ID: 435327
Sample Name: local.exe
Cookbook: default.jbs
Time: 12:25:22
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

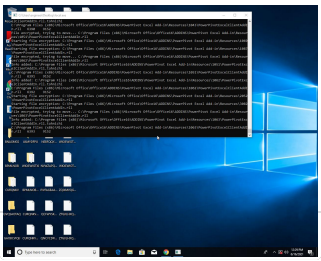
Windows Analysis Report local.exe

Overview

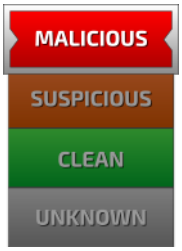
General Information

Sample Name:	local.exe
Analysis ID:	435327
MD5:	d687eb9fea18e68.
SHA1:	0e7f076d59ab24a.
SHA256:	863e4557e550dd..
Tags:	ransomware
Infos:	

Most interesting Screenshot:



Detection

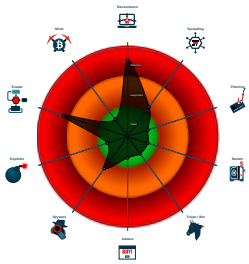


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Sigma detected: Shadow Copies De…
- Creates files in the recycle bin to hid…
- Deletes shadow drive data (may be …
- Found Tor onion address
- Machine Learning detection for samp…
- May disable shadow drive data (use…
- May drop file containing decryption i…
- May encrypt documents and picture…
- Sigma detected: Copying Sensitive …
- Sigma detected: Modification of Boo…
- Uses bcdedit to modify the Windows…
- Writes many files with high entropy

Classification



Process Tree

- **System is w10x64**
- local.exe (PID: 6376 cmdline: 'C:\Users\user\Desktop\local.exe' MD5: D687EB9FEA18E6836BD572B2D180B144)
  - conhost.exe (PID: 6392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vssadmin.exe (PID: 6476 cmdline: 'C:\Windows\sysnative\vssadmin.exe' delete shadows /all /quiet MD5: 47D51216EF45075B5F7EAA117CC70E40)
    - conhost.exe (PID: 6500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6508 cmdline: 'C:\Windows\sysnative\cmd.exe' /c bcdedit /set {current} bootstatuspolicy ignoreallfailures MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - bcdedit.exe (PID: 6700 cmdline: bcdedit /set {current} bootstatuspolicy ignoreallfailures MD5: 6E05CD5195FDB8B6C68FC90074817293)
  - cmd.exe (PID: 6612 cmdline: 'C:\Windows\sysnative\cmd.exe' /c bcdedit /set {current} recoveryenabled no MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - bcdedit.exe (PID: 6772 cmdline: bcdedit /set {current} recoveryenabled no MD5: 6E05CD5195FDB8B6C68FC90074817293)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Shadow Copies Deletion Using Operating Systems Utilities

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: Modification of Boot Configuration

Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Found Tor onion address

Spam, unwanted Advertisements and Ransom Demands:

Deletes shadow drive data (may be related to ransomware)

May disable shadow drive data (uses vssadmin)

May drop file containing decryption instructions (likely related to ransomware)

May encrypt documents and pictures (Ransomware)

Writes many files with high entropy

System Summary:

Persistence and Installation Behavior:

Uses bcdedit to modify the Windows boot settings

Hooking and other Techniques for Hiding and Protection:

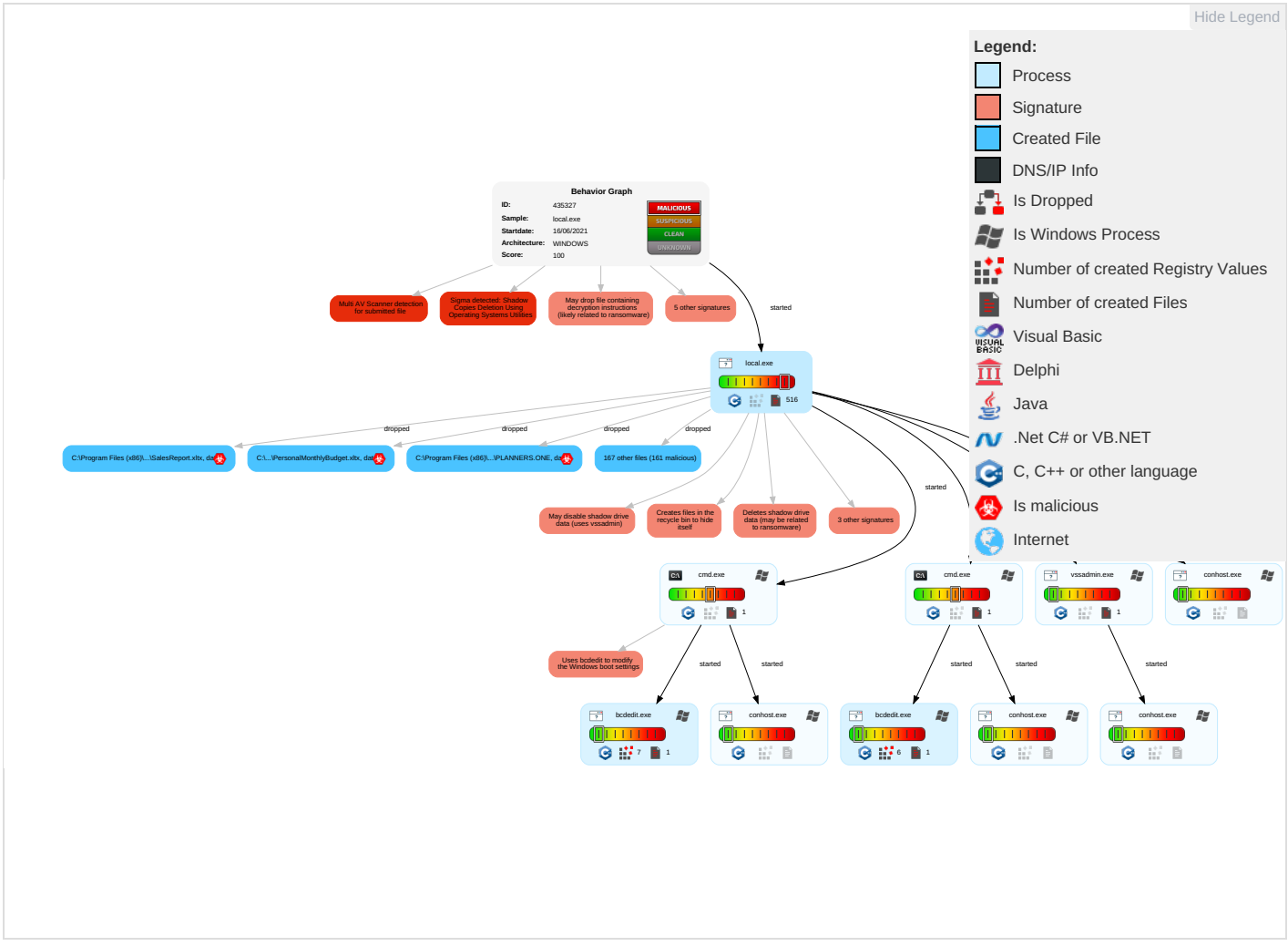
Creates files in the recycle bin to hide itself

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media 1	Native API 2	Bootkit 1	Access Token Manipulation 1	Masquerading 3	Input Capture 1	System Time Discovery 1	Replication Through Removable Media 1	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 5 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Proxy 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Peripheral Device Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Bootkit 1	Proc Filesystem	System Information Discovery 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellula Base Station

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
local.exe	49%	Virustotal		Browse
local.exe	28%	ReversingLabs	Win32.Ransomware.GarrantDecrypt	
local.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435327
Start date:	16.06.2021
Start time:	12:25:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	local.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
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
Detection:	MAL
Classification:	mal100.rans.evad.winEXE@12/1025@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 97.5%) • Quality average: 83.3% • Quality standard deviation: 24.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\$Recycle.Bin\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C

C:\$Recycle.Bin\How to decrypt files.txt	
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	**true**
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\$Recycle.Bin\S-1-5-18\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\$Recycle.Bin\S-1-5-21-3853321935-2125563209-4053062332-1000\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\$Recycle.Bin\S-1-5-21-3853321935-2125563209-4053062332-1001\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51

C:\$Recycle.Bin\S-1-5-21-3853321935-2125563209-4053062332-1001\How to decrypt files.txt	
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Esl\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\ReadMe.htm	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	16472
Entropy (8bit):	7.9886061963008475
Encrypted:	false
SSDEEP:	384:kFK+qsh1Zip8jWdFxEpPR6tE4ilf/t2Djz7kz20YPobTjR7EHQC:wh2ujO+ctKV2nPkz5YwF7EwC
MD5:	99F30D545A58BEC83C331447EAD03AA7
SHA1:	ED727EABC953D3583B63A576ECC9D7AB7D82B9A8
SHA-256:	757C23834C8F3B975394EC68F0AC1F63BFF127A1C59ACD6852920C006411136A
SHA-512:	1AB342E1F678874EB045128C0E6ED71B8F2CE6C1302D109A7E59E4527BFE48284F43A78E9B3AB182A151B4F59AF27155C61F74969042C51EE0569C34E33D7EE0
Malicious:	false

C:\Program Files (x86)\Adobe\Acrobat Reader DC\ReadMe.htm	
Preview:	K.....F}.._ `.....x..N...m.1./.....[.l.U...;~.0}.....TC.f...m.\....6#9.....EX^.....P.1..m...`r=X.V."....%/..@0.,..G...u.a.....qF.K....G.8c.. .....KL.....~.2....&.de....a...E....4..+$.-.....".g.g.6dZ.Z.....#@...A.7.&? ,.M..p.l>)m.&..-0-..~..6.M...U...\.(.*oV...<....g..k.x.b.}.ZC.T.*.D.....N...i..%.w....75..+=O.x(....O..&...:.#6'#..@b..6N{]G|)h....E+..:u.o.\..%..x.m.M...|.Vd.%d>+.s4w...X..3k...Dgt.h)c..;...]..........chH-.:..2..?u.53....Xh.....9....$!..'..N."..&7I.8.(@..A.a..f.q....X+Qq..7.?...f....Z....r.]...k .....4.G;..}....+f...c...^u....xG...!3Q.c:.JQ. ..%lCp.4.. .....b(P.2d..v...`...!(.8kRe..v.E.rk.u.EX....&.....f..7.%~.....i....R...>.X...9....@>..jO....2...?..-.cO.....a.AA.s[....".7...R...x....C.k0.P7.m....?#....'.-.....].._.6RJ.....5 .@...O.Ht...rEI.)...w..9.....&.b. ..a.....A\;...5.Ie?^.K.#.....S..<.....H..;.7..~cq..P..hI.EJ...i...7.ux....(.....bq.j!.9.*.( .\H$^...`.{.A.../.'...|..4

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\1494870C-9912-C184-4CC9-B401-A53F4D8DE290.pdf	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	184408
Entropy (8bit):	**7.998948390886746**
Encrypted:	**true**
SSDEEP:	3072:0S/9q1VWYMPykb0oxRprsKYcPNKJazX73iMWCd5fPFmCjcOklirsWNd9elsJHSp/:0ugEYoyk9prslcTXjiMxf9mW9kQY2elP
MD5:	012527F8AAFFA729A0A96C13B5A43510
SHA1:	9BB7841F2F0A7C5FDDDBF07E96C1C805037A3BD8
SHA-256:	6F7CAC6C4F2074DC4A2D5D29F9DC573F42F2DEA8315F745EB946A3C2FBB82BB6
SHA-512:	8CCBFDB75CC440FA97FE8E1B73A21C9683486FDE128BC82F5777CC08ECF401037F5DCAF7C20A47BABA808BA8493DBC41C8D8168B3B8190A0184547E64B28E3B8
Malicious:	**true**
Preview:	f..}.,...).v.P^;.Y..obX.KB.U.....Q...:.s..<.....,g?!.3..0.....l...o.j.M..S^f.h....,>.........,..G....J|.....y."|...wD/.(...E.....VvZ%...."...8...Y..?.J..*..P....F..b.'lE./H+.....B....%n,.5~&..A.z .....h...3^...X:...>a.U.ds.O.....y..Y+.r..w...P.....SFU.4.%.<.\tO..w.@$..j...)@.o..b..X..&.7..k.4|l....g.he...~^`b.....Z...{[:....r]UNrLN..}<4.aza.f.....0..TM.5"..D..O2NR.k?6.L ..X-.N....R.j.=;...o..7<1....I..f..A.....=(m.....M..<..`...`r...N.H..m.p`.t(@v.....}B..=.$..a....M....w..^.2.C..T.....].9..U...tV..6]...'.9*I...,or.....4WB.4....1...G.....;?.44.+..C.4}. .c...bZ:.X...b.~...m|.D...~#`.I.QWE.".M#s.N..m...@.p...1..&.....zdo....)V.....g.X/..e.E9.]......7d...I...Q....C.=..>2f...m....K..%.G/.H31.CY...D..5.&.wX.h1E.&..H.2@.."C+E*.n...._. r(.r?.{.t...;...,.}.Q..Y...J'?.n.....n.1..h...Ok[%%.{..u.KhK.5X>t..a.....c.....1b[...<...{R..;....L.. ...y[..\>a.#R.T....C...'..X...C..$...^.\.,B...h.X.i....).pf.,.E5r.?B.>#....t...S...V...%[..

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AGMGPUOptIn.ini	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1815
Entropy (8bit):	7.912196079796638
Encrypted:	false
SSDEEP:	48:lv6SD1FHZIP6KugFnUJxysOBYOgoa409pbcGKKDM/oA:lv6SD1e7KylYOgM0XbcGKyM/oA
MD5:	ED052F2494FA1C446C29E1819FD8D64E
SHA1:	29C3E11BC8713717CBFF2E6ED782C36270B27121
SHA-256:	C3C89A43A3AA505C9F2DF1CE8D3A9DD18BC96877F55AF92CDCE16CD04E82611A
SHA-512:	9A9A97A1AFE1BA6322CB4F0695BFF7946394AC2BFB3343F48A97E67B0BD431FC2407A57D64965C17C44FA940E703E08179B5F7F7195DFDCBC79B110F22605A9E
Malicious:	false
Preview:	........C....Lt...p<..v^,.P...W....uU>.+)....f.........6...e..(....\UJ=....Civ.>Sv.....'w..)<....!..ZS..B$^...K.....g..E.S..{.AY.h....}3.....7..#..)s.d{uf.1....N..P....WI..Dy..a.....m.~Qv...@..[H..lY. ..,...._pO4.msd.?....cO.D...C;..L..NH..."7..p.'r.)../...[..E.w.....>;../.....\.q:C../ .....2%..N..T./.w.<....jw..!...EN.Z.G'.9..;o.....Eu..5j....RX.<..m.....n..H....T,..Lh.c. EZETje..+.o... .v.4\..6.a.KF...te....b....T... cb.P9..%.r.E=;.dB..^?.mO=V.....q;7=(....rxB.Be0...M.K..c(.I.x..V....J$b=.S.e...K.9.'.H.$.....y....*|...@...C.c.`..~64.....9..*1....^'6.@.%*...U:"vVT...a; ..m..;...;.....D."4...N>.uEt].;..^...3..5..'...!..dc.....V.I..7....*d..._../R..q.....9...<3.i..qu.\\.V"....*.x.....&....].O..uj?..;.....Z....$7>.....H.S.]m..c.L.@...B.%.{..=i...F...$,...5...S...VE./ ...h|k5n.x.M`=..RAH...."..!.x..Blfn....O...l...pB8.LZ...SC..3.....JD.H...{*.0.f.r.....|"....~...y....O).7]$...v.X.CdT6h..d..2.&.#JT"..Y....q.aO.1e..(.En6G.T.&=R

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AIR\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E850D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain access to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your test files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\AppCenter_R.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	403
Entropy (8bit):	7.415041759333214
Encrypted:	false
SSDEEP:	12:jZOcM3yp6R4kNqaV5kWcNVyN1VqbLlTYj8:jZOwp6R4kNtV1cNVbg8
MD5:	7B020BBDB8DB55EBB15299D82780CDCD
SHA1:	005C7F8734959A2CF5ED592649EAE78CA830CBE7
SHA-256:	6A9327D26EC2F7D1F949100CF8863C072755F7ADC6373ACF4DF987A526CC4C98
SHA-512:	5AC47F183DDF9880709D2ECCBE3ADE76C447E7A6CCB4FB4986C92C39EEE3900E453F9079B28C530178CCD409A6C9C66E451B38C866F684FFAE3F4FE0211CD9 A
Malicious:	false
Preview:	....Q.E...kJ*.W.).M..1S.....a.RVv4|....1...w.\.g.....z.....FuX.|$J.iF...p.rR.FP....:.ir#.@.....C^Us..\|),8...c.J..g$~.....F.r..s..@7...3.....~.;.PD...|h.c.....w.U|.../R...W....c...+e. .K..cm....n|..c....0d.!H.....f..O$;.[].d.^}!+..K.....`..n.s..3e../\..~..<.....&.?.^i.....-.....%..w..,~....$..J:K.Ez...~!o.]He.2.....g...*..f\..n.#.2;. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\CPDF_Full.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	457
Entropy (8bit):	7.570111194195533
Encrypted:	false
SSDEEP:	12:KtzqPGMNLqLGEGCbPoaaV6sty3ZuxGAYj8:SPMN2LGqbgaajAZqa8
MD5:	76FF7E9E07F8B7EF1488375CC6D74E82
SHA1:	61AFDC0BC19C8F7E13C717DD80B1FBDAAB2D137B
SHA-256:	B3CE8FF4C6B39ECBD53C229683C7F12663BBCC7946EEE308B9A0FDF946BFEDDA
SHA-512:	B08598E60B35C354C87743D18D45B5870941BD50543474DEDC02F0273BE609E9867D861AE319500E253499AC1CD9390DBB93113286F3C2A525D7D987C0791F1B
Malicious:	false
Preview:	........O.....n8.80s@....j&.....XYc.....J0..m..P.~G....Pz..``}AQ..)&.a.yO...../<X....`n.....:p.....U....<hDx.....b8.xDE.n{.....#d.....s.....&m].p.H.l.../....X5.b... ...>2.....F.;.]y....R...,.G U.4..;...L.....7.BLU%?*.....x.-\{....g...B0...r3F..+..k..A.=..rw.r....s.....3.....*.d+...^.T..(...>..Ltt.c.....i7c~..5`m..9..g.!x1k.;..Oi.[.H.E#J...uo..#."..E.....(.V...].g..B.8.Z9.V.....R.$.u. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\CPDF_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	470
Entropy (8bit):	7.55416624999571
Encrypted:	false
SSDEEP:	12:DOCQPUvRFPgVp20U4+y+B6NPe4Um95LXUUTYj8:DQs7Pg20OwN5v5LXUj8
MD5:	68935C5ED6E12F61C606E573767C3B66
SHA1:	CD452A87C9D6D9F073879855DCDB3F373D925C52
SHA-256:	F7C128034B85A1E023CC7DE2E16A2B59C22E5F31888A43FCF8C298174E8142DA
SHA-512:	CF9BA34CDC0E252A1556DCC44AB0C1B20D4D85A5A0F6AD7741AC0A843522C73D69333F7EDB39D8A854DEE998ED73DEC60EDFDC77A5A10DBB41F4DD990F1A D2A
Malicious:	false
Preview:	d..<b.>....2.!..V>.L...V.;.=V..g+.p..1.....;.2.M..X[.. .~.....o....d...84^.|CHv.r.....<....3=.Oc..Wu..Am.s.z.V..:).u..rfi.3..Y...!...."....]..dC./,...26..o.t..:..jh#."..&R.Y.@...C...y.... .2!uM1.4..:.E.Bln6]o.c.b.....L@p.<.....Q...4.UUlE.....B.S!...(.....4.@..#lj6{.....L[..D.?..6.oEMI..Y.z..^.M..y.Z..A.....1Ec...v..=.&.?....iK.....1r.7.@t:.='e...Q...\. s`....:'/..H]...l. [..%.xbg...:...x...Z|.00eN...Rg. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Certificates_R.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	777
Entropy (8bit):	7.758104950981973
Encrypted:	false
SSDEEP:	24:rtE/LKeFljA7n8Zh+qI7jioVQM3nHqA+iCPFBZV8:r6TTj3CDj0M3HqA+TBZ+
MD5:	A798C19C8C7F77700D424F2AD791F929
SHA1:	08DE9FC052E99EA2CF840CAD11C3A81F4DE574FA
SHA-256:	8BCD8F4ECC1CC47CA6CBBFBAD6BBE0DEDDF7E0CF1BFB060CF126249A6D5C1577
SHA-512:	4DD786DE60A6AAC81674EAAA427B99EEF9B9B459EE3D6C0ED0DF22FEE6BD519A0E44ACE5108C0C97D70055F537B57B6F55CB107469A6D9C27F25AA8BA7BD9 4E5

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Certificates_R.aapp	
Malicious:	false
Preview:	.<.a..(.C.....(....oY?.@h.G...t*d.(2w.. ....>..SM|..h49...^..X.....\.lly.}...@..HQ.g.M.S.EN.h.`.*(..+m...v..R..8T}u=...b3.....@L.X.(..h....&..0...K.q.m.`<...Ja.....lr.p.:h....$....}9%E~U..?....J..6....i.....A.G.e..A\G..\G...j..g...d....{!w.GY4.3...%..EM.|k!...-.UJ;N...m...+.],..r%..W...dp9YO....D.1..?%.....u.....-...8.3.z.qOE.r.b^eK;..)..Y.....w.4C.....-.T|..`...7....7 {.}..dM..cj.]...u....^{.v..''6O....r..):@g..To.@.....:...j....D._..R.Y....G;..A..5..N...N.,.).....;.)..Yq..',.....k,...^....o.f.l!t.H@.s.....~Xp.....".Z....}..p.|a.....&.4..))..q.F.W.GY.t...''...i..z...A.+..n...0.YO%CWi.C.[.....;c...)..:.t..?.mD....5".!..E.|K._[...~.....-...M.h.....|..i.Z. .`.{.S..=..4A..X.....3..q..i...!. ..bI..1 ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\CollectSignatures.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	579
Entropy (8bit):	7.642361079189033
Encrypted:	false
SSDEEP:	12:Y83jMiNSczV5ALJEn3tGMnahV3Ks4uzWjiCsA9Qcz2f9e9Yj8:5fNbzrALqn3tlnaD3Ks4uqjvsAOcz2z8
MD5:	D4CE5EAC8187F75CBF8978D95D8F005B
SHA1:	459BE84ED45EFE7717A9C35888B9D2E7BC317530
SHA-256:	02B24FA037B92518BDEF97732DC66CD0D29239DC9CCF0FF0C5307B4679517E1F
SHA-512:	54B4F0D02DA0B91C50C141633B428542CEF043F2C90EEA79FBCFAC4576B967CC3592802EA6AF5C4745362D51D0422274A4AF043168A3C52F8E571EF1E74AAAD
Malicious:	false
Preview:	!a....<.L..&t.....#.tJ$.@=....#... .vH.....a#...3...h....<....l6O.H.>=i..<...o.o.L&...M.T1.vy.)^..a.%._.N...-..73.....09...n*.e..^.8./w.&...P.}p,.....`..@n9-...1.i.p....qw.r..v.H.[X..... ..N.....*.....h.JeV..f...w..^>dT.._1.W~Z...../...-.m.<,\|...^...}*.....i.....B.j.\.....,...l...c...L,4....Y.....`h.7X.....0w... .[.../.. .x.....Es.q..}...4.`g...3..m/.X+.@)...\.7 mC..y..*.....G..o.Y ..1vQ'>.YB0.F..*pF...x..u.....c....X....or.../.a...!.W.kF;5JG..-Y.7t....?$x.....HW..,.E....d@..D."2..P....r....1...O..F.Q.. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Combine_R_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	509
Entropy (8bit):	7.594902816105474
Encrypted:	false
SSDEEP:	12:1ph/8utM8Aslqo+NnG873sxOY9VTBH+x30wnpDq8JQoFfBYj8:1pi8LJSAxOYl+HDq8SCfU8
MD5:	9F4B71E499043513C8C6B50BDE687351
SHA1:	67F985DBE0A2136176B8040D16F6BB101EA39FA8
SHA-256:	50DF34E8CB3C1108F0DC068DF89A098E1A30C58FDF4A3781F2C28C5A0C04E1F1
SHA-512:	5F111CFB04881D95041FF98278FE508398E480D076BF33606ECC348718260336DC83013E79C98158CFDC62E3DB552B2FA487BA6D597409FC86FA472EBF6E5A05
Malicious:	false
Preview:	.[,W\^...'...E..N..35.6..k...gD_..n..6.....`....ZXh.....g.o....:...E..].....f.H.ye7n{u.a9gQ}....O.J....~Q#.x6.7.n..`_..c.11k.&.EB...iT.H.[...P..n.#.[T@[._..<...<...n...O....a%X4MA.b..4;~...r .....0.N+zgu.7.........<Ci(rE..M..0..; ...1.@...j.,p.?n.2b.Ok.. ..../...W...?nsQ:.xz.....@1.E.I`%...^H..^.7\_|.....oP.... .a@..''...(....I.gEv.r.....S.2.A{:.1...p..$`]r.Ja\..j.+.....b/....^&~..... ..+.....b..$..E*.~;.{.....3.#.....u.:$_.c...U.i.5.. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Comments.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	16472
Entropy (8bit):	7.987940419267157
Encrypted:	false
SSDEEP:	384:kXEnJ+x03y7ofRSZ77feHB/KAmaSMmOPgjPb4wtNraBwF:kUJU0iWRS1elMOOb4SuBwF
MD5:	B54ACC849325EDF2C27F13ED767D1A7D
SHA1:	3AAE4C083A72A3D71A0D90A9DA72A7DD7F41648A
SHA-256:	91C7415A712F1290CFE1C5A6597C9CC9C5A168FA425F6060BD8D5CE09D4C0FD8
SHA-512:	F20A741C2E709F2CCEDE8EAA047BEB08F77C78D73512A1A84999BB6CDA3250F7AC8A48094ED322438BBC7B15B93C7F53787DF1CCFBE10BEAA7EB56CF583EB 6BE
Malicious:	false
Preview:	t(....O...3....~..{H.=/..x3..~.%.5o.....q.rd.t64L.....t..UX..~..D..,..E...c..''Y`C....F.v.=..V.r...4..h..c...y.S..5..w.h.~#.....;U..x...;..L..m...p...ZA.F.-..~Hh.&....0.36..*.....~.CU..S....O e0LmI.T....*...}.....P#..}.....G..P..D..;..z.B.D1h.....''3Z....QX.H..D.....p+8. ..Y.T.9.%....C.g.:.../}Bv...;.....P..e..p._.T..l.o!tx....@.$@.P...$Q.B...Q...s.....5B..{.Y.e.8.....02..$. .h.WD..V.....V.5.\|.....4.`6&....-.O9k4...P.....c.I.....xP.c.*.....$..$.+.+.MA`.....;...22..pa..f..z.{...J.....r>..v.y.m..X.s....kWb.d.z-.....:+.. ..N33.:,..0R.K.e..e'.C.QK.T....:...@.X...] rL..-..&.P(..D?.....yD.$.+.}}&.m..).....R.....&.j...h...h....D.V.k.....&.Tabti..).....<-....Y..W.....6.kZ.b.x.^..=..d....n.k.&.>.....$CAQ.]<`....V.....h....[.....X.A.V.....L7..r:. .x`G!.....}y(w.....+...0&.....J[..5.B.>M.....WR...z0.S.(UL..l)f..P.....P...j.^...q.....k.....in.k=\.J>Y....O...m.....Zj...'..P...^.B~!..@.o..s%.0.....[. .

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Compare_R_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	88

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Compare_R_RHP.aapp	
Entropy (8bit):	6.109944260658172
Encrypted:	false
SSDEEP:	3:d/yNADq9X+SdZ7TQBdLlCAn3FVvZ9EQDiH8:8T1+SdZPKdLlCA1NYDH8
MD5:	C7DB42995E13886228AAF8D8DBB73B38
SHA1:	39BD9D778E3248FEB9EC044F3CE77EBAAE3BC285
SHA-256:	34F4FF9C1824AD0E5CE3EFFFFF5EBCAF6722C0A5E2F39A825B82C2A1403902AA
SHA-512:	CF0BEA9CB6940E0E986E0FA7FE916FA6B0369A35843C4BA5641A7E1386542284E9D6307890E4142AF79AAC9342ADB13DD7C074AAE45F730F0EC9A58099BB7A64
Malicious:	false
Preview:	..Z.X.p)..._t....R..G"Sx.....^.'($.k..xIO:h,8...CZ.R ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\EPDF_Full.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	489
Entropy (8bit):	7.57037093535382
Encrypted:	false
SSDEEP:	12:z6/VzxAryWkgh+snzU1z/pOKEi/G1mGtQLQRWFL+3NLYj8:z6RxAeWt+y8xO95tMkNO8
MD5:	CB4C75E1002B393D3838AABD452960C0
SHA1:	9FA807952ACC2E764B1D0BB8402630CA983C0796
SHA-256:	615BD4385658FC996D99135D1426A367850F1FDAAFE904DFF2E73385363C5F0D
SHA-512:	D90D38852B5E865A5A9052CC7F363F8F1AD734490A3E3246CA999CA6A19C324F803BCD356C8AB76F47ED40147955E3171552880AD8685F0B7A55195FD1073285
Malicious:	false
Preview:	.*._.w.(j..[.9..E.D...w.....@v].8.}cy...v.[....w...D'VU.....V.U..1.I.G..G..E.Z.....!S.....^yZ...._.....Z...tO.Y.;..%..YK....yU....!.....]..T..:...B..K9..e..v....#.k....v`.[...y.xo....R..M.<O..V.D9w.)..`:.....N..O?....^.5.=z..n.pEz.%... ....8.0...Hj=)zr.Q.r.Q....Z.....4..#..yM....o.........>..z.....:..8.6$~.8D....)..+.....v..g.t..a..;]n>....K..nkfuH..@Z.....N.....vq.Qs0...9...Bvf..XFaXh..WQ...b..?.Y\O.I.-....9.7.Ug...p..w.[. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\EPDF_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	7.581935929603809
Encrypted:	false
SSDEEP:	12:qEgxs964pfycCLlVPyROWNKaTjo8xzjs7jUPdYj8:qvk649CLjiOWkaYejUjWQ8
MD5:	7E56F815B220945EF08F351DFBCADF2B
SHA1:	F3B857E1128F26ED1A156BDC6752ED9B708B6ECC
SHA-256:	FCCE8F757957B8CE53676DF4198040C633E81F3BBEE03776A0914C63964C65E1
SHA-512:	27E6B3DCF2803B058B8AD6E9557C395E9CF890574873EBFF916B451FEF69966DA2512ABB29E283044389703B84FA5924770CD288526AA80EF97CF13FABFAB4EA
Malicious:	false
Preview:	..$n*....R....&.1CIC..7.U.!e..G8.a....8@D.....n..+.a.a..zV,.F1..?.H..y...5..\N._x$&&.=.d.-.I!K.x..c.....R..Ok...Pd.`x..j..='...\..:q.0.]...p..LM.O=. ..z[{".R.....E.].6[p;..s('..pe.sb...{.V..l\.r{G...fY..^;...M.g...|..he..q....Q..V.....5.Q+._4l.eH.O.....K...^..*.s<N..=...;._.1.....GWI.=...t.t.,KU.....PA..".E...O...M..W..>..O.U.Pm...P.w.TY.S..g.=.Y.Jp..t[....5...G.Klv._.$.....[0Iy!..uW..e3..&./.....].W.&...".....mj..<.k".9...^.. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Edit_R_Exp_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	496
Entropy (8bit):	7.572182205873547
Encrypted:	false
SSDEEP:	12:TzHE1EBt4bGAIwz+d/QRmzoZ5A7CFe0evTenYj8:vHAEBCbGAIwkQ/k7CFCK68
MD5:	83D186B5F552698E76F0CD506C3B240E
SHA1:	96629C196EBA445E5EEC3943566868767E9CD2D7
SHA-256:	0DE2801292425FF1358E0771B8E344D80FBA8F087A0C903D4B1C084EF65622A8
SHA-512:	31D03C456C08FA599FF93FD3CED387F35AAE99FB563166DA3A4CF170C08A045F2743D0CB7B6FD01A22D4EE5B06EDA7E2F56C8AAB32869D095F116720E475681
Malicious:	false
Preview:	.KB..M.`M.+}eX.aj@n..S..i....Ww.J*.....u...k.Y.l...f..l^.~..g.*.?...'.j.0.....)G..Zv.`@'...M,.#...j.q;.H.].../.t<..V8D..o#PG.%./.8.*..=...ilC..3....R.GS.=|hG..P5K.H)...X.==.Y."e.....=..mW.XLn..lt....4.<...?.gsa.E..L...C.b../CU_.U".|A;.d|..h./."W...Y.....]0.XX[.....m%..{8.....B..*...u.i....s\~KJ. ...1Z...-RHY..o.2.....jW.N3w:...35-./.M..^?6.Iy.....i.(.R...Y.c.2....T_.V.=.. ....s"k.e.....\4.v@v.H.....8,x.R)...=l.....]f{.>... ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Edit_R_Full.aapp	
Process:	C:\Users\user\Desktop\local.exe

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Edit_R_Full.aapp	
File Type:	MPEG ADTS, AAC, v2 Main, 32 kHz, monaural
Category:	dropped
Size (bytes):	491
Entropy (8bit):	7.621297094282669
Encrypted:	false
SSDEEP:	12:S+Orp2VVFMVkKmwawihRnUzYYsbW8miefjC2QTFzs4Jc1v0yPnC/DZNYj8:Y8VVF4kZxRnUzY9bqfWRFzsKc1v0L28
MD5:	3F02EC90C926899BA38C9E1B3F40240B
SHA1:	250D4DA75EA3BB59B9CC6C9A7D34B4099A48084C
SHA-256:	D60A7019795CF327AAA1B267839D15C647FA026010FCC7EB6D4D1E366A8B7C50
SHA-512:	6ED1B09D223DDF65C049C1A9387AA32DAB058C1A6397B2BBC4AD334EBF6D2783C9EB4E774CC6FCB8A0EF96B74820E8DDB463F63846761CA8970D0FE378E74 99
Malicious:	false
Preview:	...l.....3.e.*.7..M.L,...](P.{{...N..*.....}Vy..u;.....&.y.....(.+.].qp].....f...)y..7iNO...] .5W.2.z.....&..'.)".5.].....J @.}..m....N../.5`/.F....._R.Cm...,fL....V...m.....=.V...U'..z.j.....<.><.& .C.E:A....F@...4.....G.+.R.:.Q.},.?}.....b.2..R#...Z3..$.j.6.+<n.?}..?T."p{...2V\h.=...Zm...5\...W.j....Q_. ...M.=2.;.t....U.[B..|....~...|....p.H...-1..G.g...QD.s<..+.<O...v.7.`.. .f#.h!Xl....M.{..6d..I..$...SF..... ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Edit_R_Menu.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	501
Entropy (8bit):	7.569224026220696
Encrypted:	false
SSDEEP:	12:ox4yE+oUELu4bTjfBaUwNziW3tl8kegszvYj8:oxpoUYVbTj0UwbT8kegsu8
MD5:	3637DF304D5D1C3AFBFEE353E31D01E0
SHA1:	48D81868EE34AAD98D0F7819CFDF3CA951D439D0
SHA-256:	3AF9FB72FD07FD8014222DCE74BF3AC71E10ADEA241E2ECCC5C37B3D6C672411
SHA-512:	1CA57BABB1CA7DB62ADBE15188CB931815B4FD6371DBBEE1796CF8A2917181BAC53F799D99A552F06C5DDC3921D6FCE198D49BB595E05CB74760EEB950277 86
Malicious:	false
Preview:	K...)..kW..C..!. ;Z...Od"....?z......n....+..qq",+.&........g..^k..k.. ...j.#.o....O....<.o..D..m\....v..F..{.:...F..;.:.....e..}..2kQ\.1...".AAi.....y..dgz%M:.Z..U.A.;C...w...e...5.q.U~......*.].+..T ..X.?..a..)|pj.4=ll.T.:..>15U....d.6*..*..^..Fd..I8..x..7......%.u......9a.{.Z.?..fw.w...z.4..`.9=.............%5.{8..\.jQr........S......[t..H@.-..Ml(O.:.0..n........S...P....U.....F.B\.._o.P..."Pvs, ~>..k.y.%...6.e...>..._a..Rc.d......$.A...K.(... ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Edit_R_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1067
Entropy (8bit):	7.838936040423007
Encrypted:	false
SSDEEP:	24:H+G5qIHkCkFIWiJMVKrh9Ht+3pbzMG2Wp+18w88fhpy8:eG5BkC1WglXtWBzvp+18P8fL/
MD5:	84EEE39A0C54B642AD4A2B07DAAA6AE6
SHA1:	CAAFB1B560CD02C1430841627C96C745BC536000
SHA-256:	FEBA6360219CE45CC00A7FC7C0FE8FFD87C580CA2B12D9E262098EF2A2CA6451
SHA-512:	037185118038DAC801429FEBB09A7F12FBC732248421C70FC1F10543055DD347E6F42A4DDB00D7BABB81B0B69FF932142233B9DD29732587A0D68F6F914B68C9
Malicious:	false
Preview:	.\...0.../...q,.....@.F..3.}..FF.....").....Fd..X..5...*M.t0.O....2'..Z|....B.....]......d_.....K(.|..:.i<k.,_...HC.....nf..j.5p....(...`ei....z.-RE...y....%[Z.....v.h.B.|@.P.....:...RQ..MO.&.l.....Q.... ...Gq.<b...i.....J]..).4V4Uw.....noC.O...8{y....CG/dc...@.9.+e)>\..G..._.{CbU#."..=.<}...Qn.5e...O.y..[8....m5.VUx.^Wx%..R...~...B&4B...}..Q.q...7.....\..P.....9..w..r.v2...S.J.t.. ..|.....R...0...#C. $..a..0h...r.q..5.....\.)...<.X...or.5'...3.%\|'2X.U8D.H.tU`n<...4.$.F.....!..h..~....(-..*. .!B.DG..=~Kg..8.?.1...B/.....9,y.IZ..Pl.q.-[.J-..L..N%...WQ1.&dJ=.|.....]..6.j. ^k..Y..?|...%f.....~.v.b.~.....9.4.N9...<$..y.....&.ws.?e6.h5.i..9.Y..l..R.....u..-.....e[a9]...f.....me..'(...i..eA.V7.K<.ac.k.J..(...9N.dY.....AUO..(o...`v.....IE..C`....*.....?..... .p[}.g=.j..x.r...=.@v.@..[Y.A._V....8.<U..e..N.....h.....2.x..gk=c1..mf/".KT..B.;...|.....*..6rn>.....wM.OO.g..n..cK}.|.<..K.....;q.FC.w.....:..V[.L.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\FillSign.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	3863
Entropy (8bit):	7.948361579787758
Encrypted:	false
SSDEEP:	96:N7PlPq7Q3oPqGBQuNeLIVXLL1uOAD53Eze3iCX:NzRqk3oPqGBQuaINP1O3yefX
MD5:	91A1A5FB6C0552D84579A8158072182A
SHA1:	7448066C44773C3D54BADF426D688D3E64B8BD44
SHA-256:	FCBE441F518DBFDF4FA630A988D5261F01B88A51A69D0582BF62DA5EB2B4A1C9
SHA-512:	2FE3F1E4AD544E93C57DF28468A575C279BBB43F5768C81922B96CC55D67570B91CA6DCE8D0803FE3872B294C11A79817958813050B3B127C9B94D1D402835C7

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\FillSign.aapp	
Malicious:	false
Preview:	..!.Q#..J.. .5...s.z.x..J..IO.....1.od.KL.k..8?-...7vs.&.&.M"...f..Q..6l....Jf.+.....'......6.:...z.:..".-........iw`.Z....3$F8..V._."E.V.mlV...qm,.....Q..?F.....c...j4.7..r.~..#...!.P]..X#.. ..M E .XC.8h.n."O..*..FP....w*Ce.&...&p.....'..ma...."c.C...0...<.|.<..n...3..{..X. m2.3d=f.n|.#1.6.=.o.A$.c.L.wRX{...-5/....u.0..].r.+!.`.X...p..ol..^a.L.f.P.@.....?.+X..h';..%.LA..W..`.....n.<. ._.....Sb.V...O.+.....;....k._#.c....s.]y....;V.<.........&T..Z"[..B.H3=OxN...B.q.n.........}.p..=.../..$P .g..7....%b._.XZ.e..O/.g.j5Zc.p]5.1.^..L.$76...7..5]gU...,... .(...g;G..I.D.f..... I(....Xd?.0.....]x...:1w...b..}.A.....A.....B..y...xtHu\.............S...........o.V:...,9.\A..1k..?6..t.Q.....2!....n,....,Q[L.w.{du!...E....*e`...$....9..Oc. ...<..F...#..).\..j{..q.........8..P..(..F._? %7..{.y.d..5.2.5\.}.J6s9.....k..D.(7.f..zs.8.D.....K...M5S"..C...)d...._.........0.4....J.....s._..|....P.VT.f.qG...xr.*.}.U...Mp49?..|..O...dkV..p...]S..N.W.

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Home.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	938
Entropy (8bit):	7.802775326728441
Encrypted:	false
SSDEEP:	24:Cc/O7IOq043rzNiCkyiPK0fb0Ir0iHS5KScMiv+3jm07xoh2EZp8:I7SjrzNLkPP7tRS5Kkiv+uK
MD5:	75AF75A8732EFE06EA1D4A4F325AB551
SHA1:	8FE172AA732BD273DD48FCFEE01BE35AF4BF4648
SHA-256:	A83D8B6FA05A83EDFFEC8F4DF55AA341B208542A0DEA3F259FA4A81F997896A0
SHA-512:	23F83BCEC7A3291216291BF5C7D344E2B76F221DDA6EBD47D38E6FEB0C1A6C518E95FC50BE565627B268B9C1DB40B5482AB3C9D398143542B05758465D04551
Malicious:	false
Preview:	$0. ..S.(q.,.8..o.zW.\|tD<..0.T..\|L.....v ..,@.4&.dQ.G}.-..V..^.n..1.qd.#.&.-r..R..;+.s%A...W1.n>;q..)].U..._...\..s.....H..H..G....'j.,.,..^s.<.N&..X..M...f...{..w)2.....&c.....h. u....u.B.D...w.....y.<..>.J...s.".s.^k..W.]....y...S@.H@n.....*..l.+./q&Ty.x.....t.EUoEw6{.....kX.w..JPS.1...\|`CX9....R...X[.]9.<...w!.....R..y.g..5C9p...h\....?.....OH.M.z(.... .l.X...^r...>.7.V...3d..t.x0...$....Y(.'....9g2...u.....&..F..pP.R.E.+0.1_.[..Wk..x.zfP...,.--.l.b.....Jo.rK.^.....}z...'T?.j...3??...=wy5.u...?.. ..p*...7.\d.....cW..z..1...?...z...M...3.....i. ..~2w..q....~HS-.6.]m...6.l....J.{..px.ZQ .v@+..9...c.s.,V`q....d.!.gP...V...cp*$..J.={J.WS.s.....~t.....J.H!.k..o..BZp.$.A..X....%^d....e.|...H..}.W.It..>.....P*..+H.{.r..w.jFo5..]7.U. ..A..[...Zs..Q.E0!...q.%:C..0....C....b]g....H.[..(G.v.y.>9.0.I|...*..._O...../(.*...nCI.S ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\InAppSign.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	7.482067787891064
Encrypted:	false
SSDEEP:	12:JimlTuDUZuhMHCLEELEzo4TwThjH4FxYyMyYj8:odIGMPEAztgf8
MD5:	24F693D3DD656C7607CC863F7E4DFB25
SHA1:	FF2ACC63CFBCD2E802C8FA9A6C9D2C1AE5CD6610
SHA-256:	DCE0E055FBC6193945174B0A572F2B58D6013189870724971C12E81D4C2E2032
SHA-512:	3BC0E19027080C551FAB64A3AE2A97282DFF8E8202AB8B36C002740C844A4F1AFC6300CFDC8314E1143332BACEEF5835A16F5CF917F02E5EADC34557A749DB2 9
Malicious:	false
Preview:	`[..r...p.....qtF.H.V.P..a.S.2&M}...IW.wo.Y?.q...`.q...V.]....rTT...L{c..m..P8U/&.:U.~..6....V6._..`.....".FOG...e..|...+....S..9..Q..P.B.bD.....N..-..9.NoP...:.*&1...W4...<...!.....]..V8..m.u..^....U.9@.M..}....M..Qw.R....iJx..l..!-}..YT.`...i..\...*..-.g.0..n1.....s.$..,9.#.OG.Y...7.....D.-w....-.n..m.'..Q...oG7...^f..;2.p_...HJ....~...<......./.u...M..0".B... ...z.at.z.0lC.q... -_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Measure.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	673
Entropy (8bit):	7.627354549884335
Encrypted:	false
SSDEEP:	12:wygIsKKKVm4fyiIKRno12dbAl/KP5SVrx5qiqAtJYgXKFzOdvM0eO1l9NELOmavJ:/6KVm4qkoOAu5oxoixYguAUlO1l9sOrJ
MD5:	BEFC9112D1FDEEFC7001FD94E9AA2BD2
SHA1:	EF183749FE9FAA6733A4340B653345C849B15628
SHA-256:	C79268342F8B86B0B637CEAF2EC2138D3E04DDDCF045C16155780E42211E498C
SHA-512:	47B022F40737789987751A8D1955883D68ECFB9E18393D259439EA3FFA157D816B4A758C206874B66A3605C11CBF0B61DF490DA71A33A753202846C04C2B4FB7
Malicious:	false
Preview:	,O.X..6.)@f|q.9.v....wz.....^..Ow.%.S.1..m^...k0.(H@.....I.Jz...y.!G..G|%&{.B.bG.....i..i.I?.....T8.P..m..<k.....0.,..h.}i.....EXl.M|...OJ...*.).[..bMT..m. j.r.l.J..a..'.E..n.&...~o.. .....".e..I..!?...+..C?.....{.qm%.N...T.S.....9..w...LT.do O..t#.,....,(.....)L$...N.....}.R.\.{.....BS..[....z.o.....6.,1.o.D.._..U.....j...R....&..=.o....1.l.h.p.X.a....st..BF.w.*.b..y.)(. [cW.....k.....".D..?..-k...D.q.n>.Hu..S.Z.....h.....d.....,v6.|..D.\i3n.....k..^oW]w...\~..P..zT=j.10..b..=..U..4....28.K....!..]...?..V.~S.0y...H.-5..".W. .....O....."L.i..Z....P.-.P.....) ` ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\MoreTools.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	436
Entropy (8bit):	7.581800718200358
Encrypted:	false
SSDEEP:	6:9V8YwzSQXjHBikS4lCdmcLOMy9jbaWK1F2yheiep8vbWKOE6auY97EYZVH+2Hc+Z:38wQz0kemU8/kfFekbJZbMgpDTYj8
MD5:	81F2B499BF861A419DE1F8FD47082A7C
SHA1:	ADAC9B3AD33EC7EFA892347406401CA906C3B705
SHA-256:	B280BEB4719526641130B577D702DD86EE000333755AE3A1353563A93CB8D333
SHA-512:	025DA7329775CCCDEDBD9C4A1D1F14F94319401E93311AF98DB4CB80488F1E550319535B7C6D804220C0E98D469DB34A5AC84FB0ED0C1749C94899FBC9E19FE
Malicious:	false
Preview:	5.Rv[..Q.....l.n.- .s:../...e+..5...S.c.....)..o..l....VRW..G.n[]ZU..m.c O....M.`.C_.....7.....W|....1.ND.0..O.i.)..._.%:*.%.$=WF.....M).....7zsAQC..k#..Fd.....Sx.....?no..i....[.Vo%...l. .C..1}...:.y..=.?....<..<..m.3..t.>.....0.,.E..-.....3..w+.T.N._'.c.h...>.ep.....f.X..52..j.3.X-;...]3..P.5.....^..&.........>n....l....}.r'.U..a...''._l8L<237m.~...u.....V.^.....]{n]..b.....P ... . ..z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\OptimizePDF_R_CTX.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	553
Entropy (8bit):	7.666063351305801
Encrypted:	false
SSDEEP:	12:eWdK4y0yyKwPSBD/3x6XDLWqd2Qukhcpm/f4kOwzz6IIErSu3ks9R1hFpYj8:e3lJBDJ6XJFhRXEC6bCSu3PT08
MD5:	AECE9584B946AC7BFF2B033E71361BE9
SHA1:	1F2E6A5B68CB656EC19305320740064B63753BE6
SHA-256:	96D13AA6C52824DDD0A400B2E58708633BA1230F0CBE69AB721D4A48123EECCD
SHA-512:	9949869DAEFE72EC31F0F257C310FA83ACA365033FB493A6A84A5177B998068BB2F04D18048DF6F3A94FB36D9F6899676D6BAAB44468FF2E08D4C44E7C4D1981
Malicious:	false
Preview:	u...|.p.z....L.f|..4...9j.$%%X...F.h...r\y..G_."<..T.....9..m..d.5).Cd.....j#E....._....V.7n9.zi#..g4..Y.E.$G.....@.lf...}T.).T..7.O..1....+RmDr6ePg....-..A..7xi.Hg..qMl@m.....y..... E..0.O.....Of.7.(..Q>..U~.....4.)..+QQ.a...)qb..9.U.'...d.w...f....H..=....i[...?..p.s...../....u.AP6g.....lS.UP...H....L....y.Z....~..G.['9..y.....vp.RQ.o3.d<.$..ec...Y.'..".#..v.....6W>.....-3 .....g.....H.6k.,..D9.eS...4w.....lMK..=.a.[..c.>..J.9R.....>\.Ln[.....9.V..eJ.....[..:...A.... ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\OptimizePDF_R_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	707
Entropy (8bit):	7.729044106688942
Encrypted:	false
SSDEEP:	12:4PUxJ4dBEbjsCbK8cBBmQbWSQwpgSGCz4cct/NKHaqI3cwmkX6Yj8:ScJmBfCb5cBBm2WSQwoCz4vNM6qI39XM
MD5:	2EF0EBC38C881B860733EC32F5324AD3
SHA1:	1E130FBD61AB5B3351D04FE7E304533AF6691752
SHA-256:	D658FDD6456E28AF127CEEC29E4B4E07A599B63C141451752EFF48045B5C4389
SHA-512:	654DCC9EAE834F716D40AB609D6F948C7585DE4D8057A5177DF6B879F17B80CD092A1C70C112C247284EA1301B90C1BF8FDAC570214DB26E7BE0DA76E7D8DE D

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\OptimizePDF_R_RHP.aapp	
Malicious:	false
Preview:	.....h.P.W,..odwG.F.%.q.#:.<.K&.YK...Q..yp..j.C3..z...2.n..!...f:....c..}...<;.l....]<Q..d@....6Z>..r"..#...qC...yN....q....%.<W...1M...}y..%....OM..P.$..s..7T..P.(n..=.y..g.3....O".....K .'..K.....I'x.S.f.s..<.....-C...V8..L("G...s..8.Sqm``"5K....`z-.....*...$(4.^...r..R.. ...../&r..w.....,.8.v."..H+T.vq....n.e....2f..E.9..|".....z<..b.?*._..:..R.....C.|)....MOmT.C.@.....iGu. .....i..IH.TE.wdw.7...a.UA.k).Z.E...X'9...n.|...../...#.. ...Z`.7%...}.U!\.M..c.....C..QY.^t.C.8Z..n.we/c..Z...=.....09.$KX.'.....)dR..(.).....b...G..2L..#.....8.....4.5..I.[9nc..P{.DT. .'JP.@\...OE.....a...;lW..o..ydU....._.L.5..B ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Pages_R_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1170
Entropy (8bit):	7.85698056786616
Encrypted:	false
SSDEEP:	24:Lu6Z5KVr0hI+33xJogLlVz7ICnJ2NBxaR7tDltSt2I/MJbAdmx8:Zgwht3BCacCnJsaR7tDlLkMJAX
MD5:	E8ED3C0C6651B95B52B9A0879A798715
SHA1:	3275C8DFDCA80665AF2195D86CDB5CC942CB5E2E
SHA-256:	32544A4976B9C78A4059EE61A509C25F73FC0D888E1F0AEBC91CCFB55DA60DFB
SHA-512:	D8D4F3B0A275BC5910760DEE16429510FA24F81F1C759016FB1D5D49B30392C5269E418B9AC4BD3EDC9ACF1942FEE20A809EFD88AA9D16465AA753AA72BAFAF
Malicious:	false
Preview:	Ac..~...I(F..$..p.>..)Qi..u.-!...ME8v..m.g.Z)M.....:.8.._....7\...4n.*.2..n.d\&...~j...7Vh.{^....u:.{..q.8}.x.*...7.B.H....[..-.Z.w..j)..?5.U.d.*.8.Y.I...a..#`,.6.... o.\.g..:....N.K.Ho...Z.".y..... .k...~8...d..l...6du...y.G).k...j...j$y...t..).D.k...&.Dlc.c.JH.@.b.....$...J.D....u55.)/u...*H....D...:.MP.iA..7Py.,Y..>o.p?..{j../k.....~`kY5.;..#K.R1T..T0.M]....%.6y..w....?DI.....T....3z ...+...NQ.K.+.....[q<".b.r.@.v..t.O..o.cf..a\.....'.....^..e[.Y;..w.I..1...|.y.{9.....P..%X..-.....*....._.a5|.....(R.7.<.....>..HPn.t..&.o..5.Oy...h.t..._...\....c.]V.e.t^{s...2}...|..c.f./.r L6[..E.BH....R.....,.....Bv.P....;...1U..K.....0..a..?..c3...6..!.S"~.....af.'.\....7...>..i...8..<k./...../.....6.!L..7.../.............x*..j.5|..Q..O.:{..7..2<....s..U..D..4...x..Z.5..-.U.d..8.Z..... 9.}M[.X...I.U..... mr..6.7^.F.'.F..ep"W.S.....-Lr..7+./.n.H7....0...m].r.....\.Y..:.4.,y...R.TP...z$QG.I.LY.+.?V...0..)B.....W.%.\..

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Protect_R_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	554
Entropy (8bit):	7.643097081564045
Encrypted:	false
SSDEEP:	12:l6HjdOWhccDTJGtmkumHHGswRKPGwxtLqdGGQVLYEYj8:l62c/JyumuRKPGwxt2dRALYh8
MD5:	F81B6A5A62CE0247048F8E5E5C4FE5F5
SHA1:	DD3D80311A428D79E218ABA3B5CF8EC50AE39D09
SHA-256:	CBE275D8A125D7B6E6B80373A721B7EA8E267551C99E68B4A3A7022D91D71711
SHA-512:	A117229A1C1A661BF3D0323097F8EF6359DD3BFE325F47504788B740B1FD16E63877168A29B4759F79881279CA8501A613A9B29139279D73AA56193DDBE8DDF6
Malicious:	false
Preview:	VK.j.....P.6.....{.T.....!.*.....*Pi.y..n...|.}:...2n.....m.....^P..(e..7....k..z`....$f.....L.5.2.J1;..U..|....d...LIv....P../..@N..1c.....I...&.u.y.5..T...pnV...1tN.....[.[.K.`J8.pF..~..-..(6? .&5v.W....V..hG."..../Xg.7<.K...!gg....Q.!...?.;....S\.....?.5..u.4}3'..).....Min..^.>0.4x.....>.....t..}.....1.....D.sa.\.n.k....]..q.....r....M.CX.....0.F.!.....d.5G3..{.C....Rf.....7.. .T.1.+.7..b..>...s..J.n...'...)m..r%.#;g..+.k9.e.hr.Y.K..dp.{e.z0.C<..9.T.*.#.1.....<. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Redact_R_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	751
Entropy (8bit):	7.751543997189377
Encrypted:	false
SSDEEP:	12:jCwk+aR3HMPawnYTYz1BHxo84a8F04yFsFcrYkaADrwZdiLsuI6q5nS0cTYj8:L8lsEqiS8F0PWk2ZdLPSE8
MD5:	E7640430D3CB829C79C64F586DB61300
SHA1:	3BFB2E1D94D1C7E2D680AD8B0D48536FA86D81E0
SHA-256:	8C8666E4C3BA688821AA3039A82CD5E838C71CCD859072CE16B5B20C6D85B025
SHA-512:	49438FEDECAEB269906C84B4988EAFE4BCB451D58D6ADE878C25CA77EDDDADB117F4DAC39C86360A4412C580F174888963E222078AB0CB7DADDE9ED1A1EF687
Malicious:	false
Preview:	.')V.wu.XJ&.'.^....R.7...cr.U..;iY?...v...C.oV....p_N....~l#.Jt.H....7.d.T.6.....?..O./..(..**.U...c.=.]..=d.....K..m...4.'6.z.o.9D].a..p.D.=x."......@.E`4....a).kM.u....;Y.P.Ic..<..On ...8...uo.|A.Qs..B.v.C[..k..H0v#iz.a..R. H...Zg* .....u..;.^.uaF.....0}..!znV.#.yd....xi,..... 0x..s.R.3.....r{p)9L....`k$.....V..?7.\.Pjg.2NvO..u....7..VPz....%.D+..W....g4sZ>*.@y|. .s\3.^.(.sK..;..[2.|.LJ*.7{..~Z').cc....!.y....U9..1.rb.M(.V}..f.6'.}.&P.t...0...t..Ug&.6...|..G.....1.u..]....9....@.k...T.N._.>.#.$1....Dw6#....TtN.j...apKNE..o.....B...^..E....R,...}f..r{ .....!....L.'.x.trK...qk..eI88K6c5..|7f.QD..P...d....i..b.>/..*V..N.U...i.....}.....4>y..[...!.sB..h ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Review_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Review_RHP.aapp	
Size (bytes):	357
Entropy (8bit):	7.343532803175897
Encrypted:	false
SSDEEP:	6:yhCAcLYY5T0lIHm4jmrTotpXTXYdJXpE1e8KIQdUEbKNf+UPGU3zHM5LpeYDH8:LdLYY5eTQdhAUkg+MusYj8
MD5:	2BE5C9F1634CDF4C4A82EF51BF3ECEE8
SHA1:	68D887B612DDC43C7EA399A4AB7859036D2BC4B4
SHA-256:	C13D195A32E4303A086E5C5FA58F9D18109CC13310E8EE7975A08E4631B2C616
SHA-512:	FECFA6FC8E31237FB3394F32F9DF8580264C27E9961D7AAED0F8F34206CEAD5C726B829DF946569150D61543AB7E067965E5707D42DA8D8C267FE73A767ACE4
Malicious:	false
Preview:	....,...S.=.....G.#OW\..j.v.M..../..D..C.....{.-"`.....tm.i..J...X..}....?...`$...E.Mu.Hy.&;...C.?z ..,...vn.x.B]..y.....a..^S$...Lx..%I.3Rs.Y....]......~^.. .....m..$.P.t.....yJ.....b ..B...f...T. .....M...9..z._...s..r.....HZl.\.^..E1.a!....rAJ..dW.G..\..n.P...JE...L....P..7.,.o ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Scan_R_RHP.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1107
Entropy (8bit):	7.795772809955683
Encrypted:	false
SSDEEP:	24:hAnc26NZA5YspQL2oTzUOxVhZAyFV7utuRiwZxxpnD8VhvNk567M36/58:hAncdNZAaspy1TAaAyFV7GhwrnD+hvSp
MD5:	911633C8954B75F0C27882F7C7D9B24F
SHA1:	66A05C45804E534AE4F0FDD8E19227BA590FBD49
SHA-256:	DCC1E6AE37DAD784CA632F254CAF1D7B48EBDF9A6A70EB64DFC90AD7F7DD2999
SHA-512:	B5971D175F1939FE6753BFBA609470C1EAB206217FA4BCBAFC8E45EDB0F8634C9071BAFBFA43F8EB8E4DD77C85E715FA39CB1AB544EAEC1904AC81225D7A8F 74
Malicious:	false
Preview:	...j....0...`.;.&j.b...F.....2.o.;....5..$>.B.....`....'..~..B.. ;.....8...=.7.y..Q...PB..g.. ...E.....\|7C.D..+iA.D ..:NZa..]....1.....u...8HF..j#2cpt.]._...S@.....K#. .!.....!f..:.)....!.\z Plf.8:.UR(.J.7.5;z.6TPvX..'..i>.a..*k ...~.tG../...;...qc.&.....[L.}...u..._LvB.....n.i...(a....*.y..A.$._....x.....?.....|....ut.....$..,..&.!..>.....z...../.....O..]...K.G8{.. .$..N...u.u.H\.#.C. .%.v...;.*.R.._h.....~ao(..f.H.-..... .k.0.V..=...].\.A.....}f`....)IH.....;z...%XH..t...?0.!x.'.....w.Z.....b.MW.....Ei.:.k.6~.2.q.....;...PBT...K .d....>.....2.MK..L.K.../.0.y.K...O0.+..m.Xl5 \m....$qBNW.6.\|(..'.tY.S....B....J.*i..:.=.yz.... .A"{..-..2....Y..8.3...IK.K;.U..,.2..R.....9..=#...b.;.':'\|N..7..h.....650.'..=W6.k%....$h..F.....~.*....8X+t.:.....?..c..D.2.....W...../...,.... [....aNa....Yeq..'"Ng<,.6_l. /.[p.5....]hh..!B|A..&9..[...XWq..3Q..3#...I..h4g_.<.N.[.22_.5.e...).s.L.s.8.P5V...;.`..;..#..+<...r...

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Stamp.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	657
Entropy (8bit):	7.646975805509252
Encrypted:	false
SSDEEP:	12:m+JZe1Rb/krpBpBXzJxDMi4Ja+b7ByxRPB5eqnTqMtpYj8:meojkrLXX1FMTki9yx5beqTq2s8
MD5:	58370E642F1A038C16826E543930A2F7
SHA1:	219E3FEB07302A6851957D0971922E2AB77590A6
SHA-256:	7431745B98E91AECB1E246AA77A4891FA04BF970E57E3D44E8D3A286C5E947F5
SHA-512:	4035990161FAE94C809A6D1926E547D75EDC8E8FEEF888C2A3D316979BBBB5230C463938C7DC1150528FD6850A257CCBD642DAA321B7CF09B87903CEE869196
Malicious:	false
Preview:	.Y"2!..A.L5..B..._..&s..r.>$`..~.v;..S.,...c@.....3...W.......Z......L".E3.....4S_...g.....Zm..x.>VuP .X..n..Zd.Nr^.E.6...4...}..._.6.B.;.0.M.-..C'z-.7Y9.)1.<s1..].X..S<U....a>{..W ..XW.C....O..M..2[)M1.l..P.U.8..4.i_...kT.7J.vz..^.}2.Zk..w.+.b.l..p..].z.....vtz$..a.v.J.....}.|.......).[...W.....C.X....b<....l:..*;.j.j6.&W.=..x@...z..AiG.A..@.....Ao.mD..=Uo..%...C<. .....ND\.bf..?0.....9..E......RU-..... ._M..OEvz.z.nA5...I.{....*..x....(..2_.L.....D.i.._.v.+....*L-6....ecW...g.5{.JB...%.....K.0o'+.]P...{.F.....&9...(C0.~'.......}].u.d.".T...1....`..lu.#@"...7 .7n[0.....v..7#]*.r..M ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\TrackedSend.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	516
Entropy (8bit):	7.582564612140361
Encrypted:	false
SSDEEP:	12:4iP2q8gRqnlKCd9dF00wBbyj1/mdMGGezWfjosmHBj6ZYj8:puqpRclD9wZ2l34KjosKx8
MD5:	0BCA5925769075953A54163495847D1E
SHA1:	429F515BB7D501D5DA45EF3C9E17FB5A07E4F1B1
SHA-256:	63A9936C3F4297252C043E32BAD25D23700E168BA2DD8A1D5C82C72436BB31C9
SHA-512:	14FF624EDC28F8E0B7BD8971F7788579B8CF4F0709C77B48ACA53CF1357F075305D606CC7413E49F0606CB975E4FCA8A88D70875978CA72BA075FD0B460FFE7
Malicious:	false

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\TrackedSend.aapp	
Preview:	.+I.M..''..U....$.E..$..:..}..S|./....61.t..PD.jx....JN.-....D.....e=.....C...#a.|..Yi.....%P....hN...0..A.....8.....V.[..;*.Y....{.....*...~}_.B....x.fy.~.....,.6.l..s..B{.c.`.....''.....M...T.....S.. ...b.....zQ.....P$A..kQ..5..0C..V.4o:4..v*..!K.PY..v...)e.{..>.'[.m..$..P.r.!6.....[...B...:;..a[.v.#@|X..!.IF,..0Y.gr..(v.....e.a.P.....0....6.%....H.|OXa...u.....!'Z..#N..`p...?.o..... ..l^U.%...Z..f`jz\y.^4...s7'R ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\UnifiedShare.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	7.88169711117001
Encrypted:	false
SSDEEP:	24:ZVusxfKXGiil+t3uv3vIg/Ccq9ruKiSJVOAA0fD/0yxDAPwKrPO1T4qIsXz5ErA8:ZEsVw3pv3gsCfFiSJkCbfMIkm4qIfp
MD5:	252B01EE3A50C77D8F604282ED2E677B
SHA1:	89E908A27A79157BE1E7B6951700900E69F99E05
SHA-256:	17D36DFC51CB78387035AA63F23132EBA44733EFF21207EFF401E0190E37AA34
SHA-512:	501CF578870AA92260369C3AD1F142862DDF0FFDE20A520F6C11393405E3BA0D791C0A31CFE4A59CCDAF623CB5FB30466576E4466900FA1FE000E7AFCED5896
Malicious:	false
Preview:	.UT.&.k..4...k.5.....N,L........r>..p....s....c.C..80du@....v.@D.Y.RX..L0..e.?.n..g...q.K&.....h! ... .*L..k.t...U.p..mL.x..D..*...S.;gs.Y.v.X.G.....uB8.z..B.|..x.+X1/.....N.j._.ib: <O.tu(Er....I....P..P"S..U.....{{...A0.x.b2...Y.UvL.2rNr.`... .....p.....Q$.t...X)$.<.8c.. ..l(..K.....K<.@..u..=>..'W.X...$..1S.....tF[..1.'...C..4.}...../?...a.."....,...J^.a.BU.k.]../5...E\|^...,. .9M......U..8..Q........)lS.f.h.....`L..(.[..+..Km.....#..l.i...D.g8.j....H.%..*?...B...J;."..Mj.E....,.[O.7....G5._._.....n.Qq..p..zyoY~(.....ok.....Rcv.....5..956..6..$T....I.d..Wr..(. xMr..5.H..=..&..F.n..+d.h....N5.Q....G.....VPOgB)....mJtI.....&..@C..W..._.<D\OQ...YY....I.....g..}=.>...VI.nr....%....;~....P.z.....pg...[.dh....(.b?..n.....!.W.AW\.....b.71.82L..... S.....'-.E.=....li~..A..U..}L.p.%...2 1.kB.M...2.>....Q..Z.eF.>.J.o&....RV..0...jB..frJL.D.../er..#Ce..eO5A}6..[....6d....<..i...{N.b...NV.g.%.....$.F.{.Y2..f..e0_

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\ENU\Viewer.aapp	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	423
Entropy (8bit):	7.465453808471327
Encrypted:	false
SSDEEP:	6:fP4lLxI1pZaPnk3+29+QnmCTHZwAdjNjLZOAS1JssW4t24wixEh+y1P2jmCan7GQ:fP4laHZlmCH1jqA4u4tiB2joYmPYj8
MD5:	F85288351F54251131CE8C6CB47E186C
SHA1:	E0428308B1582CAAF541FF218F2B4FD65A8E5BFC
SHA-256:	4D0C21ABF03F436244DD2CDE8F2AB71E89C04151E09CD953D7EE05CD00EEAA5B
SHA-512:	92BE45A1AE5CFE52E47801E440E59AAB23F9CCFA2BEE125289F3C0CF3681656CD420A54F11D0F2B0B7546B2964A828F56D75E6331F15B2C6DAD179020B83371
Malicious:	false
Preview:	..Xi.a.....T....>..j]1\t..c.....5..b...B..Y.*.....-q..o...6N..Y..F....|H...`F..*...K1>.@....z.(h...1ml..U.+.j[U..*..A.........dsT.o...O.J.....e...w.Y_.....d8s.u[g.....]u.q.2..u..'-.....*m...C...b .vA..L...''..>K/:..P...K..EvC..:.....Xey~.-%..W.G3...q.E.M.T''7.........~.YH.&=.:eb.R..vhgu.r..V...?.._..'Y.....V.....9}".<|...9jy...9.....;...L(..yq.LP..''Vh..... ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroApp\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\COPYING.LGPLv2.1.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	24664

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\COPYING.LGPLv2.1.txt	
Entropy (8bit):	**7.990795263618427**
Encrypted:	**true**
SSDEEP:	384:ncwcd68r+2tcjlfodgxUFrbNpFjH7faeQY2gnxd77+8upzASAGFdXIb59g/BRAK:nR+2lwexmnFjWdY2gnXkptAGob59gpuK
MD5:	8CBACB593D4AD6DDBE5FC84B9E1FDC35
SHA1:	69650EAD8FF9BA7751B8A22C57F7CE464F498F9A
SHA-256:	CE5CEEE499918B2338F6991E3913FDAD745EF86296B4AD048408F053957EDE12
SHA-512:	1B186F0C80EE6BAC1C5E8FDFB7445C97D1AC063D6B8812962B718B41E0796B39ED117E0B3831A65C8D144171999C9C4C1529EE4D7D5F0D1E987A260BA0694D4
Malicious:	**true**
Preview:	.....w.4Q.ef..u.4.L.E.w....1.e..K.....VA...N...A.....j]s..+).(.2.O...b'f...4.4...s.a.."....8:h...h.....{.$8&.. .me9...03.....jD....i.".#..'..Lz>.l.....RMK..Y..).. .E.G.*...dy.....a.= ..s.p..U...0.....A*Xj....S...t....ft..6._9..d...u.c1.3.b....Y....).~...S.S....`.}j.E.N(i..!.9....t...Z....E?.....v...p.Y@.@.....?v.Y....ag.....$.f.....d..*k.&..q.(.L.....y).;.9/.*..s....z...i?.J..8.B...o- ..3..a.E..D.,...X.e.....cc....{..g.Tp...>.;m..}p..;.2_?.D.....kb..p.N}...G..`.....z....2..o.`.-G...@D0..SNgr...B,..M.83...+.r.....Ge..o....l....X.0hr...E..%..... 'd^...>.,.c.ruz...mHQ.. {..{..'f[=g'.FM..Q...O._Zt. .-.ma....$.hL#;....V+.-.Eu.n.....7.*:.AC...p|..B.u..h.._.....N.<.xCl.O....e.S\...z!.[...7..{J.....}41.4...f.....|v...l..I../.=...."...D*xPM..:.[.3..!.W..3...t n.G...#|...=tfr.m.....c4`?$....UG.u.]..u.....H.>.:....lO.....j..gn...l.*..G9"E_.....*...v `.X.....L...g....5....yk...9#.5.....K.1.V0.|bg.~8G.

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\LICENSE.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1779
Entropy (8bit):	7.88642949508828
Encrypted:	false
SSDEEP:	48:DtGjzbgqcNXvUwJKqnJQivHF3l88HUU0RUIxL:DtGfbgfBvXKqnt3u80U0RX9
MD5:	424E33139C9C6171DFB0152E9F81C93C
SHA1:	0E8DB77FEF71F7A6A413F9A38A663C9D26D37940
SHA-256:	3936DACDA2B53E6A28BDCD8FEAD661CB473400EB4E349B956E7D54C1E4B08E0B
SHA-512:	92BE991024338919C01A46C0DFD3034ED1E25179703D47AA9CE7686C9231B1F03CF258BD8449CE3C2AA05486ED59F680349AE2B8145D5C74FD7719C1661158B9
Malicious:	false
Preview:	...l."..[...0...Dn.....(V.a.>."......_.N...<g...&.g.D%.X.....+.u...:O.....8.h.ov.$.yr.....fF.W.`Pue...h..)...3.TWb.V.]t..n` ..4..U...#...8Ua....`X4...0(.....p.....)...XS...r1.3..9.W.dp.. +...Gv.95\.{sc..?o .{ ...U.3.....{..9..3\...%N.....I...b....>..@...T..R<q.v..y.....G..Z..a.:9..`U...<lq?F,mE`..U3&.<.a..Lr.....^`.."45;LR..@x.1m..e.>.$..&...rnX.`c?*.7.^`s.:....;o: .O.n*.....+..(....!..H....*.....K.F.*....U.[.o=.....z..?u.WL.5.Hz.o..:.....c'.B...2ct.Px.Ok.....K.x..".....zd3>..W...)`.v<..$!...5p..9<.3....a....d...:..JOw..6...gy...g....S..p.....+..\..N. ...uE.l.u ..lN.....Q.[.'. .^...[p..<.....%....y.S.....o.Z.../.e0..Q@...../H.<.*x...g..@.....ab...z..7 ..9&.P....).....O(.'...J....|....J...K.....t..u.....m.F6.E<....#s.8...H.P..3..Yfm..... D7.....@.8..S.Y..'.k.....I3.F..M.Jo3.".1|....m.)u;..0..|#..mF.N@ /w@&{H...U.KY.5....@.OVy...;('.....R...@gG`R.....KP.'.."...R..x3fI...i.;...eN.q.b.'.W..,.....W..I..T.^ud....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\cef.pak	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	88
Entropy (8bit):	6.033184175406313
Encrypted:	false
SSDEEP:	3:/V428UfF5uHl+Q3pf2epZ9EQDiH8:/SM+HAFepYDH8
MD5:	643E3C8521C6639E60C23D3BB3D4DC9F
SHA1:	8118AA097766EC1DB61E3A963943E3D7E11A8FBB
SHA-256:	C9F160A19F9DFA7F026F6F0896DB5EC7DC947F146964642E21F03534FAB9CAFB
SHA-512:	D23DECDFB854D1AEA50850B97F4D311A2FC273C3003A4FC2343DAB0C9762140A7E7165D29077D67F6B137C6511EB1324FB2C925D74331568073E1A323B7BDB0

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\cef.pak	
Malicious:	false
Preview:	...'..l...W...#...v..|c..]....l..#5-<.q.S.....v.< ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\cef_100_percent.pak	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	88
Entropy (8bit):	6.092787726518093
Encrypted:	false
SSDEEP:	3:bxCS1Ntz+GuL19yrgFj2epZ9EQDiH8:lCS1L+GuLXyrapYDH8
MD5:	17D700306808BAE48DE63BB69E74E829
SHA1:	C36F9AAB259CE256AFEC3DD8C017BACDA88BD6CE
SHA-256:	B9A09184FF7CC276A30DE76A44D9EAD4D46935BDBF268F8E7484DCDA24039086
SHA-512:	AFE382E519E8392461A61BD970972B61576E11A8BE420A3E6477BB08762F5A9D5673662EBF8E97EE9095B62F376433EE40AD89AC43AF2FE804BF22CEAD8FAD0C
Malicious:	false
Preview:	K1.8.D..9\^.....a.^..F.....N.<."v)...g!U.... ...vJ... ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\cef_200_percent.pak	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	88
Entropy (8bit):	6.23772962995177
Encrypted:	false
SSDEEP:	3:eraUrXLqFDgdgNbpzgSIFj5Z9EQDiH8:Kz6DYINOFj5YDH8
MD5:	1D53EC318F311BCF3D60FE63A918FAFC
SHA1:	1281EEF9A04A79599E6E47D1561023BC7507D0FE
SHA-256:	B576CE2C47A6B307072EA21B5AB91907CE72C8227ACD7ACAFA97242ED0948C55
SHA-512:	E9BA7A145A15DBD5F81D3A943BF68189D58161314D23BD8B806C7C87B4AF7FB16283720CEBD58DA240A98739E03A3F0BFA2C94E008ED5B1304F79ACD2FFC341
Malicious:	false
Preview:	....Ew....b.n..1B.z..4..Y!....e.x.h.."..j..V..@.L.m ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\cef_extensions.pak	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	88
Entropy (8bit):	6.0872169879308995
Encrypted:	false
SSDEEP:	3:ge+6iC4m4zuVMq/R8PpPtjffpZ9EQDiH8:gsiC4PPpPtjffpYDH8
MD5:	1039E88EFE250DC6119B2728BEC65104
SHA1:	EB8504A5B34465EE713E6F5DB84925B75DC035E3
SHA-256:	324E12A38D589E5E7D7624903AA380AE4AD2E47FC29CC2D76D9574412094C805
SHA-512:	E3E37C0E0EB7EC07EE3A7C8318BDCBC98298464FB8BD7470526D82DB092A4D26BCDABEE83088EE81488FBFFEABFCDC556FC566F134059A839CA3D19F816CE41F
Malicious:	false
Preview:	Q<(...M...-.....!..K....`(.].7|.....E..,31..<L.E. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\icudtl.dat	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	88
Entropy (8bit):	6.169547811769952
Encrypted:	false
SSDEEP:	3:oESM6PaxDpn94uG3ECOvZ9EQDiH8:o7mxQugENvYDH8
MD5:	267AD6283F94F60FADEE4F01474F9F82
SHA1:	44077D25A34E51619E2CE03A9DD691C69C1A5E0B
SHA-256:	0560B6B0E4E93A7DF922281FFE262F8C77AF46F0C7E2A79F92CE9AD82404DFE2

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\icudtl.dat	
SHA-512:	42565B8E59F10567C33E0ED53EA0AD12DAA123A7FFDED28FE32E5E42BB6A3FDD6AC94E7AEC61D0C62303A90AA9AB6F378DF1FB0D126C8976DC1CE1A8DDDB B43E
Malicious:	false
Preview:	.>).. .h7.U}w....A.<k.SR$.....C.].#.Q...O...R.. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\locales\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\locales\en-US.pak	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	88
Entropy (8bit):	6.14682053904268
Encrypted:	false
SSDEEP:	3:IHCxk/FkJCasgJnMc1ai6c40hfpZ9EQDiH8:Cyk/oCasgJ/0MfpYDH8
MD5:	7CC6B275AEA8DABCF810349D83107DFC
SHA1:	58E1E29AA31BDA38DCFE5EADDC2C01F439A2F5D3
SHA-256:	91DAE858B980141982285AB76371C568204FD1F35040E1636C9473FA7C902E8B
SHA-512:	BAC86124689A71D51AF77B21C45EF416E5D91369FE923A81997310F80F1662980036E6B51B2167765053F2639E1C5670869C9D1DB154B65326778395D507602C
Malicious:	false
Preview:	....TS....ix.T.\.Z .w....I/...5.f.Oy$_{.nn.....2 ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroLayoutRecognizer\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Adobe.Reader.Dependencies.manifest	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Adobe.Reader.Dependencies.manifest	
Category:	dropped
Size (bytes):	1897
Entropy (8bit):	7.911410036580375
Encrypted:	false
SSDEEP:	48:vyNm1kwZt9rZH5oHcVZK+jg0FbQRn0vWyBUl/3:4VwZt9rR5vZXfQRnAWme
MD5:	2D883998587F3D984943783A672D0487
SHA1:	3D682C200F4849DDDCAFA221EB54BE49E2E4B43E
SHA-256:	3486F7B94F5E3291A4AF10C812A8DB5BCC28E2EEA521D2198A3D089043D8C56D
SHA-512:	369BCE5F878F337E81415E6559E417C36BAA98296A7E8FEB796231FE899BCFFAB39850DE16E6D876C55A87D40CA8F3E6803396DBDC865E0AD4E639C12C69669
Malicious:	false
Preview:	.....v.4..4.[+o.. L. N.....J$.L...i.....uC..p.Y....pU./g.....l..n.B*..?..O.....b...O....F..2.%...E../.n.E!.}.v..K:.$.'..O.Y..gX4.e....3|.w%i....6. ...(I$.kJD...W.+..{.....u..k<.... ...i..K.J..w.+...M...W..+.....I !.Y]..p.'@I....9.d..6S#E....$.|.....5&_&vl.lK.._c.."r....QT...b...90..B..)..m...,@..8.....kj.....n....Z..z....X..q.F...(.....8.....j..M...s.^.. 8V..U.3.F....? &]..7.8[.....W..t.<.#k...4...W.H]...dm....EB..0Ci@../...b?9.C.Dn..(.A.....8.....e.dy1.....%.0.O....A.+N.c.uns.+..^Y..q...K....6...B....B.....].....M\Ni...E.%..2.l.f....PE9..!.e.P.L G..1...i...gh.&&...s...\..u(.d.cT...[s../.aWf_D<...,q^..i.....wV..&d.P#:3h..G.y..T.._.M..%.r6. ..S.A....?lr.|.K..\T..j.....i.r.....,.rgEu...n.*<].)j.....~.K.{..+0.f.4\.c&...!o....Gh....S..... .k...5D..yT..7.p.....x:_.....J.'....77*-<.4....g}..r;.h/.^U@vN..TdY.l.....:{.....T7..{.q....+.....>..IL..3....f.....Y@.....=U.y.S.f<.5V...?

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\manifest.json	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	355
Entropy (8bit):	7.361802336923919
Encrypted:	false
SSDEEP:	6:eHn9Oi7tRHs2yNhe1M4lrKeXeKlJ5Ls9fMekX74cdbhDjaJK46ufbpG9XpYDH8:KfX+NhIM4lW+eKlTuMekLoFzpG95Yj8
MD5:	CD461BE2AEFE40779ED5C8A55E7FA9D3

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\manifest.json	
SHA1:	561C446DAB43B3A6988598721EE9E3A5DD2E3A5B
SHA-256:	31FC0A7E5AE9922779FD25619B8DE64D9669AB34EC897670ECD7F9DF8DAADCB6
SHA-512:	5C8141D9CA6E71F07B50D0A6C7C0762755A8969748E85E2C6818AF6D265B28B3F06629D14DEF2DE8756EA529C137969AE60FA602D26A27F6A1F4C98C77E75D2
Malicious:	false
Preview:	....`n.b.I....6..q..p.t(.....Ux8.ur.t....L.....N.q..+.kO...}V.#BO....~..Y]W}...6...0@...me.iv..f.5....)T.{.&.N..e.Z.....]&b.>2...]...*....vl.....\O..~..%..M..l....u."k....G.>$....]Pk.r/(.d..U.4.J .&....,*....V....I....].....H<.E..1.h.....yk...R.....6.kz..1v.;.A..D....a....]~0t. J}>K..8l....=+d.6..... ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Click on 'Change' to select default PDF handler.pdf	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	184408
Entropy (8bit):	**7.999057627873936**
Encrypted:	**true**
SSDEEP:	3072:BI0T+WxOZM4HnTHXtGtOV2t4eYLKKhtKkhmG/TjnY/aXN9TIHrec:S0qUOZhHOOV9eYjtK8/T8CXNBI5
MD5:	0E1C83DBC1F15924C53EDC62CF7AEB80
SHA1:	1EA371B862033F36CDE254EE0C927D660302B309
SHA-256:	2AFB3259DB69CA95B5124DC78B32E1A8AA0C0782F835B9511C7CE778BA0E58CD
SHA-512:	3C0F062BC3E333E4730770D7FAB6913A81D84B88A540778B7722E3A11040B5DE521E3E0C770F0E5DF95C96048199BEF192D4753D940309DADF6517774D77A0A1
Malicious:	**true**
Preview:	!.(..}c".e 1...Z.Kw%.2u.BX>...V..A] ...mq.Y..B3.....R..nz....':;.6.....d. @....!h.i.....[.y"..Oz.4.....c.S0t..`?.8R....V..~.$uZ.@.z.{hg4.Y!G.r.8LBa.7=.3...C.5"Y..Br....w..E..%.!l.....e.. +Pzy.@q.F.0..m.$=7.N3...M.i...p.zU...f..3..z,...C@.,Kp..L.....M.....07..RS.S...[&Q.Mql.lsN.I..q.....z@+9]cN....xg..(.]...qc.R...O.lkW.+..:..V.....|N..r..Y.D&..-^.....*..4.].. ..$..7U..5..SB03V.w+.....R.4.....!v..O. .....Q....[dL4.s..U..|p 3M....=.-i..sG!..nl..^.RG.W..f..E.M.....Z.m.....9._....7'.Bl.o...Yt.8+/s3oc..D..p*y...ki.....E`.!..r....wv=.... ...(\..." <)w.GC..`..`P.;.../.+.[.....T...ODy.&P:.6Z...;\~...M.h{.>.z~.....wO..,?...K.....qD.^&...3.jYxa7..D.x..{J.y..4.SV.lSDJ4$U.....g....rr...|....$k.....Z.Yl.%..sk...-.).....p.r...Px.aUZ.s. p.....H.B.U....x.U...B.K.h.....+X.H.l..?.TJ..\E#..N.[,7.....s.7..E.SP...}qg..4F...~-F.q.2.i..5.....B.....8dWH.z...*1....5.Lm..0m..?b....}.D._. M.....V.(..g..lM.....!q..R.K.I...h3.R[.. ....Hg\x(..

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\IDTemplates\ENU\AdobeID.pdf	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	82008
Entropy (8bit):	**7.997643777696051**
Encrypted:	**true**
SSDEEP:	1536:1s/vVQih5LCI8wa0nP+rde8rY1g9zwKK7wFvAsI4jCJ6jSwMU1oGrDlb2:1AV5C7mP8de8LsL0lAD4jNSwt1BrDli
MD5:	CDC74642D345E2C7A6E2E4222FFA3063
SHA1:	50B847ADE690C46910ABD8904CEA26BB3F7F75A3
SHA-256:	0914A54694D58EBADDED9A340012DDAC944966929C55A440235866DF5D712B2A
SHA-512:	E77F57477C346A29200B526E3AF7F1798A6ADD2F3C7CAD6027457F8155CCFA5BC6B5C0D6846FD1B940A9B63C5957C77EA565C7DCB91A790FA75FF11A33D1B4 F
Malicious:	**true**

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\IDTemplates\ENU\AdobeID.pdf	
Preview:	x1..w&.....K .o'..9D.9^.p.$._.USj...#.....>...K.s.(..S...c....<.C9<...Db..f.#..L..-"..d..T....s..^.....P....6.f.a.?..8...,^..)]Y...<)(..;y.i....X..(....p.d.^MY..O.#t..w.....!GT....8.a..D...T]Tr.....\3 ...J0....]...6.)K.c<.8.....%..*.~.M..`V..oq+..Q...lu.....^.$..\^..s..h...Uwb-....U.|_.p.R.^...I..;...S..;.3..W...C.}$.sO..iA...hf..N.t..Z.w ...H.....7MS.....F.T1v.....~q.....[.1?..'.v..@.....X.7.l"h .g..!2..$.<.x.;.....3..I..rX..U.b.....-..)...W...f..Q.....^2ePS.<..Q...,.RB?..*..6]..7 ...#.....A)(nn...+.T...7....<Ma~..T.m.....K.h..I.zT:...SF.n..7.'^.....#{.L.@..6.. n<];..}...Bx.;G..Z.Y.:.a +.,.....D{...g..~...S...~'...>/6;.../{sc.e.`...Zl$..... .y..#8.<.bk.;.....J..Gm.....FU..S.\.dsP)...T.....-.^....v.h.'...7.E.a.R.?W.bZ..O.-9..,.6.".B...5J.....TG-RO.K....\.g.u.....F`..... +...*.t.O.<.p...g..aX...4>N.h..T&.#.7.....ipG..6.C.....\....8Dm...M.H^..._..B9Tm.Y..5.g..]$...%'.-. ..X...qh...R|...<..*;....;.G...gYO..K.z.N..A...e.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\IDTemplates\ENU\DefaultID.pdf	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	77912
Entropy (8bit):	**7.997548746297273**
Encrypted:	**true**
SSDEEP:	1536:dzP4t+2e+7oCZGaIoqlhCXHr7CcPfXgdcCjkEQ9E488l+Xao9oht+6:Rb2e+MGGaPq7C77CAfQdcCjkEul0op
MD5:	06A8B98E8B1EEAEA325002503BB38B89
SHA1:	B57DA1F22F87650B7BE47DADA34371B608DD4E0F
SHA-256:	2C097432D0326A8C75E16BA3954657E9955F1E995AEFEDC68BF8541ADEC747EF
SHA-512:	EE345C92F8DF185F66AAB3BA9B748986CED6849251B9B9FB6841110E25BECBE88DF71D33ADE20A34DFB1902BD49D83740EDEAB65262E67BAEB43865C8AFF53C5
Malicious:	**true**
Preview:	..Vk.C.. I.'.....d...=a..).{.f.8K.pM.i.....x.....:+.....Vi..j...}D.X.....7`.....X/5{...k.Q.."....;l..~i..nq ...E.u.g.z..Z.....`.....WklKq.4...0VFT..Z.@..K.GT....7T....}..\.M.9.....:....J....E+..i...j....K8\D..T..= .M...c.dpuIl.....x.J..].U#P.9..`.w.$.."SB4..S.e.....D(..GK._..f...e$..~.....%...'...I...e.....,<..g.c....$0y.5.by!.Q... y.y.m..H...c#..M..c.0*l\..?^E.....k.:.@.'... ..#.....J<...)...b...qp.....[."..}.+?..jS....o.....Nz.<j.....,GA..JVW$..f.....I.eo...7.N8.,.x4%..zh5...Ep...K.,|}%.]...G..=T6zo^..~.'..Z&.%!.._....VN.....!c..x.....u..#.V,..l.....'.V.... y0(.?..N'....`.....WZ3..o.C.z}.9_x.m.j.....bgcqI..ys.....}.]s...ek;..j.....q'....z.AWM...v.....\...W..dUYb$..o.M.T`.$...+..;S..6@.{/..k.0..V>....s;h2.....[...=..gwb..." .f;....!....<..n.vu. .n.(W.. .MN.R....z=.....D+..U~.<..ol.....5.%.L.a.*..../Rb_..?u."T..Q.5...@..-.nI_.n.-<Y.N._..$.#.....;A.3.@.7(.QWUa.p.....X...K...)N.S.

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\IDTemplates\ENU\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E850D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain access to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your test files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\IDTemplates\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E850D
Malicious:	false

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\IDTemplates\How to decrypt files.txt	
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain access to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your test files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Javascripts\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E850D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain access to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your test files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Legal\ENU\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E850D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain access to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5icgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your test files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Legal\ENU\eula.ini	
Process:	C:\Users\user\Desktop\local.exe
File Type:	DOS executable (COM, 0x8C-variant)
Category:	dropped
Size (bytes):	1128
Entropy (8bit):	7.815724294077751
Encrypted:	false
SSDEEP:	24:I6Nb5Ux7rJnbR1VfqHBAOe0PH4xpQ/R0cnxfIscI5P5q+IyMSsMy8:fF2EAOHPH4xpJIAsNV5qg/
MD5:	B9F5F951E60903B49976D8EBD4A746B5
SHA1:	5676E6A3C3A49C0B25B719DC13D526DDA18A50ED
SHA-256:	08A2581411F4A548AEE7A9FA3C2FFDE90C637B82E435939C33DDCC847C823A41
SHA-512:	C25D4A64B3FA98EA0CFB9ED6D574AA6B240682198364625C7E96BAD6D249576A25E3043326E0ECECD817B079D3B3F3F5B4E38B0A41B7874643FFCD396F28F71
Malicious:	false
Preview:	..#.....Yo.....Z.[$a..K...B..T...^....z..ds[.-rX.;./.hR..c...X.S1..V..i.....\|....c.<.8..a`j.i.....g&B.e...t.l.....s.J.....JA.}...T...u. .r...j....~...,.....T*...>.yz@JJ.....GmJ.....P..G#..1m..K..L.aRn.z\l...$.'.^..Bp..r.....f..`..c.t.+(0.@...G..95..^..G.....=e..t...s....b".o..G(m.....VD..?..zz)}.-Eh.....P*.Q.O1..C.S...}..m...@V/.&.e@...E..|...TS.....<H...~I.Q.S..p.~...*.`.I{.....8.s..fU...x....|..V.J<V.....Z..4}.R.....K.....s...R_Y....A.`..b...Z0..(..;uC.g..*a.>6.+.c.....A.9..H\.N...-.gx.g+1"f.....=.."&....>ar.W2.WC.c...._...{^..T.[..j.{x.c.'...D.:x=A.-.....h...M.'.....".Jr:.#.5..K=.S...H....y...Dy..Pyq...3lU/.."..%k...$.9....E..{.(....e,.....W'.....n.0.3.P.D.qVP.....0..+..>CZ..\|.,.V.!.....py.R4.....c...../v...p..E(.w.....h..."A.^J...b.sjP-+.W..N..zc.....o.....E.....C0a3X.<....+..\..c.{7G.4.=..._.D.i.....M....$.Q.6.....HO....0.S.=.0@k.....y...ro...2..:...E..c$..@.s.CC...

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Legal\ENU\license.html	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	45144
Entropy (8bit):	**7.994752438858387**
Encrypted:	**true**
SSDEEP:	768:YlKUkslolmCLOQB1W9nRa6CssRA5p7cNTVBJG+9bf67iLaFYwX7QKH+VWA+U:cKUVGZil13lsRAoT5Vf6uLaFBXXeoY
MD5:	35C5F15971E6E8F92E429F2A66375DBC
SHA1:	E2B81AC3FB8024195FA7F7C79A857372CA5BFC3C
SHA-256:	C9FE01A444E3503D97438DEF30F4B2974E4FE55A6B3F78345E371160BB0DCF69
SHA-512:	C54E8CA1808DE0ABACDAD55047A7C8CF99C0ADFF2946DC170970DC07B9CC620B4CEB2960BE938FCB650A166E4D7B5EBB630FAEE64F88DA4F991FC0DB4989 1F6
Malicious:	**true**
Preview:	..+I.....B....X$...P.....V;.o>...Z....L=.?...L^W2...&..'Q..0.i..%.r#...I.3..O.....6.....i$...X...%+.-.....=.G.).....pr.8Yo..wEb....H...Y.D.Z....R.....g>...i.O... (.5.9(....K@....4...P,.... r.^....U.>....^.5}.....Vh.Y.*t.}.Px..P.k.&&/df....q.ln.m,..D+.$....3.#.Y+...T....:.+u.=...O|.e...b.I].M*.8.v..78.l0L~Si.....I.5.!b1+.L....U.#.J.~}.~...y.Z.h..a...l.@'.j.EDD...</?.mV..`...9.: [..p..@.l...s....<..^g.....Wc2..Snj"1..J....Ej..y.v...b.a.....h.....~..x.j.)..._2....#).p..G..>d.y{G.Y.L.!..+C.>.k0..}..8..L..<3..b&.}.e..5..b...(.0J.'.C1...o..|.>.M...."=.".@.j.d..:=n.I..K._..g. x2.G....."..Z.9.../yW:...8.y.@f.%.T.g..FZ;..u...Q.....n..".Y..o^..Bu...\l/1I.Oc..R.9.R...)...LU._.d(...S.%.M..s0....4#Z1.L.....:8.N..t.....8.....C..&..n.../3..Z.l.F..Evx....CjF.....g.. ..bq...JS.c...j..f`..[.0.....(n.....EJ-q...']f...\P.^...uW.....I[O^8q.....K4.U...v.....`.....J.....A.G....LP..~.])....YHx"(\g..h.....s

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Legal\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Locale\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Locale\en_US\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Locale\en_US\How to decrypt files.txt	
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E85 0D
Malicious:	false
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Locale\en_US\stopwords.ENU	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	8792
Entropy (8bit):	7.979592890149775
Encrypted:	false
SSDEEP:	192:f0z/Opcd+TgUT69+dQS1iVvOlAgk9jFa4cBSiRSGuBOMR:cSCWQzVvOy9s4aRSNBOMR
MD5:	1D0701D9777468E77F1D88AF7D560C1C
SHA1:	94BA28CC68297C09DA1039313893D9763E2F3F60
SHA-256:	D59CAC0F002935D925EE8A6FB219A63002DD0A49ACCB4F581D8075518A9579E1
SHA-512:	0DCFE0DD4BFA4F597F048B8E12E7654397F14323CAB95F884D203F0598301DE066056D218F0B3CFE19164EF2715DA21241C7BCB4A377BE80BAAE52C1B7682DA
Malicious:	false
Preview:	=..U*N.g.....>...h.C~,m?...s..4..h*..d...J...Y.2#...%.J.B..W-..}.Sx.c....b....:$..i2^qj.....h...4|.!.....+d.z.3..F>.8..R.T..:.C.....y..r.w#....k.\| n..A.....T.C...:.K..G.w..8.}.....[.5Q....$... Z.....t.&=.....*..A.....K....?.}.e.&=!..M..u..#(`r..K....#C..}<..&.3.@...}t..sf"g....C/.Yl.y.....$..E...na....p.....B.....`R.Y..eS.....8.....iY.<.st...Y.,.KF..=yF..@.w0<.....0....(Z.M= .v..'.....#.i.....4..l^t.fb./.S.G.....=a}..6.[GDD.....-...=.%.Gl.....i...V.(.h.?.+...a_..../.4$c.u{...Vys..[..j5.n..t.D.d=n.(_..D..._..f@d.5..p.X4'...{.y..O.g..q....K....&.s.V....EVI.....i.B. 2..^.2.V...:...C.Z.....lt.u....vQ....p..U`...8..r....s..=...Ut.p.+.....Z6..b.].....SVo.....hA....Y.dH..Pc6.....\>c4.y|...~gWd.WW...PK.....T..y....F...j2mB"_...S}9$.v.Gy..R..t.l... .?...D..j_p.....g..Yb..4.Z.....!_=.o"...e.....mK.A.kxy=H].3...n.....U..{"T.k.....Z.@..E..f.dK..=9..q.....?vv.j&..m...@.~z.x..ZdG...5...j.

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Microsoft.VCLibs.x86.14.00.appx	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	610392
Entropy (8bit):	**7.999669339499939**
Encrypted:	**true**
SSDEEP:	12288:Bk3qI7D/h6V1I55URgBu2ZI+fpF+hgJEA4AxAnT4SoJgMzsJ6032p1:Bk64/h8nR9sl+yhzexSTyBs80g1
MD5:	C5C4CDF361997510CD2B316D7988FE03
SHA1:	0B4EF7D93B3C02274EC147D079CCEAD86465940E
SHA-256:	0AC4E58A75537EF126EC4187649147B1CE4F8512BC5FFEE7E81DD97F1C8EEE09
SHA-512:	B2AAADA9B24BE878B1A36499A53F39F7E5A6FFBD579E4F5AAEB515B1EF3FCF0C7489542E96D9A595137EECEE5497DDC5D0A4C200E0AE9F6A8C0471F502A851 EB
Malicious:	**true**
Preview:	f....,.....\i.....].L....9".....3 .@.._.k.GC.....tk.+..v.jVB.....RzS....o.d..j.-e...[<...c.-....}..&..>..3.)|y.n.8.Dx..Y.h..gkm.R-*..x....3ma/..C.W.D_...*..;'.....~...o..A.....$n4.F.... ..mK...1.r....$J..+..j....JS.....A.....4.Ke.~...=..M..o.0.n.v.a.0wV.R..Z..{....M.....{.[...y.Vj.4...$:H.Lh.~+....]n.....P.....`..}2..\|*.85#....8..P.....h6(....mh.9..e.f....m#...B..2}...`..Q.uot.. .#.....Ro$z...}s..Y.....j....N.. 1.....}..r.(.. 4.1.D..J...$9^.R..1..?q...V+..41.;.8fi2..H<q....r.. zd...?..2.`....6\|DJ..[h.l]..B...[.....-.}..R.v).M....]..*.E.u..X.>j.....b.]....Ux...j...f.w3Z/... [;nTU.)Xh...\..../.....Y1..[.lw2..]..<.....dBY..W..R\..@.L..V..o..=.l..W.(.H.5Y....<H5.{.=.....%%BW..yg..)U}.=_L.....MH.mJ.H..A8.}.].KY]?..*...s.....<..<.G....kY_dT,..S.....Ad. ..#.....?iP}f..'...^...d..:H...7.!....b....q.....kDl>.q....o...F..H.>....~...Bf.W.7iz.!.$....Q^.'.I.A'..sD.T.%=..1y.(Q.....Q.s..P...(....[E./[BZ.x%.F..y..e..0..}.b

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\PDFSigQFormalRep.pdf	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	467032
Entropy (8bit):	**7.998429394088415**
Encrypted:	**true**
SSDEEP:	12288:YKpJNrowYI3SErZ2wtrx0FH/zcXhILGytYRAW0pWWmz7:YKbNtYIpZ2qszXSOYRAZ5mv
MD5:	31D157B8495A3814505A386FFC32F9C2
SHA1:	BD93048FBF2BED110AD29A16F016E4E72560D3B7
SHA-256:	5969650799F5AE2348B7DD9AA18AA328D65D65785A850B933540DF0411EB9437

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\PDFSigQFormalRep.pdf	
SHA-512:	BCE0EA6608A9B360AD96EDB1647D27FE71C7C8EC46DBE4BA2A8229C320E2D9E112AD0360945480FC592E39FDA0F32699E45C85C74E8CD5D0DC0E6575132B6CB
Malicious:	**true**
Preview:	..u.h..'..F.#.am..z799...i....k.....S....:@.....%.[sL.../....z).....b.xJC.U..6u.`..50'.{.zBP{G...g..O8.)v...^#..f3..2.C?jbZ.....<...4.n....I.K.S;I-.....(..K..'.T.6&...J!..5yv@..@. n..i.u...m.`..$.. .r%r\|.#.iz.....4sMf%.ZU.ha.6.NX.....n....4j.M..H..co.K.U..Q.W,.bs..2J.....u"..>."..W).2..(.....w.....\|.B.l.m..sL.D.,..(.4...+HR....}.}O.3c.K.H.n..[...2.j.P.....<u. ....W.....1 .Djb.{...>....L_{....L.e.I...d5;.*.O..L.....).....F%....Z....SNG!,.}....D=.+.....j..C.4x...b.H..._;.....2..m.Y.g.%.D...._.'.....6.Ro..'.....-... x~.Y.(.{....oJ...jX....x.4.T.....t..M. .j.&...l....+@n...X. ddq{.f.5.(K*/Y...T.....8{.y.,.h.*&.J..UG[..0. .P)..d.hn.?..),...\|Mp..+{..*..36...i...[l...&u.Y.gO...c...^T!.....G..:.:..L...D*+j.}.ze..V.K..O..Z.%.`^:QEk.%...I].$.cV?. .Z...JY....l....?..C.X.=s.N.=.....d...^$.....0....+.....|~..Z.|.!..D.-.....:.dV.H.2.%R P;_H.!..\....W.j~.....2;...M...].k.....8.y,0pj7.?.....T..C.9....DT..C.....`s....#V. ..^.

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\RDCNotificationClient.appx	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1822808
Entropy (8bit):	**7.9998273658972145**
Encrypted:	**true**
SSDEEP:	49152:aG7HsuzWAEj1QbHgRs1cOYr2fD+SzKvkK5f+fPfkE:tbarxgAe9YaDMk+2fx
MD5:	72993C2ECCE93CF6C7A0F7BF121EAFFD
SHA1:	AC68D97DB162B66F6F6EACF40B4420F1588A7ABB
SHA-256:	1C6848EB40C256E384FD5D40416F335CE60792FC0F50925F0F17A9B270E9927C
SHA-512:	A2543958353B9EEE1D070A9D495AB806CFF3B83F78BFC67F4DECE060A8C4B00B5CCCEF0F242160DF0C51C12A8A7472AEC6444361D75289BABB6FF8A84B4B7F98
Malicious:	**true**
Preview:	yh....#.....m}.-.....h!SQ.....p.....eS/.<..@..0.Dd:'.Kq...Mw.....NG.Q* &r-.]....j,.....@'vz.#'....2..;3.YlG.....f.C.Q..4.....3.P..0.m.P!..8u4....+...Na`.....z.\.5.^.X.>..&t..(HK.....-.O. Bl.....Y..].8G.K...PC..E.aD.....y4..f..:3.....E..g.N....U..."s.....w6.n0@C.,3.'5.jO.R..x..`.j\.xM.....3...?.X1upV(...\../..MG..#...D.....m....O....$...>..U.....L.U....p..Z.....E..[..._....x... (..GG.Cb..o.x.%.F{P..*6.....!.....HD...6s.1...P..?=pQ.8...\U..R..7...w...7CF.....8l.....l.....k.....ll...?}.U:JN..9..dp..V.f~..<.3.X...P..R ....9.....1.&..T."..j....o..[... ...S..D.]..nj.GJ.c ...e.....Q..:..H{n5&...&.....=....5..h..FN..<.Va.X.nT.qS.1..C..8C..e.c..U....v...\|.r5.+.@.E..8..=...zYU..8L...$b..4O`ITn.Q.....9.....E.i...u.....i....Y.....%.h.%..D.V%.....yN... 9k....Q!....d.g..+0[.p...+qJ$(.s9].P..+.b.)...BHY.....4.Ke..2.l.l~.....aW"..tk.k{=;...M&g.....?...Wc12H.O..I.....iY....:.v.7..im<.0.B.,m..5ASn -.."b

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\RTC.der	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1186
Entropy (8bit):	7.840646724380258
Encrypted:	false
SSDEEP:	24:8P+1rL/OpreGQy5bObh+IdA81L3Jo1K8oCrXmWiTuHC3CeTZdKG8:8P+FLmxeyb7+5oK8tXmvuHC3CeC
MD5:	AFB599783B32617ADC642B3480DCC500
SHA1:	F3674D4CA66A192F56D2565B4755A8A87016699E
SHA-256:	6C74EF61B5A5393CE2C742DD7A390699ED2B65BBD940EEA103D4DEE9AAF8C0D2
SHA-512:	0FC89E0026A3AF49BACB56593BBEE75B6CD37001C58EA6083DC73053854BAE4501445E1A38C766C4E947045A523D9F80A19B6D68A8C739140772160A8881326A
Malicious:	false
Preview:	.l'x.:...!o4?|e&..2S..`.Upq...|0....(..mel.....m..... .P.M.J|<....'.S..!.5pb4...O....Ob.l.<0R.....b.y.@;.G@.Z....04.:f@8..5.....|9?..#.^.[!-_&.|.R..Xa...oGRY...i...i5.....c7w.@.. .?.8.$.^.....q....W@..[D....L....3..RA..~....H. ...../..AM.M..2kl.oi..$...fZ."*aYmL.g.7...Of....O.z.....fX..l....G#..5[.=.....V.....,_i2....)..8y..Z..ty....b._;....%h.5?.R)s..i6.j.u.:3zFkm. .!..3} ..R.....s.M.=..V.wA..^...-.....l..L.Cl..%w.4.....S4p..e6.`.....[..b....o:....9...y....w...6.....H..PN....S..[=&..c..E..O..%..9.G....'.Z.)...>Q.Hx....:.fL...J.....h.....b..]... .,,.a ...NH.....n....'...e.)..9.....]...\.9Pe+x.z.(..~..Z.e$M..`a8.w-...*]..V..)...|x,..b...b."..{.p..c...n8P.....NIR0FI.e%..q...LxdG...We.9..K..0.2.....h....^.....M[.h@6.....V.....1..2-....G.U...L....b .\l(.....k...8..r...4]tx...RR..h.T..S...ajG.^..pMQ.i_n.m.OpJ."+..Ys`....!.k&y.I....)..8....Bh.}d.7.(y..P.....W..*....S.f...(C7...`..y...Z.w..H.f.>.

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\How to decrypt files.txt	
Process:	C:\Users\user\Desktop\local.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.750716892507042
Encrypted:	false
SSDEEP:	24:uXbzIqJzIgAkQEcDywrTqaWFKOPcHRLhU7dfGEDGHmJlhX:uznDwKaWFKOUHZYuc9
MD5:	FADFD11B8F5B759F6910B93BB6D8949C
SHA1:	3E094839A6C9D9397BD5C38EF95223CC0B8EFA01
SHA-256:	34703C088A5C8D374AAC195036505BF31B5DD7ABCE9BB56F2C623B8ECBFD1F51
SHA-512:	3072F390746D6D45ECE82580EFA772758AFD8AE6F4D6A03ED8D69C27A48F837DB0A694C29FCCED0A2F6345067FECED1D828EFCED8061AE9969A82C2E8E9E850D
Malicious:	false

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\How to decrypt files.txt	
Preview:	Your personal identifier: 20C6BA93EB94....All files on TOHNICHI network have been encrypted due to insufficient security...The only way to quickly and reliably regain acc ess to your files is to contact us...The price depends on how fast you write to us...In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.....FAQ..Q: How to contact us..A: * Download Tor Browser - https://www.torproject.org/.. * Open link in Tor Browser http://eghv5cpdsmuj5e6tpyjk5i cgq642hqubildf6yrfnqlq3rmsqk2zanid.onion/contact.. * Follow the instructions on the website.....Q: What guarantees? ..A: Before paying, we can decrypt several of your t est files. Files should not contain valuable information.....Q: Can I decrypt my data for free or through intermediaries?..A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss. .. Decryption of your files with the help of third parties may cause increased

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\add_reviewer.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1426
Entropy (8bit):	7.87024477029722
Encrypted:	false
SSDEEP:	24:zHESwPBnsz5XY3Eq2gRAwa/Rm8Sr8oWwwkYkYQzFHiDDletLOfyh8me4qTfZq8:zHESiOz5I3EdNwa/RruWwZxppCDcOfZV
MD5:	98CA372E4898753B6B8E6792C5F894A6
SHA1:	4FCB1DB3E7A8585BEA0F2B9BB5A29DEC768F8DF4
SHA-256:	1054D4CF50677840BF76961E66E94B0F1A93BD1D81E45A5079BA41ADFD615A90
SHA-512:	24A4245BFFB0086A952ECA5C2C9DC9AEAFDA16C85F75544AE3B32E59DFF81EA50BEF974981030C99E032DAB2EC1AF1B86A34BA38C8B35DE2DCD56B01BA06A AA9
Malicious:	false
Preview:	.....(..ah}J\F..E..a....M.ky%<iy..K.|K.b..@...5.Y6J.Yj..rR...X;sh..{.K..."...ZRYO1.3...k1ck'....GG.V. L.[JZ...O.!N... .4.=.n....@...I...#.I]..@d....W.....k..ZS..1..`.U.}....).>Q..W .SLy..R.....l.77...j...gd$...L.x.c..<.[...nv)..H...}+.@.s.M..9....x...w....WI.$.....w...H..%...,9.f..2...v.....Di..,m....w.~.V...1.J.r....*...k.....jh...e....4.....7....u2..f..~.1...f.M..gM.4. .....w.O...8v.Ef....c.c...w...^Rc(m8L.....t.z.3.?.....c.54a..dRm..g.?-2.....%W...t.....nW]WN.87...GK.U....k.M.Z/..W.M.j.^!.`.........Q..`.c.>`....!..k.].o2..~..B...\.R2..T..K,..w.P)..\aF.5 z.I....u...Pw.....[.X64,..S.....t.r....)#..+.D.z...tIv.$Xl.U..n.aa.+^k.)>N.....#.1.j./f...t..mP.#.6..H..}..z.>1.."..... .....s.).....#..4.@Z.6...^.....m*.hZ.j....Z~..q.....4.f.....-...J.`..=. ..&r^.~..f.._.g.A]z...cs.I2l...A.s.~...g..B..'>.^.^.a.3u..[^pQ....@....c...n.b(..U.....+D.x....D.B.... ..X....W....I..KC".q....3..{...a..S.....|vL|n...R.....^k....b.

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\bl.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	171
Entropy (8bit):	6.945601710779676
Encrypted:	false
SSDEEP:	3:wsAW4LiTW31Pd/xq7KGLsHY+m67QpJPGCcbkSsYHzMn9JbmaeOvZ9EQDiH8:wsAW4Uad/xeJ4Y+mjJ5ctzi3maeOvYDc
MD5:	F5BFA57A15C4D13BE4B3B0A4F5706E47
SHA1:	9647E4BFEC3ECD5884BDB77043FA3EDEC26E62D4
SHA-256:	A1F7B4443B3E3A351B3265178CC00B6DAFB476551AB07F740A7E04F8B93DA560
SHA-512:	02F96B1523BBC11F7A2BBB8C41191C3393B29B80C544EC712BC53BA247E1C9AD222B7F9A8D17BC22380AA7AADFE2D6822CE4C74865D330DA5CC4FF63936C1E B1
Malicious:	false
Preview:	P9R.8#L.....`.I.<....stR.....k.Z...3?..../c.I.^..$.%Wi...y.e.5K..h..lj..Y..J..p./B...|l..|.7Ir..0..Zb.+.&....L).[gF.5#..F].]n8m.Qg.J3 ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\br.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	170
Entropy (8bit):	6.809160936035882
Encrypted:	false
SSDEEP:	3:vjocn+o38AvTVlYSkzKFUcXL1769L/xA2h9eWkjh+UeG1BYN2BZ9EQDiH8:cF88Kl/GKB0LGseWkjh+U/YN2BYDH8
MD5:	3D3B38E7131B202616D9BBFF8536BF7D
SHA1:	A2F8C5637E25593ADEA2E095CBCCC4B2C84E339F
SHA-256:	C4C668CD7A405EE1954F668B908B4EDA87255B1573C74A4B346EF2FD7DD2ACD0
SHA-512:	76863DA349CDA1381CE0AB52F6CE77EA985794F7B9C2A5E0F5AB919A516F59564E8318BF1F34EDC5989B130EF1C23964B3A841CCA64623BCD15355C004041FD
Malicious:	false
Preview:	|.F.jW.....2..H<.y.4..U.@=w...../..XB.0.rn...*...\..1.b..X.....7....[..9%..9G....7,'.t..A..Mr....q.9r....9..".>..... ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\create_form.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1282
Entropy (8bit):	7.867586921050993
Encrypted:	false

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\create_form.gif	
SSDEEP:	24:glJoxTrWsLHY9l8aqTJor9sWLqT0lUA0MrdYqTFuw4GgnWvOZT0eOeBKwYApMy78:gyoxxw8aqTWrOWLFx08dbTHgWv0T385
MD5:	3D3D572F460DDABB2556E097922D31CB
SHA1:	D38D6DB232A9BB51535ED02B7134379925B8C8C8
SHA-256:	F4F4A9364202AF1DDD557B40D66A7081C540304BAF2E0C71E07580F9404E47C3
SHA-512:	EA3F18545E59A792ACF8524858BCE32EFC9361F1B6FD90E30D56BB9B7AF54763432B70629229C5C50D9EF2ACF72A99D5A49C1D15E356770BF87E5F22C3D64DE
Malicious:	false
Preview:	0.g...FT{q.h....S....<h..;..qze"f.^h.Sgz..l...x]..7q....^&L....i..ea!.~7...e...U..Gv1....|.?.,....}.....C...._..T3.n.d;.......]dg...%.RO.&.k9.?..8..+.cJ.2....SY.=9..J~.p.=t..+xy,. =..).M..a. .:.....3..........n..r....a:..y6"d9.r^.....I."..S.BY..=A..).c...}B.yDZ.h>.......xK..p.~..|.....k.....}... '.f.........8..l..eDk..R>....U$.Obr=..I.h.........[<..$..BU..m_....S4T..s.+......2m.Q.f#.# . I.&..... ...be.o...~..&..@...3(Apc..dAt....:.....F.....au.U.. ._Q...N.mR.3....*...T...j....U]=.q.....8N.[.A.I.+U.*..O...5.\,..G..D?...\.Exm.v`...}...t;pPl*....*.......%..{.q.4...T..Z<..a....P.xe7.... .E.T}./.(2.k;qO.t.gt)m.v....z...*yfu.....V.x<...E.]:...B...3..\...!.vCy({....cO..M....".....&'.....f.H...v.._q..q..J.d/n,...|H.........G.. #.ZE..r.ZH.r)S....r.?z<.C..Djd.qWH....'..to..q.b..7] @.2....CN6N"{..g....0.N...RO..g..7.Sq.W..\0n,...S!...T..4.Z3TjW..421...]].....t9.4.....r.[..X.*nP...P.u..!.$.pq:...1.+v.^..Gv'..4F..{......r.v..lE......`w...}.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\distribute_form.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	909
Entropy (8bit):	7.760611706245038
Encrypted:	false
SSDEEP:	12:vDQlGcKOrUqFYZysjVgdTbXkhrkrpXmjrr5tk4+PaxfOx+dWBkQ2dLMdFNYj8:mKA6Z1+nkhIrFmjLw9B0dLMA8
MD5:	03FC36241EA4E3A0805B90C575934F29
SHA1:	935356A4938DC0BD2DB43082229F0F477B5DF934
SHA-256:	4979EE0E909B3EAFAB4BC47874E9BCED4988A2AD6742E5E73154AEDAE5D7157F
SHA-512:	176EF8AEE72385E97B4DE866CEF40F27D21641AE530BE6FE1171938C5FBEB1087827849401105 92B5D7FE4B86BC41140F96963C1677BE8568ED95C4DD14EB0DE
Malicious:	false
Preview:	..c..&b,...p.n.K....^m.....$..X.GB...Z....AOt?E.P,.....'@-.....[.....SR.T`..E,9....IM.....7..'W:o....`.Q$.A.3p.FGQ...b...x.Hc..+..."r')m.pS.K..H...}O2}#....6..7Y.5.f.@....wWx...K <.Y/P...w.h.\...~...U...I.E....o.nw0.(.XV.....,....6._r..c....7....'.....u.....]..J.5k^.....=....1...O...J....0(i*.i...#.]fTSO.Lk.A.}MM.H(.l..B.zA.M0ti...'.Y....."...>....!K...;..?..@!.*....&|[.9.E .#4..FVu{.[[..~.....<.....R.3.a.+\[...n..5.I*.T..#.....9.Ul....64..h.....bW.j.hL...7KhK.l...=..S..$~A\.....RlF...1#.4\|.=..o....b.i.fq.4.(..%I.....+..?..L.-u .EUIIH...):.....).8..H}. .^....~....:)..Q4..MP.....F*.).~$.`~.....:.(E"...F.0.-.\:w..x.E.X${AP..[.y>.,..:....5.,..z.I....v%....Ik[_.=O..3....#.D...Eb(....k....mZE.y.....x..W9.x..8.9.3..@.Q.)t.-[....N.C...^i.F.]D9 ...r...A....9.:.#...=<g^..a.....y.....U...7....B.0W.... ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\email_all.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1531
Entropy (8bit):	7.857685361244157
Encrypted:	false
SSDEEP:	24:tTMJ0lWgczqPCT/rTAYA9k4mKyayxDkoJHBazX2PJdpboJArUPRTROvzUbgkrJy2:tTG0AP+HgZyDQoJhayBd+lUPRtaUbgY7
MD5:	65D4756B33F1DB808D52304049848274
SHA1:	BC9B01A61AE6F61E45A82D113E7FBD27AFF92BE8
SHA-256:	E8DE98903737A2F21816C146FD2C5AF0F4B3F271F74179241D231D26D134A73A
SHA-512:	594572360BAF697F37F47F3F8DC284BB8D3481DC03A642D662EB173E397FF2B191D5956C698D42533BDC32FFC3438E32AA98F2C1D3E924AE4AD76F420C66CA1
Malicious:	false
Preview:	+.O...{._...O..v.....\"7*.....g_..7J#._U.:T..|...._P.....n.....q..YQ..<...+L..a..v.y....xc<.....|MO..jjGk..^.....d..h>72^3h.)C.f.q8Um./^C...!....f.cI..z...<.7<:..8Vc.1N..'.W!.@....l..[a! _...J.T...W.NL.....g8.^.>..eD.`.e.....L...Q<..\"wTx....._...$....j..ks.7[eEeN..v..r.C....P.%i.-!..... Gi1.$n..i.....j....S.E.D..9..;..o.....#...C2.bn.)f.._uO.....Y..^..U...+....d .....\.P..@.".6@.9!..|.B..w.D.V>..`.....r&r...a&V@.P[...]a....r.`.....2.D...../..$!C...G(..F...4....dX....V..J...."R...|.,.y..5..8.w..G ..P..a.Q.&.@...vVk.....nv.I.2...7p.....LN..]...?}...c... .....J.F3L.^.Q.. ..P...i.....i..8Is....B/b.O...v....3.5/5..Z.us.B...Wf.X...f.Hkkm..x...@.<.....M&.....gUh..6.J;H.....i.....?_.....D.3.~....p8=.G...BL..:r-.x.7./.....?.V...?V=N.90.X ..Vm5aN..}....h...W_....Y..P1.x.~.[./.R..@.N.....I#.<m.....H. .1..........r.Q.z.....QPEg(.\.....EXx=W2..B..v....6D..qQ..#.[...@.....,...!..\...\....g{..,+>U.. .U"...+....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\email_initiator.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1448
Entropy (8bit):	7.836775157217817
Encrypted:	false
SSDEEP:	24:Rr2xl+7oRiIQ3lDay/ZvpKZb28U7NVbUB7DxyiWCvZcOQn1K8lqQys6SmGDk8:h2xlVRiQGy/ZvSy8U7z2iCvyOQJlqBSd
MD5:	BD7289E39B280A98689E432609156A6A
SHA1:	654CD9C5341D0EE222DEF82ABB154BE35406D9FE
SHA-256:	8B3B5C1B1D9D243CCE505411916959351EBB44FDDBBB629F3F8E2740812EA8A7
SHA-512:	A6542F557F579E46B2FD45439A6CAA60E2218DE0448DBF437542CEE03937F884EA0E3E2232BC8C516520EFE7F5682DAFCB6163D0F43A310AF543685B5F93E9FD
Malicious:	false

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\email_initiator.gif	
Preview:	.....z..K.&...c.....A'[K.-.[j.&...N+k.9;5.....57.Q..W.....F.iO.C.*...`A...sBU.h.....~3...5/.G.=g...o..=.....g..2....B.Q...ZRM..r....ke.....o \.....;l..p...`.p....+#..(..y...F1..~..9. .4....Y..."r...`cG.o(.C.L.....t._u.SDC>D..`....5...2-..:A.p...].w..k.%.z..?.I}..../.X.`*...C..'.e..+&i.1{..!..mTm.....4.3'.Sj....P..N...YG~.CD.k..)/.}R....j.K..?..8).ZE#.!l...`"..5.CQ;e. E2J*...&.#_.kRZ..3..<>...o#l....HY.w.N.Z1...f..Q_.}og:..}.8.....u.s.\..jn....M.=.f...{.b.#.b3*.R.{....}O.rY.b....z^{V..Wc...[..4M.....}v....D.4....*.P2.NAl..*.b..(.....V..mb.@....}.j..GB R.....<g.....Ve.M.....o...\.....IY...,.X.v.....@.}^..C.p...e5.B.X.(t.W?.eO.....#...(e..6.<.?..b~Y.6.-...M-oRx.].:vEH{.....A.o..G.~.to.....y.,C.;b..a.S...f.E.A.....m...w.....5t...KN..%i.. Q.L....Y.#..*.0.C.9R.....ep.;...B^..Z._..L%X..df.m..oT.....=m.#&*....XV!v.c.7.'#...rh.....L=.=C..S:.'r..!..Y{^q.....C.....]...i...;.. .k2..c,...m...H.\....VM..o.7E>.lRA.9.....w..Bb ...l..$/..Y.d.

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\end_review.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	988
Entropy (8bit):	7.814497609559955
Encrypted:	false
SSDEEP:	24:6M6TPaArLUJjnHtbZ+0Gy0ryjH1IxzBV7ZySyct5Tw0UtXV8:6NaAMpHhULyj+xtV7ZxtRwy
MD5:	8ED0BB212A02A43A62714DAA3A65C15F
SHA1:	F97A3DF5B44A7F1F864069E784C2D41F532A4B85
SHA-256:	799611E7D3552FCBD8D2EB226BEC2C1C4E9ED04942CF08AAE643FE7811FF3DE8
SHA-512:	9F44190A04E4967CC46C7EACC90B13BCC46AE95DDC92C42B5B2F30142370A2FD81DE7764E1B1DB6057D88587C42CF71C71FCDA85AD2C78B73710CFF61E1FF E3
Malicious:	false
Preview:	...J.L.R.TA6.,..8..A.B...MT.X..`.~........$.........GhK.4_...s....P....i....c.....]..xOD..p...w..y....3...I...Z....y..:,... .....$.eA....6..p8..t..hX].t:.0O.m.Q.....i_.2.....AjSJD.....S0.u&...m. ....K[U..1z.G.:.....Y..YM"x`Y}2;E.ZC."...p....XN.~.bz....a..2..Tq\....Y|h.l.z.&..s....U..We....D.....t.m....px..$6..Nh..#.Q..lY..<fK..|..._.....z..X..c.I.....o.$.1..1H2e.Yf.q.C#.-....=7X 4..ON..:.0..Do..7I...H...1....<.neR>...'.-../#...^...$....Q.d.2.l'....b/y..r~T..p..Z.\Q.>.O...):.;t.-...t.....O.h!.d.<..h...vX...Fu..%.$|.....x.S.....k.....u^.4.F.<.:..~@)..}.H.....E...OH.A. ../Z..d....8...~.b...<.(%....)...e..A.... K..@.V.).....03p....2.3.m....4...B..gkr..L.s._....f.W.z..".1...IH..?.N..Zl&B.o...{...........LAay..A[W.\.....l%.eb.M../".0V42...ft.0(.U8%.e....+.]. .u{..!K|...Q..#.....W..$.....Ag.5._.q..F.apkA..`..@mm.....G.l.i....Z....u.e..7v.3F.f...3../.........L3}bj...0....!.Y.2*E..Z.l. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\ended_review_or_form.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	DOS executable (COM, 0x8C-variant)
Category:	dropped
Size (bytes):	895
Entropy (8bit):	7.760282422778677
Encrypted:	false
SSDEEP:	24:FKaejK3Op5jkLvvsvZGiR2IZDrgMCUqFis8:FPlQ5jbxGO26nCUyi9
MD5:	EF13F2844F1DD82A0741B18C472B264A
SHA1:	FB9F70CB8A660B02F1BB1D8E75B0785130311BE8
SHA-256:	65652851A10C5E65188D4695FBFCA8EA609EB81935EC59F3D8155BA77AF2ABA2
SHA-512:	BA77EFE0E0C5176DC84738B34C03037CCE69C49A348698B2F29C723E8E56E25FB1CFA900A10DE575EE4C06FA8750D764D90AA4008EE1448BF72B3BB9A28D795 E
Malicious:	false
Preview:	...1.p...oRRP.....Q}..n.....1P.....F[.ID..A.....N.1&..9..Y.<.....AT\.0-.5.A...dUi...X...j.....;..9:`k4?....Zg.[...F[m...."..6c.2XT..DUK...`*...Z...\..1.W..bX"....Z.v.\...%..Y.yX.X. HXm.....0.X..}f&.O.=V..WW..(Yp).vG..r.....q.....=....e.R{.f...r..5x.1c...~.iU..<...8..R..)...V.c..b`...Yc.....].9...I...Q.....i.....h|rz=.. ...2....?..uwl..^M.`/.....5%.?.Q.1.. ..=..0... `..Y..Q..u./..W=CW..R...iD.VE...4./I*.).~.~x..FY.....XV]...Z.`..>...3....JN.TF.?.qa.}B.r.OST..o..""...C..E.[....V#.kk.O...#..5.p...1.$.2.?._J.M}.r..2#.95y\s@.c.....lqm...G..... [.+..0.%..t<&.4.t.....7...>.....EON-@..%...+.....L...t..1._.{.....X.....+.\(..FI....p...Z.`....4...$..8.....q...N..|...2q.....a..$.V....1.y...[..../...R.c.I._.....xe3....(..X2..='#X...r..n.r(..3D.V... 9.I.....$....x`....~U..\..s.^q ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\form_responses.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1057
Entropy (8bit):	7.807731968582855
Encrypted:	false
SSDEEP:	24:a3l+h0VVbby8YfdywUTnd8kFi0orEYMfzjwSuJyi+fKOU8:SlHWkhOkFihcuRm
MD5:	2650D3FB120DA08517B59512E7F17575
SHA1:	606A5CDB816A4C3147C0638ACF486BEBF60015FA
SHA-256:	79DAE9CF4E145E15F7CD3411161E00912DFF181E294DFB513E5871E3C31ABD67
SHA-512:	686E413D26CD2C79FC2B9917FDF3B3F55B344292F8C963D6DB94FD98962A5AAE6A5AD5936E531AE0E3FCC38192C64A1FC21985ED54CF94D3546BE1375A1108
Malicious:	false
Preview:	.~..@S.....b....O`.....w...N.,...l.....\H.%#.,...x..O.....^0..u.*w'w.NN-.#..j.9..I.~..+I.....#.....YE...kb..H<+H..h...<@~*`...47....]^..z9,.X`v.N....}I.z&B...xO..k...LH..0s..e.o....?...._aB.{ ".hh.....]..tv..b.U.....F@y:.k.]....:Gd.vl3B...4.)....X .....i...).[....Z<.<.6..A..l....b..!UJ_.i..g.\.....I.....k...E.....`..!.....2.....ZM>M....jy..r.'.P^..n.n..6o0.0..O]....?. ...x.c.[.v.Y.z._. ^.....6...v..f...%yL...9a|..Q}...l..n.F.FM-..\...Y..C+...d@|.|..g...MiX..T..>..pXj.5..W(..."?H.I.8JB+...n2r.f._O)NI....Y..C^....B .....I.;.*..#.^.kh..wZ>.8..../b....Dxiq.u^d....pR..N..V.86E. .bBd....2g{...@.... ..e.lQ......wS.E...;.W.....\+...dEz.DS g...N.Gp$t:X..>..*.H...j.....o\F..*..s..=6._h%.....,N.d.cl.!r..~.....>.....c.G.cE..-.....[_7F.?..z.a.:....M@ FD..+..P.b,m^.Q> 68.S.L.g@...#.....bt...FR.]..|.'...3.d.;.....$Q...6Q2.....m..,\..YCR...6.....b.ZY...A..l.6..w........-/;y ...0...`...C...t....>.R...J...H...p..]...]...k+o

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\forms_distributed.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	701
Entropy (8bit):	7.679239079893645
Encrypted:	false
SSDEEP:	12:JbWIfRP61eyzjm4GSBZMiygdBB/l8Ynin6ycXWuAYBr1maB99tGnAhNC8nWaV6WY:J6C61eyvrBogdX/JYnin6nqYrmaj9ttQ
MD5:	A1B4F6A4683371EE32C21E0A8E0B1A33
SHA1:	15C771782C62C6BB762B53913410597E23FBB1E4
SHA-256:	D95B6E7DAFEC01BE36BC2D1FCAB98557EE18F94FCE51DBB36B52CA15F022D0A0
SHA-512:	E8209E83FFD1563F6CC26A707BC1DECAF20DE5C352AD4B4F4609B053F24CDB9CD3A433C4747F0E16760A6465559913BDEE27BF569F6306E5D28F2F86BA882B9
Malicious:	false
Preview:	..GrC....ja.-.DF)...ob].G.....3...V.c.....C{U.9..?,1?....4.p<....8...-.....".@yD....B....@...;.}.0n..A.-!H.....]..... .K9.LHyg.s.....*U.V!.Ep;.&ix...,...KY.l|.V.3\vJ...!.....li'<uVB~R p.]4.>9. .Zq/.Fz.b2...N~.?-S..>hn.....M.K.b.Br{..G....p.Q~SM$.....f.G...5.%....,.8.^.*..6.<<....g*R.k....QQ.C.u.ae`.1.Xr$..w>Z.=.6s.....AZ.t..j.UR.CS0h.{...S..8.<...V..4...b... ;:.%&fn.i./a....@~...66..B.>..]..4jF.f.....2T.t...GC.....".I..H...HQ..h9.z.^.....I....u.=..U.....rIR..2.....H.:]VVB.{-.....68.3wB.T'4L.T.....2Z.gIWF...Yw.6..;.@h.)..@...']C..S.,... ....yi..z@.q..,n..h(.ly.B. 8...R...Ot".@.....g...Y..1....S...b.s ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\forms_received.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	703
Entropy (8bit):	7.728909809549965
Encrypted:	false
SSDEEP:	12:6RRnkYB+4Ihcsb5OH1i2FU5WdJA9NNxrkrxVqWFPCOoy0GynRkUVJSh26WCA2M4M:6Rnx+db5OH1iAUsdW3DrkdVqWxCOf2m6
MD5:	70C9B57090F114AD1834EE976B06D213
SHA1:	FA368AEFF0FDE2D2A71CD09F8010D4CA0D272A83
SHA-256:	4AF1CD825A13AC85B23969212B909A12DD5BA418FEFA30E5970FBCE3CB5C973D
SHA-512:	73389C27BCE411AAF7D16D3D620927F6D1D3AE6FE54A3BFB78A865180A81BAE038179154BBC750E74A9CA50CB12D3291F08D685DC4C087398463ED189480497
Malicious:	false
Preview:	:.._v.c..@.s...C.G..j.."C...aE.*.8...".rt.X]...w.n..KIU.|...lA..>.....$[<.+.g.&..SA.._.d;.#..4.....sm.n2A.#.....[0.~..:...9...".g.$..sbl.A....U.J.T.5@..D.R.....K..Q.... ...e.s._..F.].=.....\. ...W.R.KMc.3..&Mm.>Z...T..>..'.....*.o...OD.7E|....T.>.....M..y.B,j..a8.U9g.r.%.Ezb?y5NqEXP..u.....8....)...x1$..9..J...H...^X....q.....B;X.>L..+8.<.....SPj.p.RP.....c..h .....$y.....*.;....{4...d.M+.l-.....c.?.c....H8.....9.:.....P...I....Qr[.1...-k...pej3.&B..>...~.g..n*.....n.^e.....)..G)...#z.tK.,.1g..V.7.Pa...w..5.".[...0.,--...9n....!..9...wLH4...(tun#..9.. <Y...@.5.!.;qP.....\.x.W.U m....M..{.7..*...rA.n..5m.. ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\forms_super.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	640
Entropy (8bit):	7.673515871096479
Encrypted:	false
SSDEEP:	12:EGcNTsfIvgnNSUE5CAAoEuu3dAZmmg0XIPjqgFsn3h+yi3HNYj8:EGNfIvgUhCACuu7mg04PjNa3gJg8
MD5:	61F5CB20D98669EFD11A43ED38B9273F
SHA1:	5CF4CE6C9193021C5D8F525B7396C3B8E6F88030
SHA-256:	D54F026AAFEA4AA2A82324D68C8EEE7D0366C3F326B5A3CF0BBBE51244A63AE5
SHA-512:	A9AB731DBD16F914A95E0E5E071C9C16FF134365503A05220297FAEFC46F4C99125B12CA0A6235B2085EAC9C847A66EB1F9DBA08477B42875A69F3E6266D13FE
Malicious:	false
Preview:	.....Lb.b...m*.L...f...}WQY.. .b.d..3..B.n...D.... ...#$..{.d..H....[..!iZ.8F..G.....'.>.UP.I.....D...w..(..uz.I.Y....~....f....B5y.[u...EMY...KA.6..:a.q.....^...D.Q..n..>..;.ZR.9C..}..p(.....DN .j.Q....n...38.~.$....p.[....Id%.H.Mo.j.....`.V.ig....*..S....).L.<.....y.oR.d.......*..*4.atW~.....ND6d..<..@.4..Y....'..m1..1^.g..@..=...@[.Ey....s{D..%..c;.V..<.uUF.....!.+7..JI.|....j)1 ..C.....(. /~.Sr.sF..._.v.E:<.0~.....h.{.....&.O....^P..L..YS.8I..MO..ws.a.....J....-.....6..._r....1.f|wS.0WR.W.....\.I.%~.z..hr...=...`...,...^.nw`..4...2] ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\info.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	666
Entropy (8bit):	7.715099470387513
Encrypted:	false
SSDEEP:	12:n9+S6wm1q5crkkOB+J56rAFvaZMU/mZFh8PTXz14sMX8Og7CiUxiYj8:IHwT5cr2m6MFuM7ZFhITX54TX8Og7A8
MD5:	CFDA1A5CA19CB1BA0E3F517D96201AD8
SHA1:	DA6D650CFAF320648967A0246646DB2A9A4A83CC
SHA-256:	32A038F899834D9028D5BC083DDBA85965DDAC9F20D063ACDEA6860ED35112BC
SHA-512:	2821B988C967EA9784D4E072B05EC89E36BA3742C6C757AEB776F8A844F773C801F4C55B0D3A566B387BB8E29A7B193AB42B2933B44D2C0A566F4987CAA477C

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\info.gif	
Malicious:	false
Preview:	_5.....\.6...6..{.\u]...:0I....V.ao.j....m..k.d..../...;...O.]](..2".....l.x.a.L... ..}.:\.....<.^.Y....p..e..vX5'O.Rw..=b..y.A<.u.....l..~8.AE.....J.\.....^(j...bM...V..E.a.{h:.}o.:P.:@.+-.4 ..@.....12...2.....65..p.m.[8>oXy.T..y..''...^.Rzm...X...E.9...g.q...s.H....#.&).t.g..mi..8...x....7|.f#+.....o..&...F..}.{t.n....!...l.l.y.$=.}%...{..L.....$.Xqc...fg.l..^`...G-]'w.|8d.! ....! .&....Vd....D)8Q.:,m..{.A....A..M..J-..''.w.Z.5..e..UAH..5[(.QX.....1L*.U....''..0....SA5..V.Y....*.g..=.5:..r.,^....{!...F.....7....O..19.b]..W.b+.....?./c...U..xhS...8... .s.aq..J]..k...v .eT..~Y..N}..^$~.(...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\main.css	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	8280
Entropy (8bit):	7.9765425160053
Encrypted:	false
SSDEEP:	192:Tz8PpglLwAYhU5HuTt7H6xdV9q6SmLV2LQIg09y:TzEgtUhUxQFaxdfq6SGzIgv
MD5:	E1D7444A470F3C00CB6AF44E0AC61B00
SHA1:	E0F698B2DF7E2F4B9FD7D43225853A74FFCA5073
SHA-256:	D2487B665395983D0D33D86F8B86BEC34141DC5A062E244F2384271D661BDF70
SHA-512:	C9470951150C6495739C9A95E176E35A154451641EF9302D51AF9ECBE4A4EE41D49461ED4726AFBC3EC7BBA843877C81A907EFD9586141AEA89BEE913FF23764
Malicious:	false
Preview:	...|.,.....&y.k..l.....P.=+.C.....@.7.l)..l.x.Ka... ...`.:.Q..... ...PU...#.95....sVy..G././._l\P.:./....$..zv*+K^.^Gx..z..8.....H.N.1L....9..k....{U....uVMG."#...2B..{.f'.K.Q{./..U.....L.; 7)..J.G..Y;y..86.4L.....r7'C[.M..}Q.3V.r..U...s...L...&9..S.w.ib.....y@..r,.....G.a.E.Z...)$.R..A.~.....z....w..._f..!.|..$....0.4.....{.yF.L.::W..b.j..).....,}.A.?...T..{.....6...P..... .S.....^...o..A.f.d.]xZsh.....r.c..|4-.O./f...0F..3..;.D.k4..o....[\...e.....D5.Sm%.Jz...h^k].T_M....:..0.@.B:..3.Z..!!..U.0....'..B....u...;...*..4J.l.b.V.6..VX...7.11./...G^..6f`.8.xf.....Ai>.t ....u....0.....F.....2....Q.\ .j....Cec.(..1.y%7....g.J...xZ,D..I.)Z..7*.9....?.].V~".`M....."<p....~....."$..m.....x._.Q$j... N.X..q}..&.a...R+..-.....|.x..W...>%.y....[!{m.A...-..s..Q&.|I.G0.f.~... ...e._...6.0....(...S.....Y'...0..T.....N(.>..mg_..E..N....]".....K6..n.....\....A....vY.....^.%WG..hoT...iXN..._;.|.....C."..1:.....P.7Z...F]TPn.

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\open_original_form.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	894
Entropy (8bit):	7.787155424304634
Encrypted:	false
SSDEEP:	24:viL+z3fDYgAqrKffRpWbE8kAzSstYUIkpk8:vZz3LYRWKfJpWb5kAzj1
MD5:	8CA7A11A427C14CC4D1CBD610DB2C05F
SHA1:	E422535B4D58304FE55B19007874FA63C50B389A
SHA-256:	57FE1979865F7D18D019C36FFE12C32BEB90252D1A8A011203241F2A27F7C880
SHA-512:	6EDF0316ABAD8FF847C321C910D8F59BD56922C7AAB9EA2485FEDDC888720A600D358E5C838CE2FF22C7438CE649D1DF6D630906D5622ABF1AAF4CC13B859E AE
Malicious:	false
Preview:	.%:Z:I.b0..R.}<.Z..%.'..]>..F.^zmv.U3.Bh..S.....jO..#.....&...@%...E...q1/...=....#{..Z..'..m...?..j.QW.>.9...f.vZ..T..t...?.....1....Q..H..Fk).../..c.P{G.....].....)z....p.frT.kP.(.9.0.}. R.o(.?.fV=.3j..4s/1V.N.z..#..}..twW..Y6*8.[!....".$1...`..JQ#...6....a..Qe....h.:.Z.E.q.~.h._.t...v.OI.....'kq...PP;....VH/..B.guj3.+.h...#.n.q;..!.o..''..%....X.:.v...Wr.\Dx.D.p.....-=9GS..n.9z|B.^.R..q.....]k.....Gg.C.....u.q..v.?.....V.P>d..=P..P.7.....]r..B.[..''....^...n.14Wi.e.].7`n..18.?.....!...9.E..nT.7...*.#..n.[].6.A.T...w|.....j....xN.<6.@..}..!.U.]....@.~. .P..>...?..N....V... ...Gw-....i^f....*...y*...Op;.....5\...1m..*F..93.d-.....".>.....u.b..+.`9.zz.P..\\.....3.w.....@.,...N.`._ >....J.....X_.....k..QQ_....w. ..]...-..r.{Fr.x.NT.q.....%.v. .Q.#.d./...l....%n4.,zt.1.m...)...".i...$ ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\pdf.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	568
Entropy (8bit):	7.617942796528097
Encrypted:	false
SSDEEP:	12:DHasz0jywnOb5WZCqR5OlIXFxwJLxmT80iIQpqPTNzNtKgGlNYj8:D6e0hQQp3O9/DiIQMTNGgGlg8
MD5:	9560E22A3F1F38BC126FC87EEF510D41
SHA1:	EBB5BAC1BEA2B1901497C70BDE32CEA7F607099F
SHA-256:	35F6D8BCC8FAA1387B4BF7695E06BF48E33CA7327A8326708F36BF6C378C2A5A
SHA-512:	50231113A9EEC9D76D19F55394B9144D7DB0311B0B63E3EF51F5DD1DA73F21EBBB0C19629B57ADAEE8B39FB22D17787CD054437A7C47BD2A10CA27172197947
Malicious:	false
Preview:	..5e{.O....*x...'.Ef;.H..\L.?$.....wI..V.)..`.Y.....d.TY..W.....l..E/.G...3.>.W.z...o.|.....1.l...x..d./g..._..{rx+.....a.u...l ..$.f.X.....o....."AP..h..!.y...c.....*j.-v.....$.gi.B.....}l....6}y\.6n ...FitU.....g.....(3W|.0-].~4t1...dP..i"6.....s$.<..-..#s.L.h.....Z..b....@....|....+FS.C...$...#...Q...e._Wk-..-...R...&.*....<.o8.....C...9@Q....%?...b.l}<....Tw....+..kW...IZ.s;.P..@ .....6.SlsS....E.r?...0.{.1.F../.....x.i.{Q.U&`.3.`...S..E..Dq.....H....u.E%y...J.....b}8...ET.2W ...z.at.z.0lC.q...-_M.... \

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\review_browser.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\review_browser.gif	
Size (bytes):	1239
Entropy (8bit):	7.8431650516437825
Encrypted:	false
SSDEEP:	24:F55JOsFmn5BZ3008WH0mNk7Rggxpm37eMbpesBBmOu/qgeDn1nz8:F55XFmZ30/v7Rgg/eeMbplxDn1nQ
MD5:	594C354BEFF5548A505B00F6802FD84B
SHA1:	6CB3E1D1E958C5A5A08737DFE11221370D666EE1
SHA-256:	A543C9B1D4DC050906605D91C1A601845BEE6E9F586BE974124A29F58FA25CE0
SHA-512:	8D25F4E62ACCC207FEEA7FA2D9D220F0C7261417C5E29CCDDE79EF6C8131E2FDDCB5DEC934ECF7852AFD9B602DE67EF49597AFB56C0B6F30622F7C76635B7FF
Malicious:	false
Preview:	d..R.b.e.?..*....-Rg....R....}...@E....};w<...nPt1.3..s.`&...'.....Mh.....3...g...k...~.[..3...i../.mk.....6.E0:.=.....h.T...r...Fy....^.r....3~)L.t..@.Ah5...E6+tx@.t..I..[.b.`...m% ..2#o.j .t.....<v.c.v.....?.n..|!.Qi.....#%&{.....J.....'R.m.?..Y...k.19.].M.o...q.m.s...2t.....aq..T.N..._... ....z._. c...x.....Y.)}.....y....b.... .V...B.....n.k...Jw.e..Y..{w..S5q.....:.3.Y._...3.=.u.../.z.`n...:.c.WK.w..'&|f<g...3.uBf..."{|FOkv....Q0..j....*..Gt%{.s..c.r.?.U.#..y.$...B...Aa..+..u`..=..1(..n#.5./....0.1=...q...O..fu.!..V.@./.|*.....'..u..&}.*.!MN...O....EZ.lA.d.....d..&. :*=}.}..}.....2.7<....;.#.+..1.RY...pW.Lb.....cRAu..[E....$p#5.O.5..9.-.;!.Q....iP..+...B..R.....k..M.F....s..5..!....c.....r1)..~D.5.Q.....4x4r'!".P.{..Lg=.....?.....*.M."..S.av..._..c..X?. g.6C.3....s[.Hi.&...u.g.!#..l..&:[.>P.up@.. .,.1&.O...Y...w...|7.*.^..sE,....S.e..e.\.._m).A..T}..a.\..Slr.G4.>.....f....c,.'{P....f...S.....l3..&`..

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\review_email.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1493
Entropy (8bit):	7.865892769194501
Encrypted:	false
SSDEEP:	24:exFXvUmFPz5YbbSaRnTxVs2nfBl1jNcKeTxuhNW2VaNPQfTHGYJxs8:eDRzExmSxj8qW2VzzJ/
MD5:	249158858BE0DD063DF132DBBAFBA75B
SHA1:	001D66A27FC210171C5C580EEF941CD77C86609A
SHA-256:	4F3CED7E542BAD3C75E0077ABA345ADAFD50F03BDEE34F84D06524488229A481
SHA-512:	2A7371710100F08FBE9B30726D3B6C15B3ABEAF87A36AFA3DF6C05A29B15D00597B234BA818159E43332CF140E33AF04DEEBA94E21B6289A4CF71EF02D22819F
Malicious:	false
Preview:	\u.d..;.V..L.H.l|..~v./...E.5.~.....V.....f.}.,.N...._.=3..h^SL...9...y|....C....!.0{.=.#.on....Z..f.2..D..br.....M-.0.YW>.I.\.*.C.=p.....2..@4eF..&.....p.m...<. .4.._.....-S..R..Z.0R..u.. ...dw..6.`..|e.N.$..T....\..."I".....FL2c.#..`..Js+5W.4.p...`....5uo..J.wj...`;!..'[iA{.(d..DjS9.0B..N....4Gu&n....I..f.Z.a..,2...v>H...^_%.>1["....1..S.-Q....w+W..s\..7@.D.D.B.b.....aZ.B g.J...6[:.J...,..E.*.....s}....H.p....\.;.....m._.9.r;0.e..m>{6at.~.g..a<....L..u.G4.yC.-=..]>.Q.z.....9.Y.)Nk...>...B.....{....,....T.=.dW..h.'._..2...D7:J/..R...[.....h.....H]...z....&3!..^.4. ...Ch..M.A.....;...".En.w>..\.|..{..B..DP.w..\....'V.=.8zr...bUn..G.....3.R..V.-|.12.9...Y...:...>BB.....e..:.....:5F..L...q.:Z.lC...1.(..N..Ee.....V.K.....{..n.....t..J.G....Y`.....I...$*.I `.x.'....~..K.|;V0|]...2..y.....I.....Ar..@V.C/...y(.J.g6.rx.[.a.;.r|j...ee.pb..jTf. .....-.|.{M..sP..V.....R..X..#....c.n.1t..{y\.../..H^.:.^.8...Y

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\review_same_reviewers.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1050
Entropy (8bit):	7.804201362122643
Encrypted:	false
SSDEEP:	24:r/qvEBlHqaxdLSycnTY6AoBDrUIEKvbubci25MKs8:roEB1jxinlpB8Kvbe25MU
MD5:	9DBD1033740EC344801317A58165895C
SHA1:	02BE8D23AF187CAFA6EA75274645FC5879016747
SHA-256:	AE177E2CE3126CB0ED9177F1C374EFE2FB1EE15C66334E12455F65A7818E8876
SHA-512:	3F05883B236B5EFECEE85C87B73B1222999D571154704F8DC4D5E881B687FE8EB8DEBC8A5B1D50AB1B860B108361CF096E4FA1B01F3595C1E0FFCF74519182B
Malicious:	false
Preview:	.p....0.JA.*V.....jJ.T.....k.``...|f.{.R..U.A@1E@QA!..C77.."..H.v..fv;..[c.-.kSj..J....G&...*.b.l!...M..:..)..R....\g.7.t.....Y2...M7..g....q...l.._B....`...h...E.`.N..FD....=9Z..!.-.K<....j8.2..2.. [C.h....S.#b.4.`.Fy..iH...2.fg..D.. .. .;.lu.$.y...4.....`u~s+...WM.....V.....u.8.....#....u....&C.....gw..'..9..g.&K.1.I.Q..(.....-..#m..y.6...]...Rw.#.....N.M...R.vqS....V..P>.sg.....*..H. .4.:..uN....B=.O*uh..b....G....t.....a.]...K....k....g6.d..E8..^.....]_.0\ak,.....J&..*....!{F.07....Y`.....U....5.M.....y.4W.....m...K ...O.....%...d...m.....M9.....Y.{` ..|).m...Tm..[..%.....ZD;l.&M.....1...-...u8....=.m~o.RR...P../.&...d=.....F.G.]z....w.`..&.f.I..{%..38|..<u_.?.sHC0F(.dI..y.I.eI.."$.....Rr...#...D..}.....@[As...%..RQ.....K...GG(. J.....C.....$yX8`Zp."..."LTs..Zy9.....Z.V.#.fvU._.o~}.mO.O.....fY.....;-..Q.:.....9.....$.....ZML.."..D.GqH@,.M.dN..0H.'g..1cY....5h%.4

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\review_shared.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1453
Entropy (8bit):	7.874629841236313
Encrypted:	false
SSDEEP:	24:NMNMQUQE4G8iHCnckDKXMXFfgft5QvQ3970WRlmlIEfHcsRNjpQvy4Ubz04q48NJ:NcMVxHHCnckDKwgVC+0WRlmljHc7vy4R
MD5:	E551C53BE056D173E975925CF42AD934
SHA1:	3542DA16C07BAC9B461DBA6A43006FD17E062461
SHA-256:	4069CD81ABE97E7249898D6D2E39FE88B6A2CFE0B77D8FF4947449CCFBC964AE
SHA-512:	8B9B1222C06EC8E7404D8A31916B5BE614C0D9164A1141BA5A3C71328B33EC0C72F9B8F83132FD83647BB69A0D814188DC779FEA4020C8478ED51401927E76DF

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\review_shared.gif	
Malicious:	false
Preview:	+a`..>...I.,<%..^|...K.....[..'.^.......%S.....*...s?.N.?.%M".N&.{....R.s...Wnc.D.'Q...._..L...`I_~f....X.)%Q8..iY.<....hy..mt.3u..H...q...Y.gMv.~...Bf.5..]w..QA.........!..b+8....:9h.G...IS ..}}..U..[~W..K.B..2.........|.9V...u5..]...K.n..it.eGW9...?A.=....q.y.(.v-o. >...RU...:gp.J}.|;....u'TV.x..".z....g.b.R'..i.<t..X..[[.o...)a,K.....x,.=P.....Q...!.....z.6.kG`.#g...1.........^XYM.....0 b..J...........o.d.>..Y..B...j.sj.2...\..&..lu..zP.....L. ...2lA.5_.J..#....x..x.;..8HA.9...k.....&..5.|.......0..)....[...y.]..[.9_.h.....A.....0..$.....E..e.}*..4.g(.7O.9.Ev...m.. 5.q{F}]..W`.....!....# {$.5}3._...../4R3HDb.n.eEkRd...~DZ;.*.pD|V..!...NM.3.2.-.V<...$M...T.).SW..I..o.X..D..f...V{..G.W4.q}.w3:6_.U..W.SV.5."...AuxA .....v...,F.0H.,...(TJ..b.)Fu.....=2E..}.f....2=W .Kwe.IC..D{...o...,...^.bx.v..0m.SG.b.....:...-/..W.&5..e.EH.J..hN.../s`..4..@a..i*z....r/.@.n.h..p.>..F..ink.....P.E..@.+.....Q.....~..s.lL.....e....F...G`

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\reviewers.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1540
Entropy (8bit):	7.876035473011575
Encrypted:	false
SSDEEP:	48:1RGvOYZss5NcADrnm/22zOmkPtRaOxjfKkMV:HSOYZss5NcADrnJUOmKraOxDK9
MD5:	C1B10717F124347622AF11406B2A72C6
SHA1:	611F8B9AA33789F28C95C039575DDF237058801B
SHA-256:	A7532B2D337D7600F5FB51B9291418E665B1AD07DEDB8147CCBCD2AD9D1EC045
SHA-512:	BA2986E0FF3788571AE9534861C0FF7C2BFE1C9A3823F05C7ABE344C8D8466F2B81E1D6C7497D189F4A3ADC2A888041C0746BA4A7685C2C471C3B168D3817E8
Malicious:	false
Preview:	..t..... ...5.RWc.....c5.1..F..H.Q[. v.....mE....P!./..e...|.....q.a4e..v.K...(..[:.l..4....."..2....K..].....7p\s.V.}):$.4H.....a2.._*....y.i%...U...v.>....9.p.`T4....P..E<.[..~>...M..^..'$*.u. U..L..&Z.4..I.)y.G.(wp....8.+mm...vE..vq.....N....#.....%.....j.),r5.w....f`.hwv7...t..B....*!...O..d...T.^.9..p...>.4...4...w.... E.p.W.@.........x....\8.N.b"$A.....U...).V.(...).t'[a...."...JT.. #&...}..4a.L_B_..k..HP..{JZU.J#.....2F.....4...Z.ni.^.I.'\...9B%w/....*De.$...P..3...\..?*.a.X.....Dz$H\.#.....9...K.C.p."....O..... .,,N.-.)..5X.....e.o.5..U..J.....F..6%.e.).....9.,.'..cZ... 3....GU.)8.@.[..E.E..>...JoKF.{<A.9.....Fr..o.I.O/.}...g.Q|:Q4..x"..R...6.....{?-.y....B..5>Z.^....6.X..X.O.x..X.h.(.~Dhv..[K...$....9........+@.....,..4.j(/.vIe...c$^y..Cv..'.............42; X......H././....3.>,L.D.X..4.fWh.F...3...V..p>....1X.....;LY.).+..z..`.....^.>.>.s...l=PZ.^...y.p._.`..Z#X.........k.9..[iil={.jn..Mv.k.."...z....S..S&.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\reviews_joined.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	1002
Entropy (8bit):	7.853300007929619
Encrypted:	false
SSDEEP:	24:6lymbIEEdc5jDmn5ZQRJFvu7Lxy9wAIC758:6lVTEdcFDcsfFvu7lyFO
MD5:	D216D8AD20CC252F9D1BA2C76A9EF4CF
SHA1:	E8577A05FDAE9081DF31482F3B6B184D1F16F029
SHA-256:	B516D66278E4DBD37405C5FC33358FF55E40ABE8F4C950A3F341F11F4E6B65F1
SHA-512:	4695D8AA2F08672B669034959B7153FE6EA78CDEC4F0EE0AABEF73D23AD30CF99D1164BE9428CDA3EF4ADF4933FAF6A9B60B28B42652596428F899E5A28643C 3
Malicious:	false
Preview:	..D`....q.o.8<E.].)2;K....X..@.E.e2.....BP.).+..o.l.........s.....^.U..&...k.Kl..V...L_T..^.@..0.O.t<....=.A.....2OvBQ.I..[..(.....q2S.q.ks.....;...1.....l..a8..B&.L>..(....L...~.9....DHV.. *y..o..?9....K.P.M....._...I.<&.dk..!.~..^jz...,..w.`.I.?,.Tl0...T.....O...F. :.N..S).....R.B LM.(..$2..Q.A/..7...;.....X.....&|ST.....<.....^-..Y.....W.'..[(%.._..]|Do.*y..Ojr.....B.@.....>$\ 5..J..<..x.I.VT..NJ...63....5.u.._F.68...-X>....`j...}Y..w.dU...n%.^.c.........P...b.2...Cja....c....3.b.Q_#v.5...e..p..Z.U..q..g....4Ev..UxH.p.}^...+...~.....).+....~,.'....U.mg".Y.n.<6^. U].m.....AA.....g..F...x7WT.c....M.5.(....k..S.?..gi.....^YXJ..@....!._.....E&.;h..>..zm}..I.....f.....DG.....+d..+.&R...D:Z.....wX..m.....<bk..tO.U.?.1.mv$.M..OU.8.X..v .Q{..1%o.#V.f.O.>V..GN.v.3..p.G.:W.-.M....Z.~.cG.._....s1.2/O.k.n..H{e. FR.eU{.S...p..yq...gGx..5.4..V.#;]..v...[..Z.+7.....Dx}F..yz.}p..7Pa..W.g*.).... ...z.at.z.0lC.q...-_M....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Tracker\reviews_sent.gif	
Process:	C:\Users\user\Desktop\local.exe
File Type:	data
Category:	dropped
Size (bytes):	997
Entropy (8bit):	7.780845734032692
Encrypted:	false
SSDEEP:	24:oj7Z8LpkeTRspJiTUUREZduy0jgzkFOIge+CQHGzBZ7p/8:Q2VTsgREy9jgp1HSA
MD5:	799654ED27C8CF051B7F64CD89587CB1
SHA1:	B75FB887F35F0B30D1551F018E3A4893E1C0C1C6
SHA-256:	B7247C1B83C35A075499CE8B71EA7C485548A3B3EEED9A728ACB218D66C68AD9
SHA-512:	9B71094D4FCF5AA46B270DFD700527001519C1E12BA5B7C4F62F79FE7442F36CF9A5CDDA9D5A68A117D7885B78DBFBAE34CBDF852572935D641EDD65B7DA1F 9
Malicious:	false
Preview:	..|=i....~.c.4\Tc....2$.h..k..j....ql.6Mi..f$Jp.y>.Q..=.f.N9.4.*..<...L..)].h}y...f..ux...H.n.I..a..f...?|q.N....d....z..@e..(h..X.s...c...|.e..y.t 4=tD?..5>.%..y. ..1.....=...G....5g....uml^. <P.S...B:....0..8..P.\T......N...2..*.2..`.....5\..q8....36$..Q@.)Nn...[...3....K.;...8.........g..L...q...D...\Hx..v.Kt\..^....1.|6'Q~;3..i#...q..>..D.M....'I!../. .%l.1....g.....!..I...X|......yi.k4.N.I.. h.y......x...[...Q...d..<...B..|u=3+...D......../.a...g.....(.Y%a..G.nkUO...#.`%.Z.s".o.J..s.%H....6ii.<..../H...;....#..7`....H.:.?.....s@.L.Yz.eqGe.....@...NW....ke..2.72.....jDNK..y....K 2.....>....y...$<9j.."sD.f.q7.....a...*U..Kaj.PbM...^(J..E3..q......'.... .....{..B.l..A.B.l.M...4.S^t..{0..UR....H..H.;..>..;..Y.P...S.'.0...mRt.`.....'."...V...qr ..H*..x.s..c...)..'...|... .%..t...>9...!.....}O}.....--,Q|.....r.3m.i:.}6.8.....}.'.Fc.e.....t.....V.(.D#.B0%.....g.?%.=K.2....T.q.D.]. ...z.at.z.0lC.q...-_M.... \

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.389871182146184
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	local.exe
File size:	131072
MD5:	d687eb9fea18e6836bd572b2d180b144
SHA1:	0e7f076d59ab24ab04200415cb35037c619d0bae
SHA256:	863e4557e550dd89e5ca0e43c57a3fc1889145c76ec9787e97f76e959fc8e1e1
SHA512:	16aed099d7d1131facb76591176566a9de9a140948f467b7a43d7518215ce24490956b0996d0f7638cf0d313947f12d91d145ebe4d584779e119707d59463684
SSDEEP:	3072:OJcoFjmIxEIltjnJZ9EL7Pkww+Jvl5tB95K:OJtmUEl0jJZ6L7PvwSYB9Y
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....fxx...+...+...+...+...+...+...+...+...+..{+...+..m+...+...+...+...+...+...+...+Rich...+.....PE..L...A..`...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40aeb9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C4DB41 [Sat Jun 12 16:05:21 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	c8318053dac1b12c686403fde752954c

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x166da	0x16800	False	0.595551215278	data	6.61817390144	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x18000	0x5790	0x5800	False	0.358265269886	data	4.97982532504	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1e000	0x601c	0x1800	False	0.305013020833	data	3.56369053698	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x25000	0x1c0	0x200	False	0.494140625	data	5.07293704483	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x26000	0x2180	0x2200	False	0.454273897059	data	4.53204397932	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: local.exe PID: 6376 Parent PID: 6132

General

Start time:	12:26:14
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\local.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\local.exe'
Imagebase:	0xf0000
File size:	131072 bytes
MD5 hash:	D687EB9FEA18E6836BD572B2D180B144
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 6392 Parent PID: 6376

General

Start time:	12:26:15
Start date:	16/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vssadmin.exe PID: 6476 Parent PID: 6376

General

Start time:	12:26:15
Start date:	16/06/2021
Path:	C:\Windows\System32\vssadmin.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\sysnative\vssadmin.exe' delete shadows /all /quiet
Imagebase:	0x7ff790230000
File size:	145920 bytes
MD5 hash:	47D51216EF45075B5F7EAA117CC70E40
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6500 Parent PID: 6476

General

Start time:	12:26:16
Start date:	16/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: cmd.exe PID: 6508 Parent PID: 6376

General

Start time:	12:26:16
Start date:	16/06/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\sysnative\cmd.exe' /c bcdedit /set {current} bootstatuspolicy ignoreallfailures
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6604 Parent PID: 6508

General

Start time:	12:26:17
Start date:	16/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6612 Parent PID: 6376

General

Start time:	12:26:17
Start date:	16/06/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\sysnative\cmd.exe' /c bcdedit /set {current} recoveryenabled no
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6632 Parent PID: 6612

General

Start time:	12:26:17
Start date:	16/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: bcdedit.exe PID: 6700 Parent PID: 6508

General

Start time:	12:26:17
Start date:	16/06/2021
Path:	C:\Windows\System32\bcdedit.exe
Wow64 process (32bit):	false
Commandline:	bcdedit /set {current} bootstatuspolicy ignoreallfailures
Imagebase:	0x7ff687c20000
File size:	461824 bytes
MD5 hash:	6E05CD5195FDB8B6C68FC90074817293
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: bcdedit.exe PID: 6772 Parent PID: 6612

General

Start time:	12:26:18
Start date:	16/06/2021
Path:	C:\Windows\System32\bcdedit.exe
Wow64 process (32bit):	false
Commandline:	bcdedit /set {current} recoveryenabled no
Imagebase:	0x7ff687c20000
File size:	461824 bytes
MD5 hash:	6E05CD5195FDB8B6C68FC90074817293
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis