ID: 230133
Sample Name: Locky
Cookbook: default.jbs
Time: 08:23:38
Date: 14/05/2020
Version: 28.0.0 Lapis Lazuli

Table of Contents

Analysis Report Locky

Overview

General Information

Joe Sandbox Version:	28.0.0 Lapis Lazuli
Analysis ID:	230133
Start date:	14.05.2020
Start time:	08:23:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Locky (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	8
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:	mal68.rans.winEXE@2/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.5% (good quality ratio 1.3%) • Quality average: 69.8% • Quality standard deviation: 37.5%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): WerFault.exe, MusNotifyIcon.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 8.248.147.254, 67.27.159.126, 8.253.204.249, 8.248.133.254, 67.26.81.254, 2.18.68.82, 51.104.136.2, 40.127.240.158, 52.158.208.111 • Excluded domains from analysis (whitelisted): umwatson.trafficmanager.net, fs.microsoft.com, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, settingsfd-geo.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

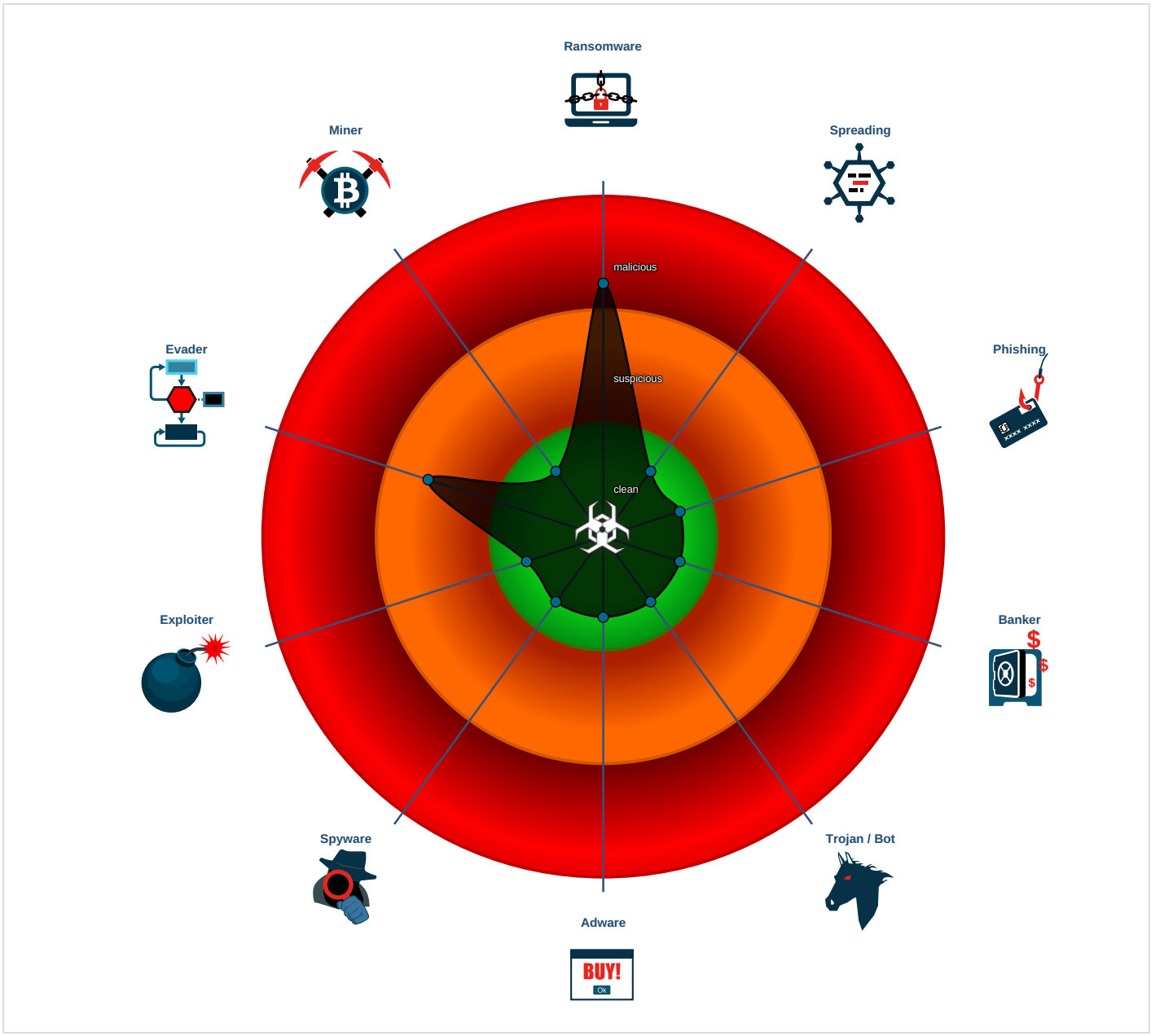
Detection

Strategy	Score	Range	Reporting	Whitelisted	Threat	Detection
Threshold	68	0 - 100		**false**	Locky	MALICIOUS SUSPICIOUS CLEAN UNKNOWN

Confidence

Strategy	Score	Range	Further Analysis Required?	Confidence
Threshold	5	0 - 5	false	99% 80% 60% 40% 20% 5%

Classification Spiderchart



Analysis Advice

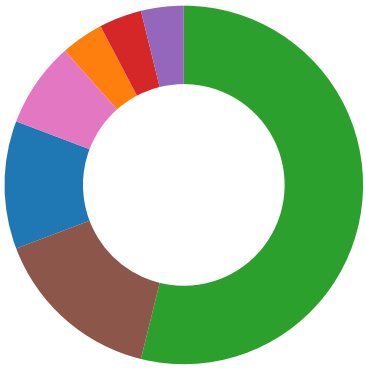
Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Remote Management	Winlogon Helper DLL	Process Injection 1	Masquerading 1 1	Credential Dumping	Virtualization/Sandbox Evasion 2	Application Deployment Software	Data from Local System	Data Encrypted 1	Standard Cryptographic Protocol 1	Eavesdrop o Insecure Network Communicat
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Virtualization/Sandbox Evasion 2	Network Sniffing	Process Discovery 1	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Fallback Channels	Exploit SS7 Redirect Pho Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Process Injection 1	Input Capture	Security Software Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptographic Protocol	Exploit SS7 Track Device Location
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	DLL Side-Loading 1	Credentials in Files	System Information Discovery 1 1	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Card Swap
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Obfuscated Files or Information 1	Account Manipulation	Remote System Discovery 1	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	Manipulate Device Communicat

Signature Overview



- AV Detection
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging

Click to jump to signature section

AV Detection:

Antivirus detection for sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Locky ransomware

System Summary:

Creates files inside the system directory

Detected potential crypto function

One or more processes crash

Sample file is different than original file name gathered from version info

Tries to load missing DLLs

Classification label

Creates files inside the user directory

Creates mutexes

Creates temporary files

PE file has an executable .text section and no other executable section

Reads software policies

Reads the hosts file

Sample is known by Antivirus

Spawns processes

Data Obfuscation:

Uses code obfuscation techniques (call, push, ret)

Hooking and other Techniques for Hiding and Protection:

Disables application error messsages (SetErrorMode)

Malware Analysis System Evasion:

May sleep (evasive loops) to hinder dynamic analysis

Queries disk information (often used to detect virtual machines)

Sample execution stops while process was sleeping (likely an evasion)

Queries a list of all running processes

Anti Debugging:

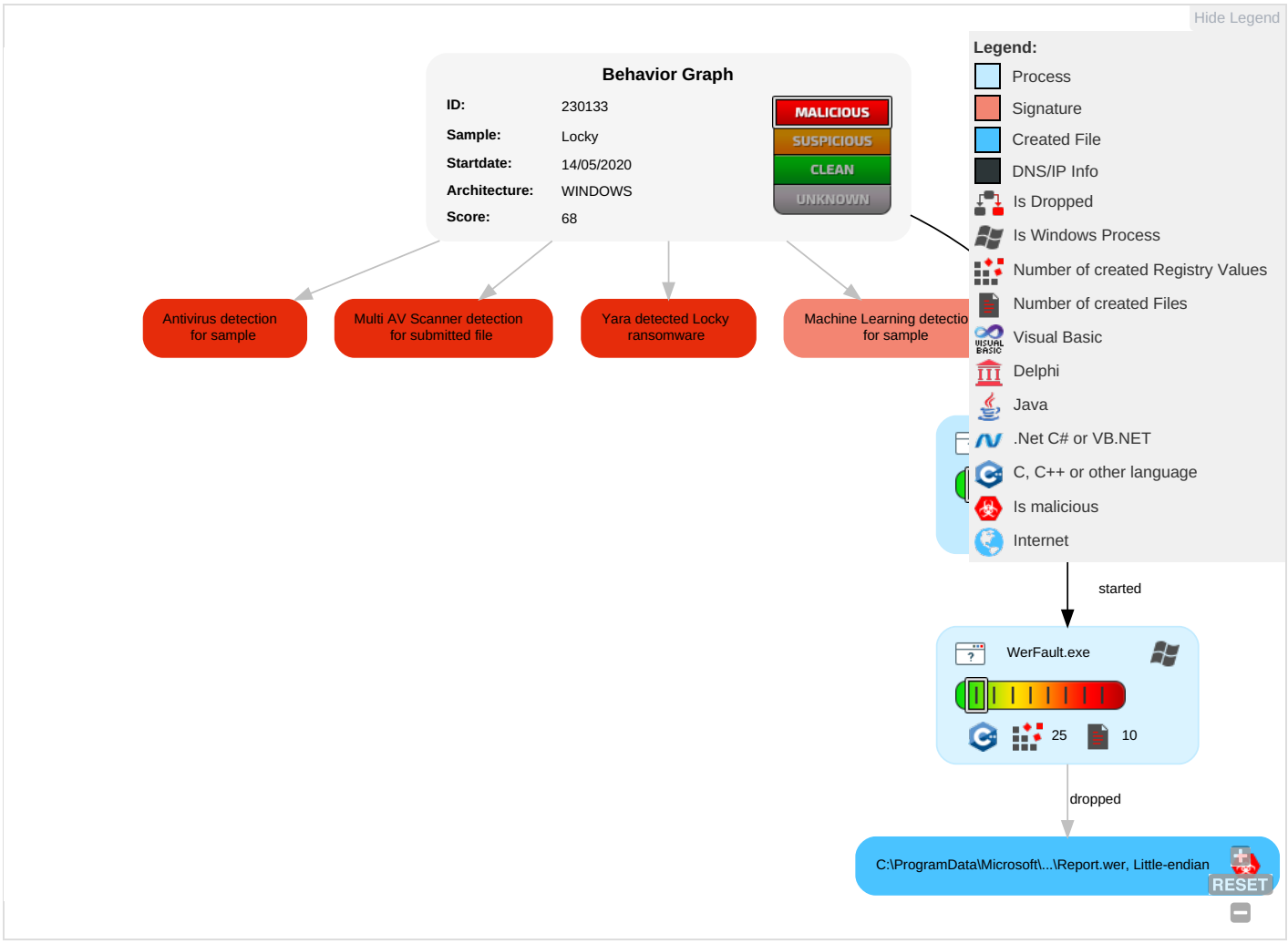
Contains functionality to read the PEB

Enables debug privileges

Malware Configuration

No configs have been found

Behavior Graph



Simulations

Behavior and APIs

Time	Type	Description
08:24:09	API Interceptor	690x Sleep call for process: Locky.exe modified
08:25:38	API Interceptor	1x Sleep call for process: WerFault.exe modified

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Locky.exe	94%	Virustotal		Browse
Locky.exe	90%	Metadefender		Browse
Locky.exe	96%	ReversingLabs	Win32.Trojan.Locky	
Locky.exe	100%	Avira	TR/Agent.53465	
Locky.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Locky.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1034763		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.Locky.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1034763		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Locky.exe	JoeSecurity_Locky_ransomware	Yara detected Locky ransomware	Joe Security	

PCAP (Network Traffic)

No yara matches

Dropped Files

No yara matches

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Locky.exe PID: 2320	JoeSecurity_Locky_ransomware	Yara detected Locky ransomware	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Locky.exe.400000.0.unpack	JoeSecurity_Locky_ransomware	Yara detected Locky ransomware	Joe Security	
0.0.Locky.exe.400000.0.unpack	JoeSecurity_Locky_ransomware	Yara detected Locky ransomware	Joe Security	

Sigma Overview

No Sigma rule has matched

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

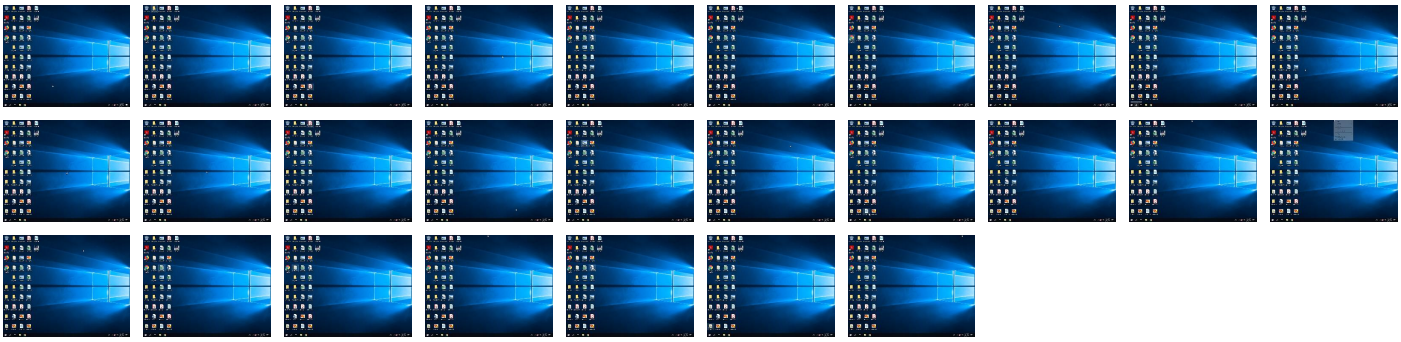
Dropped Files

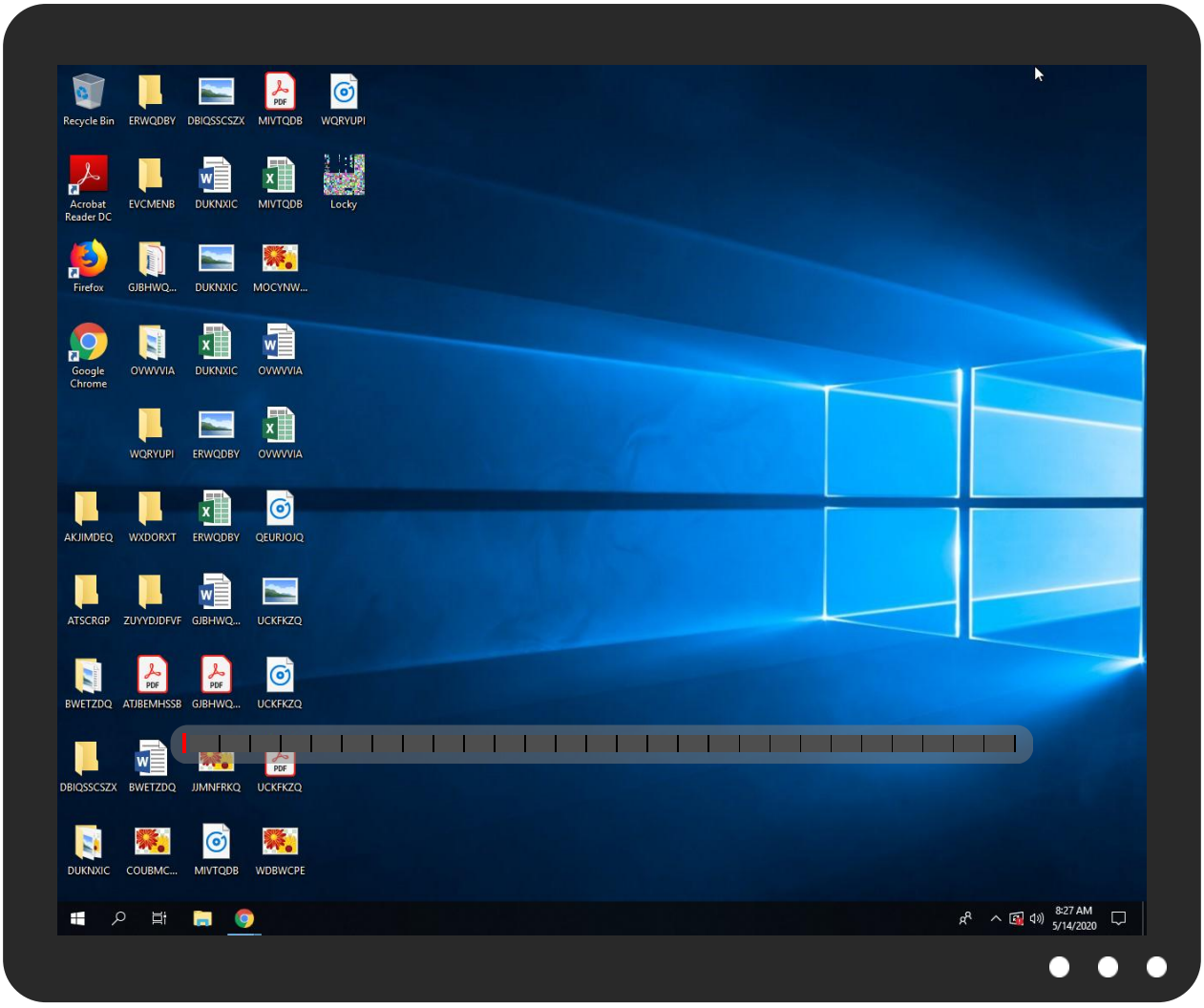
No context

Screenshots

Thumbnails

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





[redacted]

Startup

- **System is w10x64**
- Locky.exe (PID: 2320 cmdline: 'C:\Users\user\Desktop\Locky.exe' MD5: B06D9DD17C69ED2AE75D9E40B2631B42)
  - WerFault.exe (PID: 5524 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2320 -s 452 MD5: 80E91E3C0F5563E4049B62FCAF5D67AC)
- **cleanup**

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Locky.exe_cf7f314a41a72ba64d6a344af1e178bf365a56b_073a1385_15c6737b\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Size (bytes):	9494
Entropy (8bit):	3.7737750687541154
Encrypted:	false
MD5:	B651CDA17856DA50A0B203ED3149C982
SHA1:	B98D4546839859460C098C937846634FCB228FA9
SHA-256:	DC10767D63D435BCD2DC586E3BEF835CFCA7297BDBF11DD5107B2202A847EC90
SHA-512:	E8FB0391E2FC239366C5267531C292345830FBFA3BCFA732C7821CA033EE105D0047BA8469C30141DAB574354FFE15BCC51F9D91D5260247C451F8196F29827D
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.3.3.9.1.1.1.3.4.6.2.8.6.4.5.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.3.3.9.1.1.1.3.7.3.7.3.2.8.6.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.0.0.b.7.8.3.7.-.c.c.8.9.-.4.d.7.3.-.a.0.4.0.-.d.a.8.5.2.1.2.2.8.9.6.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.3.5.0.0.f.b.6.-.3.6.7.0.-.4.c.c.d.-.a.4.7.7.-.1.5.7.d.5.b.4.8.2.7.2.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.L.o.c.k.y...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.9.1.0.-.0.0.0.1.-.0.0.2.3.-.1.1.d.0.-.4.3.4.6.b.8.2.9.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.2.7.2.2.a.5.4.c.1.b.a.3.3.6.3.9.f.7.c.c.2.3.c.3.9.d.f.9.d.f.6.5.0.0.0.0.f.f.f.f.!.0.0.0.0.b.6.0.6.a.a.a.4.0.2.b.f.e.4.a.1.5.e.f.8.0.1.6.5.e.9.6.4.d.3.8.4.f.2.5.5.6.4.e.4.!.L.o.c.k.y...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 14 06:25:35 2020, 0x1205a4 type
Size (bytes):	1064228
Entropy (8bit):	1.8590230819487539
Encrypted:	false
MD5:	576E5C4F95B3AA233B373DF059BAF30C
SHA1:	7F6AD8A030007731BD5E655D575513E10F48FFDC
SHA-256:	B75A927039F60FA20C06B24C45CD2A77F1F9FF71D22CE02F5DB4289FF5115E96
SHA-512:	8BD665405AF5058804B80BEBE8309944C72EA48474BA8F0CDA22F36FEEF18FBF3DC072B4F195DFA81AE1FD5EA3C6440538977EE1B62B9FEC575667C28597695
Malicious:	false
Reputation:	low
Preview:	MDMP..... ....._.^.....?.....B.....x.....GenuineIntel.....T.....^.....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Size (bytes):	8296
Entropy (8bit):	3.6999155957209426
Encrypted:	false
MD5:	3E30F3CB3E507E67C56838067E44B2D9
SHA1:	3BD55A4D0C05EC684DED3F10A25DC975A6A4CF6A
SHA-256:	EAC93A44CCF5DCA4B850F37252E13FD4F0D81D6A2017FE82DB877823295D29D3
SHA-512:	C27F6A20AC26EAEC00C1FF2CD348E3942F15FD24C90C42257B4848E23C633023A86391758BE4459CC7C3EDD0B7DE6337E735C31D20373E2E2E427B5939B1D12
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1.6.5...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.3.2.0.<./.P.i.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6DEF.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Size (bytes):	4509
Entropy (8bit):	4.4695697308623625
Encrypted:	false
MD5:	FEC9F820D686D9CBD4DB6E69F88D752D
SHA1:	9E1E33DB3F2C2CAAEF8EF8983A329704F35D67F5
SHA-256:	6E98BE6D5546E6D75A6A24802F702ABB2396D208AEC578139650AF5D95031AB5
SHA-512:	6A41FB602918A17308B548297F27D384DEDCB0B2686DCCB2643F2DE4C8FAA8C75AED6D51511C9BFAB65F401EBEBC04306605F49908EFEE81DDE6A0A9C0D40734
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="165" />.. <arg nm="verqfe" val="165" />.. <arg nm="csdbld" val="165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="967522" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.165.17134.0-11.0.75" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="2048" />

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.774164647726848
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Locky.exe
File size:	184320
MD5:	b06d9dd17c69ed2ae75d9e40b2631b42
SHA1:	b606aaa402bfe4a15ef80165e964d384f25564e4
SHA256:	bc98c8b22461a2c2631b2feec399208fdc4ecd1cd2229066c2f385caa958daa3
SHA512:	8e54aca4feb51611142c1f2bf303200113604013c2603eea22d72d00297cb1cb40a2ef11f5129989cd14f90e495db79bffd15bd6282ff564c4af7975b1610c1c
SSDEEP:	3072:gzWgfLlUc7CIJ1tkZaQyjhOosc8MKi6KDXnLCtyAR0u1cZ86:gdLl4wkZa/UDiD7ukst1H6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R...3`..3`..3`.r,j..3`../n..3`.r,d..3`..3a..3`..,s..3`..3`..3`.r,k..3`."5f..3`.Rich.3`.....PE..L....>.B.....

File Icon

Icon Hash:	0b03039bb7b199ab

Static PE Info

General

Entrypoint:	0x40c0dc
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x42B63E17 [Mon Jun 20 03:55:03 2005 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	0fcea3af550ad0a893e93808dccf17f4

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 0040D2C8h
push 00407625h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 68h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
xor ebx, ebx
mov dword ptr [ebp-04h], ebx
push 00000002h
call dword ptr [00400D74h]
pop ecx
or dword ptr [007B67E8h], FFFFFFFFh
or dword ptr [007B67ECh], FFFFFFFFh
call dword ptr [0040D0FCh]
mov ecx, dword ptr [007B67E4h]
mov dword ptr [eax], ecx
call dword ptr [0040D0E8h]
mov ecx, dword ptr [007B67E0h]
mov dword ptr [eax], ecx
mov eax, dword ptr [0040D104h]
mov eax, dword ptr [eax]
mov dword ptr [007B67F0h], eax
call 00007F34985B2515h
cmp dword ptr [004127B0h], ebx
jne 00007F34985B240Eh
push 0040C258h
call dword ptr [0040D108h]

Instruction
pop ecx
call 00007F34985B24E7h
push 0040F00Ch
push 0040F008h
call 00007F34985B24D2h
mov eax, dword ptr [007B67DCh]
mov dword ptr [ebp-6Ch], eax
lea eax, dword ptr [ebp-6Ch]
push eax
push dword ptr [007B67D8h]
lea eax, dword ptr [ebp-64h]
push eax
lea eax, dword ptr [ebp-70h]
push eax
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [0040D110h]
push 0040F004h
push 0040F000h
call 00007F34985B249Fh

Rich Headers

Programming Language:	• [C] VS98 (6.0) build 8168 • [RES] VS98 (6.0) cvtres build 1720 • [C++] VS98 (6.0) build 8168 • [LNK] VS98 (6.0) imp/exp build 8168

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd2d4	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b7000	0x190c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd000	0x270	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb2cc	0xc000	False	0.669230143229	data	6.53694188411	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x10c2	0x2000	False	0.255859375	data	3.3412568532	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xf000	0x3a77f4	0x4000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x3b7000	0x190c8	0x1a000	False	0.797964242788	data	7.04430456199	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b8df0	0xb2d	data		
RT_ICON	0x3b9630	0xb90	data		
RT_ICON	0x3b9e70	0xaeb	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ba6b0	0x94c	data		
RT_MENU	0x3b7b28	0x4e	data		
RT_MENU	0x3b7b78	0x21e	data		
RT_DIALOG	0x3b7d98	0x162	data		
RT_DIALOG	0x3b7f00	0x192	data		
RT_DIALOG	0x3b8098	0x17e	data		
RT_DIALOG	0x3b8218	0xee	data		
RT_DIALOG	0x3b8308	0xb8	data		
RT_DIALOG	0x3b83c0	0x180	data		
RT_DIALOG	0x3b8540	0x96	data		
RT_DIALOG	0x3b85d8	0x128	data		
RT_DIALOG	0x3b8700	0x1b6	data		
RT_DIALOG	0x3b88b8	0xb8	data		
RT_DIALOG	0x3b8970	0xb0	data		
RT_DIALOG	0x3b8a20	0x172	data		
RT_DIALOG	0x3b8b98	0xfc	data		
RT_DIALOG	0x3b8c98	0x152	data		
RT_ACCELERATOR	0x3baf18	0x18	data		
RT_ACCELERATOR	0x3baf30	0x20	data		
RT_ACCELERATOR	0x3baf50	0x20	data		
RT_ACCELERATOR	0x3baf70	0x48	data		
RT_ACCELERATOR	0x3bafb8	0x60	data		
RT_ACCELERATOR	0x3bb018	0x30	data		
RT_ACCELERATOR	0x3bb048	0x68	data		
RT_ACCELERATOR	0x3bb0b0	0x40	data		
RT_ACCELERATOR	0x3bb0f0	0x40	data		
RT_ACCELERATOR	0x3bb130	0x28	data		
None	0x3baef0	0x5	data		
None	0x3bb158	0x121d5	data		
None	0x3cd330	0x2d96	data		
None	0x3baf10	0x1	very short file (no magic)		
None	0x3baef8	0x12	data		
RT_GROUP_ICON	0x3b9618	0x14	data		
RT_GROUP_ICON	0x3b9e58	0x14	data		
RT_GROUP_ICON	0x3ba698	0x14	data		
RT_GROUP_ICON	0x3baed8	0x14	data		
RT_VERSION	0x3b7840	0x2e8	data		

Imports

DLL	Import
ADVAPI32.dll	GetSecurityDescriptorDacl, RegisterEventSourceA, RegQueryInfoKeyA, GetSidSubAuthorityCount, RegSetValueExA, RegDeleteKeyA, GetKernelObjectSecurity, RegCloseKey, RegQueryValueA, RegLoadKeyA, GetSidSubAuthority, RegConnectRegistryA, LookupPrivilegeValueA, InitiateSystemShutdownA, CreateProcessAsUserA, GetSidIdentifierAuthority, OpenThreadToken, LsaQueryInformationPolicy, RegQueryValueW, EncryptFileW, RegSetValueW, MakeAbsoluteSD, RegOpenKeyExA, RegCreateKeyExW, AddAce, SetNamedSecurityInfoW, OpenEventLogW, GetUserNameW, SetSecurityDescriptorSacl, MakeSelfRelativeSD, RegFlushKey, InitializeSecurityDescriptor, InitializeAcl, SetEntriesInAclA, GetSidLengthRequired, RegSetValueA, SetEntriesInAclW, GetAclInformation
USER32.dll	DrawIconEx, IsDialogMessageA, OffsetRect, PostThreadMessageW, DialogBoxParamA, GetLastActivePopup, GetGUIThreadInfo, DrawStateA, IsWindow, OpenClipboard, InSendMessage, FindWindowW, IsMenu, EnumDisplaySettingsA, DrawAnimatedRects, FrameRect, SetMenuDefaultItem, GrayStringW, CreateDialogIndirectParamW, ClientToScreen, GetParent, TranslateMDISysAccel, CreateDesktopW, ShowCaret, GetProcessWindowStation, TrackPopupMenu, IntersectRect, DialogBoxIndirectParamA, DefWindowProcA, ReuseDDElParam, NotifyWinEvent, SetClipboardData, CloseClipboard, DdeDisconnect, GetClassNameA, GetCaretPos, CharLowerW, GetWindowModuleFileNameA, IsWindowVisible, wvsprintfA, ModifyMenuA, SendDlgItemMessageW, SetCaretBlinkTime, LoadMenuW, GetMenuState, DrawTextExA, ChangeDisplaySettingsW, CreateWindowExW, GetCapture, CreatePopupMenu, SetMenu, CharUpperBuffW, DrawStateW, LoadImageA, GetScrollPos, GetDlgItem, GetClipboardFormatNameW, ValidateRgn, GetWindowThreadProcessId, GetClassInfoExW, DdeAccessData, ShowWindow, GetKeyboardLayout, GetClassInfoW, SetCaretPos, LoadCursorA, FillRect, LoadMenuA, mouse_event, ModifyMenuW, InvalidateRgn, GetMenuItemID, IsIconic, OemToCharA, LoadCursorFromFileW, RegisterWindowMessageA, DispatchMessageW, GetCursorPos, CharPrevA, GetWindowWord
IMM32.dll	ImmGetProperty, ImmGetCandidateListCountA, ImmGetCompositionStringA, ImmSetConversionStatus, ImmSetOpenStatus, ImmCreateContext, ImmGetOpenStatus, ImmNotifyIME, ImmInstallIMEA, ImmGetContext, ImmDestroyContext, ImmSimulateHotKey, ImmConfigureIMEA, ImmAssociateContext
RASAPI32.dll	RasDialA, RasGetProjectionInfoA
KERNEL32.dll	WriteFileGather, PulseEvent, GetLongPathNameA

Version Infos

Description	Data
LegalCopyright	Intend (C) 2013
InternalName	
FileVersion	0.37.213.27
CompanyName	FileSee.com
PrivateBuild	
LegalTrademarks	
Comments	
ProductName	Lipreading Fenced
SpecialBuild	
ProductVersion	0.144.212.113
FileDescription	
OriginalFilename	

Network Behavior

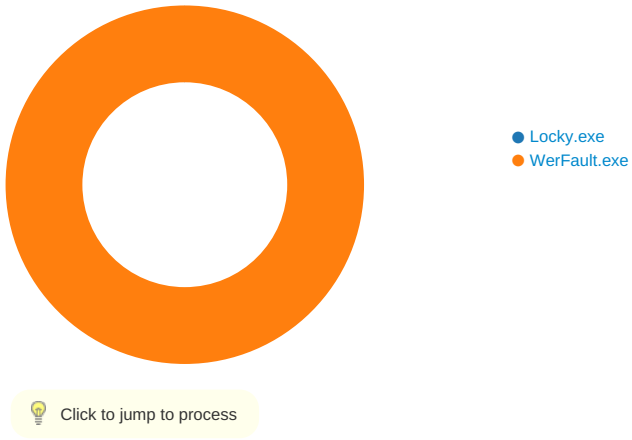
UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2020 08:24:43.915163040 CEST	49971	53	192.168.2.6	8.8.8.8
May 14, 2020 08:24:43.940545082 CEST	53	49971	8.8.8.8	192.168.2.6
May 14, 2020 08:25:00.766048908 CEST	61139	53	192.168.2.6	8.8.8.8
May 14, 2020 08:25:00.811672926 CEST	53	61139	8.8.8.8	192.168.2.6
May 14, 2020 08:25:03.822190046 CEST	58139	53	192.168.2.6	8.8.8.8
May 14, 2020 08:25:03.872055054 CEST	53	58139	8.8.8.8	192.168.2.6
May 14, 2020 08:25:04.469990015 CEST	57653	53	192.168.2.6	8.8.8.8
May 14, 2020 08:25:04.531723976 CEST	53	57653	8.8.8.8	192.168.2.6
May 14, 2020 08:25:04.860331059 CEST	61083	53	192.168.2.6	8.8.8.8
May 14, 2020 08:25:04.893973112 CEST	53	61083	8.8.8.8	192.168.2.6
May 14, 2020 08:25:05.077032089 CEST	61122	53	192.168.2.6	8.8.8.8
May 14, 2020 08:25:05.125576019 CEST	53	61122	8.8.8.8	192.168.2.6
May 14, 2020 08:25:37.817317963 CEST	50558	53	192.168.2.6	8.8.8.8
May 14, 2020 08:25:37.842662096 CEST	53	50558	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Locky.exe PID: 2320 Parent PID: 1108

General

Start time:	08:24:08
Start date:	14/05/2020
Path:	C:\Users\user\Desktop\Locky.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Locky.exe'
Imagebase:	0x400000
File size:	184320 bytes
MD5 hash:	B06D9DD17C69ED2AE75D9E40B2631B42
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 5524 Parent PID: 2320

General

Start time:	08:25:33
Start date:	14/05/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2320 -s 452
Imagebase:	0x2c0000
File size:	434584 bytes
MD5 hash:	80E91E3C0F5563E4049B62FCAF5D67AC
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72481717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7247497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6DEF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6DEF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Locky.exe_cf7f314a41a72ba64d6a344af1e178bf365a56b_073a1385_15c6737b	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Locky.exe_cf7f314a41a72ba64d6a344af1e178bf365a56b_073a1385_15c6737b\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7247497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6DEF.tmp	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	success or wait	1	72474BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	success or wait	1	72474BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6DEF.tmp.xml	success or wait	1	72474BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E1C.tmp.csv	success or wait	1	72474BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F46.tmp.txt	success or wait	1	72474BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 00 5f e4 bc 5e a4 05 12 00 00 00 00 00	MDMP..... ....._..^.....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	1420	00 00 06 00 02 3f 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 78 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c f2 06 03 00 ff fb 8b 17 00 00 00 00 54 05 00 00 f7 03 00 00 10 09 00 00 08 e4 bc 5e 00 00 00 00 00 00 00 00 a4 0d 00 00 a4 0d 00 00 a4 0d 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....?...........B......x..... ..GenuineIntel............T... ....^.................. ....0..2...............W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e............... ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 06 00 00 00 40 2a a2 00 c0 8c a2 00 00 00 00 00 00 2b a2 00 11 00 00 00 04 10 0a 00 27 6c a0 76 23 00 00 00 46 02 01 00 00 10 0a 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+.......@*...........+...... ....'l.v#...F.......+.........	success or wait	1	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	168	a4 13 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 27 6c a0 76 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fc 0f 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 14 16 00 00	........................'l.v..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	20	0b 00 00 00 00 10 3b 00 00 00 00 00 98 04 00 00 60 1c 00 00	......;.........`...	success or wait	11	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	1176	00 00 00 00 ff ff ff ff 00 00 40 00 a0 7b 36 77 f8 16 94 00 00 00 00 00 00 00 00 94 00 a0 79 36 77 00 00 00 00 00 00 00 00 01 00 00 00 00 10 b5 75 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 f8 7b 36 77 1f 00 01 00 00 00 00 00 00 00 e6 7f 00 00 00 00 30 07 e6 7f 00 00 fb 7f 28 02 fc 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 00 01 00 00 10 00 00 02 00 00 00 10 00 00 00 60 66 36 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 36 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..........@..{6w.............y 6w...............u................. {6w................0....... (...P...................m........ ....`f6w.. ....PS6w.........B......	success or wait	10	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	524288	00 00 00 00 ec 10 0a 00 41 51 b0 76 aa aa aa aa aa aa aa aa 40 2a a2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 40 2a a2 00 1f 51 b0 76 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 0c 00 00 00 aa aa aa aa 60 11 0a 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa 48 01 00 00 4c 11 0a 00 61 cd b0 76 00 00 00 00 aa aa aa aa aa aa aa	........AQ.v........@*........ ....@*...Q.v.. ....`... ....H...L... a..v...........	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	4	fc 13 af 76	...v	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	4	01 00 00 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa 40 2a a2 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 04 10 0a 00 27 6c a0 76 23 00 00 00 46 02 01 00 00 10 0a 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......@*................. ....'l.v#...F.......+.........	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	48	a4 13 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 40 3b 00 00 00 00 00 00 10 0a 00 00 00 00 00 00 f0 0f 00 0c 31 00 00 cc 02 00 00 e0 18 00 00	....@;........... ....1..........	success or wait	1	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	4	17 00 00 00	....	success or wait	23	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	24	12 00 00 00 4c 00 6f 00 63 00 6b 00 79 00 2e 00 65 00 78 00 65 00 00 00	....L.o.c.k.y...e.x.e...	success or wait	23	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	752	00 00 a9 73 00 00 00 00 00 10 01 00 b7 38 01 00 31 45 53 6e f8 15 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 8d ff 07 00 01 00 00 00 ef ff 07 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 90 3f 02 00 00 00 00 00 20 18 03 00 00 00 00 fb d6 0e 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 ca 93 03 00 00 00 00 00 d0 fa 04 00 00 00 00 00 31 0e 08 00 00 00 00 00 f0 91 1b 00 00 00 00 00 50 6d 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 15 4a 06 00 00 00 00	...s.....8..1ESn..... .....B.....B?..... .....$..... ..@A.....Zb..... ....?..... ....1.....Pm..... @.....J.....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	7000	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64D5.tmp.dmp	unknown	108	03 00 00 00 34 00 00 00 fc 06 00 00 04 00 00 00 b8 09 00 00 3c 07 00 00 05 00 00 00 b4 00 00 00 ac 1b 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 b8 11 00 00 b4 2b 10 00 15 00 00 00 ec 01 00 00 f4 10 00 00 16 00 00 00 98 00 00 00 e0 12 00 00	....4.....<..... .....T.....8..... ....T.....+.....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	138	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 36 00 35 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1.6.5...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	48	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 36 00 35 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.6.5.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 33 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.3.2.0.<./.P.i.d.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	64	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4c 00 6f 00 63 00 6b 00 79 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.L.o.c.k.y...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 38 00 35 00 30 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.8.8.5.0.7.<./.U.p.t.i.m.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 36 00 34 00 36 00 36 00 37 00 36 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.6.4.6.6.7.6.4.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 36 00 34 00 36 00 36 00 33 00 35 00 35 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.6.4.6.6.3.5.5.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 34 00 37 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.4.7.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 38 00 38 00 32 00 39 00 33 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.8.8.2.9.3.1.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 38 00 38 00 32 00 39 00 33 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.8.8.2.9.3.1.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.6.4.5.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 32 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.6.2.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 30 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.1.0.5.6.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 30 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.1.0.4.3.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 31 00 37 00 33 00 39 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.8.1.7.3.9.5.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 31 00 37 00 38 00 30 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.8.1.7.8.0.4.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 31 00 37 00 33 00 39 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.8.1.7.3.9.5.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 38 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.8.6.4.<./.P.i.d.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 30 00 31 00 30 00 36 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.4.0.1.0.6.7.<./.U.p.t.i.m.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4..g.u.e.s.t.=.".0.".h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 37 00 31 00 37 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.7.7.1.7.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 34 00 37 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.9.4.7.9.5.5.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 39 00 39 00 38 00 35 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.4.9.9.8.5.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 33 00 31 00 38 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.3.1.8.2.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 35 00 35 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.8.5.5.8.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 33 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.8.3.2.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.0.6.4.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 36 00 34 00 34 00 35 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.3.6.4.4.5.4.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 36 00 34 00 32 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.6.4.2.2.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 36 00 34 00 34 00 35 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.3.6.4.4.5.4.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	68	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 4c 00 6f 00 63 00 6b 00 79 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.L.o.c.k.y...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 45 00 33 00 38 00 42 00 36 00 30 00 42 00 33 00 2d 00 35 00 46 00 46 00 41 00 2d 00 34 00 46 00 38 00 38 00 2d 00 41 00 41 00 35 00 38 00 2d 00 43 00 44 00 44 00 34 00 39 00 37 00 45 00 37 00 43 00 42 00 32 00 32 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.E.3.8.B.6.0.B.3.-.5.F.F.A.-.4.F.8.8.-.A.A.5.8.-.C.D.D.4.9.7.E.7.C.B.2.2.<./.M.I.D.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 78 00 67 00 75 00 66 00 66 00 73 00 6a 00 20 00 47 00 6d 00 62 00 48 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.x.g.u.f.f.s.j. .G.m.b.H.<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	98	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 79 00 6f 00 6a 00 63 00 68 00 78 00 71 00 70 00 66 00 72 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.y.o.j.c.h.x.q.p.f.r.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	74	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 79 00 6f 00 6a 00 63 00 68 00 78 00 71 00 70 00 66 00 72 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.y.o.j.c.h.x.q.p.f.r.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 30 00 37 00 39 00 32 00 35 00 30 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.0.7.9.2.5.0.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 38 00 2d 00 30 00 37 00 2d 00 31 00 32 00 54 00 30 00 39 00 3a 00 30 00 32 00 3a 00 35 00 36 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.8.-.0.7.-.1.2.T.0.9.:.0.2.:.5.6.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	114	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 4e 00 6f 00 74 00 43 00 61 00 70 00 61 00 62 00 6c 00 65 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.N.o.t.C.a.p.a.b.l.e.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.8.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 30 00 2d 00 30 00 35 00 2d 00 31 00 34 00 54 00 30 00 36 00 3a 00 32 00 35 00 3a 00 33 00 36 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.0.-.0.5.-.1.4.T.0.6.:.2.5.:.3.6.Z.".>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 38 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 33 00 32 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 34 00 30 00 33 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 38 00 34 00 30 00 33 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".4.8.5.". .P.I.D.=.".2.3.2.0.". .U.p.t.i.m.e.M.S.=.".8.4.0.3.0.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".8.4.0.3.0.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 30 00 30 00 62 00 37 00 38 00 33 00 37 00 2d 00 63 00 63 00 38 00 39 00 2d 00 34 00 64 00 37 00 33 00 2d 00 61 00 30 00 34 00 30 00 2d 00 64 00 61 00 38 00 35 00 32 00 31 00 32 00 32 00 38 00 39 00 36 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.5.0.0.b.7.8.3.7.-.c.c.8.9.-.4.d.7.3.-.a.0.4.0.-.d.a.8.5.2.1.2.2.8.9.6.0.<./.G.u.i.d.>.	success or wait	1	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 30 00 2d 00 30 00 35 00 2d 00 31 00 34 00 54 00 30 00 36 00 3a 00 32 00 35 00 3a 00 33 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.0.-.0.5.-.1.4.T.0.6.:.2.5.:.3.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D52.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6DEF.tmp.xml	unknown	4509	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Locky.exe_cf7f314a41a72ba64d6a344af1e178bf365a56b_073a1385_15c6737b\Report.wer	unknown	2	ff fe	..	success or wait	1	7247497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Locky.exe_cf7f314a41a72ba64d6a344af1e178bf365a56b_073a1385_15c6737b\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	153	7247497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Locky.exe_cf7f314a41a72ba64d6a344af1e178bf365a56b_073a1385_15c6737b\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 33 00 35 00 35 00 31 00 34 00 33 00 32 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.3.5.5.1.4.3.2.2.	success or wait	1	7247497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\{11517B7C-E79D-4e20-961B-75A811715ADD}	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	success or wait	1	724936BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	72491FB2	RegCreateKeyExW
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	724743D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Windows\AppCompat\Programs\Amcache.hve.tmp!\??\C:\Windows\AppCompat\Programs\Amcache.hve	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile	WritePermissionsCheck	dword	1	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile	ProviderSyncId	unicode	{617a62e3-633c-49fe-8451-0ec50146b859}	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	ProgramId	unicode	00062722a54c1ba33639f7cc23c39df9df650000ffff	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	FileId	unicode	0000b606aaa402bfe4a15ef80165e964d384f25564e4	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	LowerCaseLongPath	unicode	c:\users\user\desktop\locky.exe	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	LongPathHash	unicode	locky.exe|17d11abc	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	Name	unicode	Locky.exe	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	Publisher	unicode	filesee.com	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	Version	unicode	0.37.213.27	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	BinFileVersion	unicode	0.170.16.207	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	BinaryType	unicode	pe32_i386	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	ProductName	unicode	lipreading fenced	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	ProductVersion	unicode	0.144.212.113	success or wait	1	724936BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	LinkDate	unicode	06/20/2005 03:55:03	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	BinProductVersion	unicode	0.195.154.99	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	Size	B	00 D0 02 00 00 00 00 00	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	Language	dword	0	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	IsPeFile	dword	1	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	IsOsComponent	dword	0	success or wait	1	724936BF	unknown
\REGISTRY\A\{a479493a-7265-30cf-0ff1-aa3913fe5e7b}\Root\InventoryApplicationFile\locky.exe|17d11abc	Usn	B	40 AF B8 0A 00 00 00 00	success or wait	1	724936BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 27 6C A0 76 02 00 00 00 01 00 00 00 FC 0F 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	72491FE8	RegSetValueExW

Disassembly

Code Analysis