ID: 831165
Sample Name: DE-1550 Installer v1.03_rev1 07-23-2018.msi
Cookbook: default.jbs
Time: 07:25:37
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

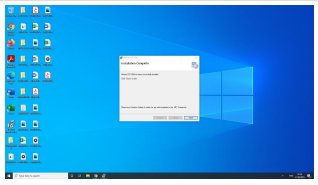
Windows Analysis Report

DE-1550 Installer v1.03_rev1 07-23-2018.msi

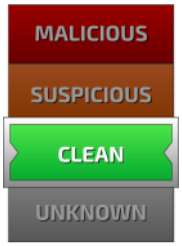
Overview

General Information

Sample Name:	DE-1550 Installer v1.03_rev1 07-23-2018.msi
Analysis ID:	831165
MD5:	08af3aac53f69…
SHA1:	f34527fe04ede…
SHA256:	cdec38d9934e…
Infos:	



Detection

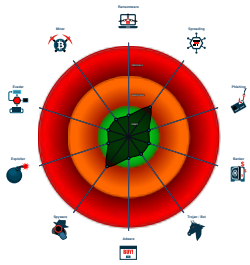


Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	20%

Signatures

- Queries the volume information (nam…
- Modifies existing windows services
- Sample file is different than original …
- Drops PE files
- Tries to load missing DLLs
- Deletes files inside the Windows fol…
- Drops PE files to the windows direc…
- Creates files inside the system direc…
- Stores files to the Windows start me…
- Checks for available system drives …
- Found dropped PE file which has no…

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox
Sample is looking for USB drives. Launch the sample with the USB Fake Disk cookbook
Sample searches for specific file, try point organization specific fake files to the analysis machine
Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Process Tree

- **System is w10x64native**
- msiexec.exe (PID: 8324 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\DE-1550 Installer v1.03_rev1 07-23-2018.msi" MD5: E5DA170027542E25EDE42FC54C929077)
- msiexec.exe (PID: 2040 cmdline: C:\Windows\system32\msiexec.exe /V MD5: E5DA170027542E25EDE42FC54C929077)
  - msiexec.exe (PID: 8944 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 84DA78192880581D6829482FFD39CF6A C MD5: 9D09DC1EDA745A5F87553048E57620CF)
  - msiexec.exe (PID: 560 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding C6401D95ECC4BE08AAC131C3978679E2 MD5: 9D09DC1EDA745A5F87553048E57620CF)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

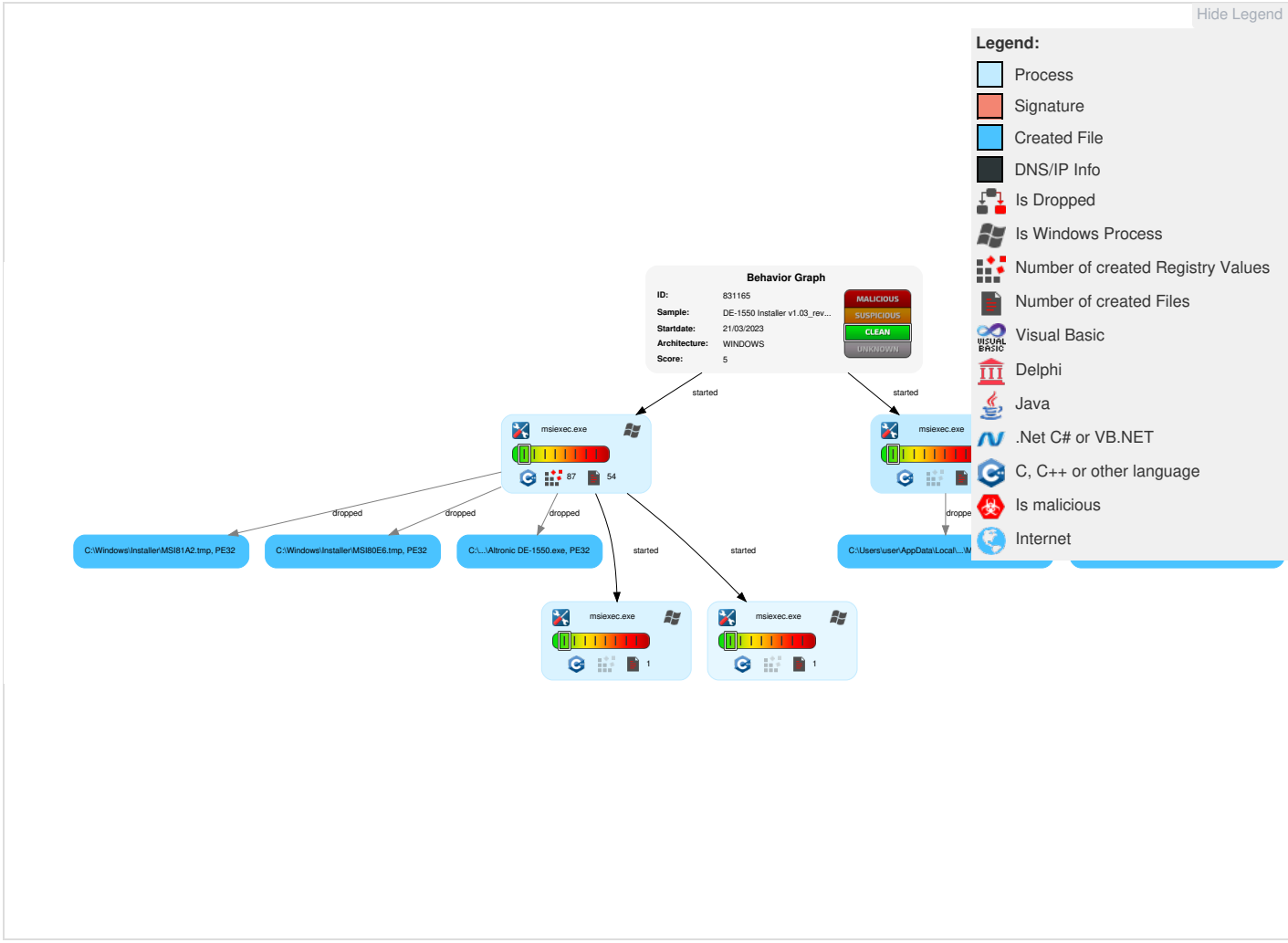
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	Windows Management Instrumentation	1 Windows Service	1 Windows Service	2 2 Masquerading	OS Credential Dumping	1 Process Discovery	1 Replication Through Removable Media	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Process Injection	1 Process Injection	LSASS Memory	1 1 Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	1 DLL Side-Loading	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	1 File Deletion	NTDS	1 1 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

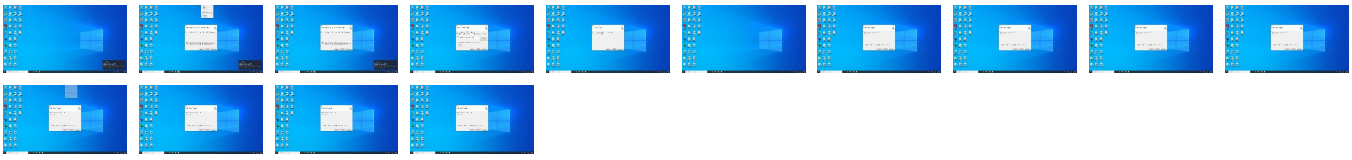
Behavior Graph

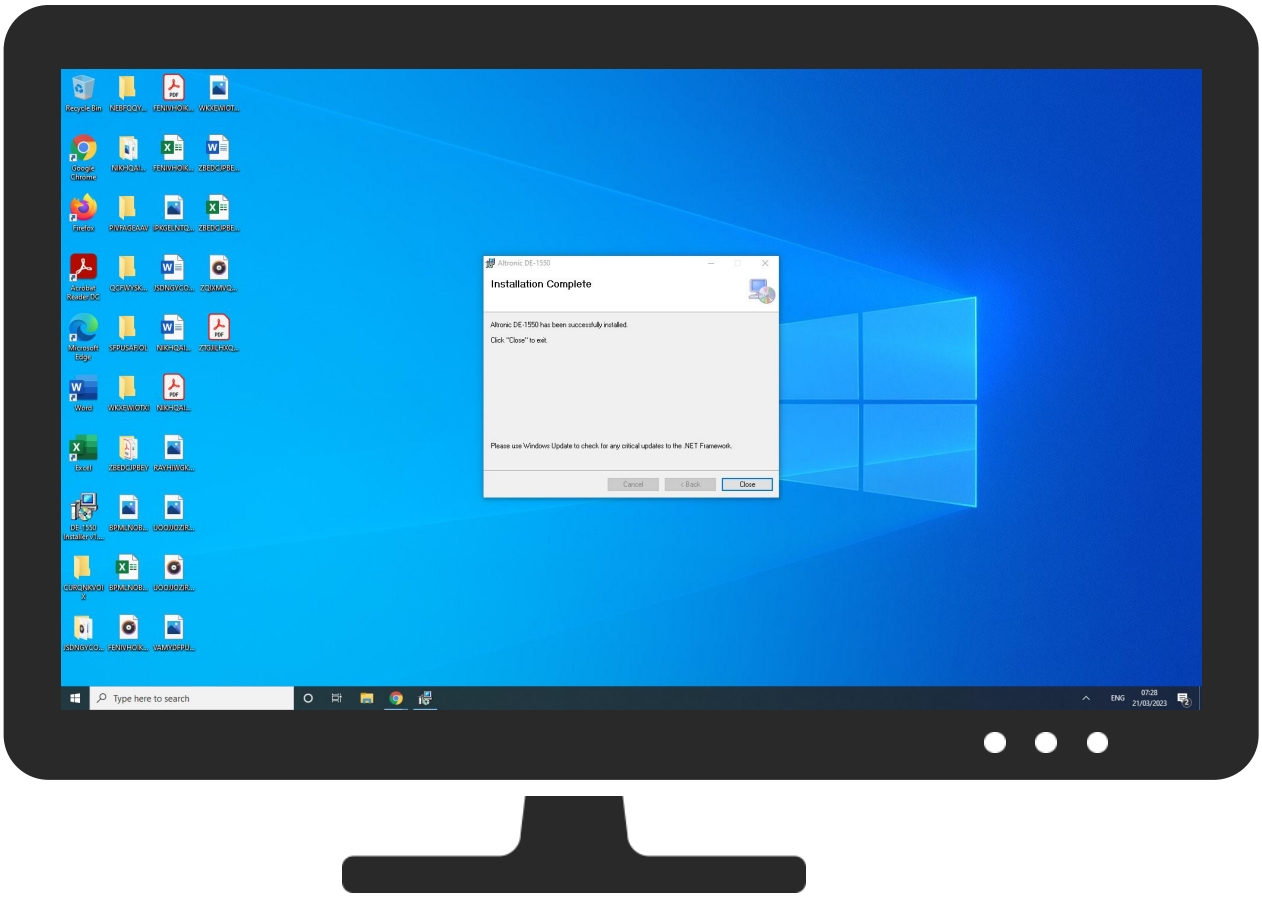


Screenshots

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
DE-1550 Installer v1.03_rev1 07-23-2018.msi	2%	ReversingLabs		
DE-1550 Installer v1.03_rev1 07-23-2018.msi	0%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MSI584F.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI584F.tmp	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MSI591B.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI591B.tmp	0%	Virustotal		Browse
C:\Windows\Installer\MSI80E6.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI80E6.tmp	0%	Virustotal		Browse
C:\Windows\Installer\MSI81A2.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831165
Start date and time:	2023-03-21 07:25:37 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	11
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
Sample file name:	DE-1550 Installer v1.03_rev1 07-23-2018.msi
Detection:	CLEAN
Classification:	clean5.winMSI@6/33@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .msi

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, VSSVC.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.190.159.0, 20.190.159.23, 20.190.159.4, 40.126.31.71, 40.126.31.73, 40.126.31.69, 20.190.159.75, 20.190.159.71, 51.124.57.242
- Excluded domains from analysis (whitelisted): prdv6a.aadg.msidentity.com, wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, www.tm.lg.prod.aadmsa.akadns.net, www.tm.v6.a.prd.aadg.akadns.net, ctldl.windowsupdate.com, wdcp.microsoft.com, wd-prod-cp.trafficmanager.net, login.msa.msidentity.com, wd-prod-cp-eu-west-3-fe.westeurope.cloudapp.azure.com

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Config.Msi\118801c.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	10406
Entropy (8bit):	5.703198333877612
Encrypted:	false
SSDEEP:	96:3TMeruVzD2weQDSwU+v9wTCsThqvU+v9wTC6jH1pFThqrHMSjH1wNymVwr6lPs+5:3G/eRPhOIdhO8Z8Lpq
MD5:	DCCCB8C335FFC3BBE967A10EAD28AA88
SHA1:	8B8268AFE4C0238E32DD60D0F202C5B91E6A2955
SHA-256:	12576A38F48B08D81C3685203E910C55278DABFC9AEA98340AB28B9ED5E3B0B3
SHA-512:	A27079FD4EAED83CE7A71A0771AC5F4ED498EC54F7752AA5BBBD3EC53E2A0B4E0928ACFD1F04E62D05C231B9AA6CB6B7A2C5AC8E875A834744498B4F25F88725
Malicious:	false
Reputation:	low
Preview:	...@IXOS.@.....@u;uV.@.....@.....@.....@.....@.....@.....&.{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}..Altronic DE-1550+.DE-1550 Installer v1.03_rev1 07-23-2018.msi.@.....@.....@.....@.....@.....&.{F6296E9E-3D64-43FF-B0A4-736C96B15080}.....@.....@.....@.....@.....@.....@.....@.....@.....Altronic DE-1550.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{FBEE690E-63CA-9123-3429-448ED52CA353}&.{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}.@.....&.{6DA9B1AE-EC52-644E-A521-C6CA345CA92A}&.{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}.@.....&.{511939AB-4664-F9F3-9CAC-7D981D8D374C}&.{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}.@.....&.{B9B828B7-EE55-8389-D0EC-44437CC85274}&.{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}.@.....&.{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}&.{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}.@.....&.{7F7B0467-8E0A-A0F2-C00F-02CD8E033A5D}&.{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}.@.....&.{92BAF562-34CE-7769

C:\Program Files (x86)\Altronic LLC\Altronic DE-1550\Altronic DE-1550.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	351744
Entropy (8bit):	5.484525406241142
Encrypted:	false
SSDEEP:	3072:lhU1Ud7MMCoNE9Fisu4M4rY7NaFWZ91PsaWTMALVAzMZ296QHlpcbZO7YaiZAcgd:l7MM1/5xxJ59gTXVB2lxaU5iZAj+
MD5:	5550DE5A2731E0E032ADA555A283B661
SHA1:	B19AE7FCB7ADF0AD9FFEF260D977D124C3C07ABB
SHA-256:	A8931E7501E1FF82D69D6DAC96E0D487FDC8203E2400CF8266B79CEDF48DA352
SHA-512:	1798836A77F5E55FD6DE059577F5EC1372847677A7C09D8AE05F0A65BE07813206BC7ED7CDB3681F357A2FF6831DA8364F4935FCC4B21F85BE66C66EA0750A1A

Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....V[.....R.....np... .....@.. ....@.....p..O..... .....o..... ....H.....text...tP... ...R..... ..`.rsrc... .....T.....@..@.rel oc.....\.....@..B.....Pp.....H.....h.....@...P9.....0..v.....}.....(.....(1.....#.....}.....#.....@}.....#.....}.....#.....@}.....{3. ..~....o.....{E...~....o.....*...0..;.....:.....{'....o.....{}....o.....{J....o.....{/....o.....{(....o.....{-....o.....{....o.....{@....o.....{3....o.....{G....o.....{=....o.....{F....o.....{H....o..... {E....o.....{L....o.....{N....o.....{8....o.....{6....o.....{:....o.....

C:\Program Files (x86)\Altronic LLC\Altronic DE-1550\Altronic DE-1550.exe.config

Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	799
Entropy (8bit):	4.95426176724379
Encrypted:	false
SSDEEP:	12:MMHd41Gqt1s26K9BQvDLI4MWiO69BAHs26K9YG6DLI4MWivBRVcXHhuGnObAHOgy:JdiIK07E449BNK6E4Ev+XwIHkvy6
MD5:	153521492A23F91BFCF6D01B80E3A39C
SHA1:	2439DED18703AFB5FA885AE1CAF2F8DC5F80C0EC
SHA-256:	6E8133C547BAF698FC1985BAC1E614DAD0184DF4470D8B9F70299D144C9F32CA
SHA-512:	2034E4DA314B9FD47D6803F4E5251E46AB5545F9441B7DE706C861A99817E7353599EFBAB318E24BCD6EC9117745B6926329789910B2DA0275F46607EA01979B
Malicious:	false
Reputation:	low
Preview:	.<?xml version="1.0" encoding="utf-8" ?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettin gsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="DE_1550.Properties.Settings" type="System.Conf iguration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermi ssion="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <DE_1550.Properties.Settings>.. <setting name="port" serializeAs= "String">.. <value>""</value>.. </setting>.. </DE_1550.Properties.Settings>.. </userSettings>..</configuration>

C:\Program Files (x86)\Altronic LLC\Altronic DE-1550\Altronic.ico

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 16 colors, 4 bits/pixel
Category:	dropped
Size (bytes):	766
Entropy (8bit):	4.232299018146602
Encrypted:	false
SSDEEP:	12:jJQ1Ih+sfBY8M4nGT6vhSYUzt8K4t33uhEIk7dwcwH1:ji+sY4nGTCSYBKa33ffScwV
MD5:	66DF1FDB899EA252FDCA66AC561F0754
SHA1:	BE444798581095030EAB1C93C9219DCDB3251F44
SHA-256:	1CAE16A1B08AA2D980554FD9DE53FDCFC6B166D919FA4957E75544C77770DD37
SHA-512:	16EAF94B247B035666FD0FAA2998688DBA74829CB50E425D22280A6716B2C1286A0C6792A18EB5B604CD01E8877C1A9778472BF7A83564A4FDB899DDDF7A83A
Malicious:	false
Reputation:	low
Preview:	....(... ...@.....%...*...1...:...D#..Q4..X=..cH..hO..t_}..m{..vy..}y...s...z.....T"4j..x.....H.....I!.....m.....I.Q.. ..=.....P.....0..... ..=.....(.....Q..... ..n.....$!..]..... .....=.....B.....T1..... .....`+.....a...z.A.....1.....].....S"#W..... .....

C:\Program Files (x86)\Altronic LLC\Altronic DE-1550\Configuration Files\DEFAULT.afd

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2039
Entropy (8bit):	2.486949337314901
Encrypted:	false
SSDEEP:	12:NRuJPHURuJ22RuJmRuJnRuJDkefwtOGsvDRuJn0RuJsQGsvUyBEWWwl/isi+h43a:6JNJ2fJvJ0JD9wJFJs0UijkXPj3J2lD
MD5:	E7BD71159DB9AA5A0A64C407D0486E4D
SHA1:	BF8640E26B3708FFF08CCF609906FDD83867AD56
SHA-256:	45B5B85C60FAE632E86843A066C97E5465BE0D9EF7DACD2E9F91FEDCB28C40AA
SHA-512:	D4DCE4F2DF28BDB5BF67D8FD6BA3F708220DA02A8D3147BA7C103E9F42657A2FEF6FBEE439D0889EDB742EADAB68977EBA6DF4C94C3A4EF890AD8C48972C 5BBE
Malicious:	false
Reputation:	low

Preview:	>(00AFR 00 000 000 000 002 014 102 000 001 001 154 216 241 039 015 000 000)..>(00AFR 01 000 000 000 002 014 102 000 001 001 154 216 241 039 015 000 000)..>(00AFR 02 000 000 000 002 014 102 000 001 001 154 216 241 039 015 000 000)..>(00AFR 03 000 000 000 002 014 102 000 001 001 154 216 241 039 015 000 000)..>(00AFR 04 000 000 000 002 014 102 000 001 001 154 216 241 039 015 000 000)..>(00AFR 05 001 000 003 232 013 250 000 000 001 142 255 006 004 226 000 000)..>(00AFR 06 001 001 005 103 015 135 250 153 000 000 250 153 005 103 000 000)..>(00AFR 07 000 000 000 001 007 000 000 001 001 202 255 180 005 192 000 000)..>(00AFR 08 000 000 000 002 014 102 000 001 001 154 216 241 039 015 000 000)..>(00AFR 09 000 000 000 002 014 102 000 001 001 154 216 241 039 015 000 000)..>(00AFR 10 003 002 000 000 000 000 000 000 000 000 000 000 000 000 000 000)..>(00AFR 11 000 000 000 001 007 000 000 001 001 202 255 180 005 192 000 000).. ..>(00AFR TRANSFER).. .. ..>(00AFR 12 000 000 000 001 000 000 000

C:\Program Files (x86)\Altronic LLC\Altronic DE-1550\Configuration Files\DEFAULT.pgd

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	3887
Entropy (8bit):	4.258827652150147
Encrypted:	false
SSDEEP:	96:8gOfif490ihmmFCQ9AAtJjqkOMiAFzn6pcRP27Gem9dlLxwFX9fi:vOfif490igmwQ9AAtJOPMiAFzn6pcRuo
MD5:	D8E63529A462613D5EC0BDF4E2F7A341
SHA1:	AB146B08EAE75EC7609A049515A52D6D340505E8
SHA-256:	3F95F9A1ADC412BB1168149E6513AE1FA1EBD9F2F2460D6131E5319908820318
SHA-512:	D5ACA92BEF5CFAC2ED29BC76DE5141EF48CFE892BE981C33643A578BFC0D24D030D9E1BFEAA99BB0BD8642E70E6306B1A3D1E2FA331FE78C1CD29C964993B6EC
Malicious:	false
Reputation:	low
Preview:	>(126PAWAKE).....>(000PA 000 3*(00 RD & N*(00 RL 00&*(00 RH 00& PSIA-|HIGH LIQUID LEVEL)..>(001PA 000 3*(00 RD & N*(00 RL 00&*(00 RH 00& PSIA-|LOW ENGINE OIL LEVEL)..>(002PA 000 3*(00 RD & N*(00 RL 00&*(00 RH 00& PSIA-|ENGINE VIBRATION)..>(003PA 000 3*(00 RD & N*(00 RL 00&*(00 RH 00& PSIA-|COOLANT LEVEL FAULT)..>(004PA 000 3*(00 RD & N*(00 RL 00&*(00 RH 00& -|LOSS OF POWER)..>(005PA 000 3*(00 RD & N*(00 RL 00&*(00 RH 00& -|TIMED SHUTDOWN)..>(006PA 000 3*(00 RD & N*(00 RL 00&*(00 RH 00& -|OVERCRANK FAILURE)..>(007PA 000 3*(00 RD & N*(00 RL 00&*(00 RH 00& -|NO ROTATION)..>(016PA 000 3*(00 RD & S*(00 RL 01&*(00 RH 01& PSIG-|SUCTION PRESSURE)..>(017PA 000 3*(00 RD & S*(00 RL 02&*(00 RH 02& PSIG-|DISCHARGE PRESSURE)..>(018PA 000 3*(00 RD & S*(00 RL 03&*(00 RH 03& PSIG-|FIELD PRESSURE)..>(019PA 000 3*(00 RD & S*(00 RL 04&*(00 RH 04& PSIG-|ENGINE MAN. VACUUM)..>(020PA 000 3*(00 RD & S*(00 RL 05&*(00 RH 05& .

C:\Program Files (x86)\Altronic LLC\Altronic DE-1550\Configuration Files\DEFAULT.trd

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1438
Entropy (8bit):	3.488534117813489
Encrypted:	false
SSDEEP:	24:O3fVvl7pmoLUzSIycgYkCmx/kCVaafQWssFESTXBpTDOxo:YfVvl7U3SIyfxtPfumXBp3OG
MD5:	190E22E6D17F591E205FADB710625084
SHA1:	6C97FAFC8707397C750DD4E68393467A03CD5A4F
SHA-256:	6770EEF98AD01BDE9BA78D855E69DC7CF110C3DB37E88D9883C5AE9F45D14DF8
SHA-512:	8D1470EC2CE68FEBF8AA1EA8857F66102003C69B6AC151FE02576421745FE2FB1B44F732F44FC24CFCA25896740706E21B21B728A6BF0E7E461DEC965886E1FF
Malicious:	false
Preview:	>(00T ON)..>(00TA 00 0 1 0 -0750 +3750)..>(00TA 01 0 1 0 -1250 +6250)..>(00TA 02 0 0 0 -0250 +1250)..>(00TA 03 0 1 0 -0125 +0625)..>(00TA 04 2 0 0 -0143 +0675)..>(00TA 05 2 0 0 -0143 +0675)..>(00TA 06 0 1 0 -0250 +1250)..>(00TA 07 0 1 0 -0250 +1250)..>(00TC 00 0410 +000.0 3686 +300.0)..>(00TC 01 0410 +000.0 3686 +500.0)..>(00TC 02 0410 +0000. 3686 +1000.)..>(00TC 03 0410 +000.0 3686 +050.0)..>(00TC 04 1409 +0032. 2984 +0572.)..>(00TC 05 1409 +0032. 2984 +0572.)..>(00TC 06 0410 +000.0 3686 +100.0)..>(00TC 07 0410 +000.0 3686 +100.0)..>(00T 00 B 030 +000.0 +000.0 B 030 +040.0 +040.0)..>(00T 01 B 060 +025.0 +025.0 A 000 +250.0 +250.0)..>(00T 02 A 000 +0000. +0000. A 000 +0500. +0500.)..>(00T 03 B 030 -012.5 -012.5 B 030 -001.0 -001.0)..>(00T 04 B 030 -0076. -0076. B 030 +0225. +0225.)..>(00T 05 A 000 -0076. -0076. A 000 +0400. +0400.)..>(00T 06 B 030 +030.0 +030.0 A 000 +110.0 +110.0)..>(00T 07 B 060 -005.0 -005.0 B 060 +045.0 +045.0)..>(00T 08 C 010 +1400. +140

C:\Users\user\AppData\Local\Temp\CFG58FB.tmp

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	117
Entropy (8bit):	4.772296691735276
Encrypted:	false
SSDEEP:	3:vFWWMNHUz/clMOoT02V7VKXRAmIRMNHjKboe+RAW4QIMOov:TMV0kl002V7VQ7V2boeuAW4QIm
MD5:	3C3D11B78E4C077C083F0B6B527D146E
SHA1:	C210C08BB3BDA4D775AA4F23BD177DBEF0BC1378
SHA-256:	55DB6CC3FCF27F20362198F28B652889F7808FFA206E2140D3F3AB3ECE879EB9
SHA-512:	03A2F82C58A640314D90070375D6AD6193E705AC63E3463511EBDDE5B727463BBD3D98C9E163A6A21C76A723E28DC9B8D94574DC2D2ECFC8CDB18CB9188C21AF

Malicious:	false
Preview:	<?xml version="1.0"?>..<configuration>...<startup><supportedRuntime version="v4.0"/>...</startup>..</configuration>..

C:\Users\user\AppData\Local\Temp\CFG8182.tmp

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	117
Entropy (8bit):	4.772296691735276
Encrypted:	false
SSDEEP:	3:vFWWMNHUz/clMOoT02V7VKXRAmIRMNHjKboe+RAW4QIMOov:TMV0kl002V7VQ7V2boeuAW4QIm
MD5:	3C3D11B78E4C077C083F0B6B527D146E
SHA1:	C210C08BB3BDA4D775AA4F23BD177DBEF0BC1378
SHA-256:	55DB6CC3FCF27F20362198F28B652889F7808FFA206E2140D3F3AB3ECE879EB9
SHA-512:	03A2F82C58A640314D90070375D6AD6193E705AC63E3463511EBDDE5B727463BBD3D98C9E163A6A21C76A723E28DC9B8D94574DC2D2ECFC8CDB18CB9188C2 AF
Malicious:	false
Preview:	<?xml version="1.0"?>..<configuration>...<startup><supportedRuntime version="v4.0"/>...</startup>..</configuration>..

C:\Users\user\AppData\Local\Temp\MSI584F.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	236872
Entropy (8bit):	6.42500790517661
Encrypted:	false
SSDEEP:	3072:Z7PyQaeLAxV9EcU95qWCn7B1kkJQGGhKTWAvdEhMqmc1wtI6M/CoKpixBrnQYaeW:8n3Nn7ByILdEODlcOnlpOuodL+8Y
MD5:	0A2626FC9E4E0CA18386C029E9EFFFD9
SHA1:	AC5576497AFAC2456F485CDB14BF52D895769651
SHA-256:	97A55524E0BF06419143B1B71778C0EC867716079AB477E8404A0F3125DA7DC3
SHA-512:	40B25E507E64B5634E13E83D4BC420196B1294D533E60B01DAE8898A8EED939417AEC8341B409F59A722D14FB63884C24C5A31985DA63933B761F1FC3ACB24D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S/...N...N...N..0....N..p8E..N...6l..N..x8D.+N..x8q..N..x8E.N...6|..N... N..FO..p8D..N..p8t..N..p8u..N..p8r..N..Rich.N.....PE..L.....K....."!..... .....~.....0.....A.....U....@.....#...D .....8.....H..... .....@.....text..... ....`.data....H...0.....$.....@....rsrc...8.....>.....@..@.reloc...@.....B...D..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\MSI591B.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	236872
Entropy (8bit):	6.42500790517661
Encrypted:	false
SSDEEP:	3072:Z7PyQaeLAxV9EcU95qWCn7B1kkJQGGhKTWAvdEhMqmc1wtI6M/CoKpixBrnQYaeW:8n3Nn7ByILdEODlcOnlpOuodL+8Y
MD5:	0A2626FC9E4E0CA18386C029E9EFFFD9
SHA1:	AC5576497AFAC2456F485CDB14BF52D895769651
SHA-256:	97A55524E0BF06419143B1B71778C0EC867716079AB477E8404A0F3125DA7DC3
SHA-512:	40B25E507E64B5634E13E83D4BC420196B1294D533E60B01DAE8898A8EED939417AEC8341B409F59A722D14FB63884C24C5A31985DA63933B761F1FC3ACB24D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S/...N...N...N..0....N..p8E..N...6l..N..x8D.+N..x8q..N..x8E.N...6|..N... N..FO..p8D..N..p8t..N..p8u..N..p8r..N..Rich.N.....PE..L.....K....."!..... .....~.....0.....A.....U....@.....#...D .....8.....H..... .....@.....text..... ....`.data....H...0.....$.....@....rsrc...8.....>.....@..@.reloc...@.....B...D..... .....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Installer\{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}_8FE7F6AC6251280AFC5837.exe

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 16 colors, 4 bits/pixel
Category:	dropped
Size (bytes):	766
Entropy (8bit):	4.232299018146602
Encrypted:	false
SSDEEP:	12:jJQ1lh+sfBY8M4nGT6vhSYUzt8K4t33uhEIk7dwcwH1:ji+sY4nGTCSYBKa33ffScwV
MD5:	66DF1FDB899EA252FDCA66AC561F0754
SHA1:	BE444798581095030EAB1C93C9219DCDB3251F44
SHA-256:	1CAE16A1B08AA2D980554FD9DE53FDCFC6B166D919FA4957E75544C77770DD37
SHA-512:	16EAF94B247B035666FD0FAA2998688DBA74829CB50E425D22280A6716B2C1286A0C6792A18EB5B604CD01E8877C1A9778472BF7A83564A4FDB899DDDF7A83A
Malicious:	false
Preview:	....(... ...@.....%...*...1...:...D#..Q4..X=..cH..hO..t_}..m{..vy..}y...s...z.....T"4j..x.....H.....I!.....m.....l.Q.. ..=.....P.....0..... ..=.....(.....Q..... ..n.....$!..]..... =.....B.....T1..... .....`+.....a...z.A.....1.....]..... .....S"#W..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Altronic LLC\DE-1550\DE-1550.lnk

Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, Icon number=0, ctime=Sun Dec 31 23:25:52 1600, mtime=Sun Dec 31 23:25:52 1600, atime=Sun Dec 31 23:25:52 1600, length=0, window=hide
Category:	dropped
Size (bytes):	3077
Entropy (8bit):	2.943614892697956
Encrypted:	false
SSDEEP:	48:8T1X3SiYUkyIDhOkMDQd9mOkMDOdu1XR/OkMD:8T1B4Ohf4Pf4OcD/f4
MD5:	E5CC45B468FD449A60EDD2A93BB1DFBA
SHA1:	4708CB476314EF8EFDC2F5A2D33BD9A860B1EC18
SHA-256:	136B05710FC1F64B45AB645A9EFFDAA071009658AF0CFD88CA7645436BCD125A
SHA-512:	8A24BF859532D76FA21C32FB5FFA97F5949D472B77B865C8D04B8C3F6FF6A67D87614884B47C4E667B01190422F63A8FCBD03B2D12A06501F1BA04B8B9945539
Malicious:	false
Preview:	L.....F.P.....y....P.O. .:i.....+00.../C:\.....x.1....."S...Users.d.....OwHuVo;.....u.....:.....8.U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....uVh;..user..>....."S.uVo;....3.....WS..A.r.t.h.u.r.....V.1....."S...AppData.@....."S.uVm;....B.....A!.A.p.p.D.a.t.a.....V.1....."S...Roaming.@....."S.uVi;....D.....R.o.a.m.i.n.g.....\.1.....uVu;..MICROS~1..D....."S.uVu;....E.....@$..M.i.c.r.o.s.o.f.t.....\.1.....uVu;..INSTAL~1..D.....uVu;uVu;....ja.....@$..I.n.s.t.a.l.l.e.r.....1.....uVu;..{78411~1..~.....uVu;uVu;....a.....{.7.8.4.1.1.D.F.8.-.D.B.1.8.-.4.7.7.4.-.A.9.F.4.-.A.5.D.6.D.0.D.A.7.8.7.C.}.....2.....uVu;!._8FE7F~1.EXE..h.....uVu;uVu;....a....._.8.F.E.7.F.6.A.C.6.2.5.1.2.8.0.A.F.C.5.8.3.7...e.x.e.....[.....\.....\.....\.....\.....\.....\.I

C:\Windows\Installer\118801b.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Create Time/Date: Mon Jun 21 08:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252, Template: Intel;1033, Number of Pages: 200, Revision Number: {F6296E9E-3D64-43FF-B0A4-736C96B15080}, Title: DE-1550 Installer, Author: Altronic LLC, Number of Words: 2, Last Saved Time/Date: Tue Jul 24 03:15:26 2018, Last Printed: Tue Jul 24 03:15:26 2018
Category:	dropped
Size (bytes):	544256
Entropy (8bit):	6.217058975674071
Encrypted:	false
SSDEEP:	6144:ded/UBn3Nn7ByILdEODIcOnlpOuodL+8sBn512bojn45S7Ix6XrU/X:8Jk3Nn7ByIuyBlpOuq+8sB512VcRXg
MD5:	08AF3AAC53F698F92B16583E6A76B2AA
SHA1:	F34527FE04EDED912253B494E4B7B9DC29150283
SHA-256:	CDEC38D9934EE64D57F09CE851DE1B9F3B4F823E4B7B5420A8C1254F53EABDEE
SHA-512:	13D9A8DEDE785FF6E1293A7B7251EC86AF6D2A71F0169700EB2837CB44C6C9FB7B1180837DFFDD28C013D42BDF119669B083F50D27FF18D26F9408231592EE2
Malicious:	false
Preview:	.....>.....8.....f...g...h...i...e.....`...a..... .....Z..... .....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...F...Q...:...;...<...=...>...?...@...A...B...C...D...Y...S...G...H...N...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...[...\...]..._...`...^...E...a...e...b...c...d.....R.....k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Windows\Installer\118801d.msi

Process:	C:\Windows\System32\msiexec.exe

File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Create Time/Date: Mon Jun 21 08:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252, Template: Intel;1033, Number of Pages: 200, Revision Number: {F6296E9E-3D64-43FF-B0A4-736C96B15080}, Title: DE-1550 Installer, Author: Altronic LLC, Number of Words: 2, Last Saved Time/Date: Tue Jul 24 03:15:26 2018, Last Printed: Tue Jul 24 03:15:26 2018
Category:	dropped
Size (bytes):	544256
Entropy (8bit):	6.217058975674071
Encrypted:	false
SSDEEP:	6144:ded/UBn3Nn7ByILdEODlcOnlpOuodL+8sBn512bojn45S7Ix6XrU/X:8Jk3Nn7ByIuyBlpOuq+8sB512VcRXg
MD5:	08AF3AAC53F698F92B16583E6A76B2AA
SHA1:	F34527FE04EDED912253B494E4B7B9DC29150283
SHA-256:	CDEC38D9934EE64D57F09CE851DE1B9F3B4F823E4B7B5420A8C1254F53EABDEE
SHA-512:	13D9A8DEDE785FF6E1293A7B7251EC86AF6D2A71F0169700EB2837CB44C6C9FB7B1180837DFFDD28C013D42BDF119669B083F50D27FF18D26F9408231592EE2
Malicious:	false
Preview:	.....>.....8.....f...g...h...i...e.....`...a..... .....Z..... .....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...F...Q...:...;...<...=...>...?...@...A...B...C...D...Y...S...G...H...N...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...[...\...]..._...`...^...E...a...e...b...c...d.....R.....k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Windows\Installer\MSI80E6.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	236872
Entropy (8bit):	6.42500790517661
Encrypted:	false
SSDEEP:	3072:Z7PyQaeLAxV9EcU95qWCn7B1kkJQGGhKTWAvdEhMqmc1wtI6M/CoKpixBrnQYaeW:8n3Nn7ByILdEODlcOnlpOuodL+8Y
MD5:	0A2626FC9E4E0CA18386C029E9EFFFD9
SHA1:	AC5576497AFAC2456F485CDB14BF52D895769651
SHA-256:	97A55524E0BF06419143B1B71778C0EC867716079AB477E8404A0F3125DA7DC3
SHA-512:	40B25E507E64B5634E13E83D4BC420196B1294D533E60B01DAE8898A8EED939417AEC8341B409F59A722D14FB63884C24C5A31985DA63933B761F1FC3ACB24D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S/...N...N...N..0....N..p8E..N...6l..N..x8D.+N..x8q..N..x8E.N...6|..N...N..FO..p8D..N..p8t..N..p8u..N..p8r..N..Rich.N.....PE..L.....K....."!..... .....~.....0.....A.....U....@.....#...D .....8.....H..... .....@.....text..... ....`.data....H...0.....$.....@....rsrc...8.....>.....@..@.reloc...@.....B...D..... .....@..B.....

C:\Windows\Installer\MSI81A2.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	236872
Entropy (8bit):	6.42500790517661
Encrypted:	false
SSDEEP:	3072:Z7PyQaeLAxV9EcU95qWCn7B1kkJQGGhKTWAvdEhMqmc1wtI6M/CoKpixBrnQYaeW:8n3Nn7ByILdEODlcOnlpOuodL+8Y
MD5:	0A2626FC9E4E0CA18386C029E9EFFFD9
SHA1:	AC5576497AFAC2456F485CDB14BF52D895769651
SHA-256:	97A55524E0BF06419143B1B71778C0EC867716079AB477E8404A0F3125DA7DC3
SHA-512:	40B25E507E64B5634E13E83D4BC420196B1294D533E60B01DAE8898A8EED939417AEC8341B409F59A722D14FB63884C24C5A31985DA63933B761F1FC3ACB24D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S/...N...N...N..0....N..p8E..N...6l..N..x8D.+N..x8q..N..x8E.N...6|..N...N..FO..p8D..N..p8t..N..p8u..N..p8r..N..Rich.N.....PE..L.....K....."!..... .....~.....0.....A.....U....@.....#...D .....8.....H..... .....@.....text..... ....`.data....H...0.....$.....@....rsrc...8.....>.....@..@.reloc...@.....B...D..... .....@..B.....

C:\Windows\Installer\MSI8211.tmp

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

Category:	dropped
Size (bytes):	5275
Entropy (8bit):	5.853728524636617
Encrypted:	false
SSDEEP:	96:STMTDjVUbyJ9fGxsMZteG+sQPQphvweXQqKib3w56EPv:SApHT5rp2SeXz5Wv
MD5:	B886CF6073879A845B0794954B9BE035
SHA1:	A9B47E19999111C824B827967CFE8F51EAB42A3A
SHA-256:	AB3092933C89843F3C9914AF4DC161F744CB06F8F4ED6B87597825B53715F809
SHA-512:	CAA8EAEB4D4307CD1D1C5F3870C6C77615B044690090EBFA6847E16D24B32BF76169FF4B287825C9418BAC3081829E4C5CB161E3A7BAC123C0806664E495982
Malicious:	false
Preview:	...@IXOS.@.....@u;uV.@.....@.....@.....@.....@.....@......&.{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}..Altronic DE-1550+.DE-1550 Installer v1.03_rev1 07-23-2018.msi.@.....@.....@.....@.....@.....&.{F6296E9E-3D64-43FF-B0A4-736C96B15080}.....@.....@.....@.....@.....@.....@.....@.....@.....@.....Altronic DE-1550.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....@.....ProcessComponents..Updating component registration.....@.....@.....@.]....&.{FBEE690E-63CA-9123-3429-448ED52CA353}T.C:\Program Files (x86)\Altronic LLC\Altronic DE-1550\Configuration Files\DEFAULT.trd.@.....@.....@.....@.....@.....&.{6DA9B1AE-EC52-644E-A521-C6CA345CA92A}T.C:\Program Files (x86)\Altronic LLC\Altronic DE-1550\Configuration Files\DEFAULT.afd.@.....@.....@.....@.....@.....&.{511939AB-4664-F9F3-9CAC-7D981D8D374C}A.C:\Program Files (x86)\Altronic LLC\Altronic DE-1550\Altronic.ico.@.....@.....@.....@.....@.....&.{B9B828B7-EE55-8389-D0EC-44437CC85274}T.C:\Program Files (x86)\Alt

C:\Windows\Installer\SourceHash{78411DF8-DB18-4774-A9F4-A5D6D0DA787C}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1810288556150716
Encrypted:	false
SSDEEP:	12:JSbX72FjHJAGiLIlHVRpGh/77777777777777777777777vDHFrEtNXFDUT9lN:JFJQI5+REtFZZF
MD5:	3E49C888580AA400ED1B9602A70FF416
SHA1:	D18E4B981F989C841D6926601EB406416332F878
SHA-256:	4C5EB78BB000C735955D1472D3C15B3D0B112BB9EF31594AD63D5D5EE4D3A39D
SHA-512:	7BC9784A4966864E659DD2135FC16B9337E2099FA3B7EF32AE0A01847DA7D65EB2E5B8E93443BF0F3F386E8D888376C39A6385C47EB76B53D497CE72E5EF01EC
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\inprogressinstallinfo.ipi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.9216879163588387
Encrypted:	false
SSDEEP:	48:d8PhJuRc06WX44nT5gR6YOQwQ8SkdymdhCyUFCyT5lQ4pW5lQ4goOirDSkddmdhG:AhJ1InT5YOQSFCbFCe1CwCbFCU
MD5:	6EB9B3FD409ECB8793C3C1A3BBF60338
SHA1:	55D018FB509A7D0F73E341E917C21C386CCD9841
SHA-256:	8FB033DCC4823281B1E1899CB632487F9D4C538B63CA06646F0A380A2487EABE
SHA-512:	71F4B8BA2069A6A02BB5EBC762D1915FF89D12ED458C25A6E0CF99A9A6A4AB7BB36A68BC22150064316059FAA7A7A742CB53B345BD45E873752C9FEDDCCB0B5B
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	631722
Entropy (8bit):	5.404008132491027
Encrypted:	false

SSDEEP:	3072:76sAoN1IAMVcB6J3l7NPh7sOyQSiMbRolrNWG6x+Rkeov8Qj9lOx2s9OW1LRuuGI:TFfxq8RfKF0Dui869jc
MD5:	E6AC735A3AC9C3524062BB08B3C68054
SHA1:	247F2F4EE1207BE61763CCB6A3627DA5E45687B7
SHA-256:	D3BACFF677DE6A3A4DBC1959E36EE0835BB0F6E2AEBE2B226E55BBA3DD6BAF28
SHA-512:	3B89689640EC99C2C429A77C673B0E93F9582F3F5FCFB6F8E92EF9EED8A8E290F08DA15C6311D1BB791BA34FFFF2CCE298190A07071F6485443573135C10B56F
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..12/07/2019 09:59:37.236 [4684]: Command line: D:\wd\compilerTemp\BMT.i51yo0aa.beh\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe executeQueuedItems /nologo ..12/07/2019 09:59:37.255 [4684]: Executing command from offline queue: install "System.Runtime.WindowsRuntime.UI.Xaml, Version=4.0.0.0, Culture=Neutral, PublicKeyToken=b77a5c561934e089, processorArchitecture=msil" /NoDependencies /queue:1..12/07/2019 09:59:37.299 [4684]: Executing command from offline queue: install "System.Web.ApplicationServices, Version=4.0.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil" /NoDependencies /queue:3..12/07/2019 09:59:37.299 [4684]: Exclusion list entry found for System.Web.ApplicationServices, Version=4.0.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil; it will not be installed..12/07/2019 09:59:37.299 [

C:\Windows\Temp\~DF164F575F959CA334.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.5122973476959292
Encrypted:	false
SSDEEP:	48:wRyxuxM+fFX4fT5hUpGylR6YOQwQ8SkdymdhCyUFCyT5lQ4pW5lQ4goOirDSkddN:w4xu8TXeGbYOQSFCbFCe1CwCbFCU
MD5:	CD2899B31400FF4BC5EEC98EE0458ED2
SHA1:	93C87C34DD84A9CAEB2A941EF098D04C6C2296CD
SHA-256:	5E688E2878BA4302AD4293DE7EC3202ADF0F71DD7414284BDD9826AF6937DC9D
SHA-512:	F416C14333196C984EC1B436A10845FA9A851C5FB52CF4B5FEEA9E8547D24AD60057750E80467EADE9DF205CCE0B911E7C96308C5599FE59B7200E61F03BA69
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF1AD6B9B44D290FF8.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF22D2B4B04A4971FD.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE

Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF23FA9ACE23FCD44B.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.9216879163588387
Encrypted:	false
SSDEEP:	48:d8PhJuRc06WX44nT5gR6YOQwQ8SkdymdhCyUFCyT5lQ4pW5lQ4goOirDSkddmdhG:AhJ1InT5YOQSFCbFCe1CwCbFCU
MD5:	6EB9B3FD409ECB8793C3C1A3BBF60338
SHA1:	55D018FB509A7D0F73E341E917C21C386CCD9841
SHA-256:	8FB033DCC4823281B1E1899CB632487F9D4C538B63CA06646F0A380A2487EABE
SHA-512:	71F4B8BA2069A6A02BB5EBC762D1915FF89D12ED458C25A6E0CF99A9A6A4AB7BB36A68BC22150064316059FAA7A7A742CB53B345BD45E873752C9FEDDCCB0B5B
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DF7B53429BE2301499.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF8B370F716CC75002.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.2874584793142082
Encrypted:	false
SSDEEP:	48:Nk1T+SkddmdhCyUFCyqSkdymdhCyUFCyT5lQ4pW5lQ4goOirawQS5R6Y:yMwCbFChFCbFCe1DgyY
MD5:	C1332DA97E0756551DD56435602B193C
SHA1:	AF9120D7E49CEF297BC25FBF9CAB844714967049
SHA-256:	5F36A4415B9E0C12BD7514212816A5E76DE2A7619A363594F216629B8FC4933A
SHA-512:	67B0DACA0E10DB1AE64DF78BD90070092DE9C461C153E06E8A9236701E18F1722DAE675D51DEBC034D6A9FF1922F71AFA7093CCDDAE941B509D9040EF8C21B29
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFA27904E46FB322E6.TMP

Process:	C:\Windows\System32\msiexec.exe

File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.5122973476959292
Encrypted:	false
SSDEEP:	48:wRyxuxM+fFX4fT5hUpGylR6YOQwQ8SkdymdhCyUFCyT5lQ4pW5lQ4goOirDSkddN:w4xu8TXeGbYOQSFCbFCe1CwCbFCU
MD5:	CD2899B31400FF4BC5EEC98EE0458ED2
SHA1:	93C87C34DD84A9CAEB2A941EF098D04C6C2296CD
SHA-256:	5E688E2878BA4302AD4293DE7EC3202ADF0F71DD7414284BDD9826AF6937DC9D
SHA-512:	F416C14333196C984EC1B436A10845FA9A851C5FB52CF4B5FEEA9E8547D24AD60057750E80467EADE9DF205CCE0B911E7C96308C5599FE59B7200E61F03BA69
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFAC25A1076C4CE445.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.08397466654906285
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOJgQEEB2QgXFTvUtqVky6l9:2F0i8n0itFzDHFrEtNXFDUT9
MD5:	1283FCAD05C3DA463169C2AA56A9DF7F
SHA1:	CE2E47BB22B8194734E6F2E19DC1B3E18E4B4558
SHA-256:	3D48FE70567A8406C89D1A1A83C21CA51CD64A70B3C1EC675024DA72E5D3AD60
SHA-512:	0CBB263DFA3D6BC6AFB7F0057A0C47EA6A432CA0D7CB8FDD58071D6494B76AFD409B8791BEBE252927B6700ADA4715D7D3C3DF8E4E0FC419409991E2EF244 04
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFB0DDA37AD60475C1.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.5122973476959292
Encrypted:	false
SSDEEP:	48:wRyxuxM+fFX4fT5hUpGylR6YOQwQ8SkdymdhCyUFCyT5lQ4pW5lQ4goOirDSkddN:w4xu8TXeGbYOQSFCbFCe1CwCbFCU
MD5:	CD2899B31400FF4BC5EEC98EE0458ED2
SHA1:	93C87C34DD84A9CAEB2A941EF098D04C6C2296CD
SHA-256:	5E688E2878BA4302AD4293DE7EC3202ADF0F71DD7414284BDD9826AF6937DC9D
SHA-512:	F416C14333196C984EC1B436A10845FA9A851C5FB52CF4B5FEEA9E8547D24AD60057750E80467EADE9DF205CCE0B911E7C96308C5599FE59B7200E61F03BA69
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFC2CAB2504A990051.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.9216879163588387
Encrypted:	false
SSDEEP:	48:d8PhJuRc06WX44nT5gR6YOQwQ8SkdymdhCyUFCyT5lQ4pW5lQ4goOirDSkddmdhG:AhJ1InT5YOQSFCbFCe1CwCbFCU
MD5:	6EB9B3FD409ECB8793C3C1A3BBF60338

SHA1:	55D018FB509A7D0F73E341E917C21C386CCD9841
SHA-256:	8FB033DCC4823281B1E1899CB632487F9D4C538B63CA06646F0A380A2487EABE
SHA-512:	71F4B8BA2069A6A02BB5EBC762D1915FF89D12ED458C25A6E0CF99A9A6A4AB7BB36A68BC22150064316059FAA7A7A742CB53B345BD45E873752C9FEDDCCB0B5B
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFD60CD8828C653DCD.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFEBA6A2164AD9C55F.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Create Time/Date: Mon Jun 21 08:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252, Template: Intel;1033, Number of Pages: 200, Revision Number: {F6296E9E-3D64-43FF-B0A4-736C96B15080}, Title: DE-1550 Installer, Author: Altronic LLC, Number of Words: 2, Last Saved Time/Date: Tue Jul 24 03:15:26 2018, Last Printed: Tue Jul 24 03:15:26 2018
Entropy (8bit):	6.217058975674071
TrID:	• Microsoft Windows Installer (77509/1) 90.64% • Generic OLE2 / Multistream Compound File (8008/1) 9.36%
File name:	DE-1550 Installer v1.03_rev1 07-23-2018.msi
File size:	544256
MD5:	08af3aac53f698f92b16583e6a76b2aa
SHA1:	f34527fe04eded912253b494e4b7b9dc29150283
SHA256:	cdec38d9934ee64d57f09ce851de1b9f3b4f823e4b7b5420a8c1254f53eabdee
SHA512:	13d9a8dede785ff6e1293a7b7251ec86af6d2a71f0169700eb2837cb44c6c9fb7b1180837dffdd28c013d42bdf119669b083f50d27ff18d26f9408231592ee22
SSDEEP:	6144:ded/UBn3Nn7ByILdEODlcOnlpOuodL+8sBn512bojn45S7Ix6XrU/X:8Jk3Nn7ByIuyBlpOuq+8sB512VcRXg

TLSH:	31C4AD2136C79B32D4D3127156BEA3704A7EEC304B7082C7A2987B9E6EB56C06735787
File Content Preview:	.....>.....8.....f...g...h...i...e.....`...a.....

File Icon

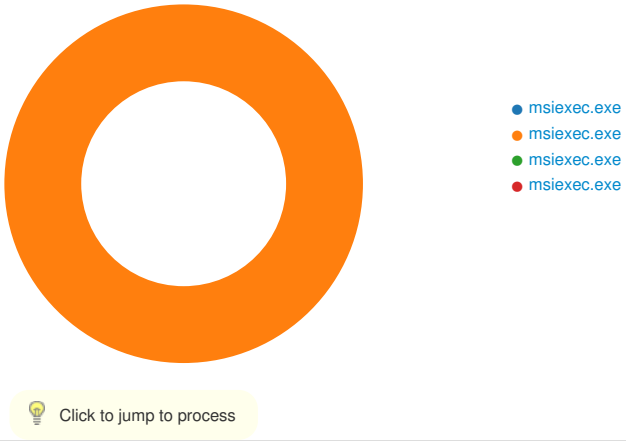
Icon Hash:	a2a0b496b2caca72

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: msiexec.exe PID: **8324**, Parent PID: **4648**

General

Target ID:	2
Start time:	07:27:30
Start date:	21/03/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\DE-1550 Installer v1.03_rev1 07-23-2018.msi"
Imagebase:	0x7ff73cc90000
File size:	69632 bytes
MD5 hash:	E5DA170027542E25EDE42FC54C929077
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: msiexec.exe PID: **2040**, Parent PID: **936**

General

Target ID:	3
Start time:	07:27:30
Start date:	21/03/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff73cc90000
File size:	69632 bytes
MD5 hash:	E5DA170027542E25EDE42FC54C929077
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	631628	94	30 33 2f 32 31 2f 32 30 32 33 20 30 37 3a 32 37 3a 34 31 2e 30 36 37 20 5b 32 30 34 30 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	03/21/2023 07:27:41.067 [2040]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFFF405CB65	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FFFF405C763	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: msiexec.exe PID: **8944**, Parent PID: **2040**

General

Target ID:	5
Start time:	07:27:30
Start date:	21/03/2023
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 84DA78192880581D6829482FFD39CF6A C
Imagebase:	0xc40000
File size:	59904 bytes
MD5 hash:	9D09DC1EDA745A5F87553048E57620CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **560**, Parent PID: **2040**

General

Target ID:	8
Start time:	07:27:41
Start date:	21/03/2023
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding C6401D95ECC4BE08AAC131C3978679E2
Imagebase:	0x7ff6fb380000
File size:	59904 bytes
MD5 hash:	9D09DC1EDA745A5F87553048E57620CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly