xcitium

MALWARE
Xcitium Final Verdict

File Name: Trojan.Autorun.ATA_virussign.com_48355a334300662fdb2771c1e73f9f92.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 888a10a075de2e80faab1faee31efa7f9ed085e8
MD5: 48355a334300662fdb2771c1e73f9f92
First Seen Date: 2023-12-21 11:06:38 UTC
Number of Clients Seen: 2
Last Analysis Date: 2023-12-21 16:42:35 UTC
Human Expert Analysis Date: 2023-12-21 16:42:28 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-12-21 12:18:38 UTC	Malware
Static Analysis Overall Verdict	2023-12-21 16:42:35 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-12-21 16:42:35 UTC	No Match
Human Expert Analysis Overall Verdict	2023-12-21 16:42:28 UTC	Malware
File Certificate Validation		Not Applicable

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Suspicious
Timestamp value suspicious	Clean
Header Checksum is zero!	Suspicious
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Suspicious
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Anti-vm present	Clean
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean
TLS callback functions array detected	Clean

Packer detection on signature database

UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus & Laszlo [overlay]

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise NI Detector 3	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise PUA Detector 6	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 13	2023-12-21 11:06:34 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2023-12-21 11:06:34 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-12-21 12:13:27 UTC
Analysis End Date: 2023-12-21 16:42:28 UTC
File Upload Date: 2023-12-21 11:06:21 UTC
Human Expert Analyst Feedback:
Verdict: Malware
Malware Family:
Malware Type: Trojan Generic

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5CD8AE36 [Sun May 12 23:37:26 2019 UTC]
Debug Artifacts	
Entry Point	0x534260 (UPX1)
Exifinfo	[object Object]
File Size	738400
File Type Enum	6
Imphash	fc6683d30d9f25244a50fd5357825e79
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	setupugc
File Version	110.713.104.654
Company Name	ktmutil
Product Name	bridgeres
Product Version	812.318.935.877
File Description	DPTopologyAppv2_0
Original Filename	AuditPolicyGPInterop
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	849b06f614b659620d5f913800c04dbe3c1ab687e202f0b850cf95f22b7fd786
Ssdeep	12288:DquErHF6xC9D6DmR1J98w4oknqOKw/zTd1RVaHvymUi6rjXrm62iU952aLovi75Q:arl6kD68JmloO7TdNaPymUi63i62xHLc
Trid	38.2,UPX compressed Win32 Executable,37.5,Win32 EXE Yoda's Crypter,9.2,Win32 Dynamic Link Library (generic),6.3,Win32 Executable (generic),2.8,OS/2 Executable (generic)

File Paths

FILE PATH ON CLIENT	SEEN COUNT
Trojan.Autorun.ATA_virussign.com_48355a334300662fdb2771c1e73f9f92.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0xde000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0xdf000	0x56000	0x55600	7.93500339093	7ae4b184fd5ef0b7aa26a58a3f42e2e2
.rsrc	0x135000	0x5f000	0x5e600	7.65562561081	46e843f20c19aa3ca9cb2b288db13fcf