...S`..&...)....f..2.....+..SP..?..a...=.....3.....K.zj.5 .fP.....2?...?.....%....d.qxC..W...~...!..W..6....iJ)*(..wg..}..}sw\..rj...r"...e _.....5_9.YN'...PO-.d:~%..wZQ...H...JMJ.6c.... g*...3.....T...o..Nyc.W....A.3..._...U%...PG.z....&.%..v....Alm.....~..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000R.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 171 x 50, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2270
Entropy (8bit):	7.845368393313232
Encrypted:	false
SSDEEP:	48:3Cxnazs22lovji2Ez2iqBU2C+hJWizJNzlu1coqAYCiBeMsk1:3dm2Ez2iUhBzhhyjAxqQ
MD5:	6EFE6733E10E011FFDD6711B5F37C9E2
SHA1:	C72549E824EAD89944A38C46FBC28BDCDAAD611
SHA-256:	92B5056DAA03DF3EA85AF49FFE4F9CFE8699BDF3539576A99F02418FF49AD9CB
SHA-512:	EC14B553A5780CD9B33D438CE13A6932DE43E346D8D2DEC8D093A6A2048675423948F8E2C604A73460980C3C68D9276B65D76C2A6BC7B24FDF10CA92FDA258E
Malicious:	false
Preview:	.PNG.....IHDR.....2.....sRGB.....gAMA.....a.....pHYs.....o.d....sIDATx^.\kL.W...*.F.....@...*(H4."iI)..B!..iD...f....y..l.h.....<..1.....C..(XSy.l.....-.....3..3...;{...{g... ..Q..x..T/q...F.V...B...'.?{;.....+.0s.e...w...{` ..5...d..9S]../.....\$Y.>..l...i..8.....;r8r!Ee"...!*&E.....n...=..@..Sp.GF..c*....1QH3...?..T.el.....t?...([Q'.0...k.G.....X..C...k p...l.q;..d..N....c.u.a.5.%..k.fS)..H..T..~!*k.[n...x2.1.....%...yK..a..l.[?#..iD%FMT..=r.jt^..fT...c.&..Lr.....\..V.lI...Br^6..U27...O..N'..K.gm.K..g...l..Fe...w?..Q ..E.....0.....7...(.e..t...x.c6..Q..n.92:%....l..4.h]Z.....w... ..p..~..B.y..&.....gl...wl.....G.6.K.\$...%-h]8.LT.....){a...^i.....4.0.ji.....n.pk7t...U9..b...l.....#...<q..(=F..... ..0@^.....+.....X..>p...S..t].f.x.0....7d..n...!... ..M.qqn...G.t8'=..V.PK....K...X.z.#..l.....@...Y....BH..l.....K....='&Z.41\$.a'o.....i{o

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000S.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	16003
Entropy (8bit):	7.959532793770661
Encrypted:	false
SSDEEP:	384:1l+zN+iNurNE/tBdEC/vkape2XHYdhOm+Bl6C4:L+zN+iNurGNEC3fpe2X8Pa+
MD5:	3A5CD52E925A7C4A345047D8F06C3C41
SHA1:	9C02828D83206BBD3EB58930C8C65A6CA5DBC40
SHA-256:	477277E8CAAEE1D3B3EAB5B3660239AEEABC433743A191727B1A71E529872AC7
SHA-512:	8D8B6AC645ECC7C8BD374E6190819006C71AC0B5993419C42463009116214E5EC4B4235D94B4AE4CDA132E7DDA9807ADC51525824AC5F12696517FFC8890891
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..[.....+)..H..C.K... ..x)x).rU..T..*E...;...*..@Z.....@...9q.g27[fgggg.....1//.."/@...0..#..t..f.C.. .."@.....@OIR.#P...0...\$..y.PI"@.....(..@zJ]...." ..Si8R*D.....S..D.....i...J.R!D....R..D..HC..T.....D.....D@.....p.T..... ..=..#..B....=>@.....4).."@.....).".@...4.HO..H..." ..@HO...."@..!@z*.GJ.....*@zJ]...." ..Si8R*D.....S..D.....i...J.R!D....R..D..HC..T.....D.....D@.....y.?..`..T....f.P...\$47.....~E...!D.X.....}. ..0..N.a...>[]...t.T.w *.. ..)...". ..=X?c.....+OE....<-84...=....w.8....7.Ro&.D@!...GS....s.....Gg..8..T...u...~.....<...S...../Y.....W.....#..vB...u...+999YYY.....wf..._[6....=..]>Y?..;=02eb.....2 ..%;%...\.P..R5....XMO.....6....W]...3g.5;:n{t.....F7S...r...[n.....AAX..j[j.;neef).2.....{ ..r..{7.-.....i..S.....<..pm.u.V....M.333....K..Mr.s..Ek..=t_#..P...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000T.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 454 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13241
Entropy (8bit):	7.931391290415517
Encrypted:	false
SSDEEP:	384:a99pmP85w/MAMszG+iHGgrw8Ld+9aEsjQR:mgP85AMs6+UtrX+9mj QR
MD5:	01367FEEE0A83E8765E971E0D3740900
SHA1:	CAE1FD22CE2539FA2ACC0242C615CB7EA3F866E1

SHA-256:	18B8E53505DA3C412890F4D74AE2A6B26C4B0827E15E830F92A024D292AF20ED
SHA-512:	8CFBDC01C42AE6417038B80424D2E9FBDD7DFDDF579E349C3C17C9B52AF33A72463154D29539457C4ADAB2DB00CC28A67902FA8D9209E4AF00EDD46D52E CA
Malicious:	false
Preview:	.PNG.....IHDR.....s>.Q....sRGB.....gAMA.....a.....pHYs.....o.d..3NIDATx^...U...Y.]:T...G.5..IX...B..Xb4F,I0X.....F...("vET4H.....*EX.....wo9..9. ...rw...;...o..... z....B.....v.mn.>.....E."...U...4s!..F...u?..@...!..~F@....p..Q.kP.#!...(U{@...!...T.TGB@...Q.....B.5.D..A.....~*.U{.].....S.e..K.A.....7^?....D...h;...!Eu...o.^..B@...# J ...B@....(5{...B@...= ...p..Q.kP.#!...(U{@...!...T.TGB@...Q.....B.5.D..A.....T..!...k..R].R...!..D...B@.....:..B@...R.....! Ju.Ju\$.....j...! \C@....H...! J...B@....(5{.. ...B@...= ...p..Q.kP.#!...(U{@...!...T.TGB@...Q.....B.5.D..A.....T..!...k.D.RK.K.m.V.....(^^^ZV^Z.7 a.....T..xsqYi....L.....z....)?..yyy.M\b..U3W.0{~..`).M%. J*.w.mdv.&*...R..o/^..5...x.g.>..ag...GM t...<s..y+6.X.? ..R...-W.m\o..0g.i...h..W.Z.i...2....o.&..@...-B .K.^.....u.}.M..6.../(...e.V.X.....nkE....5.8....-!.T!Rxs....Q.2).- ..`.....mX6i.w...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000U.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 164 x 89, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4190
Entropy (8bit):	7.94161730428269
Encrypted:	false
SSDEEP:	96:GHfueo3dRLZKOSYDzGsEgfB9nqS0Wkt/z2jOrrz7yrT7N:8A6AzZfBtqS0WKNC2vyx
MD5:	8B3AEC1986A522951942BA72B85CCAA0
SHA1:	7E0DC78FC65EE4C804A4B0C72AA53E2DFDF26C14
SHA-256:	8B02CEC726DECFO33B67689F369FDE1002ACFD5F8C32E0F248AC575997204F2F
SHA-512:	8EE1A1F6F0023EB4F60760C2E23EAFD56E6D298CAB49D819CF1D62C0CCF608D4211D3767856255F7CF8FF45AD835FE5475EB92C608989C522CD48D00A050B18
Malicious:	false
Preview:	.PNG.....IHDR.....Y.....?.....sRGB.....gAMA.....a.....pHYs.....o.d...IDATx^]jp...fu.VBBZ..V'.>.....CR.....?r...pU\...v*...T~.U)0..(".....",a..Y..\$!...D...MkvI4.Vh W/S.....{...zZw...i.....fj...\$.7.....[Z*.[[.Zk...?..tM...`^..X...sUK[.Rg.=\$.!3<....74...iY..i...k...fA.Z.n...`G.%.H.I7..7J...u.R..6....E..!...N@....M...Q`...U2.w.WP[!fX.....c @7Mz.....^..k...)....v.Q`..z..1A..P..{...}...vY.....>..`K...m.?CX./v.8....j...;...6.kw.....N....z.Q...f.q..xk.5....;?Z.c...`.....4....?.....VV.u~...<.....sU4e.....g.c.G....O/..r...`G).. ..#d5.O..w..{...twL1l)#&hF..K...M@.Dl..V2..j.3...s....3M....v..l...V..c..B... .e.1....7.WA0.{\u..)\$7f.+.....8..e2K/%.li..`w6w.E.[?_??.?..l.k2.s...}.f...HM.?w..d.9..Rr...Y.c.). s.zk..rc...a..l 9~.....m..Z.....l.....7.K::Bf.....m..1.....&.....?a..c..@..@.g%...s.#.....c6...g.lZ....}.WX.3.8....W....N.w...L...}?..?.....;cl.....pS

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000V.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 162 x 89, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4081
Entropy (8bit):	7.943373267196131
Encrypted:	false
SSDEEP:	96:KQJAeRumk2zXWySIEmWL9zi6wknB4qLx+ppNhQrW8Oy:Ke9S482LE6wQB6pNeqi
MD5:	29B87BEECD5D3899824AA390530CD47FB
SHA1:	55108E8E5692E4444F72EE5CEB91915E7A2AEFC8
SHA-256:	F00E4F1C9B1D9ABEAAEC8E5CAB02A07FD74F00ACE15E36C6F6469DE5AB07A9FC
SHA-512:	1A5AD45BBA8C29C32CDD3C4D1E460C30ECA305D851FAAC73DF165306BC338337525680B9906D367A0CD3852B9D2DAAA8FD0603276BA969495B4E29C7EC8A3 30
Malicious:	false
Preview:	.PNG.....IHDR.....Y.....2.h.....sRGB.....gAMA.....a.....pHYs.....o.d...IDATx^}.LTW.f..O.a.....*.....k..M.Z.n.q.h...ht.f.M.n.6..t.h.k.h5.6j[[[...X..p...?.g.`..7.o.of....^..ys.. {[...s.UMMM.(l.@.l.R?.....(0+0.....5...*F..#.].....1.....B>[.a..L.....x...0.5t.v..S.h!.....Y....B..&.....f#w5u.....0...x.sC....a.4j5V..Z.n....K..>..3t.wm...3hB. BD.P..FkcJ6....G.....6..P.]mf.+o..w..<.....Y..Z.whd....`zf+...#?"?.....qf+?.??"k...zgME..j..l.k.U*.....&z..N....ma.....R.{r0.S.KP..fU...g~..=.Q.n.*.* 8 T=/9,*KDW....GN;0(P3.....1.....':...; .L.a.&<^l.d.....o...Y... {E.F..}.e.\.=W..#.W...c/~..b.EWXI.#."&.....X...b....+2...5..6+)we~ja:lZ.d.Ey...l.2.5r.....l.l_ .A....j2 .5.o....WOM....V.....GC9..'.....C...,_cS....b.1....t....._.....a.3..K.>V.fj ~...K...-.....#.o.Y.P.....a.7..#..'.s..T....b..].3..dPPP..Y.i...c.b

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000010.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 452 x 277, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	22634
Entropy (8bit):	7.974332204835705
Encrypted:	false
SSDEEP:	384:5ojjiyI45m1/9gyghgFsH1ud103Pi39o0qjfsH37mNHy7QPaNbZy0:+r45m1/BWKy10tN22rmNHycobE0
MD5:	548D234C9AB4021CA5FAB7BF22502465
SHA1:	2F7495D250DC86EA99473CC342D164B859926021
SHA-256:	7D549C3418DC90F42571D00936B23D242837CE2A8B19FC4C719E182ECB2624C6
SHA-512:	261523F5EAE6FCE2829B53AAC5938B1A0021C119E00CE82EFFDBD690FE71064E0F3B313ED1AB2F67A16C488AD5B1A91F5AF98029D88A7896F271C108410D42C 5
Malicious:	false

Preview:	.PNG.....IHDR....._.....sRGB.....gAMA.....a.....pHYs.....o.d..W.IDATx^..i=YY6z@_..DP.i.lAA.....l.Dd0"p0.ON.~....s>.?zbH8.%\$`....b7..=...25*.".L. ..u_.f...j.... ...Uk.^UWj]...u..}{.}t-.(...J.....e...t.....@i.k....._(.....@Z.6J.....2.O-P....._u.=T..4p...e..q..5^f~.....@i'.....?.....@i..k.....?...u..Oj bN.~?MbT%...@..LO.Or.`....\$.y.{..o....~..(..... ...SNI...6...w....~.{.^w.....~.S...g?./ .O.....7_...Oj.....40.....9...?.<.3nw...x...g...7....(<.d...{3.K...;..\...:'5....&...>...t;...8..SO;./.....}{.D.jt.....jc...s.....Z... 0q...@...ZjS(.o....Og.u.l.i.-9..j)..~...5.l).....G.....k...Z...c.?..\...t+u...15p....[.....2...;.....w.....v.7...l-w...K/J..[.N.....W.U#.....j(.../z .kv....]j ./m....t.9;- 0...4p...@K.....~.9.\$qu.E.....l.9j.m.+').x..vak-]../...G'...4.>B6\$.....-o.q..L;*..N+....>...=!.Y..Q...?.....7...;....}
----------	---

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000011.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	17289
Entropy (8bit):	7.962998633267186
Encrypted:	false
SSDEEP:	384:ruwwXKZuqnOnZprU3+OXBruY4UkcY+Tpl/BSqCrEoMXMEr3KbzHIDqqAmk+xob:tGcxE4PBruV3Uy5SqCAoMXzrQHoqAk+m
MD5:	708E8EB906BC105CCA0535AE669AA651
SHA1:	38D82DEDFE97D3001188C2E18FE13BD741FD520F
SHA-256:	1C3D07765294566E17270D0F3B9257A3DB7905D4E7EF746AEE80CD591CE0308F
SHA-512:	1EFC74C28190DEE2D2732390B74049A1B120F05EFB8DC6925207C6990AD20450FFAB40249899A9DBB82E8F92A61F770E120A450CAAC7F8C5F0742586CCE0EDE6
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d..C.IDATx^...Uc.._oB.Hr.m(.0.....r..[1.D....R..q)%FBDiB..w*.k.Jz.Y..l....>...9{.....g..Y.z~..k?.z.^k.. +V...!(.....sMtD@...!P...HW.S...u^.....@.r.^.....B@...U.H.J..... }....".....>...! ..A@.4..EE...!)* ...B@...i<8...B@.T2xp..! ..d@...!.....(*B@....S....B ...O..QT.....! . .@<.H.....! ..O%.B@...x..9...C' ..{>Z../^s<<V4..ujo..v.Z7..EwT.....@.....?.....~{...K.....C.....bB@\$.....C.{...KfS.....T.*&....@<.....'.D'...;~v.DT]...r!...>...ru...}.....#u G.T.....>.z ...3v...P.M.....5.@<...? ...F..j..c.W[..._IP...O->.M.d<.J.....E .jZZ+.5v.p>..N.{B....>M.Nzfb...OB@.."}..D.y...ldK<..! }.....f.K..bX.T9...&T.&?..VB9.[B@...@@ .4..1}.4.@H...l..j..M.<z..l}.G.....>S...N...@vj...n..s.d_.....{.R".....WfLoO.^...h\..')...ni.'.vk.1-k.^....#.j..{.RM...~Z.S. _@Ul.&}.....h...{K...@.....W.8.N.s.Y.0)..f+...%4.... ..5.@j).k.+3...l..{

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000012.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 452 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13737
Entropy (8bit):	7.916899917415529
Encrypted:	false
SSDEEP:	384:jgxmX2Fa+/76A6M6Y7rSYRv47cwbkkapeliRmDGd+gUwOSpQ:KgyoWrJWRkkRXmad+gE8Q
MD5:	830632032C7DDBCCDE126F4BAE935540
SHA1:	9FEF1DA9FF1D7762B779553B5F873BE54C8D01EF
SHA-256:	2328D09EC845433DC31808FD6B12616F1D28B9B3BA7DD969ADEB6C32D8EB049A
SHA-512:	5C17EF9A0063499F2C34FAB2C4D968D29E20F20868921FA914E5737995AA0C166F224995109FF7ACA57B5B0F8647715DC670C4AEE385F61B5F8E6E8422C49EA8
Malicious:	false
Preview:	.PNG.....IHDR.....w.pl....sRGB.....gAMA.....a.....pHYs.....o.d..5>IDATx^...E....,"o.....&....AY\$....AE..".l....+G.>AP@D..e..".A.Y.@...K..IXB !..l..c1.On...== =3=.3=>9O..u...w.z.-.l9jB@...!.....Z...B@...^G`.Q.&S..u\$d...B.Y..P.w5j].....B.m.D...! ..@...Ls.Q"....."S...B ..D.9.(B@.....b@...!..".@..!T1i.J...B@d... B@...4.%B...! 2U...! .r@d...!.....*.....9 2..D..B@...L..B@.....D..! .D...! ..@...Ls.Q"....."S...B ..D.9.(B@.....b@...!..".@..!T1i.J...B@d...B@...4.%B...! 2U...! r.@<d...!.....*.....9 2..D...B@.....5jT.@.{.O.;k...>..._o+.....{V...&C..(?m...F...gd.....?....3u.x^L1n^..@../...XE...L..l..t...L.B.)=.sn..U.....@.O.\$..o..L...g.(D... (...Lo8.....fjo..i.f.h.9.....\../[W.9.....+...X..+d.....Xc..7.p.m.Yg.u:YO.V..l.t].Z.g.U...][...5^..._~WL...o.3f..s..Y.X.7.x5..K/-_.....{.....W.(Y....?...!...W;....iwNMW....@+Q.5.#.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000013.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 185 x 76, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2332
Entropy (8bit):	7.8822150338370776
Encrypted:	false
SSDEEP:	48;jB5Gg4vMs30Wln5iVeRy1bY7Dq bqBAeNjukXIN4AXat:PGYuEWW/YH7e1uA0AXat
MD5:	91CB7F1273AA003076401081B8A22237
SHA1:	5157144069E7D2FDAE60B397BE5851E75BDF7707
SHA-256:	80682DD6472E8D1136BC5E20F6DE87B595562414B19EAB8E965736FE992921B0
SHA-512:	5A8E3CED0DB94BFE359C63793F12F3D7B3C37F3A13A5C96634BA1DC8C9E50FB1142FE4752FD9FBFA39A682F78C54AF868AD337EAA787801FE5F66D8F55A816
Malicious:	false

Preview:	.PNG.....IHDR.....L.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..LUe.....Ji("....9....-".5L.Y.Y....\$350.."2.IK3Cg...T.DWZ.....i?!<..~x.z.....w.sw..9....s...w..l6.....p"dH...F..B<...qE,R\$G\!..E..").#.....{f.Pyl.d.l....;=S...O.S[.Y^P.aj]9^Y! ..~.##...S.s...l.h.[m....%...P..@.kG.....G..X.r[%..AO.]-..G>35..c....Ac.&[W.d.+ ..zG.....=..l...VS.d.+..tGd..k-...oL..}.p~.W\$C..j...l...n...~.....;l....e.=..?{.....>r~.Lw.+2..w.)w~..c...h..u..%...PE...f..'.m.ZE.1\....U..X....\$.P%..UH{[K..o7~.k.4 9..W.t~.^_..7.....f."q....+.....;~;c.....Xb.\?.....0h.IV..WX!..l]m.t.c..U...[.X.).....B=.0~..W...rO..j...ehI5U::66V5sJ....V...jY>...1kQH..2.....d...S...l...+..].p....m7...Z.. ..s.D>.K[.?.l....2..=..~.mq..".+.....;8. v.o.)Z.....>..Xv..i...TA...M....>[X...Y.7lJ..e7..S.....02q.O&9.....:L...N.....W...d..FqE..T..N.....R...kXv[.j.....g.K.\@'.M..B]8n
----------	---

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000014.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11332
Entropy (8bit):	7.9324721568775285
Encrypted:	false
SSDEEP:	192:vpXZavBpl00n1Pt7JquG9GYHDK/5cxektxMQjcie9ZZkx30eXJlb8FKRN:vpZaDyc1P1Je9G62/5clpjre9nQkeXJY
MD5:	31579CA3352DF8FA4E3E7F48C7CDF672
SHA1:	AA682A3C781BF8EE43B5EDC9718E64CB79135F25
SHA-256:	B0E7824BEE2C896279457D87E61E902431BEB528D830524CC4DFAE126E89FC24
SHA-512:	782FF9492E3ECB11C72D316DD94D1F3E94CD908FC9452A37DA6CA30ABCFE9AB2BCCED8583A569DA68626BCEC730408AF86997E295637BF64AFF5BC768F3E309
Malicious:	false
Preview:	.PNG.....IHDR.....R.....sRGB.....gAMA.....a.....pHYs.....o.d...+IDATx^.{...u/-...&....6..+z..Q."b*. &M.d-e.*.J.Z-T.Z\$....R.F...%*"bn.<.....W.E ..w...^...;g.. [w.5w.9g...3.....t8t.P.?\$@.\$@.5....=8qb.....5..a=...#y...@B....am.\$@.\$'.G.B.\$@..S...C.zj.#[!.. ..).....!@=.....}..H.....VH..H.z.>@.\$@.v.PO.p d+\$@.\$@=e.v8.....f.o_o{...~t...n.S.N.?..._L;j.H,7..j]...7...b...[.....ObVa1. ?X.....~.....t2..V>b..}.0.F....%'GO7.n#~..F....K~...FX..H.^.....k _Z/2v.W..M.<.;\$.~v.t.,UO~.}.....D.....o.J..Y.....5.%!.....[.....'O..dC\$...=uks.;{x.N.=...".Q}.w>.E.H.....AV=..f.& ..lpj}_0..~[pf.`.9..v.W...2.E.\$P.....+...OcC.H.=...]. [-g%(h.....W...?...UDh..T\$..?...[.j..)?[Wo.h'.2P.1.....\$..NO.5..j...c...~..x.j Q...B..6.@>..y..}...m...D~z...L#0'_..s?}[...l.....a...=N...c..._2..._6 ..j]...5....{.^>.lM...;n...k..9J.. S.G..{.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000015.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 167 x 92, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4181
Entropy (8bit):	7.943341403425058
Encrypted:	false
SSDEEP:	96:b6JWqvCl45Da8kuGzhRwZvwlutfij19MQ8EpW14LBGJVCq:b6JTCI45DalsBws1R8914V5q
MD5:	817D5A35EDB2B0E052194D4F49FDA19C
SHA1:	FA6CB2016C5F43B76102B63D60359139227E07EA
SHA-256:	0A87B8418B7F8E6E117BADDA11D7CDD38B8B7320C6BA3D3E9AF93EB9ACB2CE14
SHA-512:	E0686BDBFC589401F0EAAE2B1598199EFA285F8392742B1C928B9274088804B23DCB584B6FEF68CE6D7E54DFF9C10338104F4C0F3F80A04471F0B2E8F9935CC6
Malicious:	false
Preview:	.PNG.....IHDR.....l2a.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.]jIPTW..iv..D.....%DQ#A\$...d..h.,T~..+...TM\cj*).k.fj~L~\$..L&.....:FdU..f....._n.m.....q. s.9.=..w.9.....\$.b.*.%.....@AJA..%<.....l.h.+./..OSe.....]...>.C.....^cCy.0nz.4<.....g..?~>.1ws.B...07W65.74T...=..v.....D....6.....tR....}}]...4z..^.....7.;..".....^..... =.#.=.32..o.<Tn"Q...g.zN..n'..n'...../.....!F..]...6...m...CX..~...+..U...E..[.....7]=E?!(.(\$'e.%'.....w..._Y...l.1...@....t.P..=}.*...N...N..j.x.S5&.....Pe.....Z.Z^XjKx.....^.....?7.....WsZ.... .jG..j..^.....[y....]J....'.R?a...G5..l.i.?...MH..l.DC^_c.m....%{z.&.*+x;...S.....zxyH..^_..}...e!^.....U.T..^..p..z[6(2x...;#;o##..j)Zv[Z.....V.....0}Z.....].m.....x..)k]&e..._W !Vry..%..l..d..}w.....^.....m[.^3r.....-8.....j...>...Q..T..{V\ptH.?.....1..w...FHI...X.....\`ei.w..)}'..g..V{..Z.....8.....o..._..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000016.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 221 x 77, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2599
Entropy (8bit):	7.903700862190034
Encrypted:	false
SSDEEP:	48:PmCwDjh8w9JewaF2zQNXxj8zq1KM43sxXyjYbTgJW1MFsrJ075CawGjGj:P1Ah8UewaFcgz82Kx8xXNYb3id/yj
MD5:	E88131C9AAC52649FF044905ACAB9B76
SHA1:	34AE73B9165CBED0DDF33AC20E4B3E7D622C19BF
SHA-256:	30F22340F582F9A352A7ED3048D1088F178E83CCAACAC1CCFD86852C8F9C78E3
SHA-512:	97AFE8F3A2A3138613934AC737C390A35F6757BFC3D381EA7C7CD148F739932380DCD46D0BA6F590C274F8BFB4248286B3C0433AA69E090102A8A9ABDD7C97E11
Malicious:	false
Preview:	.PNG.....IHDR.....M.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.]kl.U...BjE..>...*.Q.....b[K.....m.(.....!%1%*-B.C~(&['.....~..w3..Kw.3wvfzn.2 {..s....{w..^...l.3...l.../..zD.x...O.K... ^1*...8.G...z...D.\$.....>!.V..^v.CQQQ!..-L...../3.2.....ZH.?s...lu\N...3.?p.N.....<...E.<=z..lu<l.dX...g....+{X.p.....t..a...cKK[.j..Yszl.N.....KPs.))T.5....&B..*.5j`@...(_r.V.j..m...?x.sg...f\ldz.^'=..h..<.y....l..w..ze.m..l.qPJuu..D..j..@....W..t.+...X.....e..H+.Ns%r.VS.N.3:~&.....#^..d! ..F... ..xc..M...q...17.z...z&C..K9(.lfm.35.v.>.'X,...p.=H...J.K,...~...7.t...R..R..9.?....l..l/..(..0z0.M.f.)H..Y.."e.....B.....L...q.K.....j;..L.....xl.K3.M.%...../..){...R...s...7... ..).q.._R.4O.a3.....<...%...3# .>..y...u..R'.P..\$Klz.....g.g....`7..l..x>.[p]>+.....e...~.Re@.N..FY_..._*....]...[.h.M.oq.S.U...c_`j].....8TP....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000017.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 232 x 50, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1570
Entropy (8bit):	7.780157858994452
Encrypted:	false
SSDEEP:	48:r+em8Tlk2APr2fEd72tTqiVJlclZqeVzYwS:r+erTlk5S+zoyGahS
MD5:	EF9AA5B2ADBE5DF68AC4F4D716DF7708
SHA1:	363B93AAAB9DB2832F6CA0EE3C27C9310C344BA8
SHA-256:	3D94FCC4821A135ABAAE6579011441B94F9C04DAD1E66BB5211B0C019A5968B9
SHA-512:	EC9B024AEA46F7B97D14F0A7E12704D09B85F0017CC9E273CE50F2F889DFDAE81DE549CCD546BBB8F8BAAAAAB7781FEF77BF783E02CCC9605304552F7DD5903D
Malicious:	false
Preview:	.PNG.....IHDR.....2.....n.f....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^[MK.W...t!.fU...b!...*JBA.....%-.F.4\$.Nw]....E.\$...)T.....?@.O{...3w..y.=/"o.9...<y...X....c .1P6..e.lx...0..J....e3.&.@).....o.*>.E;.....~. .Z.3'K..W0S.&L_.M.e.`.M.....i.....\..6g.^....4..L.Y.9.\$M...4..L.Y.9.\$M...4..L.Y.9.\$M...4..2.....q...&.. .....*.Qg.+p.....a.:X6...o2.....A.....()...p.....P.....>.....3.....z8j.....>...fww.6...../....S<.....^%4.....{N\$.`!H....`.....a.(.G^>~ bxx...K\mF...d.d:9J!.....j..i24.A...` O.....s....?={...H'...~.O.....*>...ZXX.3;...C...\.x...%.s=<w<h.....0...~.y.....+n.P.M]c...A..Er .R...\$.g...9*...jg.....x...&+jWM4xe.^....0...11.[....f....r#.h.h\$.....[=t >...r.. ..L.O.KL..B\..x.....4J.O....vY...dA. w.....g....};.....x.).....x...s....N.\$..n.g<Z.q.a9.C.....oX...%KNNN..i.8J..p].1....B>{.....n.D 3t.-lg...Q

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000018.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 340 x 79, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4490
Entropy (8bit):	7.928016176674318
Encrypted:	false
SSDEEP:	96:WXKr7Xwf6Obg+XaGOnsjbbGSb+ydWtRvEOhDE6XqPeosv02tR45boo:3rTugXZnsHKSb+n+8DdKlwmm
MD5:	7F161B19B937AB48D4FD2F6E5E16FDBD
SHA1:	BDCE4F1C73E87E609A7FDF245A512CA4F73B35B9
SHA-256:	C863C5E71D1116D69561BD0637F4FE4C4240E9CED05B8A5B056073AD13E6495D
SHA-512:	E915B76FAAC9512D2AD11CF4E4530A19BEA1C7D8508BC218C69CB041F1EEABA3E2E03B1D56E61B032A6418829752C21B8354AF1335466D7E1528A06E6742A461
Malicious:	false
Preview:	.PNG.....IHDR...T...O.....;.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..p.U.'...rD.WX.... Q.."\$.ZHP.Z...C.....R..%G8R......R.C6..A.b...0...^...#..g.....z2.....nB...l.X.&_a,...a,...a,...a,..._73'N..ukeee.6mZ.n.m.G.)...n...a.9s.DGG...y...8???.o.pE1....Y.,.....).ca.i.M.:5\$\$.....Lr...ye.....6...8...z.-r....d.{xc.U..^11...._ >.QX..y..2...T...sss1..."A.?_..w..S.F>.....4.G.....D. ...@.K.....C...K...p...q...6: QQEE.....7;;;_q.k ...z..6>..n...Y.&G*.n.S\$)).....r.....){[Dv;..w.A...`..... ...a.~.N.f.s...P...*.7n....eK...+n;..W..C..9)..O..D.q.X..5i.s~en.c..F&?...l.]3r...W'..#..7o..R.@^..*...W..?)t...{B.8..D...UPa..~.C... .C .a.9..R...c.Y0..9.u...d...C.....X.U.... WK.....5...'.PM.`...<.._z.F^^.EH.K>_0.d..S...Y <..5.?l.fZ0.@d....*.G...K....e..b e..Q.4....('z...!G.....2..XQx\.....X..2.lh..X~.e....Z....=...C.1.....w.....d.z.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000019.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11449
Entropy (8bit):	7.91552812501629
Encrypted:	false
SSDEEP:	192:/zgGDSJ0ke0kBER0C31jm1OSZi6/ccccccc3zzRmKHDr1NFnAaLJ5rBX8iaD7:/UGe6m7XdJS86kvRBHD5/nAa95rB9aD7
MD5:	163E6791C87E4999C343EC5E23843B15
SHA1:	43CE3BAE19E22876483A7FD0E93DB45790373600
SHA-256:	DEB2B126977EA150E49CDB3ACF4F5387639C7B7B5583454EDF55ADF83DFAB720
SHA-512:	98BE1F4684F99A9FD2F313B09A113B5C310EC8BA8EB0EBF5FD69765E5B48B001D39999E3F25A7E76C7344DCF57B4F0BF2E4614FB0E0DFCCB6F02E6D1CAAF7FDD
Malicious:	false
Preview:	.PNG.....IHDR.....R.....sRGB.....gAMA.....a.....pHYs.....o.d....NIDATx^...E...@^T...H..\$..(.l.3....O=Q...<.9.`@E...CE.(''..H.\$..6.....j3.....tW)U...w*~...W/.m..H..H.....'..G...W.=#.M.\$@.\$p.....!@=U.VH..H.z.g..H.....H+\$@.\$@=3@.\$@j.PO.p..... .5..j8.....PO.....O....+Z.Pb.FH.....D.g\....._.0..9>.....&..PO.z..)-.....R... '@=U..l.&.g...../....SO\.,_@7Q.g.jV+./..Ht.l.=.WZ%{.....v.....%U.)^H(!.l.q... .H.E.DG...o.../...T.i...z.%4K..# %%- (...4J'i...P.. ..F.D.zj..#..@.)...(o.....S...).i.z.g...h..8.....A<d.z...<...n.]...E... (Jj4P;_N..Q...).8U.u.e).j.e...E j]".t6.[.K..5.6....B..(.=W/...S'.....z.FY.. ..PO."tl...F...Q...c.o.....)....r>.. 3c9l./.....).l.G.~.be.5.OGb.o.....w...i.e...5&..Z.H.....g..KY.<nZ.x...HHbdS.Z\O..1Q.K...9....Z.L...\g#..._~9###%O.>.Rvu..C.....S..g01..j...?-./.Q.N:.....1!

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001C.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE

File Type:	PNG image data, 165 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	3679
Entropy (8bit):	7.931319059366604
Encrypted:	false
SSDEEP:	96:tT+LtoQ9jsUBsnwIDGThUe8ww2iJiGEjdKKnE+Gh:V+Ltt5GwIDQhUe8ww2iJi7MKnnE+K
MD5:	995CEACAD563F849C4142B6A6F29F081
SHA1:	44CB3B867CD2917541B7D5AAED2F14F10FEBB0FD
SHA-256:	3691FB8C60EA1B827092F05FBB1807E34726016C6FF56698D7B81C44D519D22A
SHA-512:	3C8EFEB966B075D06D8344483352BF92C9292F9970C9377BE254EB355EFAF017916737AECDC704B84D532B7229F9908951A6F2CC3FAD810791CAB224401AD31
Malicious:	false
Preview:	.PNG.....IHDR.....c.L.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...W...Gh...k.Hm..J.m....X...Eh...%n....PHvy\$%...[...R.l...(/...yl..Z.h..Hl.../ .y w...7d3s.s.=. {s.g.6W.^.).@.{.'O.LL.....c.^6xS&O,...J.(/?.....,\$.....@.zk..., \$.....).7]O...mH7..0.. &j..t..F...T...AZ7z.....\$H...AZ7z.....\$H...AZ7z.....\$H...AZ7z.....\$H...W.6.....0...FTcc.Wl....Q)...<.*.....{...#G...Y.f....KKK...,4.....[S'...+O[.+.\\H...(<..Qy"..ET.PM...c....~(.g..**...ol.K.....Sc8..q.F.KM"<...t.O.>b..\$*t..2..y.h."lf.08hT..m.(..C.7n.....@.....SVUU).F.).X\\....[j.U...\$x\$d..e...<W.....=;0L78t+..Gw.-...C7.....K.w..._g.....A.&M.\$^#.l...e..P.....;vD..@...Za.@*D.f...!..2w...4#J.c....K)....F.u.l.b.V2.k...5..`.....*.....M..l.,;E..BZ....K..[7....5.....K...7+6..o...\\`...z..5x...\\46x.b.....Y....s.^x=.e.4s.W..t..iu.G^.....(74....`.....].&..j+I9..3.. ..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001D.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 127 x 138, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2232
Entropy (8bit):	7.837610270261933
Encrypted:	false
SSDEEP:	48:dFQY2WmQbe+TukEC2KgYPsWOuWfK792oP/sWtGOK9Lc+rD0NTHj:3L+wKkEOgx3PG92EqI9LczFD
MD5:	EDB5ED43CC6038500A54B90BEC493628
SHA1:	A8CD63F3914E4347F4C5552FB922C6C03917F45F
SHA-256:	9F3312E33EB78C6952B5A5D881BBD18751FCFAC41D648C6F053CE781342A504F
SHA-512:	4EBCEFD69A4C249AA3B0F00A954C4E463DA22FC9CA0B61A0DC46079B438138C509B22188D966FFF6599A3A604858BC4CC8FE6E0685A764E8E0477AB7A237DB32
Malicious:	false
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d....MIDATx^..hVU.. .s::6..9g.MM3...j...*.....A..!A....R.Ai%YH..(M..".h.cf*.B.....{w{.....y.s>.{.=.....#y.r.K..K.O).....Y..b..[N.=...j.=.....!...../6...B.8...p....5P)....@.....=).....^~..@..o'n<q....Yw].mg\V*...y.W.T.>...n...s.iG.~L].d.<8..j<<1..4...CZ0...}...oDDh....]3]#"B..O.....0)B.F.L.....5.f.FD..L.....5.7""4'.p.....'kt.....>!k.oDDh....]3]#"B..O.....0)B.F.L.....5.f.FD..l..x.....Z^...>B\$1.N")4.....1:&F8..*.X.yL{..s.3.....~2.EL%w.Uc.zJ...B..S..b.7o)%..7..'.....N .Vi...q..uO,'/....W[.y..&i .l X&T.....-.....Z..o~u..U...cF.M....O4}.....~.....:T.W.._s...t.Dlb.\$Pr././...4.b.....R.T\$t..\$.>hB..+.{..m.m.W..Q..05..C.)...}....?..h.....Y..8.6^t...}.y.%.....l=\$..[~..j..h.N.....*SB..8..H....._G...;6YQ\WO.o.]].'.\$.o.E.y...i9.[cmS..@m@.Q

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001E.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 46 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.814570704154439
Encrypted:	false
SSDEEP:	48:4gv2YZ4gWlP.U9JcJREmXfFEV7NNkfKOgV60g0Z:KZgWlP.SJcj+mPFGNkfnpg
MD5:	3F1535054D4F9626F0EB10CEE47F076E
SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C60
Malicious:	false
Preview:	.PNG.....IHDR.....1.....*[.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATXG.iLTW..._23....6.....kk.5...5..IMh..Tl.....V.v.PZ.-F..."k.pCQ....#.../s>f..3s....<...=^/'~.;a...{>.g....*o.6k..k...E...O....aQ.j...X&vG.....{u-...\$...CX....xhZ...Q...Z.....O...l..ld.h....q..q.....Y..J7O7.R...~o...[.....;h...u.g.>X...o.})...>...._u....5...2]...EodZ.R.i...=ryxh...Cl..6\$!...)..W.^...Q.y...Ay[...M'o...;hh'....}.%..."h.5.?=.y.x..2/gK...4.2P.(#S.F.G.o...!Mk..w/_1'5....[U7.0.Z.w^.&/...G...Y...g...;JF.t...~!'X...uYd.E...+R....2cHG9..YC..X..Eg.).r.+%%t..6/...@...3.... O .0..:l;....._E.J'...).#R"...q....~r-..%.4...b.Q....al..6.....{y...I1.Xs.).y.;u\....sm.C..@..2.AG.K..5..}k...~.....4..<..PH .)Z.[H.G.i.H.7UR.`..B.f.....<5n7.*WR.c....l1.....<y.%...-.."Y@(. *...))(...l...y.z6..J2.s...c...z.G..Kj..^R...M..k>PA.1>s<G...8.r....dL..uF.(...q.P.j@...CPSc..^

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001F.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 749 x 126, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13084
Entropy (8bit):	7.940058639272698

Encrypted:	false
SSDEEP:	384:o4KSpFN6Ud4c3p2Il1yavNr5spYVJzimlfz:WGN6Udv4IKavLBJz/r
MD5:	0693DABBBc411538D209F32E22F622F6
SHA1:	FB7E675406FA123CDB7E058D336742D6A2E8DC8E
SHA-256:	2DFB2E7A13AA43C673D2EE540D3C366CEB12105EB5441F98992FC06F4284013
SHA-512:	F07732660EC62DAE58EB02E29476007EA92BF826F642BCA547097136AEA01D29FF69D9B0CD0F5D65A5E15AA66CA4AA4804AA171A3504AAB198631C643C90C16
Malicious:	false
Preview:	.PNG.....IHDR.....~.....sRGB.....gAMA.....a.....pHYs.....o.d...IDATx^..w....'m.9c.6"...&`.N.(.TN.Ne.N.R.eKr..T.*[...?T...l.D.S>I\$A...l.....y.9...f.....3...Gh.....)_o....n..A@.....A@.....L...2... ..x...#.1fj9.[....A@.....3fE@x.YWN....A@.....1.....Y..J.Y.N....s"...../..rc.scuyyyu...s....toi..j..lv....Gr.#9%%%%9%-...d.T...r...DH...6.....%U..A@..0.....rAD2.5.....L.R.=W...gZ`o..-?.T.Cy:...y.9..y.EE...v.....1..R....1."....."ss.....i..l.hY...Fj]....%-Gw...HJJr8..6...#.....l(.?P.(.....8(u.....*.OOO.....dgg....Q.=..c.y....A`S.@.....3.CC..GFfg..l.l.COJFFFNNV^nn^^z.%(..^b\$......a..y.LMO-.y V+.k..T>Jg..*/-/+.....M=.x.....E....`~..N.Kww.....z...%%.e.%yy.i...P.)`..A.5.d.0.Cc35==66>2::33.>...li.i.gv...DSd...l#...l.....)**,**..V..1..F.7....).SSs..7..F...C.p....(*).....(RG..B...l!2. r1

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001G.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 46 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.814570704154439
Encrypted:	false
SSDEEP:	48:4gv2YZ4gWLPuU9JcJREmXfFEV7NNkfKOGv60g0Z:KZgWLPsJcj+mPFGNkfnpg
MD5:	3F1535054D4F9626F0EB10CEE47F076E
SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB2996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C60
Malicious:	false
Preview:	.PNG.....IHDR.....1.....*[.....sRGB.....gAMA.....a.....pHYs.....o.d...IDATXG.iLTW... .23....6kK.5...5..IMh..Tl.....V.v.PZ.-F..."k.pCQ.....#/s>f..3s....<...=^'/~.;a...{>.g....*o.6k..k...E...O....aQ.j...X&vG.....{u-...\$..CX...xhZ...Q...Z.....O...l..ld.h....q..q.....Y..J7O7.R...~o...[.....;`h...u.g..>X...o.})...>...u.....5...2]... ..EodZ.R.i...=ryxh...Cl..6\$!...)..W.^...Q.y...Ay[...M'o...;hh'....}.%...._..h.5.?=.y.x..2/gK...4.2P.(#S.F.G.o...!Mk..w/_1`5...[U7.0.Z.w^.&/...G...Y...g...;JF.t...~!'X...uYd.E..+R....2cHG9..YC..X..Eg.).r..+%%%.t..6/...@...3....[O].O..l.;....._...E.J"...).#R"...q....~r...-%.4...b..Q....al..6.....{y...l1.Xs.).y.;...u\.....sm.C..@ 2.AG.K..5..}k ..~.....4..<..PH .)Z.[H.G.iH.7UR.`..B.f.....<5n7.*WR.c....l1.....<y.%...-.."Y@.*...))...(..l..y.z6...J2.s...c...z.G..Kj..^R...M..k>.PA.1>.s<.G...8.r....dL..uF.(...q.P.j@...CPSc..^

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001H.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 163 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4847
Entropy (8bit):	7.950192613458318
Encrypted:	false
SSDEEP:	96:JnieMJz5Tz/gKVp93jQvcv16kjOzbpFJJBkjcMNBqmQzOG8qx1QKnse8T:JieMJzph13Evcv16RfapFLxMNB08qxa
MD5:	A1A1017A6A7928761CEB56D1D950E123
SHA1:	28272E9C7F816A1CE8F2033FC00F489005332365
SHA-256:	72F066CD34EA71D0E1B28FB60D663B0372C5254E1A8239C94A164EEF9389DB88
SHA-512:	10F4557F102230126BC86CD4B9C93365C38D5CBEAC51F4691B90D86109886A2BDEFEBAB507731D4FA14367FEE430453BD716157F9074EF643F2B949B09E1530
Malicious:	false
Preview:	.PNG.....IHDR.....n.<.....sRGB.....gAMA.....a.....pHYs.....o.d...IDATx^.]TU..)...E.O.T...L~.....af..Z.....O..4..>Ms..Js.....5.E.d...Y....?z.3..}l..]?~...{.....s.z..Y.....E.X.6...c...u..y..W.j.....}...l.i..l-l.....MKH.E.bi.d...b.X.)...X4 .vJ6-...;+/->Qyi.t...%.T.k;U..y.C\$[;..Gm.....v..*2..2.eee..."l...)yy...lll/..u.....2...M..:"..W...o..t..._6m....'.k.T.v..."s~...O...ed.[W0X..HB.V.l....<=.E^^.....MyY..vpp.....^6....aQQQaaa.....]^^^nkg../_d'.%.....L&k..B.....?C...W.VVVV6660t.J+K...:.%q....e.cp...Kz..%qZsARiT.!.....>55.R.u.W\L....T...K..rE.U.K.-9.....y.y.....K...>...HWTT.e....+..B.....%>%%.....^... .M'.%fl/..=p...{O.../...@...DP..hw8...7o>..A.mgg.....7-]~.s.OE.E. =.....%ly.....MSn.i.....l!U.\$0SZ.P.}[.%X[;{;N.....\.....6O.....!N}.s.m...E..V..f..r...4..~.....H..F.})...4..R.=.....xT..4...../...z

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001I.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 46 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.814570704154439
Encrypted:	false
SSDEEP:	48:4gv2YZ4gWLPuU9JcJREmXfFEV7NNkfKOGv60g0Z:KZgWLPsJcj+mPFGNkfnpg
MD5:	3F1535054D4F9626F0EB10CEE47F076E
SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B

SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C60
Malicious:	false
Preview:	.PNG.....IHDR.....1.....*[".....sRGB.....gAMA.....a.....pHYs.....o.d....IDATXG.iLTW... 23....6kK.5...5..IMh..Tl.....V.v.PZ.-F..."k.pCQ.....#.../s>f..3s...<...=^'/~.;a...>.g....*o.6k..k....E....O....aQ.j...X&vG.....{u-...\$...CX....xhZ...Q...Z.....O...l..ld.h....q..q.....Y..J7O7.R...~o...[.....;h...u.g.>X....o.]]...>.....u.....5..2]...EodZ.R.i....=ryxh...C!..6\$!..).W.^...Q.y...Ay[...M'o....;hh'....}.%..."..h.5.?=.y.x..2/gK...4.2P.(#S.F.G.o...!Mk...w/_1`.5....[U7.0..Z..w^..&/...G...Y...g...JF.t...~'.X...uYd.E..+R....2cHG9..YC.X..Eg.)r..+%%.t..6/...@...3....[O].0.:!.;.....E.J"...)#R"...q....~r...%.4....b..Q....al..6.....{y...l1.Xs).y.;...u.....sm.C..@ 2.AG.K..5..).k ..~.....4..<..PH .).Z.[H.G.i.H.7UR.`.B.f.....<.5n7.*WR.c.....l1.....<y.%....-"Y@(*...)).(....l..y.z6...J2.s...c..z.G..Kj..^R...M..k>.PA.1>.s<.G...8.r.....dL..uF.(...q.P.j@...CPSc..^

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001J.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 123 x 103, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	7.80882577056055
Encrypted:	false
SSDEEP:	24:q3kLWZefR0kKbfLnNhzzt+acvt2x6pBs/j+7QJU0QbDQ883ASaoUV4hNgq1rsyhy:q322nN+X11GDsg8831Uyhi/vf
MD5:	D5F7A65469623327F799B516ACBFFD2F
SHA1:	76C6333C14AF3A7EA091819953E6E12DC289A12C
SHA-256:	F476FAE1C6D79069239C47D182631AB343749C22B1A6990250465C7EC3738FE
SHA-512:	351B9E455E97E6247E64E4BC1B59C9524E70AE0D09D3B6FB96937378A70536483B00426EE69C3590DD415A8265D21FD031B524B90E4E86814EC9AD704E57793E
Malicious:	false
Preview:	.PNG.....IHDR...{g.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..h.U..p.T..(eBR...2.....'.4kec^....0.&.....ugS.8u.i.P.F..f3...D....6.%...xal.)...y..9...s.w.s..{..y.5<<<...{0Q.....t...q/.[@.....-.e...=..J.L.....c.4H.....u?.XF.KJ..zb..0..f)..J..[&..S.6...w..9.....<.....?j....H.....>.....~..).n.8.WW..B?...?..b;.....<.....~...b...m...&1.=.Pq...w...a_3.k7'....d..z.O..w...s..Lh.x....Q;40.i..`8V_...@...rd....kF.@<@...e....=mHB;...E./\h.^...q..>...%v:O....&q....'e..9...h.iG'.L<@.....[.].n.x..c.....O...}).....S*.Q...d....A....4.t....E..v..).7...t.b....*/ .H)...8.. _@.(,".Kt....].+.[LwJ.B i.b.k.@..Js.....J.....6..J..LwS<@..J.YLwV<@G.4w.L..G...].zu.z.h....;..W.IH..+...c...F...ql....Xul...N...vv\M\$.D...+...=....?U...T..^<6../T*.{q.q.....y..XL..l.z.d....G..b..g.G..b.....SM.{q.q\$MUL..R.....^P..g...e....L/yqM../b.f.....J.<

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001K.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 59 x 61, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2210
Entropy (8bit):	7.86853667196985
Encrypted:	false
SSDEEP:	48:naUvGemgl0W5KMDRLEbGAnaHC7ew/fkDSCcE5FTaHWc:aerVIDRlewkXlIrTa2c
MD5:	73E38124F94AD20A2F1571FBBE11AEEC
SHA1:	87FB8056DC7A0A3B70D51426771C4CCE2099CFE5
SHA-256:	A700B63B30CBBE5230CC5E977D651E178EA87E73EAB18C8D5FFB1362149ADDF7
SHA-512:	320FCE64DD6F975384BEC9267348CD5CD24A55B13BB09FEF1238C2216AD8ECABDCCC15601A079CE092ACFA4954829FFEB06FBB0631F6AE26E3A39E43C10208B
Malicious:	false
Preview:	.PNG.....IHDR.....=.....sRGB.....gAMA.....a.....pHYs.....o.d....7IDAThC.yLw...r.r..... ..Eq.nnN..i.[e...-d.M.dn...x.xmQAT.Q.RN9..EA.k.P'..=)..m.&~.....o.y...k...)}x...[...g59.})~i.SY....."....7Ow../.....2...3f)n[...R...R.....U?...O...{...c..p.T.\t...5.07... ..07...7.o...+...V.c...&..%.3l...v...^....6.....??..[N.....nz..Z.B.....v.prs.q1V1 ..='...'bz..%s.cf.3..RyMNUeV..J.k.)D[~xo..d..c...sO.y....B...c.07.....Rp..J.....{b.....;u...s....N.gko.M...;6...6..c.X5.S..o..\...^)....(.....y.72.^....s%...[q!&Z...C-+o....l.....Y.{.....g.1.0..l).....<.....T...t..l;x&).[7...4.5...{...n.<...#l.....r.wW~..zr..9k.^ KR."W.J.n")...%0...)..Fbb5'4'.X.E.../t.&t(...@9...\$.....]P..jdU.....H;:\$'%.l7.....y..\$....Z..4.Cm.u#&.%N..1...+..8....y...U.(.T.....).l..5r)...l..K....>f..3.C.G..X1.(.<Gb..b(...0Qv0F.....n.z.s.Y.....\..h%1...QU..%}B CW.....sO..\...=&3....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001L.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 563 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14458
Entropy (8bit):	7.944094738048628
Encrypted:	false
SSDEEP:	384:uuT43eqJy2jEeSZE0nrAFAOpn5yIfNrfIkBQTYz8ynth2EB:EugQeS+nrAFZ8tJNrfRQM4ynH2EB
MD5:	7CEB71F78A193F8C9F7FFDA5F81AEBD8
SHA1:	EEC1597705EFF1A527C246B86A71878185BA6B1B
SHA-256:	77911FF7AEAB8FCCAF36DE6E1183FFE1A6C27F77B5714EE78097CE5189E8FD0
SHA-512:	1D1AB19B64E1E2ABCA61AE78B3B50310B0A6CF19D2ECFCB4499D8D0BF68600B4D95BC0945EF9FF9B1D016ED61EAC518DCCA1A426F460317C07AD51E2E047548C
Malicious:	false

Preview:	.PNG.....IHDR...3.....>...sRGB.....gAMA.....a.....pHYs.....o.d.8.IDATx^}.p\W.ZRKjI.).[.M.I.N.[.O..B&....?5...@.5.5EQ...T...d*U...*.C6...8..}.Wy.e.....kjs..z..^..T...s...}:.{.n..1."@...P....."@...p @f.s@.....B...6D..."@f.3@.....B...6D..."@f.3@.....B....6D..."@f.3@.....B....6D..."@f.3@.....B....5 ...f.;0..7141...L.....M.3.L....{M.T...I.C...@E{.w.Y...q....c3..gf.3..}j...l...{M...@..4555==...l.f....d...>i.%&&%&u...f..[.....O'.....G..E6l.< ..3.k...'...Y...<.....u...[9.....S^^.q.<..^...2.bb.E'r...ey.....3.....Dg@L..a'.x&"O.Y..le.c%\$. (P_d...Sj...S...BLu.[g..mK.SwVe.."@.T.@P.y.....=...40..L...\$d.J....cccw..^..RBKKK...heJiS3.0I.X<..}..*O.....QR..q.5GTA..ht. (^Hno..n.....wv:...K?..\jQ/i..h0)G..1Y....K.>FT...8.d&...+-T.b.....f.."3.V 6...E 1...?Q.6...A1Smm..K...V)...:uA'\$.v.cy.<.`Z322.r.Ll.....>.....&....."...".....@.Ccccee.[..z{.fL5..[...
----------	---

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001M.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 742 x 104, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13030
Entropy (8bit):	7.948664903731204
Encrypted:	false
SSDEEP:	384:/06UlmwT2RqfIlhmLy4tNpYGL0mvBQhTMHX4PCIVYm:s6USI2RqfGhmDrpYM0ofHX4aIVYm
MD5:	17E9FF9F735102231846936F0E2BAF1A
SHA1:	9EC1AE8A3AD55C48C02427D842D6E38DA85B5145
SHA-256:	DD1CA8DA90893E0B63ABFDD9E60CF2BF844B311964E9D9DDB855C21FCA156EBB
SHA-512:	71E690D6C87B09659296E6E6DDC8E3F91035DD80C5CE875FA557763E8138900C27FB492885291CEE203D65BCEE8C20C9C39E0590A5FD32B8A00BEB3E3F6D6E7F
Malicious:	false
Preview:	.PNG.....IHDR.....h.....2.....sRGB.....gAMA.....a.....pHYs.....o.d.2{IDATx^wp\.....sN\$....\$.Q.")R2ei,kl.%...r.v.m.x<...\...u.U.g.ry=..uX.cK.dl..l1G..\$.".Fg.q...N.nt...3.w.w...~v.O.....K.....A@.....A ..H.n.D:A@.....A@.....e.y1..P..xH..... ..e.91..P..xH..... ..e.91..@.\$9..S.....A@..4....^C..F..VR\TT.....aHll1.....VS..g..... * ..z..jEk.....<R../55+33;;;+..Y..WC..#..P.....#0:.....522...,v..D.....9.2N.L.'.F\$.e..l.....N...`1...G.....'&,f.f.X...!lp.....l.....J..z.R,YbYd&..... ~"b\...b.Z.SS.....c...&..Yf.....[...BY..... 1...Z..6NN....._zw....MKK.Z.vMMnnn.4.v....q..e... ..D%...Q....._p"M.....22..e...k}.....qU....S.a...~...P..}jv.. ...1..2...F.GCC#...]=..C..n#..K+..MOO.....".....d^2={...U.p.h%.%n...D....XB..b..""....?h.b.Bw..^Q^UC.....Q...!.....U.VD...P..{.2"A@...b..V.....jF.x.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001N.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 165 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	3879
Entropy (8bit):	7.9281351307465044
Encrypted:	false
SSDEEP:	96:k1hccap27HGvHvY2Kn+A3RS+HG3dXrjmg26vh:k1hccewlhYxRmR5
MD5:	C451B2A146BDD7EF33AB3EA27268796D
SHA1:	C040BA2F31342CBCBF597C96D4D6EDB83D473B77
SHA-256:	4C264B2A6E88712234DAA8E3A8D630CBF4EEB338554CB0B794D8031F8943EE65
SHA-512:	55915A304B261BC6F38F5CFE0389D5195F85FE2C1DA325019C3AA391E8B1773091E078A35BD57F8CEE0BA035956382AE33790F462053FCE711EEA9665B7F917
Malicious:	false
Preview:	.PNG.....IHDR.....c.L.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^}.p.U..g..Bp!..\!.`pA+....H.U..."Z...*U... ..P.D.-\$.g....\$.g.....CB.l.....l.g.pc..Lf..~.=~jS....w.9..w.'...l.L..A ..^..t..v..s4&&&%%.6.'...:G.D@.7.qS...K....[.....o..p..2%..B.Y...];..gy+{.....o..p..2%..B.Y...];..gy+{.....og...}.W.z\?..y...;_t...=.e).....6.M {...B...[_.. \^Pf.....\...../6....<5.4./...m.....l...B'.n...O...yc.....X..P...k...t..9tfg>...e..Sy'.L+**.][{..a...7...p.+.....K...y.9p...l{..i58...v..5. Op.....{.....8...S.....p..)}.....y...2...b.[>gP...C..G.H.....Osp...)}..9x!...W...^.....\$r.p.sOJ.l.=x.9s&.....h.`..W"V..l {..72....zv@.#.<...../...F]...c...4.W...:uj@1...~X.....^si...Z..l~Q.<...NAOq...+f'...)...\$L..gV.6#....F\$.hD.g.L~..H_u..].4.....h...T.BK\Z222...7))..h...1??...~.=...X...~h...y[.....p....x....c...{.....Uh.7n....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001O.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 651 x 254, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19235
Entropy (8bit):	7.944867159042578
Encrypted:	false
SSDEEP:	384:h4iuxL3Yck5lpMcTyHOypEod/G38lJxqSp5BCU:h4/xjYc2lmcOuuEoJm8fse5BCU
MD5:	AE32E846559D576FD263BD69FEDBEC28
SHA1:	D481DF71C858BAECFE33418002D368F2DCF68D4A
SHA-256:	6E21222B0EADAB8D3CFB0C7D14941D196165D6709271AF317D099F12403CD352
SHA-512:	9AA4A6DD01D3B745D674721765F2BFCCAB584CA0603F222EDBE9A88190A2A57438041E7A3706CC0656A6ABB79AA18118319F210EFFE3DD917E7B94A6294BD346
Malicious:	false
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d..J.IDATx^..X.W...D..A.....bW.A..[.5.F..D...7.ob71.....b..""("...{.../...e.....}.....;...S.X...H...@d..... &.....b..... F.....b..... F.....b..... F.....b..... F.....b..... F.....b.....O.KVIVijFzJzVF.]i{.R..l.q..'l...e.'/'..G.z.*l&>)61.UjVzf..4>Q~...U...=...s..\WE...2...t..'F...M.....'??...>BO(m.V.P...Gy.../.....B.6.....= z7.Z. hQ.u..j.....&..Z.bo?..u..S7.G>...)l..7.i...<.y..l]...Sl>...L.2.<...[.='M.Tsprp...T...cE"...P.....eefQ.NKN.x...:-#5.../q../xq.YzJ:.T.*u.j..S.C=...].2.(YF.....]...*.7t...[jz...W..Y..{...nlfj..L.6.[hS.=....{IC.....?5..+...[.a.:U.K.C.....w.....+..r@.z.7..j.qB.B...X]..=.fk...>^5[...n.z...wn...Z4...jWG..^..z6./t.....dhM.9s...Gbo?...U.V..tj.....*&)lo.{q.G..A...l..i7...&...d.E]...#.W.x.,T..&Mz4+.4.\$n..F.x.<.ppr.....y..i./..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001P.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 220 x 170, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	7374
Entropy (8bit):	7.955141875077912
Encrypted:	false
SSDEEP:	192:lfGsPejaVZWzIZKpnFFt0HK5+2Y/SLopWR:lusPe278IZKpnzt0q5+qVR
MD5:	70DAF02EC717AB54452FA4C707BCAC74
SHA1:	30F46FAC5E96470848C5A948162CC12455A05154
SHA-256:	58469BA93EA36498FF9864EB54713A001C52106DE97804506D82EE24B816712B
SHA-512:	E599FDC22A32CFEDBB23EECEAE0B278EAB9A90959FE6ACB40E2B201E45A7C19261AAF529E7A0D9CAF2A9A4C64C7831343F3BC20810513990AD5D38A32741564F
Malicious:	false
Preview:	.PNG.....IHDR.....IC.....sRGB.....gAMA.....a.....pHYs.....o.d...cIDaTx^..S[Y..l...B..`...N...t.q..j...+LU.....O..sF.l.l...w@...H.Q.w...s..{B....2....i..q..z{ }^..... .J.fQ...r.WWW.T...amt.t;...6\N.....z.n...]u.z..Q...?^.....;NO.}.c...<-.....({{...t.k...F..[m.....R2...%y.l^OOONN8)... y... ...}}.}.Hy6.^a.....\..!S...K.. >.....s.....l. .P...LFWW.l..RK...b.h.h..3.F.. ..~.....e.aa.....0H...<.Y.a`..xA!...7.X...xd.....h?o5.....Ay....?6.....*.tb.9."j...S'](.P...9.2]..?...z3wD.[.....L3.Ng2G&..0 ZK1u8.H.2...Z.../..P([...BA..aL .a.Y:...J...5^x..'\..&S...L.U.....<{..."..@x...J.N...j...W ht.<.B.....IHM...&z&..6u..hF..G.D..B.....A...n...GG....,Q...X,"...r.....3d{o.(/. .3.H...x:SX...h.8...r...<.DB...y.Y.N...o...5.....L&w...v...w..D.....l.a4...`8.U.. 0m.(.zR>.=.+L.....e....Yd2-.Z.7..D"..pX.l.....e5qYa_&..3..J..++

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001Q.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 46 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.814570704154439
Encrypted:	false
SSDEEP:	48:4gv2YZ4gWLPu9JcREmXfFEV7NNkfKOgV60g0Z:KZgWLPsJcj+mPFGNkfrngp
MD5:	3F1535054D4F9626F0EB10CEE47F076E
SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C60
Malicious:	false
Preview:	.PNG.....IHDR.....1.....[*].....sRGB.....gAMA.....a.....pHYs.....o.d.....IDATXG.iLTW... ..23.....6kK.5..5..IMh..Tl.....V.v.PZ.-F...".k.pCQ.....#.../s>f..3s....<...=^ '/~.;a...>g....*o.6k..k...E...O...aQ.j...X&vG.....{u-...\$...CX...xhZ...Q...Z.....O...l.Id.h...q.q.....Y..J7O7.R...~o...[...; 'h...u.g..>X...o.]]...>.....u.....5..2]... ...EodZ.R.i.....ryxh...C!..6\$!..).W.^...Q.y...Ay[...M'o...;..hh'....}.%....".h.5.?=.y.x..2/gK...4.2P.(#S.F.G.o...!Mk...w/_1'.5...[U7.0..Z..w^..&/...G...Y...g...;...JF.t...~'.X...uYd.E. ...+R.....2cHG9.YC..X..Eg.).r..+%%t.6/...@3...[O].0..!;.....E.J"...#R"...q...~r...%4...b.Q...al.6.....{y...l1.Xs.}.y;...u\.....sm.C..@ 2.AG.K.5..}.k ..~.....4..< ..PH].).Z.[H.G.iH.7UR...}.B.f.....<5n7.*WR.c...l1.....<y...%-... "Y@(*...)).(....l...y.z6...J2.S...c..z.G..Kj..^R...M..k>..PA.1>..s<..G...8.r.....dL..uF.(...q.P.j@...CPSc..^

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001R.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 167 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	5386
Entropy (8bit):	7.943706538857394
Encrypted:	false
SSDEEP:	96:x4F84/zVJWedudPZZRdbvczHe2tFJ0y8Ea5b2AELJj:x4FTnodRZ7c7LrabEaMAGp
MD5:	DB48555480A383CD1D4DD00E2BCFCF29
SHA1:	8060B6FE12175289F0A71F45B894030A0D9F1AB5
SHA-256:	807723D8F90A5BD41269A7A62817547026A117D666D5BEF454EB699C97CA3FA2
SHA-512:	2614C04686299CEE8D56577A1E836A26076D42E041C627177FDB295629F6A80190910947FA794A094C55A45C3D70725EEF29097118E523A38B50C9263C771A41
Malicious:	false
Preview:	.PNG.....IHDR.....gl.....sRGB.....gAMA.....a....pHYs.....o.d.....IDATx^..XTU..M..B...P.....)vQpQ.ED."","*bC..VT.. M!...@z....1...Wf.w..o29...=v .TUU.^.@_S<.;h;.5.9r...x..7N[={.....'..N...u...9..5+YW{;.N\..u...9..5.....O...,K,'./.....1..T...>.f..9.xo...u.xo...u.xo...u.xo...u.xo...u.xo...u.xo...u.xo...)...Yqq...Y.f[/]_l.W_].....S^Z^Y...++.*.pF.....?..l.&...O.,k.d...~..w;Q.....7}1y.....e_.....=y_U_{[.]w.O...~.z.{.....Wq...".....^h.....}p.+>m...d...4...a~Z^....me... ...N]..1...g..y.f.....l.g.).....e[.....Z.RB.Krd....#...{..eff..v.[[<n..?{(.....SN9%...V.yE...s2.....e@Wz..l..B.r.<.-.=/t[v. .J.....,@.A.v...s'/.....6f...L?.z[T7..)S0.;c...s.z-C ...v..}Y...[.].xF.....'#...C...k 3..8...N...5.....f...3.....f)-.p%.D.v.v.].f.....33<<.....[bbbt]w...r.....z....q...=....m.uHd...,zXg

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001T.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE

File Type:	PNG image data, 230 x 68, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4181
Entropy (8bit):	7.950380155401321
Encrypted:	false
SSDEEP:	96:L6ousL3esIFAmjb89xK6YiSTwtw5dT1W9IQ:GoFiUFAMbsxJYieZ5dGkIQ
MD5:	BC6C08F8C2C6D1EEE95ABFC40C3C3669
SHA1:	44DE7375375880ACC24938D7E92A837E85C35321
SHA-256:	6E54B502C46E1AFA57E28B8ACCCE24F102399F31407827A91E4CD7A42FCBC746
SHA-512:	2AF4A9B87FA4F362926CD77F272CECBE3ED4F0E110FB8F30F661DF7C61B77B9FD8E7716EEF9177B1038B68C792CA4F844F729DAA48B2E38B9945EC9CB44BB720
Malicious:	false
Preview:	.PNG.....IHDR.....D.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^yp....E-.....v..VY.a.d....R.euF.).KH@.*B..u@YdQ....!&.tjg.!,a'!L...@H...{^~yy....w2z...s.=,;..S.....].j..b5d.j.X...2D.....r\.#.f...Bl....5dC...f.....m....s.j.f.jK...y.^....'8.....<.....g.....=%..2.p.)<.....G....lx.m.4dm..B.....0?..+_*.c..n.....?....wa..l...p....E.L y...*...C.D.vy).....@>^\..3;.`]q.m.../d.B.../.....~.p.U...'..sP^....YH.7.../....R!...O....'.....s....< .f)....i.{.l.l.a.n...?~{...h...s.e...-.Q..R..@<;y.G.+n.....Y.Y'.V.)o...?....>}.w....`+.}. {p"d.RO=&.v..H]....k...X.c.z.{.....}.n...s:c..i7N...^..O..*....)w..[>..E..}y....q..u.!z.D.[^f.Y...>z\..x.B.h"^\)...`... _.....G...hY.../..6>..Z...8^..k.E.5d#..a"...P.CR....OL.. U...qY.{C.<~!~V...x.d..*k.Y...z;?^...3.4 i...[DL...z].._..a.....(s/...W~..q*.\#@[R.N...@*"...=....)q...<.....p...+J..)\#...{,....OQ...\$L...G...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001U.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14553
Entropy (8bit):	7.951135681293377
Encrypted:	false
SSDEEP:	384:EF7aDrPYJ1n3kaEf61xD+KvdokCixTQm7QA96dNT:EF7a/PMeaEf61IT6kCiFQCQq6zT
MD5:	3E9F7D399DF9CAD3669B7A5445EF7074
SHA1:	2FBC965DC03EF9203581F595E0D7AB1734726ED7
SHA-256:	76C80E31F37248C3C787F7972A7B22038390F9D81E72E650071A6F36D36AF27A
SHA-512:	326F8F9CBF829BF80AAA96062A57255A36EE04DE310634327AA075D14129CFA8E36E48AB2A00B10F9BDC1D94F1AC7A9E41D0D063361920A0332EC124BDF4C3FE
Malicious:	false
Preview:	.PNG.....IHDR.....R.....sRGB.....gAMA.....a.....pHYs.....o.d..8nIDATx^..xT...!~.%.%t..H.tP:.HQP@E,...QQ.^.....* E ("]:.K..R.....p..n.9{...sv.}.....7.....o..z....M +.....w.....O...>.S.J.O....<...{. x.g..l..H.....V ..}.PO..H+\$\$@.\$@=.=@.\$@.....VH..H.z.{..H...!@=#.....C.z.GZ!.. ..).....T...B.\$@..S.\$@.\$....>i..H.....H..H@ ...S]8.....POy.....>....p.... ..}.PO..H+\$\$@.\$@=.=@.\$@.....VH..H..zz?.....\$@.\$'i.....c;n.i..0.....<.....S...w..c....y..F4.p.3~.. .}....s.6[.H...N@=M..]'...3./...l.....'. .. K...r ...nX...'. .G... b ...MY89x.Ur'.. _.....5..H..d..L.\$@..l.o.;kM.\$?.....K/.wn.....Y...E..%K*=.....Y.3.lk...[V..WG/?i..H... " T,z...6h.[..-%9....WMY...z.vH..H@/..BOe. .g-P@.....I.H.O...SJ]5?^..5^)..\$.S.@...*~<gJT/....._R.C.....rj..Cg^K.....K...~Y....l@..).l.k.s..Yr.....Z]G..q.+..G...; Nj)..T1&&..?... ...W<{...g.&Ca

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001V.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 454 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8184
Entropy (8bit):	7.807848176906598
Encrypted:	false
SSDEEP:	192:ExqMHYnnEnntvA4Mesu3SXHycmflEFQp1r/:E0MGEEn29esuiXHt0FQp1
MD5:	5B386BF9A20766956A84F67F913F23D7
SHA1:	6E72E51F5B4FA64E52D2B80B41409B3DB927A3C7
SHA-256:	DDF6A1D5B29BD69C65A148B1247FDE8389CC56865E4398E4CBDCBD68A6555043
SHA-512:	99B4109439D9A688D7747C6847E0FF7399CDA01A89C3181789F913E757A82EE4727F95E506F4B01930EFC7C6E229B94BB89E385B56BC009AB5CFE332585660C5
Malicious:	false
Preview:	.PNG.....IHDR.....s>.Q...sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...].l.....!YTP.A.....-.r..\$.E.J.l;...T.M.UE[.Q..x...wKB=.m...4%.. :..9...{..o.3.g. o~..~s...k..X.r..... @Gggg.?.... P_]]]..*lu...C...h..\$...... \.....@R.....\$.k...@0.Hj0.8...r.@...F.l..G....T...@... .P.....5...@ ..\$5.J.A...@R... ..#...C.#@..H*... ..`'(q...@.l.....% ... \.....@R.....\$.k...@0.Hj0.8...r.@...F.l..G....T...@... .P.....5...@ ..\$5.J.A...@R... ..#...C.#@..H*... ..`'(q...@.l.....% ... \.....@R.....\$.k...@0.Hj0.8...r.@...F.l..G....T...@... .P.....5...@ ..\$5.J.A...@R.....W...1c.l..6..`'...@ ..l.S..l.l'..5\.;...`'1.c.k.u.Qs..).g#b.j.@..Y..QR...n!~.....h.Z..... .Xw.U..~q... ..@.%'..... P..E.T.b.j.(F.p.... .C.)3.' .z.w.a.....{.:4[.lY..~..x.'/....g...J..9.K_...'.:..);).....SO=u..E... Py.qf.}O7.o....u?:....6~..9...?7.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000020.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 213 x 85, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1924
Entropy (8bit):	7.836744258175623

Encrypted:	false
SSDEEP:	24:rl0PN36BoJ9JK5IncTww67QKf5wX5YgM5s6cahePwnR6+eA9zQU13ALcVz7wTQ8U:rYN31JH6lcbjMW5Ytmyqwp9H7wY
MD5:	B1FDE66F75507567B5F0C6C07B01A3A1
SHA1:	80B8E6A923E853232F66C874367E90B5C9CAD7AE
SHA-256:	B9C82D2F31BBE409D159EE3C9129CBAAC7C6F6C81637AB9B6DAB3C11AA74B7F1
SHA-512:	FC8C6038D3C2F5765D7524E969574ACD10AF6FCCFD45FE7C6DD4A8C2669B13EE3FB1A8833E94A046AB7037018170B5B87B1A2742E0E10557C413AD634BDF34E
Malicious:	false
Preview:	.PNG.....IHDR.....U.....Q.6.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^].O.W.....G.IT^M^..J....."4*.....j..H..R^"..m..5....&..j..B..`..>...X.....]z.[&.>..ef..gB.d...s~.=...3....m..(E...~.].E3..7.4.....).H_..D..j..).q\....7..#..ag..o .?.....;C .#.../v.H.....o~.{G.....H. ..;v...G..._...p1d2..&.....QS4<..i."X....1(.GR.R.#.}.l.E<..i.LLM.....s.: ".....Fa..b.....\T..~OD.....;j..~..p=Y...Y.....?Y.A...0l6_p.dKctjvZ.....\.....V..1).....;7...(. [...7...u... 'ra...S.].....7.#.[.<..l...[.....90d[.2a.R.....E.CJ..C..S..*_...\$^..Q...>hx.k7.'jN:.W.X..N..p..K.."....q...a.Uy.....[d..vmkk/cW.>.K..C..?d...'.@s_..?&....V_?F...;k....%+...+3bk.....f...T....S.(2=...?gQ...K..._#....?..1W.....m2.....Z....-...?..#J... ..KS.P &[<.....Dd.....\W\$z].k..-..8....>..Q'Yz.].w&....._.....?.)_[T...wy...O8.Om.....l.....l....]... "f.....q.o.V>~>s...~N{.n...w..O .D...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000021.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11886
Entropy (8bit):	7.946442244439929
Encrypted:	false
SSDEEP:	192:sqNuEpzsnKxkfLaZCdMh+cLApmRausyZwYMAisQKShDBlhr34ckckcZ:JNu6DMLaZsMhtLAla0wYMAvI5V4DDQ
MD5:	875CFB3B5C3619253223731E8C9879E5
SHA1:	6372F4F5BEB6EEAE3EDBE5B62EE73039B40AD01E
SHA-256:	CC69BAE5D2C8F56B28BA4E3C6A11F57C4E8CCCE69943ACFBE7E63B4FC90EE5F2
SHA-512:	47F45A3275B8454F8000F4567153DD7D4AF3012005D8E34CB18AED6AD69083BEC753E607F275FBF3EFCCB7BA00310A04ADFBD5FA5B73E6BBE47CE73901C35CA8
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..x.U..l...JB..;H...".(U.EE\..._v]W..b...Az..{G:j..B.\$...H.IHB.o2xE...3gf..w..2....w..sC.\$@.\$...t.l.....8.....RR....<...6..P]...\$@.\$@...PO..\$@\$...T.GZl.. ..)c..H.....H+\$@\$@\$@=e.....S1.i..H..... ..C.z*#.....1@\$@.b.PO.p... ..2.H..H@.....B.\$@..S.....!@=..VH..H.z... ..1...b8.....PO..\$@\$...T.GZl.. ..)c..H.....H+\$@\$@\$@=e.....S1.i..H..... ..C'+++kH.G.=Zl.U...73o^!H..Oljrj.D.....l.M.....Kph.....R.x.....RU8 ..".....j.....B"O.z. .9..".L.....Y.d.Rej.-Y.dhX.....xH.z. (>&..4....O.<..T.%a.e...*"..UnR....+j...2..".M.O>z.....T..]j...m...S'..&..).f..2.....+..SP..?a...=.....3.....K.zj.5 .fP.....2..?.....%....d.qxC.W..~.._...!W..6....iJ)*(..wg.}.]sw\..r]...r"...e _...5_9.YN'...PO-.d.:%.wZQ...H...JMJ.6c.... g*...3....T...o..Nyc.W....A.3.._...U%...PG.z....&.%v....Alm.....~..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000022.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 171 x 50, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2270
Entropy (8bit):	7.845368393313232
Encrypted:	false
SSDEEP:	48:3Cxnazs22lovj2Ez2iqBU2C+hJWizJNzlu1coqAYCIBeMsk1:3dm2Ez2iUhBzhyjAxqQ
MD5:	6EFE6733E10E011FFDD6711B5F37C9E2
SHA1:	C72549E824EAD899944A38C46FBC28BDCDAAD611
SHA-256:	92B5056DAA03DF3EA85AF49FFE4F9CFE8699BDF3539576A99F02418FF49AD9CB
SHA-512:	EC14B553A5780CD9B33D438CE13A6932DE43E346D8D2DEC8D093A6A2048675423948F8E2C604A73460980C3C68D9276B65D76C2A6BC7B24FDF10CA92FDA258E
Malicious:	false
Preview:	.PNG.....IHDR.....2.....sRGB.....gAMA.....a.....pHYs.....o.d....sIDATx^.\kL.W...*.F.....@.*.(H4."Il)..B!.iD...f....y.l.h.....<..1.....C.(XSy.l....,.....3.3...;{...{(g... ..Q..x.T q...F.V...B...?{(.....`.....+0s.e..w....{` ..5...d..9S]../.....\$Y> ...i..8....;r8rIEe"...!'.&E.....n...=@..Sp.GF..c*...1QH3....?.T.el.....t?..([Q'.0...k.G....X..C...k p...l.q;d..N...c.u.a.5.%k.fS)..H..T..~l*k.[.n...x2.1.....%...yK..a..l.[?#iD%FMT..=rjt^..fT...c.&..Lr.....\..V.l...Br^6..U27...O..N'.K.gm.K.g.;l..Fe...w?..Q ..E.....0.....7...{(e..t...x.c6..Q..n.92:%...l..4.h]Z....w.. .l.p..~..B.y..&.....gl... wl.....G.6.K.\$...%-h]8.LT....)}{a...^i.....4.0.ji.....n.pk,.....7t....U9..b...l.....#....<q..(=F.... ..0@^.....+.....X..>p....S..t .f.x.0....7d..n.. '...'..M.qqn...G.t8'=.V.PK....K...X.z.#..l.....@...Y....BH..l.....K....='&Z.41\$.a'o.....i{o

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000023.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	16003
Entropy (8bit):	7.959532793770661
Encrypted:	false
SSDEEP:	384:1l+zN+iNurNE/tBdEC/vkape2XHYdhOm+Bl6C4:L+zN+iNurGNEC3fpe2X8Pa+
MD5:	3A5CD52E925A7C4A345047D8F06C3C41

SHA1:	9C02828D83206BBD3EB58930C8C65A6CA5DBC40
SHA-256:	477277E8CAAAE1D3B3EAB5B3660239AEEABC433743A191727B1A71E529872AC7
SHA-512:	8D8B6AC645ECC7C8BD374E6190819006C71AC0B5993419C42463009116214E5EC4B4235D94B4AE4CDA132E7DDA9807ADC51525824AC5F12696517FFC8890891
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...>IDATx^..+)..H..C.K... ..x).rU..T..*E...;....*.@Z.....@...9q.g7[fgggg.....1//.."@...0..#t.f.C... .:@.....@OIR.#P...0..\$.y.PI"@.....(@zJ]...." ..Si8R*D.....S.D.....J.R!D....R. D..HC.T..... D..... .D@.....p.T..... ..=.#B... =>@.....4.)."@...).@...4.HO..H..." @.HO...."@!@z*.GJ...."@zJ]...." ..Si8R*D.....S.D.....J.R!D....R. D..HC.T..... D..... .D@.....y.?.`T....f.P...\$47.....~E...!D.X.....].0..N.a...>[]...t.T.w *.. ..)... ..X?c.....+OE....<-84...=.....w.8...7.Ro&D@!...GS.....s.....Gg..8..T...u...~.....<...S....Y.....W.....#..vB...u...+.999YYY.....wf..._{6...=..}>Y?..;=02eb.....2 ...;%.\\..P..R5....XMO....6...W]...3g.5;n{t.....F7S...r...[n.....AAX..j[j;neef).2....{ ..r..{7-.....i.S.....<..pm.u.V....M.333....K..Mr.s.Ek..=t_#..P...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000024.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 454 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13241
Entropy (8bit):	7.931391290415517
Encrypted:	false
SSDEEP:	384:a99pmP85w/MAMszG+iHGgrw8Ld+9aEsjQR:mgP85AMs6+UtrX+9mjQR
MD5:	01367FEEE0A83E8765E971E0D3740900
SHA1:	CAE1FD22CE2539FA2ACC0242C615CB7EA3F866E1
SHA-256:	18B8E53505DA3C412890F4D74AE2A6B26C4B0827E15E830F92A02D292AF20ED
SHA-512:	8CFBDC014C42AE6417038B80424D2E9FBDDDD7DFDDF579E349C3C17C9B52AF33A72463154D29539457C4ADAB2DB00CC28A67902F8AD9209E4AF00EDD46D52ECA
Malicious:	false
Preview:	.PNG.....IHDR.....s>Q....sRGB.....gAMA.....a.....pHYs.....o.d...3NIDATx^...U...Y.]:T...G.5..IX...B..Xb4F,l0X.....F...("vET4H.....*EX.....wo9..9 ...rw...;...;o..... z.....B.....v.mn...>.....E"...U...4s!..F...u?..@...!..~F@... ..p..Q.kP.#! ... (U{ @!...!...T.TGB@...Q.....B.5.D..A.....~*.U{.]....S.e...K.A.....7^?....D..h...!..Eu...o.^..B@..# J ...B@....(5(...B@...= ...p..Q.kP.#! ... (U{ @!...!...T.TGB@...Q.....B.5.D..A.....T..! ..k.R.]R...! ..D..B@.....:B@...R.....! Ju.Ju\$....j...! \C@...H...! J...B@....(5(.. ..B@...= ...p..Q.kP.#! ... (U{ @!...!...T.TGB@...Q.....B.5.D..A.....T..! ..k.D.RK.K.m.V.....(^^^ZV^Z.7.a.....T..xsqYi....L.....Z.....)?..yyy.M\b..U3W.0{...~..}..M% J*.w.mdv.*^..@...R..o/^..5...x.g.>..ag....GM t...<s..y+6.X.? ..R...-W.m\..o..0g.i...h..W.Z.i...2....o.&..@...-B .K.^.....u.}.M..6...{...e.V.X.....nkE....5.8....-!..!T!Rxs...Q..2).- ..`.....mX6i.w...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000025.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 164 x 89, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4190
Entropy (8bit):	7.94161730428269
Encrypted:	false
SSDEEP:	96:GHfueo3dRLZKOSYDzGsEgfB9nqS0WKt/z2jOrrz7yrT7N:8A6AzZfBtqS0WKNC2vyx
MD5:	8B3AEC1986A522951942BA72B85CCAA0
SHA1:	7E0DC78FC65EE4C804A4B0C72AA53E2DFDF26C14
SHA-256:	8B02CEC726DECF033B67689F369FDE1002ACFD5F8C32E0F248AC575997204F2F
SHA-512:	8EE1A1F6F0023EB4F60760C2E23EAFD56E6D298CAB49D819CF1D62C0CCF608D4211D3767856255F7CF8FF45AD835FE5475EB92C608989C522CD48D00A050B18
Malicious:	false
Preview:	.PNG.....IHDR.....Y.....?.....sRGB.....gAMA.....a.....pHYs.....o.d...IDATx^..jip...fu.VBBZ..V'>.....CR.....?r...pU\...v*...T~.U)0..(''.....",a..Y..\$t!..D...Mkvf4.Vh W;S.....{...zZw...i.....fj...\$.7.....[Z*.[[.Zk...?t:M...`^...X...sUK[.Rg.=\$.l3<....74...iY...i...k...fA..Z.n...`G.%..H.l7..7J...u.R..6....E..!...N@.....M...Q'...U2.w.WP[!fX.....c ./@7Mz...^..k)...v.Q'.z..1A..P.[...]...vY....>.`...K...m.?CX/v.8....].;...6..kw.....N...z.Q...f.q.xk.5....;?Z.c...`.....4....?....VV.u~..< ..sU4e.....g.c.G...O/...r...`G).. ..#d5.O..w...{...twL1l.)#&hF..K...M[@.Dl..V2..j.3..s....3M....v..!...V..c..B... .e.1....7.WA0.[\u.).\$7f.+.....8..e2K/%.li..`w6w.E..{?_??.l.k2.s....].f...HM.?w..d.9..Rr...Y.c.). s.zk.rc...a..l(9~.....m...Z.....l.....7.K!:Bf.....m.1.....&...;?a..c.@.@.g%...s.#...;c6..g.lZ...}.WX.3.8....W...N.w...L...}....?."cl.....pS

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000026.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 162 x 89, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4081
Entropy (8bit):	7.943373267196131
Encrypted:	false
SSDEEP:	96:KQJAeRumk2zXWYsIEmWL9zi6wknB4qLx+ppNhQrW8Oy:Ke9S482LE6wQB6pNeqi
MD5:	29B87BEEC5D3899824AA390530CD47FB
SHA1:	55108E8E5692E4444F72EE5CEB91915E7A2AEFC8
SHA-256:	F00E4F1C9B1D9ABEAAC8E5CAB02A07FD74F00ACE15E36C6F6469DE5AB07A9FC
SHA-512:	1A5AD45BBA8C29C32CDD3C4D1E460C30ECA305D851FAAC73DF165306BC338337525680B9906D367A0CD3852B9D2DAAA8FD0603276BA969495B4E29C7EC8A330

Malicious:	false
Preview:	.PNG.....IHDR.....Y.....2.h.....sRGB.....gAMA.....a.....pHYs.....o.d.....IDATx^].LTW.f..O.a.....*.....k..M.Z.n.q.h....ht.f.M.n.6..t.h.k.h5.6j[[...X..p...?.g.`..7.o..of....^..ys..{.[-.s.UMMM.(.l.@.l..R?.....(0+0.....5...*.F..#.).....1.....B>[.a..L.....x...0.5t.v..S.hf.....Y....B..&.....f#.w5u.....0...x.sC.....a.4j5V..Z..n....K..>..3t..wm..3hB.BD.P..FkcJ6.....O.....7...S.....6..P.]mf.+o.....w..<.....Y..Z.whd....*zf+.....#.."_"?.....`.....qf+?.?"k...zgME.j..l.k.U*.....&z..N....ma.....R.{r0.S.KP..fU...g~..=.Q.n.*.* 8 T='9.*KDW...GN;0(P3.....1.....';.j .L.a.&^\.d.....o...Y...{E.F..j.e..\.=W.#..W....c./~..b.EWXI.#."&.....X...b.....+2...5..6+)we~ja:IZ.d.Ey....!2.5r.....! .A.....j2 5.o.....WOM....V.....GC9..'.....C..;_..cS....b.1.....t....._.....a.3..K..>V.f.j]..~....K...-.....#o.Y.P.....a.7...#..'s..T....b..].3..dPPP..Y.i...c.b

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000027.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 452 x 277, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	22634
Entropy (8bit):	7.974332204835705
Encrypted:	false
SSDEEP:	384:5ojjyI45m1/9gyhgFsH1ud103PI39o0qjfsH37mNHy7QPaNbZy0:+r45m1/BWKy10tN22rmNHycobE0
MD5:	548D234C9AB4021CA5FAB7BF22502465
SHA1:	2F7495D250DC86EA99473CC342D164B859926021
SHA-256:	7D549C3418CD90F42571D00936B23D242837CE2A8B19FC4C719E182ECB2624C6
SHA-512:	261523F5EAE6FCE2829B53AAC5938B1A0021C119E00CE82EFFDBD690FE71064E0F3B313ED1AB2F67A16C488AD5B1A91F5AF98029D88A7896F271C108410D42C5
Malicious:	false
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d..W.IDATx^..i.=YY6z@..DP.i.lAA.....l.Dd0*p0.ON.~....s>?zbH8..%\$`....b7..=...25*"..L..u..f...j.....Uk..^UWj]u...).{.}t-(-J.....e..t....@i.k....._(.....@Z.6J.....2.O.-P.....u.=T..4p...e..q..5^f~....@i'....?.....@i..k.....?...u..O bN.~?MbT%....@.LO.Or.`....\$.y.{.o....~..(.;...S.Ni...6....w....~{.^w.....~S...g?../.O.....7...Oj].....40.....9....?..<3nw...x...g...7....(<d...{3.K...;...;...5....&...>...t;...8..SO:/.....}.{.D.jt.....jc..s.....Z...0q...@...Z]S(..o....Og.u.l.i.-9..j)..~...5.l).....G....k..Z..c....}.c.?..t+u...15p....[.....2.;;.....w.....v.7...l..w...K/.J..[.N.....W..U#....._j(../z.. ..kv....]j]../m....t.9;-0...4p...@K.....~.9.\$qu.E...!9 .m.+').x..vak-]../.....G'....4.>B6\$......o.q..L;*.N+....>...=!.Y..Q...?.....7.,...}

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000028.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	17289
Entropy (8bit):	7.962998633267186
Encrypted:	false
SSDEEP:	384:ruwwXKZuqnOnZprU3+OXBruY4UkcY+Tpl/BSqCrEoMXMEr3KbzHIDqqAmk+xob:tGcxE4PBruV3Uy5SqCAoMXzrQHoqAk+m
MD5:	708E8EB906BC105CCA0535AE669AA651
SHA1:	38D82DEDfE97D3001188C2E18FE13BD741FD520F
SHA-256:	1C3D07765294566E17270D0F3B9257A3DB7905D4E7EF746AEE80CD591CE0308F
SHA-512:	1EFC74C28190DEE2D2732390B74049A1B120F05EFB8DC6925207C6990AD20450FFAB40249899A9DBB82E8F92A61F770E120A450CAAC7F8C5F0742586CCE0EDE6
Malicious:	false
Preview:	.PNG.....IHDR.....R.....sRGB.....gAMA.....a.....pHYs.....o.d..C.IDATx^...Uc.._ "oB.Hr.m(0.....r..[1.D....R..q)%FBDiB.."w*.k.Jz.Y..l....>..9{.....g..Y.z~..k?.z.^k..+V...!.....{.....sM.tD@...!P...HW.S...u^.....@.r.^.....B@...U.H.J..... }.....>...!..A@.4.EE...!}*...B@...i<8....B@.T2xp..!.....d@...!.....(*B@...S...B...O.QT.....!..@<H.....!..O%.B@...x...9...C ..{>Z../~^s<<V4.ujo..v.Z7..EwT.....@.....?.....~{...K.....C.....bB@.\$.....C.{...KfS.....T.*&....@<.....'.D'...;~v.DT]...r!...>...ru...})....#u G.T.....>..z...3v...P.M.....5.@<..?....F..}.c.W[..._IP..._O.>.M.d<..J...E..)ZZ+.5v.p>..N.{B...>M.Nzf...OB@.."}..D.y...ldK<..!..}.....f.K..bX.T9...&T.&?.VB9.[B@..@.@.4..1}.4.@H..-l..j)..~M.<z..l .G....>..S...N...@y .n...s.d.....(.R"...Wf..oO..^..\h\..')...ni.'.vk.1..k..^....#..}.{.RM...~Z.S...@U!&}.....h...{K...@.....W.8.N.s.Y.0)..f+...%4......5.@j).k+3...l..(

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000029.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 452 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13737
Entropy (8bit):	7.916899917415529
Encrypted:	false
SSDEEP:	384:jgmxm2Fa+/76A6M6Y7rSYRv47cwbkkapeliRmDGd+gUwOSpQ:KgyoWrJWkrkRXmad+gE8Q
MD5:	830632032C7DDBCCDE126F4BAE935540
SHA1:	9FEF1DA9FF1D7762B779553B5F873BE54C8D01EF
SHA-256:	2328D09EC845433DC31808FD6B12616F1D28B9B3BA7DD969ADEB6C32D8EB049A
SHA-512:	5C17EF9A0063499F2C34FAB2C4D968D29E20F20868921FA914E5737995AA0C166F224995109FF7ACA57B5B0F8647715DC670C4AEE385F61B5F8E6E8422C49EA8
Malicious:	false

Preview:	.PNG.....IHDR.....w.pl....sRGB.....gAMA.....a....pHYs.....o.d.5>IDATx^....E....,"o....&....AY\$...AE..".l....+G.>AP@D.e..".A.Y.@...K.IXB !..l..c1.On...== =3=.3=>9O..u....w.z.-].t9]B@...l.....Z...B@...^G`.Q.&S.u\$d....B.Y..P.w5[].....B.m.D...! ..@...Ls.Q"....."S...B ..D.9.(.B@.....b@.....".@..!T1i. J...B@d.... B@...4. %B...! 2U...! .r@...d...l.....*.....9 2..D...B@...L..B@.....D..! .D..! ..@...Ls.Q"....."S...B ..D.9.(.B@.....b@.....".@..!T1i. J...B@d....B@...4. %B...! 2U...! .r@...d...l.....*.....9 2..D...B@.....5]T.@.{.O.;k...>...o.+.....{V...&C..(?m....F....gd....?....3u..x^L.1n^...@./....XE...L..l..t...L.B.)=.sn.U.....@.O..\$.o..L...g.(D... (...Lo8.....f.o.i.f.h.9.....\./. [W.9.....+....X...+d....Xc..7.p.m.Yg.u:YO.V..l.t].Z.g.U...].5...^..._..WL...o.3f..s.,Y.X.7.x5...K/-.....{.....W.(Y....?...!...W;.....iwNMW....@+Q.5.#.
----------	---

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002A.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 185 x 76, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2332
Entropy (8bit):	7.8822150338370776
Encrypted:	false
SSDEEP:	48;jB5Gg4vMs30Wln5iVeRy1bY7DqbqQBAeNjukXIN4AXat:PGYuEWW/YH7e1uA0AXat
MD5:	91CB7F1273AA003076401081B8A22237
SHA1:	5157144069E7D2FDAE60B397BE5851E75BDF7707
SHA-256:	80682DD6472E8D1136BC5E20F6DE87B595562414B19EAB8E965736FE992921B0
SHA-512:	5A8E3C0ED0DB94BFE359C63793F12F3D7B3C37F3A13A5C96634BA1DC8C9E50FB1142FE4752FD9FBFA39A682F78C54AF868AD337EAA787801FE5F66D8F55A81F6
Malicious:	false
Preview:	.PNG.....IHDR.....L.....sRGB.....gAMA.....a....pHYs.....o.d....IDATx^..L.LUe.....Ji(".....9.....". ..5L.Y.Y....\$350.."2.IK3Cg...T..DWZ.....i.?!<..~x..z.....w.sw..9....s...w...l6.....p"dH...F..B<...qE,R\$G\!..E..").#....".{f.Pyl.d.l.;...=S...O.S[\Y^P.aj]9*Y! ..~.#...S.s...l.h.[m....%...P..@.kG.....G..X.r)%..AO.}-.G>35..c....Ac.&[W.d..+.. ..zG.....=..l...VS.d.+...tGd..k-_-oL..).p~.W\$C.. ...l..n...~.....i.....e.=..?{.....>r~.Lw.+2..w.)w~..c....h..u..%..PE...f..'.m.ZE.1.l...U`X.....\$.P%.UH{[K..o7~.k.4 9..W.t~.^_7.....f."q....+.....;c.....Xb.?.....0h.IV..WX!.....ljm.1c..U...{..X.).....B=.0~..W...rO...j...ehI5U...66V5sJ....V..j>...1kQH..2.....d...S...l...+..].p....m7...Z.. ..s.D>.K].?.l...2..=..~.mq.."." +.....8. v.o.)Z.....>Xv..i..TA...M.....>[X..Y.7lJ..e7..S....02q.O&9.....:L...N.....W....d..FqE..T..N.....R....kXv[.j.....g.K.\@`.M..B)8n

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002B.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11332
Entropy (8bit):	7.9324721568775285
Encrypted:	false
SSDEEP:	192:vpXZavBpl00n1P17JquG9GYHDK/5cxektxMQjcie9ZZkx30eXJlb8FKRN:vpZaDyc1P1Je9G62/5clpjre9nQkeXJY
MD5:	31579CA3352DF8FA4E3E7F48C7CDF672
SHA1:	AA682A3C781BF8EE43B5EDC9718E64CB79135F25
SHA-256:	B0E7824BEE2C896279457D87E61E902431BEB528D830524CC4DFAE126E89FC24
SHA-512:	782FF9492E3ECB11C72D316DDD94D1F3E94CD908FC9452A37DA6CA30ABCFE9AB2BCCED8583A569DA68626BCEC730408AF86997E295637BF64AFF5BC768F3E309
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a....pHYs.....o.d..+IDATx^{..u./...&....6..+z..Q."b*. &M.d-e.*.....J..Z-T.Z\$...R..F...%*"bn.<....W.E ..w...^...;g.. [w.5w.9g...3.....t8t.P.?@\$@.\$@.5....= 8qb.....5...a=...#..y. ...@B...am.\$@.\$'.....G.B.\$@..S... ..C.zj.#[l.. ..).....!@=.....}.H.....VH..H.z.>@.\$@.v.PO.p d+\$@\$@=e. .;...v8.f.o_o[?...~.n.S.N.?..._L;j.H.....7..]. ...7...b...ObVa1..?X.....~.....t2..V>b.}.0F...%'GO7.n#~..F....K~...FX..H.^....k .Z/2v.W..M.<.\$;v.t.,UO..-].....D....o.J..Y.....5.%l...{.....'O..dC\$=uks..;{x.,N.=...".Q].w>.E.H.....AV=...f.&.. .ip]_0..~[pf.`9..v.W...2.E.\$P.....+...OcC.H.=..]. [.g%(h....W...?..UDh..T\$.?...; .)]?[Wo.h.'.2P.1...l.....\$..NO.5..).c.;...~x. Q....B..6.@>..y..}.m...D~z...L#..0`_'.s? ...l.....a...=N....c.._2..._6..]...S....{^>.lM...;n...k..9J.. S.G...{.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002C.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 167 x 92, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4181
Entropy (8bit):	7.943341403425058
Encrypted:	false
SSDEEP:	96:b6JWqvCl45Da8kuGzhRwZvwlutfij19MQ8EpW14LBGJVCq:b6JTCI45DalsBws1R8914V5q
MD5:	817D5A35EDB2B0E052194D4F49FDA19C
SHA1:	FA6CB2016C5F43B76102B63D60359139227E07EA
SHA-256:	0A87B8418B7F8E6E117BADDA11D7CDD38B8B7320C6BA3D3E9AF93EB9ACB2CE14
SHA-512:	E0686BDBFC589401F0EAAE2B1598199EFA285F8392742B1C928B9274088804B23DCB584B6FEF68CE6D7E54DFF9C10338104F4C0F3F80A04471F0B2E8F9935CC0
Malicious:	false

Preview:	.PNG.....IHDR.....\.....!2a....sRGB.....gAMA.....a....pHYs.....o.d....IDATx^.]IPTW.iv..D....%DQ#A\$.~d.h.,T~..+...TM'cj*).k.fj~L~\$.~L&.....:FdU..f.....n.m.....q.s.9.=..w.9.....\$.~b.*.%.....@AJA.~%.<.....l.h.+./..OSE.....j....>...C.....^cCy.0nz.4<.....g.?~>..1ws.B....07W65.74T....=.v.....D.....6.....tR....}})....4z..^.....7...;:".....^..... =#.=32..o.<Tn*Q....g.zN...n*.../.....l....F.j)...6...m...CX.~...+...U..E.j].....7]=E?!((\$~e.%~.....w...Y...l.1...@....t.P..=;)...*...N...N.j.xS.5&.....Pe.....Z.Z^XJkx.....^.....?7..._....Wsz....)G..j].....[y....].J....'R?aa..G5.l.i.?...MH..l.DC^_c.m.....%{(z.&.*+x;..S....zxyH..`...].~el^.....U.T..^..p..z[.6(2x...;#;o#...;)Zv[Z.....V.....0)Z.....].m.....x..).k]e..._W!Vry..%...l..d..j)w....^..l.....m[l.^3r.....-8.....j]....>...Q..T..{\VptH.?.....1..w...FHI...x....\`~ei.w..)`...g..V{..Z.....8.....o..._..
----------	---

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002D.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 221 x 77, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2599
Entropy (8bit):	7.903700862190034
Encrypted:	false
SSDEEP:	48:PmCwDjH8w9JewaF2zQNXxJ8zq1KM43sxXyYbTgJW1MFsrJ075CawGjGj:P1Ah8UewaFcgz82Kx8xXNYb3id/yj
MD5:	E88131C9AAC52649FF044905ACAB9B76
SHA1:	34AE73B9165CBED0DDF33AC20E4B3E7D622C19BF
SHA-256:	30F22340F582F9A352A7ED3048D1088F178E83CCAACAC1CCFD86852C8F9C78E3
SHA-512:	97AFE8F3A2A3138613934AC737C390A35F6757BFC3D381EA7C7CD148F739932380DCD46D0BA6F590C274F8BFB4D4286B3C0433AA69E090102A8A9ABDD7C97E11
Malicious:	false
Preview:	.PNG.....IHDR.....M.....sRGB.....gAMA.....a....pHYs.....o.d....IDATx^.]kl.U....BjE..>...*.~Q.....b[K.....m.(.....!%1%*-B.C~(&[.....~.w3..Kw.3wvfn.2{.s....{w..l..l3...:.....zD.x...O.K...^1*...8.G..z...D.\$.....>!.V..`v.CQQQ!..-L.../3.2.....ZH.?s...lu\N...,3?.p.N.....<....E.<=z..lu<ll.dX...g...+{X.p.....t..a...cKk[.~.Yszl.N.....KPs.~).T.5...&B...*.5j`@...(_r.V.j..m...?x.sg...t\dz.^.=\h.<y.....l..w..ze.m.\qPJu....D.j].@.....W..t.+....X....e....\H+.Ns%*r.VS.N.3:...&....._#^....d!..F....xc..M...q...17.z...z&C.K9(lfm.35.v.>:X,...p:=H..J.K....~...7.t....R.R..9.?....l./.(...0z0.M.f.)H..Y_"e.....B.....L..q.K.....];..L.....xl.K3.M..%...../.){....R....s...7...}.q..._R.4O.a3.....<..%....3# .~.y...u...R'.P..\$KlZ.....g.....7..l..x>.{p >+.....e..~.Re@.N..FY.....*....})...[.~h.M.oq.S.U...c_}.....8TP....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002E.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 232 x 50, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1570
Entropy (8bit):	7.780157858994452
Encrypted:	false
SSDEEP:	48:r+em8Tlk2APr2fEd72tTqiVJlLzqeVzYwS:r+erTlk5S+zoyGahS
MD5:	EF9AA5B2ADBE5DF68AC4F4D716DF7708
SHA1:	363B93AAAB9DB2832F6CA0EE3C27C9310C344BA8
SHA-256:	3D94FCC4821A135ABAAE6579011441B94F9C04DAD1E66BB5211B0C019A5968B9
SHA-512:	EC9B024AEA46F7B97D14F0A7E12704D09B85F0017CC9E273CE50F2F889DFDAE81DE549CCD546BBB8F8BAAAAAB7781FEF77BF783E02CCC9605304552F7DD5903D
Malicious:	false
Preview:	.PNG.....IHDR.....2.....n.f.....sRGB.....gAMA.....a....pHYs.....o.d....IDATx^.]MK.W...t!fU..bl.....*JBA.....%-.F.4\$.Nw]....E.\$...)T.....?@.O{...3w..y.=/'o.9...<y...X....c..1P6..e.lx....0..J...e3.&\@).....o.*>E;.....~..Z.3'K..W0S.&L...M.e.`..M....i.....6g.^....4..L.Y.9.\$M...4..L.Y.9.\$M...4..L.Y.9.\$M...4..L.Y.9.\$M...4..2.....q...&.....*Qg.+p.....a.:X6...o2...A....j]..p.p...P.....>.....3.....z8j].....>..fww.6.....S<.....^%4.....{N\$.~!H....~.....a.(.G^>~ bxx...K\mF..`d.d:9J!.....j..i24.A...`O.....s6?={...H'...~.O.....>...ZXx.3...;C...l....%.s=...w<h.....0...~.y.....+n.P.M]c...A.Erj.R...\$g...9*_jg.....x...&+JWM4xe.^.....0...11.[.....f....r#h.h\$....[=t>...r...L.O.KL..B\..x.....4J.O...vY...dA..w.....g...};}......:.....x.l.j].....).....x....s....N.\$n.g<Z.q.a9.C.....oX..%KNNN..i.8J..p].1....B>{.....n.Dj3t..lg...Q

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002F.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 340 x 79, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4490
Entropy (8bit):	7.928016176674318
Encrypted:	false
SSDEEP:	96:WXKr7Xwf6Obg+XaGOnsjbbGSb+ydWtRvEOhDE6XqPeosv02tR45boo:3rTUGXZnsHKSb+n+8DdKlwm
MD5:	7F161B1B9B937AB48D4FD2F6E5E16FDBD
SHA1:	BDCE4F1C73E87E609A7FDF245A512CA4F73B35B9
SHA-256:	C863C5E71D1116D69561BD0637F4FE4C4240E9CED05B8A5B056073AD13E6495D
SHA-512:	E915B76FAAC9512D2AD11CF4E4530A19BEA1C7D8508BC218C69CB041F1EEABA3E2E03B1D56E61B032A6418829752C21B8354AF1335466D7E1528A06E6742A461
Malicious:	false
Preview:	.PNG.....IHDR...T...O.....;.....sRGB.....gAMA.....a....pHYs.....o.d....IDATx^..p.U..'.rD.WX....Q....."\$ZHP.Z...C.....R.%G8R.....R.C6..A.b...0...^..#..g.....z2.....nB...l.X.&...a....a....a...._73'N.ukeee.6mZ.n.m.G.j)...n...a.9s.DGG...y...8???.o.pE1...Y.....)ca.i.M:5\$\$.....Lr...ye.....6...8...z.-r...d.{xc.U..^11...>QX..y..2...T...sss1..."A.?_..w..S.F>.....4.G.....D.j]...@.K.....C...k...P...q...6:QQUEE.....7;;;...q.k.j]..z..6j>..n...Y.&G*.n.S\$)).....r.....}.[Dv;..w.A...`.....a~.N.f.s...P...*.~7n...eK...+n;..W..C..9)..O..D.q.X..5i.s~en.c.F&?...i.lj3r..W'..#..7o..R.@^..*..W..?j...t...{B.8..D...UPa..~.C...j.C]a.9..R...c.Y0..9u...d...C.....X.U...WK....5...'.PM:~<.._..z.F^..EH.K>_0.d..S...Yj<~.5?l.fZ0.@d....*G..K....e..b.je..Q.4....(z'..lG.....2.XQx).....X..2\h.X~e...Z...=...C.1.....w....d.z

File Type:	PNG image data, 59 x 61, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2210
Entropy (8bit):	7.86853667196985
Encrypted:	false
SSDEEP:	48:naUvGemgl0W5KMDRLEbGAnaHC7ew/fkDSCcE5FTaHWc: aerVIDRl LewkXl rTa2c
MD5:	73E38124F94AD20A2F1571FBBE11AEEC
SHA1:	87FB8056DC7A0A3B70D51426771C4CCE2099CFE5
SHA-256:	A700B63B30CBBE5230CC5E977D651E178EA87E73EAB18C8D5FFB1362149ADDF7
SHA-512:	320FCE64DD6F975384BEC9267348CD5CD24A55B13BB09FEF1238C2216AD8ECABDCCC15601A079CE092ACFA4954829FFEB06FBFB0631F6AE26E3A39E43C10208B
Malicious:	false
Preview:	.PNG.....IHDR...;...=.....sRGB.....gAMA.....a.....pHYs.....o.d...7IDAThC.yL.w...r.r.....Eq.nnN..i.[e...-d.M.dn...x.xmQAT.Q.RN9..EA.k..P`..=)...m.&~.....o y...k...)}x...[...g59.]}...~i.SY....."....7Ow../.....2...3f)n[...R..R.....U?.....O.{...c..pT..\t...5.07..07...7.o...+.,V.c...&..%3l.....v...6.....??..[.N.....nz..Z.B.....v.prs.q1V1 ..='...'bz..%s.cf.3..RyMNUeV..J.k.]D[~xo..d..c...sO.y...B...c.07.....Rp..J.....{b.....;u...s...N.gko.M...;6...6..c.X5.S..o...^.....).....y.72.^...s%...[q!&Z...C-...+o....l.....,Y.{g.1.0..l).....<.....T..}...t.lx&)...[7...4.5...{...n.<...#l.....r.wW~..zr..9k.^jKR.*W.J.n.")....%0...)...Fbb5`4'.X..E.../t.&t{(...@9...\$.....}.P..jdU.....H;.\$.%).l7.....y..\$. ...Z..4.Cm.u#&.%N..1...+8...y...U.(.T....).l.5f)...l.K....>f..3.C.G..X1.(<.Gb..b(...0Qv0F.....n.z.s.Y.....\,h%1...QU..%}B CW.....sO..\=..&3...;

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002K.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 127 x 138, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2232
Entropy (8bit):	7.837610270261933
Encrypted:	false
SSDEEP:	48:dFQY2WmQbe+TukEC2KgYPsWOuWfK792oP/sWtGOK9Lc+rD0NTHj;3L+wKkEOgx3PG92Eq t9LczFD
MD5:	EDB5ED43CC6038500A54B90BEC493628
SHA1:	A8CD63F3914E4347F4C5552FB922C6C03917F45F
SHA-256:	9F3312E33EB78C6952B5A5D881BBD18751FCFAC41D648C6F053CE781342A504F
SHA-512:	4EBCEFD69A4C249AA3B0F00A954C4E463DA22FC9CA0B61A0DC46079B438138C509B22188D966FF6599A3A604858BC4CC8FE6E0685A764E8E0477AB7A237DB32
Malicious:	false
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d...MIDATx^..hVU..}..s...6..9g.MM3..j...*.....A..!A.....R.Ai%YH..(M.."h.cf*.B.....{w{.....y.s>.{#y.r.K..K.O).....Y..b..[N...=...j.....!...../6...B.8....p....5P)....@.....=).....^~..@.o'n<q....Yw].mg\V`...y.W.T.>...\n...s.iG.~L].d.<.8..j<.<1..4...CZ0...}... ..oDDh....}3}#"B..O.....0)B.F.L.....5.f.FD..L.....5.7""4`..p.....'.kt.....>!\k.oDDh....}3}#"B..O.....0)B.F.L.....5.f.FD..l..x.....Z^...>B\$1.N")4....1:&F8..*.X.yL{(.s.3.....~2. EL%w.Uc.zJ..B..S..b.7o)%7..'.....N.].Vi...q..uO../...W{..y...&iL. X&T.....~.....Z.o~o..U...oCF.M....O4).....~.....:T..W...s...t..Dlb.\$Pr../.._4.b.....R.T\$.\$.>hB..+.{m.w..Q...05..C.)...}.....?..h.....Y..8.6^t....).y.%.....l=\$[~..].h..N.....*.....SBj...8..H.....G...j.....;6YQ WO.o.}].".\$.oE.y...i'9.[cmS..@m@Q

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002L.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 742 x 104, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13030
Entropy (8bit):	7.948664903731204
Encrypted:	false
SSDEEP:	384:/06ULmwT2RqfILhmLy4tNpYGL0mvBQhTMHX4PCiVYm:s6USi2RqfGhmDrpYm0ofHX4aIVYm
MD5:	17E9FF9F735102231846936F0E2BAF1A
SHA1:	9EC1AE8A3AD55C48C02427D842D6E38DA85B5145
SHA-256:	DD1CA8DA90893E0B63ABFDD9E60CF2BF844B311964E9D9DDB855C21FCA156EBB
SHA-512:	71E690D6C87B09659296E6E6DDC8E3F91035DD80C5CE875FA557763E8138900C27FB492885291CEE203D65BCEE8C20C9C39E0590A5FD32B8A00BEB3E3F6D6EF
Malicious:	false
Preview:	.PNG.....IHDR.....h.....2.....sRGB.....gAMA.....a.....pHYs.....o.d...2[IDATx^..wp\.....sN\$...\$.)..Q.")R2ei,kl.%....r..vm.x<...\.u.U.g.ry=.uX.cK.dl..l1G..\$".Fg.q... N.nt...3.w.w...~v.O.....K.....A@.....A..H.n.D;A@.....A@.....e.y1..P..xH.e.91..P..xH.e.91.@.\$9..S...A@..4....^C..F..VR\TT.....aHl1.... VS..g.....*.....Z..jEk.....<R../55+33;;;+.Y..WC..#..P.....s#0.....522...,V..D.....9.2N.L'.F\$.e..!.....N...`1...G....'&.f.fX...!Ip.....l.....J..z.R.YbYd&.... ... ~~"b\..b.Z.SS...c.c.&..Yf-.....,.[..BY..... 1..Z..6NN....._zw...MKK.Z.vMMnnn.4.v....q.e...D%...Q....._p*M.....22..e..k.}....qU....S.a...~...P..}v... ..1..2..F.GCC#...]=...C.n#..K+..MOO.....".....d^2={...U.p.h%.%n...D....XB..b..""....?h.b.B.w..^Q^UC.....Q...l...U.VD...P...{2"A@...b..V.....}fF.x.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002M.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 563 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14458

Entropy (8bit):	7.944094738048628
Encrypted:	false
SSDEEP:	384:uuT43eqJy2jEeSZE0onrAFAOpn5ytFfNrfIkBQTYz8ynth2EB:EugQeS+nrAFZ8tJNrfRQM4ynH2EB
MD5:	7CEB71F78A193F8C9F7FFDA5F81AEBD8
SHA1:	EEC1597705EFF1A527C246B86A71878185BA6B1B
SHA-256:	77911FF7AEAB8FCCAF36DE6E1183FFE1A6C27F77B5714EE780976CE5189E8FD0
SHA-512:	1D1AB19B64E1E2ABCA61AE78B3B50310B0A6CF19D2ECFCB4499D8D0BF68600B4D95BC0945EF9FF9B1D016ED61EAC518DCCA1A426F460317C07AD51E2E047648C
Malicious:	false
Preview:	.PNG.....IHDR...3.....>....sRGB.....gAMA.....a.....pHYs.....o.d...8.IDATx^}.p W.ZRK l.}.[.M.I.N.[.O..B&...?5...@.5.5EQ...T...d*U..*.C6...8..}.Wy.e.....kjs..z..^..T...s...}:{.n.1.."@...P....."@...p @f.s@.....B....6D..."@f.3@.....B....6D..."@f.3@.....B....6D..."@f.3@.....B....5 ...f.;0.7141...L....M.3.L....{M.T...l.C...@E{.w.Y...q....c3..gf.3..j}...l...{M...@.4555==...l.f.....d...>i.%&&%&.u...f..[.....O'.....G..E6l.< ..3.k...'....Y...<.....u...{9.....S^^.q.<..^.....2.bb.E'r...ey.....3.....Dg@L..a'.x&".O.Y...le.c%\$. (P___d.....Sj..S...BLu.[g..mK.SwVe.."@_T.@P.y.....=...40..L...\$d..j....cccw...^..RBKKK...heJiS3.0l.X<..}.*O.....QR..q.5GTA..ht..(^.Hno..n.....wv:...K?..j\Q ..l.h0)G)..1Y....K.>FT....8.d&...+-T.b.....f.."3.V 6....E 1...?Q.6....A1Smm..K...V}....:uA'\$v.cy.<.`.Z322.r.Ll.....>.....&....."...".....@.Cccee..[.z{.fL5..{...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002N.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 123 x 103, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	7.80882577056055
Encrypted:	false
SSDEEP:	24:q3kLWZefR0kKbfLnNhzzt+acvt2x6pBs/j+7QUJ0QbDQ883ASaoUV4hNgq1rsyhy:q322nN+X11GDsg8831Uyhi/vf
MD5:	D5F7A65469623327F799B516ACBFFD2F
SHA1:	76C6333C14AF3A7EA091819953E6E12DC289A12C
SHA-256:	F476FAE1C6D79069239C471D182631AB343749C22B1A6990250465C7EC3738FE
SHA-512:	351B9E455E97E6247E64E4BC1B59C9524E70AE0D09D3B6FB96937378A70536483B00426EE69C3590DD415A8265D21FD031B524B90E4E86814EC9AD704E57793E
Malicious:	false
Preview:	.PNG.....IHDR...{...g.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..h.U..p.T..(eBR...2.....':4kec^....0.&.....ugS.8u.i.P.F..f3..D....6.%...xal.)...y..9...s.w.s..{.y.5<<<...(0Q.....t...q/[@.....-e.....=..J.L.....c.4H.....u?XF.KJ..zb..0..f)..J..[&..S.6...w..9..._.....<.....?j...H.....>.....~}.n.8.WW..B?...?b;.....<.....~..b..m...&1.=Pq...w...a_3.k7'....d.z.O..w...s..Lh.x.....Q;40.i..'8V_@_@rd....kF.@<@..e.....e....=mHB;...E./\h.^...q...>...%v:O...&q...:'.e..9...hiG'.L<@.....([.].n.x..c.....O...}).S*..Q...d....A...4..t....E..v..j...7...t.b.../* .H. ...8... @.(.'..Kt....].+.[LwJ.B]i.b.k.@..Js.....J.....6..J..LwS<@..J.YLwV<@G.4w.L.G...].zu.z.h...;..W.IH..+...c..F...qXul..}.N...wv\M\$.D...+...=....?U...T..^<6./T*. {q.q;.....y..XL..l.z.d....G..b..g.G..b.....SM.{q.q\$MUL..R.....^P..g..e....L/yqM../b.f.....J.<

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002O.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 163 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4847
Entropy (8bit):	7.950192613458318
Encrypted:	false
SSDEEP:	96:JnieMJ5zTz/gKVp93jQvcv16kjOzbapFJBkjcMNBqmQzOG8qx1QKnse8T:JieMJzph13Evcv16RfapFLxMNB08qxa
MD5:	A1A1017A6A7928761CEB56D1D950E123
SHA1:	28272E9C7F816A1CE8F2033FC00F489005332365
SHA-256:	72F066CD34EA71D0E1B28FB60D663B0372C5254E1A8239C94A164EEF9389DB88
SHA-512:	10F4557F102230126BC86CD4B49C93365C38D5CBEAC51F4691B90D861098866A2BDEFEBA507731D4FA14367FEE430453BD716157F9074EF643F2B949B09E1530
Malicious:	false
Preview:	.PNG.....IHDR.....n.<.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^}. TU..}.E.O.T....L~....af...Z.....O..4..>Ms..Js_....5.E.d...Y....?z.3..}.l.]?~...{.....s.z..Y.....E.X.6....c..u..y..W.j....."}...l.i.`.l~..MKH.E.bi.d...b.X.)...X4 .vJ6-...;+/->Qyi.t...%.T..k;U..y.C\$[...Gm.....v..*2..2.eee..."!.)...yy...l l/..u.....2...M.:..."W....o..t..._6m....'.k.T.v".q.....S~.....O.....ed.[W0X..HB.V.i.....<=..E^^.....MyY..vpp.....^6....aQQQaaa.....]^^nkg../_d'.%.....L&k..B.....?C...W.VVV6660t.J+K:...%q.....e.cp....Kz..%qZsARiT.!.....>55.R.U.W\..L...T...K..rE.U.K.-9.....y.y.....K...>..HWTt.e...+..B.....%...%.....^..... ...M'.%f /..=p...{O.../...@...DP..hw8...7o>..A.mgg.....7-]?~.s.OE.E. .=.....%ly.....MSn.i.....l..U.\$0SZ.P.][.%X[;{;{N.....\.....6O.....'Nj}.s.m...E..V..f..r...4..~.....H..F.}....4..R.=.....xT.4...../...z

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002P.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 46 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.814570704154439
Encrypted:	false
SSDEEP:	48:4gv2YZ4gWLPu9JcJREmXfFEV7NNkfKOgV60g0Z:KZgWLPsJcj+mPFGNkfnpg
MD5:	3F1535054D4F9626F0EB10CEE47F076E

SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C60
Malicious:	false
Preview:	.PNG.....IHDR.....1.....*[*.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATXG.iLTW... 23.....6kk.5...5..IMh..Tl.....V.v.PZ.-F..."k.pCQ.....#/s>f..3s...<...=^ '/~.;a...[>.g...."o..6k..k....E....O....aQ.j...X&vG.....{u-...\$...CX.....xhZ...Q...Z.....O...l..ld.h....q..q.....Y...J7O7.R...~o...[.....;'n...u.g.>X...o.]]>...__u.....5...2]...EodZ.R.i...=ryxh...Cl!.6\$!..).W.^...Q.y...Ay[...M'o...;.hh'...}.%..."..h.5.?=.y.x..2/gK...4.2P.(#S.F.G.o...!Mk...w/_1`5...[U7.0.Z.w^.&/...G...Y...g...;JF.t...~'.X...uYd.E. ..+R....2cHG9..YC..X..Eg.)r..+%%.t..6/...@...3.... O .0.:l.;....._E.J"...).#R"...q...~r...-.%4...b..Q...al..6.....{y...l1.Xs.}.y;...u\.....sm.C..@ 2.AG.K..5..}.k ..~.....4..< ..PH .)Z.[H.G.iH.7UR.`.B.f.....<.5n7.*WR.c...l1.....<y.%...-..."Y@.*...)).(....l..y.z6...J2.s...c...z.G..Kj..^R...M..k>.PA.1>.s<.G...8.r....dL...uF.(...q.P.j@...CPSc..^

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002Q.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 165 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	3879
Entropy (8bit):	7.9281351307465044
Encrypted:	false
SSDEEP:	96:k1hccap27HGvHvY2Kn+A3RS+HG3dXrjmg26vh:k1hccewlhYxRmR5
MD5:	C451B2A146BDD7EF33AB3EA27268796D
SHA1:	C040BA2F31342CBCBF597C96D4D6EDB83D473B77
SHA-256:	4C264B2A6E88712234DAA8E3A8D630CBF4EEB338554CB0B794D8031F8943EE65
SHA-512:	55915A304B261BC6F38F5CFE0389D5195F85FE2C1DA325019C3AA391E8B1773091E078A35BD57F8CEE0BA035956382AE33790EF462053FCE711EEA9665B7F917
Malicious:	false
Preview:	.PNG.....IHDR.....c.L.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATX^].p.U..g..Bp!..l..!`pA.+....H.U..."Z..*U.. ..P.D.-.\$...\$.g.....CB.l.....l.g.pc..Lf..~.=~]S.....w.9..w.'...l.L..A ..^..t..v..s4&&%%%.6..':.G.D@7.qS...K...[.....o...p..2%..B.Y...];.gy+.[.....o...p..2%..B.Y...];.gy+.[.....og...}.W.z]?..y...;_t....=.e\.....6.M ([...B_....[_\^Pf.....f...l\.../6...<S.4./..m.....l..B'.n...O...yc.....X..P...k...t..9tf.g>...e..Sy'.L+**.][.a...7...p.+.....K..y.9p..l[.i58...v..5: `Op.....{.....8._S.....p..).....;.....y..2...b.> gP....C..G.H.....Osp...).9x!...W...^...\$r.p.sOJ.l.=.x.9s&:.....h.`.W"V.. l[.72.....zv@.#<...../...F][...c...4.W...:uj@1...~X.....^Si....Z...l.Q<.....NAOq...+')...\$ L..gV.6#.....F\$.hD.g.L~..H_u..j4.....h...T.BK\Z222....7))..h...1??...~-=..X...~h...y[.....p....x...c...{.....Uh.7n....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002R.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 46 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	7.814570704154439
Encrypted:	false
SSDEEP:	48:4gv2YZ4gWLPuU9JcJREmXfFEV7NNkfKOgV60g0Z:KZgWLPsJcj+mPFGNknfngp
MD5:	3F1535054D4F9626F0EB10CEE47F076E
SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C60
Malicious:	false
Preview:	.PNG.....IHDR.....1.....*[*.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATXG.iLTW... 23.....6kk.5...5..IMh..Tl.....V.v.PZ.-F..."k.pCQ.....#/s>f..3s...<...=^ '/~.;a...[>.g...."o..6k..k....E....O....aQ.j...X&vG.....{u-...\$...CX.....xhZ...Q...Z.....O...l..ld.h....q..q.....Y...J7O7.R...~o...[.....;'n...u.g.>X...o.]]>...__u.....5...2]...EodZ.R.i...=ryxh...Cl!.6\$!..).W.^...Q.y...Ay[...M'o...;.hh'...}.%..."..h.5.?=.y.x..2/gK...4.2P.(#S.F.G.o...!Mk...w/_1`5...[U7.0.Z.w^.&/...G...Y...g...;JF.t...~'.X...uYd.E. ..+R....2cHG9..YC..X..Eg.)r..+%%.t..6/...@...3.... O .0.:l.;....._E.J"...).#R"...q...~r...-.%4...b..Q...al..6.....{y...l1.Xs.}.y;...u\.....sm.C..@ 2.AG.K..5..}.k ..~.....4..< ..PH .)Z.[H.G.iH.7UR.`.B.f.....<.5n7.*WR.c...l1.....<y.%...-..."Y@.*...)).(....l..y.z6...J2.s...c...z.G..Kj..^R...M..k>.PA.1>.s<.G...8.r....dL...uF.(...q.P.j@...CPSc..^

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002S.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 165 x 131, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	3679
Entropy (8bit):	7.931319059366604
Encrypted:	false
SSDEEP:	96:tT+LtoQ9jsUBsnwIDGtHue8ww2JiGEjdKKnE+Gh:V+Ltt5GwIDQHue8ww2JiJ7MKnnE+K
MD5:	995CEACAD563F849C4142B6A6F29F081
SHA1:	44CB3B867CD2917541B7D5AAED2F14F10FEBB0FD
SHA-256:	3691FB8C60EA1B827092F05FBB1807E34726016C6FF56698D7B81C44D519D22A
SHA-512:	3C8EFEB966B075D06D8344483352BF92C9292F9970C9377BE254EB355EFAF017916737AECDCD704B84D532B7229F9908951A6F2CC3FAD810791CAB224401AD3I
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000030.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 749 x 126, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13084
Entropy (8bit):	7.940058639272698
Encrypted:	false
SSDEEP:	384:o4KSpFN6Ud4c3p2ll1yavNr5spYVJzimlfZ:wGN6Udv4IKavLBJz/r
MD5:	0693DABBBC411538D209F32E22F622F6
SHA1:	FB7E675406FA123CDB7E058D336742D6A2E8DC8E
SHA-256:	2DFB2E7A1A3AA43C673D2EE540D3C366CEB12105EB5441F98992FC06F4284013
SHA-512:	F07732660EC62DAE58EB02E2E9476007EA92BF826F642BCA547097136AEA01D29FF69D9B0CD0F5D65A5E15AA66CA4AA4804AA171A3504AAB198631C643C90C16
Malicious:	false
Preview:	.PNG.....IHDR.....~.....sRGB.....gAMA.....a.....pHYs.....o.d..2.IDATx^..w....'m.9c.6"....&.`.N.(.TN.Ne.N.R.eKr..T.*[...?T...l.D.S>I\$A...l.....y.9...f.....3...Gh....)_ .o....n..A@....A@....L...2... ..x...#... ..1fj9.[....A@.....3fE@x.YWN....A@.....1Y..J.Y.N....s"...../..rc.scuyyyu...s....t.o.i..j..lv....Gr.#9 %%%9%-...d.T...r...DH...6.....%U..A@..0.....rAD2.5.....L.R.=W...gZ`o..-?.T.Cy:...y.9..y.EE...v.....1..R.....1".....`"...ss.....i.lhY...Fj*....%-Gw...HJJr8..6...#.....l.(? P.(.....8(u.....*.OOO.....dgg....Q.=..c.y....A`S_@.....3.CC..GFfg..l.l.COrrJFFFNNV^nn^^.z..%...(....b\$......a..y.LMO-.yIV+.k..T>Jg..*/!/+.....M=.x.....E.....`~..N.Kww.z...%%.e.%yy.i...P.)'.A.5.d.0.Cc35==66>2::33.>.;.li.i.gv...DSd...l#...l.....)**,**...V..1 .F.'7....)..SSs..7..F...C.p....(*,.....(RG..B...l!2... ..l)r1

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000031.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	17289
Entropy (8bit):	7.962998633267186
Encrypted:	false
SSDEEP:	384:ruwwXKZuqnOnZprU3+OXBruY4UkcY+Tpl/BSqCrEoMXMER3KbzHIDqqAmk+xob:tGcxE4PBruV3Uy5SqCAoMXzrQHoqAk+m
MD5:	708E8EB906BC105CCA0535AE669AA651
SHA1:	38D82DEDFE97D3001188C2E18FE13BD741FD520F
SHA-256:	1C3D07765294566E17270D0F3B9257A3DB7905D4E7EF746AEE80CD591CE0308F
SHA-512:	1EFC74C28190DEE2D2732390B74049A1B120F05EFB8DC6925207C6990AD20450FFAB40249899A9DBB82E8F92A61F770E120A450CAAC7F8C5F0742586CCE0EDE6
Malicious:	false
Preview:	.PNG.....IHDR.....R.....sRGB.....gAMA.....a.....pHYs.....o.d..C.IDATx^..Uc.._oB.Hr.m(0.....r..[1.D....R.q)%FBDiB.."w*.k.Jz.Y..l...>...9{.....g..Y.z~..k?.z.^k.. +V...l ..(.....sM.tD@...!P...HW.S...u^.....@.r^.....B@...U.H.J..... }....".....>...! ..A@.4..EE...! }*...B@...i<8...B@.T2xp..!d@...l.....(*B@...S...B ...O..QT.....! . .@<.H.....! ..O%.B@...x..9..C'[{>Z../~^s<<V4..ujo..v.Z7..EwT.....@.....?.....~{...K.....C.....bB@\$.....C.{...KfS....T.*&...@<.....'.D`...~v.DT].r!..>...ru...})....#u G.T....>..z ..3v...P.M.....5.@<...?..F..}.c.W[[_!P...O.>..M.d<..J....E ..ZZ+.5v.p>..N.[B...>M.Nzfb...OB@.."}..D.y...ldK<..! }.....f.K..bX.T9...&T.&?.VB9.[B@..@@ .4..1}.4.@H..-!..}.~M.<.z.l}.G.....>..S...N..@yj..n..s.d_.....(.R"....Wf!oO^..h\..")...ni.'.}.vk.1-.k.^.....#..}.{.RM...~Z.S. .@U!&}).....h...{K..@.....W.8.N.s.Y.0)..f+...%4.... ..5.@j..}.k.+3...l..l(

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000032.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 185 x 76, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2332
Entropy (8bit):	7.8822150338370776
Encrypted:	false
SSDEEP:	48;jB5Gg4vMs30Wln5iVeRy1bY7DqbqQBAeNjukXIN4AXat:PGYuEWW/YH7e1uAOAXat
MD5:	91CB7F1273AA003076401081B8A22237
SHA1:	5157144069E7D2FDAE60B397BE5851E75BDF7707
SHA-256:	80682DD6472E8D1136BC5E20F6DE87B595562414B19EAB8E965736FE992921B0
SHA-512:	5A8E3C0ED0DB94BEF359C63793F12F3D7B3C37F3A13A5C96634BA1DC8C9E50FB1142FE4752FD9FBFA39A682F78C54AF868AD337EAA787801FE5F66D8F55A816
Malicious:	false
Preview:	.PNG.....IHDR.....L.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..LUe.....Ji("...9....-".5L.Y.Y....\$350.."2.lK3Cg...T..DWZ.....i?!<..~x..z.....w.sw..9...s...w...l6....p"dH...F..B<...qE,R\$G\!..E..").#....".{f.Pyl.d.l.;;=S...O.S[\Y^P.aj]9*Y! ..~.#...S.s...l.h.[m....%...P..@.kG.....G.X.r)%..AO}-..G>35..c....Ac.&[W.d.+ ..zG.....=..l...VS.d.+..tGd..k-_-oL..}.p~W\$C.. ..l..n..~.....i.....e.=..?{.....>r~.Lw.+2..w.)w~..c...h..u..%..PE..f..'..m.ZE.1\..U.`X.....\$..P%.UH[(K..o7~.k.4 9...W.t~^_7....f."q....+.....~;..c.....Xb.\?.....0h.IV..WX!.....ljm.1c..U..[.X.).....B=.0~W...rO..j...ehl5U...66V5sJ....V..jY>...1kQH..2.....d...S...l...+..}.p.....m7...Z.. ..s.D>K[.]?.!...2..=..~.mq.."..+.....8. v.o.)Z.....>..Xv..l...TA...M.....>[X...Y.7lJ..e7..S....02q.O&9.....L...N.....W....d..FqE..T..N.....R....kXv[.j.....g.K.\@'.M..B)8n

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000033.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE

File Type:	PNG image data, 452 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13737
Entropy (8bit):	7.916899917415529
Encrypted:	false
SSDEEP:	384:jgmx2Fa/+76A6M6Y7rSYRv47cwbkkapeliRmDGd+gUwOSpQ:KgyoWrJWRkkRXmad+gE8Q
MD5:	830632032C7DDBCCE126F4BAE935540
SHA1:	9FEF1DA9FF1D7762B779553B5F873BE54C8D01EF
SHA-256:	2328D09EC845433DC31808FD6B12616F1D28B9B3BA7DD969ADEB6C32D8EB049A
SHA-512:	5C17EF9A0063499F2C34FAB2C4D968D29E20F20868921FA914E5737995AA0C166F224995109FF7ACA57B5B0F8647715DC670C4AEE385F61B5F8E6E8422C49EA8
Malicious:	false
Preview:	.PNG.....IHDR.....w.pl....sRGB.....gAMA.....a....pHYs.....o.d..5>IDATx^.....E...."o....&....AY\$....AE..".l....+G.>AP@D..e..".A.Y.@...K..IXB !..l..c1.On...== =3=.3=>9O...u....w.z.-].t9]B@...l.....Z...B@...^G`.Q.&S..u\$d....B.Y..P.w5[].....B.m.D..! ..@...Ls.Q"....."S....B ..D.9.(.B@.....b@...l...".@..!T1i. J....B@d... B@...4.>%B...! 2U...! .r@.@d...l.....*.....9 2..D...B@...L..B@.....D..! .D..! ..@...Ls.Q"....."S....B ..D.9.(.B@.....b@...l...".@..!T1i. J....B@d....B@...4.>%B...! 2U...! .r@.@d...l.....*.....9 2..D...B@.....5]T.@.{.O.;k.>...o.+.....{V...&C.(? m....F....gd.....?.....3u.x^L.1n^...@../.....XE...L...t....L.B.)=..sn..U.....@.O.\$..o..L....g.(D... (...Lo8.....f.o..i.f.h.9.....\./.[W.9.....+....X..+d.....Xc..7.p.m.Yg.u:YO.V..l.t].Z.g.U...].5^..._~.WL...o.3f..s..Y.X.7.x5...K/-..._{.....W.(Y....?..!....W;.....iwnMW.....@+Q.5.#.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000034.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 213 x 85, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1924
Entropy (8bit):	7.836744258175623
Encrypted:	false
SSDEEP:	24:rloPN36BoJ9JK5IncTww67QKf5wX5YgM5s6cahePwnR6+eA9zQU13ALcVz7wTQ8U:rYN31JH6lcbjMW5Ytmyqwp9H7wY
MD5:	B1FDE66F75507567B5F0C6C07B01A3A1
SHA1:	80B8E6A923E853232F66C874367E90B5C9CAD7AE
SHA-256:	B9C82D2F31BBE409D159EE3C9129CBAAC7C6F6C81637AB9B6DAB3C11AA74B7F1
SHA-512:	FC8C6038D3C2F5765D7524E969574ACD10AF6FCCFD45FE7C6DD4A8C2669B13EE3FB1A8833E94A046AB7037018170B5B87B1A2742E0E10557C413AD634BDF34E
Malicious:	false
Preview:	.PNG.....IHDR.....U....Q.6....sRGB.....gAMA.....a....pHYs.....o.d....IDATx^..O.W....G.IT^M^..J...."4*....j..H..R^".m..5....&.j..B..`..`..>...X.....]z.[&.>..ef..gB.d... s~.=...3...m..(E...~.[..... ..E3..7.4.....).H...D..j..).q\.....7..#..ag.o . ?.....C .#.../v.H.....o~.{G.....H. .;.v...G..._.p1d2..&.....QS4<..i..X.....1(.GR.R#.)!E<...LLM.....s.: ".....Fa..b.....\T..~OD... ..j~..p=Y...Y.....?Y.A...0l6_p.dKctjvZ...\\.....V..1)...::;7...([...7...u...ra...S.].....7.#[.<..l....[.....90d[2a.R.....E.CJ..C..S..*..._..\$^..Q... :-hx.k7.jN:W.X.N..p..K..."...q....a.Uy.....[d..vmkk./cW.>K..C..?d...'@s_?&.....V .?F..;k....%+...+3bk....f...T....S.(2=...?gQ...K..._#....?1W.....m2.....Z...-:..?#J... ..KS.P &[<.....Dd.....\....W\$z].k.-.8...>.Q`Yz.]w&.....?..)[T...wy...O8.Om.....l.....l....]...".f.....q.o.V>~s...~N{.n....w..O .D...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000035.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11886
Entropy (8bit):	7.946442244439929
Encrypted:	false
SSDEEP:	192:sqNuEpzsnKxkfLaZCdMh+cLApmRausyZwYMAisQKShDBlhr34ckckcZ:JNu6DMLaZsMhtLAla0wYMAvI5V4DDQ
MD5:	875CFB3B5C3619253223731E8C9879E5
SHA1:	6372F4F5BEB6EEAE3EDBE5B62EE73039B40AD01E
SHA-256:	CC69BAE5D2C8F56B28BA4E3C6A11F57C4E8CCCE69943ACFBE7E63B4FC90EE5F2
SHA-512:	47F45A3275B8454F8000F4567153DD7D4AF3012005D8E34CB18AED6AD69083BEC753E607F275FBF3EFCB7BA00310A04ADFBD5FA5B73E6BBE47CE73901C35CA8
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a....pHYs.....o.d....IDATx^..x.U..l...JB...;H...".(U.EE\..._v]W..b...Az..{G:j..B.\$...H.IHB.o2xE..3gf..w..2....w..s].....C.\$ @...t!...8.....RR...<...6.P ...\$@\$@...PO..\$@\$@...T.GZ!...)c..H.....H+\$@\$@\$@=e.....S1.i..H..... ..C.z*#.....1@\$@.b.PO.p... ..2.H..H@.....B.\$@...S..!@=..VH..H.z... ..1...b8.....PO..\$@\$@...T.GZ!...)c..H.....H+\$@\$@\$@=e.....S1.i..H..... ..C.'++kH.G.=Z!U...73o^..IH..O jrj.D.....I.M.....Kph.....R.x.....RU8 _..."...j.....B"O.z .9..".L...Y.d.Rej.-Y.dhX....xH.z.!(>.&.4....O.<..T.%a.e...*.UnR....+j..2... ..MO>z.....T...].j...m...S..`..&...)..f..2.....+...SP..?a...=...3....K.zj.5 .fP.....2?...?.....%....d.qxC..W~..._...!W..6....lJ)*..(.wg..)]sw\..r]...r"...e_...d_5_Y.N!'..PO-...:..%..wZQ...H...JMj.6c...[g*...3....T...O...Nyc.W....A.3..._U%...PG.z....&.%V.... Alm.....~.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000036.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	16003

Entropy (8bit):	7.959532793770661
Encrypted:	false
SSDEEP:	384:1l+zN+iNurNE/tBdEC/vkape2XHYdhOm+Bl6C4:L+zN+iNurGNEC3fpe2X8Pa+
MD5:	3A5CD5E2E95A7C4A345047D8F06C3C41
SHA1:	9C02828D83206BBD3EB58930C8C65A6CA5DBCF40
SHA-256:	477277E8CAAEE1D3B3EAB5B3660239AEEABC433743A191727B1A71E529872AC7
SHA-512:	8D8B6AC645ECC7C8BD374E6190819006C71AC0B5993419C42463009116214E5EC4B4235D94B4AE4CDA132E7DDA9807ADC51525824AC5F12696517FFC8890891
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...>IDATx^.+)...H..C.K.....x).rU..T..*E...;...*.@Z.....@...9q.g7[fgggg.....1//.."@...0..#.t.f.C..'.@.....@OIR.#P...0..\$..y.PI"@.....(@zJ]...." ...Si8R*D.....S..D....i...J.R.I.D....R..D..HC..T.....D.....D@.....p.T..... ..=..#..B... =>@.....4.)."@.....)."@...4.HO..H..."@.HO..."@!@z*.GJ..."@zJ]...." ...Si8R*D.....S..D....i...J.R.I.D....R..D..HC..T.....D.....D@.....y.?.`T... .f.P...\$47.....~E...!D.X.....].`.....0..N.a...>[]...t.T.w *.. ..)'..=X?c.....+OE.....<-84...=.....w.8...7.Ro&.D@!...GS....s.....Gg..8..T...u...~.....<...S...../Y.....W.....#..vB...u... .+999YYY.....wf..._{6....=..}>Y?...;=02eb.....2...;%.\\..P..R5....XMO.....6....W]...3g.5;n{t.....F7S....r.[n.....AAX..j{j;.neef).2....{ ..r.{7-.....i..S.....<.pm.u.V....M.333....K..Mr.s.Ek..=t_#..P...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000037.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 164 x 89, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	4190
Entropy (8bit):	7.94161730428269
Encrypted:	false
SSDEEP:	96:GHfueo3dRLZKOSYDzGsEgfB9nqS0WKt/z2jOrrz7yrT7N:8A6AzZfBtqS0WKNC2vyx
MD5:	8B3AEC1986A522951942BA72B85CCAA0
SHA1:	7E0DC78FC65EE4C804A4B0C72AA53E2DFDF26C14
SHA-256:	8B02CEC726DECF033B67689F369FDE1002ACFD5F8C32E0F248AC575997204F2F
SHA-512:	8EE1A1F6F0023EB4F60760C2E23EAFD56E6D298CAB49D819CF1D62C0CCF608D4211D3767856255F7CF8FF45AD835FE5475EB92C608989C522CD48D00A050B18
Malicious:	false
Preview:	.PNG.....IHDR.....Y.....?.....sRGB.....gAMA.....a.....pHYs.....o.d...>IDATx^. jp...fu.VBBZ..V'.>.....CR.....?r...pU.....v*...T~.U)0..(''.....",a..Y..\$t!...D...MkvI4.Vh W:S.....{...zZw.....fj..\$.7.....[Z*.[{.Zk...?t.M.....`^...X...sUK[.Rg.=\$.l3<....74...iY..i..k..fA..Z.n...`G.%..H.I7..7J...u.R..6...E..!...N@.....M...Q'...U2.w.WP[IfX.....c ./@7Mz.....^...k.)...v.Q ..z..1A..P.{...} ...vY.....>.`K...m.?CX./v.8...];...6..kw.....N....z.Q...f.q..xk.5...;?Z.c...`.....4....?.....VV.u~...<_.....sU4e.....g.c.G....O/..r...`G).. ..#d5.O..w..{.....twL1l)#&fH.K...M[@.DI..V2..j.3..s....3M....v..!...V..c..B...].e.1....7.WA0.{\u.).\$7f.+.....8..e2K/%.li.`w6w.E..[?_??.?..l.k2.s...].f...HM.?w..d.9..Rr...Y.c}. s.zk..rc...a..l(9~.....m..Z.....l.....7.K::Bf.....m.1.....&.....?a..c.@.@.g%...s.#.....c6...g.IZ....}.WX.3.8....W....N.w..L...}....?.".....;cl.....pS

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000038.bin (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11332
Entropy (8bit):	7.9324721568775285
Encrypted:	false
SSDEEP:	192:vpXZavBpI00n1Pt7JquG9GYHDK/5cxeKtMQjcie9ZZkx30eXJlb8FKRN:vpZaDyc1P1Je9G62/5clpjre9nQkeXJY
MD5:	31579CA3352DF8FA4E3E7F48C7CDF672
SHA1:	AA682A3C781BF8EE43B5EDC9718E64CB79135F25
SHA-256:	B0E7824BEE2C896279457D87E61E902431BEB528D830524CC4DFAE126E89FC24
SHA-512:	782FF9492E3ECB11C72D316DDD94D1F3E94CD908FC9452A37DA6CA30ABCFE9AB2BCCED8583A569DA68626BCEC730408AF86997E295637BF64AFF5BC768F3E309
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...+IDATx^.{...u/-...&...6..+z..Q."b*. &M.d-e.*.J..Z-T.Z\$....R..F...%*"bn.<.....W.E ..w....^...;g.. [w.5w.9g...3.....t8t.P.?\$@.\$@.5...=8qb.... ..5...a=#.y. ...@B.....am.\$@.\$'.....G.B.\$@..S... ..C.zj.#[!.. ..).....!@=.....}.H.....VH..H.z.>@.\$@.v.PO.p d+\$@\$@=e.;...v8.....f.o_o[...~t..n.S.N...?.....L;j.H7.]... ...7...b...ObVa1. ?X.....~t2..V>b.).0.F....%'GO7.n#~..F....K..~..FX..H.^....k .Z/.2v.W..M.<;\$.v.t..UO.-].....D....o.J..Y.....5%.l....{.....'O..dC\$=uks..;[x..N.=."..Q].w>.E.H.....AV=...f.&.. p]_0~[pf.`.9..v.W...2.E.\$P.....+...OcC.H.=.. .. [.g%(h.....W...?...UDh..T\$.?.... .)?[Wo.h'.2P.1.!.....\$.NO.5.)...c.;...~x. Q....B..6.@>.y.)...m...D~z...L#0_`_s? ...l....a...=N....c.._2..._6.]..5....{^>.lM...;n...k..9J.. S.G..{.

Static File Info	
General	
File type:	data
Entropy (8bit):	6.730632576999535
TrID:	Microsoft OneNote note (16024/2) 100.00%
File name:	OMICS_Online_1.one

File size:	120428
MD5:	238f7e8cd973a386b61348ab2629a912
SHA1:	f87f164125c9506a16ca21cb03104f6a04321592
SHA256:	1c3a7f886a544fc56e91b7232402a1d86282165e2699b7bf36e2b1781cb2adc2
SHA512:	6dc853dac43d4754c7e78ee19f0ac016d935d4c53344091c06ed4eefc1afec53cbd3276d24d53eb37613a8d14c5be0116f2d984b8ca1c0e1cb2bf3101cc5b1be
SSDEEP:	1536:RDBoTVdaeNtuXndCrJmT4HVnteV4FrdMiYcx7bfCb6HPdnXW:1BoC+tCYvSMVnte8ZP1Y6Jm
TLSH:	2AC33BF1A8025C0AE123C976B1FB661399D051ED42283B2BF87D507DD978A20D5DD8EF
File Content Preview:	.R\{...M..Sx.).....i.E.....&.....?.....l.....* ..* ..*_fh.*.E.....n.w.....h.....8.....

File Icon



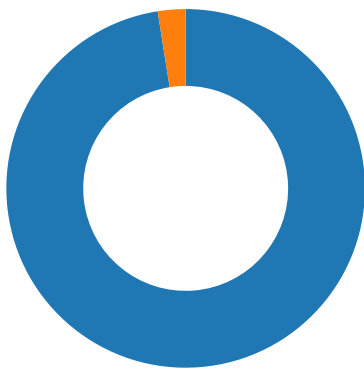
Icon Hash: d4dce0626664606c

Network Behavior							
Snort IDS Alerts							
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3182.162.143.5 6497034432404312 03/17/23-09:07:17.288903	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49703	443	192.168.2.3	182.162.143.56
192.168.2.391.121.146.47 4970080802404344 03/17/23-09:07:02.528103	TCP	2404344	ET CNC Feodo Tracker Reported CnC Server TCP group 23	49700	8080	192.168.2.3	91.121.146.47
192.168.2.3167.172.199.1 654970580802404308 03/17/23-09:07:29.350313	TCP	2404308	ET CNC Feodo Tracker Reported CnC Server TCP group 5	49705	8080	192.168.2.3	167.172.199.165
192.168.2.3213.239.212.5 497344432404320 03/17/23-09:10:04.212745	TCP	2404320	ET CNC Feodo Tracker Reported CnC Server TCP group 11	49734	443	192.168.2.3	213.239.212.5
192.168.2.3104.168.155.1 434971080802404302 03/17/23-09:07:42.102850	TCP	2404302	ET CNC Feodo Tracker Reported CnC Server TCP group 2	49710	8080	192.168.2.3	104.168.155.143
192.168.2.345.235.8.3049 73880802404324 03/17/23-09:10:10.312810	TCP	2404324	ET CNC Feodo Tracker Reported CnC Server TCP group 13	49738	8080	192.168.2.3	45.235.8.30
192.168.2.3206.189.28.19 94972680802404318 03/17/23-09:09:10.341885	TCP	2404318	ET CNC Feodo Tracker Reported CnC Server TCP group 10	49726	8080	192.168.2.3	206.189.28.199
192.168.2.366.228.32.314 970270802404330 03/17/23-09:07:12.052554	TCP	2404330	ET CNC Feodo Tracker Reported CnC Server TCP group 16	49702	7080	192.168.2.3	66.228.32.31
192.168.2.3119.59.103.15 24973980802404304 03/17/23-09:10:17.568030	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49739	8080	192.168.2.3	119.59.103.152

Network Port Distribution

Total Packets: 40

53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 09:06:19.534312010 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:19.534394026 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:19.534646988 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:19.537698030 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:19.537751913 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:20.159828901 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:20.160007000 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:20.164401054 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:20.164443016 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:20.164989948 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:20.213004112 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:20.386521101 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:20.386583090 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:20.762649059 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:20.762722969 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:20.762742996 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:20.762898922 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:20.762943029 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:20.806890011 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.062736034 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.062786102 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.062952042 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.062995911 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.063009977 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.063133955 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.063164949 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.063218117 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.063230991 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.063245058 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.063296080 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.063354015 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.063370943 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.063383102 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.063412905 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.103813887 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.103876114 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.150677919 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.362915039 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.362951040 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363008022 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363029957 CET	443	49698	203.26.41.131	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 09:06:21.363073111 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363110065 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.363176107 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363197088 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.363199949 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363213062 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363236904 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.363235950 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363260031 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363275051 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.363303900 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.363315105 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363334894 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363389969 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.363400936 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363451004 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363500118 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.363504887 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363522053 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.363615990 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.416321039 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.416353941 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.463228941 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.663800001 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.663820982 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.663991928 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.664041996 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664092064 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664103031 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664127111 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664144039 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.664163113 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664177895 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.664431095 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664453983 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664463043 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664505959 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.664524078 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664551020 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.664813042 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664827108 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.664968014 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.664999008 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.665168047 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.665178061 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.665246010 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.665268898 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.665285110 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.665541887 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.665594101 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.665637016 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.665654898 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.665671110 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.665848970 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.665937901 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.665970087 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.666254997 CET	443	49698	203.26.41.131	192.168.2.3
Mar 17, 2023 09:06:21.666331053 CET	49698	443	192.168.2.3	203.26.41.131
Mar 17, 2023 09:06:21.666347980 CET	443	49698	203.26.41.131	192.168.2.3

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 09:06:19.504734993 CET	57840	53	192.168.2.3	8.8.8.8
Mar 17, 2023 09:06:19.522384882 CET	53	57840	8.8.8.8	192.168.2.3

DNS Queries								
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 17, 2023 09:06:19.504734993 CET	192.168.2.3	8.8.8.8	0xbfe2	Standard query (0)	penshorn.org	A (IP address)	IN (0x0001)	false

DNS Answers										
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 17, 2023 09:06:19.522384882 CET	8.8.8.8	192.168.2.3	0xbfe2	No error (0)	penshorn.org		203.26.41.131	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph										
- penshorn.org 182.162.143.56										

Statistics

Behavior

- ONENOTE.EXE
- wscript.exe
- regsvr32.exe
- regsvr32.exe
- regsvr32.exe
- ONENOTEM.EXE

Click to jump to process

System Behavior	
Analysis Process: ONENOTE.EXE PID: 5812, Parent PID: 3452	
General	
Target ID:	0
Start time:	09:05:52
Start date:	17/03/2023
Path:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE

Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\OMICS_Online_1.one
Imagebase:	0x13d0000
File size:	1676072 bytes
MD5 hash:	8D7E99CB358318E1F38803C9E6B67867
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
File Path	Access		Attributes	Options	Completion	Count	Source Address	Symbol
File Path					Completion	Count	Source Address	Symbol
Old File Path	New File Path			Completion	Count	Source Address	Symbol	
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
File Path	Offset		Length	Completion	Count	Source Address	Symbol	

Registry Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
Key Path			Completion	Count	Source Address	Symbol		
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol	
Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 5592, Parent PID: 5812								
General								
Target ID:	10							
Start time:	09:06:17							
Start date:	17/03/2023							
Path:	C:\Windows\SysWOW64\wscript.exe							
Wow64 process (32bit):	true							
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\AppData\Local\Temp\click.wsf"							
Imagebase:	0x13c0000							
File size:	147456 bytes							
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884							
Has elevated privileges:	true							
Has administrator privileges:	true							
Programmed in:	C, C++ or other language							
Yara matches:	- Rule: WEBSHELL_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 0000000A.00000003.349816910.0000000005E26000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp - Rule: WEBSHELL_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 0000000A.00000003.350703760.0000000005E94000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp							
Reputation:	high							

File Activities							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
File Written							

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\click.wsf	0	9	62 61 64 75 6d 20 74 73 73	badum tss	success or wait	1	6F749601	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: regsvr32.exe PID: 5304, Parent PID: 5592

General

Target ID:	11
Start time:	09:06:22
Start date:	17/03/2023
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\regsvr32.exe" "C:\Users\user\AppData\Local\Temp\rad98E2D.tmp.dll
Imagebase:	0x7ff745070000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rad98E2D.tmp.dll	unknown	64	success or wait	1	F51909	ReadFile
C:\Users\user\AppData\Local\Temp\rad98E2D.tmp.dll	unknown	248	success or wait	1	F51942	ReadFile

Analysis Process: regsvr32.exe PID: 4884, Parent PID: 5304

General

Target ID:	12
Start time:	09:06:22
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\rad98E2D.tmp.dll"
Imagebase:	0x7ff659210000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.331944852.0000000000D00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.332682576.0000000000D31000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: regsvr32.exe PID: 5328, Parent PID: 4884

General

Target ID:	13
Start time:	09:06:25
Start date:	17/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\STfmTSAbIwWdRVZ\mmatLGgYnezL.dll"
Imagebase:	0x7ff659210000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.830903189.0000000000E21000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.829181595.0000000000CE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 0000000D.00000002.829371998.0000000000D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: ONENOTEM.EXE PID: 1920, Parent PID: 5812

General

Target ID:	14
Start time:	09:06:31
Start date:	17/03/2023
Path:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE
Wow64 process (32bit):	true
Commandline:	/tsr
Imagebase:	0x140000
File size:	157872 bytes
MD5 hash:	DBCFA6F25577339B877D2305CAD3DEC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

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

Disassembly

 No disassembly