ID: 385475
Sample Name: scan_doc.exe
Cookbook: default.jbs
Time: 15:17:17
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report scan_doc.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 15
Public 15
Private 15
General Information 15
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 19
ASN 19
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 20
Static File Info 22
General 22
File Icon 22
Static PE Info 22
General 22
Entrypoint Preview 23
Data Directories 24
Sections 24
Resources 25
Imports 25
Version Infos 25
Network Behavior 25
Network Port Distribution 25
TCP Packets 25
UDP Packets 27

DNS Queries 28
DNS Answers 28
HTTP Request Dependency Graph 28
HTTP Packets 29
HTTPS Packets 29
Code Manipulations 29
Statistics 29
Behavior 29
System Behavior 30
Analysis Process: scan_doc.exe PID: 496 Parent PID: 6136 30
General 30
File Activities 30
File Created 30
File Written 30
File Read 31
Registry Activities 32
Analysis Process: WerFault.exe PID: 5972 Parent PID: 496 32
General 32
File Activities 32
File Created 32
File Deleted 33
File Written 33
Registry Activities 55
Key Created 55
Key Value Created 55
Disassembly 56
Code Analysis 56

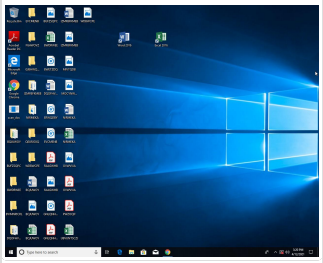
Analysis Report scan_doc.exe

Overview

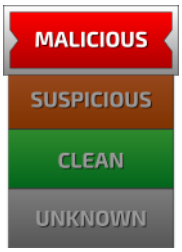
General Information

Sample Name:	scan_doc.exe
Analysis ID:	385475
MD5:	a01c6a3db8e862..
SHA1:	40a1b88e94c926..
SHA256:	29859bac1ca736..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

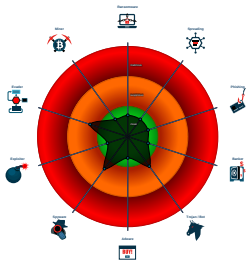


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Binary contains a suspicious time st…
- Checks if the current process is bein…
- Creates a DirectInput object (often fo…
- Enables debug privileges
- HTTP GET or POST without a user …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Monitors certain registry keys / valu…
- One or more processes crash
- Queries the volume information (nam…
- Sample file is different than original …

Classification



Startup

- **System is w10x64**
- scan_doc.exe (PID: 496 cmdline: 'C:\Users\user\Desktop\scan_doc.exe' MD5: A01C6A3DB8E862AB85386B6700E941BB)
  - WerFault.exe (PID: 5972 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 496 -s 1800 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

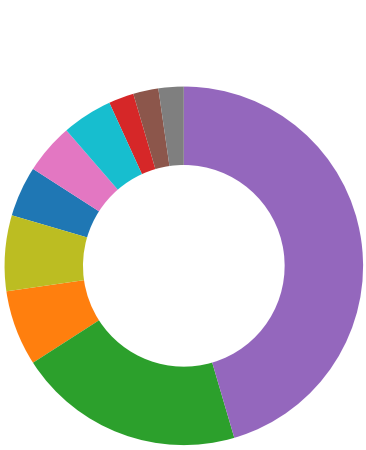
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

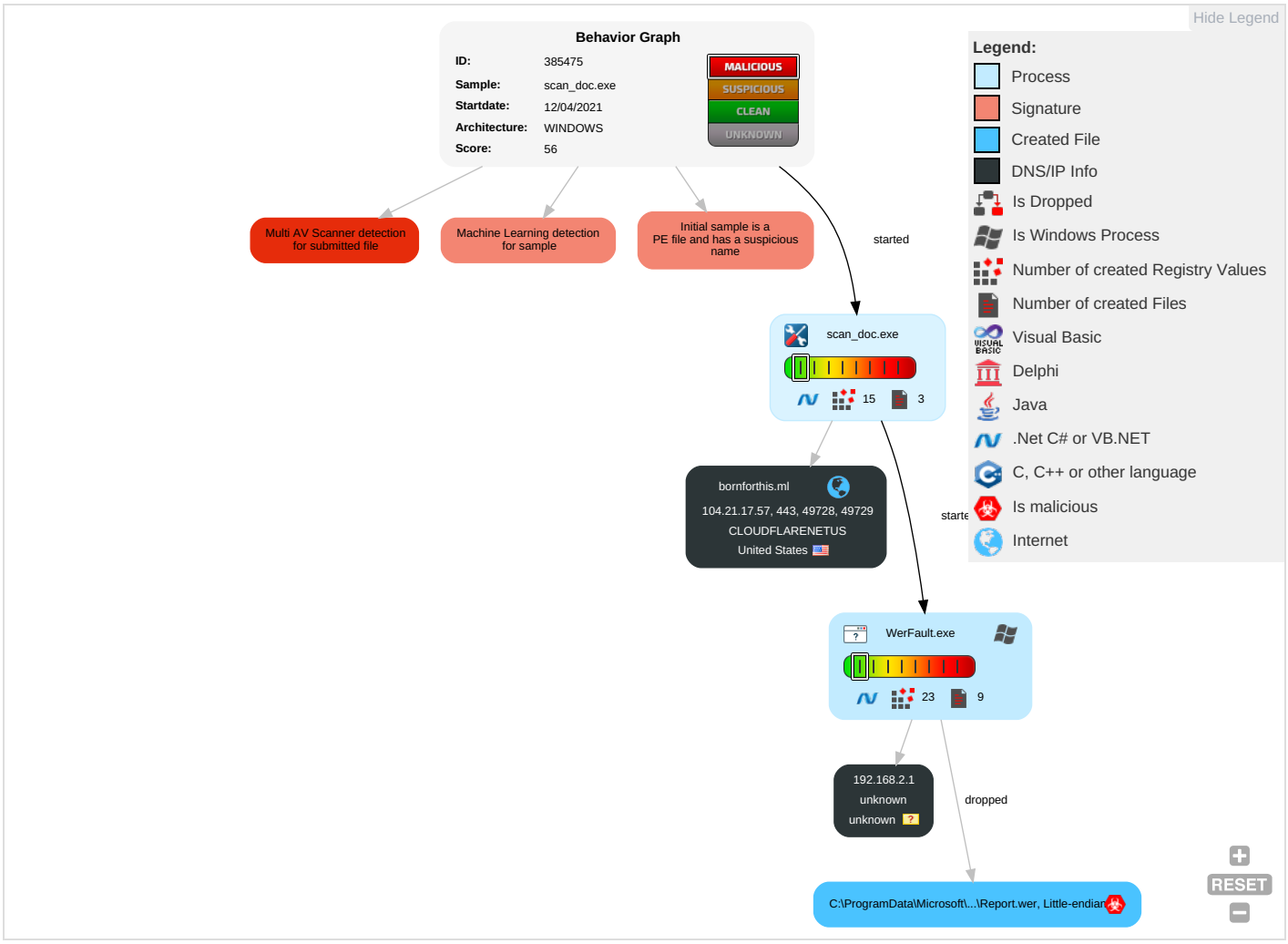
System Summary:

Initial sample is a PE file and has a suspicious name

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remo Servi Effec
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remo Track Witho Autho
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remo Wipe Witho Autho
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtai Devic Cloud Backu
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
scan_doc.exe	26%	Virustotal		Browse
scan_doc.exe	29%	ReversingLabs	Win32.Trojan.Generic	
scan_doc.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bornforthis.ml	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-358	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://reachplc.hub.loginradius.com"	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bornforthis.ml	104.21.17.57	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-358B343CE000A6025E950DB85DC9DF85.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 00000004.00000003.660974058.00000000058D0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-358	scan_doc.exe, 00000000.00000002.745649271.00000000023E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresshttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 00000004.00000003.660974058.00000000058D0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://c.amazon-adsystem.com/aax2/apstag.js	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 00000004.00000003.660974058.00000000058D0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 00000004.00000003.660974058.00000000058D0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 00000004.00000003.660974058.00000000058D0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 00000004.00000003.660974058.00000000058D0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/premier-league	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://schema.org/ImageObject	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 00000004.00000003.660974058.00000000058D0000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

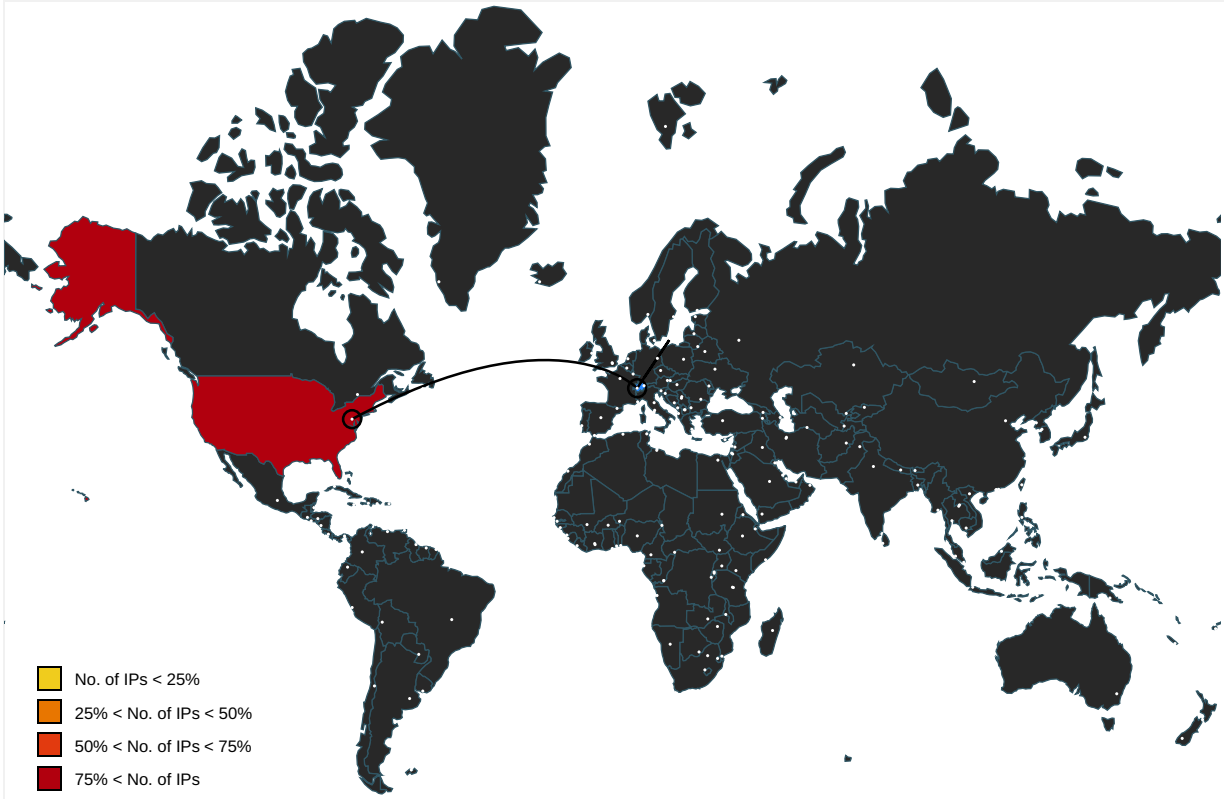
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	scan_doc.exe, 00000000.00000002.745620202.00000000023B1000.00000004.00000001.sdmp, WerFault.exe, 00000004.00000003.660974058.00000000058D0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ads.pubmatic.com/AdServer/js/pwt/156997/3236/pwt.js	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 00000004.00000003.660974058.00000000058D0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://reachplc.hub.loginradius.com"	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.liverpool.com	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com	scan_doc.exe, 00000000.00000003.643965706.00000000033DA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/contact-us/	scan_doc.exe, 00000000.00000002.745712918.0000000002413000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://felix.data.tm-awx.com/felix.min.js	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/corrections-clarifications/	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s270b/0_RobertsonCross1.jpg	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.64396 5706.00000000033DA000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s458/0_GettyImages-1273716690.	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/ozan-kabak	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.64396 5706.00000000033DA000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.mirror.co.uk/	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/privacy-notice/	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-02-	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/champions-league	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/curtis-user	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/terms-conditions/	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/all-about/steven-gerrard	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-ozan-kabak-future-audition-19954616	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://bornforthis.ml	scan_doc.exe, 00000000.0000000 2.745620202.00000000023B1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s458/1_WhatsApp-Image-2021-03-	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-penalties-premier-league-var-17171391	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/NewsArticle	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/BreadcrumbList	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false		high
http://https://securepubads.g.doubleclick.net/tag/js/gpt.js	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false		high
http://https://www.liverpool.com	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s2-prod.liverpool.com/	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-champions-league-jurgen-klopp-1996194	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s220b/0_GettyImages-1231353837	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.64396 5706.00000000033DA000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s458/0_GettyImages-1302496803.	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com/ampconfig.json"	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s615/0_GettyImages-1273716690.	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bornforthis.ml41k	scan_doc.exe, 00000000.0000000 2.745649271.00000000023E5000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s270b/0_Salah-Pressing.jpg	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s615/0_Salah-Goal-vs-Leeds.jpg	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s270b/0_WhatsApp-Image-2021-02	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s220b/0_RobertsonCross1.jpg	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.64396 5706.00000000033DA000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddressz http://schemas.xmlsoap.org/ws/20	WerFault.exe, 00000004.0000000 3.660974058.00000000058D0000.0 0000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-andy-robertson-valuable-quality-19946	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-jurgen-klopp-pressing-tactics-1993836	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s615/0_Salah-Pressing.jpg	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/ListItem	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false		high
http://https://www.liverpool.com/all-about/georginio-wijnaldum	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mab.data.tm-awx.com/rhs"	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s180/0_GettyImages-1231353837.	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.64396 5706.00000000033DA000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/andrew-robertson	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.64396 5706.00000000033DA000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article17166876.ece/ALTERNATES/s615/0_GettyImages-1175998874.	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-gini-wijnaldum-rumours-fitness-199533	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish-199590	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s180/0_GettyImages-1304940818.	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp, scan_doc.exe, 00000000.00000003.64396 5706.00000000033DA000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/cookie-policy/	scan_doc.exe, 00000000.0000000 2.745712918.0000000002413000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/all-about/transfers	scan_doc.exe, 00000000.0000000 3.643965706.00000000033DA000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.17.57	bornforthis.ml	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	385475
Start date:	12.04.2021
Start time:	15:17:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	scan_doc.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
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:	mal56.winEXE@2/5@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 1.1%) • Quality average: 1.2% • Quality standard deviation: 7.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 13.88.21.125, 13.64.90.137, 20.50.102.62, 92.122.213.194, 92.122.213.247, 40.88.32.150, 52.155.217.156, 20.54.26.129, 205.185.216.42, 205.185.216.10, 104.42.151.234 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:18:48	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.17.57	KHAWATMI CO.IMPORT & EXPORT_PDF.exe	Get hash	malicious	Browse	• bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-7E01452C0469561541C13E621DA21CFA.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ieuHgdpuPo.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-B86F8FF0FC5B4DFA84D548466676F331.html
	Payment Slip.doc	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-9B8523D461F26385D631D5F620BB8B2E.html
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-563A37589B0D2B59C10374B2A5702724.html
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-411168C7CB32589BC9FA46F44C581051.html
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A354FBFCCC9BAC28AE0C0FFC172C1EF9.html
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-9B8523D461F26385D631D5F620BB8B2E.html
	COMMERCIAL INVOICE N#U00c2#U00ba 0001792E21.exe	Get hash	malicious	Browse	• bornforth is.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-217C604161C10233520053A33E0A764C.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MINUSCA P01-21.exe	Get hash	malicious	Browse	• bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A39FCD8B5C8720A97DC432DDA40A393E.html
	P195 NOVO Cinema#2021.exe	Get hash	malicious	Browse	• bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5573265BC294D44B8ECD9F019E83F237.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bornforthis.ml	INV_0008434567987.doc	Get hash	malicious	Browse	• 172.67.222.176
	KHAWATMI CO.IMPORT & EXPORT_PDF.exe	Get hash	malicious	Browse	• 104.21.17.57
	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	Payment Slip.doc	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• 104.21.17.57
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 172.67.222.176
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57
	COMMERCIAL INVOICE N#U00c2#U00ba 0001792E21.exe	Get hash	malicious	Browse	• 104.21.17.57
	9479_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	MINUSCA P01-21.exe	Get hash	malicious	Browse	• 104.21.17.57
	2EGv1FEjOU.exe	Get hash	malicious	Browse	• 172.67.222.176
	P195 NOVO Cinema#2021.exe	Get hash	malicious	Browse	• 104.21.17.57

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	March Financial Reports & Statements.html	Get hash	malicious	Browse	• 172.67.141.111
	V3kT2daGkz.exe	Get hash	malicious	Browse	• 104.16.19.94
	SecuriteInfo.com.Trojan.GenericKD.45979987.7892.exe	Get hash	malicious	Browse	• 172.67.197.219
	Bank Details.xlsx	Get hash	malicious	Browse	• 104.21.71.76
	RFQ No A'4762QHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 172.67.188.154
	Rechung-2021.12.04.2021.pdf.exe	Get hash	malicious	Browse	• 162.159.130.233
	INV_0008434567987.doc	Get hash	malicious	Browse	• 172.67.222.176
	mfalomirm@gentalia.eu.HTM	Get hash	malicious	Browse	• 104.19.133.58
	KHAWATMI CO.IMPORT & EXPORT_PDF.exe	Get hash	malicious	Browse	• 104.21.17.57
	YNzE2QUkvaTK7kd.exe	Get hash	malicious	Browse	• 172.67.148.14
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 23.227.38.74
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 172.67.130.43
	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 23.227.38.74
	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	Payment Slip.doc	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	INQUIRY 1820521 pdf.exe	Get hash	malicious	Browse	• 104.21.82.58
	PaymentCopy.vbs	Get hash	malicious	Browse	• 172.67.222.131

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 104.21.28.135

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	RFQ No A'4762QHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.17.57
	Rechung-2021.12.04.2021.pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	KHAWATMI CO.IMPORT & EXPORT_PDF.exe	Get hash	malicious	Browse	• 104.21.17.57
	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• 104.21.17.57
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 104.21.17.57
	Confirm Order for SK TRIMS & INDUSTRIES_DK4571,pdf .exe	Get hash	malicious	Browse	• 104.21.17.57
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	SOA.exe	Get hash	malicious	Browse	• 104.21.17.57
	RFQ No A'4762GHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.17.57
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57
	JSTCG21040600210 xlxs.exe	Get hash	malicious	Browse	• 104.21.17.57
	PAYMENT RECEIPT.exe	Get hash	malicious	Browse	• 104.21.17.57
	COMMERCIAL INVOICE N#U00c2#U00ba 0001792E21.exe	Get hash	malicious	Browse	• 104.21.17.57
	9479_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	fyi.exe	Get hash	malicious	Browse	• 104.21.17.57
	MINUSCA P01-21.exe	Get hash	malicious	Browse	• 104.21.17.57

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_scan_doc.exe_7f6cbb862bf213b5a645f615b3146ad992fef2_a4c72f23_1717e2d8\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15502
Entropy (8bit):	3.757460873141975
Encrypted:	false
SSDEEP:	192:zi6LhikSHBUZMX6aKsUAeZJ/u7sHS274ItQz:++hiJBUZMX6almJ/u7sHX4ItQz
MD5:	00945C0CD5E7E6AEABE10267E229ED71
SHA1:	B6C81FE02D87728CE19DDA61A9D329063F734F26
SHA-256:	99C520250B83E5B12FC35598A713752379E6BEB00FB8EE28952A15273248FA43
SHA-512:	76F8FF2A55FE62E93A2C24DDE0928D741D7366347805A7E18CF0CEF921E7841607A989C00B92BE684C3A6A034C5420038B78C52200F4D69291A386DEF3924B78
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.7.0.7.0.9.0.1.1.0.5.6.6.5.....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.=.1.3.2.6.2.7.0.7.0.9.5.7.5.1.1.7.1.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.9.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.f.8.c.3.9.1.4.-.7.6.8.a.-.4.6.5.b.-.9.2.1.e.-.0.2.2.6.7.1.8.3.6.3.9.b.....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.=.a.7.f.6.8.9.d.6.-.0.8.0.5.-.4.1.0.3.-.8.c.4.4.-.3.c.5.a.6.2.9.3.e.4.6.4.....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.=.s.c.a.n._.d.o.c...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.b.a.d.e.n.b.e.r.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.f.0.-.0.0.0.1.-.0.0.1.b.-.b.c.2.1.-.b.8.4.3.9.e.2.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.c.a.c.6.6.c.0.6.8.3.e.a.6.d.0.3.a.5.6.9.d.0.4.f.0.a.e.9.d.a.e.0.0.0.0.0.0.0.0.!.0.0.0.0.4.0.a.1.b.8.8.e.9.4.c.9.2.6.8.e.7.1.2.0.e.4.8.c.c.0.b.6.4.f.6.b.2.0.7.7.9.a.2.4.!.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Apr 12 13:18:12 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	269057
Entropy (8bit):	3.7887465108160403

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	
Encrypted:	false
SSDEEP:	3072:ljd+p/XyA+7KI9gIOgF5T07TUCgU/HI+Q7o61KjUkA0WH4:6p/aKI9RpDTWTTjQ3jJ0E4
MD5:	F1C173D8C13B19C28814E0B5EFECE894
SHA1:	9E369D9C9037C56CDEE8C59126F5BB3FA2A5A6A7
SHA-256:	F79FC4695B1A699A7281F2F7B0C90ED34879126EB30B1186C7C52D74669F6038
SHA-512:	CCF8869FD7AEA440728EBC02E56C30BB58E6BCB541D6A242730FDF8CD8CAA0815920A4B3F9511B50416B010059A6072F1D04F445B2DA83ED3C571B272E6E088
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....Ht`.....U.....B.....+.....GenuineIntelW.....T.....Ht`.....0.....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\WER57FE.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
Category:	dropped
Size (bytes):	8388
Entropy (8bit):	3.691392657666039
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiC86K6Yr4SU8LlNgmfZHS2+pry89b9Wsfcfm:RrlsNiB6K6Y0SU8LfgmfZSh91fp
MD5:	7D336EAC90103B0A60C979B6B1005DEA
SHA1:	5E09033CB8141B3D4C7EE756047F287EA67DBB81
SHA-256:	B10ED05DF89CB86042726D3FAA95AE3455452239BA487C3A6601B75366C64EED
SHA-512:	5DE6DBF2B666883136053EC7A9E1B19FE39BF87A3E4DA936029735B3D142661D91C3340BAE510BF21037C3179B563C667A9FF4ED9C89E8325587939A594239CA
Malicious:	false
Reputation:	low
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...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.<./.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.>.4.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A80.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4737
Entropy (8bit):	4.44049776208093
Encrypted:	false
SSDEEP:	48:cvIwSD8zsvJgtWI9h3VWSC8B+8fm8M4JKh+sFD+q8vC+YuxMzx9DGd:uITfRe3kSNxJAKMuSN9DGd
MD5:	8D38F911788CF43996D8835020530AB3
SHA1:	4EF73ABF33E08AD20F876355179E6DC0FBDC5DAC
SHA-256:	7DF41BA5CEDC453D966A46AB8A67E06FCA30A92C37F870520248D3E7FF09105E
SHA-512:	5CC86F886650F9BA073B59041AD50589B2F6D007E12599A51B42E2AB81C5CE06D495C8C50A061D8881A98509A89FB92A2884DB9DF12315BDEE95951028DF03CE
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="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <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="943108" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\WqRbEwRhliboqTZtUQoyfj	
Process:	C:\Users\user\Desktop\scan_doc.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1023400
Entropy (8bit):	3.095278840820652
Encrypted:	false
SSDEEP:	12288:XoHiWE0og/v1K/jmNeaFPq0+cggwLU4BCPyniAkfrayCl0vCmw7cXX6V/fhkTKvn:YHEgk6FK1kkANj+8IRFn0B
MD5:	94A7CAB58BBE8E975C78D9F323E751F1
SHA1:	A6B3E2A742329BF6FBD3D950DD832E0D2E6D0809

C:\Users\user\WqRbEwRhIiboqTZtUQoyfj	
SHA-256:	47E46FD290331253830A51638BA70FBB9395985CF8BD905B1D0F0E04D7E9ACD5
SHA-512:	E88D4DF49D0382CF4E1D64214EE0DB3520BA4BE694D9CCAB6CF06F1643E318C3A23F9DB83EBA32F18B86827B7FB5FA8A5EFBFEA949DEC3D01E9DB27829D96204
Malicious:	false
Reputation:	low
Preview:	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 1 84 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116 32 98 101 32 114 117 110 32 105 110 32 68 79 83 32 109 111 100 101 46 13 13 10 36 0 0 0 0 0 0 0 80 69 0 0 76 1 3 0 76 142 41 180 0 0 0 0 0 0 0 0 224 0 34 0 11 1 80 0 0 14 5 0 0 6 0 0 0 0 0 0 158 44 5 0 0 32 0 0 0 64 5 0 0 0 0 128 0 32 0 0 0 2 0 0 4 0 0 0 0 0 0 0 4 0 0 0 0 0 0 0 0 128 5 0 0 2 0 0 0 0 0 0 2 0 64 133 0 0 16 0 0 16 0 0 0 0 16 0 0 16 0 0 0 0 0 0 16 0 0 0 0 0 0 0 0 0 0 0 68 44 5 0 87 0 0 0 0 64 5 0 212 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 96 5 0 12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 8 0 0 0 0 0 0 0 0 0 0 0 8 32 0 0 72 0 0 0 0 0 0 0 0 0 0 0 46 116 101 120 116 0 0 0 164 12 5 0 0 32 0 0 0 14 5 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 96 46 114 115 11

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.0724450501210985
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	scan_doc.exe
File size:	14848
MD5:	a01c6a3db8e862ab85386b6700e941bb
SHA1:	40a1b88e94c9268e7120e48cc0b64f6b20779a24
SHA256:	29859bac1ca73683bf6c9ff17a91d249d0fa9ecb18b6b03ef03cf17545fad2be
SHA512:	6ecf3d22560c660a397c40f919ec69af4fb74a4b30fbcdce06e6cf23c57fc80a98d6023dba0c3a90331898e4bb7b19a4285ffc086f33bb6225178fe1b317a99d
SSDEEP:	384:M87FybegpzmEDTO4jCCNWiElvkr/sV3D0FX0XRno5J:M8pjgxNMZ9SkBnw
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.............."...0..0...........N... ...`....@.. ....@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x404e9e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xDCE3B2C8 [Sun Jun 8 11:26:00 2087 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4

General

Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4e44	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6000	0x5a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x2ea4	0x3000	False	0.625162760417	data	6.44315164568	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6000	0x5a8	0x600	False	0.414713541667	data	4.05648932077	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x60a0	0x31c	data		
RT_MANIFEST	0x63bc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

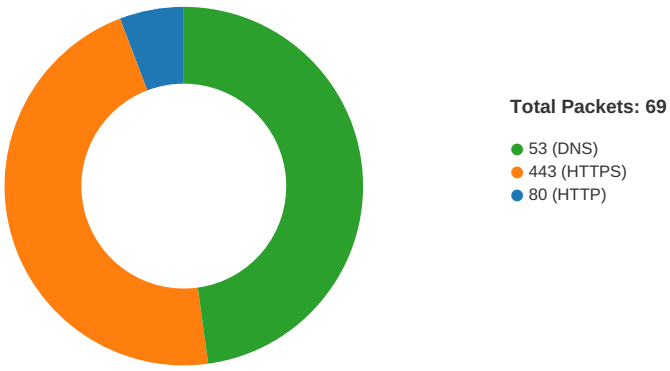
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	badenberg.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	badenberg
ProductVersion	1.0.0.0
FileDescription	badenberg
OriginalFilename	badenberg.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:18:02.994107008 CEST	49728	80	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.035154104 CEST	80	49728	104.21.17.57	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:18:03.035382986 CEST	49728	80	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.036384106 CEST	49728	80	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.077194929 CEST	80	49728	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.089163065 CEST	80	49728	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.136288881 CEST	49728	80	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.179992914 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.221195936 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.221438885 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.260107040 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.301035881 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.306374073 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.306427002 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.306530952 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.312634945 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.353512049 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.353753090 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.418001890 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.458873034 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.637876034 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.637907982 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.637939930 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.637965918 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.638004065 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.638041973 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.638084888 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.638098001 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.638137102 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.638149023 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.638189077 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.638237000 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.638814926 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.683130980 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.798628092 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.798666000 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.798857927 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.798901081 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.798943043 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.799029112 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.799316883 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.799367905 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.799498081 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.801959991 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.802022934 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.802216053 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.803157091 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.803211927 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.803251982 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.803289890 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.803339005 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.803399086 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.803402901 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.803493023 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.804120064 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.804167032 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.804260015 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.805100918 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.805154085 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.805236101 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.808427095 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.808482885 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.808522940 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.808561087 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.808579922 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.808602095 CEST	443	49729	104.21.17.57	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:18:03.808635950 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.808653116 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.808722973 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.809468985 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.809528112 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.809654951 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.810226917 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.810252905 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.810337067 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.811381102 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.811408043 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.811490059 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.812110901 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.812138081 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.812259912 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.813270092 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.813299894 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.813393116 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.814256907 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.814284086 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.814368010 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.814636946 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.814661980 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.814733982 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.839907885 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.839936972 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.840059996 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.840230942 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.840368032 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.840440989 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.841684103 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.841711044 CEST	443	49729	104.21.17.57	192.168.2.4
Apr 12, 2021 15:18:03.841773033 CEST	49729	443	192.168.2.4	104.21.17.57
Apr 12, 2021 15:18:03.843086004 CEST	443	49729	104.21.17.57	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:17:55.462335110 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:17:55.512383938 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 15:17:56.260565042 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:17:56.319855928 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:00.738564968 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:00.787394047 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:02.896759987 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:02.967135906 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:03.107773066 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:03.178096056 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:16.752629995 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:16.804238081 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:20.697263956 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:20.746068001 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:21.771446943 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:21.821866989 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:22.982064009 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:23.044863939 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:24.665678978 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:24.714654922 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:29.143795967 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:29.205219030 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:33.796684027 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:33.848850012 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:34.871316910 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:34.921916008 CEST	53	56534	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:18:36.472376108 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:36.524621964 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:43.981081009 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:44.029949903 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:44.450367928 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:44.507607937 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:45.090960026 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:45.148017883 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:45.727173090 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:45.775980949 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:45.801820040 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:45.859163046 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:46.194634914 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:46.261265993 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:46.884013891 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:46.935630083 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:47.487596989 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:47.545852900 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:48.536902905 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:48.594139099 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:49.549026966 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:49.606879950 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:49.618057966 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:49.678318024 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:50.925111055 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:50.985768080 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 15:18:51.494111061 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:18:51.559489965 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 15:19:02.951266050 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:19:03.009776115 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 15:19:16.478255033 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:19:16.527057886 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 15:19:17.546921015 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:19:17.604051113 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 15:19:33.298777103 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:19:33.347456932 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 12, 2021 15:19:35.441929102 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:19:35.516921997 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 12, 2021 15:19:49.407648087 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:19:49.464689970 CEST	53	61531	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:18:02.896759987 CEST	192.168.2.4	8.8.8.8	0xf22b	Standard query (0)	bornforthis.ml	A (IP address)	IN (0x0001)
Apr 12, 2021 15:18:03.107773066 CEST	192.168.2.4	8.8.8.8	0x8042	Standard query (0)	bornforthis.ml	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:18:02.967135906 CEST	8.8.8.8	192.168.2.4	0xf22b	No error (0)	bornforthis.ml		104.21.17.57	A (IP address)	IN (0x0001)
Apr 12, 2021 15:18:02.967135906 CEST	8.8.8.8	192.168.2.4	0xf22b	No error (0)	bornforthis.ml		172.67.222.176	A (IP address)	IN (0x0001)
Apr 12, 2021 15:18:03.178096056 CEST	8.8.8.8	192.168.2.4	0x8042	No error (0)	bornforthis.ml		104.21.17.57	A (IP address)	IN (0x0001)
Apr 12, 2021 15:18:03.178096056 CEST	8.8.8.8	192.168.2.4	0x8042	No error (0)	bornforthis.ml		172.67.222.176	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bornforthis.ml

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49728	104.21.17.57	80	C:\Users\user\Desktop\scan_doc.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:18:03.036384106 CEST	876	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-358B343CE000A6025E950DB85DC9DF85.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: bornforthis.ml Connection: Keep-Alive
Apr 12, 2021 15:18:03.089163065 CEST	877	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 12 Apr 2021 13:18:03 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Mon, 12 Apr 2021 14:18:03 GMT Location: https://bornforthis.ml/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-358B343CE000A6025E950DB85DC9DF85.html cf-request-id: 0967d4773a0000975a302c2000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ac0Pz3GaDiF15%2FFVtAmWcxNvlY2cQ6Rjft9404BSZhcAprliuQpQum4bHSgoJbALMQKOxf54izDvVdFzONY6ZQMua8NmJL0q4R2%2FhhWepA%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63ecbd052ef8975a-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

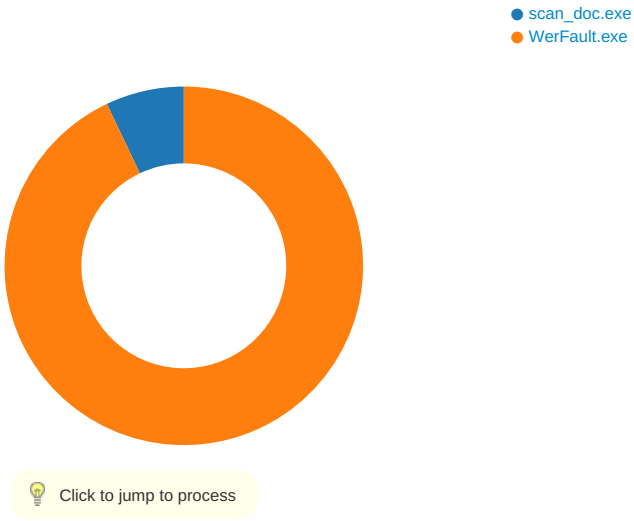
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 15:18:03.306427002 CEST	104.21.17.57	443	192.168.2.4	49729	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Apr 03 02:00:00 CEST 2021	Sun Apr 03 01:59:59 CEST 2022	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: scan_doc.exe PID: 496 Parent PID: 6136

General

Start time:	15:18:01
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\scan_doc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\scan_doc.exe'
Imagebase:	0x10000
File size:	14848 bytes
MD5 hash:	A01C6A3DB8E862AB85386B6700E941BB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D17CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D17CF06	unknown
C:\Users\user\WqRbEwRhIiboqTZtUQoyfj	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BFC1E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\WqRbEwRhIiboqTZtUQoyfj	unknown	4096	37 37 20 39 30 20 31 34 34 20 30 20 33 20 30 20 30 20 30 20 34 20 30 20 30 20 30 20 32 35 35 20 32 35 35 20 30 20 30 20 30 20 31 38 34 20 30 20 30 20 30 20 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 30 20 20 30 20 30 20 30 20 31 32 38 20 30 20 30 20 30 20 20 31 34 20 33 31 20 31 38 36 20 31 34 20 30 20 31 38 30 20 39 20 32 30 35 20 33 33 20 31 38 34 20 31 20 37 36 20 32 30 35 20 33 33 20 38 34 20 31 30 34 20 31 30 35 20 31 31 35 20 33 32 20 31 31 32 20 31 31 34 20 31 31 31 20 31 30 33 20 31 31 34 20 39 37 20 31 30 39 20 33 32 20 39 39 20 39 37 20 31 31 30 20 31 31 30 20 31 31 31 20 31 31 36 20	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116	success or wait	249	6BFC1B4F	WriteFile
C:\Users\user\WqRbEwRhIiboqTZtUQoyfj	unknown	3496	36 20 31 32 31 20 36 36 20 31 31 30 20 31 32 31 20 31 30 39 20 31 31 34 20 36 37 20 31 32 30 20 31 31 36 20 31 30 32 20 37 36 20 36 38 20 31 32 30 20 31 30 35 20 31 30 30 20 31 30 37 20 30 20 31 31 31 20 31 32 30 20 31 31 39 20 31 30 35 20 37 33 20 37 35 20 31 30 31 20 36 37 20 39 30 20 31 30 34 20 36 37 20 38 33 20 39 37 20 31 30 30 20 38 39 20 38 34 20 31 31 33 20 31 30 36 20 31 30 37 20 30 20 20 31 32 31 20 31 31 39 20 31 32 32 20 31 31 38 20 31 31 33 20 38 37 20 36 38 20 38 31 20 31 32 31 20 38 35 20 36 36 20 31 31 35 20 31 31 32 20 36 36 20 37 35 20 36 39 20 37 36 20 31 31 31 20 31 32 30 20 38 31 20 38 35 20 37 30 20 31 30 39 20 31 30 37 20 30 20 36 38 20 36 35 20 31 31 39 20 31 31 31 20 31 31 38 20 31 32 32 20 38 37 20 31 31 32 20 31 31 31 20 36 39 20	6 121 66 110 121 109 114 67 120 116 102 76 68 120 105 100 107 0 111 120 119 105 73 75 101 67 90 104 67 83 97 100 89 84 113 106 107 0 121 119 122 118 113 87 68 81 121 85 66 115 112 66 75 69 76 111 120 81 85 70 1 09 107 0 68 65 119 111 118 122 87 112 111 69	success or wait	1	6BFC1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\WqRbEwRhIiboqTZtUQoyfj	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\WqRbEwRhIiboqTZtUQoyfj	unknown	4096	success or wait	249	6BFC1B4F	ReadFile
C:\Users\user\WqRbEwRhIiboqTZtUQoyfj	unknown	600	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\WqRbEwRhIiboqTZtUQoyfj	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6D13D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D13D72F	unknown
C:\Users\user\Desktop\scan_doc.exe	unknown	4096	success or wait	1	6D13D72F	unknown
C:\Users\user\Desktop\scan_doc.exe	unknown	512	success or wait	1	6D13D72F	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 5972 Parent PID: 496

General

Start time:	15:18:07
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 496 -s 1800
Imagebase:	0x1200000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	object name collision	1	698D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	698C497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A80.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A80.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_scan_doc.exe_7f6cbb862bf213b5a645f615b3146ad992fef2_a4c72f23_1717e2d8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_scan_doc.exe_7f6cbb862bf213b5a645f615b3146ad992fef2_a4c72f23_1717e2d8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	698C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A80.tmp	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A80.tmp.xml	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A6E.tmp.csv	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D9C.tmp.txt	success or wait	1	698C497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 94 48 74 60 a4 05 12 00 00 00 00 00	MDMP..... .....Ht`.....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 84 2b 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 f0 01 00 00 89 48 74 60 00 00 00 00 01 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 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	.....U...........B.......+.... ..GenuineIntelW...........T... ....Ht`................. ....0.................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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	716	7f 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 01 00 00 00 78 ea 1a 00 05 00 00 00 00 00 00 00 05 00 00 00 b8 e9 1a 00 10 ea 1a 00 22 d7 ae 74 23 00 00 00 16 02 00 00 b8 e9 1a 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...+. ..+.......x................... ...."..t#...........+.........	success or wait	1	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	168	3c 14 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 ae 74 00 00 00 00 05 00 00 00 00 00 00 00 0b 00 07 80 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fe 6c 00 00 00 00 a8 25 6d 00 00 00 00 00 cc ea 1a 00 00 00 00 00 01 00 00 00 00 00 00 00 e8 f3 6e 00 00 00 00 00 40 ea 1a 00 00 00 00 00 02 00 00 00 00 00 00 00 1c ea 1a 00 00 00 00 00 98 eb 1a 00 00 00 00 00 12 00 00 00 00 00 00 00 d8 e9 1a 00 00 00 00 00 cc 02 00 00 88 34 00 00	<.......RCC............"..t.. ....l.....%m....... ....n.....@....... ....4..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	20	73 02 00 00 d0 b1 05 6b 00 00 00 00 7c 01 00 00 e4 82 00 00	s......k....|.......	success or wait	627	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	380	00 00 00 00 07 5a 8e 5a 00 00 00 00 02 00 00 00 1c 01 00 00 08 b2 77 00 08 90 77 00 00 00 00 00 07 5a 8e 5a 00 00 00 00 02 00 00 00 28 00 00 00 24 b3 77 00 24 91 77 00 52 53 44 53 01 48 d8 f1 e0 52 9a da 60 ad 49 c6 d1 6a 3b 6d 01 00 00 00 53 79 73 74 65 6d 2e 43 6f 72 65 2e 6e 69 2e 70 64 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....Z.Z..............w...w... ...Z.Z........ (...$.w.$.w.RSDS .H...R..`.I..j;m....System.Core.ni.pdb.....................	success or wait	626	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	4	7c 6e 00 6c	|n.l	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	4	0d 00 00 00	....	success or wait	13	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.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 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 50 db 1a 00 bc 9a 11 77 23 00 00 00 16 02 00 00 c0 d9 1a 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...+. ..+.......................... P......w#...........+.........	success or wait	13	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	48	94 0c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 10 30 00 00 00 00 00 a8 f6 31 05 00 00 00 00 58 09 00 00 b8 1c 01 00 cc 02 00 00 e4 58 00 00	....0.......1... ..X............X..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	4	4a 00 00 00	J...	success or wait	74	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	30	18 00 00 00 73 00 63 00 61 00 6e 00 5f 00 64 00 6f 00 63 00 2e 00 65 00 78 00 65 00 00 00	....s.c.a.n._.d.o.c...e.x.e...	success or wait	74	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	120	00 00 b5 69 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a 08 34 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 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 00 0c 00 00 00 18 00 00 00 02 00 00 00	...i.............`.Z.4........ ....?........... ....)............ ..@A.........................	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n .R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	668	00 00 0a 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 6a 34 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 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 50 c2 02 00 00 00 00 00 50 f4 02 00 00 00 00 8d 53 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 50 6e 03 00 00 00 00 00 ba 70 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 f1 1a 00 00 00 00 00 2f 0e 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 e4 26 05 00 00 00 00 00 f0 55 92 35 01 00 00 00 b3 36 5f 15 00 00 00 00 ab ee ca 0c 00 00 00 00 f1 f2 e2 00 00 00 00 00 63 9b 00 00 47 b4 00 00 d3 05 05 00 44 9d 0a 00 2f 0e 05 00 fb 7e 15 00 e4 26 05 00 09 fa 1e 00 87 3a 01 00 b3 70 10 00 00 00 00 00 a6 1a 0e 00 c0 ac 04	...s.....*.,.j4.....Zb ....P.....P .....S.....Pn.. .....p...../. .....@.....&.....U.5.... .6_.....c...G. .....D.../....~...&.....:.. .p.....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	29024	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	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D3F.tmp.dmp	unknown	120	03 00 00 00 74 02 00 00 08 07 00 00 04 00 00 00 3c 1f 00 00 88 09 00 00 0e 00 00 00 3c 00 00 00 c4 28 00 00 05 00 00 00 34 27 00 00 b0 5b 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 b0 46 00 00 99 d4 03 00 15 00 00 00 ec 01 00 00 00 29 00 00 16 00 00 00 98 00 00 00 ec 2a 00 00	....t.....<.....<....(.....4'...[.....`....8.....T.....F .....).....*..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	134	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 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...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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 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.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	28	3c 00 50 00 69 00 64 00 3e 00 34 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.9.6.<./.P.i.d.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 73 00 63 00 61 00 6e 00 5f 00 64 00 6f 00 63 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.>.s.c.a.n._.d.o.c...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 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	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 31 00 38 00 31 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.>.1.1.1.8.1.<./.U.p.t.i.m.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	88	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 32 00 32 00 34 00 31 00 36 00 31 00 37 00 39 00 32 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.>.2.2.4.1.6.1.7.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	72	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 32 00 32 00 34 00 31 00 35 00 33 00 36 00 30 00 30 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.>.2.2.4.1.5.3.6.0.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 37 00 38 00 39 00 37 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.>.1.7.8.9.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 35 00 32 00 32 00 38 00 35 00 34 00 34 00 30 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.>.5.2.2.8.5.4.4.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 34 00 37 00 31 00 34 00 30 00 38 00 36 00 34 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.>.4.7.1.4.0.8.6.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 33 00 31 00 39 00 35 00 36 00 30 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 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.>.3.1.9.5.6.0.<./.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 33 00 31 00 39 00 35 00 36 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.>.3.1.9.5.6.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 38 00 38 00 33 00 32 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.>.2.1.8.8.3.2.<./.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 38 00 35 00 36 00 30 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.>.2.1.8.5.6.0.<./.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 36 00 33 00 31 00 31 00 30 00 34 00 30 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.>.3.6.3.1.1.0.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 34 00 37 00 38 00 35 00 33 00 35 00 36 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.>.4.7.8.5.3.5.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 36 00 33 00 31 00 31 00 30 00 34 00 30 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.>.3.6.3.1.1.0.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./.P.i.d.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 34 00 31 00 32 00 35 00 34 00 39 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.>.4.4.1.2.5.4.9.<./.U.p.t.i.m.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 35 00 31 00 33 00 34 00 32 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.>.5.1.3.4.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	100	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 30 00 36 00 34 00 31 00 38 00 31 00 37 00 36 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.>.1.0.6.4.1.8.1.7.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	84	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 30 00 36 00 30 00 34 00 39 00 35 00 33 00 36 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.>.1.0.6.0.4.9.5.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 39 00 38 00 30 00 33 00 38 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.>.9.8.0.3.8.4.<./.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 39 00 34 00 34 00 35 00 30 00 34 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.>.9.4.4.5.0.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 34 00 35 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.>.7.4.5.2.0.<./.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 33 00 30 00 30 00 30 00 30 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.>.7.3.0.0.0.<./.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 35 00 35 00 36 00 39 00 36 00 36 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.>.3.5.5.6.9.6.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 39 00 39 00 38 00 35 00 39 00 32 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.>.3.7.9.9.8.5.9.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 35 00 35 00 36 00 39 00 36 00 36 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.>.3.5.5.6.9.6.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 73 00 63 00 61 00 6e 00 5f 00 64 00 6f 00 63 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.>.s.c.a.n._.d.o.c...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 6b 00 68 00 6d 00 65 00 6c 00 6b 00 2c 00 20 00 49 00 6e 00 63 00 2e 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.>.k.h.m.e.l.k.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	96	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 6b 00 68 00 6d 00 65 00 6c 00 6b 00 37 00 2c 00 31 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.>.k.h.m.e.l.k.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	120	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 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 37 00 34 00 32 00 35 00 33 00 34 00 30 00 30 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.>.1.5.7.4.2.5.3.4.0.0.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 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.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	96	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 30 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.>.0.<./.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 31 00 2d 00 30 00 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 31 00 38 00 3a 00 31 00 33 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.=.".2.0.2.1.-.0.4.-.1.2.T.1.3.:.1.8.:.1.3.Z.".>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	260	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 33 00 36 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 39 00 36 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 34 00 34 00 38 00 34 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 34 00 34 00 38 00 34 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 00 3d 00 22 00 31	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.0.". .P.I.D.=.".4.9.6.". .U.p.t.i.m.e.M.S.=.".4.4.8.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".4.4.8.4.". .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.=.".1	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 66 00 38 00 63 00 33 00 39 00 31 00 34 00 2d 00 37 00 36 00 38 00 61 00 2d 00 34 00 36 00 35 00 62 00 2d 00 39 00 32 00 31 00 65 00 2d 00 30 00 32 00 32 00 36 00 37 00 31 00 38 00 33 00 36 00 33 00 39 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.0.f.8.c.3.9.1.4.-.7.6.8.a.-.4.6.5.b.-.9.2.1.e.-.0.2.2.6.7.1.8.3.6.3.9.b.<./.G.u.i.d.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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 31 00 2d 00 30 00 34 00 2d 00 31 00 32 00 54 00 31 00 33 00 3a 00 31 00 38 00 3a 00 31 00 33 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.>.2.0.2.1.-.0.4.-.1.2.T.1.3.:.1.8.:.1.3.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER57FE.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	698C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A80.tmp.xml	unknown	4737	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	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_scan_doc.exe_7f6cbb862bf213b5a645f615b3146ad992fef2_a4c72f23_1717e2d8\Report.wer	unknown	2	ff fe	..	success or wait	1	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_scan_doc.exe_7f6cbb862bf213b5a645f615b3146ad992fef2_a4c72f23_1717e2d8\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	202	698C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_scan_doc.exe_7f6cbb862bf213b5a645f615b3146ad992fef2_a4c72f23_1717e2d8\Report.wer	unknown	46	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 31 00 38 00 30 00 38 00 31 00 32 00 30 00 39 00 35 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.8.0.8.1.2.0.9.5.2.	success or wait	1	698C497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	success or wait	1	698E36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	698E1FB2	RegCreateKeyExW
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	698C43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	ProgramId	unicode	0006bcac66c0683ea6d03a569d04f0ae9dae00000000	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	FileId	unicode	000040a1b88e94c9268e7120e48cc0b64f6b20779a24	success or wait	1	698E36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	LowerCaseLongPath	unicode	c:\users\user\desktop\scan_doc.exe	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	LongPathHash	unicode	scan_doc.exe|7734a1cc	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	Name	unicode	scan_doc.exe	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	Publisher	unicode		success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	Version	unicode	1.0.0.0	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	BinFileVersion	unicode	1.0.0.0	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	BinaryType	unicode	pe32_clr_32	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	ProductName	unicode	badenberg	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	ProductVersion	unicode	1.0.0.0	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	LinkDate	unicode	06/08/2087 11:26:00	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	BinProductVersion	unicode	1.0.0.0	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	Size	B	00 3A 00 00 00 00 00 00	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	Language	dword	0	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	IsPeFile	dword	1	success or wait	1	698E36BF	unknown
\REGISTRY\A\{3d9595d5-913c-9a3c-391d-fe70d5d35fcc}\Root\InventoryApplicationFile\scan_doc.exe|7734a1cc	IsOsComponent	dword	0	success or wait	1	698E36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 AE 74 05 00 00 00 0B 00 07 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FE 6C A8 25 6D 00 CC EA 1A 00 01 00 00 00 E8 F3 6E 00 40 EA 1A 00 02 00 00 00 1C EA 1A 00 98 EB 1A 00 12 00 00 00 D8 E9 1A 00	success or wait	1	698E1FE8	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis