ID: 830538
Sample Name:
malware.malware
Cookbook: default.jbs
Time: 13:32:10
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000G.bin (copy)	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000H.bin (copy)	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000I.bin (copy)	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000J.bin (copy)	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000K.bin (copy)	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000M.bin (copy)	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000N.bin (copy)	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000O.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000P.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000Q.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000R.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000S.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000T.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000U.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000V.bin (copy)	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000010.bin (copy)	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000011.bin (copy)	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000012.bin (copy)	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000013.bin (copy)	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000014.bin (copy)	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000015.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000016.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000017.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000018.bin (copy)	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000019.bin (copy)	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001C.bin (copy)	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001D.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001E.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001F.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001G.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001H.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001I.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001J.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001K.bin (copy)	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001L.bin (copy)	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001M.bin (copy)	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001N.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001O.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001P.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001Q.bin (copy)	45
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001R.bin (copy)	45
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001T.bin (copy)	45
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001U.bin (copy)	46
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001V.bin (copy)	46
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000020.bin (copy)	46
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000021.bin (copy)	47
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000022.bin (copy)	47
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000023.bin (copy)	47
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000024.bin (copy)	48
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000025.bin (copy)	48
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000026.bin (copy)	48
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000027.bin (copy)	48
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000028.bin (copy)	49
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000029.bin (copy)	49
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002A.bin (copy)	49
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002B.bin (copy)	50
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002C.bin (copy)	50
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002D.bin (copy)	50
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002E.bin (copy)	51
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002F.bin (copy)	51
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002G.bin (copy)	51
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002H.bin (copy)	52
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002I.bin (copy)	52
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002J.bin (copy)	52
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002K.bin (copy)	53
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002L.bin (copy)	53
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002M.bin (copy)	53
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002N.bin (copy)	54
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002O.bin (copy)	54
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002P.bin (copy)	54
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002Q.bin (copy)	55
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002R.bin (copy)	55
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002S.bin (copy)	55
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002T.bin (copy)	55
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002U.bin (copy)	56
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002V.bin (copy)	56
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000030.bin (copy)	56

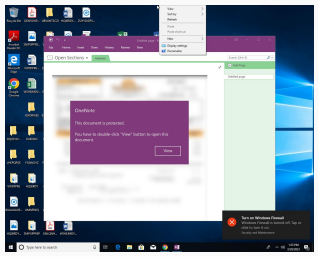
Windows Analysis Report

malware.one

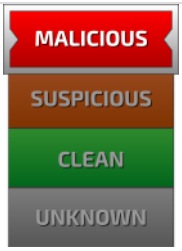
Overview

General Information

Sample Name:	malware.one (renamed file extension from malware to one, renamed because original name is a hash value)
Original Sample Name:	malware.malwa..
Analysis ID:	830538
MD5:	80a381f900f30…
SHA1:	1acac99bb134…
SHA256:	59ecfd5be8b5d..
Infos:	



Detection



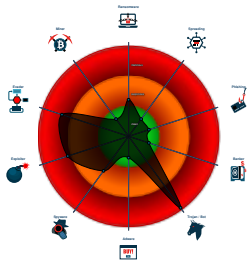
Emotet

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 networ…
- 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…
- Yara signature match
- Contains functionality to check if a d…
- Contains functionality to query local…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- ONENOTE.EXE (PID: 1760 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\malware.one MD5: 8D7E99CB358318E1F38803C9E6B67867)
  - wscript.exe (PID: 5836 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\AppData\Local\Temp\click.wsf" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - regsvr32.exe (PID: 5188 cmdline: C:\Windows\System32\regsvr32.exe "C:\Users\user\AppData\Local\Temp\rad66B18.tmp.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
      - regsvr32.exe (PID: 5268 cmdline: "C:\Users\user\AppData\Local\Temp\rad66B18.tmp.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
        - regsvr32.exe (PID: 4420 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JMgyzwrCUAZpIA\OfEg.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - ONENOTEM.EXE (PID: 848 cmdline: /tsr MD5: DBCFA6F25577339B877D2305CAD3DEC3)
- ONENOTEM.EXE (PID: 6140 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE" /tsr MD5: DBCFA6F25577339B877D2305CAD3DEC3)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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-1http://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/http://ropgadget.com/posts/defensive_pcres.htmlhttps://adalogics.com/blog/the-state-of-advanced-code-injectionshttps://asec.ahnlab.com/en/33600/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet

Malware Configuration

Threatname: Emotet


```
{
  "C2 list": [
    "138.197.14.67:8080",
    "193.194.92.175:443",
    "93.84.115.205:7080",
    "115.178.55.22:80",
    "218.38.121.17:443",
    "186.250.48.5:443",
    "174.138.33.49:7080",
    "83.229.80.93:8080",
    "175.126.176.79:8080",
    "209.239.112.82:8080",
    "37.59.103.148:8080",
    "185.148.169.10:8080",
    "82.98.180.154:7080",
    "103.224.241.74:8080",
    "103.41.204.169:8080",
    "202.28.34.99:8080",
    "198.199.70.22:8080",
    "62.171.178.147:8080",
    "37.44.244.177:8080",
    "195.77.239.39:8080",
    "159.65.135.222:7080",
    "139.196.72.155:8080",
    "46.101.98.60:8080",
    "85.214.67.203:8080",
    "54.37.228.122:443",
    "93.104.209.107:8080",
    "178.62.112.199:8080",
    "103.85.95.4:8080",
    "139.59.80.108:8080",
    "64.227.55.231:8080",
    "160.16.143.191:8080",
    "87.106.97.83:7080",
    "128.199.217.206:443",
    "178.238.225.252:8080",
    "128.199.242.164:8080",
    "85.25.120.45:8080",
    "103.254.12.236:7080",
    "114.79.130.68:443",
    "104.244.79.94:443",
    "78.47.204.80:443"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0Xqm08QAUAJA=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCWu6mj8QANAJA="
  ]
}
```


Yara Signatures

Initial Sample

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

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\malware.one	JoeSecurity_MalOneNote	Yara detected Malicious OneNote	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.572181479.00000000006EA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3	Yara detected Emotet	Joe Security	
0000000F.00000002.573776336.0000000002030000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000003.386000568.0000000005771000.00000004.00000020.00020000.00000000.sdmp	WEBSHELL_asp_generic	Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file	Arnim Rupp	• 0x73fe:$asp_gen_obf1: "+" • 0x742e:$asp_gen_obf1: "+" • 0x10ff2:$tagasp_classid1: 72C24DD5-D70A-438B-8A42-98424B88AFB8 • 0x11112:$tagasp_classid1: 72C24DD5-D70A-438B-8A42-98424B88AFB8 • 0x7720:$jsp4: public • 0x7a6c:$jsp4: public • 0x7212:$asp_input1: request • 0x7cee:$asp_input1: request • 0x7d30:$asp_input1: request • 0x7e46:$asp_input1: request • 0x754c:$asp_payload11: wscript.shell • 0x7134:$asp_multi_payload_one1: createobject • 0x7222:$asp_multi_payload_one1: createobject • 0x729a:$asp_multi_payload_one1: createobject • 0x72f4:$asp_multi_payload_one1: createobject • 0x7530:$asp_multi_payload_one1: createobject • 0x7f44:$asp_multi_payload_one1: createobject • 0x7134:$asp_multi_payload_four1: createobject • 0x7222:$asp_multi_payload_four1: createobject • 0x729a:$asp_multi_payload_four1: createobject • 0x72f4:$asp_multi_payload_four1: createobject
0000000A.00000003.393189517.0000000005915000.00000004.00000020.00020000.00000000.sdmp	webshell_asp_obfuscated	ASP webshell obfuscated	Arnim Rupp	• 0x30d2:$tagasp_classid5: 0D43FE01-F093-11CF-8940-00A0C9054228 • 0xb38:$jsp4: public • 0xe84:$jsp4: public • 0x159a:$jsp4: public • 0x1e80:$jsp4: public • 0x21cc:$jsp4: public • 0x28e2:$jsp4: public • 0x964:$asp_payload11: wscript.shell • 0x1cac:$asp_payload11: wscript.shell • 0x54c:$asp_multi_payload_one1: createobject • 0x63a:$asp_multi_payload_one1: createobject • 0x6b2:$asp_multi_payload_one1: createobject • 0x70c:$asp_multi_payload_one1: createobject • 0x948:$asp_multi_payload_one1: createobject • 0x135c:$asp_multi_payload_one1: createobject • 0x1698:$asp_multi_payload_one1: createobject • 0x1894:$asp_multi_payload_one1: createobject • 0x1982:$asp_multi_payload_one1: createobject • 0x19fa:$asp_multi_payload_one1: createobject • 0x1a54:$asp_multi_payload_one1: createobject • 0x1c90:$asp_multi_payload_one1: createobject
0000000A.00000003.393189517.0000000005915000.00000004.00000020.00020000.00000000.sdmp	WEBSHELL_asp_generic	Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file	Arnim Rupp	• 0x816:$asp_gen_obf1: "+" • 0x846:$asp_gen_obf1: "+" • 0x1b5e:$asp_gen_obf1: "+" • 0x1b8e:$asp_gen_obf1: "+" • 0x30d2:$tagasp_classid5: 0D43FE01-F093-11CF-8940-00A0C9054228 • 0xb38:$jsp4: public • 0xe84:$jsp4: public • 0x159a:$jsp4: public • 0x1e80:$jsp4: public • 0x21cc:$jsp4: public • 0x28e2:$jsp4: public • 0x62a:$asp_input1: request • 0x1106:$asp_input1: request • 0x1148:$asp_input1: request • 0x125e:$asp_input1: request • 0x1972:$asp_input1: request • 0x244e:$asp_input1: request • 0x2490:$asp_input1: request • 0x25a6:$asp_input1: request • 0x964:$asp_payload11: wscript.shell • 0x1cac:$asp_payload11: wscript.shell

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.regsvr32.exe.2030000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
15.2.regsvr32.exe.2030000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
14.2.regsvr32.exe.e00000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
14.2.regsvr32.exe.e00000.0.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 DNS Query for .su TLD (Soviet Union) Often Malware Related - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.857840532014169 03/20/23-13:33:35.045170
SID:	2014169
Source Port:	57840
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET CNC Feodo Tracker Reported CnC Server TCP group 4 - Source IP: 192.168.2.3 - Destination IP: 138.197.14.67

Timestamp:	192.168.2.3138.197.14.674970580802404306 03/20/23-13:34:39.278063
SID:	2404306
Source Port:	49705
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 24 - Source IP: 192.168.2.3 - Destination IP: 93.84.115.205

Timestamp:	192.168.2.393.84.115.2054970870802404346 03/20/23-13:35:12.925218
SID:	2404346
Source Port:	49708
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: 115.178.55.22

Timestamp:	192.168.2.3115.178.55.2249709802404304 03/20/23-13:35:29.032640
SID:	2404304
Source Port:	49709
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 12 - Source IP: 192.168.2.3 - Destination IP: 218.38.121.17

Timestamp:	192.168.2.3218.38.121.17497104432404322 03/20/23-13:35:36.187246
SID:	2404322
Source Port:	49710
Destination Port:	443

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

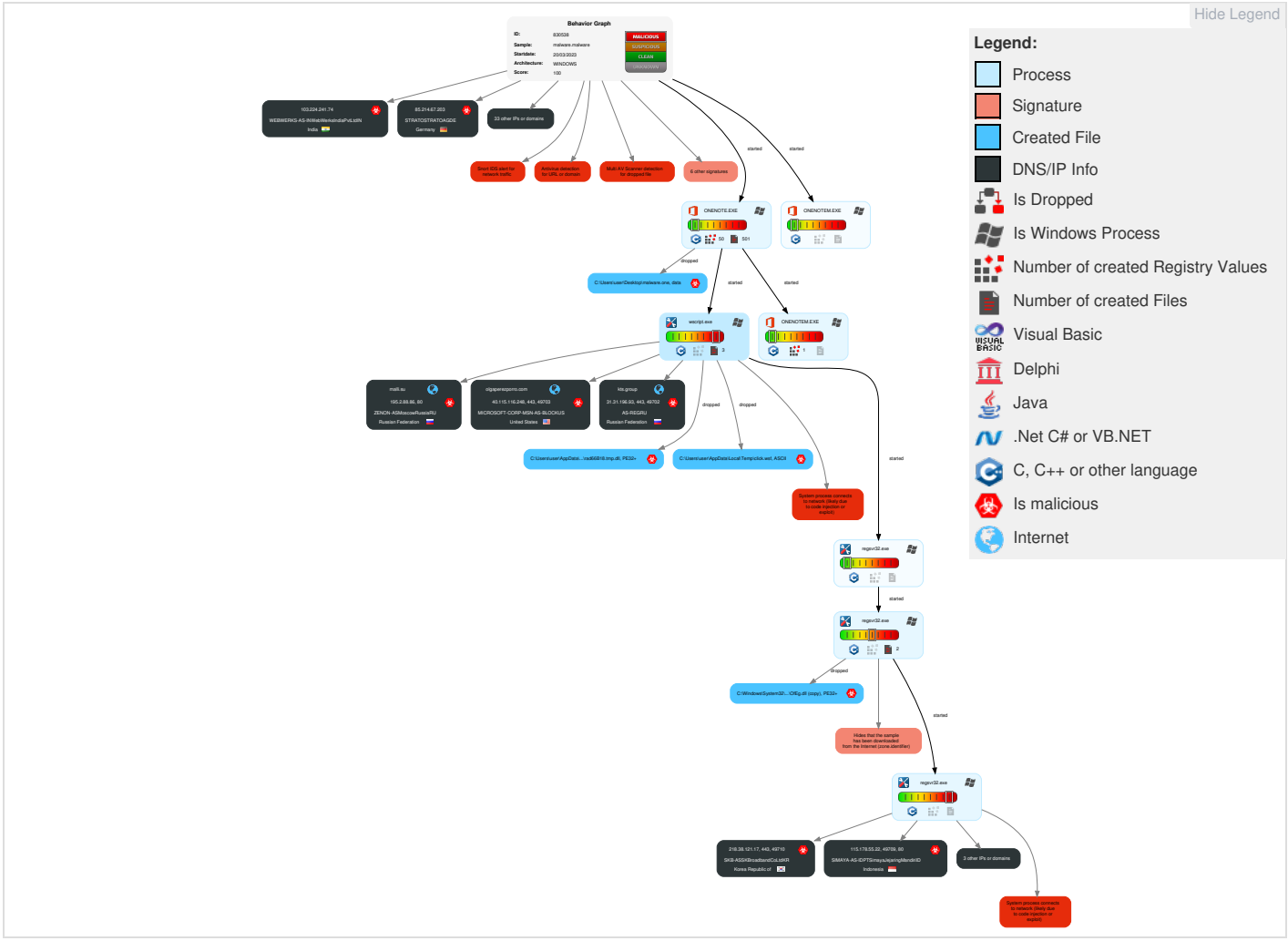
Yara detected Malicious OneNote

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Scripting	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	3 5 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Regsvr32	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

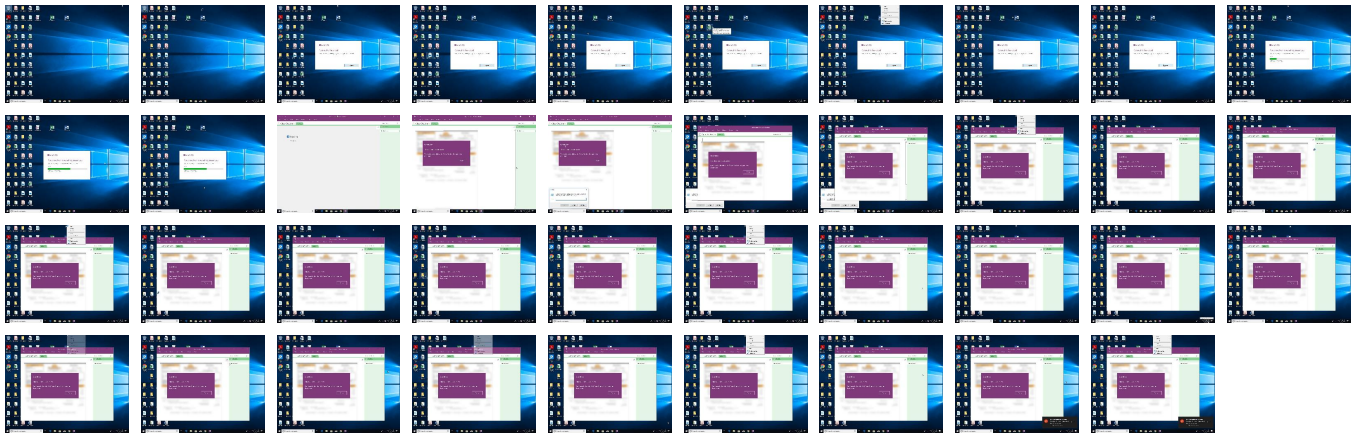
Behavior Graph

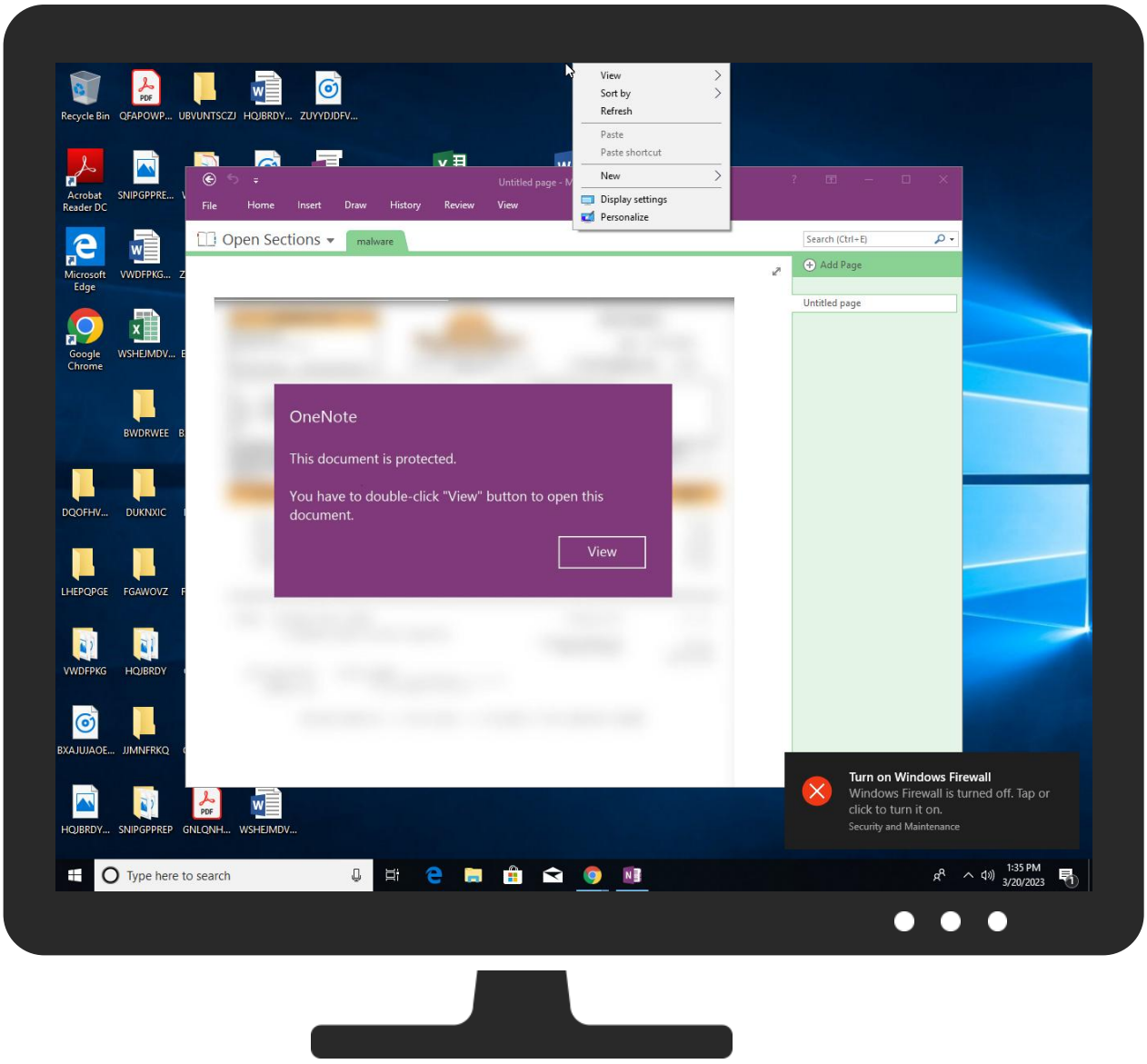


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
malware.one	29%	ReversingLabs	Win32.Trojan.Worefflint	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\rad66B18.tmp.dll	79%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\JMgyzwrCUAZpIA\OfEg.dll (copy)	79%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.regsvr32.exe.e00000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
15.2.regsvr32.exe.2030000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://115.178.55.22:80/	0%	URL Reputation	safe	
http://https://193.194.92.175/	0%	Avira URL Cloud	safe	
http://https://115.178.55.22:80/tcbvserkm/kigv/rbwmds/rw	100%	Avira URL Cloud	malware	
http://uk-eurodom.co	0%	Avira URL Cloud	safe	
http://https://218.38.121.17/tcbvserkm/kigv/rbwmds/	100%	Avira URL Cloud	malware	
http://https://115.178.55.22:80/tcbvserkm/kigv/rbwmds/0	100%	Avira URL Cloud	malware	
http://https://218.38.121.17:443/tcbvserkm/kigv/rbwmds/	100%	Avira URL Cloud	malware	
http://https://138.197.14.67:8080/tcbvserkm/kigv/rbwmds/	100%	Avira URL Cloud	malware	
http://https://218.38.121.17/	0%	URL Reputation	safe	
http://https://218.38.121.17/tcbvserkm/kigv/rbwmds/T(	100%	Avira URL Cloud	malware	
http://https://olgaperezporro.com/js/ExGBiCZdkkw0GBAuHNZ/6	100%	Avira URL Cloud	malware	
http://https://218.38.121.17/tcbvserkm/kigv/rbwmds/wn	100%	Avira URL Cloud	malware	
http://https://thailandcan.org/assets/ulRa/P	100%	Avira URL Cloud	malware	
http://https://4fly.su:443/search/OfGA/wM	100%	Avira URL Cloud	malware	
http://https://olgaperezporro.com/js/ExGBiCZdkkw0GBAuHNZ/vM	100%	Avira URL Cloud	malware	
http://https://olgaperezporro.com/js/ExGBiCZdkkw0GBAuHNZ/	100%	Avira URL Cloud	malware	
http://semedacara.com.br/ava/ahhz/	100%	Avira URL Cloud	malware	
http://staging-demo.com/public_html/wTG/	100%	Avira URL Cloud	malware	
http://malli.su:80/img/PXN5J/	100%	Avira URL Cloud	malware	
http://1it.fit	0%	Avira URL Cloud	safe	
http://https://115.178.55.22:80/tcbvserkm/kigv/rbwmds/	100%	Avira URL Cloud	malware	
http://https://93.84.115.205:7080/T	100%	Avira URL Cloud	malware	
http://https://olgaperezporro.com/	100%	Avira URL Cloud	malware	
http://https://115.178.55.22:80/l	100%	Avira URL Cloud	malware	
http://www.polarkh-crewing.com/aboutu	0%	Avira URL Cloud	safe	
http://efirma.sg	0%	Avira URL Cloud	safe	
http://https://198.38.121.17/	0%	Avira URL Cloud	safe	
http://uk-eurodom.com/bitrix/9HrzPY66D1F/	100%	Avira URL Cloud	malware	
http://malli.s4	0%	Avira URL Cloud	safe	
http://https://olgaperezporro.com	100%	Avira URL Cloud	malware	
http://https://olgaperezporro.com/js/ExGBiCZdkkw0GBAuHNZ/esqu	100%	Avira URL Cloud	malware	
http://https://138.197.14.67:8080/tcbvserkm/kigv/rbwmds/a	100%	Avira URL Cloud	malware	
http://https://4fly.su:443/search/OfGA/	100%	Avira URL Cloud	malware	
http://staging-demo.com/public_html/wTG/xM	100%	Avira URL Cloud	phishing	
http://semedacara.com.br/ava/ahhz/yM	100%	Avira URL Cloud	malware	
http://https://kts.group/35ccbf2003/jKgk8/uM	100%	Avira URL Cloud	malware	
http://1it.fit/site_vp/4PwK3s6Bf9K7TEA/	100%	Avira URL Cloud	malware	
http://efirma.sglwebs.com/img/2mmLuv7SxhhYFRVn/8	100%	Avira URL Cloud	malware	
http://https://4fly.su:443/search/OfGA/ata	100%	Avira URL Cloud	malware	
http://https://kts.group	100%	Avira URL Cloud	malware	
http://staging-demo.com/public_html/wT	100%	Avira URL Cloud	phishing	
http://uk-eurodom.com/bitrix/9HrzPY66D1F/24Q	100%	Avira URL Cloud	malware	
http://efirma.sglwebs.com/img/2mmLuv	0%	Avira URL Cloud	safe	
http://https://kts.group/35ccbf2003/jKgk8/	100%	Avira URL Cloud	malware	
http://semedacara.com.br/ava/a	0%	Avira URL Cloud	safe	
http://https://thailandcan.org/assets/ulRa/	100%	Avira URL Cloud	malware	
http://malli.su:80/img/PXN5J/tM	100%	Avira URL Cloud	malware	
http://1it.fit/site_vp/4PwK3s6Bf9K7TEA/EC24%	100%	Avira URL Cloud	malware	
http://https://138.197.14.67:8080/	100%	Avira URL Cloud	malware	
http://efirma.sglwebs.com/img/2mmLuv7SxhhYFRVn/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
malli.su	195.2.88.86	true	true		unknown
kts.group	31.31.196.93	true	true		unknown
c-0001.c-msedge.net	13.107.4.50	true	false		unknown
olgaperezporro.com	40.115.116.248	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://olgaperezporro.com/js/ExGBiCZdkkw0GBAuHNZ/	true	• Avira URL Cloud: malware	unknown
http://https://kts.group/35ccbf2003/jKgk8/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://218.38.121.17:443/tcbvserkm/kigv/rbwmds/	regsvr32.exe, 0000000F.00000002.57218147.0000000000788000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://218.38.121.17/tcbvserkm/kigv/rbwmds/	regsvr32.exe, 0000000F.00000002.57218147.0000000000788000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000F.00000002.572181479.000000000077A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://193.194.92.175/	regsvr32.exe, 0000000F.00000002.57218147.0000000000788000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://uk-eurodom.co	wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394701314.00000000058A2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://115.178.55.22:80/tcbvserkm/kigv/rbwmds/0	regsvr32.exe, 0000000F.00000002.57218147.00000000007C3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://hypernite.5v.pl/vendor/hvlVMsl9jGafBBTa/	wscript.exe, wscript.exe, 0000000A.00000002.394746955.00000000058EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379175657.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388681276.00000000055AA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388352589.00000000057EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.384898008.000000000561F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382616382.00000000005541000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389287393.0000000005904000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379710983.00000000005345000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381147538.0000000005534000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.383882868.000000000566D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388670695.000000000576D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393765942.00000000056CF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380261353.00000000054B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379756871.00000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.376996553.0000000002DB5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379986129.00000000053BD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381405615.00000000005558000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380405706.000000000545A000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://staging-demo.com/public_html/wTG/	wscript.exe, wscript.exe, 0000000A.00000003.379175657.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388681276.00000000055AA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388352589.00000000057EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.384898008.000000000561F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382616382.0000000005541000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389287393.0000000005904000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379710983.0000000005345000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381147538.0000000005534000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.383882868.000000000566D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388670695.000000000576D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393765942.00000000056CF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380261353.00000000054B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379756871.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.376996553.0000000002DB5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379986129.00000000053BD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381405615.0000000005558000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380405706.000000000545A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382922576.000000000564F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://115.178.55.22:80/tcbvserkm/kigv/rbwmds/rw	regsvr32.exe, 0000000F.00000002.57218147 9.00000000007C3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://semedacara.com.br/ava/ahhz/	wscript.exe, 0000000A.00000003.388829355 .000000000589B000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.380405706.000000000545A000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382922576 .000000000564F000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.381734544.0000000005502000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.391066699 .00000000059A5000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.380726054.0000000005502000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381193898 .00000000054BF000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.389552765.00000000058D1000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381193898 .00000000054D6000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.381071407.0000000005518000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.391066699 .00000000059A7000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.386373392.0000000005794000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380565209 .00000000054D6000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.384344893.000000000569B000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380087000 .0000000005498000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.385194824.00000000056D8000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393045342 .00000000056E6000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.380087000.000000000545A000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381296278 .0000000005577000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.385805896.000000000575C000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.378645005 .0000000002DF1000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://malli.su:80/img/PXN5J/	wscript.exe, wscript.exe, 0000000A.00000003.379175657.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388681276.00000000055AA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388352589.00000000057EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.384898008.000000000561F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382616382.0000000005541000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389287393.0000000005904000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379710983.0000000005345000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381147538.0000000005534000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.383882868.000000000566D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388670695.000000000576D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393765942.00000000056CF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380261353.00000000054B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379756871.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.376996553.0000000002DB5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379986129.00000000053BD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381405615.0000000005558000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388829355.0000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380405706.000000000545A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.392433354.0000000003324000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://138.197.14.67:8080/tcbvserkm/kigv/rbwmds/	regsvr32.exe, 0000000F.00000002.572181479.00000000006EA000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000F.00000002.572181479.0000000000762000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://218.38.121.17/tcbvserkm/kigv/rbwmds/T(	regsvr32.exe, 0000000F.00000002.572181479.00000000007C3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://4fly.su:443/search/OfGA/wM	wscript.exe, 0000000A.00000003.392112546.0000000004FDB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://thailandcan.org/assets/uIRa/P	wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388916629.00000000058A4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394717076.00000000058AB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://olgaperezporro.com/js/ExGBiCZdkkw0GBAuHNZ/vM	wscript.exe, 0000000A.00000003.392112546.0000000004FDB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://218.38.121.17/tcbvserkm/kigv/rbwmds/wn	regsvr32.exe, 0000000F.00000002.572181479.0000000000788000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://olgaperezporro.com/js/ExGBiCZdkkw0GBAuHNZ/6	wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.386373392.0000000005794000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.385630751.000000000578C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387429953.00000000057B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394545937.00000000057CA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387506954.00000000057C2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://115.178.55.22:80/	regsvr32.exe, 0000000F.00000002.572181479.0000000000788000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://1it.fit	wscript.exe, 0000000A.00000003.389552765.00000000058D1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389268464.00000000058D1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394733751.00000000058D2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://115.178.55.22:80/tcbvserkm/kigv/rbwmds/	regsvr32.exe, 0000000F.00000002.572181479.0000000000788000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://93.84.115.205:7080/T	regsvr32.exe, 0000000F.00000002.572181479.0000000000788000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://olgaperezporro.com/	wscript.exe, 0000000A.00000003.375930591.0000000005A12000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393332313.0000000005A5E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.395019547.0000000005A20000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://115.178.55.22:80/l	regsvr32.exe, 0000000F.00000002.572181479.0000000000788000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://uk-eurodom.com/bitrix/9HrzPY66D1F/	wscript.exe, wscript.exe, 0000000A.00000002.394746955.00000000058EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379175657.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388681276.00000000055AA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388352589.00000000057EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.384898008.000000000561F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382616382.0000000005541000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389287393.0000000005904000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379710983.0000000005345000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394765226.0000000005917000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381147538.0000000005534000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.383882868.000000000566D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388670695.000000000576D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393765942.00000000056CF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380261353.00000000054B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379756871.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379986129.00000000053BD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381405615.0000000005558000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380405706.000000000545A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://olgaperezporro.com	wscript.exe, 0000000A.00000003.392888867.0000000004FD2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.392584081.0000000004FB7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394237064.0000000004FD3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.392354536.0000000004FB4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.392777257.0000000004FCC000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.392625530.0000000004FBD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.392754360.0000000004FC8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.392789218.0000000004FCF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://efirma.sg	wscript.exe, 0000000A.00000003.389552765.00000000058D1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389268464.00000000058D1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394733751.00000000058D2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.polarkh-crewing.com/aboutu	wscript.exe, 0000000A.00000003.388681276.00000000055AA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382444301.00000000055A3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.386310650.00000000055A9000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382820492.00000000055A3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394355887.00000000055AB000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.383863308.00000000055A3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://198.38.121.17/	regsvr32.exe, 0000000F.00000002.572181479.000000000073C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://malli.s4	wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394701314.00000000058A2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://olgaperezporro.com/js/ExGBiCZdkkw0GBAuHNZ/esqu	wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.386373392.0000000005794000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.385630751.000000000578C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387429953.00000000057B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394545937.00000000057CA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387506954.00000000057C2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://kts.group/35ccbf2003/jKgk8/uM	wscript.exe, 0000000A.00000003.392112546.0000000004FDB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://138.197.14.67:8080/tcbvserkm/kigv/rbwmds/a	regsvr32.exe, 0000000F.00000002.572181479.00000000006EA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://staging-demo.com/public_html/wTG/xM	wscript.exe, 0000000A.00000003.392112546.0000000004FDB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://4fly.su:443/search/OfGA/	wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380405706.000000000545A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382922576.000000000564F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381734544.0000000005502000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.391066699.00000000059A5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380726054.0000000005502000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381193898.00000000054BF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389552765.00000000058D1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381193898.00000000054D6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381071407.0000000005518000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.391066699.00000000059A7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.386373392.0000000005794000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380565209.00000000054D6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.384344893.000000000569B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380087000.0000000005498000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.385194824.00000000056D8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393045342.00000000056E6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380087000.000000000545A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381296278.0000000005577000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.385805896.000000000575C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.378645005.0000000002DF1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

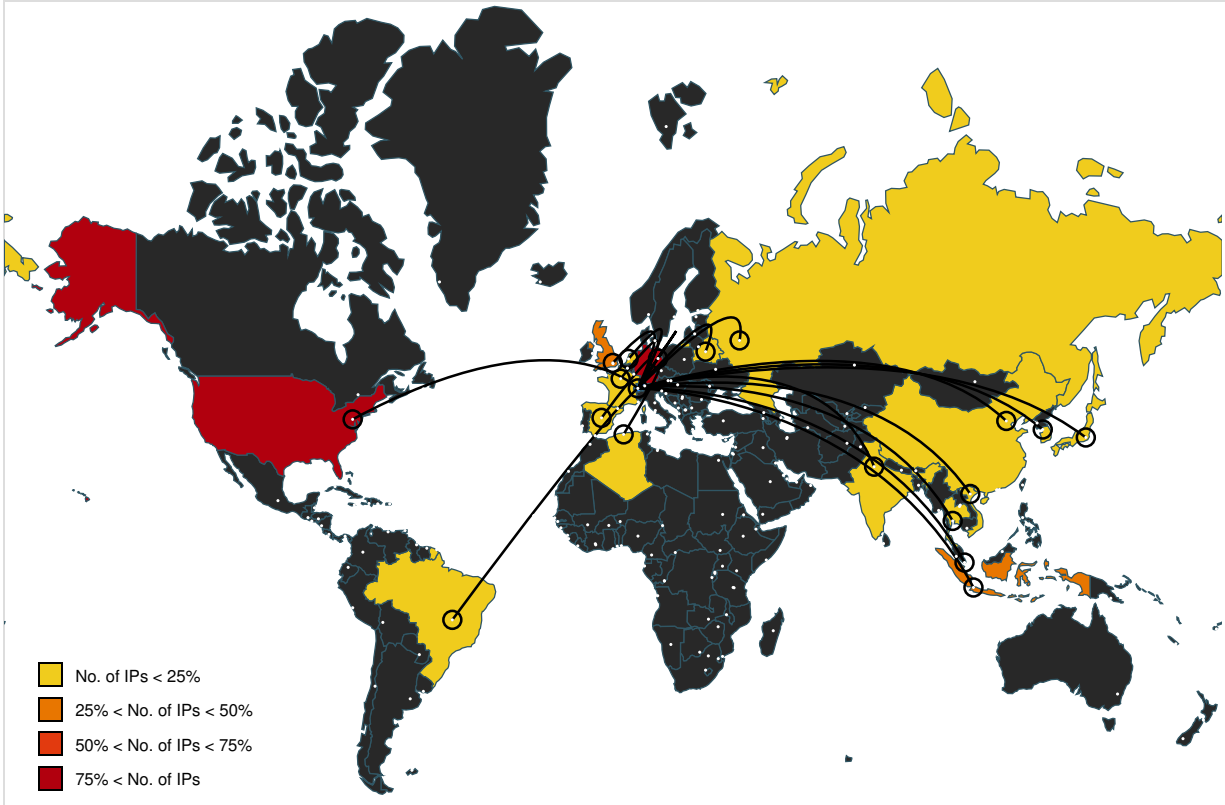
Name	Source	Malicious	Antivirus Detection	Reputation
http://1it.fit/site_vp/4PwK3s6Bf9K7TEA/	wscript.exe, 0000000A.00000003.388681276.00000000055AA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388352589.00000000057EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.384898008.000000000561F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382616382.0000000005541000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389287393.0000000005904000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379710983.0000000005345000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394765226.0000000005917000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381147538.0000000005534000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.383882868.000000000566D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388670695.000000000576D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393765942.00000000056CF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380261353.00000000054B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379756871.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379986129.00000000053BD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381405615.0000000005558000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380405706.000000000545A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382922576.000000000564F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381734544.0000000005502000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.391066699.00000000059A5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://semedacara.com.br/ava/ahhz/yM	wscript.exe, 0000000A.00000003.392112546.0000000004FDB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://efirma.sglwebs.com/img/2mmLuv7SxhhYFRVn/8	wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.386373392.0000000005794000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.385630751.000000000578C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387429953.00000000057B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394545937.00000000057CA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387506954.00000000057C2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://4fly.su:443/search/OfGA/ata	wscript.exe, 0000000A.00000003.379175657.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379756871.00000000053A3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380055179.00000000053A3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379248511.0000000005397000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394303780.00000000053A9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://kts.group	wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394701314.00000000058A2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://staging-demo.com/public_html/wT	wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394701314.00000000058A2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://hypernite.5v.pl/vendor/hvlVMsl9jGafBBTa/zM	wscript.exe, 0000000A.00000003.392112546.0000000004FDB000.00000004.00000020.00020000.00000000.sdmp	false		high
http://efirma.sglwebs.com/img/2mmLuv	wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394701314.00000000058A2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://thailandcan.org/assets/ulRa/	wscript.exe, wscript.exe, 0000000A.00000002.394746955.00000000058EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379175657.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388681276.00000000055AA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388352589.00000000057EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.384898008.000000000561F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382616382.0000000005541000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389287393.0000000005904000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379710983.0000000005345000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394765226.0000000005917000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381147538.0000000005534000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.383882868.000000000566D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388670695.000000000576D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393765942.00000000056CF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380261353.00000000054B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379756871.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379986129.00000000053BD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381405615.0000000005558000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380405706.000000000545A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://218.38.121.17/	regsvr32.exe, 0000000F.00000002.572181479.0000000000788000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://hypernite.5v.pl/vendo	wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394701314.00000000058A2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://malli.su:80/img/PXN5J/tM	wscript.exe, 0000000A.00000003.392112546.0000000004FDB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://uk-eurodom.com/bitrix/9HrzPY66D1F/24Q	wscript.exe, 0000000A.00000003.381296278.0000000005577000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381439650.000000000557E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382616382.000000000558C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394341142.000000000558C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://semedacara.com.br/ava/a	wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394701314.00000000058A2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://138.197.14.67:8080/	regsvr32.exe, 0000000F.00000002.572181479.00000000006EA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://hypernite.5v.pl/vendor/hvlVMsI9jGafBBTa/cw1122	wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.386373392.0000000005794000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.385630751.000000000578C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387429953.00000000057B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394545937.00000000057CA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387506954.00000000057C2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://1it.fit/site_vp/4PwK3s6Bf9K7TEA/EC24%	wscript.exe, 0000000A.00000003.381296278.0000000005577000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381439650.000000000557E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382616382.000000000558C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.394341142.000000000558C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://efirma.sglwebs.com/img/2mmLuv7SxhhYFRVn/	wscript.exe, wscript.exe, 0000000A.00000002.394746955.00000000058EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379175657.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388681276.00000000055AA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388352589.00000000057EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.384898008.000000000561F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.382616382.0000000005541000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.387365837.000000000579E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.389287393.0000000005904000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379710983.0000000005345000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381147538.0000000005534000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.383882868.000000000566D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388670695.000000000576D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.393765942.00000000056CF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380261353.00000000054B3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379756871.0000000005359000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.376996553.0000000002DB5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.379986129.00000000053BD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.381405615.0000000005558000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.388829355.000000000589B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.380405706.000000000545A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.194.92.175	unknown	Algeria		3208	ARNDZ	true
93.84.115.205	unknown	Belarus		6697	BELPAK-ASBELPAKBY	true
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
160.16.143.191	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
83.229.80.93	unknown	United Kingdom		8513	SKYVISIONGB	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
198.199.70.22	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
159.65.135.222	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
186.250.48.5	unknown	Brazil		262807	RedfoxTelecomunicacoesLtdaBR	true
209.239.112.82	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
175.126.176.79	unknown	Korea Republic of		9523	MOKWON-AS-KRMokwonUniversityKR	true
37.59.103.148	unknown	France		16276	OVHFR	true
138.197.14.67	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
128.199.242.164	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
115.178.55.22	unknown	Indonesia		38783	SIMAYA-AS-IDPTSimayaJejaringMandiriID	true
178.238.225.252	unknown	Germany		51167	CONTABODE	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
46.101.98.60	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
82.98.180.154	unknown	Spain		42612	DINAHOSTING-ASES	true
114.79.130.68	unknown	India		45769	DVOIS-IND-VoisBroadbandPvtLtdIN	true
195.2.88.86	malli.su	Russian Federation		6903	ZENON-ASMoscowRussiaRU	true
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true
31.31.196.93	kts.group	Russian Federation		197695	AS-REGRU	true
202.28.34.99	unknown	Thailand		9562	MSU-TH-APMahasarakhamUniversityTH	true
87.106.97.83	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
103.254.12.236	unknown	Viet Nam		56151	DIGISTAR-VNDigiStarCompanyLimitedVN	true
103.85.95.4	unknown	Indonesia		136077	IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID	true
40.115.116.248	olgaperezporro.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
54.37.228.122	unknown	France		16276	OVHFR	true
218.38.121.17	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
185.148.169.10	unknown	Germany		44780	EVERSCALE-ASDE	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
139.59.80.108	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
104.244.79.94	unknown	United States		53667	PONYNETUS	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
64.227.55.231	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830538
Start date and time:	2023-03-20 13:32:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 34s
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:	malware.one (renamed file extension from malware to one, renamed because original name is a hash value)
Original Sample Name:	malware.malware
Detection:	MAL
Classification:	mal100.troj.expl.evad.winONE@12/696@3/43
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.9% (good quality ratio 79.1%) • Quality average: 77.4% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.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): 52.109.88.191, 20.126.106.131, 20.224.224.21, 13.107.4.50
- Excluded domains from analysis (whitelisted): fs.microsoft.com, prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, nexus.officeapps.live.com, ctldl.windowsupdate.com, officeclient.microsoft.com, wu-bg-shim.trafficmanager.net, 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.
- Report size getting too big, too many NtWriteFile calls found.
- VT rate limit hit for: malware.one

Simulations

Behavior and APIs

Time	Type	Description
13:33:48	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Send to OneNote.lnk
13:34:11	API Interceptor	2x Sleep call for process: wscript.exe modified
13:34:50	API Interceptor	4x Sleep call for process: regsvr32.exe modified

Time	Type	Description

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.....,.....I.....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$.Hg.z.d~...../q..C.....`...A[ W(.....9...GZ.;....I&?.....F...p?... .p.....{S.L4..v.+...7.T?.....p..`..&..9.....f...0+.L.....1.2b)..vX5L'.~....2vz.,E.Ni.{#...o..w.?.#.3 ..h.v<.S%.].tD@!Le.w.q.7.8....QW.FT.....hE.....Y...../.%Q...k...*.Y.n..v.A..../...>B..5\..-Ko.....O<.b.K.{.O.b...._.7...4.;%9N..K.X>.....kg-9..r.c.g.G|.*[.-...HT...",?.q...ad. ...7RE.....!f..#../....?.-.^.K.c^...+{.g.....]<..$.=.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):	3.110837479881124
Encrypted:	false
SSDEEP:	6:kKlAAry/7UN+SkQlPlEGYRMY9z+4KlDA3RUecZUt:JCvkPlE99SNxAhUext
MD5:	B382B63E355A94F9858E5B2B358E97A9
SHA1:	4809ACEF83D520EEA515162B05A52C3417752B49

SHA-256:	C6F9D731F3E1F52E924FB59741313C99E629067550A0A9001D602F7A684B1A1D
SHA-512:	686852AA263CE017FF812B121A0E391F99D491F2810371CA08D23E8563065AC24E7E0704948FF431A44444AF7012C8C2B8BD3D30AAF7E75BBB1452CD3F42E51E
Malicious:	false
Preview:	p..... .....2-.dk[..(..... .....).K.....&.....v...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.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\C41609EF-1ECD-4EEF-916A-7808B4AAB9B7

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):	5.352011512322313
Encrypted:	false
SSDEEP:	1536:J+C76gfYBIB9guw6LQ9DQl+zQxik4F77nXmvidlXRpE6Lhz67:4cQ9DQl+zrXgb
MD5:	E673D9934734A836E871EC298C700859
SHA1:	2BC4788E9D068A6B04DFA5A1EB7F2C86384B07F8
SHA-256:	4B21A2AA4ECDE1423635F3671C23A273F698A2D677342C3E980100E7065B4452
SHA-512:	8C247A4E227C9B19B00184D406E3550D377FC09DCA971285558B078C7037D0D8C93BE633221C7B8E72BD66B19BDA1123795E1BF7BE72DEB6F9907B50A54FB23
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2023-03-20T12:33:09">.. Build: 16.0.16310.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId" o:authentication="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:headerValue="Passport1.4 from-PP='{}&p='" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAuthorityU

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+LtoQ9jsUBsnwlDGThUe8ww2iJiGEjdKKnnE+Gh:V+Ltt5GwlDQhUe8ww2iJi7MKnnE+K
MD5:	995CEACAD563F849C4142B6A6F29F081
SHA1:	44CB3B867CD2917541B7D5AAED2F14F10FEBB0FD
SHA-256:	3691FB8C60EA1B827092F05FBB1807E34726016C6FF56698D7B81C44D519D22A
SHA-512:	3C8EFEB966B075D06D8344483352BF92C9292F9970C9377BE254EB355EFAF017916737AECCDC704B84D532B7229F9908951A6F2CC3FAD810791CAB224401AD3
Malicious:	false
Preview:	.PNG.....IHDR.....c.L.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....W...Gh...k.Hm..J.m....,X...Eh..%.n.....PHvy$%...[...R..l...(/..-..yl..Z.h..H!.../.|.y|w...7d3 s.s.=.{.s.g.6W.^..)..@..{..'O.LL.....c.^.6xS&O.,...J.(|?.....,.$.....@.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."!f.08hT..m. (..C.7n.....@....SVUU).F.).X\\....[j.U....xd..e...<.W.....=;0L78t+..Gw..-....].....C7.....K.w...._..g.....A.&M.$^.#.!....e.\.P.....;vD..@...Za.@*D..f...! .2w...4#.J..c....K}... .F.u.I.b.V2.k...5..`....*.....M..!.,.;.E..BZ....K..[7....5....,.....K...7+.6..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+wKkEOgx3PG92Eqt9LczFD
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$1.N"}4.....1:&F8..*.X.yL(..s.3.....~2.EL%.w.Uc.zJ...B..S..b.7o\|%..7..'.....N.|..Vi...q..uO,`/....\W{..y...&iI..|X&T.....-.....Z..o.~u..U....cF.M....O4}.....~.....:T..W._s...t..Dlb.$Pr././._4.b.....R.T$t..$.>hB. +.{.....m.w .Q...05..C.}...}.....?..h.....Y .8.6^t....}.y.%.....I=$..[.~..]..h..N.....*....SB.|....8..H....._...G...|.....;6YQ\|WO.o.}]..'.$..oE.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:	48:4gv2YZ4gWLpU9JcjREmXfFEV7NNkfKOgV60g0Z:KZgWLpSJcj+mPFGNkfngp
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-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[....;.'n...u.g..>X....o.]}...>...._..u.....5...2]....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;.....,.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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:o4KSpFN6Ud4c3p2Il1yavNr5spYVJzimlfZ: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..:I.D.S>I$A...I.....y.9...f.....3...Gh.....}_.o....n..A@.....A@...L...2... ..... .x...#. ....1f]9.[.....A@.....3 ....fE@x.YWN.....A@.....1..... .....Y..J.Y.N.....s"......./..rc.scuyyyu...\s....t.oi..j..lv.....Gr.#9%%%9%--....d.T...r...DH...6.....%U..A@.0.....rAD .....2.5.....L.R..=W...gZ.`o..-?.T.Cy.:...y.9..y.EE...v.....1..R.....1."..... `"...ss.....i.!.hY...Fj*....%.-.Gw...HJJr8..6...#.....!(.?P.(.....8(u.....*..OOO.....dgg....Q..=..c.y....A`S.@.....3.CC..GFfg. .I.I.COrJFFFNNV^nn^^.z..%..(...^.b$.....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..>..;..Ii.i.gv...DSd....I#...I.....)**,**...V..1 .F.'7....)..SSs..7..F...C.p....(*,.....(RG..B...I!.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:	48:4gv2YZ4gWLpU9JcjREmXfFEV7NNkfKOgV60g0Z:KZgWLpSJcj+mPFGNkfngp
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-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[....;.'n...u.g..>X....o.]}...>...._..u.....5...2]....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;.....,.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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/gKVp93jQvcv16kjOzbapFJBkjcMNBqmQzOG8qx1QKnse8T:JieMJzph13Evcv16RfapFLxMNBo8qxan
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.0.T....L~....af..Z.....O..4..>Ms..Js_.....5.E.d...Y....?\z.3..}.I..|?~...{.....s.z..Y.....E.X.6...c..u...y..W.j.....}...I.i.`.!-!-.....MKH.E.bi.d...b.X.)...X4 .vJ6-...;..+/.->Qyi.t...%.T..k;.U..y.C$[;..Gm.....v..*2..2..eee..."I..)...yy...III./..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.!.....>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.|=.....'%!y.....\.....MSn.i.....!...U.$0S .....Z.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:	48:4gv2YZ4gWLpU9JcjREmXfFEV7NNkfKOgV60g0Z:KZgWLpSJcj+mPFGNkfngp
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..TI.....V.v.PZ.-F...".k.pCQ.....#.../s>f..3s....<...=^'/.~.;.a....{>.g.....*o..6k..k....E....O....aQ.j....X&vG.....{u-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[....;'n...u.g..>X....o.]}...>...._..u.....5...2]....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;.....,.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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+7QJU0QbDQ883ASaoUV4hNgq1rsyhy: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.%...xaI.}...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...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....qI....XuI..]...N...wv\.M$..D...+...=.....?U....T..^<6../T*.{q.q..:....y..XL..I..z.d....G..b..g.G..b.....SM.{q.q$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:aerVlDRlewkXlrTa2c
MD5:	73E38124F94AD20A2F1571FBBE11AEEC
SHA1:	87FB8056DC7A0A3B70D51426771C4CCE2099CFE5
SHA-256:	A700B63B30CBBE5230CC5E977D651E178EA87E73EAB18C8D5FFB1362149ADDF7
SHA-512:	320FCE64DD6F975384BEC9267348CD5CD24A55B13BB09FEF1238C2216AD8ECABDCCC15601A079CE092ACFA4954829FFEB06FBB0631F6AE26E3A39E43C1020 8B
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...&..%.3I.....: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.....I.....,Y.{. .....g.1.0..I}.....<.....T..}....t.!x&)..[.7....4.5..{....n.<...#I...:.....r.wW~..zr..9k.^.]KR.*W.J.n.")....%0...)...Fbb5`4'.X..E.../.t.&,t(...@9....\$.....].P..jdU.....H;.$.'%}.I7.....y..$.. ...Z..4.Cm.u#&.%N..1..+..8....y...U.(.T.....}.I..5r}...!..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\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:uuT43eqJy2jEeSZE0onrAFAOpn5ytFfNrfIkBQTYz8ynth2EB:EugQeS+nrAFZ8tJNrfRQM4ynH2EB
MD5:	7CEB71F78A193F8C9F7FFDA5F81AEBD8
SHA1:	EEC1597705EFF1A527C246B86A71878185BA6B1B
SHA-256:	77911FF7AEAB8FCCAF36DE6E1183FFE1A6C27F77B5714EE780976CE5189E8FD0
SHA-512:	1D1AB19B64E1E2ABCA61AE78B3B50310B0A6CF19D2ECFCB4499D8D0BF68600B4D95BC0945EF9FF9B1D016ED61EAC518DCCA1A426F460317C07AD51E2E0479 48C
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.....k]s..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...I...{M..@..4555==-...!..f.....d...>i.%&&&%.u....f..[.....O`.....G..E6I.< ..3.k...',....Y...<.....u...{9.....S^^.q.<..^....2.bb.E`r...ey..... ..3.....Dg@L..a'.x&".O.Y..!e.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.....wvv:..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.LI.....>.....&....."...".....@.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:/06ULmwT2RqfILhmLy4tNpYGL0mvBQhTMHX4PCIVYm:s6USI2RqfGhmDrpYM0ofHX4aIVYm
MD5:	17E9FF9F735102231846936F0E2BAF1A
SHA1:	9EC1AE8A3AD55C48C02427D842D6E38DA85B5145
SHA-256:	DD1CA8DA90893E0B63ABFDD9E60CF2BF844B311964E9D9DDB855C21FCA156EBB
SHA-512:	71E690D6C87B09659296E6E6DDC8E3F91035DD80C5CE875FA557763E8138900C27FB492885291CEE203D65BCEE8C20C9C39E0590A5FD32B8A00BEB3E3F6D6E F
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.dI..I1G..$.".Fg.q... N.nt...3.w.w..~.v.O.....K.....A@.....A ..H.n.D;A@.....A@.....e.y ....1..P..xH.. ....e.9 ....1..P..xH.. ....e.9 ....1.@.$9..S....A@..4....^C..F..VR\\TT.....aHII1..... .VS..g..... .*....z..\|Ek.....<R../55+33;;;+..Y..WC..#...P..... ...s#0::.....522...,.v..D....._.....9.2N.L.'..F$.....e..!.... ...N...`1....G.....'&,f..f.X....!.lp.....I_.....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..2...F.GCC#...].=..C..n#...K+..MOO....."....d^2=.{....U.p.h%.%n...D.....XB..b..'"....?h.b.B\v..^Q^.UC.....Q...I.....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:k1hccap27HGVhY2Kn+A3RS+HG3dXrjmg26vh:k1hccewIhYxRmR5
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!...\.!.`pA.+....H.U..."Z..*U.. ..P.D.-.$..,,..$.g.....CB.l.....l.g.pc..Lf..~.=.~ ]S.....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.[> gP....C..G.H.....Osp...)..9x!...W.,..^....$r.p.sOJ.l..=.x.9s&:.....h.`..W"V..|.l{..72.....zv@.#.<...../....F\|...c...4.W....:uj@1...~.X.....^si....Z..I~.Q.<.....NAOq...+i`.)...$ L..gV.6#.....F$..hD.g.L-\..H._.u..]4.....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:	9AA4A6DD01D3B745D674721765F2BFCCAB584CA0603F222EDBE9A88190A2A57438041E7A3706CC0656A6ABB79AA18118319F210EFFE3DD917E7B94A6294BD34 6
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.KVfVfjFzJzVF.}i{.R..l..q..`I....e.'./.'.G.z.*I&>)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>.....]I..7.i...3....<.y.l]....SI>...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.=.....(!C.....?5..+...[...a.:U.K..C.....w.....+..r@.z.7..j..qB..B.....X}..=.fk...>^5[....n.z....wn....Z 4.._iWG.^..z6./]t.....dhM.9s...Gbo?...U.V..tj.....*&)Io.{q.G...A...l...i7...&....d.E]....#.W.x,.T...&Mz4+].4.$n..F..x...<.ppr.....,.i./..

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:IfGsPejaVZWzIZKpnFFt0HK5+2Y/SLopWR:IusPe278IZKpnzt0q5+qVR
MD5:	70DAF02EC717AB54452FA4C707BCAC74
SHA1:	30F46FAC5E96470848C5A948162CC12455A05154
SHA-256:	58469BA93EA36498FF9864EB54713A001C52106DE97804506D82EE24B816712B
SHA-512:	E599FDC22A32CFEDBB23EECEAE0B278EAB9A90959FE6ACB40E2B201E45A7C19261AAF529E7A0D9CAF2A9A4C64C7831343F3BC20810513990AD5D38A327415 64F
Malicious:	false
Preview:	.PNG.....IHDR.....IC.....sRGB.....gAMA.....a.....pHYs.....o.d...cIDATx^..S[Y..I...B..`...N....t.q..j...+LU.....O..sF.!.I...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.I^OOONN8)....\y....}...}}.}.Hy6.^.a.....\...!S....K..|>.....s.....I. .P...LFWW.I..RK..b.h.h .3.F..|..~.....e.aa.....0H...<.Y.a`..xA!...7.X....xd=.....h?o5.....Ay....?6.....*..tb.9.*j...S`](.,P...9.2j..?...z3wD.[.....L3.Ng2G|.....&..0 ZK1u8.H.2...Z../..P(....BA..aL|..a.Y:.....J...5^x..'.\..&S...L..U..;....<{..."..@x ....J.N...;....WIht.<..B.....!HM...&z&..6u..hF..G.D..B.....A.....n...GG...,..Q....X,`"....r.....3d.{o.(/.. .3.H...x:sX....h.8... ....r <..DB. ...y.N...o....5.....L&w....v....w..D.....!.a4...."8.U.|.0m.(..zR>..=.+.L.....e....Yd2.-Z.7..D"..pX.I.....e5qYa._&..3..J..++

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000J.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+mPFGNkfngp
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-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[....;.'n...u.g..>X....o.]}...>....._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;......_.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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\0000000K.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/zVJWedudPZZRdbvczHe2ftFJ0y8Ea5b2AELJj:x4FTnodRZ7c7LrabEaMAGp
MD5:	DB48555480A383CD1D4DD00E2BCFCF29
SHA1:	8060B6FE12175289F0A71F45B894030A0D9F1AB5
SHA-256:	807723D8F90A5BD41269A7A62817547026A117D666D5BEF454EB699C97CA3FA2
SHA-512:	2614C04686299CEE8D56577A1E836A26076D42E041C627177FDB295629F6A80190910947FA794A094C55A45C3D70725EEF29097118E523A38B50C9263C771A41
Malicious:	false
Preview:	.PNG.....IHDR.....gI.....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.....'L...g.UVVz.[.n)...Yqq...Y.f.)//_.I.W_}.,.....S^Z^Y..++.*..pF.....?...I.&...O,.k.d...~..w;Q.....7}1y.....e_.....=y._U....{..}.w.O..~.z.{.....W\q..".....^.h.....}p.+.>m...d...4...`a~Z^....me... ....:N]..1...g..y.f.....I..g.).....e[.....Z..RB.KrJ.....#...{..eff..v.[[<.n..?{.....SN9%...V.yE...s2.....e@Wz..I...B.r..<.-.=/t{.v.|..J.....,@.A.v...s`/.....6f....L?.z[T7..)S0.;c....\s..z-C .....v..}Y..{..j..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\0000000M.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:L6ousL3eslFAmjb89xK6YiSTwtw5dTA1W9lQ:GoFiUFAMbsxJYieZ5dGklQ
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....r.....: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.{.I..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.[`Uf.Y...>z\..x.B.h" \.}...`...|._.....G...hY.../..6>..Z...8^..k.E.5d#..a."....P.CR....OL.. U...qY.{.C.<~I=V..x.J..*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\0000000N.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/PMeaEf61lT6kCiFQCQq6zT
MD5:	3E9F7D399DF9CAD3669B7A5445EF7074
SHA1:	2FBC965DC03EF9203581F595E0D7AB1734726ED7
SHA-256:	76C80E31F37248C3C787F7972A7B22038390F9D81E72E650071A6F36D36AF27A
SHA-512:	326F8F9CBF829BF80AAA96062A57255A36EE04DE310634327AA075D14129CFA8E36E48AB2A00B10F9BDC1D94F1AC7A9E41D0D063361920A0332EC124BDF4C3E
Malicious:	false

Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d..8nIDATx^..xT...!=!$..%t..H.tP:.HQP@E,...QQ.^.....* E.("]:.K..R.....p..n.9{...sv.}.....7.....o..z...,\|. .....M +.....w.....O...>.SJ.O...<...{. .x..g..I..H.....V .. .}.PO..H+$@.$@=.=@.$@.....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./...I....'..|.. K...r|...nX...'.. .G...ib|...MY8|.....9x..Ur'.. ._ .....5..H..d..L.$@..I..o.;kM.$.?.....K/.wn.....Y....E..%K*.=.....Y.3.!k....[V..WG/?i..H..." T.,z...6h.[..-%9....WMY...z.vH..H@/.BOe. ...g-P.@.....IH.O...SJ}5.|....?.^..5^}..$.. .....S.@...*<.gJT/....._.R.C.....rj..Cg"\K.....K....~Y....l@..)..I.k.s..Yr.....Z]jG..q.+..G...;lNJj.}..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:ExqMHYnnEnntvA4Mesu3SXHycmfIEFQp1r/:E0MGEn29esuiXHt0FQp1
MD5:	5B386BF9A20766956A84F67F913F23D7
SHA1:	6E72E51F5B4FA64E52D2B80B41409B3DB927A3C7
SHA-256:	DDF6A1D5B29BD69C65A148B1247FDE8389CC56865E4398E4CBDCBD68A6555043
SHA-512:	99B4109439D9A688D7747C6847E0FF7399CDA01A89C3181789F913E757A82EE4727F95E506F4B01930EFC7C6E229B94BB89E385B56BC009AB5CFE332585660C5
Malicious:	false
Preview:	.PNG.....IHDR.....s>.Q....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...]...!.....!.YTP.A.....-..r..$.E.J.I;....T.M.UE[..Q..x....wKB=.m...4.%..\|:...9...\{..o.3..g. o~..~s...k...X.r..... ..@Gggg.?.... P_.]]]..*Iu....C...h..$..:... ..... .\.....@R..... ..$.k....@0.Hj0.8... ..r.@....F.I...G.....T...@.... ..P.....5...@ ..$5.J.A...@R.. ....#...C.#.@..H*... .. `...`(q...@.I..... .....%. ... .\.....@R..... ..$.k....@0.Hj0.8... ..r.@....F.I...G.....T...@.... ..P.....5...@ ..$5.J.A...@R.. ....#...C.#.@..H*... ..`...`(q...@.I..... .....%. ... .\.....@R..... ..$.k....@0.Hj0.8... ..r.@....F.I...G.....T...@.... ..P.....5...@ ..$5.J.A.....W_...1c.l..6..`...@ ..I.S..I.I'...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\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:rloPN36BoJ9JK5lncTww67QKf5wX5YgM5s6cahePwnR6+eA9zQU13ALcVz7wTQ8U:rYN31JH6lcbjMW5Ytmyqwp9H7wY
MD5:	B1FDE66F75507567B5F0C6C07B01A3A1
SHA1:	80B8E6A923E853232F66C874367E90B5C9CAD7AE
SHA-256:	B9C82D2F31BBE409D159EE3C9129CBAAC7C6F6C81637AB9B6DAB3C11AA74B7F1
SHA-512:	FC8C6038D3C2F5765D7524E969574ACD10AF6FCCFD45FE7C6DD4A8C2669B13EE3FB1A8833E94A046AB7037018170B5B87B1A2742E0E10557C413AD634BDF343 E
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...0!6_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.....\....]..."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:	47F45A3275B8454F8000F4567153DD7D4AF3012005D8E34CB18AED6AD69083BEC753E607F275FBF3EFCCB7BA00310A04ADFBD5FA5B73E6BBE47CE73901C35C A8
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..x.U..I...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..".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.... AIm.....~.

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+hJWizJNzIu1coqAYClBeMsk1:3dm2Ez2iUhBzhyjAxqQ
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...I-....y.I.h.....<..1.....C..(XSy.I....,-.....3..3...;.{...{.{g... ..Q..x.T/q...F.V...B..'..?{:.:..`.....+.0s.e...w....{.`. ....5...d..9S]../.....$Y.>.I...i..8....;,r8r!Ee'"..!*.&E.....n...=.@..Sp.GF..c*....1QH3....?,.T.el.....t?..([Q`.0....k.G.....X.. C...k\|p...I.q;.d..N....c.u.a.5.%.k.fS\)..H..T.~l*k.[.n...x2.1.....%...yK..a..I.[.?#..fD%.FMT. =r.jt^..fT...c.&..Lr.....\..V.ll....Br^6..U27...O..N*..K.gm.K..g.;..I..Fe...w?..Q .E.....0.....7...(.e..t...x.c6..Q..n.92:%....I..4.h]Z.....w..|..!.p.~..B.y..&.....gl...\.wI.....G.6.K.$...%.-.h]\8.LT.....}{a...^.i.....4.0.ji.....n.pk .....7t....U9..b...I.....#...<q..(|=F..... ..0@^.....+.....X. .>p....S..t.].f.x.0....7d..n..'..'.... .M.qqn...G.t8'.=..V.PK....K...X.z.#..I.....@...Y....BH..I.....,..K....=`&Z.41$..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:	384:1I+zN+iNurNE/tBdEC/vkape2XHYdhOm+BI6C4:L+zN+iNurGNEC3fpe2X8Pa+
MD5:	3A5CD52E925A7C4A345047D8F06C3C41
SHA1:	9C02828D83206BBD3EB58930C8C65A6CA5DBCF40
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.Pl"@....(@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+9mjQR
MD5:	01367FEEE0A83E8765E971E0D3740900
SHA1:	CAE1FD22CE2539FA2ACC0242C615CB7EA3F866E1
SHA-256:	18B8E53505DA3C412890F4D74AE2A6B26C4B0827E15E830F92A024D292AF20ED
SHA-512:	8CFBDC014C42AE6417038B80424D2E9FBDDD7DFDDF579E349C3C17C9B52AF33A72463154D29539457C4ADAB2DB00CC28A67902FA8D9209E4AF00EDD46D52ECA
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....-.!.TtRxs....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:	8B02CEC726DECF033B67689F369FDE1002ACFD5F8C32E0F248AC575997204F2F
SHA-512:	8EE1A1F6F0023EB4F60760C2E23EAFD56E6D298CAB49D819CF1D62C0CCF608D4211D3767856255F7CF8FF45AD835FE5475EB92C608989C522CD48D00A050B1
Malicious:	false
Preview:	.PNG.....IHDR.....Y.....?.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.]ip...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.=$..!.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.....]..;...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\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:KQJAeRumk2zXWySlEmWL9zi6wknB4qLx+ppNhQrW8Oy:Ke9S482LE6wQB6pNeqi
MD5:	29B87BEEC5D3899824AA390530CD47FB
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.h5.6][[....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.....O.....7...S.....6..P.]mf.+o....w..<.....Y..Z.whd.....*zf+.....#."_?....`._... qf+.?.?"k...zgME..j..!.k.U*.....&z..N....ma.....R.{.r0.S..KP..fU....g~..=..Q.n.*.* 8 T=/'9,*.KDW...GN;0(P3_....1.....';..;|.L.a.&<*\.d.....o...Y... {E.F..}.e.\..=W..#..W....c./~..b.EWXI.#."&.....:....X...b.....+2...5..6+)we~ja:lZ.d.Ey....l.2.5r.....!.!._|.A.....j2 .5.o.....WOM....V.....GC9..'.... ....C..,_...cS....b.1....t.....,_.....a.3..K..>V.f]...~....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:	384:5ojjyi45m1/9gyhgFsH1ud103Pl39o0qjfsH37mNHy7QPaNbZy0:+r45m1/BWKy10tN22rmNHycobE0
MD5:	548D234C9AB4021CA5FAB7BF22502465
SHA1:	2F7495D250DC86EA99473CC342D164B859926021
SHA-256:	7D549C3418CD90F42571D00936B23D242837CE2A8B19FC4C719E182ECB2624C6
SHA-512:	261523F5EAE6FCE2829B53AAC5938B1A0021C119E00CE82EFFDBD690FE71064E0F3B313ED1AB2F67A16C488AD5B1A91F5AF98029D88A7896F271C108410D42C 5
Malicious:	false
Preview:	.PNG.....IHDR....._.....sRGB.....gAMA.....a.....pHYs.....o.d..W.IDATx^..i.=YY6z@..DP.i.IAA.....l.Dd0"p0.ON.~....s>.?zbH8..%$`....b7..=....25*.".L. ..u_..f...j..... ...Uk..^UW]...u..}.{.]t.-.(...J.....e...t.....@i.k....._.(.....@...Z.6J.....2.O.-P...._.u.=T..4p...e..q..5^f~....@i`....?.....@i..k.....?...u..O\|bN.~?MbT%...@.LO.Or.`....$..y.{..o....~..(.;... ...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...@.....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....];|../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\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+TpI/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..I....>...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@.T2 .....xp..! .....d@...!.....(*B@....S....B ...O..QT.....! ..@<.H.....! ..O%.B@...x..9...C'|..{.>Z../~^.s<<V4..ujo..v.Z7..EwT.....@.....?.....~{...K.....C.....bB@.$.....C.{....Kf'S.....T.*&....@<.....'..D`...;~v.DT]...r!..>....ru...}.....#uG.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...IdK<..! }.:.....f.K..bX.T9...&T.&?.VB9.[B@..@@.4..1}.4.@H..-!..}..~M.<.z..I}.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...I..(

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/+76A6M6Y7rSYRv47cwbkkapeIiRmDGd+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$....AE..".I....+G.>AP@D..e..".".A.Y.@...K..IXB !..!..c1.On...==3=.3=.>9O..u....w.z..-].t9]B@...!.....Z...B@...^G`.Q.&S..u$d....B.Y..P.w5[]......B.m.D...! ..@...Ls.Q".....".S....B ..D.9.(.B@.....b@...!...".@..! ....T1 .....i. 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@...!...".@..! ....T1 .....i. J....B@d....B@...4..%B...! 2U...! .r@@d....!.....*.....9 2..D...B@.....5jT.@.{..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..I.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:jB5Gg4vMs30WIn5IVeRy1bY7DqbqQBAeNjukXIN4AXat:PGYuEWV/YH7e1uA0AXat
MD5:	91CB7F1273AA003076401081B8A22237
SHA1:	5157144069E7D2FDAE60B397BE5851E75BDF7707
SHA-256:	80682DD6472E8D1136BC5E20F6DE87B595562414B19EAB8E965736FE992921B0
SHA-512:	5A8E3C0ED0DB94BFE359C63793F12F3D7B3C37F3A13A5C96634BA1DC8C9E50FB1142FE4752FD9FBFA39A682F78C54AF868AD337EAA787801FE5F66D8F55A816
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.PyI.d..I;...;.=.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$C..|...I...n...~.....,i.....e..=..?{.....>r~.Lw.+2..\w.)w~...c....h..u..%...PE...f..'..m.ZE.1.\....U.`X.....$...P%..UH{[K..o7~.k.49..W.t.~.^_..7.,....f."q....+....;...~;.c.....Xb.\?.....0h.lV..WX!.....ljm.1c..U...[..X.).....B=.0~..W...rO..j...ehI5U:..66V5sJ.....V...]Y>...1kQH..2.....d....S....I...+..].p.....m7...Z...s.D>.K/]..?.I....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/5cxektxMQjcie9ZZkx30eXJIb8FKRN: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.>@.$@.v.PO.pd+$@.$@=e. .. .;...v8... .....f.o_o{....~t...n.S.N..?..._..L;J.H .,....7.}...|....7...b...|.....ObVa1. .?.X.....~.....t2..V>.b.}..0.F....%`GO7.n#~..F....K.~...FX..H.^....k.Z/.2v.W..M.<.;$...v.t..,UO.-]...........D.....o.J..Y.....5.%.I....{.....'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$..?....|.].)?[Wo.h.'..2P.1..!.....$.NO.5..}....c.;...~.x,|Q....B..6.@>..y..}....m...D~z....L#.0`_.`.s?|....I.....a...=N....c._.2._..6 .]...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:b6JWqvCl45Da8kuGzhRwZvwIutfij19MQ8EpW14LBGJVCq:b6JTCl45DalsBws1R8914V5q
MD5:	817D5A35EDB2B0E052194D4F49FDA19C
SHA1:	FA6CB2016C5F43B76102B63D60359139227E07EA
SHA-256:	0A87B8418B7F8E6E117BADDA11D7CDD38B8B7320C6BA3D3E9AF93EB9ACB2CE14
SHA-512:	E0686BDBFC589401F0EAAE2B1598199EFA285F8392742B1C928B9274088804B23DCB584B6FEF68CE6D7E54DFF9C10338104F4C0F3F80A04471F0B2E8F9935CC(
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.....$..b.*..%....@A]A..%..<.....l.h.+../..OSe....]...>..C.....^cCy.0nz.4<.....g..?~..>.1ws.B....07W65.74T....=..v.....D....6.....tR....}]}....4z..^....7..;.."......^.....|=.#.=.32..o.<.Tn*Q....g.zN...n*...!/.....!....F..]...6...m...CX..~...+..U...E.|.....7]=rE?i(..$`e.%.`.....w._.Y...l.1...@....t.P..=.}..*...N...N..|.xS.5&.....Pe.....Z.Z^XJkx.....^.....?7..._....Wsz....}G..]...\.....[.y....}.J....'.R?a...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..}w.....^..\.....m[.^.3r.....-8.....j....>...Q..T..{\V\ptH.?.....1..w....FHl...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:PmCwDJh8w9JewaF2zQNXXj8zq1KM43sxXxjYbTgJW1MFsrJ075CawGjGj:P1Ah8UewaFcgz82Kx8xXNYb3id/yj
MD5:	E88131C9AAC52649FF044905ACAB9B76
SHA1:	34AE73B9165CBED0DDF33AC20E4B3E7D622C19BF
SHA-256:	30F22340F582F9A352A7ED3048D1088F178E83CCAACAC1CCFD86852C8F9C78E3
SHA-512:	97AFE8F3A2A3138613934AC737C390A35F6757BFC3D381EA7C7CD148F739932380DCD46D0BA6F590C274F8BFB4D4286B3C0433AA69E090102A8A9ABDD7C97E1
Malicious:	false
Preview:	.PNG.....IHDR.....M.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.]kl.U....B|E..>...*..Q.....b[.K.....m.(..... ...!%1%*-B.C~(&`[.....-.....~.w3..Kw.3wvfzn.2{..s.....{w..\....!.3..:..!.../..zD.x...O.K... ^.1*...8.G...z...D.$.....>!..V..`v.CQQQ!..-L...../3.2.....ZH.?s...Iu\N..,3.?.p..N.....<....E.<.=z..Iu<ll.dX...g....+.{X.p.....:..t...a...cKK.\|..Yszl.N.:.....KPs.):).T.5...&B...*..5j``@...(_r.V.j..m...?x.sg...t\.dz.'^.=.\.h..<.y....:.l...w..ze.m.\.qPJu.....D.\|..@.....W..t.+.....X....e....\H+.Ns%^r.VS.N.3:...&...._..#^....d! ..F...xc..M...q...17.z...z&C...K9(.lfm.35.v.>.'X,...p.:=.H...J.K.,...:~...7.t.....R..R..9..?....l../.(...0z0.M.f.)H..Y_"e.....B.....L...q.K.....\|;..L.....xl.K3.M..%...../..){....R....s...7....).q.._R.4O.a3.....<..%....3#.\|>..y...u...R'.P..$Klz.....,...g.....`.7..\...x>.{p\;>+.,.....e.-..Re@.N..FY_....*....]}...[..h.M.oq.S.U...c_}`.....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.$M...4..L.Y.9.$M...4..2.....q...&.. .....*.Qg.+.p.....a.:.X6...o2.....A.....[).,.p.....P....._..>.....3.....z8j.....>...fww.6...../....S<.....^%.4.....{.N$..`.!H....`.....a..(.G^>~\|txx....K\mF..'d.d:9J!....j..i24.A...` O.....s.....?={....H'._..~..O.....*>...ZXX.3...;C....\....%..s=...w<h.....0...~..y..._.....+.n.P.M]c...A..Er\|.R...$.g...9*._.jg.....x...&+.JWM4xe..^....0...11.[.....f....r#.h.h$....[=t >...r.. ..L.0.KL..B\..x.....4J.0....vY...\dA. w.....g....};.}.....;.....x.\|.....).....x....s....N.$.n..g<Z.q.a9.C.....oX..%,KNNN..i.8J..p].1....B>{.....n.D|3t.-\g...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+8DdKlwm
MD5:	7F161B19B937AB48D4FD2F6E5E16FDBD
SHA1:	BDCE4F1C73E87E609A7FDF245A512CA4F73B35B9
SHA-256:	C863C5E71D1116D69561BD0637F4FE4C4240E9CED05B8A5B056073AD13E6495D
SHA-512:	E915B76FAAC9512D2AD11CF4E4530A19BEA1C7D8508BC218C69CB041F1EEABA3E2E03B1D56E61B032A6418829752C21B8354AF1335466D7E1528A06E6742A46 1
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,...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..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.]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...Yj<..~.5.?I.fZ0.@d.....*..G...K.....e...b.|e..Q.4.....('z...!G.....2..XQx\.....X...2.\h..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:	98BE1F4684F99A9FD2F313B09A113B5C310EC8BA8EB0EBF5FD69765E5B48B001D39999E3F25A7E76C7344DCF57B4F0BF2E4614FB0E0DFCCB6F02E6D1CAAF7F DD
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d..,NIDATx^....E...@^.T.....H..$..(.!..3....O=Q...<.9.`@E...CE.(""..H.$..6.....]3.....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..I.&.g...../....SO.\.,._@7Q.g.}V+../..Ht.l=..WZ%.{....._v.....%U.)^H(!!..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|.]."..t6.[.K..5.6.....B..(.=W./....S'.....z.FY.. ...PO.".tI...F...Q....c.o.....}...r>.. 3c9I../.....}.....I..G.|..|...~.b.e.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+LtoQ9jsUBsnwlDGThUe8ww2iJiGEjdKKnnE+Gh:V+Ltt5GwlDQhUe8ww2iJi7MKnnE+K
MD5:	995CEACAD563F849C4142B6A6F29F081
SHA1:	44CB3B867CD2917541B7D5AAED2F14F10FEBB0FD
SHA-256:	3691FB8C60EA1B827092F05FBB1807E34726016C6FF56698D7B81C44D519D22A
SHA-512:	3C8EFEB966B075D06D8344483352BF92C9292F9970C9377BE254EB355EFAF017916737AECCDC704B84D532B7229F9908951A6F2CC3FAD810791CAB224401AD3I
Malicious:	false

Preview:	.PNG.....IHDR.....c.L.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....W...Gh...k.Hm..J.m.....X...Eh..%.n.....PHvy$%...[...R..I...(/..-..yl..Z.h..H!.../.|.y|w...7d3 s.s.=.{.s.g.6W.^..)..@..{..'O.LL.....c.^.6xS&O.,...J.(|?.....,$.....@.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."!f.08hT..m. (..C.7n.....@....SVUU).F.).X\\....[j.U....xd..e...<..W.....=;0L78t+..Gw..-....]..... .C7.....K.w..._..g.....A.&M.$^.#.!....e.\.P.....;vD..@...Za.@*D..f...! .2w...4#.J..c....K}... .F.u.I.b.V2.k...5..`....*.....M..!.,.;.E..BZ....K..[7....5....,.....K...7+.6..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\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+wKkEOgx3PG92Eqt9LczFD
MD5:	EDB5ED43CC6038500A54B90BEC493628
SHA1:	A8CD63F3914E4347F4C5552FB922C6C03917F45F
SHA-256:	9F3312E33EB78C6952B5A5D881BBD18751FCFAC41D648C6F053CE781342A504F
SHA-512:	4EBCEFD69A4C249AA3B0F00A954C4E463DA22FC9CA0B61A0DC46079B438138C509B22188D966FFF6599A3A604858BC4CC8FE6E0685A764E8E0477AB7A237DB 32
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..I..x.....Z^...>B$1.N"}4.....1:&F8..*.X.yL(..s.3.....~2. EL%.w.Uc.zJ...B..S..b.7o|%..7..'.....N.|..Vi...q..uO,`/....\W{..y...&iI..|X&T.....-.....Z..o.~u..U....cF.M....O4}.....~.....:T..W..._s...t..Dlb.$Pr././.._4.b.....R.T$t..$.>hB. +.{.. ....m.w .Q...05..C.}...}.....?..h.....Y .8.6^t....}.y.%.....l=$..[.~..].h..N.....*....SB.|....8..H....._...G...|.....;6YQ|WO.o.}]..'.$..oE.y...i'9.[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:	48:4gv2YZ4gWLpU9JcjREmXfFEV7NNkfKOgV60g0Z:KZgWLpSJcj+mPFGNkfngp
MD5:	3F1535054D4F9626F0EB10CEE47F076E
SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C6 0
Malicious:	false
Preview:	.PNG.....IHDR.....1.....*[.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATXG.iLTW... .23..,..6 .....kK.5...5..IMh..TI.....V.v.PZ.-F...".k.pCQ.....#.../s>f..3s....<...=^ '/.~.;.a....{>.g.....*o..6k..k....E....O....aQ.j....X&vG.....{u-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[....;'n...u.g..>X....o.]}...>...._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;.....,.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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:o4KSpFN6Ud4c3p2Il1yavNr5spYVJzimIfZ:wGN6Udv4IKavLBJz/r
MD5:	0693DABBBC411538D209F32E22F622F6
SHA1:	FB7E675406FA123CDB7E058D336742D6A2E8DC8E
SHA-256:	2DFB2E7A1A3AA43C673D2EE540D3C366CEB12105EB5441F98992FC06F4284013
SHA-512:	F07732660EC62DAE58EB02E2E9476007EA92BF826F642BCA547097136AEA01D29FF69D9B0CD0F5D65A5E15AA66CA4AA4804AA171A3504AAB198631C643C90C1 6
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..:I.D.S>I$A...I.....y.9...f.....3...Gh.....}_ .o....n..A@.....A@...L...2... ..... .x...#. ....1f]9.[.....A@.....3 ....fE@x.YWN.....A@.....1..... .....Y..J.Y.N.....s"......./..rc.scuyyyu...\s....t.oi..j..lv.....Gr.#9 %%%9%--....d.T...r...DH...6.....%U..A@.0.....rAD .....2.5.....L.R..=W...gZ.`o..-?.T.Cy.:...y.9..y.EE...v.....1..R.....1."..... `"...ss.....i.!.hY...Fj*....%.-.Gw...HJJr8..6...#.....!(.? P.(.....8(u.....*..OOO.....dgg....Q..=..c.y....A`S.@.....3.CC..GFfg. .I.I.COrJFFFNNV^nn^^.z..%..(...^.b$.....a..y.LMO-.,ylV+.k...T>Jg..*//-+-.....M=..x.....E.... `~..N.Kww. .....z...%%.e.%.yy.i...P.)'.,A.5.d.0.Cc35==66>2::33..>..;..Ii.i.gv...DSd....I#...I.....)**,**...V..1 .F.'7....)..SSs..7..F...C.p....(*,.....(RG..B...I!.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:	48:4gv2YZ4gWLpU9JcjREmXfFEV7NNkfKOgV60g0Z:KZgWLpSJcj+mPFGNkfngp
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-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[.....;'n...u.g..>X....o.]}...>...._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;....._.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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/gKVp93jQvcv16kjOzbapFJBkjcMNBqmQzOG8qx1QKnse8T:JieMJzph13Evcv16RfapFLxMNBo8qxan
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.0.T....L~....af..Z.....O..4..>Ms..Js_.....5.E.d...Y....?\z.3..}.I..|?~...{.....s.z..Y..... ....E.X.6...c..u...y..W.j....."}...l.i.`.!-!-.....MKH.E.bi.d...b.X.)...X4 .vJ6-...;..+/.->Qyi.t...%.T..k;.U..y.C$[;..Gm.....v..*2..2..eee..."!..)...yy...III./..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.!.....>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.|=.....'%!y.....\.....MSn.i.....!...U.$0S .....Z.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:	48:4gv2YZ4gWLpU9JcjREmXfFEV7NNkfKOgV60g0Z:KZgWLpSJcj+mPFGNkfngp
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-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[.....;'n...u.g..>X....o.]}...>...._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;....._.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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:	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.%...xaI.}...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...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....qI....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\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:aerVlDRlewkXlrTa2c
MD5:	73E38124F94AD20A2F1571FBBE11AEEC
SHA1:	87FB8056DC7A0A3B70D51426771C4CCE2099CFE5
SHA-256:	A700B63B30CBBE5230CC5E977D651E178EA87E73EAB18C8D5FFB1362149ADDF7
SHA-512:	320FCE64DD6F975384BEC9267348CD5CD24A55B13BB09FEF1238C2216AD8ECABDCCC15601A079CE092ACFA4954829FFEB06FBB0631F6AE26E3A39E43C1020 8B
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.&~.....oy....k...}}x..[....g59.}]...~i.SY.....".....7Ow../.....2...3f)n{..R..R.....U?.....O.{....c..pT.\.t....5.07.. .....07...7.o..,+.,.V.c...&..%.3I.....: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.....I.....,Y.{. .....g.1.0..I}.....<.....T..}....t.!x&)..[.7....4.5..{....n.<...#I...:.....r.wW~..zr..9k.^.]KR.*W.J.n.")....%0...)...Fbb5`4'.X..E.../.t.&,t(...@9....\$.....].P..jdU.....H;.$.'%}.I7.....y..$.. ...Z..4.Cm.u#&.%N..1..+..8....y...U.(.T.....}.I..5r}...!..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:uuT43eqJy2jEeSZE0onrAFAOpn5ytFfNrfIkBQTYz8ynth2EB:EugQeS+nrAFZ8tJNrfRQM4ynH2EB
MD5:	7CEB71F78A193F8C9F7FFDA5F81AEBD8
SHA1:	EEC1597705EFF1A527C246B86A71878185BA6B1B
SHA-256:	77911FF7AEAB8FCCAF36DE6E1183FFE1A6C27F77B5714EE780976CE5189E8FD0
SHA-512:	1D1AB19B64E1E2ABCA61AE78B3B50310B0A6CF19D2ECFCB4499D8D0BF68600B4D95BC0945EF9FF9B1D016ED61EAC518DCCA1A426F460317C07AD51E2E0479 48C
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.....k]s..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...I...{M..@..4555==-...!..f.....d...>i.%&&&%.u....f..[.....O`.....G..E6I.< ..3.k...',....Y...<.....u...{9.....S^^.q.<..^....2.bb.E`r...ey..... ..3.....Dg@L..a'.x&".O.Y..!e.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.....wvv:..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.LI.....>.....&....."..."....@.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:s6USl2RqfGhmDrpYM0ofHX4aIVYm
MD5:	17E9FF9F735102231846936F0E2BAF1A
SHA1:	9EC1AE8A3AD55C48C02427D842D6E38DA85B5145
SHA-256:	DD1CA8DA90893E0B63ABFDD9E60CF2BF844B311964E9D9DDB855C21FCA156EBB
SHA-512:	71E690D6C87B09659296E6E6DDC8E3F91035DD80C5CE875FA557763E8138900C27FB492885291CEE203D65BCEE8C20C9C39E0590A5FD32B8A00BEB3E3F6D6E F
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..I1G..$.".Fg.q... N.nt...3.w.w..~.v.O.....K.....A@.....A ..H.n.D;A@.....A@.....e.y ....1..P..xH.. ....e.9 ....1..P..xH.. ....e.9 ....1.@.$9..S....A@..4....^C..F..VR\\TT.....aHII1..... .VS..g..... .*....z..|Ek.....<R../55+33;;;+..Y..WC..#...P..... ...s#0::.....522...,.v..D....._.....9.2N.L.'..F$.....e..!..... ...N...`1....G.....'&,f..f.X....!.lp.....I_.....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..2...F.GCC#...].=..C..n#...K+..MOO....."....d^2=.{....U.p.h%.%n...D.....XB..b..'"....?h.b.B\v..^Q^.UC.....Q...I.....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:k1hccap27HGVhY2Kn+A3RS+HG3dXrjmg26vh:k1hccewIhYxRmR5
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!...\.!.`pA.+....H.U..."Z..*U.. ..P.D.-.$.,,..$.g.....CB.I.....I.g.pc..Lf..~.=.~ ]S.....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.....I....B'.n...O...yc.....X...P...k....t..9tf.g>....e..Sy'.L+**.]{..a...,7...p..+.....K..y.9p...I{..i58....v..5.`Op.....{.....8..._.S.....p..).....;....y...2...b.[> gP....C..G.H.....Osp...)..9x!...W.,..^....$r.p.sOJ.I..=.x.9s&:.....h.`..W"V..|.I{..72....zv@.#.<...../....F|...c...4.W....:uj@1...~.X.....^si....Z..I~.Q.<.....NAOq...+i`.)...$ L..gV.6#.....F$..hD.g.L-\..H._.u..]4.....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\00000010.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:	9AA4A6DD01D3B745D674721765F2BFCCAB584CA0603F222EDBE9A88190A2A57438041E7A3706CC0656A6ABB79AA18118319F210EFFE3DD917E7B94A6294BD34 6
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..... F.....b..O.KVfVfjFzJzVF.}i{.R..l..q..`l....e.'./.'.G.z.*!&>)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>.....]I..7.i...3....<.y.l]....SI>...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.=.....(!C.....?5..+...[..a.:U.K..C.....w.....+..r@.z.7..j..qB..B.....X}..=.fk...>^5[....n.z....wn....Z 4.._iWG.^..z6./]t.....dhM.9s...Gbo?...U.V..tj.....*&)Io.{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:IfGsPejaVZWzIZKpnFFt0HK5+2Y/SLopWR:IusPe278IZKpnzt0q5+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..I...B..`...N....t.q..j...+LU.....O..sF.!.I...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.I^OOONN8)....\y....}...}}.}.Hy6.^.a.....\...!S....K..|>.....s.....I. .P...LFWW.I..RK..b.h.h .3.F..|..|..~.....e.aa.....0H...<.Y.a`..xA!...7.X....xd=.....h?o5.....Ay....?6.....*..tb.9.*j...S`](.,P...9.2j..?...z3wD.[.....L3.Ng2G|.....&..0 ZK1u8.H.2...Z../..P(....BA..aL|..a.Y:.....J...5^x..'.\..&S...L..U..;....<{..."..@x ....J.N...;....WIht.<..B.....!HM...&z&..6u..hF..G.D..B.....A.....n...GG...,.,Q....X,`"....r.....3d.{o.(/.. .3.H...x:sX....h.8... ....r <..DB. ...y.N...o....5.....L&w....v....w..D.....!.a4...."8.U.|.0m.(..zR>..=.+.L.....e....Yd2.-Z.7..D"..pX.I.....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:	48:4gv2YZ4gWLpU9JcjREmXfFEV7NNkfKOgV60g0Z:KZgWLpSJcj+mPFGNkfngp
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-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[.....;'n...u.g..>X....o.]}...>....._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;.....,_.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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/zVJWedudPZZRdbvczHe2ftFJ0y8Ea5b2AELJj:x4FTnodRZ7c7LrabEaMAGp
MD5:	DB48555480A383CD1D4DD00E2BCFCF29
SHA1:	8060B6FE12175289F0A71F45B894030A0D9F1AB5
SHA-256:	807723D8F90A5BD41269A7A62817547026A117D666D5BEF454EB699C97CA3FA2
SHA-512:	2614C04686299CEE8D56577A1E836A26076D42E041C627177FDB295629F6A80190910947FA794A094C55A45C3D70725EEF29097118E523A38B50C9263C771A41
Malicious:	false
Preview:	.PNG.....IHDR.....gI.....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.....'L...g.UVVz.[.n)...Yqq...Y.f.)//_.I.W_}.,.....S^Z^Y..++.*..pF.....?...I.&...O,.k.d...~..w;Q.....7}1y.....e_.....=y._U....{..}.w.O..~.z.{.....W\q.."....."..h.....}p.+.>m...d...4...`a~Z^....me... ....:N]..1...g..y.f.....I..g.).....e[.....Z..RB.KrJ.....#...{..eff..v.[[<.n..?{.....SN9%...V.yE...s2.....e@Wz..I...B.r..<.-.=/t{.v.|..J...,.@.A.v...s`/.....6f....L?.z[T7..)S0.;c....\s..z-C .....v..}Y..{..j..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:L6ousL3eslFAmjb89xK6YiSTwtw5dTA1W9lQ:GoFiUFAMbsxJYieZ5dGklQ
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...BI.....5dC....r.....:m.....s..j.f..jK....y.^....'8.....<.....g.....=.%..2.p..}<.....G.....Ix.m.4dm..B.....0?..+_.*..c..n.....?....wa..l...p....E.Ly.}...*...C.D.vy).....@.>\...3;.`].q..m../.d.B.../.....~.p.U..'...sP\....YH.7.../....R!...O...'.....s....<|.f)....i.{.I..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.[`Uf.Y...>z\..x.B.h" \.}...`...|._.....G...hY.../..6>..Z...8^..k.E.5d#..a."....P.CR....OL..U...qY.{.C.<~I=V..x.J..*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/PMeaEf61lT6kCiFQCQq6zT
MD5:	3E9F7D399DF9CAD3669B7A5445EF7074
SHA1:	2FBC965DC03EF9203581F595E0D7AB1734726ED7
SHA-256:	76C80E31F37248C3C787F7972A7B22038390F9D81E72E650071A6F36D36AF27A
SHA-512:	326F8F9CBF829BF80AAA96062A57255A36EE04DE310634327AA075D14129CFA8E36E48AB2A00B10F9BDC1D94F1AC7A9E41D0D063361920A0332EC124BDF4C3E
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d..8nIDATx^..xT...!=!$..%t..H.tP:.HQP@E,...QQ.^.....* E.("]:.K..R.....p..n.9{...sv.}.....7.....o..z...,\|.....M +.....w.....O...>.SJ.O...<...{. .x..g..I..H.....V .. .}.PO..H+$@.$@=.=@.$@.....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./...I.....'..|..K...r|...nX...'.. .G...ib|...MY8|.....9x..Ur'.. ._ .....5..H..d..L.$@..I..o.;kM.$.?.....K/.wn.....Y....E..%K*.=.....Y.3.!k....[V..WG/?i..H..." T.,z...6h.[..-%9....WMY...z.vH..H@/.BOe.....g-P.@.....IH.O...SJ}5.|....?.^..5^}..$.. .....S.@...*<.gJT/....._.R.C.....rj..Cg"\K.....K....~Y....l@..)..I.k.s..Yr.....Z]jG..q.+..G...;lNJj.}..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:ExqMHYnnEnntvA4Mesu3SXHycmfIEFQp1r/:E0MGEn29esuiXHt0FQp1
MD5:	5B386BF9A20766956A84F67F913F23D7
SHA1:	6E72E51F5B4FA64E52D2B80B41409B3DB927A3C7
SHA-256:	DDF6A1D5B29BD69C65A148B1247FDE8389CC56865E4398E4CBDCBD68A6555043
SHA-512:	99B4109439D9A688D7747C6847E0FF7399CDA01A89C3181789F913E757A82EE4727F95E506F4B01930EFC7C6E229B94BB89E385B56BC009AB5CFE332585660C5
Malicious:	false
Preview:	.PNG.....IHDR.....s>.Q....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...]...!.....!.YTP.A.....-..r..$.E.J.I;....T.M.UE[..Q..x....wKB=.m...4.%..\|:...9...\{..o.3..g.o~..~s...k...X.r..... ..@Gggg.?.... P_.]]]..*Iu....C...h..$...:... ..... .\.....@R..... ..$.k....@0.Hj0.8... ..r.@....F.I...G.....T...@.... ..P.....5...@ ..$5.J.A...@R.. ....#...C.#.@..H*... .. `...`(q...@.I..... .....%. ... .\.....@R..... ..$.k....@0.Hj0.8... ..r.@....F.I...G.....T...@.... ..P.....5...@ ..$5.J.A...@R.. ....#...C.#.@..H*... ..`...`(q...@.I..... .....%. ... .\.....@R..... ..$.k....@0.Hj0.8... ..r.@....F.I...G.....T...@.... ..P.....5...@ ..$5.J.A.....W_...1c.I..6..`...@ ..I.S..I.I'...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:rIoPN36BoJ9JK5lncTww67QKf5wX5YgM5s6cahePwnR6+eA9zQU13ALcVz7wTQ8U:rYN31JH6lcbjMW5Ytmyqwp9H7wY
MD5:	B1FDE66F75507567B5F0C6C07B01A3A1
SHA1:	80B8E6A923E853232F66C874367E90B5C9CAD7AE
SHA-256:	B9C82D2F31BBE409D159EE3C9129CBAAC7C6F6C81637AB9B6DAB3C11AA74B7F1
SHA-512:	FC8C6038D3C2F5765D7524E969574ACD10AF6FCCFD45FE7C6DD4A8C2669B13EE3FB1A8833E94A046AB7037018170B5B87B1A2742E0E10557C413AD634BDF343E
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...0!6_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.....\....]..."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:JNu6DMLaZsMhtLAIa0wYMAvl5V4DDQ
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..I...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..".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.... AIm.....~.

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:	48:3Cxnazs22lovji2Ez2iqBU2C+hJWizJNzIu1coqAYClBeMsk1:3dm2Ez2iUhBzhyjAxqQ
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...I-....y.I.h.....<..1.....C..(XSy.l....,-,.....3..3...;.{...{.{g... ..Q..x.T/q...F.V...B..'..?{:.:..`.....+.0s.e...w....{.` ....5...d..9S]../.....$Y.>.I....i..8....;,r8r!Ee'"..!*.&E.....n...=.@..Sp.GF..c*....1QH3....?,.T.el.....t?..([Q`.0....k.G.....X.. C...k\|p...I.q;.d..N....c.u.a.5.%.k.fS\)..H..T.~I*k.[.n...x2.1.....%...yK..a..l.[.?#..fD%.FMT. =r.jt^..fT...c.&..Lr.....\..V.ll....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...\.wI.....G.6.K.$...%.-.h]\8.LT.....}{a...^.i.....4.0.ji.....n.pk .....7t....U9..b...l.....#...<q..(|=F..... ..0@^.....+.....X. .>p....S..t.].f.x.0....7d..n..'..'... .M.qqn...G.t8'.=..V.PK....K...X.z.#..I.....@...Y....BH..I.....,..K....=`&Z.41$..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:	384:1I+zN+iNurNE/tBdEC/vkape2XHYdhOm+Bl6C4:L+zN+iNurGNEC3fpe2X8Pa+
MD5:	3A5CD52E925A7C4A345047D8F06C3C41
SHA1:	9C02828D83206BBD3EB58930C8C65A6CA5DBCF40
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.Pl"@....(@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\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:	18B8E53505DA3C412890F4D74AE2A6B26C4B0827E15E830F92A024D292AF20ED
SHA-512:	8CFBDC014C42AE6417038B80424D2E9FBDDD7DFDDF579E349C3C17C9B52AF33A72463154D29539457C4ADAB2DB00CC28A67902FA8D9209E4AF00EDD46D52E 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....-.!.TtRxs....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:	8EE1A1F6F0023EB4F60760C2E23EAFD56E6D298CAB49D819CF1D62C0CCF608D4211D3767856255F7CF8FF45AD835FE5475EB92C608989C522CD48D00A050B1
Malicious:	false
Preview:	.PNG.....IHDR.....Y.....?.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.]ip...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.=$..!.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.....]..;...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..[?_.?.?..I.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:KQJAeRumk2zXWySlEmWL9zi6wknB4qLx+ppNhQrW8Oy:Ke9S482LE6wQB6pNeqi
MD5:	29B87BEEC5D3899824AA390530CD47FB
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.h5.6][[....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.....O.....7...S.....6..P.]mf.+o....w..<.....Y..Z.whd.....*zf+.....#."_?....`.._... qf+.?.?"k...zgME..j..!.k.U*.....&z..N....ma.....R.{.r0.S..KP..fU....g~..=..Q.n.*.* 8 T=/'9,*.KDW...GN;0(P3_....1.....',;..;|.L.a.&<*\.d.....o...Y... {E.F..}.e.\..=W..#..W....c./~..b.EWXI.#."&.....:....X...b.....+2...5..6+)we~ja:lZ.d.Ey....l.2.5r.....!.!._|.A.....j2 .5.o.....WOM....V.....GC9..'.... ....C..,_...cS....b.1.....t.....,_.....a.3..K..>V.f]...~....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:	384:5ojjyi45m1/9gyhgFsH1ud103Pl39o0qjfsH37mNHy7QPaNbZy0:+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.IAA.....l.Dd0"p0.ON.~....s>.?zbH8..%$`....b7..=....25*.".L. ..u_..f...j.....Uk..^UW]...u..}.{.]t.-.(...J.....e...t.....@i.k....._.(.....@...Z.6J.....2.O.-P...._.u.=T..4p...e..q..5^f~....@i`....?.....@i..k.....?...u..O\|bN.~?MbT%...@.LO.Or.`....$..y.{..o....~..(.;...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...@.....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....];|../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@.T2 .....xp..! .....d@...!.....(*B@....S....B ...O..QT.....! ..@<.H.....! ..O%.B@...x..9...C'|..{.>Z../~^.s<<V4..ujo..v.Z7..EwT....@.....?.....~{...K.....C.....bB@.$.....C.{....Kf'S.....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...IdK<..! }.:.....f.K..bX.T9...&T.&?.VB9.[B@..@@.4..1}.4.@H..-!..}..~M.<.z..I}.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...I..(

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:jgxmx2Fa/+76A6M6Y7rSYRv47cwbkkapeIiRmDGd+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$....AE.."..l....+G.>AP@D..e..".".A.Y.@...K..IXB !..!..c1.On...==3=.3=.>9O..u....w.z..-].t9]B@...!.....Z...B@...^G`.Q.&S..u$d....B.Y..P.w5[].....B.m.D...! ..@...Ls.Q".....".S....B ..D.9.(.B@.....b@...!...".@..! ....T1 .....i. J....B@d....B@...!.....!.....*.....9 2..D...B@..L..B@.....D..! .D...! ..@...Ls.Q".....".S....B ..D.9.(.B@.....b@...!...".@..! ....T1 .....i. J....B@d....B@...4..%B...! 2U...! .r@@d....!.....*.....9 2..D...B@.....5jT.@.{..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\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:jB5Gg4vMs30WIn5IVeRy1bY7DqbqQBAeNjukXIN4AXat:PGYuEWV/YH7e1uA0AXat
MD5:	91CB7F1273AA003076401081B8A22237
SHA1:	5157144069E7D2FDAE60B397BE5851E75BDF7707
SHA-256:	80682DD6472E8D1136BC5E20F6DE87B595562414B19EAB8E965736FE992921B0
SHA-512:	5A8E3C0ED0DB94BFE359C63793F12F3D7B3C37F3A13A5C96634BA1DC8C9E50FB1142FE4752FD9FBFA39A682F78C54AF868AD337EAA787801FE5F66D8F55A81 6
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.PyI.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.....=..I...VS.d..+...tGd..k-._.....oL.:}.p.~.W$C..|...I...n...~.....,i.....e..=..?{.....>r~.Lw.+2..\w.)w~...c....h..u..%...PE...f..'..m.ZE.1.\....U.`X.....$...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...ehI5U:..66V5sJ.....V...]Y>...1kQH..2.....d....S....I...+..].p.....m7...Z.. ..s.D>.K/]..?.I....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:vpXZavBpl00n1Pt7JquG9GYHDK/5cxektxMQjcie9ZZkx30eXJIb8FKRN:vpZaDyc1P1Je9G62/5clpjre9nQkeXJY
MD5:	31579CA3352DF8FA4E3E7F48C7CDF672
SHA1:	AA682A3C781BF8EE43B5EDC9718E64CB79135F25
SHA-256:	B0E7824BEE2C896279457D87E61E902431BEB528D830524CC4DFAE126E89FC24
SHA-512:	782FF9492E3ECB11C72D316DDD94D1F3E94CD908FC9452A37DA6CA30ABCFE9AB2BCCED8583A569DA68626BCEC730408AF86997E295637BF64AFF5BC768F3E 309
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.>@.$@.v.PO.p d+$@.$@=e. .. .;...v8... .....f.o_o{....~t...n.S.N..?..._..L;J.H ..,....7.}...|....7...b...|.....ObVa1. .?.X.....~.....t2..V>.b.}..0.F....%`GO7.n#~..F....K.~...FX..H.^....k .Z/.2v.W..M.<.;$...v.t..,UO.-]..........D.....o.J..Y.....5.%.I....{.....'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$..?....|.]..)?[Wo.h.'..2P.1..!.....$.NO.5..}...c.;...~.x,|Q....B..6.@>..y..}...m...D~z....L#.0`_.`.s?|....I.....a...=N....c._.2._..6 .]...5....{.^>.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:b6JTCl45DalsBws1R8914V5q
MD5:	817D5A35EDB2B0E052194D4F49FDA19C
SHA1:	FA6CB2016C5F43B76102B63D60359139227E07EA
SHA-256:	0A87B8418B7F8E6E117BADDA11D7CDD38B8B7320C6BA3D3E9AF93EB9ACB2CE14
SHA-512:	E0686BDBFC589401F0EAAE2B1598199EFA285F8392742B1C928B9274088804B23DCB584B6FEF68CE6D7E54DFF9C10338104F4C0F3F80A04471F0B2E8F9935CC
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.....$..b.*..%....@A]A..%..<.....l.h.+../..OSe.....]...>..C.....^cCy.0nz.4<.....g..?~..>.1ws.B....07W65.74T....=..v.....D....6.....tR....}}}....4z..^....7..;..."....^.....\|=.#.=.32. .o.<.Tn*Q....g.zN...n*...!/.....!....F..]...6...m...CX..~...+..U...E.\.....7]=rE?i(..$`e.%.`.....w._.Y...l.1...@....t.P..=.}..*...N...N.|.xS.5&.....Pe.....Z.Z^XJkx.....^.....?7..._....Wsz.... ..}G..]...\.....[.y....}.J....'.R?a...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..%...I..d..}w.....^..\.....m[.^.3r.....-8.....j....>...Q..T..{\V\ptH.?.....1..w....FHl...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:PmCwDJh8w9JewaF2zQNXXj8zq1KM43sxXxjYbTgJW1MFsrJ075CawGjGj:P1Ah8UewaFcgz82Kx8xXNYb3id/yj

MD5:	E88131C9AAC52649FF044905ACAB9B76
SHA1:	34AE73B9165CBED0DDF33AC20E4B3E7D622C19BF
SHA-256:	30F22340F582F9A352A7ED3048D1088F178E83CCAACAC1CCFD86852C8F9C78E3
SHA-512:	97AFE8F3A2A3138613934AC737C390A35F6757BFC3D381EA7C7CD148F739932380DCD46D0BA6F590C274F8BFB4D4286B3C0433AA69E090102A8A9ABDD7C97E 1
Malicious:	false
Preview:	.PNG.....IHDR.....M.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.]kl.U....B|E..>...*..Q.....b[.K.....m.(..... ...!%1%*-B.C~(&`[.....-.....~.w3..Kw.3wvfzn.2 {..s.....{w..\....!.3..:..!.../..zD.x...O.K... ^.1*...8.G...z...D.$.....>!..V..`v.CQQQ!..-L...../3.2.....ZH.?s...Iu\N..,3.?.p..N.....<....E.<.=z..Iu<ll.dX...g....+.{X.p.....:..t...a...cKK.\|.. .Yszl.N.:.....KPs.):).T.5...&B...*..5j``@...(_r.V.j..m...?x.sg...t\.dz.'^.=.\.h..<.y....:.l...w..ze.m.\.qPJu.....D.\|..@.....W..t.+.....X....e....\H+.Ns%^r.VS.N.3:...&...._..#^....d! ..F... ..xc..M...q...17.z...z&C...K9(.Ifm.35.v.>.'X,...p.:=.H...J.K.,...:~...7.t.....R..R..9..?....l../.(...0z0.M.f.)H..Y_"e.....B.....L...q.K.....\|;..L.....xI.K3.M..%...../..){....R....s...7... .).q..._R.4O.a3.....<..%....3#.\|>..y...u...R'.P..$Klz.....,...g.....`.7..\...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+em8Tlk2APr2fEd72tTqiVJlcLzqeVzYwS:r+erTlk5S+zoyGahS
MD5:	EF9AA5B2ADBE5DF68AC4F4D716DF7708
SHA1:	363B93AAAB9DB2832F6CA0EE3C27C9310C344BA8
SHA-256:	3D94FCC4821A135ABAAE6579011441B94F9C04DAD1E66BB5211B0C019A5968B9
SHA-512:	EC9B024AEA46F7B97D14F0A7E12704D09B85F0017CC9E273CE50F2F889DFDAE81DE549CCD546BBB8F8BAAAAAB7781FEF77BF783E02CCC9605304552F7DD59 03D
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.$M...4..L.Y.9.$M...4..2.....q...&.. .....*.Qg.+.p.....a.:.X6...o2.....A.....[).,.p.....P....._..>.....3.....z8j.....>...fww.6...../....S<.....^%.4.....{.N$..`.!H....`.....a..(.G^>~\|txx....K\mF..'d.d:9J!....j..i24.A...` O.....s.....?={....H'._..~..O.....*>...ZXX.3...;C....\....%..s=...w<h.....0....~..y..._.....+.n.P.M]c...A..Er\|.R...$.g...9*._.jg.....x...&+.JWM4xe..^....0...11.[....f....r#.h.h$....[=t >...r.. ..L.0.KL..B\..x.....4J.0....vY...\dA. w.....g....};.}.....;.....x.\|.....).....x....s....N.$.n..g<Z.q.a9.C.....oX..%,KNNN..i.8J..p].1....B>{.....n.D|3t.-\g...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:	7F161B19B937AB48D4FD2F6E5E16FDBD
SHA1:	BDCE4F1C73E87E609A7FDF245A512CA4F73B35B9
SHA-256:	C863C5E71D1116D69561BD0637F4FE4C4240E9CED05B8A5B056073AD13E6495D
SHA-512:	E915B76FAAC9512D2AD11CF4E4530A19BEA1C7D8508BC218C69CB041F1EEABA3E2E03B1D56E61B032A6418829752C21B8354AF1335466D7E1528A06E6742A46 1
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,...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..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&..?.....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...Yj<..~.5.?I.fZ0.@.d....*..G...K.....e...b.|e..Q.4.....('z...!G.....2..XQx\.....X...2.\h..X~.e....Z....=....C.1.....w.....d.z.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002G.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:	98BE1F4684F99A9FD2F313B09A113B5C310EC8BA8EB0EBF5FD69765E5B48B001D39999E3F25A7E76C7344DCF57B4F0BF2E4614FB0E0DFCCB6F02E6D1CAAF7F DD
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d..,NIDATx^....E...@^.T.....H..$..(.!..3....O=Q...<.9.`@E...CE.(""..H.$..6.....]3.....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..I.&.g...../....SO.\.,._.@7Q.g.}V+../..Ht.I=..WZ%.{....._v.....%U.)^H(!!..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|.]."..t6.[.K..5.6.....B..(.=W./....S'.....z.FY.. ...PO.".tI...F...Q....c.o.....}...r>.. 3c9I../.....}.....I..G.|..|...~.b.e.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\0000002H.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:IfGsPejaVZWzIZKpnFFt0HK5+2Y/SLopWR:IusPe278IZKpnzt0q5+qVR
MD5:	70DAF02EC717AB54452FA4C707BCAC74
SHA1:	30F46FAC5E96470848C5A948162CC12455A05154
SHA-256:	58469BA93EA36498FF9864EB54713A001C52106DE97804506D82EE24B816712B
SHA-512:	E599FDC22A32CFEDBB23EECEAE0B278EAB9A90959FE6ACB40E2B201E45A7C19261AAF529E7A0D9CAF2A9A4C64C7831343F3BC20810513990AD5D38A327415 64F
Malicious:	false
Preview:	.PNG.....IHDR.....IC.....sRGB.....gAMA.....a.....pHYs.....o.d...cIDATx^..S[Y..I...B..`...N....t.q..j...+LU.....O..sF.!.I...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.I^OOONN8)....\y....}...}}.}.Hy6.^.a.....\...!S....K..|>.....s.....I. .P...LFWW.I..RK..b.h.h .3.F..|..|..~.....e.aa.....0H...<.Y.a`..xA!...7.X....xd=.....h?o5.....Ay....?6.....*..tb.9.*j...S`](.,P...9.2j..?...z3wD.[.....L3.Ng2G|.....&..0 ZK1u8.H.2...Z../..P(....BA..aL|..a.Y:.....J...5^x..'.\..&S...L..U..;....<{..."..@x ....J.N...;....WIht.<..B.....!HM...&z&..6u..hF..G.D..B.....A.....n...GG...,.,Q....X,`"....r.....3d.{o.(/.. .3.H...x:sX....h.8... ....r <..DB. ...y.N...o....5.....L&w....v....w..D.....!.a4...."8.U.|.0m.(..zR>..=.+.L.....e....Yd2.-Z.7..D"..pX.I.....e5qYa._&..3..J..++

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002I.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:	9AA4A6DD01D3B745D674721765F2BFCCAB584CA0603F222EDBE9A88190A2A57438041E7A3706CC0656A6ABB79AA18118319F210EFFE3DD917E7B94A6294BD34 6
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.KVfVfjFzJzVF.}i{.R..I..q..`I....e.'./.'.G.z.*!&>)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>.....]I..7.i...3....<.y.I]....SI>...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.=.....(!C.....?5..+...[..a.:U.K..C.....w.....+..r@.z.7..j..qB..B.....X}..=.fk...>^5[....n.z....wn....Z 4._iWG.^..z6./]t.....dhM.9s...Gbo?...U.V..tj.....*&)Io.{q.G...A...I...i7...&....d.E]....#.W.x,.T...&Mz4+].4.$n..F..x...<.ppr.....y.,i./..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002J.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:aerVlDRlewkXlrTa2c
MD5:	73E38124F94AD20A2F1571FBBE11AEEC
SHA1:	87FB8056DC7A0A3B70D51426771C4CCE2099CFE5
SHA-256:	A700B63B30CBBE5230CC5E977D651E178EA87E73EAB18C8D5FFB1362149ADDF7
SHA-512:	320FCE64DD6F975384BEC9267348CD5CD24A55B13BB09FEF1238C2216AD8ECABDCCC15601A079CE092ACFA4954829FFEB06FBB0631F6AE26E3A39E43C1020 8B
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.&~.....oy....k...}}x..[....g59.}]...~i.SY.....".....7Ow../.....2...3f)n{..R..R.....U?.....O.{....c..pT.\.t....5.07.. .....07...7.o..,+.,.V.c...&..%.3I.....: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.....I.....,Y.{.....g.1.0..I}.....<.....T..}....t.!x&)..[.7....4.5..{....n.<...#I...:.....r.wW~..zr..9k.^.]KR.*W.J.n.")....%0...)...Fbb5`4'.X..E.../.t.&,t(...@9....\$.....].P..jdU.....H;.$.'%}.I7.....y..$.. ...Z..4.Cm.u#&.%N..1..+..8....y...U.(.T.....}.I..5r}...!..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+wKkEOgx3PG92Eqt9LczFD
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..I..x.....Z^...>B$1.N"}4.....1:&F8..*.X.yL(..s.3.....~2. EL%.w.Uc.zJ...B..S..b.7o\|%..7..'.....N.\|..Vi...q..uO,`/....\W{..y...&iI..\|X&T.....-.....Z..o.~u..U....cF.M....O4}.....~.....:T..W..._s...t..Dlb.$Pr././.._4.b.....R.T$t..$.>hB. +.{.. ....m.w .Q...05..C.}...}.....?..h.....Y .8.6^t....}.y.%.....l=$..[.~..].h..N.....*....SB.\|....8..H....._...G...\|.....;6YQ\|WO.o.}]..'.$..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:s6USl2RqfGhmDrpYM0ofHX4aIVYm
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.dI..I1G..$.".Fg.q... N.nt...3.w.w..~.v.O.....K.....A@.....A ..H.n.D;A@.....A@.....e.y ....1..P..xH.. ....e.9 ....1..P..xH.. ....e.9 ....1.@.$9..S....A@..4....^C..F..VR\\TT.....aHII1..... .VS..g..... .*....z..\|Ek.....<R../55+33;;;+..Y..WC..#...P..... ...s#0::.....522...,.v..D....._.....9.2N.L.'..F$.....e..!..... ...N...`1....G.....'&,f..f.X....!.lp.....I_.....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..2...F.GCC#...].=..C..n#...K+..MOO....."....d^2=.{....U.p.h%.%n...D....XB..b..'"....?h.b.B\v..^Q^.UC.....Q...I.....U.VD...P..{.2"A@...b..V.....jF.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:	1D1AB19B64E1E2ABCA61AE78B3B50310B0A6CF19D2ECFCB4499D8D0BF68600B4D95BC0945EF9FF9B1D016ED61EAC518DCCA1A426F460317C07AD51E2E0479 48C
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.....k]s..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...I...{M..@..4555==-..!..f.....d...>i.%&&&%.u....f..[.....O`.....G..E6I.< ..3.k...',....Y...<.....u...{9.....S^^.q.<..^....2.bb.E`r...ey..... ..3.....Dg@L..a'.x&".O.Y..!e.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.....wvv:..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.LI.....>.....&....."..."....@.Ccccee. [..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+7QJU0QbDQ883ASaoUV4hNgq1rsyhy: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.%...xaI.}...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...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....qI....XuI..]...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:JnieMJz5Tz/gKVp93jQvcv16kjOzbapFJBkjcMNBqmQzOG8qx1QKnse8T:JieMJzph13Evcv16RfapFLxMNBo8qxan
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.0.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.`.!-!-.....MKH.E.bi.d...b.X.)...X4 .vJ6-...;..+/.->Qyi.t...%.T..k;.U..y.C$[;..Gm.....v..*2..2..eee..."!..)...yy...III./..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.!.....>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.|=.....'%!y.....\.....MSn.i.....!...U.$0S .....Z.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\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+mPFGNkfngp
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..TI.....V.v.PZ.-F...".k.pCQ.....#.../s>f..3s....<...=^ '/.~.;.a....{>.g.....*o..6k..k....E....O....aQ.j....X&vG.....{u-....$...CX.....xhZ...Q...Z.....O...I..Id.h.....q..q.....Y..J7O7.R...~o...[....;.'n...u.g..>X....o.]}...>....._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;.....,_.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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:k1hccap27HGVhY2Kn+A3RS+HG3dXrjmg26vh:k1hccewIhYxRmR5
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!...\.!.`pA.+....H.U..."Z..*U.. ..P.D.-.$..,,..$.g.....CB.l.....l.g.pc..Lf..~.=.~ ]S.....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.[> gP....C..G.H.....Osp...)..9x!...W.,..^....$r.p.sOJ.l..=.x.9s&:.....h.`..W"V..|.l{..72.....zv@.#.<...../....F|...c...4.W....:uj@1...~.X.....^si....Z..I~.Q.<.....NAOq...+i`.)...$ L..gV.6#.....F$..hD.g.L-\..H._.u..]4.....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\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:	48:4gv2YZ4gWLpU9JcjREmXfFEV7NNkfKOgV60g0Z:KZgWLpSJcj+mPFGNkfngp
MD5:	3F1535054D4F9626F0EB10CEE47F076E
SHA1:	92EF4F27A33F7704952ECDBA4FA69C68FC32FD4B
SHA-256:	4AB29996D02D93CAD184DD05F7A027D00425B90F5657F1E51CC4C37297A0035A
SHA-512:	2E0EC758B2C28C8DB9F7B5EDBBE8130F049E66842F2F5CC1C013CF23F7C4443CD211BA297250471CDB4F91F1E3251C1E3F7E2151C576FD1A1AE6A36C3776C6 0
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-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[....;'n...u.g..>X....o.]}...>....._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;.....,.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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+LtoQ9jsUBsnwIDGThUe8ww2iJiGEjdKKnnE+Gh:V+Ltt5GwlDQhUe8ww2iJi7MKnnE+K
MD5:	995CEACAD563F849C4142B6A6F29F081
SHA1:	44CB3B867CD2917541B7D5AAED2F14F10FEBB0FD
SHA-256:	3691FB8C60EA1B827092F05FBB1807E34726016C6FF56698D7B81C44D519D22A
SHA-512:	3C8EFEB966B075D06D8344483352BF92C9292F9970C9377BE254EB355EFAF017916737AECCDC704B84D532B7229F9908951A6F2CC3FAD810791CAB224401AD3
Malicious:	false
Preview:	.PNG.....IHDR.....c.L.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....W...Gh...k.Hm..J.m....,X...Eh..%.n.....PHvy$%...[...R..l...(/..-..yl..Z.h..H!.../.|.y|w...7d3 s.s.=.{.s.g.6W.^..)..@..{..'O.LL.....c.^.6xS&O.,...J.(|?.....,.$.....@.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."!f.08hT..m. (..C.7n.....@....SVUU).F.).X\\....[j.U....xd..e...<.W.....=;0L78t+..Gw..-....].....C7.....K.w..._..g.....A.&M.$^.#.!....e.\.P.....;vD..@...Za.@*D..f...! .2w...4#.J..c....K}... .F.u.I.b.V2.k...5..`....*.....M..!.,.;.E..BZ....K..[7....5....,.....K...7+.6..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\0000002T.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+mPFGNkfngp
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-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[....;.'n...u.g..>X....o.]}...>...._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;.....,_.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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\0000002U.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/zVJWedudPZZRdbvczHe2ftFJ0y8Ea5b2AELJj:x4FTnodRZ7c7LrabEaMAGp
MD5:	DB48555480A383CD1D4DD00E2BCFCF29
SHA1:	8060B6FE12175289F0A71F45B894030A0D9F1AB5
SHA-256:	807723D8F90A5BD41269A7A62817547026A117D666D5BEF454EB699C97CA3FA2
SHA-512:	2614C04686299CEE8D56577A1E836A26076D42E041C627177FDB295629F6A80190910947FA794A094C55A45C3D70725EEF29097118E523A38B50C9263C771A41
Malicious:	false
Preview:	.PNG.....IHDR.....gI.....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.....'L...g.UVVz.[.n)...Yqq...Y.f.)//_.I.W_}.,.....S^Z^Y..++.*..pF.....?...I.&...O,.k.d...~..w;Q.....7}1y.....e_.....=y._U....{..}.w.O..~.z.{.....W\q.."....^.h.....}p.+.>m...d...4...`a~Z^....me... ....N]..1...g..y.f.....l..g.).....e[.....Z..RB.KrJ.....#...{..eff..v.[[<.n..?{.....SN9%...V.yE...s2.....e@Wz..I...B.r..<.-.=/t{.v.|..J.....,@.A.v...s`/.....6f....L?.z[T7..)S0.;c....\s..z-C .....v..}Y..{..j..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\0000002V.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+mPFGNkfngp
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-....$...CX.....xhZ...Q...Z.....O...I..ld.h.....q..q.....Y..J7O7.R...~o...[....;.'n...u.g..>X....o.]}...>...._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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.:.I.;.....,_.....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.iH.7UR.`..B.f.....<.5n7.*WR.c....I1.....<y.%...-..."Y@.*...)).(...I...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\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:o4KSpFN6Ud4c3p2Il1yavNr5spYVJzimlfZ:wGN6Udv4IKavLBJz/r

MD5:	0693DABBBC411538D209F32E22F622F6
SHA1:	FB7E675406FA123CDB7E058D336742D6A2E8DC8E
SHA-256:	2DFB2E7A1A3AA43C673D2EE540D3C366CEB12105EB5441F98992FC06F4284013
SHA-512:	F07732660EC62DAE58EB02E2E9476007EA92BF826F642BCA547097136AEA01D29FF69D9B0CD0F5D65A5E15AA66CA4AA4804AA171A3504AAB198631C643C90C1 6
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..:I.D.S>I$A...I.....y.9...f.....3...Gh.....}_ .o....n..A@.....A@...L...2... ..... .x...#. ....1f]9.[.....A@.....3 ....fE@x.YWN.....A@.....1..... .....Y..J.Y.N.....s"...../..rc.scuyyyu..\s....t.oi..j..Iv.....Gr.#9 %%%9%--....d.T...r...DH...6.....%U..A@.0.....rAD .....2.5.....L.R..=W...gZ.`o..-?.T.Cy.:...y.9..y.EE...v.....1..R.....1."....`"...ss.....i.!.hY...Fj*....%.-.Gw...HJJr8..6...#.....!(.? P.(.....8(u.....*..OOO.....dgg....Q..=..c.y....A`S.@.....3.CC..GFfg. .I.I.COrJFFFNNV^nn^^.z..%..(...^.b$.....a..y.LMO-.,ylV+.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\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:	1EFC74C28190DEE2D2732390B74049A1B120F05EFB8DC6925207C6990AD20450FFAB40249899A9DBB82E8F92A61F770E120A450CAAC7F8C5F0742586CCE0EDE 6
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@.T2 .....xp..! .....d@...!.....(*B@....S....B ...O..QT.....! . .@<.H.....! ..O%.B@...x..9...C'|..{.>Z../~^.s<<V4..ujo..v.Z7..EwT.....@.....?.....~{...K.....C.....bB@.$.....C.{....Kf'S.....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..I}.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...I..(

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:jB5Gg4vMs30WIn5IVeRy1bY7DqbqQBAeNjukXIN4AXat:PGYuEWV/YH7e1uA0AXat
MD5:	91CB7F1273AA003076401081B8A22237
SHA1:	5157144069E7D2FDAE60B397BE5851E75BDF7707
SHA-256:	80682DD6472E8D1136BC5E20F6DE87B595562414B19EAB8E965736FE992921B0
SHA-512:	5A8E3C0ED0DB94BFE359C63793F12F3D7B3C37F3A13A5C96634BA1DC8C9E50FB1142FE4752FD9FBFA39A682F78C54AF868AD337EAA787801FE5F66D8F55A81 6
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.PyI.d..I;...;.=.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$C..\|...I...n...~.....,i.....e..=..?{.....>r~.Lw.+2..\w.)w~...c....h..u..%...PE...f..'..m.ZE.1.\....U.`X.....$...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...ehI5U:..66V5sJ.....V...]Y>...1kQH..2.....d....S....I...+..].p.....m7...Z.. ..s.D>.K/]..?.I....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\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:jgxmx2Fa/+76A6M6Y7rSYRv47cwbkkapeIiRmDGd+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$....AE..".l....+G.>AP@D..e..".".A.Y.@...K..IXB !..!..c1.On...== =3=.3=.>9O..u....w.z..-].t9]B@...!.....Z...B@...^G`.Q.&S..u$d....B.Y..P.w5[].....B.m.D...! ..@...Ls.Q".....".S....B ..D.9.(.B@.....b@...!...".@..! ....T1 .....i. J....B@d.... B@...4..%B...! 2U...! .r@@d....!.....*.....9 2..D...B@.....5jT.@.{..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..I.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:rloPN36BoJ9JK5lncTww67QKf5wX5YgM5s6cahePwnR6+eA9zQU13ALcVz7wTQ8U:rYN31JH6lcbjMW5Ytmyqwp9H7wY
MD5:	B1FDE66F75507567B5F0C6C07B01A3A1
SHA1:	80B8E6A923E853232F66C874367E90B5C9CAD7AE
SHA-256:	B9C82D2F31BBE409D159EE3C9129CBAAC7C6F6C81637AB9B6DAB3C11AA74B7F1
SHA-512:	FC8C6038D3C2F5765D7524E969574ACD10AF6FCCFD45FE7C6DD4A8C2669B13EE3FB1A8833E94A046AB7037018170B5B87B1A2742E0E10557C413AD634BDF343 E
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...0!6_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.....\....]..."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:JNu6DMLaZsMhtLAIa0wYMAvI5V4DDQ
MD5:	875CFB3B5C3619253223731E8C9879E5
SHA1:	6372F4F5BEB6EEAE3EDBE5B62EE73039B40AD01E
SHA-256:	CC69BAE5D2C8F56B28BA4E3C6A11F57C4E8CCCE69943ACFBE7E63B4FC90EE5F2
SHA-512:	47F45A3275B8454F8000F4567153DD7D4AF3012005D8E34CB18AED6AD69083BEC753E607F275FBF3EFCCB7BA00310A04ADFBD5FA5B73E6BBE47CE73901C35C A8
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..x.U..I...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..".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.... AIm.....~.

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:	384:1I+zN+iNurNE/tBdEC/vkape2XHYdhOm+BI6C4:L+zN+iNurGNEC3fpe2X8Pa+
MD5:	3A5CD52E925A7C4A345047D8F06C3C41
SHA1:	9C02828D83206BBD3EB58930C8C65A6CA5DBCF40
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.Pl"@....(@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\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^.]ip...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.=$..!.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.....]..;...6..kw.....N....z.Q...f..q...xk.5....;.?.Z.c...`.....4....?.....VV.u~..<_.....sU4e.....g.c.G....O/..r...`.G).. ..#d5.O..w..{....twL1I.)#&hF..K...M[@.Dl..V2..j.3..s....3M.....v..!....V..c..B...|..e.1....7.WA0.[.\.u.).$7.f.+.....8..e2K/.%.li..`w6w.E..[?_..?.?..I.k2.s....]..f....HM.?w..d.9..Rr....Y.c.}. s.zk..rc...a..I(9~.....m...Z.....I.....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:vpXZavBpl00n1Pt7JquG9GYHDK/5cxektxMQjcie9ZZkx30eXJIb8FKRN:vpZaDyc1P1Je9G62/5clpjre9nQkeXJY
MD5:	31579CA3352DF8FA4E3E7F48C7CDF672
SHA1:	AA682A3C781BF8EE43B5EDC9718E64CB79135F25
SHA-256:	B0E7824BEE2C896279457D87E61E902431BEB528D830524CC4DFAE126E89FC24
SHA-512:	782FF9492E3ECB11C72D316DDD94D1F3E94CD908FC9452A37DA6CA30ABCFE9AB2BCCED8583A569DA68626BCEC730408AF86997E295637BF64AFF5BC768F3E 309
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.>@.$@.v.PO.p d+$@.$@=e. .. .;...v8... .....f.o_o{....~t...n.S.N..?..._..L;J.H ..,....7.}...|....7...b...|.....ObVa1. .?.X.....~.....t2..V>.b.}..0.F....%`GO7.n#~..F....K.~...FX..H.^....k .Z/.2v.W..M.<.;$...v.t..,UO.-]..... D.....o.J..Y.....5.%.I....{.....'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$..?....|.]..)?[Wo.h.'..2P.1..!.....$.NO.5..}...c.;...~.x,|Q....B..6.@>..y..}...m...D~z....L#.0`_.`.s?|....I.....a...=N....c._.2._..6 .]...5....{.^>.lM..;n...k..9J.. S.G..{.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000039.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:	7F161B19B937AB48D4FD2F6E5E16FDBD
SHA1:	BDCE4F1C73E87E609A7FDF245A512CA4F73B35B9
SHA-256:	C863C5E71D1116D69561BD0637F4FE4C4240E9CED05B8A5B056073AD13E6495D
SHA-512:	E915B76FAAC9512D2AD11CF4E4530A19BEA1C7D8508BC218C69CB041F1EEABA3E2E03B1D56E61B032A6418829752C21B8354AF1335466D7E1528A06E6742A46 1
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...I..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..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.]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...Yj<..~.5.?I.fZ0.@d.....*..G...K.....e...b.|e..Q.4.....('z...!G.....2..XQx\.....X...2.\h..X~.e....Z....=....C.1.....w.....d.z.

Static File Info

General

File type:	data
Entropy (8bit):	6.672417559895415
TrID:	• Microsoft OneNote note (16024/2) 100.00%
File name:	malware.one
File size:	134140
MD5:	80a381f900f302d1be5673f54f76321c
SHA1:	1acac99bb1343a9dfd0100042e58e5f4e3a16f61
SHA256:	59ecfd5be8b5d602353660723377ea0b2d517f621b350ce25a9b6f1f1386fd15
SHA512:	b12eca092c29234f9378542ad663f12c89f2a95bc33034985eb64ab7d67a475598b2dad4f261465e36ed9f26327cc75b0bcb59b5d93faf57fc71edac5cdb4269
SSDEEP:	3072:PrfWMlNYf3K19kzCnEEQvSMVnte8ZP1Y6J0cTgGt:d6nInM8TXJ5t
TLSH:	9BD3F8F17A520C85F013EC351AF4CA12EA34876E472D2B0FF5A904BE0DFBD499A585E6
File Content Preview:	.R\{...M..Sx.)...3.1...M.....?.....I.....*...*...*...*....._fh.*..E.....n.....h.....2.* <.L....V...I.....Y....H.).~.....

File Icon

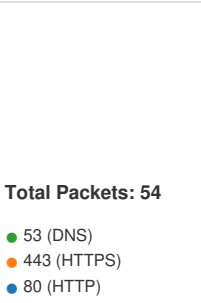
Icon Hash:	d4dce0626664606c

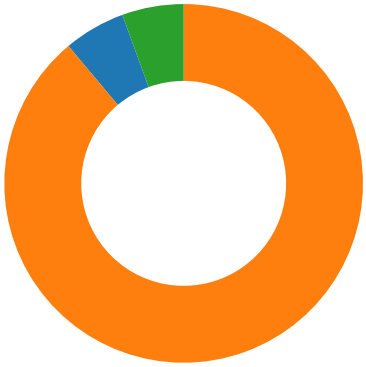
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8.857840532014169 03/20/23-13:33:35.045170	UDP	2014169	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	57840	53	192.168.2.3	8.8.8.8
192.168.2.3138.197.14.674970580802404306 03/20/23-13:34:39.278063	TCP	2404306	ET CNC Feodo Tracker Reported CnC Server TCP group 4	49705	8080	192.168.2.3	138.197.14.67
192.168.2.393.84.115.2054970870802404346 03/20/23-13:35:12.925218	TCP	2404346	ET CNC Feodo Tracker Reported CnC Server TCP group 24	49708	7080	192.168.2.3	93.84.115.205
192.168.2.3115.178.55.224970980240430403/20/23-13:35:29.032640	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49709	80	192.168.2.3	115.178.55.22
192.168.2.3218.38.121.174971044324043222 03/20/23-13:35:36.187246	TCP	2404322	ET CNC Feodo Tracker Reported CnC Server TCP group 12	49710	443	192.168.2.3	218.38.121.17

Network Port Distribution





TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:33:35.128829002 CET	49699	80	192.168.2.3	195.2.88.86
Mar 20, 2023 13:33:38.128187895 CET	49699	80	192.168.2.3	195.2.88.86
Mar 20, 2023 13:33:44.284966946 CET	49699	80	192.168.2.3	195.2.88.86
Mar 20, 2023 13:33:56.577743053 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:56.577814102 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:56.577928066 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:56.582045078 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:56.582112074 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:57.764643908 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:57.764847994 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:57.768184900 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:57.768219948 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:57.768601894 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:57.817334890 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:58.128768921 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:58.128812075 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:58.193140984 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:58.193356037 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:58.193492889 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:58.240739107 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:58.240808010 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:58.240839005 CET	49702	443	192.168.2.3	31.31.196.93
Mar 20, 2023 13:33:58.240856886 CET	443	49702	31.31.196.93	192.168.2.3
Mar 20, 2023 13:33:58.445207119 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.445261955 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.445363998 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.453694105 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.453731060 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.565243959 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.565422058 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.620685101 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.620740891 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.621772051 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.624670029 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.624694109 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.729959965 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.730043888 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.730103970 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.730142117 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.730175018 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.730192900 CET	49703	443	192.168.2.3	40.115.116.248

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:33:58.730249882 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.731909037 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.732028961 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.732049942 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.732068062 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.732124090 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.733721972 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.773612976 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.773691893 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.773788929 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.773830891 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.773850918 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.773884058 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.774624109 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.774677992 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.774724960 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.774738073 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.774759054 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.775361061 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.775418997 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.775438070 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.775446892 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.775470018 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.775500059 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.775523901 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.817564964 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.817715883 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.817773104 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.818037033 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.818514109 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.818628073 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.818630934 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.818670988 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.818733931 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.818756104 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.819329023 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.819433928 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.819473028 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.819489956 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.819526911 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.819556952 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.819849014 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.819900036 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.819979906 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.819988012 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.820014954 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.820035934 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.820126057 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.822726965 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.822781086 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.822858095 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.822875023 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.822890997 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.822911978 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.857629061 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.857688904 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.857760906 CET	49703	443	192.168.2.3	40.115.116.248
Mar 20, 2023 13:33:58.857798100 CET	443	49703	40.115.116.248	192.168.2.3
Mar 20, 2023 13:33:58.857815027 CET	49703	443	192.168.2.3	40.115.116.248

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:33:35.045170069 CET	57840	53	192.168.2.3	8.8.8.8
Mar 20, 2023 13:33:35.114526033 CET	53	57840	8.8.8.8	192.168.2.3
Mar 20, 2023 13:33:56.351597071 CET	57990	53	192.168.2.3	8.8.8.8
Mar 20, 2023 13:33:56.568110943 CET	53	57990	8.8.8.8	192.168.2.3
Mar 20, 2023 13:33:58.269056082 CET	52387	53	192.168.2.3	8.8.8.8
Mar 20, 2023 13:33:58.316931009 CET	53	52387	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Mar 20, 2023 13:35:12.983458996 CET	93.84.115.205	192.168.2.3	90e9	(Unknown)	Destination Unreachable
Mar 20, 2023 13:35:15.991839886 CET	93.84.115.205	192.168.2.3	90e9	(Unknown)	Destination Unreachable
Mar 20, 2023 13:35:21.992082119 CET	93.84.115.205	192.168.2.3	90e9	(Unknown)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 13:33:35.045170069 CET	192.168.2.3	8.8.8.8	0x245d	Standard query (0)	malli.su	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:33:56.351597071 CET	192.168.2.3	8.8.8.8	0xe1d0	Standard query (0)	kts.group	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:33:58.269056082 CET	192.168.2.3	8.8.8.8	0x92e	Standard query (0)	olgaperezporro.com	A (IP address)	IN (0x0001)	false

DNS Answers

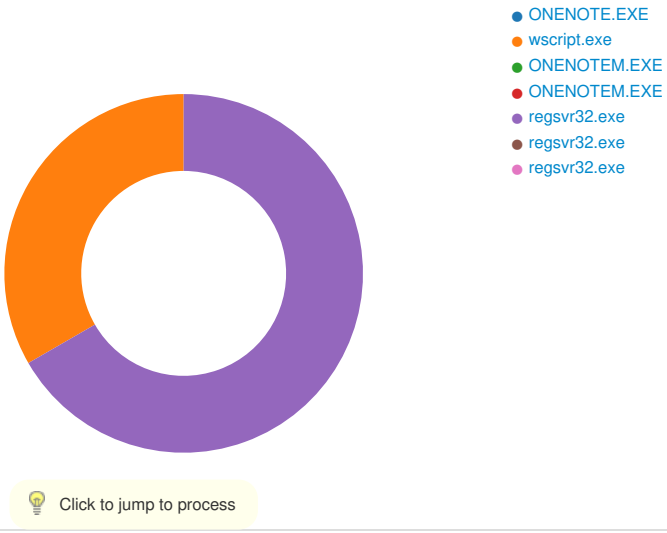
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 13:33:35.114526033 CET	8.8.8.8	192.168.2.3	0x245d	No error (0)	malli.su		195.2.88.86	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:33:56.568110943 CET	8.8.8.8	192.168.2.3	0xe1d0	No error (0)	kts.group		31.31.196.93	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:33:58.316931009 CET	8.8.8.8	192.168.2.3	0x92e	No error (0)	olgaperezporro.com		40.115.116.248	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:34:40.165296078 CET	8.8.8.8	192.168.2.3	0x61d7	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 13:34:40.165296078 CET	8.8.8.8	192.168.2.3	0x61d7	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- kts.group
- olgaperezporro.com

Statistics

Behavior



System Behavior

Analysis Process: ONENOTE.EXE PID: 1760, Parent PID: 3452

General

Target ID:	0
Start time:	13:33:07
Start date:	20/03/2023
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\malware.one
Imagebase:	0x3d0000
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: **5836**, Parent PID: **1760**

General

Target ID:	10
Start time:	13:33:32
Start date:	20/03/2023
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:	0x3d0000
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.00000003.386000568.0000000005771000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: 0000000A.00000003.393189517.0000000005915000.00000004.00000020.00020000.00000000.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.00000003.393189517.0000000005915000.00000004.00000020.00020000.00000000.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.00000003.385846809.0000000005765000.00000004.00000020.00020000.00000000.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	6F969601	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ONENOTEM.EXE PID: **848**, Parent PID: **1760**

General

Target ID:	11
Start time:	13:33:44
Start date:	20/03/2023
Path:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE
Wow64 process (32bit):	true
Commandline:	/tsr
Imagebase:	0x12c0000
File size:	157872 bytes
MD5 hash:	DBCFA6F25577339B877D2305CAD3DEC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: ONENOTEM.EXE PID: **6140**, Parent PID: **3452**

General

Target ID:	12
Start time:	13:33:56
Start date:	20/03/2023
Path:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE" /tsr
Imagebase:	0x12c0000
File size:	157872 bytes
MD5 hash:	DBCFA6F25577339B877D2305CAD3DEC3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities

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

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

Analysis Process: regsvr32.exe PID: **5188**, Parent PID: **5836**

General

Target ID:	13
Start time:	13:34:00
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\regsvr32.exe" "C:\Users\user\AppData\Local\Temp\rad66B18.tmp.dll
Imagebase:	0x2a0000
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\rad66B18.tmp.dll	unknown	64	success or wait	1	2A1909	ReadFile
C:\Users\user\AppData\Local\Temp\rad66B18.tmp.dll	unknown	248	success or wait	1	2A1942	ReadFile

Analysis Process: regsvr32.exe PID: **5268**, Parent PID: **5188**

General

Target ID:	14
Start time:	13:34:00
Start date:	20/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\rad66B18.tmp.dll"
Imagebase:	0x7ff7bfa30000

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: 0000000E.00000002.373894564.0000000002601000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.373814331.0000000000E00000.00000040.00001000.00020000.00000000.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: **4420**, Parent PID: **5268**

General

Target ID:	15
Start time:	13:34:03
Start date:	20/03/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JMgyzwrCUAZpIA\OfEg.dll"
Imagebase:	0x7ff7bfa30000
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_3, Description: Yara detected Emotet, Source: 0000000F.00000002.572181479.00000000006EA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.573776336.0000000002030000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000F.00000002.573888713.0000000002061000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

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

Disassembly

No disassembly