ID: 458974
Sample Name: TMB1fxNaqR
Cookbook: default.jbs
Time: 23:37:18
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

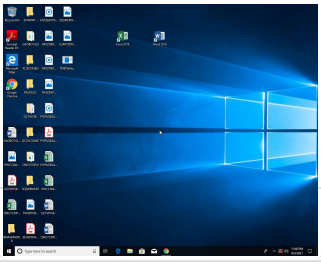
Windows Analysis Report TMB1fxNaqR

Overview

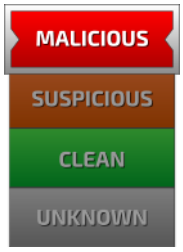
General Information

Sample Name:	TMB1fxNaqR (renamed file extension from none to exe)
Analysis ID:	458974
MD5:	a92922a71a9bf58.
SHA1:	f419ba1e6da5dfc..
SHA256:	213ea943865069..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

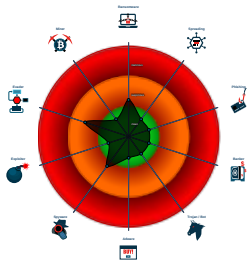


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Creates processes via WMI
- Contains functionality to dynamically…
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function
- Dropped file seen in connection with…
- Drops PE files
- Found dropped PE file which has no…
- IP address seen in connection with o

Classification



Process Tree

- **System is w10x64**
- TMB1fxNaqR.exe (PID: 1740 cmdline: 'C:\Users\user\Desktop\TMB1fxNaqR.exe' MD5: A92922A71A9BF58CC2D95A6039C9A1B6)
  - conhost.exe (PID: 2332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - TMB1fxNaqR.exe (PID: 4704 cmdline: 'C:\Users\user\Desktop\TMB1fxNaqR.exe' -a MD5: A92922A71A9BF58CC2D95A6039C9A1B6)
    - conhost.exe (PID: 5376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

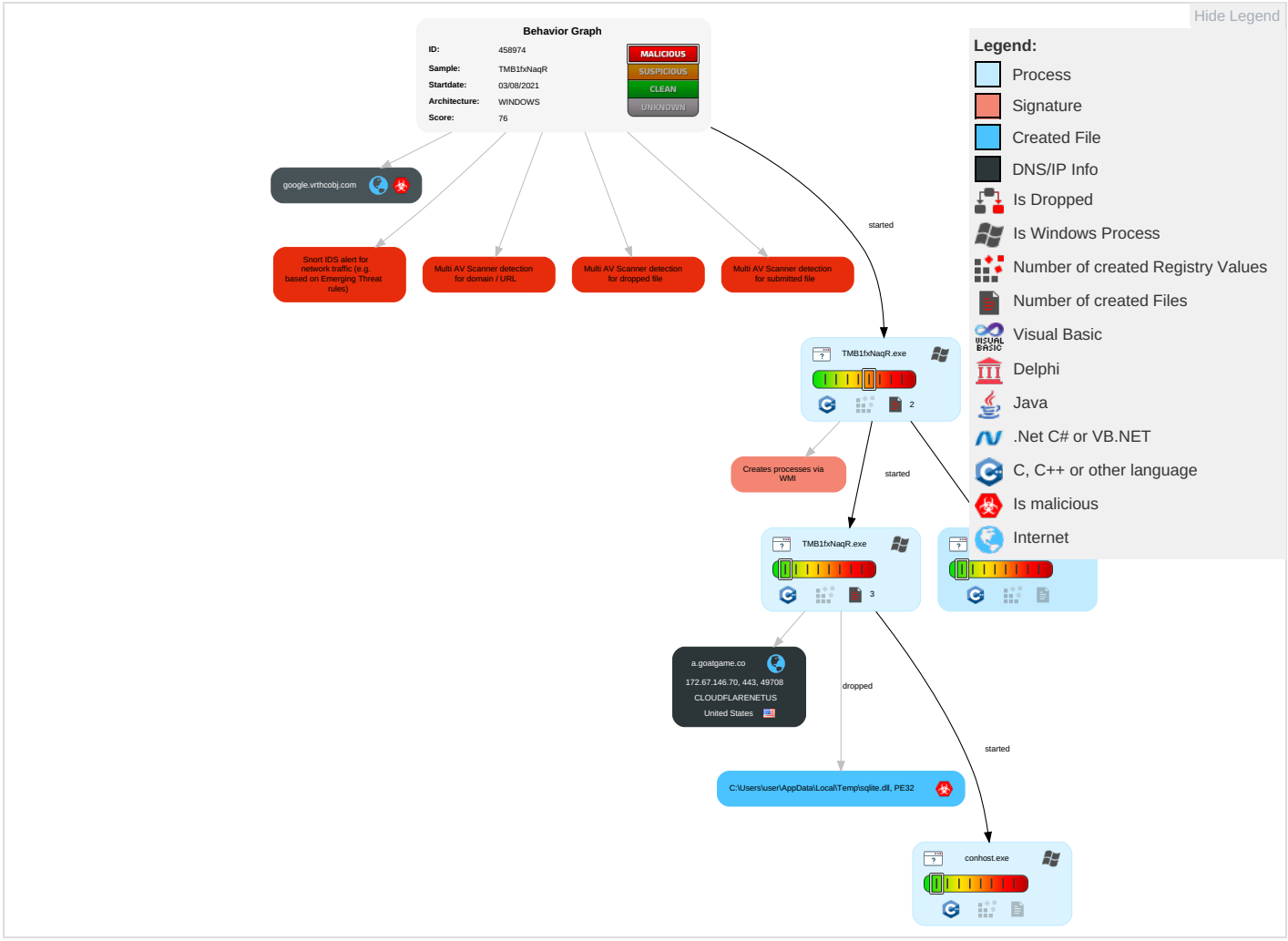
Persistence and Installation Behavior:

Creates processes via WMI

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1	Input Capture 1	Security Software Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Networ Commu
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service

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
TMB1fxNaqR.exe	45%	Virustotal		Browse
TMB1fxNaqR.exe	59%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\sqlite.dll	14%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\sqlite.dll	15%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
google.vrthcobj.com	8%	Virustotal		Browse
a.goatgame.co	2%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.vrthcobj.com	34.97.69.225	true	true	• 8%, Virustotal, Browse	unknown
a.goatgame.co	172.67.146.70	true	false	• 2%, Virustotal, Browse	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.146.70	a.goatgame.co	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458974
Start date:	03.08.2021
Start time:	23:37:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TMB1fxNaqR (renamed file extension from none to 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:	27
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:	mal76.winEXE@5/2@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 93.6%) • Quality average: 79.3% • Quality standard deviation: 28.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:38:09	API Interceptor	4x Sleep call for process: TMB1fxNaqR.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.146.70	LRios3pM39.exe	Get hash	malicious	Browse	
	85d8c.exe	Get hash	malicious	Browse	
	QfVER41Fwx.exe	Get hash	malicious	Browse	
	O3h9kRdG7d.exe	Get hash	malicious	Browse	
	1A263B2603212FF1E492D9E0C718F12601789E27EAABA.exe	Get hash	malicious	Browse	
	U7HCBc2SVy.exe	Get hash	malicious	Browse	
	76xAf6BYg8.exe	Get hash	malicious	Browse	
	E4lwAiXNCE.exe	Get hash	malicious	Browse	
	pLF8TJmHlD.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
google.vrthcobj.com	LRios3pM39.exe	Get hash	malicious	Browse	• 34.97.69.225
	85d8c.exe	Get hash	malicious	Browse	• 34.97.69.225
	QfVER41Fwx.exe	Get hash	malicious	Browse	• 34.97.69.225
	93ejLcdBh5.exe	Get hash	malicious	Browse	• 34.97.69.225
	k2VFD3gNGE.exe	Get hash	malicious	Browse	• 34.97.69.225
	MIN56KgzBN.exe	Get hash	malicious	Browse	• 34.97.69.225
	U7HCBc2SVy.exe	Get hash	malicious	Browse	• 34.97.69.225
	TIoFSlDlv6.exe	Get hash	malicious	Browse	• 34.97.69.225
	76xAf6BYg8.exe	Get hash	malicious	Browse	• 34.97.69.225
	E4lwAiXNCE.exe	Get hash	malicious	Browse	• 34.97.69.225
	pLF8TJmHlD.exe	Get hash	malicious	Browse	• 34.97.69.225
	sonia_6.exe	Get hash	malicious	Browse	• 34.97.69.225
	5H4iRfY1ek.exe	Get hash	malicious	Browse	• 34.97.69.225
	Copy.exe	Get hash	malicious	Browse	• 34.97.69.225
	pMVkvSyeIy.exe	Get hash	malicious	Browse	• 34.97.69.225
	w7pR0EOMwd.exe	Get hash	malicious	Browse	• 34.97.69.225
	BoLQVCmlZB.exe	Get hash	malicious	Browse	• 34.97.69.225
	DhWFvSKvSb.exe	Get hash	malicious	Browse	• 34.97.69.225
	U2HHCJvDj4.exe	Get hash	malicious	Browse	• 34.97.69.225
	CLnraL1yNc.exe	Get hash	malicious	Browse	• 34.97.69.225
a.goatgame.co	LRios3pM39.exe	Get hash	malicious	Browse	• 172.67.146.70
	85d8c.exe	Get hash	malicious	Browse	• 104.21.79.144
	85d8c.exe	Get hash	malicious	Browse	• 172.67.146.70
	QfVER41Fwx.exe	Get hash	malicious	Browse	• 172.67.146.70
	O3h9kRdG7d.exe	Get hash	malicious	Browse	• 172.67.146.70
	puzlXYxqKK.exe	Get hash	malicious	Browse	• 104.21.79.144
	k2VFD3gNGE.exe	Get hash	malicious	Browse	• 104.21.79.144
	MIN56KgzBN.exe	Get hash	malicious	Browse	• 104.21.79.144
	U7HCBc2SVy.exe	Get hash	malicious	Browse	• 172.67.146.70
	TIoFSlDlv6.exe	Get hash	malicious	Browse	• 104.21.79.144
	76xAf6BYg8.exe	Get hash	malicious	Browse	• 172.67.146.70
	E4lwAiXNCE.exe	Get hash	malicious	Browse	• 172.67.146.70
	pLF8TJmHlD.exe	Get hash	malicious	Browse	• 172.67.146.70
	sonia_6.exe	Get hash	malicious	Browse	• 104.21.79.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	LRios3pM39.exe	Get hash	malicious	Browse	• 172.67.146.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	State Settlement Copy.html	Get hash	malicious	Browse	• 172.67.75.3
	Request Quotation.exe	Get hash	malicious	Browse	• 172.67.188.154
	invoice.vbs	Get hash	malicious	Browse	• 162.159.130.233
	kKZZ0J8y0c.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ 29.exe	Get hash	malicious	Browse	• 104.21.19.200
	ATT80307.HTM	Get hash	malicious	Browse	• 104.16.19.94
	2C.TA9.HTML	Get hash	malicious	Browse	• 104.18.11.207
	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	• 172.67.145.176
	RoyalMail_Requestform0729.exe	Get hash	malicious	Browse	• 172.67.188.154
	sbcss_Richard.DeNava_#inv0549387TWQYqzTP aYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	• 104.16.18.94
	Fake.HTM	Get hash	malicious	Browse	• 104.16.19.94
	RoyalMail_Requestform1.exe	Get hash	malicious	Browse	• 172.67.188.154
	Nouveau bon de commande. 3007021_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	MFS0175, MFS0117 MFS0194.exe	Get hash	malicious	Browse	• 172.67.188.154
	ORIGINAL PROFORMA INVOICE COAU7220898130,PDF.exe	Get hash	malicious	Browse	• 172.67.176.89
	Purchase Requirements.exe	Get hash	malicious	Browse	• 23.227.38.74
	items.doc	Get hash	malicious	Browse	• 104.21.19.200
	ZI09484474344.exe	Get hash	malicious	Browse	• 104.21.49.41
	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	• 104.16.19.94

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	LRios3pM39.exe	Get hash	malicious	Browse	• 172.67.146.70
	24um7vU1BD.exe	Get hash	malicious	Browse	• 172.67.146.70
	JQ2bNBDOcO.exe	Get hash	malicious	Browse	• 172.67.146.70
	Dpwipnj1gx.exe	Get hash	malicious	Browse	• 172.67.146.70
	19G1ZLyqr2.exe	Get hash	malicious	Browse	• 172.67.146.70
	ULylDR5F36.exe	Get hash	malicious	Browse	• 172.67.146.70
	SecuriteInfo.com.W32.AIDetect.malware2.26285.exe	Get hash	malicious	Browse	• 172.67.146.70
	banload.msi	Get hash	malicious	Browse	• 172.67.146.70
	yQShMhZ7Hi.exe	Get hash	malicious	Browse	• 172.67.146.70
	zW4oE2ASRB.exe	Get hash	malicious	Browse	• 172.67.146.70
	run.exe	Get hash	malicious	Browse	• 172.67.146.70
	RNrtE1qOSL.exe	Get hash	malicious	Browse	• 172.67.146.70
	hDJzf1oo7U.exe	Get hash	malicious	Browse	• 172.67.146.70
	hpDcwMoScr.exe	Get hash	malicious	Browse	• 172.67.146.70
	JGJtVyC9dr.exe	Get hash	malicious	Browse	• 172.67.146.70
	QqcQ1EteWS.exe	Get hash	malicious	Browse	• 172.67.146.70
	Ya50avl5OT.exe	Get hash	malicious	Browse	• 172.67.146.70
	8xCetBLoAt.exe	Get hash	malicious	Browse	• 172.67.146.70
	7xt9iOfzN2.exe	Get hash	malicious	Browse	• 172.67.146.70
	5mTnLT28B7.exe	Get hash	malicious	Browse	• 172.67.146.70

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\sqlite.dll	LRios3pM39.exe	Get hash	malicious	Browse	
	CyLELjM5zk.exe	Get hash	malicious	Browse	
	setup_x86_x64_install.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\sqlite.dat	
Process:	C:\Users\user\Desktop\TMB1fxNaqR.exe
File Type:	data
Category:	dropped
Size (bytes):	578669
Entropy (8bit):	7.965453587440716

C:\Users\user\AppData\Local\Temp\sqlite.dat	
Encrypted:	false
SSDEEP:	12288:C11ticqWIMMXa2ad3KNjZi+VUYgokNxcg8aVg1gKtY7SQgCO:ePeBaRKNjoklalbVygKtY7xgd
MD5:	C78BF51EE294161707A6766E71CEE582
SHA1:	3BB4FF0B06FC5B3753AB39F21E959895834BF7F8
SHA-256:	BE449F187EC6EE4C4FA40642E698FFA3BFA19EC08848F4E0273B70427A1F1FC2
SHA-512:	B2D7D6D8C12B0DBDD677BC8ACD764AB0687E976268E46F461B98C5CF941197785B5D5718D2E3A734EAE49B0D358064EE23D9AAE217AF5F98DA5252A8A11D53D
Malicious:	false
Reputation:	low
Preview:	.<..Hh.j...?...O}3..8v,)cml.T/.....V.r.....n.?y..oz#V.....N.{.....!....Y."..)v.T.....Ub.V..*.)..8...%.{4.yWrA.a36&..,...V...l9.y....39.y...wW.j.ox.....I..;..%..p.b..>..j.....j..awT..r...j....o./.7...,=uk..i../h..j*j.P.j..?.-X.k..R}.j.5.b-F.k..c.....j...j..Q?...).qe.....,o'k.....j.J..))O.....k..\.....u,..k...,..k....k...tOT.X.jXe-.k..7.k...83U.....%..o.....Y%.....7.F.(j...KP..I..j..y...o..no...z.....u/..DJP.e+.Dj..Z....k.....j$T.X.j[..`....o....k{..2|6...H.....c%.....z.....~^..j.-s.....o.-.....6.L.`.j.-s.....i|..y.Q'....k...}FT.X.jY..Y....o.....y..=|6..%..z/.....s....>.j.-s.k../.:.....>|/...h...2/..R..-.....k....9.y.....j.6Z.j.o....l&..%.UD..`....&..t>".6g..j,..../W=..5...n.....X..h>.k..'...|/h..jfDX.S...`&*...Y....)U]bc[.....'(..I..+....b.i....[...If!S...r.....i.....Q^..*.....aeddT.`.'....*.[.h....e...?>....n....5.....-..j..T..ow.....k....-...k16.+i(~..L....j,...c.L./w=j...~./

C:\Users\user\AppData\Local\Temp\sqlite.dll	
Process:	C:\Users\user\Desktop\TMB1fxNaqR.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	81408
Entropy (8bit):	6.295064838876099
Encrypted:	false
SSDEEP:	1536:jkOh0YR+kfbE+2AJk64OceTbkS9Co5sWzcdSzEdY+wJpxpbcNop//:jkcjHY+fJhPN9H2SIdY+wJpxpQ8//
MD5:	05250AA12AD3C6A86DAB6DAB708D17FF
SHA1:	E41AD72C9A43070BB11FD7411800F71DDDF6BDD8
SHA-256:	7250A8A1B98D09BE823CD6EFD30D85E5418DFC3541D220BB0694DFCC547478BD
SHA-512:	A56DF11AF5243150753154E1CBA74E3CDD0CDECF09269B88A3944AC12B73DE59909CE6DBBBD3B1B6DA691D144FAC2599645B2017F66BAC64A106437168EC388
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 15%
Joe Sandbox View:	• Filename: LRios3pM39.exe, Detection: malicious, Browse • Filename: CyLELjM5zk.exe, Detection: malicious, Browse • Filename: setup_x86_x64_install.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V..f.x.5.x.5.x.5..r5.x.5..p5dx.5..q5.x.5@..4.x.5@..4.x.5@..4.x.5...5.x.5.x.5Jx.5...4.x.5...4.x.5..|5.x.5...4.x.5Rich.x.5.....PE..L...f@.a.....!.....8.....p.....@.....&..L...<'..(....P.....`..... ...p.....0.....@.....text...M..... ..`.rdata...]....^.....@..@.data.....0..... .....@....rsrc.....P.....(.....@..@.reloc.....`.....@..B.....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	4.581071120397606
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	TMB1fxNaqR.exe
File size:	57344
MD5:	a92922a71a9bf58cc2d95a6039c9a1b6
SHA1:	f419ba1e6da5dfc295857598e44b0a4eb0b3ecfc
SHA256:	213ea943865069cf1210a58860c619a8fa8928258abe8919fee8180feafea547
SHA512:	0bb8f350ab4ba4570806b70e6bf82d986782d4635f5058eaf8c36550b1ba9e3bd6b6e5df098fbb9167dece0684bbae047824822bb55f54ee8a17993f29fd8007
SSDEEP:	768:URFJRVA3O2pxNojkTnJQ6XWzQjkpC/xbjNxxuCqXKClZt9:MMoITVXGpC5bpHPmlZt9

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$......../Q..N?..N?..N?.CF`..N?..l4..N?.NR1..N?..h4..N?..h5..N?.NFb..N?..N>..N?..m...N?.Rich.N?.....PE..L...RF.a.....p.

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40268e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x61074652 [Mon Aug 2 01:11:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	2cdeda7a0aa27475a825e9c41d4d95f0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6bb7	0x7000	False	0.593296595982	data	6.44358253732	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1186	0x2000	False	0.270629882812	data	3.63030337834	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x365c	0x3000	False	0.0801595052083	data	0.843436221473	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xe000	0x1000	0x1000	False	0.111083984375	data	1.09363315293	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-23:38:25.660129	UDP	1948	DNS zone transfer UDP	58824	53	192.168.2.3	34.97.69.225
08/03/21-23:38:31.551839	UDP	1948	DNS zone transfer UDP	58824	53	192.168.2.3	34.97.69.225
08/03/21-23:38:39.386795	UDP	1948	DNS zone transfer UDP	58824	53	192.168.2.3	34.97.69.225
08/03/21-23:38:50.171576	UDP	1948	DNS zone transfer UDP	58824	53	192.168.2.3	34.97.69.225

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 23:38:06.049623966 CEST	192.168.2.3	8.8.8.8	0x9251	Standard query (0)	a.goatgame.co	A (IP address)	IN (0x0001)
Aug 3, 2021 23:38:14.363015890 CEST	192.168.2.3	8.8.8.8	0xc59	Standard query (0)	google.vrthcobj.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:38:14.364244938 CEST	192.168.2.3	8.8.8.8	0x3308	Standard query (0)	google.vrthcobj.com	28	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 23:38:06.085091114 CEST	8.8.8.8	192.168.2.3	0x9251	No error (0)	a.goatgame.co		172.67.146.70	A (IP address)	IN (0x0001)
Aug 3, 2021 23:38:06.085091114 CEST	8.8.8.8	192.168.2.3	0x9251	No error (0)	a.goatgame.co		104.21.79.144	A (IP address)	IN (0x0001)
Aug 3, 2021 23:38:14.388151884 CEST	8.8.8.8	192.168.2.3	0xc59	No error (0)	google.vrthcobj.com		34.97.69.225	A (IP address)	IN (0x0001)

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
Aug 3, 2021 23:38:06.144718885 CEST	172.67.146.70	443	192.168.2.3	49708	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	Sun Jul 18 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Mon Jul 18 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					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

Click to jump to process

System Behavior

Analysis Process: TMB1fxNaqR.exe PID: 1740 Parent PID: 5572

General

Start time:	23:38:02
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\TMB1fxNaqR.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TMB1fxNaqR.exe'
Imagebase:	0x400000
File size:	57344 bytes
MD5 hash:	A92922A71A9BF58CC2D95A6039C9A1B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 2332 Parent PID: 1740

General

Start time:	23:38:03
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: TMB1fxNaqR.exe PID: 4704 Parent PID: 1740

General

Start time:	23:38:03

Start date:	03/08/2021
Path:	C:\Users\user\Desktop\TMB1fxNaqR.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TMB1fxNaqR.exe' -a
Imagebase:	0x400000
File size:	57344 bytes
MD5 hash:	A92922A71A9BF58CC2D95A6039C9A1B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: conhost.exe PID: 5376 Parent PID: 4704

General

Start time:	23:38:04
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis