ID: 626600
Sample Name:
ZunmmW7pe5.exe
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 15:16:19
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

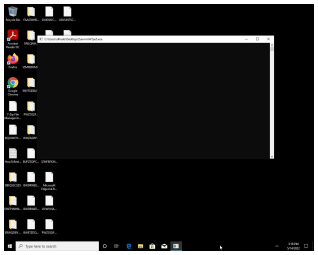
Windows Analysis Report

ZunmmW7pe5.exe

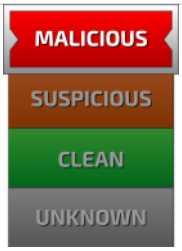
Overview

General Information

Sample Name:	ZunmmW7pe5.exe
Analysis ID:	626600
MD5:	6d87be9212a1a0.
SHA1:	19ce538b2597da..
SHA256:	c2d46d256b8f94..
Infos:	



Detection



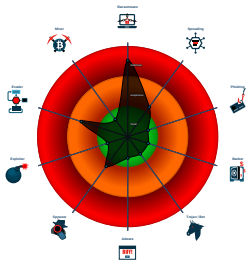
Rook

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Rook Ransomware
- Malicious sample detected (through…
- May disable shadow drive data (use…
- Deletes itself after installation
- Deletes shadow drive data (may be …
- Machine Learning detection for sam…
- Modifies existing user documents (l…
- Yara signature match
- Contains functionality to check if a d…

Classification



Process Tree

- **System is start**
- ZunmmW7pe5.exe (PID: 8072 cmdline: "C:\Users\user\Desktop\ZunmmW7pe5.exe" MD5: 6D87BE9212A1A0E92E58E1ED94C589F9)
  - conhost.exe (PID: 8036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
  - cmd.exe (PID: 7756 cmdline: "C:\Windows\System32\cmd.exe" /c vssadmin.exe delete shadows /all /quiet MD5: 9D59442313565C2E0860B88BF32B2277)
    - conhost.exe (PID: 7980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
    - vssadmin.exe (PID: 8152 cmdline: vssadmin.exe delete shadows /all /quiet MD5: 02A10DBF904883B1F8EE9F3CC70F5EB8)
- **cleanup**

Malware Configuration

Threatname: Rook Ransomware

{
"Ransom Note": "----------Welcome. Again. ----------\r\n[+]Whats Happen?[+]\r\n\r\nYour files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.\r\n\r\nBy the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).\r\n\r\n[+] What guarantees?[+]\r\n\r\nIts just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.\r\n\r\nTo check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of restoring.\r\n\r\nIf you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.\r\n\r\nIf we find that a security vendor or law enforcement agency pretends to be you to negotiate with us, we will directly destroy the private key and no longer provide you with decryption services.\r\n\r\nYou have 3 days to contact us for negotiation. Within 3 days, we will provide a 50% discount. If the discount service is not provided for more than 3 days, the files will be leaked to our onion network. Every more than 3 days will increase the number of leaked files.\r\n\r\nPlease use the company email to contact us, otherwise we will not reply.\r\n\r\n[+] How to get access on website?[+] \r\n\r\nYou have two ways:\r\n\r\n1) [Recommended] Using a TOR browser!\r\n\ta) Download and install TOR browser from this site:https://torproject.org/\n\tb) Open our website:gamol6n6p2p4c3ad7gxmx3ur7wwdwlywebo2azv3vv5qlmjmole2zbyd.onion\r\n\r\n2) Our mail box:\r\n\ta)rook@onionmail.org\r\n\tb)securityRook@onionmail.org\r\n\tc)If the mailbox fails or is taken over, please open Onion Network to check the new mailbox\r\n----------\r\n!!!DANGER!!!\r\nDONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.\r\n!!!!!!!\r\n\r\nAGAIN: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, please should not interfere.\r\n!!!!!!!\r\n\r\nONE MORE TIME: Security vendors and law enforcement agencies, please be aware that attacks on us will make us even stronger.\r\n\r\n!!!!!!!\r\n"
}

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
ZunmmW7pe5.exe	MALWARE_Win_Babuk	Detects Babuk ransomware	ditekSHen	• 0x4c738:$s6: bootsect.bak • 0x4cc30:$s7: Can't open file after killHolder • 0x4cbd0:$s8: Can't OpenProcess • 0x4cd60:$arg4: shares • 0x4cd70:$arg5: paths

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: ZunmmW7pe5.exe PID: 8072	JoeSecurity_Rook	Yara detected Rook Ransomware	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ZunmmW7pe5.exe.7ff7e3710000.0.unpack	MALWARE_Win_Babuk	Detects Babuk ransomware	ditekSHen	• 0x4d338:$s6: bootsect.bak • 0x4d830:$s7: Can't open file after killHolder • 0x4d7d0:$s8: Can't OpenProcess • 0x4d960:$arg4: shares • 0x4d970:$arg5: paths
0.0.ZunmmW7pe5.exe.7ff7e3710000.0.unpack	MALWARE_Win_Babuk	Detects Babuk ransomware	ditekSHen	• 0x4d338:$s6: bootsect.bak • 0x4d830:$s7: Can't open file after killHolder • 0x4d7d0:$s8: Can't OpenProcess • 0x4d960:$arg4: shares • 0x4d970:$arg5: paths

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Spam, unwanted Advertisements and Ransom Demands

Yara detected Rook Ransomware

May disable shadow drive data (uses vssadmin)

Deletes shadow drive data (may be related to ransomware)

Modifies existing user documents (likely ransomware behavior)

System Summary

Malicious sample detected (through community Yara rule)

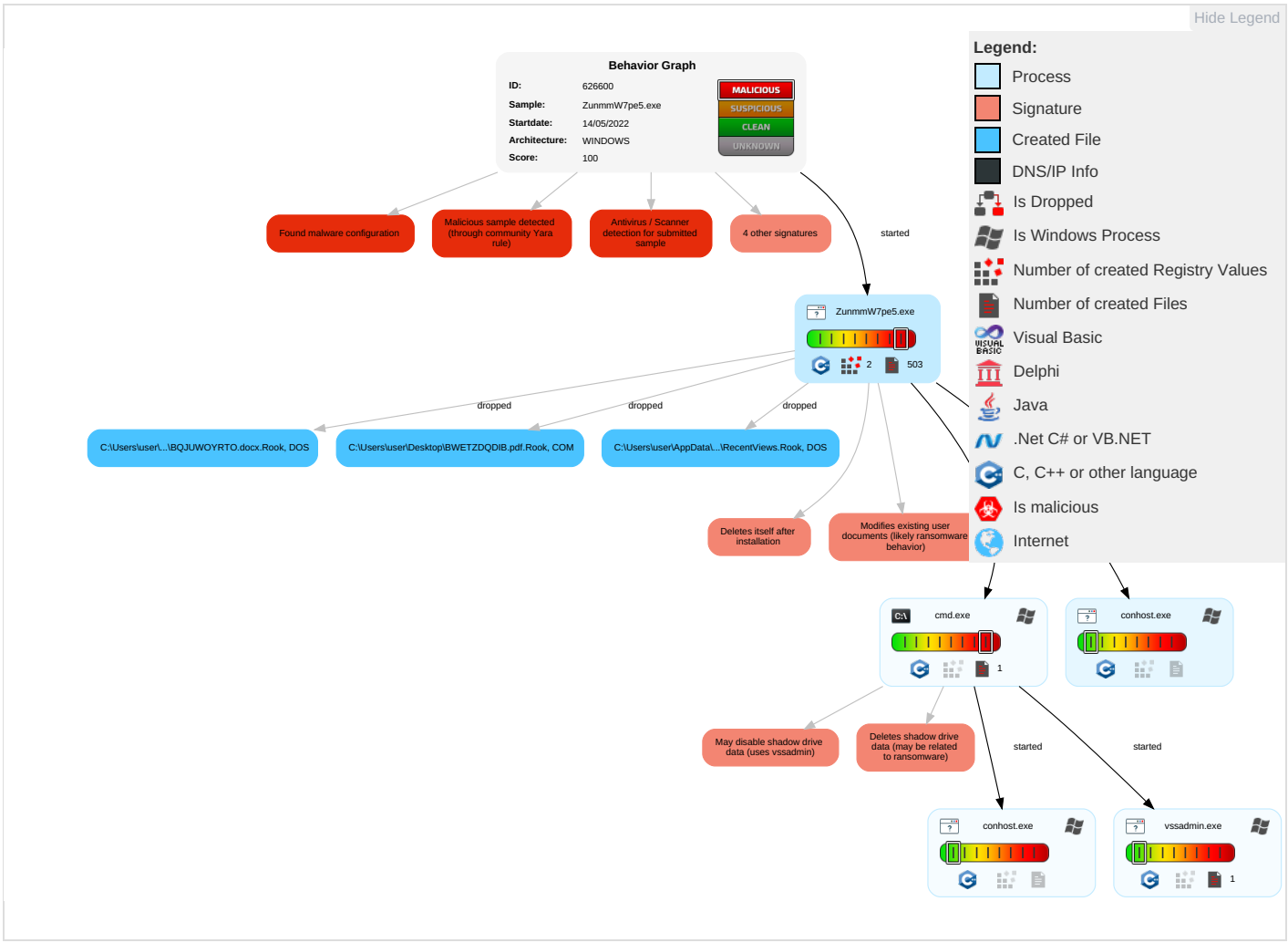
Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	1 Native API	Path Interception	1 1 Process Injection	1 Modify Registry	OS Credential Dumping	1 System Time Discovery	1 Replication Through Removable Media	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Process Injection	LSASS Memory	2 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 1 Peripheral Device Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 File Deletion	LSA Secrets	3 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

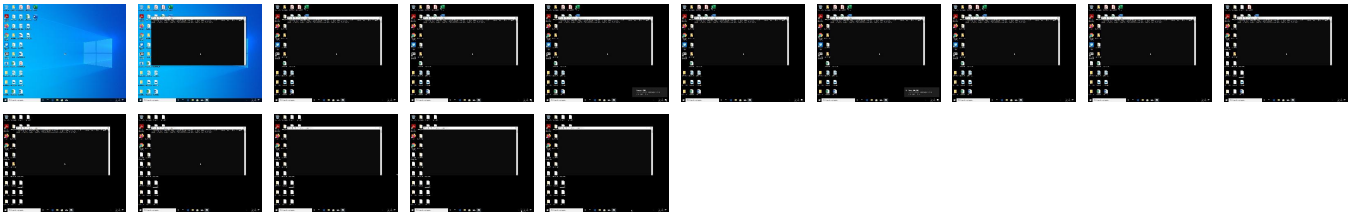
Behavior Graph



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
ZunmmW7pe5.exe	79%	Virustotal		Browse
ZunmmW7pe5.exe	28%	Metadefender		Browse
ZunmmW7pe5.exe	89%	ReversingLabs	Win64.Ransomware.Rook	
ZunmmW7pe5.exe	100%	Avira	HEUR/AGEN.1228742	
ZunmmW7pe5.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.ZunmmW7pe5.exe.7ff7e3710000.0.unpack	100%	Avira	HEUR/AGEN.1228742		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://torproject.org/	ZunmmW7pe5.exe, HowToRestoreYourFiles.txt61.0.dr, HowToRestoreYourFiles.txt77.0.dr, HowToRestoreYourFiles.txt73.0.dr, HowToRestoreYourFiles.txt42.0.dr, HowToRestoreYourFiles.txt114.0.dr, HowToRestoreYourFiles.txt108.0.dr, HowToRestoreYourFiles.txt54.0.dr, HowToRestoreYourFiles.txt95.0.dr, HowToRestoreYourFiles.txt5.0.dr, HowToRestoreYourFiles.txt21.0.dr, HowToRestoreYourFiles.txt102.0.dr, HowToRestoreYourFiles.txt69.0.dr, HowToRestoreYourFiles.txt1.0.dr, HowToRestoreYourFiles.txt30.0.dr, HowToRestoreYourFiles.txt66.0.dr, HowToRestoreYourFiles.txt15.0.dr, HowToRestoreYourFiles.txt111.0.dr, HowToRestoreYourFiles.txt22.0.dr, HowToRestoreYourFiles.txt91.0.dr, HowToRestoreYourFiles.txt34.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626600
Start date and time: 14/05/202215:16:19	2022-05-14 15:16:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZunmmW7pe5.exe
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.winEXE@7/291@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 88.8%) • Quality average: 69% • Quality standard deviation: 32.9%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, RuntimeBroker.exe, ShellExperienceHost.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, VSSVC.exe, svchost.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.21, 92.123.224.60, 92.123.224.68
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, nexusrules.officeapps.live.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Documents and Settings\user\Local Settings\Application Data\Microsoft\CLR_v2.0_32\UsageLogs\howtorestoreyourfiles.txt.Rook (copy)

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Reputation:	low
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Reputation:	low
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\3D Objects\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe

File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\ARM\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\ARM\S\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\ARM\{291AA914-A987-4CE9-BD63-AC0A92D435E5}\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500

Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZfzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt21.lst.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	PGP\011Secret Sub-key -
Category:	dropped
Size (bytes):	3624
Entropy (8bit):	7.858548964543015
Encrypted:	false
SSDEEP:	96:buTuG0M3LkSo47Ko4/AAUn5U50+NS43LPuLjv:buTuG0M3LkSgoiM5U50B43LPun
MD5:	524136C47461F448ECA116B8BA9BF4D9
SHA1:	DB4A33F5763BA0964F04D6A6DCF8EEBEEF202432
SHA-256:	F55D36EEE0465C29D618B81552CC0DE5A1DE5BA6E0D172C29B8AED5D81FF8B20
SHA-512:	70BA5CC351B911C0BD94195E24C8D8A39607E0EAC4BB3C99BF45D91BE9E4CDB69B48CEB662FDB867EF6DF88B03503771D6A28BAB242267DEBD4A599211366535
Malicious:	false
Preview:	.....O.H.A(.l.?. 1.16.%Locale:0x..v..6.....=.Handler:Director.sg..j..a...`.`e:CMap.CMapName:k....+..Dz.D.V..try:Adobe.Orderi\e.....I..<....ineFileName:C:\P].^.-.......".6)\Adobe\Acrobat9&.`nd:..+.Q.SMrce\CMap\Identit...7*.'.6.4.,Z228.FileModTime:^.!.%..FW...^..ont..%BeginFont.........6.o.'~.0yHandler.FontTyp.*.E.#TH..|.#...Identity-V.Regis.As..U.......|L^ng:Identity.UseC..X...Vk...:..i.utlineFileName:C5....)..K9....(x86)\Adobe\Acrou.bd...?....L...source\CMap\Iden.r..A....Vs`...h:2761.FileModTi.UR.\.a..h.. .58.ndFont..%BeginFo...gW.:/..%R....toryHandler.Font.#F.+f..W.vvW..me:Identity-H.Rey...e...4x.....ering:Identity.O.....o....h....:\Program Files a.=X.>L0h7.k..fbat Reader DC\Re.+..(..3.;.....^tity-H.FileLengts..v..x.^..a.4;me:1426606452.%E....Y.q.>4^..nt.Handler:Direc.>..8!.7.~.j.~.Type:CMap.CMapNaT.j.!...^.....gistry:Adobe.Ord...U.d..R. B.h.7.seCMap:Identity-...E.........{e:C:\Program FilB.7....{...\P.crobat Reader DC%...HP..F..)/.dentity-V.FileLe.+..j=.%

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt21.lst.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	103272
Entropy (8bit):	7.248282755289467
Encrypted:	false
SSDEEP:	3072:YPoEk4YF/bSAky+4VqE0aiOmIEfXprtkakykXXFq0o7GI:YPob/p+xENiOmIEfXprtkaky8XFboaI
MD5:	DC452B0FAC7EA25177C6041944989CDD
SHA1:	69EBF17FFD565AA62F086F76ABC28F93B720D07F
SHA-256:	FFCDC603DAEDF772A54F00FDE883FC26039FE1D0530777482CC2BDFDA19C2A02
SHA-512:	6F94A8C5DBDF2281CA424438A7C82A4E30323CDCAC48625333929ADB95796BF0C8302EF44CC946CB1ECBEFA2667314BDC35D0845F38D02663D3007DD35775E0
Malicious:	false
Preview:	u..}q...9....fv 1.16.%Locale:0x.@...^]..k.q/g.:Handler:WinTTHan.(.h?."....@ZueType.FontName:..;...S..m.....me:Marlett.Style1I..T....y.6...wuName:Marlett.St0...Q.3.Q..~V.. .Class:500.WidthCQ..w<..#b.P..Ibts:0.FullName:Mar..IY.Zc.....2.T%pt:Roman.WinName...G.....~`/E.qgth:27724.NameAr;.Yd.Q:.Fx..}.(Gett.NameArray:0,?.=.C.m.l/...A.m eArray:0,Win,1,.p.ms....".+....%BeginFont.Han.....<..n..v.\.r.FontType:TrueTq.~.....c.].f7alMT.FamilyName:...#.=.....sH.Regular.MenuNames.E.uy..{"....@H:0.WeightClass: 4.0-'.4-..R....AngleClass:0.FulU.._...d..3...%.ingScript:Roman.^.....T.B..g3..leLength:1036584tr$...B. ...W_,1,Arial.NameArrJ2..7...xtk.z..NameArray:0,Win.M...Ve..b..SG.t ..%BeginFont.Ha..H...u....}v.er.FontType:True..p.....M..,.(.ial-BoldMT.Famil...4.P.....&+.feName:Bold.MenuN.9K.@.W..1h..5h.its:2.WeightClasw...m..e.D.....:5.AngleClass:0 ....5...ex.o....old.WritingScrip.k:.{.G..\...NArial Bold.FileLf..^8B]....q..l.eArray:0,Win,1,A.3=F.*..;.5..u.,Mac,4,Arial Bol.....6

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt21.lst.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	12152
Entropy (8bit):	7.491876770035443
Encrypted:	false

SSDEEP:	192:02ffJNRlIRg7EeyZ4JbT8eBpBTJJ5PQCe1TBLuW6da35ZCpmlWNdOxewoiM5U50p:02XJNjPXMevPJ5YH1TBKW6CZCpRTJO3C
MD5:	F8BD16339FA33D903066A363C067D27B
SHA1:	84D8C68DDB78EF71466CF2A3E3023453C81B16D2
SHA-256:	1C146135FC08657505233FD058DFA34F6F826F99F17C766E90CB24AF750E0760
SHA-512:	1DAB38C394008C74355AC5668B279C0DF5822D6479E69C6374F6D6DEE19B080F75A04DB607F9FD1F123D0F3F3D6A6E84E653413CDF41C36F002787C7760CBAF
Malicious:	false
Preview:	...~.....~.$..C 1.16.%Locale:0x....,..vZRy5@h9.Handler:Director..P..|)iQ....(.Be:CMap.CMapName:..Z.....p\_..stry:Adobe.OrderiD.GN....h....%.ineFileName:C:\P.:.....K..j... {..6)\Adobe\Acrobat.....j{..'"..b..rce\CMap\Identit...4.....e..-.228.FileModTime:.@.....#\....ont..%BeginFont.....<..gY.!..pyHandler.FontTyp..pKj.&6.....QIdentity-V.Regisa. .0....:F....ng:Identity.UseC...m..j....- ..utlineFileName:C..Y..0..5.7D.3.B(x86)\Adobe\Acro..i.B..^.....t..source\CMap\Iden....G..^...U...>h:2761.FileModTi.K..8..E'Q..z.. .ndFont..%BeginFo..{=@..@.0..7..toryHandler.Fonto\..z..2 .n..(.same:AdobePiStd.F..". ._.V..+5B.Pi Std.StyleName... =c-.j....e:Adobe Pi Std.M..q,...].3z.= Std.StyleBits:0. X..A...{.,.b..oman.OutlineFile}..b.v?t..(.(..hFiles (x86)\Adob..Cp..'~!....{<. DC\Resource\Fon6L..X:...$..pm..DataFormat:sfntKK...M.:F".1.m{!dEncoding:yes.is.....gb..s.% ..th:85552.FileModH...$G.m8.....OWeightClass:400.....9E3..X.;.leClass:0.Designr.SS.!..)o...)ay:0,Mac,4,Adobe..K[....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	315496
Entropy (8bit):	5.5998530440528835
Encrypted:	false
SSDEEP:	1536:amGS52KTac07W9SdQ/CvaTrdnDHAONhsUvr0fEpRXTJ7Tz/y23y0s+yKe:qakUvQEpd5TH3y0s+yx
MD5:	0EA226A6D268E527C14C8B7261900458
SHA1:	72D361D45E519482B25225C8378A6C6B4FC28FC4

SHA-256:	15A97E85612BF50D0CCDE77D7AE5A80FB8FE30F06744815A061A9E90F904155B
SHA-512:	9074DFCFD350D822300848AA437BB38A896E81D38992AB8EE30C5AF2D98FA37B4420F19AFB62048B3E92E9AF86591FEA39620BEE0ECFDC9B4ECB72C68A79300A
Malicious:	false
Preview:	"S.b..E}C .....ader DC (32-bit)i+..J....5.....A12_SelectObject....A."...DY...X.....g.....b.....g.....b.....g.....b.....g.....b....~~~@~~~ .....g.....b.....g.....b.....g.....b....~~~.~~~.~~~.....g.....b.....g.....b.....g.....b....~~~.~~~.~~~.~~~.gP...1"".....'.....g.....b.....g.....b....~~~.~~~.~~~.~~~.~~~.~~~GGA..5>i.j8../6.....g.....b.....g.....b....~~~.~~~.~~~.~~~.~~~.;.6M...P<.m.N5.....g.....b.....g.....b....~~~.~~~.~~~.~~~..M...xl..{.q..>0.....g.....b.....g.....b....~~~.~~~.~~~.~~~m...'.6.d....p.".~~~.....g.....b.....g.....b....~~~.~~~.~~~.~~~m...'.6.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5lJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5lJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\TESTING.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	2600
Entropy (8bit):	7.915296420723999
Encrypted:	false
SSDEEP:	48:2L4NykCxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:2L4Nyp7Ko4/AAUn5U50+NS43LPuLjv
MD5:	A57E57E3C2239A0C522601122E5EE727
SHA1:	B881D07CFCA064F12B4FCB9F8909CE19CA332F4A
SHA-256:	52736B5F60165A324C17BBE5F2E9AB997EAC7E98AA58AEB9B03E5A794587753B
SHA-512:	DFC6EE42EFBD727F001B09C5AB266D198D49180DD2B24590DD075A7B821C274893FB400211D5EFE8474EAA5F2BD626FC30E76E913C594C025E18375E3759FF2
Malicious:	false

Preview:	.%&`".C.].R~.....W....Eb..E.....#.... ..6....rS{.....?V...`.$..@.c..h..<....O...d.....L[j=.H...../..s...f..E.%.n.....5....%.99u.....#.p."#..H.b)..t.....#..'Z.l^....k$l.1...Z .H....V./<..*3wc./..d.mXw.W.&DV..E... ...?mC.tC.n.3.r..^...j..K..../.S.V.q.%.a....7.~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10l....e.....x...U.../.8.c..].-+.+.F.!...A.6...3|;e..c...M ....st{A...G^...B.TU.[L.....N.....{{.y.q...sz%^?..{]G>..F..>r.il.4.....2. ...0q..Z-..I_..4L....^...."X([P..OD....}.P.....Bq..Ls.-....=...x..::x.....g...81ew.4.....3.....},,..|^.%.3...\s...jC. .n6.....)C)f.5....r.K2.7.W....D..`.."W.. .U.3/ep..F...?.{..HDe.R\v..KK.7*.K5P...._B.F.wC.%..... .z).y0GTk.t.....F_..A.J.....7....E.....c5..x5aI.....b..1..N.....G..+u...*S/Z[SIR?..G ....._..o..k'.d,. (....O...`..)...N.<.c..'1.Hu$d...6[..9v9.OQr..q.....|....~....7.u..\.BZ.M.o..,...9...[N..~.E.....G.E.$...c....P}.....'#....._...j).....o..B.V...d

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5lJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	2728
Entropy (8bit):	7.919274006579648
Encrypted:	false
SSDEEP:	48:Vb974u/oPaCxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:v74gY7Ko4/AAUn5U50+NS43LPuLjv
MD5:	59FD9542CB701828F487E0F1BE570D5F
SHA1:	AAF88BCC4FCE9BEE570CC4A8CDC488CC553518A8
SHA-256:	38B6F6CF277C9646E0B5ED558AD196230F1A6FE4284D9F155DC3061424986077
SHA-512:	3C8F2E396580BA7E2CF08A61B34843E1ED35DD637BDD0525ED163F6A66743820D58596E093A5C21B94DEDFC0A99634A247450940AEEC042CF9236438DF43058
Malicious:	false
Preview:	.WS.....a8u&%.PESTING","info":{.]W.....R.N...."TESTING"},"mime..-.....}.a.)...ze":4,"ts":16231.....&.:.@fo":{"Version":".Q...$?..X-5.....#.6..I...G.....y6...0....I..2 !..p.G9.12j...\,....i..M+]!..Yn..U$d....0|...P.[<.....|&.4.t.C/.....]..4.../..@ C.W.v.l.@.....C4.VV&.. ..1.eE.!z4..^w.,..-....h..K....Z.@.. .cg..R..[..k.....d*.T..K./.F.F\ .h.>,.!5o.. _(5....B.Z....t.....~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10l....e.....x...U.../.8.c..].-+.+.F.!...A.6...3|;e..c...M....st{A...G^...B.TU.[L.....N.....{{.y.q...sz%^?..{]G>..F..>r.il.4. ....2. ...0q..Z-..I_..4L....^...."X([P..OD....}.P.....Bq..Ls.-....=...x..::x.....g...81ew.4.....3.....},,..|^.%.3...\s...jC..n6.....)C)f.5....r.K2.7.W....D..`.."W.. .U.3/ep..F...?.{..HDe.R\v. .KK.7*.K5P...._B.F.wC.%..... .z).y0GTk.t.....F_..A.J.....7....E.....c5..x5aI.....b..1..N.....G..+u...*S/Z[SIR?..G....._..o..k'.d,. (....O...`..)...N.<.c..

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SharedDataEvents.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	14872
Entropy (8bit):	4.860663064397955
Encrypted:	false
SSDEEP:	96:Nj3kfnKaWxRw7U3Oqv7Ko4/AAUn5U50+NS43LPuLjv:Nj35aWx+7gOquoiM5U50B43LPun
MD5:	40280AE29CCD2955847ED110868BA68A
SHA1:	795897E8891BEDAE4DE904727E57F5158FB5C1A3
SHA-256:	0EC7AF79008CB7C15DA5CD2D9A275E924BBA3BB4DA234BBAEB0AF91971BDBAC3
SHA-512:	E79250A034B8B62E086E2B55D41D8455BC3C120692FC6182CE90A6E52E68227E6AF6A473DD58A503FB139A1CD5C0CC02049D6F54DEF118B496A20E8CE08FD5 D
Malicious:	false
Preview:	h?...T.$Z[r....[.....@ .....\w..p...../jgAF.....)6.n.....90.....y..CoS...a..$.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n..... .90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n..... .....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n... .....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n.....90.....)6.n..... .)6.n.....90.....)6.n....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\ToolsSearchCacheRdr\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	42984
Entropy (8bit):	7.313426658250603
Encrypted:	false
SSDEEP:	768:k6IBxfZWn3/PLZkQrrIBtKHyAV/C+gioe:k6ihZWnXTrwtKSANC7e
MD5:	6A37309E354D08FABBD692670358C633
SHA1:	65EFE9E2921073258BBA96569E861650A9227E3C
SHA-256:	6D88AE87F284A96B420E266D56CEB0C4A363AA6F2E434B54E5E42D57DE0E50F5
SHA-512:	35E4F58908E8809CFC83DC18EF25B459332CDE50250FF68DCA543C80338D8ACC135A6351C09EB3920D4943AC232CB7DB20495B4807AFA7F1DFE3DDEF8AA0E3 17
Malicious:	false
Preview:	..q%ZQh.i_j9ZM.0:.....:F:Aria..O.....m.Narrow.L:$.....fj.F.ol..B....."F:Arial Nar....z.O.h...'..o:.....:F:Ari.....Fw..V.0...P:Arial Narrow Io.iD...p...&[v.....J .wF.K{&.)*.ow.#.103.FID.2:o.$..}.I...4Bc.INarrow-Bold.P:A1.!....[n.w...$..L:%.....!...:Arial Narrow.#...=i:.6.....1.~....:F:ArialNarr...,...k.....;Arial Narrow Bol.....qVv...: 8.....#2.E..(%...arrow.#.75.FID.2..5#..._...-'..ialMT.P:Arial.L:.._*.I.....?.$....."F:Ar.~.h.(O....oi-.f:.....:F:Aria:.2.yu...&._y.al Italic.L:$...'.b<K...h.(]....."F:Ar ial.x.b`...{.j..l.r.....:F:Arial-Bo.H*..v..zL.....d.L:$.....Y....j...o..^.=.F:Arial.#.98.FID=..i..1..hs_.Arial-BoldItalicS..NJ...B..~vor.Italic.L:$.....c..[S...g.{.O...."F:Arial.#.9^^.vY..... ..&...:F:Arial-Black.....?a..>.B..:-.....rB....w`t..9..S.rial Black.#.103/.A..q.%....?...:F:Bahnschrift.H.s..<.4jB.0RQ|.ght.L:&.....F.....7.+..g.."F:Bahnschrift [...-gP.

C:\Users\user\AppData\Local\Adobe\Acrobat\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\Color\ACECache11.lst.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data

Category:	dropped
Size (bytes):	3192
Entropy (8bit):	7.773423683959449
Encrypted:	false
SSDEEP:	96:cAufnd1P9K7Ko4/AAUn5U50+NS43LPuLjv:Cfd1P9xoiM5U50B43LPun
MD5:	1B794924D1DD881266AD571BAA53C296
SHA1:	78701080E25502DAFC6FBC341B182EAC7A029AC3
SHA-256:	71EB7B55938137E9625534335A06FEF2C0158DA28C31F179A9DDAB484B9AC45F
SHA-512:	90962112ADF9B7F07C4C7682E3729B077904E02409596CBC2D57F1BDC6A4537517249936149688A3CF9560018DA384920527732223E6385F85124694097A4584
Malicious:	false
Preview:	.0?.....Ga.h. ..j..doog.....1C:..e.,...&?n.Y..2\spool\drivers\.J.@z.a....gH.....,.....m.bAS.....@.YMC baLsffo.....T...i.@*..J..{.esc.....Agfa .~\r".~..)4....:.....>.b C..*.w,.2[m.....>.bC..*.w,.2[m.....Q@g...}..l.D0..... .:..`=~....Xdoog.....DC:\Win...2Yu\...\.}(.ool\drivers\coloK3....}...eB7.ce Profile.icm..1...!.0r?G..t9... .....rtnm B..v.]...s..r..N..1...TFSMl...deT..]`*.\3.{..K.EC61966-2.1.....%+..-%...R.D...1966-2.1.....>.bC..*.w,.2[m.....*...'.....?.$..W*....dZ....H..... .V.....\.2..Z:.u.nz..65uaw.....u.j....5X.U...W.4...i.l.b....._..[i. .C=...D."...v.}..@E..COn(.A...4....>&P).A.-.i+.rd..6..R..6.w.\?". .Q.P..N...@NaI.;I.....?./..@..q.rp..G....r... .$..?....T...-+.b.....\.yJ...!...?../M.}z.r..%....k.(.._V&.....~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10I....e.....x...U.../.8.c..].-+.+.F.!...A.6...3|;e..c.

C:\Users\user\AppData\Local\Adobe\Color\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\Color\Profiles\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Adobe\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false

SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Comms\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Comms\UnistoreDB\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Comms\UnistoreDB\USS.jcp.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	10776
Entropy (8bit):	5.035506064356338
Encrypted:	false
SSDEEP:	96:Wg+gg+xMywZ7Ko4/AAUn5U50+NS43LPuLjv:v+h+i6oiM5U50B43LPun
MD5:	7B3C45555D21132929AD44A8EF58D6B8
SHA1:	002C80D0D54B275799662D40F63CD978EE8CCAE8

SHA-256:	E35B85831F317CFABDDB8EA1970BBD34013C612F52B24AF0059231532F5F457B
SHA-512:	D155DCE07E3AC960EF3E463C760725E71B6053E0488E424166DA73D62ED5CF737DFE4E3A885A59CB3DCBB80972C37E8926946587667FB1B76ED610B478BD787 4
Malicious:	false
Preview:	[..r...X...(<.....MNU5....y.....C.D....$rUGC:\Users\user.s..f.....x.\.omms\UnistoreDB\....C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....C. D....$rUG.....C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....C:\Users\al....h..... .k9m\|cal\Comms\Unisto.C?...oF9.~X.....C.D....$rUG.... .....C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....R/*...:F.7..z.....C.D....$ rUG.....E.\!.....>.s.....C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....C.D....$rUG..... C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....C.D....$rUG.....C.D.

C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00001.jrs.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	3148312
Entropy (8bit):	1.7938862729105274
Encrypted:	false
SSDEEP:	48:EcviGCxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:Ees7Ko4/AAUn5U50+NS43LPuLjv
MD5:	9D114D4C08E13FDA7E02630FA290E927
SHA1:	8F8ADD9927C2D2D4CECBF1FEE34EC6089B65DC04
SHA-256:	B615478E617EF11644D347FC2E73E9495A61A52EC107C6E2BB31D54665AD92DD
SHA-512:	3150C079D089450A96F9D90416DBF18B5A5A44EF5673763AEB0360A1B8EF32B98C89B8A2C7D72A9372307BFFE3D1B0D4EAF67C083C29E0F329EE41034AD7948 A
Malicious:	false
Preview:	.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g..... .....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g..... 0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....0.g..... .....0.g.....0.g.....0.g.....0.g.....0.g.....0.g.....

C:\Users\user\AppData\Local\Comms\UnistoreDB\USSres00002.jrs.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	3148312
Entropy (8bit):	1.7939047759740043
Encrypted:	false
SSDEEP:	48:z+TBR1bCxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:idR1y7Ko4/AAUn5U50+NS43LPuLjv
MD5:	1825BF691F69DD82164A3A13E00B66E6
SHA1:	239665FA7E28270254FF3B99C1DC6366183394A7
SHA-256:	055CC13AA6AEF835F1F0C3BC257BD69F5CA3BC93740B66FA7AA3E07CD4A9FB16
SHA-512:	02E152206765E5F2689EB3EEF8EA93ECB974D095206E1DDF57217FCC8225452F4F5A5D052F1377C6265BE271260ABFCEBCC11D9C5FF42589AC9D5342DEEC1B 8
Malicious:	false
Preview:	..XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV.. .]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0` ..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~... .....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~.....XV...]..0`..~..... .....XV...]..0`..~.....XV...]..0`..~.....XV...]

C:\Users\user\AppData\Local\Comms\UnistoreDB\USStmp.jtx.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	3148312
Entropy (8bit):	1.8249947086115008
Encrypted:	false
SSDEEP:	48:hccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccf:tcG7Ko4/AAUn5U50+NS43LPuLjv
MD5:	9B305A76846F1896F42941FD38DE1F4E
SHA1:	D0FD364C09D3EB83B1C020F37192FDB72564FFE1
SHA-256:	EA26A33D765C0893E458F31B56AD4246955532C0D5F4F7AEBA4AFE901F934281
SHA-512:	BFE4E6F8B864481CE6E5FC9D9AE980F623FC2589B9495FCB00DC842A5C427E5393F99F8802F48604E1E7E576113BB5DB1AB2E38BF9287C07088771D0FDED96D 4
Malicious:	false

Preview:	j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y... ....j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g... (..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y............ ......j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g...(..y..................j..b.g..

C:\Users\user\AppData\Local\Comms\Unistore\HowToRestoreYourFiles.txt	
Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	-----------Welcome. Again. --------------------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Comms\Unistore\data\AggregateCache.uca.Rook	
Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	2600
Entropy (8bit):	7.917119827967215
Encrypted:	false
SSDEEP:	48:XrkCxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:Xrp7Ko4/AAUn5U50+NS43LPuLjv
MD5:	DDC69C49A4CC61AF79BE4E3E22139588
SHA1:	1FFA68AE78088E53A52DD97DDF899A1A1A4536B8
SHA-256:	66609A678DE4466CA7C70DA8A4DFE951E6A8A75FF52A8493765976A6821C5F1F
SHA-512:	F045624568BC18F4A7426418B33B9B424FE5AA7EF9DBE964A5621E3A5E4016B8212220476BD501C5ACB9FCD28C31DAE06BA2652AA7878C574EB1372F4CA383D 7
Malicious:	false
Preview:	....?.....L................................;..7.........W>ak.....A...W.H $..3.D[e.Q.%......oukQ-...{..s.S.a.&{n]..e..y...8&.RF..\|.+G.A.MZ....q....#......5..S.'.:x..... ....m3..F.z.$.8...s.Y......A!Q. ...u.+...~.......w.D....W./...........F...}=(.i..4.*c..$.<.^...8..!I... !...X.~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{........j10I....e.....x...U.../.8.c..].-+.+.F.!...A.6...3\|;e..c...M....st{A...G^...B.TU. [L........N......{{.y.q...sz%^?..{]G>..F..>r.il.4.....2. ...0q..Z-..I_..4L....^...."X([P..OD....}.P......Bq..Ls.-....=...x..:x.......g...81ew.4.......3......}.,..\|^.%.3...\s...jC..n6.........)C)f.5....r.K 2.7.W....D..`.."W.. .U.3/ep..F...?.{..HDe.R\v..KK.7*.K5P...._B.F.wC.%..... .z).y0GTk.t........F_..A.J.....7....E......c5..x5aI.....b..1..N.......G..+u...*S/Z[SIR?..G....._..o..k'.d,. (....O. ..`..)...N.<.c..'1.Hu$d...6[..9v9.OQr..q.....|....~....7.u..\.BZ.M.o..,...9...[N..~.E.....G.E.$...c....P}........'#....._...j).....o..B.V...d

C:\Users\user\AppData\Local\Comms\Unistore\data\HowToRestoreYourFiles.txt	
Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	-----------Welcome. Again. --------------------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\ConnectedDevicesPlatform\CDPGlobalSettings.cdp.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	6808
Entropy (8bit):	7.4818250079373065
Encrypted:	false
SSDEEP:	192:gnkswNCe8lCGeiH3IAmpd5VZwjeoiM5U50B43LPun:gIM70IXINv5gTJO3LPG
MD5:	E1D5EDA0A269B1F98A03FB24A6A3C442
SHA1:	9319E42B74EE6EED212E1504D0E98CF5FEEB479F
SHA-256:	9C1C4EDF9D94E8F7D23C3D2E0D7D2EDA15E87AEE4FDED5428F4B3746691B438A
SHA-512:	125983E9C44F7614D8296DA0A16AF820DB076F5A2BFF30796D23E6A158C5683A8EFAC1766DAD98A206C62B4B9B0EE17FB5DC2A2157DAB49DE43DDB96DA3CB AC0
Malicious:	false
Preview:	.}..B.].+.....ronment" : 0,. V.1Bf...4....>P.ps://activity.wi.. ..9m5#....A.VAccountSettings".L{...P....d.ityStoreInfo" : ..3Z.?...3.o..- "active" : tr.VBn.T...h..t.g.tivityStoreId" :...? Yw..N.V.G..;16A3-B512-7562E0.]..fb.....N "stableUserId".u.8m..).....7. }.],. bd....e8.*vU.M. : "undefined",.H(.@..}.....W..ttings" : {. g.....G^,..]<.. : 0,. "Clo..{.a.. 6..x..6= "PublishUserA..FC*...n.1d.... "UploadUserAo...U....~i#:.+},. "AfsConnec'.q.D..i....#.(. true,. "AfsPo..#.J...#.M...WaitMs" : 10000,.....5..g.&..Y.uencyMs" : 86400 &..&.~U.....ication.Environm....Eh..g..I.O.uetoothTransport..@..]..29.uT... "BluetoothTr.,.....>lowed" : true,. +.....O.6.." : "/api/v1",. a'..X....k|.j.s2verName" : "rome.... .....`...m",. "CcsPolli.@..gRE.j!..3..se,. "CcsPolli/.k..3.....y. "CcsSeenRequ.(.+.UoDyZ..cY% "CcsSeenRequest%.-..V".T..2.g.#me" : "0000-00-0.er...6=O?.....Y. "Cloud.SessiM.F..g.U.:.v]l.ervalSecs" : 360-...{...

C:\Users\user\AppData\Local\ConnectedDevicesPlatform\Connected Devices Platform certificates.sst.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	3240
Entropy (8bit):	7.869523026263373
Encrypted:	false
SSDEEP:	96:NLsrw7FMW4T7Ko4/AAUn5U50+NS43LPuLjv:NLsPW4ioiM5U50B43LPun
MD5:	BD1BEB14DE09694607086CE6BF037D55
SHA1:	6831FD562379842FECC7D2BA7ED681A90DC7355E
SHA-256:	C9CE3952273A33DF7E787F5BF4A5CD3AA011D6B8D4E086D2EA0E9352977BC4A1
SHA-512:	5F1C2FEBD3D7AD1F8EB08D7BBD2DA97DACA92F1475E47C9417F5CAEFCBA1B7E6F6EA5E06DBBA38455F4A9728DD80051B44D0D7C19B3414583924DA2D22295 F99
Malicious:	false
Preview:	4....k...vM2.'.....21Y...wIQ.K.9..M.i.c.r.o.s.o.f..<.g.5E.a.q.E...t.e.d. .D.e.v.i.p.F...../.iff.o.r.m. .d.e.v.!.x....l;X..).i.f.i.c.a.t.e...k>..25&..8:ZEM.Gt. .S.o.f.t.w.a.e7.. .D.a.@..%K.`t.o.r.a.g.e. .P...A.{,"Ru(."... .....0...sz.3^..%k...S.C.MGDM5..#0...*`.....r.3.....I'...7Microsoft Co{.....j..w+.....Platform device ~......7F..e.20514221658Z..2 1.....i...g,..c.@0>..U...7Microsx.?Qe.v...[Uy...vices Platform d...\...p<...0.e0Y0...*.H.=....4.....@.qUr....sq...SA..z.X.SK.Z..II.w<.4..g.!.4...e..''T.@.Sh..C9..../T.*...*.H.=.. ..G.0D. 4.....*.!I]$..4..J)'....6)....\..4..d.Ytt...z.4...YK.V....x.f.b[.. /..=.`.....V.?.....Y..,A.u..[P.j`s.d....F1% ...]H.T...+.TG;..2....>.3WI.e.....U..H.a.I..Q.o.....%.? .e.....s.[.QK.....6<t..'~^.....+.V.r:p...=*>9.(.jY.....d.sL.....Vj$...'.T..S.Y....y.....\.v2.-R.,.9.3u7.vI.4}.Eb. .?..Y....8b&hgj..H..~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10I....e. ..

C:\Users\user\AppData\Local\ConnectedDevicesPlatform\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\ConnectedDevicesPlatform\L.user.cdp.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	3544
Entropy (8bit):	7.84390677273578
Encrypted:	false
SSDEEP:	96:9fcoxu1hDT7Ko4/AAUn5U50+NS43LPuLjv:eoxloiM5U50B43LPun
MD5:	8911050C45CAC22B475104DDC916AEFC
SHA1:	39B417425EEE6EACE202F09D2EC75DF690EB85A3
SHA-256:	4450C1E96EEE3B344DBFE9A3FC2C119F73A610B81F27A9CCEDE3CF8D95337DF4
SHA-512:	3B8218EEB40D6D7EBF961427167739402E5E0C8EAE95245DC5E48164A72CFBB2C76D78531C3C4EE6266E2667C70A1B38AFE38B90DE7E3E5EE4C29BFFE02DF105
Malicious:	false
Preview:	...{?.v.d.&.3"..baseSettings" : d.. .@..Q....8.%eInstanceId" : 0.Z....pFS..c..S.ated" : "2021-06.$1.Z.Iu..I....". },. "AfsA... .....~.-..E.[],. "AfsChann...Z\N.U.;D".6D"AfsEnvironment"..=..5.v..%|g.bscriptionId" : >.....RaQ...}..riptionUpdateTim...SU*h.....R.T00:00:00.000",.t.$....9j.....edInfoHash" : "".a...m..%.S4..ationUri" : "",._.....r....}ionUriExpiration.K...a.....d..-00T00:00:00.000..&&+."....L.cationUriLastSyn.\...:..@.v..)d00T00:00:00.000"...?j..0X...w..ationExpiryTickCm...../.....K81680,. "Devic.f.H.>....jrmatVersion" : 1m.....{..a.1teredNotificatiov>V...'.....XV.LastRegisteredNo.<.7.. ..i.a.np.irationTime" : ".??9.....MM.....:00.000",. "La.JN..7..?...."0000-00-00T00:0.Y....EA...:..ogicalDeviceId" ?...0.\..;..T...taEncryptionKeyRW..v....rO.[..e.0000-00-00T00:00....]%.....o...gisteredInfoHash/.vG...TN....lsteredWithStrongt.....N5D...J.T "StableUserId"..7.l]?~.....g.....m..g.h.....t...

C:\Users\user\AppData\Local\ConnectedDevicesPlatform\L.user.cdpresource.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	2648
Entropy (8bit):	7.910962549011603
Encrypted:	false
SSDEEP:	48:sZIpCxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:sZb7Ko4/AAUn5U50+NS43LPuLjv
MD5:	233790AFC4079116C25F720414D8ADA2
SHA1:	5FB6C6114FB6D0399E165A830FA807651D10AA32
SHA-256:	23B7A6C32DF9D6D3FC456365EFB324CD3A9ECF2913772BE857E1560573EC5991
SHA-512:	9E6047AF5EEB648C924D8CC5BF597BECAFF37A9FE86C931EC8CDCD194AE79A05031D91ABD4608680FC3E925A98CCF38FBE2C5B76C1B95C081D6A8F31C68BFA2
Malicious:	false
Preview:	....O.$.z..'.Ctions" : [],. 3.~.^.s,..z.Q*\|=: 0.}.....6.....N{T...P...Bz.e\. ..sK.A.....ty..w..j..B.?.<..=..}.~.P%..5.#.> ll.....P^U._to.....#&$....._r..L.:..X.x..._.TG5[.3..@..r2l.cBA*...%\.....7"..h...6F.gE..o.....ESg.....T@N.....I.v..~....r.fo6...#j..{.|...c...^X..#k..V.t.Z.W(},O.<P.YH..~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10l....e.....x..U.../.8.c..].-+.+.F.!...A.6...3|;e..c...M....st{A...G^...B.TU.[L.....N.....{{.y.q...sz%^?..{]G>..F..>r.il.4.....2. ...0q..Z-..l_..4L....^...."X([P..OD....}.P.....Bq..Ls.-....=...x...:x.....g...81ew.4.....3.....}.,..|^.%.3...\s...jC..n6.....)C)f.5....r.K2.7.W....D..`.."W.. .U.3/ep..F...?.{..HDe.R\v..KK.7*.K5P...._B.F.wC.%..... .z).y0GTk.t.....F_..A.J.....7....E.....c5..x5aI.....b..1..N.....G..+u...*S/Z[SIR?..G...._..o..k'.d,. (....O...`..)...N.<.c..'1.Hu$d...6[..9v9.OQr..q.....\....~....7.u..\.BZ.M.o..,...9...[N..~.E.....G.E.$.

C:\Users\user\AppData\Local\ConnectedDevicesPlatform\L.user\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of restoring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped

Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\howtorestoreyourfiles.txt.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	5096
Entropy (8bit):	7.673584831254344
Encrypted:	false

SSDEEP:	96:fisg+o7ljHFe8W0r8KKo2pr65a9Ypg67Ko4/AAUn5U50+NS43LPuLjv:GFe8W0r8KKo+8NghoiM5U50B43LPun
MD5:	3EABF51E8670170127E92745ADA00301
SHA1:	36DD155F87C2793CE9E39496688B63A13AC0FFFB
SHA-256:	60251F55058DD1CB6C90F9897FCC42726C57C8AF73CB822770D480B3BD49E501
SHA-512:	3C032920FB707CBBBDB8D2ADE511C3C851CFCB9687EFD51029DBB32B6A90E2C908BC0516C3764DDA5B4F42432DC5F95D215978FFDAFAF1557875E8414DD0AAA
Malicious:	false
Preview:	_:.l...'.l(..K.me. Again. -----.L.,J$...X.C.s.@.[+]Whats Happen...W..OSy.L2_`N.es are encryptedN.Nn.G'..l!...{.navailable. You [....Y...%.LT.l files on you cb.....5.=X.b e...nsion robet.....$e.s..d0.WUI.+Nthing is possibl....&0..9e.....store), but you .A{.$v.....O.ur instructions...bP..o.v...1Rt.cant return your....._D.!..[.3..[+] What guara..v .....X... just a business.P.%l...*..g.X{.do not care abou.Ml..Ay..g(F._b'eals, except get.B.U.,.....`f we do not do o.....D....=.i...ilities - nobody....h.:.8P.#..Sate with us. Its..h+.l.'...TUi.rests.....To che.^..]4.O..Gs.u\lcity, please sen.....=^/..`F.rger than 1M to &.!...Y..L_b...prove that we ar.....Am....n..rtoring.....If yoc.g.DlB.y.z.Mu.rate with our s e.G.....^.jw..its does not mat8.1..o.U.o.|.$@Nl lose your time..e]..(Z....q..5just we have the.L...~.7....B... practise - timeVT....G.b.uF...4luable than monew}.`..^.....%.x that a security;....<..:.....5nforcement agenc.....D$V..... you to negotiat.@.a....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\vncpassword.exe.log.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	2616
Entropy (8bit):	7.902324977708148
Encrypted:	false
SSDEEP:	48:HYGLzbCxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:HYYy7Ko4/AAUn5U50+NS43LPuLjv
MD5:	C00ABE5C441AED38A89AE99AB5565082
SHA1:	CFFCEDDECD4D808C6653A3E6E0554F89BF9598B9
SHA-256:	2C04688ED7F4D6808C25EE07D90668D001D28919EAD818A1CDF7CF822A65ACFD
SHA-512:	23E1FC35AECDA2F497C71FA66CB80A3B4A795F620E6C232EFC4235959C69877C791E2FAF977BC7CC35D8C393F1C767DBE7D36492013E87015B79C8542794536
Malicious:	false
Preview:	...4S..b. e.4s.,0.....H{.....T.V.iVP.B...b.....x.O....f>.%i<=.~.!..z....p4.LZHo.wR..xP.n...&1J#.J..xt_....Fl..q.....l..>..d...>6....}...u.r....JQ(..,.s.. .x...G...t. ..Lt|.y....C..=.....,.....,_s....8Tr...y...2.....-..U...W.x...f(..P.jmV.4_.6b...U.j.56..h....~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10l....e.....x...U.../.8.c..].-+.+.F.!...A.6...3|;e..c.. .M....st{A...G^...B.TU.[L.....N.....{{.y.q...sz%^?..{]G>..F..>r.il.4.....2. ...0q..Z-..I_..4L....^...."X([P..OD....}.P.....Bq..Ls.-....=...x..:x.....g...81ew.4.....3.....}.,..|^.%.3...\s...j C..n6.....)C)f.5....r.K2.7.W....D..`.."W.. .U.3/ep..F...?.{..HDe.R\v..KK.7*.K5P...._B.F.wC.%..... .z).y0GTk.t.....F_..A.J.....7....E.....c5..x5aI.....b..1..N.....G..+u...*S/Z[SIR?. .G....._..o..k'.d,. (....O...`..)...N.<.c..'1.Hu$d...6[..9v9.OQr..q.....|....~....7.u..\.BZ.M.o..,...9...[N..~.E.....G.E.$...c....P}.....'#...._...j)

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0

SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\mmc.exe.log.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	4472
Entropy (8bit):	7.810578743346678
Encrypted:	false
SSDEEP:	96:0RhZR9DAGKvL1WIOHQHLgRW+UwHgeVQ7e7Ko4/AAUn5U50+NS43LPuLjv:O/2GKj1WIOHQrgRHUuu7loiM5U50B43C
MD5:	8EA40DAAFC9645EDE70C6E9EB48A72DA
SHA1:	8FFC6D4EFE9E1751C3CF446DAFE6A8042C3D97F3
SHA-256:	1D8F442FE2BDFBD34A30B4F038B040B1245D27E8F04C76CEEF5198844F5E8386
SHA-512:	377C9CC50C4285A702AEFB13BC8C684A9E40018F2B529F147AF1066A6595E84F5BD3052B34272A44B179B5D038659D3AA6824B4748F84242F1960815B9A5A91A
Malicious:	false
Preview:	.....,0..1,"WinRT","N....B.W.B..H.o..tem, Version=4.0.....`O.*e.Gq..utral, PublicKey...M.:@.....x:..34e089","C:\Windq<...,.ch.I..6.iveImages_v4.0.3....-.....:.2Q.074a852d0b7a87fc.....puW..Frn.n.System.ni.dll",0m..<0?./.....s, Version=4.0.0.>...d....v1.:..Bal, PublicKeyTok+..(.F..A.|..l=089","C:\Windows.>..X...7._....Images_v4.0.3031Y..z.M.Z....f.\5aa66136dfbf2cc.m....C....[5M.f\System.Core.ni...M._.a..I\.o3em.Configuration.O...e.>.<Q.8..40, Culture=neutr.....!.. m...p.en=b03f5f7f11d50.~E...j<.KE.f.w.\assembly\Native...n..0....'Fh..9_64\System.Confm2..L!w?I~.sy.._c5e8c851f974088e.<..Ot`..I.r.Y[xm.Configuration.e....OJHz.....stem.Xml, Versio6.Hu..N....M.Y.Ere=neutral, Publ..J.[....IM.,..c561934e089","C:...x.....8M>/y\NativeImages_v.....&....?....tem.Xml\6dbfb468..-.`..n.#,..q..dee7df9b\System..r....4...^.../.,"System.Drawing.O...e.>.<Q.8..40, Culture=neutr.....!.. m...p.en=b03f5f7f11d50.~E...j<.KE.f.w.\assembly\Native...n..0....'Fh..9_64\System.Draw.(.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	6552
Entropy (8bit):	7.6809740067488335
Encrypted:	false
SSDEEP:	192:arNlg+2Ep4al8Tv1hL4wJrN8ZE7koiM5U50B43LPun:arN2Sual8Tv1l3rN8Z4TJO3LPG
MD5:	45E8DDC5A1FCA1EB8280490D96210FC2
SHA1:	FE3D54B2D77BB37C5212A6AB8DAF7A8CC5257D00
SHA-256:	011833BF2F0742337E121E4F375FD89DB4DE68911C5C676E91DB10DAE4174F55
SHA-512:	C46D531DAFE6A58B6E4150A86330FC444857E0C333CEC2FE4BE99B985FE9A1DDC38070B4357CACD8740DB02333C04AF9404BF4579CF8560F079C821F03DE08I9
Malicious:	false
Preview:	V.....i....:..,0..1,"WinRT","Nx....p.C.Q.E....tem, Version=4.0,.....;.x8".R.utral, PublicKey.L.).&.....n.f.34e089","C:\WindIkf.}.....e..7..iveImages_v4.0.3+.E.cG.i.+....W.074a852d0b7a87fc1...20=..J.t?.GYSystem.ni.dll",0>.`l....=h.r.d:., Version=4.0.0....(B...gqn..g{.al, PublicKeyTok..Y.ZS.u...-.089","C:\Windowsz`..F.Om...$.k].Images_v4.0.3031.L;D.6.....".\5aa66136dfbf2cc.....rB:..f\System.Core.ni^...;8[bt.].1.A.osoft.PowerShell.u5..d..Pw7.h.2.rsion=3.0.0.0, C.....y..%+...y|.PublicKeyToken=3.....7..a...0,"C:\Windows\assIp....P,.....tes_v4.0.30319_64|.?.w....*i..X1ec07#\fb0a968672..Z.M,<$$...)..627b6b\Microsoft.lp[.l..o...GWoleHost.ni.dll",.g.E.B.0A...w(e.agement.Automati..<.u....e..v.0.0, Culture=neu..+6.^...c..m+l<oken=31bf3856ad3r.....U`.....ws\assembly\Nati...A.f.'w.R...(.319_64\System.Ma....P.1y...s....1f0fd6cc913157b1x...mf..~..9..@.tem.Management.A<...E,...>.....",0..3,"System.M....6..!$t8...Fon=4.0.0.0, Cult.....C...licKeyToken=b03f.....-.

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false

Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	6360
Entropy (8bit):	7.698133853401283
Encrypted:	false
SSDEEP:	192:3S2mw6HOV2P0JDkgeXf+QcFoiM5U50B43LPun:C2mvC2P0DkgA2QcqTJO3LPG
MD5:	D5DE0A9E064955E7FEFD9675BA58ED1C
SHA1:	3AD33E375D1CD3F33150F552FF358584EB21D501
SHA-256:	18C33A5EB0220D6F0F177AF8DE2D75EBA17AB817DEB75DA27F6AD18D49B576CE
SHA-512:	6A7F4B5660C2927C350B92E938D4FFC4FDB641D14519F5F8AFBE9DD3C183E1010A6EB1149357AF5622907659AE38F75DD392BED51C0D0D6A7385EF914BD087F E
Malicious:	false
Preview:	OY;..HK...,....K,0..1,"WinRT","N.P%.`..J.D...M..tem, Version=4.0w...V....%4....eutral, PublicKey2v#e....9..w.}34e089","C:\Wind.....^....T..iveImages_v4.0.3w.G...8<....." 340a40c55ba464d0.....H.I.[...System.ni.dll",0.....D._b.|.~.., Version=4.0.0.w....6..V.....al, PublicKeyTok.SX.13ls`..u.F..089","C:\Windows.Xg..W.....I.Images_v4.0 .3031...\i.....4..8.m\d47bd74620ae94b}..V.....O}=w.b\System.Core.ni.LE.(....._.z.osoft.PowerShelloK..)(.Q...#...rsion=3.0.0.0, Cte.9. g.w...jj.[PublicKeyToken=3{{j.S.. <...>.9..,"C:\Windows\assB..G.e..:.ZT..?.es_v4.0.30319_32H...../.q ..-.\.ec07#\5e5547a60c.....i.....fb1f28\Microsoft...CJ....."oleHost.ni.dll",.B...&..;.-..Nagement.Automati! 'g'}T.".8.W8...0.0, Culture=neuE..D...v.....oken=31bf3856ad3..v..K.s.Wj.b..Lws\assembly\Nati....{y..v.[.,319_32\System.Ma..*4.....U..DZF861607b17a00ea9e...E...`]."v..t em.Management.Aw<.H..G....Q._.",0..3,"System.M"tB...~t@7f.....on=4.0.0.0, Cult..N|.Fa...bBj([.licKeyToken=b03f2.<.%...

C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	13688
Entropy (8bit):	7.984463822481459
Encrypted:	false
SSDEEP:	384:0d8fQyKPCGRqNzQKajIULdaB108Ro7RtqI+szbTJO3LPG:0SfQ5aGAmMOUB100ARt7+goe
MD5:	2F273B15F7A8CEA40A2B267400635B0B
SHA1:	819CAC3EBB1F4B2B6F446C8525C7B4701BAA6CE6
SHA-256:	F8D238B82C223DC507B621D3D9F7F920594E164620D233356BACE848B181EE89
SHA-512:	7B0D4C9FD7606F9E40EEC213874211283996ED5609AA6E35928799BBE59C9162C2AD478C9582D8BCF6C9D8DDE7D0F0C62C01617AFF3E5C4F8C7E69C481DCE8 7
Malicious:	false

Preview:	....k.....1.....z..O..6../.M.:$...SV..... 0...L.o.og,...G..wF.Y.Oe.n.t.i.a.l. .D..wV." ....HfG..... ...G0.f.~cw..z8Z.e..z.l..S[....t.....c...C....E.....aYN..3w...j...sd>P ..op#F.<LB... ..A.ITe.n...V.....:H}7...../.....b#. [.....].Z. ..W...H...vF.^.....p...K../..c.....P'..0..2..1.K..::..).g.J..a.-.....a..k..P..K.V.o....]..".2).3...=...j.=.2Ey..Y.L4.~d^...0.....*...h(vN...}.....h5.. U.g..3.S.D..h.; K..._..<.n...~X..i...E. '1.4.X.....f.8..n:Z..`\|.....x...yEl..w4.L^.....![...2....ZA..l.wz.?%>/.Q..>...Q...,..G.....(`.{..z.....'.wE..G^.....O]...(..j..-/..i..Qh..E.W...Q....4:..S.8. /....!.....t{.>.....U..e!.....p....~...{h v.pq.pH.7C..Q>...3....<.....'.#..JQ./.j..i..6.I[@.?..G....0..X\.Bu...u.@'c.....T....P...).K.e..*..@.%...s...u.0....<.@....I.....9.,..h.~.....q0.@....4R] ..x.FI.]_te.q1.l*...TD..|..i.).L.....^4....CdB.?.lfU...RR]pJ....Z.B...O..g{.....hm.....'.Z.....z.a.9.[qI^.`.....W.v.$...8SX.....

C:\Users\user\AppData\Local\Microsoft\Credentials\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5lJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Event Viewer\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5lJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Event Viewer\RecentViews.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	3544
Entropy (8bit):	7.837191448360416
Encrypted:	false
SSDEEP:	96:9+/tWSLiDHc5NFs3B7Ko4/AAUn5U50+NS43LPuLjv:9+/tfm0qwoiM5U50B43LPun
MD5:	C084D757D0D752CC5F14772D00C79A76
SHA1:	CACF820E737E03335DCFEC89A5619B1DB73E2B13
SHA-256:	3EE581ACF110EB1656389BBBB275E3B2EA0D28E642BF5EA762CEC4EF597D07A6
SHA-512:	A2706FE56F143E25C9609C5CBDA50E494E231B7A6C7759F06DECB8194900A1F0B3C9C940DB32E8A2FC322B5477385DD9B8BA07FFF0A803F38871FDB87093F01D
Malicious:	false

Preview:	.Th.^Z...9U.=.h.....System.Co6b*n..b.'..;:GYist....._items._.ct.W.37o...W.cN.....<7....88.I.....PMIGUIContro.x.t..P.&....Xl.0.0, Culture=neu.0,.....-oken=31b f3856ad3.(<...@...v...FCsoft.Windows.Man...)b.s.AP."..edControls.Recenmy~.U.(Y.s..7.%$odePath.eventNod.3..%E....$YXS>h.ticks.descript....Iw.....G!7.createdTime .....h...[1..".....Hndows.Managemente.=.S..kx..].@ols.RecentViewsD.a.-.q.M.....=Microsoft.Wi....4Hf!q..u7p.UI.CombinedContr.t%.]R<-1.V..e.....K... ..... indows.Managemen!.].D..9_.{Q.Wrols.EventNodeTy.>..~..i?R;..Cd.....ApF.}.....p.'....j.....N/A.....r^x.t.!T.7..rh. AM.....5/27/20.;r;.....-....KMicrosoft.Win.. ...."u .dIP.%I.CombinedContro..a.^.+....xj..ta+MmcNodePath....Q$a...|...p.String.name.descv.@.q..#.....em.Collections.A..#.....6.J.D.D.....Windows L.....6p8...O.....Appli cation..H.D....A.$Au.....w..;..@.[.?s Logs.....9..{P=.....#~!

C:\Users\user\AppData\Local\Microsoft\Event Viewer\Settings.Xml.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	2696
Entropy (8bit):	7.913341360690768
Encrypted:	false
SSDEEP:	48:q0fQ2Z2CxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:/l7Ko4/AAUn5U50+NS43LPuLjv
MD5:	B0D1D4C2AF2CA4C47F3FCDAB4865AD1F
SHA1:	CAB81B4911638BA9A797247D237CC85DF3EB8020
SHA-256:	7F5A051837D24374A456AF5C7020CC5CB7B988CE7EF5DFB0DE10ABC2030A5C52
SHA-512:	84908663611E6666B23659B063B7AE98DFC0CFCFDE4503FDE159E1278701ADB8A2D9D7FCCEB941337D7A3517AA3046DC798DA8780EA59D7972AC0C92DC7BD4 71
Malicious:	false
Preview:	g.[c.B.u86.>.M..review Visible="....XL..;..q\..irectChannelsVisu.r...j..A.E...annelsVisible></.nc..h._.!./...m.....H...#t.IXK.3.....:(.%...W...BD..;..`..E.2.Cu.iV....J.. )e..^w....yv...l..&.%.....86Q&vc5.....{.o7chgGV{#..f2..|<.@.%&.U..jb..g,....[...>.....r...e.Oy...l%3.. .H..5.<^O>4R_.[oW..yRir.Z>&..g..@*.:%.....`.c.N3l..@.,y&@.C[.y...-qy..Q.HI. ...._.~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10I....e.....x...U.../.8.c..].-+.+.F.!...A.6...3|;e..c...M....st{A...G^...B.TU.[L.....N.....{{.y.q...sz%^?..{]G>..F..>r.il.4.....2. ...0q..Z-. .I_..4L....^...."X([P..OD....}.P.....Bq..Ls.-....=...x..:x.....g...81ew.4.....3.....}.,..|^.%.3...\s...jC..n6.....)C)f.5....r.K2.7.W....D..`.."W.. .U.3/ep..F...?.{..HDe.R\v..KK.7*. K5P...._B.F.wC.%..... .z).y0GTk.t.....F_..A.J.....7....E.....c5..x5aI.....b..1..N.....G..+u...*S/Z[SIR?..G...._..o..k'.d,. (....O...`..)...N.<.c..'1.Hu$d...6[..9v9.OQr..q.....|..

C:\Users\user\AppData\Local\Microsoft\Event Viewer\Views\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Feeds Cache\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false

Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Feeds\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\GameDVR\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false

Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\DNTException\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\DNTException\Low\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\ESE\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false

Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\Low\ESE\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\Low\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false

Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\PrivacIE\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\PrivacIE\Low\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\input\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false

Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\input\af-ZA\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\input\ar-AE\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\input\ar-BH\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false

Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\input\ar-DZ\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\input\ar-EG\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\input\ar-IQ\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false

Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\input\ar-JO\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Local\Microsoft\input\ar-KW\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	modified
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Collab\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false

Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Forms\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\JSCache\GlobData.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	2616
Entropy (8bit):	7.908741655130932
Encrypted:	false
SSDEEP:	48:6xUE3oCxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:sd7Ko4/AAUn5U50+NS43LPuLjv
MD5:	F342F81E075A32AADE4BA56EC313B4C2
SHA1:	E457D56E61E0A4565824DAA25CAFAF5190D0C72A
SHA-256:	335D7BFF63C3936BF5DEC6C950CFD42F65ACAFA805D71D06C22F1B205206F874
SHA-512:	CF00BA8B35E8E9EE73F2B80FBB6692BD4A4573E819AF0ED0159C93274C0D462DB4897B9E8E653657CE197DBEC1539267FB09D857C61E2FF03BAB4F93C3F0948 5
Malicious:	false

Preview:	......TD.b..q{R.>>].>>.....+.v...AM.2?"].c....C>..X.S.<r../xD9...O..O....x..h.>&.I).G.x..%..O..x.....k..]'..tP2.v.%W...w..3DGvx.9.o5...{9.F....y...^..t.&.. '.T.U..|.Z..D/.x4UKT;.gJ-.m.....7..T.|...+....g..9s..R..|..i..Z.@S.{..Q.I.....~.D.8e.f.t.k. ...Dt...n...y..~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10I....e.....x...U.../.8.c..].-+.+.F.!...A.6 ...3|;e..c...M....st{A...G^...B.TU.[L.....N.....{{.y.q...sz%^?..{]G>..F..>r.il.4.....2. ...0q..Z-..I_..4L....^...."X([P..OD....}.P.....Bq..Ls.-....=...x..:x.....g...81ew.4.....3.....},..|^. %.3...\s...jC..n6.....)C)f.5....r.K2.7.W....D..`.."W.. .U.3/ep..F...?.{..HDe.R\v..KK.7*.K5P...._B.F.wC.%..... .z).y0GTk.t.....F_..A.J.....7....E.....c5..x5aI.....b..1..N.....G..+u. ..*S/Z[SIR?..G....._..o..k'.d,. (....O...`..)...N.<.c..'1.Hu$d...6[..9v9.OQr..q.....|....~....7.u..\.BZ.M.o..,...9...[N..~.E.....G.E.$...c....P}.....'#....._...j)

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\JSCache\GlobSettings.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	2616
Entropy (8bit):	7.916110571802551
Encrypted:	false
SSDEEP:	48:jPvVKfAECxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:jn3J7Ko4/AAUn5U50+NS43LPuLjv
MD5:	113BA9541F5582EF95A8B65ADB108402
SHA1:	8C4BD778CF5E245F084258D897FE4BEAC8EEEBA2
SHA-256:	96390BE0CDF7CF029F085A4445A2E6E83DE26D73F72FE1D3F348788898737F17
SHA-512:	BEC6A909C03E4D374203AF0CE82BA2DEC13059C7FE74C1C5B7DCC369D469871EC5D93FFCBD3E1158806AC5F99AD685DACE67211FEEC38918EBA4A4FB6488 BBE
Malicious:	false
Preview:	.....;...m.RYj<<>>].>>.....fM....1&.x~.t[.....D.Rh.....&...~8.....ki....K.[.H.....7.y[...H..4.].[..;....,.0V.p...{^....1?.:-.....b.49.a%...T.Q.....0.T).n=.|../m..gE....b.&Qa E...S.I..I...>.....:.k.J\.<..oS>.....p.T.L4...i.I.</ylWa.....g.....j....H....9.....F..)#.~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10I....e.....x...U.../.8.c..].-+.+.F.!...A.6...3|;e.. c...M....st{A...G^...B.TU.[L.....N.....{{.y.q...sz%^?..{]G>..F..>r.il.4.....2. ...0q..Z-..I_..4L....^...."X([P..OD....}.P.....Bq..Ls.-....=...x..:x.....g...81ew.4.....3.....},...|^.%.3...\s. ..jC..n6.....)C)f.5....r.K2.7.W....D..`.."W.. .U.3/ep..F...?.{..HDe.R\v..KK.7*.K5P...._B.F.wC.%..... .z).y0GTk.t.....F_..A.J.....7....E.....c5..x5aI.....b..1..N.....G..+u...*S/Z[SI R?..G....._..o..k'.d,. (....O...`..)...N.<.c..'1.Hu$d...6[..9v9.OQr..q.....|....~....7.u..\.BZ.M.o..,...9...[N..~.E.....G.E.$...c....P}.....'#....._...j)

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\JSCache\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache\0FDED5CEB68C302B1CDB2BDDD9D0000E76539CB0.crl.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	3224
Entropy (8bit):	7.914455736606722
Encrypted:	false
SSDEEP:	96:fz/sgr7Z3o7BJl6z7Ko4/AAUn5U50+NS43LPuLjv:ffrN47jlJoiM5U50B43LPun
MD5:	510B3D79D154E73BEDC253736F367882
SHA1:	4F26C8627C70D1CB4F5CC2C00588CB0FC365B7F6
SHA-256:	0A24D69CB29B886D19E36AD31204B585AE2DB81C8FB153A7624E2EDED6B9A60C
SHA-512:	BAA8745C27BC98DC86A591800667BE1DA224D3571EC0CF96AFE794603BB306D0AADFA75616AB1CBC6D77ED957812AC5CEC72B144520704C54D1C1CA9DCAF 262
Malicious:	false
Preview:	..r...w.C.. ^$...H.....0i1.0.v2.}....e.q""N.....Adobe System....Q.~.G.e.5K0...U....Adobe Ti...5.....}.....U....Adobe RoB.".*...C..\3H|000Z..2301092359|rT+.V].M....[.....-..1.. ...1009..Od..1V+Q&.J.....040117013929Z.y~cx.@+..0bt}...>.....04011701..3.....`.A....0#..>.....100'..b).~.>.sx....U...../0-0.....vL.@t..D....T.....0..P.U.I.bt'..Fh>..... c..IT.w..:.Q._..7..y.Z..]d*.x.Dd....0D..;.}..P\..3.|...'9C...F.....R...OD[..V.....-...}.L.4.d_.....@.....(..y...e>Y.....J....Bc..e....8..r.....a.....5ul;.....A .u.....SnP.?.`...".5YO.NL... 5y...x.^...9...c.3...V..RZ~}U..^..Z.).{O..kd....}.....&....u..%....s8.z@.%\..j...g=...!..c...Z../b..>*._..9c..g.u.5.]CEy...(?.5.k....2..(#j;&.c.@..;.t.D..u1..e.`.g]d..!.....i....X.. W.;\..!G.R.Dd....Q5.....e?.#.....us.,+.).....x..lnl....N...]G....w..a-p..M.9.%...oi6.^T...sV.3.}"..]....TTr,w.xA...~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10I....e.....x...U.../.8.

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache\CE338828149963DCEA4CD26BB86F0363B4CA0BA5.crl.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	3016
Entropy (8bit):	7.923165176538331
Encrypted:	false
SSDEEP:	48:ticEMQ0Dil6Qd6CxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwu/pBBlyK:In0s6Qh7Ko4/AAUn5U50+NS43LPuLjv
MD5:	45E277DDD6E2A5A2D084EE67F58AD13C
SHA1:	1223B8828B1BC5211BDBBFC85EC50CF04105DCBC
SHA-256:	1D92820D60A487F7ADAF4375C7EEAAD7C6AEC96B8B6CA3A06089EAF8AFC6B46D
SHA-512:	E3F1BE95F389EAF7CD2D39DBC4AE439255919180C6161E90A67E801F5065E491A763F8E4F89A037849BADC2B7CD7E66A2BBCBA8D8CBD33421AC008687FA427 24
Malicious:	false
Preview:	eh.x....oNvS.....0_1.0...U.!V...a}A..M....GeoTrust Inc.1.0.P.m.....{..B:ust Services1.0.....`..`dD.ervices..1808170...9l.P.X.....2300Z0...*.H.....".j....Yi...yn-.'f.,.qR.. +...sn...@ ...&..]lF..e./..e.O. 4..$..(...I.Ov..UQHW..8U.)....{O;w"C...T.c...GNK%E.[.....P5....,...#*....oYd.....U..+^.{..L..S...OX>....b...Y..@{[1...V...}.wT...r..S.....:.e&a."NN i.>9..F4..|f[.$c;.....X..!@$.d.j.?.n..e.S%+[R.....6...DY.j.p.vM./.$.=l.....c?....f.)....c..5.|.1.....Ew.....?.tS.`..c5h...,B.....l..@.v....t..t.;.}..'|...6.R.[tM..T.s!.cc.j. .$\ECsGR.R.7.....)j.....eUS,..D<.[.Pd.ZM?).D..I.! ..z=...Rw...av...d.....5.2.l.....Ha..F.f^DF.....l...8.....f..~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10I....e.....x...U.../.8.c..].- +.+.F.!...A.6...3|;e..c...M....st{A...G^...B.TU.[L.....N.....{{.y.q...sz%^?..{]G>..F..>r.il.4.....2. ...0q..Z-..I_..4L....^...."X([P..OD....}.P.....Bq..Ls.-....=...x..:x.....g...81ew

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_store.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	12824
Entropy (8bit):	4.796053283513675
Encrypted:	false
SSDEEP:	96:7AJ7QuMBimYo7Ko4/AAUn5U50+NS43LPuLjv:S7QVBidHoiM5U50B43LPun
MD5:	A990D98FD151DBB8AC16E6C807E7E420
SHA1:	F4342212E0FCE4DA85F7E985089216A16FF2C2E0
SHA-256:	261EDED39E013046D408131DFBE02492403723EF88747CABAD9ECA81B0DBB365
SHA-512:	1EE30B54BAEDF1462B7F2FEB44A985C79F7BD956958CBC8C15C9D45AEEF8AF64AB4C8240DD0314AB999E9E2984066B33607EC3DB201F5113F7BCB453CA9DA 471
Malicious:	false
Preview:	.T...v.o....)..(....-.....S...d@L....@..-..Q.&.F..g.oN.j..\uz.L..@U.\.U3...._. ...Z4n`a|[....e3...V.....V.1.....I.t.....2...OUc.....Lq5...?$j.q..{E8.>..=.H./.U...}k..q6`.pd,...5.G.?..A.H.O^ ...H...R..F..".sjE.k.....xA..)..`....S.{..z.&.Q...~...F..u.dIQ..n5..+..;.H...0z.|.s...8.....>a.s...r..<...G&b..B...|.RG..X.AJ.q$.+..)....TR...Vm..Q....D"..l.;6..0.....>s.MQRyh7.Ed..& .0SS.....I..W.A.....__...x(...`....MZ...$4.6....]..s.3.....Og.T.m..K$.U.{(+.b$.....S..B.@%..|lUq..L..'..wOL....J&..X.h?...z8&.....W)a,.AW.,...*.....W)a,.AW.,...*..... .....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW.,...*..... .....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW.,...*.....W)a,.AW

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storei.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe

File Type:	data
Category:	dropped
Size (bytes):	26744
Entropy (8bit):	4.251228707363468
Encrypted:	false
SSDEEP:	96:vmq1+ZOYXB+7Ko4/AAUn5U50+NS43LPuLjv:v/+EWFoiM5U50B43LPun
MD5:	B151A641B9B233DC2B781644105E59BB
SHA1:	D03ACA22C2E78CA5475750C3CB2BECAE3AF2F7EC
SHA-256:	8DD042D7E9129C7B85748B8A3ABF7E659EAAB3223B1F43649789512B286FC417
SHA-512:	C45729E9637DE4919BF6328F13C9C1ABC46DD21D0566C897FFBF05D8CABBF3BF9BAC15223C3A3F49714552AE3641280BD415B2E13AAF8671CB2C6C97BC99C6F9
Malicious:	false
Preview:	=..O4./#.2.....2.<.?.....Of;k.swS."G.....=..t.@`M.sV..<w~H.O.ud.....e.TX..../..rg.Bk..g.p]zQ...S5+%.l....y6..l@.*.|.{.....8/..h..I.....C.gB.s....>.3+x{Df..*]e..J...l...B.8.{WoZ.~>>...RYq.9A..Mx.pp.....r6..R.Y@..gk&|.....Hg*X..4...E..`-.b.~..tHMO..Q&..5.n.l...fj..E..:..6....q.g.y$...'.8\=<..v~.....5....5...`g.....5].....2Hs...V..N...3...ET...<....x..<.D0.[...:...g.io7..|.:x.....'..\.x.nY.[.ZB)...X.eg|.IP.(i....H..".%^.&.x.....X .m.....<HI.u(...F+.j...tMy.H...7..U.w..N.....[.....;...S./.MAFI....p.MW.....P..x8p....kY.{ezz....9...z~x..../..P..,.....7...N...1.y .&R&..J.....8.V....0.c.ns.....E*U..r2....@sUJ.Aw.lG.....aN..%....c...]n.!.k9..L]je.(..../.jn..7.b.....(..../.jn..7.b.....(..../.jn..7.b.....(..../.jn..7.b.....(..../.jn..7.b.....(..../.jn..7.b.....(..../.jn..7.b.....(..../.jn..7.b.....(..../.

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storek.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	2856
Entropy (8bit):	7.910592091593916
Encrypted:	false
SSDEEP:	48:Eb/VfRNsJmUMP6W9MmnRCxV7wAOo4LVGXsAAa3n5lLq5mhL+NSdTmyO13KmhUwun:EbNf/KMPj9NQ7Ko4/AAUn5U50+NS43Le
MD5:	5533844DE13B189DA28C93531A16219A
SHA1:	E6157687DA561C5E01E874616FAC3FA1BD184D83
SHA-256:	6A894701E7356EE1A85B0EE8210A52574B1350A02CF8E1F108DB2F0103C3C5C2
SHA-512:	2B6B858873B5C01CF24A9661E6A316111DE54414A7CB64C1291BEBB4928F9B2DC2A11C8C40852D74C6B237FB306E9D413A695DE7C7FC50E6BC67A2C00CECA4AD
Malicious:	false
Preview:	i..v}.....{C.\.O.....AC....O..8...2Xp..0W.sgx....f..... .....<...0...]..{.{....9.:=e.Z}.8..d..7..OS...a.7]%..V{.6...$..'..J..B7lt$..[.0.....Zq.+5.6..C}p.U.}G5}.z.....'.....*.O"...7.g.....D.@..x.K.R.....T.,i.....px.\..9G'.....-...+O._...I..,'.....N.H.rn..M.k....X..a..4...b...n.t...cl`.C.H...w..32..I....V.....t...`?n...`...Rf2...L.n...91!u,E.L..=u.Bi....(.....O@.2.^..7tG....x.Cf.$u.a...J'?a.ek...&G5.R..4.-..7.../?.".N]...u~...dnf.....u+s..6..+}m..;....9..BL...|TvL.~../. %....7.....".~..~...Z.!.U.;=.(.-+q.ekKV.zv}.L...M.b.q.{.....j10I....e.....x...U.../.8.c..].-+.+.F.!...A.6...3|;e..c...M....st{A...G^...B.TU.[L.....N.....{{.y.q...sz%^?..{]G>..F..>r.il.4.....2. ...0q..Z-..I_..4L....^....."X([P..OD....}.P.....Bq..Ls.-....=...x..::x.....g...81ew.4.....3.....}.,..|^.%.3...\s...jC..n6.....)C)f.5....r.K2.7.W....D..`..."W.. .U.3/ep..F...?.{..HDe.R\v..KK.7*.K5P...._B.F.wC.%..... .z).y0GTk.t..

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\addressbook.acrodata.Rook

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	data
Category:	dropped
Size (bytes):	17048

Entropy (8bit):	7.122976821020622
Encrypted:	false
SSDEEP:	384:CMhS27SJ+eEGCQCvthKh2fUh2LgULzUY+TJO3LPG:CMhS27ECG9h+JgPoe
MD5:	A8847CCF87E692A78A73B309AC1500C6
SHA1:	E151EE9680B3A8B732ACD3A5ED7AE0301C2C60E4
SHA-256:	3A43C5A657FB3A78FE647050A054C431900A094907098A0CE3AA4386A3CAA1C2
SHA-512:	41AAC7DEED94A02E68CE68BE4684DF2DD86CAF7955B7BFA03BA5F62A45A40766FC408C8B6572A633FAE0E835B0EB727770A5F8D51AC3C08815A73B18B4C2A4 15
Malicious:	false
Preview:	.<.x\mg...ZWN.Z6....1 0 obj.<</P......}...+&/.f.<</Entries[2 0 R.b}lF.....M. R 6 0 R]/NextID_...eZ..;..dMC..ssBook>>/Type/PP./R..O..:X..._@er>>/V 65537>>/T.='a...X.f..!. .dobj.2 0 obj.<</..@P"._JvL*...08204A130820389A.BV.g?.02.:.....CBD28300D06092A8....nK.8(..{..v5003069310B30090...C."."..J.VB..3312330210603550....\m..,=k..5205 3797374656D79k...t....L.WK..F7261746564311D3r.}KP...1..L..#.441646F626520547Z.....q.Ld.6696365733116301%.n.`r.Z.n>3P..1646F626520526F6|.....S. ....HD303330313038323.nf....x....j.A2333031303930303..{..~.....B300906035504061E....C..`.....60355040A131A416%z.....%..:t..v.4656D7320496E636....gT#.v.... ..g4311D301B0603550/L.X.y%....._5205472757374205....8j.!u.b..P.1163014060355040Hl.Z.v.]w....T0526F6F742043413l.....+7z.U...A864886F70D01010Z.!...{ L.....P082010A028201010.9.....n"=hY..733537F3F9C12886...L....~?+=..W9AD1488F9C310D81.r.%..t.U....c+935B0CC6CA94C9C1dtz.[...m...M..4E2E02066453F398Ywk .S..'T.e.....624F60112B035DF5...L{..1

C:\Users\user\AppData\Roaming\Adobe\Acrobat\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Flash Player\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false

SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Headlights\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0
SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

C:\Users\user\AppData\Roaming\Adobe\Linguistics\HowToRestoreYourFiles.txt

Process:	C:\Users\user\Desktop\ZunmmW7pe5.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2500
Entropy (8bit):	4.814779713246776
Encrypted:	false
SSDEEP:	48:LLgLRIpHKeZDesgKpXw5IJM8M6SZRXJRgcf6jk/wwkOSX38aieJRuor:LkeZDewAiJFSZFzyjk/wV3ucRu4
MD5:	00F71CDE522689585EAA9C62385AFA22
SHA1:	350E319806F7A71267A5E4A749EB190EAD38DBB0

SHA-256:	B14EC2FCCCAC5059464E800EDF56049C0277124ABD60EE49C1F726861DF925BF
SHA-512:	47442D335F16E259C4593370467C741AC2B41F329330AFDD649B89B44C4233EDD7D2AF70883403993D6022C617235C20B89AE667CA4B3F82D678836ADC34F4DF
Malicious:	false
Preview:	----------Welcome. Again. ----------..[+]Whats Happen?[+]....Your files are encrypted,and currently unavailable. You can check it: all files on you computer has expansion robet.....By the way,everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).....[+] What guarantees?[+]....Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.....To check the file capacity, please send 3 files not larger than 1M to us, and we will prove that we are capable of resto ring.....If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,cause just we have the private key. In practise - time is much more valuable than money.....If we find that a security vendor or law enforcement agency pretends to be you to negotiate with u

Static File Info

General

File type:	PE32+ executable (console) x86-64, for MS Windows
Entropy (8bit):	5.926790694756029
TrID:	• Win64 Executable Console (202006/5) 81.26% • UPX compressed Win32 Executable (30571/9) 12.30% • Win64 Executable (generic) (12005/4) 4.83% • Generic Win/DOS Executable (2004/3) 0.81% • DOS Executable Generic (2002/1) 0.81%
File name:	ZunmmW7pe5.exe
File size:	415232
MD5:	6d87be9212a1a0e92e58e1ed94c589f9
SHA1:	19ce538b2597da454abf835cff676c28b8eb66f7
SHA256:	c2d46d256b8f9490c9599eea11ecef19fde7d4fdd2dea93604cee3cea8e172ac
SHA512:	278cc5f0215058c6c6943f9e432a335cb824bbb44437b9e28cb4a2ba710e0485aa1388e8a06257b0eaea7aceeb8dabe57663e62b83f0e517eb53a8d3ff7aec67
SSDEEP:	6144:wmwG6/BAIy0q4KT1Y/Itk5bMTRiGaSD8KM/RiPl+MlfV50kR:wm16/BAIy0q4KT1DaMAGa0nJ
TLSH:	66948E19F7E044F8D977C278C6660616E6F2BC590361DBEF23A44AA51F23AE14E3E710
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (e.Tl...l...l.....S.i.....Q.....P.a....Z..k....Z..p....Z.....e|1.}...l.....Z..\....Z].m....Z..m...Richl.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x14002add0
Entrypoint Section:	UPX0
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x619D04C9 [Tue Nov 23 15:12:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	5248c5944a1d330e94f2cebc3ead99ee

Entrypoint Preview

Instruction
dec eax

Instruction
sub esp, 28h
call 00007F7A30A8D598h
dec eax
add esp, 28h
jmp 00007F7A30A8D15Bh
int3
int3
dec eax
sub esp, 28h
call 00007F7A30A8DAE8h
test eax, eax
je 00007F7A30A8D303h
dec eax
mov eax, dword ptr [00000030h]
dec eax
mov ecx, dword ptr [eax+08h]
jmp 00007F7A30A8D2E7h
dec eax
cmp ecx, eax
je 00007F7A30A8D2F6h
xor eax, eax
dec eax
cmpxchg dword ptr [00029E38h], ecx
jne 00007F7A30A8D2D0h
xor al, al
dec eax
add esp, 28h
ret
mov al, 01h
jmp 00007F7A30A8D2D9h
int3
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
movzx eax, byte ptr [00029E53h]
test ecx, ecx
mov ebx, 00000001h
cmove eax, ebx
mov byte ptr [00029E43h], al
call 00007F7A30A8D8CBh
call 00007F7A30A8DC9Ah
test al, al
jne 00007F7A30A8D2E6h
xor al, al
jmp 00007F7A30A8D2F6h
call 00007F7A30A92225h
test al, al
jne 00007F7A30A8D2EBh
xor ecx, ecx
call 00007F7A30A8DCB6h
jmp 00007F7A30A8D2CCh
mov al, bl
dec eax
add esp, 20h
pop ebx
ret

Instruction
int3
int3
int3
dec eax
mov dword ptr [esp+08h], ebx
push ebp
dec eax
mov ebp, esp
dec eax
sub esp, 40h
mov ebx, ecx
cmp ecx, 01h
ja 00007F7A30A8D38Ch
call 00007F7A30A8DA4Ch
test eax, eax
je 00007F7A30A8D30Dh
test ebx, ebx
jne 00007F7A30A8D309h
dec eax
lea ecx, dword ptr [00029DB8h]

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x65600	0xb4	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x65000	0x1dc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x5c000	0x2bf8	UPX1
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x656c0	0xb58	.rsrc
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	0x64c00	0x94	UPX1
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
UPX0	0x1000	0x3a000	0x3a000	False	0.517679148707	zlib compressed data	6.48037413747	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x3b000	0x2a000	0x29e00	False	0.356570662313	data	4.35889885933	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x65000	0x2000	0x1400	False	0.4736328125	data	5.16346554145	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x6505c	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.DLL	GetProcAddress, FindVolumeClose, GetVolumePathNamesForVolumeNameW, FindNextVolumeW, GetTickCount, lstrcmpW, GetDriveTypeW, EnterCriticalSection, WriteFile, LeaveCriticalSection, InitializeCriticalSection, lstrlenA, CreateFileW, DeleteCriticalSection, ReadFile, GetLogicalDrives, FindFirstFileW, GetFileSizeEx, GetCommandLineW, FindNextFileW, GetModuleFileNameW, WaitForMultipleObjects, SetProcessShutdownParameters, SetVolumeMountPointW, CreateMutexA, WaitForSingleObject, ExitThread, SetFileAttributesW, OpenMutexA, SetFileInformationByHandle, lstrcatW, GetSystemInfo, CreateThread, SetFilePointerEx, MoveFileExW, ExitProcess, GetCurrentProcessId, WideCharToMultiByte, lstrcpyW, lstrcmpiW, HeapFree, HeapAlloc, GetProcessHeap, ReleaseSemaphore, CreateSemaphoreA, CloseHandle, RaiseException, Process32FirstW, LoadLibraryA, Process32NextW, GetLastError, Sleep, CreateToolhelp32Snapshot, OpenProcess, GetModuleHandleA, TerminateProcess, lstrlenW, GetCurrentProcess, FindClose, WriteConsoleW, HeapReAlloc, HeapSize, FlushFileBuffers, GetConsoleCP, FindFirstVolumeW, GetConsoleMode, GetStringTypeW, SetStdHandle, SetEnvironmentVariableA, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCPInfo, GetOEMCP, IsValidCodePage, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, IsProcessorFeaturePresent, GetModuleHandleW, RtlUnwindEx, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, GetStdHandle, GetModuleFileNameA, MultiByteToWideChar, GetModuleHandleExW, GetCommandLineA, GetACP, CompareStringW, LCMapStringW, GetFileType, FindFirstFileExA, FindNextFileA
ADVAPI32.dll	CryptGenRandom, RegCloseKey, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, EnumDependentServicesA, CryptAcquireContextW, CloseServiceHandle, OpenSCManagerA, ControlService, QueryServiceStatusEx, OpenServiceA, CryptReleaseContext
MPR.dll	WNetGetConnectionW, WNetOpenEnumW, WNetEnumResourceW, WNetCloseEnum
NETAPI32.dll	NetShareEnum, NetApiBufferFree
RstrtMgr.DLL	RmStartSession, RmRegisterResources, RmGetList, RmEndSession
SHELL32.dll	CommandLineToArgvW, SHEmptyRecycleBinA, ShellExecuteW
SHLWAPI.dll	PathFileExistsW
USER32.dll	wsprintfA

Possible Origin

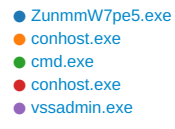
Language of compilation system	Country where language is spoken	Map
English	United States	

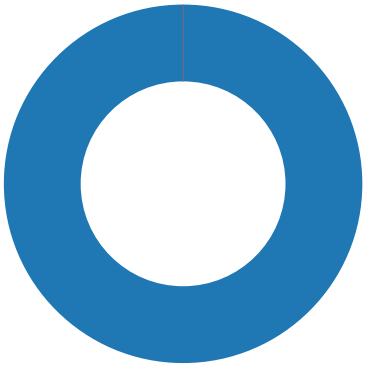
Network Behavior

No network behavior found

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: ZunmmW7pe5.exe PID: **8072**, Parent PID: **3896**

General

Target ID:	0
Start time:	15:16:53
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\ZunmmW7pe5.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\ZunmmW7pe5.exe"
Imagebase:	0x7ff7e3710000
File size:	415232 bytes
MD5 hash:	6D87BE9212A1A0E92E58E1ED94C589F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software	RookPublicKey	binary	2D 2D 2D 2D 2D 42 45 47 49 4E 20 50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D 0A 4D 49 49 42 49 6A 41 4E 42 67 6B 71 68 6B 69 47 39 77 30 42 41 51 45 46 41 41 4F 43 41 51 38 41 4D 49 49 42 43 67 4B 43 41 51 45 41 6E 73 2B 6A 36 4D 52 7A 58 58 53 4F 62 49 44 48 59 70 38 53 0A 55 70 42 37 4F 56 69 79 49 35 75 76 59 35 38 33 44 51 6A 54 36 59 51 42 73 58 64 49 70 63 72 67 51 77 6E 66 49 38 4A 74 49 72 42 41 42 41 54 66 74 43 32 4C 35 43 6E 4A 6B 47 76 37 67 52 54 50 0A 6D 2B 31 4A 59 30 4F 6C 7A 47 63 4A 6D 5A 71 43 48 49 6F 4C 42 62 47 72 69 47 37 6A 67 42 73 2B 39 52 43 71 74 4A 2F 4A 50 39 4C 31 4E 65 53 34 48 6D 61 61 6E 38 48 43 78 47 56 54 35 79 73 71 0A 49 78 76 31 70 7A 30 42 77 31 61 6F 41 75 32 6D 50 7A 49 77 79 30 63 6C 33 50 35 62 34 43 79 67 41 62 42 55 75 6F 38 50 4B 31 4F 7A 6C 34 73 50 49 59 31 4F 32 31 50 51 43 6F 7A 69 4D 32 6B 6B 0A 52 6D 43 44 46 76 38 52 65 52 55 77 62 68 55 6D 6E 4C 5A 68 33 74 4B 30 34 33 4A 78 4C 45 62 2F 71 5A 6E 6A 64 39 54 41 4A 78 50 48 48 78 68 39 57 6E 57 42 4E 30 34 5A 72 4A 33 64 31 50 6F 6D 0A 48 39 64 44 73 62 78 34 46 63 70 62 4B 6B 4E 38 66 43 4B 43 62 34 39 4C 45 66 71 43 45 66 4C 48 62 71 7A 33 4F 4D 36 49 4D 4F 4E 4A 42 6C 31 6D 75 4C 6F 46 62 6F 2F 62 62 43 64 30 57 32 6E 6F 0A 4E 77 49 44 41 51 41 42 0A 2D 2D 2D 2D 2D 45 4E 44 20 50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D 0A	success or wait	1	7FF7E3711F30	RegSetValueExW
HKEY_CURRENT_USER\Software	RookPrivateKey	binary	0F 7E C9 04 BF 5A 95 21 91 55 FE 3B 3D DC 92 28 A9 2D 2B 71 89 65 6B 4B 56 C0 7A 76 7D A5 4C 86 BB C6 88 4D 00 62 8D 71 9F 7B 9D A9 EA E6 DA C9 9F D0 8E 12 6A 31 30 49 11 82 AE 04 65 EC 0A 1F F2 0C 78 0E A1 9B 55 0B D1 DD 2F EB 86 9A 38 BB 63 17 00 5D AF 2D 2B DA 2B D0 46 C6 AC 21 91 EC 8A 13 41 9A 36 F8 B5 81 33 7C 3B 65 C1 F6 63 B9 B8 2E 4D 0B F3 A4 93 B4 CB 73 74 7B 41 C7 F3 A5 AE DB 47 5E 9D E2 D6 42 D7 54 55 E1 5B 4C AC EF A5 BD DD 9B 0C 87 1A FA 92 4E 90 1A 1E F1 C0 C7 7B 7B 19 79 AE 71 18 09 90 73 7A 25 5E 3F 86 81 7B 5D 47 3E C1 CE 46 0F FD 3E 72 10 69 6C 8E 34 CC 0E AD 10 FF 32 7F 20 A5 B5 C0 30 71 1C D2 5A 2D AD 03 49 5F 8C 9A 34 4C 0C FB 92 EC 9C 5E FC AD C0 F4 22 58 28 5B 50 E3 04 4F 44 8A B0 BD BA 7D DB 50 98 F5 1A 2E D6 E9 42 71 DC 88 13 4C 73 11 2D EB 80 F9 11 C9 3D 01 83 E9 78 1D EE 3A 78 D4 C3 A5 8C 19 15 A3 D4 67 D1 F8 D0 38 31 65 77 7F 34 1A 18 C3 EB F2 F7 89 33 8E ED F1 C3 F4 EF 7D 08 2C 89 FB 7C 5E 9E 25 D6 33 C7 9B 9F AE 5C 73 BF EA E3 6A 43 DE FB 6E 36 7F 8B 18 B6 E0 F8 C1 EC 04 29 43 29 66 9B 35 E3 BA C9 FC 16 72 E2 A0 4B 32 BF 37 FF 57 CA D2 0B F6 44 C4 FA 60 99 E0 AA 94 22 57 E5 A0 83 8F 20 C5 55 12 33 2F 65 70 16 9E 46 A7 D5 80 E2 3F 9C 7B 13 AE 48 44 65 D0 52 5C 76 A1 83 4B 4B AB 37 2A 8E 4B 35 50 8B F8 93 D4 5F 42 C5 8F 46 D1 77 43 05 25 18 A8 BB D6 E8 20 EC 7A 29 FB 79 30 47 54 6B 00 74 AC FE 9C C0 0A 8C 0D 97 46 5F 83 D0 41 BF 4A 82 2E 9D A0 ED 91 37 C6 DA D3 B4 E3 45 C9 BA 89 B1 12 B0 E4 B8 63 35 FD 07 78 35 61 49 18 FD 92 91 1E 62 CE B0 DB 31 AC E7 4E 90 A5 FD 86 07 98 0C 47 05 A8 2B 75 0C E0 F2 2A 53 2F 5A 5B 53 49 52 3F 15 DD 47 F1 CF C0 99 A4 5F 82 A7 6F 85 9E 6B 27 B1 64 2C D3 20 28 DB E5 C1 D4 4F 0F AF DC 96 60 82 B9 29	success or wait	1	7FF7E3711F5A	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			DF C9 9D B4 4E B5 3C E8 A0 8C 63 8A D2 85 27 31 E7 48 75 24 64 1B 1B BC 36 5B A3 A7 39 76 39 8E 4F 51 72 2E 7F 71 D6 06 1B 91 CE 7C 04 87 E7 C0 7E BD 97 88 08 37 8E 75 85 9F 5C F8 42 5A BD 4D D8 6F 8F B8 2C 9F 0F 1B 39 F0 C4 04 5B 4E 08 CA 7E DD 45 C0 92 83 17 04 47 8E 45 CD 24 D6 B4 E5 D8 9F 63 9B F8 8A DB 50 7D BB 8E 16 D5 D0 14 91 1D 27 23 18 F9 89 94 C8 5F 0A 15 E7 6A 29 FA C5 D3 02 96 6F 8F 0D 42 EB 56 EB 94 C5 EB 64 2E 90 11 23 A9 20 BE C1 20 71 42 4B 68 03 C5 20 FB 82 40 40 7C F9 88 39 3A 0E 7C 74 44 70 14 9E 59 E1 47 B4 EF 16 5C 20 60 40 56 7F A5 12 70 B7 AF 5C FC 5B 8F 64 2D 11 4E 8E 3D CD 9E 7E D0 7C A4 53 EE 43 E8 90 CB 67 39 19 54 34 DA B0 0D 90 12 CC 74 99 8A 39 8B A8 A8 55 16 52 F5 CE 1C 14 E9 DA 2F A1 9C 51 B2 B6 CF 2A D7 11 65 AA CD 92 EC DB E0 57 9B 46 96 7B A3 73 76 3F 18 D6 71 3A 9F 38 13 B9 05 2D C1 68 28 77 3E C0 25 F7 5F 9F 6C 7C A6 15 50 06 20 D0 A8 09 6B B2 7B CA 64 64 52 68 D3 34 DB D1 A5 97 77 B9 61 77 D9 F9 DD 76 75 95 FC 46 67 62 0F 8E A9 3C 0D 15 D9 7D A4 FF DB 2C 18 E8 21 B1 62 9D 76 D0 42 D7 49 37 43 B0 F3 32 26 F5 6F 16 86 BE 71 35 BF 1C 3B 02 64 E0 7F ED AF 5A 4A E4 66 50 1E D1 5E 95 91 C2 08 6E E3 19 71 1C 43 F5 4C 43 95 C1 2D 53 94 E9 C0 B5 E0 04 80 4A D0 16 B7 40 E0 C7 24 20 72 0C BD CA 3A 29 E1 6D 4C 51 38 7D 95 45 52 45 3D E7 94 69 1C 5B FF 5E 40 03 8F 98 B7 94 DB 3D BF CC 8F C2 A3 92 B9 F4 0E E0 E5 53 E0 33 32 70 A8 AB 4B 1E 6B 5A 1A 6F 4A 52 AC 80 A2 33 48 D3 BA D9 08 E7 37 C9 07 BB 7F 1E 25 9A E7 37 CA E2 E0 DA 8C E3 EF A4 4D 16 BB CC 18 C2 A6 32 42 89 3C D5 BC D8 AE 1C 3C 07 8C 46 54 F6 BD 6C 9E CA 1D 7F 91 09 29 0A 24 8C 2A BE 99 5E 30 D0 78 21 8E 16 76 53 06 16 6C 7C 23 2E F6 4D 02 B7 E0 1F 21 B0 CE E0 B8 9E D0 DD 05 23 D0 34 F3 53 E8 06 5F B0 6A D0 B5 A7 34 FC 92 AD BF D1 D4 0E F6 65 5E D3 05 EA 57 9E FE DB A6 3C 2F 52 7F 31 A3 1B 3C 5B 02 2F AB 38 FF BC 6D 7D 97 24 23 E4 FF 43 6D 6C BA A3 22 56 4F 38 A4 EA F7 84 DB D2 08 41 9E 04 71 76 BC 1C 49 96 F9 E0 B4 A4 0F 13 90 4A 8F 71 E7 2B 98 3C 68 76 5B DB 61 63 3A AA 6D 1A 29 BA 1A 7A FB 73 00 D3 47 7F CC D3 33 91 B8 47 FE C4 4B C0 B3 76 1A 0B E7 4D 57 12 8E 7E 96 1D 5A D0 F6 79 E3 41 36 0C 40 81 93 B6 40 AB 39 56 08 C7 7E C7 78 41 27 8F FA 9B 16 08 08 04 F1 47 8C 24 35 50 F9 1A 1B 9F EF A2 49 F3 C8 BB 64 D5 57 D1 19 2A 83 30 DF 82 75 EB 03 96 9F 00 2D 9B CD 0C FF DB 1D 2D 94 82 E0 94 1B 56 FD 1F 4A 39 75 DF FB 0D 27 9B E2 C2 18 A2 9F 22 A5 B3 63 8A A1 1F 1A D0 D8 99 3B 6B 03 FE 80 81 B6 4D A5 48 47 5E D6 CB 1D 4C CC AF 5B 7F CC 52 CE B0 6E CC D3 46 8F 34 D2 14 7B 48 70 0B 1A 16 E6 D6 1E E3 91 9B 53 86 CE D4 F2 94 D4 A3 88 67 D8 D5 37 A4 56 EB 81 8A 5E 32 02 3F 94 75 07 AA 11 E8 DA 1D E2 B7 22 9C E8 FA 28 F0 E1 B9 A6 52 10 B2 D2 0E FF F3 4E 06 10 BA 11 42 6A A0 CC 92 E8 BE FD 12 DD DE 4E 55 98 CB 3F 4D 56 62 06 87 5F 43 61 71 F7 B2 ED F6 7B 47 BF 9D 67 09 5D 76 50 5E 6E 08 FB BD 10 56 81 3C 7B 02 82 66 00 3B 11 85 DD 93 94 C0 EC 1C D7 A0 F6 BC 7F 1F B8 9C AA 49 A8 DF 2D 7C AE AA 9F 0A CE 5A D8 51 D7 A8 D0 EA FD 14 78 49 02 4F 3B 3C DE 6E E7 F0 2F 61 E3 27 C3 4D 00 08 D8 E6 4C F9 AB AC 09 39 BB 4D 51 B5 A3 1B 16 26 11 70 AB D2 D6 FE 15 E7 81 0A B7 FB 72				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			A5 6F B3 52 72 76 A4 11 D9 5F 8B D2 AF E9 6A 01 C4 F9 27 FE 46 B1 EA DD A9 68 F3 83 CD 55 DD 76 CD 03 FA 6D 5E CF 36 0A D6 B8 AA 39 BC CD 07 32 79 2C 62 0C D6 3F E6 89 9C A4 62 BE C2 8C 65 8D 00 79 2B A0 16 AF E4 EE 62 6C D5 F0 A5 61 5C DC 17 38 51 A9 DE B5 B6 8E AE 20 A5 D2 DC C7 2A 1A 85 71 8F 4E 44 4F B1 D3 BC 63 55 4E 0E DE 5A B6 B7 B2 F1 C0 8E 50 F7 EC 5A F9 37 22 2E F2 F3 25 0F 7A 0A 17 A6 19 0A A5 D1 75 31 9A 21 D2 33 3E 08 BD A8 85 37 86 AC B8 DD EF 84 AA 47 D1 F5 CF 04 A3 FE 0F AD 43 DE 2D 42 84 64 DE B0 87 9D A6 AF EC 56 CA 0D 2D 72 7B 81 7E C8 C1 DB AA E3 25 EB 80 B2 F0 19 9B A6 15 39 38 FD E7 36 CD F2 6D DE ED 1E C9 9E 1C A9 00 E8 16 53 6C F7 41 2A E9 F6 23 FC F7 DE AD 68 35 CC EC B0 5A 7A 85 15 4B 4E 65 27 BC 4D 5F 30 55 2C BA B0 65 83 9B C9 99 11 0B DF 44 1A B1 CC D1 82 E7 0B A8 A8 60 D4 62 A9 46 CA 21 21 17 23 9F 38 59 95 29 86 C4 8A 6F D5 53 E5 03 D4 84 F0 65 7C 26 B1 B4 D0 35 CA 26 C6 A3 0D 7F 72 10 E8 F5 BA 6D CD 1A 9D 7E 43 02 78 F5 4B E5 51 5E E9 C1 44 00 C1 BE 8C 44 25 44 1C BB F2 4C 27 DF F1 90 8F 36 6F 7E 80 1D AB F0 D2 A3 03 A4 E5 55 5B 27 25 8C 36 86 03 DA 7D FF 64 EC 22 21 8E A6 3C 68 2F 0B 3E 39 7D 83 91 B8 78 69 16 D6 08 F8 BF 98 94 64 BC 6E F2 11 89 FD 95 1A D0 7E 3C 9F 07 A1 C5 88 F9 DA 75 6E 40 48 8A 72 43 26 81 FD 00 5B 1D DA 71 12 B9 21 52 72 02 9C AC 7E 28 AD E9 FF 8A DE 1E 8B D1 F6 A1 7F F1 DF 4D E3 FD 27 11 5C 48 0E 27 C3 A1 34 63 E0 63 C5 D3 69 1E 8B 9C 9E 21 5E F4 FF 47 AA 8E 90 82 15 7C A0 00 E6 0C 3E E5 18 CA AA 49 04 AF 34 F5 97 3D 00 6F F6 73 4A D1 C4 14 95 DE C3 F4 96 8A DD 90 65 31 59 31 41 A2 50 EA DC DA 05 34 AE 43 5E A6 17 13 BB AC 25 F2 DF 00 79 9D 55 0F 01 85 43 A9 5A 1F B2 BB FA F3 E8 9B B9 60 71 16 E0 91 42 59 3D A4 90 E7 D9 09 C6 28 CA A8 C1 99 B5 82 2D 95 01 06 27 F6 43 4A B8 04 26 E5 F8 68 93 2B 7F 38 28 4A D3 33 5C 12 DE 5F A0 CB EA 44 F1 34 15 3E F4 CE 08 31 F8 1D 9B 57 02 78 E4 04 21 C4 11 12 12 F3 9B 8B 10 69 AF F0 4E F4 12 3A EE 2D E2 B4 E5 34 15 15 D2 DE E4 A7 C0 12 A0 88 B0 99 58 E5 CF 70 EB 25 AC 56 87 8B E5 1C 9F A1 D5 55 B6 B6 3F BA 1E 3C 6B A1 8C CF 00 0F C4 C9 68 9D 2E 98 FA B0 79 71 0D 1B AF FC AE C9 EB F8 E3 DB 03 72 62 85 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Analysis Process: conhost.exe PID: **8036**, Parent PID: **8072**

General

Target ID:	1
Start time:	15:16:53
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a8820000
File size:	885760 bytes
MD5 hash:	C5E9B1D1103EDCEA2E408E9497A5A88F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **7756**, Parent PID: **8072**

General

Target ID:	6
Start time:	15:16:55
Start date:	14/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /c vssadmin.exe delete shadows /all /quiet
Imagebase:	0x7ff70ecc0000
File size:	280064 bytes
MD5 hash:	9D59442313565C2E0860B88BF32B2277
Has elevated privileges:	true

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7980**, Parent PID: **7756**

General

Target ID:	7
Start time:	15:16:56
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a8820000
File size:	885760 bytes
MD5 hash:	C5E9B1D1103EDCEA2E408E9497A5A88F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: vssadmin.exe PID: **8152**, Parent PID: **7756**

General

Target ID:	8
Start time:	15:16:56
Start date:	14/05/2022
Path:	C:\Windows\System32\vssadmin.exe
Wow64 process (32bit):	false
Commandline:	vssadmin.exe delete shadows /all /quiet
Imagebase:	0x7ff713280000
File size:	144384 bytes
MD5 hash:	02A10DBF904883B1F8EE9F3CC70F5EB8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly